Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	6. Oktober 2021
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN, BAG, Swissmedic

Aktuelles (Juli – September)

Im Sommer 2021 wurden wieder vermehrt Unternehmen und Organisationen in der Schweiz erfolgreich angegriffen und mit Ransomware verschlüsselt. Die Risikoexposition des Gesundheitssektors bleibt hoch.

- Exponierte Systeme mit Verwundbarkeiten begünstigen Ransomware-Angriffe
- Weiterhin Ransomware-Angriffe auf Spitäler
- Studie: Hälfte der US Spitäler «offline» Aufgrund von «Ransomware»
- Ransomware «DoppelPaymer» als «Grief» wieder aktiv
- «Supply Chain Attack» trifft mehrere Unternehmen in Österreich
- Interview mit LockBit 2.0 Ransomware Täterschaft

Zudem haben wir den Schutz vor dem «QakBot»-Botnetz intensiviert.

Exponierte Systeme mit Verwundbarkeiten begünstigen Ransomware-Angriffe

Seit Jahren weist das NCSC (früher MELANI) immer wieder auf ein konsequentes Patch- und Lifecycle-Management hin. Verwundbarkeiten auf internen Systemen ermöglichen es Angreifern, die in das Netzwerk eingedrungen sind, sich lateral im Netzwerk des Opfers zu bewegen und weitere Systeme und Dienste zu kompromittieren.

Noch fataler sind Verwundbarkeiten in Systemen, welche gegen das Internet hin exponiert sind und aus der Ferne ohne Weiteres ausgenutzt werden können, um Schadcode auf dem verwundbaren System auszuführen («Remote Code Execution» - RCE). Solche werden auch zunehmend von Ransomware-Gruppierungen verwendet, um einen initialen Zugang zu Unternehmensnetzwerken zu erhalten.

Im Sommer 2021 wurden gleich mehrere, schwerwiegende Verwundbarkeiten publik, welche ein solches Vorgehen erlauben:

- Local Privilege Escalation (CVE-2021-26084) in Atlassian Confluence Server: https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html
- Arbitrary File Upload (CVE-2021-22005) in VMware vCenter: https://www.vmware.com/security/advisories/VMSA-2021-0020.html
- Diverse Verwundbarkeiten in Pulse Connect Secure (PCS): https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/

Das NCSC hat aufgrund der Häufung von Ransomware-Angriffen sowie der Tatsache, dass scheinbar viele Unternehmen und Organisationen nach wie vor die «Best-Practices» in Bezug auf die Cybersicherheit nicht umgesetzt haben, noch einmal Nachdrücklich auf die Umsetzung solcher Massnahmen hingewiesen[1].

Schutz vor «QakBot»-Botnetz

Neben «TrickBot» und «Dridex» hat sich mittlerweile auch «QakBot» als beliebter Infektionsvektor für Ransomware etabliert. Dabei setzt QakBot auf ein Vorgehen, welches bereits von «Emotet» verwendet wurde: «Email thread hijacking» (auch «dynamite phishing[2]» genannt). Dabei werden von bereits infizierten Computern E-Mails entwendet, welche dann mit Malware versehen und an den Absender der E-Mail versendet werden. Dadurch schaltet sich die Täterschaft in eine legitime, tatsächlich existierende E-Mail-Konversation ein und animiert den Empfänger, einen Link in der E-Mail anzuklicken oder einen Datei-Anhang zu öffnen. Dies führt dann sogleich zu einer Infektion mit Malware.

Um Netzwerkverkehr zu bekannten QakBot Botnetz C&C Servern zu detektieren und zu unterbinden, speist das GovCERT seit September 2021 IP Adressen von bekannten, aktiven QakBot C&C Server in die Dienstleistung «MELANI BGP Feed ein». Unternehmen und Organisationen, welche die Dienstleistung verwenden, erhalten einen zusätzlichen Schutz gegen Qakbot.

