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 2014/I (janvier – juin)

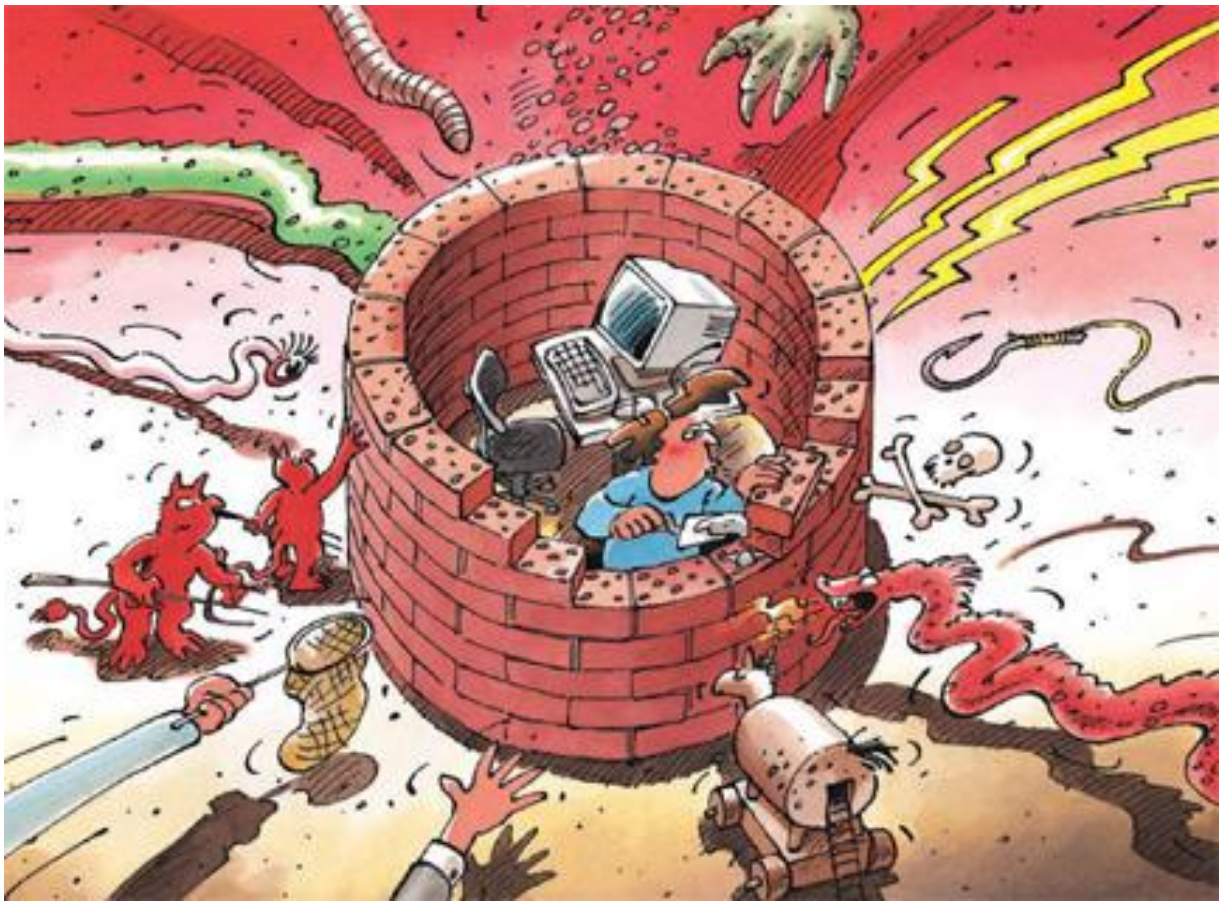

Table des matières

1 Temps forts de l'édition 2014/I

- **Faille de sécurité dans une des principales bibliothèques de chiffrement**
  Une faille d'OpenSSL – une des plus importantes bibliothèques de chiffrement – rendue publique le 7 avril 2014 concerne d'innombrables internautes. OpenSSL est installé par défaut sur de nombreux serveurs Web ou services Internet, afin de sécuriser la communication. Grâce à cette faille, un agresseur était en mesure de lire une partie de la mémoire d'un serveur, qui renferme pendant un bref laps de temps les données transmises par l'utilisateur.

  ► Situation sur le plan international: chapitre 4.1

- **Ingénierie sociale – une menace multiforme**
  Les attaques d'ingénierie sociale utilisent la serviabilité, la bonne foi ou l'incertitude des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques. Les exemples ne manquent pas et MELANI a souvent eu l'occasion d'évoquer ce thème dans ses précédents rapports semestriels. Au cours des six premiers mois de l'année 2014, MELANI a à nouveau reçu plusieurs annonces de sociétés suisses visées par des tentatives d'escroquerie utilisant des méthodes d'ingénierie sociale . Toute entreprise active en Suisse est désormais une cible potentielle pour ce type d'attaques, indépendamment de sa taille ou du secteur d'activité.

  ► Situation en Suisse: chapitre 3.1
  ► Situation sur le plan international: chapitre 4.6
  ► Tendances / Perspectives: chapitre 5.1

- **Tentatives de phishing adaptées à la Suisse**
  Les tentatives de phishing sont restées nombreuses au premier semestre 2014. Outre les envois passe-partout opérés au niveau international, plusieurs courriels de phishing conçus pour le marché suisse ont été repérés. Les escrocs visaient surtout à s'emparer des données de cartes de crédit de leurs victimes.

  ► Situation en Suisse: chapitre 3.2

- **Développements d'Internet après l'affaire Snowden**
  Les premières publications d'Edward Snowden ont mis à mal la sphère privée sur Internet. L'utilisateur se sent démuni et dépassé par la situation. Or qu'est-ce qui a changé dans l'évolution d'Internet, suite aux leçons tirées de l'affaire Snowden? Le présent rapport revient plus en détail, avec des exemples concrets à l'appui, sur cette question déjà abordée dans le précédent rapport semestriel.

  ► Situation sur le plan international: chapitre 4.5
  ► Tendances / Perspectives: chapitre 5.3

Attaque contre des installations industrielles occidentales
Une campagne d'espionnage et de sabotage (ou du moins d'actes préparatoires), visant des installations industrielles ou des fournisseurs d'énergie occidentaux, a été rendue publique fin juin 2014. Des indices montrent que le groupe de pirates, baptisé par les entreprises de sécurité «Dragonfly», «Energetic Bear» ou «Crouching Yeti», aurait été actif dès 2010. Les attaques révélées, réalisées en phases successives depuis le début de 2013, ont emprunté différents canaux.

► Situation sur le plan international: chapitre 4.3

2 Introduction

Le dix-neuvième rapport semestriel (janvier à juin 2014) de la Centrale d’enregistrement et d’analyse pour la sûreté de l’information (MELANI) commente les grandes tendances et les risques liés aux technologies de l’information et de la communication (TIC), livre un aperçu des événements survenus en Suisse et à l’étranger, signale divers thèmes de la prévention et résume les activités des acteurs étatiques ou privés. Les termes techniques ou spécialisés (écrits en italique) sont expliqués dans un glossaire (chapitre 6) à la fin du rapport. Quant aux jugements portés par MELANI, ils figurent à chaque fois dans des encadrés en couleur.

Le **chapitre 1** esquisse certains thèmes du présent rapport semestriel.

Les **chapitres 3 et 4** passent en revue les pannes et les incidents, les attaques, la criminalité et le terrorisme visant les infrastructures TIC. Des exemples choisis illustrent les principaux événements des six premiers mois de l’année 2014. La situation nationale est analysée au **chapitre 3** et la situation internationale au **chapitre 4**.

Le **chapitre 5** décrit les tendances et donne un aperçu des développements à prévoir.

Le **chapitre 5.5** passe en revue les principales interventions parlementaires se rapportant à la sûreté de l’information.

3 Situation en Suisse de l'infrastructure TIC

3.1 Tentatives d'escroquerie visant des entreprises suisses

MELANI a reçu au cours des six premiers mois de l'année 2014 plusieurs annonces de sociétés suisses visées par des tentatives d'escroquerie utilisant des méthodes d'ingénierie sociale (social engineering). Un travail d'information sur l'entreprise cible est mené en amont, ce qui permet aux escrocs de se faire une idée précise de l'environnement visé: secteur d'activité, postes clefs, modèles utilisés pour les adresses e-mails. Puis typiquement, un courriel semblant venir d'un cadre dirigeant, et imitant en réalité son e-mail, est envoyé à un employé du service de comptabilité. Le comptable y est informé d'une opération commerciale confidentielle en cours et mis en contact avec un «cabinet juridique», chargé de lui fournir les indications en vue du versement. Là encore, les escrocs se font passer pour un cabinet existant. Les auteurs insistent notamment sur le caractère exceptionnel de la demande, la nécessité de discrétion, mais également sur l'urgence de la situation. Des appels téléphoniques sont parfois effectués en parallèle ou préalablement à l'attaque, pour appuyer le scénario mis en place et inciter la cible à effectuer un versement vers un compte contrôlé par les escrocs.

Par ailleurs, un type d'escroquerie spécifique utilisant également des méthodes d'ingénierie sociale a touché en 2014 des établissements bancaires helvétiques. Il s'agit là d'une des manières possibles de valoriser des comptes e-mails piratés, par ex. grâce à une méthode de phishing. Dans ce mode opératoire, les escrocs analysent les comptes auxquels ils ont accédé. Ils y recherchent spécifiquement des communications que leur propriétaire aurait pu avoir avec sa banque. Par la suite, les escrocs écrivent aux employés de banque en question, en se faisant passer pour le client. Ils leur demandent d'effectuer un transfert d'argent vers un compte qu'ils contrôlent à l'étranger.[1]

Face à ces phénomènes ciblant les entreprises, la règle de base consiste à ne fournir aucune information interne et à ne procéder à aucune action lors de prises de contacts semblant douteuses ou inhabituelles. Le cas échéant, il est fortement recommandé de vérifier par téléphone la légitimité d'une demande ou d'une prise de contact. Les processus, en particulier ceux concernant les transferts d'argent, devraient être clairement définis à l'intérieur de l'entreprise et dûment suivis en toute circonstance. MELANI recommande de mettre un accent particulier sur la prévention du personnel envers ces phénomènes, notamment aux postes clefs.

3.2 Phishing sur mesure en Suisse

Les tentatives de *phishing* sont restées nombreuses au premier semestre 2014. Outre les envois passe-partout opérés au niveau international, plusieurs courriels de phishing conçus pour le marché suisse ont été repérés. Les escrocs visaient surtout à s'emparer des données de cartes de crédit de leurs victimes.

[1] http://www.tio.ch/News/Ticino/803356/Pirata-informatico-preleva-un-milione-di-franchi-da-un-conto-luganese/ (état: le 1er septembre 2014).

Offre spéciale pour le chocolat

Une attaque spécifiquement destinée à des victimes suisses est survenue en février dernier. Un courriel expédié à grande échelle annonçait une promotion du chocolatier Läderach sur ses pralinés. Il était possible de payer commodément sur son site, par carte de crédit. Or un regard plus attentif révélait que l'adresse Web était incorrecte: au lieu de l**ae**derach.ch, le site avait été enregistré à l'adresse l**ea**derach.ch. En outre, il y manquait le cryptage d'usage sur les sites demandant au visiteur d'introduire les données de sa carte de crédit.

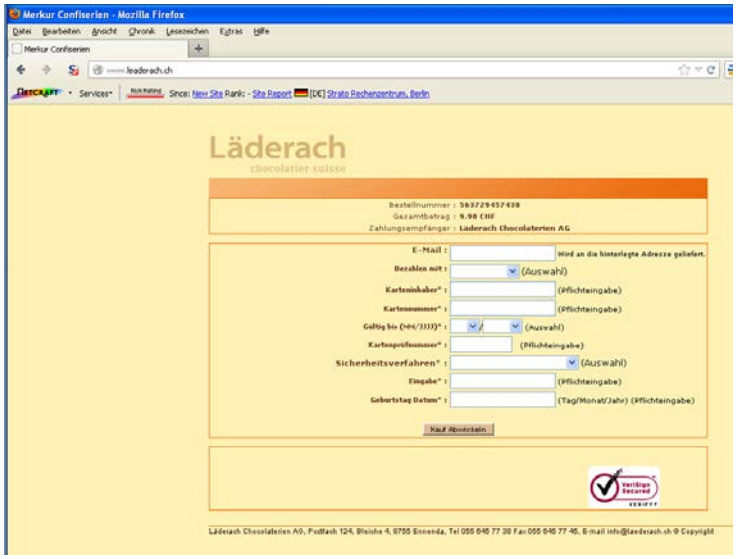

Fig. 1: La page de phishing se fait passer pour le site officiel du chocolatier Läderach.

La société Läderach a aussitôt publié une mise en garde sur son site Web. De son côté, MELANI a cherché à désactiver le site frauduleux. D'autres attaques du même type ont suivi, avant de cesser brusquement. Il est possible que peu de personnes s'étaient laissé piéger, et donc les escrocs ont renoncé à cette arnaque.

Usage du logo de l'administration fédérale pour du phishing

Une autre vague de phishing apparue pour la première fois en 2014 a été beaucoup plus tenace. Les escrocs ont cherché à maintes reprises, dans des courriels expédiés au nom de l'Office fédéral de l'énergie (OFEN) ou de Suisse Energie, à s'emparer de données de cartes de crédit. Les destinataires étaient appâtés par un prétendu remboursement de 165 francs auquel ils auraient eu droit. Pour obtenir ce versement, il fallait se rendre sur la page Internet indiquée. Or la page ressemblant à s'y méprendre au site d'origine exigeait non seulement le nom et l'adresse, mais aussi le numéro de carte de crédit, y c. la date d'expiration et le chiffre de contrôle.

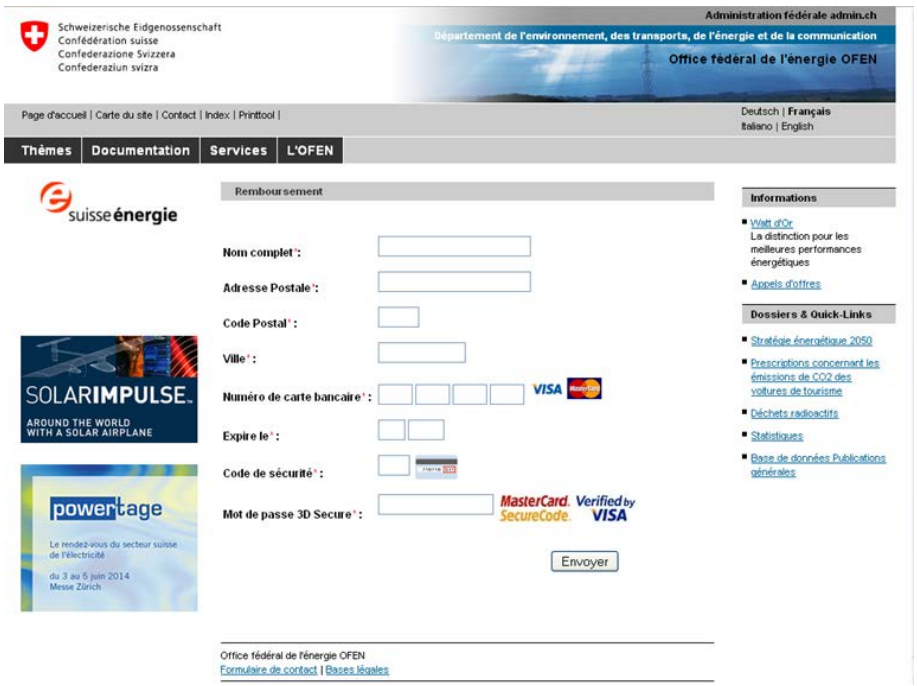

Fig. 2: Page de phishing prétendant émaner de l'Office fédéral de l'énergie.

