Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Kompromittierte Exchange-Server - Zunahme von Angriffen per Mail

CSW-Nr. 2021-269486-1032, Version 1.0, 11.11.2021

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet derzeit eine signifikante Zunahme von Angriffen per E-Mail. Wie schon in der Vergangenheit bei Emotet nutzen die Angreifenden vermeintliche Antworten auf tatsächlich getätigte E-Mail-Konversationen der Betroffenen, um Schadsoftware-Links zu verteilen. Neu ist allerdings, dass die gefälschten E-Mails dabei über die legitimen Mailserver der Absender selbst verschickt werden, sodass technische Detektion und Erkennung durch den Leser deutlich erschwert werden. Es ist also davon auszugehen, dass die Angreifenden Zugriff auf den Mailserver haben, welcher dann selbst "ordnungsgemäß" als Absender fungiert.

Die Links verweisen auf verschiedene Schadsoftware-Varianten, wie Qakbot (aka: Pinkslipbot, QBot) (siehe [MAL2021a]), DanaBot (siehe [MAL2021b]) und SquirrelWaffle (siehe [TAL2021], [MAL2021c]). Eine Infektion zum Beispiel mit QakBot führt meist zur Kompromittierung des gesamten Netzwerks und schlussendlich zu einem Ransomware-Vorfall bei den Betroffenen. Allerdings kann auch eine Infektion mit DanaBot oder SquirrelWaffle einen Ransomware-Vorfall nach sich ziehen.

Wie die Täter Zugriff auf den Mailverkehr erhalten, ist zum aktuellen Zeitpunkt noch unklar.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Bewertung

Das BSI geht davon aus, dass für die Angriffe seit längerem kompromittierte Exchange-Server verwendet werden. Anlass für diese Einschätzung sind die im Laufe des Jahres immer wieder erfolgreichen Angriffe über kritische Schwachstellen in diesen Systemen. Vor diesen Angriffen hatte das Bundesamt bereits damals gewarnt (u.a. im März [BSI2021a], Oktober [BSI2021b]).
Gleichzeitig ist nicht klar, welche Schwachstelle konkret für diese derzeitigen Attacken genutzt wird.

Selbst ein aktueller Patch-Stand auf Exchange-Servern ist kein sicherer Indikator dafür, dass eine Kompromittierung ausgeschlossen werden kann. Oftmals bestand die akute Gefahr, dass das System sehr schnell, also bereits vor dem Einspielen eines Updates, kompromittiert wurde. Zugangsdaten für diese infizierten Systeme werden aktuell auf Untergrund-Marktplätzen im Internet gehandelt (Access Broker / Access-as-a-Service).

Bei dem Verdacht auf Kompromittierung des Exchange-Servers empfiehlt das BSI, den Server neu aufzusetzen und nötige Daten wiederherzustellen. Weitere reaktive Empfehlungen können [BSI2021a] entnommen. Die dortigen Ausführungen beziehen sich zwar auf einen anderen Sachverhalt im Kontext "Exchange", behalten jedoch grundsätzlich ihre Gültigkeit.

Bei einer Infektion mit Qakbot kommt es in der Folge häufig zu einer vollständigen Kompromittierung des ganzen Netzwerks. Aufgrund der zumeist weitreichenden Infektion muss in der Regel das ganze Netzwerk neu aufgesetzt werden! Derart massive Vorfälle, wie bei Kompromittierungen mit QakBot, konnten unabhängig von der jetzt beobachteten Kampagne auch bei der Malware DanaBot beobachtet werden. SquirrelWaffle ist eine relativ neue Malware, welche als Loader auch weitere Malware nachladen kann und somit ebenfalls einen Einstiegspunkt für Ransomware-Angreifer darstellen kann. So wurde bereits beobachtet, dass über SquirrelWaffle die Malware QakBot nachgeladen wurde [TAL2021], denn all diese Netzkompromittierungen sind i.d.R. Grundlage für den dann anschließenden Einsatz von Ransomware.

Aus Sicht des BSI muss grundsätzlich davon ausgegangen werden, dass diese gefälschten E-Mails mit ihrer erweiterten Vortäuschmethodik erfolgreicher sein könnten, als damals Emotet. Noch ist die Anzahl der versandten / geharvesteden E-Mails aber viel geringer, wodurch das akute Schadenspotenzial derzeit relativiert wird.

Mögliche Auswirkungen

Der geschilderte Vorfall kann grundsätzlich alle Internetnutzenden treffen und die dargestellten Konsequenzen haben:

- vollständige Kompromittierung von einzelnen IT-Systemen oder ganzen Netzen
- Kompromittierung von IT-Systemen und ganzen Netzen bei Kunden, Lieferanten und anderen Partnern durch E-Mails, die im Namen der eigenen Institution versandt wurden
- Verschlüsselung und Datenverlust durch den anschließenden Einsatz von Ransomware
- Offenlegung von vertraulichen Daten durch Angreifende
- weitere Druckmaßnahmen

Fragen an IT-Sicherheitsverantwortliche

- Sind die aktuellen Updates auf Exchange-Servern eingespielt?
- Wie groß waren die Zeitfenster zwischen dem Bekanntwerden von Exchange-Server Schwachstellen und dem Ausrollen der Patches?
- Kam es in der Vergangenheit bereits zu Auffälligkeiten beim Exchange-Betrieb?
- Wurden die vom BSI bereitgestellten Empfehlungen umgesetzt? [BSI2021a]

Links

[MAL2021a] - QakBot (Malware Familiy)
https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot

[MAL2021b] - DanaBot (Malware Familiy)
https://malpedia.caad.fkie.fraunhofer.de/details/win.danabot

[MAL2021c] - SquirrelWaffel (Malware Familiy)
https://malpedia.caad.fkie.fraunhofer.de/details/win.squirrelwaffle

[TAL2021] - SQUIRRELWAFFLE Leverages malspam to deliver Qakbot, Cobalt Strike
https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html

[BSI2021a] - Microsoft Exchange Schwachstellen Detektion und Reaktion
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.html

[BSI2021b] - Sicherheitslücken bei Microsoft Exchange Servern – schnellstmöglich aktualisieren
https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/CSW-MS-Exchange-Server_061020.html

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.