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

Aktuelles (April 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.
- Wir stellen eine erhöhte Ransomware Aktivität in der Schweiz fest.
- Hohe Risikoexposition durch «0day» Verwundbarkeit in Pulse Connect Secure und SonicWall Email Security (ES) sowie durch die Verwundbarkeiten in MS Exchange.
- Cyber-Kriminelle verkaufen 1'300'000 RDP-Zugangsdaten auf dem Dark Market. Mehrere tausend Organisationen in der Schweiz sind potentiell betroffen.

Erhöhte Ransomware Aktivität in der Schweiz

Im Monat April 2021 wurden dem NCSC ungewöhnlich viele Ransomware-Fälle gemeldet. Vor allem aktiv sind die Ransomware-Familien QLocker, *Avaddon*, *Lockbit*, *Conti*, *Himynameisransom*, *Ryuk*, *Sodinokibi, BlackKingdom* und *Makop*.

Neben dem für Ransomware üblichen Infektionsvektor über schädliche Office-Dokumente in E-Mails wurden dem NCSC auch Fälle gemeldet, bei welchen eine unbekannte Täterschaft das Opfer anruft und sich dabei als Mitarbeiterin eines Zustellservice ausgibt. Daraufhin versucht diese mittels «Social Engineering» an die E-Mail-Adresse des Opfers zukommen. Oftmals verwendet der vermeintliche Zustellservice dazu den Vorwand, dass der Lieferschein per E-Mail zugestellt werde. In der darauffolgenden E-Mail ist ein Link enthalten, welcher zu einem namhaften Anbieter von Cloudspeicherdiensten führt. Öffnet das Opfer die dort angebotene Datei, wird der Computer mit Malware infiziert, welche sogleich «Cobalt Strike» nachlädt. Dies ermöglicht es der Täterschaft, sich lateral im Netzwerk des Opfers zu bewegen, sich Zugang zu weiteren Systemen zu verschaffen und diese schlussendlich mit Ransomware zu verschlüsseln. Oft geht dieser Angriff mit einer Exfiltration der gestohlenen Daten

einher. Das Opfer wird dann zusätzlich damit erpresst, dass diese Daten entweder veröffentlicht oder verkauft werden.

Seit Mitte April läuft zudem eine grosse Ransomware-Kampagne, bei welcher Angreifer versuchen, NAS-Produkte des Herstellers Qnap mit einer Ransomware namens QLocker[1] zu verschlüsseln. Dazu nutzen die Angreifer offenbar eine bereits bekannte Sicherheitslücke in den Add-ons (Apps) Multimedia Console, Media Streaming und Hybrid Backup Sync aus, um Zugang zu QNAP NAS zu erhalten, welche über das Internet erreichbar sind. Innerhalb von nur 5 Tagen hat die unbekannte Täterschaft hinter QLocker gemäss Medienberichten[2] so über 250'000 USD ergaunert.

In der Schweiz gibt es mehrere Dutzend QLocker Vorfällle, oftmals bei KMUs. In einigen Fällen wurde so nicht nur die Dateiablage verschlüsselt, welche sich auf dem NAS-Speicher befand, sondern sogleich auch das Backup, welches ebenfalls auf demselben Medium gespeichert wurde.

«0day» Verwundbarkeiten in Pulse Secure und SonicWall

Nach den kritischen Verwundbarkeiten vom März in Microsoft Exchange sind im April nun zwei weitere Hersteller betroffen[3]. Betroffen sind die Produkte der Hersteller von IT-Sicherheitslösungen «Pulse Secure» und «SonicWall»:

SonicWall Email Security (ES)

Verwundbarkeit	Beschreibung
CVE-2021-20021	Unauthorized administrative account creation
CVE-2021-20022	Post-authentication arbitrary file upload
CVE-2021-20023	Post-authentication arbitrary file read

Pulse Connect Secure

Verwundbarkeit	Beschreibung
CVE-2021-20021	Remote Code Execution (RCE)

Die genannten Verwundbarkeiten sind kritisch und werden gemäss den uns vorliegenden Informationen bereits vereinzelt von Akteuren ausgenutzt, um Zugang zu Unternehmensnetzwerken zu erhalten («0day exploitation»). Dem NCSC sind auch bereits Organisationen in der Schweiz bekannt, deren Netzwerke durch die genannten Verwundbarkeiten übernommen wurden.

Das NCSC weist zudem explizit darauf hin, dass ähnliche Verwundbarkeiten in den vergangenen Monaten von Akteuren dazu verwendet wurden, in Unternehmens-Netzwerke einzudringen und diese mittels Ransomware zu verschlüsseln und grosse Datenbestände zu entwenden, mit welchen das Opfer zusätzlich erpresst werden konnte. Das NCSC schätzt die Gefahr durch die genannten Verwundbarkeiten daher als "sehr hoch" ein.

[1] https://www.qnap.com/en/security-news/2021/response-to-qlocker-ransomware-attacks-take-actions-to-secure-qnap-nas

[2] https://www.bleepingcomputer.com/news/security/a-ransomware-gang-made-260-000-in-5-days-using-the-7zip-utility/

[3] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/news/news-aktuell/pulse-secure-sonicwall.html

1'300'000 RDP-Zugangsdaten verkauft

Im März sind Sicherheitsforscher auf 1'300'000 gestohlene RDP-Zugangsdaten gestossen[4], welche auf einem Dark Marketplace namens «UAS» verkauft wurden. Die Zugangsdaten wurden höchstwahrscheinlich mittels Brute-Force-Angriffen von aus dem Internet erreichbaren RDP-Diensten gewonnen.

Das NCSC hat Kenntnis von mehreren tausend betroffenen Organisationen in der Schweiz. Zu beachten ist jedoch, dass ein Grossteil der Daten bereits mehrere Jahre alt ist. Für die beiden Monate Dezember 2020 und Januar 2021 (neuster Datensatz) hat das NCSC die betroffenen Organisationen in der Schweiz direkt oder über deren Internet Service Provider (ISP) informiert.

Empfehlungen:

- Gegen das Internet hin exponierte Systeme wie RDP, VPN Dienste, etc. müssen stets auf dem aktuellsten 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.
- Falls Sie **SonicWall** Email Security (ES) in Ihrer Organisation verwenden:
  - Stellen Sie sicher, dass das Produkt die aktuellsten Sicherheits-Updates eingespielt hat (Hotfix 10.0.9.6173 bzw. 10.0.9.6177).
- Falls Sie **Pulse Connect Secure** verwenden:
  - Stellen Sie sicher, dass das Produkt mit der aktuellsten Software Version läuft (9.1R.11.4)
- Falls Sie **QNAP** verwenden:
  - Stellen Sie sicher, dass das Produkt mit der aktuellsten Software Version läuft sowie allenfalls installierte Apps / Add-ons ebenfalls auf dem aktuellsten Stand sind.
  - Vermeiden Sie es, das Produkt direkt gegen das Internet hin zu exponieren.
- 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

[4] https://rdpwned.adv-gate.com/

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[5], 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

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