Sicherheitslücken

Wenn die Technik zum Einfallstor wird

Im Fokus

Die IT-Landschaften von Unternehmen werden mit jeder neuen App komplexer. Wenn nur eine Konfigurationseinstellung fehlerhaft ist oder schlicht vergessen geht, dann bieten selbst ausgeklügelte Sicherheitsmechanismen irgendwann keinen adäquaten Schutz mehr. Wer sich einige grundlegende Abwehrszenarien und Praktiken aneignet, kann die Komplexität von IT und Security zumindest auf ein beherrschbares Mass reduzieren.

- **Wegleitung:** Das Patchen von Sicherheitslücken sollte eine Routinetätigkeit für jeden IT-Administrator sein. Genau wie die Incident-Analyse bei einem Datenabfluss. Diese und andere technische Sicherheitsrisiken beleuchtet Stephan Berger von InfoGuard.
- **Interview:** Der Head of Investigations von InfoGuard wird zu Schweizer Kunden gerufen, wenn es einen Sicherheitsvorfall gegeben hat. Aus dieser Praxis kennt Stephan Berger die häufigsten Fehler. Und er weiss auch, wie sie sich vermeiden lassen.

Incident Response

Hacker haben häufig leichtes Spiel

Hacker nutzen Fehler in der IT-Security gnadenlos aus, um in Netzwerke einzubrechen und sich dort fortzubewegen. Häufig wären diese jedoch einfach vermeidbar.

→ **VON STEPHAN BERGER**

Hundertprozentiger Schutz vor Cyberattacken ist in der heutigen Bedrohungslandschaft unmöglich. Umso wichtiger ist ein möglichst effektives Sicherheitsdispositiv. Insbesondere auf technischer Ebene werden jedoch häufig eigentlich vermeidbare Fehler gemacht – vor allem die sieben folgenden.

1 **Fehlendes Patch-Management:** Am 16. Mai 2022 kommunizierte das Nationale Zentrum für Cybersicherheit der Schweiz, dass mehr als 200 Unternehmen und Gemeinden erneut über verwundbare Exchange-Server in ihrem Netzwerk informiert wurden. Computer Security Incident Response Teams (CSIRT), welche Sicherheitsvorfälle analysieren und bei akuten Vorfällen die Abwehr- sowie Beseitigungsmassnahmen übernehmen, sehen jedoch noch immer verwundbare Exchange-Server. Dies ist insofern erstaunlich, weil eine dieser Schwachstellen im Juni 2021 veröffentlicht und im August 2021 der Exploit-Code dafür ins populäre Framework Metasploit aufgenommen wurde. Dennoch haben es viele Administratorinnen und Administratoren verpasst, die notwendigen Security-Updates einzuspielen. Gleiche Szenarien spielten sich bei Confluence und VMware Horizon ab. In der heutigen Angriffslandschaft sind Administratoren dazu angehalten, regelmässig Security-News zu konsumieren, um frühzeitig über kritische Lücken und Patches informiert zu sein und rechtzeitig Massnahmen ergreifen zu können.

2 **Fehlende Multi-Faktor-Authentisierung**: Fehlende Multi-Faktor-Authentisierung – sprich, eine zum Passwort zusätzliche Verifikation per SMS, Token oder Authenticator-App – ist nebst dem Ausnützen von kritischen Schwachstellen eine der Haupteinfallstore in Netzwerke. Trotz Sensibilisierungskampagnen und Phishing-Trainings fallen viele Mitarbeitende auf die teils sehr professionellen Phishing-E-Mails herein, wodurch sie beispielsweise Passwörter auf einem gefälschten Login-Portal eingeben. Fehlt der zweite Faktor, können sich Hacker problemlos als «legitime» User einloggen. Daher ist es wichtig, dass alle von extern erreichbaren Zugänge in das Firmennetzwerk oder zu Firmeninformationen mit einem zweiten Faktor geschützt werden, sei es der Zugang zum E-Mail-Konto oder der VPN-Zugang.

