7 PRAXISTIPPS

BEI CYBER-ATTACKEN DIE OBERHAND BEHALTEN

23. Juli 2018

Während seiner EU-Ratspräsidentschaft will Österreich im zweiten Halbjahr 2018 einen deutlichen Schwerpunkt auf das Thema Cyber-Sicherheit setzen. Aus gutem Grund: Die Gefährdung durch Angriffe auf die IT-Infrastruktur großer Organisationen aber auch Unternehmen jeder Größe ist in den letzten Jahren erheblich gestiegen.

In Österreich stieg die Zahl der angezeigten Fälle von 2016 auf 2017 um 34,8 Prozent. Rund ein Drittel dieser Anzeigen betraf den Tatbestand der Datenbeschädigung.

"Mitverantwortlich dafür ist die steigende Verbreitung von Ransomware", erklärt Manuel Kern, CTO bei Iphos IT Solutions. "Durch die dabei eingesetzten Kryptotrojaner

werden Daten auf den befallenen Rechnern verschlüsselt und sind damit für die User nicht mehr nutzbar." Gegen ein Lösegeld (engl. Ransom) versprechen die Täter einen Schlüssel zur Wiederherstellung zur Verfügung zu stellen - ein Versprechen, das oft nicht gehalten wird. Verbreitet werden die Verschlüsselungstrojaner im Allgemeinen durch E-Mails, unsichere Downloads aus dem Internet sowie Sicherheitslücken in den verwendeten Web-Browsern und Betriebssystemen.

Ebenfalls auf die Verbreitung durch E-Mails setzen Cyberkriminelle bei ihren Phishing-Attacken. Durch zusehends besser gefälschte Nachrichten von Institutionen wie Banken, Online-Shops, etc. werden User zu ebenfalls täuschend echt aussehenden Webportalen weitergeleitet, über die die Login-Daten ausspioniert werden. Aber auch Mails, in denen Betrüger sich als Vorgesetzten ausgeben und Zahlungen anordnen - Stichwort Social Engeneering -, sind immer häufiger an der Tagesordnung.

Die dritte Cybercrime Schiene, die oft die IT eines Unternehmens lahmlegt und dadurch enormen Schaden verursacht - durch den Entgang von Einnahmen genauso wie durch Reputationsverlust, sind Angriffe über sogenannte Botnets: Nicht erreichbare Websites und Webshops durch DDoS-Attacken (Distributed-Denial-of-Service-Angriffe) sowie durch Schadsoftware selbst zum Botnet-Zombie gemachte Rechner mit hohen Performanceverlusten zählen dazu. Ebenso das Hijacking von Computern, die dann zum Schürfen von Kryptowährungen wie Bitcoin, Monero und Etherum missbraucht werden und durch die Überbeanspruchung nicht nur stark an Rechenleistung einbüßen, sondern durch hohe Auslastung auch physischen Schaden nehmen können.

Wie können sich Unternehmen gegen solche Cyber-Angriffe wehren?

Wir haben sieben Tipps für Sie zusammengestellt, die Sie dabei unterstützen sollen, auch im Falle einer Cyber-Attacke auf Ihr Unternehmen die Oberhand zu behalten:

Effizientes Patchmanagement - Regelmäßige Updates von Betriebssystem, Software, Virenschutz & Firewall

Eine regelmäßige und vor allem zeitnahe Installation von Updates der im Unternehmen eingesetzten Software, des Betriebssystems und natürlich des Antivirusprogramms und der Firewall sollten selbstverständlich sein. Die Sicherheitslücke "EternalBlue", welche für die Ausbreitung der derzeit größten Ransomware-Angriffswelle für die Verbreitung ausgenutzt wurde, konnte von Microsoft bereits 59 Tage vor erstmaliger Ausnutzung durch WannaCry über ein Sicherheitsupdate beseitigt werden. Die Installation dieses Sicherheitsupdates hätte die rasante Ausbreitung auf über 220.000 infizierten Computern in über 150 Ländern innerhalb von drei Tagen verhindert. Wie dieses Beispiel zeigt, ist ein effizientes Patchmanagement einer der wichtigsten Schritte in Richtung IT-Sicherheit und Schutz vor Cybercrime. "Sicherheitslücken werden durch die Patches gestopft,

potentiellen Angreifern, welche es auf die breite Masse abgesehen haben, bleibt der Weg zu Ihrer IT-Infrastruktur so versperrt", erklärt Kern.