Weiterhin Ransomware-Angriffe auf Spitäler

Leider verlief der Sommer nicht ohne Ransomware-Angriffe. Auch Spitäler waren erneut von solchen Angriffen betroffen. So traf es im August 2021 beispielsweise auch das Gesundheitswesen in den USA. In Folge eines Ransomware-Angriffs[3] musste der Spital-Komplex von Memorial Health System (MHS) in Marietta (Ohio) Operationen verschieben und Notfallpatienten abweisen. Zudem musste MHS auf «Notfall Backup-Systeme» zurückgreifen, um einen Minimalbetrieb zu gewährleisten.

Gemäss mehreren Medienberichten sowie Aussagen des FBI[4] steckt die Ransomware «Hive» hinter dem Angriff auf MHS, welche sich mittels Malspam und Remote Desktop Pro-

[1] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/ransomware-8.html

[2] https://www.heise.de/news/Ransomware-Qakbot-tritt-in-Emotets-Fussstapfen-6181387.html

[3] https://www.beckershospitalreview.com/cybersecurity/surgeries-canceled-ambulances-diverted-it-system-down-at-ohio-health-system-after-ransomware-attack.html

[4] https://www.ic3.gov/Media/News/2021/210825.pdf

tokoll (RDP) Zugang zu Unternehmensnetzwerken verschafft haben. Es wurde nicht bekannt, ob die Angreifer eine Lösegeldforderung gestellt haben und ob das betroffene Spital auf diese eingegangen ist. Das Fachmagazin «Bleeping Computer» hat nach eigenen Aussagen[5] jedoch Beweise erhalten, dass die Angreifer Datenbanken mit Informationen von 200'000 Patienten gestohlen haben.

Im Mai 2021 berichteten wir über den US Gesundheitsanbieter «Scripps Health» welche Opfer der Ransomware «Conti» wurde. Der Gesundheitsanbieter betreibt 5 Spitäler und 19 Ambulatorien im US Bundestaat Kalifornien. Im August 2021 gab dieser bekannt, dass der Verlust aufgrund des erfolgreichen Ransomware-Angriffs auf USD 106,8 Millionen geschätzt wird. Der Grossteil des Verlusts von USD 91.6 Millionen wird mit der Abschaltung der IT-Systeme begründet, welche nach eigenen Angaben 4 Wochen anhielt. Weitere USD 21,1 Millionen wurden für den Incident Response Prozess sowie für das wiederhochfahren der Systeme aufgewendet[6]. Gemäss Aussage von «Scripps Health» waren lediglich USD 5,9 Millionen durch eine Versicherungspolice gedeckt und wurden von dieser übernommen.

Die Ransomware-Angriffe im Sommer dieses Jahres beschränkten sich aber nicht auf die USA. Auch wurden Ransomware-Angriffe auf Spitäler in Frankreich publik, wie beispielsweise derjenige gegen das Spital in der Stadt Arles. Gemäss Angaben des Spitals wurde dieses durch eine Gruppierung namens «Vice Society» verschlüsselt und komplett lahmgelegt[7]. So wurden nicht nur Clients und Server durch die Angreifer verschlüsselt, sondern auch das Backup «unleserlich» gemacht. Immerhin machte der Direktor des betroffenen Spitals eine klare Aussage in Bezug auf mögliche Lösegeldzahlungen: «[…] wir haben die Forderung nicht einmal gelesen weil wir nicht bezahlen werden.[…]». Ob tatsächlich kein Lösegeld bezahlt und ob Patientendaten entwendet wurden ist nicht bekannt. «Vice Society» nutzt unter anderem die Mitte 2021 veröffentlichte Sicherheitslücke «PrintNightmare» in Windows aus (CVE-2021-36958), um sich lateral im Netzwerk des Opfers zu bewegen.

