Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	3. November 2021
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN, BAG, Swissmedic

Aktuelles (Oktober)

Im Oktober 2021 wurden erneut verschiedene Organisationen in der Schweiz Opfer von Cyberangriffen. Oftmals wurden dabei Unternehmensdaten durch eine «Ransomware» verschlüsselt. Das NCSC weisst deshalb noch einmal explizit auf die bereits seit längerem bestehenden Empfehlungen betreffend Cyber-Sicherheit hin:

Erfolgreiche Ransomware-Angriffe auf Schweizer Unternehmen:
https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/ransomware-8.html

Das aktuelle Healthcare Update behandelt zudem folgende Themen:

- Hohes Volumen an «QuakBot» malspam
- Der «König der Ransomware» im DarkWeb
- US Präsident Joe Biden fordert den Einsatz von Multi-Faktor-Authentisierung (MFA)
- Ransomware-Angriffe auf Gesundheitsorganisationen können zu einer erhöhten Sterblichkeitsrate führen
- Klage gegen US-Spital wegen Ransomware-Angriff
- Niederlande kann Nachrichtendienst oder die Armee einsetzen, um Ransomware-Angriffen entgegen zu wirken
- Cyber-Angriff auf mehrere israelischen Krankenhäuser
- 2021: 83% der Opfer von Ransomware bezahlen Lösegeld

Hohes Volumen an «QuakBot» malspam

Im letzten Cyber Security Update (Ausgabe September 2021) haben wir bereits über die Malware «QuakBot» (auch bekannt unter dem Namen «Qakbot» und «Qbot») berichtet. Diese scheint in den Sommer Monaten, aber vor allem vermehrt im Monat Oktober den Platz von «Emotet» eingenommen zu haben. Im Oktober 2021 wurde dem NCSC eine Vielzahl an bösartigen E-Mails gemeldet, bei welchen die unbekannte Täterschaft legitime E-Mail Konversationen aus dem Mailpostfach von mit «QuakBot» infizierten Computer gestohlen hat. Diese E-Mail Konversationen wurden dann von den Tätern für die Infektion von weiteren Computer verwendet («E-Mail threat hijacking» oder «dynamite phishing» genannt).

«QuakBot» fügt dazu einen Link zu einer schädlichen Webseite in die legitime E-Mail Konversation ein, über welche eine bösartige Excel-Datei heruntergeladen wird. Diese wiederum beinhaltet schädlichen Macro Code. Nach dem Öffnen der Excel-Datei versucht diese mittels «Social Engineering» das Opfer dazu zu überzeugen, die in der Excel-Datei vorhandenen Macros zu aktivieren. Aktiviert das Opfer diese, lädt der schädliche Macro Code «QuakBot» von einer weiteren (gehackten) Webseite nach und infiziert das System.