Là encore l'OFEN, mais aussi le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) ainsi que MELANI ont publié une mise en garde. En outre, des efforts ont été entrepris pour désactiver rapidement les pages de phishing. Les résultats ont d'abord été mitigés, alors même que les pages Web étaient toujours hébergées sur le même serveur (tchèque). A peine une page était-elle désactivée que la suivante était publiée. Le processus a été optimisé par la suite, permettant de neutraliser le dispositif des escrocs en quelques minutes. De nouvelles vagues de phishing de ce type sont néanmoins régulièrement signalées.

Ces deux exemples montrent l'importance de réagir rapidement aux premiers essais d'une nouvelle variante de phishing. Car si l'on parvient à endiguer les premières vagues et à priver les pirates des résultats escomptés, les attaques cessent généralement très vite. Faute d'un tel succès, rien ne pourra arrêter les vagues successives d'une cyberattaque, même si l'on progresse dans la désactivation des sites Web et limite ainsi sérieusement le butin des escrocs.

Tentative de phishing déguisée en sondage

Un autre scénario a été utilisé lors d'une tentative de phishing pour laquelle le logo de Swisscom avait été usurpé. La victime était appâtée par un sondage. Tout d'abord, dix questions portaient sur les produits et la qualité des services de cette entreprise. A la fin du sondage, il fallait indiquer non seulement son nom et son adresse, mais aussi les données de sa carte de crédit. L'intention des escrocs était claire: leurs questions certes logiques n'étaient qu'une astuce pour dissiper la méfiance des victimes. A quoi bon sinon réaliser un questionnaire de satisfaction?

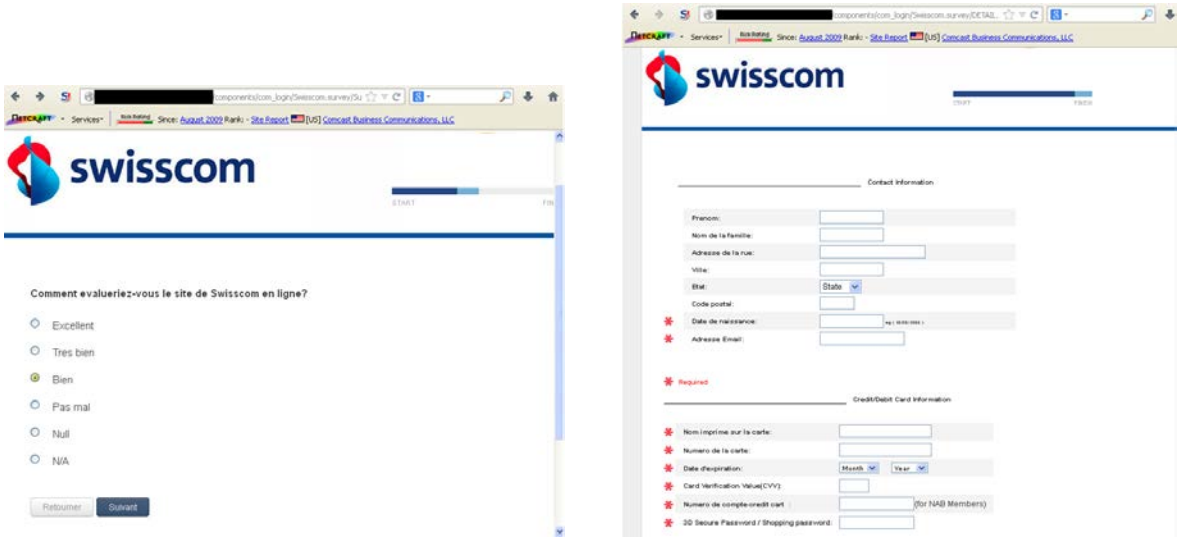

Fig. 3: Une des dix questions posées (à gauche); à la fin du questionnaire, un formulaire invite à indiquer les données de sa carte de crédit: «Ce champ est obligatoire» (à droite).

Les tentatives actuelles de phishing montrent qu'il est toujours plus difficile pour les destinataires de reconnaître le piège tendu. Une grande prudence s'impose avec les courriels invitant à fournir des données personnelles. Les courriels non sollicités demandant des mots de passe ou les données de carte de crédit ont toutes les chances d'être une tentative d'escroquerie. D'où les fréquentes mises en garde de MELANI: «aucune entreprise ne vous demandera jamais par courriel vos données d'ouverture de session, vos mots de passe et les données de vos cartes de crédit.»
Aussi élémentaire cette règle soit-elle à première vue, elle confronte les entreprises à divers défis, à l'âge de la communication électronique. Comment une entreprise doit-elle communiquer avec sa clientèle, pour qu'elle n'ait pas l'impression d'avoir affaire à un courriel frauduleux? Plus grave encore: une entreprise désinvolte dans sa communication risque d'influencer négativement l'attitude des clients face aux courriels frauduleux.

Cette problématique doit être prise au sérieux, comme le montrent les annonces par la population de messages pris pour du phishing alors qu'ils émanent d'entreprises respectables. L'exemple le plus frappant signalé à MELANI au premier semestre provient de PayPal. Le destinataire de l'envoi était prié d'actualiser les données de sa carte de crédit. Mais comme le lien vers le site était dissimulé derrière un bouton, il n'était pas possible de vérifier sans autre sous quel *URL* la page était enregistrée. En l'occurrence, le courriel provenait réellement de PayPal.

Fig. 4: Courriel pris par erreur pour une tentative de phishing. Il provenait bel et bien de Paypal.

En pareil cas, il est recommandé de NE PAS cliquer malgré tout sur l'*URL* figurant dans l'e-mail, mais d'inscrire l'URL de l'entreprise manuellement dans la *barre d'adresse* du navigateur, puis de naviguer sur le site en question. En cas de doute, il est indiqué de s'adresser directement à l'entreprise.

Les entreprises prêteront attention aux points suivants lors de l'envoi de lettres d'information:

- Recourir autant que possible au format texte dans les courriels.
- Veiller à la régularité des envois de Newsletters par e-mail.
- Limiter autant que possibles les liens, et ne se référer qu'à son propre domaine.
- Si possible, utiliser des liens vers des *sites sécurisés (https://...)* et l'indiquer au destinataire.
- Ne pas créer de renvoi à des sites Web qui demandent le nom d'utilisateur, le mot de passe ou d'autres données personnelles.
- Signaler la lettre d'information sur la page d'accueil du site Web.
- S'adresser aux clients par leurs prénom et nom, si ces informations sont disponibles.

3.3 Essor des serveurs C&C en Suisse – une tendance?

La plupart des ordinateurs infectés sont surveillés et gérés par un ou plusieurs serveurs de commande et de contrôle. Ces serveurs C&C (*botnet command & control server*) contrôlent les fonctions des maliciels mis en circulation. Les annonces concernant de tels serveurs localisés en Suisse ont explosé au semestre sous revue. De son côté également, MELANI en a identifié et neutralisé davantage. Le nombre de serveurs C&C signalés ou détectés en Suisse a ainsi largement doublé par rapport aux exercices 2012 et 2013.

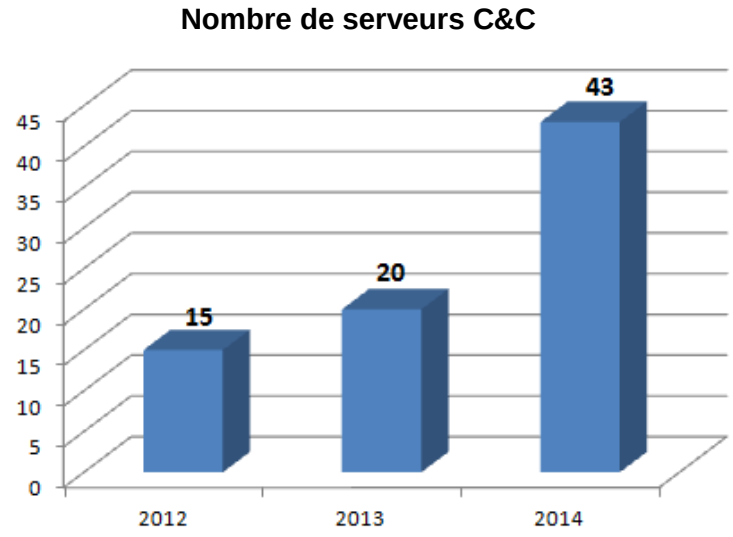

Fig. 5: Nombre de serveurs C&C commandant un réseau de zombies détectés en Suisse.

Une grande partie des infrastructures détectées consistent en des serveurs C&C utilisés pour piloter les ordinateurs préalablement infectés avec des chevaux de Troie spécialisés dans l'e-banking – comme p. ex. ZeuS, Citadel ou KINS. Outre de tels maliciels attaquant les internautes à grande échelle, MELANI a également repéré des infrastructures utilisées lors d'attaques ciblées visant des organisations gouvernementales. Dans le jargon professionnel,

on parle d'attaques de type APT (*advanced persistent threat*). Dans de nombreux cas, tout porte à croire que ces tentatives d'espionnage émanent d'acteurs étrangers.

Il s'agit donc de comprendre pourquoi des cybercriminels généralement basés à l'étranger et d'autres acteurs étrangers se servent du cyberespace suisse pour leurs activités illégales. Outre que la Suisse dispose d'excellentes infrastructures raccordées à Internet, un autre aspect entre certainement en ligne de compte, soit le fait que la protection des données y soit très développée. La police et les services de renseignement doivent respecter un cadre légal strict, lors de leurs investigations sur Internet. A la lumière de l'affaire Snowden, il s'agit d'un avantage concurrentiel qui séduit les entreprises ou les particuliers soucieux de la protection des données et de leur sphère privée. Ces facteurs rendent le cyberespace suisse attrayant pour les citoyens ou organisations étrangers souhaitant se soustraire aux cybercontrôles parfois sévères en vigueur dans leur pays. Les cybercriminels savent hélas aussi exploiter la situation à leur avantage.

Certains fournisseurs d'hébergement étrangers ont à leur tour découvert la situation attrayante de la Suisse, où ils ont récemment étendu leur offre, et cherchent à attirer des clients en vantant un service de qualité suisse en matière d'«offshore hosting». Or bien souvent, ils ne sont guère regardants sur les contenus ou infrastructures qu'ils hébergent ainsi en Suisse.

MELANI examine de près les annonces de citoyens ou de partenaires concernant de telles infrastructures criminelles et, le cas échéant, sollicite les services concernés au niveau fédéral ou cantonal.

3.4 Messagerie piratée – députée au Grand Conseil visée

L'envoi de courriels prétendant qu'une personne se trouve à l'étranger et qu'elle a perdu tout son argent est connu depuis plusieurs années déjà. Le vrai propriétaire du compte de messagerie s'est fait dérober ses données d'accès. L'escroc écrit à tous les contacts du carnet d'adresses, ou à ceux lui paraissant le plus prometteurs. Ces courriels consistent généralement en de faux appels à l'aide, dont l'expéditeur prétend être bloqué quelque part à l'étranger après s'être fait voler son téléphone mobile, tout son argent et son passeport. Le destinataire est instamment prié de verser de l'argent. De tels messages parviennent encore ponctuellement à MELANI. Les politiciens ne sont pas épargnés. Deux ans après le député au Grand Conseil thurgovien Josef Brägger[2], la députée PLR au Grand Conseil soleurois et présidente de la commune de Gänsbrunnen Rosmarie Heiniger[3] a subi pareille mésaventure. Les pirates ont écrit en son nom à tous ses contacts qu'elle était en difficulté en Afrique du Sud, où elle passait ses vacances, et qu'elle avait un urgent besoin d'aide financière. Le cas échéant, il peut être utile d'avertir tous les destinataires potentiels du courriel frauduleux se trouvant dans son carnet d'adresses. On procédera à partir d'une autre adresse électronique ou par téléphone/*SMS*. Car pour éviter une telle réaction qui compromettrait leurs chances de succès, les escrocs s'empressent généralement de supprimer le carnet d'adresses et d'effacer tous les courriels de la victime. Autrement dit, la perte de tous ses contacts et de sa correspondance électronique vient s'ajouter aux autres embarras et aux demandes d'informations des connaissances ayant reçu l'appel au secours.

---

2 http://www.tagblatt.ch/ostschweiz/thurgau/kantonthurgau/tz-tg/Kantonsrat-von-Unbekannten-gehackt;art123841,2977642 (état: le 1er septembre 2014).

3 http://www.oltnertagblatt.ch/solothurn/thal-gaeu-niederamt/kantonsraetin-rosmarie-heiniger-wird-opfer-eines-hacker-angriffs-127848961 (état: le 1er septembre 2014).

A l'heure actuelle, la plupart des courriels ne sont plus téléchargés et sauvegardés localement sur un ordinateur. Ils sont traités à l'aide d'un *Webmail*, et se trouvent dans le nuage (*cloud*). Les utilisateurs jugent donc souvent superflu d'effectuer une sauvegarde des données (*backup*). Inconsciemment, la plupart des utilisateurs ont délégué cette tâche à leur fournisseur de messagerie. Ils partent de l'idée qu'il se chargera des sauvegardes. Il est vrai que le fournisseur duplique les données pour faire face aux problèmes techniques (p. ex. panne de serveur). Mais si des personnes non autorisées accèdent à un compte et y effacent intentionnellement des données – selon la procédure habituelle dont tout utilisateur peut se servir –, les sauvegardes des fournisseurs n'auront généralement guère d'utilité. Il est par conséquent vivement recommandé de procéder régulièrement soi-même à la sauvegarde de ses contacts et de ses courriels.

Les escrocs accèdent d'ordinaire aux données par des méthodes de phishing. De nombreuses tentatives visent à s'emparer, directement ou indirectement, des données d'accès aux comptes de messagerie. Une variante de phishing connue depuis longtemps consiste à prétendre qu'un document confidentiel est sur le point d'être délivré. Pour l'obtenir, la personne doit cliquer sur le lien reçu. Elle sera ensuite priée de sélectionner son fournisseur de messagerie et d'indiquer son nom d'utilisateur et son mot de passe. Ces informations seront ensuite envoyées aux pirates.

Fig. 6: Site de phishing créé pour accéder aux données d'accès des comptes de messagerie.

3.5 Méthodes modernes d'alarme – chances et limites

Une fois par année, les sirènes sont soumises à des tests en Suisse, ce qui a été le cas le 5 février 2014. Le cas échéant, l'information est assurée par les autorités locales et les stations de radio nationales. C'est également à travers ses canaux que se déroulerait la communication de crise en cas de catastrophe réelle. Les stations de radio de la SRG/SSR sont spécialement bien protégées contre les pannes (voir MELANI, rapport semestriel 2010/2[4]). Toutefois, toujours plus de gens s'informent aujourd'hui aussi par Internet, p. ex. sur le site de l'Office fédéral de la protection de la population (OFPP). Ce dernier est toutefois resté brièvement injoignable lors du test du 5 février 2014, où les internautes recevaient le message d'erreur «service unavailable». Le site n'aurait pas résisté à l'afflux de demandes.