3 **Ignorieren oder Falschinterpretieren von Antivirus-Meldungen:** Zur Erläuterung des dritten Fehlers ist das vom Sicherheitsforscher Florian Roth erstellte «Antivirus Event Analysis Cheat Sheet» hilfreich. Insbesondere die rote Spalte ist für IT-Administratoren und SOC-Analysten wertvoll. Hier sind die wichtigsten Keywords aufgeführt, auf die bei Virenalarmen besonders geachtet werden muss. Häufig wird bei der Analyse von Incident-Response-Fällen deutlich, dass der lokale Antivirus-Dienst einen oder mehrere Schritte (und natürlich auch Skripts und Programme) der Angreifer erkannt hat. Leider wird Antivirusalarmen oft zu wenig Beachtung geschenkt oder die Alarme können zu wenig detailliert analysiert werden. Genau deshalb ist das Cheat Sheet hilfreich, da es Anhaltspunkte liefert, bei welchen Keywords eine Untersuchung eingeleitet oder externe Expertinnen und Experten mit der Vorfallsanalyse beauftragt werden sollten.

4 **Fehlendes Active Directory Hardening:** Das Active Directory ist das Herzstück eines Windows-Netzwerks, und die Kompromittierung des Domänen-Administratorenkontos das Endziel vieler Angreifer. Es kursieren detaillierte Dokumentationen über Angriffspfade, über die man sich höchste Rechte in einem Netzwerk verschaffen →

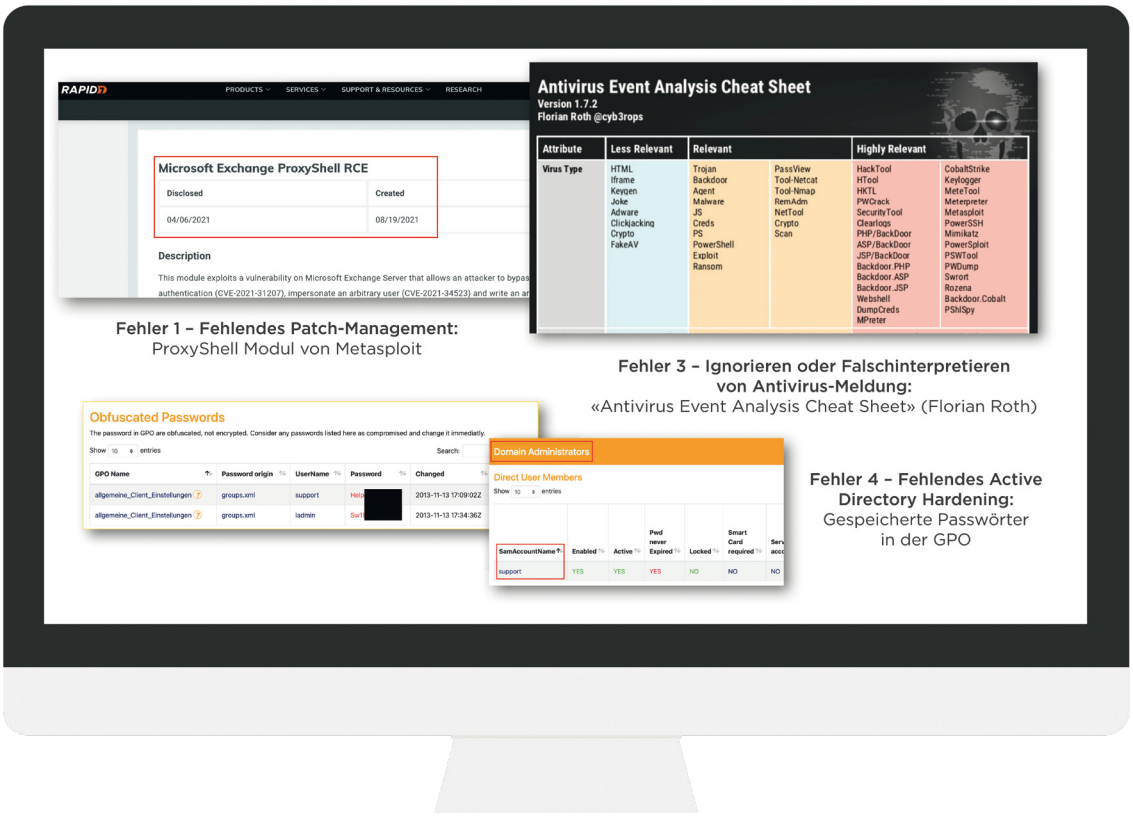
DER AUTOR

Stephan Berger
ist Head of Investigations bei InfoGuard.
→ **www.infoguard.ch**

«Auf technischer Ebene werden häufig vermeidbare Fehler gemacht»

