CYBERCRIME: DER TAG, AN DEM DIE FLOTTE STILLSTAND

cyber[contact].at
INFORMATION SECURITY & CERT-TEAM

Der Sommer 2017 markiert den Beginn einer neuen Ära der Cyberkriminalität und ihrer Bekämpfung.. Der Hackerangriff auf den Logistik- und Transport-Giganten „Maersk“ verändert die digitale Welt der Informationssicherheit grundlegend, nicht nur der größten Container-Reederei der Welt steht damals wegen der Ransomware „NotPetya“ das Wasser bis zum Hals. Parallelen zum gegenwärtigen Ukraine-Konflikt und das Spiel mit der Angst vor globaler Destabilisierung spielen dabei eine zentrale Rolle.

27. Juni 2017. „Maersk“-Mitarbeiter rund um den Globus bekommen verdächtige Meldungen von Reparaturarbeiten an ihren Dateisystemen. Andere sollen 300 Dollar in Bitcoin zahlen, um verschlüsselte Dateien zu entsperren. Es ist nicht der Anfang vom Ende, sondern die letzte Stufe eines groß angelegten und rücksichtslosen Cyberangriffs auf die globalisierte Welt.
Die Schäden, die die Ransomware „NotPetya“ zu diesem Zeitpunkt angerichtet hat, sind irreparabel.
753 Schiffe können innerhalb weniger Minuten nicht mehr geortet werden, die Satelliten-Kommunikation wird unterbrochen, dutzende Häfen rund um den Globus werden blockiert. Ca. 20 % des gesamten Welthandels werden lahmgelegt, 30.000 Mitarbeiter sind betroffen.

Ab dem Zeitpunkt des Sicherheitsvorfalls war Maersk mehrere Wochen lang nicht geschäftsfähig, Experten rechnen mit einem wirtschaftlichen Schaden zwischen 250 und 400 Millionen Dollar.
Auch andere Unternehmen waren von dem Hackerangriff betroffen - zum Beispiel die europäische Tochtergesellschaft des Transportunternehmens FedEx oder der Pharma-Gigant Merck. Insgesamt dürfte sich der Schaden der Cyberattacke auf mehrere Milliarden Dollar belaufen.

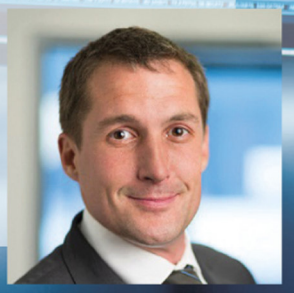
„Petya“ vs. „NotPetya“, Russland vs. Ukraine

Der Hackerangriff vom 27. Juni 2017 steht für eine große Zäsur in der Bekämpfung von Cyberkriminalität. Beispielhaft dafür ist auch der Name der Ransomware „NotPetya“. Denn im Gegensatz zum Vorgänger – dem Verschlüsselungstrojaner „Petya“ - geht es nicht um Erpressen von Lösegeldsummen für eine System- bzw. Datenwiederherstellung. „NotPetya“ hingegen wurde zwar als „herkömmliche“ Malware getarnt, war aber einzig und alleine auf Verbreitung und Schadensmaximierung ausgerichtet. Als Drahtzieher im Hintergrund wird das russische Militär vermutet, das eigentliche Ziel: Die systematische Destabilisierung der Ukraine. Doch „NotPetya“ geriet außer Kontrolle. Betroffen war schlussendlich die gesamte globalisierte Welt.
Der Handel mit hochprofessioneller Schadsoftware und „Cybercrime as a Service“ entwickelt sich daraufhin zu einem riesigen Geschäftsfeld. Eine Welle von Cyberattacken mit Fokus auf Erpressung, Vernichtung und Identitätsdiebstahl beginnt.
Aus Tätersicht stehen nun nicht mehr internationale Konzerne oder militärische Einrichtungen im Fokus, sondern klein – und mittelständische Betriebe, Spitäler, Behörden und NGO´s.

Cyberdefense: Prävention, Reaktion, Training

Die österreichische Firma „Cybercontact“ ist seit vielen Jahren auf Sicherheitskonferenzen rund um den Globus unterwegs. In Gesprächen wie zum Beispiel mit dem ehemaligen Chief Information Security Officer der Royal Air Force und jetzigem CISO der MÄRSK, Andy Powell, werden wichtige Erkenntnisse über den „Maersk“-Cyberangriff zu Tage gefördert:
„Setze Präventivmaßnahmen, bereite dich darauf vor dass es passiert, und trainiere dieses Szenario mit Deinem Team einmal im Jahr“ (Recovery Plan)“

Wir haben als MSSP - Managed Security Service Provider für unsere Kunden ein Lösungsportfolio für alle Bereiche der Informationssicherheit entwickelt, (Mensch, Technologie, Organisation). Dieser 360°-Ansatz ermöglicht es uns punktgenaue Maßnahmen zu erarbeiten, Risiken frühzeitig zu erkennen und nachweislich den bestmöglichen Schutz vor z. B. Ransomware sicherzustellen.



CEO Alexander Franz

W: cybercontact.at
E: info@cybercontact.at
T: +43 1 96266 100