Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	8. Juli 2021
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN, BAG, Swissmedic

Aktuelles (Juni 2021)

Die Situation im Bereich Cyber-Sicherheit hat sich im Monat Juni leicht entspannt:

- Kritische Verwundbarkeit im Druckdienst von Windows
- Erneuert Ransomware-Angriff auf Spital
- Ransomware-Akteure ändern ihren Modus Operandi
- Ransomware-Akteure raten vom Einsatz von bekannten VPN Produkten ab

Das «Cyber Security Update» geht in die Sommerferien

Aufgrund der vergleichsweise entspannten Lage im Zusammenhang mit COVID19 sowie den anstehenden Sommerferien, welche erfahrungsgemäss zu einem Signifikaten Einbruch der Cyber-Angriffe führen, hat sich GovCERT.ch dazu entschlossen, das «Cyber Security Update» in die Sommerferien zu schicken. **Für die Monate Juli und August sind daher keine Cyber Security Updates für den Healthcare Sektor geplant.** Die nächste planmässige Ausgabe wird Ende September erscheinen.

Selbstverständlich sind wir auch während den Sommerferien jeder Zeit für Sie da und beobachten die aktuelle Gefahrenlage stetig. Sollte sich diese ändern behalten wir uns vor, Sie auch während den Sommerferien mit einem Cyber Security Update zu beliefern.

Kritische Verwundbarkeit im Druckdienst von Windows

Am 8. Juni 2021 veröffentlichte Microsoft einen Patch für sämtliche noch unterstützen Windows-Betriebssysteme, welcher eine von Microsoft mit «low» eingestufte Sicherheitslücke im Druckdienst von Windows («Print Spooler Service») schliesst (CVE-2021-1675[1]). Gemäss von Microsoft zunächst veröffentlichten Informationen kann ein Angreifer die Sicherheitslücke lokal ausnutzen, um sich unbefugt Administratorenrechte zu verschaffen («local privilege escalation»).

Am 21. Juni 2021 aktualisierte Microsoft ihre Einschätzung der Kritikalität der Verwundbarkeit von «low» auf «critical». Weitere Analysen haben gezeigt, dass sich die Verwundbarkeit auch aus der Ferne ausnützen lässt, um Zugang zum System des Opfers zu erlangen («Remote Code Execution – RCE»). Am 28. Juni 2021 haben Sicherheitsforscher zudem einen Proof of Concept (PoC) veröffentlich, mit welcher sich die Verwundbarkeit aus der Ferne ausnützen lässt.

Weitere, von Sicherheitsforschern durchgeführte Tests haben nun ergeben, dass der am 8. Juni 2021 veröffentlichte Patch die Verwundbarkeit scheinbar nicht behebt. **Es ist daher davon auszugehen, dass gepatchte Windows Systeme derzeit Verwundbar sind.**[2] Ein Statement von Microsoft sowie eine Aktualisierung des Patches steht noch aus.

Erneuter Ransomware-Angriff auf Spital

Auch im Juni 2021 waren Organisationen im Gesundheitssektor Ziel von Cyber-Angriffen. Das «Humber River Hospital» in Toronto (Kanada) wurde Mitte Monat von Cyber-Kriminellen mit einer unbekannten Ransomware Angegriffen. Das Spital verfügt über 772 Betten und behandelt jährlich über 150'000 Patienten. Gemäss eigenen Angaben[3] wurden als Reaktion auf den Angriff sämtliche Systeme temporär heruntergefahren und Notfallpatienten zeitweise umgeleitet.

Es ist leider nicht bekannt, welche Ransomware-Familie hinter dem Angriff steht oder ob und welche Art von Daten aus dem Unternehmensnetzwerk des Spitals entwendet wurden.

Ransomware-Akteure ändern ihren Modus Operandi

Im Juni 2021 gab es gleich zwei Änderungen im Modus Operandi von Ransomware-Akteure:

- **Babuk Ransomware:** Im Juni hat die unbekannte Täterschaft hinter der Ransomware «Babuk» verkündet[4], in Zukunft keine Daten oder Systeme mehr zu verschlüsseln. Vielmehr wollen sie in Zukunft sich auf das «kidnapping» von Unternehmensdaten konzentrieren, mit welchen Sie die Opfer erpressen können. Babuk geriet im Frühling 2021 in die Schlagzeilen, nachdem diese Polizei-Organisationen in den USA verschlüsselt und Daten entwendet haben.

- **REvil Ransomware:** Ende Juni 2021 haben Sicherheitsforscher Malware-Samples

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675

[2] https://isc.sans.edu/forums/diary/CVE20211675+Incomplete+Patch+and+Leaked+RCE+Exploit/27588/

[3] https://www.hrh.ca/2021/06/15/code-grey/

[4] https://hotforsecurity.bitdefender.com/blog/babuk-ransomware-gang-says-its-no-longer-interested-in-encrypting-data-would-rather-kidnap-it-instead-25910.html

gesichtet, welche der «REvil» Ransomware (auch bekannt als «Sodinokibi») zugeordnet werden können. Anders als die bisherigen Malware-Samples haben es diejenigen jedoch nicht auf Windows basierte System sondern auf Netzwerkspeicher (NAS) und Virtuelle Systeme (VMware ESXi) abgesehen[5].

Ransomware-Akteure raten vom Einsatz von bekannten VPN Produkten ab

In einem Tweet[6] erklärten die Sicherheitsforscher des «MalwareHunterTeam» auf Twitter, dass Ransomware-Akteure vom Einsatz von «Pulse Secure» und «SonicWall VPN» abraten. Beide Produkte haben dieses Jahr kritische Sicherheitslücken aufgewiesen, über welche sich Cyber-Kriminelle Zugang zu Unternehmensnetzwerke verschaffen und diese mit Ransomware verschlüsseln konnten. Um Welche Ransomware-Akteure es sich handelt und woher das Zitat stammt ist nicht klar. Wir vermuten, dass dieses höchstwahrscheinlich aus einem Chat zwischen den Akteuren und einem Ransomware-Opfer stammt.

Empfehlungen:

- Gegen das Internet hin exponierte Systeme wie RDP, VPN Dienste, etc. müssen stets auf dem Patchlevel gehalten werden. **Sicherheitsaktualisierungen müssen zeitnah eingespielt werden.**

- **Remotezugänge** wie VPN und RDP sowie sämtliche andere Zugänge auf interne Ressourcen (z.B. Webmail, Sharepoint, etc) müssen zwingend mit einem zweiten Faktor abgesichert werden (**Zwei-Faktor-Authentisierung** – 2FA). Stellen Sie sicher, dass sie über einen genügend langen Zeitraum Logdaten aller erfolgreichen und fehlgeschlagenen Zugriffsversuchen haben. Speichern Sie diese Logdaten zentral und werten Sie diese regelmässig aus.

- 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** für den Gesundheitssektor (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

[5] https://www.heise.de/news/Verschluesselungstrojaner-REvil-hat-es-nun-auf-virtuelle-Maschinen-abgesehen-6122156.html

[6] https://twitter.com/malwrhunterteam/status/1400339083596083201

- 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[7], 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.

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 GovCERT Dienstleistungen:
outreach@govcert.ch

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