Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Unité de pilotage informatique de la Confédération UPIC
Service de renseignement de la Confédération SRC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI
www.melani.admin.ch

SÛRETÉ DE L'INFORMATION

SITUATION EN SUISSE ET SUR LE PLAN INTERNATIONAL

Rapport semestriel 2015/I (janvier à juin)

29 OCTOBRE 2015

CENTRALE D'ENREGISTREMENT ET D'ANALYSE POUR LA SÛRETÉ DE L'INFORMATION MELANI
http://www.melani.admin.ch

1 Aperçu / Sommaire

2 Editorial

Pascal Lamia, 48 ans, dirige depuis 2008 la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI.

Chère lectrice, cher lecteur,

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a soufflé ses dix bougies le 1er octobre 2014. D'innombrables cas nous ont été signalés durant cette première décennie. Des banales tentatives d'escroquerie aux attaques ciblées et raffinées d'espionnage, MELANI a ainsi acquis une vaste expérience. De même, bien des exploitants d'infrastructures critiques ont bénéficié depuis 2004 de notre soutien dans les domaines de la prévention et de la lutte contre les cyberattaques.

MELANI doit son succès essentiellement au secteur privé. Sans le fructueux partenariat public-privé mis en place par la Confédération, la Centrale MELANI n'aurait jamais réussi à atteindre ses objectifs. Je tiens donc à exprimer ma vive gratitude à toutes les personnes issues tant de l'administration que du secteur privé qui ont permis à MELANI de devenir, en dix ans, ce qu'elle est aujourd'hui.

Le début de la deuxième décennie d'existence de MELANI nous a incités à faire peau neuve. Le nouvel emblème adopté symbolise tout d'abord les flux mondiaux de données numériques. Ensuite, il illustre les réseaux internationaux. Sans un solide réseau personnel, mis en place avec des organisations partenaires dans le monde entier, il serait impensable à l'heure actuelle de combattre efficacement les cybermenaces.

Pour bien marquer le cap des dix ans franchi par MELANI, le présent rapport semestriel a lui aussi évolué: sa structure a été entièrement remaniée, afin d'en rendre la lecture encore plus simple et plus agréable.

Je vous souhaite beaucoup de plaisir à lire ce nouveau rapport.

Pascal Lamia

3 Thème prioritaire: sécurité des sites Internet

Internet a connu un formidable essor depuis quinze ans. Des milliers de nouveaux sites Web sont mis en ligne chaque jour. Selon Netcraft[1], on trouve aujourd'hui plus de 850 millions de sites Web actifs. L'une des raison de cet essor tient à l'usage de systèmes de gestion de contenu (*content management system, CMS)* comme WordPress, Typo3, Joomla ! et Drupal. Un CMS permet aux internautes de publier très facilement des contenus dans Internet, sans avoir besoin de solides connaissances en informatique. En outre, les nombreux plugiciels (*plug-in*) mis à disposition permettent de personnaliser les sites Web. La convivialité des CMS fait que les administrateurs de sites amateurs, mais aussi de petites et moyennes entreprises (PME), aiment s'en servir pour publier leurs informations dans Internet.

D'un côté, un *CMS* s'avère très pratique, de l'autre il est une cible de choix pour les pirates informatiques. Une grande partie des pages de *phishing* (hameçonnage) et des infections par *drive-by download* sont placées sur des sites Web administrés par des CMS n'ayant pas été actualisés. Comme beaucoup de programmes, les CMS présentent régulièrement des failles de sécurité, pour lesquelles les fabricants fournissent en général très vite des mises à jour de sécurité. En 2014, pas moins de quatorze failles de sécurité ont été découvertes et corrigées dans le logiciel CMS Drupal, neuf dans Joomla!, et même 29 dans Wordpress.[2] Or il existe des outils permettant de détecter et d'attaquer automatiquement les sites Web vulnérables. Les escrocs ont donc beau jeu de repérer et de manipuler de très nombreux sites Web. Il est donc essentiel que chaque exploitant de site Web actualise régulièrement son logiciel CMS (*patching*) – activité trop souvent négligée. Les administrateurs utilisant un CMS désuet (et donc peu sûr) ne font pas seulement courir des risques aux autres internautes, mais en prennent eux-mêmes: au premier semestre 2015, plusieurs cas dans lesquels des CMS obsolètes avaient été compromis ont été signalés à MELANI. Les escrocs avaient copié les données trouvées dans le CMS, puis s'en étaient servis comme moyen de chantage contre le propriétaire du site. Les PME sont d'autant plus menacées que beaucoup de CMS renferment aussi des données de clients.

Les fabricants fournissent en général rapidement des mises à jour destinées aux CMS. Or à la différence de la plupart des systèmes d'exploitation, le processus n'est pas automatisé et l'exploitant doit souvent le lancer manuellement. Malheureusement, on constate qu'une grande partie des exploitants de sites Web utilisant un CMS l'installent une fois pour toutes, puis exploitent pendant des années la même version du système (généralement désuète et peu sûre). Les exemples qui suivent de vulnérabilités de Wordpress – transposables par analogie aux autres CMS – illustrent ce comportement négligent.

70 % des installations Wordpress suisses sont vulnérables

Une faille de WordPress révélée en avril 2015 permettait à un agresseur d'opérer une attaque de type *cross-site scripting (XSS)* contre les sites Web vulnérables, en y postant un commentaire avec un *JavaScript* spécialement préparé (CVE-2015-3429). Wordpress a publié le même jour une mise à jour de sécurité pour corriger cette vulnérabilité. Le 6 mai 2015, une autre vulnérabilité de Wordpress a été rendue publique, permettant à nouveau à une personne malveillante d'exécuter une attaque de type XSS contre WordPress (CVE-2015-3440). Là encore, Wordpress proposait une mise à jour dès le lendemain.

[1] http://news.netcraft.com/archives/2015/08/13/august-2015-web-server-survey.html (état: le 31 août 2015).

[2] https://cve.mitre.org (état: le 31 août 2015).

Les réactions des exploitants concernés ont été terriblement lentes. En Suisse 6 % des sites Web sont des sites Wordpress. Malgré les mises à jour de sécurité publiées, plus de 70 % de ces sites sont restés vulnérables.[3]

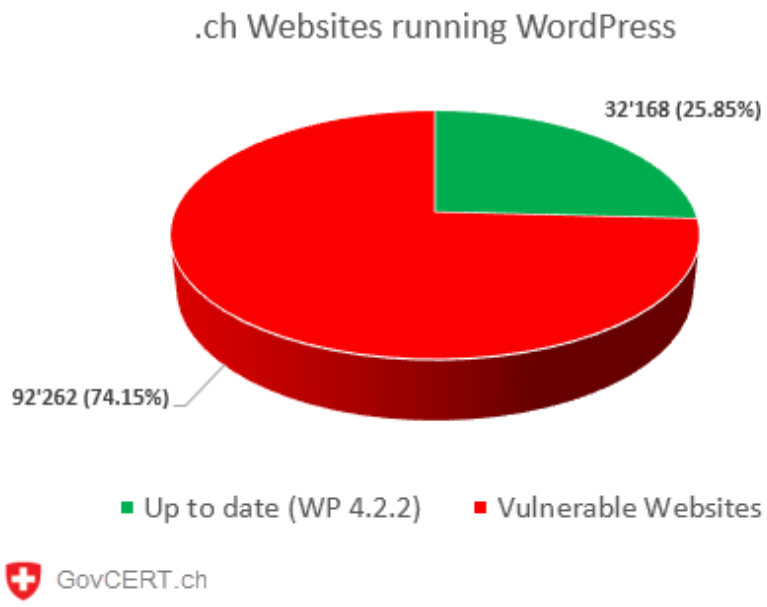


Fig. 1: Pourcentage des utilisateurs de Wordpress vulnérables aux failles CVE-2015-3440 et CVE-2015-3429 (en rouge), deux mois après la publication des correctifs de sécurité correspondants.

Des mises à jour régulières s'imposent – et d'autres mesures également !

Les conclusions de l'analyse menée par MELANI inquiètent et amènent à se demander pourquoi tant d'exploitants de sites Web utilisent des versions vulnérables de CMS. Outre le manque de sensibilité à cet enjeu et l'absence de temps à consacrer à leur système, cela tient aussi à la loi du moindre effort. Beaucoup de gens ne voient pas la nécessité de corriger leur CMS, ou ignorent les conséquences qu'une installation vulnérable peut avoir. Pourtant, la gestion d'un CMS implique une certaine responsabilité, qu'il s'agit d'assumer. Outre la reprise des mises à jour de sécurité dès leur publication (*patch management*), d'autres mesures sont susceptibles d'améliorer la sécurité des systèmes CMS:

- **Authentification à deux facteurs**

  En plus de l'authentification habituelle (nom d'utilisateur et mot de passe) pour l'accès à l'interface d'administration, MELANI recommande la mise en place d'une authentification à deux facteurs. Ce mot de passe unique (ou OTP pour « One Time Password ») peut par exemple être implémenté avec « Google Authenticator ». Une application est alors installée sur un téléphone mobile (Androïd, iOS, Blackberry), qui va générer un nouveau OTP tous les 60 secondes. Sur le webserver (CMS), Google Authenticator peut être implémenté à travers un module (« plug-in »), existant déjà pour de nombreux CMS comme par exemple Wordpress ou Typo3.

[3] GovCERT.ch Blog-Post: «Outdate WordPress: Thousands of websites in Switzerland are vulnerable». http://www.govcert.admin.ch/blog/8/outdate-wordpress-thousands-of-websites-in-switzerland-are-vulnerable (état: le 31 août 2015).

- **Limitation de l’accès administrateur à certaines adresses IP**

  Une telle limitation peut se baser sur des adresses IP précises, des plages d’adresses ou sur leur géolocalisation. Des modules spécifiques existent déjà pour de nombreux CMS.

- **Limitation de l’accès administrateur par des fichiers .htaccess avec le serveur Apache**

  Ceci présente l’avantage de ne pas uniquement permettre la limitation à une plage d’adresses IP, mais également une authentification supplémentaire (nom d’utilisateur et mot de passe) basique.

- **Sécurisation de la machine du webmaster**

  Les sites web et les CMS sont souvent également compromis à travers le vol de données d’accès FTP. Cela arrive souvent par l’entremise d’un cheval de Troie se trouvant sur la machine du webmaster. Il appartient donc à ce dernier d’éviter qu’une telle infection ne se produise et de se protéger à l’aide d’un logiciel antivirus à jour. Par ailleurs, il est recommandé lorsque cela est possible de chiffrer les communications FTP (utilisation de sFTP).

- **Web Application Firewall.**

  Les attaques depuis le web sont blocables à l’aide d’un « Web application Firewall » (WAF), avant que ces dernières n’atteignent l’application visée. Il existe différentes solutions, la plus connue parmi les solutions open source étant ModSecurity.

- **Détection précoce des failles de sécurité**

  Le but est ici de détecter les failles de sécurité potentielles sur son site avant que les criminels ne le fassent. Différentes solutions, payantes comme gratuites, sont disponibles sur Internet.

Des instructions avec des listes de contrôle sont téléchargeables sur le site www.melani.admin.ch:

Mesures de prévention pour les systèmes de gestion de contenu (CMS):

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-prevention-pour-les-systemes-de-gestion-de-contenu--c.html

Vous y trouverez en outre des instructions avec une liste de contrôle des mesures à prendre, au cas où vous auriez déjà été victime d’une cyberattaque:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/instructions-relatives-a-la-suppression-des-maliciels-sur-les-si.html

4 Situation nationale

4.1 Espionnage

Au premier semestre, deux affaires d'espionnage concernant la Suisse soit directement, soit à titre indirect ont éveillé l'intérêt public. Il faut distinguer à chaque fois si l'attaque vise une cible spécifique en Suisse, ou si les infrastructures suisses servent de base à des activités d'espionnage menées contre des tiers. Il est évident que dans le domaine de l'espionnage, tous les cas ne sont pas rendus publics. Expérience à l'appui, les entreprises victimes d'espionnage économique se montrent très réservées, craignant pour leur réputation. De façon générale, on constate que les données sensibles restent très convoitées et que la pression ne se relâche pas. Un cas survenu au premier semestre 2015 a fait grand bruit, soit la découverte et la publication du maliciel Duqu2, qui aurait servi dans le contexte des négociations sur le nucléaire avec l'Iran.

4.1.1 Duqu reloaded: logiciel d'espionnage raffiné contre les participants aux négociations sur le nucléaire avec l'Iran

En mars 2015, le Wall Street Journal révélait, en s'appuyant sur des sources provenant de la Maison Blanche, que des pourparlers confidentiels américains liés à l'accord nucléaire avec l'Iran avaient été espionnés. Les soupçons des Etats-Unis se sont portés sur Israël.[4,5] Mais des politiciens israéliens ont immédiatement et vivement démenti toute implication de leur pays. Le 10 juin 2015, l'entreprise de sécurité informatique Kaspersky a indiqué qu'un virus espion s'en était pris non seulement à ses propres serveurs, mais avait également ciblé différents sites où avaient lieu les discussions sur le nucléaire avec l'Iran. Le maliciel renfermait en partie des passages «très similaires voire presque identiques»[6] au maliciel Duqu révélé en 2011, et était également apparenté à Stuxnet. Ce qui a conduit Kaspersky à le baptiser Duqu2. Toutefois, comme lors de presque tous les incidents d'espionnage, les méthodes d'attaque révélées par les analyses techniques n'ont pas permis de tirer des conclusions claires quant à leur auteur.

Dans les cas rendus publics, les cibles étaient notamment les festivités du 70e anniversaire de la libération du camp d'Auschwitz-Birkenau et les entretiens du P5+1 sur le programme nucléaire iranien. Sur trois des sites ayant accueilli les réunions du P5+1, des experts informatiques ont découvert le maliciel. Les dernières séances de négociations se sont tenues à Lausanne, Montreux, Genève, Munich et Vienne.[7]

En Suisse, le Conseil fédéral a chargé le Ministère public de la Confédération dès le 6 mai 2015, sur la base d'indices transmis par le Service de renseignement de la Confédération (SRC), d'ouvrir dans cette affaire une procédure pénale contre inconnu[8]. Une perquisition réalisée à la mi-mai a abouti à la saisie de différents appareils à Genève.[9] En Autriche aussi, les autorités ont ouvert une enquête pour espionnage présumé, concentrant leurs efforts sur

---

4 http://www.wsj.com/articles/israel-spied-on-iran-talks-1427164201 (état: le 31 août 2015).

5 http://www.theguardian.com/world/2015/mar/24/israel-spied-on-us-over-iran-nuclear-talks (état: le 31 août 2015).

6 http://www.zeit.de/digital/internet/2015-06/duqu-2-kaspersky-labs (état: le 31 août 2015).

7 http://www.kaspersky.com/about/news/virus/2015/Duqu-is-back (état: le 31 août 2015).

8 http://www.heise.de/newsticker/meldung/Kaspersky-Trojaner-hatte-auch-Atomverhandlungen-im-Visier-2689929.html (état: le 31 août 2015).

9 http://www.rts.ch/info/suisse/6856954-les-hotels-abritant-les-negociations-sur-le-nucleaire-iranien-espionnes.html (état: le 31 août 2015).

l'hôtel Palais Coburg à Vienne, où s'étaient tenues plusieurs réunions au cours des négociations sur le nucléaire iranien.[10]

Dans cette affaire, le logiciel ne s'en prend plus seulement aux cibles proprement dites, mais a aussi directement attaqué l'entreprise de sécurité informatique Kaspersky. Les agresseurs semblent avoir épluché le réseau de cette société, afin d'y découvrir des données utiles à leur attaque contre les cibles convoitées. Les entreprises de sécurité IT représentent un pilier essentiel de la confiance de base envers Internet. En cherchant à les compromettre pour atteindre d'autres cibles, on nuit fortement aux efforts visant à assurer qu'Internet soit un moyen de communication fiable, en particulier pour les activités économiques. Il faudra certainement aborder à l'avenir la mise en place de garde-fous sur ce terrain.

D'autres informations sont disponibles dans le chapitre 5.1 du rapport semestriel 2013/2 de MELANI:

https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2013-2.html

4.1.2 Le BND et la NSA auraient espionné des lignes de Swisscom

Aux dires du député au Parlement autrichien Peter Pilz, le Service fédéral de renseignement allemand (Bundesnachrichtendienst, BND) et son homologue américain (National Security Agency, NSA) auraient, dans le cadre de l'opération Eikonal,[11] recherché la présence de certains mots-clés dans les données transitant via le nœud de routage Internet de Francfort. Les investigations visaient à en apprendre davantage sur des personnes soupçonnées de terrorisme et sur des trafiquants d'armes. La NSA communiquait à chaque fois au BND les mots-clés à vérifier. Or au fil du temps, on aurait régulièrement constaté la présence de mots-clés surprenants et hors sujet, qui le cas échéant n'avaient qu'un lien indirect avec la mission première.

L'opération se concentrait sur 250 lignes de transit. Dont selon la liste de Peter Pilz neuf lignes avec des extrémités opérées par Swisscom en Suisse et conduisant à Prague, Sydney, Tokyo, Séoul, Luxembourg, Varsovie ou Moscou. La Suisse aurait ainsi fait partie des 64 pays concernés par l'opération d'écoutes du BND et de la NSA. Ces affirmations reposent sur un contrat conclu en 2004 entre le BND et l'opérateur Deutsche Telekom et publié par Peter Pilz. Swisscom a fait savoir que ces lignes n'étaient cependant plus en sa possession.[12]

[10] http://www.tagesschau.de/ausland/duqu-103.html (état: le 31 août 2015).

[11] http://www.zeit.de/politik/deutschland/2015-04/bnd-nsa-kooperation-verantwortliche (état: le 31 août 2015).

[12] http://www.nzz.ch/schweiz/bnd-und-nsa-sollen-swisscom-kunden-ausspioniert-haben-1.18549890 (état: le 31 août 2015).

