Vier Arten von Cyberangriffen, auf die man vorbereitet sein sollte

Florian Malecki, International Product Marketing Director, StorageCraft

Cyberkriminelle sind schlauer denn je und es ist zu befürchten, dass in den kommenden Monaten weitere ausgereifte Cyberangriffe stattfinden werden. Bis zum Jahr 2021 entstehen durch Cyberkriminalität schätzungsweise Schäden in Höhe von rund 6 Billionen US-Dollar – eine Summe, die deutlich macht, wie lukrativ es ist, Unternehmen mit digitalen Attacken anzugreifen. Aus diesem Grund wird Cyberkriminalität auch in Zukunft nicht abnehmen. Aber es lässt sich zumindest einiges tun, um sich gegen derartige Angriffe zu wappnen. Wer die von Cyberkriminellen eingesetzten neuen Technologien kennt und ihre Funktionsweise versteht, der kann sich, sein Unternehmen und seine Reputation besser schützen.

Hier sind die vier größten Bedrohungen, auf die man achten sollte:

Angriffe, die auf künstlicher Intelligenz und maschinellem Lernen basieren
KI und maschinelles Lernen sind derzeit die beiden am weitesten verbreiteten Technik-Buzzwords und Cyberkriminelle haben bereits damit begonnen, diese Tools auf clevere Art und Weise auszunutzen. So setzen sie maschinelles Lernen beispielsweise für die Erzeugung gefälschter Nachrichten ein. Sie nutzen also die praktischen Möglichkeiten dieser Technologie, um ihre Phishing-Angriffe durchzuführen. Zudem kann die künstliche Intelligenz von Cyberkriminellen auch dazu missbraucht werden, um Malware zu entwickeln, die in der Lage ist, Sandboxes zu täuschen und über diese auf Unternehmenssysteme zuzugreifen.

Ransomware
Bedrohungen wie WannaCry und Dutzende andere Bedrohungen erinnern permanent daran, wie groß die Schäden sind, die durch Ransomware verursacht

werden. Und dieses Problem wächst weiter. Laut einem Bericht von McAfee sind die Ransomware-Probleme im Jahr 2017 um 56 Prozent gestiegen. Trend Micro führte Ransomware sogar als Cyber-Bedrohung Nummer eins für 2018 an und bezeichnet Ransomware als das „Paradies für Cyberkriminelle". Glücklicherweise holt die Cybersicherheitswelt inzwischen auf: Verbraucher sind gewissenhafter, es taucht weniger handelsübliche Ransomware auf und die Strafverfolgungsbehörden arbeiten intensiv daran, nachhaltig gegen diese Art von Cyberbetrug vorzugehen. Trotz dieser Bemühungen nimmt Ransomware weiter zu, so dass zu noch mehr Wachsamkeit geraten wird. Der beste Weg, sich vor durch Ransomware verursachten Problemen zu schützen, ist es, eine zuverlässige Backup- und Wiederherstellungssoftware im Einsatz zu haben.

E-Mail-Betrug

Auch E-Mail-Betrug wird immer innovativer. In der Tat stehlen Cyberkriminelle Milliarden von Dollar, indem sie einfach gefälschte E-Mails versenden, die für das ungeübte Auge überzeugend echt aussehen. Das FBI berichtet, dass geschäftliche E-Mail-Betrügereien zwischen Januar 2015 und Dezember 2016 um 2.370 Prozent zugenommen haben. Für das Jahr 2018 wurden sogar weltweite Schäden von fast neun Milliarden Dollar durch E-Mail-Betrügereien vorhergesagt. Das hängt vermutlich damit zusammen, dass Unternehmen Protokolle für die verschiedene Arten ihrer Transaktionen erstellen müssen: Ein System von „Checks and Balances“ innerhalb des Unternehmens soll so verhindern, dass betrügerische Transaktionen durchgeführt werden. Wenn es um Phishing-Angriffe per E-Mail geht, sollten Benutzer deshalb unbedingt wissen, woran sie gefälschte E-Mails erkennen, damit sie diese niemals aus Versehen öffnen.

Connected-Device-Attacken

Allein im vergangenen Jahr gab es viele verteilte Denial-of-Service (DDoS)-Angriffe, die mittels Hunderten geklauter IoT-Geräte umgesetzt wurden. Auch diese Art von Angriffen wird wahrscheinlich noch zunehmen. Sie ermöglichen es Hackern vielfach Proxys zu erstellen und Standortdaten, sowie den Webverkehr zu verstecken. Damit

ist es für die Strafverfolgungsbehörden sehr schwierig ist herauszufinden, woher ein Angriff ursprünglich kommt. Trend Micro stellt auch fest, dass IoT-Geräte oftmals seltener gepatcht werden als andere Geräte, so dass Schwachstellen nicht selten über einen längeren Zeitraum bestehen.