[4] MELANI, rapport semestriel 2010/2, chapitre 3.7: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=fr (état: le 1er septembre 2014).

Un tel incident amène à se demander à quelles conditions, à l'ère de la communication numérique, les technologies modernes peuvent servir à donner l'alarme. Divers essais sont réalisés dans ce sens. Ainsi, la résilience du site web de l'OFPP a été fortement améliorée suite au test de cette année. Par ailleurs, de nombreux projets sont consacrés à l'utilisation des nouveaux moyens de technologie dans ce domaine. Par exemple en cas de risque d'inondation, les habitants du quartier de la Matte à Berne sont d'ores et déjà prévenus additionnellement par *SMS* des pompiers de l'évolution de la situation Depuis 2012 à Bâle, un service d'abonnement par sms permet aux personnes malentendantes d'être informé lorsque les sirènes d'alarme sont déclenchées.[5] Un système de diffusion cellulaire («cell broadcast») est également à l'étude à l'OFPP. Tous les téléphones mobiles ayant activé ce service et se trouvant à l'intérieur de la même zone géographique recevraient les messages SMS diffusés. Ces divers projets ne visent toutefois pas à remplacer les alarmes existantes, mais à compléter les systèmes actuels. Ils permettent à la fois de tenir compte des nouveaux besoins de la population, et d'optimiser la portée des alarmes. En outre, l'OFPP songe à utiliser d'autres canaux de communication pour alerter et informer la population, à l'instar des systèmes d'information en place dans les transports publics ou des réseaux sociaux.

Les systèmes TIC modernes sont souvent favorisés, même dans les domaines où la sécurité est primordiale. L'usage du GPS dans la navigation aérienne en est un bon exemple[6]. Dans bien des cas, les partisans de tels systèmes cherchent à réduire leurs coûts d'exploitation. Or cette efficience ne doit en aucun cas porter préjudice à la sécurité. En revanche, les systèmes TIC peuvent compléter judicieusement les systèmes de sécurité plus anciens et plus stables, à l'instar des messages SMS désormais envoyés en cas de catastrophe.

3.6 Données sensibles en libre accès

Le 31 mars 2014, la NZZ a publié un rapport révélant qu'à l'Université de Bâle, des documents se rapportant aux procédures d'appel étaient enregistrés sans protection spéciale sur des serveurs reliés à Internet et accessibles à l'aide d'un moteur de recherche.[7]

N'importe qui avait ainsi accès à plus de 1500 documents, dont des lettres de postulation, des certificats de travail, des lettres de recommandation et des diplômes. Or les dossiers de postulation contiennent beaucoup d'informations qu'il est préférable de ne pas montrer au premier venu, a fortiori à son employeur actuel.

C'est une personne concernée qui a alerté l'Université de Bâle. La fuite a aussitôt été comblée et les intéressés prévenus. La panne provenait apparemment d'une erreur commise durant la migration des serveurs vers un logiciel plus récent. Les droits d'accès des dossiers n'avaient pas été repris correctement. Des documents figurant dans des dossiers protégés sont ainsi devenus accessibles à tout le monde. L'université estime que les données ont été accessibles du 27 février au 15 mars 2014.

L'accès aux dossiers concernés a été supprimé aussitôt l'erreur connue. En outre, une demande pour chaque document a été adressée à Google, afin que le *cache* de ce moteur de recherche soit vidé. Cette procédure de longue haleine est nécessaire, car il ne suffit pas d'effacer les documents du serveur. Les moteurs de recherche stockent temporairement dans des caches les documents publiés, afin de réduire le temps de réponse aux requêtes.

---

5 http://www.polizei.bs.ch/aktuell/gehoerlose-hoerbehinderte.html (état: le 1er septembre 2014).

6 MELANI, rapport semestriel 2011/1, chapitre 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=fr (état: le 1er septembre 2014).

7 http://www.nzz.ch/aktuell/startsesite/heikles-datenleck-an-der-universitaet-basel-1.18273869 (état: le 1er septembre 2014).

De telles publications surviennent accidentellement[8], et on ne peut jamais complètement les exclure. MELANI s'efforce toutefois depuis plusieurs années de mieux faire connaître certaines règles utiles pour prévenir ce genre de pannes. Lors de la sauvegarde des données, le gros des efforts porte sur les mesures techniques. Or ce n'est pas suffisant, et les mesures d'organisation jouent un rôle essentiel dans la sûreté de l'information. Chaque dossier doit ainsi être attribué à une classe d'importance. Le cas échéant, il ne sera pas enregistré et protégé de la même façon. D'où ici la question de savoir pourquoi les données avaient été enregistrées sur un serveur accessible par Internet. Un mauvais réglage des droits d'accès est susceptible d'entraîner de sérieux problèmes.

3.7 Curieuses fenêtres s'ouvrant lors de sessions d'e-banking

Plusieurs incidents rapportés à MELANI au semestre sous revue concernent des sessions d'e-banking, au cours desquelles une enquête s'affichait dans une fenêtre. Il fallait répondre à des questions simples, portant par ex. sur le sexe, l'âge et les préférences personnelles. L'enquête faisait ensuite croire à la victime qu'elle avait gagné un iPad ou un iPhone. Il suffisait de choisir d'un clic le cadeau souhaité. On aboutissait alors à un site appelé Bogabids, apparemment géré par Flamingo Intervest qui possède également la société Ziinga. Cette dernière avait déjà fait parler d'elle lors d'un cas similaire[9]. Il semble que ces offres ne sont qu'en apparence gratuites, puisqu'il faut d'abord souscrire à un abonnement onéreux. Il est en effet indiqué en petits caractères que seules ont droit au cadeau les personnes ayant payé pendant au moins un mois leur cotisation de membre. La taxe peut atteindre 100 dollars, selon le type d'abonnement choisi. Aucun cas n'a permis d'établir un lien avec l'e-banking. De même, ces pages n'ont jamais servi à répandre des maliciels.

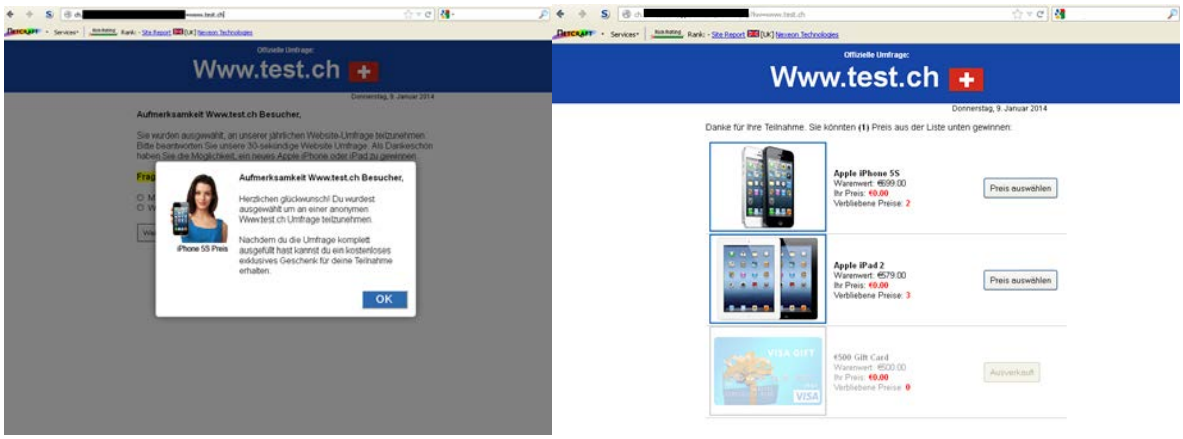

Fig. 7: Fenêtre contextuelle apparaissant pendant une session d'e-banking.

Le drapeau helvétique sur la page Web de la fig. 7 fait croire à un site d'origine suisse, pour inspirer confiance au destinataire. Or une analyse plus poussée révèle que les drapeaux de 19 pays figurent sur ce site et sont susceptibles de s'afficher – en fonction de la cible. La liste inclut l'Australie, la Belgique, le Brésil, les Etats-Unis et la Finlande. Autrement dit, l'opération n'est pas dirigée contre la Suisse, mais menée à grande échelle. La raison sociale ou l'adresse Web affichées à gauche du drapeau (www.test.ch) sont également

[8] MELANI, rapport semestriel 2008/1, chapitre 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=fr (état: le 1er septembre 2014).

[9] MELANI, rapport semestriel 2012/2, chapitre 3.7: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=fr (état: le 1er septembre 2014).

susceptibles de changer. Ce texte peut être généré à volonté, en introduisant une variable dans l'adresse Web. Les annonces sont lancées par les *adwares* figurant sur l'ordinateur. De tels programmes sont souvent fournis avec les programmes gratuits, les *pilotes gratuits* ou *codecs vidéo*, et manipulent l'ordinateur pour afficher de la publicité durant la navigation.

4 Situation internationale de l'infrastructure TIC

4.1 Faille Heartbleed d'OpenSSL

Une faille d'*OpenSSL* – une des plus importantes bibliothèques de chiffrement – rendue publique le 7 avril 2014 concerne d'innombrables internautes. OpenSSL est installé par défaut sur de nombreux serveurs Web ou services Internet, afin de sécuriser la communication. Selon une analyse réalisée par la société britannique Netcraft, 17,5% des sites SSL utilisant les certificats d'un organisme de certification (digne de confiance) comportaient cette fonction vulnérable.[10]

La raison était due à une faille de sécurité de la fonction «Heartbeat». Cette dernière veille à ce que la liaison sécurisée soit maintenue pendant un certain temps, évitant ainsi de devoir établir une nouvelle connexion. Grâce à cette vulnérabilité, un agresseur était en mesure de lire une partie, soit les derniers 64 *kilobytes* (kB), de la mémoire d'un serveur, qui renferme pendant un bref laps de temps les données transmises par l'utilisateur. D'où la possibilité de voir les mots de passe, les données des transactions, mais aussi des données se rapportant au serveur, comme p. ex. des *clés privées*.

Au-delà des fournisseurs de messagerie ou d'établissements financiers, cette faille de sécurité concerne plus généralement tous les portails Web proposant une connexion chiffrée et utilisant le logiciel vulnérable. D'autres services non basés sur le Web, comme les applications pour *smartphones*, les services de conversation instantanée (*chat*), ceux de stockage dans le nuage (*cloud*), de transmission en continu (*streaming*) ou de messagerie, ou encore les accès par *VPN* ont également été affectés.

Alors qu'il était compliqué d'intercepter un jeu complet de données, il se peut tout à fait que des clés de chiffrement et des données d'accès soient tombées entre les mains d'agresseurs, et qu'ils cherchent à utiliser plus tard ces informations. Les fournisseurs de service concernés ont donc dû non seulement combler la faille de sécurité, mais aussi remplacer les certificats.

MELANI a informé les opérateurs d'infrastructures d'information critiques ainsi que le public des mesures à prendre.[11] Globalement, on constate que les travaux se sont effectués rapidement et efficacement en Suisse. Des difficultés ont toutefois été constatées lors de la commande des certificats. Submergés par les demandes, les émetteurs ont eu besoin de plusieurs jours parfois pour délivrer un nouveau *certificat*.

[10] http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html (état: le 1er septembre 2014).

[11] http://www.melani.admin.ch/dienstleistungen/archiv/01564/index.html?lang=fr (état: le 1er septembre 2014).

Aspects techniques et enseignements tirés de l'incident

La faille de sécurité d'OpenSSL a conduit à reparler de la confidentialité de transmission parfaite (perfect forward secrecy, PFS). Concrètement, des pirates ayant intercepté un échange de données cryptées ne sont pas en mesure de le déchiffrer sur le moment. Or il est à craindre qu'ils n'y parviennent ultérieurement, si la clé nécessaire devait tomber entre leurs mains. Heartbleed est un exemple révélateur de la manière d'accéder plus tard à des clés ou certificats.

C'est précisément là qu'intervient le mode de cryptage PFS: normalement, les clés de chiffrement des sessions sont renégociées à de brefs intervalles. Autrement dit, un pirate ne peut pas décrypter toute la session, mais seulement une partie. Or sans PFS, ces clés temporaires sont générées par une unique clé de session de longue durée. Donc si cette dernière est dérobée, il devient possible d'obtenir toutes les clés de session et, du même coup, de décrypter les échanges complets. Grâce à PFS, la clé de longue durée ne permet toutefois pas a posteriori de découvrir les clés de courte durée. La clé de longue durée n'a ici qu'une fonction de signature des clés temporaires. Avec ces dernières, une clé de session est générée par un échange de clés de *Diffie-Hellman*. Donc si un serveur est compromis, l'escroc ne découvre que la clé de signature de longue durée et la dernière clé des sessions actives. Toutes les clés de session antérieures ont déjà été effacées et il n'est plus possible de les retrouver.[12]

Les mésaventures d'OpenSSL ont fait reparler de diverses variantes *SSL* qui cherchent à résoudre les problèmes de la bibliothèque OpenSSL (a évolué petit à petit, avec de nombreuses fonctions rarement utilisées). Le tableau ci-dessous passe brièvement en revue les bibliothèques SSL à code source ouvert:

Bibliothèque	Description	Remarques
OpenSSL	Reste la bibliothèque la plus souvent utilisée.	OpenSSL fait actuellement l'objet d'un examen systématique (*code review*). Il s'agit de détecter et de corriger d'autres erreurs encore.
LibreSSL	Développement d'OpenSSL visant à l'alléger des fonctions inutiles, tout en cherchant à rester aussi proche que possible d'OpenSSL et à faciliter les migrations.	Produit des développeurs d'OpenBSD, réputés pour leurs logiciels sûrs.
PolarSSL	La bibliothèque PolarSSL a été développée parce qu'OpenSSL était devenu trop vaste et complexe. Elle s'en tient aux fonctions nécessaires aux connexions TLS.	PolarSSL s'obtient sous GPL v2 et en version commerciale (double licence).
GnuTLS	GnuTLS est aussi complexe par ses fonctions qu'OpenSSL. En outre, des failles de sécurité sont apparues à tout moment.	GnuTLS a été développé comme alternative à OpenSSL il y a longtemps, et fait partie du projet GNU.

[12] http://fr.wikipedia.org/wiki/Confidentialit%C3%A9_persistante (état: le 1er septembre 2014).

MELANI recommande de façon générale de configurer les connexions sécurisées par cryptage de façon à obtenir une sécurité maximale[13].

D'où l'importance de respecter les règles suivantes pour le protocole SSL/TLS:

- N'utiliser que des chiffrements sûrs, p. ex.
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  ou
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Prendre en charge la confidentialité de transmission parfaite (PFS), pour que si une clé privée est compromise, il soit impossible de décrypter plus tard les éventuelles communications piratées. Les algorithmes susmentionnés répondent à cette exigence.
- Conserver les clés privées de la manière la plus sûre possible, idéalement sur un module de sécurité matériel (*hardware security module, HSM)*.
- Implémenter le mécanisme *HSTS (HTTP Strict Transport Security)*. Avec HSTS, le serveur déclare au navigateur comment procéder avec les connexions sécurisées. Par conséquent, seule une communication cryptée, basée sur des certificats valables, est possible avec ce serveur.
- Eviter les contenus mixtes (une partie seulement du contenu étant cryptée). Des agresseurs pourraient sinon manipuler des informations de la session à partir des contenus non sécurisés.
- Recourir à une autorité de certification (*certificate authority, CA)* digne de confiance. De façon générale et en cas d'incident notamment, il est précieux que la CA fasse partie de la même juridiction. Selon l'orientation stratégique de l'entreprise et le degré de menace, il convient de s'assurer que la CA ait son siège en Suisse.