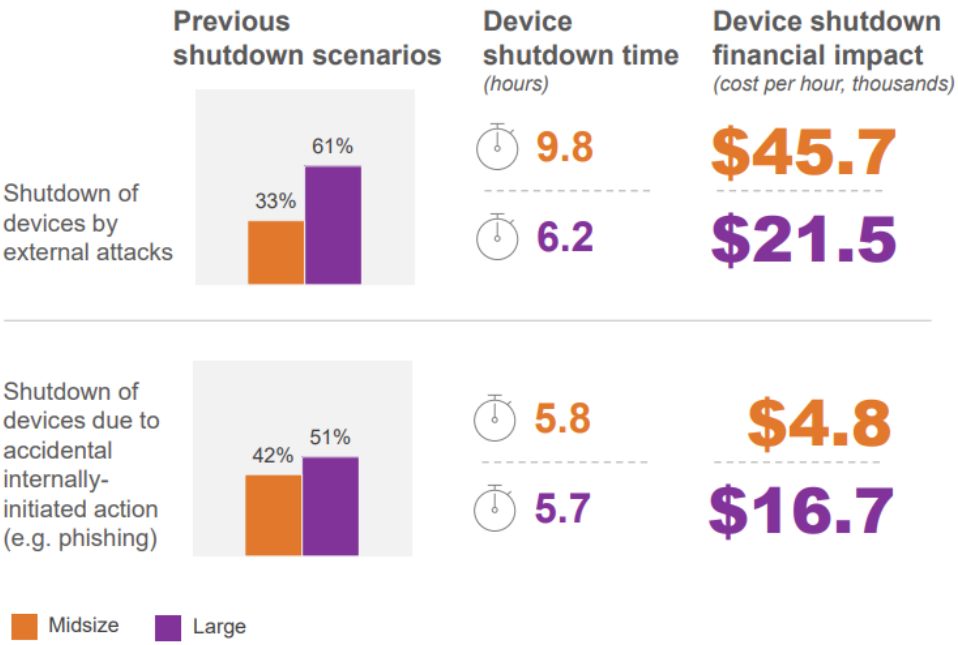
[5] https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/

[6] https://therecord.media/healthcare-provider-expected-to-lose-106-8-million-following-ransomware-attack/

[7] https://www.dna.fr/faits-divers-justice/2021/08/19/l-hopital-d-arles-pirate-les-hackers-demandent-une-rancon

Studie: Hälfte der US Spitäler «offline» Aufgrund von «Ransomware»

Eine Studie[8] des US Cybersicherheits-Spezialisten CyberMDX und Philips kam zum Schluss, dass im ersten Halbjahr 2021 knapp die Hälfte (48%) der US Spitäler aufgrund von Ransomware-Angriffen temporär Systeme abschalten mussten. Dies aufgrund von direktem Ransomware-Befall oder als präventive Massnahme aufgrund von Angriffen oder Hinweisen von extern. Mittelgrosse US Spitäler berichteten zudem, dass die Beeinträchtigung der Systeme durchschnittlich 10 Stunden betrug, wobei die Kosten pro Stunde auf 45'700 USD geschätzt wurden.



Quelle Grafik: Studie cybermdx

Abbildung 1 - Auszug aus der Studie von CyberMDX

Die Studie zeigt einmal mehr die hohe Risikoexposition von Organisationen im Gesundheitssektor. Es ist daher essentiell, dass Massnahmen zur Erhöhung der IT-Sicherheit getroffen und umgesetzt werden und diese laufend auf die sich verändernden Bedrohungen angepasst werden. Entsprechende Empfehlungen des NCSC finden sich am Ende dieses Dokuments.

Ransomware «DoppelPaymer» als «Grief» wieder aktiv

Auch Ransomware braucht ab und zu einen neuen Anstrich, so auch geschehen bei der Ransomware «DoppelPaymer». Diese erlangte im Jahr 2020 einen hohen Bekanntheitsgrad, als diese die Uniklinik Düsseldorf mit einem erfolgreichen Angriff lahmlegte. Im Mai 2021 wurde es dann aber plötzlich still um «DoppelPaymer». So wurden beispielsweise auch, mit einer Ausnahme im September 2021, keine neuen Daten von Opfer auf deren «Leak-Webseite» publiziert, was zunächst darauf hindeutete, dass die Gruppierung hinter «DoppelPaymer» sich eine Auszeit gönnt oder ihre Aktivitäten gänzlich aufgegeben hat.

