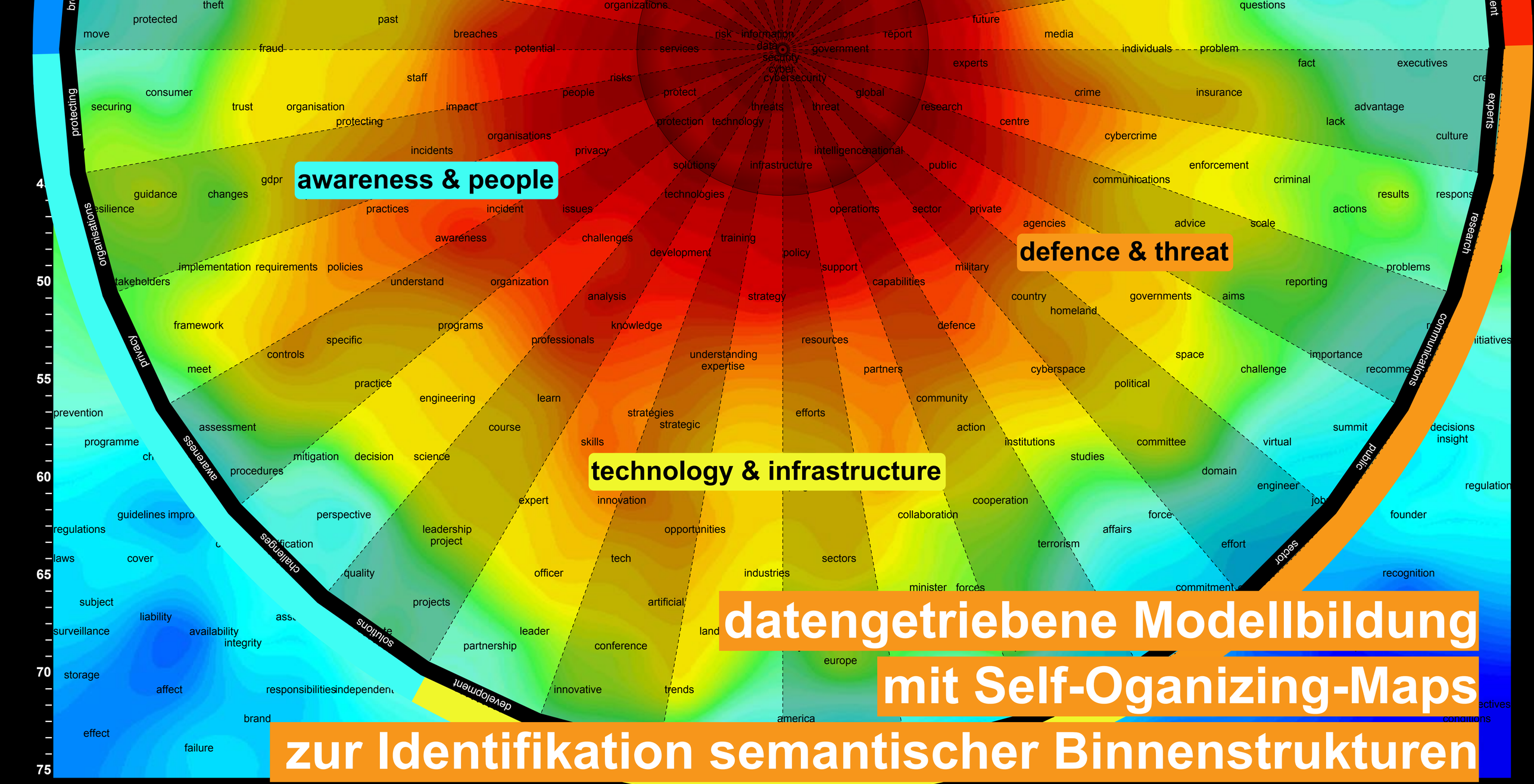
Datenmodelle zur Reduktion textlicher Komplexität mit künstlichen neuronalen Netzen

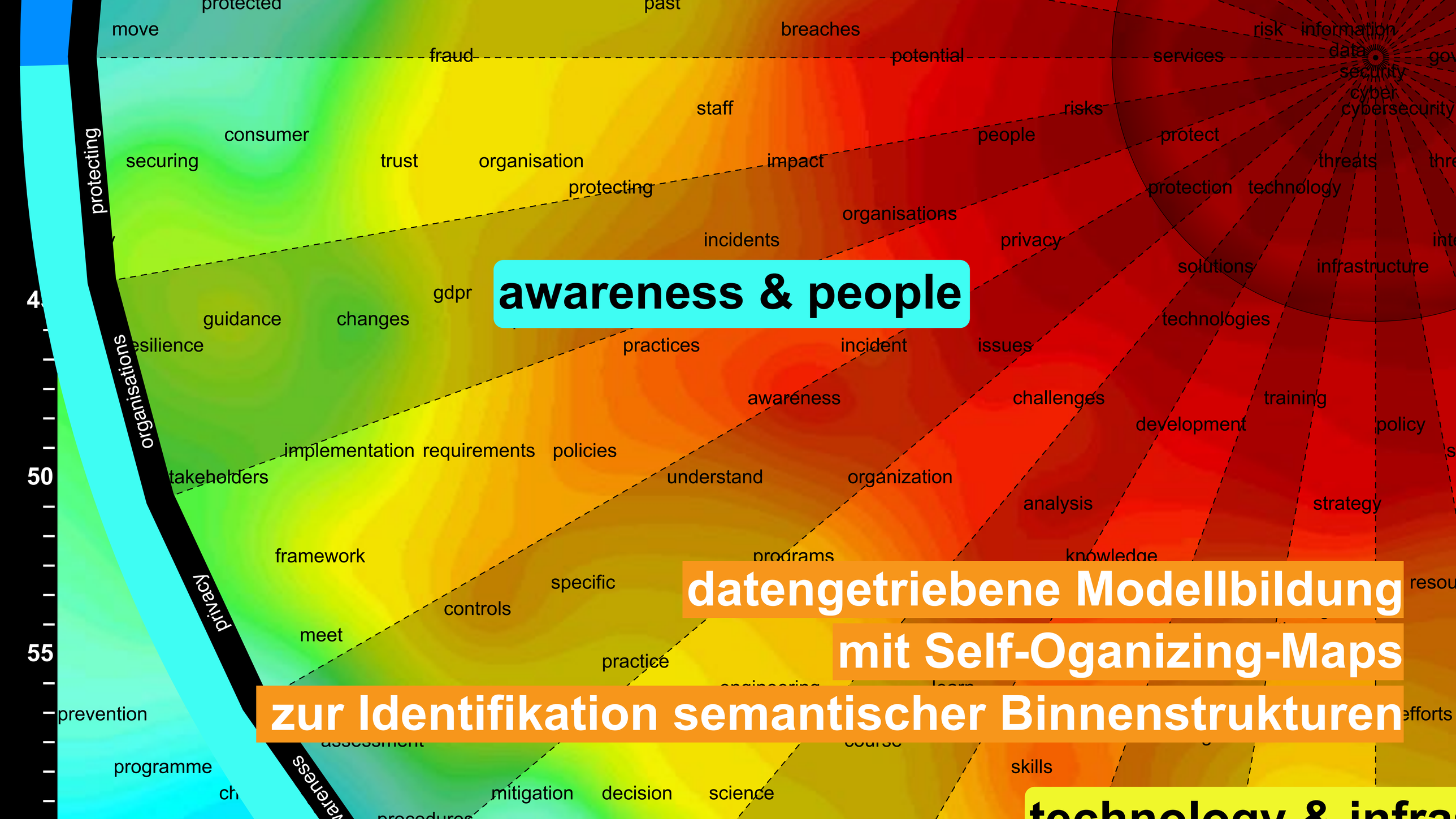
SOMTXT UG
haftungsbschränkt

Datenmodelle zur Reduktion textlicher Komplexität mit künstlichen neuronalen Netzen

Somtxt Kernkompetenz

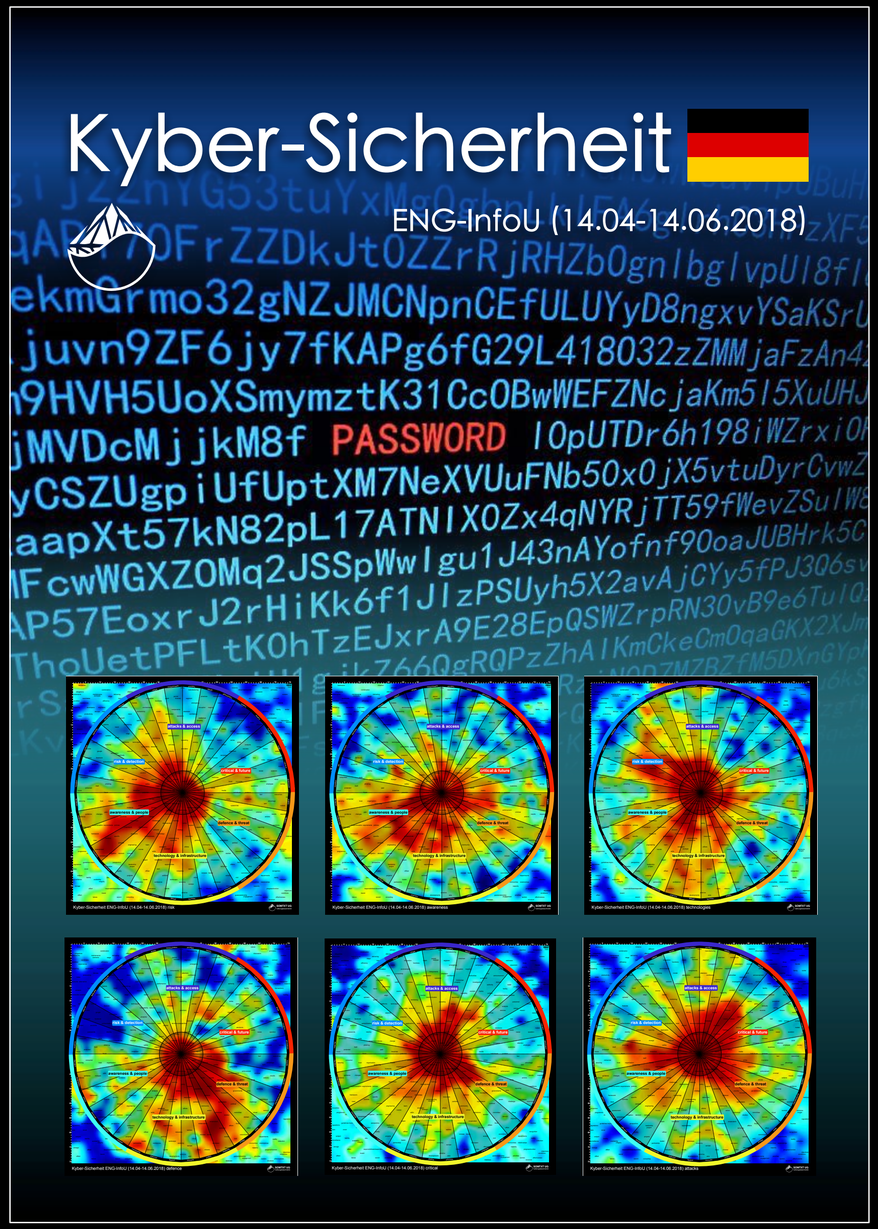
- Erzeugung von Modellen
- unterschiedliche Datenprovenienz und -modalität
- mittels künstlicher-neuronaler-Netze KNN
- ca. 500 Modelle seit 2014 trainiert


awareness & people
defence & threat
technology & infrastructure
datengetriebene Modellbildung
mit Self-Oganizing-Maps
zur Identifikation semantischer Binnenstrukturen
Kyber-Sicherheit ENG-InfoU (14.04-14.06.2018)
SOMTXT UG
haftungsbeschränkt


protected
past
move
breaches
risk
information
fraud
potential
services
data
security
cyber
cybersecurity
staff
risks
consumer
people
protect
securing
trust
organisation
impact
threats
protecting
protection
technology
organisations
incidents
privacy
awareness & people
solutions
infrastructure
gdpr
guidance
changes
technologies
practices
incident
issues
awareness
challenges
training
development
policy
implementation
requirements
policies
takeholders
understand
organization
analysis
strategy
framework
programs
knowledge
specific
controls
meet
practice
prevention
programme
skills
mitigation
decision
science
protecting
organisations
privacy
datengetriebene Modellbildung
mit Self-Oganizing-Maps
zur Identifikation semantischer Binnenstrukturen

Daten → KNN → Bereitstellung für Analyst

- unbekannten Domänen
- unstrukturierte & unkuratierte Daten
- unsupervised learning



siehe Anhang

Datenmodelle zur Erzeugung von strukturierten Exzerpten

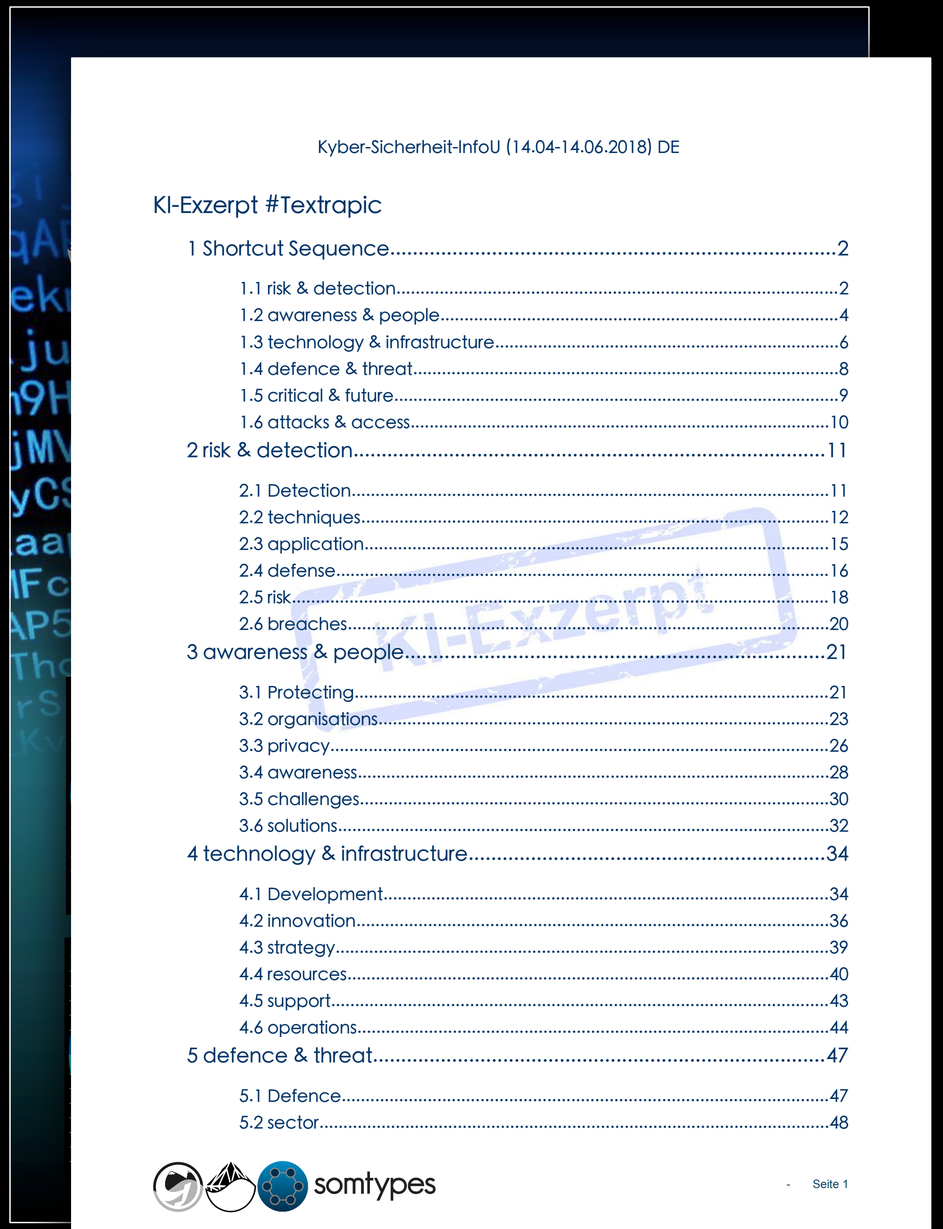
mit KNN: Reduktion textlicher Komplexität - aktiv

gegeben: inhaltlich unerschlossenes InfoU, bspw. 250.000 Quellen, nichtdeutsch

gesucht: Narrative, Indikatoren für Krisenfrüherkennung

geliefert: Filter, Animationen, KI-Exzerpt 50 Seiten - deutsch

Datenmodelle zur Erzeugung von strukturierten Exzerpten



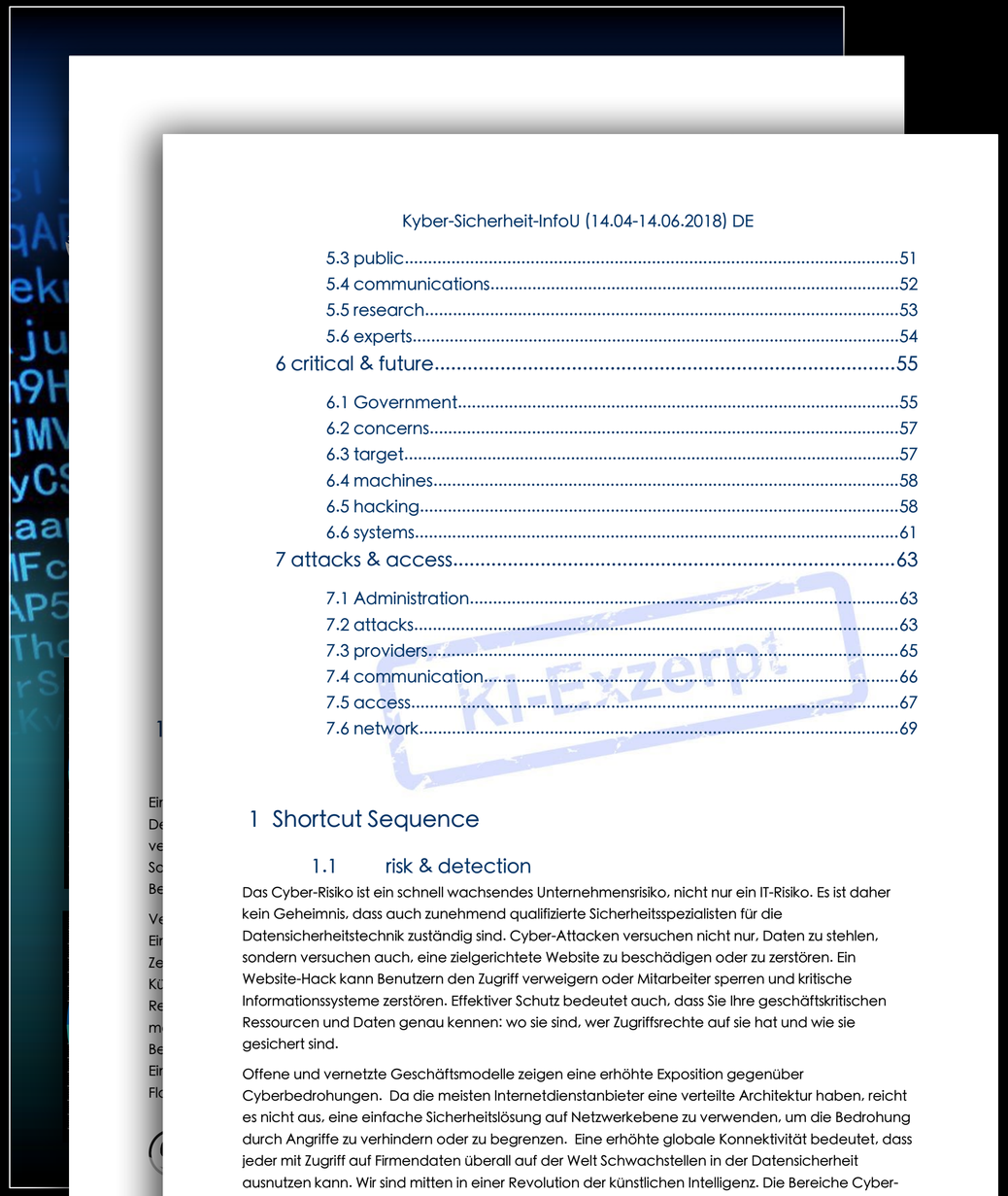
Kyber-Sicherheit-InfoU (14.04-14.06.2018) DE

KI-Exzerpt #Textrapic

somtypes

Datenmodelle zur Erzeugung von strukturierten Exzerpten

Code UniBW (11.07.2018) Künstliche-Neuronale-Netze in der operativen und strategischen Kommunikation



1 Shortcut Sequence

1.1 risk & detection

Das Cyber-Risiko ist ein schnell wachsendes Unternehmensrisiko, nicht nur ein IT-Risiko. Es ist daher kein Geheimnis, dass auch zunehmend qualifizierte Sicherheitsspezialisten für die Datensicherheitstechnik zuständig sind. Cyber-Attacken versuchen nicht nur, Daten zu stehlen, sondern versuchen auch, eine zielgerichtete Website zu beschädigen oder zu zerstören. Ein Website-Hack kann Benutzern den Zugriff verweigern oder Mitarbeiter sperren und kritische Informationssysteme zerstören. Effektiver Schutz bedeutet auch, dass Sie Ihre geschäftskritischen Ressourcen und Daten genau kennen: wo sie sind, wer Zugriffsrechte auf sie hat und wie sie gesichert sind.

Offene und vernetzte Geschäftsmodelle zeigen eine erhöhte Exposition gegenüber Cyberbedrohungen. Da die meisten Internetdienstanbieter eine verteilte Architektur haben, reicht es nicht aus, eine einfache Sicherheitslösung auf Netzwerkebene zu verwenden, um die Bedrohung durch Angriffe zu verhindern oder zu begrenzen. Eine erhöhte globale Konnektivität bedeutet, dass jeder mit Zugriff auf Firmendaten überall auf der Welt Schwachstellen in der Datensicherheit ausnutzen kann. Wir sind mitten in einer Revolution der künstlichen Intelligenz. Die Bereiche Cyber-

somtypes

Datenmodelle zur Erzeugung von strukturierten Exzerpten

Code UniBW (nd strategischen Kommunikation

Neue Medien – Bundeswehr: Monatsbericht (01.02-28.01.2018)

Kyber-Sicherheit-InfoU (14.04-14.06.2018) DE

Sicherheit und KI sind in jüngster Vergangenheit zunehmend miteinander verbunden. Bis jetzt hat sich das maschinelle Lernen beim Blockieren von Sicherheitsverletzungen als weitaus effektiver und effizienter erwiesen als die herkömmliche Sicherheitslösungen. Da Cyber-Angriffe immer häufiger und ausgefeilter werden, werden die Bereiche Big Data und KI zunehmend miteinander verbunden sein, um fortschrittlichere Lösungen zur Erkennung und Verhinderung von Bedrohungen der Informationssicherheit zu entwickeln.

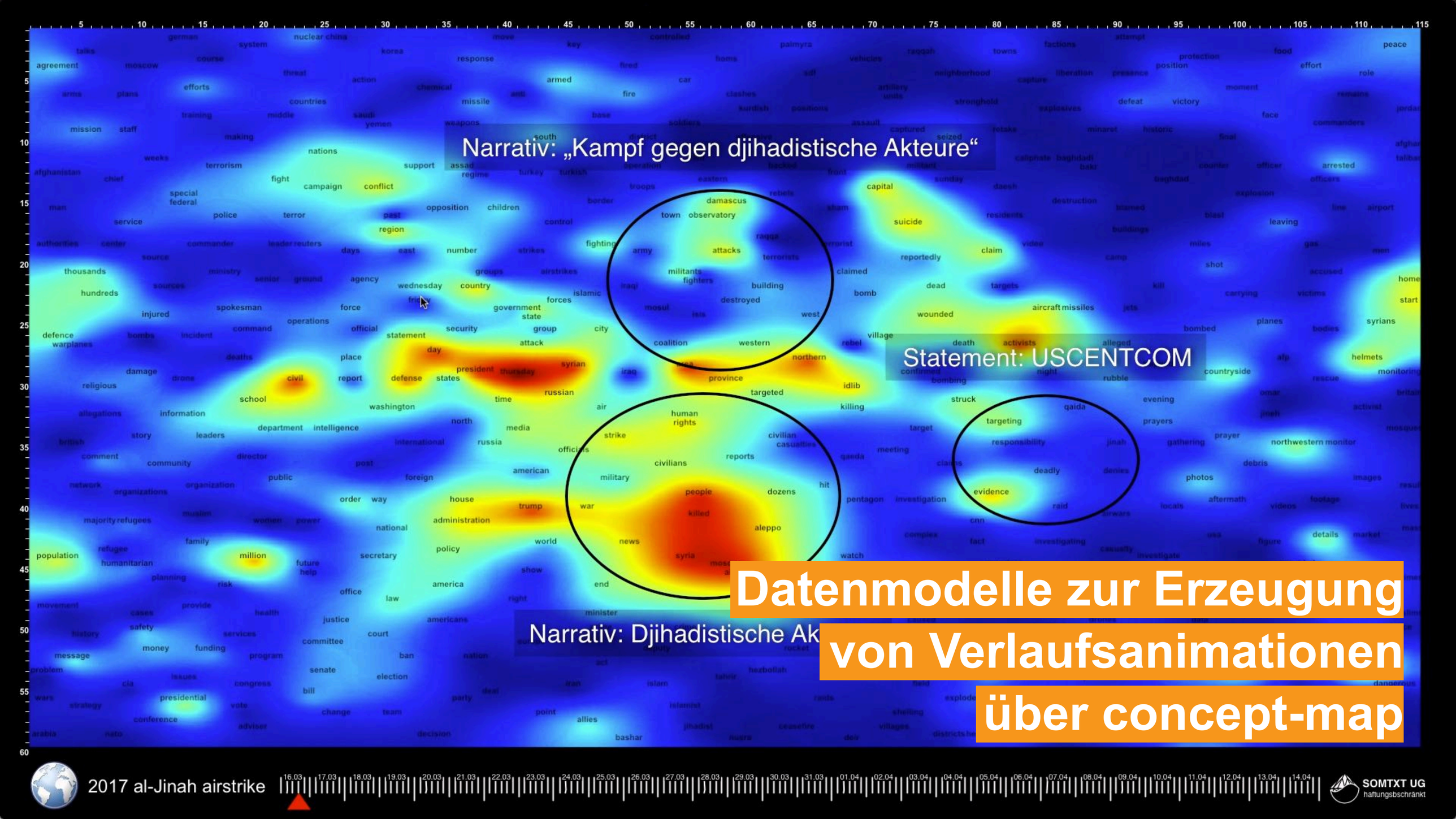
Es ist an der Zeit, die Art und Weise, wie Daten im Cyberspace gesammelt, weitergegeben und verkauft werden, gründlich zu prüfen. Yahoos britischer Arm wurde vom britischen Information Commissioner Office (ICO) wegen eines Datenmissbrauchs im Jahr 2014 mit 250.000 £ (335.000 $) belegt. Yahoo konnte nicht sicherstellen, dass ihr Datenverarbeiter die angemessenen Datenschutzstandards einhält. Google hat auch auf den Sicherheitsaspekt seiner AI-Tools und -Dienste hingewiesen. Sowohl native Android-App-Entwickler als auch iOS-App-Entwickler müssen eine Verantwortung für die Entwicklung einer Anwendung übernehmen. Datenschutzgrundsätze werden auch in die Entwicklung und den Einsatz von KI-Technologien einfließen müssen.

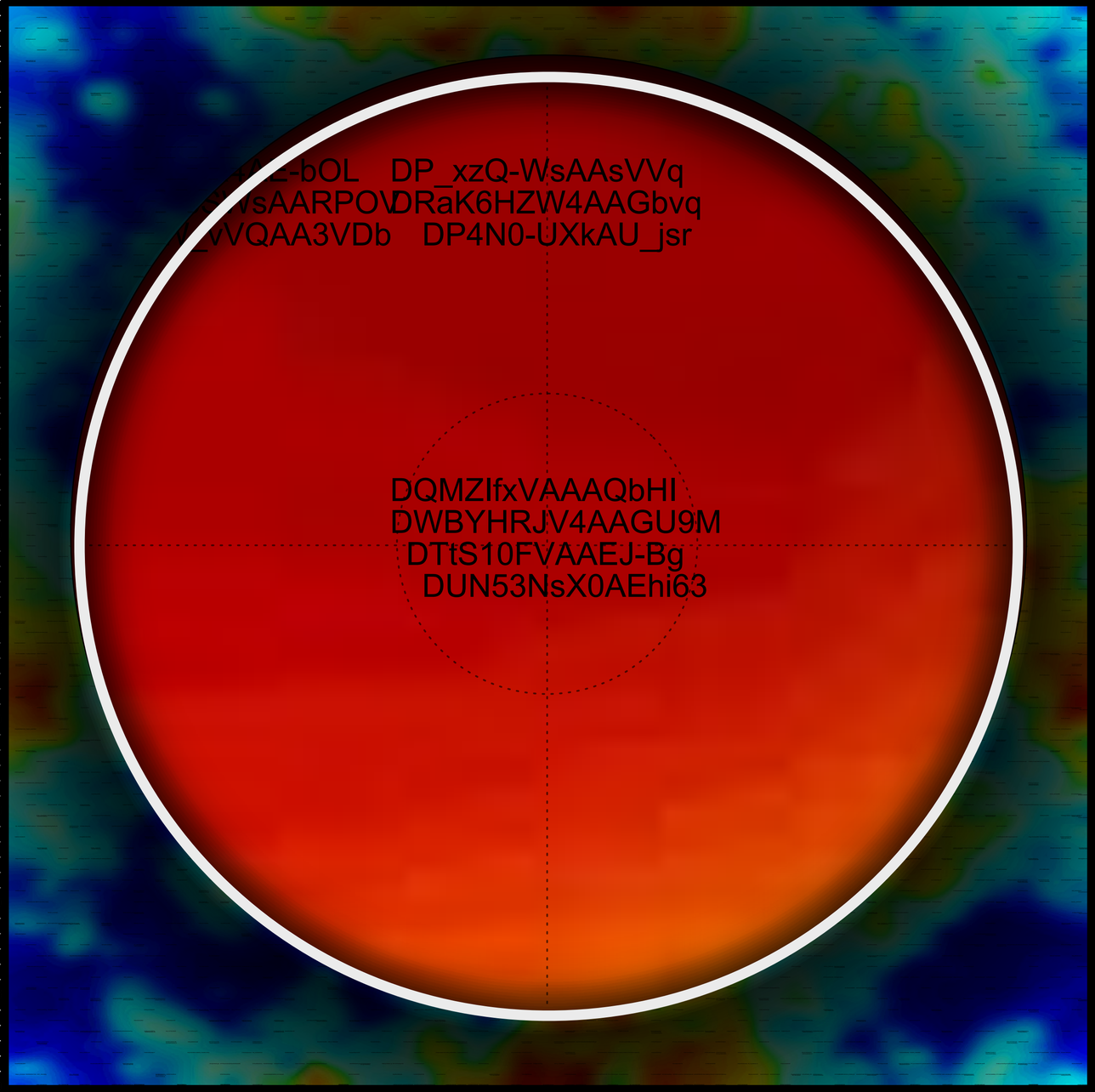
Die Nachfrage nach fortschrittlichen Analysetools und Analyseanwendungen nimmt rapide zu. Da täglich neue Bedrohungen auftreten und Angreifer ihre Techniken kontinuierlich verfeinern, könnte es schwierig sein, mitzuhalten. Eine Kombination aus menschlicher Intuition und der Verarbeitungsfähigkeiten von Computern bietet die Möglichkeit, die Zeit zwischen Bedrohungserkennung und -antwort zu verkürzen. Eine digitale Forensik braucht Methoden zur Erkennung von Cyberbedrohungen, um intelligente Systeme zur Bekämpfung von Cyberkriminalität zu entwickeln. Threat Intelligence Platforms (TIP) fassen Bedrohungsdaten zusammen und ermöglichen maßgeschneiderte Aufklärung und Analyse Maßnahmen . Dark Web Intelligence liefert wichtige Einblicke in die Cybersicherheit und Bedrohungsdaten und bleibt ein Schlüsselelement für effektive Automatisierungslösungen in der Cyber-Sicherheitsbranche.

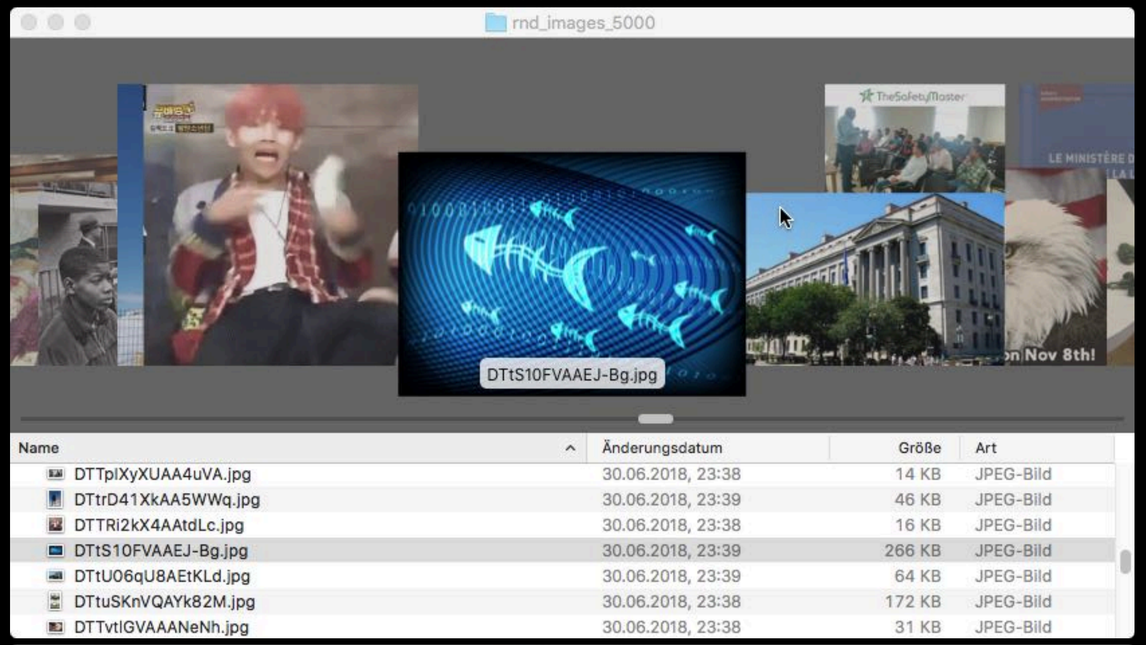
Unternehmen und Regierungsbehörden müssen mehr Infrastruktur entwickeln, um den sich ständig ändernden Bedrohungen gewachsen zu sein. Regierungsorganisationen können nicht länger nur auf Bedrohungen reagieren, sondern müssen eine Infrastruktur schaffen, die agil und anpassungsfähig ist, das Verstöße behoben werden, bevor sie auftreten. Da sich Regierungsbehörden bei der täglichen Arbeit häufig auf Informationstechnologie-Systeme und Computernetzwerke verlassen, kann ein systemweiter Ausfall die Funktionalität einer Organisation erheblich beeinträchtigen. Mehr als sieben von zehn großen Wohltätigkeitsorganisationen sind im vergangenen Jahr Opfer von Cyberangriffen oder -verstößen geworden, wie neue Untersuchungen der Abteilung für Digitales, Kultur, Medien und Sport ergeben haben. Ein auf der Untersuchung beruhender Bericht, die Cyber Security Breaches Survey 2018, ergab, dass 73 Prozent der Wohltätigkeitsorganisationen mit einem Jahreseinkommen von mehr als 5 Millionen Pfund, die an der Umfrage teilnahmen, im vergangenen Jahr Opfer von Cyberangriffen wurden.

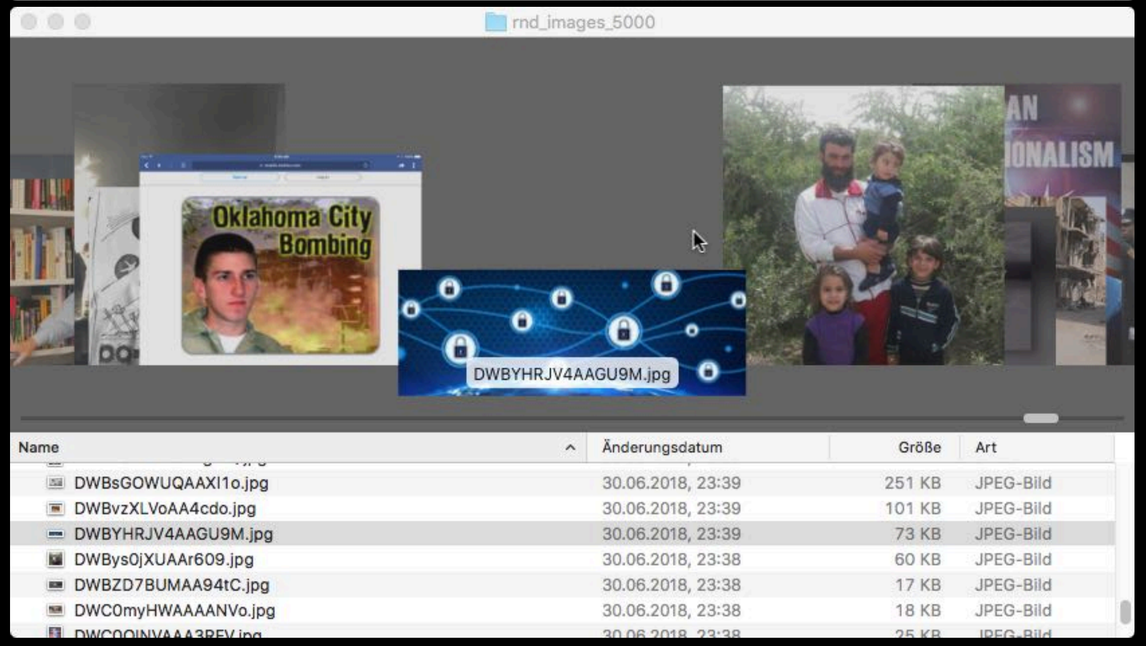
Der National Exposure Index, der am Donnerstag von Rapid7 veröffentlicht wurde, bewertet die USA zuerst und China als die Länder mit der größten Exposition gegenüber möglichen Angriffen, der durchdringenden Überwachung und dem Missbrauch durch Amplifikation. Bei einer Reihe von chinesischen Verbrauchern, die eine Datenschutzverletzung durch mobile Geräte erlitten haben, ist Cyber-Sicherheit ein wichtiges Anliegen. Rapid7 ist ein führender Anbieter von Sicherheitsdaten- und -analyse-Lösungen, mit denen Unternehmen einen aktiven, analysegesteuerten Ansatz für die

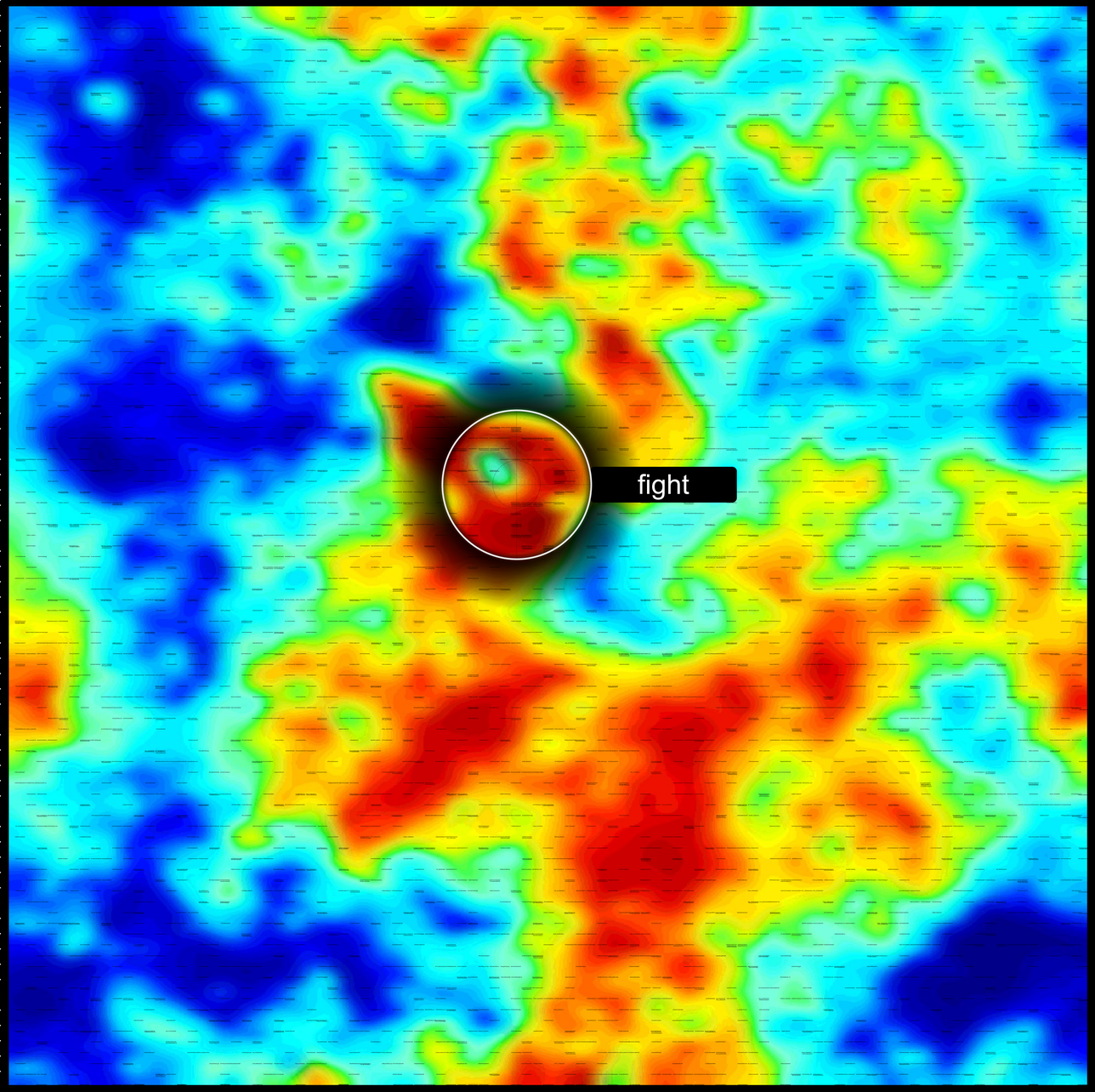
Datenmodelle zur Erzeugung von strukturierten Exzerpten