Le Service de renseignement de la Confédération (SRC) a notamment consacré à l'espionnage économique une brochure intitulée «Prophylax». Cette brochure fait partie de son action de prévention et de sensibilisation dans le domaine de la non-prolifération et de l'espionnage économique. Elle a pour but la sensibilisation des entreprises et des institutions de formation. Elle explique comment prévenir les dangers et reconnaître les affaires illégales, et quelles mesures de prévention et de lutte les autorités peuvent mettre en place.

http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/publication/snd_publ.html

4.2 Fuites d'information

Un vol de données stockées numériquement peut être le fait d'acteurs aux motivations diverses: des Etats seront intéressés aux données elles-mêmes, si ces dernières peuvent par ex. leur procurer un avantage stratégique ou économique. Un vol de données permettra à des cybercriminels d'obtenir un rapide gain financier. Pour cela, le recours au chantage est à l'heure actuelle un des modes opératoires les plus fréquents. Pour pouvoir exiger de l'argent de la part de leur victime, les criminels doivent disposer d'un moyen de pression. D'où l'utilité des données volées. Cette thématique a déjà été abordée lors de notre dernier rapport semestriel.[13]

4.2.1 Rex Mundi

Rex Mundi est un acteur spécialisé dans ce type de mode opératoire. Il a acquis une certaine notoriété après avoir fait de nombreuses victimes, notamment en Belgique, durant l'année 2014. En janvier 2015, la Suisse était également touchée, avec l'attaque d'une entreprise romande. Cet événement était en tout point identique à ce qui avait été observé jusqu'ici. Dans un premier temps, une attaque par *injection sql* a été utilisée pour accéder à une base de données. Elle contenait des informations saisies sur un formulaire de contact utilisé par les internautes et disponible sur le site Web de l'entreprise. Il s'agissait de données personnelles (adresses, numéros de téléphone, etc.) et des communications transmises à travers ce formulaire. Pour ne pas dévoiler ces informations, les criminels exigeaient de l'entreprise le paiement d'une rançon. Rex Mundi a bien conscience des dommages potentiels en termes d'image pouvant être générés par l'écho dont bénéficie l'attaque, et en profite pour tenter d'obtenir un paiement, ce qui constitue une forme de chantage à la réputation. Afin d'accentuer la pression sur l'entreprise, Rex Mundi a ainsi utilisé twitter, comme à son habitude, pour communiquer sur l'incident, ses propres revendications et les réactions de l'entreprise à son encontre. L'entreprise n'ayant pas cédé au chantage, les données ont été divulguées. Ayant anticipé cette issue, elle avait déjà commencé à contacter sa clientèle pour l'informer de la fuite et des possibles risques d'utilisations de ces données.

En plus du dommage à l'image pour l'entreprise, la nature et la valeur des informations divulguées peuvent poser problème en elles-mêmes. Tout d'abord, par la nature confidentielle des données portant sur l'individu, l'entreprise et ses activités. Mais aussi, dans le cas exposé, en raison de l'exploitation potentielle de données personnelles et privées pouvant donner lieu, par la suite, à des tentatives d'escroquerie utilisant les techniques d'ingénierie sociale. La valeur de ces informations peut, par ailleurs, constituer

[13] MELANI rapport semestriel 2014/2, chapitre 5.3: https://www.melani.admin.ch/melani/fr/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-2.html (état: le 31 août 2015).

une chance de monétiser l'attaque en l'absence de paiement de l'entreprise. On pense notamment à une possible revente des données sur un marché underground. Plus généralement, ce type de cas pose à nouveau la question de la sécurisation des sites web publics, qui sont bien souvent des cibles rêvées pour différents types d'attaques.

La question a été fréquemment thématisée par MELANI (voir par ex. le rapport semestriel 2014/2, chap. 3.5 «CMS – failles de sécurité et négligence des administrateurs Web») et fait l'objet du document suivant:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-prevention-pour-les-systemes-de-gestion-de-contenu--c.html

4.3 Systèmes de contrôle industriels

Les systèmes de contrôle industriels sont au cœur de l'actualité, alors que toujours plus de processus sont pilotés grâce à l'informatique. *L'industrie 4.0*, la quatrième révolution industrielle, est aussi concernée. Il est vrai que le terme de système de contrôle industriel (SCI) a un sens très large et peut ainsi englober à peu près tout, du pilotage d'une centrale nucléaire à la domotique. Le cas échéant, on s'expose à mélanger des problématiques très différentes. Les sous-chapitres suivants se concentrent donc sur les systèmes d'importance vitale – dont les systèmes d'approvisionnement en électricité font indiscutablement partie.

4.3.1 Honeypot simulant une centrale hydroélectrique – 31 attaques

L'emploi de *honeypots* (pots de miel) permet de juger du risque réel de cyberattaque. Des experts mettent en ligne, en observant de près les événements, des systèmes imitant à s'y méprendre les vrais systèmes pris pour cibles par les pirates, afin de provoquer des attaques sans qu'aucun dommage ne soit causé.

La Sonntagszeitung[14] a présenté en février 2015 une telle étude portant sur les centrales hydroélectriques. Pendant trois semaines, un système spécialement conçu s'est fait passer pour une centrale hydroélectrique. Il a subi 31 attaques, dont trois dues à des pirates qui ont cherché à provoquer une erreur dans le système et à le faire tomber en panne. Même si cet essai n'est pas entièrement transposable aux systèmes en activité, l'incident montre bien l'intérêt des pirates pour de tels systèmes. Ce n'était pas la première fois qu'un tel outil montrait dans quelle mesure il est possible de s'introduire notamment dans les systèmes de pilotage de petites centrales hydroélectriques. Il y a deux ans déjà, un rapport sur la question avait fait les gros titres: il avait suffi de quinze minutes pour s'emparer d'une centrale située dans le canton de Glaris.[15] Même si le sabotage d'une petite centrale hydroélectrique n'a pas d'impact sur le réseau électrique, une attaque orchestrée contre un grand nombre de tels systèmes pourrait aboutir à de soudaines variations de tension et à d'éventuelles réactions en chaîne, pouvant aller jusqu'à une panne à grande échelle.

[14] http://www.sonntagszeitung.ch/read/sz_08_02_2015/nachrichten/Angriff-auf-die-Stromversorgung-27051 (état: le 31 août 2015).

[15] http://www.srf.ch/sendungen/10vor10/spur-von-snowden-entlastung-fuer-sachs-angriffe-via-internet (état: le 31 août 2015).

La question fondamentale qui se pose ici est de savoir pourquoi, en dépit des vulnérabilités connues et de l'intérêt manifeste qu'elles suscitent chez les pirates (du moins les leurres de systèmes ou honeypots), il n'y a pas eu jusqu'ici de défaillance à grande échelle ou d'autre panne. Il n'est pas facile d'y répondre. La raison tient peut-être à l'absence de modèle commercial exploitable pour les pirates. Comme outre l'accès virtuel les systèmes offrent généralement aussi une possibilité d'accès physique, un système peut être facilement retiré d'Internet en cas de cyberattaque (en raison des exigences d'autonomie des solutions de repli). Par ailleurs, les pirates motivés par des intérêts essentiellement pécuniaires éprouvent peut-être des scrupules, faute de connaître les répercussions (par ex. en termes de vies humaines) qu'une attaque contre un tel système pourrait avoir.

4.3.2 Système de commande ouvert de réseaux d'approvisionnement en eau

Il n'est pas toujours facile à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) d'évaluer dans quelle mesure les systèmes ouverts doivent être considérés comme étant d'importance vitale, ou si des systèmes sensibles ont été manipulés, et le cas échéant comment[16]. Un bon exemple datant d'il y a deux ans est fourni par le Chaos Communication Congress (CCC), à l'occasion duquel des pirates avaient publié de nombreuses copies d'écran de systèmes où ils se seraient introduits. Dont l'approvisionnement en eau d'une petite commune Suisse. Or une analyse minutieuse du cas et une demande à la commune ont révélé que cet accès n'est pas publié, mais que les citoyens intéressés sont autorisés à voir ces données. Les graphiques indiquaient quelle quantité d'eau provenant de chaque source alimente le réservoir. On n'y voyait cependant pas de données d'importance vitale, et aucune manipulation n'était possible à distance.

Un incident analogue de la période sous revue montre pourtant que ce n'est pas toujours le cas. Là encore, il s'agissait d'un réseau suisse d'approvisionnement en eau, dont un intrus pouvait apprendre les valeurs de chaque source ou réservoir. Au cours d'une analyse plus détaillée, MELANI a découvert la présence sur le site Web de mots de passe fixes programmés, permettant d'accéder à des éléments de commande. Un mot de passe aussi facilement accessible risque de susciter de dangereuses attaques de la part de pirates.

[16] http://www.suedostschweiz.ch/zeitung/wasserwerk-wurde-gehackt (état: le 31 août 2015).

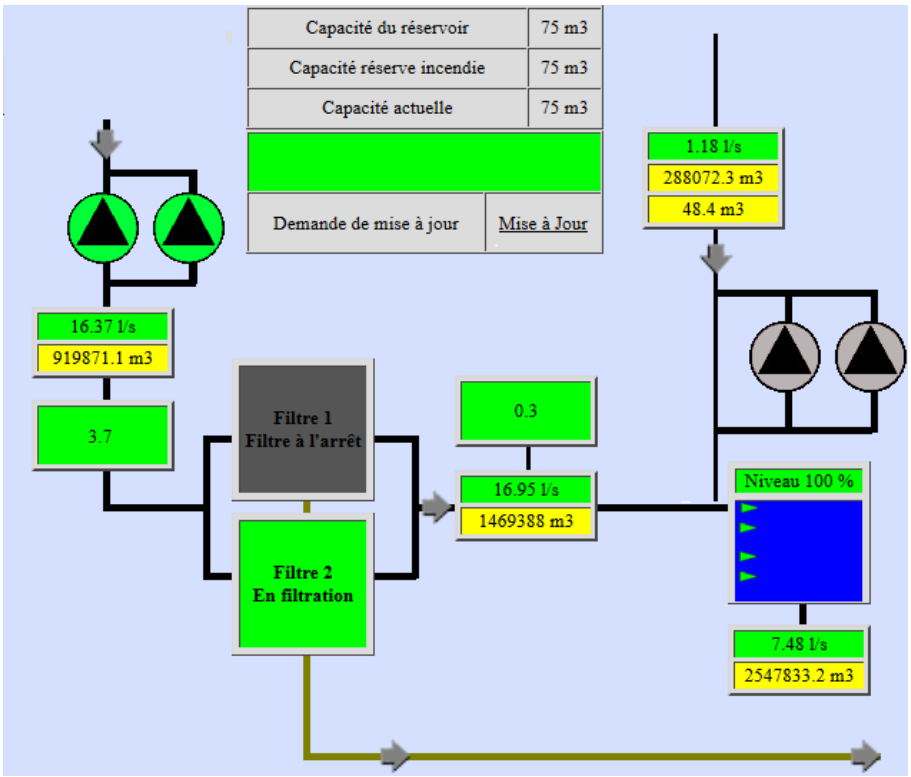


Fig. 2: exemple d'une plate-forme accessible au public d'un approvisionnement en eau en Suisse

MELANI tient à disposition une liste de contrôle des mesures de protection des systèmes de contrôle industriels. Lesdites mesures devraient faire partie intégrante d'un processus global de sécurité, qui en garantisse la bonne mise en place et qui prévoie des contrôles réguliers et des améliorations constantes. En outre, il est important que l'exploitant d'une installation connaisse les menaces actuelles et qu'il procède à des contrôles ponctuels, débouchant sur de nouvelles mesures de sécurité ou des optimisations en la matière. A cet effet, une étroite collaboration s'avère cruciale entre les processus concernés – gestion des risques, ingénierie et exploitation.

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-protection-des-systemes-de-controle-industriels--sci-.html

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié en février 2015 une nouvelle étude (en anglais). On y trouve des informations sur les enjeux actuels et des recommandations visant à développer des systèmes de certification des compétences pour les cyber-experts qui travaillent en Europe avec des systèmes de contrôle industriels (SCI) ou des systèmes servant à la surveillance et à la gestion des processus techniques (systèmes SCADA).

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals

4.4 Cyberattaques (DDoS, défiguration de sites)

Les citoyens et entreprises suisses restent en butte à différents types d'attaques, ayant notamment pour cible leur site Web. Les attaques par déni de service et les défigurations de

sites sont d'autant plus problématiques pour les entreprises qu'elles ont besoin d'une présence en ligne crédible.

4.4.1 DDoS et extorsion: vague d'attaques par DD4BC

L'extorsion est actuellement une des méthodes favorites des cybercriminels visant un rapide gain financier. Différents types d'attaques peuvent être utilisées comme levier afin de soutirer de l'argent à une cible, dont des attaques par déni de service (*Denial of Service, DoS*). DD4BC est un acteur spécialisé dans ce type d'attaques depuis juillet 2014. Il fait preuve d'une grande flexibilité en termes de choix des cibles. DD4BC a en effet sévi tant en Europe qu'aux Etats-Unis, en Asie ou en Océanie. Par ailleurs, il cible des secteurs bien précis par phases successives. Après s'être focalisé sur l'industrie du *bitcoin* puis les casinos en ligne, DD4BC a fait de nombreuses victimes parmi les banques et les entreprises de la finance.

Ce groupe a été particulièrement actif en Suisse au premier semestre 2015. MELANI a été informé d'une dizaine de cas ayant touché différentes entreprises, notamment dans le domaine de la finance. Les éléments récoltés recoupent ce qui a été observé dans d'autres pays et illustrent bien le mode opératoire de cet acteur. L'agression débute généralement par une attaque DDoS de faible intensité (en règle générale de 10 à 15 Go/s). Après cette démonstration de son savoir-faire, l'attaquant envoie un courriel de chantage à sa victime. Pour s'épargner une attaque plus sérieuse, il lui est demandé de payer une somme de 30 à 40 bitcoins (soit 7500 à 10 000 francs d'alors). Pour justifier ce chantage, DD4BC prétend être en mesure de déployer une attaque de 400 à 500 Go/s. Il ne l'a toutefois jamais fait. En cas de non-paiement, une attaque allant jusqu'à 30 Go/s[17] a parfois été observée, alors que dans d'autres cas, l'agresseur n'a pas mis sa menace à exécution.

Un site Web inaccessible peut signifier un grave manque à gagner pour son propriétaire, à fortiori si le service attaqué est de nature commerciale. L'attaquant espère ainsi que la cible, souhaitant se prémunir des effets négatifs d'une telle attaque, fera le choix de payer.

MELANI recommande en pareil cas de ne pas céder au chantage. Il convient de prendre immédiatement contact avec l'hébergeur du site Web et le fournisseur en amont (upstream provider) pour adopter des mesures de protection. Les victimes ont par ailleurs la possibilité de déposer une plainte pénale auprès de la police cantonale. MELANI a publié un document sur le thème des attaques DDoS et les possibilités d'y faire face:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/massnahmen-gegen-ddos-attacken.html

4.4.2 Défiguration de sites en Suisse romande

Des vagues de défiguration de sites (*defacement*) ont à nouveau fait l'actualité au premier semestre, en Suisse romande notamment. Tout d'abord, suite à l'attaque terroriste ayant visé la rédaction de Charlie Hebdo, de nombreux cas de défiguration de sites ont été observés en France et, dans une moindre mesure, en Suisse romande. Différents groupes ont publié à cette occasion un message de propagande islamiste et de justification des attentats. En France, les autorités ont recensé 1300 attaques, ayant abouti au piratage de 25 000 sites (voir chap. 5.4.3). Les sites suisses visés l'ont apparemment été en raison de

[17] Des rapports externes attestent d'attaques allant jusqu'à 60 Go/s. Voir notamment: http://pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf (état: le 31 août 2015).

leur appartenance à l'espace francophone. On peut supposer que les attaquants n'ont pas ciblé spécifiquement des sites suisses, mais qu'ils ont plutôt pris ces derniers pour des sites français.

En avril, plusieurs autres cas de défiguration de sites romands ont été rapportés à MELANI et ont fait l'objet d'articles de presse. Là aussi, les pages piratées ont été utilisées à des fins de propagande par un groupe se réclamant de l'Etat islamique. En l'occurrence, il serait exagéré de parler d'une véritable vague. L'analyse des différents cas signalés à MELANI a montré qu'ils étaient tous l'œuvre d'un seul et même attaquant. Selon le site zone-h.org, qui recense ce genre de cas, un pirate se faisant appeler «cwne» aurait piraté 180 pages entre le 24 et le 26 avril. Tous les sites étaient hébergés chez le même fournisseur. Selon toute vraisemblance, cwne a exploité une faille de sécurité sur un serveur hébergeant de nombreux sites (pratique du *mass defacement*). Cet exemple montre qu'une seule attaque peut aboutir à un grand nombre de défigurations de sites et à une grande visibilité, d'autant plus si les sites touchés appartiennent à des entreprises ou organisations implantées dans le même périmètre. Ce qui est parfois perçu par les médias ou le public comme une action de grande ampleur est en réalité le résultat de l'exploitation d'une seule faille par un pirate.

Par ailleurs, on cherche parfois à établir un lien entre les sites piratés et les messages diffusés. Or ce lien est généralement inexistant, les attaquants opérant en opportunistes et ciblant des sites vulnérables, indépendamment de leur contenu.

