Cyber-Sicherheit und Risikoexposition von Spitälern in der ausserordentlichen Lage

NUR FÜR DEN INTERNEN GEBRAUCH

Datum: 17. März 2020
Author: NCSC/GovCERT.ch
Kontakt: outreach@govcert.ch
Verteiler: Gesundheitssektor MELANI, H+, HIN

Ausgangslage

Durch das Verschicken von gefälschten Informationen (E-Mails mit Malware oder Phishing Mails) können Angreifer versuchen, Zugang zu Spitälern zu erlangen. Bisher haben wir vor allem ungezielte Angriffe mit Information Stehlern (z.B. Hawkeye, AgentTesla) gesehen, prinzipiell können dies aber auch für gezielte Angriffe verwendet werden. Durch die hohe Arbeitslast in den Spitälern werden Fehlmanipulationen, gerade im Bereich der IT höher und die Auswirkungen sind gravierender. Zusätzliche Massnahmen sind im Moment schwierig umzusetzen und müssen genau abgewogen werden, da diese durch das Implementationsrisiko auch selbst eine Störung verursachen können. Durch den verstärkten Einsatz von Home-Office aufgrund der aktuellen Situation verändert sich die Angriffsfläche ebenfalls. Die Geräte zu Hause sind weniger gut geschützt und haben eine geringere Überwachung durch das IT-Security Team der Organisationen. Die Nutzung von Remote Access Gateways (RAS) erhöht das Risiko von erfolgreichen Phishing-Angriffen, sowie weiteren Angriffen auf Passwörter (z.B. Dictionary[1], Password Spray[2] und Bruteforce Attacks[3]) beträchtlich, insbesondere falls nur ein einzelner Faktor zur Authentisierung zum Einsatz kommt.

[1] https://en.wikipedia.org/wiki/Dictionary_attack
[2] https://www.triaxiomsecurity.com/2018/11/08/password-spraying-attack/
[3] https://attack.mitre.org/techniques/T1110/

Das vorliegende Dokument versucht, in konzentrierter Form einige zentrale Punkte für den Schutz vor Phishing, Malware und vor lateralen Bewegungen aufzuzeigen. Es gibt darüber hinaus eine Vielzahl von Information von MELANI (anlässlich der Gesundheitsworkshops), sowie Publikationen auf MELANI-NET (nur geschlossener Kundenkreis von MELANI), der MELANI Homepage und dem Blog von NCSC/GovCERT sowie von weiteren Organisationen wie z.B. dem Deutschen BSI oder dem französischen ANSSI, welche weitergehende und vertiefte Massnahmen auflisten.

Prävention

Technisch

Präventive, technische Massnahmen sind zum jetzigen Zeitpunkt schwierig zu empfehlen und umzusetzen. Es gibt dennoch einige, die zumindest prüfenswert sind:

- Überprüfen der Einstellungen auf dem Mailserver in Bezug gefährlicher Dateien. Eingehende E-Mails mit folgenden Dateiendungen sollten generell blockiert werden[4].
- Überprüfen der Backup Strategien: Gibt es offline kopien der absolut kritischen Daten, evtl. besonders in Bezug von COVID-19?
    - Gibt es die Möglichkeit, besonders kritische Daten auf WORM Medien zu schreiben?
    - Gibt es die Möglichkeit, aktuelle Patientendaten auf einem zweiten, vom Internet komplett abgetrennten System vorzuhalten?
- Home-Office:
    - Ist eine 2 Faktor Authentifizierung im Einsatz (z.B: SMS, Authenticator, RSA-Token)? Falls nein, gibt es die Möglichkeit einer GeoIP Restriction einzufügen, um nur IP Adressen aus der Schweiz zulassen? Werden die Logs auf viele *failed Logins* gefolgt von einem erfolgreichen Login überwacht?
    - Falls dies die Netzwerk-Performance zulässt, sollte auf allen Geräten ein Zwangstunneling eingesetzt werden, so dass sämtlicher Traffic durch die Schutz- und Detektionsinfrastruktur der Organisation geleitet wird. Alternativ kann ein «Cloud-Proxy» eines IT-Sicherheitsanbieters in Betracht gezogen werden. Dies ist umso wichtiger, da der starke Fokus auf Home-Office sowie die Krisensituation vermutlich zu einer Zunahme von Phishing Versuchen führen wird.
- Für Kritische Infrastrukturen: Mit dem ISP vereinbaren, dass Emotet/TrickBot und MELBL BGP Feed implementiert sind.

[4] https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/assets/blocked-filetypes.txt

Für Nicht Kritische Infrastrukturen: Kontaktaufnahme mit incidents@govcert.ch für Hinweise zur Implementierung der Sperrlisten.

- Falls schon Sperrlisten auf Proxies vorhanden sind und diese ohne grösseren Change umsetzbar sind:
    - Implementierung von der MELANI Botnetz Liste (MELBL).[5] Kontakt: incidents@govcert.ch
    - URLHaus Blockliste:
      https://urlhaus.abuse.ch/api/
      Feodo Tracker Blocklist:
      https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt
    - Spamhaus Don't Route Or Peer List (DROP):
      https://www.spamhaus.org/drop/
    - Optional: schlecht bewertete TLDs:
      https://www.spamhaus.org/statistics/tlds/
- Ein weiterer Schritt ist das blockieren von Web Webseiten, welche durch den Proxyhersteller (noch) nicht klassifiziert wurden, d.h. noch nicht kategorisiert sind. Diese Massnahme wird Zusatzarbeit generieren, ist gleichzeitig aber auch effizient.

