Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
GovCERT.ch

Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

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

Aktuelles (Mai 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.
- Die Ransomware Aktivitäten in der Schweiz führen weiterhin zu beträchtlichen Schäden.
- Es gab «Conti» Ransomware Angriffe gegen Gesundheitssektor unter anderem in den USA[1] und in Irland.
- Cyberangriff auf Spitäler in Neuseeland.
- Cyberkriminelle greifen kritische Infrastruktur in der USA an.
- Erneut kritische Verwundbarkeit in Pulse Connect Secure.

«Conti» Ransomware Angriffe gegen Gesundheitssektor

Die irische Gesundheitsverwaltung (Health Service Executive - HSE) wurde im Mai 2021 Ziel eines erfolgreichen Ransomware Angriffs. Dabei gelang es unbekannten Tätern in das Netzwerk von HSE einzudringen und Systeme mit einer Ransomware namens «Conti» zu verschlüsseln. Der Angriff hat zahlreiche System beeinträchtig, weshalb sich HSE dazu entschlossen hat, temporär sämtliche IT-Systeme herunter zu fahren. Als Folge davon konnten beispielsweise COVID-19 Tests nicht mehr durchgeführt werden. Spitäler mussten zudem bei der Erfassung und Dokumentation von Behandlungen auf Papier umstellen. Am 28. Mai 2021 bestätigte HSE, dass infolge des Angriffs Daten von 520 Patienten entwendet und im Internet publiziert wurden. Gemäss Medienberichten[2] konnte die unbekannte Täterschaft

[1] https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

[2] https://www.bleepingcomputer.com/news/security/irelands-health-services-hit-with-20-million-ransomware-demand/

700G GB Daten entwenden und fordert für diese 20 Millionen USD Lösegeld. Am 27. Mai 2021 äusserte sich Paul Reid, Direktor von HSE, dass sich die Kosten für die Bewältigung des Cyberangriffs wohl auf über 100 Millionen USD belaufen würden[3].

Bei einer Analyse der betroffenen Systeme konnte das irische National Cyber Security Centre NCSC «Cobalt Strike» finden. Dabei handelt es sich um ein kommerzielles Penetration Testing Werkzeug, welches oftmals von Cyberkriminellen für den Einbruch in Unternehmensnetzwerke verwendet wird. NCSC.ch sind dieses Jahr bereits diverse Fälle in der Schweiz bekannt, bei welchen «Cobalt Strike» sowie auch die Ransomware «Conti» dazu verwendet wurden, Unternehmensdaten zu verschlüsseln, diese zu exfitrieren sowie das Opfer damit zu erpressen.

Praktisch zeitgleich zu dem Angriff auf HSE wurde Scripps Health, eine gemeinnütziges Gesundheitssystem mit Sitz in Kalifornien (USA) Ziel der «Conti» Ransomware[4]. Gemäss eigenen Aussagen betreibt Scripps Health fünf Spitäler und 19 ambulante Einrichtungen und behandelt jährlich eine halbe Million Patienten durch 2'600 angeschlossene Ärzte. Auch bei diesem Angriff musste ein Grossteil der Prozesse von digital auf Papier umgeschaltet werden, da Scripps Health viele Systeme vom Netz nahm, um den Angriff einzudämmen. Gemäss eigenen Aussagen konnte der Angriff jedoch detektiert werden, bevor eine Verschlüsselung durch die «Conti» Ransomware stattgefunden hat.

Cyberangriffe auf Spitäler in Neuseeland

Mitte Mai 2021 wurden zahlreiche Spitäler des Waikato District Health Board in Neuseeland Opfer von Cyberangriffen. Offensichtlich gelang es unbekannten Angreifern dabei Daten, darunter scheinbar auch Patientendaten, zu entwenden. Diese wurden Ende Mai 2021 diversen Medienhäusern in Neuseeland zugespielt. Gemäss Aussage des neuseeländischen Gesundheitsministers Andrew Little wurden bei dem Cyberangriff Server mit der Ransomware «Zeppelin» verschlüsselt. Gemäss Medienberichten[5] wurde dabei die Behandlung von Patienten sowie die Lohnabrechnungen während über einer Woche beeinträchtigt. Diverse Prozesse mussten währenddessen temporär von digital auf manuell umgestellt werden. Mittlerweile konnten jedoch über 600 Server wieder in Betrieb genommen werden. Über eine Lösegeldforderung sind derzeit öffentlich keine Informationen bekannt.

«Zeppelin» ist ein «Ransomware-as-a-Service» (RaaS), welche im Darkweb angeboten wird und mit welcher bereits mehrfach Organisationen im Gesundheitswesen angegriffen wurden. Als Infektionsvektor wird in der Regel Malspam verwendet.