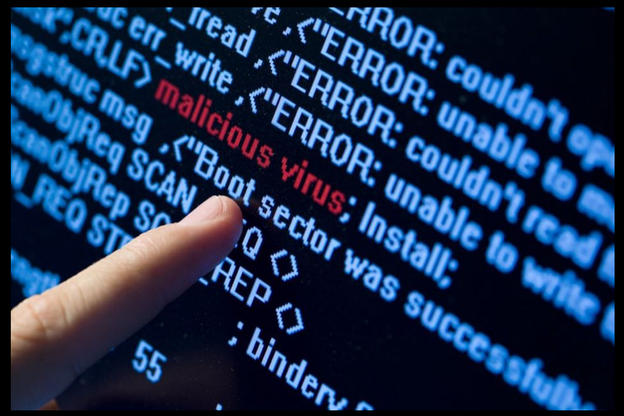

Narrativ: „Kampf gegen djihadistische Akteure“
Statement: USCENTCOM
Narrativ: Djihadistische Ak
Datenmodelle zur Erzeugung
von Verlaufsanimationen
über concept-map
2017 al-Jinah airstrike
SOMTXT UG
haftungsbeschränkt

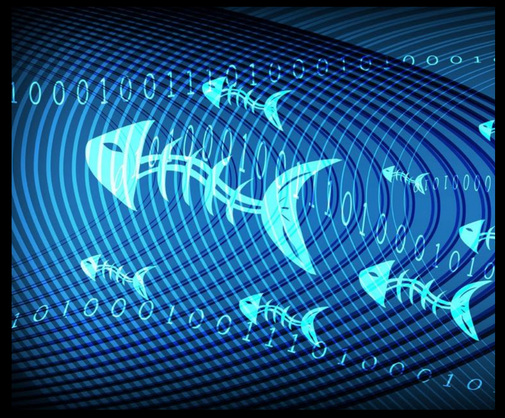












Code UniBW (11.07.2018) Künstliche-Neuronale-Netze in der operativen und strategischen Kommunikation: Bilderkennung und inhaltsgetriebene Sortierung

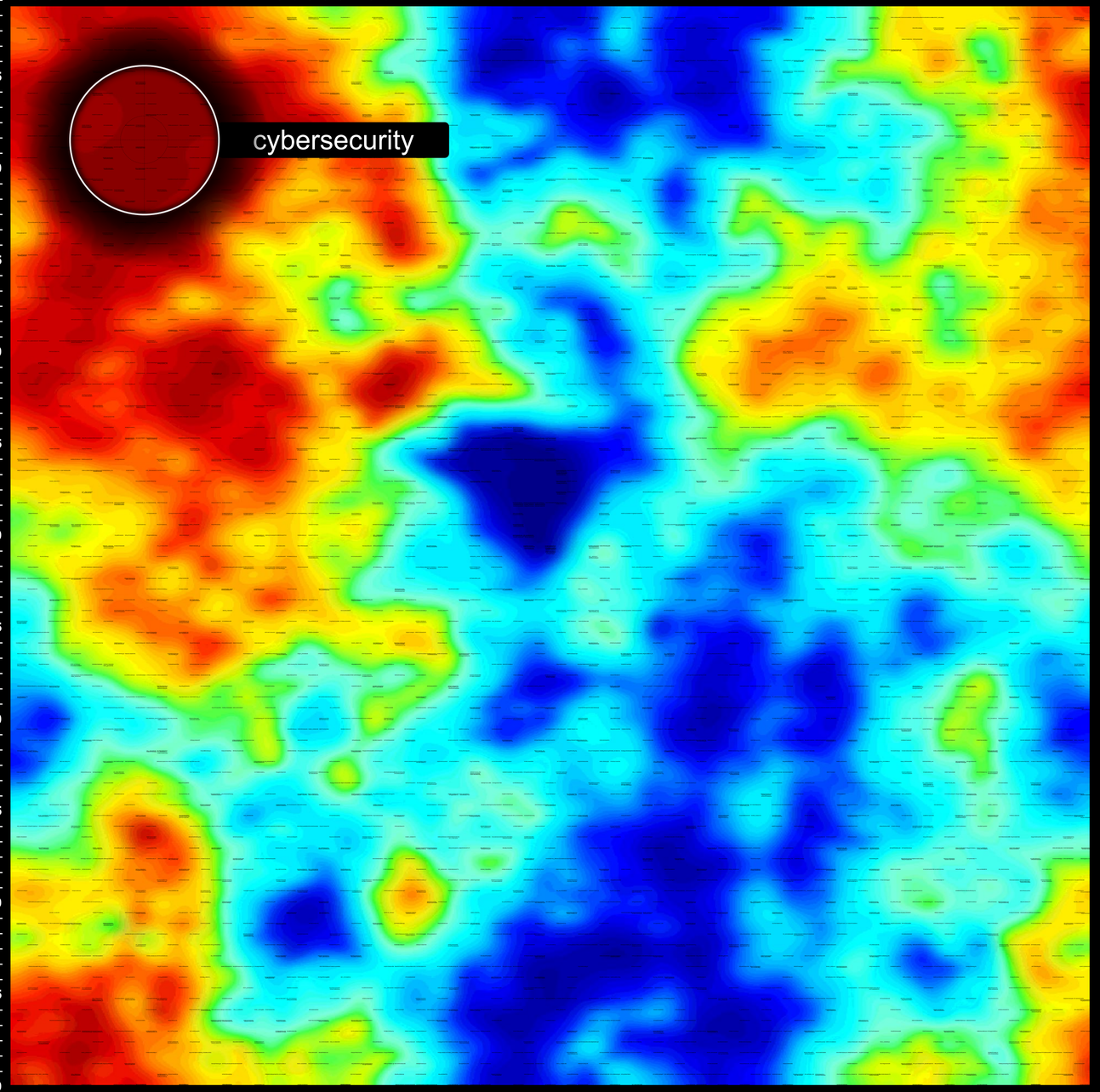
SOMTXT UG
haftungsbschränkt

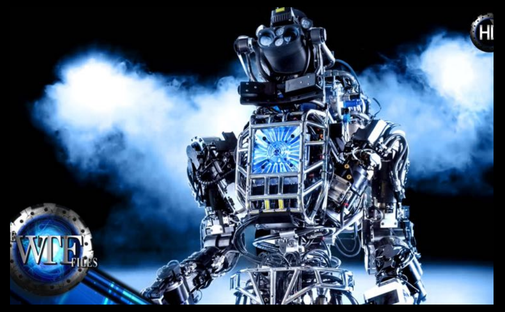
mit KNN: Bilderkennung und inhaltsgetriebene Sortierung - aktiv

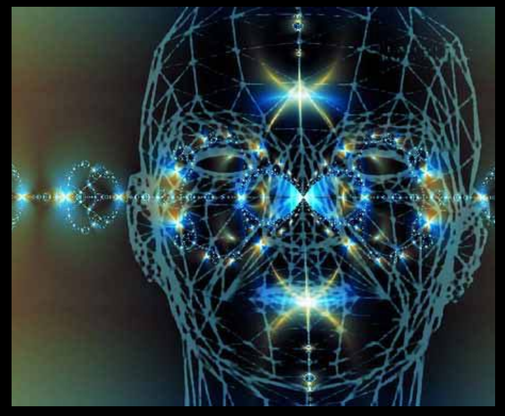
gegeben: bildlich unerschlossenes InfoU, bspw. 50.000 Bilder aus Twitter

gesucht: Bilderkennung (Tensorflow) und -aufstellung (Textrapic)

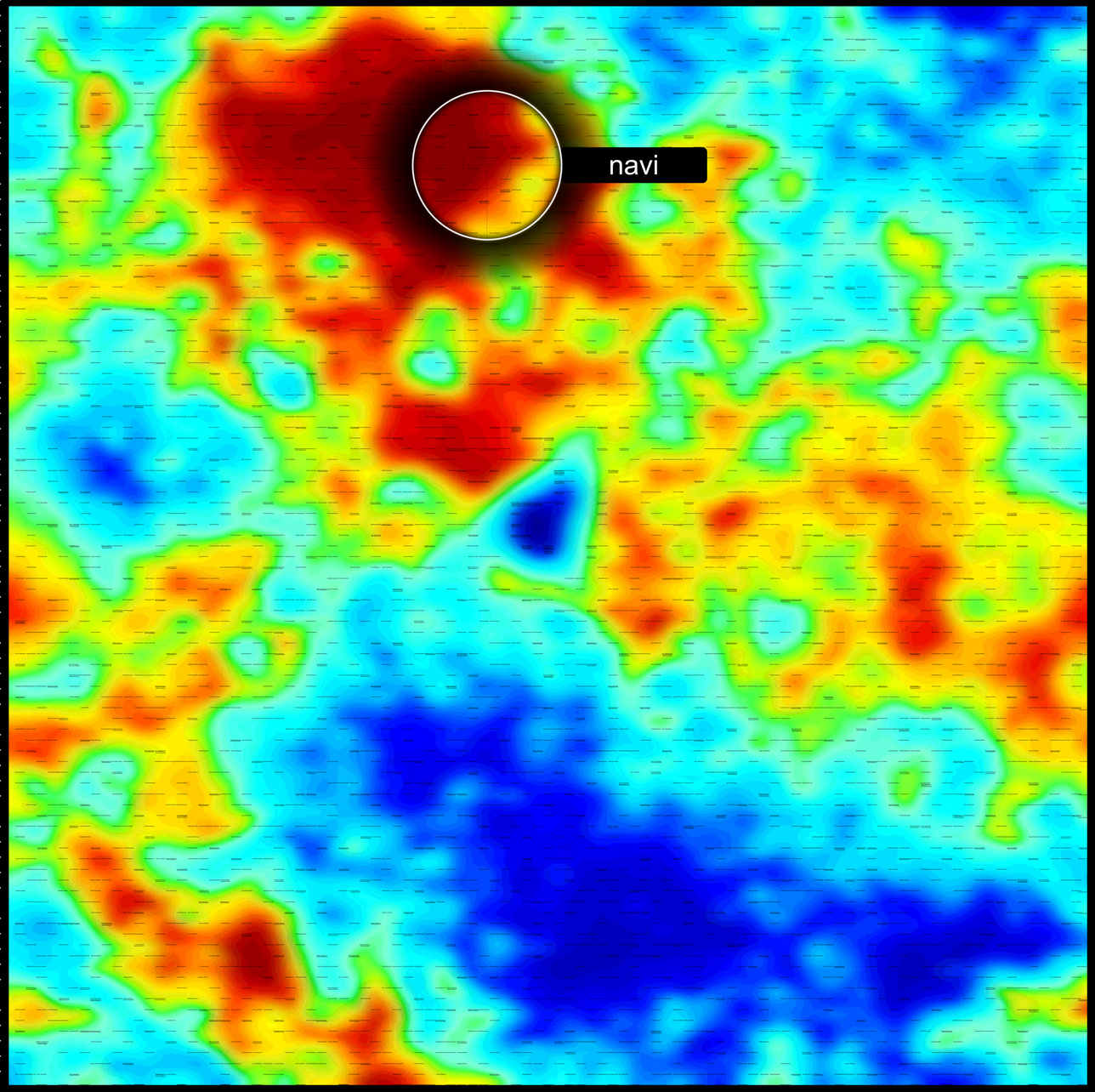
geliefert: semantische Collage





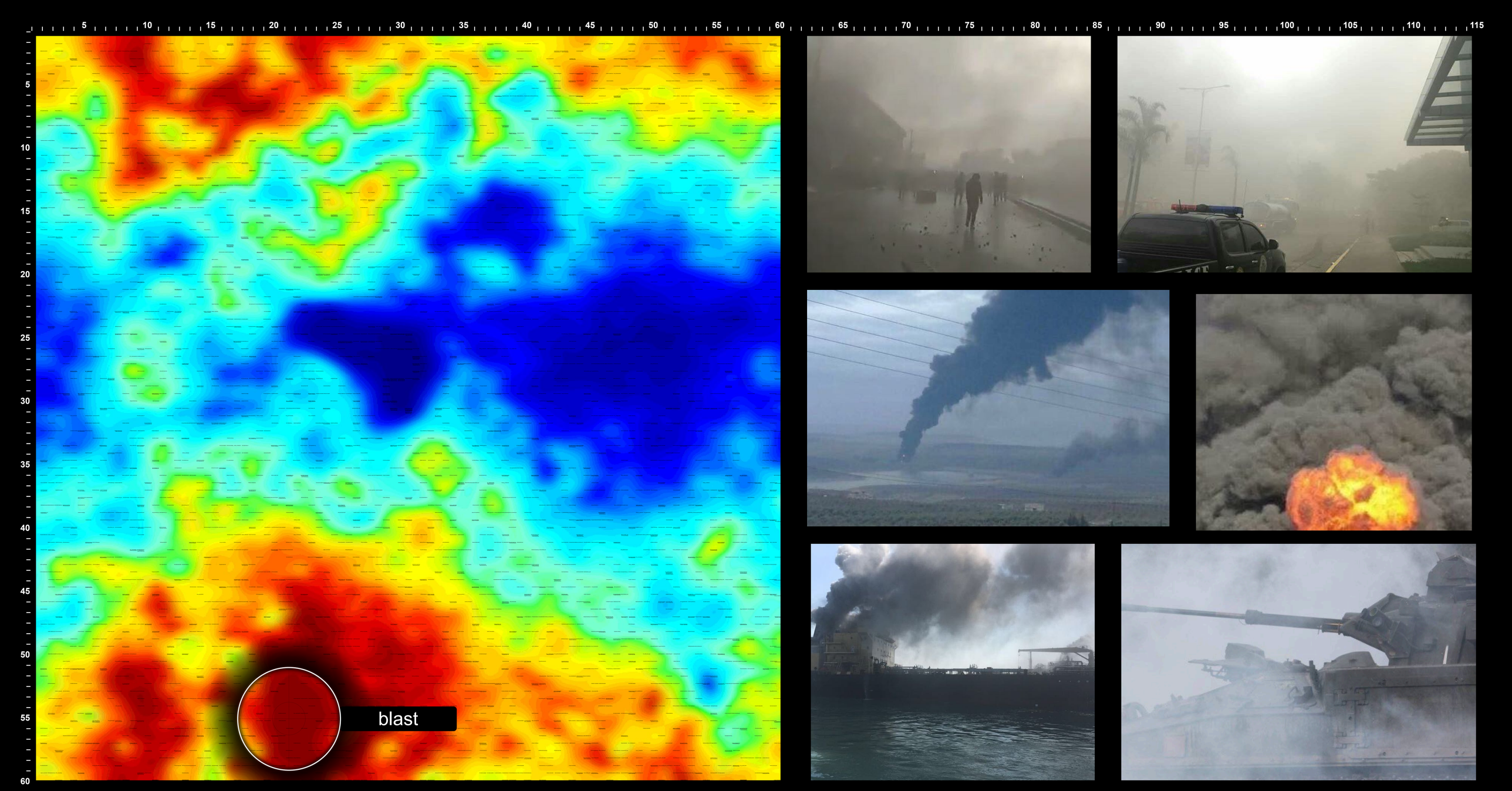


Code UniBW (11.07.2018) Künstliche-Neuronale-Netze in der operativen und strategischen Kommunikation: Bilderkennung und inhaltsgetriebene Sortierung

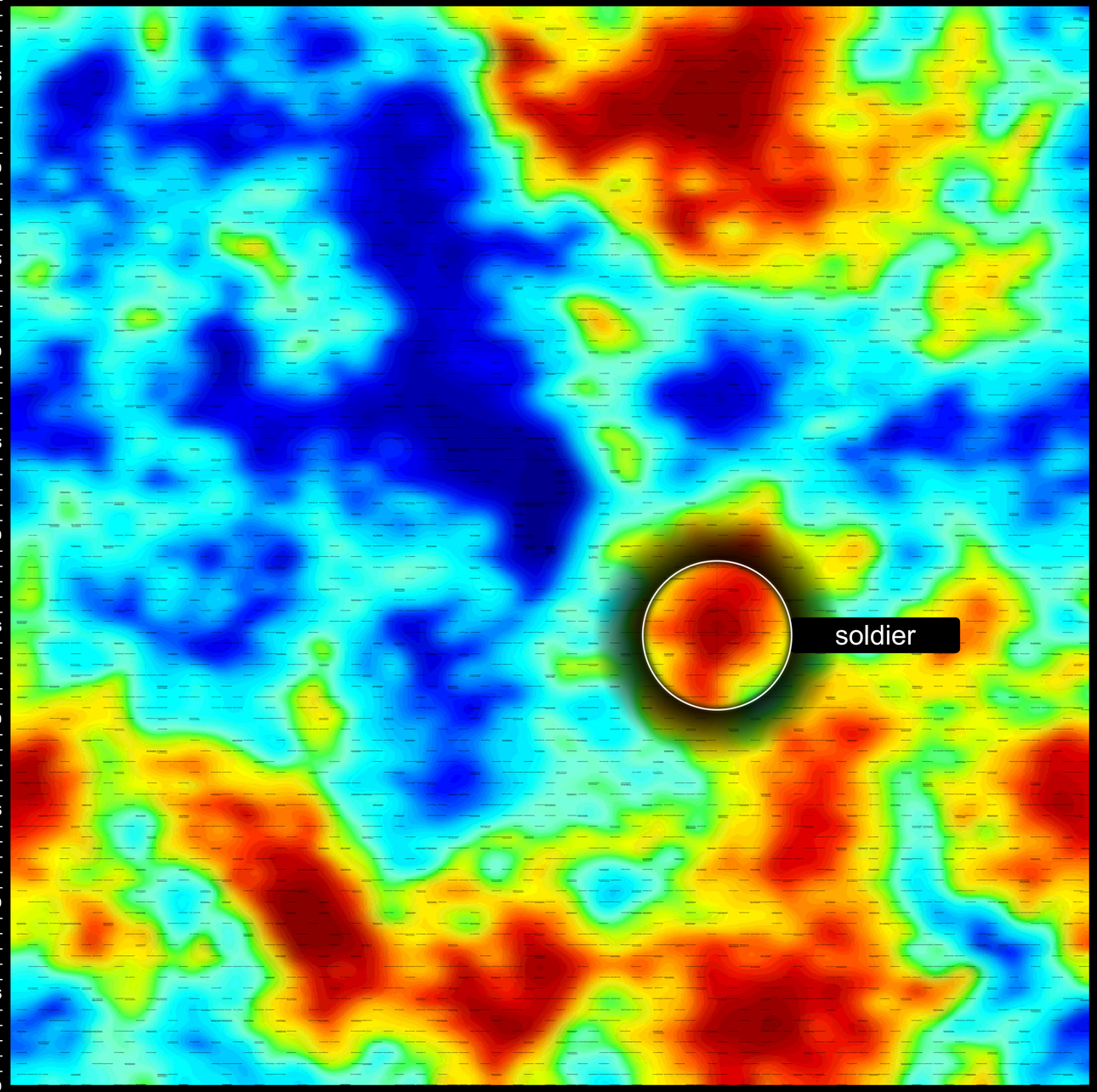


Code UniBW (11.07.2018) Künstliche-Neuronale-Netze in der operativen und strategischen Kommunikation: Bilderkennung und inhaltsgetriebene Sortierung

SOMTXT UG
haftungsbschränkt



Code UniBW (11.07.2018) Künstliche-Neuronale-Netze in der operativen und strategischen Kommunikation: Bilderkennung und inhaltsgetriebene Sortierung



Code UniBW (11.07.2018) Künstliche-Neuronale-Netze in der operativen und strategischen Kommunikation: Bilderkennung und inhaltsgetriebene Sortierung

mit KNN: Infiltrationsdetektion in Cloud Sandbox - explorativ (Invisible Cyber Attack)

gegeben: Sandbox mit Projektverwaltung, Dokumentenbearbeitung, EPK T3CQ

gesucht: Früherkennung von Identitätsdiebstahl und Systemkompromittierung

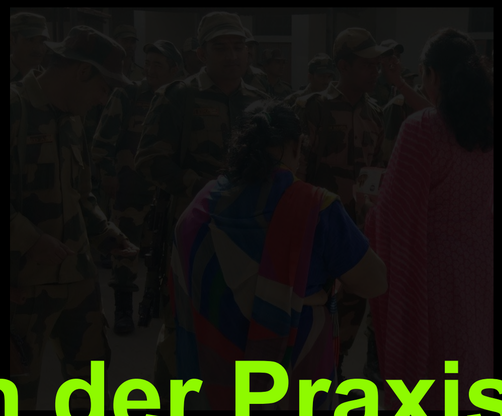
geliefert: Monitoring, Alert & Sperrung - Blockchain Anbindung

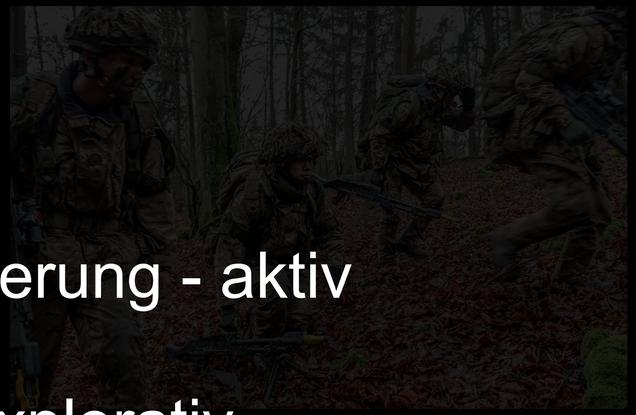
Zusammenfassung: KNN in der Praxis

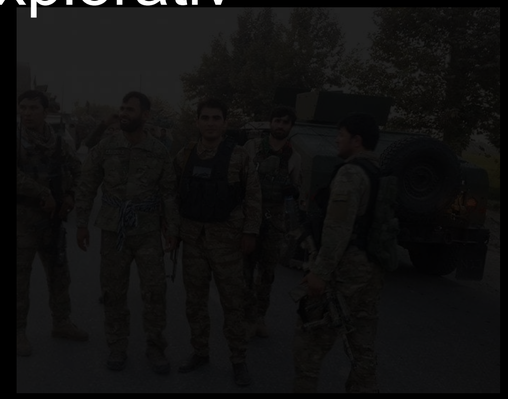
- Reduktion textlicher Komplexität - aktiv

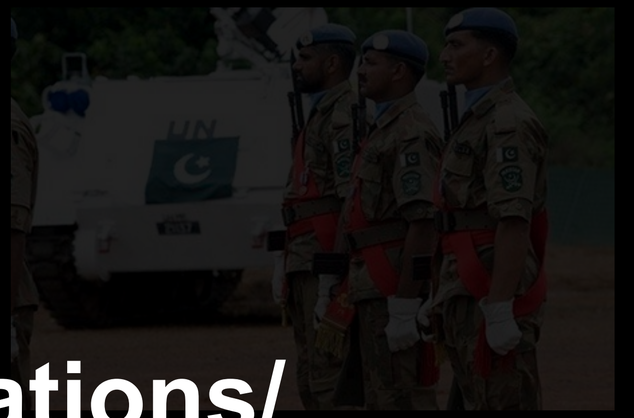
- Bilderkennung und inhaltsgetriebene Sortierung - aktiv

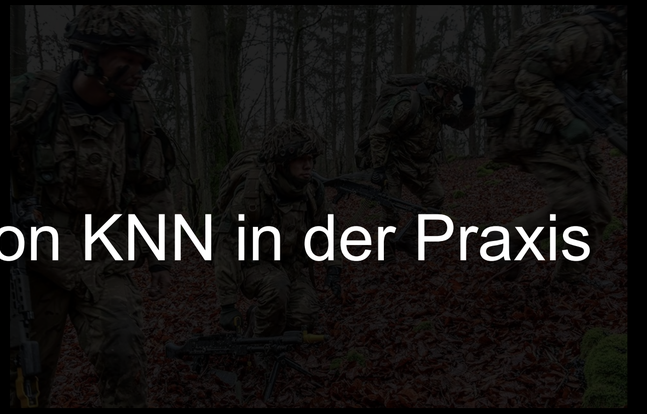
- Infiltrationsdetektion in Cloud Sandbox - explorativ
  (Invisible Cyber Attack)

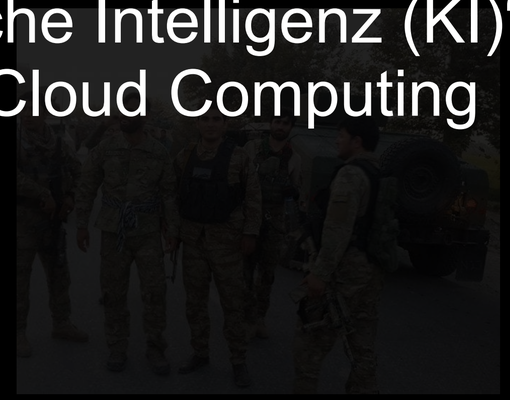










Meet the Speakers Military Communications/ Command & Control/

geboten: Erklärungen zu Somtxt Nutzung von KNN in der Praxis

gesucht: Austausch zu:

1) F&T-Vorhaben „Künstliche Intelligenz (KI)“
2) Infiltrationsdetektion in Cloud Computing
3) neuen Paradigmen

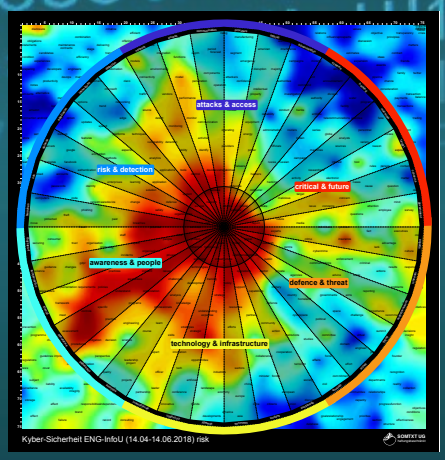
Vielen Dank

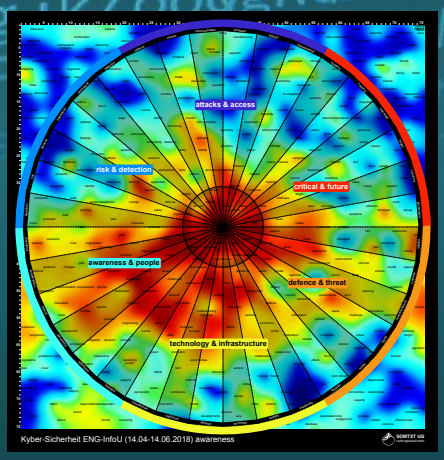
Dipl. Päd. Stefan Pforte
Geschäftsführer Somtxt UG
Brahmsstrasse 36
18069 Rostock

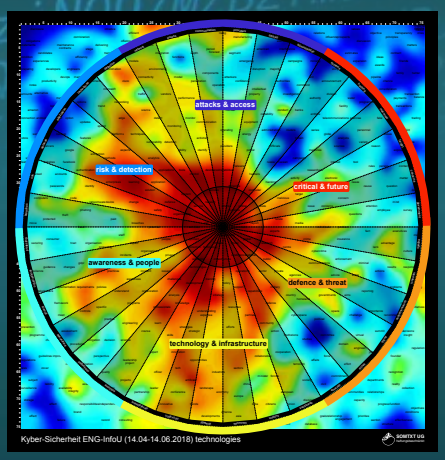
twitter: @vanforte

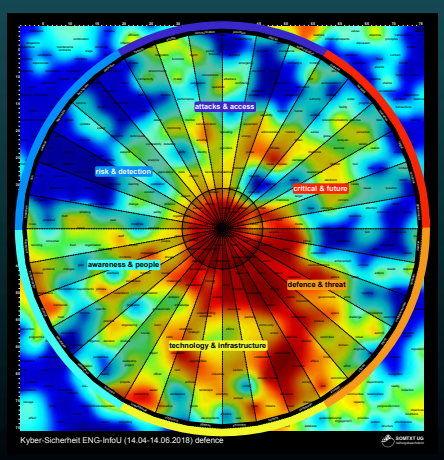
Kyber-Sicherheit

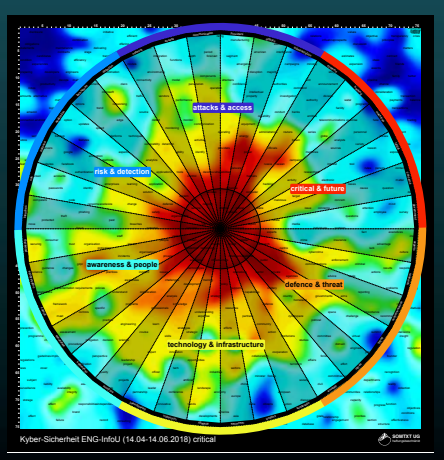
ENG-InfoU (14.04-14.06.2018)

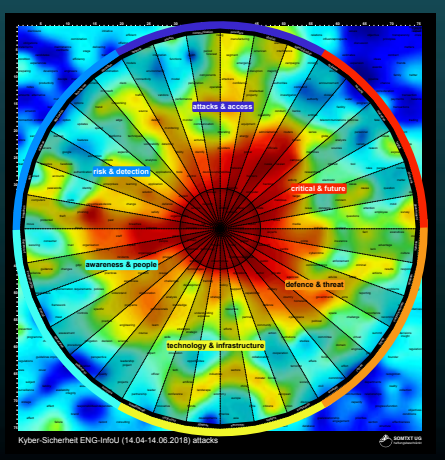


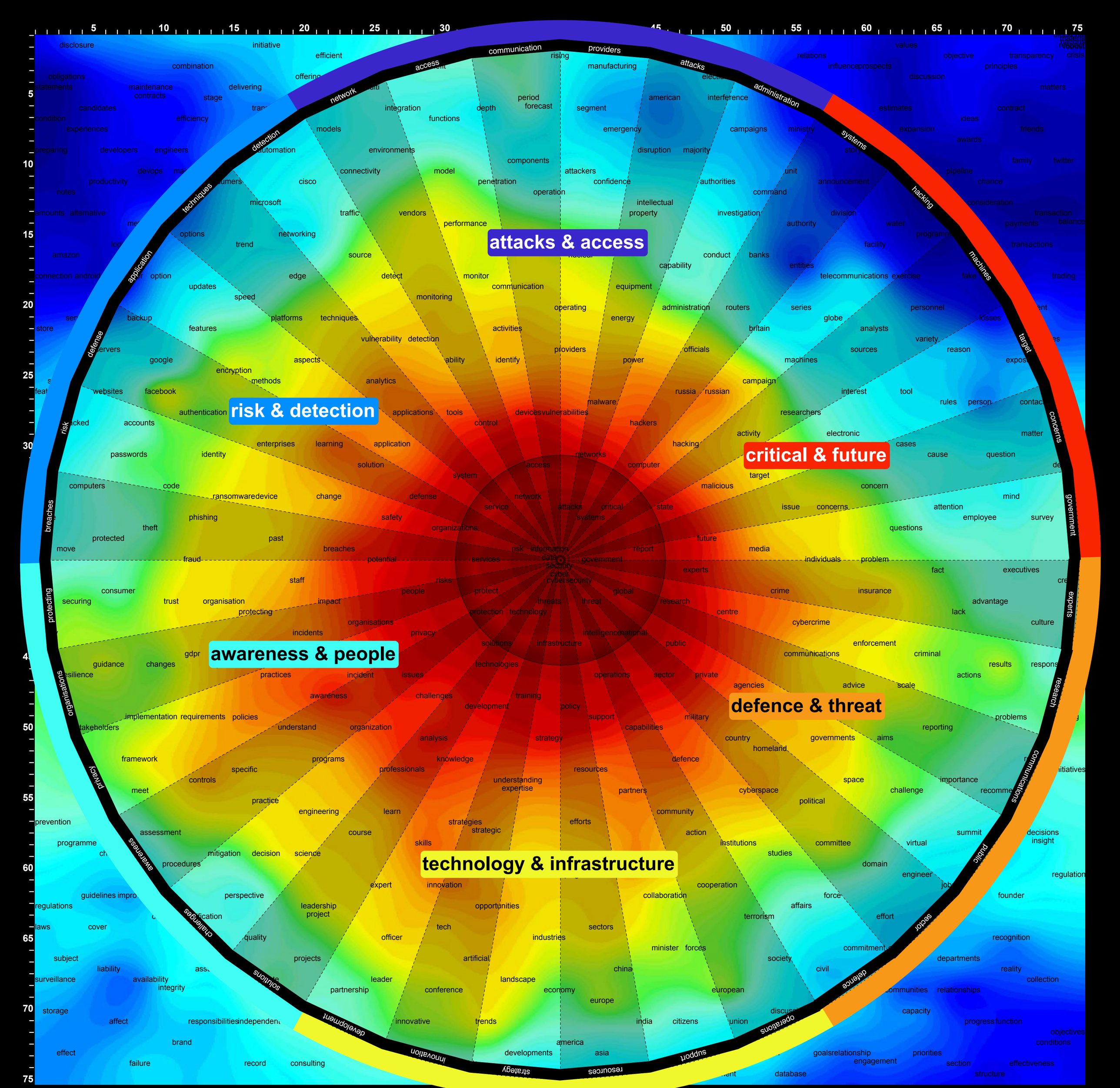












Kyber-Sicherheit ENG-InfoU (14.04-14.06.2018)

SOMTXT UG
haftungsbeschränkt

KI-Exzerpt #Textrapic

1 Shortcut Sequence

1.1 risk & detection

Das Cyber-Risiko ist ein schnell wachsendes Unternehmensrisiko, nicht nur ein IT-Risiko. Es ist daher kein Geheimnis, dass auch zunehmend qualifizierte Sicherheitsspezialisten für die Datensicherheitstechnik zuständig sind. Cyber-Attacken versuchen nicht nur, Daten zu stehlen, sondern versuchen auch, eine zielgerichtete Website zu beschädigen oder zu zerstören. Ein Website-Hack kann Benutzern den Zugriff verweigern oder Mitarbeiter sperren und kritische Informationssysteme zerstören. Effektiver Schutz bedeutet auch, dass Sie Ihre geschäftskritischen Ressourcen und Daten genau kennen: wo sie sind, wer Zugriffsrechte auf sie hat und wie sie gesichert sind.

Offene und vernetzte Geschäftsmodelle zeigen eine erhöhte Exposition gegenüber Cyberbedrohungen. Da die meisten Internetdienstanbieter eine verteilte Architektur haben, reicht es nicht aus, eine einfache Sicherheitslösung auf Netzwerkebene zu verwenden, um die Bedrohung durch Angriffe zu verhindern oder zu begrenzen. Eine erhöhte globale Konnektivität bedeutet, dass jeder mit Zugriff auf Firmendaten überall auf der Welt Schwachstellen in der Datensicherheit ausnutzen kann. Wir sind mitten in einer Revolution der künstlichen Intelligenz. Die Bereiche Cyber-

Kyber-Sicherheit-InfoU (14.04-14.06.2018) DE

Sicherheit und KI sind in jüngster Vergangenheit zunehmend miteinander verbunden. Bis jetzt hat sich das maschinelle Lernen beim Blockieren von Sicherheitsverletzungen als weitaus effektiver und effizienter erwiesen als die herkömmliche Sicherheitslösungen. Da Cyber-Angriffe immer häufiger und ausgefeilter werden, werden die Bereiche Big Data und KI zunehmend miteinander verbunden sein, um fortschrittlichere Lösungen zur Erkennung und Verhinderung von Bedrohungen der Informationssicherheit zu entwickeln.

Es ist an der Zeit, die Art und Weise, wie Daten im Cyberspace gesammelt, weitergegeben und verkauft werden, gründlich zu prüfen. Yahoos britischer Arm wurde vom britischen Information Commissioner Office (ICO) wegen eines Datenmissbrauchs im Jahr 2014 mit 250.000 £ (335.000 $) belegt. Yahoo konnte nicht sicherstellen, dass ihr Datenverarbeiter die angemessenen Datenschutzstandards einhält. Google hat auch auf den Sicherheitsaspekt seiner AI-Tools und -Dienste hingewiesen. Sowohl native Android-App-Entwickler als auch iOS-App-Entwickler müssen eine Verantwortung für die Entwicklung einer Anwendung übernehmen. Datenschutzgrundsätze werden auch in die Entwicklung und den Einsatz von KI-Technologien einfließen müssen.

Die Nachfrage nach fortschrittlichen Analysetools und Analyseanwendungen nimmt rapide zu. Da täglich neue Bedrohungen auftreten und Angreifer ihre Techniken kontinuierlich verfeinern, könnte es schwierig sein, mitzuhalten. Eine Kombination aus menschlicher Intuition und der Verarbeitungsfähigkeiten von Computern bietet die Möglichkeit, die Zeit zwischen Bedrohungserkennung und -antwort zu verkürzen. Eine digitale Forensik braucht Methoden zur Erkennung von Cyberbedrohungen, um intelligente Systeme zur Bekämpfung von Cyberkriminalität zu entwickeln. Threat Intelligence Platforms (TIP) fassen Bedrohungsdaten zusammen und ermöglichen maßgeschneiderte Aufklärung und Analyse Maßnahmen . Dark Web Intelligence liefert wichtige Einblicke in die Cybersicherheit und Bedrohungsdaten und bleibt ein Schlüsselelement für effektive Automatisierungslösungen in der Cyber-Sicherheitsbranche.

Unternehmen und Regierungsbehörden müssen mehr Infrastruktur entwickeln, um den sich ständig ändernden Bedrohungen gewachsen zu sein. Regierungsorganisationen können nicht länger nur auf Bedrohungen reagieren, sondern müssen eine Infrastruktur schaffen, die agil und anpassungsfähig ist, das Verstöße behoben werden, bevor sie auftreten. Da sich Regierungsbehörden bei der täglichen Arbeit häufig auf Informationstechnologie-Systeme und Computernetzwerke verlassen, kann ein systemweiter Ausfall die Funktionalität einer Organisation erheblich beeinträchtigen. Mehr als sieben von zehn großen Wohltätigkeitsorganisationen sind im vergangenen Jahr Opfer von Cyberangriffen oder -verstößen geworden, wie neue Untersuchungen der Abteilung für Digitales, Kultur, Medien und Sport ergeben haben. Ein auf der Untersuchung beruhender Bericht, die Cyber Security Breaches Survey 2018, ergab, dass 73 Prozent der Wohltätigkeitsorganisationen mit einem Jahreseinkommen von mehr als 5 Millionen Pfund, die an der Umfrage teilnahmen, im vergangenen Jahr Opfer von Cyberangriffen wurden.

Der National Exposure Index, der am Donnerstag von Rapid7 veröffentlicht wurde, bewertet die USA zuerst und China als die Länder mit der größten Exposition gegenüber möglichen Angriffen, der durchdringenden Überwachung und dem Missbrauch durch Amplifikation. Bei einer Reihe von chinesischen Verbrauchern, die eine Datenschutzverletzung durch mobile Geräte erlitten haben, ist Cyber-Sicherheit ein wichtiges Anliegen. Rapid7 ist ein führender Anbieter von Sicherheitsdaten- und -analyse-Lösungen, mit denen Unternehmen einen aktiven, analysegesteuerten Ansatz für die

Cyber-Sicherheit implementieren können. Kanada rangiert an dritter Stelle auf einer Liste der schlechtesten Länder, deren Organisationen und Benutzer ungesicherte Internetdienste haben, die für Cyberangriffe offen sind. Georgiens Außenminister Brian Kemp hat erklärt, dass umfangreiche Sicherheitsmaßnahmen und Cyber-Verteidigungs-Upgrades das derzeitige System des Staates verlässlich machen. Zum Schutz des parlamentarischen Computernetzwerks Australiens werden sieben Mitarbeiter in einem 9 Millionen Dollar teuren Cyber-Sicherheits-Operationszentrum für das Parlament arbeiten. Die britische Regierung hat sich verpflichtet, Großbritannien zum sichersten Ort zu machen, an dem man online leben und Geschäfte machen kann. Die Malabo-Konvention ist der erste Schritt zur Entwicklung nationaler Rechtsrahmen für Cybersicherheit und Datenschutz in Afrika. Vizepräsident, Premierminister und Herrscher von Dubai zielt mit Schulungsprogramm darauf ab, Regierungsangestellte mit Schlüsselkompetenzen zu befähigen, um von AI und ihren Anwendungen zu profitieren.

1.2 awareness & people

Das Bewusstsein muss wachsen, um den Menschen zu verdeutlichen, wie wichtig es ist, Daten sicher zu sichern und zu schützen. Künstliche Intelligenz benötigt Daten, um zu funktionieren, während Datenschutz- und Cybersicherheitsrahmen versuchen, die Verwendung dieser Daten zum Schutz von Individuen zu gestalten. Ein Großteil des internationalen Fokus lag auf den Vorbereitungen für die Umsetzung der EU-DSGVO im Mai 2018. Die APAC-Region ist aus mehreren Gründen bemerkenswert, darunter Chinas laufende Umsetzung seines Cyber-Sicherheitsgesetzes, die Verschärfung der Datenschutzgesetze in Japan und Australien sowie ein allgemeiner Trend zu einer strengeren Durchsetzung und einer stärkeren Sensibilisierung der Öffentlichkeit für ihre Datenrechte Schutzgesetze. Cyber-Sicherheit und die Sorge um mögliche Fehlinformationskampagnen während der Wahlen stehen auch vor den Europawahlen 2019 ganz im Vordergrund.

Bedrohungsintelligenz ist eine Cyber-Sicherheitsdisziplin, die das Verständnis komplexer Cyberbedrohungen und deren Erkennung, Analyse und vorhersehbare Behebung sucht. Threat Intelligence-Lösungen bieten eine effektive und zuverlässige Erkennung von Bedrohungen, um Cyberbedrohungen aufgrund von Sicherheitsereignissen und Sicherheitsinformationen zu minimieren, Geschäftsrisiken zu bewältigen, potenzielle Schäden zu reduzieren und die gesamte Sicherheitsinfrastruktur von Unternehmen zu verbessern. EY davon aus, dass Fortschritte in der Technologie, insbesondere in den Bereichen künstliche Intelligenz, maschinelles Lernen und Automatisierung, ebenfalls eine wichtige Rolle bei der Umwandlung von Rechts- und Compliance-Funktionen spielen werden. Die von der EY-Umfrage befragten Befragten umfassen 2.550 Führungskräfte aus 55 Ländern und Gebieten.

Der schnelle Wandel in der Kommunikationstechnologie hat neue Sicherheitsherausforderungen hervorgebracht. In der Cyber-Sicherheit bezieht sich die Insider-Bedrohung auf potenzielle Aktionen von Personen innerhalb einer Organisation, die Schaden anrichten können, im Gegensatz zu Hackern, die von außen angreifen. Manchmal ergreift ein Insider böswillige Aktionen, um Daten zu stehlen oder Schaden zu verursachen. In anderen Fällen ergreift der Insider versehentlich Aktionen, weil er einen Fehler macht oder die Konsequenzen seiner Aktionen nicht versteht. Alle Mitarbeiter müssen ihr Sicherheitsbewusstsein teilen und ihre Rollen und Verantwortlichkeiten bei der Verhinderung von Cyberangriffen verstehen. Jeder Teil der Organisation kann Opfer eines

Eindringens werden, und ein Versagen in einem Bereich kann sich auf andere auswirken.

