Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	31. März 2021
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN, BAG, Swissmedic

Aktuelles (März 2021)

Die Situation im Bereich Cyber-Sicherheit bleibt aufgrund von aktuellen Angriffen auf kritische Infrastrukturen und im Speziellen auf Organisationen im Gesundheitssektor angespannt.

- Die von uns detektierten Malspam-Wellen bleiben auf einem hohen Niveau.
- Hohe Risikoexposition durch «0day» Verwundbarkeit in Microsoft Exchange.
- Neue Malspam Kampagnen in der Schweiz führen erneut zu Kompromittierungen durch Ransomware

«0day» Verwundbarkeit in Microsoft Exchange

Anfang März 2021 wurden gleich mehrere Verwundbarkeiten in Microsoft Exchange bekannt, wobei eine als «kritische» eingestuft wurde. Dabei handelt es sich um CVE-2021-26855[1], eine Sicherheitslücke, welche sich aus der Ferne ausnutzen lässt, um unautorisiert Code auf dem System des Opfers auszuführen (Remote Code Execution – RCE). Die Sicherheitslücke ist auch unter dem Namen «ProxyLogon[2]» bekannt. Da gemäss Angaben von Microsoft die Sicherheitslücke bereits aktiv von mutmasslich staatlichen Akteuren aus China mit dem Namen «HAFNIUM[3]» bei gezielten Angriffen ausgenutzt wurde, hat Microsoft einen Notfallpatch ausserhalb des monatlichen Updatezyklus bereitgestellt («Out-of-band Patch»). Das NCSC hat in der Nacht vom 2. März auf 3. März die Betreiber/innen kritischer Infrastrukturen in der Schweiz auf die kritische Verwundbarkeit hingewiesen, Sofortmassnahmen empfohlen, sowie jeweils einen Tweet in den vier Landesprachen veröffentlicht. Wenige Stunden nach der Publikation der Lücke haben andere Gruppierungen, auch aus dem cyberkriminellen Umfeld damit begonnen, aktiv nach dieser Lücke zu scannen und sie automatisiert auszunutzen.

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
[2] https://proxylogon.com/
[3] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Zusätzlich hat das NCSC bereits kurz nach Bekanntgabe der Verwundbarkeit damit begonnen, durch Informationen von Partnerorganisationen sowie aus eigenen Sensoren gewonnene Daten auszuwerten um verwundbare, öffentlich zugängliche Microsoft Exchange Server in der Schweiz zu identifizieren und deren Eigentümer/innen per E-Mail zu benachrichtigen. Insgesamt wurden bis heute **4'316 solcher Benachrichtigungen** zu 5'484 Domain-Namen an 3'059 Empfänger durch das NCSC versendet. Betroffen waren vor allem KMUs aber auch Organisationen aus dem Gesundheitssektor, welche mit heiklen Patientendaten arbeiten.

Die folgende Grafik zeigt die von ESET detektierten Angriffe auf die besagte Verwundbarkeit. Klar ersichtlich ist, dass diese bereits vor der Veröffentlichung des Sicherheitsupdates am 3. März 2021 ausgenutzt wurde. Ebenfalls ersichtlich ist, dass die Verwundbarkeit innerhalb der ersten Tage nach Veröffentlichung bereits massiv ausgenutzt wurde:

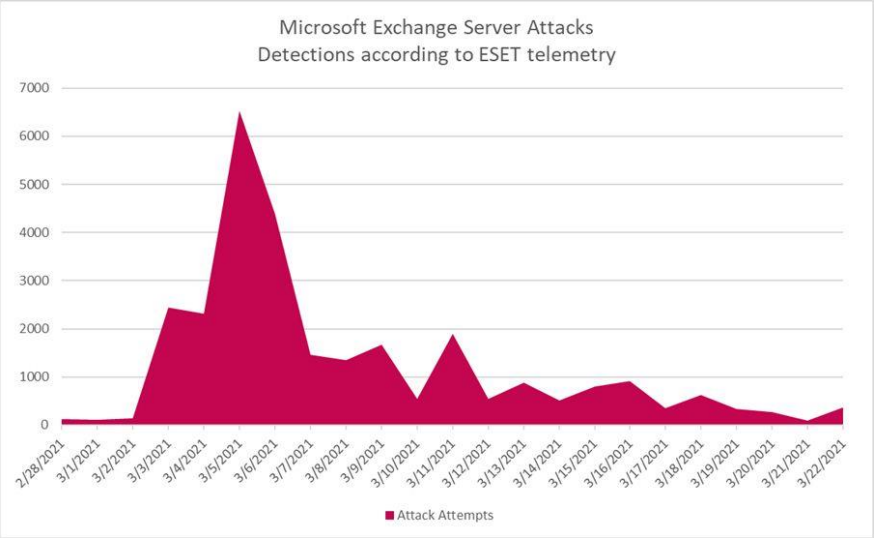

Figure 1 - Anzahl Angriffe auf die Microsoft Exchange Verwundbarkeit
Quelle: ESET

