Cyber-Sécurité et Exposition aux Risques des Hôpitaux en Situation Exceptionnelle

POUR USAGE INTERNE UNIQUEMENT

Date : 17 mars 2020
Auteur : NCSC/GovCERT.ch
Contact : outreach@govcert.ch
Distributeur : Secteur de la Santé MELANI, H+, HIN

Situation Initiale

Les criminels usent de divers stratagèmes, tels que l'envoi de fausses informations (courriels contenant des logiciels malveillants ou des courriels de phishing) pour tenter d'accéder aux réseaux ou données d'hôpitaux. NCSC/GovCERT.ch observe actuellement surtout des attaques non ciblées, utilisant des maliciel spécialisés dans le vol d'information tels que Hawkeye ou AgentTesla. Ce type de malware peut cependant également être utilisés lors d'attaques ciblées. En raison de la charge de travail élevée dans les hôpitaux, les manipulations incorrectes, en particulier dans le domaine informatique, sont plus nombreuses et les effets plus sérieux. Des mesures de sécurité supplémentaires sont délicates à mettre en œuvre actuellement et doivent soigneusement être étudiées, car tout changement comporte des risques et peut également contribuer à des perturbations. L'utilisation accrue du travail à domicile en raison de la situation actuelle modifie également la surface d'attaque. Les appareils à la maison sont moins bien protégés et moins surveillés par l'équipe de sécurité informatique des organisations. L'utilisation de passerelles d'accès à distance (RAS) augmente considérablement le risque de réussite des attaques de phishing et autres attaques sur les mots de passe (par exemple, attaques par dictionnaire,[1] « Password Spraying »[2] ou attaque par brute force[3]), notamment quand un seul facteur est utilisé pour l'authentification.

[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/

Le présent document tente de présenter, sous une forme concentrée, quelques points centraux de protection contre le phishing, les logiciels malveillants et les mouvements latéraux. Ces sujets sont approfondis dans un grand nombre d'informations provenant de MELANI (par exemple à l'occasion des ateliers dans le Secteur de la Santé), dans les publications sur MELANI-NET (uniquement pour le cercle fermé des clients de MELANI), la page d'accueil de MELANI, le blog du NCSC/GovCERT.ch ainsi que de nombreuses autres organisations telle que le BSI allemand ou l'ANSSI française.

Prévention

Au Niveau Technique

Des mesures techniques préventives sont difficiles à recommander et à mettre en œuvre à l'heure actuelle. Néanmoins, certaines méritent d'être considérées :

- Vérifiez les paramètres du serveur de messagerie concernant les fichiers dangereux. Les courriers électroniques entrants portant les extensions de fichier suivantes doivent généralement être bloqués[4].
- Vérification des stratégies de sauvegarde : existe-t-il des copies hors ligne des données absolument critiques, peut-être surtout en ce qui concerne COVID-19 ?
    - Est-il possible d'écrire des données particulièrement critiques sur des supports de type WORM ?
    - Est-il possible de conserver les données actuelles des patients sur un second système complètement séparé de l'Internet ?
- Travail à domicile / distant :
    - Une authentification à deux facteurs est-elle utilisée (par exemple, SMS, Authenticator, RSA-Token) ? Si tel n'est pas le cas, est-il possible d'implémenter une restriction de type « GeoIP » pour n'autoriser que les adresses IP provenant de Suisse ? Les journaux de logs sont-ils surveillés pour détecter de nombreux échecs de connexion finalement suivis d'une connexion réussie ?
    - Si possible (tenez compte de la bande passante et des ressources des systèmes impactés) faites transiter tout le trafic réseau des ordinateurs portables et des tablettes via la solution de tunnel sécurisée (VPN) de l'entreprise, afin de bénéficier de l'infrastructure de protection et de détection de l'organisation.

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

- Pour les infrastructures critiques : vérifiez avec le fournisseur d'accès à Internet (FAI) que ce dernier mette bien en œuvre la protection MELBL BGP ainsi qu'un flux contre Emotet/TrickBot.
- Pour les infrastructures non critiques : contactez incidents@govcert.ch pour obtenir des conseils sur la mise en œuvre de telles listes noires.
- Si les serveurs de proxy supportent des listes de blocage et que ces dernières peuvent être mises en œuvre sans changements majeurs :
    - Mise en œuvre de la liste MELANI Botnet List (MELBL).[5]
      Contact : incidents@govcert.ch
    - Liste de blocage de URLHaus :
      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/
    - Facultatif – Liste des TLD mal notés :
      https://www.spamhaus.org/statistics/tlds/
- Une étape supplémentaire consiste à bloquer les pages web qui n'ont pas (encore) été classifiées par le fabricant du proxy, c'est-à-dire qui n'ont pas encore été catégorisées. Cette mesure génère du travail supplémentaire, mais elle est également efficace.