Ansonsten gelten die anlässlich der Workshops für kritische Infrastrukturen gemachten Empfehlungen, sowie die von MELANI und GovCERT veröffentlichten Ratschläge:

Blog «Severe Ransomware Attacks Against Swiss SMEs»:
https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/

Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs:
https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/sicherheitsrisiko-durch-ransomware.html

Merkblatt Informationssicherheit für KMUs:
https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

Organisatorisch

Hier steht primär die Information im Fokus:

- Allfällige Phishing Awareness sollten ausgesetzt werden, bis sich die Situation beruhigt hat

[5]

- In den meisten Organisationen gibt es bereits COVID-19 Kampagnen. Diese können mit folgendem Zusatz (z.B. ein PostIT auf das Plakat) ergänzt werden:

Kriminelle und staatliche Akteure versuchen die Aufmerksamkeit, welche COVID-19 verursacht, auch für ihre Zwecke zu nutzen und verschicken im Namen von Gesundheitsorganisationen Schadsoftware. Seien Sie vorsichtig beim Öffnen von Dokumenten, welche Sie via E-Mail erhalten haben, und aktivieren Sie keinesfalls die darin enthaltenen Makros. Fragen Sie im Zweifelsfalle bei Ihrem Helpdesk oder Ihrem IT-Security Team nach.

Detektion

Technisch

Können die von NCSC/GovCERT bereitgestellten Blacklists (oder auch andere Quellen) nicht präventiv durch Blockierung eingesetzt werden, bietet es sich an, diese in das Logmonitoring zu integrieren. So wird zwar eine Initialinfektion nicht verhindert, aber bei einer entsprechend schnellen Reaktion kann die laterale Bewegung oft noch verhindert werden. Darüber hinaus bietet sich der Einsatz eines leichtgewichtigen Detektionssystems wie z.B. passiveDNS von NCSC/GovCERT oder ein Suricata (Intrusion Detection System - IDS) ebenfalls an. Auf der Ebene der Endgeräte wie Notebooks und PCs sollte der Einsatz von Sysmon (in Sysinternals Suite von Microsoft enthalten) geprüft werden (wobei hier wiederum das Implementationsrisiko während der Krisensituation zu beachten ist).

Verdächtige E-Mails, Dateianhänge oder Links können jederzeit an incidents@govcert.ch zur Analyse geschickt werden.

Organisatorisch

MitarbeiterInnen gehören zu den wichtigsten Sensoren überhaupt. Sie sollten verdächtige Aktivitäten wie E-Mails immer melden. Idealerweise wird ein Spam-Meldebutton (in Outlook) eingesetzt, mit welchem MitarbeiterInnen auf einfache Weise verdächtige E-Mails an eine zentrale Stelle senden können.

Reaktion

Technisch

Werden Geräte infiziert, sind weitere Abklärungen nötig. Informieren Sie in diesem Falle unbedingt rasch möglichst Ihren IT-Dienstleister und/oder NCSC/GovCERT.ch. Es muss abgeklärt werden, ob es sich um einen Dropper handelt, welcher dafür bekannt ist, dass danach bei gewissen Zielen eine laterale Bewegung erfolgt (z.B. Emotet/Trickbot, OSTAP, Get2/SDBBot). In solchen Fällen muss immer eine vertiefte Analyse gemacht werden, ob bereits eine laterale Bewegung erfolgt ist. Im Zweifelsfalle und/oder falls der Verdacht besteht, dass bereits eine laterale Bewegung erfolgt ist (d.h., dass der Angreifer sich bereits im Netz auf andere Geräte ausgebreitet hat), kann NCSC/GovCERT zur Unterstützung beigezogen werden. Ist bereits ein Schaden entstanden, z.B. durch einen Angriff aufs Active Directory oder durch Verschlüsselung von Daten, sollte ebenfalls NCSC/GovCERT möglichst rasch beigezogen werden.

Organisatorisch

Es empfiehlt sich, intern offen zu informieren und gegen aussen ein Kommunikationskonzept zu haben, das so offen und transparent wie möglich auftritt, um allfälligen Gerüchten effektiv begegnen zu können. Der Incident Response auf operativer Ebene muss von dem technischen Schutzgedanken geleitet sein und soll so gemacht werden, dass Daten soweit erhalten bleiben, dass auch zu einem späteren Zeitpunkt Strafanzeige gestellt werden kann. Wir empfehlen generell, Strafanzeige zu erstatten, sobald eine laterale Bewegung festgestellt worden ist und/oder Schaden entstanden ist.

Kontaktaufnahme

Im Falle eines IT-Sicherheitsvorfalles, von verdächtigen E-Mails, etc:

E-Mail: incidents@govcert.ch

Pikett-Telefon: +41 79 152 20 80 (**nur in Notfällen!**)

Für Rückfragen technischer Art: outreach@govcert.ch