Der Schutz von Organisationen vor Cyberbedrohungen erfordert eine Strategie zur Verteidigung des Netzwerks. Das Risiko Nummer Eins ist die Fähigkeit eines Unternehmens, Probleme zu erkennen und zu eskalieren. Fast 60% der Führungskräfte kritischer Infrastrukturbetreiber, die kürzlich befragt wurden, geben an, dass ihnen keine angemessenen Kontrollen zum Schutz ihrer Umgebungen vor Sicherheitsbedrohungen zur Verfügung stehen. Eine Kombination aus Security Analytics und Security Orchestration kann jedoch in Zukunft Marktchancen eröffnen. Die zunehmende Bedrohung durch Cyberkriminalität ist ein weiterer wichtiger Faktor für das Marktwachstum.

Spezialisierte Unternehmen identifizierten die Hauptrisiken, lieferten pragmatische Abhilfemaßnahmen, priorisierten Risiken und lieferten ein umfangreiches Programm zur Verbesserung des Datenschutzes. Sie helfen dabei effektive interne Sicherheitsrichtlinien für Unternehmens IT-Ressourcen entwickeln - einschließlich von Datenschutzrichtlinien, die Mitarbeiter bei der Handhabung und dem Schutz von Verbraucherdaten unterstützt. Eine Umsetzungsstrategie muss geplant werden und die Maßnahmen müssen definiert werden, und der Umsetzungsplan muss überprüft und genehmigt werden, bevor die Umsetzung erfolgt. Sobald die Kontrollen implementiert sind, erfolgt die Bewertung der Sicherheitskontrollen, um herauszufinden, ob die Kontrollen korrekt implementiert wurden, wie vorgesehen funktionieren und die gewünschte Ausgabe in Bezug auf die Sicherheitsanforderungen liefern. Von Datenschutzbeauftragten wird erwartet, dass er kompetent in der Verwaltung von IT-Prozessen, Datensicherheit (einschließlich Umgang mit Cyber-Angriffen) und anderen kritischen Fragen der Geschäftskontinuität rund um das Halten und Verarbeiten persönlicher und sensibler Daten ist. Unternehmensleiter schätzen, dass bis zu 10% der Gesamtkosten der Cloud-ERP-Implementierung benötigt werden, um ein gutes Sicherheits- und Kontrollsystem zu gewährleisten.

Die Kosten der Cyberkriminalität für die Weltwirtschaft wurden auf 445 Milliarden Dollar pro Jahr geschätzt. Cyberbedrohungen sind ein ständiges Problem für Unternehmen und dürften bis 2018 Schäden in Höhe von über einer Billion Dollar verursachen. Um sich besser vor diesen Angriffen zu schützen, erwägen Cybersicherheitsanbieter maschinelles Lernen, um eine dynamischere und intuitivere Verteidigung zu bieten. Ein Bericht legt nahe, dass der Cybersecurity-Markt für maschinelles Lernen den Wert der Ausgaben für Big Data, Intelligence und Analytics bis 2021 auf 96 Milliarden US-Dollar steigern wird. Cyber-Bedrohungen betreffen mehr als nur die IT-Infrastruktur eines Unternehmens. Diese Bedrohungen können Störungen im gesamten Netzwerk verursachen und die wichtigsten Geschäftsfunktionen und -missionen beeinträchtigen. Mehrere Organisationen integrieren die Cyber-Verteidigung in traditionelle Sicherheitsaktivitäten wie physische und personelle Sicherheit als Teil einer übergreifenden Anstrengung, um den Geschäftsbetrieb vor externen und internen Bedrohungen zu schützen. Ein zunehmender Trend ist der Einsatz von Cyberangriffen auf kritische Infrastrukturen und strategische Industriesektoren, die im schlimmsten Fall einen Zusammenbruch der Systemen auslösen könnten. Als Folge von Vorfällen werden Dateien vorübergehend oder sind dauerhaft verloren, Software oder Systeme werden beschädigt, Firmen oder Wohltätigkeitsorganisationen haben langsamere oder oder heruntergefahrene Websiten und Geld, Vermögenswerte oder geistiges Eigentum können gestohlen werden.

1.3 technology & infrastructure

Europol hat 2013 das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) ins Leben gerufen, um die Reaktion der Strafverfolgungsbehörden auf Cyberkriminalität in der EU zu stärken, um EU-Bürger, Unternehmen und Regierungen besser vor Online-Kriminalität zu schützen. Das WEF hat kürzlich gemeinsam mit Europol ein globales Zentrum für Cyber-Sicherheit eingerichtet, in dem sie gemeinsam versuchen werden, die Bekämpfung der Cyberkriminalität durch den Austausch von Wissen, Fachwissen und Informationen über Cyberbedrohungen zu verbessern. Das MoU umfasst den Austausch von Wissen über wichtige Cyberbedrohungen und -attacken. Die Vereinbarung, die von beiden Parteien in der Europol-Zentrale in Den Haag unterzeichnet wurde, bietet BT und Europol einen Rahmen für den Austausch von Bedrohungsdaten und Informationen über Cyber-Sicherheitstrends.

Die kanadische Regierung übernimmt eine führende Rolle in der Cyber-Sicherheit, um Organisationen und Kanadiern dabei zu helfen, den Wert von Cyber-Sicherheit zu erkennen und Bemühungen zu unterstützen, die Grundlagen der Cyber-Sicherheit in Kanada zu verbessern. Experten hoffen, dass sich die Regierung weiterhin auf die Erforschung, Entwicklung und Kommerzialisierung neuer Cyber-Sicherheitstechnologien konzentriert und Programme entwickelt, um das Wachstum der dynamischen Cybersicherheitsindustrie Kanadas zu unterstützen. Digitale Technologien und das Internet werden für Innovation und wirtschaftliches Wachstum immer wichtiger, und eine starke Cyber-Sicherheit ist entscheidend für Kanadas Wettbewerbsfähigkeit, wirtschaftliche Stabilität und langfristigen Wohlstand. Zu diesem Zweck ist die Nationale Cybersicherheitsstrategie (die Strategie) darauf ausgerichtet, die Regierung Kanadas und ihre Partner an das anhaltende Wachstum und den Wohlstand in dem Sektor anzupassen, auch wenn sich Technologien und Bedrohungen weiterentwickeln.

Mit der Unterstützung beider Regierungen zielt die UK-India Tech Alliance darauf ab, die Zusammenarbeit in Bezug auf Qualifikationen und neue Technologien zu verbessern, indem sie die Entwicklung von Politiken unterstützt und Innovationen fördert. Die neue Partnerschaft zwischen der britischen und der indischen Technologiebranche wird auch das Wachstum von Kompetenzen in Bereichen wie künstliche Intelligenz, maschinelles Lernen, Big-Data-Analysen und Cyber-Sicherheit fördern. Indien und Schweden geeinigten sich unter anderem darauf, die Zusammenarbeit in Bereichen der Rüstungsproduktion und der Cybersicherheit zu verstärken. Cyber Threat Intelligence Fusion und Analyse, zur Unterstützung von Cyber-Sicherheitsoperationen mit Kontext zu Cyberbedrohungen und Modellierung der neuesten Tools, Taktiken und Verfahren (TTPs) von Bedrohungsakteuren und zur proaktiven Überwachung von Cyberbedrohungen.

Google hat eine Reihe von Zielen aufgelistet, die verhindern sollen, dass seine AI-Dienste für bestimmte Zwecke eingesetzt werden. Dazu gehören Technologien, die Menschen wie Waffen und Überwachungsinstrumente schädigen würden. Google stellte auch klar, dass es weiterhin KI-Unterstützung für Regierungsbehörden und Militär bei Anwendungen wie Cyber-Sicherheit, Ausbildung, Militärwerbung, Veteranengesundheitspflege und Suche und Rettung bereitstellen würde. Organisationen sind bereit, schnell in neue Technologien wie Maschinenlernen, künstliche Intelligenz und Cyber-Sicherheit zu investieren. Die Faktoren, die das Wachstum des proaktiven Dienstleistungsmarktes in Nordamerika vorantreiben, sind eine stabile Wirtschaft, technologische Verbesserungen und optimierte Infrastrukturkosten.

Der pakistanische Minister sagte, dass sein Land ein enormes Potenzial habe, um Platz unter den Top-Ökonomien der Welt zu bekommen, für die es auf modernen Boden Forschung betreibt, er fügte hinzu, dass die Regierung bereits Projekte zur Einrichtung von Exzellenzzentren für künstliche Intelligenz, Cybersicherheit, Daten, Cloud Computing und Roboter gestartet habe. Auf der einen Seite, sagte Chinas Minister of Public Security Guo, sollten souveräne Rechte über das Internet respektiert werden, während auf der anderen Seite weitere Anstrengungen unternommen werden sollten, um eine reibungslos vernetzte Welt aufzubauen. Neben dem Schutz unserer Informationsressourcen und der Souveränität des Internets sollten wir weitere Anstrengungen unternehmen, um dieses Konzept einer Gemeinschaft mit gemeinsamer Zukunft im Cyberspace zu bereichern, sagte Guo head of Data Science Institute of Imperial College London, der sich intensiv mit Chinas Internet-Plus-Strategie beschäftigt.

Die Dragonfly 2.0-Hacker, die von Homeland Security als Cyber-Akteure der russischen Regierung identifiziert wurden, verfolgten einen längeren Cyberangriff auf ein US-Kraftwerk und Computernetzwerke, die das Netz kontrollierten. Malware wurde in den Betriebssystemen verschiedener Organisationen und Unternehmen im US-amerikanischen Energie-, Nuklear-, Wasser- und kritischen Produktionssektor gefunden, und die Malware sowie andere Formen von Cyberangriffen wurden bis nach Moskau zurückverfolgt. Das Nuclear Energy Institute (NEI) behauptet, dass kritische Systeme in einer Kernreaktoranlage nicht mit dem Internet oder dem Internet verbunden sind das interne Netzwerk der Einrichtung und somit das Cybersicherheitsrisiko für diese kritischen Systeme minimiert wird. Im vergangenen Monat beschuldigte die Trump-Regierung Russland für eine Cyber-Attacke auf das US-Stromnetz. Amerikanische und britische Offizielle sagten, dass die am 16. April veröffentlichten Angriffe eine breite Palette von Organisationen betrafen, darunter Internetdienstanbieter, private Unternehmen und kritische Infrastrukturanbieter. Die könnten sich in Zeiten der Spannung vorpositionieren, sagte Ciaran Martin, Geschäftsführer der Cyber-Verteidigungsagentur des britischen Cyber Security Centers, der hinzufügte, dass Millionen von Maschinen in der Kampagne ins Visier genommen wurden. Die russischen Angriffe haben eine Vielzahl von Organisationen betroffen.

Die Entscheidung, die Cyber-Policy-Rolle des Weißen Hauses zu eliminieren, ist empörend, vor allem angesichts der Tatsache, dass uns feindseligere Bedrohungen durch ausländische Gegner drohen als je zuvor, sagte Lieu. Dieser Schritt behindert die strategischen Bemühungen unseres Landes, Cybersicherheitsbedrohungen gegen unser Land zu begegnen. Glücklicherweise wird unser Gesetz diese Lücken in der Cybersicherheitsaufsicht der Regierung füllen, indem ein nationales Büro für den Cyberspace im Weißen Haus eingerichtet wird. Homeland Security Secretary Kirstenen Nielsen sagte : "Die Cyberbedrohungslandschaft verändert sich in Echtzeit und wir haben einen historischen Wendepunkt erreicht. Die digitale Sicherheit nähert sich jetzt der persönlichen und physischen Sicherheit an, und es ist klar, dass unsere Cyber-Gegner jetzt die Struktur unserer Republik selbst bedrohen können. "

Die Unternehmen, die von der DSGVO profitieren werden, sind diejenigen, die Programme zur Nutzung dieser Möglichkeiten strukturieren und die Resilienz entwickeln, um künftigen regulatorischen Herausforderungen, Verbrauchererwartungen, Partneranforderungen und Bedrohungen zu begegnen. Angesichts der Komplexität einer großen, verteilten IT-Umgebung sollte die Sicherheit proaktiv geplant und vorbereitet werden und nicht als Reaktion auf Veränderungen in der Landschaft dienen. Abteilungen der Georgia State University versuchen die komplexen

Entwicklungen, die Nutzung und die sozialen Auswirkungen der entstehenden Cybersicherheitstechnologien und -politiken zu verstehen und mitzugestalten.

1.4 defence & threat

Cyberkriminalität betrifft weltweit über eine Million Menschen pro Tag, und Cyberangriffe auf öffentliche Einrichtungen und Unternehmen nehmen zu. Ransomware-Angriffe haben sich als eine der wichtigsten Gefahren für die Cyber-Sicherheit globaler Organisationen herausgestellt. Ransomware ist die häufigste Art von Malware, auf die 39% der durch Malware verursachten Datenschutzverletzungen zurückzuführen sind.

Der Schutz von Kunden und eines Unternehmens vor Betrug und Datenschutzverletzungen hat im digitalen Zeitalter oberste Priorität. Cyber-Sicherheit stellt eine allgegenwärtige Bedrohung dar, aber künstliche Intelligenz kann jetzt einen gewissen Schutz gegen diese Angriffe und Verstöße bieten. Um der Bedrohung durch Cyberangriffe entgegenzuwirken, Geschwindigkeit und Agilität zu haben muss man den Angreifern voraus bleiben, muss man sich anpassen und verbessern. Sicherheitsbehörden müssen sich über die besten Praktiken im Klaren sein, und alle Agenturen müssen zusammenarbeiten, um solche Angriffe zu verhindern, solche Angriffe zu untersuchen und die Angreifer strafrechtlich zu verfolgen.

Die Art der Bedrohungen ändert sich weiter - daher muss innovativ und agil reagiert werden. Es gilt Technologien zu entwickeln und herzustellen, die diese Bedrohungen angehen. Der Cyber Security Data Science Engineer setzt modernste Technologien ein, um statistische Analyse- und Inferenz-Datenmodellierungs-Clustering und Predictive Analysis durchzuführen. Das SANS Security Awareness-Programm umfasst alles, was Sicherheitsbeauftragte benötigen, um einfach und effektiv ein erstklassiges Sicherheitsbewusstseinsprogramm zu entwickeln. Ein Vorhersagemodell, das auf modernster Datenwissenschaft basiert, ist effizienter, erfordert weniger Aufwand und bietet eine bessere Abdeckung der Angriffsfläche eines Unternehmens. Der Schaden, den eine Datenverletzung verursachen kann, ist genauso schwer zu quantifizieren ist wie zu prognostizieren. Tatsächlich gaben 28% der Unternehmen in einer Studie an, dass sie ihr gesamtes oder den größten Teil ihres Cybersicherheits-Budgets für Versicherungen aufwenden und sich bei Datenkompromittierung eher auf Entschädigung als auf Schutz verlassen.

Die Vereinigten Staaten sehen sich Bedrohungen durch eine wachsende Zahl raffinierter bösartiger Akteure ausgesetzt, die den Cyberspace ausnutzen wollen. Einige Cybersecurity-Experten des privaten Sektors haben die US-Regierung dafür kritisiert, dass sie zu langsam ist, um Informationen über Cyber-Angriffe zu veröffentlichen. Ein hochrangiger US-Beamter, der unter der Bedingung der Anonymität sprach, sagte, es habe in den letzten Jahren einen stetigen Anstieg der russischen Cyberangriffe gegeben. Zu den Motivationen gehören Spionage, politische und ideologische Interessen sowie finanzieller Gewinn.

Das britische nationale Cybersicherheitszentrum hat in Zusammenarbeit mit dem FBI und dem US-Heimatschutzministerium eine beispiellose gemeinsame technische Warnung herausgegeben, die die Bedrohung im öffentlichen und privaten Sektor aufzeigt. Die Kosten der Internetkriminalität für das Vereinigte Königreich werden derzeit auf 18 bis 27 Milliarden Pfund Sterling geschätzt. In einer Stellungnahme erklärte das britische National Cyber Security Center (NCSC), dass es dem britischen Fußballverband vor der Abreise nach Russland für die FIFA Fussball-Weltmeisterschaft 2018

fachkundige Ratschläge zur Cyber-Sicherheit gegeben habe. Wahlbeobachter sagen, dass Indien vor Cybersicherheitsangriffen sicher bleibt, weil der Staat Vorkehrungen trifft, um seine Wahlsysteme zu schützen. Der Schutz der kanadischen Wirtschaft vor Cyber-Angriffen erfordert eine umfassende gemeinschaftliche Herangehensweise und Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor. Kanada hat das Potenzial, weltweit führend in der Cybersicherheit zu sein - und es ist entscheidend, dass wir nicht zurückfallen. UNSW Canberra ist eine der weltweit führenden Forschungseinrichtungen, ein Pionier in der Verteidigung und ein weltweit führendes Unternehmen in der Cyber Security-Bildung Im Rahmen des Cyber Defence Policy Framework von 2014 wurde die Förderung der zivil-militärischen Zusammenarbeit und der Synergien mit der EU-weiten Cyberpolitik, den einschlägigen EU-Institutionen und -Agenturen sowie mit dem Privatsektor gefordert. Zusammen mit CSIRO Data61, der größten Dateninnovationsgruppe in Australien, baut der Cyber Security Hub der Optus Macquarie University ein Team von Forschern und Experten auf, um neuartige und effiziente Technologien zum Schutz der Privatsphäre zu entwickeln, mit einem Schwerpunkt auf Datenanalyse- und Datenfreigabeanwendungen. Cyber-Kriminalität und Cyber-Attacken sind zu einer wachsenden Bedrohung für Regierungen, Unternehmen und Einzelpersonen geworden, wenn die digitalen Technologien voranschreiten.

1.5 critical & future

Die Bedrohung durch Cyberkriminalität und Cyberterrorismus ist eine relativ neue Bedrohung. Die Vereinigten Staaten und Großbritannien warfen Russland vor, Cyber-Angriffe auf Computer-Router, Firewalls und andere Geräte zu starten, die von Regierungsbehörden und Unternehmen auf der ganzen Welt verwendet werden. Laut US-amerikanischen und britischen Behörden zielen russische Hacker auf Millionen von Routern auf der ganzen Welt ab, darunter Geräte in Privathaushalten und Büros. Washington und London gaben eine gemeinsame Warnung heraus, dass die Kampagne der von der russischen Regierung unterstützten Hacker Spionage, Diebstahl geistigen Eigentums und andere bösartige Aktivitäten vorantreiben. Es folgte eine Reihe von Warnungen westlicher Regierungen, dass Moskau hinter einer Reihe von Cyberangriffen steckt. Die Beziehungen zwischen Russland und Großbritannien waren bereits angespannt, nachdem Ministerpräsidentin Theresa May Moskau vorgeworfen hatte, am 4. März die Nervenkraftstoffvergiftung des ehemaligen russischen Spions Sergei Skripal und seiner Tochter Julia in der Stadt Salisbury begangen zu haben.

Der technische Alarm wurde vom britischen Cyber Security Center, dem US Federal Bureau of Investigation und dem Department of Homeland Security herausgegeben. Wenn wir bösartige Cyber-Aktivitäten sehen, sei es vom Kreml oder anderen bösartigen Akteuren des Nationalstaats, werden wir uns zurückdrängen, sagte Rob Joyce, der Cyber Security Coordinator des Weißen Hauses. Russische Cyber-Akteure nutzen eine Reihe von älteren oder schwachen Protokollen und Service-Ports, die mit Netzwerkadministrationsaktivitäten verbunden sind. Die Ziele dieser bösartigen Cyber-Aktivität sind in erster Linie staatliche und private Organisationen, Anbieter kritischer Infrastrukturen und die Internet Service Provider (ISPs), die diese Sektoren unterstützen, heißt es in der Erklärung. Die Regierungen haben die Opfer aufgefordert, alle Infektionen zu melden, damit sie die Auswirkungen der Kampagne besser verstehen können. Der Verteidigungssektor sieht sich auch vielen Herausforderungen in Bezug auf Cyber-Sicherheit gegenüber, um Online-Cyber-Angriffen durch Hacker entgegenzuwirken. Um eine große Datenmenge zu verwalten und die militärischen Daten zu schützen, sind fortschrittliche IT-Lösungen erforderlich.

Politische Parteien, Kampagnen und Organisationen sind ein wachsendes Ziel. Diese Organisationen sind kritische Teile des demokratischen Prozesses und sie verdienen die gleiche Verteidigung gegen Cyber-Angriffe, die wir Nachrichtenorganisationen auf der ganzen Welt angeboten haben. Russische Akteure scannten Datenbanken nach Schwachstellen, versuchten Eindringlingen und in einer kleinen Anzahl von Fällen erfolgreich eine Wählerregistrierungsdatenbank durchdrungen. Durch die einfache Überforderung von Computersystemen und Servern mit gezieltem Flood-Verkehr werden DDoS-Angriffe genutzt, um die politische Sprache und den Zugang der Wähler zu den benötigten Informationen zum Schweigen zu bringen. Millionen von Geräten auf der ganzen Welt sollen auf diese Weise kompromittiert worden sein, mit inhärent schlechter Sicherheit und von den Angreifern ausgenutzten Standard-Passwörtern. Was wir in diesem Fall gesehen haben, sind Standard-Passwörter, die ausgenutzt werden, ungesicherte Geräte werden ausgenutzt, sagte Joyce.

1.6 attacks & access

In den letzten Wochen haben wir Nachrichten über bösartige Agenten gelesen, die daran arbeiten, die Sicherheit der Energieinfrastruktur unseres Landes zu untergraben. Laut dem Department of Homeland Security umfasst dies russische Cyber-Angriffe, die aus der Ferne auf das Stromnetz, Energie, Atomkraftwerke, kommerzielle Einrichtungen und kritische Produktionssektoren abzielen. Moskau hat frühere Vorwürfe zurückgewiesen, dass es Cyberangriffe auf die Vereinigten Staaten und andere Länder durchgeführt habe. Obwohl die Bedrohung für IoT-Geräte nichts Neues ist, hat die Tatsache, dass diese Geräte von fortgeschrittenen nationalstaatlichen Akteuren zur Durchführung von Cyber-Operationen verwendet werden, was möglicherweise zur Zerstörung des Geräts führen könnte, die Dringlichkeit des Umgangs mit diesem Gerät stark erhöht . Die zunehmende Verfeinerung und Durchdringung von Cyberattacken hat Unternehmen in den Sektoren BFSI, Regierung, Telekommunikation sowie Öl und Gas veranlasst, Cybersicherheitslösungen zu übernehmen, um die Sicherheit wichtiger Informationen in Computersystemen oder digitalen Speichergeräten sicherzustellen.

Die Hacker der russischen Regierung müssen keine Zero-Day-Sicherheitslücken ausnutzen oder Malware installieren, um Netzwerkgeräte auszunutzen, warnte der Advisor, da sie Schwachstellen ausnutzen können, die auf die Verwendung von Legacy-Protokollen oder schlechte Sicherheitsmaßnahmen zurückzuführen sind. Sicherheitslücken in der Cyber-Sicherheit sind weltweit ein großes Problem für die Stromnetze, die versuchen, ihre kritischen Ressourcen über ein IT-Netzwerk miteinander zu verbinden. Mit der Verbreitung verteilter Energieressourcen, der zunehmenden Dezentralisierung und der Vernetzung einer Reihe von intelligenten Energieanlagen wie intelligenten Zählern und intelligenten Heimen / Gebäuden besteht die Möglichkeit, Schadcode in die öffentlichen Stromnetze einzudringen. Großbritanniens Top-Energiekonzerne wurden gewarnt, Stromausfälle genauer zu untersuchen, da häufige oder lange Unterbrechungen das Zeichen eines Cyber-Angriffs sein könnten. Cyber-Attacken ergänzen die Liste der Bedrohungen für ein Atomkraftwerk und sie haben die einzigartige Eigenschaft, von weit her und anonym anzugreifen. So können Terroristen Kernkraftwerke anvisieren, die Zugang zu Kernbrennstoffen suchen, um eine schmutzige Bombe oder eine Sprengvorrichtung zu schaffen, die radioaktive Partikel über ein großes Gebiet verteilen soll.

Darüber hinaus wird erwartet, dass die zunehmende Häufigkeit von Cyberattacken aus aufstrebenden Volkswirtschaften wie China, Japan, Indien und Ländern in Südamerika den Markt im Prognosezeitraum antreiben wird. Da Nordamerika und Europa jedoch ausgereifte Märkte für den Schutz von Spearfishing in Bezug auf Systembewusstsein und -akzeptanz sind, werden sich diese Regionen in diesem Prognosezeitraum voraussichtlich stabil, aber relativ langsam entwickeln. Ein Bericht zeigt auch allgemeine Schwächen auf, die die am Markt tätigen Unternehmen vermeiden müssen, um im Verlauf des Prognosezeitraums ein nachhaltiges Wachstum zu erzielen. Die Faktoren, die das Marktwachstum beeinflussen, werden im Detail untersucht. Darüber hinaus wurden Profile von einigen der führenden Akteure, die das Wachstum des globalen Marktes vorantreiben und fördern, in die Studie einbezogen.

Herkömmliche Netzwerksicherheit beruht auf einem sicheren Perimeter - alles innerhalb des Perimeters ist vertrauenswürdig, und alles außerhalb des Perimeters ist es nicht. Ein Netzwerk ohne Vertrauenswürdigkeit behandelt den gesamten Datenverkehr als nicht vertrauenswürdig und beschränkt den Zugriff auf sichere Geschäftsdaten und sensible Ressourcen so weit wie möglich, um das Risiko zu verringern und den Schaden von Sicherheitsverletzungen zu mindern. Der Technologiekonzern Google hat in den letzten Jahren ein Sicherheitsmodell namens BeyondCorp entwickelt. Cisco-Forscher forderten sowohl Verbraucher als auch Unternehmen auf, die Bedrohung durch VPNFilter ernst zu nehmen. Array Networks hat seine Management-Plattform für zentralisierte Konfiguration, Überwachung und Analyse für private Cloud-Umgebungen eingeführt. Symantec hat seine integrierte Cyber Defense-Plattform um Endpoint-Schutz, Isolationstechnologie und softwaredefinierte Cloud-Dienste erweitert. Der IoT-Sicherheitsanbieter Bullguard hat auf seiner Dojo-Plattform einen intelligenten IoT-Vulnerability-Scanner für Kommunikationsdienstleister eingeführt.

Durch das Testen der Infrastruktur, der Auslastung, des Netzwerks und anderer Computerressourcen, die mit Ihrem System verbunden sind, können Unternhemen Fehler in Ihrem System besser verstehen. Wenn Unternehmen ein Intrusion Detection System (IDS) in Ihr System integrieren, können Sie bösartige Aktivitäten in Ihrem Netzwerk überwachen und verfolgen. Wenn IDS Änderungen feststellt, löst es eine Bestätigung an das Hauptverwaltungssystem aus, um alle laufenden Aktivitäten zu beenden und die Systemsicherheit zu verbessern. Maschinelles Lernen ist eine Technik, die den täglichen Betrieb eines Netzwerks beobachtet, um eine Basis für das zu schaffen, was als normal angesehen wird, und vergleicht diese Baseline mit Aktivitäten, Prozessen und Netzwerkverkehr in Echtzeit. Wenn das Verhalten von legitimer oder akzeptabler Leistung abweicht, wird es als anomal und potenziell bösartig gekennzeichnet.

2 risk & detection

2.1 Detection

Google hat auch auf den Sicherheitsaspekt seiner AI-Tools und -Dienste hingewiesen und erklärt, dass ein fortlaufender Entwicklungsprozess durchgeführt wird, um starke Sicherheitsvorkehrungen anzuwenden, um unbeabsichtigte Ergebnisse zu vermeiden. Datenschutzgrundsätze werden auch in die Entwicklung und den Einsatz von KI-Technologien einfließen, unter denen eine angemessene Transparenz und Kontrolle über die Verwendung von Daten durch das Unternehmen bereitgestellt wird. 11.06.18 #tools http://somtxt.de/s/P9j

Die Verwendung persönlicher Geräte zum Speichern oder Zugreifen auf vertrauliche Client-Informationen - insbesondere über einen nicht sicheren Server - könnte Cyber-Kriminellen die Möglichkeit bieten, auf Ihr Familienbüro zu zielen. Stellen Sie, wo immer möglich, sicher, dass Ihre Mitarbeiter getrennte persönliche und geschäftliche Geräte verwenden, und dass auf die Unternehmensinformationen nur mit zugelassenen Sicherheitswerkzeugen über eine sichere Verbindung zugegriffen werden kann. Investieren in Cyber-Versicherung 24.05.18 #tools http://somtxt.de/s/P39

Rosenfeld erklärte, dass eine Kombination aus menschlicher Intuition, Wertschätzung und gesundem Menschenverstand zusammen mit den Automatisierungs- und Verarbeitungsfähigkeiten von Computern Menschen, die alleine arbeiten, bei fast jeder Aufgabe besiegen könnte. Solche Lösungen würden die Möglichkeit geben, die Zeit zwischen Bedrohungserkennung und -antwort zu verkürzen. Es ist, als ob Sie ein Team von virtuellen Analysten haben, die 24/7 arbeiten, um jeden Alarm im System zu untersuchen, sagte er. 12.05.18 #detection http://somtxt.de/s/Ps9

Es umfasst Cyber Threat Intelligence-Konzepte gegen eine Reihe von Bedrohungsakteuren und Bedrohungstools (z. B. Ransomware) in Spitzentechnologien wie Internet der Dinge (IoT), Cloud Computing und mobile Geräte. Dieses Buch enthält auch die technischen Informationen zu den Methoden zur Erkennung von Cyberbedrohungen, die für die Forscher und Experten für digitale Forensik erforderlich sind, um intelligente automatisierte Systeme zur Bekämpfung fortgeschrittener Cyberkriminalität zu entwickeln. 03.05.18 #detection http://somtxt.de/s/PqB

2.2 techniques

Der Senior Privacy Counsel leistet einen wesentlichen Beitrag für die Arbeitsgruppe Datenschutz, Cybersicherheit und Information Governance, die in Zusammenarbeit mit dem Datenschutzbeauftragten (EPA) und dem Datenschutzbeauftragten der EU (DPO) das globale Datenschutzprogramm der Organisation leitet, einschließlich, aber nicht beschränkt auf Tägliche Durchführung des Programms, Implementierung, Pflege von Richtlinien und Verfahren, Überwachung der Programmeinhaltung und Schulung. 12.06.18 #information http://somtxt.de/s/P9q

Dark Web Intelligence liefert wichtige Einblicke in die Cybersicherheit und Bedrohungsdaten und bleibt ein Schlüsselelement für effektive Automatisierungslösungen in der Cyber-Sicherheitsbranche. Beispielkopie dieses Berichts abrufen @: http://qyreports.com/request-samplereport-id=81934 Bei der Marktforschung zu Dark Web Intelligence handelt es sich um einen Intelligence-Bericht mit akribischen Bemühungen, die richtigen und wertvollen Informationen zu untersuchen. 07.06.18 #information http://somtxt.de/s/P9o

Die Nachfrage nach fortschrittlichen Analysetools und Analyseanwendungen nimmt rapide zu. Die Fähigkeit, eine bessere Cyber-Sicherheit und erweiterte Analysefunktionen bereitzustellen, sind die Hauptfaktoren, die den Markt für Unified Network Management vorantreiben. Das vereinheitlichte Netzwerkmanagement bietet viele Lösungen, nämlich Netzwerkverkehrsmanagement, Netzwerküberwachungsmanagement, Netzwerksicherheitsmanagement, Netzwerkanwendungsmanagement, Konfigurations- und Servermanagement. 05.06.18 #applications http://somtxt.de/s/P3J

Wir kombinieren unsere umfassende Erfahrung mit Sicherheitsdaten und -analysen und tiefe Einblicke in Angreiferverhalten und -techniken, um den Datenreichtum zu ermitteln, der Organisationen über ihre IT-Umgebungen und Benutzer zur Verfügung steht. Unsere Lösungen ermöglichen es Unternehmen, Angriffe zu verhindern, indem sie Schwachstellen sichtbar machen und schnell Kompromisse erkennen, auf Sicherheitsverletzungen reagieren und ... Job Description 22.05.18 #techniques http://somtxt.de/s/P3z

Unternehmensbeschreibung Rapid7 ist ein führender Anbieter von Sicherheitsdaten- und -analyse-Lösungen, mit denen Unternehmen einen aktiven, analysegesteuerten Ansatz für die Cyber-Sicherheit implementieren können. Wir kombinieren unsere umfassende Erfahrung mit Sicherheitsdaten und -analysen und tiefe Einblicke in Angreiferverhalten und -techniken, um den Datenreichtum zu ermitteln, der Organisationen über ihre IT-Umgebungen und Benutzer zur Verfügung steht. 22.05.18 #techniques http://somtxt.de/s/P3z

Risiken Schlüsselminderungen Cyber- und Datensicherheit Wir haben eine Reihe IT-Sicherheitskontrollen Cyber-und Datensicherheit bleibt bestehen, einschließlich der aktuellen Antivirus ein zentrales Risiko, da es Software über den Nachlass, Netzwerk / System die Wirksamkeit unserer Systemüberwachung und regelmäßige Penetrationstests oder führen zu einem Verlust von Daten. 18.05.18 #system http://somtxt.de/s/P3k

Netzwerksicherheits-Appliances sind als eine Reihe von Netzwerkmanagement- und Sicherheitstools definiert, die von großen Organisationen vor Ort installiert werden, um den unbefugten Zugriff auf die Netzwerke zu verhindern und die Datensicherheit zu gewährleisten. Die verschiedenen Typen von Netzwerksicherheitsappliances, die auf dem Markt verfügbar sind, sind Firewall, Intrusion Detection Prevention, Content Management, Unified Threat Management und Virtual Private Network. 18.05.18 #data http://somtxt.de/s/P37

Um sich besser vor diesen Angriffen zu schützen, erwägen Cybersicherheitsanbieter maschinelles Lernen, um eine dynamischere und intuitivere Verteidigung zu bieten. Der Bericht legt nahe, dass der Markt für Machine-Learning-Cybersecurity den Wert von Big Data, Intelligence und Analytics bis 2021 auf 96 Milliarden Dollar steigern wird. Wir sind mitten in einer Revolution der künstlichen Intelligenz, sagte ABI Research Industry Analyst Dimitrios Pavlakis. 15.05.18 #analytics http://somtxt.de/s/PsR

Die Sicherheitssoftware von BluSapphire verwendet eine Kombination aus maschinellem Lernen, künstlicher Intelligenz und Datenanalyse, um Bedrohungen in Millisekunden zu erkennen, proaktiv zu reagieren und zu beheben. Die Experten von BluSapphire haben die letzten vier Jahre damit verbracht, komplexe Malware-Verhaltensweisen zu erforschen und fortschrittliche Machine Learning-Modelle zu entwickeln, die mehrere Vektoren umfassen und eine frühzeitige Erkennung von Bedrohungen sowie eine schnelle Reaktion ermöglichen. 11.05.18 #analytics http://somtxt.de/s/Psn

Experten aus der ganzen Welt greifen auf spezielle Themen mit Tools und Techniken zurück, die jeder Art oder Größe von Organisationen dabei helfen, ein robustes System zu entwickeln, das auf ihre Bedürfnisse zugeschnitten ist. Kapitelzusammenfassungen der erforderlichen Fähigkeiten werden zusammengefasst, um ein neues Reifegradmodell für Cyber-Risiken zu erstellen, das zur Bewertung von Fähigkeiten und zur Verbesserung der Lücken im Straßenplan verwendet wird. Das Cyber-Risiko

ist ein schnell wachsendes Unternehmensrisiko, nicht nur ein IT-Risiko. 10.05.18 #system http://somtxt.de/s/Pse

Sammlung von Papieren von führenden Forschern und Praktikern synthetisiert modernste Arbeit bei der Analyse von dynamischen Netzwerken und statistischen Aspekten der Cyber-Sicherheit. Das Buch ist so strukturiert, dass die Anwendung der Sicherheit im Vordergrund der Diskussionen steht. Es bietet Lesern einen einfachen Zugang in den Bereich der Datenanalyse für komplexe Cyber-Security-Anwendungen, mit besonderem Fokus auf zeitliche und Netzwerkaspekte.Chapters 06.05.18 #applications http://somtxt.de/s/PsW

Über Market Research Future Bei Market Research Future (MRFR) versetzen wir unsere Kunden in die Lage, die Komplexität verschiedener Branchen durch unseren Cooked Research Report (CRR), halbgeöffneten Research Reports (HCRR), Raw Research Reports (3R), Continuous- Futterforschung (CFR) und Marktforschung Beratungsdienste. Das MRFR-Team hat das oberste Ziel, unseren Kunden Marktforschungs- und Nachrichtendienstleistungen von höchster Qualität zu bieten. 05.05.18 #data http://somtxt.de/s/Ps7

WER DU BIST . Sie sind ein Ingenieur, der über Domänenkenntnisse oder ein Interesse an der Vernetzung von Big-Data-Machine Learning und Cybersecurity verfügt. Sie sind bereit für eine aufregende Gelegenheit, mit den modernsten Kommunikationstechnologien der Welt zu arbeiten und in einer schnelllebigen Umgebung zu florieren darauf gesetzt, ein globales Satellitennetzwerk vor den modernsten Cyberbedrohungen zu schützen. 03.05.18 #edge http://somtxt.de/s/PqU

RegTech-Fähigkeiten werden durch Fortschritte in Technologien wie Cloud-Plattformen, maschinelles Lernen und künstliche Intelligenz, Blockchain, Cyber-Sicherheit, digitale Identität und Datenanalyse unterstützt, sagte sie. Australien hat große, reife Finanzmärkte, und die Aufsichtsbehörden suchen nach innovativen Lösungen zur Verbesserung der Finanzregulierung. 01.05.18 #analytics http://somtxt.de/s/PqG

So könnte die erweiterte Realität Finanzdienstleistungsunternehmen schließlich dabei helfen, die Herausforderungen der Einhaltung von Vorschriften, des Risikomanagements und der Cyber-Sicherheit zu bewältigen. Mithilfe von ER-Tools werden Menschen Teil des Systems. Sie können zum Beispiel durch eine 3D-Umgebung laufen oder klicken, die Ergebnisse einer erweiterten Überwachung von Mitarbeiter-E-Mails, Chats über Instant Messaging und Anrufe darstellt. 30.04.18 #system http://somtxt.de/s/PqK

Cyber-Attacken versuchen nicht nur, Daten zu stehlen, sondern versuchen auch, eine zielgerichtete Website zu beschädigen oder zu zerstören. Da sich Regierungsbehörden bei der täglichen Arbeit häufig auf Informationstechnologie-Systeme und Computernetzwerke verlassen, kann ein systemweiter Ausfall die Funktionalität einer Organisation erheblich beeinträchtigen. Ein Website-Hack kann den Fluss einer Website stören, Benutzern den Zugriff verweigern oder Mitarbeiter sperren und kritische Informationssysteme zerstören. 24.04.18 #data http://somtxt.de/s/PqL

Diese Unternehmen wurden hinsichtlich ihrer Herstellungsbasis, ihrer Basisinformationen und ihrer Wettbewerber analysiert. Darüber hinaus bilden die von jedem dieser Unternehmen eingeführten Anwendungen und Produkttypen einen wesentlichen Teil dieses Berichtsabschnitts. Die jüngsten Verbesserungen auf dem globalen Markt und ihr Einfluss auf das zukünftige Marktwachstum wurden ebenfalls in dieser Studie vorgestellt. 18.04.18 #applications http://somtxt.de/s/P1B

Wir verfügen über ein multidisziplinäres Team von Spezialisten für Datenschutz, Cybersicherheit, Regulierung und Compliance, Risikomanagement und Business Change, die bei der Konzeption und Umsetzung eines nachhaltigen Datenschutz- und Datenschutzprogramms helfen können. Unsere Erfahrung Wir kombinieren nachgewiesene Erfahrung und technisches Know-how Bewertung und Bereitstellung von Informationsmanagement-, Datenschutz- und DSPR-Programmen für alle Branchen. 17.04.18 #information http://somtxt.de/s/P1y

2.3 application

Diese Cookies sind notwendig, damit Sie sich auf den Sites bewegen und deren Funktionen nutzen können, z. B. Zugriff auf sichere Bereiche der Sites und die Nutzung der Vistage-Services. Da diese Cookies für den Betrieb der Websites und Dienste von Vistage unerlässlich sind, besteht keine Möglichkeit, diese Cookies zu deaktivieren. Diese Cookies sammeln Informationen darüber, wie Besucher unsere Websites besuchen, beispielsweise welche Seiten Besucher am häufigsten besuchen. 12.06.18 #features http://somtxt.de/s/P9i

Bei der Bereitstellung dieser Dienste sammelt und verarbeitet Neustar DNS-Abfragen, die sowohl Quell- als auch Ziel-IP-Adressinformationen enthalten. Wir verwenden diese Informationen, um unseren Kunden Konnektivitäts- und Routing-Dienste bereitzustellen und unseren Kunden dabei zu helfen, Cyber-Angriffe und andere bösartige Online-Zugriffe zu erkennen und darauf zu reagieren, einschließlich DDoS-Angriffen (Distributed Denial of Service). Website-Leistung und Betrugserkennung. 06.06.18 #service http://somtxt.de/s/P9M

Mit den Appliances der Quest DR Series können Sie: - Sichern Sie mehr Ihrer Server und Anwendungen - mit Unterstützung für mehr als 15 Backup-Anwendungen und erweiterte Sicherheitsfunktionen wie Verschlüsselung im Ruhezustand und sicheres Löschen. - Speichern Sie weniger Backup-Daten - mit variablen Blöcken, In-Line-Deduplizierung und -Komprimierung, um den Backup-Speicherbedarf durchschnittlich um 20: 1 zu reduzieren, bei durchschnittlichen Kosten von $ 0,05 - $ .17 / GB. 04.06.18 #encryption http://somtxt.de/s/P3x

Anwendung von KI in der Informationssicherheit Die Bereiche Cyber-Sicherheit und KI sind in jüngster Vergangenheit zunehmend miteinander verbunden, da das Ziel von Cyber-Angriffen darin bestand, die legitime Leistung auf der Ebene der menschlichen Benutzer und der unteren Systeme zu stimulieren. Vollständig automatisierte öffentliche Turing-Tests, um Computer und Menschen voneinander zu unterscheiden, sind gute Beispiele für die Anwendung von KI in der Informationssicherheit. 30.05.18 #application http://somtxt.de/s/P3G

Maschinelles Lernen wurde in mehreren Sektoren erfolgreich eingesetzt, ist aber in der Sicherheitslandschaft aufgrund seiner Fähigkeit, Daten zu kategorisieren und bösartigen Code in Echtzeit zu analysieren, populär geworden, um zu verhindern, dass Bedrohungen seitlich über Netzwerke hinweg verschoben werden. Bis jetzt hat sich das maschinelle Lernen im erweiterten Endpoint-Schutz und beim Blockieren von Sicherheitsverletzungen als weitaus effektiver und effizienter erwiesen als die herkömmliche Sicherheit. 29.05.18 #machine http://somtxt.de/s/P3m