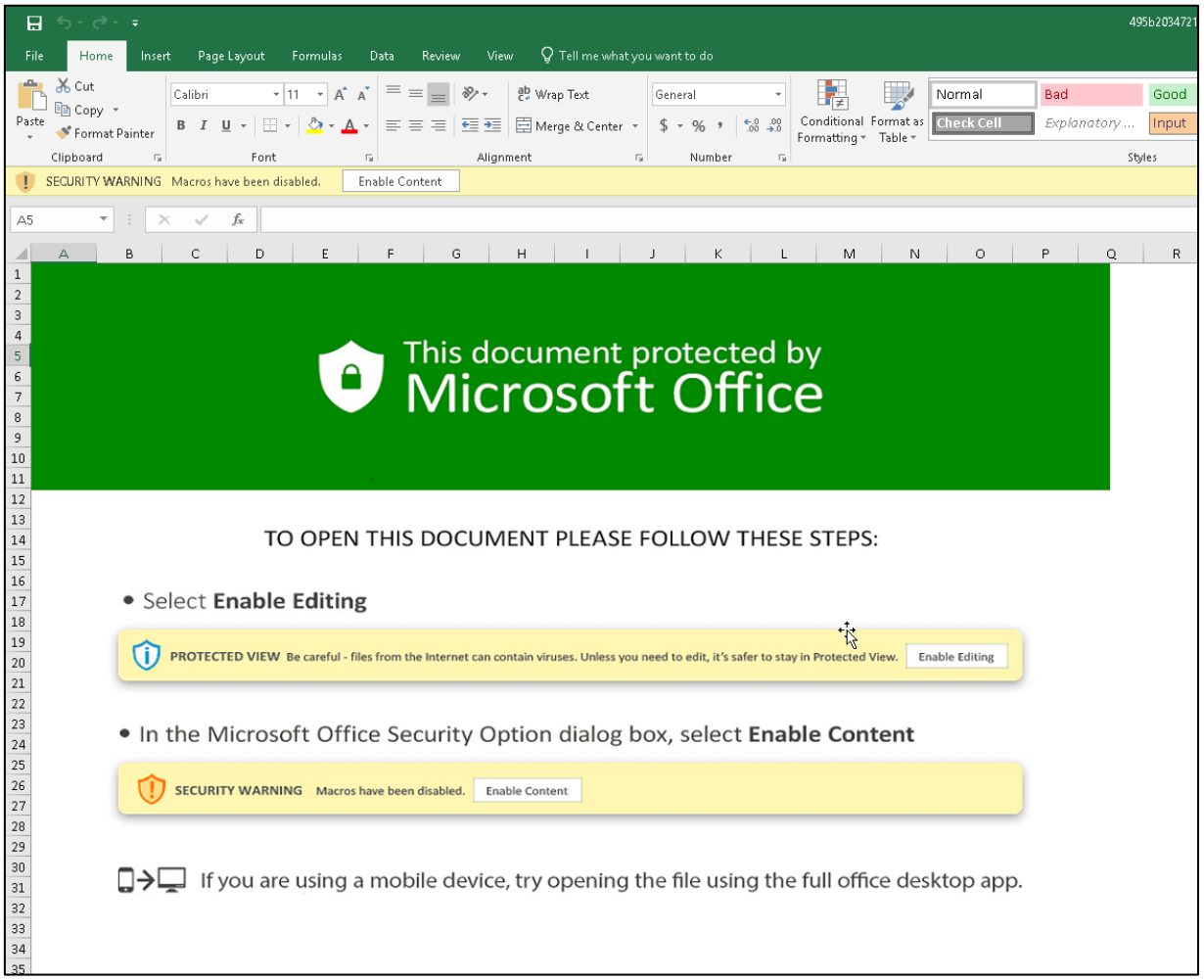

Figure 1 - Beispiel einer schädlichen Excel-Datei (QuakBot)

Trotz der legitimen E-Mail Konversation kann das E-Mail durch überprüfen der E-Mail Adresse des Absenders als Malspam in der Regel relativ einfach als Malspam identifiziert werden: Dieses verwendet nämlich einen beliebigen Absender anstelle der original E-Mail Adresse des ursprünglichen Absenders. Es lohnt sich also einen zweiten Blick auf die E-Mail

Adresse des Absenders zu werfen sowie auch allfällige legitime Emails kritisch zu betrachten.

Wer ist der «König der Ransomware» im Dark Web?

IT-Sicherheitsforscher des Unternehmens «DarkTracer», welches sich auf die Überwachung von Akteuren im DarkWeb spezialisiert hat, führte eine Erhebung der erfolgreichsten Ransomware Familien im DarkWeb durch. Dabei wurden die Anzahl Unternehmen, welche Opfer von Ransomware wurden, pro Ransomware Familie zusammengezählt. Über die Zeitspanne der Datenerhebung ist nichts bekannt, jedoch liefert die von DarkTracer veröffentlichte Statistik einen guten Eindruck über die Landschaft von Ransomware Familien:

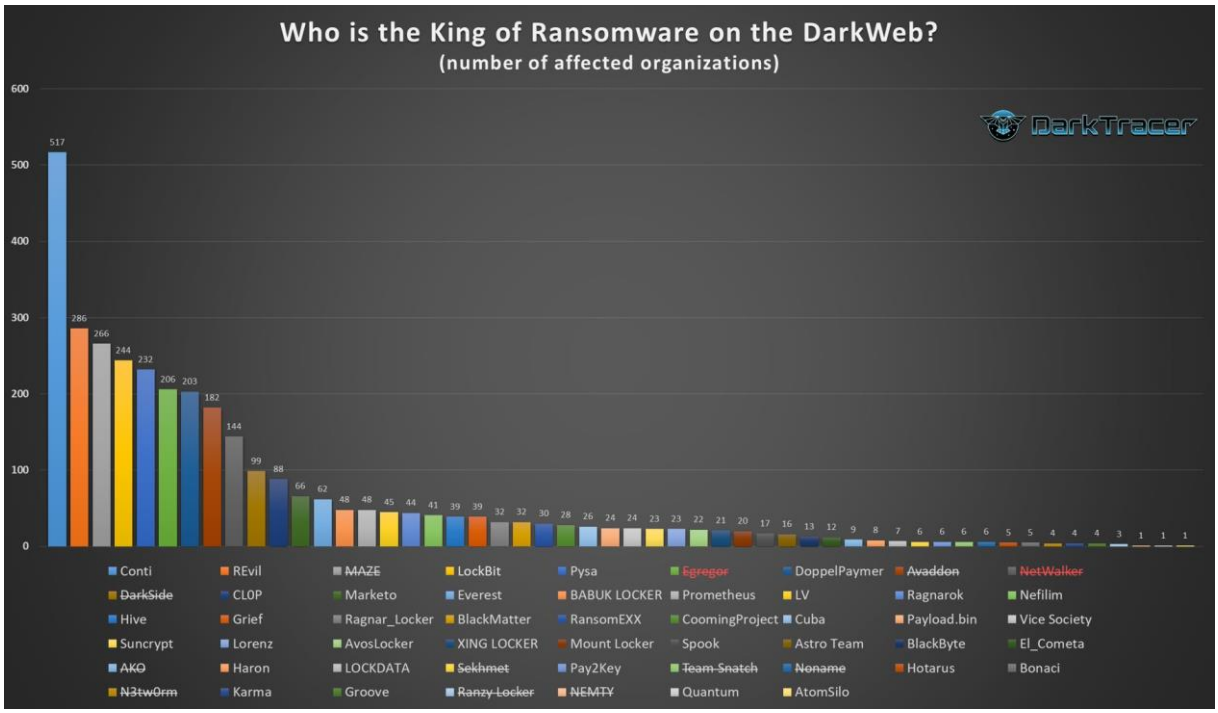

Figure 2 - Anzahl Opfer (Unternehmen) pro Ransomware Familie

Die Ransomware «Conti» ist gemäss Auswertung die erfolgreichste Ransomware Familie gemessen an der Anzahl Opfer. Weit abgeschlagen aber auf dem zweiten Platz wird die Ransomware «REvil» (auch bekannt als «Sodinokibi») geführt. Beide haben in den vergangenen Jahren leider auch erfolgreich Unternehmen in der Schweiz angegriffen und verschlüsselt.

US Präsident Joe Biden fordert den Einsatz von Multi-Faktor-Authentisierung (MFA)

In einer vom Weissen Haus veröffentlichten Erklärung[1] des US-Amerikanischen Präsidenten Joe Biden fordert dieser unter anderem den Einsatz von Multi-Faktor-Authentisierung (MFA),

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/01/statement-by-president-joe-biden-on-cybersecurity-awareness-month/

um der Bedrohung durch Ransomware entgegen zu treten. Es ist das erste Mal, dass sich ein Staatspräsident öffentlich für den Einsatz von MFA einsetzt.

Das NCSC fordert bereits seit Jahren den flächendeckenden Einsatz von Zwei-Faktor- Authentisierung (2FA), welche zu MFA gehört. Trotz dieser Empfehlungen werden auch Unternehmen in der Schweiz immer wieder durch gestohlene Zugangsdaten für Remote-Zugänge (wie z.B. VPN oder RDP) mit Ransomware verschlüsselt. Dies, weil die Remote-Zugänge nicht durch einen zweiten Faktor geschützt wurden. Auch der vergangene Monat blieb dahingehend leider keine Ausnahme: Eine Vielzahl der Ransomware-Fälle in der Schweiz wurde in den vergangenen Monaten durch das Fehlen einer Zwei-Faktor-Authentisierung überhaupt ermöglicht.

Ransomware-Angriffe auf Gesundheitsorganisationen können zu einer erhöhten Sterblichkeitsrate führen

Im Monat Oktober publizierte Resultate einer Untersuchung[2] des US-Amerikanischen «Ponemon Institute»[3] zeigen, dass Ransomware-Angriffe auf Organisationen aus dem Gesundheitssektor während der COVID-19 Pandemie zu einer erhöhten Sterblichkeitsrate führen können. Dazu haben die Wissenschaftler 597 IT experten befragt. Die Ergebnisse der Untersuchung zeigen, dass fast jedes vierte Unternehmen im Gesundheitssektor durch Ransomware-Angriffe eine erhöhte Sterblichkeitsrate aufführten.