[8] https://www.cybermdx.com/press-releases/perspectives-in-healthcare-security-report/

Anfangs Juli 2021 betrat eine neue Ransomware die Bühne: «Grief». Technische Analysen der «Grief» Malware Samples deuteten jedoch schnell darauf hin, dass es sich bei der Ransomware um eine Neuauflage von «DoppelPaymer» handelt. Ein wesentlicher Unterschied zu DoppelPaymer ist, dass das Lösegeld bei Grief in Form der Crypto-Währung «Monero» (XMR) anstelle von Bitcoin (BTC) bezahlt wird. Leider liess das erste Opfer auch in der Schweiz nicht auf sich warten. Anfangs Juli wurde der Vergleichsdienst «Comparis» Opfer von «Grief» und hat nach eigenen Angaben auch eine nicht genannte Summe an Lösegeld an die Erpresser bezahlt.

DoppelPaymer war aber nicht die erste und auch nicht die letzte Ransomware-Operation, welche sich einen neuen Anstrich verpasste. Auch die Gruppierung hinter der Ransomware «DarkSide» verpasste sich nach dem schwerwiegenden Angriff auf das US Unternehmen «Colonial Pipeline» einen neuen Anstricht und tritt seit Sommer 2021 unter dem Namen «BlackMatter» auf. Eben erst im September gelang «BlackMatter» mit einem erfolgreichen Angriff auf den japanische Tech-Gigant «Olympus» ein weiterer Coup.

Wieso sich solche hin und wieder neu erfinden, dafür gibt es mehrere mögliche Gründe. Ein wichtiger Faktor sind sicherlich die Aktivitäten in den geschlossenen Foren und Markplätze im Dark Web, wo sich Akteure und «Kunden» («Affiliates») austauschen und Dienstleistungen anbieten bzw. beziehen. Gerät ein Akteur dort in Verruf, verstösst gegen geltende Regeln oder wird ein solche gar von der Handelsplattform permanent ausgeschlossen, so bleibt diesem oftmals nur ein «rebranding».

Ein weiterer Grund für ein «rebranding» kann aber auch innen- oder aussenpolitischer Druck sein, so beispielsweise die vom Office of Foreign Assets Control (eine Behörde des U.S. Treasury Department) im Jahr 2020 verhängten Restriktionen und Sanktionen im Zusammenhang mit Ransomware.

«Supply Chain Attack» trifft mehrere Unternehmen in Österreich

Im September ereignete sich einer der wohl schwerwiegendsten Cyberangriffe in der Geschichte von Österreich. Unbekannten gelang es das Gerät eines Systemadministrators eines IT-Dienstleister zu kompromittieren[9]. Dadurch erhielten die unbekannten Täter Zugriff auf 34 Unternehmen welche durch diesen betreut wurden. Die Angreifer konnten durch den Administratoren-Zugriff Netzwerke der Kunden mit Ransomware verschlüsselen. Wie hoch die Lösegeldforderung war und ob die Opfer bezahlt haben, ist nicht bekannt. Die Angreifer haben nach dem erfolgten Angriff jedoch Daten der betroffenen Unternehmen im Dark-Web veröffentlicht, was darauf schliessen lässt, dass die Opfer den Lösegeldforderungen nicht nachgekommen sind. Gemäss Medienberichten[10] steht die Ransomware-Gruppierung «BlackMatter» hinter dem Cyberangriff.

Das Vorgehen der Angreifer ist nicht neu: Wie wir in einer früheren Ausgabe des «Cybersecurity Updates» bereits berichteten gelang es Cyberkriminellen im Frühling 2021 sich durch eine solche «Supply Chain Attack» gegen den US IT-Dienstleister «Kaseya» Zugriff zu duzenden Unternehmen zu verschaffen und diese mit Ransomware zu verschlüsseln.