Da die meisten Internetdienstanbieter eine verteilte Architektur haben, reicht es nicht aus, eine einfache Sicherheitslösung auf Netzwerkebene zu verwenden, um die Bedrohung durch Angriffe zu verhindern oder zu begrenzen. Daher wird die Nachfrage nach Internet-Cyber-Sicherheitssoftware

steigen. Auch im Bereich der Hardware für die industrielle Cyber-Sicherheit wird aufgrund der steigenden Popularität der integrierten Firewall im Prognosezeitraum ein Wachstum erwartet. 29.05.18 #application http://somtxt.de/s/P38

Sowohl native Android-App-Entwickler als auch iOS-App-Entwickler müssen eine Verantwortung für die Entwicklung einer Anwendung übernehmen, die mit einem hohen Sicherheitsstandard geschützt ist. Die Entwicklungsindustrie für mobile Apps wächst und Entwickler sehen sich einer großen Nachfrage gegenüber, Anwendungen innerhalb kurzer Zeit zu entwickeln. Während die grundlegende Sicherheitsregel nicht den ultimativen Schutz bietet, verwenden Hacker einige erweiterte Codes, um auf Ihre vertraulichen Daten zuzugreifen. 22.05.18 #application http://somtxt.de/s/P3f

Das Projekt befasst sich mit den Bedrohungen für Zuverlässigkeit, Ausfallsicherheit und Sicherheit, die sich aus dem Übergang von einer gut verstandenen, einfachen Netzwerkumgebung zu einem dynamischen und virtualisierten softwaredefinierten Netzwerk (SDN) für industrielle Kontrollnetzwerke ergeben können, die wesentlich sensibler reagieren Leistung und Qualität der Dienstleistung im Vergleich zu regulären Informationsnetzwerken wie bei der Automatisierung von elektrischen Systemen. 15.05.18 #service http://somtxt.de/s/Psp

Die Entwicklungs- und Unterstützungsarbeit im Center, das eine Weltklasse-Belegschaft beschäftigt, spielt eine Schlüsselrolle bei der Unterstützung der führenden Technologieplattformen der Firma, darunter elektronischer Handel mit geringer Latenz, Cloud-Engineering, Cyber-Sicherheit, künstliche Intelligenz und maschinelles Lernen sowie digitale Technologien. Das Zentrum wurde auch als Arbeitgeber der Wahl und als starker Teilnehmer in der lokalen Gemeinschaft anerkannt. 26.04.18 #machine http://somtxt.de/s/PqY

In der Tat wird maschinelles Lernen eingesetzt, um Systeme und Netzwerke in einer wachsenden Zahl von Branchen und Unternehmen zu verteidigen. Es ist daher kein Geheimnis, dass auch zunehmend qualifizierte und qualifizierte Sicherheitsspezialisten für die Datensicherheitstechnik zuständig sind. Dieser Video-Kurs führt Sie in das Konzept unbeaufsichtigtes Modelltraining oder Lernen in einem Sicherheitskontext ein. 18.04.18 #machine http://somtxt.de/s/P18

Simplilearns GSA-Planvertrag umfasst Schulungsprogramme für Mitarbeiter in digitalen Technologien wie Big Data und Analytics, Data Science, Künstliche Intelligenz (AI) und Maschinelles Lernen, Projektmanagement, Digitales Marketing, Cybersicherheit, Cloud Computing, DevOps, Agile und Scrum, IT-Service und Architektur, Salesforce [辜], Softwareentwicklung und Qualitätsmanagement. , Gründer und CEO, Simplilearn. 17.04.18 #service http://somtxt.de/s/P11

2.4 defense

Seit Jahren versuchen die weltweit am stärksten auf Sicherheit ausgerichteten und verteilten Organisationen - Banken, Militär- / Verteidigungsbehörden, globale Unternehmen - Cloud-Technologien einzusetzen, die Kosten senken, zukunftssicher gegen Datenwachstum sind und die Benutzerproduktivität verbessern. Die Herausforderungen der Cloud-Transformation für diese Art von sicheren Organisationen haben sich auf Datensicherheit, Migration von Altsystemen und Leistung konzentriert. 12.06.18 #defense http://somtxt.de/s/P98

Weitere Details zu den Produkten und Dienstleistungen des Unternehmens finden Sie unter

http://www.orange.ro. Über Simplilearn Simplilearn ermöglicht es Fachleuten und Unternehmen, in der sich schnell verändernden digitalen Wirtschaft erfolgreich zu sein. Das Unternehmen bietet ergebnisbasiertes Online-Training für digitale Technologien und Anwendungen wie Big Data, maschinelles Lernen, KI, Cloud Computing, Cyber-Sicherheit, digitales Marketing und andere aufkommende Technologien. 07.06.18 #enterprises http://somtxt.de/s/P9N

Es heißt auch, es sei an der Zeit, die Art und Weise, wie Daten im Cyberspace gesammelt, weitergegeben und verkauft werden, gründlich zu prüfen und zu fordern, dass dies für das neue Zentrum für Datenethik und Innovation der Regierung Priorität erhält, sobald es etabliert ist. Alex Neill, welcher? Es ist alles andere als klar, dass wir Google, Facebook und anderen Unternehmen vertrauen können, als verantwortliche Hüter unserer Daten zu agieren. 05.06.18 #facebook http://somtxt.de/s/P94

ThreatModeler ™ wurde in den Kategorien Threat Modeling -Produkt mit dem 1. Platz des Cybersecurity Excellence Awards 2017 und 2018 ausgezeichnet und erhielt den 1. Platz beim Cyber-Verteidigungsnetzwerk-InfoSec-Award als innovativstes Produkt zur Bedrohungsmodellierung. Threat-Modeling-as-a-Service wird ab Juni 2018 in der Public Cloud von ThreatModeler Software verfügbar sein. Die Veröffentlichung von Private Clouds ist für das dritte Quartal 2018 geplant. 05.06.18 #defense http://somtxt.de/s/P3H

QA-Personal- und Sicherheitsteams - Verstehen Sie die Sicherheits- und Qualitätssicherungsprobleme, während sich die Anwendungen noch in der Entwurfsphase befinden. ThreatModeler ™ -Ausgaben umfassen spezifische Testfälle, mit denen Sicherheitsteams sicherstellen können, dass die risikomindernden Kontrollen ordnungsgemäß implementiert werden. QA-Teams können mithilfe von Threat-Model-Outputs Funktionstests proaktiv gestalten und verstehen, wo Geschäftsanforderungen höchstwahrscheinlich fehlschlagen werden. 05.06.18 #solution http://somtxt.de/s/P3H

Dennoch besteht bei der Erfassung, Analyse, Speicherung und Nutzung ein gewisses Sicherheitsrisiko sowie ein Schutz der Privatsphäre. Es gibt mehrere Anwendungen von Big Data, wenn es um Cyber-Sicherheit geht. Auf der anderen Seite ist maschinelles Lernen oder künstliche Intelligenz (KI) ein wertvolles Werkzeug, das von Cyber-Sicherheitsfirmen verwendet wird, um ihre Antworten auf die zunehmenden Bedrohungen durch die Malware-Industrie zu skalieren. 30.05.18 #learning http://somtxt.de/s/P3G

Aus geografischer Sicht ist der globale Markt für industrielle Cyber-Sicherheitslösungen in die Vereinigten Staaten, Südostasien, Indien, China, Japan und Europa unterteilt. Von diesen wird erwartet, dass die Vereinigten Staaten den größten Beitrag zu den Einnahmen des Marktes für industrielle Cybersicherheitslösungen leisten werden. Die hohe Akzeptanz dieser Lösungen durch die verarbeitende Industrie und den Versorgungssektor wird das Wachstum dieses Marktes in der Region vorantreiben. 29.05.18 #solution http://somtxt.de/s/P38

Georgiens Außenminister Brian Kemp hat erklärt, dass umfangreiche Sicherheitsmaßnahmen und Cyber-Verteidigungs-Upgrades das derzeitige System des Staates verlässlich machen. Zu diesen Maßnahmen gehören externe Sicherheitsüberwachung, regelmäßige Überprüfung auf Systemschwachstellen und eine Sicherung von Wählerdaten, die an einem sicheren Ort gespeichert sind. Amanda Strudwick, eine 43-jährige Krankenschwester aus Decatur, sagte, sie müsse Georgia-

Wahlbeamte bei ihrem Wort nehmen. 17.05.18 #defense http://somtxt.de/s/Psx

In letzter Zeit gibt es neue Entwicklungen in der Cybersicherheitsindustrie mit dem Aufkommen neuerer Technologien zur Unterbrechung des Cybersicherheitsraums, wie der Entwicklung von Benutzerhardwareauthentifizierung, Cloud-Technologie sowie maschinellem Lernen und künstlicher Intelligenz mit dem Ziel, Bedrohungen zu bekämpfen und auszurotten. Cloud-Technologie hat einen großen Einfluss! Cloud-Technologie macht eine große Veränderung im Bereich der Informationssicherheit. 19.04.18 #learning http://somtxt.de/s/P1J

Die neue Partnerschaft zwischen der britischen und der indischen Technologiebranche wird auch das Wachstum von Kompetenzen in Bereichen wie künstliche Intelligenz, maschinelles Lernen, Big-Data-Analysen und Cyber-Sicherheit fördern. Dieses bahnbrechende MoU zwischen Nasscom und techUK wird Menschen mit hochmodernen Fähigkeiten in aufstrebenden Technologiefeldern wie KI und Robotik ausstatten ... 18.04.18 #learning http://somtxt.de/s/P1w

Der Schwerpunkt dieser Studie liegt auf Cybersicherheitsprodukten / -lösungen und -services, die derzeit zum Schutz von mit dem Internet verbundenen Geräten gegen Cyberkriminelle verfügbar sind, sowie auf der wahrscheinlichen Entwicklung neuer Technologien / Plattformen auf mittlere bis lange Sicht. Unterstützt durch die Finanzierung von mehreren Risikokapitalfirmen und strategischen Investoren, hofft dieser sich entwickelnde Markt auf die Bemühungen mehrerer Start-ups. 18.04.18 #solution http://somtxt.de/s/P1C

Die zunehmende Macht und Raffinesse dieser Systeme gegen Eindringlinge und Datendiebstahl zu entfesseln, ist keine theoretische Aufgabe mehr. In der Tat wird maschinelles Lernen eingesetzt, um Systeme und Netzwerke in einer wachsenden Zahl von Branchen und Unternehmen zu verteidigen. Es ist daher kein Geheimnis, dass auch zunehmend qualifizierte und qualifizierte Sicherheitsspezialisten für die Datensicherheitstechnik zuständig sind. 18.04.18 #enterprises http://somtxt.de/s/P1m

2.5 risk

Unsere Fähigkeit, maßgeschneiderte Bedrohungsdaten in automatisierte Sicherheitsmaßnahmen umzuwandeln, ermöglicht es den Kunden, intelligenter und nicht härter zu arbeiten, da sie einen kontinuierlichen Ansturm gezielter Angriffe bekämpfen. IntSights Cyber Intelligence wurde 2015 auf den Markt gebracht und ist eine der ersten Threat Intelligence Platforms (TIP), die Bedrohungsdaten wirklich zusammenfasst und es Unternehmen ermöglicht, basierend auf dieser maßgeschneiderten Aufklärung und Analyse Maßnahmen zu ergreifen. 12.06.18 #risk http://somtxt.de/s/P9D

Diese Innovation hebt die beliebtesten mobilen Geräte der Welt zu echter Sicherheit der Enterprise-Klasse. Die Version verbessert die Sicherheit für MacOS mit erweiterten Funktionen zur Gerätekompatibilität und Always-On VPN mit Lockdown-Kontrolle des Internet-Datenverkehrs, so dass Unternehmensbenutzer unabhängig von ihrem Standort sicher sind. Pulse Connect Secure 9.0 erweitert auch die Schwachstellenanalyse für Endpunkte, um IT-Angriffe wie die WannaCry-Ransomware zu verhindern. 10.06.18 #device http://somtxt.de/s/P9h

Nicht nach einem neuen Bericht. Kanada rangiert an dritter Stelle auf einer Liste der schlechtesten Länder, deren Organisationen und Benutzer ungesicherte Internetdienste haben, die für Cyberangriffe offen sind, sagt eine Sicherheitsverkäuferumfrage. Der National Exposure Index, der

am Donnerstag von Rapid7 veröffentlicht wurde, bewertet die USA zuerst und China als die Länder mit der größten Exposition gegenüber möglichen Angriffen, der durchdringenden Überwachung und dem Missbrauch durch Amplifikation. 08.06.18 #organizations http://somtxt.de/s/P9a

Effektiver Schutz bedeutet auch, dass Sie Ihre geschäftskritischen Ressourcen und Daten genau kennen: wo sie sind, wer Zugriffsrechte auf sie hat und wie sie gesichert sind. Ein risikobasierter Ansatz für die Datensicherheit und die Verwendung fortschrittlicher Bedrohungsdaten schützen Ihre Ressourcen zusammen mit den Anwendungen, die Ihre Informationen verwalten. Die DSGVO erfordert, dass Sie System- und Datenverstöße wirksam und schnell erkennen können. 06.06.18 #risk http://somtxt.de/s/P9c

Die Information Security Media Group (ISMG) ist das weltweit größte Medienunternehmen für Informationssicherheit und Risikomanagement. Jede ihrer 28 Medienseiten bietet relevante Bildung, Forschung und Nachrichten, die speziell auf die wichtigsten vertikalen Sektoren wie Banken, Gesundheitswesen und den öffentlichen Sektor zugeschnitten sind; Geographien von Nordamerika bis Südostasien; und Themen wie Datenschutzvorbeugung, Cyber-Risikobewertung und Betrug. 04.06.18 #risk http://somtxt.de/s/P3V

Cyber Threat Landscape - Ein umfassender Überblick über die verschiedenen Cyberbedrohungen im Gesundheitswesen wie Ransomware, Phishing und DDos sowie mögliche Auswirkungen auf Gesundheitsorganisationen. Business E-Mail-Kompromiss (BEC) - BEC ist ein ausgefeilter Betrug mit E-Mail und / oder anderer elektronischer Kommunikation sich als Führungskraft, Mitarbeiter oder andere Person auszugeben, die befugt ist, Zahlungen oder Zugriff auf Lohn- und W9-Informationen von Mitarbeitern anzufordern. 30.05.18 #ransomware http://somtxt.de/s/P3E

Unternehmen müssen täglich eine Vielzahl von Risiken bewältigen. Während große Unternehmen dazu neigen, spezialisierte Risikomanagement -Abteilungen zu haben, die die Risiken für die Rentabilität überwachen, beginnt und endet das Risikomanagement bei den KMU oft mit physischen Risiken, einschließlich solcher, die sich aus Gesundheits- und Sicherheitsrisiken ergeben. Aber was ist mit dem Risiko von Wettbewerb, Marktbedingungen, Cyber-Sicherheitsverletzungen und aufstrebenden Industrieunterbrechern? 22.05.18 #safety http://somtxt.de/s/P3b

Die Scorecard kann Daten nach Asset-, Organisationsgruppen- und Aufgabenergebnissen filtern. Solche Funktionen bieten einen entscheidenden Vorteil, wenn Unternehmen die Fähigkeiten ihrer Teams maximieren müssen, um Bedrohungen effektiv zu erkennen, Risiken zu reduzieren und Compliance sicherzustellen. Diese neueste McAfee SIA-Partnerintegration mit Tychon bietet Kunden eine zertifizierte, integrierte Lösung, die es ihnen ermöglicht, Bedrohungen mit weniger Ressourcen schneller zu beheben. 22.05.18 #organizations http://somtxt.de/s/P3a

Verbraucher erhalten eine sichere Zahlungslösung, und Einzelhändler haben Zugriff auf wertvolle Echtzeit-Verbraucherdaten. Bei einer Reihe von chinesischen Verbrauchern, die eine Datenschutzverletzung durch mobile Geräte erlitten haben [6], ist Cyber-Sicherheit ein wichtiges Anliegen. Für sechs von zehn Käufern ist die Online-Zahlungssicherheit (61 Prozent) und die Echtheit der Produkte (60 Prozent) bei der Entscheidung für einen Online-Kauf von entscheidender Bedeutung [7]. 21.05.18 #safety http://somtxt.de/s/P3F

Während zur Sicherung des Unternehmensnetzwerks angemessene Mitarbeiterschulungen und vorbeugende IT-Sicherheitsmaßnahmen erforderlich sind, besteht die letzte Verteidigungslinie im

Schutz der Wiederherstellungsdaten von den sogenannten Ransomware-Angriffsschleifen. Eine Attack-Loop tritt auf, wenn Hacker ausführbaren Code in die Backup-Daten der Organisation einfügen. Wenn ein Angriff auftritt, sind sowohl primäre als auch sekundäre Daten betroffen, wodurch die Möglichkeit einer sauberen Wiederherstellung verhindert wird. 15.05.18 #ransomware http://somtxt.de/s/PsK

Die 15 Global Fraud Survey von Ernst Young (EY) mit dem Thema Integrität im Blickpunkt: Die Zukunft der Compliance hat herausgefunden, dass offene und vernetzte Geschäftsmodelle wahrscheinlich zu einer erhöhten Exposition gegenüber Cyberbedrohungen und Ransomware führen. Eine erhöhte globale Konnektivität bedeutet, dass jeder mit Zugriff auf Firmendaten überall auf der Welt Schwachstellen in der Datensicherheit ausnutzen kann. 03.05.18 #ransomware http://somtxt.de/s/PqV

Neben den bestehenden Sicherheits-Gegenmaßnahmen wie IDS / IPS * 3 und Firewalls * 4 zur Verhinderung von Cyber-Attacken durch Malware * 5 und DDoS * 6 sind in den letzten Jahren Maßnahmen gegen fortschrittliche Cyber-Angriffe zur Überwachung des Betriebs notwendig geworden Eigenschaften und Steuerbefehle des Zielgeräts und ändern das Timing der Netzwerkkommunikation oder den Inhalt von Befehlen, um das Zielgerät zum Fehlschlagen zu bringen. 25.04.18 #device http://somtxt.de/s/PqS

Cyber-Sicherheitsbedrohungen, Änderungen der Kundenerwartungen, regulatorische Änderungen des Datenschutzes und der Compliance, Dritte wie Partner und sogar Kunden, Weltereignisse und politische Veränderungen sind Risiken, die, wenn sie nicht ordnungsgemäß gemanagt werden, einem Bankgeschäft einen konkreten und schwerwiegenden Schaden zufügen können und finanzielle Organisationen. (Siehe die Hauptrisiken gemäß Forrester Research in Abbildung 1 unten). 24.04.18 #organizations http://somtxt.de/s/PqF

NC4 verfolgt einen umfassenden und integrierten Ansatz für Sicherheit und Schutz durch Bereitstellung von: Cyber-Bedrohungsaustausch, der die Entwicklung einer Sharing-Kultur und von Vertrauenskreisen vorantreibt; globale Sicherheits- und Reiseintelligenz, Analyse, Traveller-Tracking und relevante Echtzeit-Bedrohungsalarmierung zur Minderung von Unternehmensrisiken und ein einheitliches Betriebsbild zur Verbrechensbekämpfung und Bewältigung von Notfällen. 17.04.18 #safety http://somtxt.de/s/P19

2.6 breaches

Lance Spitzner, Direktor von SANS Security Awareness, sagt: Angesichts der jüngsten großen Verstöße, wie sie Equifax, Yahoo! und der WannaCry-Ransomware-Angriff auf den NHS erlitten haben, und mit neuen Vorschriften wie der EU-Datenschutz-Grundverordnung Schutz in scharfem Fokus, gibt es ein neues Gefühl der Dringlichkeit um Cyber-Sicherheit, das sowohl Unterstützung als auch Veränderung anregt. 13.06.18 #breaches http://somtxt.de/s/P96

Wir haben so viel wie möglich getan, um die Sicherheitsstufe DoD [Department of Defense] mit einer nahtlosen Benutzererfahrung wiederherzustellen, und wir freuen uns darauf, Benutzer mit unseren Angeboten zu schützen. Die Paladin Browser-Erweiterung bietet den umfassendsten verfügbaren Browserschutz Die fünf wichtigsten Sicherheitssicherheitsschwachstellen: Phishing-Versuche, Einschleusen von Schadcode, bösartige Websites, ungesicherte Wi-Fi-Verbindungen und schwache

Kennwörter. 13.06.18 #phishing http://somtxt.de/s/P9C

Über Finjan Finjan Holdings, Inc., ein Cybersicherheitsunternehmen, bietet Lizenz- und Vollstreckungsdienste für geistiges Eigentum in den USA und international an. Das Unternehmen besitzt ein Portfolio von Patenten im Zusammenhang mit Software- und Hardwaretechnologien, die proaktiv bösartigen Code erkennen und dadurch Endbenutzer vor Identitäts- und Datendiebstahl, Spyware, Malware, Phishing, Trojanern und anderen Web- und Netzwerkbedrohungen schützen. 12.06.18 #phishing http://somtxt.de/s/P93

Eine gute Nachricht ist, dass es einige recht geradlinige Dinge gibt, die Sie tun können, um die große Mehrheit der Cyberangriffe und Datenverstöße davon abzuhalten, Sie zu beeinflussen. Ändern Sie Ihr Passwort, wenn Sie glauben, dass jemand es hat. Wenn eine Datenverletzung die Nachrichten trifft und Ihre Daten preisgegeben werden könnten, könnten Kriminelle möglicherweise auf Ihre Daten zugreifen und diese verwenden, um Ihr Geld oder Ihre Identität zu stehlen oder Sie mit ausgefeilten Phishing-Angriffen zu belästigen. 24.05.18 #breaches http://somtxt.de/s/P3s

Da täglich neue Bedrohungen auftreten und Angreifer ihre Techniken kontinuierlich verfeinern, könnte es schwierig sein, mitzuhalten. Unternehmen und Regierungsbehörden müssen mehr Infrastruktur entwickeln, um den sich ständig ändernden Bedrohungen gewachsen zu sein. Landschaftsorganisationen können nicht länger nur auf Bedrohungen reagieren, sondern müssen eine Infrastruktur schaffen, die agil und anpassungsfähig ist, wenn Verstöße behoben werden, bevor sie auftreten, riet er. 10.05.18 #breaches http://somtxt.de/s/Psb

Der kostenlose Cybersicherheits-Leitfaden für gemeinnützige Organisationen zielt darauf ab, den dritten Sektor dabei zu unterstützen, Technologie intelligent anzunehmen, indem er sie über die große Bandbreite von Cyberbedrohungen informiert, die von Ransomware, Malware und Denial of Service bis hin zu Phishing, Passwortangriffen und menschlichem Versagen reichen können. Es bietet eine Fülle von praktischen Ratschlägen für Wohltätigkeitsorganisationen zur Minderung dieser Risiken, einschließlich Leitlinien zum Schutz vor Datenverletzungen. 30.04.18 #phishing http://somtxt.de/s/Pqi

Mehr als sieben von zehn großen Wohltätigkeitsorganisationen sind im vergangenen Jahr Opfer von Cyberangriffen oder -verstößen geworden, wie neue Untersuchungen der Abteilung für Digitales, Kultur, Medien und Sport ergeben haben. Ein auf der Untersuchung beruhender Bericht, die Cyber Security Breaches Survey 2018, ergab, dass 73 Prozent der Wohltätigkeitsorganisationen mit einem Jahreseinkommen von mehr als 5 Millionen Pfund, die an der Umfrage teilnahmen, im vergangenen Jahr Opfer von Cyberangriffen wurden. 26.04.18 #past http://somtxt.de/s/PqT

3 awareness & people

3.1 Protecting

Die Zahlen zu Cyber-Sicherheitsbedrohungen für die Bundesregierung kommen, nachdem im Bundeshaushalt vom letzten Monat ein 9 Millionen Dollar teures Cyber-Sicherheits-Operationszentrum für das Parlament angekündigt wurde. Laut der Abteilung für Parlamentsdienste sollen sieben Mitarbeiter in dem neuen Zentrum arbeiten, das im Geschäftsjahr 2018-1919 eingerichtet wird und sich auf den Schutz des parlamentarischen Computernetzwerks konzentrieren

wird. 09.06.18 #protecting http://somtxt.de/s/P9u

Dies zeigte sich in Verbindung mit Sicherheitsmängeln, die mit standardisierten Industrie-Chips in Verbindung gebracht wurden, wobei bestimmte Abhilfemaßnahmen das Potenzial hatten, Software-Leistung, Geschwindigkeit und Latenzzeit zu beeinträchtigen, die für den Betrieb der Handelsplattformen des Unternehmens von wesentlicher Bedeutung sind. Es gibt auch einen zunehmenden Trend zur Einführung von Sicherheitslücken in der Lieferantenkette, indem vertrauenswürdige Software-Patches und Updates verseucht werden. 08.06.18 #potential http://somtxt.de/s/P9f

Dieser Forschungsbericht bietet eine gründliche Analyse des globalen Aviation Cyber Security Marktes basierend auf Unternehmensgröße, Services, Lösungen, Endverbraucher-Industrie und Geografie. Der Bericht enthält auch eine Analyse der Faktoren, die das Wachstum des Aviation Cyber Security-Marktes antreiben und bremsen. Es diskutiert die vorherrschenden Markttrends, zukünftige Wachstumschancen und wichtige Strategien, die die Popularität des globalen Marktes erhöhen. 08.06.18 #services http://somtxt.de/s/P9z

Salient CRGT bietet agile Softwareentwicklungs-, Gesundheits-, Datenanalyse-, Mobilitäts-, Cybersicherheits- und Infrastrukturlösungen. Wir unterstützen diese Kernfunktionen mit umfassenden IT-Services und -Trainings für den gesamten Lebenszyklus, damit unsere Kunden kritische Ziele für zentrale Missionen erreichen können. Wir sind speziell für die IT-Transformation konzipiert und unterstützen bundesweit Zivil-, Gesundheits-, Verteidigungs-, Heimat- und Nachrichtendienste sowie Fortune-1000-Unternehmen. 04.06.18 #services http://somtxt.de/s/P3Q

Internationale Zeitschrift für kritische Infrastrukturen (IJCIS), Vol. 14, Nr. 2, 2018 Kurzfassung: Der schnelle Wandel in der Kommunikationstechnologie in Form von Verbindungen, Integration, Supply Chain Management, die essentiell und Teil der kritischen Infrastruktur sind, hat neue Sicherheitsherausforderungen hervorgebracht. Die Sicherung kritischer Daten, Vorgänge, Verbraucherprofile und Daten liegt somit jenseits der vier Wände der physischen Sicherheit. 22.05.18 #securing http://somtxt.de/s/P3u

auf die Sicherheit und die Sicherheit der Verhinderung oder Reaktion auf eine wichtige unserer Kunden oder Mitarbeiter und der Sicherheitsvorfall könnte nachteilige Auswirkungen auf den Handel haben. Auswirkungen auf unsere Geschäftstätigkeit und finanzielle Leistung. Wir investieren in Schulungen auf Standortebene, um feindliche Aufklärungsaktivitäten zu identifizieren und sicherzustellen, dass wir im Falle eines solchen Ereignisses angemessen reagieren. 18.05.18 #staff http://somtxt.de/s/P3k

Weiter: Schutz der königlichen Familie Obwohl die Steuerzahler die Kosten der königlichen Sicherheit tragen, wird keine spezifische Aufschlüsselung dieser Kosten gemeldet, da die Offenlegung solcher Informationen die Integrität dieser Vereinbarungen gefährden und die Sicherheit der geschützten Personen beeinträchtigen könnte. Jahresbericht hat Information Assurance Awareness Training und Cyber Security Training für die Mitarbeiter im Jahr 2016 hervorgehoben. 05.05.18 #staff http://somtxt.de/s/Ps5

Minimierung der Auswirkungen von Cyber-Sicherheitsvorfällen - Dieses Ziel konzentriert sich auf die Fähigkeit eines Unternehmens, die Auswirkungen eines Cyber-Sicherheitsvorfalls auf die Bereitstellung wesentlicher Dienste zu minimieren. Es fordert, dass OES einen soliden

Notfallreaktionsplan hat, um alle relevanten potenziellen Vorfälle abzudecken. Darüber hinaus muss jeder Vorfall, der erhebliche Auswirkungen auf die Kontinuität wesentlicher Dienste hat, formell gemeldet werden. 01.05.18 #potential http://somtxt.de/s/PqE

Sage, das 240 Kunden hat, hat drei Hauptpraktiken: Beratungsdienste, die darauf ausgerichtet sind, Kunden bei der Entwicklung von Richtlinien zur Risikoabsicherung und bei der Beratung von Kunden zu helfen, wenn eine Datenverletzung aufgetreten ist; das ethische Hacking-Geschäft, bei dem Angriffe auf die Client-Infrastruktur simuliert werden, um nach Sicherheitslücken zu suchen, und die Erkennung von Bedrohungen, bei der Experten tägliche Protokolle überprüfen, um nach Bedrohungen im Netzwerk zu suchen. 01.05.18 #services http://somtxt.de/s/Pqp

Yahoo hat sich auch nicht mit seinen Wirtschaftsprüfern oder externen Anwälten über seine Offenlegungspflichten beraten. Schließlich stellt die Anordnung der SEC fest, dass Yahoo keine Offenlegungskontrollen und -verfahren aufrechterhalten konnte, die sicherstellen sollten, dass Berichte des Informationssicherheitsteams von Yahoo bezüglich Cyber-Verstößen oder das Risiko solcher Verstöße richtig und rechtzeitig auf mögliche Offenlegung geprüft werden, sagte die SEC. Lesen Sie hier mehr über die SEC-Bestellung. 30.04.18 #potential http://somtxt.de/s/Pql

Das Büro des für Information zuständigen Kommissionsmitglieds bietet eine leicht verständliche Anleitung zur DSGVO und eine Beratungslinie, die kleinen Unternehmen dabei hilft, sich auf die Veränderungen vorzubereiten. Sie haben auf der Compliance Officer Conference 2017 Ratschläge gegeben. Das nationale Cybersicherheitszentrum und der Aktionsbetrug geben eine Reihe von Leitlinien zum Schutz der Informationssicherheit vor Betrug und Cyberbedrohungen. 17.04.18 #protecting http://somtxt.de/s/P1K

3.2 organisations

Ein Großteil des Fokus lag in letzter Zeit auf der bevorstehenden EU-DSGVO, aber es gibt auch viele Entwicklungen in der APAC-Region, die bemerkenswert sind, wie etwa die fortwährende Umsetzung des Cyber-Sicherheitsgesetzes durch China. Ist künstliche Intelligenz der ultimative Test für die Privatsphäre? Künstliche Intelligenz benötigt Daten, um zu funktionieren, während Datenschutz- und Cybersicherheitsrahmen versuchen, die Verwendung dieser Daten zum Schutz von Individuen zu gestalten. 09.06.18 #gdpr http://somtxt.de/s/P9n

Laut der Abteilung für Parlamentsdienste sollen sieben Mitarbeiter in dem neuen Zentrum arbeiten, das im Geschäftsjahr 2018-1919 eingerichtet wird und sich auf den Schutz des parlamentarischen Computernetzwerks konzentrieren wird. UNSW Canberra Cyber-Sicherheitsstrategie und Diplomatie Professor Greg Austin sagte, während es eine erhebliche Anzahl von Cyber-Sicherheitsbedrohungen in 2016-17, die tatsächliche Anzahl der Vorfälle möglicherweise nicht bekannt ist. 09.06.18 #incidents http://somtxt.de/s/P9u

Obwohl 55% der Befragten angaben, ihre Organisationen hätten Prozesse zur Verwaltung von privilegierten Accounts geändert oder weiterentwickelt, hielten 40% der Organisationen weiterhin privilegierte und administrative Passwörter in einem Word-Dokument oder einer Tabelle und 28% verwendeten einen gemeinsam genutzten Server oder USB-Stick. Darüber hinaus erlaubte jede zweite Organisation (49%) Drittanbietern wie Supply-Chain- und IT-Management-Firmen, Remote-Zugriff auf ihre internen Netzwerke zu erhalten. 23.05.18 #processes http://somtxt.de/s/P3y

Die End-to-End-Sicherheitslösung blockiert böswillige Angriffe über eine Hardware-Root-of-Trust, unveränderliche Schlüssel, die in Silizium gebrannt werden, authentifizieren Server-Boot und Firmware. Zu den weiteren Schutzfunktionen gehört die Sperrung von Systemabbildern, eine branchenweit erste Funktion, die Konfigurationsänderungen verhindert, die Sicherheitslücken verursachen, vertrauliche Daten offenlegen und Standardkennwörter schützen. Eine zuverlässige Erkennung ist entscheidend für die schnelle Erkennung schädlicher Aktivitäten. 22.05.18 #changes http://somtxt.de/s/P3N

Doch trotz der wachsenden Anzahl von Angriffen scheint das Bewusstsein für das Problem und die Bedeutung der Verhinderung der Angriffe nachzulassen , sagte John Zanni, Präsident von Acronis. Das Bewusstsein muss wachsen, um den Menschen zu verdeutlichen, wie wichtig es ist, Daten sicher zu sichern und zu schützen. Im Rahmen unseres 15-jährigen Jubiläums engagieren wir uns dafür, Menschen über den Schutz ihrer Daten zu informieren, unabhängig davon, wo sie sich befinden. 21.05.18 #incidents http://somtxt.de/s/P3t

In der Cyber-Sicherheit bezieht sich die Insider-Bedrohung auf potenzielle Aktionen von Personen innerhalb einer Organisation, die Schaden anrichten können, im Gegensatz zu Hackern, die von außen angreifen. Manchmal ergreift ein Insider böswillige Aktionen, um Daten zu stehlen oder Schaden zu verursachen. In anderen Fällen ergreift der Insider versehentlich Aktionen, indem er auf einen Link klickt oder Informationen teilt, weil er einen Fehler macht oder die Konsequenzen seiner Aktionen nicht versteht. 21.05.18 #people http://somtxt.de/s/P3A

Wenn wir unsere Privatsphäre und Sicherheit wirklich effektiv wahren wollen, müssen wir auch einen Weg finden, die Heimnetzbenutzer zu schulen, damit sie ihre Heimnetzwerke schützen können. Es liegt im Interesse aller Organisationen sicherzustellen, dass ihre Teammitglieder auch sichere Heimnetzwerke haben, so dass es für Unternehmen von Vorteil ist, Schulungen zur Sensibilisierung der Heimnetzsicherheit für ihre Teammitglieder mit einzubeziehen. 16.05.18 #organisations http://somtxt.de/s/Ps2

Ein Großteil des internationalen Fokus lag auf den Vorbereitungen für die Umsetzung der EU-DSGVO im Mai 2018. Die APAC-Region ist jedoch auch aus mehreren Gründen bemerkenswert, darunter Chinas laufende Umsetzung seines Cyber-Sicherheitsgesetzes, die Verschärfung der Datenschutzgesetze in Japan und Australien sowie ein allgemeiner Trend zu einer strengeren Durchsetzung und einer stärkeren Sensibilisierung der Öffentlichkeit für ihre Datenrechte Schutzgesetze. 16.05.18 #gdpr http://somtxt.de/s/PsE

Im März 2015 gründete sie in Singapur ihre eigene Anwaltskanzlei mit den Schwerpunkten Datenschutz / Privatsphäre und Cyber-Sicherheit und beriet parallel zu Zahlungsverkehr und -regulierung. Lyn verfügt über Expertise in den Bereichen geistiges Eigentum und Informationstechnologie und praktiziert allgemeines Gesellschafts- und Handelsrecht, insbesondere im Zusammenhang mit Technologie-Joint-Ventures. 12.05.18 #people http://somtxt.de/s/Pss

Ciaran Martin, Chief Executive des NCSC, sagte: Diese neuen Maßnahmen werden dazu beitragen, die Sicherheit der britischen Infrastruktur zu stärken. Indem sie auf die fachliche Beratung und Meldung von Vorfällen durch das National Cyber Security Center reagieren, können sich Organisationen vor denen schützen, die uns schaden würden. Die britische Regierung hat sich verpflichtet, Großbritannien zum sichersten Ort zu machen, an dem man online leben und

Geschäfte machen kann, aber das können wir nicht alleine tun. 12.05.18 #organisations http://somtxt.de/s/Psd

Diese Experten sind in der Lage, Risikoniveaus zu bewerten und Lösungen bereitzustellen, um das Netzwerk besser gegen Bedrohungen zu schützen, die sich auf Daten und Systeme als Teil einer Business Continuity-Reaktion auswirken können. CSIH-Experten arbeiten möglicherweise mit oder als Teil eines CSIRT zusammen und sind an Aktivitäten beteiligt, die für das Empfangen, Überprüfen und Beantworten von Berichten und Aktivitäten zu Computer-Sicherheitsvorfällen zuständig sind. 11.05.18 #impact http://somtxt.de/s/PsY

Dazu gehören Profis im Bereich Datensicherheit und Datenschutz. Tatsache ist jedoch, dass wir im Land nicht genügend Arbeitskräfte haben , fügte er hinzu. Obwohl sich Unternehmen mit vorhandenen Talenten begnügen, sagte Aditya Narayan Mishra, CEO von CIEL HR Services, dass es in Indien an der Verfügbarkeit von Menschen mit den erforderlichen Fähigkeiten mangelt. 09.05.18 #people http://somtxt.de/s/PsX

Ihr Team hat eine unabhängige Aufsicht und Anleitung für das Risikomanagement und die Einhaltung der Compliance einschließlich der Entwicklung und Implementierung von Risikomanagementmaßnahmen im gesamten Unternehmen übernommen. Das Team hat auch Anstrengungen unternommen, um eine starke Risikokultur aufzubauen und aufrechtzuerhalten, in der alle Mitarbeiter ihrer Verantwortung für strategische, Markt-, Kredit-, Liquiditäts-, Compliance-, Betriebs-, Reputations- und Informationssicherheit einschließlich Cyber-Risiken nachkommen. 08.05.18 #guidance http://somtxt.de/s/Pso

Es ist daher nicht verwunderlich, dass 37 Prozent unserer Befragten Cyberangriffe als eines der größten Risiken für ihr Geschäft ansehen. Die von der EY-Umfrage befragten Befragten umfassen 2.550 Führungskräfte aus 55 Ländern und Gebieten. Dennoch geht EY davon aus, dass Fortschritte in der Technologie, insbesondere in den Bereichen künstliche Intelligenz, maschinelles Lernen und Automatisierung, ebenfalls eine wichtige Rolle bei der Umwandlung von Rechts- und Compliance-Funktionen spielen werden. 03.05.18 #risks http://somtxt.de/s/PqV

Erkennen von Cyber-Sicherheitsereignissen - OES muss nachweisen, dass es die Fähigkeit hat, die Wirksamkeit der Sicherheitsmaßnahmen zu gewährleisten und Cyber-Sicherheitsereignisse zu erkennen, die wesentliche Dienste beeinträchtigen oder potenziell beeinträchtigen können. Minimierung der Auswirkungen von Cyber-Sicherheitsvorfällen - Dieses Ziel konzentriert sich auf die Fähigkeit eines Unternehmens, die Auswirkungen eines Cyber-Sicherheitsvorfalls auf die Bereitstellung wesentlicher Dienste zu minimieren. 01.05.18 #impact http://somtxt.de/s/PqE

Als Folge von Vorfällen wurden Dateien vorübergehend oder dauerhaft verloren, Software oder Systeme wurden beschädigt, Firmen oder Wohltätigkeitsorganisationen haben ihre Website verlangsamt oder heruntergefahren und Geld, Vermögenswerte oder geistiges Eigentum wurde gestohlen. In der Regel entstehen laut dem Bericht keine spezifischen finanziellen Kosten für Cyber-Sicherheitsverletzungen. Aber dort, wo Verstöße zu einem materiellen Ergebnis führen, können die Kosten erheblich sein. 25.04.18 #organisations http://somtxt.de/s/PqP

Die Kosten der Cyberkriminalität für die Weltwirtschaft wurden auf 445 Milliarden Dollar pro Jahr geschätzt.Ein zunehmender Trend ist der Einsatz von Cyberangriffen auf kritische Infrastrukturen und strategische Industriesektoren, was die Befürchtung aufkommen lässt, dass Angreifer im schlimmsten

Fall einen Zusammenbruch auslösen könnten in den Systemen, die Gesellschaften funktionieren lassen. (Global Risks Report 2018, Weltwirtschaftsforum) 20.04.18 #risks http://somtxt.de/s/Pqc

Durchführung einer detaillierten Bewertung der Datensicherheitslücke gemäß den Anforderungen internationaler Standards für einen großen britischen Einzelhändler. Wir identifizierten die Hauptrisiken, lieferten pragmatische Abhilfemaßnahmen, priorisierten Risiken und lieferten ein umfangreiches Programm zur Verbesserung des Datenschutzes. Im Allgemeinen haben wir umfangreiche Erfahrung darin, Organisationen dabei zu helfen, digitales Vertrauen aufzubauen und ihre Cyber-Sicherheit zu verbessern. 17.04.18 #risks http://somtxt.de/s/P1y

Einige unserer jüngsten Arbeiten umfassen: Unterstützung einer in Großbritannien ansässigen Privatkundenbank, eine detaillierte Bewertung ihrer bestehenden Datenschutzkapazitäten gemäß dem britischen Datenschutzgesetz und der DSGVO vorzunehmen und Hauptbereiche der Verbesserung und Sanierung zu identifizieren, die eine detaillierte Datenlückenabschätzung durchführen die Anforderungen internationaler Standards für einen großen britischen Einzelhändler. 17.04.18 #gdpr http://somtxt.de/s/P1y

Was können die Praktiker angesichts der hohen Bußgelder, die die DSGVO mit sich bringen könnte, erwarten, dass sich die Implikationen und Auswirkungen ändern und die geschäftlichen Erfordernisse ändern? Und was können indische Praktizierende von den Veränderungen in der weltweiten Datenschutzlandschaft lernen? In dieser Sitzung wird sich ein Gremium aus Experten für Informationssicherheit, Cyber-Recht und Datenschutz mit folgenden Themen befassen: 16.04.18 #changes http://somtxt.de/s/P1S

3.3 privacy

Das Cybersicherheitsprogramm, das vom Hochschulrat für Informationssicherheit (HEISC) geleitet wird, bietet eine Fülle von Ressourcen und Veranstaltungen, die Sie bei der Entwicklung und Aufrechterhaltung erstklassiger Informationssicherheit, Governance, Compliance, Datenschutz und Datenschutzprogrammen unterstützen. Die jährlich stattfindende Security Professionals Conference ist das führende Forum für die Verbindung von Fachleuten und Lösungsanbietern von Informationssicherheit und Datenschutz an Hochschulen und Universitäten. 13.06.18 #privacy http://somtxt.de/s/P9G