"Der Punkt Patchmanagement sollte idealerweise in jedem IT-Wartungsvertrag inkludiert sein, denn so wird sichergestellt, dass Unternehmen raschest möglich wichtige Updates und Upgrades eingespielt bekommen und damit auf der sicheren Seite sind. Wichtig ist auch, dass dieser Prozess in unregelmäßigen Abständen, im besten Fall von einem unabhängigem Dritten, überprüft wird", so Kern weiter. "Im Tagesgeschäft ist schließlich keine Zeit, sich mit der nötigen Intensität mit dem Thema IT-Sicherheit auseinanderzusetzen."

Bewusstsein für die Gefährdung bei Mitarbeitern schaffen

In den meisten Fällen wird Malware von Mitarbeitern durch unbedachtes Öffnen von E-Mail Anhängen, Folgen von Hyperlinks, privatem Surfverhalten oder mittels externer Medien (USB-Sticks, etc.) in das Unternehmensnetzwerk eingeschleust. Eine aktuelle Antivirus-Software soll vor Malware-Angriffen schützen und gehört mittlerweile zur Grundinstallation eines jeden IT-Systems, jedoch ist diese oder eine zusätzliche Security-Software nicht immer der Weisheit letzter Schluss. Je nach Produkt und Funktionsumfang schützt sie zwar vor den meisten Angriffen, doch verspricht kein seriöser Hersteller oder Lieferant 100%igen Schutz. Wenn von IT-Security gesprochen wird, denken viele nur an technische, produktorientierte Lösungen.

"Der Faktor Mensch spielt bei Erreichung eines sicheren Unternehmensnetzwerks jedoch ein entscheidende, wenn nicht sogar die entscheidendste Rolle. So müssen neben technischen, auch immer organisatorische und personelle Maßnahmen in Betracht gezogen werden", hält Kern fest.

"Der beste Malware-Schutz hilft nichts, wenn gefälschte Nachrichten nicht als solche erkannt und hinterfragt werden, Logins und Passwörter einladend auf einem Post-It am Bildschirm kleben oder unverschlüsselte Notebooks oder USB-Sticks mit wichtigen Unternehmensdaten im Bus vergessen werden. Die Mitarbeiter müssen über Gefahren aufgeklärt und im sicheren Umgang mit Informations-Systemen geschult werden", meint Kern.

Mit der richtigen Backup-Strategie zu Business Continuity

Hat sich ein Unternehmen trotz Security Maßnahmen einen Verschlüsselungstrojaner eingefangen, sollte man besser auf eine umfassende Backup-Strategie gesetzt haben. Dazu gehören zum Beispiel gespiegelte, sich gegenseitig überwachende Server-Systeme und tägliche Sicherungen, die offline - also außerhalb der Zugriffsmöglichkeit von Ransomware - aufbewahrt werden.

Unternehmensweite Passwort-Regelung

"Unsichere Passwörter wie einfache Zahlenkombinationen oder persönliche Informationen machen es Kriminellen einfach, ins Unternehmensnetzwerk einzudringen und

sollten mittlerweile Tabu sein. Klare Vorgaben bezüglich der Passwort-Generierung und Aufbewahrung - keine Post-Its! - sowie das regelmäßige Ändern von Passwörtern, vor allem aber auch die Verwendung unterschiedlicher Passwörter für Anwendungen sorgen für einen besseren Schutz der diversen Login-Daten im Unternehmen. Zur Verwaltung sicherer, einzigartiger Passwörter pro Anwendung eignet sich die Verwendung eines Passwort-Safes wie die kostenfreie Software LastPass", erläutert Kern. "Zugänge sollten da wo möglich mittels Zwei-Faktor-Authentifizierung geschützt sein."