Stephan Berger

Bild: Shutterstock/Bits And Splits



Fehler 1 – Fehlendes Patch-Management: ProxyShell Modul von Metasploit

Fehler 3 – Ignorieren oder Falschinterpretieren von Antivirus-Meldung: «Antivirus Event Analysis Cheat Sheet» (Florian Roth)

Fehler 4 – Fehlendes Active Directory Hardening: Gespeicherte Passwörter in der GPO

Häufig ist es schon zu spät, wenn Administratorinnen oder Administratoren einen dieser drei Fehler entdecken

kann. Voraussetzungen für diese Angriffe sind aber vielfach Fehlkonfigurationen, die relativ einfach behoben werden könnten. Einige Klassiker, die bei Active Directory Assessments regelmässig vorgefunden werden:

- In der Group Policy Object sind Passwörter abgespeichert, teils für hochprivilegierte Accounts.
- Serviceaccounts sind Teil von hochprivilegierten Gruppen (Gefahr der «Kerberoasting-Attacke»).
- Bei hochprivilegierten Accounts wurden die Passwörter seit Jahren nicht mehr geändert.
- Kein Tiering Model: Hochprivilegierte Accounts loggen sich auf normalen Clients wie Arbeitslaptops ein.
- Active Directory Assessments decken solche Fehlkonfigurationen auf – dadurch wird ein erfolgreicher Angriff erheblich erschwert.

5 Keine vertiefte Incident-Analyse: Nach der Infektion eines Clients oder Servers oder nach dem Abfluss von Passwörtern, beispielsweise durch Phishing, werden vielfach keine vertieften Analysen durchgeführt. Ein Beispiel: Ein Benutzer erkennt eine Phishing-E-Mail nicht und gibt seine Credentials auf einer gefälschten Login-Seite ein. Und nun? Das Zurücksetzen des Passworts reicht nicht. Es sollte unter anderem 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. Aber auch die VPN-Zugriffe sollten überprüft werden. Wichtig ist ebenfalls, alle aktiven Sessions zu schliessen, bevor das Passwort zurückgesetzt wird. Das gleiche Vorgehen sollte auch bei einem infizierten Gerät oder Server geschehen: Über welchen Zeitraum war der Host infiziert, bevor der Vorfall bemerkt wurde? Wurden allenfalls noch weitere Credentials gestohlen (die aus dem Memory ausgelesen werden konnten)? Haben sich die Angreifer über den infizierten Host womöglich schon weiter im Netzwerk ausgebreitet?

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 im internen Netzwerk 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. Angreifer können dadurch nicht mehr so einfach Programme nachladen und Befehle auf den kompromittierten Maschinen absetzen.

7 Kein EDR-Agent: Um professionelle Angreifer an der Kompromittierung des Netzwerkes zu hindern, genügt ein einfacher Antivirenscanner nicht mehr. Ein Endpoint-Detection-and-Response-Agent (EDR) ist heutzutage ein Muss zum Schutz von grösseren Netzwerken. Einerseits verschaffen solche Agents tiefe Einblicke in die Prozesse und Netzwerkverbindungen der Hosts, andererseits kann dadurch bösartiges Verhalten entdeckt werden. IT- und Cyber-Security sind zwar komplex und immer schwieriger ohne externe Expertise zu bewältigen. Nichtsdestotrotz ist es wichtig, grundlegende Regeln und Praktiken zu befolgen, denn Fahrlässigkeit ist eine der grössten Gefahren. ←

Bild: InfoGuard/Florian Roth

«IT-Security wird vielfach zu wenig stark gewichtet»

Das Absichern von IT-Landschaften in Unternehmen ist eine grosse Herausforderung. Oftmals wird die IT-Security zu wenig stark gewichtet, beobachtet Stephan Berger von InfoGuard. Dann klafften Lücken in der Infrastruktur, sodass Angreifer ein leichtes Spiel hätten, doppelt er nach. Das müsse und dürfe nicht sein.

→ **INTERVIEW: MARK SCHRÖDER**

Administratorinnen und Administratoren haben mit dem Betrieb der IT-Infrastruktur in Schweizer Unternehmen schon vielfach alle Hände voll zu tun. Parallel steigt die Komplexität von IT-Gefahren nahezu täglich. Überall lauern Bedrohungen, und sei es nur wegen eines zu spät eingespielten Patches. Die IT-Security quasi nur im «Nebenjob» zu betreiben, sei dann keine gute Idee, sagt Stephan Berger von InfoGuard.

