Angriff auf Exchange-Server ProxyLogon Schwachstellen

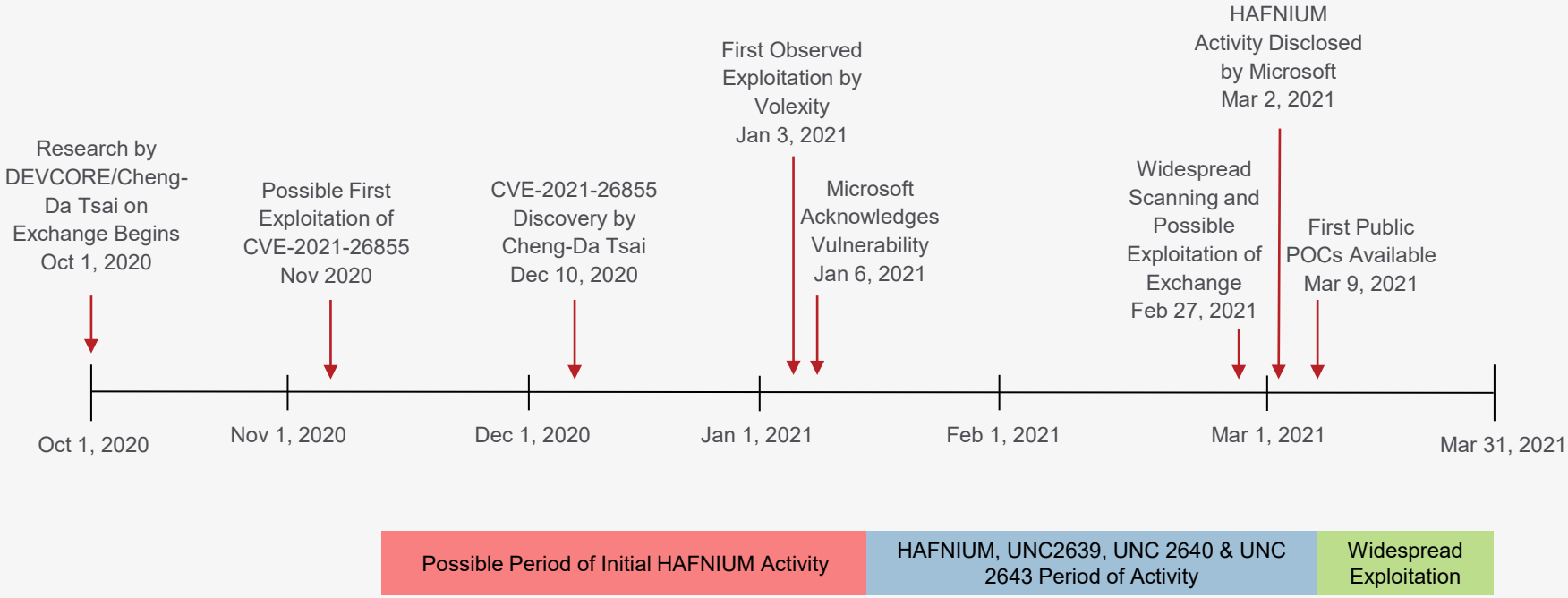
20. Mai 2021

Michael Kristen, Senior Cyber UW, CISSP | CISM | ISO 27001 LA & LI

Munich RE

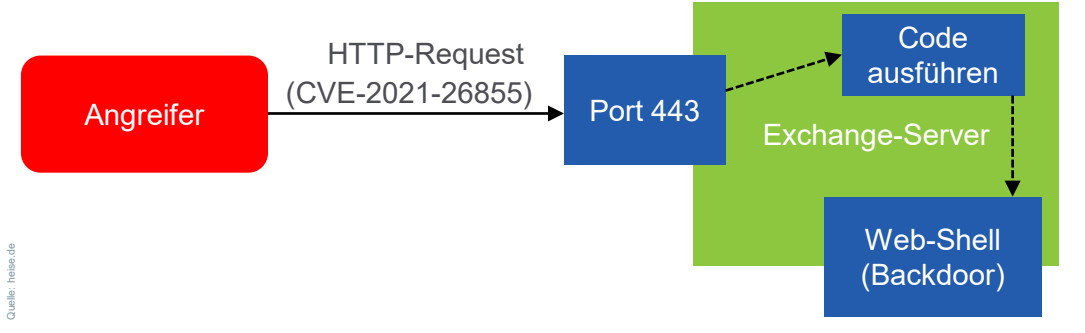
Image: Alexander Spatari / Getty Images

Was ist passiert?