[9] https://futurezone.at/digital-life/oesterreich-ransomware-angriff-unternehmen-hacker-angriff/401722305

[10] https://www.ots.at/presseaussendung/OTS_20210908_OTS0194/cyberangriff-auf-ooe-firmen-wichtige-daten-sichergestellt

Interview mit LockBit 2.0 Ransomware Täterschaft

Die Ransomware «LockBit» dürfte vielen Lesern bekannt sein. Bereits in der Ausgabe unseres Cybersecurity Updates vom Februar 2021 haben wir über ein Interview mit den Urhebern von «LockBit» berichtet. Seit Juni 2021 ist die Täterschaft nun mit einer überarbeiteten Version ihrer Ransomware zurück: «LockBit 2.0». Die Ransomware wird weiterhin als «Ransomware-as-a-Service» (RaaS) im Dark Web angeboten. In einem Interview mit dem russischsprachigen YouTube Kanal «Russian OSINT»[11] gab die Täterschaft erneut Auskunft über ihre Operationen. Dabei machte die Täterschaft unter anderem folgende Aussagen:

- **Supply Chain Attacks:** Die Täterschaft geht davon aus, dass Supply Chain Angriffe wie diejenige auf den US IT-Dienstleister Kaseya sich in Zukunft häufen werden.
- **Cybersicherheit bei Unternehmen weiterhin schlecht:** Die Täterschaft ist der Meinung, dass sich Unternehmen beim Schutz ihrer Infrastruktur vor Ransomware nicht verbessert haben. Dies obwohl die Anzahl von Cyberangriffen mit Ransomware zugenommen hat.
- **COVID-19 Pandemie:** Die Täterschaft sagt, dass es durch COVID-19 Pandemie bedingtes Home Office einfacher geworden ist, «Ziele zu infizieren».
- **Ziel Europa und USA:** Die Täterschaft gibt an, dass die Häufigkeit von (erfolgreichen) Ransomware-Angriffe gegen Unternehmen in Europa und der USA dadurch begründet ist, dass diese eher über eine Cyber-Versicherung verfügen.

Empfehlungen:

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

- Administrationszugänge sollten nie ins Internet exponiert werden, sondern Beispielsweise nur über eine separate Netzzone («Management-Zone») zugänglich sein. Der Zugang auf eine solche Zone muss stark authentifiziert (Zwei Faktor Authentisierung – 2FA) und sämtliche Zugriffe sollten aufgezeichnet werden. Geräte, welche für die Administration verwendet werden, sollten für keine anderen Zwecke gebraucht werden (insbesondere nicht für das Surfen im Web oder für E-Mails).

- **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

[11] https://ke-la.com/lockbit-2-0-interview-with-russian-osint/

  - 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

- Erstellen **Sie regelmässig Sicherungskopien (Backups)** Ihrer Daten. Nutzen Sie dabei das Generationenprinzip (täglich, wöchentlich, monatlich - mindestens 2 Generationen, besser 3). 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[12], um das Nachladen von Malware zu verhindern.

- Schützen und Überwachen sie zentrale Ressourcen wie ein Active Directory und bereiten Sie Notfallpläne für eine mögliche Kompromittierung vor.

- 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.

- Wählen Sie Ihre Zulieferer (Supplier), insbesondere solche von IT-Dienstleistungen, sorgfältig aus und achten Sie darauf, dass Ihr Dienstleister «Best Practices» im Bezug zur Cybersicherheit ebenfalls umgesetzt hat. Stellen Sie vertraglich sicher, dass der Zulieferer Sie über relevante Cybervorfälle in seiner Firma sowie den möglichen Diebstahl von Kundendaten (Data breach) zeitnah informiert. Gewähren Sie Dienstleistern keine uneingeschränkten Remote Zugänge und sichern Sie diese soweit als möglich ab.

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

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