Research Institute
Cyber Defence
Bundeswehr University Munich

Zusammenfassung Workshop 2
Challenges and Application of Threat Intelligence

In diesem Workshop wurde durch Marco Barros Lourenco zunächst das von ENISA entwickelte „Fähighkeits Framework für Threat Intelligence Lösungen“ präsentiert. Ein Cyber Threat Intelligence Framework muss die Implementierung von Prozessen und Fähigkeiten welche auf die kontinuierliche Erzeugung von relavanter, kontextualisierter und umsetzbarer Information abzielt. Den heutigen Lösungen fehlt oft der Kontext, denn Unternehmen benötigen mehr Informationen um Risiken zu identifizieren und zu managen und letztlich Cyberangriffe zu verhindern.

Danach berichtete Dr. Thomas Schreck einen Erfahrungsbericht aus der betrieblichen Praxis bei Siemens. Er betonte insbesondere die Wichtigkeit des Faktors Zeit im Unternehmenskontext sowie die Notwendigkeit einer Kultur des Austauschs von Tools und IoCs (Indicators of Compromise). Jedoch wird dieser Austausch insbesondere durch juristische Bedenken häufig verzögert bzw. behindert. Threat Intelligence sollte (a) auf gängigen Standtards - wie beispielsweise dem „Traffic Light Protocol“ - basieren, (b) Es sollte ein Standard für den Austausch definiert werden, (c) Es sollte so früh/schnell wie möglich mit Partnern ausgetauscht werden, und (d) Kommerzielle Anbieter sollten regelmäßig evaluiert werden.

Im anschließenden Panel wurden drei Herausforderungen für die zukünftige TI Lösungen identifiziert. Erstens müssen zuverlässige und anonymisierte Lösungen für Anonymisierung geschaffen werden, da diese heute noch einen wesentlichen Hinderrungsgrund darstellen, dass Unternehmen sich nicht am aktiven Austausch beteiligen.

Zweitens wurde die Schafftung von Austauschsystemen und -plattformen zwischen verschiedenen isolierten bereits exisitierenden Communities als wichtiger nächster Schritt für die Zukunft von Cyber Threat Intelligence identifiziert.

Die dritte große Herausforderung ist die Beteiligung von kleinen und mittelständischen Unternehmen (KMUs) am Austausch von TI, denn diesen fehlt oft das nötige Personal. Die Panelisten und das Auditorium waren sich einig, dass es hierfür zukünftig einen Cyber Threat-Intelligence-as-a-Service Markt geben muss.