Fordern Sie eine Beispielkopie des Healthcare Cyber Security Market unter http://bit.ly/2t1sKwY Healthcare Cyber Security ist eine Technik, mit der Sie Ihre Netzwerke, Computer, Daten und Programme vor jeder Art von Cyber-Angriffen schützen können, die für die Ausnutzung von Cyber-Attacken gedacht sind die Systeme. Die Cyber-Sicherheit umfasst den Schutz der Daten, Programme und Systeme vor jeder Art von Cyber-Bedrohungen wie Phishing, Malware, Angriffen auf Anwendungen und vielem mehr. 12.06.18 #protect http://somtxt.de/s/P9l

Zu den wichtigsten Faktoren, die den Markt für Sicherheits-Orchestrierung antreiben, gehören die schnelle Bereitstellung von Cloud-basierten Lösungen, das Wachstum des BYOD-Trends und zunehmende Sicherheitsverletzungen. Darüber hinaus setzen Unternehmen Sicherheits-Orchestrierungslösungen ein, um die Netzwerke vor Datenverlusten und Bedrohungen zu schützen. Eine Kombination aus Security Analytics und Security Orchestration kann jedoch in Zukunft Marktchancen eröffnen. 12.06.18 #protect http://somtxt.de/s/P9s

Um herauszufinden, wie IT Governance Ihnen bei Ihren Anforderungen an Cybersicherheit und Datenschutz helfen kann, einschließlich Ihres Projekts zur Einhaltung der Datenschutzrichtlinie, besuchen Sie unsere Website, E-Mail servicecentre@itgovernance.co.uk oder rufen Sie uns an unter +44 (0) 333 800 7000. IT Governance ist ein führender globaler Anbieter von IT-Governance-, Risikomanagement- und Compliance-Lösungen mit besonderem Fokus auf Cyber-Sicherheit und ISO 27001, PCI DSS und Datenschutz. 12.06.18 #requirements http://somtxt.de/s/P9I

Eine Umsetzungsstrategie muss geplant werden und die Maßnahmen müssen definiert werden, und der Umsetzungsplan muss überprüft und genehmigt werden, bevor die Umsetzung erfolgt. Sobald die Kontrollen implementiert sind, erfolgt die Bewertung der Sicherheitskontrollen, um herauszufinden, ob die Kontrollen korrekt implementiert wurden, wie vorgesehen funktionieren und die gewünschte Ausgabe in Bezug auf die Sicherheitsanforderungen liefern. 08.06.18 #requirements http://somtxt.de/s/P9P

Gewährleistung der Vertraulichkeit und Sicherheit von EHR-Daten auf staatlichen Krankenversicherungsmarktplätzen und von Nutzern bei der Verwendung von Gesichtserkennungssystemen. Das GAO empfiehlt außerdem, das Informationssicherheitsprogramm des Federal Information Security Management Act umzusetzen, die Reaktion auf Cyber-Incidents zu verbessern, qualifizierte Cybersicherheitsmitarbeiter zu rekrutieren und zu halten und die Leitlinien für die Meldung von Datenpannen zu aktualisieren. 30.05.18 #practices http://somtxt.de/s/P3g

Gulshan Rai, nationaler Chef der Cyber-Sicherheit, sagte vor einer parlamentarischen Diskussionsrunde, dass Indien keine konzertierten Anstrengungen unternommen habe, um die Verwaltung populärer Social-Media-Plattformen wie Facebook und WhatsApp zu konfrontieren, angesichts wachsender Ängste vor Missbrauch von Nutzerdaten. Rai sagte dies auf einer Sitzung des parlamentarischen Ständigen Ausschusses für Informationstechnologie, der im Zusammenhang mit dem Cambridge Analytica-Skandal Fragen des Datenschutzes und des Datenschutzes erörterte. 12.05.18 #privacy http://somtxt.de/s/Ps3

Cyber Security for Educational Leaders ist ein dringend benötigter Text zur Entwicklung, Integration und zum Verständnis von Technologiepolitiken, die Schulen und Distrikte steuern. Auf der Grundlage von Forschung und Best Practices erörtert dieses Buch die Bedrohungen im Zusammenhang mit Technologieeinsatz und -politik sowie Waffen für aufstrebende und praktizierende Führungskräfte mit den notwendigen Instrumenten zum Schutz ihrer Schulen und zur Vermeidung von Rechtsstreitigkeiten. Besondere Merkmale: 06.05.18 #practices http://somtxt.de/s/PsM

Dies wird durch die Einführung von Canadas erstem Open-Access- und Ultra-High-Speed-Glasfaser-Service über die Waterfront veranschaulicht. Das Mandat des Gremiums besteht darin, Waterfront Toronto objektiven und fachkundigen Rat zu geben, um sicherzustellen, dass die Grundsätze der ethischen Nutzung von Technologie, Rechenschaftspflicht, Transparenz, Schutz der Privatsphäre, Datenverwaltung und Cybersicherheit eingehalten werden. 27.04.18 #privacy http://somtxt.de/s/Pqq

Umfrage: 60% der Execute-Anfälligkeit für Cyberbedrohungen Fast 60% der Führungskräfte kritischer Infrastrukturbetreiber, die kürzlich befragt wurden, geben an, dass ihnen keine angemessenen Kontrollen zum Schutz ihrer Umgebungen vor Sicherheitsbedrohungen zur Verfügung stehen. Indegy gibt bekannt, dass fast 60% der befragten Führungskräfte kritischer Infrastrukturbetreiber in einer

aktuellen Umfrage angeben, dass ihnen keine angemessenen Kontrollen zum Schutz ihrer Umgebungen vor Sicherheitsbedrohungen zur Verfügung stehen. 26.04.18 #protect http://somtxt.de/s/Pqu

Wenn Sie diese Frage mit Nein beantwortet haben, müssen Sie Ihre Richtlinien und Verfahren überprüfen, um sicherzustellen, dass Sie die personenbezogenen Daten Ihrer Website-Nutzer nicht gefährden. Best Practices umfassen, sind jedoch nicht beschränkt auf, organisatorische und technische Maßnahmen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten: Pseudonymisierung und Verschlüsselung personenbezogener Daten Haben Sie einen Datenschutzbeauftragten ernannt und in Ihrer Datenschutzerklärung aufgeführt? 24.04.18 #practices http://somtxt.de/s/PqA

Jeder Fall würde im Rahmen der Leitlinien einzeln geprüft. Die Debatte über den Datenschutz und die Privatsphäre der Bürger in dieser Woche steht vor der Frist für die Umsetzung der DSGVO im Mai, mit der ich die Verhandlungen für die EVP-Fraktion im Europäischen Parlament geführt habe. Cyber-Sicherheit und die Sorge um mögliche Fehlinformationskampagnen während der Wahlen stehen auch vor den Europawahlen 2019 ganz im Vordergrund. 18.04.18 #implementation http://somtxt.de/s/P1E

3.4 awareness

Datenschutz ist jedoch im Allgemeinen kein großes Problem, da Twitter-Daten öffentlich gepostet werden und Dataminr Informationen zu einem bestimmten Ereignis sammelt und nicht die individuellen Daten eines bestimmten Twitter-Benutzers. In den letzten Jahren haben wir die vertikale Sicherheit weiter ausgebaut, sagt Twombly. Der Markt ist offen für den Wert von Social Media als ein Werkzeug für Benutzer, die auf eine ganze Reihe von Fragen umfassend reagieren müssen. 10.06.18 #issues http://somtxt.de/s/P9y

Obwohl keine Kontrolle garantieren kann, dass ein Risikoereignis niemals eintreten wird, sind dies Kontrollen, von denen wir glauben, dass sie zu einem gut konzipierten Rahmen für Risikomanagement und -minderung beitragen. Wir haben das Cyber-Risiko zum ersten Mal in diesem Jahr als spezifisches Hauptrisiko identifiziert. Liquiditätsrisiko Das Risiko, dass die NEX nicht über ausreichende Mittel verfügt, um ihren Verpflichtungen unter normalen und angemessen gestressten Bedingungen nachzukommen. 08.06.18 #controls http://somtxt.de/s/P9f

Die Veröffentlichungen der NIST 800-Serie bieten einen strukturierten Ansatz für das Risikomanagement. Sie bietet eine umfassende Anleitung und nicht unbedingt alle Vorschriften, was bedeutet, dass sie auf die spezifischen Bedürfnisse der Organisation zugeschnitten werden kann und die für die verschiedenen Organisationen erforderliche Flexibilität bietet. Die Verwendung des NIST RMF hilft Organisationen mit Risikomanagement nicht nur auf wiederholbare Weise, sondern auch mit mehr Effizienz und Effektivität. 08.06.18 #specific http://somtxt.de/s/P9P

Wie bei jedem anderen kritischen Risiko müssen C-Level-Führungskräfte und der Vorstand in Budgetierung für Sicherheit und Förderung einer Sicherheitskultur in der gesamten Organisation engagiert sein. Alle Mitarbeiter müssen ihr Sicherheitsbewusstsein teilen und ihre Rollen und Verantwortlichkeiten bei der Verhinderung von Cyberangriffen verstehen. Jeder Teil der Organisation kann Opfer eines Eindringens werden, und ein Versagen in einem Bereich kann sich

auf andere auswirken. 22.05.18 #understand http://somtxt.de/s/P3X

Die Informationskommunikationstechnologie (IKT) verdient eine besondere Erwähnung, zum Teil, weil unsere Prüfer weiterhin grundlegende Probleme finden, aber auch aufgrund der wachsenden Bedeutung von IKT-bezogenen Risiken und ihrer potenziell weit verbreiteten nachteiligen Auswirkungen. Unsere Prüfer stellten fest, dass Unternehmen sich der Probleme der Cybersicherheit und des Zugangs zu Betrugsfällen stärker bewusst sind und ihre Praktiken generell verbessert haben. 17.05.18 #awareness http://somtxt.de/s/PsU

Sie müssen auch effektive interne Sicherheitsrichtlinien für ihre IT-Ressourcen entwickeln - einschließlich einer Datenschutzrichtlinie, die Mitarbeiter bei der Handhabung und dem Schutz von Verbraucherdaten unterstützt. Andere Sicherheitsprotokolle, die in einer Standardsicherheitsrichtlinie enthalten sein sollten, umfassen Kennwortverwaltungsrichtlinien, Zugriffssteuerungen und -verwaltung, Geräterichtlinien und so weiter. Sie sollten Mitarbeiter auch darin schulen, wie sie die Protokolle in der Richtlinie verwenden können. 14.05.18 #controls http://somtxt.de/s/PsD

Der Schutz von Organisationen vor Cyberbedrohungen erfordert eine Strategie zur Verteidigung des Netzwerks. das richtige Bewusstsein in der Organisation und die Annahme, dass bereits ein Angreifer im Netzwerk gefunden werden muss. Die Arbeit des Verteidigers wird sehr schwer sein. Aber wenn wir keine Automatisierung übernehmen, haben wir keine Chance, damit umzugehen - wir brauchen die Kraft der Automatisierung, um Fehlalarme zu reduzieren. 12.05.18 #awareness http://somtxt.de/s/Ps9

Es ist, als ob Sie ein Team von virtuellen Analysten haben, die 24/7 arbeiten, um jeden Alarm im System zu untersuchen, sagte er. Ich denke nicht, dass sich die Situation verbessern wird, sagte Rosenfeld abschließend. Der Schutz von Organisationen vor Cyberbedrohungen erfordert eine Strategie zur Verteidigung des Netzwerks. das richtige Bewusstsein in der Organisation und die Annahme, dass bereits ein Angreifer im Netzwerk gefunden werden muss. 12.05.18 #awareness http://somtxt.de/s/Ps9

In der Kategorie Datenschutz bietet es Lösungen für Datenverlustprävention, Verschlüsselung, Service, VIP Access Manager und Data Loss Prevention sowie CloudSOC. Das Unternehmen bietet auch Beratungsdienste, Kundenerfolgsdienste, Cyber-Sicherheitsdienste und Bildungsdienstleistungen an. Zu den Cyber-Sicherheitsdiensten gehört die DeepSight Intelligence-Software, die eine Analyse von Angriffen bietet. 12.05.18 #protection http://somtxt.de/s/Psq

Aufsichtsbehörden und Regierungen sollten Maßnahmen ergreifen, um sicherzustellen, dass Dienstleister und Produktanbieter ihre Geschäftsmodelle und Produktfähigkeiten transparent darstellen, so dass Verbraucher fundierte Entscheidungen über die Auswirkungen von Produkten und Dienstleistungen auf die Privatsphäre treffen können. Die Malabo-Konvention ist der erste Schritt zur Entwicklung nationaler Rechtsrahmen für Cybersicherheit und Datenschutz in Afrika. 09.05.18 #protection http://somtxt.de/s/Psz

Führungskräfte müssen sicherstellen, dass ihre Organisation die Notwendigkeit erkennt, das mit den heutigen Cloud-ERP-Plattformen verbundene Risiko zu mindern und ein angemessenes Programm und Budget zu entwickeln. In unserer Risk Is Real-Studie haben wir festgestellt, dass Unternehmensleiter schätzen, dass bis zu 10% der Gesamtkosten der Cloud-ERP-Implementierung benötigt werden, um ein gutes Sicherheits- und Kontrollsystem zu gewährleisten. Welche

Stakeholder sind für das laufende Management des Cloud-ERP-Risikos verantwortlich? 01.05.18 #controls http://somtxt.de/s/PqC

Das Risiko Nummer eins war die Fähigkeit eines Unternehmens, Probleme zu erkennen und zu eskalieren. Die folgenden Themen waren ebenfalls wichtig: schnelle Geschwindigkeit von disruptiven Innovationen 22%, unsere Kultur ist widerstandsfähig gegenüber Veränderungen von 20%, Cyber-Sicherheitsbedrohungen 20% und regulatorische Änderungen 11%. Auf der Board-Ebene, als die Frage im Webinar gestellt wurde: Gibt es ein System für regelmäßiges Cyber-Reporting an der Tafel? Waren die Antworten etwas überraschender. 30.04.18 #issues http://somtxt.de/s/PqZ

Das Mandat des Gremiums besteht darin, Waterfront Toronto objektiven und fachkundigen Rat zu geben, um sicherzustellen, dass die Grundsätze der ethischen Nutzung von Technologie, Rechenschaftspflicht, Transparenz, Schutz der Privatsphäre, Datenverwaltung und Cybersicherheit eingehalten werden. Das Gremium wird weiterhin sicherstellen, dass geistiges Eigentum und Daten geschützt werden, während Innovation und wirtschaftliche Entwicklung gefördert werden. 27.04.18 #protection http://somtxt.de/s/Pqq

Haben Sie einen Datenschutzbeauftragten ernannt und in Ihrer Datenschutzerklärung aufgeführt? Wenn Sie diese Frage mit Nein beantwortet haben, müssen Sie eine solche Person ernennen und in den Datenschutzrichtlinien Ihrer Websites aufführen. Von dem Datenschutzbeauftragten wird erwartet, dass er kompetent in der Verwaltung von IT-Prozessen, Datensicherheit (einschließlich Umgang mit Cyber-Angriffen) und anderen kritischen Fragen der Geschäftskontinuität rund um das Halten und Verarbeiten persönlicher und sensibler Daten ist 1. 24.04.18 #issues http://somtxt.de/s/PqA

3.5 challenges

Die quantifizierbare und berechenbare Methode bewertet nicht nur die operationellen Systeme und Verbindungen eines Schiffes, sondern auch die menschliche und maschinelle Identität, wobei das Ausmaß der Cyber-Risikobelastung klar aufgezählt wird. Dies ist datengesteuerte Entscheidungsfindung in Aktion, sagte Wiernicki. Mit den Ergebnissen des FCI-Cyber-Risk-Prozesses können Kunden eine kosteneffektive Risikominderungsstrategie für ihre Vermögenswerte und Flotten anwenden. 06.06.18 #decision http://somtxt.de/s/P9F

In jüngster Zeit hat das Zentrum für geistiges Eigentum und das IT-Recht der Universität Strathmore in Kenia Bedenken hinsichtlich des Datenschutzes hinsichtlich des Missbrauchs biometrischer Daten durch die unabhängige Wahl- und Grenzkommission des Landes (IEBC) geäußert. Einige Herausforderungen sind nicht leicht zu überwinden Einige Mitgliedstaaten der Afrikanischen Union (AU) haben das AU-Übereinkommen von 2014 über Cybersicherheit und Schutz personenbezogener Daten unterzeichnet. 06.06.18 #challenges http://somtxt.de/s/P9W

THRIVE-Forschung, Standpunkte und Analysen untersuchen geschäftliche Herausforderungen und beleuchten den weiteren Weg. Wir sprechen über neue Technologien wie künstliche Intelligenz und Blockchain, transformative Technologien für den digitalen Arbeitsplatz, prädiktive Analyse und Cyber-Sicherheit sowie Strategien für Themen, die Sie wahrscheinlich nachts am Leben erhalten, wie die zukünftige Belegschaft und Kultur von Veränderung. 06.06.18 #challenges

http://somtxt.de/s/P9k

Hauptbereiche des Studiums Data Science, Cyber-Sicherheit, Software-Entwicklung, Benutzererfahrung. Zu den Spezialeinheiten gehören fortschrittliche Cyber-Sicherheit, Big-Data-Analyse, computergestützte Intelligenz und maschinelles Lernen, Computer-Forensik, Internet-Engineering, umfassende und immersive Benutzererfahrung, Programmierung für das Internet der Dinge, mobile und Cloud-Systeme. 01.06.18 #science http://somtxt.de/s/P3B

Die Workshops und Schulungsprogramme werden im ABB Ability Innovation Center (ABB AIC) abgehalten. Als weltweit größtes Forschungs- und Entwicklungszentrum der Welt mit Sitz in Bengaluru entwickelt das Unternehmen Technologien in den Bereichen KI, Cyber-Sicherheit, Automatisierungstechnik, Datenanalyse, Augmented und Virtual Reality sowie Industriesoftware. 23.05.18 #engineering http://somtxt.de/s/P3j

Angesichts des dynamischen Zustands der globalen Beziehungen und der sich ständig weiterentwickelnden Bedrohungen auf der ganzen Welt sind unsere Kunden in der US-Regierung darauf angewiesen, dass wir die unzähligen Technologieplattformen optimieren, die die Sicherheit der Menschen gewährleisten. Unsere Innovationskultur fördert überlegene Kriegskämpfer an Land, im Meer, in der Luft, im Weltraum und im Cyberspace. Wir verleihen unser technisches Know-how einigen der wichtigsten und technologisch fortschrittlichsten militärischen Programme der Geschichte. 23.05.18 #engineering http://somtxt.de/s/P3Y

Das Team ist verantwortlich für die Entwicklung, Durchsetzung und Überwachung von Sicherheitskontrollen, Richtlinien und Verfahren, Disaster-Recovery-Programmen, GRC- (Governance, Risk and Compliance) -Berichterstattung und die Bereitstellung von Sicherheitsdiensten einschließlich des Cyber-Sicherheitsprogramms des Unternehmens. Information Risk and Security Management legt die strategische Ausrichtung für IT-Risiko und -Sicherheit fest und stimmt sich mit Stakeholdern im gesamten Unternehmen ab. 17.05.18 #organization http://somtxt.de/s/P34

Um den Herausforderungen der Big-Data-Sicherheit und des Datenschutzes sowie Big-Data-Analysen für Cyber-Security-Anwendungen gerecht zu werden, veranstalteten wir im September 2014 einen von der National Science Foundation gesponserten Workshop und präsentierten die Ergebnisse im Rahmen eines inter-agentur Workshops in Washington DC. Seither wurden verschiedene Entwicklungen im Bereich der Datensicherheit und des Datenschutzes sowie der Big-Data-Analyse von Cyber-Sicherheit veröffentlicht. 17.05.18 #challenges http://somtxt.de/s/Ps0

Das SANS-Institut wurde 1989 als kooperative Forschungs- und Bildungsorganisation gegründet. SANS ist das vertrauenswürdigste und bei weitem größte Anbieter von Schulungen und Zertifizierungen für Cyber-Sicherheit für Fachleute in Regierungen und kommerziellen Einrichtungen weltweit. Renommierte SANS-Instruktoren unterrichten mehr als 60 verschiedene Kurse bei mehr als 200 Live-Cyber-Sicherheitstrainings sowie online. 26.04.18 #organization http://somtxt.de/s/Pqh

Mit der Integration von Dwight und Dian Diercks Computational Science Hall und seinem neuen Bachelor of Science in Informatik-Programm, wird MSOE an der Bildungsspitze in der künstlichen Intelligenz (KI), Deep Learning, Cyber-Sicherheit, Robotik, Cloud Computing und anderen positioniert werden Technologien der nächsten Generation. Dr. Diercks erwarb 1990 seinen Bachelor-Abschluss in Informatik und Ingenieurwesen bei MSOE. 19.04.18 #engineering

http://somtxt.de/s/P1x

3.6 solutions

Bedrohungsintelligenz ist eine Cyber-Sicherheitsdisziplin, die das Verständnis komplexer Cyberbedrohungen und deren Erkennung, Analyse und vorhersehbare Behebung sucht. Threat Intelligence-Lösungen bieten eine effektive und zuverlässige Erkennung von Bedrohungen, um Cyberbedrohungen aufgrund von Sicherheitsereignissen und Sicherheitsinformationen zu minimieren, Geschäftsrisiken zu bewältigen, potenzielle Schäden zu reduzieren und die gesamte Sicherheitsinfrastruktur von Unternehmen zu verbessern. 29.05.18 #solutions http://somtxt.de/s/P3C

Er ist außerdem Autor und leitender Ausbilder des SANS Hacker Exploits and Incident Handling Kurses und des Penetration Testing Kurses. Michael Assante war Vice President und Chief Security Officer bei NERC, leitete eine wichtige Kontrollsystemgruppe bei Idaho National Labs und war das CSO von American Electric Power. Er leitet jetzt das globale Programm zur Entwicklung von Cyber-Kompetenzen bei SANS für Energie, Öl Gas und andere kritische Infrastrukturindustrien. 29.05.18 #course http://somtxt.de/s/P3l

Aufgrund der erheblichen Bedrohung durch Terroranschläge in verschiedenen Ländern wird erwartet, dass die Nachfrage nach besseren Überwachungs- und Kommunikationsanalyselösungen im Prognosezeitraum erheblich steigen wird. Die zunehmende Bedrohung durch Cyberkriminalität ist ein weiterer wichtiger Faktor für das Marktwachstum. Wettbewerbs-Insights: 28.05.18 #technologies http://somtxt.de/s/P3i

Die Studie umfasst eine Mischung von Daten zu den Haupteinschränkungen, Treibern, Wettbewerbslandschaft, regulatorischen Kräften, Schlüsselstrategien, die von den Hauptakteuren umgesetzt werden, und Chancen, von denen erwartet wird, dass sie einen tiefgreifenden Einfluss auf das Wachstum des Marktes haben. Eine detaillierte Analyse dieser Faktoren ermöglicht es dem Bericht, eine verlässliche Prognose hinsichtlich der zukünftigen Wachstumsdynamik der Künstlichen Nachrichtendienste in der Sicherheit vorzulegen. 24.05.18 #analysis http://somtxt.de/s/P3q

Unsere Ingenieure haben ein System entwickelt, das mithilfe von Lasern improvisierte Sprengsätze (IEDs) zerstört. Wir stellen die erforderlichen Modellierungs- und Simulationstechnologien zur Verfügung, um sicherzustellen, dass Amerikas komplexe Raketenabwehrsysteme vollständig integriert sind. Wir sichern die mit militärischem Personal eingesetzten Befehls- und Kontrollsysteme, und unsere konvergenten Cyber-Physical-Security-Lösungen schützen die Infrastruktur und die Operationen des Militärs im In- und Ausland. 23.05.18 #technologies http://somtxt.de/s/P3Y

Zusätzlich zu seinem Abendgespräch wird Tilbury auch den FOR500: Windows Forensic Analysis-Kurs unterrichten. Dieser Kurs konzentriert sich auf das Erstellen von detaillierten digitalen Forensik-Kenntnisse von Microsoft Windows-Betriebssystemen. Die Teilnehmer lernen, wie sie forensische Daten auf Windows-Systemen wiederherstellen, analysieren und authentifizieren, die Benutzeraktivität in einem Netzwerk verfolgen und Ergebnisse für die Reaktion auf Vorfälle, interne Untersuchungen und zivil- / strafrechtliche Prozesse organisieren können. 22.05.18 #course http://somtxt.de/s/P3P

Über IT Leaders Africa Der IT Leaders Africa Summit bietet IT-Führungskräften seit ihrer Gründung vor 8 Jahren praktisches Wissen von Branchenexperten und Vordenkern. Mit Unterstützung eines

Beratungsgremiums von erfahrenen C-Level-IT-Führungskräften umfasst der Gipfel die aktuellsten Trends in Bezug auf die Umsetzung von Geschäftsstrategien in IT-Funktionen sowie Cybersicherheit, Governance und disruptive Technologie. 22.05.18 #technology http://somtxt.de/s/P3S

Das Schulungsprogramm konzentriert sich auf die Einführung von KI für die Teilnehmer und die zukünftigen Herausforderungen, zusätzlich zu Cyber-Sicherheit, Datenerfassung und -analyse sowie Planung und Entwurf von Lösungen. Das Schulungsprogramm zielt auch darauf ab, Regierungsangestellte mit Schlüsselkompetenzen zu befähigen, von AI und ihren Anwendungen zu profitieren, damit sie einen Beitrag zur Erreichung der Centennial Vision der VAE 2071 leisten können. 18.05.18 #analysis http://somtxt.de/s/P35

Sevatec ist ein führendes nationales Sicherheitsunternehmen, das sich auf Agile, DevSecOps, Data Sciences, Cyber Engineering und Cloud-Lösungen spezialisiert hat. Gegründet im Jahr 2003 nach dem Konzept von Seva, bedeutet Inspiriert, um einen größeren Zweck zu erfüllen, umfasst unser Portfolio an unternehmenskritischen Technologielösungen die Heimat- und Strafverfolgungsbehörden, das Verteidigungsministerium, das Department of Transportation, das Department of State sowie mehrere zivile Abteilungen und Behörden . 16.05.18 #technology http://somtxt.de/s/PsG

Raytheon Company, mit einem Umsatz von 24 Milliarden US-Dollar im Jahr 2016 und 63.000 Mitarbeitern, ist ein Technologie- und Innovationsführer, der sich auf Verteidigungs-, Zivil- und Cybersicherheitslösungen spezialisiert hat. Mit einer Geschichte von Innovationen aus 95 Jahren bietet Raytheon State-of-the-Art-Elektronik, Integration von Missionssystemen, C5ITM-Produkte und -Dienstleistungen, Sensorik, Effekte und Missionsunterstützung für Kunden in mehr als 80 Ländern. 08.05.18 #solutions http://somtxt.de/s/PsN

Der Schwerpunkt des Buches liegt darin, einer Organisation Einblicke in praktische und angewandte Lösungen, Rahmenbedingungen, Technologien und Praktiken zu technologischen und organisatorischen Faktoren zu geben. Das Buch zielt darauf ab, eine Sammlung von Wissen für Fachleute, Wissenschaftler, Forscher und Akademiker zu sein, die in diesem Bereich arbeiten, der sich schnell entwickelt und als ein Bereich der Informationssicherung wächst. 07.05.18 #professionals http://somtxt.de/s/Pst

Dieser Kurs wird Ihnen helfen zu lernen, wie Sie Websites und Anwendungen hacken, indem Sie verschiedene Cyber-Angriffe als Black Hat-Hacker gegen Sie ausführen, aber beheben Sie diese Löcher, mit denen Sie sie wie einen weißen Hut hacken können. 7. Praktische Übungen, Interactive Penetration Testing Ethical Hacking In diesem Kurs lernen Sie in Echtzeit jede Phase einer Penetrationstestumgebung kennen, in der Sie Ihre Fähigkeiten optimieren und testen können. 25.04.18 #learn http://somtxt.de/s/Pqz

BRACHIN LLC bietet Business Intelligence, Informationssicherheit, Einhaltung gesetzlicher Vorschriften sowie Technologie-Software und Beratungsdienste. Wir betreuen Kunden und bieten Unterstützung bei der Verwaltung von Informationen und Geschäftsrisiken, bei Big Data, bei der Verbesserung von Analyseabläufen und bei der Verbesserung der Business Intelligence-Leistung. BRACHIN LLC bietet Unternehmenslösungen einschließlich IT-Service-Management, Cyber-Sicherheit, Analytics, Big Data und SAP S / 4 HANA. 24.04.18 #solutions http://somtxt.de/s/Pqt

Wir bilden Informationssicherheit und IT-Professionals seit 1998 mit einem vielfältigen Angebot an

relevanten Schulungen aus. In den vergangenen 16 Jahren haben mehr als 50.000 Personen dem InfoSec Institute für ihre beruflichen Entwicklungsbedürfnisse vertraut! InfoSec Institute respektiert Ihre Privatsphäre und wird niemals Ihre persönlichen Daten für etwas anderes verwenden, als Sie über Ihre angeforderten Kursgebühren zu informieren. 19.04.18 #professionals http://somtxt.de/s/Pq7

Möglichkeiten, die zum Wachstum des Marktes führen, wurden analysiert und dargelegt. Der Bericht konzentriert sich auf den globalen Markt und beantwortet einige der kritischsten Fragen, mit denen die Interessengruppen derzeit weltweit konfrontiert sind. Informationen über die Größe des Marktes (bis zum Ende des Prognosejahres), Unternehmen, die am ehesten ihre Wettbewerbsfähigkeit steigern, führende Segmente und Herausforderungen, die das Wachstum des Marktes behindern, werden gegeben. 18.04.18 #analysis http://somtxt.de/s/P16

Als Fachexperte wird er Anstrengungen im Bereich maschinelles Lernen und Deep-Learning-Analysen vorantreiben, um die Ausfallsicherheit von Unternehmen zu erhöhen und die IT-Infrastruktur der Kunden vor Cyber-Sicherheitsbedrohungen zu schützen. Als Teil eines der am schnellsten wachsenden Bereiche bei Regierungsaufträgen teilte Vishnubhotla kürzlich seine Gedanken zur Cybersicherheit als Industrie und wie Profis in diesem gefragten Bereich auf dem neuesten Stand bleiben können. 17.04.18 #professionals http://somtxt.de/s/P1O

Cyber-Bedrohungen betreffen mehr als nur die IT-Infrastruktur eines Unternehmens. Diese Bedrohungen können Störungen im gesamten Netzwerk verursachen und die wichtigsten Geschäftsfunktionen und -missionen beeinträchtigen. Mehrere Organisationen integrieren die Cyber-Verteidigung in traditionelle Sicherheitsaktivitäten wie physische und personelle Sicherheit als Teil einer übergreifenden Anstrengung, um den Geschäftsbetrieb vor externen und internen Bedrohungen zu schützen. 17.04.18 #technology http://somtxt.de/s/P1s

Unsere Lösungen und niedrigen Lieferkosten bieten eine einzige Lösung für die Kunden. 3. Neue Kundenkontaktdienste wie sichere Call-Center-Zahlungslösungen und sprachaktivierte Zahlungen mit Diensten wie Amazon Alexa erfordern neue Lösungen, um Zahlungen innerhalb dieser Technologien zu adressieren. 4. Datenschutzverletzungen haben dazu geführt, dass der Schutz von Kundendaten strategisch entscheidend für den Erfolg und den Markenwert unserer Kunden ist. 17.04.18 #technologies http://somtxt.de/s/P1Y

4 technology & infrastructure

4.1 Development

Unser offenes Plattform-Community- und Partnerschaftsmodell ist zweifellos der Grund für die positive Entwicklung und wir sind stolz darauf, ein vertrauenswürdiger und zuverlässiger Partner in der Community zu sein , sagt Lars Thinggaard, Präsident und CEO von Milestone Systems, und fährt fort: Wir Wir werden weiter in unsere Partnergemeinschaft investieren, mit Fokus auf neue Technologien in den Bereichen Kameras, Zugangskontrolle und Videoanalyse. 12.06.18 #development http://somtxt.de/s/P91

Das Zentrum für Forschung in Fragen der Informationssicherheit und des Datenschutzes ist ein Programmbereich des Zentrums für Forschung in Informationssystemen und ein Schwerpunkt für die Forschung in Cybersicherheit und Datenschutz in verschiedenen Abteilungen der Georgia State

University. Das Zentrum ist der Forschung gewidmet, die versucht, die komplexen Entwicklungen, die Nutzung und die sozialen Auswirkungen der entstehenden Cybersicherheitstechnologien und -politiken zu verstehen und mitzugestalten. 23.05.18 #development http://somtxt.de/s/P3T

Die Zusammenarbeit zwischen den Mitgliedstaaten, aber auch auf europäischer Ebene ist daher von wesentlicher Bedeutung. Europa ist stärker, wenn es Bedrohungen gemeinsam angeht, in einem gemeinsamen und koordinierten Ansatz. Und genau hier ist dieses Memorandum of Understanding der Schlüssel und wo der Mehrwert der Europäischen Union liegt: zusammenarbeiten, Kräfte bündeln, die Erfahrungen und das Wissen aller in den Dienst der Sicherheit unserer Bürger stellen. 23.05.18 #knowledge http://somtxt.de/s/P3h

CIS 8394 - Fortgeschrittene Themen in Cybersecurity - Security Analytics Dieser Kurs vermittelt den Teilnehmern die Kenntnisse und Fähigkeiten, die sie brauchen, um kognitiv zu denken, um sowohl Cyber-Sicherheit als auch Big-Data-Probleme anzugehen. Der Kurs wird die Teilnehmer durch einen Fallstudienansatz zusammen mit der Verwendung einer Vielzahl von State-of-the-Art-Software von IBM für die Organisation, Analyse und Visualisierung von Cyber-Sicherheitslösungen in einer Vielzahl von Möglichkeiten erziehen. 22.05.18 #skills http://somtxt.de/s/P3n

Am Ende des Kurses erhalten die Teilnehmer ein umfassendes Verständnis der rechtlichen und Compliance-Fragen im Zusammenhang mit Cloud Computing und können Probleme in Bezug auf Cloud-Daten, Infrastruktur und Betriebssicherheit diskutieren und lösen. CIS 8394 - Fortgeschrittene Themen in Cybersecurity - Security Analytics Dieser Kurs vermittelt den Teilnehmern die Kenntnisse und Fähigkeiten, die sie brauchen, um kognitiv zu denken, um sowohl Cyber-Sicherheit als auch Big-Data-Probleme anzugehen. 22.05.18 #skills http://somtxt.de/s/P3n

Darüber hinaus werden in der Studie wichtige Marktteilnehmer von Critical National Infrastructure Cyber Security, die den Markt beeinflussen, zusammen mit ihren SWOT-Analysen und Marktstrategien vorgestellt. Der Bericht konzentriert sich auch auf führende Akteure der Branche mit Informationen wie Unternehmensprofile, Produkte und Dienstleistungen, Finanzinformationen der letzten 3 Jahre, Schlüsselentwicklung in den letzten fünf Jahren. Grund zu kaufen 22.05.18 #development http://somtxt.de/s/P3o

Ein CSIH-Kandidat kann sein Wissen und sein Bewusstsein für verschiedene Phasen der Ereignisbehandlung demonstrieren, einschließlich aller Aktivitäten und Prozesse zum Erkennen, Melden, Aussortieren, Analysieren und Reagieren auf Computersicherheitsvorfälle. Das CERT-CSIH-Zertifizierungsprogramm bereitet Personal für die Reaktion auf Computer-Sicherheitsvorfälle und andere Informationssicherheitsexperten vor, um sich an der Vorfallbehandlung zu beteiligen. 11.05.18 #knowledge http://somtxt.de/s/PsY

Darüber hinaus ist der Anstieg der BYOD-Anwendungen einer der Hauptfaktoren, der für den Wachstum des Markts für Spear-Phishing-Schutz im Prognosezeitraum verantwortlich ist. Der Markt für Spear-Phishing-Schutz dürfte daher zwischen 2017 und 2025 zu einem Anstieg des Marktwachstums führen. Es wird jedoch erwartet, dass ein Mangel an angemessenem Wissen und Bewusstsein für Cyber-Angriffe das Wachstum des Marktes für Spear-Phishing-Schutz behindern wird. 02.05.18 #knowledge http://somtxt.de/s/Pq0

Die Kap-Innovations- und Technologieinitiative wird ihr Tech-Ausbildungsprogramm auf 3 000 Studenten in den nächsten drei Jahren aufstocken. Das Injini African Ed-Tech Incubation Program

bietet R590 700 für eine Lösung zur Lösung dringender Bildungsprobleme an. Das Unternehmen hat sich mit der Kap-Innovations- und Technologieinitiative zusammengeschlossen, um Kompetenzen in den Bereichen Softwareprogrammierung, Cybersicherheit, Fintech und KI zu erweitern. 16.04.18 #skills http://somtxt.de/s/P1M

4.2 innovation

Darüber hinaus hat Google eine Reihe von Zielen aufgelistet, die verhindern würden, dass seine AI-Dienste für bestimmte Zwecke eingesetzt werden. Dazu gehören Technologien, die Menschen wie Waffen und Überwachungsinstrumente schädigen würden. Google stellte zwar klar, dass es weiterhin KI-Unterstützung für Regierungsbehörden und Militär bei Anwendungen wie Cyber-Sicherheit, Ausbildung, Militärwerbung, Veteranengesundheitspflege und Suche und Rettung bereitstellen würde. 11.06.18 #training http://somtxt.de/s/P9j

Laut dem jährlichen Tech Nation-Bericht, der die Entwicklung des britischen Tech-Sektors abbildet, zogen britische Firmen 2017 mehr Kapital an als jedes andere europäische Land. Cluster, die auf künstlicher Intelligenz, maschinellem Lernen, Cyber-Sicherheit und Big Data basieren Industrien unterstützen Wachstum, Arbeitsplätze und Produktivität in großen und kleinen Gemeinschaften , sagte die Premierministerin in ihrer Einführung zum Tech Nation Report 2018. 10.06.18 #artificial http://somtxt.de/s/P9T

Folgen Sie uns auf Twitter @IndustryToday Cyber Security für Öl Gas - Global Market Status- und Trendbericht 2013-2023 bietet eine umfassende Analyse zur Cyber Security für die Öl- und Gasindustrie, die aus der Leserperspektive besteht und detaillierte Marktdaten und penetrierende Erkenntnisse liefert. Unabhängig davon, ob der Kunde Brancheninsider, potentieller Neueinsteiger oder Investor ist, der Bericht liefert nützliche Daten und Informationen. 08.06.18 #innovation http://somtxt.de/s/P9X

Das CSIT-Testlabor umfasst ein Hochgeschwindigkeitsnetzwerk, das über eine Multi-Gigabit-Glasfaser mit dem öffentlichen Internet verbunden ist. Das experimentelle Testnetzwerk ist eine Sammlung verschiedener Informations- und Kommunikationstechnologien mit einzigartigen Verbindungseigenschaften. Es enthält auch eine hochmoderne Cyber Range, eine virtuelle Umgebung, die für Cyber-Defense-Training und Cyber-Technologie-Entwicklung verwendet wird. 01.06.18 #training http://somtxt.de/s/P3U

Wie Big Data und Hadoop-Trainingsprogramme einen großen Unterschied machen Laut Jason Biggs, einem Berater für Informationssicherheit bei check-caller.net, haben Big Data und KI zahlreiche Anwendungen in der Cyber-Sicherheit. Da Cyber-Angriffe immer häufiger und ausgefeilter werden, werden die Bereiche Big Data und KI zunehmend miteinander verbunden sein, um fortschrittlichere Lösungen zur Erkennung und Verhinderung von Bedrohungen der Informationssicherheit zu entwickeln. 30.05.18 #training http://somtxt.de/s/P3G

Als Partner wird das Georgia-Tech-Programm militärische Mitglieder in Bereichen schulen, die ihre beruflichen Aufgaben direkt erfüllen. Georgia Tech Professional Education ermöglicht es Berufstätigen und Industriepartnern, auf das Know-how einer weltweit anerkannten technologischen Forschungsuniversität zuzugreifen. Als akademische Abteilung des Georgia Institute of Technology haben wir die Georgia Tech-Werte von Integrität, Exzellenz, Wirkung und

Innovation angenommen. 25.05.18 #innovation http://somtxt.de/s/P3D

Die Unternehmen, die von der DSGVO profitieren werden, sind diejenigen, die Programme zur Nutzung dieser Möglichkeiten strukturieren und die Resilienz entwickeln, um künftigen regulatorischen Herausforderungen, Verbrauchererwartungen, Partneranforderungen und Bedrohungen zu begegnen. Steve Durbin ist Managing Director des Forums für Informationssicherheit (ISF), einem globalen Konsortium aus Fortune-500- und Forbes-2000-Organisationen, die im Bereich Sicherheitsforschung, Standards und Best Practices zusammenarbeiten. 24.05.18 #threats http://somtxt.de/s/P33

Das Unternehmen durchläuft eine aufregende Phase des organisatorischen Wachstums und wir arbeiten mit hochkarätigen Kunden in einer vielfältigen und interessanten Landschaft zusammen. Unser Geschäft entwickelt sich ständig weiter, um den höheren Sicherheitsbedürfnissen unserer Kunden gerecht zu werden, und dieser ständige Wandel bietet unseren Mitarbeitern neue Karriere- und Lernmöglichkeiten. Wir belohnen den Erfolg und setzen uns voll und ganz dafür ein, die kontinuierliche Karriereentwicklung und das zukünftige Wachstum unserer Mitarbeiter zu fördern. 21.05.18 #opportunities http://somtxt.de/s/P3M

Die Empfänger der Bedrohungsdaten von BT waren dann in der Lage, geeignete Maßnahmen zu ergreifen, um ihre Kunden und Interessenvertreter vor den spezifischen Bedrohungen zu schützen. Europol hat 2013 das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) ins Leben gerufen, um die Reaktion der Strafverfolgungsbehörden auf Cyberkriminalität in der EU zu stärken, um EU-Bürger, Unternehmen und Regierungen besser vor Online-Kriminalität zu schützen. 17.05.18 #threats http://somtxt.de/s/Ps6

BT hat mit Europol, der Polizeibehörde der Europäischen Union, ein Memorandum of Understanding (MoU) unterzeichnet. Das MoU umfasst den Austausch von Wissen über wichtige Cyberbedrohungen und -attacken. Die Vereinbarung, die von beiden Parteien in der Europol-Zentrale in Den Haag unterzeichnet wurde, bietet BT und Europol einen Rahmen für den Austausch von Bedrohungsdaten und Informationen über Cyber-Sicherheitstrends. 15.05.18 #understanding http://somtxt.de/s/PsC

Bei einer anderen Veranstaltung am 11. Mai starteten Debjani Ghosh und der britische Staatssekretär für Digital, Kultur, Medien und Sport, Matt Hancock, die 4. Ausgabe der Indien-UK TECH Rocketship Awards. Die Auszeichnungen sollen indischen Start-ups im aufstrebenden Technologiefeld - Künstliche Intelligenz, Big Data, Cybersicherheit, Fintech, Medtech und IoT - dabei helfen, Zugang zu Kapital zu erhalten und eine Plattform für die globale Verbreitung über Großbritannien zu schaffen. 11.05.18 #tech http://somtxt.de/s/Psy