Obwohl das NCSC über alle ihr zur Verfügung stehenden Kanäle zeitnah über die kritische Verwundbarkeit informiert hat und das Thema auch in den Medien breit thematisiert wurde, kam es leider zu einer Vielzahl von Infektionen in der Schweiz. Während bei einem Grossteil der Infektionen bislang lediglich eine «Web-Shell» platziert wurde, welche den Angreifern jederzeit und uneingeschränkt Zugang zum betroffenen System ermöglicht (und dies auch noch nach Einspielung des Sicherheitsupdates von Microsoft), wurden in einigen Fällen Crypto-Miner aber auch Ransomware installiert. Dies führte in einigen, wenigen Fällen zu einer kompletten Verschlüsselung der IT-Infrastruktur durch Ransomware, was zu einem Stillstand der geschäftskritischen Prozesse führte.

Inzwischen sind mindestens zwei kriminelle Akteure aktiv, welche «ProxyLogon» für Angriffe mit Ransomware nutzen: «DoejoCrypt» (auch bekannt als «DearCry») und «Black Kingdom». Beide Gruppierungen verwenden die «ProxyLogon»-Verwundbarkeit als Einfallstor in Unternehmen. Danach versuchen sie sich via Microsoft Exchange Server lateral im Netzwerk des Opfers zu bewegen, um so möglichst viele Systeme mit Ransomware zu verschlüsseln.

«IcedID» auf dem Vormarsch

Nach dem Take-down des Emotet Botnetzes Anfang Februar sind nun bereits andere Schädlinge auf dem Vormarsch. GovCERT verzeichnet einen Anstieg bei Malspam Kampagnen, welche einen Trojaner mit dem Namen «IcedID» verteilen. Dabei setzen die Akteure auf präparierte Excel Dokumente, welche mit schädlichem Macro-Code versehen sind. Wird dieser ausgeführt, lädt das Macro IcedID aus dem Internet nach.

IcedID ist bereits seit längerem aktiv, hatte bislang jedoch einen starken US-Fokus. Nun wurden dem NCSC jedoch Fälle in der Schweiz bekannt, bei denen die Akteure mittels IcedID in Unternehmensnetzwerke eingedrungen sind, durch laterale Bewegung im Netzwerk des Opfers Zugriff auf weitere Systeme erlangten und diese so mit Ransomware verschlüsseln konnten.

