Netzwerke hacken – oft einfacher als gedacht

Das Fehlen von Patch-Management und das Ignorieren oder Falschinterpretieren von Antiviren-Meldungen sind nur zwei von sieben eigentlich leicht vermeidbaren Fehlern in der IT-Security, die Hacker häufig für das Einbrechen in Netzwerke und das unbemerkte Weiterbewegen darin (aus)nutzen.

DER AUTOR

Stephan Berger
Head of Investigations, Infoguard

Hundertprozentiger Schutz vor Cyberattacken ist heutzutage unmöglich. Umso wichtiger ist es, auf technischer Ebene ein effektives Sicherheitsdispositiv zu errichten – und insbesondere unnötige Fehler zu vermeiden.

1. Fehlendes Patch-Management
Im Mai 2022 kommunizierte das Nationale Zentrum für Cybersicherheit der Schweiz (NCSC), dass mehr als 200 Organisationen erneut über verwundbare Exchange-Server in ihrem Netzwerk informiert wurden. Ein Jahr zuvor war diese Schwachstelle jedoch bereits veröffentlicht worden, kurz darauf ein Exploit Code. Dies zeigt, dass notwendige Security-Updates häufig nicht umgehend eingespielt werden, was heutzutage schlichtweg ein Muss ist.

2. Fehlende Multi-Faktor-Authentisierung
Fehlende Multi-Faktor-Authentisierung ist eine der Haupteinfallstore in Netzwerke. Trotz Sensibilisierungskampagnen und Phishing-Trainings fallen viele Mitarbeitende auf Phishing-E-Mails herein, wodurch oftmals Passwörter auf einem gefälschten Login-Portal eingegeben werden. Fehlt ein zweiter Faktor, können sich Hacker problemlos als «legitime» User einloggen. Daher ist der Schutz durch Multi-Faktor-Authentisierung zwingend notwendig.

3. Ignorieren oder Falschinterpretieren von Antivirus-Meldungen
Der Sicherheitsforscher Florian Roth führt in seinem «Antivirus Event Analysis Cheat Sheet» eine Liste von Keywords auf, auf die bei Viren-Alarmen besonders geachtet werden muss.

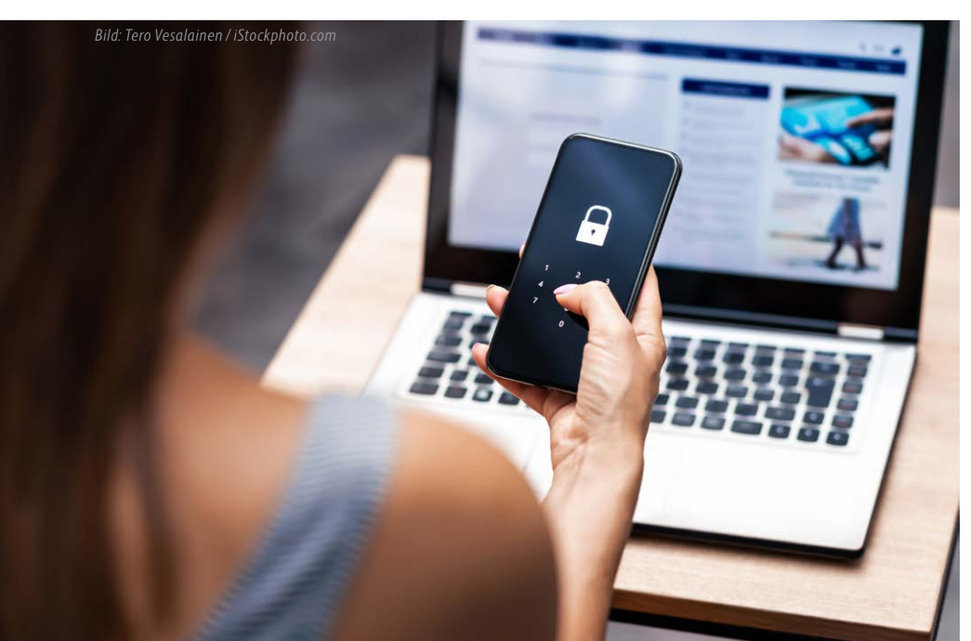

Bild: Tero Vesalainen / iStockphoto.com

Häufig erkennen Antiviren-Scanner zwar Anomalien, jedoch werden Alarme ignoriert oder falsch interpretiert. Solche Keyword-Listen helfen, die Kritikalität rascher und besser zu bewerten.

4. Fehlendes Active Directory Hardening
Das Active Directory ist das Herzstück eines Windows-Netzwerks, und die Kompromittierung des Domänen-Administrator-Kontos das Endziel vieler Angreifer. Einfach zu behebende Fehlkonfigurationen wie zum Beispiel veraltete Passwörter für hochprivilegierte Konten könnten dies verhindern.

5. Keine vertiefte Incident-Analyse
Nach einem Incident werden vielfach keine vertieften Analysen durchgeführt. Ein Benutzer erkennt beispielsweise ein Phishing-E-Mail nicht und gibt seine Credentials auf einer gefälschten Login-Seite ein. Hier reicht das Zurücksetzen des Passworts nicht. Auch sollte kontrolliert werden, ob bereits erfolgreiche Logins von einer unbekannten IP-Adresse stattgefunden haben, ob sich die Angreifer in die Mailbox eingeloggt und neue Inbox Rules erstellt haben usw. Wichtig ist ebenfalls, zuerst alle aktiven Sessions zu schliessen, bevor das Passwort zurückgesetzt wird.