Zu den Lieferpartnern für den Inkubator gehören das Handelsunternehmen Manchester Digital, das Talent-Support-Services-Geschäft Complete Resourcing und das auf Vielfalt ausgerichtete Social Enterprise Sharp Futures. Das Zentrum richtet sich an Start-ups, die in den Bereichen künstliche Intelligenz, Datenanalyse, Cyber-Sicherheit, Cloud-Technologie, digitale Gesundheit und anderen Bereichen arbeiten. Es befindet sich im Manchester Technology Center, einem Teil des Circle Square. 11.05.18 #artificial http://somtxt.de/s/Psh

Angesichts der Komplexität einer großen, verteilten IT-Umgebung sollte die Sicherheit proaktiv geplant und vorbereitet werden und nicht als Reaktion auf Veränderungen in der Landschaft

dienen. Strategische und praktische Ansätze für Informationssicherheit Governance: Technologien und angewandte Lösungen präsentiert qualitativ hochwertige Forschungsarbeiten und Praxisartikel zu Management- und Governance-Fragen im Bereich der Informationssicherheit. 07.05.18 #strategic http://somtxt.de/s/Pst

zu einer Vielzahl von Branchen. Bevor er zu 1010data kam, war Afshin bei Equifax, wo er neue Datenprodukte und unterstützende Analysen für die Finanzdienstleistungsbranche entwickelte; Er leitete die Entwicklung von Prognosemodellen für Hypotheken bei Loan Performance (Corelogic); arbeitete bei BlackRock; das Forschungszentrum für Verizon und Norkom Technologies. Seine Publikationen umfassen Data Mining, Datenvisualisierung, Optimierung und künstliche Intelligenz. 03.05.18 #artificial http://somtxt.de/s/Pqx

Das Management Engagement Failure und Cyber Committee trifft auch auf Angriffe. auf einer jährlichen Basis Jede Schwäche in der Überprüfung der Investition ihre Information Manager und andere Sicherheit könnte Service-Provider in einer Störung der Gesamtleistung, die Handelsverfahren, Unabhängigkeit, Ressourcen, Buchhaltung und Zahlungs-Know-how und Compliance-Prozess führen. 30.04.18 #expertise http://somtxt.de/s/PqD

Die Rolle des Information Security Analyst umfasst umfangreiches Wissen in mehr als einem Bereich von unterstützenden Systemen oder Sicherheitstechnologien. Bietet Wartung, Problemlösung und Analyse von Sicherheitsrisiken und -chancen auf mehreren Plattformen. Bietet hochrangige Forschung zu ungewöhnlichen oder einzigartigen Projekten und empfiehlt strategische Anweisungen und Pläne, die unternehmensweite Sicherheitsprobleme auf der Grundlage von Sicherheitsrisikoprioritäten angehen. 26.04.18 #strategic http://somtxt.de/s/Pqy

Darüber hinaus werden die Kundendetails in fast allen Branchen benötigt und aufgrund der steigenden Anzahl von Cyber-Bedrohungen und Identitätsdiebstählen wird erwartet, dass das Consumer Identity Access Management in naher Zukunft ein gesundes Wachstum erleben wird. Die mangelnde Standardisierung und die wachsenden Bedenken hinsichtlich der Sicherheit im Bereich des Identitäts- und Zugriffsmanagements von Verbrauchern können voraussichtlich das Marktwachstum für das Consumer Identity Access Management beeinträchtigen. 19.04.18 #threats http://somtxt.de/s/P1H

Ressourcen Aktuelle Nachrichten Vorgestellte Jobs Anwendung Sicherheitsmanager - EXPERIAN - Dallas, TX SVP Leiter Informationssicherheit - Voya Financial - Windsor, CT Informationssicherheitstechniker Cyber Security Innovationsteam - Wells Fargo - Glen Allen, VA Leiter Informationssicherheit - Deluxe Entertainment - Burbank , CA Chief Datenschutzbeauftragter - Change Healthcare - Alpharetta, GA 17.04.18 #innovation http://somtxt.de/s/P1D

Die Teilnehmer erhalten Zugang zu einer Reihe von Schulungssitzungen zu aktuellen und neu aufkommenden Themen und Trends, die von unternehmerischer Nachhaltigkeit, Informationssicherheit und Governance bis hin zu Risiko, Betrug und Korruption reichen. Darüber hinaus werden bewährte Praktiken der Branche vorgestellt, um gemeinsame Herausforderungen anzugehen und Möglichkeiten des Wissensaustauschs zu nutzen. Weitere Informationen zur internationalen Konferenz der IIA 2018 finden Sie unter https://ic.globaliia.org/program 17.04.18 #opportunities http://somtxt.de/s/P1f

4.3 strategy

Es konzentriert sich hauptsächlich auf unbekannte Bedrohungen und improvisiert Cyber-Risiko-Analyse, und dies hilft, vorbeugende Maßnahmen zu ergreifen. Dark Web Intelligence liefert wichtige Einblicke in die Cybersicherheit und Bedrohungsdaten und bleibt ein Schlüsselelement für effektive Automatisierungslösungen in der Cyber-Sicherheitsbranche. Beispielkopie dieses Berichts erhalten @: http://qyreports.com/request-samplereport-id=81934 07.06.18 #trends http://somtxt.de/s/P9o

Dies ist datengesteuerte Entscheidungsfindung in Aktion, sagte Wiernicki. Mit den Ergebnissen des FCI Cyber Risk-Prozesses können Kunden eine kosteneffektive Risikominderungsstrategie für ihre Vermögenswerte und Flotten anwenden. Die Entwicklung folgt dem zweijährigen Forschungsvertrag von ABS mit dem Maritime Security Center - einem US-Heimatschutzministerium Center of Excellence - unter der Leitung des Stevens Institute of Technology und des US-Verteidigungsministeriums. 06.06.18 #strategy http://somtxt.de/s/P9F

Die Entscheidung, die Cyber-Policy-Rolle des Weißen Hauses zu eliminieren, ist empörend, vor allem angesichts der Tatsache, dass uns feindseligere Bedrohungen durch ausländische Gegner drohen als je zuvor, sagte Lieu. Dieser Schritt behindert die strategischen Bemühungen unseres Landes, Cybersicherheitsbedrohungen gegen unser Land zu begegnen. Glücklicherweise wird unser Gesetz diese Lücken in der Cybersicherheitsaufsicht der Regierung füllen, indem ein nationales Büro für den Cyberspace im Weißen Haus eingerichtet wird. 16.05.18 #strategy http://somtxt.de/s/Psg

DB Networks gibt Änderung des Firmennamens auf DB CyberTech bekannt Neuer Name unterstreicht das Know-how des Unternehmens bei der Anwendung von maschinellem Lernen für die prädiktive Prävention von Datenverlust vor Datenbanken SAN DIEGO, 11. Mai 2018 / PRNewswire / - DB CyberTech, ein Pionier auf dem Gebiet des maschinellen Lernens , gab heute bekannt, dass sich ihr Name von DB Networks zu DB CyberTech ändert, um sich besser auf ihre Strategie und Technologien in der Cyber-Sicherheit auszurichten. 12.05.18 #strategy http://somtxt.de/s/Psl

Die Trends und Zukunftsaussichten des Marktes sind auch in dem Bericht enthalten, der ein intellektuelles Verständnis der Branche vermittelt. Der Bericht quantifiziert den Marktanteil der wichtigsten Akteure der Branche und gibt einen detaillierten Einblick in das Wettbewerbsumfeld. Dieser Markt gliedert sich in verschiedene Segmente mit jeweils einer detaillierten geographischen Analyse für den Untersuchungszeitraum. 25.04.18 #trends http://somtxt.de/s/Pqe

Die Forschungsstudie ist eine deskriptive Analyse dieses Marktes, die die Markttreiber und -beschränkungen, die das gesamte Marktwachstum bestimmen, betont. Die Trends und Zukunftsaussichten des Marktes sind auch in dem Bericht enthalten, der ein intellektuelles Verständnis der Branche vermittelt. Der Bericht quantifiziert den Marktanteil der wichtigsten Akteure der Branche und gibt einen detaillierten Einblick in das Wettbewerbsumfeld. 25.04.18 #landscape http://somtxt.de/s/Pqe

Verschiedene Faktoren sind für den Wachstumspfad des Marktes verantwortlich, die ausführlich im Bericht behandelt werden. Darüber hinaus listet der Bericht die Beschränkungen auf, die den globalen Markt für Cyber-Sicherheit von Sicherheitsdiensten bedrohen. Außerdem werden die Verhandlungsmacht von Lieferanten und Käufern, die Bedrohung für die neuen Marktteilnehmer und den Produktersatz sowie der Grad des Wettbewerbs auf dem Markt untersucht. 18.04.18

#trends http://somtxt.de/s/P16

4.4 resources

BlackBerry ist ein Mobile-Native-Security-Software- und Dienstleistungsunternehmen, das sich der Sicherung von Personen, Geräten, Prozessen und Systemen für das heutige Unternehmen verschrieben hat. Das Unternehmen mit Sitz in Waterloo, Ontario, wurde 1984 gegründet und ist in Nordamerika, Europa, Asien, dem Nahen Osten, Lateinamerika und Afrika tätig. Das Unternehmen handelt unter den Tickersymbolen BB an der Toronto Stock Exchange und BBRY an der NASDAQ. 12.06.18 #europe http://somtxt.de/s/P99

Regionale Analyse: Der globale Markt für Sicherheits-Orchestrierung wird in Nordamerika, Europa, Asien-Pazifik und Rest der Welt untersucht. Es wird erwartet, dass der nordamerikanische Markt den größten Marktanteil im globalen Markt für Sicherheits-Orchestrierung aufgrund der Präsenz von wichtigen Akteuren, eines gut etablierten Forschungs- und Entwicklungszentrums und der Nachfrage nach hochmoderner Sicherheitstechnologie hat. 12.06.18 #europe http://somtxt.de/s/P9s

Die Dragonfly 2.0-Hacker, die von Homeland Security als Cyber-Akteure der russischen Regierung identifiziert wurden, verfolgten einen längeren Cyberangriff auf ein US-Kraftwerk und Computernetzwerke, die das Netz kontrollierten. Malware wurde in den Betriebssystemen verschiedener Organisationen und Unternehmen im US-amerikanischen Energie-, Nuklear-, Wasser- und kritischen Produktionssektor gefunden, und die Malware sowie andere Formen von Cyberangriffen wurden bis nach Moskau zurückverfolgt 07.06.18 #cyber http://somtxt.de/s/P9S

In dieser Region sind Organisationen bereit, schnell in neue Technologien wie Maschinenlernen, künstliche Intelligenz und Cyber-Sicherheit zu investieren. Die Faktoren, die das Wachstum des proaktiven Dienstleistungsmarktes in Nordamerika vorantreiben, sind eine stabile Wirtschaft, technologische Verbesserungen und optimierte Infrastrukturkosten. Die BFSI-Branche dürfte im Prognosezeitraum den größten Marktanteil halten. 06.06.18 #america http://somtxt.de/s/P9L

Nordamerika besteht aus entwickelten Volkswirtschaften wie den USA und Kanada. In dieser Region sind Organisationen bereit, schnell in neue Technologien wie Maschinenlernen, künstliche Intelligenz und Cyber-Sicherheit zu investieren. Die Faktoren, die das Wachstum des proaktiven Dienstleistungsmarktes in Nordamerika vorantreiben, sind eine stabile Wirtschaft, technologische Verbesserungen und optimierte Infrastrukturkosten. 06.06.18 #economy http://somtxt.de/s/P9L

Ziel dieser Zusammenarbeit ist die Entwicklung eines robusteren und widerstandsfähigeren globalen Cyber-Sicherheitsansatzes durch die Förderung von öffentlich-privaten Partnerschaften. Das WEF hat kürzlich gemeinsam mit Europol ein globales Zentrum für Cyber-Sicherheit eingerichtet, in dem sie gemeinsam versuchen werden, die Bekämpfung der Cyberkriminalität durch den Austausch von Wissen, Fachwissen und Informationen über Cyberbedrohungen zu verbessern. 30.05.18 #efforts http://somtxt.de/s/P3p

Mit Unterstützung eines Beratungsgremiums von erfahrenen C-Level-IT-Führungskräften umfasst der Gipfel die aktuellsten Trends in Bezug auf die Umsetzung von Geschäftsstrategien in IT-Funktionen sowie Cybersicherheit, Governance und disruptive Technologie. Wir haben die besten IT-Führungskräfte in Afrika rekrutiert, um die IT-Verantwortlichen auf dem sich schnell entwickelnden

Markt von heute zu präsentieren, um sicherzustellen, dass Sie der Zeit voraus sind. Über Kinetic 22.05.18 #leaders http://somtxt.de/s/P3S

Wir unterstützen den NIST-Cybersicherheitsrahmen und die Bemühungen, die Cybersicherheitspolitik mit diesen Richtlinien in Einklang zu bringen. Um die Anleger besser zu schützen, setzt sich SIFMA auch für eine stärkere Harmonisierung der regulatorischen Standards und der Aufsicht ein, um die effiziente Nutzung kritischer Cyber-Ressourcen zu verbessern. Wie bereits erwähnt, ist die Datensicherheit für unsere Kunden ein Thema, das von unserer nächsten Sprecherin und derzeitigen SIFMA-Vorsitzenden, Lisa Kidd Hunt, priorisiert wurde. 08.05.18 #policy http://somtxt.de/s/PsS

Dieses Buch präsentiert Arbeiten des NATO Advanced Research Workshop (ARW) mit dem Titel Ein Rahmen für eine militärische Cyber-Verteidigungsstrategie, der im April 2016 in Norfolk, Virginia, USA, stattfand. Der Workshop konzentrierte sich auf die wichtigsten prioritären Bereiche der Cyber-Verteidigung Cyber-Verteidigungspolitik umgesetzt und brachte Experten mit einer vielseitigen Mischung aus Hintergründen und Spezialitäten aus einer Gruppe von NATO-Mitgliedstaaten und Partnerländern zusammen. 07.05.18 #infrastructure http://somtxt.de/s/PsF

Das Buch gibt eine tiefgründige Vorstellung des am meisten gesprochenen Phänomens dieser Zeit. Das Buch eignet sich für ein breites Publikum von Absolventen bis hin zu Fachleuten / Praktikern und Forschern. Relevante Disziplinen für das Buch sind Telekommunikation / Netzwerksicherheit, Angewandte Mathematik / Datenanalyse, Mobile Systeme / Sicherheit, Engineering / Sicherheit kritischer Infrastrukturen und Militärwissenschaft / Sicherheit. 05.05.18 #policy http://somtxt.de/s/Psk

Relevante Disziplinen für das Buch sind Telekommunikation / Netzwerksicherheit, Angewandte Mathematik / Datenanalyse, Mobile Systeme / Sicherheit, Engineering / Sicherheit kritischer Infrastrukturen und Militärwissenschaft / Sicherheit. Die Wahrscheinlichkeit eines weltweiten Cyber-Konflikts ist gering. Dennoch könnte die Wahrscheinlichkeit von Cyber- Konflikten, regional oder sogar global, als sehr hoch eingeschätzt werden. 05.05.18 #policy http://somtxt.de/s/Psk

Wir müssen die Revolution des Wissens und der Information im Land einführen und Innovationen in allen Sektoren einführen , sagte er. Der Minister sagte, dass Pakistan ein enormes Potenzial habe, um Platz unter den Top-Ökonomien der Welt zu bekommen, für die wir auf modernen Boden Forschung betreiben müssen, fügte hinzu, dass die Regierung bereits Projekte zur Einrichtung von Exzellenzzentren für künstliche Intelligenz, Cybersicherheit, groß gestartet habe Daten, Cloud Computing und Roboter. 02.05.18 #sectors http://somtxt.de/s/Pq2

Shire ist abhängig von der Informationstechnologie, und seine Systeme und Infrastruktur sind bestimmten Risiken ausgesetzt, einschließlich von Serviceunterbrechungen, dem Verlust sensibler oder vertraulicher Informationen, Cyberangriffen und anderen Sicherheitslücken oder Datenlecks, die erhebliche negative Auswirkungen auf die Einnahmen von Shire haben könnten Zustand oder Ergebnisse der Operationen; Shire ist mit Risiken im Zusammenhang mit dem erwarteten Austritt des Vereinigten Königreichs aus der Europäischen Union konfrontiert; 01.05.18 #infrastructure http://somtxt.de/s/Pqg

Unser Ziel für das MSc-Programm ist es, den Fokus auf den strategischen Einsatz und die Implementierung von Cyber Security innerhalb einer Organisation zu legen. Wir möchten strategische Denker entwickeln, die die Cyberbedrohung für ein Unternehmen und seine Ressourcen verstehen und in der Lage sind, sichere Systeme aufzubauen und zu unterstützen, die

das strategische Wachstum eines Unternehmens unterstützen. 30.04.18 #resources http://somtxt.de/s/Pqm

Um unseren Kunden einen erstklassigen Service zu bieten, brauchen wir intern erstklassigen Support. Internal Firm Services ist ein Netzwerk von spezialisierten Support-Profis und umfasst Marketing, Rekrutierung, Humankapital, Finanzen, Technologie, Lernen und Entwicklung, Beschaffung, um nur einige zu nennen. Jedes Team spielt eine entscheidende Rolle dabei, sicherzustellen, dass wir die richtigen Ressourcen, Services und Technologien in unserem gesamten Unternehmen zur Verfügung haben. 28.04.18 #resources http://somtxt.de/s/Pqs

Nachdem er das FBI verlassen hatte, leitete Riggi die Cybersecurity and Financial Crimes Practice von BDO USA, wo er eng mit der AHA zusammenarbeitete, um AHAs Cybersecurity Education- und Awareness-Initiativen zu entwickeln und zu leiten. Bei der FBI Cyber Division leitete er das nationale Programm zur Entwicklung von Partnerschaften mit dem Gesundheitswesen und anderen kritischen Infrastruktursektoren für die Untersuchung und den Austausch von Informationen in Bezug auf nationale Sicherheit und kriminelle Cyberbedrohungen. 27.04.18 #infrastructure http://somtxt.de/s/Pq1

Folgen Sie uns auf Twitter @IndustryToday Die Studie umfasst geografische Analysen, die Regionen wie Nordamerika, Westeuropa, Zentralosteuropa, Naher Osten und Afrika, Lateinamerika und Asien-Pazifik sowie wichtige Akteure / Anbieter wie NXP Semiconductors, Continental AG, Daimler umfasst AG, Fortinet Inc., Capgemini SA, FICO usw. Der Bericht wird Nutzern helfen, Markteinblicke, zukünftige Trends und Wachstumsaussichten für den Prognosezeitraum 2015-2020 zu gewinnen. 27.04.18 #america http://somtxt.de/s/Pqj

Auf der einen Seite, sagte Guo, sollten souveräne Rechte über das Internet respektiert werden, während auf der anderen Seite weitere Anstrengungen unternommen werden sollten, um eine reibungslos vernetzte Welt aufzubauen. Neben dem Schutz unserer Informationsressourcen und der Souveränität des Internets sollten wir weitere Anstrengungen unternehmen, um dieses Konzept einer Gemeinschaft mit gemeinsamer Zukunft im Cyberspace zu bereichern, sagte Guo, der sich intensiv mit Chinas Internet-Plus-Strategie beschäftigt. 22.04.18 #resources http://somtxt.de/s/PqW

Geografisch sind die globalen Märkte für Informationssicherheitsprodukte und -dienstleistungen weitgehend in Lateinamerika, Europa, den Nahen Osten und Afrika sowie Asien-Pazifik unterteilt. Der Weltmarkt befindet sich in den meisten Bereichen noch in Exploration, aber er hat das vielversprechende Potenzial, in den nächsten Jahren stetig zu wachsen. Die Hauptakteure, die in diesen Markt investieren, sind Kanada, das Vereinigte Königreich, die Vereinigten Staaten, Indien, China und einige Länder des asiatisch-pazifischen Raums. 18.04.18 #america http://somtxt.de/s/P10

Im vergangenen Monat beschuldigte die Trump-Regierung Russland für eine Cyber-Attacke auf das US-Stromnetz. Amerikanische und britische Offizielle sagten, dass die am 16. April veröffentlichten Angriffe eine breite Palette von Organisationen betrafen, darunter Internetdienstanbieter, private Unternehmen und kritische Infrastrukturanbieter. Sie haben keine Opfer identifiziert oder Einzelheiten zu den Auswirkungen der Angriffe angegeben. 17.04.18 #cyber http://somtxt.de/s/P1u

Am Nachmittag rief er den schwedischen König Carl XVI Gusta an und tauschte sich über die Verstärkung der bilateralen Zusammenarbeit in verschiedenen Sektoren aus. Später wird er mit führenden Wirtschaftsführern interagieren und einen zukünftigen Fahrplan für die Zusammenarbeit in

Bereichen wie Handel und Investitionen, Wissenschaft und Technologie, saubere Energie und intelligente Städte entwerfen. Indien und Schweden werden am Mittwoch gemeinsam den indisch-nordischen Gipfel in Stockholm organisieren. 17.04.18 #leaders http://somtxt.de/s/P1b

Sie könnten sich in Zeiten der Spannung vorpositionieren, sagte Ciaran Martin, Geschäftsführer der Cyber-Verteidigungsagentur des britischen Cyber Security Centers, der hinzufügte, dass Millionen von Maschinen in der Kampagne ins Visier genommen wurden. Die russischen Angriffe haben eine Vielzahl von Organisationen betroffen, darunter Internet-Service-Provider, private Unternehmen und kritische Infrastrukturanbieter, sagten die Beamten. 16.04.18 #cyber http://somtxt.de/s/P1t

Es werden Anstrengungen unternommen, um die Merkmale der wirksamsten Programme sowohl für Opfer als auch für Straftäter zu ermitteln, um wirksame faktengestützte Praktiken für Programme im Bereich der opferorientierten Justiz in Kanada zu stärken. Im Rahmen der Sicherheits- und Polizeiarbeit im Zusammenhang mit dem G7-Gipfel der Staats- und Regierungschefs wird die Abteilung im Zeitraum 2018-2019 die wichtigsten internationalen Rahmenpläne für die Sicherheitskosten verwalten und mit Partnern zusammenarbeiten, um die Sicherheit der Veranstaltungen zu gewährleisten. 16.04.18 #efforts http://somtxt.de/s/P1F

4.5 support

Wir hoffen, dass sich die Regierung weiterhin auf die Erforschung, Entwicklung und Kommerzialisierung neuer Cyber-Sicherheitstechnologien konzentriert und Programme entwickelt, um das Wachstum der dynamischen Cybersicherheitsindustrie Kanadas zu unterstützen und unsere Cyber-KMU zu vergrößern eine globale Cyberökonomie von 100 Milliarden Dollar , fügte Watson hinzu. In der heutigen Bekanntmachung wurde nur ein Bruchteil der im Haushalt der Bundesregierung für das Jahr 2018 vorgesehenen Mittel berücksichtigt. 12.06.18 #support http://somtxt.de/s/P9K

Das kanadische Zentrum für Cyber-Sicherheit wird der Industrie eine zentrale Kontaktstelle für das Engagement zur Verfügung stellen - eine starke Bestätigung, dass Veränderungen notwendig sind. In der Vergangenheit hat sich der Ansatz der kanadischen Regierung für Cyber-Sicherheit auf zahlreiche Abteilungen ausgedehnt. ITAC begrüßt die Ankündigung von Scott Jones als ersten Leiter des kanadischen Zentrums für Cyber-Sicherheit und freut sich auf die enge Zusammenarbeit mit ihm und unseren Industriepartnern. 12.06.18 #partners http://somtxt.de/s/P9K

Die kanadische Regierung übernimmt eine führende Rolle in der Cyber-Sicherheit, um Organisationen und Kanadiern dabei zu helfen, den Wert von Cyber-Sicherheit zu erkennen und Bemühungen zu unterstützen, die Grundlagen der Cyber-Sicherheit in Kanada zu verbessern. Sie wird diese Bemühungen im Inland ergänzen, indem sie mit internationalen Partnern und Verbündeten zusammenarbeitet, um die Bedrohung Kanadas durch Cyberkriminelle und auch durch staatliche Akteure und ihre Stellvertreter, die uns möglicherweise Schaden zufügen wollen, zu verringern. 12.06.18 #partners http://somtxt.de/s/P9O

Digitale Technologien und das Internet werden für Innovation und wirtschaftliches Wachstum immer wichtiger, und eine starke Cyber-Sicherheit ist entscheidend für Kanadas Wettbewerbsfähigkeit, wirtschaftliche Stabilität und langfristigen Wohlstand. Zu diesem Zweck ist die Nationale Cybersicherheitsstrategie (die Strategie) darauf ausgerichtet, die Regierung Kanadas und ihre

Partner an das anhaltende Wachstum und den Wohlstand in dem Sektor anzupassen, auch wenn sich Technologien und Bedrohungen weiterentwickeln. 12.06.18 #partners http://somtxt.de/s/P9v

Alibaba-Gründer Jack Ma ist in einem Steuerungskomitee der indonesischen Regierung für E-Commerce tätig und berät in Bereichen wie Steuern, Internetsicherheit und Personalwesen. Der indonesische Kommunikationsminister Rudiantara sagte, es bestehe kein Interessenkonflikt in Mas Rolle, er beschreibe ihn als Guru, der helfen könne, das Potenzial des Landes zu verkaufen. Aber einige Richtlinien scheinen sich auf Mas Heimatgebiet zuzuwenden. 15.05.18 #minister http://somtxt.de/s/Psi

Um dies bis zum Ende des dritten Quartals zu unterstützen, wird die Behörde ein rund um die Uhr einsatzbereites Maritime Security Operation Center einrichten, das die Fähigkeiten zur Früherkennung, Überwachung, Analyse und Reaktion auf potenzielle Cyberangriffe erweitern soll. Die Cyber-Sicherheit ist heute eine der wichtigsten Herausforderungen, die die maritime Industrie ernst nehmen und als Priorität betrachten muss. Wir müssen über das Bewusstsein hinaus in Richtung Handeln gehen. 25.04.18 #support http://somtxt.de/s/PqX

Mit der Unterstützung beider Regierungen zielt die UK-India Tech Alliance darauf ab, die Zusammenarbeit in Bezug auf Qualifikationen und neue Technologien zu verbessern, indem sie die Entwicklung von Politiken unterstützt und Innovationen fördert. Die neue Partnerschaft zwischen der britischen und der indischen Technologiebranche wird auch das Wachstum von Kompetenzen in Bereichen wie künstliche Intelligenz, maschinelles Lernen, Big-Data-Analysen und Cyber-Sicherheit fördern. 18.04.18 #support http://somtxt.de/s/P1w

4.6 operations

Cyber Threat Intelligence Fusion und Analyse, zur Unterstützung von Cyber-Sicherheitsoperationen mit Kontext zu Cyberbedrohungen und Modellierung der neuesten Tools, Taktiken und Verfahren (TTPs) von Bedrohungsakteuren und zur proaktiven Überwachung von Cyberbedrohungen. Unterstützung und Wartung von Technologien zur Erkennung und Abwehr von Cyberbedrohungen und führen Überwachungs- und Reaktionsprozesse für Cyber-Sicherheit mit dem Ziel durch, die neuesten Cyberbedrohungen zu erkennen.Lead 31.05.18 #intelligence http://somtxt.de/s/P36

Es gibt mehrere Anwendungsbereiche der industriellen Cyber-Sicherheit. Einige von ihnen sind: Bereitstellung der Sicherheit der enormen Menge an kritischen Daten im Versorgungssektor, die Nutzung von Kommunikationsnetzen wie WLAN, Internet und Zigbee, die Verwendung von Energiemanagementsystemen zur Steuerung von Stromnetz-Oma-Betriebstechnologien wie Energiemanagementsysteme, SCADA, intelligente elektronische Geräte und Powerline-Kommunikation. 29.05.18 #cybersecurity http://somtxt.de/s/P38

NIC beschäftigt derzeit 4.500 Mitarbeiter in ganz Indien und wird im nächsten Jahr 800 Mitarbeiter einstellen, darunter 355 Cyber-Sicherheitsexperten, um die steigenden Risiken der Cyber-Sicherheit zu bewältigen. NIC bietet Technologieunterstützung für alle Governance-Dienste und beherbergt fast 10.000 Websites der Regierung 28.05.18 #operations http://somtxt.de/s/P3K

Das GCSB stellt seine CORTEX-Fähigkeiten zur Cyber-Verteidigung bereits einer Vielzahl national bedeutender Organisationen zur Verfügung. Malware-freie Netzwerke werden ein zusätzlicher Service sein, der vielen anderen Organisationen eine zusätzliche Schutzschicht bietet.

Organisationen von nationaler Bedeutung wurden durch einen Prozess identifiziert, der von der Abteilung des Premierministers und Kabinetts geleitet wurde. 27.05.18 #capabilities http://somtxt.de/s/P3O

Unser Cybersecurity-Service baut auf der Erfahrung von GHD in Design, Betrieb und Wartung der Infrastruktur auf, um diese Risiken für unsere Kunden zu bewältigen, sagte Parakala. Parakala fügte hinzu, dass GHD Digital sich für eine Partnerschaft mit Virsec entschieden hat, da Virsec-Lösungen eine neue Möglichkeit bieten, Prozesse und Speicher in Echtzeit zu schützen. Die Lösung bildet eine akzeptable Anwendungsausführung ab und erkennt durch Angriffe verursachte Abweichungen sofort. 22.05.18 #operations http://somtxt.de/s/P3r

Hongkong, China, 17. Mai 2018 /ChinaNewswire / - BT beteiligt sich an Europol, um einen sichereren Cyberraum zu schaffen BT hat mit Europol, der Agentur der Europäischen Union für die Zusammenarbeit in Strafverfolgungsbehörden, ein Memorandum of Understanding (MoU) unterzeichnet Wissen über die wichtigsten Cyberbedrohungen und -attacken auszutauschen, während die beiden Organisationen ihre Bemühungen verstärken, einen sichereren Cyberspace für Bürger, Unternehmen und Regierungen zu schaffen. 17.05.18 #european http://somtxt.de/s/Ps6

Cyberbedrohungen sind ein ständiges Problem für Unternehmen und dürften bis 2018 Schäden in Höhe von über einer Billion Dollar verursachen, prognostizierte der Bericht. Um sich besser vor diesen Angriffen zu schützen, erwägen Cybersicherheitsanbieter maschinelles Lernen, um eine dynamischere und intuitivere Verteidigung zu bieten. Der Bericht legt nahe, dass der Cybersecurity-Markt für maschinelles Lernen den Wert der Ausgaben für Big Data, Intelligence und Analytics bis 2021 auf 96 Milliarden US-Dollar steigern wird. 15.05.18 #intelligence http://somtxt.de/s/PsR

Hyderabad, 10. Mai: Künstliche Intelligenz und maschinelles Lernen Der Cybersicherheits-Tool-Entwickler BluSapphire hat am Donnerstag die Eröffnung seines Advanced Threat Research Centers (ATRC) und des Security Operations Center (SOC) angekündigt. In der ATRC- und SOC-Einrichtung wird BluSapphire aktiv die neuesten Malware-Techniken testen, die von Angreifern verwendet werden, und mithilfe modernster Machine-Learning-Modelle Abwehrtechniken entwickeln. 11.05.18 #intelligence http://somtxt.de/s/Psn

Die Zusammenarbeit zwischen Indien und den Vereinigten Staaten im Bereich der globalen Sicherheit ist die Zusammenfassung eines Workshops, den die Nationale Akademie der Wissenschaften (NAS) zusammen mit ihrem mehr als 15-jährigen Partner, dem National Institute for Advanced Studies (NIAS) in Bangalore, Indien, abgehalten hat. Der Workshop identifizierte und untersuchte potenzielle Bereiche für die inhaltliche wissenschaftliche und technische Zusammenarbeit zwischen den beiden Ländern in Fragen der nuklearen Materialsicherheit. 09.05.18 #cooperation http://somtxt.de/s/Psf

Die Einstellung ist nicht in großer Zahl, aber Indien wird zu gegebener Zeit aufholen. Gegenwärtig bauen die Rechtsabteilungen, Cybersecurity-Experten und Informationsbeauftragte Kapazitäten auf oder prüfen Zertifizierungen nach der DSGVO, um Organisationen bei der bevorstehenden Änderung zu unterstützen. Der indische IT-Sektor, der in Europa stark vertreten ist, bereitet sich auf die neuen Anforderungen vor, die sich aus der neuen DSGVO-Regelung ergeben. 09.05.18 #cybersecurity http://somtxt.de/s/PsX

Ein Informationsaustausch- und Analysezentrum kann dem NRK und Kernkraftwerken in den USA

auch Erkenntnisse und Fachwissen vermitteln. Das Nuclear Energy Institute (NEI) behauptet, dass kritische Systeme in einer Kernreaktoranlage nicht mit dem Internet oder dem Internet verbunden sind das interne Netzwerk der Einrichtung und somit das Cybersicherheitsrisiko für diese kritischen Systeme minimiert wird. Die Kernenergie ist jedoch immer hoch. 02.05.18 #cybersecurity http://somtxt.de/s/Pq6

Und David Ferbrache, CTO von Cyber, KPMG UK sagt: Cyberkriminalität kostet britische Institutionen Milliarden, aber noch wichtiger: Sie erodiert das Vertrauen und macht Kunden anfällig. Als Gemeinschaft müssen wir mehr tun, um die Denkweise der Kriminellen zu verstehen, Informationen über ihre Handlungen zu teilen und bereit zu sein, diese Operationen zu stören. In dem heute vorgelegten Bericht werden die Herausforderungen hervorgehoben, vor denen die Institutionen bei der Bekämpfung der Internetkriminalität stehen, und eine Agenda für Maßnahmen festgelegt. 25.04.18 #community http://somtxt.de/s/Pqa

Premierminister Narendra Modi wird wahrscheinlich auch daran teilnehmen. Die SCO mit Sitz in Peking wurde 2001 gegründet. Die SCO besteht aus China, Russland, Kasachstan, Usbekistan, Tadschikistan, Kirgisistan, Indien und Pakistan und zielt auf die militärische Zusammenarbeit zwischen den Mitgliedsstaaten ab Asien und gemeinsame Arbeit gegen Cyber-Terrorismus. 24.04.18 #cooperation http://somtxt.de/s/PqN

Während dieses Vortrags werden ein SANS-Experte und Dennis Murphy, Director of US Operations, die Erfahrungen aus mehr als 5 Jahren Erfahrung in der Verwaltung großer Netzwerksicherheitsüberwachungsprojekte und darüber, wie wir diese Erfahrungen in Selbstlernfähigkeiten, intelligente Automatisierung und fortschrittliche Bedrohungen umgesetzt haben, diskutieren Bibliotheken, die durch die Analyse von Informationsquellen und realen Bedrohungen, die durch Zusammenarbeit mit Kunden entdeckt wurden, kontinuierlich aktualisiert werden. 20.04.18 #capabilities http://somtxt.de/s/Pqc

Sicherheitsressourcen sind knapp, und viele Organisationen suchen nach Anbietern, die als Dienst eine leichte und schnelle Reaktionsfähigkeit bieten. Jedes Unternehmen hat unterschiedliche Reifegrade bei der Reaktion auf Vorfälle. Informieren Sie sich über Erkennung und Reaktion als Service und erfahren Sie, wie Sie den richtigen Partner und das richtige Bereitstellungsmodell finden, um Unternehmen bei ihren Ad-hoc- oder etablierten Methoden zur Erkennung und Abwehr von Cyber-Angriffen zu unterstützen. 19.04.18 #capabilities http://somtxt.de/s/P1V

Während des Gipfels versprach der Premierminister, die Zusammenarbeit zwischen Indien und den nordischen Ländern zu vertiefen und konzentrierte sich auf wichtige Fragen in Bezug auf globale Sicherheit, Wirtschaftswachstum, Innovation und Klimawandel, sagte das indische Außenministerium in einer Erklärung nach dem Treffen. Klicken Sie hier, um den vollständigen IANS-Bericht zu lesen. 18.04.18 #cooperation http://somtxt.de/s/P1I

Der Bericht baut auf früheren DHS-Berichten und Advisories aus Großbritannien, Australien und der Europäischen Union auf, heißt es auf der Website. Das FBI hat großes Vertrauen darauf, dass russische staatlich finanzierte Cyber-Akteure kompromittierte Router einsetzen, um Man-in-the-Middle-Angriffe zur Unterstützung von Spionage, zur Extraktion von geistigem Eigentum, zum dauerhaften Zugriff auf Opfernetzwerke und möglicherweise zur Vorbereitung künftiger offensiver Operationen durchzuführen , die Webseite hinzugefügt. 17.04.18 #operations http://somtxt.de/s/P1Z

5 defence & threat

5.1 Defence

Professor Michael Frater von UNSW Canberra sagte, dass das UNSW Defence Research Institute ein Licht auf die bahnbrechenden Forschungsergebnisse des akademischen Personals der Universität werfen würde. UNSW Canberra ist eine der weltweit führenden Forschungseinrichtungen, ein Pionier in der Verteidigung und ein weltweit führendes Unternehmen in der Cyber Security-Bildung, sagte Frater. Es ist das natürliche Zuhause für Australiens größtes universitäres Forschungsinstitut für Verteidigung. 24.05.18 #studies http://somtxt.de/s/P3d

Der vollständige Bericht ist http://www.theinsightpartners.com/inquiry/TIPTE100001086 Die Global Network Security Appliance Marktanalyse bis 2025 ist eine spezialisierte und gründliche Studie der Netzwerksicherheitsgeräteindustrie mit einem Fokus auf die globaler Markttrend. Ziel des Berichts ist es, einen Überblick über den globalen Markt für Netzwerksicherheitsgeräte mit detaillierter Marktsegmentierung nach Typ, Bereitstellungsmodus, vertikaler Ausrichtung und geografischer Ausrichtung zu geben. 18.05.18 #threat http://somtxt.de/s/P37

Ransomware-Angriffe haben sich als eine der wichtigsten Gefahren für die Cyber-Sicherheit globaler Organisationen herausgestellt, so der kürzlich veröffentlichte Bericht Data Breach Investigations von Verizon aus dem Jahr 2018. Die 11. Ausgabe des Berichts enthält Daten von 67 beitragenden Organisationen und Analysen von mehr als 53.000 Vorfällen und 2.216 Verstößen aus 65 Ländern. Es besagt, dass Ransomware die häufigste Art von Malware ist, die in 39% der durch Malware verursachten Datenschutzverletzungen gefunden wird. 09.05.18 #threat http://somtxt.de/s/Psr

Der Schutz Ihrer Kunden und Ihres Unternehmens vor Betrug und Datenschutzverletzungen hat im digitalen Zeitalter oberste Priorität. Cyber-Sicherheit stellt eine allgegenwärtige Bedrohung dar, aber künstliche Intelligenz kann jetzt einen gewissen Schutz gegen diese Angriffe und Verstöße bieten. USAA, Bank of America, BBVA und PayPal sind einige Finanzorganisationen, die KI einsetzen, um sie und ihre Kunden vor Betrug zu schützen. 27.04.18 #threat http://somtxt.de/s/PqI

Die Staats- und Regierungschefs der NATO-Ukraine-Kommission haben bei ihrem Treffen am 9. Juli 2016 in Warschau die GAP für die Ukraine gebilligt. Ziel des Pakets ist es, die Unterstützung der NATO für die Ukraine zu konsolidieren und auszubauen, um die Verteidigungs- und Sicherheitsinstitutionen des Landes effektiver, effizienter und rechenschaftspflichtiger zu machen. Im Rahmen der GAP wurden im Rahmen des SPS-Programms mehrere Aktivitäten in den vorrangigen Bereichen der Zusammenarbeit der Ukraine durchgeführt. 18.04.18 #institutions http://somtxt.de/s/P1G

Die beiden Seiten hätten sich auf einen gemeinsamen Aktionsplan geeinigt und hinzugefügt, dass sich Indien und Schweden unter anderem darauf geeinigt hätten, die Zusammenarbeit in Bereichen der Rüstungsproduktion und der Cybersicherheit zu verstärken. PM Modi sagte auch, dass Schweden einen starken Beitrag zum Programm Make in India geleistet habe. Dies ist mein erster Besuch in Schweden und der Besuch eines indischen Premierministers nach fast 30 Jahren. 17.04.18 #defence http://somtxt.de/s/P1q

Premierminister Narendra Modi nannte Schweden Indiens natürlichen Partner beim Projekt Make in

India. Der wachsende Beitrag von Stockholm zur Entwicklung Indiens sei ein stolzer Moment für uns alle. Der Premierminister gab am Dienstag in Stockholm mit seinem schwedischen Amtskollegen Stefan Lofven eine gemeinsame Erklärung ab. Dies ist Modis erster Besuch in Schweden und er ist auch die erste indische Premiere, die das Land in den letzten 30 Jahren besucht hat. 17.04.18 #defence http://somtxt.de/s/P1b

Ein Sprecher des Nationalen Cybersicherheitszentrums fügte hinzu: Wir sind immer wachsam gegenüber Angriffen, wo immer sie herkommen, und wir verfügen über ein breites Spektrum an Fähigkeiten, auf die wir uns bei Bedarf stützen können. In einer robusten Verteidigung ihrer Handlungen wird der Premierminister eine Erklärung an die Abgeordneten abgeben, in der sie darauf dringen, dass Großbritannien Syrien in unserem nationalen Interesse treffen muss. Geheimdienstexperten akzeptieren, dass die wahrscheinlichste Reaktion Russlands durch verdeckte Cyberkriegsführung sein wird. 15.04.18 #defence http://somtxt.de/s/P1W

5.2 sector

Statt mehrerer Abteilungen wird das Cyber-Zentrum ein einziges Fenster für Expertenberatung und -dienste für Regierungen, kritische Infrastrukturbetreiber, den öffentlichen und den privaten Sektor bieten, um ihre Cyber-Sicherheit zu stärken. Die Strategie beinhaltet auch die Ankündigung einer neuen Nationalen Koordinierungsstelle zur Bekämpfung der Cyberkriminalität im Rahmen des RCMP, die Koordinierungsdienste für die Strafverfolgung zur Bekämpfung der Cyberkriminalität bereitstellen wird. Vorgeschlagene Maßnahme 12.06.18 #national http://somtxt.de/s/P9v

Eric Rosenbach, Co-Direktor des Belfer Zentrums für Wissenschaft und internationale Angelegenheiten der Harvard Kennedy School und ehemaliger Stabschef des Verteidigungsministers und stellvertretender Verteidigungsminister für Heimatschutz und globale Sicherheit, bezeugte vor dem US-Senatsausschuß für Geheimdienste 21. März 2018 über die russische Interferenz bei den US-Wahlen 2016 31.05.18 #committee http://somtxt.de/s/P30

Wir brauchen eine fundierte rechtliche Bewertung und modernste technische Fähigkeiten. Dort müssten der private Sektor und die Regierungsbehörden zusammenarbeiten, sagte er auf der von FICCI organisierten Konferenz. Der Innenminister sagte, dass man, um der Bedrohung durch Cyberangriffe entgegenzuwirken, Geschwindigkeit und Agilität haben muss und um den Angreifern voraus zu bleiben, muss man sich anpassen und verbessern. 31.05.18 #sector http://somtxt.de/s/P32