Des règles élémentaires de sécurité, comme la mise à jour des programmes utilisés sur le site et le serveur Web, permettent de se prémunir en grande partie de ce type d'attaques. MELANI a publié à ce sujet le document suivant:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-prevention-pour-les-systemes-de-gestion-de-contenu--c.html

4.5 Social Engineering, phishing

Outre les attaques techniques en tous genres, les pirates cherchent aussi à exploiter les faiblesses humaines. Un cas survenu aux Etats-Unis illustre les possibilités insoupçonnées de l'ingénierie sociale (*social engineering*): un manager de l'entreprise américaine Scoular a versé au total 17,2 millions de dollars sur un compte bancaire chinois appartenant à des escrocs, en croyant agir sur mandat direct de son chef. Une étude du cabinet d'audit KPMG corrobore cette observation et montre que les entreprises continuent à trop miser sur la technologie, en négligeant le facteur humain dans la protection contre les cyberattaques. En principe, mieux vaudrait suivre une approche intégrée et équilibrée, qui tienne compte aussi bien des individus et des processus que des technologies.[18]

4.5.1 Phishing – attaques contre les banques cantonales et les données de cartes de crédit; amélioration des courriels de phishing

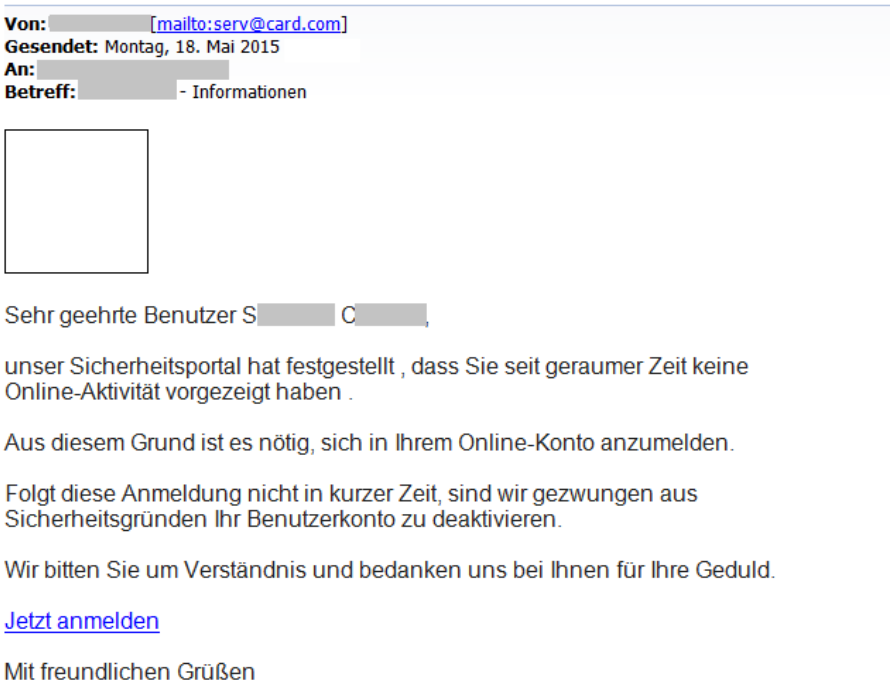
Le *phishing* continue de se tailler la part du lion dans les activités d'ingénierie sociale (*social engineering*). La plupart des attaques observées obéissent désormais à un modèle standard. Les escrocs commencent par choisir un établissement financier. Ils reproduisent alors le graphisme de son site et de ses courriels, inventent une histoire crédible pour les victimes (la clientèle de la banque), et déclenchent les mêmes attaques pendant des jours voire des

[18] http://www.kpmg.com/CH/en/topics/cyber-security/Pages/default.aspx (état: le 31 août 2015).

mois. On a parfois affaire à des vagues de phishing, où le site Web est à chaque fois hébergé auprès du même fournisseur d'accès. Et quand ce dernier désactive la page de phishing, elle réapparaît ailleurs quelques instants plus tard.

Les fréquentes attaques de phishing observées au printemps 2015 contre des banques cantonales se sont déroulées selon ce schéma. Autre particularité à souligner, elles ne visaient pas un établissement spécifique, mais plus généralement la clientèle des banques cantonales alémaniques. D'où bien entendu davantage de victimes potentielles. Ce n'est que dans un second temps que la victime était invitée à dire dans quelle banque cantonale elle détenait son compte d'e-banking, et bien sûr à indiquer ses données personnelles.

Plus les utilisateurs de l'e-banking sont sur leurs gardes, plus les escrocs doivent innover et améliorer leurs méthodes. Notamment en appelant les gens par leur nom et prénom, dans des envois personnalisés pour inspirer confiance aux victimes potentielles. La méthode ne s'est pas partout imposée jusqu'ici – sans doute les efforts requis pour relier les noms et prénoms avec la bonne adresse électronique sont-ils encore dissuasifs. Pourtant, diverses vagues de phishing lancées au deuxième semestre 2015 ont franchi cette étape. Il est difficile de dire où les pirates ont obtenu leurs données. Elles peuvent par ex. provenir de comptes de messagerie compromis et dont les criminels ont récupéré les informations.



Von: [mailto:serv@card.com]
Gesendet: Montag, 18. Mai 2015
An:
Betreff: - Informationen

Sehr geehrte Benutzer S C,

unser Sicherheitsportal hat festgestellt , dass Sie seit geraumer Zeit keine Online-Aktivität vorgezeigt haben .

Aus diesem Grund ist es nötig, sich in Ihrem Online-Konto anzumelden.

Folgt diese Anmeldung nicht in kurzer Zeit, sind wir gezwungen aus Sicherheitsgründen Ihr Benutzerkonto zu deaktivieren.

Wir bitten Sie um Verständnis und bedanken uns bei Ihnen für Ihre Geduld.

Jetzt anmelden

Mit freundlichen Grüßen

Fig. 3: Exemple de courriel de phishing s'adressant à la victime par son prénom et son nom

Le fait d'appeler les victimes par leur nom, d'inventer une histoire plausible et donc de professionnaliser l'ingénierie sociale joue un rôle important, comme le montrent plusieurs cas où la banque de données clients d'une entreprise avait été attaquée et copiée au préalable. Les escrocs procèdent généralement par *injection SQL*. Ils envoient ensuite, au nom de l'entreprise, des courriels ciblés munis d'un lien menant à une copie parfaite du vrai site Web, en exigeant des victimes qu'elles y inscrivent leur numéro de carte de crédit, pour une quelconque raison. Comme elles ont probablement déjà été en contact avec la véritable entreprise et le prétexte semble plausible, les chances sont bien réelles qu'elles se fassent

piéger. Par conséquent, il ne reste à l'entreprise piratée qu'à informer sa clientèle de cette tentative de fraude.

4.5.2 Phishing après une défiguration de sites, ou parfois l'inverse

Ces derniers temps, MELANI a constaté que la défiguration de sites allait fréquemment de pair avec des tentatives de *phishing*: pour installer une page de phishing, les pirates doivent d'abord acquérir un domaine ou compromettre un site existant, en tirant parti de ses failles de sécurité. Or le *defacement* exploite lui aussi les failles de sécurité de pages Web pour en modifier le contenu et y publier des déclarations personnelles, religieuses ou politiques. En outre, les pages Web défigurées sont fréquemment publiées sur des sites publics comme zone-h.org[19]. Il est dès lors facile aux escrocs de repérer les pages Web vulnérables, et d'y placer leurs pages de phishing. La situation inverse, soit la défiguration d'une page de phishing existante, est beaucoup moins probable. Non seulement il n'existe pas de liste publique des sites de phishing, mais lorsque de telles pages sont découvertes, elles sont aussitôt retirées du réseau.

MELANI a néanmoins observé pour la première fois un tel mode opératoire en mai 2015. D'abord, une attaque normale de phishing contre un établissement financier suisse lui avait été signalée. Comme le veut l'usage, la page a été analysée puis signalée à l'hébergeur compétent pour qu'il la désactive. Or avant même que ce dernier ait pu réagir et supprimer la page frauduleuse, un *hacktiviste* avait déjoué l'arnaque. En défigurant la page pour y publier un message contre la xénophobie, il a empêché – certainement sans le vouloir – des victimes potentielles de divulguer leurs données sur ce site de phishing.

4.5.3 Faux formulaires fiscaux

Au premier semestre, de nombreuses entreprises de la région genevoise ont reçu un courriel accompagné d'un formulaire censé provenir de l'administration fiscale genevoise. Ce formulaire, sur lequel il fallait indiquer ses gains immobiliers et d'autres détails sur l'entreprise, devait ensuite être renvoyé avec la dernière quittance de loyer à une adresse électronique. Le formulaire en question a beau exister, l'adresse d'envoi n'avait rien à voir avec les autorités fiscales genevoises et appartenait à un escroc.

Un cas proche a été observé dans le canton de Vaud[20].

A quelles fins de telles données peuvent-elles être détournées, une fois tombées aux mains des escrocs? Il s'agit en général d'actes préparatoires à l'«arnaque au président». Les escrocs commencent par récolter des informations sur la société, afin de se faire une idée précise de son organisation et du contexte où elle évolue. Ces renseignements proviennent en partie de recherches actives, comme dans le cas décrit ici. L'arnaque peut alors commencer. En règle générale, un courriel usurpant l'identité d'un membre de la direction est adressé à un collaborateur du service financier. Il y est généralement question de transactions confidentielles en cours. Les escrocs soulignent le caractère unique et confidentiel de l'ordre de paiement, en insistant sur l'urgence de la situation. Dans bien des cas, les escrocs téléphonent en parallèle au comptable afin de donner davantage de crédibilité à leur scénario.

---

[19] Zone-h.org est un site d'archivage des pages Web défigurées.

[20] http://www.24heures.ch/vaud-regions/arnaqueurs-utilisent-adresse-fisc-vaudois/story/10817017 (état: le 31 août 2015).

Le canton de Genève a publié une mise en garde sur son site Web.[21]

Les principales règles de comportement à suivre avec les courriels reçus aident à se protéger du phishing et d'autres types de fraude:

Méfiez-vous du courrier électronique non sollicité: faites preuve de prudence non seulement avec les expéditeurs vous sont inconnus, mais aussi avec ceux qui vous sont familiers. Les fraudeurs usurpent souvent l'adresse électronique d'entreprises jouissant d'une bonne réputation pour tromper le destinataire.

- Méfiez-vous des courriels qui exigent une action de votre part, en vous menaçant sinon de conséquences (perte financière, plainte pénale ou procès, blocage de compte ou de carte de crédit, occasion manquée, malheur).
- N'ouvrez aucun document joint aux courriels suspects et ne cliquez sur aucun des liens y figurant, au risque d'infecter votre appareil. Si vous avez des doutes sur l'origine du message, utilisez les possibilités de contact indiquées sur le véritable site Web du prétendu expéditeur, pour savoir de quoi il s'agit et si le courriel émane réellement de lui.
- La règle de base consistant à ne fournir aucune information interne et à ne pas suivre les instructions données lors de prises de contact semblant douteuses et insolites est plus que jamais d'actualité, au vu des cas actuels.

Recommandations spécifiques aux entreprises:

- Tous les processus liés au trafic des paiements devraient faire l'objet de règles internes, et les collaborateurs s'y tenir dans tous les cas.
- MELANI recommande de sensibiliser les collaborateurs à ce genre d'incidents, notamment les personnes occupant des postes clés.
- Le cas échéant, il est vivement indiqué de vérifier par téléphone à l'interne la légitimité de la demande formulée.

Sur son site, MELANI a publié un aide-mémoire conçu pour les PME sous le lien:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

4.6 Logiciels criminels (crimeware)

L'expression *crimeware* désigne tout logiciel malveillant spécialement conçu par des fraudeurs pour automatiser la cybercriminalité économique. Comme l'indique la statistique ci-dessous, les chevaux de Troie bancaires restent très répandus. En Suisse, une grande partie des annonces de systèmes infectés faites à MELANI sont dues à des chevaux de Troie comme Torpig, Dyre, Tinba, Gozi ou ZeuS.

[21] http://ge.ch/impots/courrier-lectronique-frauduleux (état: le 31 août 2015).

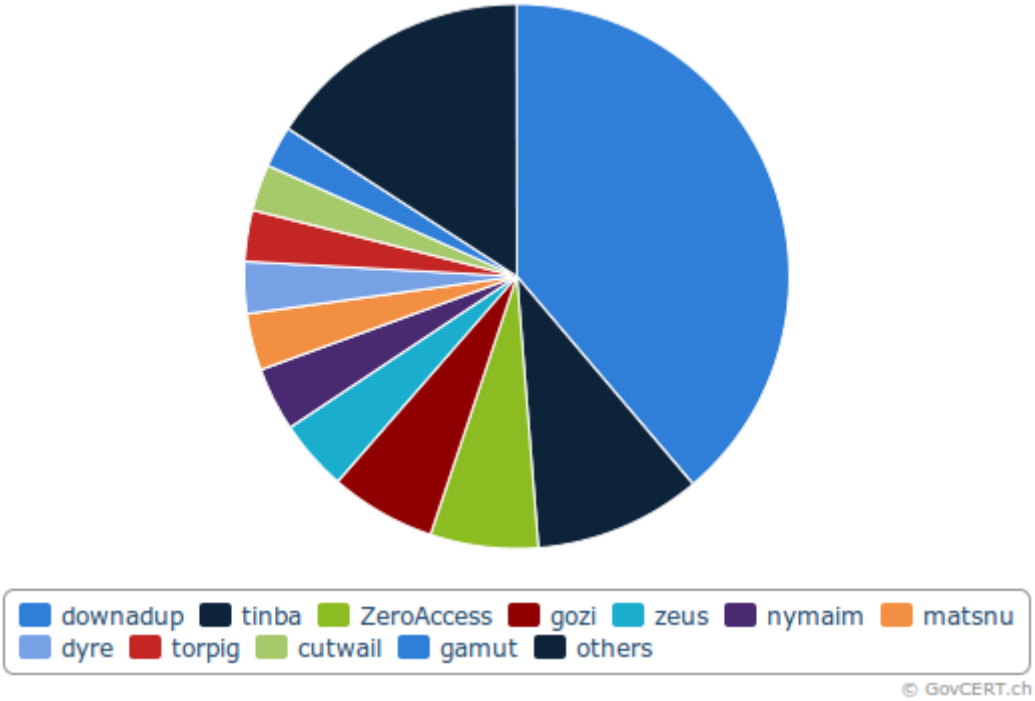


Fig. 3: Répartition en Suisse des logiciels malveillants, selon les connaissances dont dispose MELANI. Jour de référence: le 30 juin 2015. Données actuelles sur :http://www.govcert.admin.ch/statistics/drone/

Sur le plan géographique, Zurich et le Valais sont les deux cantons affichant (au prorata de leur population) un taux d'infection supérieur à la moyenne.

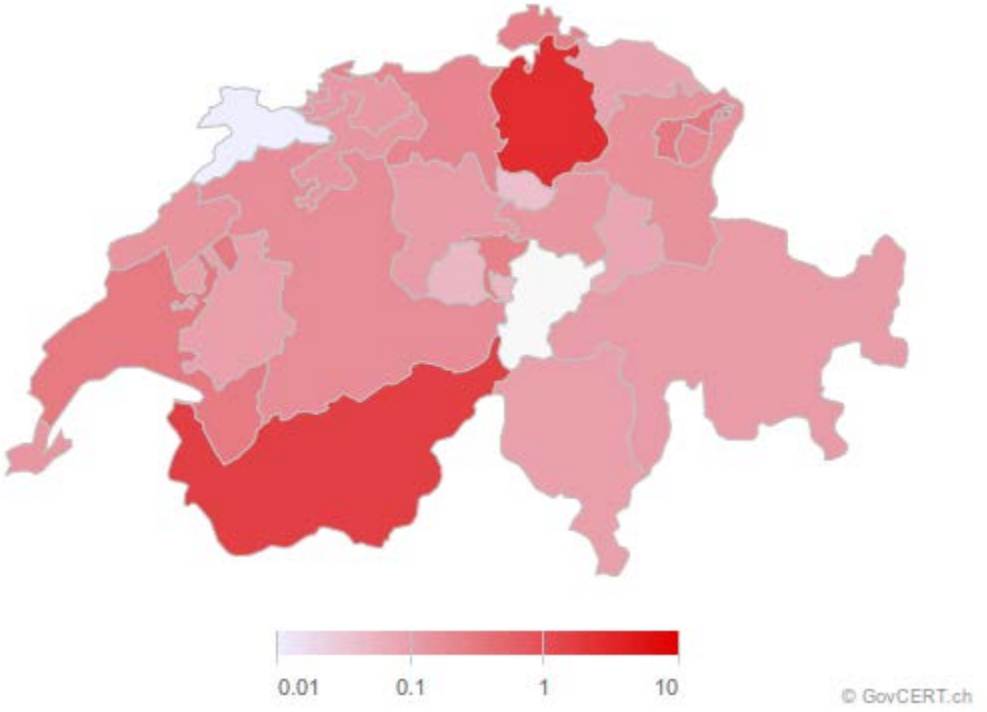


Fig. 4: Nombre d'infections par canton, en fonction de la population. Date de référence: le 30 juin 2015.: Données actuelles sur : http://www.govcert.admin.ch/statistics/drone/

4.6.1.1 Downadup

Il est inquiétant de constater, à propos des infections par *Downadup* (aussi appelé *Conficker*), que ce ver qui existe depuis plus de huit ans reste manifestement très répandu. *Downadup* se propage par une faille de sécurité découverte en 2008 dans les systèmes d'exploitation Windows, dont il est possible de tirer parti depuis Internet; le ver permet ensuite d'installer n'importe quel logiciel malveillant sur le système compromis. Le nombre toujours élevé d'infections tient peut-être à ce qu'en Suisse, beaucoup d'internautes utilisent une version désuète de Windows (Windows XP) et négligent d'actualiser régulièrement leur système d'exploitation. Autre explication possible, certains fournisseurs de services Internet suisses continuent de ne pas traiter les annonces concernant les clients infectés (notamment par manque de ressources, de moyens techniques ou de savoir-faire).

4.6.1.2 Dyre

Au premier semestre 2015, le maliciel Dyre (aussi appelé Dyreza) s'est propagé en Suisse. Il s'agit d'un cheval de Troie bancaire se répandant par courriel. Les escrocs préparent des envois faisant mention d'une télécopie, d'une facture ou d'un document analogue et qui renferment en annexe le maliciel (généralement sous forme de fichier exécutable de type .exe, dissimulé dans une archive ZIP). Après s'être concentré les premiers mois sur les PME suisses[22] et avoir délesté une entreprise fribourgeoise d'un montant à sept chiffres, Dyre s'attaque toujours plus aux particuliers, depuis mai 2015[23]. Lors de ses pics d'activité, jusqu'à 2000 infections par jour ont été signalées à MELANI.

Au cas où vous auriez déjà reçu de tels courriels et ouvert leur annexe, nous vous recommandons d'analyser votre système avec un antivirus ou un outil de suppression des logiciels malveillants (malware removal tool). Des explications figurent sous le lien suivant:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/instructions-relatives-a-la-suppression-des-maliciels.html

MELANI a conçu un aide-mémoire pour aider les PME suisses à améliorer la sécurité dans leurs réseaux. Cet aide-mémoire est téléchargeable sous le lien:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

En outre, vous trouverez sur le Portail PME de la Confédération un programme en dix points visant à accroître la sécurité informatique:

http://www.kmu.admin.ch/kmu-betreiben/03710/03712/03715/index.html?lang=fr

4.6.1.3 Retefe

Le maliciel Retefe continue à sévir en Suisse. MELANI en a parlé pour la première fois il y a deux ans. Retefe se diffuse exclusivement par courriel, généralement dans de fausses factures de boutiques en ligne bien connues, comme par ex. Zalando ou Ricardo.

---

22 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/pme-visees-par-un-cheval-de-troie-bancaire.html (état: le 31 août 2015).