Gemeinsam mit dem ISP DDoS-Attacken abwehren

DDoS-Angriffe richten sich im Allgemeinen gegen Web-, Mail oder DNS-Server. Im Zuge solcher Attacken wird mehr Datenverkehr auf bestimmte IP-Adressen umgeleitet als diese verarbeiten kann - bis der Server kracht. "Verhindern lassen sich DDoS-Attacken nicht, aber man kann dafür sorgen, dass sie nicht in einem Stillstand der IT-Infrastruktur enden", meint Manuel Kern. "Entscheidend dabei ist die richtige Konfiguration der eingesetzten Software, sowie die passende Dimensionierung der Infrastruktur, die auch mal, zumindest für kurze Zeit, eine stärkere Last tragen kann. Eine gute Zusammenarbeit mit dem Provider ist in der Abwehr allerdings der wichtigste Schritt. Dieser kann den Datenverkehr im Backbone des Netzes überwachen und bei auffälligen Abweichungen nach oben eingreifen. Im Vorfeld sollten mittels Baselining die normale Systemlast festgestellt werden, damit Abweichungen schneller erkannt werden. Für den Fall eines Angriffs sollten gemeinsam mit dem Provider entsprechende Prozesse und Checklisten erstellt werden. So ist eine schnelle und gezielte Reaktion auf DDoS-Attacken möglich", erklärt Kern weiter.

Incident Management für Business Continuity

Prozesse und Checklisten, unter anderem für DDoS-Attacken, sollten auch Bestandteil einer Incident Management Strategie sein. Genau festzuhalten, was im Falle eines Falles zu tun ist, spart Zeit und kann helfen, das Schlimmste zu verhindern oder Folgeschäden zu minimieren. "Oftmals ist das Wissen, welche Schritte bei der Behebung einer Störung notwendig sind zwar verfügbar, jedoch über die Institution oder Dienstleister verstreut und vor allem in Ausnahmesituationen nicht effizient abzurufen. Wissen Sie und Ihre Kollegen, was im Falle eines Ransomware Angriffs, oder eines DDos-Angriffs zu tun und wer zu kontaktieren ist?", stellt Kern die entscheidende Frage in den Raum.

Egal, ob es sich um Cyber-Angriffe oder andere die IT-Infrastruktur betreffende Vorfälle handelt, um für Business Continuity zu sorgen, ist eine Desaster Recovery Strategie mit zuvor festgelegten und getesteten Prozessen von essentieller Bedeutung.

IT-Riskmanagement

Spätestens seit der im Mai in Kraft getretenen EU-DSGVO ist bekannt, in einer sauber geführten IT-Landschaft darf eine Risiko-Analyse hinsichtlich der Unternehmens-IT nicht fehlen. "Gerade bei Cyber-Angriffen ist das Risiko hoch, dass auch sensible personenbezogene Daten im Unternehmen kompromittiert werden", erläutert Manuel Kern die gestiegene Bedeutung einer IT-Riskmanagement Strategie. "Wenn dann doch trotz optimaler Sicherheitsvorkehrungen etwas passiert, ist man mit einer detaillierten Risiko-Analyse und den im Incident Management festgelegten Strategien zur Schadensbegrenzung und -behebung abgesichert."

Manuel Kern, CTO bei Iphos IT Solutions, www.iphos.com

Firewall (/component/tags/tag/firewall)

Cyberangriff (/bitcoin-hacker-co/cyberangriff)

Cyber Crime (/bitcoin-hacker-co/cyber-crime)

Passwort (/component/tags/tag/passwort)

GRID LIST

(/it-sicherheit/enterprise-security/19183-cyberschutz-unternehmen-brauchen-wirksame-

(/it-sicherheit/enterprise-security/19130-airlock-waf-7-1-automatisierung-der-it-security)

(/it-sicherheit/enterprise-security/19063-cloud-account-defense-sicherheit-bei-office-365-accounts)