→ Gefährdet sind Exchange-Server der Versionen 2010 bis einschließlich 2019, die über das Internet zugänglich sind.

Wie funktioniert der Angriff?



- Betroffen sein können alle Arten von Unternehmen weltweit, die anfällige lokale Microsoft Exchange-Server verwenden.
- Unternehmen, die ausschließlich O365 oder andere Mailserver verwenden, sollten nicht betroffen sein.
- Nach Meldung der ersten Lücke benötigte Microsoft zwei Monate, um Sicherheitsupdates bereitzustellen.
- Nach Schätzungen des BSI waren Anfang März in Deutschland mindestens 26.000 verwundbare Exchange-Server (Exchange-Server 2010, 2013, 2016 & 2019) direkt aus dem Internet erreichbar und somit angreifbar. Der Großteil galt bereits als kompromittiert.
- Am 16. März warnte das BSI immer noch vor fast 12.000 verwundbaren Servern.
- Stand heute sind immer noch eine große Anzahl von Servern nicht gepatcht und können als definitiv kompromittiert angesehen werden.

Sind Unternehmen, die ihre Systeme gepatcht haben, sicher?

Munich RE

- Nein! Unternehmen können vor dem Patchen gehackt worden sein und Hacker haben möglicherweise Hintertüren implementiert. Daher müssen Unternehmen weitergehende Maßnahmen ergreifen um sicherzustellen, dass keine Infektion stattgefunden hat oder sich Angreifer im eigenen Netzwerk befinden.

- Darüber hinaus ist eine beträchtliche Anzahl von Exchange-Servern weltweit noch nicht gepatcht. Da die Sicherheitslücken, Methoden und Werkzeuge zur Ausnutzung jetzt öffentlich sind, versuchen Cyber-Kriminelle mit unterschiedlichen Motiven, die Situation auszunutzen.

Was bedeutet dies für die Cyber-Versicherung?

Munich RE

- Aus heutiger Sicht ist es immer noch schwierig, die Konsequenzen vorherzusagen. Mit Zugang zum Netzwerk haben Angreifer weitreichende Möglichkeiten, Schäden zu verursachen.

- Wie bei früheren Ereignissen, kann es Monate oder sogar länger dauern, bis Schäden aus diesem Ereignis eintreten (z.B. Ransomware-Angriff im Krankenhaus Düsseldorf, September 2020, basierend auf einer Citrix-Schwachstelle von 2019).

- Nach aktuellem Kenntnisstand ist ein Kumulereignis eher unwahrscheinlich, da die Schwachstellen es den Angreifern nicht ermöglichen, Schadsoftware automatisiert im Netzwerk zu verbreiten.

Erwägungen im Underwriting

Munich RE

- Patchen!
- Reifegrad des gesamten Informationssicherheitsmanagementsystems (ISMS).
- Erklärung des Versicherungsnehmers zum Umgang mit ProxyLogon kann helfen, die Wirksamkeit von einzelnen Kontrollen besser einzuschätzen (z.B. Protokollierung und Überwachung, Technisches Schwachstellenmanagement, usw.).
- Risiken ohne Auskunft zu ProxyLogon, die nicht oder verspätet gepatcht haben, oder „nur“ gepatcht haben, sind mit Vorsicht zu behandeln.