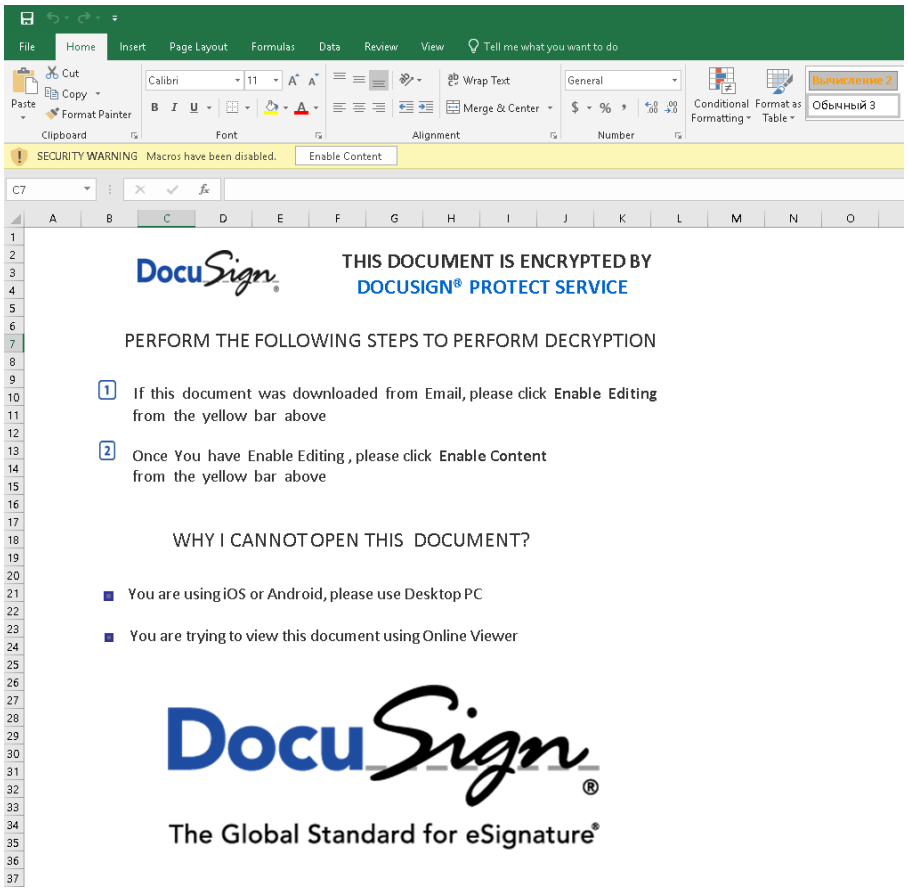

Figure 2 - Excel-Datei mit schädlichem Macro-Code

Empfehlungen:

- Sperrung von IP-Adressen bekannter Botnetz Command&Control Server (C&Cs) durch Implementierung des **MELANI BGP Feeds** (Kontakt: outreach@govcert.ch). Ob Sie oder Ihr Provider diese bereits einsetzen, kann mit einem Aufruf der folgenden Test-Einträge mittels Web-Browser überprüft werden. Schlägt die Verbindung fehl, sind Sie bereits geschützt:
  - http://ip-protection.govcert.ch
  - http://melbl-protection.govcert.ch

- Sperren von Domain-Namen bekannter Botnetz Command&Control Server (C&Cs) durch Implementierung der **MELANI RPZ** oder des **Secure DNS Resolvers** (Kontakt: outreach@govcert.ch)

- Blockieren Sie den Empfang von **gefährlichen E-Mail-Anhängen** auf Ihrem E-Mail-Gateway, dazu zählen auch **Office-Dokumente mit Makros**. Eine Empfehlung von zu sperrenden Dateianhängen finden Sie hier:
  - https://www.govcert.ch/downloads/blocked-filetypes.txt

- Setzen Sie LAPS (Local Administrator Password Solution) sowie Managed Service Accounts ein.
  - https://www.microsoft.com/en-us/download/details.aspx?id=46899
  - https://docs.microsoft.com/de-de/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts

- Erstellen **Sie regelmässig Sicherungskopien (Backups)** Ihrer Daten. Nutzen Sie dabei das Generationenprinzip (täglich, wöchentlich, monatlich - mindestens 2 Generationen). Stellen Sie jeweils sicher, dass Sie das Medium, auf welchem Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer bzw. Netzwerk **physisch trennen und sicher aufbewahren**.

- Einsatz einer Liste wie URLHaus[4], um das Nachladen von Malware zu verhindern.

- Nehmen Sie Meldungen von Behörden betreffend IT-Sicherheitsprobleme in Ihrem Unternehmen ernst. Bei Zweifel der Authentizität einer Meldung, fragen Sie telefonisch bei der Absenderbehörde nach.

- Stellen Sie sicher, dass Sicherheitsupdates zeitnah eingespielt werden. Hoch kritische Sicherheitsupdates müssen zudem sofort eingespielt und dürfen nicht auf das nächste Wartungsfenster verschoben werden.

- Infizierte Geräte müssen immer neu aufgesetzt werden. Eine Reinigung (oder ein nachträgliches Patchen) gibt nicht genügend Sicherheit, dass der Angreifer effektiv sämtliche Zugänge verloren hat. In diesem Zusammenhang muss auch untersucht werden, ob bereits eine laterale Bewegung stattgefunden hat und welche Benutzer Accounts potentiell kompromittiert worden sind.

[4] https://urlhaus.abuse.ch/

Kontakt GovCERT

Im Falle eines IT-Sicherheitsvorfalles, von verdächtigen E-Mails, etc. steht Ihnen das GovCERT jederzeit gerne zur Verfügung:

E-Mail: incidents@govcert.ch
Pikett-Telefon: +41 79 152 20 80 (**nur in Notfällen!**)

Für Rückfragen technischer Art oder Implementierung von NCSC Dienstleistungen:
outreach@govcert.ch