Schwachstelle Passwort

Cyberattacken können schwerwiegende Folgen für Unternehmen haben, starke Passwörter schützen

Die digitale Transformation und die damit einhergehende Verzahnung von Information Technology (IT) und Operational Technology (OT) machen Unternehmen weltweit zunehmend anfällig für die Attacken von Cyberkriminellen. Sind diese erfolgreich können die Folgen vielfältig sein: Vom Abfluss personenbezogener Daten, die jedes Unternehmen erhebt und deren Schutz gesetzlich geregelt ist, über den Diebstahl interner Daten bspw. aus der Forschungs- und Entwicklungsabteilung, bis hin zum Totalausfall der Produktion oder dem Entzug von Kapital durch CEO Fraud. Cyberattacken können also schwerwiegende wirtschaftliche Folgen für das betroffene Unternehmen haben. Doch wie erlangen Cyberkriminelle Zugang und wie können sich Unternehmen dagegen schützen?

Tagtäglich sehen sich Unternehmen mit hunderten bis tausenden Angriffen über Brute Force, Password Spraying oder Password Dictionary Attacks konfrontiert. Angriffspunkt Nummer eins sind die Mitarbeiter bzw. die von ihnen verwendeten schwachen Passwörter.

Stephan Halbmeier, Specops Software

Ransomware-Angriffe: Es kann teuer werden

Auch Ransomware-Angriffe bauen auf diesen genannten Methoden auf, haben aber in erster Linie die (vorübergehende) Sabotage der IT/OT zum Ziel, die allein durch Zahlung eines Lösegelds rückgängig gemacht werden kann. Im Unterschied zu anderen Cyberangriffen geht es daher primär nicht darum, Schaden zu erzeugen, sondern „nur" darum, Geld zu erpressen. Die Höhe des Lösegelds hängt von den Tätern, die den Angriff durchführen, und der bedrohten Organisation ab. Angestrebt ist seitens der Kriminellen, ein möglichst großes Schadensszenario aufzubauen. In der Folge stehen Unternehmen, die zur kritischen Infrastruktur eines Landes zählen, wie dies oftmals bei Chemieunternehmen der Fall ist, besonders im Fadenkreuz. Ein neueres Beispiel ist der Ransomware-Angriff im Sommer dieses Jahres auf eine Gaspipeline des Luxemburger Energieunternehmens Encevo. Hierbei wird davon ausgegangen, dass es sich um die gleichen Angreifer handelt, wie bei der Colonial-Pipeline-Attacke 2021.

Die Auswirkungen eines Angriffs können weitreichend und schnell sein. Unternehmen haben sofort keinen Zugriff mehr auf wichtige Dokumente und Systeme, in manchen Fällen sogar auf ihr gesamtes Netzwerk. Die Produktivität kann für einige Tage bis hin zu einigen Wochen zum Erliegen kommen.

Das kann sehr teuer werden. So zahlte das Management der Colonial Pipeline 4,4 Mio. USD Lösegeld. Und dies ist nur ein Teil des verursachten Schadens. Die Auswirkungen eines Angriffs lassen sich an den finanziellen Kosten, dem Produktivitätsverlust, den zusätzlichen Aufwand für die Behebung der Schwachstelle und der Schädigung des Rufs ablesen. Sophos, ein weltweit führender Anbieter von Cybersicherheit, hat in seiner Studie „The State of Ransomware 2021" herausgefunden, dass sich die durchschnittlichen Gesamtkosten für die Wiederherstellung nach einem Ransomware-Angriff innerhalb eines Jahres von 761.106 USD im Jahr 2020 auf 1,85 Mio. USD im Jahr 2021 mehr als verdoppelt haben.

Ein Muss: Verbessern Sie Ihre Passwortsicherheit

Was tun? Die Nutzung von Passwörtern ist immer noch die häufigste, Methode, um sich im Netzwerk zu authentifizieren. Sofern ausreichend starke Passwörter verwendet werden, ist diese Methode Stand heute immer noch effektiv und sicher. Durch den Faktor Mensch, kann sie zugleich aber auch zu einer Schwachstelle innerhalb der IT-Sicherheitskette werden – dann, wenn schwache oder kompromittierte Passwörter verwendet werden. Vor diesem Hintergrund gilt es im ersten Schritt zu prüfen, ob die dokumentierten Anforderungen an Passwortsicherheit den aktuellen Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) Rechnung tragen.

Startpunkt: Analyse des Ist-Zustands

Zunächst ist es wichtig, eine Bestandsaufnahme der im Unternehmen verwendeten Passwortrichtlinien zu machen. Für dieses Sicherheits-Assessment helfen Tools wie der Specops Password Auditor. Er analysiert die Benutzerkonten im Active Directory auf sämtliche passwortrelevanten Schwachstellen. Die Software scannt und überprüft die Passwort-Hashes der Benutzerkonten und gleicht sie gegen eine Datenbank mit kompromittierten Passwörtern, eine sog. Breached-Password-List, ab. Die Offline-Datenbank umfasst bspw. bei der kostenlosen Version des Specops Password Auditor mehr als 800 Mio. Passwort-Hashes (die in der Vergangenheit durch Datendiebstahl bekannt geworden sind). Bei kostenpflichtigen Angeboten sind die Datenbanken bedeutend größer: So umfasst die Specops Gesamtdatenbank 2,6 Mrd. kompromittierte Kennwörter. Die gesammelten Informationen werden anschließend in einem Audit-Bericht ausgegeben und ermöglichen es Unternehmen, die Sicherheitsrisiken zu bewerten und entsprechend zu handeln.