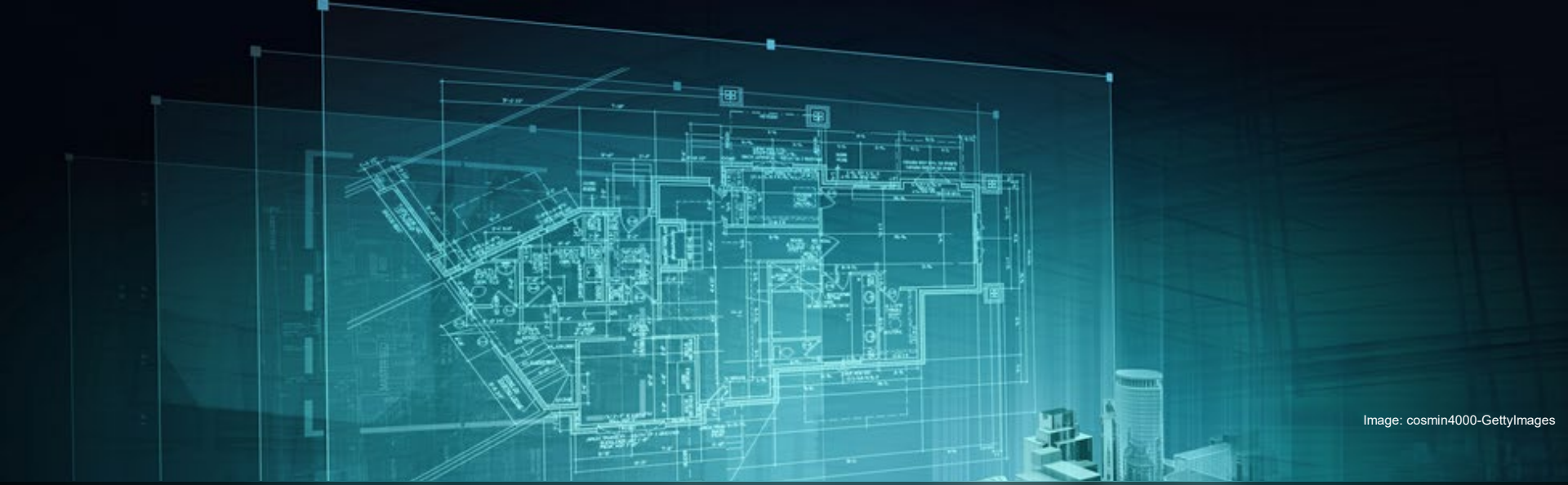


Image: cosmin4000-GettyImages

Gedanken zum Patch-Management

20. Mai 2021

Martin Kreuzer, Corporate Underwriting (CU 1.3.1)

Munich RE

Gedanken zum Patch-Management:
Herausforderungen und Fragen für den Versicherten

Munich RE

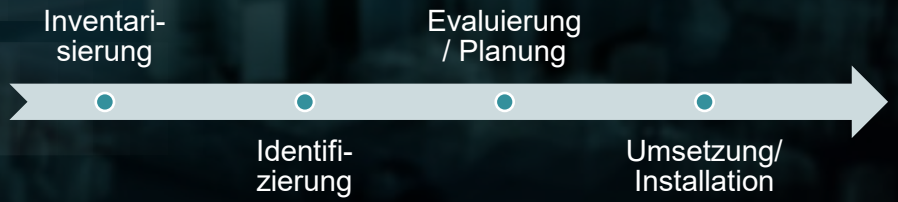
Es gibt keine Patches für unbekannte Schwachstellen (“Zero Day Exploits”)

Was ist kritisch? Gibt es allgemeingültige Standards oder Metriken, welche Schwachstellen und Prozesse / Patches definieren und kategorisieren?

Schwachstellen-Management ist sehr individuell. Neben Patches gibt es auch mitigierende Maßnahmen

Patch-Management ist ressourcenintensiv

Der Patchzyklus muss holistisch sein



Gedanken zum Patch-Management:
Herausforderungen und Fragen für die Assekuranz

Munich RE

- Adäquate Behandlung vor Vertragsschluss im Rahmen der Risikobewertung
- Reichen aktuelle Obliegenheiten aus oder bedarf es Ausschlüssen?
- Wo liegt die Grenze zwischen Fahrlässigkeit, grober Fahrlässigkeit und Vorsatz?
- Beweislast im Schadenfall

Image: cosmin4000-GettyImages

Gedanken zum Patch-Management:
Fragen an die Gäste

Munich RE

Bitte nutzen Sie die Chat-Funktion

1. Erachten Sie das Thema Schwachstellen- und Patch-Management als Mindestvoraussetzung für Versicherungsschutz?
a) Ja b) Nein

2. Glauben Sie, dass es Bedarf gibt, das Thema Patch-Management vor Vertragsschluss im Rahmen der Risikobewertung intensiver zu hinterfragen?
a) Ja b) Nein

3. Glauben Sie, dass das Thema Schwachstellenmanagement / Patching in den Versicherungsbedingungen bzw. Obliegenheiten hinreichend adressiert ist?
a) Ja b) Nein