Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	27. November 2020
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN

Aktuelles (November 2020)

Die Situation im Bereich Cyber Sicherheit bleibt aufgrund von aktuellen Angriffen kritische Infrastrukturen und im Speziellen auf Organisationen im Gesundheitssektor sowie den weiterhin hohen COVID19 Neuinfektionen angespannt. So warnte auch das FBI sowie die US Behörde CISA Ende Oktober vor Ransomware Angriffen auf Organisationen im Gesundheitssektor[1].

In der Schweiz beobachten wir nach wie vor eine hohe Intensität von Malspam Wellen, es gibt diverse Ransomware Vorfälle bei kleineren Organisationen (KMUs und Gemeinden) und eine überdurchschnittlich hohe Anzahl an DDoS Angriffen.

Netzstörungen durch DDoS-Angriffe

Seit anfangs November gingen bei der Meldestelle NCSC mehrere Meldungen über verteilte Denial-of-Service-Angriffe (DDoS) auf vom Internet her erreichbare Ressourcen (wie Beispielsweise Online-Services Webauftritte) ein. Bei einem Grossteil der Betroffenen handelt es sich um Unternehmen aus dem Finanzsektor, jedoch wurden vereinzelt auch Unternehmen aus anderen Sektoren angegriffen [2].

Empfehlungen

Das NCSC empfiehlt allen Organisationen im Gesundheitssektor, eine Risikoanalyse zur Exposition ihrer Systeme durchzuführen. Darin sollten folgende Fragen geklärt werden:

- Welche Systeme sind aus dem Internet erreichbar?
- Welche dieser Systeme sind kritisch für die Betriebsprozesse?
- Existieren Notfallpläne für den Fall, dass diese Systeme durch einen DDoS-Angriff

[1] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[2] https://www.20min.ch/story/hacker-greifen-tx-group-an-119923568553

angegriffen werden? Sind die Verantwortlichkeiten (Netzwerk-Technik, Internet Service Provider) geklärt?
- Teilen sich vom Internet her erreichbare Systeme Ressourcen mit Systemen, die kritisch für das Funktionieren der Organisation sind? (z.B. denselben Internet Uplink, dieselbe Firewall)? Gibt es einen Umschaltplan für den Fall, dass durch den Angriff auf die öffentlich zugängliche Ressource andere, interne Systeme in Mitleidenschaft gezogen werden?

Für Business-kritische Systeme empfiehlt das NCSC, einen kommerziellen DDoS-Schutz (DDoS Mitigation Service) zu abonnieren. **Viele Internet Service Provider (ISPs) bieten eine solche Dienstleistung für einen entsprechenden Aufpreis an. Erkundigen Sie sich bei Ihrem Account Manager über die Kosten und den Umfang eines solchen Service.**

Technische Eckdaten:
- Die Angreifer geben sich als «Fancy Bear» oder «»Lazarus aus. In der Tat hat haben diese Angriffe aber nichts mit den genannten Akteuren zu tun.
- Die meisten Angriffe sind volumetrisch und basieren auf der Verwendung von UDP Protokollen mit einem hohen Amplifizierungsfaktor. Die maximalen Traffic Volumina, die wir beobachtet haben, lag zwischen 150Gb/s und 200Gb/s.
- In einigen Fällen haben die Angreifer auch TCP basierte Protokolle verwendet und damit entweder Netzwerkkomponenten zu überlasten versucht (TCP SYN Flood) oder die Anwendungen selbst angegriffen (z.B. mit HTTPs Requests).

Ransomware Angriffe auf Unternehmensnetzwerke

Wie eingehend erwähnt stellen Verschlüsselungstrojaner (sogenannte «Ransomware») weiterhin eine grosse Bedrohung dar – auch für Organisationen aus dem Gesundheitssektor. Viele Akteure sind dazu übergegangen, nicht nur Daten zu verschlüsseln, sondern diese auch zu exfiltrieren und damit ihre Opfer zu erpressen. Gerade bei Gesundheitsdaten, aber auch bei Forschungsdaten kann der verursachte Schaden sehr gross sein. Beiliegend zu diesem Cyber Security Bulletin erhalten Sie eine Liste von aktuellen Indicators Of Compromise (IOCs), welche im Zusammenhang mit solchen Angriffen stehen. **Wir empfehlen Ihnen, Logdateien Ihres Security Perimeters (insb. Web-Proxy, DNS- und Firewall Logs) der letzten 60 Tage auf diese hin zu überprüfen.**

Dateiname	Beschreibung
cobalt_domains.txt	Cobalt Strike botnet C&C Domains
cobalt_ips.txt	Cobalt Strike botnet C&Cs IPs
trickbot.txt	TrickBot C&C IPs (inkl. Port)
emotet.txt	Emotet C&C IPs (inkl. Port)
dridex.txt	Dridex C&C IPs (inkl Port)

- Sollten Sie ausgehenden Netzwerkverkehr zu einer der genannten Cobalt Strike Domains oder IP Adressen detektieren (**any dst port**), melden Sie sich bitte rasch möglichst bei GovCERT (incidents@govcert.ch)
- Sollten Sie ausgehenden Netzwerkverkehr zu einer der genannten TrickBot, Emotet oder Dridex **IP:Port Kombinationen** detektieren, melden Sie sich bitte rasch möglichst beim bei GovCERT (incidents@govcert.ch)

Das Risiko einer Infektion mit Malware kann durch den Einsatz des **MELANI BGP Feeds** sowie der Response Policy Zone (RPZ) oder des **Secure DNS Resolvers** reduziert werden. Die genannten Services werden kostenlos angeboten. Für weitere Informationen wenden Sie sich bitte an das GovCERT: outreach@govcert.ch

Technische Eckdaten:

- Der initiale Angriffsvektor für Ransomware sind weiterhin **oftmals E-Mails mit bösartigen Dateianhängen oder Links**, welche zu einem den Malware Download führen. Das Risiko von Malware Downloads können durch den Einsatz von Beispielsweise URLhaus[3] reduziert werden.
- Auch Remote Zugänge wie Beispielswiese **Citrix, RDP und VPN** sind weiterhin beliebte Angriffsvektore. Solche müssen **konsequent auf dem aktuellen Patchlevel gehalten werden und mit einer zwei-Faktor-Authentifizierung abgesichert** werden.
- Die Angreifer bewegen sich lateral, sobald sie einen initialen Zugang zum Netzwerk des Opfers haben. Das heisst, dass Infektionen mit Emotet, Trickbot oder anderer Malware sehr ernst genommen werden muss und, bei einer möglichen Infektion, eine Analyse bezüglich einer möglichen Ausbreitung im Netzwerk und in Richtung Active Directory geprüft werden muss.
- Warnmeldungen von Antivirenprodukten in Bezug von Angriffswerkzeugen wie Mimikatz, Metasploit oder Powershell Empire sind Hinweise auf eine tiefer gehende Kompromittierung des Netzwerks.

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 NCSC Services:
outreach@govcert.ch

[3] https://urlhaus.abuse.ch/api/