23 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/information_dyre_2.html (état: le 31 août 2015).

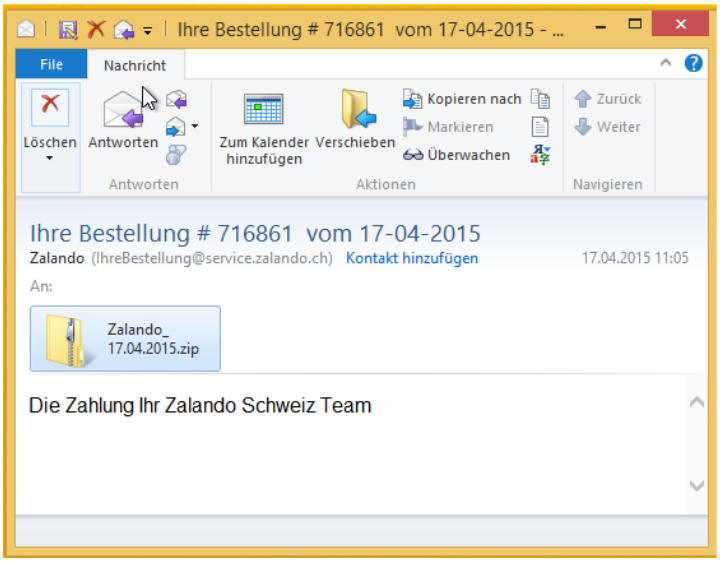


Fig. 5: Exemple de courriel frauduleux diffusé par le maliciel Retefe

En cas d'ouverture du fichier exécutable figurant en annexe du courriel, le système du destinataire s'infecte avec Retefe. Après quoi le maliciel modifie les paramètres d'Internet Explorer pour que certains sites Web – dont les portails d'e-banking de certains établissements financiers suisses – soient redirigés vers un serveur mandataire (proxy server) situé à l'étranger. En outre, Retefe installe un *certificat racine* falsifié. Il est possible pour Retefe de délivrer des certificats pour n'importe quel établissement financier, et donc de faire croire à l'utilisateur qu'il est bien en contact avec ces derniers.

Lorsqu'une victime de Retefe s'annonce au moyen de l'ordinateur infecté sur un prétendu portail d'e-banking, elle voit s'afficher un *code QR*. Ce code mène vers un site malveillant, qui l'invite à télécharger et installer une application pour « améliorer la sécurité » – en vérité cependant un maliciel pour Android (cheval de Troie SMS). Si la victime installe l'application Android proposée, tous les SMS envoyés par la banque pour l'identification à deux facteurs seront transférés aux malfaiteurs via un serveur Web situé à l'étranger. Ceux-ci contrôlent dès lors les accès e-banking de leur victime, et pourront vider son compte.

Si vous utilisez un smartphone ou une tablette Android, assurez-vous de n'installer que les applications issues de l'application officielle Google Play Store. N'installez jamais d'applications provenant de sources tierces, même si on vous demande de le faire. Assurez-vous également que les réglages suivants soient paramétrés sur votre appareil Android:

Paramètres -> Sécurité -> Sources inconnues -> DÉSACTIVÉ

Paramètres Google -> Sécurité -> Analyser appareil pour détecter menaces de sécurité -> ACTIVÉ

Des compléments d'informations sur Retefe figurent (en anglais) dans le blog de GovCERT.ch:

4.6.1.4 Tinba

Tinba (aussi appelé Tiny Banker) a également donné des sueurs froides aux internautes au premier semestre 2015 et a été par moments – avec Downadup – l'infection la plus souvent signalée à MELANI sur le plan suisse. Il s'agit d'un cheval de Troie bancaire qui s'en prend à

plusieurs établissements financiers suisses. Mais à la différence de Dyre ou Retefe, Tinba est une boîte à outils (toolkit) vendue pour quelques milliers de francs sur des forums en ligne de cybercriminels. Les escrocs achètent le logiciel et peuvent s'en servir à leur guise. Outre les campagnes découvertes en Suisse, des dizaines d'autres campagnes Tinba s'en prennent au niveau mondial aux établissements financiers.

4.6.1.5 Chevaux de Troie verrouillant les données – Cryptowall 3.0, Teslascript et un auteur pris de remords

Divers cas de données verrouillées par un cheval de Troie ont été signalés au premier semestre 2015. Il s'agissait généralement de Cryptowall 3.0, mais toujours plus de méfaits imputables au logiciel de rançon (ransomware) Teslacrypt ont été communiqués à MELANI. Les victimes étaient généralement des particuliers, mais des cas d'entreprises sont également connus. A moins d'avoir à disposition une sauvegarde récente, toutes les données ou du moins une partie sont perdues. Le cas du logiciel escroc Locker mérite encore d'être signalé. Ce maliciel s'était déjà installé sur divers systèmes et attendait pour s'activer et chiffrer les données, ce qu'il a fait au début de juin 2015. Or son auteur s'est manifesté peu après, non seulement pour s'excuser, mais encore pour donner au maliciel l'ordre de déchiffrer les données, en publiant en même temps la clé de chiffrement utilisée.[24]

Les données figurant sur l'ordinateur devraient être copiées régulièrement sur des supports externes (*backup*). Ceux-ci seront connectés à l'ordinateur uniquement lors de la sauvegarde des données.

4.7 Mesures préventives

Les mesures préventives sont essentielles pour lutter contre les menaces en tous genres. Ces mesures peuvent être de nature technique ou organisationnelle, ou relever du droit pénal. La sensibilisation de la population s'avère aussi un pilier important de la lutte contre les cyberattaques. En effet, la plupart des cyberattaques misent sur l'ignorance et la bonne volonté des victimes, en cherchant à les prendre au dépourvu. Une autre mesure importante contre les cyberincidents consiste à établir une véritable culture de l'annonce, au sein des entreprises comme dans le grand public. Car les collaborateurs ne continueront à signaler des incidents que s'ils ont l'impression d'être pris au sérieux. MELANI a donc créé le portail «Antiphishing.ch», auquel chacun peut signaler les courriels et site Web soupçonnés de dérober des données d'accès ou des données de carte de crédit.

4.7.1 Antiphishing.ch

MELANI a lancé le portail antiphishing.ch en été 2015, afin de mieux canaliser les annonces de pages de phishing et de les analyser plus efficacement. Les annonces se font au moyen d'un formulaire en ligne. Le portail indique en outre une adresse électronique à laquelle les courriels de phishing peuvent être transmis. Le portail d'annonce est disponible à l'adresse https://www.antiphishing.ch.

[24] http://www.heise.de/security/meldung/Krypto-Trojaner-ueberlegt-es-sich-anders-und-entschluesselt-alles-wieder-2678669.html (état: le 31 août 2015).

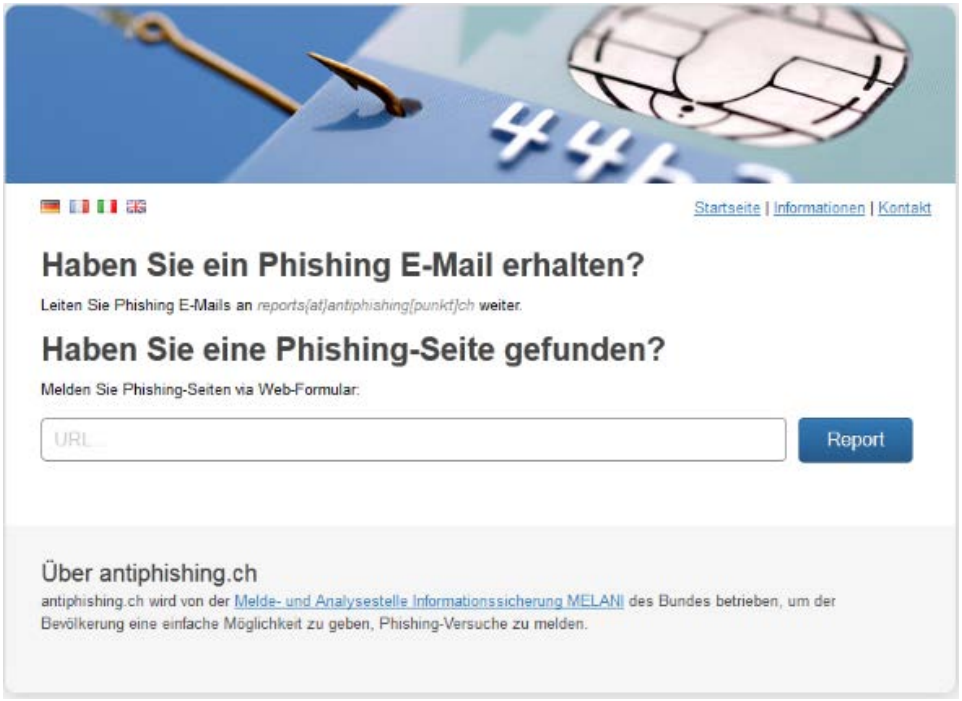


Fig. 6: Copie d'écran du nouveau site antiphishing.ch, sur lequel les citoyens peuvent signaler des pages de phishing.

Toutes les annonces de phishing transmises sont automatiquement vérifiées. Sur la base des résultats de cet examen préliminaire, les annonces seront soigneusement contrôlées par un collaborateur, avant d'être transmises aux fabricants de logiciels de sécurité informatique, aux navigateurs Web, aux hébergeurs et, sur demande, aux établissements financiers et fournisseurs de service Internet touchés, afin d'obtenir un effet de protection maximale.

5 Situation internationale

5.1 Espionnage

5.1.1 Cyberattaque contre le Parlement allemand

Le 15 mai 2015, on a appris que le réseau du Parlement allemand, baptisé «Parlakom», avait subi une attaque ciblée, et que les pirates avaient copié quelque 16 gigaoctets de données.[25] Les pirates étaient à l'affût de mots de passe système, de documents Word et de courriels enregistrés localement. D'après le quotidien Die Welt, l'infection aurait débuté, comme bien souvent, par l'envoi de courriels ciblés et de liens spécialement préparés.[26,27] Selon un procès-verbal, rendu public par la presse, d'une commission du Bundestag allemand [28], une «communication inhabituelle» entre des systèmes de serveurs avait été détectée le 8 mai 2015. Un serveur de l'administration du Bundestag aurait reçu une quantité anormalement élevée de données. En outre, des liaisons non prévues avec un bureau des députés aboutissaient à ce serveur. Quatre jours plus tard, une nouvelle analyse révélait que deux ordinateurs auraient été en contact avec des serveurs potentiellement dangereux, soit des *serveurs de commande et de contrôle (C&C)*. Il s'agissait des mêmes systèmes ayant déjà eu des réactions suspectes quelques jours plus tôt. Apparemment, seuls quelques terminaux étaient concernés, mais les malfaiteurs auraient pénétré en profondeur dans le système, où ils pouvaient se mouvoir librement, et ils risquaient de reprendre leur activité à tout moment.

Il a été difficile par la suite d'expulser les intrus du réseau. Comme mesure concrète, les responsables ont envisagé de renouveler une partie du réseau. Le réseau interne du Bundestag a donc été désactivé pour quatre jours le 20 août 2015, afin de réparer les dégâts dus à la cyberintrusion. Cette mesure radicale montre la portée de l'incident, mais n'offre bien entendu aucune garantie contre de futures infections.

Le procureur général examine si dans cette affaire, des indices donnent à penser qu'une infraction relevant de sa compétence aurait été commise. Le programme d'espionnage utilisé pour lancer cette attaque aurait été identifié. On a supposé qu'il s'agissait du groupe de pirates russes désigné sous le nom de Sofacy ou d'APT28.[29] La structure du programme s'apparenterait à un maliciel déjà observé en 2014 lors d'une cyberattaque contre un réseau de données allemand.

5.1.2 Carbanak – hold-up en ligne

Dans le passé, les attaques informatiques lancées contre les banques ne s'en prenaient qu'aux clients finaux. Un *maliciel* d'e-banking infectait l'ordinateur d'un client, et prenait le contrôle de sa session d'e-banking. Des cyberattaques d'un genre nouveau, rendues publiques en février 2015, ont servi à cambrioler virtuellement des banques. Pendant deux

---

25 http://www.spiegel.de/politik/deutschland/cyberangriff-auf-bundestag-abgeordneten-e-mails-erbeutet-a-1039388.html (état: le 31 août 2015).

26 http://www.welt.de/politik/deutschland/article142372328/Verfassungsschutz-verfolgt-Spur-nach-Russland.html (état: le 31 août 2015).

27 https://www.tagesschau.de/inland/bundestag-cyberattacke-105.html (état: le 31 août 2015).

28 http://www.bild.de/politik/inland/bundestag/spielte-cyber-angriff-laut-geheimprotokoll-herunter-41314062.bild.html (état: le 31 août 2015).

29 http://www.focus.de/politik/deutschland/bundestag-cyber-angriff-auf-bundestag-dauert-schon-laenger-als-bekannt_id_4761526.html (état: le 31 août 2015).

ans, des systèmes bancaires ont été manipulés à grande échelle par un programme baptisé «Carbanak». Les efforts déployés dans ce cadre rappellent les attaques d'espionnage ciblées d'origine étatique. Des tentatives ont d'abord été faites pour infecter les ordinateurs d'employés de banque. La méthode classique a été utilisée, méthode qui consiste à envoyer de manière ciblée un courriel avec un maliciel annexé. Les agresseurs ont ensuite localisé les postes informatisés d'où les collaborateurs gèrent les versements, ainsi que les distributeurs automatiques de billets connectés au réseau. Ils ont passé deux à quatre mois dans le réseau, afin de découvrir comment utiliser à leur profit les processus internes à la banque.[30] Après avoir collecté les informations requises, les escrocs se sont fait passer pour les employés de banque et se sont versé de l'argent, ou ont manipulé les distributeurs automatiques afin que ceux-ci leur remettent une forte somme à un moment précis. Un complice attendait vers l'automate en question et s'emparait des billets. Et pour que leurs agissements passent inaperçus, les malfaiteurs commençaient par alimenter les comptes avant d'y prélever exactement le même montant.

Selon Kaspersky, les malfaiteurs auraient infiltré au moins 100 banques situées dans 30 pays, principalement en Russie. L'argent détourné justifie les efforts accomplis – pendant deux ans parfois: les montants subtilisés vont jusqu'à 10 millions de dollars par banque.

5.1.3 Espionnage des Cartes SIM par la NSA et le GCHQ

De nouvelles révélations basées sur les documents publiés par Edward Snowden ont été faites au semestre dernier. Elles concernaient notamment les *cartes SIM*, soit les cartes insérées dans les téléphones mobiles et qui servent à identifier l'utilisateur du réseau. Selon le quotidien en ligne The Intercept, une unité commune des services secrets britanniques (GCHQ) et de la NSA appelée Mobile Handset Exploitation Team (MHET) aurait compromis les réseaux internes des grands fabricants de cartes SIM, des principaux fabricants de terminaux ainsi que de nombreux exploitants de réseaux. A commencer par le fabricant de cartes SIM Gemalto. Ce dernier a confirmé avoir observé ou reconnu dans son réseau, en 2010 et en 2011, des attaques raffinées faisant penser aux activités déployées par la NSA et le GCHQ. En juillet 2010, des collaborateurs auraient aussi reçu des envois ciblés de courriels[31]. Les agresseurs s'intéressaient surtout aux échanges de clés entre les opérateurs mobiles et leurs fournisseurs, échanges généralement chiffrés depuis 2010. Leurs attaques visaient exclusivement la bureautique, à l'exclusion des réseaux de production. On ignore si la NSA en est réellement l'auteur. Gemalto a écarté l'hypothèse d'un vol massif des clés de chiffrement de cartes SIM, ce qui aurait été le pire scénario pour un spécialiste du cryptage.

5.1.4 Espionnage dans le sport professionnel

Il n'est guère étonnant que le cyberespionnage s'en prenne aussi au sport professionnel, où l'on brasse de très grosses sommes. La ligue américaine de baseball en a fait l'expérience. Les Cardinals de Saint Louis et les Houston Astros sont deux équipes qui s'affrontent depuis des années dans les stades. Or des collaborateurs des Cardinals ont apparemment décidé de s'imposer aussi dans le cyberespace. Ils ont ainsi collecté toutes sortes d'informations (statistiques à l'entraînement et en match des joueurs, conditions contractuelles, achats de joueurs envisagés, stratégies, etc.), qui peuvent naturellement s'avérer très précieuses.

---

30 http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide (état: le 31 août 2015).

31 http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx (état: le 31 août 2015).

Les Cardinals n'auraient pas digéré le départ de leur ancien directeur général, Jeff Luhnow, qui a rejoint Houston en 2011. Cet ancien consultant a la réputation de mettre l'accent sur les analyses statistiques. Du temps où il dirigeait les Cardinals, il identifiait déjà et recrutait les jeunes talents à fort potentiel pour son équipe à l'aide d'une base de données et d'une forme de dépistage électronique très fructueuse. Après son recrutement par les Astros, il a proposé d'utiliser les mêmes méthodes pour relancer l'équipe et s'est imposé. Les Cardinals ont publiquement exprimé leurs craintes que Luhnow ait divulgué à ces adversaires des informations à leur sujet.

A l'ère du numérique et dans un monde toujours plus interconnecté, le sport subit lui aussi des pressions en vue de sa modernisation. Les analyses et les statistiques sont de plus en plus largement utilisées, et du même coup les abondantes données collectées s'avèrent d'attrayantes cibles d'espionnage. Dans le baseball en particulier, les analyses des performances sont d'autant plus répandues que les variables peu nombreuses et se rapportant à des individus permettent de procéder à des mesures. De telles méthodes sont moins répandues dans le football et en hockey sur glace, où ce ne sont pas directement des individus, mais deux équipes qui s'affrontent et où les variables sont donc plus nombreuses. Le club de football Manchester City a néanmoins lancé en 2012 un concours visant à encourager les jeunes analystes à développer des méthodes dans ce secteur.