Computerworld: Sie skizzieren sieben vermeidbare Fehler in IT-Organisationen. Welcher kommt in der Praxis am häufigsten vor?
Stephan Berger: Das fehlende Patch-Management. Diesen Punkt sehen wir natürlich auch sehr häufig bei unseren Incident-Response-Fällen, wenn kritische Schwachstellen nicht oder erst zu spät gepatcht wurden. Ein Beispiel ist die neuste Fortinet-Lücke (CVE-2022-40684): Nach Veröffentlichung des Patches wurde nach nur drei Tagen öffentlicher Exploit-Code publiziert. Danach untersuchten wir bereits die ersten kompromittierten Firewalls bei einigen Kunden. Das Patchfenster ist sehr klein geworden. Unternehmen müssen ihr Patchmanagement entsprechend ausrichten.

CW: Aus welchem Grund passieren diese vermeidbaren Fehler typischerweise?
Berger: Nicht nur IT-Security, sondern die ganze IT-Landschaft ist in den letzten Jahren immer komplexer geworden. Von typischen IT-Administratoren wird heute erwartet, dass sie verschiedene Produkte und Technologien in einer gewissen Tiefe verstehen. Es ist klar, dass bei diesem Anspruch natürlich nicht alle Bereiche abgedeckt werden können. Gerade IT-Security wird dabei vielfach zu wenig stark gewichtet. Oftmals ist es auch eine Abwägung der Prioritäten, da operative Probleme behoben werden müssen und langfristige Investitionen in die Sicherheit im Tagesgeschäft fast keinen Platz haben.

CW: Wenn trotz aller Vorkehrungen einer der Fehler doch passiert ist: Was sind Ihre Empfehlungen?
Berger: Mit der «Defense in Depth», sprich der Verteidigung in der Tiefe, können Fehler im Sicherheitsdispositiv kompensiert werden. Dazu gehören unter anderem regelmässige Assessments, ausgearbeitete Tiering-Modelle, Least-Privilege für die Benutzer sowie das Überwachen des Firmennetzwerkes mit einem Endpoint Detection and Response Agent usw.

CW: Die Bedrohungslage wird immer unübersichtlicher. Wo starten Unternehmen bestenfalls, um sich gegen die grössten Gefahren zu wappnen?
Berger: Wir empfehlen Unternehmen vielfach, mit einem Compromise Assessment zu starten, das auch eine vertiefte Untersuchung des Active Directorys beinhaltet. Durch solch ein gezieltes Assessment können schon erste gröbere Fehler entdeckt werden. Danach ist es sicherlich auch sinnvoll, einen vertieften Penetrationstest durchführen zu lassen, der auch das Perimeter beinhaltet, um noch weitere Löcher im Sicherheitsdispositiv erkennen und dadurch schliessen zu können. Natürlich sollten Unternehmen auch IT-(Security-)News regelmässig lesen, um über die neusten Angriffstechniken und die entprechende Verwundbarkeit im Bilde zu sein.

CW: Viele Firmen können sich ein eigenes Sicherheitsteam schlicht nicht leisten. Oder sie bekommen die Talente nicht. Was raten Sie diesen Kunden?
Berger: IT-Security ist ein komplexes Thema, und jeden Tag werden neue Bedrohungen und Angriffe veröffentlicht. Bei dieser Informationsflut den Überblick zu behalten ist schwer, wenn man sich nicht in Vollzeit damit befasst. Deshalb raten wir unseren Kunden, die IT-Security – auch die Überwachung des Netzwerks – nicht inhouse durchzuführen, sondern entsprechende Dienstleistungen durch einen erfahrenen Managed Security Provider durchführen zu lassen. Denn die Gefahr, dass ein Alarm falsch interpretiert oder ein Netzwerk schlecht geschützt wird, ist gross. Diese Fehler sehen wir vielfach auch bei unseren Incident-Response-Fällen, bei denen nicht adäquat auf eine akute Bedrohung reagiert wurde. ←

ZUR PERSON

Stephan Berger
ist heute als Head of Investigations bei InfoGuard tätig. Er stiess 2020 als Senior Cyber Security Analyst zu dem Sicherheitsspezialisten aus Baar/Zug. Zuvor war er jeweils vier Jahre in ähnlicher Funktion beim Bundesamt für Informatik und Telekommunikation BIT und der Schweizerischen Post beschäftigt. Berger hält einen Master in Engineering mit Vertiefung Computer Science/IT-Security von der Berner Fachhochschule.