Die Regierung muss das Mandat der nationalen Sicherheit erfüllen und die individuelle Sicherheit gewährleisten. Sicherheitsbehörden müssen sich über die besten Praktiken im Klaren sein, und alle Agenturen müssen zusammenarbeiten, um solche Angriffe zu verhindern, solche Angriffe zu untersuchen und die Angreifer strafrechtlich zu verfolgen, sagte er. Der Innenminister sagte, viele der Cyberangriffe des Landes seien auf Jamtara, Jharkhand, zurückzuführen, von wo aus viele Angreifer ihren Modus Operandi betreiben. 31.05.18 #country http://somtxt.de/s/P32

Ressourcen Aktuelle Nachrichten Vorgestellte Stellen Chief Information Security Officer - Mohegan Sun - Uncasville, Chief Information Security Officer von CT - Entelo - San Francisco, Kalifornien Chief Information Security Officer - Oliver James Associates - Raleigh, North Carolina Oliver Associates - Raleigh, NC Dir und Chief Privacy Offizier - UC Gesundheit - Cincinnati, OH Informationssicherheits-Ingenieur Cybersicherheit-Innovationsteam - Wells Fargo - Glen Allen, VA 23.05.18 #engineer

http://somtxt.de/s/P3I

Die Ankündigung erfolgt aufgrund von Bedenken hinsichtlich der Sicherheit der US-Kongresswahlen im Jahr 2018 und zahlreichen prominenten Hackern von US-Unternehmen. Die Vereinigten Staaten sehen sich Bedrohungen durch eine wachsende Zahl raffinierter bösartiger Akteure ausgesetzt, die den Cyberspace ausnutzen wollen. Zu den Motivationen gehören Spionage, politische und ideologische Interessen sowie finanzieller Gewinn, so der 35-seitige Bericht von Reuters vor seiner Veröffentlichung. 15.05.18 #cyberspace http://somtxt.de/s/Psm

Ressourcen Aktuelle Nachrichten Vorgestellte Jobs CHIEF PRIVACY OFFICER - Bundesstaat Arizona - Phoenix, AZ Chief Datenschutzbeauftragter - BBC - London W12 Anwendungssicherheitsmanager - EXPERIAN - Dallas, TX Informationssicherheitstechniker Cyber Security Innovationsteam - Wells Fargo - Glen Allen, VA Chief Information Sicherheitsbeauftragter (CISO) - Georgetown Universität - Washington, DC 15.05.18 #engineer http://somtxt.de/s/PsZ

Laut Zacks ist die KEYW Corporation mit ihren Tochtergesellschaften in der Bereitstellung von geschäftskritischen Cyber-Sicherheit und Cyber-Überlegenheit Lösungen für Verteidigung, Nachrichtendienste und nationale Sicherheitsbehörden tätig. Seine Lösungen, Dienste und Produkte unterstützen die Erfassung, Verarbeitung, Analyse und Nutzung von nachrichtendienstlichen Informationen und Informationen im Cyberspace. Beginnen Sie die Unterhaltung oder lesen Sie mehr unter Daily Political. 12.05.18 #national http://somtxt.de/s/Ps1

Cyberkriminalität betrifft weltweit über eine Million Menschen pro Tag, und Cyberangriffe auf öffentliche Einrichtungen und Unternehmen nehmen zu. In diesem Buch werden die sich entwickelnden Cybersicherheitspolitiken und -strategien der Europäischen Union hinterfragt und argumentiert, dass trotz des Fortschritts noch viel zu tun bleibt, um in Zukunft einen sicheren und widerstandsfähigen Cyberspace zu gewährleisten. Die Kosten der Internetkriminalität für das Vereinigte Königreich werden derzeit auf 18 bis 27 Milliarden Pfund Sterling geschätzt. 07.05.18 #cyberspace http://somtxt.de/s/PsL

CYBERSECURITY Wahlbeobachter sagen, dass Indiana vor Cybersicherheitsangriffen sicher bleibt, weil der Staat Vorkehrungen trifft, um seine Wahlsysteme zu schützen. Indiana-Außenminister Connie Lawson schrieb kürzlich in einem Op-Ed, um sicherzustellen, dass die Wähler alle Wahlausrüstungen testen, die vor den Wahlen im Land verwendet werden, und mit dem Department of Homeland Security zusammenarbeitet, um Cyberbedrohungen besser zu identifizieren. 05.05.18 #homeland http://somtxt.de/s/Psc

Wir brauchen eine ernsthafte Debatte über Irlands Fähigkeiten im Bereich Sicherheit und Verteidigung. Und ich entschuldige mich nicht für mehr Ressourcen und bessere Bedingungen für unsere Streitkräfte, um sicherzustellen, dass sie über die Ausrüstung, die Ressourcen, die Karrierewege und die operativen Kapazitäten verfügen, um ihre Aufgabe bei der Verteidigung dieses Landes zu erfüllen. Es gibt drei Gründe, warum jetzt die richtige Zeit ist, die irische Sicherheit und Verteidigung zu überprüfen. 03.05.18 #country http://somtxt.de/s/PqH

Und ich entschuldige mich nicht für mehr Ressourcen und bessere Bedingungen für unsere Streitkräfte, um sicherzustellen, dass sie über die Ausrüstung, die Ressourcen, die Karrierewege und die operativen Kapazitäten verfügen, um ihre Aufgabe bei der Verteidigung dieses Landes zu erfüllen. Es gibt drei Gründe, warum jetzt die richtige Zeit ist, die irische Sicherheit und Verteidigung

zu überprüfen. Erstens, die Debatte über die Zukunft Europas ist im Gange, und Sicherheit wird in dieser Debatte groß geschrieben. 03.05.18 #country http://somtxt.de/s/PqH

WAS SIE BEWIRKEN KÖNNEN Der Cyber Security Data Science Engineer setzt modernste Technologien ein, um statistische Analyse- und Inferenz-Datenmodellierungs-Clustering und Predictive Analysis durchzuführen. Als wichtiges Mitglied des technischen Teams werden Sie Cyber- und Netzwerksicherheitsfragen in ausgereifte Modelle übersetzen und neue Einsichten gewinnen, um Geschäftsentscheidungen zu treffen und sich gegen Cyber-Angriffe zu wehren. 03.05.18 #engineer http://somtxt.de/s/PqU

Es war eine Rote Mannschaft gegen eine Blaue Mannschaft, mit 22 Blue Teams, die in die Rolle von nationalen Schnellreaktionsteams versetzt wurden, die eingesetzt wurden, um einem fiktiven Land dabei zu helfen, mit einem großen Cyber-Vorfall umzugehen. Zu den Blauen Teams gehörten Teams aus der NATO und der Europäischen Union, die hauptsächlich aus nationalen militärischen und zivilen Cyber-Sicherheitsexperten bestanden. Locked Shields umfassten insgesamt etwa 4.000 virtuelle Systeme und mehr als 2.500 Angriffe. 29.04.18 #military http://somtxt.de/s/Pq9

Travis Sharp ist Offizier im US Navy Reserve und Doktorand in Sicherheitsstudien an der Woodrow Wilson School für öffentliche und internationale Angelegenheiten an der Princeton University. Seine aktuellen Forschungsprojekte untersuchen das militärische Engagement, die Cyber-Sicherheit und die Verteidigungsstrategie. Zuvor war er als wissenschaftlicher Mitarbeiter am Center for a New American Security und am Center for Arms Control and Non-Proliferation tätig. 28.04.18 #military http://somtxt.de/s/Pq3

Wir sind im ganzen Land landesweit präsent und bieten Dienstleistungen für Kunden im gewerblichen und öffentlichen Sektor an. BRACHIN LLC bietet Business Intelligence, Informationssicherheit, Einhaltung gesetzlicher Vorschriften sowie Technologie-Software und Beratungsdienste. Wir betreuen Kunden und bieten Unterstützung bei der Verwaltung von Informationen und Geschäftsrisiken, bei Big Data, bei der Verbesserung von Analyseabläufen und bei der Verbesserung der Business Intelligence-Leistung. 24.04.18 #national http://somtxt.de/s/Pqt

Im Jahr 2015 haben wir eine neue Partnerschaft für Verteidigung und internationale Sicherheit (DISP) zugesagt, um Sicherheit und Verteidigung zu einem Eckpfeiler unserer Beziehungen zu machen. Die Art der Bedrohungen, mit denen wir konfrontiert sind, ändert sich weiter - daher müssen wir innovativ und agil reagieren. Wir werden Technologien entwickeln, herstellen und herstellen, die diese Bedrohungen angehen. und unsere Sicherheits- und Streitkräfte werden Technologien, Fähigkeiten und Ausrüstung teilen. 18.04.18 #military http://somtxt.de/s/P12

NC4 bietet auch Lösungen für die Cyber-Threat-Sharing, sowohl durch sichere Collaboration-Services als auch kürzlich (über Soltra Edge), durch automatisierte, strukturierte und standardisierte (STIX / TAXII) Mechanismen. NC4-Lösungen werden von Unternehmen des Privatsektors verwendet, die in den Bereichen Finanzdienstleistungen, Hightech, Versicherung, Fertigung, Luft- und Raumfahrt und Verteidigung, Öl und Gas, Pharma und Gesundheitswesen sowie in anderen Branchen tätig sind. 17.04.18 #sector http://somtxt.de/s/P19

Einige Cybersecurity-Experten des privaten Sektors haben die US-Regierung dafür kritisiert, dass sie zu langsam ist, um Informationen über Cyber-Angriffe zu veröffentlichen. Die Ankündigung vom Montag scheint den Wunsch zu widerspiegeln, eine Drohung schnell und breit zu verbreiten, noch

bevor Beamte ihre Breite vollständig verstehen. Ein hochrangiger US-Beamter, der unter der Bedingung der Anonymität sprach, sagte, es habe in den letzten Jahren einen stetigen Anstieg der russischen Cyberangriffe gegeben. 17.04.18 #sector http://somtxt.de/s/P1T

5.3 public

Ein ICO-Sprecher sagte am Mittwoch: Ein Vorfall mit Dixons Carphone wurde uns gemeldet und wir stehen in Verbindung mit dem National Cyber Security Center, der Financial Conduct Authority und anderen relevanten Agenturen, um die Details und Auswirkungen auf die Kunden zu ermitteln. Jeder, der sich über verlorene Daten und seine Verwendung Gedanken macht, sollte den Ratschlägen von Action Fraud folgen. 13.06.18 #agencies http://somtxt.de/s/P9B

In einer Stellungnahme erklärte das britische National Cyber Security Center (NCSC), dass es dem britischen Fußballverband vor der Abreise nach Russland für die FIFA Fussball-Weltmeisterschaft 2018 fachkundige Ratschläge zur Cyber-Sicherheit gegeben habe. Der private Cyber-Sicherheitsexperte Patrick Wardle sagte, die offiziellen Warnungen seien wirklich gute Ratschläge. Wenn ich nach Russland reise, bringe ich Brenner -Geräte mit, also wenn sie gehackt werden, ist es nicht wirklich wichtig, sagte er. 13.06.18 #private http://somtxt.de/s/P90

Der NCSC, eine Zweigstelle der Government Communications Headquarters (GCHQ), Großbritanniens elektronische Abhörbehörde, warnte auch die Öffentlichkeit. Der private Cyber-Sicherheitsexperte Patrick Wardle sagte, die offiziellen Warnungen seien wirklich gute Ratschläge. Wenn ich nach Russland reise, bringe ich Brenner -Geräte mit, wenn sie gehackt werden, spielt es keine Rolle. 12.06.18 #private http://somtxt.de/s/P9m

Der Schutz der kanadischen Wirtschaft vor Cyber-Angriffen erfordert eine umfassende gemeinschaftliche Herangehensweise und Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor. Kanada hat das Potenzial, weltweit führend in der Cybersicherheit zu sein - und es ist entscheidend, dass wir nicht zurückfallen. ITAC hat die Regierung bereits aufgefordert, ein Programm zur Cyber-Zertifizierung einzuführen, insbesondere für kleine und mittlere Unternehmen (KMU). 12.06.18 #public http://somtxt.de/s/P9K

Petra Nijenhuis-Timmers, koordinierende Policy Officer, Task Force Cyber, niederländisches Außenministerium Paolo Prinetto, Direktor, Cybersecurity National Lab, CINI Theo van Ruijven, leitender Experte für den Schutz kritischer Infrastrukturen, TNO Nynke Stegink, koordinierende Policy Officer Public Private Cooperation in Cybersecurity , National Cyber Security Center, niederländisches Ministerium für Justiz und Sicherheit 11.06.18 #public http://somtxt.de/s/P9Y

Deshalb ist es so wichtig, mit unseren Kollegen und Partnern in den anderen Unterzeichnern dieses Memorandums zusammenzuarbeiten. Im Rahmen des Cyber Defence Policy Framework von 2014 wurde die Förderung der zivil-militärischen Zusammenarbeit und der Synergien mit der EU-weiten Cyberpolitik, den einschlägigen EU-Institutionen und -Agenturen sowie mit dem Privatsektor gefordert. ENISA, EDA, EUROPOL und CERT-EU begannen im Jahr 2016 erste Gespräche, die schließlich zu dieser Meilenstein-Signatur führten. 28.05.18 #agencies http://somtxt.de/s/P3Z

Die Agenturen werden sich selbst überlassen, sich selbst, ihre Interessen und ihre Autorität vor andere stellen, prophezeite Stifel, jetzt Cyber Policy Director bei Public Knowledge. Das Ergebnis, sagte sie, könnte durchsetzungsfähigeres Handeln des US Cyber Command sein, der militärischen

Einheit, die für die Cyberkriegsführung verantwortlich ist, oder eine Rückkehr zu den Tagen, als 3-4 Komponenten der Abteilung in einem US-Privatsektor an erster Stelle standen Entität wurde verletzt. 10.05.18 #agencies http://somtxt.de/s/Psu

Wer hat dich gehackt? Wenn man weiß, wer hinter einem Hack steckt, kann das für den privaten Sektor nützlich sein, aber der Akt der Identifizierung selbst wird am besten den Militär- und Geheimdiensten überlassen, sagen Experten. Das Hacker-Playbook Eine große Cyber-Lücke bei Energieunternehmen auf der ganzen Welt ist zu einem virtuellen Handbuch geworden, um moderne Angriffe auf kritische Infrastrukturen zu erkennen und zu verhindern. 19.04.18 #private http://somtxt.de/s/Pqk

In der gemeinsamen Erklärung hieß es, dass multiple Quellen - einschließlich Forschungseinrichtungen und Verbündete des privaten und öffentlichen Sektors für Cyber-Sicherheit - solche Aktivitäten den Regierungen der USA und des Vereinigten Königreichs gemeldet hätten. Herr Martin sagte: Dies ist das erste Mal, dass die USA und das Vereinigte Königreich, als sie einen Cyber-Angriff auf Russland zurückführten, gleichzeitig der Industrie einen gemeinsamen Ratschlag zur Verfügung gestellt haben, wie sie die Risiken von Angriffen handhaben können. 17.04.18 #governments http://somtxt.de/s/P1l

Das britische nationale Cybersicherheitszentrum hat in Zusammenarbeit mit dem FBI und dem US-Heimatschutzministerium eine beispiellose gemeinsame technische Warnung herausgegeben, die die Bedrohung im öffentlichen und privaten Sektor aufzeigt. LEADERS in Großbritannien und den USA haben eine offizielle Warnung vor bösartigen Cyberaktivitäten herausgegeben Von Russland, mit der Befürchtung, dass persönliche Informationen über prominente Bürger enthüllt werden könnten. 17.04.18 #public http://somtxt.de/s/P1j

5.4 communications

In einer Erklärung sagte das britische Cyber Security Center, dass es dem britischen Fußballverband vor dem Abflug nach Russland für die FIFA Fussball-Weltmeisterschaft ™ 2018 fachkundige Ratschläge zur Cybersicherheit geben werde. Der NCSC, eine Zweigstelle des Hauptquartiers der Regierungskommunikation (GCHQ), Großbritanniens elektronische Abhöragentur, warnte auch die Öffentlichkeit. 13.06.18 #advice http://somtxt.de/s/P9p

Cyber Security für Oil Gas - Global Market Status- und Trendbericht 2013-2023 bietet eine umfassende Analyse zur Cyber Security für die Öl- und Gasindustrie, die aus der Sicht des Lesers besteht und detaillierte Marktdaten und eindringliche Einblicke liefert. Unabhängig davon, ob der Kunde Brancheninsider, potentieller Neueinsteiger oder Investor ist, der Bericht liefert nützliche Daten und Informationen. Zu den wichtigsten Fragen, die in diesem Bericht beantwortet werden, gehören: 08.06.18 #global http://somtxt.de/s/P9X

Eine detaillierte Analyse dieser Faktoren ermöglicht es dem Bericht, eine verlässliche Prognose hinsichtlich der zukünftigen Wachstumsdynamik der Künstlichen Nachrichtendienste in der Sicherheit vorzulegen. Dieser Bericht untersucht die globalen Artificial Intelligence Services auf dem Sicherheitsmarkt, analysiert und untersucht die Artificial Intelligence Services im Hinblick auf den Sicherheitsstatus und Prognosen in Nordamerika, Asien-Pazifik, Europa, dem Nahen Osten und Afrika und Lateinamerika 24.05.18 #global http://somtxt.de/s/P3q

Der Bericht gibt einen umfassenden Überblick über die gegenwärtige Wachstumsdynamik der globalen Sicherheitsdienste für Künstliche Intelligenz mit Hilfe umfangreicher Marktdaten, die alle wichtigen Aspekte und Marktsegmente abdecken. Der Bericht gibt einen Überblick über die vergangenen und gegenwärtigen Trends sowie die Faktoren, die die Marktwachstumsaussichten der Künstlichen Nachrichtendienste auf dem Sicherheitsmarkt in naher Zukunft voraussichtlich beflügeln oder behindern werden. 24.05.18 #global http://somtxt.de/s/P3q

Die CIOs von Abteilungen und Agenturen haben im Allgemeinen keinen ausreichenden Einblick in oder Kontrolle über die IT-Ressourcen ihrer Agenturen, heißt es in der Bestellung, was zu Doppelarbeit, Verschwendung und mangelhafter Bereitstellung von Diensten führt. Durch die Verbesserung der Effektivität der CIOs der Agenturen werden Agenturen besser in die Lage versetzt, ihre Systeme zu modernisieren, IT-Programme effizienter auszuführen, Cyber-Sicherheitsrisiken zu reduzieren und den amerikanischen Bürgern einen guten Dienst zu leisten. 21.05.18 #agency http://somtxt.de/s/P3L

Agenturen können und sollten heute damit beginnen, eine robuste LKW-Pipeline zu bauen, um 2018 großartige Ergebnisse zu erzielen. Kontaktieren Sie uns unter (518) 222-6392 für eine 15-minütige LKW-Diskussion - und erfahren Sie, wie und warum andere Agenturen mit diesem bewährten Vorsprung erfolgreich sind Generierungslösung. Es gibt viele zwingende Gründe, warum Websites von Versicherungsagenturen auf SSL umgestellt werden sollten, einschließlich Sicherheit, Verschlüsselung und Vertrauen. 17.04.18 #agency http://somtxt.de/s/P1d

5.5 research

Ein ICO-Sprecher sagte: Ein Vorfall, an dem Dixons Carphone beteiligt war, wurde uns gemeldet, und wir stehen in Verbindung mit dem National Cyber Security Center, der Financial Conduct Authority und anderen relevanten Behörden, um die Einzelheiten und Auswirkungen auf die Kunden zu ermitteln. Jeder, der sich über verlorene Daten und seine Verwendung Gedanken macht, sollte den Ratschlägen von Action Fraud folgen. Carphone Warehouse schlug mit einer Geldbuße in Höhe von 400.000 Euro für den Datenmüll von 2015 ein 13.06.18 #centre http://somtxt.de/s/P9E

Weitere Cyber-Sicherheitsexperten werden bei der Veranstaltung für informative Updates und Beratung anwesend sein. Bitte bringen Sie einen Laptop mit Windows mit, um die Plattformen zu nutzen und die Szenarien zu starten. Das Yorkshire Cyber Project wird von CENTRIC (Center of Excellence in den Bereichen Terrorismus, Resilience, Intelligence und Organized Crime Research) betrieben, die die Plattform geschaffen haben und über eine Fülle von Wissen, Erfahrung und Fachwissen verfügen, um mit Ihnen zu teilen. 06.06.18 #centre http://somtxt.de/s/P95

Das Potomac Institute for Policy Studies ist ein unabhängiges, 501 (c) (3), nicht gewinnorientiertes Forschungsinstitut für öffentliche Politik. Das Institut identifiziert und offensiv die Diskussion über die wichtigsten wissenschaftlichen und technologischen Probleme unserer Gesellschaft. Aus diesen Diskussionen und Foren entwickeln wir sinnvolle wissenschafts- und technologiepolitische Optionen und sorgen für deren Umsetzung an der Schnittstelle von Wirtschaft und Politik. 29.05.18 #research http://somtxt.de/s/P3R

Eine Richtlinie erleichtert es einem Mitarbeiter, der die Regeln befolgt, einer Person, die Social-Engineering-Taktiken verwendet, Nein zu sagen. Wenn keine Unterlagen vorhanden sind oder der

Arbeitgeber die Arbeitnehmer nicht darüber informiert, dass dies der Fall ist, kann der Arbeitgeber keinen Rückgriff darauf nehmen, wenn ein Arbeitnehmer Maßnahmen ergreift, die Sicherheitsprobleme verursachen. Das Unternehmen muss auch geeignete Beweise dafür vorlegen, dass ein Mitarbeiter die Richtlinie nicht befolgt und die Richtlinie konsequent durchsetzt. 21.05.18 #actions http://somtxt.de/s/P3A

Aber es gibt Hoffnung - ein Vorhersagemodell, das auf modernster Datenwissenschaft basiert, ist effizienter, erfordert weniger Aufwand und bietet eine bessere Abdeckung der Angriffsfläche eines Unternehmens. Zusammenfassung der Nachrichten Kenna Security, ein führendes Unternehmen im Bereich des prädiktiven Cyberrisikos, hat heute eine neuer Forschungsbericht, der in Zusammenarbeit mit dem Cyentia Institute durchgeführt wurde und eine Analyse der heute gängigen Schwachstellenmanagement-Strategien in der Industrie bereitstellt. 15.05.18 #research http://somtxt.de/s/Psl

Dieses Papier untersucht die strukturellen, systemischen und kulturellen Probleme des britischen Anti-Geldwäsche-Regimes in Bezug auf die Informations- und Informationsflüsse von und zu den nichtfinanziellen Sektoren von Rechtsberatungsdiensten, Buchhaltungsdienstleistern, Immobilien- und Immobilienagenturen und Vertrauen und Unternehmensdienstleister. Tags: Zentrum für Finanzkriminalität und Sicherheit Studien, AML / CTF, Gelegenheitspapiere, Großbritannien, organisierte Kriminalität Anton Moiseienko 11.05.18 #centre http://somtxt.de/s/PsT

Die Studie bietet eine ganzheitliche Perspektive auf das Wachstum des Marktes in Bezug auf Umsatz (US $ Bn), in verschiedenen geografischen Regionen, nämlich der Bericht bietet Ökosystemanalysen und Porters Five Forces-Analyse für die Cyber-Sicherheit als ein Service-Markt.Die Cyber-Sicherheit als Dienstleistung Marktdatenschätzungen sind das Ergebnis unserer vertieften Sekundärforschung, Primärinterviews und hausinternen Expertengremien. 07.05.18 #research http://somtxt.de/s/PsA

Darüber hinaus wird die Verantwortung für das Risiko von Cyberkriminalität und Informationssicherheit vom Komitee für Finanzsystemanfälligkeiten an das Group Risk Committee übertragen. Dies ermöglicht uns, Cyberkriminalität und Informationssicherheitsrisiken im Rahmen einer ganzheitlichen Betrachtung von strategischen Fragen, die HSBC betreffen, besser zu berücksichtigen. In Bezug auf die Leistung Ihres Konzerns haben unsere Ergebnisse für 2017 sowohl die Stärke als auch das Potenzial von HSBC gezeigt. 20.04.18 #results http://somtxt.de/s/Pq5

5.6 experts

Es wurde eingeräumt, dass nicht-finanzielle personenbezogene Daten wie Namen, Adressen oder E-Mail-Adressen abgerufen wurden, aber es bestand erneut darauf, dass es in dieser Phase keine Beweise für Betrugsfälle gesehen habe. Die National Crime Agency gab bekannt, dass sie mit dem Nationalen Cybersicherheitszentrum, der Finanzaufsichtsbehörde und dem Büro des Informationskommissars (ICO) zusammenarbeitet, um zu verstehen, was passiert ist. 14.06.18 #crime http://somtxt.de/s/P9U

Inhalte für Sicherheitsbewusstseinstrainings werden in über 20 Sprachen übersetzt und von einem globalen Netzwerk der weltweit erfahrensten Cyber-Sicherheitsexperten erstellt. Organisationen vertrauen darauf, dass der Inhalt und das Training von SANS Security Awareness weltklasse und für ein globales Publikum bereit sind. Das SANS Security Awareness-Programm umfasst alles, was

Sicherheitsbeauftragte benötigen, um einfach und effektiv ein erstklassiges Sicherheitsbewusstseinsprogramm zu entwickeln. 13.06.18 #experts http://somtxt.de/s/P92

Tatsächlich gaben 28% der Unternehmen in einer Studie an, dass sie ihr gesamtes oder den größten Teil ihres Cybersicherheits-Budgets für Versicherungen aufwenden und sich bei Datenkompromittierung eher auf Entschädigung als auf Schutz verlassen. Der Mangel an Realismus in diesem Ansatz ist offensichtlich, wenn man bedenkt, dass der Schaden, den eine Datenverletzung verursachen kann, genauso schwer zu quantifizieren ist wie zu prognostizieren. Effektivere Lösungen für IT-Sicherheit und Datensicherheit 24.05.18 #insurance http://somtxt.de/s/P31

Zusammen mit CSIRO Data61, der größten Dateninnovationsgruppe in Australien, baut der Cyber Security Hub der Optus Macquarie University ein Team von Forschern und Experten auf, um neuartige und effiziente Technologien zum Schutz der Privatsphäre zu entwickeln, mit einem Schwerpunkt auf Datenanalyse- und Datenfreigabeanwendungen. Wir werden qualitativ hochwertige und wirkungsvolle Forschung durchführen, die auf die Bedürfnisse der Industrie und der Gemeinde abgestimmt ist und einen multidisziplinären Ansatz verfolgt. 17.05.18 #experts http://somtxt.de/s/PsB

Die wichtigsten Ergebnisse der KPMG ERP Controls Umfrage 2017: Risk Is Real umfasste: Um die Umfrageergebnisse weiter zu beleuchten, hat sich CFO.com mit dem Co-Autor der Umfrage, Laeeq Ahmed, Managing Director, Advisory, bei KPMG getroffen Risiken und besser verstehen, wie Organisationen ERP-Cloud-Strategien verwalten können, um ihre Finanzfunktionen zu sichern. CFO.com: Die Umfrage zeigt, dass eine große Anzahl von Führungskräften besorgt über den Wechsel in die Cloud sind. 01.05.18 #executives http://somtxt.de/s/PqC

Zu den Blauen Teams gehörten Teams aus der NATO und der Europäischen Union, die hauptsächlich aus nationalen militärischen und zivilen Cyber-Sicherheitsexperten bestanden. Locked Shields umfassten insgesamt etwa 4.000 virtuelle Systeme und mehr als 2.500 Angriffe. Neben dem Management komplexer IT-Systeme sagte die CCDCOE, dass die Blue Teams bei der Meldung von Vorfällen effektiv sein müssten; Ausführung strategischer Entscheidungen; und lösen forensische, mediale und rechtliche Herausforderungen. 29.04.18 #experts http://somtxt.de/s/Pq9

Cyber-Kriminalität und Cyber-Attacken sind zu einer wachsenden Bedrohung für Regierungen, Unternehmen und Einzelpersonen geworden, wenn die digitalen Technologien voranschreiten. In einigen Wahlkampagnen wurden auch Cyber-Spionage, die Verbreitung gefälschter Nachrichten und der Missbrauch der sozialen Medien kritisiert. Die Europäische Kommission hat die Cyber-Sicherheitsstrategie der Europäischen Union im September 2017 aktualisiert, um die Widerstandsfähigkeit gegenüber Cyber-Angriffen und die gemeinsame Reaktion in der gesamten Union zu fördern. 27.04.18 #crime http://somtxt.de/s/Pqd

6 critical & future

6.1 Government

Der Markt für jede Region wird später nach Ländern und Segmenten unterteilt. Der Bericht umfasst die Analyse und Prognose von 13 Ländern weltweit sowie aktuelle Trends und Chancen in der

Region. Der Bericht analysiert marktbeeinflussende Faktoren sowohl auf der Angebots- als auch auf der Nachfrageseite und bewertet weiterhin Marktdynamiken, die den Markt während des Prognosezeitraums beeinflussen, dh Faktoren, Beschränkungen, Chancen und zukünftige Trends. 12.06.18 #future http://somtxt.de/s/P9l

Die Bundesregierung führt eine neue Cyber-Sicherheitsstrategie ein, die das Land und seine Bürger vor der wachsenden Bedrohung durch Online-Angriffe und Kriminalität schützen soll. DIE KANADISCHE PRESSE / Nathan Denette OTTAWA - Die Bundesregierung führt eine neue Cybersicherheitsstrategie ein, die das Land und seine Bürger vor der wachsenden Bedrohung durch Online-Angriffe und Kriminalität schützen soll. 12.06.18 #government http://somtxt.de/s/P9Z

IntSights Cyber Intelligence wurde 2015 auf den Markt gebracht und ist eine der ersten Threat Intelligence Platforms (TIP), die Bedrohungsdaten wirklich zusammenfasst und es Unternehmen ermöglicht, basierend auf dieser maßgeschneiderten Aufklärung und Analyse Maßnahmen zu ergreifen. Heute ist IntSights ein Marktführer im DRP- und TIP-Markt mit Hunderten von Kunden und Partnern weltweit. Zur Überprüfung der neuen Technologie von Forrester Research: Digitaler Risikoschutz, Q2 2018 , klicken Sie bitte hier. 12.06.18 #report http://somtxt.de/s/P9D

Vorbehaltlich der fortgesetzten Verpflichtungen des Unternehmens gemäß den AIM-Regeln und den geltenden Gesetzen und Vorschriften übernimmt der Konzern keine Verpflichtung, zukunftsgerichtete Aussagen zu aktualisieren oder zu revidieren, sei es aufgrund neuer Informationen, zukünftiger Ereignisse oder aus anderen Gründen. 3.4 Cyber-Risiko Dieses Risiko ergibt sich aus dem rasanten technischen Fortschritt, insbesondere im Bereich der sozialen Medien. 12.06.18 #media http://somtxt.de/s/P9d

Zu den in diesem Bericht aufgeführten Top-Unternehmen gehören: Exelis, Inc., Raytheon, Booz Allen Hamilton, Presagis, Elbit Systems, SAP AG, Thales, Lockheed Martin, Northrop Grumman, BAE Systems, DRS Tactical Systems, Dynamic Research Corporation, SAIC, Microsoft, Allgemeine Dynamik, Hewlett Pack. Bedenken hinsichtlich der Datensicherheit und des Datenschutzes bleiben eine Herausforderung für das Wachstum des Marktes. Der Verlust sensibler Daten kann eine Bedrohung für das Land darstellen. 17.05.18 #report http://somtxt.de/s/PsJ

Der Homeland Security Marktforschungsbericht liefert detaillierte Informationen über die Branche basierend auf den Einnahmen für den Prognosezeitraum. Die Forschungsstudie ist eine deskriptive Analyse dieses Marktes, die die Markttreiber und -beschränkungen, die das gesamte Marktwachstum bestimmen, betont. Die Trends und Zukunftsaussichten des Marktes sind auch in dem Bericht enthalten, der ein intellektuelles Verständnis der Branche vermittelt. 25.04.18 #future http://somtxt.de/s/Pqe

Sie werden außerdem Zugriff auf ein internationales Netzwerk von Cyber-Clustern haben, um Handels- und Investitionsmöglichkeiten auf globaler Ebene zu schaffen. Das Zentrum wird von der Abteilung für Digital, Kultur, Medien und Sport finanziert. CBI-Bericht Smooth Operations: Eine AZ der EU-Regeln, die für die Wirtschaft wichtig sind, fordert das Vereinigte Königreich auf, die Initiative des EU-Binnenmarkts für digitale Produkte nach dem Brexit zu replizieren 18.04.18 #media http://somtxt.de/s/P1U

Das Zentrum wird von der Abteilung für Digital, Kultur, Medien und Sport finanziert. CBI-Bericht Smooth Operations: Eine AZ der EU-Regeln, die für die Wirtschaft wichtig sind, fordert Großbritannien

auf, die EU-Initiative für einen digitalen Binnenmarkt zu replizieren, nachdem Brexit-Organisationen einen Anteil von bis zu 20 Millionen Pfund für die Entwicklung von Quantenprototypen beantragen könnten einen Durchbruch in den Bereichen Sensorik, Bildgebung und Informationsaustausch. 18.04.18 #media http://somtxt.de/s/P1U

Markante Regionen sind darüber hinaus aufgeklärt worden, wo der Markt funktioniert, und die Regionen, in denen die Akteure lukrative, offene Einfahrten finden, wurden später ebenfalls in dem Bericht erwähnt. Der Bericht diskutiert nicht nur ausführlich die verschiedenen Wachstumstreiber für den Global Cyber Security als Servicemarkt, sondern diskutiert auch die Hauptfaktoren, die bei den Marktteilnehmern Anlass zur Besorgnis geben. 18.04.18 #future http://somtxt.de/s/P1B

Representational image: Reuters Washington und London gaben eine gemeinsame Warnung heraus, dass die Kampagne der von der russischen Regierung unterstützten Hacker Spionage, Diebstahl geistigen Eigentums und andere bösartige Aktivitäten vorantreiben sollte und zu offensiven Angriffen eskaliert werden könnte. Es folgte eine Reihe von Warnungen westlicher Regierungen, dass Moskau hinter einer Reihe von Cyberangriffen steckt. 17.04.18 #government http://somtxt.de/s/P1u

Großbritannien, US-Regierung warnt vor böswilliger Cyber-Aktivität in Russland Der technische Alarm wurde vom britischen Cyber Security Center, dem US Federal Bureau of Investigation und dem Department of Homeland Security herausgegeben. Die Ziele dieser bösartigen Cyber-Aktivität sind in erster Linie staatliche und private Organisationen, Anbieter kritischer Infrastrukturen und die Internet Service Provider (ISPs), die diese Sektoren unterstützen, heißt es in der Erklärung. 16.04.18 #government http://somtxt.de/s/P1a

Sowohl Moskau als auch Trump haben die Vorwürfe bestritten. Die Regierungen der USA und Großbritanniens erklärten, dass sie planten, am Montag Nachmittag einen gemeinsamen Bericht mit technischen Details zu den Angriffen zu veröffentlichen, damit Organisationen feststellen können, ob sie gehackt wurden und ähnliche Hackerangriffe vereiteln. Die Regierungen haben die Opfer aufgefordert, alle Infektionen zu melden, damit sie die Auswirkungen der Kampagne besser verstehen können. 16.04.18 #report http://somtxt.de/s/P1o

6.2 concerns

Der Schutz Ihrer Privatsphäre ist ein Sicherheitsproblem. Diejenigen, die illegal IMSI-Catcher in der Gegend von Washington, DC betreiben, tun dies möglicherweise für rein kriminelle Aktivitäten. Wenn Ihre Daten von einem dieser Geräte erfasst werden, können Sie daher ein Ziel der Gelegenheit werden. Das bedeutet, dass die Sicherheit Ihrer Familie gefährdet sein könnte, weil Ihre Konversation oder SMS-Nachrichten abgefangen wurden. 19.04.18 #issue http://somtxt.de/s/P1Q

6.3 target

North Carolina A T betreibt zwei Forschungszentren, die sich auf diese Themen konzentrieren. Forscher des Center for Advanced Study für Identitätsforschung arbeiten mit Partnern an der Clemson University und der University of North Carolina in Wilmington zusammen, um Techniken zu entwickeln, die Identitätsdiebstahl und andere bösartige Cyber-Aktivitäten verhindern. Das Center for Cyber Defense befasst sich mit breiteren Themen der Cyber-Sicherheit und ist ein

Exzellenzzentrum des Verteidigungsministeriums. 13.06.18 #malicious http://somtxt.de/s/P9w

Die Bedrohung durch Cyberkriminalität und Cyberterrorismus ist eine relativ neue Bedrohung. North Carolina A T betreibt zwei Forschungszentren, die sich auf diese Themen konzentrieren. Forscher des Center for Advanced Study für Identitätsforschung arbeiten mit Partnern an der Clemson University und der University of North Carolina in Wilmington zusammen, um Techniken zu entwickeln, die Identitätsdiebstahl und andere bösartige Cyber-Aktivitäten verhindern. 13.06.18 #malicious http://somtxt.de/s/P9w

Zu den weiteren Schutzfunktionen gehört die Sperrung von Systemabbildern, eine branchenweit erste Funktion, die Konfigurationsänderungen verhindert, die Sicherheitslücken verursachen, vertrauliche Daten offenlegen und Standardkennwörter schützen. Eine zuverlässige Erkennung ist entscheidend für die schnelle Erkennung schädlicher Aktivitäten. Dies beinhaltet Konfigurations- und Firmware-Drift-Schutz, dauerhafte Ereignisprotokollierung und sichere Alarmierung, wenn abnormale Aktivität erkannt wird. 22.05.18 #malicious http://somtxt.de/s/P3N

Am Montag warfen die Vereinigten Staaten und Großbritannien Russland vor, Cyber-Angriffe auf Computer-Router, Firewalls und andere Geräte zu starten, die von Regierungsbehörden und Unternehmen auf der ganzen Welt verwendet werden. Ciaran Martin, Hauptgeschäftsführer des National Cyber Security Centers, einem Arm des britischen Geheimdienstes GCHQ, sagte am Montag: Dies ist eine nachhaltige Ausrichtung auf mehrere Entitäten über Monate hinweg, von denen wir glauben, dass der russische Staat dahinter steckt. 18.04.18 #state http://somtxt.de/s/P1p

Wenn wir bösartige Cyber-Aktivitäten sehen, sei es vom Kreml oder anderen bösartigen Akteuren des Nationalstaats, werden wir uns zurückdrängen, sagte Rob Joyce, der Cyber Security Coordinator des Weißen Hauses. Die Beziehungen zwischen Russland und Großbritannien waren bereits angespannt, nachdem Ministerpräsidentin Theresa May Moskau vorgeworfen hatte, am 4. März die Nervenkraftstoffvergiftung des ehemaligen russischen Spions Sergei Skripal und seiner Tochter Julia in der Stadt Salisbury begangen zu haben. 17.04.18 #state http://somtxt.de/s/P1u

Die US-Regierung bezeichnet bösartige Cyber-Aktivitäten der russischen Regierung als GRIZZLY STEPPE. NCCIC ermutigt Benutzer und Administratoren, die Seite GRIZZLY STEPPE - Russian Malicious Cyber Activity [https://www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity] zu lesen, die mit TA18-106A Russian State verlinkt ist -Sponsored Cyber Actors Targeting Network Infrastructure Devices für weitere Informationen. 16.04.18 #state http://somtxt.de/s/P1z

6.4 machines

Sie beriefen sich auf Cyber-Sicherheitsforschungsorganisationen und andere Regierungen, die Beweise für solche Angriffe liefern, ohne Angaben zu ihrem Zeitplan oder ihrer Größe zu machen. Der aktuelle Stand der US-amerikanischen und britischen Netzwerkgeräte, gekoppelt mit einer Kampagne der russischen Regierung zur Nutzung dieser Geräte, bedroht unsere Sicherheit und unser wirtschaftliches Wohlergehen. 17.04.18 #activity http://somtxt.de/s/P1h

6.5 hacking

IT ist heute genauso wichtig wie die meisten anderen von Gesundheitssystemen verwalteten Infrastrukturen. Es ist wichtig, dass Informationssicherheitsrisiken die gleiche oder größere Bedeutung

und Priorität erhalten wie anderen organisatorischen Risiken. Da Gesundheitsdaten von papierbasierten zu digitalen Systemen wechseln, ist es von entscheidender Bedeutung, dass Organisationen über Programme zum Risikomanagement von Risiken und Sicherheitsverfahren verfügen, die in die Unternehmenskultur integriert sind. 08.06.18 #critical http://somtxt.de/s/P9P

Zu den Spezialeinheiten gehören fortschrittliche Cyber-Sicherheit, Big-Data-Analyse, computergestützte Intelligenz und maschinelles Lernen, Computer-Forensik, Internet-Engineering, umfassende und immersive Benutzererfahrung, Programmierung für das Internet der Dinge, mobile und Cloud-Systeme. Lernergebnisse Kurs-Lernergebnisse drücken den Lernerfolg dahingehend aus, was ein Schüler nach Abschluss eines Kurses wissen, verstehen und tun können sollte. 01.06.18 #computer http://somtxt.de/s/P3B

REUTERS / Leah Millis UNPRÄSIDENTIERT, KOORDINIERT Ein US-Senatsbericht vom 8. Mai sagte, dass im Jahr 2016 Cyberakteure, die der russischen Regierung angegliedert sind, eine beispiellose, koordinierte Cyberkampagne gegen staatliche Wahlinfrastruktur durchgeführt haben. Russische Akteure scannten Datenbanken nach Schwachstellen, versuchten Eindringlingen und in einer kleinen Anzahl von Fällen erfolgreich eine Wählerregistrierungsdatenbank durchdrungen. 22.05.18 #campaign http://somtxt.de/s/P3e

Die Details, die sich Sorgen machen Stimmen- und Cybersicherheitsexperten, die das Fehlen einer Hardcopy sagen, machen es schwierig, die Ergebnisse auf Anzeichen von Manipulation zu überprüfen. Im aktuellen System, nach der Wahl, wenn die Leute befürchten, dass es gehackt wurde, können die besten Beamten sagen:, Vertraue uns , sagte Alex Halderman, ein Experte für Wahlmaschinen, Direktor des Computerzentrums der Universität von Michigan Sicherheit und Gesellschaft. 17.05.18 #computer http://somtxt.de/s/PsH

Durch die einfache Überforderung von Computersystemen und Servern mit gezieltem Flood-Verkehr werden DDoS-Angriffe genutzt, um die politische Sprache und den Zugang der Wähler zu den benötigten Informationen zum Schweigen zu bringen. Politische Parteien, Kampagnen und Organisationen sind ein wachsendes Ziel. Diese Organisationen sind kritische Teile des demokratischen Prozesses und sie verdienen die gleiche Verteidigung gegen Cyber-Angriffe, die wir Nachrichtenorganisationen auf der ganzen Welt angeboten haben. 16.05.18 #computer http://somtxt.de/s/Psw