5.2 Fuites d'informations

5.2.1 Piratage de 21,5 millions de données sur les fonctionnaires américains

En avril 2015, l'Office of Personnel Management (OPM, homologue américain de l'Office fédéral du personnel, OFPER) a découvert que des données personnelles de 4,2 millions de fonctionnaires actuels ou d'anciens agents avaient été copiées. Les informations piratées comprenaient le nom, la date de naissance, l'adresse et le numéro de sécurité sociale. En analysant l'incident, l'OPM a constaté un second vol de données encore plus massif, incluant des données sensibles d'employés et partenaires contractuels tant présents qu'anciens et futurs. Le second assaut englobe selon toute probabilité 21,5 millions de données individuelles et d'informations recueillies lors de contrôles de sécurité.[32] Quelque 19,7 millions d'informations proviendraient de personnes ayant sollicité un emploi, les 1,8 million de données restantes étant liées aux proches des candidats, comme le conjoint ou les colocataires. On trouve encore parmi les données dérobées les conclusions des inspections réalisées sous forme d'entretiens, sans oublier des renseignements sur la santé psychique ou les antécédents financiers. De même, 1,1 million d'empreintes digitales ont été copiées. En 2014, le service d'audit interne de l'OPM avait recommandé d'abandonner onze des 47 systèmes informatiques, faute de certificat de sécurité valable. L'OPM n'avait pas suivi cette recommandation. On ignore si l'intrusion s'est faite par l'un des systèmes vulnérables. Cette attaque, la plus grave à ce jour menée contre un réseau informatique du gouvernement américain, a coûté son poste à la directrice de l'OPM.

Les enquêteurs américains pensent qu'un groupe chinois serait à l'origine de ces attaques lancées contre l'administration fédérale. Comme il fallait s'y attendre, la Chine a aussitôt démenti toute implication dans ces opérations.

[32] https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/ (état: le 31 août 2015).

Les services du personnel intéressent spécialement les pilleurs de données. A fortiori quand toutes les données des employés d'une administration ou d'un groupe sont collectées et gérées au même endroit. Comme il s'y traite des masses de documents de provenances diverses, le potentiel de nuisance d'un maliciel qui se serait infiltré par l'une ou l'autre de ces sources sera d'autant plus grand.

Sachant que les contrôles de sécurité amènent l'Etat à récolter des informations personnelles sur des candidats ou des tiers ne travaillant pas pour lui, les autorités suisses devraient elles aussi se demander comment il faut gérer de telles données, et s'il y a réellement lieu de les conserver à l'issue des vérifications préliminaires, quand la personne n'est pas embauchée.

5.2.2 AdultfriendFinder, British Airways ou assurance-maladie – fuites d'informations dans toutes sortes de branches

La quête d'aventures amoureuses se fait toujours plus en ligne. Grâce aux développements d'Internet et aux possibilités qu'offrent les médias sociaux, il est encore plus simple de trouver la personne adéquate. Mais si le portail utilisé est victime de cybercriminels qui publient les données des utilisateurs, avec leurs préférences sexuelles, c'en est fini de l'anonymat tant prisé. Le site de rencontres Adultfriendfinder[33] a commis un tel faux pas en mai dernier. Près de quatre millions de données d'utilisateurs ont abouti sur un forum, où n'importe qui pouvait apprendre qui se cache derrière les noms d'emprunt. Le site de rencontres extra-conjugales Ashley Madison[34] a subi en juillet une attaque encore plus spectaculaire: les données d'accès de 32 millions d'utilisateurs ont été publiées.

Des fuites de données autrement plus sensibles ont été signalées au premier semestre. British Airways s'est ainsi fait dérober les données de la clientèle de son programme de fidélisation[35]. De telles informations permettent notamment de reconstituer les profils de déplacement des individus.

La situation devient encore plus délicate quand des données fiscales détaillées tombent entre de mauvaises mains, mésaventure survenue en mai à l'administration fiscale américaine (IRS)[36]. Des méthodes d'ingénierie sociale avaient permis aux agresseurs de contourner un processus d'authentification de l'IRS, afin de s'emparer de données au nom des contribuables concernés.

Les données de patients sont tout aussi sensibles. Personne n'a envie que tout le monde soit au courant de ses visites chez le médecin ou de ses maux. Or ces données sensibles ne sont pas toujours à l'abri des regards indiscrets. En février le groupe Anthem[37], deuxième plus grand assureur-maladie américain, a déploré une intrusion dans sa banque de données de 80 millions de clients. Un autre assureur-maladie (Premera Health Care)[38] a lui aussi été victime d'un vol de données en mars.

---

33 http://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web (état: le 31 août 2015).

34 http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (état: le 31 août 2015).

35 http://www.theregister.co.uk/2015/03/29/british_airways_frequent_flyers_hacked/ (état: le 31 août 2015).

36 http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application (état: le 31 août 2015).

37 http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (état: le 31 août 2015).

38 http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html (état: le 31 août 2015).

Les exploitants feront bien de se rappeler qu'un pirate motivé n'a de respect pour personne. D'où la recommandation de prendre toutes les précautions possibles pour éviter de se faire dérober des données. Notre aide-mémoire pour les PME concernant la sécurité informatique donne un bon aperçu de la situation:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

5.3 Systèmes de contrôle industriels

Après les *systèmes de contrôle industriels et les systèmes SCADA*, devenus au cours des dernières années un véritable objet de recherche et d'expérimentation, les experts en sécurité informatique s'intéressent désormais aussi aux composantes installées dans les automobiles, les trains, les bateaux et les avions – aujourd'hui où toutes sortes d'appareils sont mis en réseau et reliés à Internet, y compris les moyens de transport. En effet les compagnies aériennes, les opérateurs ferroviaires et les compagnies de navigation tiennent à ce que leurs passagers aient accès à Internet à bord, et même les automobiles sont toujours plus souvent reliées au réseau.

Il convient de distinguer ici entre deux aspects, soit l'accès à l'offre d'information et de divertissement en ligne, d'une part, et le recours à l'électronique et aux technologies de l'information pour le pilotage opérationnel du moyen de transport, et donc comme système d'aide à la conduite.

Alors que le premier cas suppose l'accès au Web, il faut encore distinguer dans le second cas entre les applications tributaires d'informations extérieures (par ex. données *GPS*, prévisions météo et informations routières) et les systèmes purement internes, soit par ex. dans une automobile la jauge à carburant, le contrôleur de pression des pneus ou la caméra de recul – mais aussi les systèmes d'assistance basés sur l'interaction entre des capteurs et des actionneurs, qui maintiennent une distance constante par rapport au véhicule précédent, accélèrent et freinent automatiquement, ou se chargent des manœuvres de stationnement.

5.3.1 Sécurité dans la branche automobile

Les véhicules automobiles pouvaient déjà être contactés par voie électronique avant même d'être connectés à Internet par le réseau sans fil. Des escrocs ont d'emblée su tirer parti du verrouillage électronique des portes: en épiant les signaux émis par la clé, afin de pouvoir ouvrir eux-mêmes plus tard la porte (la plupart des fabricants ont entre-temps identifié et corrigé le problème), ou en brouillant le signal pour que la porte ne reçoive pas la commande de verrouillage.

Désormais les véhicules s'apparentent toujours plus à des ordinateurs ambulants: au garage, on commence souvent par brancher un ordinateur portable de diagnostic pour savoir comment ils se portent. Une telle interface donne accès à toute l'électronique de la voiture – ce qui est prévu et ne constitue pas une faiblesse en soi (it's not a bug, it's a feature). Pourtant, de telles interfaces peuvent servir de vecteur d'attaque – à condition d'avoir typiquement un accès physique au véhicule. Par contre, divers systèmes communiquent aussi entre eux sans fil: par ex., les contrôleurs de pression des pneus transmettent leurs valeurs de mesure et le téléphone mobile est relié par *Bluetooth* à l'électronique du véhicule, pour permettre d'utiliser le dispositif mains libres intégré. En outre, certains véhicules disposent d'un raccordement mobile leur permettant d'envoyer et de recevoir des informations par Internet. Un tel équipement sert non seulement aux services d'entretien, mais permet également au fabricant, le cas échéant, de connaître l'emplacement du véhicule, d'ouvrir à distance ses portes (si l'on a oublié ses clés à l'intérieur) ou d'activer le dispositif d'immobilisation, en cas de déclaration de vol. Or ces fonctions supposent une liaison entre l'informatique et l'électronique du véhicule, qui est donc susceptible de subir des cyberattaques.

Il paraît évident que dans un véhicule, les systèmes de divertissement doivent être clairement séparés de l'électronique opérationnelle, afin que celle-ci ne puisse être manipulée de l'extérieur soit directement, soit par le biais d'équipements de divertissement compromis. Or les fabricants ne respectent pas toujours cette règle, comme des chercheurs l'ont récemment démontré à plusieurs reprises et pour diverses marques automobiles.

Bien souvent, il n'y a pas de cloison étanche entre les diverses composantes. D'où d'audacieux piratages, comme la manipulation des systèmes d'assistance au moyen de maliciels infiltrés par un CD dans l'autoradio, voire par le système de radiodiffusion de données (RDS, *radio data system)*[39]. En donnant des ordres aux systèmes d'assistance – par maliciel ou par connexion sans fil directe –, il devient possible le cas échéant de faire accélérer, freiner ou bifurquer la voiture. En outre, il est possible de provoquer des réactions inadéquates des systèmes d'assistance, en faussant les valeurs transmises par les capteurs.

La communication sans fil à l'intérieur d'un véhicule doit toujours être chiffrée. Ce serait trop facile sinon de la lire et de l'intercepter. En outre, les différents composants devraient s'authentifier mutuellement. Moyennant de telles précautions, il sera très difficile de donner au véhicule des instructions malveillantes, ou de fausser les valeurs de ses capteurs. Par ailleurs, il faut s'assurer que les composants qui communiquent en ligne ne permettent pas à des pirates d'accéder au système électronique de bord.

[39] http://www.bbc.com/news/technology-33622298 (état: le 31 août 2015)

5.3.2 Redémarrage du système d'un Boeing 787 Dreamliner

La solution recommandée aux utilisateurs informatiques quand une application de bureau ne fonctionne pas comme elle devrait, semble parfois fonctionner avec les avions aussi: un redémarrage s'avère utile non seulement pour les ordinateurs professionnels ou privés, mais porte ses fruits dans certains cas même avec le Dreamliner de Boeing.[40]

Le Dreamliner fait lui aussi appel à de nombreux logiciels. Les tests effectués dans les laboratoires internes de Boeing ont révélé, lors des contrôles du logiciel de commande des générateurs assurant la production électrique, que la commande automatique du système de sécurité (*fail safe modus*) s'enclenchait après 248 jours, en raison de la saturation du compteur. D'où une panne de courant dans l'avion. La solution au problème est simple, et consiste à redémarrer le logiciel de commande du Dreamliner.

Les passagers n'ont heureusement rien à craindre. Comme un tel redémarrage intervient lors des vérifications de routine, le compteur ne risque pas d'être saturé.

5.3.3 Systèmes d'infodivertissement des avions

Chris Roberts, chercheur américain en sécurité informatique, prétend avoir découvert dans le système de divertissement en vol (*in-flight entertainment*, IFE) des avions de type Boeing 757-200, Boeing 737-800, Boeing 737-900 et Airbus A-320, des failles donnant accès à des systèmes critiques de l'électronique embarquée (*on board electronic*). Le 13 février 2015, il a spontanément informé de ses découvertes la police fédérale (FBI), dans l'espoir que les failles de sécurité seraient corrigées. Or le FBI l'a arrêté à sa descente d'avion le 15 avril, pour s'être vanté dans un Tweet de pouvoir manipuler le contrôle des masques à oxygène des passagers, et les appareils qu'il portait sur lui ont été confisqués.

Selon le mandat de perquisition sollicité après cet incident le 17 avril 2015[41], Roberts portait sur lui plusieurs instruments lui permettant de faire des tests de pénétration dans toutes sortes d'environnements de réseau. En outre, des schémas de câblage et toute une documentation technique sur les systèmes de commande de vol et d'information ont été confisqués à son domicile. Les experts en avionique ont confirmé que les instructions de commande publiées par Roberts existaient bel et bien dans les protocoles correspondants. Par ailleurs, les vérifications opérées dans l'avion après son arrestation à l'aéroport de Syracuse ont révélé qu'il avait forcé les deux boîtiers SEB (*seat electronic box*) des sièges passager situés devant lui. Lui-même prétendait avoir accédé ainsi au système IFE, grâce à des câbles Ethernet munis de connecteurs modifiés, et avoir pu de là s'introduire dans d'autres systèmes embarqués, suite à des tests de pénétration.

Dans l'incident décrit par Roberts, tout indique qu'il a au moins essayé de pénétrer dans les systèmes IFE et, à partir de là, de s'introduire dans d'autres parties du réseau. Si les mesures de sécurité s'étaient avérées insuffisantes, ses connaissances techniques et ses outils lui auraient permis d'arriver à ses fins. Il n'est cependant pas entièrement exclu que ses démarches aient été couronnées de succès. Mais il est aussi possible qu'il ait exagéré les faits, à des fins de marketing personnel.

---

40 https://s3.amazonaws.com/public-inspection.federalregister.gov/2015-10066.pdf (état: le 31 août 2015).

41 http://www.wired.com/wp-content/uploads/2015/05/Chris-Roberts-Application-for-Search-Warrant.pdf (état: le 31 août 2015).

5.3.4 Panne de courant – soupçon non confirmé de cyberattaque

Ce n'est que lorsque quelque chose tombe en panne que l'on réalise à quel point on en est tributaire. Le 27 mars 2015, bien des personnes qui séjournaient aux Pays-Bas ont sans doute repensé à cette vérité élémentaire. Ce jour-là, les feux de signalisation, les moyens de transport publics et les antennes de téléphonie mobile ont cessé de fonctionner après une gigantesque panne électrique. Les supermarchés ont dû fermer, car leurs caisses enregistreuses et les systèmes antivol ne fonctionnaient plus. Il a fallu évacuer les ascenseurs et fermer les écoles.[42] Des vols au départ de l'aéroport de Schiphol ont été annulés et faute de pouvoir y atterrir, les avions ont été redirigés vers d'autres aéroports. Même si des voix isolées ont cru à une cyberattaque, la panne provenait de la surcharge d'un transformateur situé dans une banlieue d'Amsterdam. Dans le passé, il est régulièrement arrivé qu'une défaillance provoque une réaction en chaîne, lorsqu'elle survenait à un emplacement central de la distribution d'électricité.

Les spéculations à propos d'une cyberattaque ont redoublé quelques jours après l'incident d'Amsterdam. Le 31 mars 2015, une panne d'électricité paralysait une grande partie de la Turquie: les villes d'Istanbul, Ankara et Izmir ont été privées de courant. Au total, 30 des 81 provinces turques – jusqu'à 80 selon d'autres sources – auraient été affectées. Ce n'est que dix heures plus tard que le ministère turc de l'énergie annonçait le retour à la normale. Dans les grandes villes comme Istanbul et Ankara, les entreprises privées avaient pris leurs précautions, en s'équipant de générateurs de secours. L'événement n'y a donc eu que des conséquences limitées. Par contre, les transports publics ont été sérieusement perturbés, à l'instar du métro circulant sous la mer de Marmara. Là non plus, les rumeurs de cyberattaque n'ont pas été confirmées. La raison serait plutôt à chercher dans les fluctuations de tension, provoquées par l'arrêt de plusieurs centrales électriques.

5.3.5 Stations-service américaines: nouvelles cibles des cyberpirates?

Les distances sont longues sur la route 66, et selon la jauge à carburant il faudrait refaire le plein. La petite station-service qui surgit à l'horizon suscite de l'espoir, mais la pompe à essence est vide. Un tel scénario serait particulièrement désagréable. Mais la pompe à essence est-elle bien vide? Pas forcément. Des experts ont constaté la vulnérabilité des systèmes informatiques gérant les pompes, dans les stations-service américaines excentrées et gérées à distance pour cette raison[43]. Ainsi, 3 % des 150 000 indicateurs du niveau de remplissage des cuves n'étaient protégés par aucun mot de passe, et surtout pouvaient être configurés librement. D'où par exemple la possibilité de faire croire, en modifiant les paramètres, qu'une station-service aux cuves vides dispose de réserves suffisantes, avec pour effet l'absence de ravitaillement. En outre, des instructions spécifiques pourraient aisément mettre les pompes à essence hors service.

---

42 http://nos.nl/artikel/2027141-noord-holland-heeft-weer-stroom.html (état: le 31 août 2015).

43 https://community.rapid7.com/community/infosec/blog/2015/01/22/the-internet-of-gas-station-tank-gauges (état: le 31 août 2015).

Il est délicat de raccorder à Internet, afin de pouvoir commodément les surveiller à distance, les systèmes initialement gérés au sein de réseaux cloisonnés. D'où l'utilité en pareil cas de la liste de contrôle MELANI «Mesures de protection des systèmes de contrôle industriels (SCI)».

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-protection-des-systemes-de-controle-industriels--sci-.html

5.4 Cyberattaques (DDoS, Defacements)

5.4.1 Ecran noir sur TV5MONDE

Parmi les nombreuses attaques ayant eu lieu au premier semestre 2015, celle ayant touché la chaîne de télévision francophone TV5MONDE le 8 avril a indéniablement marqué les esprits. C'était la première fois qu'une chaîne de télévision était autant malmenée. En plus d'être privée de sa présence sur Internet, son outil de production – et c'est là le caractère inédit de l'attaque – était lui aussi hors service.

5.4.1.1 Déroulement de l'attaque

Le 8 avril 2015, la chaîne TV5MONDE a subi une attaque comportant différentes facettes, qui a touché plusieurs outils de production ou plateformes. Elle a dû cesser de diffuser dès 22 heures, son infrastructure de diffusion des programmes ayant été sabotée. Ce n'est que trois heures plus tard que la chaîne est parvenue à réoccuper l'antenne, dans un premier temps avec des programmes préenregistrés. En parallèle, elle a perdu le contrôle de ses comptes Facebook et Twitter, détournés pour diffuser des messages de soutien au djihad. Le site Web de la chaîne a par ailleurs été défiguré. Selon les informations disponibles sur des sources ouvertes, l'attaque a encore paralysé la communication par courriel au sein de l'entreprise. L'attaque a rapidement été revendiquée par un groupe se faisant appeler Cyber Caliphate, affirmant son allégeance à l'Etat islamique. L'identité exacte de cet acteur et du commanditaire s'avérera cependant moins claire par la suite, rappelant à quel point le processus d'attribution d'une attaque reste périlleux (voir plus bas).