Heartbleed a montré qu'il peut valoir la peine, du point de vue de l'architecture, d'avoir un point d'entrée central pour toutes les connexions SSL, qui bénéficie de la surveillance requise et qui, en cas de faille de sécurité, puisse être très rapidement corrigé.

4.2 Incidents d'espionnage

Au premier semestre 2014 également, plusieurs incidents d'espionnage ont fait les gros titres. La société russe de solutions de sécurité informatique Kaspersky a ainsi publié le 10 février 2014 un cas d'espionnage répondant au nom de «Careto/The Mask».[14]

Careto / The Mask

L'opération Careto aurait débuté en 2007, et donc être restée inaperçue pendant plus de six ans. Cette campagne d'espionnage se caractérise par son caractère universel et par sa grande capacité d'adaptation. Outre que le maliciel parvient à infecter divers systèmes d'exploitation comme Windows, Mac, Linux, etc., Kaspersky a même soupçonné l'existence d'une version pour smartphones. L'infection avait lieu lors de l'envoi de courriels de *spear phishing*. Ces courriels renfermaient des liens vers des sites Web où figuraient divers *exploits* adaptés aux victimes potentielles. Ces *exploits* étant dissimulés dans des sous-répertoires de sites Web, on y accédait uniquement par le lien direct et non en cas de visite

[13] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report/at_download/fullReport (état: le 1er septembre 2014).

[14] http://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/ (état: le 1er septembre 2014).

par hasard du site infecté. Pour donner une impression de légitimité à leurs liens, les escrocs utilisaient des URL imitant les noms de domaine des principaux quotidiens d'Espagne, mais aussi de journaux internationaux comme «The Guardian» ou le «Washington Post».

Une fois installé, le *maliciel* s'attaque à différents canaux de communication, comme p. ex. Skype, et cherche à collecter un maximum de documents de divers types. Kaspersky a identifié plus de 380 victimes dans 31 pays, en Suisse aussi. Des secteurs très variés étaient concernés, dans le secteur tant public (gouvernements, représentations diplomatiques) que privé (énergie, recherche, finances). Des attaques aussi complexes laissent supposer la présence d'un acteur étatique. Le texte espagnol contenu dans le maliciel, qui suggère que l'auteur viendrait du monde hispanophone, est plutôt surprenant dans ce contexte. Mais il peut naturellement aussi s'agir d'un brouillage volontaire des pistes.

Uroburos/ Turla/ Snake/ Epic

Au premier semestre 2014, divers prestataires de sécurité[15] ont fait état d'une opération d'espionnage baptisée tantôt Epic, Turla, Uroburos ou Snake. Ainsi, le spécialiste allemand de sécurité informatique G-Data[16] a publié en mars 2014 un rapport sur le maliciel d'espionnage Uroburos. Ce maliciel complexe possède notamment une fonction *P2P (peer to peer*). D'où son aptitude à se disséminer et à communiquer même dans les réseaux internes dont les ordinateurs ne sont pas tous nécessairement reliés à Internet. Les cibles évoquées comprennent des institutions étatiques, des services de renseignement et de grandes entreprises. G-Data situe le début de la campagne en 2011, année de compilation des plus anciens pilotes. Le développement du maliciel remonterait toutefois à 2005, selon un rapport de la société BAE Systems Applied Intelligence[17]. Une attaque d'espionnage révélée en mai, visant le Ministère belge des affaires étrangères, impliquerait également Uroburos. C'est le quotidien belge « De Standaard » qui a révélé l'affaire, en se référant à une source digne de confiance[18]. Dans le cas précis, il semble que les pirates s'intéressaient surtout aux documents, analyses ou rapports concernant la crise ukrainienne.

Opération Newscaster

Un groupe de pirates iraniens est parvenu à lancer une attaque ciblée de *spear phishing* qui, en trois ans, a infecté plus de 2000 ordinateurs.[19] Pour mener à bien son opération intitulée Newscaster, le groupe a créé des dizaines de faux profils sur les principaux réseaux sociaux. Les personnes dissimulées derrière ces profils prétendaient travailler dans le journalisme, dans le secteur de l'armement ou pour leur gouvernement. Elles cherchaient ainsi à persuader un maximum de victimes de les accepter comme «amis». Un faux site d'actualités, pour lequel travaillaient les prétendus journalistes, avait même été créé pour cette opération. En réalité, « Newsonair.org » copiait le contenu d'autres portails d'information et le publiait en son nom. Dans un premier temps, des courriels anodins de correspondance courante étaient envoyés. Il s'agissait d'inspirer confiance aux victimes choisies. Le moment venu, des courriels préparés avec des maliciels prenaient le relais. Les personnes visées comprenaient surtout des dirigeants militaires ou politiques vivant aux Etats-Unis et en Israël.

---

15 http://securelist.com/analysis/publications/65545/the-epic-turla-operation/ (état: le 1er septembre 2014).

16 https://blog.gdata.de/artikel/uroburos-hochkomplexe-spionagesoftware-mit-russischen-wurzeln/ (état: le 1er septembre 2014).

17 http://www.baesystems.com/what-we-do-rai/the-snake-campaign? (état: le 1er septembre 2014).

18 http://www.standaard.be/cnt/dmf20140512_01103164 (état: le 1er septembre 2014).

19 http://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/ (état: le 1er septembre 2014).

Action symbolique contre de supposés espions chinois?

Le Ministère américain de la justice a mis en accusation pour cyberespionnage cinq militaires chinois.[20] Les faits reprochés se situaient entre 2006 et 2014.[21] Les accusés font partie de l'armée populaire de libération chinoise. Mais comme ces personnes ne mettront sans doute jamais les pieds aux Etats-Unis ou dans un Etat ayant conclu avec eux un accord en matière d'extradition, l'accusation revêt un caractère plutôt symbolique.

Depuis longtemps, les activités de cyberespionnage ont cessé d'être des événements isolés. Les données sensibles suscitent un intérêt qui ne se relâche pas et sont soumises à des pressions permanentes. La Suisse est d'autant plus concernée qu'elle abrite de nombreuses entreprises de pointe, dont le savoir-faire et les connaissances ont une valeur inestimable.

4.3 Installations industrielles occidentales piratées

Une campagne d'espionnage et de sabotage (ou du moins d'actes préparatoires), visant des installations industrielles ou des fournisseurs d'énergie occidentaux, a été rendue publique à fin juin 2014. Des indices montrent que le groupe de pirates, baptisé par les entreprises de sécurité «Dragonfly[22]», «Energetic Bear[23]» ou «Crouching Yeti[24]», aurait été actif dès 2010. Les agressions révélées, réalisées en phases successives dès le début de 2013, ont emprunté différents canaux. La première étape a consisté à envoyer des courriels contenant en annexe un maliciel à des collaborateurs spécialement choisis des entreprises visées (*spear phishing*). Les pirates ont par ailleurs infiltré plusieurs sites consacrés aux questions d'approvisionnement énergétique, pour y placer des *infections par drive-by download* (attaques de point d'eau ou *watering hole*). Enfin, le groupe est parvenu à remplacer, sur les sites de fabricants d'*automates programmables*, des logiciels d'origine par des versions manipulées.

Les escrocs ont recouru à divers types de maliciels pour atteindre leurs fins:

- *chevaux de Troie* (Havex et Sysmain);
- *portes dérobées* (Karagany et Oldrea);
- autres outils adaptés au but visé (persistance de la présence dans le réseau, vol de données).

Ces attaques ont exclusivement tiré parti de failles de sécurité connues. Les victimes sont principalement des entreprises tant européennes qu'américaines.

Il est intéressant de noter ici l'automatisation faite de la recherche des *serveurs OPC*, au niveau tant local que dans Internet. En manipulant de tels serveurs, il devient possible de

---

[20] http://www.spiegel.de/netzwelt/netzpolitik/cyberspionage-usa-klagen-chinesische-regierungsbeamte-an-a-970259.html (état: le 1er septembre 2014).

[21] MELANI, rapport semestriel 2013/1, chapitre 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 1er septembre 2014).

[22] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat (état: le 1er septembre 2014).

[23] http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf (état: le 1er septembre 2014).

[24] http://www.kaspersky.com/about/news/virus/2014/crouching-yeti-an-ongoing-spying-campaign-with-2800-highly-valuable-targets-worldwide (état: le 1er septembre 2014).

perturber les processus physiques commandés à partir de là. Le maliciel possède l'aptitude d'identifier les systèmes OPC à l'aide de leur empreinte digitale (*fingerprint*) et transmet les informations sur les systèmes découverts au serveur *Command & Control (C&C server).*

La campagne a un but d'espionnage essentiellement. Mais une présence durable dans les systèmes et réseaux cibles semble aussi prévue, afin de pouvoir le cas échéant commettre par la suite des activités de sabotage.

La dissimulation de chevaux de Troie dans des logiciels de fabricants a permis de déjouer toutes les précautions de sécurité prises par les utilisateurs – après tout, ils sont censés installer de tels paquets logiciels pour utiliser l'appareil ou le service en question.

Cette campagne illustre bien le déroulement des attaques contre les infrastructures critiques. Des mesures ciblées cherchent à identifier, dans les réseaux des exploitants, une brèche permettant de s'implanter à proximité des systèmes jugés intéressants. Par la suite, un maximum d'informations est collecté (reconnaissance). Les agresseurs veillent en outre à pérenniser leur accès, pour pouvoir continuer à collecter des informations et, le cas échéant, procéder à des manipulations.

Divers moyens permettent de sécuriser l'interface OPC:

- introduire et régulièrement actualiser les listes de contrôle d'accès (*access control list, ACL*) entre les clients et les serveurs OPC, selon le principe du droit d'accès minimal (*least privilege*);
- effectuer les communications basées sur le protocole *RPC (remote procedure call*, appel de procédure distante) sur des réseaux séparés, avec liaison point à point;
- sécuriser de telles connexions par une technique de tunnellisation (*tunneling*);
- contrôler les accès (journalisation centralisée et surveillance régulière du fichier journal);
- si le logiciel porte une signature numérique, la vérifier avant toute installation.

De façon générale, MELANI recommande tout à la fois d'ériger autant que possible une barrière hermétique entre l'infrastructure TIC usuelle et les équipements de contrôle industriels, et de fortifier ces derniers contre les attaques directes. Voir aussi les mesures de protection des systèmes de contrôle industriels (SCI) préconisées par MELANI.[25]

4.4 Conflits dans le cyberespace

Outre le conflit au Proche-Orient, où des hacktivistes arabes s'en prennent à Israël, et les escarmouches incessantes de l'Armée électronique syrienne (Syrian Electronic Army) fidèle à Damas, la crise ukrainienne a incité divers protagonistes à lancer des opérations dans le cyberespace. Avant et pendant l'invasion de la Crimée par les troupes armées à fin février 2014, des intrusions physiques dans les installations de télécommunication et sans doute aussi des cyberattaques avaient gravement perturbé sur la presqu'île le réseau de téléphone mobile et l'accès à Internet. Peu après, les sites Web du gouvernement ukrainien sont devenus temporairement inaccessibles, et divers membres du Parlement se sont plaints de ne pas pouvoir utiliser normalement leur téléphone mobile. En Russie aussi, comme les sites Internet d'opposants au gouvernement avaient été coupés du réseau au début de mars, des hacktivistes s'en sont pris aux pages Web du Kremlin, qui n'ont pu être consultées pendant

[25] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=fr (état: le 1er septembre 2014).

un certain temps. Les mêmes pirates informatiques ou d'autres ont également perturbé l'accès aux pages Web de l'OTAN.

Dans quelle mesure les attaques contre les installations industrielles occidentales décrites au chapitre 4.3 ci-dessus s'inscrivent-elles dans le même contexte? Seules des conjectures sont possibles à l'heure actuelle. Aux Etats-Unis, un scénario envisagé depuis quelque temps prévoit qu'une puissance étrangère cherche à infiltrer l'approvisionnement énergétique local, pour priver le pays de courant électrique en cas de besoin.

Comme signalé dans de précédents rapports semestriels, les conflits dans le monde physique déclenchent toujours plus souvent des actions et réactions en chaîne dans le cyberespace. Dans les cas notamment où les armes conventionnelles ne sont d'aucune utilité contre un protagoniste – parce qu'une agression physique ne ferait qu'aggraver la situation, que l'adversaire est hors de portée ou encore que les rapports de force sont gravement asymétriques –, une cyberattaque constitue un moyen bien commode de causer du tort à l'adversaire, ou du moins de lui montrer son mécontentement.

De petits groupes de personnes, voire des individus isolés sont susceptibles de nuire gravement aux Etats dont l'économie et/ou les infrastructures critiques sont largement tributaires du bon fonctionnement de leurs TIC, et donc vulnérables sur ce plan.

Enfin il ne faut pas négliger, en cas d'actions menées dans le cyberespace, la volonté des protagonistes ou d'autres groupes d'intérêts de faire passer leur message (propagande). Car dans tout conflit, celui qui domine voire contrôle la sphère de l'information possède un sérieux avantage.

4.5 NSA – nouvelles publications

Les révélations d'Edward Snowden et l'affaire de la NSA se sont poursuivies en 2014, mais à moindre échelle. Le présent sous-chapitre passe brièvement en revue les principales publications. Les premières retombées des documents publiés sur l'évolution d'Internet font l'objet d'un autre sous-chapitre du rapport semestriel (voir chap. 5.3).

Failles de sécurité informatiques non divulguées par les Etats-Unis

Une publication basée sur les révélations de Snowden affirme que la NSA exploiterait souvent à son profit les failles de sécurité découvertes dans des logiciels. Un conseiller du président Obama a expliqué qu'il existait bel et bien des critères permettant de décider si une faille devait être rendue public ou non. Leur exploitation peut également s'avérer une mine d'informations pour la NSA. Les critères décidant de l'utilisation d'une vulnérabilité à des fins d'espionnage comprennent p. ex. le degré de diffusion de la technologie défaillante et le risque que quelqu'un d'autre ne la découvre et ne l'exploite. Une variante consisterait à exploiter la lacune dans un premier temps, avant de la rendre publique.[26]

[26] http://www.tagesanzeiger.ch/digital/internet/USA-halten-Sicherheitsluecken-in-Computersystemen-geheim/story/12638578 (état: le 1er septembre 2014).

Cette découverte n'a rien d'inédit. En 2005 déjà, une campagne d'espionnage avait tiré systématiquement parti de lacunes de sécurité des produits Microsoft. Elle avait été attribuée à l'époque à la Chine.[27]

Possible Manipulation par la NSA d'appareils destinés au réseau et expédiés par poste

Une autre publication des journalistes et avocats Glenn Greenwald et Jacob Appelbaum a révélé que la NSA interceptait «en partie» les envois postaux d'appareils reliés au réseau et de périphériques pour y installer des logiciels d'espionnage. Des collaborateurs de TAO (Tailored Access Operations) ajoutaient à ces appareils des techniques spéciales leur offrant des possibilités d'espionnage. Après quoi ils étaient réemballés et envoyés à leur destinataire. Selon Greenwald, cette pratique concernait aussi les routeurs et serveurs de Cisco, entreprise américaine fabriquant une bonne partie des composantes réseau utilisées au monde et assurant leur maintenance.[28] Il est intéressant de noter que ces dernières années, les Etats-Unis aient invité à se méfier des entreprises chinoises Huawei et ZTE, qui elles aussi produisent des composantes réseau.[29] Concrètement, ils accusaient la technologie de ces deux entreprises de servir à espionner les réseaux américains.