Par ailleurs, les recommandations formulées lors des ateliers sur les infrastructures critiques et les avis publiés par MELANI et GovCERT s'appliquent :

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

« Prudence : un nombre croissant de PME victimes de rançongiciels » :
https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/sicherheitsrisiko-durch-ransomware.html

« Sécurité de l'information : aide-mémoire pour les PME » :
https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

---

5

Au Niveau Organisationnel

L'accent doit principalement être mis sur l'information :

- Toute sensibilisation à l'hameçonnage devrait être suspendue jusqu'à ce que la situation se soit calmée
- Dans la plupart des organisations, il existe déjà des campagnes COVID-19. Celles-ci peuvent être complétées par le message suivant - par exemple par l'ajout d'un « Post-it » sur l'affiche :

Des criminels et des acteurs étatiques tentent d'exploiter l'attention que COVID-19 suscite et envoient des logiciels malveillants au nom d'organisations de santé. Soyez prudent lorsque vous ouvrez des documents que vous avez reçus par courrier électronique, SMS ou n'importe quel type de messagerie et n'activez pas les macros qu'ils contiennent. En cas de doute, demandez à votre service d'assistance ou à votre équipe de sécurité informatique.

Détection

Au Niveau Technique

Si les listes noires fournies par NCSC/GovCERT.ch (ou d'autres sources) ne peuvent pas être utilisées de manière préventive en mode bloquant, considérez leur intégration dans la surveillance des journaux pour une détection à postériori. Bien qu'une telle mesure n'empêche pas l'infection initiale, une rapide réponse suite à un incident limite voire évite le mouvement latéral des attaquants. En outre, l'utilisation d'un système de détection léger tel que le passiveDNS de NCSC/GovCERT.ch ou un Intrusion Detection System (IDS) tel que Suricata est également une option. Au niveau des terminaux (ordinateurs portables et PC), l'utilisation de Sysmon, inclus dans la suite Sysinternals de Microsoft, devrait être examinée, sans cependant oublier le risque de mise en œuvre d'une telle solution en situation de crise.

Les e-mails, pièces jointes ou liens suspicieux peuvent être envoyés en tout temps pour analyse à incidents@govcert.ch.

Au Niveau Organisationnel

Les employés sont les mieux placés pour détecter et signaler toute activité inhabituelle ou suspicieuse, telles que les courriers électroniques malicieux. L'idéal est d'utiliser un bouton de signalement de spam (dans Outlook), permettant aux employés d'envoyer facilement des e-mails suspects à une entité centrale pour analyse.

Réaction

Au Niveau Technique

En cas d'incident de sécurité IT, informez immédiatement votre fournisseur de service informatique et/ou NCSC/GovCERT.ch. Toute infection doit être étudiée, notamment pour clarifier la nature de la menace détectée. La détection d'un « dropper » tel que Emotet/Trickbot, OSTAP ou Get2/SDBBot nécessite par exemple une enquête approfondie pour identifier si le maliciel a déjà installé d'autres composants ou s'il s'est déjà manuellement ou automatiquement propagé dans le réseau de la victime. NCSC/GovCERT.ch peut soutenir les investigations, que ce soit en cas de doute sur une infection ou de son ampleur. NCSC/GovCERT.ch doit immédiatement être informé en cas de dommage important avéré, tel qu'une compromission de l'Active Directory ou le déploiement de rançongiciels.

Au Niveau Organisationnel

Il est conseillé de communiquer ouvertement en interne et d'avoir un concept de communication externe aussi ouvert et transparent que possible afin de contrer efficacement toute rumeur. La réponse à incidents au niveau opérationnel doit être guidée par l'idée de préservation technique, notamment par rapport aux données et traces devant être conservées adéquatement pour permettre d'ultérieures poursuites pénales. De manière générale, nous recommandons un dépôt de plainte dès qu'un mouvement latéral a été détecté et/ou qu'un dommage est survenu.

Coordonnées NCSC/GovCERT.ch

En cas d'incident de sécurité informatique, de courriers électroniques suspects, etc. :

Courrier électronique : incidents@govcert.ch

Téléphone de garde : +41 79 152 20 80 (**uniquement en cas d'urgence !**)

Pour tout autres questions de nature technique : outreach@govcert.ch