5.4.1.2 Vulnérabilité de l'outil de production?

La prise de contrôle de comptes de réseaux sociaux est un type d'incident souvent observé, notamment lors d'attaques visant à diffuser un message de soutien au djihad. En revanche, le blocage de l'outil de production d'une grande chaîne constitue une nouveauté. Pour être plus précis, c'est l'infrastructure servant à diffuser les programmes à l'antenne (encodeurs et multiplexeurs) qui a été touchée. Cet événement pose naturellement la question de l'exposition de ce type d'infrastructure. A moins d'un accès physique aux appareils, permettant par exemple de propager une infection par une clé USB, l'attaque suppose un accès à distance. Selon des éléments disponibles sur des sources ouvertes, différents systèmes de la chaîne étaient visibles depuis Internet, augmentant d'autant la surface d'attaque. La deuxième question que soulève ce type d'attaques est celle de la séparation entre le système bureautique et le système de production. Les détails à ce sujet ne sont pas connus, mais certains experts ont fait l'hypothèse de carences à ce niveau. Il est vrai que dans certains cas, c'est le système bureautique qui est d'abord infecté. Puis vient le tour du système de production, en l'absence de compartimentation efficace. Indépendamment des

mesures prises avant l'attaque, l'incident ayant touché TV5MONDE nous rappelle combien tout système de contrôle industriel doit être protégé.

L'accès à distance, lorsqu'il est absolument nécessaire, doit faire l'objet d'une procédure de sécurisation adéquate. Un document de MELANI fournit diverses recommandations à ce sujet:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-protection-des-systemes-de-controle-industriels--sci-.html

5.4.1.3 Difficile travail d'attribution

Au lendemain des attaques, aucun commentateur ne mettait en doute l'attribution à un groupe appartenant à la nébuleuse islamiste active sur Internet. Seule l'implication de l'Etat islamique était discutée. Ce n'est qu'au mois de juin que de nouveaux éléments ont amené à nuancer ces propos. Tout d'abord, il s'est avéré que les auteurs avaient pénétré le réseau en début d'année déjà. Ils ont ainsi eu tout loisir de l'explorer en long et en large, afin de repérer des systèmes intéressants. Autrement dit, l'attaquant possédait un degré relativement élevé de professionnalisation. Par ailleurs, des révélations journalistiques s'appuyant sur les analyses des entreprises de sécurité Trend Micro et FireEye ont évoqué une nouvelle piste, celle d'un lien entre cette attaque et une campagne de cyberespionnage baptisée Sofacy (également connue sous le nom de Pawn Storm et APT28), que l'on suppose être d'origine russe et étatique. Ces parallèles s'appuient sur différents indicateurs retrouvés sur les réseaux de TV5MONDE, et qui font partie de l'infrastructure de Sofacy. Si la présence de Sofacy sur les réseaux de TV5MONDE semble établie, les avis divergent sur le lien entre cette campagne et l'attaque d'avril 2015 ayant notamment occasionné une interruption des programmes. Une première hypothèse veut que l'attaque ait bien été menée par l'acteur responsable de Sofacy, qui aurait voulu faire croire à la piste islamiste («false flag»). Le principal défaut de cette interprétation est que ce type d'attaque ne cadre pas avec les méthodes et les buts de Sofacy, campagne d'espionnage extrêmement furtive. De même, l'intérêt potentiel d'un supposé acteur étatique russe pour ce genre d'action n'est guère évident, malgré les tensions avérées entre la France et la Russie sur le plan diplomatique à cette période[44]. Selon une deuxième hypothèse, le maliciel Sofacy aurait été implémenté par des groupes sympathisants du djihad. Aucun élément concret ne vient cependant soutenir cette explication, qui nécessiterait d'expliquer les modalités de l'acquisition du maliciel par les groupes en question. La troisième hypothèse, qui est aussi la plus plausible, est celle de deux opérations parallèles et non liées. Un acteur étatique russe peut très bien s'être intéressé à des médias comme TV5. Fidèle à son habitude, il aura cherché à pénétrer le réseau sur la durée, pour y acquérir des informations sensibles. Une cyberopération menée par un autre acteur, ayant comme but principal de faire passer un message de soutien au djihad, aurait conduit aux dégâts constatés en janvier.

5.4.1.4 Les médias, cible privilégiée

Dans son rapport semestriel 2014/1[45], MELANI soulignait déjà à quel point les médias étaient des cibles intéressantes – et vulnérables – pour des attaques informatiques.

[44] Tensions liées à la vente de deux navires de guerre Mistral de la France à la Russie, puis son annulation.

[45] MELANI rapport semestriel 2014/1, chapitre 5.2: https://www.melani.admin.ch/melani/fr/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-1.html (état: le 31 août 2015).

L'attaque contre TV5 confirme cette tendance, qui ne concerne pas uniquement la presse écrite. Les médias sont intéressants car ils traitent un grand nombre d'informations parfois sensibles, mais également parce qu'ils offrent un retentissement maximal à un acteur souhaitant faire passer un message de propagande ou diffuser des informations falsifiées. Par ailleurs, certains éléments inhérents à l'activité d'un média sont difficilement compatibles avec des exigences sécuritaires qui devraient justement être particulièrement élevées. On pense par exemple à la nécessité de pouvoir passer rapidement de la réception au traitement, puis à la publication d'une information. En outre, il s'avère difficile de mettre en place des protocoles de communication sécurisés en présence d'une multitude de correspondants, parfois indépendants, mobiles et se trouvant à de nombreux endroits différents. Enfin, il faut souligner que les acteurs visant ce type de cibles ont bien souvent beaucoup plus de ressources à allouer à l'attaque que les médias n'en ont pour assurer leur défense.

Au vu des risques nombreux et variés qui les guettent (par ex.: attaques DDoS, espionnage, sabotage), il convient pour les médias d'intégrer des procédures de sécurité à la fois préventives et réactives. L'entreprise doit notamment être en mesure de détecter les intrusions ou d'autres événements anormaux, et de mettre en place des mesures d'urgence adaptées aux différents scénarios.

5.4.2 Cyberattaque: annulation de vols de Polish Airlines

Les cyberattaques lancées contre les moyens de transport, comme le rail ou l'avion, suscitent un vif intérêt mêlé de crainte. Le 21 juin 2015, un incident a fait les gros titres, laissant d'abord supposer un problème majeur. Suite à une cyberattaque lancée contre son système informatique, la compagnie Polish Airlines (LOT) a dû annuler certains vols, laissant sur le carreau 1400 passagers au total. Elle ne parvenait plus à générer les plans de vol (informations détaillées sur les aéroports de départ et d'arrivée, route suivie, etc.). De telles données sont notamment utilisées par les aiguilleurs du ciel, pour optimiser la trajectoire de vol. S'il n'est pas possible de les transmettre ou de les imprimer, les avions ne peuvent pas décoller. Aucun détail n'a filtré ce jour-là sur les circonstances de l'incident.[46]

Le lendemain, le porte-parole a parlé d'une surcharge du réseau due à une attaque par déni de service distribué. Il n'a toutefois pas dit si cette dernière était ciblée ou non, ni quel était le genre d'attaque et son ampleur. Normalement, les systèmes d'importance vitale reliés à Internet devraient être dûment protégés contre les *attaques DDoS.* Sebastian Mikosz, CEO de LOT, a expliqué qu'il s'agissait d'un problème général auquel toute l'industrie est confrontée. A ses yeux, une telle mésaventure pourrait se produire n'importe quand et partout.

Ruben Santamarta, conseiller en sécurité informatique d'IOActive, a évoqué un possible renversement de tendance dans le secteur aérien, lui aussi susceptible de tenter les cybercriminels. En effet, les systèmes de sécurité en place dans la navigation aérienne ont suscité un intérêt croissant au cours des derniers mois. On le voit par exemple au cas exposé au chap. 5.3.3, où un individu a tenté d'accéder via le système d'infodivertissement aux commandes de vol de l'appareil.

---

[46] http://www.reuters.com/article/2015/06/22/us-poland-lot-cybercrime-idUSKBN0P21DC20150622 (état: le 31 août 2015).

On constate actuellement un intérêt accru des chercheurs en sécurité pour les moyens et les entreprises de transport. Mais les cybercriminels s'y intéresseront-ils pour autant? De façon générale, il faut toujours distinguer entre les systèmes ayant besoin d'être reliés à Internet et ceux qui, pour des raisons de sécurité, ne le sont pas. La première catégorie comprend notamment les systèmes de réservation et tous les systèmes qui reposent sur des échanges entre différents services. Dans de tels cas, les modèles d'affaires classiques comme le chantage aux attaques *DDoS* ou le vol des données d'utilisateur suivi de chantage fonctionnent comme dans n'importe quelle autre branche. Il est donc permis de supposer qu'à l'avenir de tels systèmes (à l'instar de tous les autres secteurs) seront eux aussi pris pour cibles par les cybercriminels. Mais dans le cas d'espèce, il paraît exagéré de parler d'un retournement de tendance dans le secteur aérien.

5.4.3 Cyberattaques lancées après l'attentat contre Charlie Hebdo

L'attentat de janvier 2015 contre la rédaction parisienne de Charlie Hebdo a eu des répercussions sur Internet, moins dévastatrices toutefois que les tragiques fusillades. Le nombre de ces attaques virtuelles, estimé entre-temps à 25 000, impressionne toutefois davantage que leur qualité intrinsèque. Dans la plupart des cas, il s'agissait de *defacement*, soit de l'exploitation de failles de sécurité de sites Web pour y introduire des slogans politiques ou religieux. Un visiteur y aurait découvert des phrases comme «Mort à la France» ou «Mort à Charlie Hebdo». La plupart des attaques ont été menées par des groupes baptisés par exemple «Middle East Cyber Army», «Fallaga team» et «Cyber Caliphate». Loin d'être concertées, les opérations étaient en réalité arbitraires, ce qui correspond à l'usage en pareil cas. Des écoles, des universités, des églises et des entreprises en ont ainsi pâti. Les victimes n'ont pas été choisies de façon ciblée. Les pirates se sont contentés de repérer des systèmes vulnérables et d'en exploiter systématiquement les lacunes de sécurité. Cette méthode est très courante parmi les pirates à motivations religieuses. Alors qu'en temps normal les attaques sont menées au niveau mondial, en cas d'incident les forces se concentrent sur une cible visible. Des sites romands ont aussi subi les retombées de ces attaques (voir chap. 4.4.2).

Une branche belge d'Anonymous s'est aussi engagée dans le conflit. Elle avait réagi en annonçant qu'elle suivrait de près toutes les activités en ligne des djihadistes, pour verrouiller leurs comptes Twitter, YouTube et Facebook.

5.4.4 Piratage du site Web de l'armée américaine

En juin 2015, l'armée américaine a été confrontée à une attaque contre son infrastructure Web. Défiguré par de la propagande, son site officiel www.army.mil a dû être brièvement retiré du réseau. Cette page ne renfermant pas de données confidentielles ou personnelles, il n'était cependant pas non plus possible d'en dérober. L'Armée électronique syrienne a revendiqué l'attaque via Twitter. Ce groupe avait déjà attiré l'attention sur lui dans le passé par plusieurs agressions, notamment contre de différents médias[47]. Il ne cherche pas à

[47] MELANI, rapport semestriel 2013/1, chapitre 4.4: https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2013-1.html (état: le 31 août 2015).
MELANI, rapport semestriel 2013/2, chapitre 4.8: https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2013-2.html (état: le 31 août 2015).

dérober des données, mais à faire de la désinformation et à placer des messages politiques. Le Pentagone a également souligné qu'il ne s'agissait que de cybervandalisme.

En janvier déjà, des adeptes supposés de l'Etat islamique s'étaient brièvement emparés des comptes Twitter et Youtube du CENTCOM (Commandement central des Etats-Unis). Pendant ces 30 minutes de cauchemar, son compte Twitter a affiché le texte «Cyber Caliphate» et des images de propagande. Là aussi, il s'agissait d'une attaque rudimentaire; les pirates se seraient procuré les données d'accès du compte en expédiant des courriels de phishing à partir d'adresses usurpées (*spear phishing*). Youtube et Twitter proposent entre-temps des méthodes d'authentification à deux facteurs, pour déjouer de telles attaques. Les comptes piratés n'y recouraient semble-t-il pas encore.

5.4.5 Superfish/Lenovo

Le fabricant de PC et de Notebooks Lenovo a commercialisé des ordinateurs portables équipés d'un logiciel préinstallé du nom de Superfish. Or il s'agit, selon les experts en sécurité informatique, d'un logiciel publicitaire (*adware*) qui peut notamment injecter des annonces de tiers dans le navigateur, lors d'une recherche dans Google.

En février 2015, on a appris que Superfish installait son propre certificat racine dans le magasin de certificats Windows. D'où la possibilité pour ce logiciel intrusif de se faire passer pour n'importe quel site Web (par ex. Google) et de réaliser des injections même en cas de connexion chiffrée via HTTPS. Et comme la clé secrète du certificat racine installé par Superfish est programmée dans le logiciel, il est techniquement possible de l'extraire de Superfish. Des escrocs peuvent dès lors émettre des certificats pour n'importe quel site Web, que les appareils Lenovo jugeront ensuite digne de confiance.

Superfish rend vulnérables par ex. aux attaques de l'intermédiaire (man-in-the-middle-attack, MITM) les machines sur lesquelles il a été préinstallé. Il serait ainsi possible en théorie à un escroc de se faire passer pour une banque, afin de dérober les informations de connexion de sa victime (nom d'utilisateur, mot de passe et jeton) à des fins de fraude à l'e-banking.

Lenovo a publié sur son site une déclaration officielle concernant Superfish[48].

[48] http://forums.lenovo.com/t5/Lenovo-P-Y-and-Z-series/Removal-Instructions-for-VisualDiscovery-Superfish-application/ta-p/2029206 (état: le 31 août 2015).

MELANI recommande aux utilisateurs d'appareils Lenovo de vérifier si Superfish y est installé, et le cas échéant de désinstaller ce logiciel. Le site suivant permet de savoir si un appareil présente ce problème.

Superfish, Komodia, PrivDog vulnerability test (en anglais)

https://filippo.io/Badfish/

En outre, Lenovo a fourni un outil permettant d'éliminer Superfish (désinstallation):

https://support.lenovo.com/us/en/product_security/superfish_uninstall

Lorsqu'ils sont destinés à un usage particulièrement sensible, MELANI recommande de reformater les ordinateurs fixes ou portables avant de s'en servir, et d'y installer à nouveau le système d'exploitation. Cette précaution permet d'éviter que des logiciels préinstallés et qui sont inutiles voire indésirables (par ex. adware) ne perturbent le fonctionnement de l'appareil ou ne transmettent des données sensibles à des tiers à l'insu de l'utilisateur.

5.4.6 Kits d'exploits

Un kit d'exploits (*exploit kit*) est un outil servant aux pirates à exploiter les failles des terminaux, soit directement dans le navigateur, soit par le biais de logiciels utilitaires comme Flash, Acrobat Reader ou Java.

Conçus pour pouvoir être utilisés presque sans connaissances informatiques, les kits d'exploits reflètent la division poussée des tâches au sein des groupes criminels. En règle générale, il s'agit d'une interface Web offrant les fonctions requises – choix des exploits, statistiques des appareils infectés, autres possibilités de configuration, etc.

Le mode opératoire des groupes criminels est presque toujours le même:

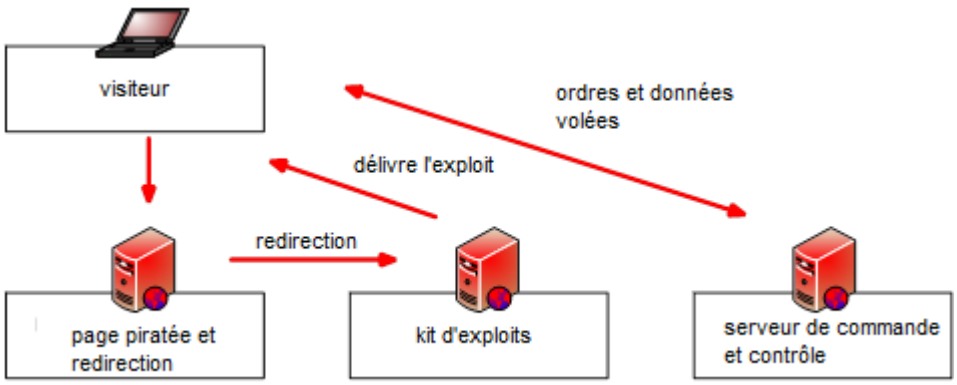


Fig. 7: schéma illustrant le fonctionnement d'un kit d'exploits

Le pirate détourne un maximum de victimes potentielles vers son kit d'exploits. Il peut le faire de diverses manières:

- en s'emparant de sites Web qui utilisent un CMS vulnérable, et en y plaçant une redirection cachée vers le serveur où est installé son kit d'exploits. Il est par

conséquent essentiel que tous les exploitants de sites protègent leur CMS et l'actualisent régulièrement;[49,50]

- en plaçant de la publicité attirant les visiteurs sur de tels sites. A cet effet, le pirate peut acheter de telles bannières, ou s'emparer de serveurs de publicité vulnérables;
- en achetant à un prestataire de service le trafic correspondant. Les exploitants de systèmes de distribution du trafic (*traffic distribution system, TDS)* ne sont pas tous des criminels, et redirigent souvent les flux de visiteurs dans le contexte légal.

Le kit d'exploits lui-même analyse souvent les appareils-cibles à l'aide de *JavaScripts*, qui contrôlent les plugiciels installés et leurs versions pour repérer une lacune propice et l'attaquer à l'aide d'un exploit. On trouve de nombreux kits d'exploits, aux performances variées. Les plus connus sont Angler, Neutrino, Rig, Nuclear et Magnitude. Lorsque de nouvelles failles de sécurité sont publiées, les kits d'exploits se mettent à jour étonnamment vite. Tous ne comportent pas les mêmes exploits, et les variations peuvent être considérables.[51] Par ailleurs, il est toujours plus fréquent que les kits d'exploits incluent des *0-day-exploits*.[52]

Les criminels ordinaires ne sont pas seuls à se servir de kits d'exploits, les agresseurs étatiques y recourent parfois aussi pour leurs activités d'espionnage.

5.4.7 Failles de sécurité LogJam et FREAK

FREAK et LogJam, deux failles de sécurité majeures rendues publiques durant la période sous revue, peuvent affecter les connexions sécurisées. Toutes deux résultent des restrictions d'exportation auxquelles les Etats-Unis soumettaient dans le passé leurs produits cryptographiques. En effet, le code source des bibliothèques cryptographiques renferme encore parfois les solutions de repli (*fallback function*) correspondantes, qu'il suffira d'activer lors d'une attaque pour déchiffrer les communications.