La Chambre des représentants a adopté en juin 2014 un projet interdisant à la NSA et à la CIA de financer l'introduction, à des fins de surveillance, de failles de sécurité ou de portes dérobées dans les produits ou services conçus sur sol américain.[30] Une autre pratique courante et de notoriété publique pourrait être prohibée, soit les analyses a posteriori des données déjà collectées ou obtenues pour y découvrir des informations sur des citoyens américains. Mais le dossier doit encore obtenir l'aval du Sénat.

Enregistrement de communications téléphoniques dans tout le pays

Il est également apparu que sous le nom de code «Somalget», les conversations sur les appareils mobiles sont épiées à grande échelle aux Bahamas. Les appels téléphoniques subiraient un espionnage systématique dans au moins un autre pays. Somalget fait partie du programme Mystic, collectant des informations sur les appels téléphoniques au Mexique, aux Philippines et au Kenya.[31] A ceci près que Mystic n'enregistre que les métadonnées et Somalget aussi les contenus. La NSA a apparemment profité de la coopération instaurée entre les autorités des Bahamas et l'agence américaine de lutte contre les stupéfiants (Drug Enforcement Administration, DEA), qui collaborent dans la surveillance de certains raccordements au titre de la lutte antidrogue, afin d'accéder à la totalité du réseau de téléphonie mobile.

Prise d'influence sur la norme d'encryptage des communications

Selon des documents publiés au premier semestre 2014, le GCHQ (Government Communications Headquarter, pendant britannique de la NSA) aurait d'emblée obtenu que

---

27 MELANI, rapport semestriel 2006/1, chapitre 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/00162/index.html?lang=fr (état: le 1er septembre 2014).

28 http://www.droemer-knaur.de/buch/7943698/die-globale-ueberwachung (état: le 1er septembre 2014).

http://www.heise.de/newsticker/meldung/NSA-manipuliert-per-Post-versandte-US-Netzwerktechnik-2187858.html (état: le 1er septembre 2014).

29 http://www.spiegel.de/netzwelt/netzpolitik/us-kongress-will-chinas-telekom-firmen-huawei-und-zte-aussperren-a-860014.html (état: le 1er septembre 2014).

30 http://thehill.com/blogs/floor-action/house/210027-house-votes-to-limit-nsa-spying (état: le 1er septembre 2014).

31 https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (état: le 1er septembre 2014).

la norme de téléphonie mobile A5/1 renferme des clés courtes. Alors qu'au départ une clé de chiffrement de 128 *bits* était préconisée, le GCHQ avait insisté dans les années 1980 pour obtenir une clé de 48 bits. Un compromis avait finalement été trouvé sur une clé de 64 bits, dont dix chiffres sont toujours nuls. Autrement dit, l'algorithme de cryptage A5/1 a d'emblée été facile à casser.[32] Les premières attaques connues remontent à 2000.[33] La norme âgée de 25 ans reste utilisée, et ce n'est que peu à peu que la norme A5/3 prend le relais.

Pour rappel, l'année dernière, c'est surtout la norme «Dual_EC_DRBG» qui s'est retrouvée au centre de l'attention, ce générateur de nombres aléatoires conçu par la NSA n'étant pas aussi imprévisible qu'il le devrait.

La NSA et le GCHQ auraient accès aux données des utilisateurs d'apps

On savait depuis longtemps que diverses données d'applications pour smartphones, ou apps, sont transmises à l'exploitant. Nous avions signalé dans le rapport semestriel 2011/2[34] que les droits qu'une app s'attribue, à l'insu des utilisateurs non avertis, vont parfois au-delà de ce dont elle a réellement besoin pour fonctionner de façon irréprochable. La nouveauté signalée par le « New York Times », le « Guardian » et « ProPublica », c'est que la NSA et le GCHQ accèdent également aux données que les apps pour smartphones collectent sur les utilisateurs. Au-delà d'informations élémentaires (âge, sexe, localisation, etc.), elles renferment le cas échéant de données complexes sur leur profil individuel. La valeur de telles données est telle que la NSA aurait dépensé plus d'un milliard de dollars pour se procurer ce programme. En outre, les Etats-Unis se félicitent dans une des présentations publiées de l'usage croissant fait des smartphones.

WLAN à l'aéroport – les services secrets canadiens auraient surveillé le réseau

A l'ère de la communication mobile, l'un des premiers réflexes à la descente de l'avion est d'allumer son téléphone mobile pour contrôler ses messages ou télécharger d'autres informations – de préférence à un réseau local sans fil (*WLAN*) mis à disposition par l'aéroport. Le Centre de la sécurité des télécommunications Canada (CSTC), service de renseignement du gouvernement canadien, en a apparemment profité pour localiser les voyageurs dans le pays, à partir des données WLAN d'un grand aéroport canadien. En effet, chaque fois qu'ils se connectent à un réseau public, les appareils transmettent des *métadonnées* qui permettront de les identifier à nouveau plus tard. D'où la possibilité de suivre à la trace les personnes surveillées, grâce aux données recueillies à l'aéroport.[35]

Capacité de la NSA de réacheminer les communications par Internet

Selon les publications tirées des révélations de Snowden, la NSA serait en mesure, dans le cadre du programme Qfire de réacheminer n'importe quelle connexion par Internet. De telles attaques menées de façon décentralisée permettraient à la NSA de capturer et de manipuler des données à proximité de leurs cibles.[36]

---

32 http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html#.UtFDAvZuTGK (état: le 1er septembre 2014).

33 http://fr.wikipedia.org/wiki/A5/1 (état: le 1er septembre 2014).

34 MELANI, rapport semestriel 2011/2, chapitre 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: le 1er septembre 2014).

35 http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881 (état: le 1er septembre 2014).

36 http://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigng-der-nsa-fotostrecke-105358.html (état: le 1er septembre 2014).

L'OSCE aurait également été prise pour cible par la NSA

Les organisations internationales constituent une cible de choix pour des opérations d'espionnage. Des collaborateurs de nombreux pays s'y côtoient dans un périmètre restreint, et de multiples outils de communication électronique y sont utilisés. On savait depuis août 2013 que la NSA espionne le siège des Nations Unies de New York.[37] Entre-temps, le quotidien autrichien « Die Presse » a signalé que les services de renseignement américains auraient également mis sous écoute le siège de l'OSCE à Vienne.[38] Il le tient d'un journaliste allemand ayant eu accès au matériel collecté par Snowden. Le document en question parlait surtout d'«objectifs de politique extérieure» ainsi que du «contrôle et des ventes d'armes».

4.6 Réactivité des escrocs face à l'actualité

Les arnaques à l'avance des frais sont un phénomène largement connu et documenté. Les escrocs élaborent un scénario dans lequel la cible aurait soi-disant la chance de bénéficier d'une grosse somme d'argent, par ex. suite à un héritage, un fonds tombé en déshérence ou un gain à la loterie. Si une réponse à la première prise de contact est donnée, des paiements seront réclamés sous divers prétextes, et bien entendu la somme promise ne sera jamais versée. Une des spécificités de ces escrocs est leur capacité d'adaptation, que ce soit à la cible ou au contexte. Un exemple typique est la façon dont les auteurs utilisent l'actualité pour augmenter leurs chances de tromper leur victime. En 2014, la Coupe du monde au Brésil a par ex. été largement utilisée par les fraudeurs. La rareté des billets, et le côté exceptionnel de l'événement ont constitué un terreau fertile à l'élaboration de scénarios où la cible se voyait promettre une chance exceptionnelle de participer à l'événement, moyennant un paiement préalable. Bien entendu, il s'agissait là uniquement d'une astuce visant à récolter de l'argent, mais également des informations personnelles.

La catastrophe aérienne de Malaysia Airlines en début d'année 2014, et en particulier la confusion ayant régné suite à la disparition de l'avion, a également été une source d'inspiration pour différents types d'escrocs. Des liens promettant l'accès à une vidéo de l'avion retrouvé se sont notamment répandus sur les réseaux sociaux. L'utilisateur suivant ces derniers risquait une infection, puisqu'en lieu et place de la vidéo, il se voyait redirigé vers un site chargé de lui transmettre un *virus*. Dans certains cas, c'est vers une page de *phishing* que la victime était dirigée, où il lui était demandé de fournir des informations de connexion pour accéder au contenu promis.

Les escrocs actifs sur Internet font souvent preuve d'une grande capacité d'adaptation. Les événements ayant une résonnance internationale constituent pour eux autant d'opportunités. En s'appuyant sur ces actualités, ils élaborent des scénarios visant à susciter l'intérêt de leurs cibles. Il convient pour les internautes d'adopter une attitude prudente et sceptique face à toute offre non sollicitée. Avant de suivre un lien, d'ouvrir une pièce jointe ou de fournir des informations, il convient de toujours s'assurer de la légitimité du message et de l'expéditeur. S'il n'est pas possible de dissiper ses doutes, il convient d'effacer l'E-mail.

[37] http://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-918421.html (état: le 1er septembre 2014).

[38] http://diepresse.com/home/politik/aussenpolitik/3809719/NSAAffaere_Obama-laesst-OSZE-ausspionieren (état: le 1er septembre 2014).

4.7 Sécurité aérienne perturbée par un exercice militaire?

Les 5 et 10 juin 2014, les services de la navigation aérienne civile d'Europe centrale et orientale ont ponctuellement perdu le contact radar avec les aéronefs, durant 20 à 25 minutes. L'incident a touché le radar secondaire, qui communique les données du transpondeur de l'aéronef, comme son code d'identification et son altitude. La position des avions était par contre visible. De même, les liaisons radio sont restées garanties en tout temps avec tous les avions.

Peu après, on a supposé qu'un exercice militaire organisé par l'OTAN en Hongrie et en Italie avait causé la panne du radar secondaire. L'OTAN a confirmé avoir testé le brouillage local de certaines fréquences, tout en jugeant hautement improbable que les perturbations proviennent de tels exercices, car les fréquences brouillées lors de l'exercice différeraient de celles utilisées dans l'aviation civile. L'autorité de contrôle du trafic aérien Eurocontrol a ouvert une enquête sur ces incidents.

Selon l'état actuel des connaissances, la probabilité d'un dysfonctionnement de logiciel ou de matériel, voire d'une manipulation des radars est faible. On ne s'expliquerait guère sinon que les services de la navigation aérienne de plusieurs pays aient constaté le même phénomène avec des appareils différents. Une perturbation externe paraît plus plausible. Un rapport provisoire d'Eurocontrol a beau considérer que les fréquences étaient suffisamment séparées entre la navigation militaire et la navigation civile[39], la corrélation spatiotemporelle des événements avec l'exercice est frappante.

4.8 Mots de passe découverts et volés

34 millions de mots de passe volés découverts par le BSI

A fin janvier 2014, l'Office fédéral allemand de la sécurité dans la technologie de l'information (BSI) a révélé que l'analyse d'un *réseau de zombies* avait fait découvrir 16 millions de données d'accès, formées d'une adresse électronique et d'un mot de passe.[40] Ces données provenaient de toutes sortes de comptes en ligne reposant sur une adresse électronique et un nom d'utilisateur. Elles avaient visiblement été obtenues d'ordinateurs infectés par un maliciel. Chaque fois que l'utilisateur saisissait sur un ordinateur compromis une adresse électronique et un mot de passe, ses données d'accès étaient dérobées et communiquées à un serveur central contrôlé par les escrocs.

Au début d'avril 2014, le BSI a signalé une autre découverte de mots de passe. Il s'agissait cette fois de 18 millions de données d'utilisateurs.[41] Outre le lien URL installé depuis janvier 2014[42], où chacun pouvait vérifier si son adresse électronique avait été compromise, d'autres moyens d'informer les victimes ont été utilisés. Ainsi, le BSI a prévenu de l'incident des fournisseurs de messagerie comme GMX et Web.de, qui ont bloqué les comptes concernés en signalant le piratage de données. Dans les deux cas, des comptes de messagerie helvétiques ont aussi été touchés.

---

39 http://www.n24.de/n24/Nachrichten/Politik/d/5260064/militaeruebungen-koennten-radar-gestoert-haben.html (état: le 1er septembre 2014).

40 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html (état: le 1er septembre 2014).

41 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Neuer_Fall_von_Identitaetsdiebstahl_07042014.html (état: le 1er septembre 2014).

42 https://www.sicherheitstest.bsi.de/ (état: le 1er septembre 2014).

Vol de données chez eBay

En mai dernier, eBay publiait un communiqué où l'entreprise reconnaissait avoir été victime d'une attaque ayant permis à des pirates d'accéder à une base de données contenant des informations de clients. Les auteurs de l'attaque auraient ainsi eu accès à des adresses électroniques, mots de passe (encryptés), adresses postales, numéros de téléphone, mais apparemment à aucune information de nature financière. Le nombre de données compromises n'a pas été révélé. Même si rien n'indique que les criminels aient réussi à décrypter les mots de passe, Ebay a recommandé à tous les utilisateurs de les changer.

Cet incident soulève en particulier la question de la faille initiale. En l'occurrence et comme l'a confirmé eBay, des données d'accès d'employés de l'entreprise ont été compromises fin février déjà. Les auteurs ont ainsi pu accéder au réseau de l'entreprise. On ignore par contre de quelle manière les données d'accès ont été initialement acquises. L'hypothèse selon laquelle une attaque empruntant en partie au moins des méthodes d'ingénierie sociale aurait été déployée a été avancée par plusieurs experts, et semble à l'heure actuelle la piste la plus probable. Là encore, un envoi de *spear phishing* pourrait avoir été utilisé.

Cet incident démontre qu'une compromission initiale de taille restreinte peut selon les cas donner un accès étendu à un réseau et à tout ce qu'il contient, notamment à des bases de données. Pour les criminels, il est ainsi souvent judicieux d'investir des ressources considérables pour cibler quelques comptes dans une entreprise, qui leur permettront d'accéder à des sources importantes d'information. Pour les entreprises, cela signifie que le nombre de comptes avec des privilèges étendus doit être autant que possible limité et surveillé, afin de détecter d'éventuelles activités inhabituelles.

4.9 Nouvelles variantes d'attaques DDoS

Les attaques par déni de service visent à rendre un service inaccessible aux utilisateurs, ou du moins à en limiter sérieusement la disponibilité. Très fréquentes, de telles *attaques DDoS* constituent pour de nombreuses infrastructures TIC une menace à prendre au sérieux. Outre les attaques bien connues par amplification et réflexion DNS, qui tirent parti de *serveurs DNS* publics, diverses techniques novatrices sont apparues ces derniers mois. D'autres services accessibles à tout le monde ont été compromis de la même façon. On peut citer par ex. la norme de gestion de réseau *SNMP* (simple network management protocol), le protocole de réseau *NTP* (network time protocol), utilisé pour synchroniser les horloges des ordinateurs d'un réseau, ou le protocole CHARGEN (Character Generator Protocol), utilisé à des fins de test et débogage. Il est typique de ce genre d'attaques qu'une brève requête débouche sur une réponse bien plus volumineuse, acheminée ensuite vers la cible de l'attaque. Les services précités reposent sur le protocole *UDP (User Datagram Protocol)*, très prisé pour les attaques DDoS parce qu'il est «sans connexion» et donc ne valide pas les *adresses IP* intervenant dans la communication.