Dieser Online-Workshop zum Wi-Fi und Network Ethical Hacking ist so strukturiert, dass Sie umfassende und umfassende Informationen über Wi-Fi Hacking und dessen Sicherheit erhalten, um sie vor Cyberangriffen zu schützen. Am Ende dieses Kurses können Sie unabhängig von Ihrer Erfahrung alle Arten von WLAN-Verschlüsselungsmethoden durchbrechen und Ihre Karriere in der Netzwerksicherheit fortsetzen. 9. Cyber Security Volume I: Hacker ausgesetzt 25.04.18 #hacking http://somtxt.de/s/Pqz

Die Warnung kommt zwei Monate nachdem die Vereinigten Staaten und Großbritannien Russland vorgeworfen haben, 2017 den zerstörerischen Cyberangriff NotPetya durchgeführt zu haben, der einen Virus hervorbrachte, der Teile der ukrainischen Infrastruktur lahm legte und Computer auf der ganzen Welt beschädigte. Amerikanische und britische Offizielle sagten, dass die Angriffe eine breite Palette von Organisationen betrafen, darunter Internet Service Provider, private Unternehmen und kritische Infrastrukturanbieter. 18.04.18 #critical http://somtxt.de/s/P1R

Die US-Regierung bewertete, dass Cyber-Akteure, die von der russischen Regierung unterstützt werden, diese weltweite Kampagne durchführten. Diese Operationen ermöglichen Spionage und geistiges Eigentum, die die nationale Sicherheit und wirtschaftliche Ziele der Russischen Föderation unterstützt, sagte die Website. Russische Cyber-Akteure nutzen eine Reihe von älteren oder schwachen Protokollen und Service-Ports, die mit Netzwerkadministrationsaktivitäten verbunden sind. 17.04.18 #campaign http://somtxt.de/s/P1Z

In einer gemeinsamen Ankündigung vom US-Heimatschutzministerium, dem FBI und dem Nationalen Cybersicherheitszentrum des Vereinigten Königreichs warnten Beamte, dass russische Spione nach Sicherheitslücken auf Millionen von Routern als Werkzeug für zukünftige Angriffe gesucht haben. Die Ziele umfassen Router in Haushalten und Büros sowie Firewalls und Switches von Internetdienstanbietern, kritischer Infrastruktur und großen Privatunternehmen. 17.04.18 #russian http://somtxt.de/s/P1i

Kurz darauf nutzte die Hacker-Gruppe JHT die Schwachstelle des Cisco Smart Install Clients auf Maschinen in Iran und Russland. Die Hacker hinterließen die Nachricht: Leg dich nicht mit unseren Wahlen an, gefolgt von einer US-Flagge. Die Gruppe behauptete, dass sie einfach eine Nachricht senden wollte, da sie genug von Angriffen von Regierungshackern auf die Vereinigten Staaten und andere Länder seien. 17.04.18 #hacking http://somtxt.de/s/P13

Monitoring Desk Die Vereinigten Staaten und Großbritannien warnten am Montag vor einer weltweiten Cyber-Attacke gegen Router und andere Netzwerkgeräte und gaben russischen Regierungshackern die Schuld für die Kampagne gegen Regierungsbehörden, Unternehmen und kritische Infrastrukturbetreiber. Washington und London gaben eine gemeinsame Warnung heraus und sagten, dass die weit verbreitete globale Kampagne im Jahr 2015 begann und zu offensiven Angriffen eskaliert werden könnte. 17.04.18 #critical http://somtxt.de/s/P1T

Es folgte eine Reihe von Warnungen westlicher Regierungen, dass Moskau hinter einer Reihe von Cyberangriffen steckt. Die Vereinigten Staaten, Großbritannien und andere Nationen beschuldigten Russland im Februar, das NotPetya -Virus freigegeben zu haben, das im Jahr 2017 Teile der ukrainischen Infrastruktur lahmlegte und Computer auf der ganzen Welt beschädigte, die Unternehmen Milliarden von Dollar kosteten. Der Kreml reagierte nicht sofort auf eine Bitte um Stellungnahme. 17.04.18 #globe http://somtxt.de/s/P1e

Millionen von Geräten auf der ganzen Welt sollen auf diese Weise kompromittiert worden sein, mit inhärent schlechter Sicherheit und von den Angreifern ausgenutzten Standard-Passwörtern. Was wir in diesem Fall gesehen haben, sind Standard-Passwörter, die ausgenutzt werden, ungesicherte Geräte werden ausgenutzt, sagte Joyce. Es wird davor gewarnt, dass eine Kampagne der russischen Regierung zur Ausbeutung dieser Geräte die Sicherheit und das wirtschaftliche Wohlergehen der USA und Großbritanniens bedroht. 16.04.18 #campaign http://somtxt.de/s/P1P

Vertreter der USA und des Vereinigten Königreichs sagten, die infizierten Router könnten genutzt werden, um zukünftige offensive Cyber-Operationen zu starten. Sie könnten sich in Zeiten der Spannung vorpositionieren, sagte Ciaran Martin, Geschäftsführer der Cyber-Verteidigungsagentur des britischen Cyber Security Centers, der hinzufügte, dass Millionen von Maschinen in der Kampagne ins Visier genommen wurden. 16.04.18 #russian http://somtxt.de/s/P1t

Wenn wir bösartige Cyber-Aktivitäten sehen, sei es vom Kreml oder anderen bösartigen Akteuren

des Nationalstaats, werden wir uns zurückdrängen, sagte Rob Joyce, der Cybersicherheitskoordinator des Weißen Hauses. Sie könnten in Zeiten von Spannungen vorpositioniert werden, sagte Ciaran Martin, Geschäftsführer der Cyber-Verteidigungsagentur des britischen Cyber Security Centers, der hinzufügte, dass Millionen von Maschinen in der Kampagne ins Visier genommen wurden. 16.04.18 #russian http://somtxt.de/s/P1L

6.6 systems

Wenn Sie vorhaben, ein Mobiltelefon, einen Laptop, einen PDA oder ein anderes elektronisches Gerät mitzunehmen, dürfen Sie keinen Fehler machen - alle Daten auf diesen Geräten (insbesondere Ihre personenbezogenen Daten) dürfen von der russischen Regierung oder von Cyberkriminellen abgerufen werden. er sagte. Unternehmens- und Regierungsbeamte sind am meisten gefährdet, aber gehen Sie nicht davon aus, dass Sie zu unbedeutend sind, um ins Visier genommen zu werden, fügte Evanina hinzu. Wenn Sie auf das Gerät verzichten können, nehmen Sie es nicht. 12.06.18 #hackers http://somtxt.de/s/P9R

Die anfänglichen Kosten für die Implementierung von Firewalls und Intrusion Detection-Systemen der nächsten Generation in militärischen Einrichtungen werden in den kommenden vier Jahren voraussichtlich hoch sein. Der Verteidigungssektor sieht sich auch vielen Herausforderungen in Bezug auf Cyber-Sicherheit gegenüber, um Online-Cyber-Angriffen durch Hacker entgegenzuwirken. Um eine große Datenmenge zu verwalten und die militärischen Daten zu schützen, sind fortschrittliche IT-Lösungen erforderlich. 17.05.18 #systems http://somtxt.de/s/PsJ

Die führende Technik, um Geld zu erpressen, war Malware - einschließlich Angriffen durch Ransomware und Kryptojacken. (1) Während zur Sicherung des Unternehmensnetzwerks angemessene Mitarbeiterschulungen und vorbeugende IT-Sicherheitsmaßnahmen erforderlich sind, ist die letzte Verteidigungslinie der Schutz von Wiederherstellungsdaten heißt jetzt Ransomware Attack-Loops. Eine Attack-Loop tritt auf, wenn Hacker ausführbaren Code in die Backup-Daten der Organisation einfügen. 15.05.18 #hackers http://somtxt.de/s/PsK

Der Kandidat wird das Incident Response-Team des Enterprise Security and Risk Management Office (ESRMO) unterstützen und Netzwerke und Systeme mit verschiedenen Sicherheitsgrenzwerkzeugen und -funktionen für anomale Aktivitäten, Triage und gegebenenfalls Korrekturen überwachen. Pflichten und Verantwortlichkeiten: • Unterstützung / Unterstützung von ESRMO mit Echtzeitüberwachung und Triage des empfangenen Vorfalls. 30.04.18 #systems http://somtxt.de/s/Pq8

Die erste Studienreise konzentrierte sich auf zwei umstrittene Themen: Cyber-Sicherheit und die nordkoreanische Krise. Während der Woche verhandelten die Studenten beide Probleme und erstellten schließlich zwei politische Memos mit Empfehlungen für die Regierungen der USA und Russlands. Die Studenten hörten auch von einer Vielzahl von russischen Regierungsbeamten und Experten zu Fragen im Zusammenhang mit Nordkorea, Informationssicherheit und Soft Power. 26.04.18 #officials http://somtxt.de/s/Pqb

Die meiste Erfahrung mit SCADA-Systemen bestand in der Integration von Daten zwischen IT- und OT-Netzwerken. Im Jahr 2005 erkannte er, dass Sicherheit eher ein nachträglicher Einfall war und verlagerte seinen Fokus auf die Sicherung von ICS-Netzwerken. Jetzt ist er ein

Netzwerksicherheitsüberwachungsspezialist (NSM) und nutzt diese Technologie, um Systemingenieuren und IT-Sicherheitsexperten zu helfen, die Auswirkungen auf die Sicherheit von Steuerungssystemnetzen zu verstehen. 20.04.18 #systems http://somtxt.de/s/Pqc

Die Syrien-Streiks und der erbitterte diplomatische Streit um den Angriff der Salisbury-Nervenagenten haben dazu beigetragen, dass die angespannten Beziehungen mit Russland in den letzten Wochen zugenommen haben. In einer gemeinsamen Erklärung des Vereinigten Königreichs und der USA heißt es, der Zustand der US-amerikanischen und britischen Netzwerkgeräte sowie eine Kampagne der russischen Regierung zur Nutzung dieser Geräte bedroht unsere jeweilige Sicherheit, unser wirtschaftliches Wohlergehen. 17.04.18 #russia http://somtxt.de/s/P1j

Von Jim Finkle und Doina Chiacu (Reuters) - Die USA und Großbritannien haben Russland am Montag beschuldigt, Cyberangriffe auf Computer-Router, Firewalls und andere Netzwerkgeräte zu starten, die von Regierungsbehörden, Unternehmen und Betreibern kritischer Infrastrukturen auf der ganzen Welt eingesetzt werden. 17.04.18 #routers http://somtxt.de/s/P1n

Laut US-amerikanischen und britischen Behörden zielen russische Hacker auf Millionen von Routern auf der ganzen Welt ab, darunter Geräte in Privathaushalten und Büros. In einer gemeinsamen Ankündigung vom US-Heimatschutzministerium, dem FBI und dem Nationalen Cybersicherheitszentrum des Vereinigten Königreichs warnten Offizielle, russische Spione hätten nach Sicherheitslücken auf Millionen von Routern als Werkzeug für zukünftige Angriffe gesucht. 16.04.18 #hackers http://somtxt.de/s/P1X

Dies ist das erste Mal, dass die USA und Großbritannien, wenn sie Russland einen Cyber-Angriff zuschreiben, gleichzeitig der Industrie einen gemeinsamen Ratschlag gegeben haben, wie sie die Risiken von Angriffen handhaben können. Es ist ein wichtiger Schritt in unserem Kampf gegen staatlich geförderte Aggression im Cyberspace. Seit mehr als 20 Jahren verfolgt GCHQ die wichtigsten russischen Cyber-Angriffsgruppen und die heutige gemeinsame Warnung der Vereinigten Staaten und der Vereinigten Staaten zeigt, dass die Bedrohung nicht verschwunden ist. 16.04.18 #russia http://somtxt.de/s/P1r

Die gemeinsame Warnung der USA und Großbritanniens kommt wenige Tage nachdem Innenministerin Amber Rudd gewarnt hatte, dass das Vereinigte Königreich in den letzten sechs Monaten von 49 Cyberattacken von russischen Gruppen getroffen wurde. Auch Jeremy Fleming, der Direktor des britischen Geheimdienstes GCHQ, hat kürzlich Russlands Aktionen im Cyberspace zur Sprache gebracht. Sie spielen nicht nach den gleichen Regeln, sie verwischen die Grenzen zwischen kriminellen und staatlichen Aktivitäten, sagte er 16.04.18 #russia http://somtxt.de/s/P1P

Vertreter der USA und des Vereinigten Königreichs sagten Reportern in einer Telefonkonferenz, dass sie eine gemeinsame Warnung über die Angriffe auf Router, die einen wesentlichen Teil der Internet-Infrastruktur bilden, in einer Cyber-Spionage-Kampagne veröffentlichen würden, die in Zukunft offensiv gestartet werden könnte Anschläge. 16.04.18 #routers http://somtxt.de/s/P1N

Laut der Sunday Times haben britische Spionageoffiziere auch darauf vorbereitet, dass russische Hacker peinliche Informationen über britische Politiker und andere hochrangige Leute nach dem Angriff auf die Skripals ausliefern. Großbritannien ist nicht das einzige Land, das durch Russlands jüngste Aktivitäten im Internet verärgert ist, da die deutsche Regierung bekannt gegeben hat, dass Russland am wahrscheinlichsten hinter einem Cyber-Angriff auf sein Außenministerium steckt.

16.04.18 #officials http://somtxt.de/s/P1A

7 attacks & access

7.1 Administration

Energiesektor vor Cyber-Angriffen im britischen Stromnetz gewarnt Großbritanniens Top-Energiekonzerne wurden gewarnt, Stromausfälle genauer zu untersuchen, da häufige oder lange Unterbrechungen das Zeichen eines Cyber-Angriffs sein könnten, berichtet die Financial Times. Vor dem Hintergrund des Nervenangriffs in Salisbury und der US-geführten Militärschläge gegen Syrien sind die Befürchtungen über die Fähigkeit Russlands, insbesondere das Stromnetz zu stören, gestiegen. 18.04.18 #power http://somtxt.de/s/P1g

Moskau hat frühere Vorwürfe zurückgewiesen, dass es Cyberangriffe auf die Vereinigten Staaten und andere Länder durchgeführt habe. US-Geheimdienste beschuldigten Russland im vergangenen Jahr, sich mit einer Hacker- und Propagandakampagne zur Unterstützung von Donald Trumps Präsidentschaftskampagne in die Wahlen 2016 einzumischen. Letzten Monat beschuldigte die Trump-Regierung Russland für eine Cyber-Attacke, die mindestens zwei Jahre zurückreicht und auf das US-Stromnetz ausgerichtet war. 18.04.18 #power http://somtxt.de/s/P1R

Latta begann seine Befragung beim E C-Unterausschuss Energie-Anhörung mit den Worten: In den letzten Wochen haben wir Nachrichten über bösartige Agenten gelesen, die daran arbeiten, die Sicherheit der Energieinfrastruktur unseres Landes zu untergraben. Laut dem Department of Homeland Security umfasst dies russische Cyber-Angriffe, die aus der Ferne auf das Stromnetz, Energie, Atomkraftwerke, kommerzielle Einrichtungen und kritische Produktionssektoren abzielen. 15.04.18 #power http://somtxt.de/s/P1c

7.2 attacks

Sicherheitslücken in der Cyber-Sicherheit sind weltweit ein großes Problem für die Stromnetze, die versuchen, ihre kritischen Ressourcen über ein IT-Netzwerk miteinander zu verbinden. Mit der Verbreitung verteilter Energieressourcen, der zunehmenden Dezentralisierung und der Vernetzung einer Reihe von intelligenten Energieanlagen wie intelligenten Zählern und intelligenten Heimen / Gebäuden besteht die Möglichkeit, Schadstoffe in die öffentlichen Stromnetze einzudringen. 07.06.18 #energy http://somtxt.de/s/P9t

Mit der Verbreitung verteilter Energieressourcen, der zunehmenden Dezentralisierung und der Vernetzung einer Reihe von intelligenten Energieanlagen wie intelligenten Zählern und intelligenten Heimen / Gebäuden besteht die Möglichkeit, Schadstoffe in die öffentlichen Stromnetze einzudringen. Aus diesem Grund arbeiten Energieversorger auf der ganzen Welt an Maßnahmen zur Bewertung, Eindämmung und Vorbereitung dieser Cyber-Sicherheitslücken. 07.06.18 #energy http://somtxt.de/s/P9t

OK Cancel Free Report) kündigte kürzlich die Übernahme von Bradford Networks, einem Anbieter von Netzwerksicherheit, an, indem die Zugriffssteuerung aller mit dem Unternehmensnetzwerk verbundenen Geräte sichergestellt wird. Das Ziel bietet eine agentenlose Überwachung und Bewertung von Endgeräten, einschließlich derjenigen, die durch das Internet der Dinge (Internet of

Things, IoT) ermöglicht werden, und deckt mehrere Branchen ab, unter anderem Fertigung, Regierung, Einzelhandel und Technologie. 06.06.18 #networks http://somtxt.de/s/P9A

Die Bundesregierung schreitet zu einer kontinuierlichen und kontextbewussten Sicherheitsagenda für die Netzwerkzugriffskontrolle und Endpunktsicherheit voran, um Mobilität, IOT-Bedrohungen, hybride IT und umfassendere militärische Risiken anzugehen. Dies stellt eine größere Belastung für die Agenturen dar, um ihre Legacy-Systeme, neue Initiativen und Bereitschaftsfähigkeiten zu bewerten, um die NIST-Richtlinien einzuhalten , sagte Corey Solivan, Director of Strategic Accounts bei Consolidated Networks. 05.06.18 #networks http://somtxt.de/s/P97

Obwohl die Bedrohung für IoT-Geräte nichts Neues ist, hat die Tatsache, dass diese Geräte von fortgeschrittenen nationalstaatlichen Akteuren zur Durchführung von Cyber-Operationen verwendet werden, was möglicherweise zur Zerstörung des Geräts führen könnte, die Dringlichkeit des Umgangs mit diesem Gerät stark erhöht Frage , schrieben sie. Wir rufen die gesamte Sicherheitsgemeinschaft dazu auf, uns bei der aggressiven Bekämpfung dieser Bedrohung zu unterstützen. 31.05.18 #malware http://somtxt.de/s/P3w

Dazu gehören Regierungsabteilungen, wichtige wirtschaftliche Erzeuger, Nischenexporteure, Forschungseinrichtungen und kritische nationale Infrastruktur. Der nächste Schritt besteht darin, dass der GCSB einen Plan entwickelt, wie er mit den Telekommunikationsnetzbetreibern zusammenarbeiten kann, um den erweiterten Service bereitzustellen, der voraussichtlich einige Monate dauern wird. Die Kosten für die Erweiterung von Malware-Free Networks werden aus der Baseline des GCSB bezahlt. 27.05.18 #malware http://somtxt.de/s/P3O

Er sagte, dass der Ausschuss auch Themen wie Chinas legale und illegale Bemühungen zum Erwerb nationaler Sicherheitstechnologien und des geistigen Eigentums in den USA, seine Einflusskampagne und seine Technologiestrategie untersuchen werde. Die öffentliche Anhörung - ungewöhnlich für ein Komitee, das die meisten Geschäfte hinter verschlossenen Türen abwickelt - fand am selben Tag statt, an dem Washington und Peking eine zweite Verhandlungsrunde begannen, um einen Handelskrieg abzuwenden. 17.05.18 #property http://somtxt.de/s/PsV

Beamte glauben, dass es wenig Abschreckung gibt, um sie davon abzuhalten, es erneut zu versuchen, besonders mit den Vereinigten Staaten, die das Atomabkommen verlassen und amerikanische Unternehmen, einschließlich derjenigen im Finanzdienstleistungssektor und im Energiesektor, wahrscheinlich die Hauptlast der Angriffe tragen. Angesichts der Geschichte der iranischen Cyber-Aktivitäten als Antwort auf geopolitische Probleme, hat der amerikanische Energiesektor allen Grund zu erwarten, dass der Iran eine Art von Reaktion erwartet, sagte Olsen. 12.05.18 #energy http://somtxt.de/s/Psj

Darüber hinaus können Terroristen Kernkraftwerke anvisieren, die Zugang zu Kernbrennstoffen suchen, um eine schmutzige Bombe oder eine Sprengvorrichtung zu schaffen, die radioaktive Partikel über ein großes Gebiet verteilen soll. Cyber-Attacken ergänzen die Liste der Bedrohungen für ein Atomkraftwerk und sie haben die einzigartige Eigenschaft, von weit her und anonym anzugreifen. In diesem Artikel werden SCADA-Systeme in kommerziellen Kernkraftwerken in den USA behandelt, wobei der Schwerpunkt auf SCADA-Systemen liegt 02.05.18 #property http://somtxt.de/s/Pq6

Es wird jedoch davon ausgegangen, dass ein Mangel an angemessenem Wissen und Bewusstsein

für Cyber-Angriffe das Wachstum des Marktes für Spear-Phishing-Schutz behindern wird. Der Bericht besagt, dass der globale Spear-Phishing-Schutz-Markt 2016 bei 817,2 Mio. USD lag. Die Studie prognostiziert, dass der globale Spear-Phishing-Schutzmarkt im Zeitraum von 2017 bis 2025 bei einer CAGR von 9,6% expandieren und auf US-Werte steigen wird 1.825,8 Mio. USD bis 2025. 02.05.18 #attacks http://somtxt.de/s/Pq0

Von den grundlegenden technischen Steuerelementen von Cyber Essentials hatten 75 Prozent der Wohltätigkeitsorganisationen Softwareupdates angewendet, 73 Prozent verfügten über einen aktuellen Malware-Schutz und 69 Prozent verfügten über effektive Firewalls. Nur 65 Prozent der Wohltätigkeitsorganisationen in der Forschung beschränkten die IT-Verwaltung und die Zugriffsrechte auf bestimmte Benutzer, und 42 Prozent hatten Sicherheitskontrollen auf unternehmenseigenen Geräten. Zwei Drittel der Wohltätigkeitsorganisationen gaben an, dass sie den Mitarbeitern erlauben, persönliche Geräte für die Arbeit zu verwenden. 26.04.18 #malware http://somtxt.de/s/PqT

Die zunehmende Verfeinerung und Durchdringung von Cyberattacken hat Unternehmen in den Sektoren BFSI, Regierung, Telekommunikation sowie Öl und Gas veranlasst, Cybersicherheitslösungen zu übernehmen, um die Sicherheit wichtiger Informationen in Computersystemen oder digitalen Speichergeräten sicherzustellen. Analysten von HTF prognostizieren, dass der Markt für Cyber-Sicherheit in der MEA-Region im Zeitraum 2014-2019 mit einer durchschnittlichen jährlichen Wachstumsrate von 14,63% wachsen wird. In diesem Bericht behandelt 19.04.18 #networks http://somtxt.de/s/Pq4

Eine gemeinsame Erklärung des US-Heimatschutzministeriums, des FBI und des britischen National Cyber Security Center warnte vor russischen staatlich geförderten Cyber-Akteuren, die Router, Switches, Firewalls und Netzwerk-Intrusion-Detection-Systeme von staatlichen und privaten Organisationen ausnutzen gut kritische Infrastrukturanbieter, ISPs und sogar kleine Heimbüros. Um diesen Artikel vollständig zu lesen, klicken Sie bitte hier 17.04.18 #attacks http://somtxt.de/s/P1v

Die Ziele dieser bösartigen Cyber-Aktivität sind in erster Linie staatliche und private Organisationen, Anbieter kritischer Infrastrukturen und die Internet Service Provider (ISPs), die diese Sektoren unterstützen, heißt es in der Erklärung. Sie warnte alle Internet-Service-Provider vor den Kunden im Home-Office, um die Warnung zu beachten, nachdem die Behörden Cyber-Attacken auf Geräte wie Internet-Router festgestellt hatten. 16.04.18 #attacks http://somtxt.de/s/P1a

7.3 providers

In Bezug auf den Wert wird das BFSI-Segment im Prognosezeitraum voraussichtlich die attraktivste Branche im globalen Markt für Sicherheits- und Schwachstellenmanagement sein. Im Jahr 2016 war das BFSI-Segment die dominierende Vertikale mit einem Wert von mehr als. Es wird erwartet, dass es im gesamten Prognosezeitraum wertmäßig dominant bleibt. Das Gesundheitssegment dürfte jedoch im gesamten Prognosezeitraum hohe Wachstumsraten im Jahresvergleich verzeichnen. 13.06.18 #segment http://somtxt.de/s/P9g

Unter diesen wird erwartet, dass die Audit- und Protokollserviceabteilung im Prognosezeitraum des Berichts die angenehmste Rate erreichen wird. Basierend auf dem Sicherheitstyp wird der globale Cyber-Security-Markt als Servicemarkt in die Sicherheit von Unternehmen, Endpunkten, Clouds,

Netzwerken und Anwendungen unterteilt. Unter diesen wird erwartet, dass das Segment der Netzwerksicherheit im Prognosezeitraum ein angemessenes Umsatzwachstum verzeichnen wird. 19.05.18 #segment http://somtxt.de/s/P3c

Zum Schutz vor Sicherheitslücken und Angriffen können Service Provider IT-Assessments durchführen, um Ihnen einen ganzheitlichen Überblick über Ihre IT-Infrastruktur und eine Technologie-Risikoanalyse zu geben, um sicherzustellen, dass Ihre Daten und Sicherheitseinstellungen Ihren geschäftlichen Anforderungen und Zielen entsprechen. Dabei werden Faktoren wie Compliance und die Bandbreite interner und externer Bedrohungen berücksichtigt, die in der heutigen Geschäftswelt von großer Bedeutung sind. 01.05.18 #providers http://somtxt.de/s/PqR

Das Thema für dieses Jahr lautet IKT - Unterstützung für den Schub in Richtung einer Wirtschaft des 21. Jahrhunderts. Die Ziele der IKT-Woche sind die Förderung des Wachstums und der Entwicklung unseres lokalen IKT-Sektors; ICT-Lösungsanbieter mit Lösungssuchenden zu verbinden; das Bewusstsein für kritische IKT-Themen wie Cyber-Sicherheit, Cloud Computing, Blockchain-Technologien und künstliche Intelligenz zu schärfen und das Interesse an IKT als Karriereweg für unsere Jugend zu wecken. 23.04.18 #providers http://somtxt.de/s/PqM

7.4 communication

Ziel des Berichts ist es, einen Überblick über den globalen Markt für Cyber-Sicherheit im Gesundheitswesen mit detaillierter Marktsegmentierung nach Lösungen, Service, Lieferart, Anwendung, Endnutzer und Geografie zu geben. Der globale Markt für Cyber-Sicherheit im Gesundheitswesen dürfte im Prognosezeitraum ein hohes Wachstum verzeichnen. Der Bericht liefert wichtige Statistiken über den Marktstatus der führenden Marktteilnehmer und bietet wichtige Trends und Chancen auf dem Markt. 12.06.18 #period http://somtxt.de/s/P9l

Der Bericht enthält Analysen für den Zeitraum 2016-2026, wobei 2018 bis 2026 der Prognosezeitraum und das Basisjahr 2017 ist. Eine gründliche und unvoreingenommene Markteinschätzung wurde vorgenommen, um den Lesern aufschlussreiche und genaue Analysen zu bieten. Der Bericht konzentriert sich auf alle wichtigen Trends und Dienstleistungen, die im Zeitraum 2018 - 2026 eine Schlüsselrolle für das Wachstum des industriellen Internetsicherheitsmarktes spielen. 25.05.18 #forecast http://somtxt.de/s/P3v

Der Bericht konzentriert sich auf alle wichtigen Trends und Dienstleistungen, die im Zeitraum 2018-2026 eine Schlüsselrolle beim Wachstum des industriellen Internetmarktes für Cyber-Sicherheit spielen. Er konzentriert sich auch auf Hemmfaktoren, Markttreiber und Chancen des Wachstums des industriellen Internetsicherheitsmarkts in diesem Zeitraum . Der Bericht enthält eine detaillierte Ökosystemanalyse, die einen umfassenden Überblick über den globalen Markt für industrielle Cyber-Sicherheit bietet. 25.05.18 #factors http://somtxt.de/s/P3v

Auf der Grundlage der Endnutzung wurde der Markt für Heimatschutz und Notfallmanagement in Strafverfolgung und Informationsbeschaffung, Risiko- und Notfalldienste, Grenzsicherheit, maritime Sicherheit, Luftsicherheit, Cybersicherheit, kritische Infrastruktursicherheit und CBRNE-Sicherheit unterteilt. Das Segment für Cyber-Sicherheit wird voraussichtlich im Prognosezeitraum auf dem Markt für Heimatschutz und Notfallmanagement auf dem höchsten CAGR wachsen. 14.05.18 #forecast http://somtxt.de/s/Psv

Die Cyber-Sicherheit als Dienstleistungsmarkt, der auf dem Endnutzersegment basiert, wird in BFSI, IT und Telekommunikation, Einzelhandel, Gesundheitswesen, Verteidigung / Regierung, Automobil und andere kategorisiert. Globaler Cyber-Sicherheit als Service-Markt: Umfang des Berichts Umfang der Cyber-Sicherheit als Service-Markt-Studie umfasst Markt-Indikator, der den Überblick der Elternmarkt unterstreicht das Wachstum des Sub-Segment-Marktwachstums im Prognosezeitraum unterstützt.Vergleich 07.05.18 #period http://somtxt.de/s/PsA

Globaler Cyber-Sicherheit als Service-Markt: Umfang des Berichts Umfang der Cyber-Sicherheit als Service-Markt-Studie umfasst Markt-Indikator, der den Überblick der Elternmarkt, die das Wachstum des Sub-Segment-Marktwachstums unterstützt während des Prognosezeitraums unterstreicht.Comparison Matrix ist ebenfalls enthalten Für die globale Cyber-Sicherheit als Service-Markt und Marktpositionierung wird Cyber Security als Service-Anbieter bereitgestellt. 07.05.18 #period http://somtxt.de/s/PsA

Darüber hinaus wird erwartet, dass die zunehmende Häufigkeit von Cyberattacken aus aufstrebenden Volkswirtschaften wie China, Japan, Indien und Ländern in Südamerika den Markt im Prognosezeitraum antreiben wird. Da Nordamerika und Europa jedoch ausgereifte Märkte für den Schutz von Spearfishing in Bezug auf Systembewusstsein und -akzeptanz sind, werden sich diese Regionen in diesem Prognosezeitraum voraussichtlich stabil, aber relativ langsam entwickeln. 02.05.18 #forecast http://somtxt.de/s/Pq0

Detaillierte Analyse von Unternehmen, die in Defence Industry Equipment vertreten sind, zusammen mit ihren starken Strategien / Starke und unternehmensinterne SWOT-Profile Analyse und Prognosen von Makro- und Mikrofaktoren / Auswirkungen auf die aktuellen Akteure in der Rüstungsindustrie auf Unternehmen, die in Südkorea tätig sind und planen, in die Verteidigungsindustrie einzusteigen 25.04.18 #factors http://somtxt.de/s/Pqo

Die Faktoren, die das Marktwachstum beeinflussen, werden im Detail untersucht. Der Bericht zeigt auch allgemeine Schwächen auf, die die am Markt tätigen Unternehmen vermeiden müssen, um im Verlauf des Prognosezeitraums ein nachhaltiges Wachstum zu erzielen. Darüber hinaus werden Profile von einigen der führenden Akteure, die das Wachstum des globalen Marktes vorantreiben und fördern, in die Studie einbezogen. 18.04.18 #factors http://somtxt.de/s/P16

7.5 access

Herkömmliche Netzwerksicherheit beruht auf einem sicheren Perimeter - alles innerhalb des Perimeters ist vertrauenswürdig, und alles außerhalb des Perimeters ist es nicht. Ein Netzwerk ohne Vertrauenswürdigkeit behandelt den gesamten Datenverkehr als nicht vertrauenswürdig und beschränkt den Zugriff auf sichere Geschäftsdaten und sensible Ressourcen so weit wie möglich, um das Risiko zu verringern und den Schaden von Sicherheitsverletzungen zu mindern. Der Technologiekonzern Google hat in den letzten Jahren ein Sicherheitsmodell namens BeyondCorp entwickelt. 08.06.18 #access http://somtxt.de/s/P9e

Ein solcher Ansatz basiert auf dem Konzept eines Zero Trust Network. Herkömmliche Netzwerksicherheit beruht auf einem sicheren Perimeter - alles innerhalb des Perimeters ist vertrauenswürdig, und alles außerhalb des Perimeters ist es nicht. Ein Netzwerk ohne Vertrauenswürdigkeit behandelt den gesamten Datenverkehr als nicht vertrauenswürdig und

beschränkt den Zugriff auf sichere Geschäftsdaten und sensible Ressourcen so weit wie möglich, um das Risiko zu verringern und den Schaden von Sicherheitsverletzungen zu mindern. 08.06.18 #access http://somtxt.de/s/P9e

Agile Entwicklungs- und DevOps-Teams - Die integrierte bidirektionale Integration für viele Industriestandard-Produkte wie JIRA, Jenkins und Qualys bedeutet eine schnelle Entwicklung und DevOps-Teams können die Ergebnisse von Bedrohungsmodellen direkt über ihre vorhandenen Toolsets nutzen. Der Self-Service-Zugriff auf die Threat-Model-Ausgaben bedeutet, dass spezifische Sicherheitsanforderungen nach Bedarf verfügbar sind, wenn eine Anwendung die CI / CD-Pipeline durchläuft. 05.06.18 #access http://somtxt.de/s/P3H

Cisco-Forscher forderten sowohl Verbraucher als auch Unternehmen auf, die Bedrohung durch VPNFilter ernst zu nehmen. Obwohl die Bedrohung für IoT-Geräte nichts Neues ist, hat die Tatsache, dass diese Geräte von fortgeschrittenen nationalstaatlichen Akteuren zur Durchführung von Cyber-Operationen verwendet werden, was möglicherweise zur Zerstörung des Geräts führen könnte, die Dringlichkeit des Umgangs mit diesem Gerät stark erhöht Frage , schrieben sie. 31.05.18 #devices http://somtxt.de/s/P3w

Durch das Testen der Infrastruktur, der Auslastung, des Netzwerks und anderer Computerressourcen, die mit Ihrem System verbunden sind, können Sie Fehler in Ihrem System besser verstehen. Wenn Sie ein Intrusion Detection System (IDS) in Ihr System integrieren, können Sie bösartige Aktivitäten in Ihrem Netzwerk überwachen und verfolgen. Wenn es Änderungen feststellt, löst es eine Bestätigung an das Hauptverwaltungssystem aus, um alle laufenden Aktivitäten zu beenden und die Systemsicherheit zu verbessern. 15.05.18 #activities http://somtxt.de/s/Ps8

Sicherheitsanalysten können diese Analysen nutzen, um verdächtiges Verhalten zu überwachen und zu identifizieren. Maschinelles Lernen ist eine Technik, die den täglichen Betrieb eines Netzwerks beobachtet, um eine Basis für das zu schaffen, was als normal angesehen wird, und vergleicht diese Baseline mit Aktivitäten, Prozessen und Netzwerkverkehr in Echtzeit. Wenn das Verhalten von legitimer oder akzeptabler Leistung abweicht, wird es als anomal und potenziell bösartig gekennzeichnet. 09.05.18 #identify http://somtxt.de/s/Psa

Alle sechs Vorschläge der Aktionäre wurden abgelehnt: Erweiterung der Möglichkeit, eine besondere Aktionärsversammlung einzuberufen; einen Bericht über Lobbying-Aktivitäten veröffentlichen; Verabschiedung einer unabhängigen Stuhlpolitik; einen Bericht über die Durchführbarkeit der Einbeziehung von Leistungsindikatoren für Cyber-Sicherheit und Datenschutz in die Vergütung von Führungskräften erstellen; Änderung der Claw-Back-Politik der Geschäftsleitung; und die Anlageoptionen im nicht qualifizierten Sparplan ändern. 03.05.18 #activities http://somtxt.de/s/PqQ

ECS, das vor der Übernahme zu den größten privaten Auftragnehmern für öffentliche Dienstleistungen in den Vereinigten Staaten zählte, ist gut positioniert, um von höheren Ausgaben der Bundesregierung für unternehmenskritische Technologielösungen der nächsten Generation, einschließlich Cyber Security, Data Analytics, zu profitieren , Künstliche Intelligenz und Cloud-Integration. Finanzergebnisse für das erste Quartal 2018 25.04.18 #integration http://somtxt.de/s/Pqf

Post navigationControl-Systeme, Schutz- und Steuerungsautomatisierung sowie Berichtsautomatisierungs-Reportserien von Newton-Evans Research Finden Sie in wichtigen

Bereichen der Cybersicherheit und -kommunikation eine gemeinsame Basis MARKTTRENDS DIGEST Neuigkeiten und Updates zu unserer laufenden Forschung; zusammenfassende Bewertungen und Highlights aus abgeschlossenen Studien 25.04.18 #devices http://somtxt.de/s/Pqr

Die Russen nutzen das Smart Install Exploitation Tool (SIET), das seit November 2016 online ist und in die Steuerung und Kontrolle übergeht. Die Hacker der russischen Regierung müssen keine Zero-Day-Sicherheitslücken ausnutzen oder Malware installieren, um Netzwerkgeräte auszunutzen, warnte der Advisor, da sie Schwachstellen ausnutzen können, die auf die Verwendung von Legacy-Protokollen oder schlechte Sicherheitsmaßnahmen zurückzuführen sind. 17.04.18 #devices http://somtxt.de/s/P13

7.6 network

Array Networks hat seine Management-Plattform für zentralisierte Konfiguration, Überwachung und Analyse für private Cloud-Umgebungen eingeführt. Symantec hat seine integrierte Cyber Defense-Plattform um Endpoint-Schutz, Isolationstechnologie und softwaredefinierte Cloud-Dienste erweitert. Der IoT-Sicherheitsanbieter Bullguard hat auf seiner Dojo-Plattform einen intelligenten IoT-Vulnerability-Scanner für Kommunikationsdienstleister eingeführt. 08.06.18 #monitoring http://somtxt.de/s/P9r

Mit Pulse Secure haben unsere Kunden dank der integrierten Zugriffs- und Endpunktsichtbarkeit mehr Einblick und Effizienz gewonnen, um diese neuen Anforderungen zu erfüllen und Benutzer-, Geräte- und IOT-Sicherheitsprobleme zu lösen. Die Bundesregierung ist kontinuierlich und kontextbewusst Sicherheitsagenda für die Netzwerkzugriffskontrolle und Endpunktsicherheit, um Mobilität, IOT-Bedrohungen, hybride IT und umfassendere militärische Risiken anzugehen. 05.06.18 #control http://somtxt.de/s/P97

Während Cybersicherheit und Datenschutz in den letzten zehn Jahren ein natürlicher Schwerpunkt der Bundesregierung waren, hat die jüngste weit verbreitete Expansion in die Welt der IOT und die Ermöglichung von Mobilität und die damit verbundenen Schwachstellen die Schutzlast exponentiell erhöht Bundesnetzwerke gegen Bedrohungsakteure und gleichzeitig neue, komplexe Compliance-Anforderungen für unsere Kunden , sagte Sheryl Dunlap, CEO von Empower Solutions. 05.06.18 #control http://somtxt.de/s/P97

Pro Warenkorb kann nur ein Gutscheincode verwendet werden. Manager, Ingenieure und andere technische Fachkräfte mit wachsender Verantwortung für Design / Administration / Management oder Netzwerkadministration von Cyber-Sicherheit, Fachleute in Regierungs- oder datenintensiven Branchen wie Energie, Finanzen, Gesundheitswesen und Verteidigung, deren Rollen stark von der Sicherheit der Daten beeinflusst werden, Fachleute, die in Rollen für Cyber-Sicherheit wechseln 25.05.18 #network http://somtxt.de/s/P3D

Unsere nationalen Telekommunikationsanbieter werden außerdem eine hochentwickelte Sicherheitsüberwachung einsetzen, um ihr Netzwerk vor ständigen Angriffen zu erkennen und zu schützen. Aber wie können wir sicher sein, dass das Silizium nicht an der Quelle kompromittiert wurde? Es gab in der Vergangenheit Berichte über verkaufte und im großen Stil eingesetzte Geräte mit Hintertüren, die in der Software konfiguriert wurden, um eine absichtliche Sicherheitsumgehung zu erzeugen. 20.05.18 #monitoring http://somtxt.de/s/P3W

Es wird prognostiziert, dass selbstfahrende Autos 4000 GB Daten pro Fahrstunde ausgeben werden. Big Data Analytics, als aufstrebende Analysetechnologie, hat die Fähigkeit, diese riesigen Datenmengen zu sammeln, zu speichern, zu verarbeiten und zu visualisieren. Big Data Analytics in Cybersecurity untersucht Sicherheitsherausforderungen, die Big Data betreffen, und liefert verwertbare Erkenntnisse, die zur Verbesserung der aktuellen Praktiken von Netzwerkbetreibern und Administratoren verwendet werden können. 06.05.18 #network http://somtxt.de/s/PsW

Tool erhält auch E-Mail-Benachrichtigungen Darüber hinaus hat Facebook auch die Möglichkeit hinzugefügt, Domaininhaber per E-Mail zu benachrichtigen, wenn eine neue verdächtige Phishing-Domain in CT-Protokollen erscheint. Frühere Berichte und Umfragen haben gezeigt, dass Phishing-Angriffe in den ersten Stunden nach dem Start einer Phishing-Kampagne in der Regel am effektivsten sind. Wenn Sie also Warnungen erhalten und so schnell wie möglich reagieren, kann dies schwerwiegende Cyber-Sicherheitsvorfälle für Ihre Benutzer oder Mitarbeiter verhindern. 03.05.18 #ability http://somtxt.de/s/PqJ

Darüber hinaus zwingen stringente regulatorische Normen und Datenschutzgesetze Organisationen dazu, Cyber-Sicherheitstools in ihre Netzwerkinfrastruktur zu integrieren. Unter den Regionen wird erwartet, dass Nordamerika 2017 den weltweit verwalteten Markt für Cyber-Sicherheitsdienste dominieren wird, und dieser Trend dürfte sich im gesamten Prognosezeitraum fortsetzen. Der von Nordamerika gemanagte Markt für Cyber-Sicherheitsdienste wird zwischen 2017 und 2026 bei einer CAGR von 18,5% wachsen. 02.05.18 #network http://somtxt.de/s/Pqw

International könnte das Unternehmen eine Aufmerksamkeit haben, in Verlust oder klar definiert, es hat keine Kompromisse gemacht, die Mitarbeiter von sensiblen Richtlinien und eine materielle IT-geschützte Kontrolle der Zugriffsverletzung auf unsere Informationen, Rechte. Unsere Operationen. Kommunikationsinformationen und IT-Business-Sicherheitskontinuität Rahmen und Störungsinfrastruktur über Operationen. 30.04.18 #control http://somtxt.de/s/PqO