> *Starke Passwörter müssen heutzutage in erster Linie lang sein, dafür aber nicht mehr zwingend komplex.*

Dreh- und Angelpunkt: Starkes Passwort

Im Anschluss geht es darum technische und/oder organisatorische Maßnahmen zu implementieren, die den Einsatz starker Passwörter im Idealfall unternehmensweit garantieren. Um deren Stärke zu gewährleisten ist es wichtig, möglichst lange Passwörter zu nutzen. Denn wo in den vergangenen Jahren bspw. eine Kennwortlänge von mindestens acht Zeichen und hoher Komplexität empfohlen wurde, ist heute klar, dass man damit keine starken Passwörter mehr bilden kann. Im Gegenteil: starke Passwörter müssen heutzutage in erster Linie lang sein, dafür aber nicht mehr zwingend komplex. Eine einfache und effektive Methode ist es, Passphrasen zur Generierung starker Kennwörter zu verwenden.

Die Durchsetzung dieser und weiterer Richtlinien, wie z.B. eine jährliche Passwortänderung, kann durch den Einsatz einer Third Party Password Policy bzw. eines externen Passwortfilters für das Active Directory sichergestellt werden.

Um die Stärke der Passwörter noch besser zu gewährleisten, müssen zudem zwingend alle Kennwörter gegen Listen mit kompromittierten Passwörtern validiert und einfach zu erratende Kennwörter blockiert werden.

Fazit

Die Bedrohungslage durch Cyberkriminelle nimmt weiter zu, auch getrieben durch weltpolitische Krisenherde. Gleichzeitig ist die Bedeutung der Durchsetzung von starken Passwörtern in einer sich zunehmend dezentral organisierten Unternehmenswelt, in der sich IT und OT mehr und mehr vernetzen, wichtiger denn je und sollte nicht dem Zufall überlassen werden.

Nötig ist es daher, die Schwachstelle Passwort in einen effektiven Schutz und aktiven Posten in der Gefahrenabwehr umzugestalten. Hilfreich, wenn nicht unentbehrlich, ist dabei der Einsatz von Third-Party-Passwort-Filtern als technische Maßnahme.

Stephan Halbmeier,
Product Specialist,
Specops Software GmbH, Berlin

- stephan.halbmeier@specopssoft.com
- http://www.specopssoft.de/

Zur Person

Stephan Halbmeier verfügt über mehr als 25 Jahre Erfahrungen im Design und im Betrieb globaler IT-Umgebungen, u.a. war er als Service Owner Global Active Directory & PKI Services und im Bereich IT Security & Compliance tätig. Bei Specops Software ist er als Product Specialist für die reibungslose Einführung der Produkte und technische Betreuung der Kunden verantwortlich.

Achtung: Unbedingt Datenschutzverordnung beachten

Um weiteren Schaden von Ihrem Unternehmen abzuwehren, müssen die regulatorischen Vorgaben, wie sie durch die Datenschutz-Grundverordnung (DSGVO) festgesetzt sind, eingehalten werden. Außerdem sollten die Empfehlungen des NIST (National Institute of Standards and Technology) und des BSI IT-Grundschutzes berücksichtigt werden Kommt es zu einer Datenschutzverletzung und stellt sich dabei heraus, dass die gesetzlichen Mindeststandards gemäß DSGVO nicht befolgt worden sind, droht ein empfindliches Bußgeld von bis zu 20 Mio. EUR oder bis zu 4% des weltweit erwirtschafteten Jahresumsatzes im vorangegangenen Jahr.

Brenntag entscheidet sich für Amazon Web Services

Integration von digitalen Prozessen und Services

Brenntag hat ein mehrjähriges Projekt mit Amazon Web Services (AWS) angekündigt. AWS soll den Weltmarktführer in der Distribution von Chemikalien und Inhaltsstoffen in die Lage versetzen, die Integration von digitalen Prozessen und Services zu beschleunigen und den Wert von Daten weiter zu erschließen. In einer schnelllebigen und komplexen Welt wünschen sich Kunden und Lieferpartner einfache, aber personalisierte Interaktionen, um effizient arbeiten und bei Bedarf schnell reagieren zu können. Das globale Supply-Chain-Netzwerk von Brenntag liefert proprietäre Daten und Erkenntnisse, die es dem Unternehmen ermöglichen, seinen Kunden und Lieferpartnern einen höheren Mehrwert zu bieten.

Mit AWS sei Brenntag in der Lage, Plattformen und Datenverarbeitung über eine Vielzahl von Systemen hinweg bereitzustellen und gleichzeitig die internen Kapazitäten auszubauen, um eine flexible modulare Bereitstellung von Systemen, Automatisierungslösungen und Services zu ermöglichen.

„Die nahtlose, schnelle und sichere Verknüpfung von Daten und Data-as-a-Service für unsere Kunden und Lieferpartner auf der ganzen Welt und über eine Vielzahl von Plattformen und Systemen hinweg ermöglicht es uns, unsere Partner effizienter zu bedienen", sagte Ewout van Jarwaarde, Chief Transformation Officer bei Brenntag.

AWS leistet Support und bietet Schulungen an, die für eine konsistente Skalierbarkeit und eine umfassende Integration miteinander verbundener Plattformen auf globaler Ebene sorgen. Dadurch werden interne und externe Datenverbindungen schneller, reibungsloser und sicherer. Die Schulungen werden an mehreren Brenntag-Standorten durchgeführt und unterstützen die digitale Transformation durch die Bereitstellung einer Cloud-Infrastruktur, die ein Hub-and-Spoke-System der Datenkonnektivität ermöglicht.

In den kommenden Jahren wird Brenntag die AWS-Infrastruktur und den Support nutzen, um eine Reihe von Best-Practice-Lösungen zu implementieren, wie z.B. ein multimodales Track-and-Trace-Programm für Kunden- und Lieferpartnerbestellungen. (mr) ■