Andere anfällige Geräte sind Drohnen, drahtlose Heimgeräte oder sogar Bioimplantate wie Herzschrittmacher. Viele dieser Geräte haben keine eingebauten Daten-Sicherheitssysteme. Das bedeutet, dass die Benutzer die Verantwortung für ihre eigene Sicherheit übernehmen müssen, etwa indem sie sicherstellen, dass sichere Passwörter verwendet werden und sich die Gerätesoftware immer auf dem neuesten Stand befindet.

Wie kann man sich schützen

Da Cyberangriffe, insbesondere durch Ransomware, immer häufiger und dreister werden, müssen Unternehmen darüber nachdenken, wie sie einen mehrschichtigen Sicherheitsansatz entwickeln und umsetzen können. Dieser sollte u.a. folgendes umfassen:

- Mitarbeiterschulung – Mitarbeiter sind in den meisten Fällen an vorderster Front. Deshalb sollte sichergestellt sein, dass sie genau wissen, was von ihnen verlangt wird und vor was sie auf der Hut sein müssen.
- Adminrechte – nicht alle Mitarbeiter benötigen die gleichen Zugriffsrechte. Deshalb sollte man die Adminrechte beschränken. Es sollte etwa gewährleistet sein, dass gerade für sensible Daten nur derjenige Admin-Rechte hat, der diese Daten auch wirklich benötigt.
- Patch Management – alle Betriebssysteme, Software und Firmware von Endgeräten sollten regelmäßig gepatcht werden – spätestens dann, wenn Schwachstellen entdeckt werden.
- Antivirenschutz – es sollte ein Antiviren-Endpunktschutz mit aktualisierten Signaturen, Endpoint Sandboxing und Antivirenschutz der nächsten Generation implementiert sein.

- Phishing-Angriffe – Netzwerk-Sandboxing, Firewalls der nächsten Generation und E-Mail-Sicherheitslösungen sollten Phishing-Angriffe blockieren.
- Backup- und Recovery – der Backup- und Wiederherstellungsprozess sollte in festgelegten Abständen überprüft werden. Dabei sollte sichergestellt werden, dass keine kritischen Daten gesichert werden.
- Scale-Out-Speicher – es ist sicherzustellen, dass das Unternehmen mit einem Scale-Out-Speicher der neuesten Generation ausgestattet ist. Weil Lösungen, die mittels kontinuierlicher Snapshots für Datensicherheit sorgen, ein zunehmendes Datenwachstum mit sich bringen, können nur skalierbare Speicherlösungen bestmögliche Sicherheit leisten.

Jeder weiß, dass ein einziger Fall von Hacking und Datenverlust ein Unternehmen Millionen kosten kann. Aber es gibt auch viele indirekte Kosten – vom Reputationsverlust bis hin zur negativen Wahrnehmung bei Kunden- und Investoren, oder gar Rechtsstreitigkeiten. Die Risiken sind enorm. Während die genaue Summe möglicher Schäden vielfach nur schwer zu berechnen ist, ist es offensichtlich, dass Investitionen in die richtigen Technologien und Strategien, Cyberangriffe abwehren können. Wenn es um den Schutz von Daten und die Verhinderung von Cyberangriffen geht, zahlen sich diese Tools und Strategien schon dann aus, wenn sie nur einen einzigen Cyberangriff erfolgreich vereiteln.

###

StorageCraft Technology Corporation
380 Data Drive, Suite 300, Draper, Utah 84020 USA
P 801.545.4700 F 801.545.4705

Über StorageCraft

Mit den Lösungen von StorageCraft für Datensicherung, Datenmanagement und Business Continuity halten Unternehmen ihre kritischen Informationen stets sicher, zugänglich und optimiert. Die leistungsstarken Angebote für Datensicherheit von StorageCraft bieten sofortige, zuverlässige und vollständige Datenwiederherstellung und eliminieren Ausfallzeiten. Die innovative und konvergente Scale-Out-Plattform für Primär- und Sekundärspeicher mit integrierter Datensicherung löst die Herausforderungen des Datenwachstums. Sie ist effizient und einfach in der Anwendung für lokale, Cloud-basierte oder hybride Umgebungen. Weitere Informationen finden Sie unter www.StorageCraft.com.

Unternehmenskontakt

Jock Breitwieser
StorageCraft Technology Corp.
+1 408.800.5625
jock.breitwieser@storagecraft.com

Agenturkontakt

TC Communications
Arno Lücht
+49 (8081) 9546-19
Thilo Christ
+49 (8081) 9546-17
storagecraft@tc-communications.de
www.tc-communications.de