Le rapport semestriel 2013/2[43] de MELANI avait déjà parlé d'attaques NTP faisant appel à la commande «monlist», sujet qui reste d'actualité. Cette commande publie une liste des 600 dernières *adresses IP* s'étant connectées au serveur NTP. Moyennant une falsification de l'adresse d'origine de la requête, il est possible de transmettre cette liste complète à la victime. Au début de 2014, des attaques DDoS au débit supérieur à 400Gb/s ont été

[43] MELANI, rapport semestriel 2013/2, chapitre 3.10: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=fr (état: le 1er septembre 2014).

mesurées. Le protocole SNMP offre des possibilités d'amplification équivalentes, et des pirates informatiques s'en servent déjà activement.

Une nouvelle variante d'attaque DDoS tire parti d'une fonction de Wordpress, système de blog et de gestion de contenu très répandu (*blog/CMS software)*. Wordpress dispose d'une fonction *PingBack*, qui permet à un site d'exiger une notification chaque fois que d'autres sites postent un lien vers lui. A supposer qu'un pirate manipule cette fonction et expédie l'adresse de sa victime à un grand nombre d'instances Wordpress, ces dernières enverront une telle requête *HTTP* au site indiqué, qui risquera de s'effondrer sous l'afflux des messages. Il est impossible pour la victime de connaître l'auteur de l'agression, qui mobilise des milliers d'installations Wordpress légitimes. Lors d'un tel incident, plus de 160 000 sites Wordpress avaient été mis à contribution pour lancer l'attaque DDoS.

De façon générale, MELANI recommande de protéger les systèmes, pour éviter qu'ils ne servent à lancer des attaques DDoS. Les ressources utiles pour sécuriser les serveurs DNS ou NTP sont disponibles sur Internet, à l'instar des services de Team Cymru.[44] Il n'est pas facile de protéger les objets créés avec Wordpress, la fonction PingBack du système étant en principe souhaitable. Il est néanmoins possible de créer un module de filtrage qui désactive cette fonction.

Il est crucial que les fournisseurs de services Internet (*Internet Service Provider, ISP)* s'inspirent du document BCP 38[45] (Best Current Practice), pour résoudre à moyen ou long terme le problème des attaques DDoS. Ce document technique indique comment protéger un réseau du trafic indésirable (paquets de requêtes avec des adresses IP falsifiées ou incorrectes) en filtrant les requêtes entrantes (*ingress filtering*).

4.10 Attaques visant les monnaies virtuelles

La monnaie électronique décentralisée Bitcoin a fait l'objet d'un chapitre du précédent rapport semestriel MELANI[46]. Les enjeux sécuritaires de cette monnaie y étaient relevés: vol de clés privées, attaques visant les plateformes d'échange, maliciels cherchant à dérober aux utilisateurs des bitcoins ou utilisant la puissance de calcul de leur appareil à des fins de minage.

Il a beaucoup été question de Bitcoin en 2014, pour des raisons sécuritaires notamment. En particulier, des maliciels s'en sont pris aux utilisateurs d'Android. Google a dû retirer du Google Play Store plusieurs applications, qui contenaient des maliciels visant à miner des Bitcoins et d'autres monnaies du même type à l'insu du propriétaire du smartphone. Dans le cas de Bitcoin, le nombre croissant d'utilisateurs et donc l'augmentation des ressources nécessaires au travail de minage expliquent que les criminels tentent d'accéder à de la puissance de calcul additionnelle, notamment à travers les téléphones mobiles. De nombreux experts notent cependant qu'à l'heure actuelle, ce type de procédé reste peu rentable, à cause du temps nécessaire au minage. Ce détournement de ressources entraîne une baisse d'efficacité de l'appareil des victimes, dont la batterie se décharge très vite.

Les plateformes sur lesquelles les utilisateurs peuvent échanger des monnaies traditionnelles contre des Bitcoins n'ont pas été épargnées. Comme le signalait le précédent

---

44 http://www.team-cymru.org/ReadingRoom/Tips/dns.html (état: le 1er septembre 2014).

45 http://tools.ietf.org/html/bcp38

46 MELANI, rapport semestriel 2013/2, chapitre 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=fr (état: le 1er septembre 2014).

rapport semestriel, elles constituent une cible de choix. Le cas de la faillite de Mt. Gox[47] témoigne de l'importance de ces bourses et de leur vulnérabilité. Cette plateforme, l'une des plus anciennes et des principales du marché, a cessé toute transaction le 7 février 2014, avant de se placer le même mois sous la protection de la loi japonaise sur les faillites. Elle aurait perdu 750 000 Bitcoins appartenant à ses clients et 100 000 lui appartenant en propre, soit 620 millions de dollars au total. Une des causes de cette débâcle serait à rechercher dans l'exploitation, sur la plateforme Mt. Gox, du problème de la malléabilité des transactions. Certains experts doutent cependant qu'il s'agisse de l'unique raison du fiasco. Parmi les autres pistes évoquées figurent la gestion interne défaillante de Mt. Gox et l'emploi par des hackers, le cas échéant, d'autres méthodes pour s'emparer de Bitcoins.

Bitcoin et les monnaies virtuelles restent au centre de l'attention publique, et soulèvent en particulier des questions sécuritaires et des doutes sur leur fiabilité. Leur rôle dans des investigations pénales en cours justifie un intérêt tout particulier de la part des autorités de poursuite pénale, à l'heure où les Etats cherchent encore à en clarifier le statut légal. Au niveau suisse, un rapport du Conseil fédéral a récemment fait le point sur le fonctionnement des monnaies virtuelles et sur les problèmes qu'elles soulèvent.[48]

4.11 Succès contre des escrocs

La lutte contre les escrocs et les cyberpirates a enregistré plusieurs succès au premier semestre 2014.

Razzia contre les propriétaires du maliciel Blackshades

Le 20 mai 2014, une razzia a été faite contre les propriétaires du logiciel d'espionnage Blackshades. L'action lancée par le FBI a débouché sur des perquisitions dans 19 pays, auprès de plus de 300 propriétaires présumés de ce maliciel.[49] Une centaine de personnes ont été arrêtées, dont le cerveau supposé Alex Yucel. Le maliciel Blackshades permet un contrôle quasiment illimité à distance des machines Windows. Les pirates auraient utilisé ce logiciel d'espionnage à toutes sortes de fins. Le maliciel a également sévi en Syrie et en Libye, aux dépens de membres de l'opposition.

Fin de partie pour GameOver Zeus

Le 2 juin 2014, le Département américain de la justice (DOJ) et le FBI ont annoncé avoir désactivé les *réseaux de zombies* GameOver ZeuS (GOZ) et CryptoLocker.[50] GOZ se base sur le maliciel ZeuS / Zbot, qui sévit depuis quatre ans en Suisse et qui est l'un des rares réseaux de zombies à se baser sur la technique *P2P* (peer to peer, par opposition à client-serveur). Les deux réseaux visaient à commettre des fraudes à l'e-banking ou utilisaient le chantage (*ransomware*).

MELANI a adopté dès juillet 2013 des mesures en vue de réduire la menace posée par cryptolocker, en collaboration avec les *fournisseurs Internet suisses*.

---

47 http://de.wikipedia.org/wiki/Mt.Gox (état: le 1er septembre 2014).

48 http://www.admin.ch/aktuell/00089/?lang=fr&msg-id=53513 (état: le 1er septembre 2014).

49 http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown (état: le 1er septembre 2014).

50 http://www.abuse.ch/?p=7822 (état: le 1er septembre 2014).

Après la désactivation du réseau de zombies Cryptolocker, les prestataires de sécurité FireEye et Fox-IT ont mis à disposition des victimes un service gratuit leur permettant de récupérer les données encore cryptées par le maliciel.[51]

Arrestation avec l'aide de la Suisse

Au début de mars 2014, la police thaïlandaise a arrêté à Bangkok, avec l'aide de la Suisse, le présumé cyberpirate Diab10, qui aurait notamment diffusé en 2005 Zotob.[52] Ce ver informatique avait paralysé de nombreux ordinateurs à l'époque. Marocain de naissance et en possession d'un passeport russe, l'escroc était recherché en Suisse pour «utilisation frauduleuse d'un ordinateur». Placé sous mandat d'arrêt, il sera extradé en Suisse.

4.12 Vulnérabilités des systèmes cyber-physiques

Maliciel dans une centrale nucléaire japonaise

La présence d'un maliciel a été constatée sur un ordinateur au début de 2014, dans la salle de contrôle de la centrale nucléaire de Monju au Japon. La machine aurait été infectée par la mise à jour d'un logiciel vidéo gratuit effectuée par un collaborateur. Par la suite, près de 42 000 courriels ainsi que la documentation de formations internes ont abouti en Corée du Sud, ou du moins transité par ce pays. L'infection a été signalée par le système de surveillance du réseau, qui avait détecté les connexions à un site Web inconnu.

Les comptes rendus de l'incident ne permettent pas de savoir si la machine infectée n'était utilisée qu'à des fins administratives ou aussi destinée au pilotage de processus critiques de la centrale. On ignore également si, en cas de fonctionnement normal du réacteur – la centrale étant hors service au moment de l'incident –, la machine aurait disposé d'un accès à Internet et dans quelle mesure elle est séparée, le cas échéant, des systèmes opérationnels de la salle de contrôle. Selon l'exploitant, l'incident n'aurait perturbé à aucun moment la sécurité des réacteurs.

Un incendie avait déjà obligé à arrêter en 1995 ce réacteur de type «surgénérateur», peu après sa mise en service. Un nouvel essai avait été tenté au printemps 2010. Or moins de quatre mois plus tard, un accident survenu lors du chargement de combustible avait entraîné son arrêt vraisemblablement définitif.

Même sans attaque ciblée contre une centrale nucléaire et si l'infection semble plutôt due au hasard, il est préoccupant qu'un maliciel puisse infecter un ordinateur situé dans la salle de commande d'où le réacteur en activité est piloté. Les réseaux opérationnels et ceux destinés à l'administration devraient autant que possible être hermétiquement séparés – a fortiori si les processus pilotés sont potentiellement aussi dangereux que la production d'énergie nucléaire.

Technique médicale informatisée et failles de sécurité

Le chercheur en sécurité Scott Erven a examiné pendant deux ans les appareils médicaux électroniques d'hôpitaux américains, et constaté la présence de lacunes gravissimes. Elles concernaient surtout des services Web incorporés, permettant aux appareils de

[51] http://www.melani.admin.ch/dienstleistungen/archiv/01583/index.html?lang=fr (état: le 1er septembre 2014).

[52] http://www.nzz.ch/aktuell/panorama/hacker-diab10-in-thailand-verhaftet-1.18265704 (état: le 1er septembre 2014).

communiquer entre eux et d'envoyer des données directement dans les dossiers des patients. Les problèmes tenaient moins à la programmation des logiciels qu'aux paramètres d'installation des systèmes. Les appareils étaient souvent protégés par des mots de passe faibles ou non modifiables, ils transmettaient en ligne sans les crypter les données des patients, et l'envoi d'ordres inconnus et donc vides de sens suffisait à les dérégler.

On n'ose imaginer ce qu'il adviendrait si un robot chirurgical tombait en panne en pleine intervention, si une pompe à perfusion administrait une dose trop élevée (ou trop faible) d'un médicament, ou si un stimulateur cardiaque transmettait au mauvais moment des impulsions électriques au patient. De même, des manipulations d'appareils à rayons X ou de scanners pourraient déboucher sur des doses de radiation excessives. Outre que les appareils médicaux électroniques sont directement exposés à des influences extérieures, la mise en réseau croissante de la domotique constitue un facteur de risque en milieu hospitalier: dès le moment où la température de systèmes de réfrigération des stocks de sang ou de médicaments peut être réglée à distance, il devient possible d'altérer lesdites réserves.

On trouve dans le domaine de la santé – tout comme dans les installations industrielles traditionnelles – des systèmes ou appareils cyber-physiques qui pilotent, à l'aide de logiciels, différents processus physiques. Ils sont souvent administrés à l'aide d'ordinateurs usuels faisant partie d'un réseau (au moins interne). D'où la nécessité de veiller dans les hôpitaux à ce que ces systèmes soient dûment séparés d'Internet et à l'abri d'une attaque ciblée ou due au hasard. En cas d'attaque ciblée, de banals ordinateurs reliés à Internet risquent de servir à des pirates de point d'entrée dans le réseau interne.

Vulnérabilité de l'approvisionnement électrique d'une ville

Les services industriels d'une ville allemande de taille moyenne ont laissé une équipe de pirates informatiques partir à l'assaut de leurs installations, afin de vérifier la sécurité de leur approvisionnement en électricité et en eau potable.[53] Les pirates ont testé tout le spectre des méthodes d'infiltration. Outre des tentatives directes d'intrusion par Internet, ils ont installé physiquement un point d'accès à une prise réseau facilement atteignable sur le site même – p. ex. dans la zone d'accueil ou les salles de conférences –, d'où ils avaient directement accès au réseau interne. Or là aussi, la méthode la plus simple a consisté à convaincre un collaborateur, par des méthodes d'ingénierie sociale, d'ouvrir l'annexe spécialement préparée d'un courriel. D'où l'installation d'un logiciel permettant aux agresseurs d'accéder au réseau interne. Les pirates mandatés sont finalement parvenus à infiltrer le logiciel de commande du poste central du fournisseur électrique, au point de pouvoir s'emparer des fonctions de contrôle et de commande. Les experts en sécurité ont conclu de l'incident qu'une prise de contrôle était certes possible, mais qu'il serait très difficile à l'agresseur de garder durablement le pouvoir, car le défenseur avait physiquement accès à tous les appareils, et donc possédait un avantage décisif face à la partie adverse. De même, les systèmes usuels d'approvisionnement continuent à disposer de nombreux éléments de protection électromécaniques et d'un affichage analogique, qui échappent au contrôle d'un cyberpirate. Une panne électrique ne serait par conséquent que de brève durée.

Un pirate très motivé et disposant de beaucoup de temps, et donc faisant preuve de la persévérance requise, peut s'introduire dans quasiment tout système. La première étape consiste toujours à se procurer un maximum d'informations sur l'entreprise, sur ses collaborateurs et, le cas échéant, sur les données relatives au système cible déjà connues par des sources publiques.

[53] http://heise.de/-2165153; voir aussi le documentaire télévisé: http://www.arte.tv/guide/fr/048364-000/netwars-la-guerre-sur-le-net et le web-documentaire interactif http://netwars-project.com/de/ (allemand) ou http://netwars-project.com (anglais).

Il n'est hélas jamais possible de protéger complètement un système. D'où l'importance de surveiller efficacement ses réseaux, afin de reconnaître immédiatement les événements et de pouvoir rapidement intervenir pour rétablir l'ordre.

4.13 Les routeurs comme point d'entrée

Comme l'expliquait déjà le dernier rapport semestriel (2/2013), les cybercriminels s'intéressent toujours plus aux *routers*. La période sous revue a également été marquée par diverses attaques visant des routeurs et leurs vulnérabilités:

En début d'année, les fabricants Cisco, Netgear et Linksys ont confirmé la possibilité d'exploiter une faille de sécurité pour lire et manipuler les fichiers de configuration de leurs routeurs.[54] Il était également possible de dérober les mots de passe et certificats des connexions *VPN* de certains appareils. En effet, un service de ces appareils repose sur le *port* 32764. On ignore toutefois si cette lacune de sécurité ne pouvait être exploitée qu'à partir du réseau local ou aussi à partir d'Internet. Il est surprenant de constater que différents produits comportent cette lacune, qui existerait depuis plusieurs années.