FREAK (Factoring Attack on *RSA*-EXPORT Keys) permet d'accepter pour certains navigateurs des clés faibles, que les escrocs seront en mesure de déchiffrer. Ce qui suppose toutefois qu'un navigateur vulnérable se connecte à un serveur selon un principe de chiffrement (*cipher*) laissant à désirer. Un grand nombre de navigateurs et de programmes clients étaient concernés.[53]

LogJam est une attaque apparentée à FREAK visant les connexions sécurisées, où le chiffrement est volontairement défini à un niveau beaucoup trop bas. A cet effet, les nombres premiers de base utilisés pour l'échange de clés de *Diffie-Hellman* sont réduits au point qu'il devient possible de déchiffrer les communications.[54]

---

49 Voir liste de contrôle MELANI: Mesures de prévention pour les systèmes de gestion de contenu (CMS): https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-prevention-pour-les-systemes-de-gestion-de-contenu--c.html

50 Voir aussi chap. 2 du présent rapport semestriel.

51 http://contagiodump.blogspot.ch/2010/06/overview-of-exploit-packs-update.html (état: le 31 août 2015).

52 http://malware.dontneedcoffee.com/ (état: le 31 août 2015).

53 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204 (état: le 31 août 2015).

54 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000 (état: le 31 août 2015).

5.5 Mesures de prévention

5.5.1 Nouvelle gestion des correctifs de Microsoft

Alors que pour les systèmes d'exploitation des téléphones mobiles on songe actuellement à l'introduction d'une gestion régulière des correctifs, Microsoft veut abandonner son traditionnel *Patchday* (jour de mise à disposition des correctifs) pour les utilisateurs de Windows 10 afin d'introduire des mises à jour continues. Un *Patchday* répondait aux pressions des administrateurs des grandes entreprises, qui tenaient à pouvoir dûment planifier et tester les mises à jour afin d'éviter que leurs systèmes vitaux ne cessent brusquement de fonctionner après l'installation d'une mise à jour.

Pour les entreprises, Microsoft entend régler ces problèmes par des anneaux de distribution portant le nom de « Windows Update for Business ». Tout réseau serait subdivisé en catégories pour la maintenance. En fonction de l'anneau, certains systèmes recevraient les mises à jour plus tôt que les autres. Une telle solution permet d'installer les mises à jour en fonction des risques. Les ordinateurs présentant un risque d'infection accru les recevraient en priorité. En outre, les administrateurs pourraient définir des fenêtres de maintenance, où l'installation des mises à jour serait autorisée ou non. Enfin, Microsoft veut s'en tenir dans un premier temps au *Patchday* pour certaines infrastructures d'importance critique pour une entreprise.[55]

5.6 Autres thèmes

5.6.1 Vols simples, mais lourds de conséquences

Dans la société occidentale, presque plus personne ne peut se passer d'un *smartphone*, pour écouter de la musique, lire ses courriels, gérer ses rendez-vous ou mesurer ses performances sportives. La quasi-totalité de nos données y sont archivées. Il est bien clair que le smartphone est devenu une cible intéressante pour les escrocs en tous genres. On pense sans doute d'abord, à propos des appareils électroniques, aux méthodes d'attaque électroniques, comme au vol de données par maliciel ou aux tentatives de chantage à l'aide de *ransomware*. Or en juin 2015, les médias allemands ont relayé des faits divers nous rappelant qu'il ne faut pas sous-estimer les méthodes de chantage traditionnelles. Les managers et les patrons sont toujours plus souvent victimes en Allemagne de vols de smartphones et d'ordinateurs, à des fins de chantage. Les baisses de prix et les mesures de sécurité accrues rendent en soi le vol d'un smartphone toujours moins attrayant. Mais si un appareil renferme des données très précieuses pour une personne donnée, ou alors pour son employeur ou sa clientèle, il redevient financièrement attrayant de le subtiliser.

Un vol médiatisé a été commis aux dépens de Dieter Kempf, personnalité en vue du monde informatique. Le président du fournisseur de solutions Datev et président de l'association faîtière allemande BITKOM se rendait au 14e congrès allemand sur la sécurité de l'information, où il devait animer une table ronde sur la communication mobile sans risque. Or quand Kempf a voulu descendre du train, trois inconnus se sont approchés de lui et lui ont subtilisé son ordinateur portable et un Blackberry. Ce mode opératoire recoupe les témoignages d'autres victimes: les pickpockets agissent en petits groupes, généralement aux heures de pointe, dans les trains ou les gares et s'en prennent aux voyageurs d'affaires.

[55] http://blogs.windows.com/windowsexperience/2015/05/04/announcing-windows-update-for-business/ (état: le 31 août 2015).

Il ne s'agit pas ici de cybercriminels cherchant à mettre la main sur des données, mais de simples voleurs à la tire, qui ont compris que ce modèle d'affaires peut rapporter gros. Il ne faut toutefois pas s'attendre à une multiplication des cas, sachant que les voleurs doivent opérer au niveau local et qu'ils courent de sérieux risques en contactant leur victime. Mais cet incident rappelle que les données confidentielles et appareils TIC courent de nombreux dangers.

Les mesures suivantes aident à prévenir cette forme de chantage:

- Veiller à ce que les mesures de sécurité soient correctement activées sur son smartphone (par ex. saisie du PIN et verrouillage automatique de l'écran).
- Ne pas enregistrer d'informations commerciales confidentielles sur un appareil privé.
- Ne jamais laisser sans surveillance un appareil contenant des données confidentielles.
- Effectuez des sauvegardes régulières de vos données (Backup / Cloud-Sync), afin de ne pas perdre toutes vos données en même temps que votre appareil.
- Dispositif antivol (P.ex.. „find my iPhone")
- Assurance antivol pour appareils et données

6 Tendances et perspectives

6.1 Quand les données circulent à l'étranger

Le précédent rapport semestriel avait déjà signalé le problème de la collecte de données personnelles et de leur exploitation subséquente.[56] Or bien souvent, seuls les abus potentiels dus aux entreprises ou aux particuliers sont dénoncés dans ce contexte. Rien n'est dit des démarches possibles pour les particuliers, quand des services étatiques ou des autorités de surveillance commettent des fautes, comme dans le cas décrit ci-après. Les victimes auraient pourtant besoin de conseils concrets pour faire rectifier les informations erronées, et surtout pour prévenir de tels incidents.

Des problèmes surgissent par exemple quand deux personnes qui portent le même nom et sont nées le même jour vivent en Suisse. Le risque de confusion leur vaut parfois des situations embarrassantes. Le Beobachter, magazine des consommateurs alémaniques, a consacré un article au sujet. On y voit que les problèmes peuvent être réglés dans chaque cas d'espèce, mais que la victime du malentendu doit systématiquement exiger les corrections utiles. Les personnes mentionnées dans l'article, Peter Moser d'Ipsach et Peter Moser de Winterthour, sont nées exactement le même jour, ce qui fait que l'AVS et d'autres entreprises ou autorités se trompent régulièrement sur elles.[57]

Un cas similaire a été signalé à MELANI au semestre sous revue. Il s'agissait d'un citoyen suisse ayant un double – personne ayant les mêmes nom et prénom, ainsi que le même jour de naissance. L'informateur de MELANI[58] s'en distinguait seulement par son second prénom. La série des confusions a commencé le jour où il a reçu une inscription au casier

---

56 MELANI, rapport semestriel 2014/2, chap. 5.1: https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2014-2.html (état: le 31 août 2015).

57 http://www.beobachter.ch/justiz-behoerde/buerger-verwaltung/artikel/verwechslung_der-doppelte-moser/ (état: le 31 août 2015).

58 Nom connu de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information.

judiciaire qui s'adressait en fait à son double. Il est désagréable de devoir contester une ordonnance pénale qui ne nous concerne pas. D'autres malentendus ont suivi avec les caisses-maladie, les autorités fiscales et les administrations communales, à l'occasion d'un déménagement. Même le service de médiation (ombudsman) à qui le problème avait été signalé a répondu par erreur au double. Chaque fois qu'une entreprise ou une autorité s'étaient trompées, le fardeau de la preuve a été à la charge de la victime. Dans d'autres cas, l'informateur est intervenu fructueusement auprès des services compétents pour éviter des confusions, qui auraient abouti à des interdictions d'entrée dans certains pays ainsi qu'à l'attribution des mauvaises données biométriques au bureau des passeports. Là encore, le système aurait commis des erreurs si la victime innocente n'avait rien fait.

De l'avis de la personne lésée, le vrai problème tient à ce que les incidents évoqués plus haut sont tous dus à la même confusion d'identité. Or il faut à chaque fois s'adresser au service compétent, au niveau de la branche ou des offices, etc. D'où un énorme effort dont la victime est rarement récompensée, alors qu'elle n'a rien à se reprocher. Il faut combattre un à un tous les symptômes. Faute d'un guichet central qui corrigerait à l'origine et pour toutes les institutions l'identification fautive, et qui veillerait à la coordination avec les intéressés. Et comme les fausses informations se propagent rapidement, l'actualisation des systèmes ne se fait pas automatiquement une fois la correction apportée à la source, et donc de nouvelles démarches de la victime s'imposent.

A l'approche des accords sur l'échange automatique de renseignements (EAR), les problèmes liés à la confusion d'identité risquent de prendre rapidement une ampleur internationale, ce qui compliquerait encore la rectification des erreurs sur la personne. D'où l'importance, lors de l'élaboration de nouveaux accords ou lois, de ne pas seulement chercher à éviter les abus du système par des individus, mais de veiller encore à l'assurance-qualité du système. En outre, il faudrait s'assurer que les erreurs puissent être aisément corrigées.

6.2 Un problème de vie ou de mort – l'informatique dans le secteur de la santé

Les pompes à perfusion sont d'une grande utilité pratique dans les traitements au quotidien. En fonction du tableau clinique, elles fournissent automatiquement le dosage correct du médicament. L'idée qu'un tiers puisse contrôler le débit d'une perfusion intraveineuse n'a donc rien de rassurant.

Dans le dernier rapport semestriel, nous avions évoqué la problématique de l'Internet des objets (*Internet of Things, IoT)*, soit le branchement au réseau d'un nombre croissant d'appareils. Même le domaine médical n'échappe pas à cette tendance, qui comporte pourtant de graves risques. Le chercheur sur la sécurité Billy Rios a ainsi découvert des failles de sécurité dans les pompes à perfusion de la marque Hospira.[59] A son premier essai, il n'a réussi qu'à manipuler les limites auxquelles le personnel soignant reçoit un message d'alerte. Il est toutefois parvenu plus tard à modifier à distance les doses à administrer. Ce chercheur a prévenu au début de juin 2015 le fabricant et l'agence américaine compétente, la FDA (Food and Drug Administration). A fin juillet seulement, la FDA publiait un avertissement officiel.[60] Elle a donc eu en théorie suffisamment de temps pour vérifier

[59] http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/ (état: le 31 août 2015)

[60] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm (état: le 31 août 2015)

concrètement les résultats des recherches et pour tester la faille. Sa mise en garde révèle un autre problème: la FDA recommande certes de séparer du réseau les pompes à perfusion, mais rappelle en même temps la nécessité d'actualiser manuellement les banques de données des doses. D'où de nouvelles sources d'erreurs. Dans de nombreuses branches, on a tôt fait de s'habituer aux avantages pratiques des fonctionnalités informatisées. Il faut par conséquent se concentrer sur la sécurité, lors des travaux d'automatisation, et définir des solutions de repli en cas de problème.

Avec la tendance à l'IoT, toujours plus de composants et de processus sont automatisés et reliés entre eux. Tout en faisant bénéficier les utilisateurs de nouvelles possibilités ou d'optimisations, ces applications confrontent aussi leurs responsables à de nouveaux problèmes. Comme le montre au chap. 5.3.2 l'exemple du Boeing Dreamliner, on a plutôt tendance à chercher une solution de contournement qui fonctionne plutôt que de modifier la configuration autorisée par des correctifs ciblés, ce qui nécessiterait de re-certifier les systèmes.

Les utilisateurs ne sont pas seuls à être confrontés à de nouveaux problèmes, les régulateurs des branches concernées doivent toujours plus se plonger dans les questions informatiques. Dans le cas des dispositifs médicaux, la directive 93/42/CEE traite de leur autorisation dans l'Union européenne et en Suisse aussi. Or sur 65 pages l'informatique en l'occurrence le terme logiciel, n'apparaît qu'à un seul endroit: «Pour les dispositifs qui incorpore (sic) des logiciels ou qui sont eux-mêmes des logiciels médicaux, le logiciel doit être validé sur la base de l'état de l'art, en tenant compte des principes du cycle de développement ainsi que de gestion des risques, de validation et de vérification.»

L'état de l'art est défini ici dans la norme EN62304, norme exhaustive d'un point de vue méthodologique de 2006 sur le cycle de vie des logiciels des dispositifs médicaux. En cas de défaillance, le problème ne provient souvent pas seulement du produit en question, mais d'une mauvaise configuration des réseaux environnants.

Les assureurs s'intéressent d'ores et déjà de près aux nouveaux risques. Car les dangers récents correspondent naturellement à de nouveaux modèles d'affaires potentiels. Quiconque ne maîtrise pas lui-même les risques des réseaux intelligents pourra au moins se protéger de cette manière des préjudices financiers à craindre.

7 Politique, recherche et politiques publiques

7.1 Interventions parlementaires

Objet	N°	Titre	Déposé par	Date de dépôt	Conseil	Dépt	Etat des délibérations et lien
Ip	15.3656	La télémaintenance des systèmes informatiques représente un danger pour la centrale nucléaire de Mühleberg. Surveillance de l'IFSN remise en cause	Martina Munz	18.06.2015	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20153656
Po	15.3359	Pour une armée innovante	Fathi Derder	20.03.2015	CN	DDPS	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153359
Po	15.3769	Rapport sur le service public. Limiter l'offre de la SSR sur Internet à une audiothèque et à une vidéothèque	Marco Romano	19.06.2015	CN	DETEC	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153769
Ip	15.3723	Protéger la jeunesse dans le domaine des médias. Suivre les recommandations des experts	Barbara Schmid-Federer	19.06.2015	CN	DFI	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153723
Ip	15.3661	Violation de la concession SSR. Mettre un terme à la diffusion de séries illégales sur Internet	Gregor A. Rutz	18.06.2015	CN	DETEC	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153661
Ip	15.3657	Droit à l'oubli pour les internautes	Martina Munz	18.06.2015	CN	DFJP	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153657
Po	15.3618	Rapport sur le mandat de service public de la SSR. Effectuer une analyse selon le principe de subsidiarité	Christian Wasserfallen	18.06.2015	CN	DETEC	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153618
Ip	15.3615	Service public dans le secteur des médias	Edith Graf-Litscher	18.06.2015	CN	DETEC	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153615
Po	15.3407	Protéger les droits de la personnalité	Yvonne Feri	05.05.2015	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20153407
Mo	15.3358	Accélérer un programme d'investissement dans la société numérique	Fathi Derder	20.03.2015	CN	DEFR	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153358
Ip	15.3352	Impôts. Que paient les grandes sociétés Internet en Suisse?	Margret Kiener Nellen	20.03.2015	CN	DFF	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153352
Po	15.3307	Rapport sur la société Internet en Suisse à l'horizon 2030	Edith Graf-Litscher	20.03.2015	CN	DEFR	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153307
Ip	15.3291	Exportations de technologies de surveillance et d'interception. Et les droits de l'homme?	Pierre-Alain Fridez	19.03.2015	CN	DEFR	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153291
Qst.	15.1027	Quelles actions préventives le Conseil	Christian	20.03.2015	CE	DFJP	http://www.parlament.ch/f/suche/pages/geschaefte.a

		fédéral entend-il mener pour éviter l'implantation d'extrémismes violents en Suisse?	van Singer				spx?gesch_id=20151027
Po	15.3759	Projet de réseau de données sécurisé et autres projets informatiques pour la protection de la population. Etat, perspectives et ressources requises	Ida Glanzmann-Hunkeler	19.06.2015	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20153759
Ip	15.3692	Informatique au sein de l'administration fédérale. Un puits sans fond?	Sylvia Flückiger-Bäni	18.06.2015	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20153692
Ip	15.3137	Externalisation du traitement de données fiscales	Philipp Hadorn	16.03.2015	CN	DFF	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153137
Ip	15.3448	Quels soutiens à l'introduction des véhicules autonomes?	Fathi Derder	06.05.2015	CN	DETEC	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153448
Ip	15.3375	Subtilisation de codes SIM par la NASA et le GCHQ auprès de la société Gemalto	Luc Recordon	20.03.2015	CE	DETEC	http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20153375

7.2 Autres thèmes

7.2.1 Big Data: programme national de recherche

Le Conseil fédéral a lancé à la fin juin 2015 un nouveau programme national de recherche (PNR) intitulé *Big Data*. Doté d'un budget de 25 millions de francs, il prévoit de créer les bases d'une utilisation efficace et adéquate des mégadonnées dans tous les aspects de la société. La durée des travaux a été fixée à cinq ans. Les projets escomptés livreront les bases scientifiques nécessaires à des solutions informatiques novatrices (analyse des données, algorithmes, cryptologie, services de gestion des données, sécurité et contrôles des accès), permettant une utilisation efficace et sûre de grands volumes de données. A partir de là, il s'agira de soumettre à un examen critique les domaines de la société (santé, infrastructures publiques) et les secteurs économiques déjà confrontés à de grandes quantités de données et où cette tendance se renforcera encore. Les examens porteront notamment sur la sécurité des données et des systèmes, ainsi que sur les aspects réglementaires (protection des données, protection de la sphère privée).

Le comité de direction du projet Big Data du PNR a été constitué en été 2015. Les appels d'offres pour les projets individuels devraient paraître durant l'automne 2015. Les esquisses de projets devront ensuite être remises dans un délai de trois mois, et le choix définitif des projets de recherche interviendra au cours de l'année prochaine.