6. Direkter Internetzugang
In vielen Fällen wird ersichtlich, dass Server direkt ins Internet kommunizieren können, ohne über einen Proxy geführt zu werden. Diesen Umstand nutzen Angreifer aus, um einfach Daten aus dem Netzwerk zu exfiltrieren oder den Command-&-Control-Server (C2) anzusprechen. Sobald der Verkehr über einen Proxy geleitet wird, können verschiedene Blockierungsregeln eingerichtet werden, die einen Angriff erschweren.

7. Kein EDR Agent
Um Angreifer an der Netzwerk-Kompromittierung zu hindern, reicht ein einfacher Antiviren-Scanner nicht. Ein Endpoint Detection & Response Agent (EDR) ist heutzutage ein Muss. Einerseits verschaffen solche Agents tiefe Einblicke in die Prozesse und Netzwerk-Verbindungen der Hosts, andererseits kann dadurch bösartiges Verhalten entdeckt werden.

IT Security ist zwar komplex, aber häufig geschehen Fehler aus Fahrlässigkeit. Umso wichtiger ist es, grundlegende Regeln und Praktiken konsequent zu befolgen.

« In der Hektik passieren schnell Fehler, was die Aufarbeitung erschweren kann »

Vermeidbare Nachlässigkeiten begünstigen in vielen Fällen Angriffe auf Unternehmensnetzwerke. Aber selbst wenn Fehler vermieden werden, geschehen Cyberattacken. Dann ist schnelles und richtiges Handeln kompetenter Experten gefragt, wie Stephan Berger von Infoguard weiss. Interview: Marc Landis

Wie kommt es zu den sieben im Beitrag beschriebenen Nachlässigkeiten? Wer ist dafür verantwortlich, dass sie ausgemerzt werden?
Stephan Berger: Heutige Computernetzwerke sind komplexe Architekturen, die einen hohen Anspruch an die betreuenden Personen stellen. Komplexität ist sicher ein Hauptgrund, wieso es zu den beschriebenen «Fehlern» kommen kann. Ein guter IT-(Security-)Partner kann bei der Priorisierung der wichtigsten Punkte helfen und bei der Umsetzung von wichtigen Security-Mechanismen unterstützen.

Wie findet man «schlafende» Cyberangreifer, die erst zu einem späteren Zeitpunkt zuschlagen und wie macht man diese unschädlich?
Das gelingt durch ein sogenanntes Compromise Assessment. In einem Compromise Assessment werden auf jedem Server und Computer ein Forensik-Agent installiert, mit dem gezielt nach (aktiven) Angreifern sowie Backdoors im Netzwerk gesucht werden kann. Dieses Vorgehen ist sehr zielführend und kann einem Unternehmen helfen, Backdoors und infizierte Computer zu entdecken, bevor sich die Angreifer über diesen Zugriff in das Netzwerk einloggen, um Daten zu entwenden und schlimmstenfalls das Netzwerk zu verschlüsseln.

Wie sollen Unternehmen auf einen gerade stattfindenden Cyberangriff konkret reagieren?
So rasch wie möglich sollte eine spezialisierte IT-Forensik-Firma um Unterstützung bei der Bewältigung des Cyberangriffs angefragt werden. In der Hektik eines Vorfalls passieren schnell Fehler, was die Aufarbeitung erschweren kann – das Löschen von Log-Files, das Neuaufsetzen von Systemen etc. Diese und weitere Schritte müssen koordiniert mit Experten abgesprochen werden.

Welche Lehren sollen Unternehmen aus einem überstandenen Cyberangriff ziehen und wie sollen diese «Lessons Learned» dokumentiert werden, damit sich vergleichbare Attacken nicht wiederholen können?
Die Lehren unterscheiden sich natürlich je nach Art des Angriffs. So ist ein DDoS-Angriff nicht vergleichbar mit einem Ransomware-Angriff. Grundsätzlich sollten die «Lessons Learned» aber darauf ausgerichtet sein, das System sicherer zu machen, damit der Angriff nicht wieder oder nur erschwert durchgeführt werden kann. Als Beispiel bei einem Ransomware-Angriff: Auf welchem Weg sind die Angreifer in das Netzwerk eingedrungen? Wie konnten sie ihre Privilegien erhöhen? Und wie könnte das Unternehmen die Angreifer das nächste Mal schneller im Netzwerk entdecken? Diese und weitere Fragen müssen im Anschluss an einen Vorfall geklärt werden. Dazu gibt es in vielen Unternehmen eine dedizierte Stelle (meist Security Officer oder CISO), bei der die Dokumentation und das Tracking von solchen Massnahmen zum Aufgabengebiet gehört.

« Heutige Computernetzwerke sind komplexe Architekturen, die einen hohen Anspruch an die betreuenden Personen stellen. »

Stephan Berger, Head of Investigations, Infoguard

Abgesehen von den technischen Massnahmen gibt es auch kulturelle und organisationale Massnahmen, um Cyberangriffe abzuwehren. Welche Massnahmen erachten Sie als besonders wichtig und zielführend?
Die Mitarbeitenden sollten in regelmässigen Awareness-Schulungen auf die Gefahren und Risiken von Cyberangriffen aufmerksam gemacht werden. Eine gute Portion Misstrauen, gerade im Umgang mit E-Mails, ist sicher nicht verkehrt. Insbesondere beim Öffnen von Dokumenten oder dem Anklicken von Links ist Vorsicht geboten – auch, wenn der Absender bekannt ist. Denn Kriminelle könnten dieses E-Mail-Konto gehackt haben, um darüber bösartige Inhalte zu verschicken.

Das Dossier finden Sie auch online
www.netzwoche.ch