Au début de février, on a appris qu'en abusant du routeur de la société «AVM-Fritzbox», des pirates avaient effectué des appels téléphoniques surtaxés. Après que l'on ait pensé dans un premier temps à un vol de mots de passe, on soupçonne qu'il s'agissait d'une faille de sécurité. Presque tous les appareils, avec ou sans *accès à distance*, étaient concernés.[55]

En mars, le fabricant D-Link a prévenu ses utilisateurs d'une faille de sécurité du modem DSL-321B et livré la mise à jour nécessaire.[56] Des pirates pouvaient accéder par Internet à cet appareil, en exploitant ladite faille de sécurité. Lors des attaques constatées, des *entrées de serveur DNS* avaient été modifiées.[57] D'où p. ex. la possibilité pour le pirate de rediriger la victime ayant composé certains noms de sites sur une page définie par lui. Les escrocs recourent à de telles manipulations, par ex., pour détourner des sessions d'e-banking.

Un autre cas de déréglage des paramètres DNS a été rendu public au début de mars. Selon Team Cymru, près de 300 000 routeurs auraient subi des modifications DNS. Il s'agissait principalement de routeurs des sociétés D-Link, TP-Link et Zyxel, mais aussi d'appareils spécialement conçus pour de petits bureaux (SOHO, Small Office, Home Office). Là encore, des failles de sécurité avaient permis les manipulations.

Les routeurs subissent des attaques tantôt automatisées, tantôt manuelles ou encore commises à l'aide de maliciels. On trouve ainsi différents vers se diffusant par infection des routeurs. Par ex., le ver Moon s'attaque aux appareils des fabricants Linksys et Netgear, en tirant parti d'une vulnérabilité existante.

---

54 http://www.heise.de/security/meldung/Mysterioese-Router-Backdoor-Viele-tausend-Router-in-Deutschland-haben-eine-Hintertuer-jetzt-testen-2080913.html (état: le 1er septembre 2014).
http://www.golem.de/news/port-32764-cisco-bestaetigt-backdoor-in-routern-1401-103882.html (état: le 1er septembre 2014).
http://www.golem.de/news/dsl-router-netgear-schliesst-endlich-hintertuer-zu-port-32764-1404-105705.html (état: le 1er septembre 2014).

55 http://www.heise.de/security/meldung/Hack-gegen-AVM-Router-Fritzbox-Luecke-offengelegt-Millionen-Router-in-Gefahr-2136784.html (état: le 1er septembre 2014).

56 http://www.dlink.com/de/de/press-centre/press-releases/2014/march/10/ma_sicherheitspatch-modem-dsl-321b-revision-z1 (état: le 1er septembre 2014).

57 http://www.heise.de/security/meldung/Akute-Angriffsserie-auf-D-Link-Modems-2135158.html (état: le 1er septembre 2014).

Les routeurs sont devenus une cible de choix des cyberpirates, car ils présentent souvent des configurations peu sûres ou des failles de sécurité. D'un autre côté, les utilisateurs font rarement attention à la sécurité des routeurs. Une fois leur appareil raccordé au réseau, aucune activité de maintenance ou actualisation n'est généralement prévue pendant toute sa durée de vie. C'est d'autant plus préoccupant que les mises à jour des anciens modèles ne sont pas automatisées.

MELANI recommande de limiter au maximum les interfaces servant à la maintenance des routeurs. De nombreux appareils permettent d'opérer une restriction à une seule *adresse IP* du réseau interne. Et s'il n'utilise pas des appareils dont son fournisseur d'accès assure la maintenance, l'utilisateur ferait bien de vérifier régulièrement s'il existe des mises à jour pour son routeur et, le cas échéant, de les reprendre. En outre, il importe de désactiver les services superflus.

4.14 La conservation des données viole le droit européen

Par conservation des données, il faut entendre l'enregistrement, par les autorités ou à leur intention, de données sans utilité immédiate se rapportant au trafic des télécommunications. Elles permettront par ex. de découvrir plus tard, en cas de procédure pénale, à qui appartenait l'adresse IP à l'origine d'une infraction. Les ordinateurs reliés au réseau n'ont en effet besoin que d'un numéro impersonnel pour qu'Internet procède à l'adressage correct des informations. La conservation des données renseigne encore sur les appels téléphoniques et les SMS, ainsi que sur la localisation des personnes au moment où elles se sont servies de leur téléphone.

Selon une décision de la Cour de justice de l'Union européenne (CJUE) datant du 8 avril 2014, la loi européenne controversée sur la conservation des données bafoue le droit européen et n'est pas valide. La CJUE a examiné la compatibilité de la directive UE avec les art. 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne. A ses yeux, la conservation des données comporte une ingérence d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel. La Cour estime que ces données sont susceptibles de fournir des indications très précises sur la vie privée des personnes – habitudes de la vie quotidienne, lieux de séjour permanents ou temporaires, déplacements journaliers ou autres, activités exercées, relations sociales et milieux sociaux fréquentés. Au risque de générer, dans l'esprit des citoyens, le sentiment de faire l'objet d'une surveillance constante.

La CJUE reconnaît certes que la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et que son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte. S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige en effet que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire. Or la formulation de la directive européenne aboutirait à une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne, puisqu'elle couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées. La Cour déplore encore que les abonnés ou utilisateurs ne soient pas informés de la conservation et de l'utilisation ultérieure de données les concernant, et qu'aucun critère objectif ne délimite l'accès des autorités nationales aux données.

Il convient de préciser que tout en jugeant disproportionné l'enregistrement des données prévu par la directive, la CEDH n'a pas pour autant conclu à l'impossibilité a priori de toute mesure dans ce sens.

Les Etats membres ont eu des réactions différentes. Or si diverses tentatives ont été faites pour trouver, en matière de conservation des données, un modèle de solution conforme à la Constitution européenne, il n'existe pas à ce jour de réelle alternative. Et comme la Commission ne semble pas vouloir instaurer de nouvelle directive dans ce domaine, certains Etats membres referont sans doute usage ici de leurs compétences réglementaires.

L'arrêt de la CJUE n'aura pas seulement des conséquences pour l'avenir mais exige aussi, depuis son entrée en vigueur le 30 juin 2014, un apurement complet des données collectées jusque-là. L'effacement de ces données confronte les fournisseurs d'accès à de réels défis, en les obligeant à intervenir dans de grandes banques de données.

La décision de la CJUE amènera sans doute à revoir en profondeur la manière d'envisager au niveau européen la conservation des données. Cet arrêt n'aura pas de répercussions directes sur la Suisse. Toutefois, le refus net de la conservation des données pratiquée jusque-là affectera la coopération européenne et internationale en matière de poursuite pénale et ne contribuera guère à la sécurité du droit européen sur le terrain de la lutte contre la criminalité. Il est encore trop tôt pour dire si l'arrêt de la CJUE, avec les modifications qui s'ensuivent dans l'UE, aura une valeur de signal pour les révisions de lois imminentes en Suisse et la volonté de prolonger la durée de stockage des données de six mois à un an.

L'avenir de la conservation des données en Suisse dépendra également de l'évolution du traitement de la plainte déposée par Digitale Gesellschaft. Ce groupement d'acteurs intéressés par la politique en matière d'Internet a demandé par voie de recours au service de surveillance de la correspondance par poste et télécommunication (SCPT) de supprimer la conservation des données en Suisse, en faisant valoir qu'elle violait les droits fondamentaux et qu'elle était disproportionnée. Or le SCPT a rejeté la demande dans sa réponse du 30 juin 2014. Digitale Gesellschaft maintient sa plainte et fera appel au Tribunal administratif fédéral, voire s'il le faut à la Cour européenne des droits de l'homme à Strasbourg.

5 Tendances / Perspectives

5.1 L'ingénierie sociale: une menace multiforme

Les attaques d'ingénierie sociale (social engineering) utilisent la serviabilité, la bonne foi ou l'incertitude des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques. A cet effet, l'attaquant exploite une faille humaine et gagne la confiance de son interlocuteur par divers artifices (usurpation d'identité, audace, intimidation, etc.) pour obtenir ce qu'il souhaite[58].

Cette définition englobe toutes sortes de comportements, et les exemples ne manquent pas – MELANI en a souvent parlé dans ses précédents rapports semestriels. L'ingénierie sociale

[58] On retiendra également la définition de l'ouvrage de référence de Kevin Mitnick «The Art of Deception» (2002): «Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.»

joue un grand rôle dans les cas d'escroquerie. Cela vaut notamment pour les attaques visant des entreprises décrites au chapitre 3.1. Toute entreprise active en Suisse est désormais une cible potentielle pour des attaques utilisant des méthodes d'ingénierie sociale, indépendamment de sa taille ou du secteur d'activité. Il s'agit généralement, par différents moyens, d'obtenir un versement d'argent sans l'aide de moyens technologiques avancés. Il serait cependant faux de limiter le phénomène à ce type d'attaques. Car l'ingénierie sociale a de nombreux visages, et intervient dans le cadre d'attaques bien plus complexes. Quel que soit l'acteur et son but, les attaques les plus complexes ont souvent en commun la méthode utilisée pour la compromission initiale, destinée à «mettre un pied» dans un réseau ciblé. C'est à ce niveau qu'intervient l'ingénierie sociale, puisque les auteurs expédient bien souvent un courriel piégé, parfois extrêmement ciblé, à un employé de la structure visée (*spear phishing*). Ils cherchent donc à tromper l'employé en question, pour l'inciter à révéler des données d'accès, à cliquer sur un lien ou à ouvrir une pièce jointe aboutissant dans les deux cas à une infection de son ordinateur. Cette méthode joue notamment souvent un rôle dans des attaques complexes menées à des fins d'espionnage (Advanced Persistent Threats- APT). Par ex., dans le cas de Careto/The Mask (voir chapitre 4.2), des liens imitant des noms de domaines de journaux connus ont été utilisés pour appâter les victimes. Toujours à des fins d'espionnage, l'opération Newscaster (voir chapitre 4.2) est un autre exemple d'ingénierie sociale sophistiquée, impliquant la création de nombreuses fausses identités.

Les attaques complexes effectuées à des fins financières ont souvent des modus operandi similaires pour la compromission initiale. L'attaque ayant touché la chaîne de magasins Target en fin d'année dernière[59] a ainsi débuté par le vol de données d'accès chez un fournisseur, à l'aide d'un courriel ciblé contenant *une pièce jointe* malicieuse. Dans ce cas, les criminels ont d'abord identifié un fournisseur ayant un accès étendu au réseau de l'entreprise, puis adressé à un de ses employés un courriel piégé sur mesure. Les informations disponibles en ligne ont permis aux attaquants de préparer leur attaque. L'hypothèse de l'utilisation d'ingénierie sociale est également très vraisemblable pour le vol de données ayant affecté en 2014 Ebay (voir chapitre 4.8).

Les outils technologiques à disposition des criminels sont en perpétuelle évolution. De nouvelles failles sont découvertes, de nouveaux protocoles utilisés et des *codes malveillants* toujours plus complexes voient le jour. Dans cet environnement en constante mutation, un angle d'attaque reste le même: l'utilisation par les criminels de failles humaines. Si la manière de les exploiter change, témoignant de l'inventivité et de la capacité d'adaptation des «ingénieurs sociaux», ces derniers activent toujours les mêmes leviers chez leurs cibles: la curiosité, la crédulité, l'appât du gain, la bonne volonté, etc. Ce phénomène est donc à considérer dans son ensemble et non pas uniquement sous le prisme d'un type d'attaque en particulier. Ces méthodes continueront à être massivement utilisées dans le futur, tant qu'elles permettront d'obtenir des informations, de l'argent ou un accès, alors que les moyens technologiques seuls ne le permettent pas, ou alors moins facilement.

La priorité absolue reste de sensibiliser les utilisateurs face à ces menaces. Ces derniers doivent apprendre à développer une attitude générale prudente, sinon méfiante, vis-à-vis de tout interlocuteur les invitant à fournir une information, à suivre un lien ou à ouvrir une pièce jointe. La vérification de la légitimité de chaque demande doit être un réflexe de base de tout utilisateur. Dans les entreprises, les processus internes doivent être clairement définis et respectés en tout temps, à plus forte raison s'ils concernent des mouvements d'argent. Il faut encore empêcher un agresseur d'accéder à l'ensemble d'un réseau par la compromission

[59] Voir MELANI, rapport semestriel 2013/2, chapitre 4.4: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=fr (état: le 1er septembre 2014).

d'un compte, en limitant par principe les accès et privilèges et en les accordant seulement là où c'est indispensable. Enfin, il s'agit de contrôler les informations qu'une structure ou un individu mettent en ligne, sur un site web ou dans un réseau social par ex., dans l'optique d'un possible usage mal intentionné. Car les «ingénieurs sociaux» savent s'en servir pour affiner leurs attaques et augmenter leurs chances de succès.

5.2 Médias et journalistes: des cibles attractives

Les auteurs de cyberattaques cherchent à affecter principalement la disponibilité, l'intégrité et la confidentialité (DIC) de l'information. Les acteurs possédant de grandes quantités d'informations, ou ceux dont la diffusion d'informations est le métier sont en toute logique des cibles intéressantes. Les médias et les journalistes sont doublement concernés: leurs activités les amènent à traiter des informations sensibles et en tant que diffuseur, les informations qu'ils publient ont parfois un impact et un effet multiplicateur majeur. Ainsi, les médias sont bien souvent en première ligne et régulièrement visés par différents types d'attaques. Outre les journalistes professionnels, d'autres diffuseurs («journalistes citoyens», blogueurs) peuvent être pris pour cibles. De nombreuses sources d'information confirment que cette tendance se renforce.

Attaques visant la confidentialité des données

Les professions habituées à traiter un grand nombre d'informations sont des cibles intéressantes. En toute logique, différents acteurs convoitent divers types d'informations en possession des médias et de leurs employés, y compris des acteurs étatiques. En outre, les journalistes sont une cible attractive en raison de leur grande mobilité, qui augmente les angles d'attaques potentiels. Les appareils mobiles (smartphone, ordinateur portable) sont en ce sens des cibles très prisées.

Le mode d'accès à l'information dépend de la nature et des possibilités de l'agresseur et de sa relation à la cible. Dans un premier cas de figure, un acteur étatique peut utiliser un accès privilégié à une infrastructure IT lui permettant d'obtenir l'information. Cet accès peut, comme dans certains Etats totalitaires, permettre une surveillance quasi systématique, liée à une mainmise sur l'infrastructure IT et les systèmes de communication de son propre territoire Dans ce type de régime, les journalistes, en particulier ceux relayant une opinion contraire à celle du pouvoir en place, constituent une cible de choix pour de telles méthodes. Le réseau d'informateurs du journaliste sera dans ce cas également une information ciblée.

Les acteurs ne pouvant pas utiliser ce type d'accès privilégié, mais ayant des objectifs en terme d'acquisition d'informations et les ressources nécessaires vont recourir à des opérations sur les réseaux informatiques («*computer network operation*», CNO). On pense ici à des campagnes de type *APT*, dont il a souvent été question dans les rapports MELANI, ou à des attaques de moindre ampleur pouvant aussi cibler des journalistes. Il peut par ex. s'agir de méthodes de phishing «classique» visant à obtenir des données d'identification ou d'e-mails frauduleux ayant comme finalité l'installation d'un logiciel malveillant sur l'ordinateur d'une cible. Certaines de ces attaques ont fait l'objet d'une attention soutenue du public, suite à des déclarations des victimes ou à la publication de rapport d'entreprises de sécurité. On pense ici aux attaques ayant visé les comptes de messagerie de journalistes de grands médias américains (« New York Times », « Wall Street Journal », « Bloomberg », « Washington Post ») et ayant été suivies par la publication du rapport APT1 par Mandiant. Néanmoins, de nombreuses victimes préfèrent ne pas ébruiter les attaques subies.

