HPE GreenLake
Nutzen Sie Ihren Wettbewerbsvorteil im richtigen Umfang. Das ist **Ihr KI-Vorteil**
Mehr erfahren



Harness the power of your data.
Join Cloudland and turn your data & AI challenges into opportunities.
cloudland
Join the event →

ZDNet : Sicherheit : Cyberkriminalität

# Zehn Hackergruppen starten Cyberangriffe auf Microsoft Exchange Server

**Die schwersten Sicherheitslücken im Microsoft Exchange Server locken zahlreiche Hackergruppen an. Allein in Deutschland wurden 11.000 Server kompromittiert.**

von **Dr. Johnb Jung** am **15. März 2021**, 09:26 Uhr

Der Angriff auf Microsoft Exchange ist einer der schwersten Cyberattacken der jüngsten Vergangenheit. Zwar hat Microsoft rasch reagiert und Patches bereitgestellt, aber die Schwachstellen locken Nachahmer an und noch immer sind auf zehntausenden von Servern keine Patches installiert.

Anzeigen
Read Discover
Wer stiehlt Ihre persönlichen Daten?
Mit dem Premium VPN von Surfshark sind Ihre Daten und Geräte vor Viren und Hacken geschützt. Surfen Sie sicher im Internet.

„Seit dem Tag der Veröffentlichung der Patches durch Microsoft beobachten wir, dass immer mehr Hacker massenhaft Exchange-Server scannen und kompromittieren. Interessanterweise heads in sich dabei durchweg um Advanced Persistent Threats (APT-Gruppen, die für Spionagetätigkeiten berüchtigt sind. Wir sind uns sicher, dass auch andere Gruppen, beispielsweise Ransomware-Betreiber, diese Exploits für ihre Zwecke ausnutzen und auf den Zug aufspringen werden", sagt Matthieu Faou, der die Forschungsarbeiten von ESET zu diesem Thema leitet.

Die ESET-Forscher stellen ebenfalls fest, dass einige APT-Gruppen die Schwachstellen bereits ausnutzten, bevor die Patches zur Verfügung gestellt wurden. „Wir können daher ausschließen, dass diese Gruppen einen Exploit durch Reverse Engineering von Microsoft-Updates erstellt haben", fügt Faou hinzu.

Zu ähnlichen Erkenntnissen kommt Palo Alto Networks. Die Analyst der nicht gepatchten Exchange-Server ging diese Woche stark zurück, als Microsoft-Kunden last neuen Daten, die von der Palo Alto Networks Expanse-Plattform gesammelt wurden, schnell Schwachstellupdates installierten. Das schnelle Patchen folgt Warnungen, dass Hacker vier Zero-Day-Schwachstellen in der weit verbreiteten E-Mail-Software ausnutzten.

Die Anzahl der anfälligen Server, die denen alte Versionen von Exchange ausgeführt werden, auf denen die kürzlich veröffentlichten Sicherheitspatches nicht direkt angewendet werden können, ist laut Expanse-Internet-Scans vom 8. und 11. März um über 30% von geschätzten 125.000 auf 80.000 gesunken.

„Ich habe noch nie gesehen, dass die Sicherheitspatch-Raten für ein System so hoch sind, gewonnen dem für ein System, das so weit verbreitet ist wie Microsoft Exchange", sagte Matt Knaring, Chief Technology Officer von Cortex bei Palo Alto Networks. „Wir fordern Unternehmen, die alte Versionen von Exchange ausführen, dringend auf, davon auszugehen, dass sie kompromittiert wurden, bevor sie ihre Systeme gepatcht haben, da wir wissen, dass Angreifer diese Zero-Day-Schwachstellücken mindestens zwei Monate lang in freier Wildbahn ausnutzten, bevor Microsoft die Patches am 2. März veröffentlichte. "

Palo Alto Networks verwendete die Expanse-Plattform, um im Internet exponierte Server zu identifizieren, auf denen alte Versionen von Exchange ausgeführt werden, auf denen der kürzlich veröffentlichte Sicherheitspatch für die Zero-Day-Schwachstellücken nicht direkt angewendet werden kann.

Sowohl die Schwachstellen selbst als auch der Zugriff, der durch deren Ausnutzung ermöglicht werden kann, sind erheblich. Es ist daher nicht überraschend, dass mehrere Angreifer versuchten und weiterhin versuchen, anfälliger Systeme zu kompromittieren, bevor diese neue Netzwerkadministratoren gepatcht werden. Diese Angriffe geschahen in einem noch nie dagewesenen Ausmaß.

