Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

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

Ransomware DearCry nutzt aktuelle Sicherheitslücke in Exchange Server

Nr. 2021-198218-1022, Version 1.0, 18.03.2021

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

Am 11. März 2021 berichtete Bleeping Computer über die Ransomware DearCry, die für Angriffe auf Microsoft Exchange Server die Schwachstelle ProxyLogon ausnutzt [BPC2021]. Entdeckt wurde das Schadprogramm durch das ID-Ransomware-Projekt [IDR2021] des Malware Hunter Teams, nachdem mehrere Uploads mit möglichem Bezug zu Microsoft Exchange Daten auftauchten [TWI2021a].

Microsoft bestätigte die Beobachtungen schließlich am folgenden Tag. Nach Einschätzung des Unternehmens wird die Ransomware manuell verbreitet. Das heißt, dass sie sich nach derzeitigem Kenntnisstand nicht selbstständig weiter verbreitet [TWI2021b]. DearCry erstellt zuerst eine verschlüsselte Kopie der angegriffenen Datei (Copy Encryption) und überschreibt dann das Original, um eine Wiederherstellung zu verhindern (In Place Encryption) [SOP2021].

Auf Twitter erklärte ein Mitarbeiter des ID-Ransomware-Projekts am Abend des 11. März 2021, dass sechs einzigartige IP-Adressen mit den Strings "mx" oder "mail" in ihren DNS-Namen (Ergebnis einer Reverse DNS-Suche) Daten auf dem Portal hochgeladen hätten. Die Uploads stammten aus Österreich (1), Australien (1), Kanada (1), Dänemark (1) und den USA (2) [TWI2021c], [TRD2021]. Basierend auf den Upload-Zeitpunkten könne schlussgefolgert werden, dass DearCry mindestens seit dem 9. März 2021 im Einsatz sei.

Bleeping Computer ergänzte am 12.03.2021 außerdem eine Einschätzung von McAfee's Head of Cyber Investigations, John Fokker, wonach das Unternehmen DearCry-Infektionen in den USA, Luxemburg,

* 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.

Indonesien, Irland, Indien und Deutschland identifiziert habe [BPC2021]. Entgegen dieser Aussagen zeigt die dem Artikel beigefügte Heat Map von McAfee jedoch keine Infektion für Deutschland auf.

Bewertung

Basierend auf öffentlich verfügbaren Informationen zeigt DearCry derzeit keine Schwächen in der Verschlüsselung auf, wodurch eine Entschlüsselung ohne das notwendige Schlüsselmaterial möglich wäre. Die Ransomware stellt demnach eine große Bedrohung für Organisationen dar.

Eine Zuordnung der Schadsoftware zu einer Tätergruppe – und damit ggf. die Ableitung potenzieller Angriffsziele – ist zum aktuellen Zeitpunkt jedoch nicht seriös möglich und wäre spekulativ.

Bei VirusTotal wurden zumindest zwei Samples aus Deutschland hochgeladen. Hieraus lässt sich allerdings keine unmittelbare Betroffenheit in Deutschland ableiten, da der Upload auch durch einen Proxy oder einen VPN aus einem anderen Land erfolgt sein könnte. Denkbar ist ebenfalls, dass der Upload durch einen deutschen IT-Dienstleister erfolgte, der für ein ausländisches Unternehmen agierte.

Mögliche Auswirkungen

Die geschilderte Bedrohung stellt für alle Institutionen, in denen Server mit Microsoft Exchange im Einsatz sind, eine erhebliche Gefahr dar.

Fragen an IT-Sicherheitsverantwortliche

- Sind die Ausführungen der Cyber-Sicherheitswarnung des BSI [BSI2021a] bekannt?
- Werden in Ihrer Organisation Server mit den betroffenen Versionen von Microsoft Exchange eingesetzt?
- Wurden die Patches bereits installiert bzw. steht die Installation kurz bevor?
- Besteht die Möglichkeit, eine Kompromittierung der Server mithilfe der Indicators of Compromise unter [BPC2021] bzw. anhand der YARA-Regeln unter [ViT2021a], [ViT2021b] und [ViT2021c] zu überprüfen?
- Besteht ein Anschluss an einen Malware Information Sharing Portal (MISP) Verbund, sodass die Informationen des MISP-Events "OSINT - DearCry ransomware (abusing Exchange Server)" (UUID: 0165e5d7-51e6-4c2e-a382-1dd1e706f7bb) genutzt werden können?
- Sind die allgemeinen Handlungsanweisungen des BSI [BSI2021b] zur Reaktion auf Ransomware-Vorfälle bekannt?
- Wurde der Vorfall schon über die etablierten Kanäle an das BSI gemeldet?

Links

[BPC2021] DearCry ransomware attacks Microsoft Exchange with ProxyLogon exploits: https://www.bleepingcomputer.com/news/security/new-dearcry-ransomware-is-targeting-microsoft-exchange-servers/

[IDR2021] ID Ransomware: https://id-ransomware.malwarehunterteam.com

[SOP2021] Hafnium-Nutznießer: Ist DearCry als Prototyp ins Rennen geschickt worden?: https://news.sophos.com/de-de/2021/03/16/hafnium-nutzniesser-ist-dearcry-als-prototyp-ins-rennen-geschickt-worden/

[TWI2021a] Tweet des MalwareHunterTeam: https://twitter.com/malwrhunterteam/status/1370148335949127682

[TWI2021b] Tweet von Microsoft Security Intelligence: https://twitter.com/MsftSecIntel/status/1370236539427459076

[TWI2021c] Tweet von Michael Gillespie: https://twitter.com/demonslay335/status/1370125343571509250

[TRD2021] Microsoft Exchange servers targeted by DearCry ransomware abusing ProxyLogon bugs:

https://therecord.media/microsoft-exchange-servers-targeted-by-dearcry-ransomware-abusing-proxylogon-bugs/

[BSI2021a] Mehrere Schwachstellen in MS Exchange: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf

[ViT2021a] VirusTotal: https://www.virustotal.com/gui/file/2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff/community

[ViT2021b] VirusTotal: https://www.virustotal.com/gui/file/e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6/community

[ViT2021c] VirusTotal: https://www.virustotal.com/gui/file/feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede/community

[BSI2021b] Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf

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.