Cyberkriminelle greifen kritische Infrastruktur in der USA an

Anfang Monat wurde bekannt, dass Colonial Pipeline, Betreiber des grössten Pipelinesystems für raffinierte Ölprodukte in den USA, Opfer eines Cyberangriffs wurde. Die genauen Umstände waren zunächst unklar, wobei das Unternehmen mittlerweile bekannt gab, es sei Opfer der Ransomware «DarkSide» geworden. Der Cyberangriff hatte weitreichende Folgen: Das Unternehmen musste den Betrieb seiner Pipeline zeitweise komplett einstellen. Dadurch kam es im Osten der USA zu Versorgungsengpässen. In einem Interview mit dem Wall

[3] https://www.irishtimes.com/news/health/cyberattack-hse-faces-final-bill-of-at-least-100m-1.4577076

[4] https://www.bleepingcomputer.com/news/security/health-care-giant-scripps-health-hit-by-ransomware-attack/

[5] https://www.reuters.com/article/us-newzealand-cyber-idCAKCN2D7024

Street Journal räumte Joseph Blount, Chef von Colonial Pipeline, ein, eine Lösegeldzahlung in Höhe von 4,5 Millionen USD geleistet zu haben. Er argumentiert, die Lösegeldzahlung sei im Interesse des Landes richtig gewesen.

Das Ausmass der Cyberattacke sorgte in den USA für Diskussionen. Mitte Mai verkündeten die Hacker hinter «DarkSide», dass diese sich aus dem Geschäft zurückziehen würden. Begründet haben die Hacker diesen Schritt damit, dass sie den Zugang zu Ihrer Infrastruktur verloren hätten. Es ist nicht klar, ob die Infrastruktur durch Strafverfolgungsbehörden vom Netz genommen wurde oder ob die unbekannte Täterschaft hinter «DarkSide» aufgrund des Druckes aus den USA sich dazu entschlossen haben, ihre Tätigkeiten einzustellen oder ob es ein reines Ablenkungsmanöver der Täter ist.

Bei der Analyse der von «DarkSide» verwendeten Bitcoin-Konten konnten Sicherheitsforschen[6] über einen Zeitraum von 9 Monaten Lösegeldzahlungen von 47 Opfern mit einem Volumen von über 90 Millionen USD rekonstruieren.

Nach dem Cyberangriff auf Colonial Pipeline sorgt sich der Präsident des Deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), Arne Schönbohm, um die Cybersicherheit der medizinischen Infrastruktur in Deutschland. In einem Interview mit der Zeit Online[7] sagt er, er sehe eine grössere Gefahr bei Krankenhäusern und verwies dabei auf mehrere Hackerangriffe gegen solche in den vergangenen Jahren.

Während die Cybersicherheitslage betreffend Ransomware in der Schweiz derzeit angespannt ist, sind dem NCSC bislang keine Fälle von «DarkSide» in der Schweiz Fällen bekannt. Der Fall Colonial Pipeline zeigt jedoch einmal mehr, dass auch kritische Infrastrukturen nicht vor Cyberangriffen verschont werden.

Erneut kritische Verwundbarkeit in Pulse Connect Secure

Bereits im April 2021 hat das NCSC.ch vor mehreren kritischen Verwundbarkeiten in Pulse Connect Secure gewarnt. Das Produkt wird von vielen Unternehmen in der Schweiz eingesetzt, um den Fernzugriff auf das Unternehmensnetzwerk zu ermöglichen (VPN). Besonders in Zeiten von COVID-19 werden solche Fernzugänge rege gebraucht und sind daher ein beliebtes Ziel von Cyberkriminellen. Im Mai 2021 wurde nun eine weitere kritische Verwundbarkeit im genannten Produkt bekannt[8], über welche Angreifer SMB-Netzwerkfreigaben einsehen und willkürlich Code ausführen können. Um die Verwundbarkeit auszunutzen muss ein Angreifer sich zuvor jedoch am System erfolgreich authentisieren, weshalb valide Zugangsdaten (Benutzername, Passwort) erforderlich sind.

Verwundbarkeiten in Pulse Connect Secure und ähnlichen Produkten wie beispielsweise Citrix wurden in der Vergangenheit immer wieder von Cyberkriminellen dazu verwendet in Unternehmensnetzwerke einzubrechen, Daten zu stehlen sowie sich lateral im Netzwerk zu bewegen. In vielen Fällen führte dies zu einer Kompromittierung von Unternehmensdaten und einer Verschlüsselung von einem Grossteil der Systeme im Netzwerk des Opfers.

[6] https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin
[7] https://www.heise.de/news/BSI-Chef-sieht-Gefahr-von-Hackerangriffen-auf-Krankenhaeuser-6052664.html
[8] https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44800

Empfehlungen:

Die beiden vorgestellten Angriffe auf den Gesundheitssektor, wie auch anderweitig beobachtete Cyberangriffe auf kritische Infrastrukturen zeigen deutlich, dass zwar einerseits eine hohe Risikoexposition besteht, dass aber andererseits mit relativ einfach umsetzbaren Werkzeugen das Risiko schon beträchtlich reduziert werden kann, insbesondere mit der Absicherung der Gatewaysyteme und einer restriktiven Policy, welche Datentypen per Mail oder Web heruntergeladen und ausgeführt werden dürfen.

- 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

- 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[9], 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.

[9] 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