Anhand der rekonstruierten Zeitachse ist nun klar, dass zwischen der ersten bekannten Ausnutzung dieser Schwachstelle am 3. Januar und der Veröffentlichung des Patches durch Microsoft am 2. März mindestens 58 Tage lagen. Das Ausfüllen des Patches ist ein notwendiger erster Schritt, aber nicht ausreichend, wenn man bedenkt, wie lange die Schwachstelle in der freien Wildbahn war. Das Aufspielen des Patches beseitigt nicht den Zugang, den Angreifer möglicherweise bereits zu anfälligen Systemen erlangt haben. Unternehmen können sich im Leitfaden von Unit 42 für Abhilfemaßnahmen über die nötigen Schritte informieren, um sicherzustellen, dass sie ihre Exchange Server ordnungsgemäß abgesichert haben.

In der zweiten Woche nach Bekanntwerden der Schwachstellen gibt es erste Schätzungen, dass die Zahl der betroffenen Unternehmen in die Zehntausende geht. Dies stellt damit die Auswirkungen des jüngsten SolarStorm-Angriffs auf die Lieferkette in Bezug auf die Zahl der Opfer und die geschätzten Kosten für die Beseitigung der Schwachstellen weitweit in den Schatten. Angesichts der Bedeutung dieses Ereignisses veröffentlichte Unit 42 eine Zeitleiste des Angriffs, die auf den umfangreichen Recherchen zu den derzeit verfügbaren Informationen und der direkten Erfahrung bei der Abwehr solcher Angriffe basiert. Während sich die Situation weiterentwickelt, bittet Unit 42 auch andere Forschungsteams, ihre Erkenntnisse mitzuteilen, damit sich die Cybersicherheitscommunity so schnell wie möglich ein vollständiges Bild machte kann.

Laufende Untersuchungen zeigen, dass diese Schwachstellen von mehreren Bedrohungsgruppen ausgenutzt werden. Es ist nicht neu, dass hochqualifizierte Angreifer neue Schwachstellen in verschiedenen Produkt-Ökosystemen ausnutzen. Die Art und Weise, wie diese Angriffe durchgeführt werden, um die Authentifizierung zu umgehen und damit unbeschränkten Zugriff auf E-Mails zu erhalten und Remote Code Execution (RCE) zu ermöglichen, ist jedoch besonders perfide.

Unit 42 geht davon aus, dass die Angriffe, die diese Schwachstellen ausnutzen, sich nicht nur fortsetzen, sondern auch an Umfang zunehmen werden. Dies wird sich wahrscheinlich auch in vielfältigeren Angriffen mit unterschiedlichen Motiven äußern, wie etwa die Infektion und/oder Verteilung von Ransomware. Aufgrund der Tatsache, dass aktive Angriffe verschiedener Bedrohungsgruppen, die diese Schwachstellen ausnutzen, andauern, ist es zwingend erforderlich, die betroffenen Systeme nicht nur zu patchen, sondern auch die Anleitungen zu befolgen, die Unit 42 in einem früheren Remediation Blog beschrieben hat.

Die Forscher des IT-Sicherheits-Herstellers ESET haben mehr als zehn verschiedene APT-Gruppen (Advanced Persistent Threats), welche die Schwachstellen derzeit weitstärkt ausnutzen, um E-Mail-Server zu kompromittieren und an Unternehmensdaten zu gelangen. Die Bedrohung ist also nicht auf die chinesische Hafnium-Gruppe beschränkt, wie bislang vermutet wurde. ESET identifizierte weitweit rund 5.000 E-Mail-Server von Unternehmen und Regierungseinrichtungen, die kompromittiert wurden. Die meisten Ziele der Hackergruppen liegen in Deutschland. Die Telemetrie der Security-Software zeigte das Vorhandensein von sogenannten Webshells. Diese bösartigen Programme oder Skripte ermöglichen die Fernsteuerung eines Servers über einen Webbrowser. Die Installation der von Microsoft bereitgestellten Sicherheits-Updates ist davon ungeachtet zwingend erforderlich.

Der Einsatz sogenannter Endpoint Detection und Response Lösungen (EDR-Lösungen) hilfte in vielen Fällen den Diebstahl von Unternehmensdaten eingrenzen bzw. verhindern können. „Mit Hilfe von EDR-Lösungen, wie beispielsweise ESET Enterprise Inspector, seien Administratoren frühzeitig auf verdächtige Aktivitäten aufmerksam gemacht worden. So hätte der Abfluss von Unternehmensdaten trotz Ausnutzung des Sicherheitslücke frühzeitig registriert werden können, um diesen durch entsprechende Maßnahmen zu unterbinden", erklärt Michael Schröder, Security Business Strategy Manager bei ESET Deutschland.