Klage gegen US Spital wegen Ransomware-Angriff

Wie das US-amerikanische Informatik-Magazin «TechRepublic» im Oktober berichtete, hat eine Patientin Klage gegen ein Spital im US-Bundesstaat Alabama eingereicht. Dies nachdem ihr Baby bei der Geburt mit Hirnschäden geboren worden ist[4]. Die Patientin beschuldigt das Spital, dass dieses während der Geburt im Juli 2019 von einem Ransomware Angriff betroffen war, was angeblich dazu führte, dass diverse Computer-Systeme nicht funktionierten. Dies führte gemäss Anklage dazu, dass «Überwachung Technology» auf der Geburtenstation, welche zur Überwachung des Herzrhythmus des Babys verwendet wurden, nicht ordnungsgemäss funktioniert hat, was zu einem irreversiblen Hirnschaden beim Baby geführt hat. Das Baby starb darauf im Alter von 9 Monaten. Die Geburtenhilfe gab später an, dass sie das Baby mittels Kaiserschnitt auf die Welt gebracht hätte, hätte die Überwachung des Herzrhythmus funktioniert.

Niederlande kann Nachrichtendienst oder die Armee einsetzen, um Ransomware-Angriffen entgegen zu wirken

Der niederländische Aussenminister Ben Knapen antwortete auf eine parlamentarische Anfrage betreffend «Ransomware», dass die Regierung Nachrichtendienste oder die Armee einsetzen könnte, um solchen Angriffen entgegen zu wirken[5]. Dies dann, wenn die nationale

[2] https://www.businesswire.com/news/home/20210922005436/en/New-Ponemon-Institute-Research-Shows-Ransomware-Attacks-on-Healthcare-Delivery-Organizations-Can-Lead-to-Increased-Mortality-Rate

[3] https://www.ponemon.org/

[4] https://www.techrepublic.com/article/lawsuit-claims-ransomware-attack-caused-fatal-injury-to-infant-at-alabama-hospital/

[5] https://therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/

Sicherheit gefährdet wäre. Dazu könnte beispielsweise die IT-Infrastruktur der Angreifer «offline» genommen werden. Neben den Nachrichtendiensten könne auch das niederländische «Defense Cyber Command» der Armee Gegenangriffe durchführen.

Cyber-Angriff auf mehrere israelischen Krankenhäuser

Im Oktober teilte das israelische Gesundheitsministerium mit, dass mehrere israelischen Krankenhäuser Ziel von Cyber-Angriffen geworden sind[6]. Die meisten Angriffe wurden jedoch abgewehrt. Das Krankenhaus «Hillel Jaffe» in der Küstenstadt Chadera kämpfte jedoch mehrere Tage mit den Folgen eines Ransomware-Angriffs. Gemäss Medienberichten musste das Personal zeitweise auf alternative Systeme ausweichen und Patientenaufnahmen mit Stift und Papier durchführen. Über den Infektionsvektor, die verwendete Ransomware Familie sowie ob Lösegeld bezahlt wurde ist nicht bekannt.

2021: 83% der Opfer von Ransomware bezahlen Lösegeld

Im Oktober 2021 veröffentliche das IT-Sicherheitsunternehmen «ThycoticCentrify» eine Untersuchung zu Ransomware. Diese kommt zum Schluss, dass 83% der 300 befragten US IT-Unternehmen, welche 2021 Opfer von Ransomware wurden, ein Lösegeld bezahlt haben [7]. Die US-Behörde zur Verfolgung von Finanzkriminalität gibt zudem an[8], dass im ersten Halbjahr in den USA 590 Millionen US-Dollar an Lösegeld durch Ransomware erpresst wurde[9].

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 authentisiert (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

[6] https://www.gov.il/he/departments/news/17102021-01

[7] https://www.darkreading.com/attacks-breaches/2021-state-of-ransomware-report-reveals-83-of-victims-paid-to-get-data-restored

[8] https://www.heise.de/news/Ransomware-Im-ersten-Halbjahr-allein-in-den-USA-590-Millionen-US-Dollar-gezahlt-6220438.html

[9] https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

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

- 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[10], 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.

[10] 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 GovCERT Dienstleistungen:
outreach@govcert.ch