7.2.2 Réorganisation de l'attribution des noms de domaine

L'ordonnance sur les domaines Internet (ODI), entrée en vigueur le 1er janvier 2015, a complètement redéfini l'attribution des noms de domaine en Suisse. Jusque-là, SWITCH cumulait les fonctions de registre (gestion de la banque de données des noms de domaine, en anglais *registry*) ainsi que de registraire (commercialisation des noms de domaine, en anglais *registrar*). La nouvelle ODI bannit ce double rôle. A son art. 8, elle confie à l'OFCOM le rôle de Centre d'information du réseau (*Network Information Center*, NIC). Il devient ainsi

l'organisation gérant de manière centralisée les ressources nécessaires à l'exploitation du système de noms de domaine (DNS) de la Suisse, avec possibilité de déléguer ce rôle à un tiers. Nul ne peut proposer sur le marché helvétique des domaines de premier niveau (*Top Level Domain,* ccTLD ou gTLD) sans avoir conclu un contrat de registraire avec l'*ICANN* et le registre. Entre-temps, 79 registraires du monde entier, dont 46 entreprises suisses, ont été admis comme interface pour le domaine de premier niveau «.ch». Le transfert des noms de domaine .ch de SWITCH aux registraires a commencé il y a un certain temps. L'ODI précise toutefois que le domaine générique de premier niveau «.swiss» relève de la compétence exclusive de la Confédération (OFCOM), afin que la Suisse continue d'en profiter pour des besoins spécifiques à long terme.

L'OFCOM a prolongé le contrat de délégation conclu avec SWITCH jusqu'au 30 juin 2017, dans le cadre d'une disposition transitoire fondée sur l'art. 62 ODI, pour garantir un processus de migration ordonné et transparent, ainsi que pour dûment préparer l'attribution de la fonction de registraire. Dès lors, la fonction de registre sera remise au concours.

8 Produits publiés par MELANI

Outre ses rapports semestriels, MELANI met à disposition du grand public des produits aussi nombreux que variés. Les sous-chapitres suivants passent en revue les Blogs, lettres d'informations, listes de contrôle, instructions et fiches d'information parus durant la période sous revue.

8.1 GovCERT.ch Blog

8.1.1 Joining the DNSSEC Day in Germany (en anglais)

30.06.2015 - DNSSEC stands for Domain Name System Security Extensions and has been introduced in 1999. The goal of DNSSEC is to implement authenticity and integrity in the DNS by taking advantage of digitally signing DNS records using public-key cryptography. DNSSEC helps you to prevent man-in-the-middle attacks on the DNS layer and DNS cache poisoning. Besides that, DNSSEC also provides a secure ground that allows you making usage of further security mechanisms that rely on DNSSEC, such as DNS-based Authentication of Named Entities (DANE).

➔ http://www.govcert.admin.ch/blog/9/joining-the-dnssec-day-in-germany

8.1.2 Outdate WordPress: Thousands of websites in Switzerland are vulnerable (en anglais)

08.06.2015 - The internet has grown very fast in the past 15 years. Thousands of new websites are going online every day. According to Netcraft, there are currently more than 850'000'000 active websites in the internet (May 2015). One of the reasons why the number of websites has grown that much is the use of content management systems (CMS), for example WordPress, Typo3, Joomla and Durpal. By using a CMS, you can easily publish content in the internet without needing IT knowledge. While CMS are something great, they are also a valuable target for hackers.

➔ http://www.govcert.admin.ch/blog/8/outdate-wordpress-thousands-of-websites-in-switzerland-are-vulnerable

8.1.3 Increase in DDoS extortion (DD4BC) (en anglais)

08.05.2015 - In the past days MELANI / GovCERT.ch has received several requests regarding a Distributed Denial of Service (DDoS) extortion campaign related to 'DD4BC'. The DD4BC Team (that is how the attackers call themselves) started its DDoS extortion campaigns in 2014. Since earlier this week, the DD4BC Team expanded their operation to Switzerland. MELANI / GovCERT.ch is aware of several high profile targets in Switzerland that have recently received a blackmail from DD4BC and have consequently suffered from DDoS attacks, obviously conducted by DD4BC.

➔ http://www.govcert.admin.ch/blog/6/increase-in-ddos-extortion-dd4bc

8.1.4 e-Banking Trojan Retefe still spreading in Switzerland (en anglais)

01.05.2015 - In July 2014, Trend Micro published a report about a threat called Retefe, an ebanking Trojan that is targeting financial institutions in Switzerland, Austria, Sweden and Japan. In fact, Retefe is already around since November 2013. Back then, MELANI already took appropriate action together with the affected financial institutions and ISPs in Switzerland to mitigate the threat. However, Retefe is still being distributed in recent spam campaigns, targeting Swiss Internet users.

➔ http://www.govcert.admin.ch/blog/5/e-banking-trojan-retefe-still-spreading-in-switzerland

8.1.5 Critical vulnerability in Magento: Many Swiss websites are still vulnerable (en anglais)

30.04.2015 - In February 2015, Magento (a popular eCommerce software for webshops) released a security patch addressing a critical vulnerability in its product. The vulnerability allows an attacker to send a special prepared HTTP request to any website running a vulnerable version of Magento in order to execute malicious code on the remote webserver (a so called Remote Code Execution RCE vulnerability). More than two months later, MELANI / GovCERT.ch still sees a fairly big amount of websites in Switzerland running an old, vulnerable version of Magento, exposing themselves and its visitors to cyber-attacks from the internet. Hackers can (ab)use the vulnerability to e.g. place malicious code on the victims website to infect its visitors with malware (Drive-By exploits).

➔ http://www.govcert.admin.ch/blog/4/critical-vulnerability-in-magento-many-swiss-websites-are-still-vulnerable

8.2 Lettres d'information de MELANI

MELANI a publié au premier semestre 2015 les lettres d'information suivantes:

8.2.1 Formulaire d'annonce des cas d'hameçonnage

29.07.2015 - Au cours de ces dernières années, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a traité un nombre croissant de demandes concernant des affaires d'hameçonnage (phishing). Les tentatives d'hameçonnage au moyen de courriers électroniques ou de sites Internet qui ont été signalées visaient la plupart du temps des clients d'établissements financiers suisses ainsi que des utilisateurs de plateformes en ligne de renommée mondiale (telles que des réseaux sociaux, des services de messagerie électronique ou des fournisseurs de services de paiement en ligne). Afin

d'assurer un traitement plus efficace des annonces de phishing, MELANI a lancé un site Internet sur lequel les cas présumés d'hameçonnage peuvent être signalés.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/meldeportal_gegen_phishing.html

8.2.2 Attaques DDoS et extorsion : une combinaison très actuelle

20.05.2015 - Différents cas portés à l'attention de MELANI ces dernières semaines témoignent d'une recrudescence d'attaques DDoS couplées à des tentatives d'extorquer de l'argent à la cible. MELANI conseille de ne pas céder au chantage et publie un document contenant différentes mesures de protection face aux attaques DDoS.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/ddos_angriffe_und_erpressung.html

8.2.3 Cheval de Troie bancaire «Dyre»: propagation massive

07.05.2015 - La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a déjà publié une alerte concernant le cheval de Troie bancaire Dyre en février 2015. Au cours des dernières semaines, ce sont quotidiennement des centaines de nouvelles infections qui sont constatées. Ce ne sont désormais plus uniquement les PME qui sont ciblées, mais de plus en plus également aussi les utilisateurs individuels.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/information_dyre_2.html

8.2.4 Dans son 20e rapport semestriel, MELANI passe en revue ses dix premières années et les menaces actuelles du cyberespace

30.04.15 - La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) fête son dixième anniversaire. A cette occasion, le 20e rapport semestriel ne se concentre pas uniquement sur les principaux événements du deuxième semestre 2014, qui a été marqué en particulier par des chantages et des attaques contre des systèmes mal protégés. Paru aujourd'hui, le rapport examine également l'évolution de la cybercriminalité ces dix dernières années.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/20_melani_halbjahresbericht.html

8.2.5 Clients de PME suisses visés par des attaques de phishing sur mesure

31.03.2015 - Les attaques de phishing, par lesquelles des escrocs cherchent à accéder à des données sensibles (mots de passe, données de cartes de crédit, etc.) sont toujours actuelles. La plupart du temps, des sites web imitant ceux d'entreprises connues (par exemple une banque ou un émetteur de cartes de crédit) sont créés à cet effet. MELANI intervient au quotidien pour retirer ce type de contenus frauduleux du web et protéger les utilisateurs. Depuis quelques temps déjà, les escrocs ne s'attaquent plus uniquement à des grandes marques connues, mais mettent sur pied des attaques de phishing imitant les sites de plus petites entreprises. Cette tendance semble s'accentuer et différents cas portés à l'attention de MELANI récemment témoignent même d'une sophistication accrue des attaques. Ils concernent différents types de PME ayant un site web et qui enregistrent des adresses E-mail de clients, par exemple pour l'envoi d'une Newsletter.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/clients-de-pme-suisses-vises-par-des-attaques-de-phishing-sur-me.html

8.2.6 PME visées par un cheval de Troie bancaire

02.02.2015 - Ces derniers jours, toujours plus de PME suisses ont prévenu la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI qu'elles avaient reçu des pourriels suspects. Ces messages, manifestement expédiés au nom de partenaires commerciaux, cherchent à infecter leur destinataire avec un cheval de Troie spécialisé dans l'e-banking. Dans un cas récemment signalé, la fraude a permis de dérober plus d'un million de francs à une entreprise fribourgeoise.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/pme-visees-par-un-cheval-de-troie-bancaire.html

8.3 Listes de contrôle et instructions

Au premier semestre 2015, MELANI a publié les listes de contrôle et instructions suivantes:

8.3.1 Mesures à prendre contre les attaques DDoS

25.06.2015 - Le terme DDoS (Distributed Denial of Service = déni de service distribué) désigne une attaque destinée à rendre inaccessibles des systèmes informatiques. Les dommages économiques peuvent être graves pour la victime.

En règle générale, les attaques DDoS relèvent de l'activisme politique, constituent une arme de chantage ou visent à nuire à un concurrent. MELANI observe à l'heure actuelle une recrudescence d'attaques DDoS avec demande de rançon en crypto-monnaies, telles que Bitcoin ou Litecoin.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/massnahmen-gegen-ddos-attacken.html

8.3.2 Sécurité informatique: aide-mémoire pour les PME

30.01.2015 - Le présent aide-mémoire a été conçu pour les PME suisses, afin de les aider à accroître la sécurité informatique de leurs réseaux d'entreprise.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

9 Glossaire

Terme	Définition
0-day Exploit	Faille de sécurité pour laquelle il n'existe pas encore de correctif.
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Adware	Les «adware», terme issu de la contraction des mots anglais «advertising» (publicité) et «software», s'utilisent fréquemment à des fins publicitaires. Ils enregistrent les habitudes de surf de l'utilisateur pour lui offrir ensuite les produits correspondants (p. ex. via des liens).
Big Data	Ensembles de données tellement volumineux qu'ils en deviennent difficiles à traiter avec des outils classiques de gestion de l'information.
Bitcoin	«Bitcoin» désigne à la fois un système de paiement à travers le réseau Internet et l'unité de compte utilisée par ce système de paiement.
Bluetooth	Technologie permettant d'établir une communication sans fil entre deux équipements terminaux, mise en œuvre surtout dans les téléphones mobiles, les ordinateurs portables, les PDA (assistants numériques personnels) et les périphériques d'entrée (p.ex. la souris).
Certificat	Un certificat numérique est l'équivalent, dans le cyberespace, d'une pièce d'identité et sert à attribuer une clé publique spécifique à une personne ou organisation. Il porte la signature numérique de l'autorité de certification.
Ciphers	Une procédure de chiffrement ou cryptage (cipher) permet de rendre la compréhension d'un texte impossible, et inversement de déchiffrer le message codé.
Command and Control Server	La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C).
Cross-Site-Scripting (XSS)	Le Cross-Site-Scripting (XSS) est une vulnérabilité parfois présente sur les applications web. Elle permet à un attaquant d'injecter du code sur un site web visité par un utilisateur.

Cryptage RSA	Du nom de ses inventeurs Rivest, Shamir et Adleman. Méthode de cryptage avec clé publique introduite en 1978. RSA est une procédure asymétrique.
Cryptographie	Discipline scientifique s'attachant à protéger les messages à l'aide du chiffrement.
Defacement	Défiguration de sites Web.
Distributed Denial of Service (DDoS)	Attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux systèmes et vise à rendre impossible l'accès à des ressources, ou du moins à le restreindre fortement aux utilisateurs.
Drive-by Infection	Infection par «drive-by download» Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site Web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
Echange de clés Diffie-Hellman	Procédé où deux correspondants conviennent d'une clé de chiffrement connue d'eux seuls.
Ethernet	Ethernet est un protocole de réseau local, où un câble diffuse les données à toutes les machines connectées.
Fallback function	Solution de repli, système secondaire relayant le système primaire en cas de dysfonctionnement, pour éviter une panne totale.
FTP	File Transfer Protocol (FTP) est un protocole de transfert de fichiers sur un réseau TCP/IP. Il s'utilise par exemple pour charger des pages Web sur un serveur Web.
Géolocalisation	Détermination de la position géographique.
Global Positioning System (GPS)	Global Positioning System (GPS), dont le nom officiel est NAVSTAR GPS, est un système mondial de navigation par satellite, permettant de déterminer à un moment précis une position géographique.
Hacktivisme	On entend par hacktivisme le piratage d'un système de communication avec des motivations politiques ou sociales.
Honeypot	Le terme honeypot (pot de miel) désigne, en jargon informatique, un programme ou un serveur simulant un ordinateur, un réseau complet ou le comportement d'utilisateurs fictifs. Les pots de miel servent à observer

	le comportement et à enregistrer les méthodes d'attaque des pirates.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN). L'ICANN est une organisation de droit privé à but non lucratif dont le siège est à Marina del Rey, petite ville côtière de Californie. Elle fixe les standards de base pour la gestion des domaines de premier niveau. Ainsi, l'ICANN coordonne les aspects techniques d'Internet, sans édicter de droit contraignant. Elle est soumise au Ministère américain du commerce (Department of Commerce) et dépend à ce titre du gouvernement américain.
Industrie 4.0	L'industrie 4.0 ou la quatrième révolution industrielle est un terme regroupant des tendances contemporaines dans l'automation, l'interconnexion intégrale et l'échange de données. L'industrie 4.0 intervient dans la mise en œuvre et la conceptualisation des "usines intelligentes" (smart factories).
Injection SQL	Une injection SQL exploite une lacune de sécurité liée aux banques de données SQL, dès lors que le concepteur du site Web néglige de contrôler les variables utilisées dans les requêtes SQL.
Internet of Things (IoT)	L'Internet des objets (Internet of Things, IoT) désigne la tendance des objets courants à être de plus en plus intelligents et mis en réseau.
Javascript	Langage de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les Javascripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
Kit d'exploits	Outil permettant de générer des scripts, programmes ou codes, visant à exploiter des failles de sécurité.
Malware	Maliciel. Le terme anglais "malware" est la contraction de "malicious" et de "software".
Mot de passe unique	Un mot de passe unique est un code d'authentification ou d'autorisation. Il n'est valable que pour l'opération définie et ne peut servir une seconde fois.

On board electronic	Electronique embarquée, systèmes conçus pour effectuer des tâches fonctionnelles précises à bord de moyens de transport.
Patch management	Gestion des correctifs, organisation adoptée pour la distribution des mises à jour logicielles.
Patchday	Jour où la société Microsoft publie les mises à jour de ses logiciels.
Phishing	Via l'hameçonnage, des pirates tentent d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir p. ex. d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (p. ex. eBay) ou des données d'accès pour le e-banking. Les pirates font appel à la bonne foi, à la crédulité ou à la serviabilité de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur et logos d'entreprise falsifiés.
Plug-In, Plugin	Plugiciel. Logiciel complémentaire qui étend les fonctions de base d'une application. Exemple : les plugiciels Acrobat pour navigateurs Internet permettent un affichage direct des fichiers PDF.
QR code	Le code QR (abréviation de Quick Response) est un type de code-barres bidimensionnel pouvant être lu et interprété rapidement par un smartphone notamment.
Radio Data System (RDS)	Service de transmission de données numériques en parallèle aux signaux audio de la radio.
Ransomware	Rançongiciel. Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate chiffre ou bloque la machine et demande de l'argent pour permettre de reaccéder aux données ou à la machine
SIM	La carte SIM (de l'anglais: subscriber identity module) est une petite carte à puce que l'on insère dans un appareil de téléphonie mobile et qui contient des données identifiant l'abonné.
Smartphone	Un smartphone est un téléphone mobile doté des fonctions d'un assistant numérique personnel (agenda, calendrier, navigation Web, consultation du courrier électronique, messagerie instantanée, GPS, etc.).
Social Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.

Spear Phishing	Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
SSL/TLS Tunnel	La tunnellisation (tunneling) est l'encapsulation de données d'un protocole réseau dans un autre afin qu'elles circulent sans être épiées ou bloquées. SSL et TLS permettant de communiquer en toute sécurité sur Internet.
Système de gestion du contenu (CMS, acronyme de content management system)	Un système de gestion du contenu (CMS, acronyme de content management system) est une solution flexible et dynamique permettant aux entreprises ou organisations de corriger et ajouter sur des sites Web des textes, des photos et des fonctions multimédias. Un auteur peut actualiser un tel système sans connaissances préalables en programmation ou en langage HTML. Les informations gérées dans ce contexte sont appelées contenu (content).
Systèmes de contrôle industriels (SCI)	Les systèmes de contrôle-commande sont formés d'un ou plusieurs appareils qui pilotent, règlent et/ou surveillent le fonctionnement d'autres appareils ou systèmes. Dans le domaine industriel, l'expression «systèmes de contrôle industriels» (Industrial Control Systems, ICS) est entrée dans le langage courant.
Systèmes SCADA	Supervisory Control And Data Acquisition Systèmes servant à la surveillance et à la gestion de processus techniques (p. ex. approvisionnement en énergie et en eau).
Top Level Domains	Tout nom de domaine dans Internet est formé d'une série de signes séparés par des points. Le domaine de premier niveau ou de tête (TLD) désigne le dernier élément de cette série et se situe au niveau hiérarchique le plus élevé du nom. Par exemple, si le nom de domaine d'un ordinateur ou d'un site est de.example.com, le TLD sera «com».
Traffic Distribution System (TDS)	Les systèmes de distribution du trafic redirigent les internautes appelant de la publicité en ligne vers des sites spécifiques. Les TDS sont souvent utilisés pour propager des infections.
Web Application Firewall (WAF)	Un pare-feu applicatif (WAF) analyse les connexions http pour éviter les abus.