Um den Sicherheitsstatus beurteilen zu können, sollten Exchange-Server auf die folgenden Erkennungen überprüft werden:

JS/Exploit.CVE-2021-26855.Webshell.A

JS/Exploit.CVE-2021-26855.Webshell.B

ASP/Webshell

ASP/ReGeorg

Administratoren wird geraten, nach Webshells und weiteren bösartigen Aktivitäten zu suchen und diese umgehend zu entfernen. Anmeldedaten sollten umgehend geändert werden.

„Der Vorfall ist eine sehr gute Erinnerung daran, dass komplexe Anwendungen wie Microsoft Exchange oder SharePoint nicht zum Internet hin offen sein sollten", rät Matthieu Faou.

APT-Gruppen und ihre Verhaltensmuster

Tick – kompromittierte den Webserver eines Unternehmens mit Sitz in Ostasien, das IT-Dienstleistungen anbietet. Wie im Fall von LuckyMouse und Calypso hatte die Gruppe wahrscheinlich schon vor Veröffentlichung der Patches Zugang zu einem Exploit.

LuckyMouse – infizierte den E-Mail-Server einer Regierungsbehörde im Nahen Osten. Diese APT-Gruppe verfügte wahrscheinlich bereits einen Tag vor Veröffentlichung der Patches über einen Exploit, als dieser noch ein Zero-Day war.

Calypso – griff die E-Mail-Server von Regierungsstellen im Nahen Osten und in Südamerika an. Die Gruppe hatte wahrscheinlich Zugang zu dem Exploit als Zero-Day. In den folgenden Tagen griffen die Calypso-Betreiber weitere Server von Regierungsstellen und Unternehmen in Afrika, Asien und Europa an.

Websiix – zielte auf sieben E-Mail-Server ab, die Unternehmen (in den Bereichen IT, Telekommunikation und Technik) in Asien und einer staatlichen Einrichtung in Osteuropa gehören.

Winnti Group – kompromittierte die E-Mail-Server eines Ölunternehmens und einer Firma für Baumaschinen in Asien. Die Gruppe hatte wahrscheinlich schon vor Veröffentlichung der Patches Zugang zu einem Exploit.

Tonto Team – attackierte die E-Mail-Server eines Beschaffungsunternehmens und eines auf Softwareentwicklung und Cybersicherheit spezialisierten Beratungsunternehmens, beide mit Sitz in Osteuropa.

ShadowPad activity – infizierte die E-Mail-Server eines Softwareentwicklungsunternehmens mit Sitz in Asien und eines Immobilienunternehmens mit Sitz im Nahen Osten. ESET entdeckte eine Variante der ShadowPad-Backdoor, die von einer unbekannten Gruppe eingeschleust wurde.

Operation* Cobalt Strike – zielte auf rund 650 Server, hauptsächlich in den USA, Deutschland, Großbritannien und anderen europäischen Ländern, nur wenige Stunden nach Veröffentlichung der Patches.

IIS-Backdoors – ESET beobachtete IIS-Backdoors, die über die bei diesen Kompromittierungen verwendeten Webshells auf vier E-Mail-Servern in Asien und Südamerika installiert wurden. Eine der Backdoors ist öffentlich als Owlproxy bekannt.

Mikrocosm – kompromittierte den Exchange-Server eines Versorgungsunternehmens in Zentralasien, einer Region, die typischerweise Ziel dieser Gruppe ist.

DLTMiner – ESET entdeckte den Einsatz von PowerShell-Downloadern auf mehreren E-Mail-Servern, die zuvor über die Exchange-Schwachstellen angegriffen wurden. Die Netzwerkinfrastruktur, die bei diesen Angriff verwendet wurde, steht im Verbindung mit einer zuvor gemeldeten Coin-Mining-Kampagne.

WEBINAR
**Beim Endpoint-Schutz zählt jede Sekunde: Warum die Entscheidung in Echtzeit entscheidend ist**
Carsten Maciejewski, Systems Engineer bei Fortinet, erläutert in diesem Webinar, wie eine moderne IT-Sicherheitsarchitektur in Unternehmen aussehen sollte. Er illustriert dies am Beispiel eines Fußballstadions wie Bengaldo, Pitzer, Dortner und Zuschauer kennen.
Jetzt registrieren und Webinar Aufzeichnung ansehen
ZDNet Webinar
Jetzt registrieren
Jetzt registrieren und Webinar Aufzeichnung ansehen
Jetzt registrieren und Webinar Aufzeichnung ansehen
Jetzt registrieren und Webinar Aufzeichnung ansehen