Attaques visant la disponibilité ou l'intégrité des données

En tant que diffuseurs d'information, avec souvent un effet multiplicateur important selon leur notoriété ou légitimité, les sites d'informations, de même que les comptes sur des réseaux sociaux des journaux ou agences de presse constituent une cible d'attaque privilégiée. Ils sont principalement visés par des acteurs désireux de faire passer un message religieux ou politique, cherchant à augmenter leur notoriété voire à déstabiliser l'opinion publique à travers des informations erronées. La Syrian Electronic Army (SEA) a fréquemment utilisé ces méthodes au cours des dernières années[60]. Une de ses attaques les plus marquantes reste le piratage du compte Twitter de l'agence Associated Press (AP), puis la publication d'un tweet annonçant qu'une explosion avait eu lieu à la Maison Blanche et que le Président Obama était blessé. Ce message a fait grand bruit, en raison du nombre de suiveurs ayant relayé l'information, et a eu un impact visible sur les marchés américains. Il a été rendu possible par plusieurs vols d'identifiants chez des employés d'AP, lors d'une campagne éclair de phishing. En plus de leurs attaques visant les réseaux sociaux, de tels acteurs n'hésitent pas à défigurer des sites d'informations (*defacement*).

Le développement d'Internet a engendré non seulement une multiplication des diffuseurs d'information (médias classiques, blogs, journalistes citoyens), mais également une diversification des technologies utilisées et des plateformes (réseaux sociaux, sites web, forums, etc.). Cette évolution offre de nouvelles opportunités pour certains acteurs, en multipliant tant les moyens d'accéder à l'information que la possibilité de diffuser un message efficacement. D'où une pression croissante sur l'information et ses diffuseurs. Une vigilance accrue s'impose donc de la part des journalistes et médias. Une analyse du risque spécifique devra prendre en compte différents éléments. Tout d'abord, les méthodes de compromission initiale utilisées pour accéder aux systèmes ou aux comptes des cibles (*spear phishing* et plus globalement *ingénierie sociale*) requièrent une sensibilisation particulière. A ce niveau, la mobilité s'avère un facteur de vulnérabilité supplémentaire, puisqu'elle augmente les surfaces potentielles d'attaque. La question de la surveillance pouvant être menée dans certaines situations par des acteurs bénéficiant d'un accès privilégié à une infrastructure et les solutions permettant d'y faire face sont un autre aspect de l'analyse. A ce sujet, les possibilités existantes de sécuriser les communications doivent rester au centre des préoccupations. Le choix du fournisseur de services Internet, notamment pour les services de messagerie ou de stockage de données, doit également être envisagé sous l'angle des garanties en termes de confidentialité des données.

5.3 Développements d'Internet après l'affaire Snowden

Les premières publications d'Edward Snowden ont mis à mal la sphère privée dans Internet. Les documents publiés donnent à penser que la plupart des flux de données sont surveillés et que les données en possession de sociétés états-uniennes ne sont pas à l'abri des regards de l'Etat américain. L'utilisateur individuel se sent démuni et dépassé par la situation. Il peut certes modifier jusqu'à un certain point son comportement, par ex. en choisissant bien son prestataire TIC ou en adoptant des méthodes de cryptage supplémentaires (Threema, alternative suisse à WhatsApp, a connu un réel engouement ces derniers temps[61]). Or dans bien des cas, il est tributaire de composants matériels ou logiciels standardisés. Dans quelle mesure les leçons tirées de l'affaire Snowden ont-elles vraiment

[60] Voir MELANI, rapport semestriel 2013/2, chapitre 4.8: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=fr (état: le 1er septembre 2014).

[61] http://www.handelsblatt.com/unternehmen/it-medien/instant-messenger-whatsapp-alternative-threema-waechst-rasant/9519942.html (état: le 1er septembre 2014).

déjà influencé l'évolution d'Internet durant la période sous revue? Il est certainement trop tôt pour constater de quelconques changements durables. Mais des initiatives tant étatiques que privées reposent, en partie du moins, sur les récents rebondissements de cette affaire.

Deux tendances sont reconnaissables à l'heure actuelle: d'un côté, des Etats s'engagent pour soustraire certains pans d'Internet à l'influence des Etats-Unis. Ce qui implique de créer de nouveaux réseaux ou d'utiliser des composants de leur propre fabrication. De l'autre, des entreprises américaines cherchent à regagner la confiance du système Internet, en proposant de meilleures techniques de cryptage et d'autres mesures encore.

Interventions en faveur d'une indépendance accrue des réseaux

Angela Merkel a lancé un appel en faveur d'un trafic de données intra-européen. La Commission européenne l'a déjà assurée de son soutien.[62] Dès le début des publications de documents de la NSA, des propositions ont été faites en faveur d'un réseau où le trafic se déroulerait entièrement sur sol européen. L'idée étant que les paquets de données échangés entre les internautes de l'espace Schengen demeurent réellement dans ces frontières. A l'heure actuelle, tout paquet de données recherche la voie la plus favorable et peut donc très bien transiter par les Etats-Unis. Il est trop tôt pour dire dans quelle mesure un tel projet est réalisable. Il faut également garder à l'esprit que des considérations d'ordre économique ou politique peuvent jouer un rôle en pareil cas.[63]

Dès l'automne 2013, la Présidente brésilienne Dilma Rousseff a annoncé que son pays augmenterait le nombre de connexions Internet indépendantes avec d'autres pays.[64]

En Suisse aussi, les informations publiées ont eu de premiers effets. Au début de février 2014, le Conseil fédéral a décidé que les infrastructures critiques, à l'instar des réseaux de communication de l'administration, seraient si possible construites par nos soins et qu'il fallait autant que possible confier les commandes correspondantes à des entreprises suisses. Cette décision concerne surtout les infrastructures TIC de la Confédération, pour lesquelles la confidentialité est essentielle. En font notamment partie la téléphonie fixe et mobile, les ordinateurs et réseaux, ainsi que les installations militaires.[65]

L'ICANN (Internet Corporation for Assigned Names and Numbers) disposera d'ici septembre 2015 d'une structure internationale, avec la participation du secteur privé, des gouvernements et de la société civile. En sa qualité d'organisation à but non lucratif, l'ICANN coordonne l'attribution de noms de domaine et d'adresses uniques dans Internet et relève de la surveillance du Ministère du commerce américain. Le contrat actuel avec le gouvernement américain expirera en 2015. La Russie et la Chine surtout réclamaient vainement depuis longtemps une telle mesure, face au lobbying de l'économie d'Internet. Les Etats-Unis ont beau démentir tout lien avec les publications actuelles d'Edward Snowden, ils consentent désormais à céder le contrôle de la gouvernance d'Internet par l'ICANN.[66]

---

62 http://www.heise.de/newsticker/meldung/Bruessel-unterstuetzt-Merkels-Vorstoss-fuer-Schengen-Netz-2116663.html (état: le 1er septembre 2014).

63 http://www.welt.de/politik/ausland/article126925318/Schengen-Cloud-koennte-zum-Handelskrieg-fuehren.html (état: le 1er septembre 2014).

64 http://www.theguardian.com/world/2013/sep/20/brazil-dilma-rousseff-internet-us-control (état: le 1er septembre 2014).

65 http://www.nzz.ch/wirtschaft/newsticker/chus-geheimdienstaffaere-br-will-mehr-sicherheit-fuer-telekom-und-informatik-1.18236385 (état: le 1er septembre 2014).

66 http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/amerika-gibt-aufsicht-ueber-internet-verwaltung-auf-12849181.html (état: le 1er septembre 2014).

Investissements du secteur privé dans la sécurité informatique et juridique

Au premier semestre 2014, plusieurs fournisseurs de messagerie sont passés simultanément au *chiffrement du transport des données*. Yahoo avait signalé dès novembre 2013 vouloir accroître par étapes la sécurité au profit des utilisateurs. Depuis le début de l'année, toutes les communications s'effectuent par le protocole *HTTPS*. Puis les échanges entre les services Yahoo et les centres de données ont été systématiquement cryptés au début d'avril. Une nouvelle version cryptée de Yahoo Messenger est également annoncée.[67] De même, les fournisseurs de messagerie allemands Freenet, GMX, Web.de ainsi que deutsche Telekom n'autorisent depuis la fin d'avril que les communications cryptées entre les utilisateurs et leurs centres de données.[68]

Le chiffrement des données pendant l'acheminement, dont il est question ici, ne se réfère qu'aux échanges entre l'utilisateur et son fournisseur de messagerie. Il en va différemment du transport de données entre deux prestataires différents. A supposer que celui du destinataire refuse les données cryptées, les messages restent transmis en clair. Google a publié dans ce contexte un premier rapport sur la transparence et tient une liste des fournisseurs de messagerie n'acceptant aucun chiffrement. Selon ce rapport, 75% des messages expédiés via Gmail sont cryptés, contre 57% seulement des messages reçus.[69] Ces deux valeurs ont progressé au semestre écoulé. Le trafic de données cryptées est de façon générale en hausse ces derniers mois, selon une étude parue en mai 2014. Il a doublé en un an, et même triplé en Europe.[70]

Un cas actuel impliquant Microsoft pourrait avoir un impact majeur sur la conservation des données, notamment les services de stockage dans le nuage. Il s'agit de savoir si les données de clients d'entreprises américaines sauvegardées en Europe doivent aussi être livrées aux Etats-Unis. Le monde a les yeux rivés sur ce litige, en raison des publications liées à l'affaire Snowden. Concrètement, un tribunal de district américain exige de Microsoft la publication de courriels et d'autres données d'un client sauvegardées dans un centre de données de Dublin. Microsoft objecte que la justice américaine n'a pas le droit de lui réclamer des données enregistrées en dehors des Etats-Unis. Le jugement aura une forte charge symbolique: au-delà de la confiance accordée à long terme par la clientèle aux entreprises américaines, il a pour enjeu la juridiction des données stockées dans le nuage.

Les Etats-Unis eux-mêmes donnent l'impression de vouloir davantage réglementer l'acquisition de données par leurs services de renseignement. Ainsi, le Président Obama a ordonné de revoir la pratique de collecte des données de la NSA. Par ex., les Etats-Unis n'épieraient plus la communication des chefs d'État et de gouvernement de leurs «amis et alliés» à l'étranger, tant qu'aucune raison impérieuse de sécurité nationale ne l'exige. De même, les citoyens non américains devraient bénéficier à l'avenir d'une partie des prescriptions protectrices qui, jusqu'ici, ne s'appliquaient qu'aux citoyens américains.[71] Il est vrai que ces affirmations sont encore peu concrètes et difficiles à interpréter.

---

67 http://yahoo.tumblr.com/post/81529518520/status-update-encryption-at-yahoo (état: le 1er septembre 2014).

68 http://www.computerbild.de/artikel/cb-Aktuell-Sicherheit-E-Mail-made-in-Germany-Telekom-GMX-Web.de-Freenet-SSL-8593819.html (état: le 1er septembre 2014).

69 http://www.google.com/transparencyreport/saferemail/ (état: le 1er septembre 2014).

70 https://www.sandvine.com/trends/global-internet-phenomena/ (état: le 1er septembre 2014).

71 http://www.nzz.ch/aktuell/startseite/obama-setzt-geheimdiensten-engere-grenzen-1.18223803 (état: le 1er septembre 2014).

5.4 Authentification à deux facteurs pour tous les services

Les mots de passe ou plus généralement les authentifications reposant sur un seul facteur n'offrent plus une sécurité suffisante, au vu des menaces actuelles. Pour cette raison, MELANI recommande de toujours prévoir un second facteur d'authentification. De façon générale, on trouve les facteurs suivants:

- ce que sait un individu: «j'atteste de mon identité par une information dont j'ai connaissance», par ex. mot de passe;
- ce qu'il possède: «je présente un document en ma possession»; par ex. Smartcard;
- ce qu'il est: «une caractéristique physique ou biométrique confirme mon identité», par ex. empreinte digitale.

En cas de combinaison de deux de ces facteurs, on parle d'authentification à deux facteurs. Il s'agit très souvent d'un élément que l'on connaît et d'un élément que l'on détient. C'est la norme depuis quelque temps dans l'e-banking, dont beaucoup d'applications de grands fournisseurs Internet s'inspirent peu à peu. Bien souvent, la technique utilisée consiste à envoyer à un numéro de téléphone défini d'avance un *SMS* comportant un code. Une partie des services ne prévoient cette étape qu'à la première connexion, l'appareil du visiteur restant ensuite enregistré comme digne de confiance. D'autres privilégient un mot de passe unique (*one time password, OTP*) et font appel à une App, qui génère de manière aléatoire des chiffres valables un court laps de temps (par ex. Google Authenticator).

Quelques fournisseurs de services Internet acceptent une authentification à deux facteurs, dont notamment:

- applications Google (gmail, google+, etc.)
- Outlook.com
- Dropbox
- …..

Une telle forme d'authentification est vivement recommandée pour l'administration des systèmes de gestion de contenu (*content management system, CMS*) et, plus généralement, pour toute interface d'administration accessible via Internet. Car une perte de mot de passe à ce niveau est susceptible de causer de sérieux dommages, à des tiers également. La plupart des CMS supportent une authentification à deux facteurs, soit directement (par ex. Joomla), soit par le biais de plugiciels (par ex. plugiciel créé par le Danois Henrik Schack pour Wordpress)[72]. De même, le logiciel Google Authenticator ou une procédure à clé privée/clé publique sont pratiques pour renforcer le protocole *SSH* sous Linux, servant au transfert de données cryptées et souvent hélas victime d'attaques par *force brute*.

Il serait judicieux d'envisager comme procédure d'authentification, pour tout accès particulièrement délicat ou dans le cas des grandes entreprises, des technologies comme les certificats enregistrés sur carte à puce, ou alors des procédures spécifiques à mot de passe unique. En effet, les smartphones sont eux-mêmes reliés à Internet et donc eux aussi exposés aux cyberattaques.

[72] https://wordpress.org/plugins/google-authenticator/ (état: septembre 2014).

5.5 Objets politiques

Objet	N°	Titre	Déposé par	Date de dépôt	Conseil	Dépt	Etat des délibérations et lien
Ip	14.3019	Marchés publics. Projets TIC	Noser Ruedi / Groupe libéral-radical	03.03.2014	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143019
Qst.	14.5063	Système d'écoutes téléphoniques ISS	Glättli Balthasar	05.03.2014	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20145063
Iv ca	14.305	Appels anonymes à manifester	Canton de Berne	19.03.2014			http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20140305
Ip	14.3204	Consensus trouvé par le groupe de travail Agur 12. Suite des opérations	Gutzwiller Felix	20.03.2014	CE	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143204
Po	14.3193	Améliorer l'efficacité des enquêtes policières dans les réseaux sociaux	Vogler Karl	20.03.2014	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143193
Mo	14.3288	Faire de l'usurpation d'identité une infraction pénale en tant que telle	Comte Raphaël	21.03.2014	CE	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143288
Ip	14.3240	Gouvernance globale d'Internet. Une opportunité sans précédent pour la Genève internationale	Sommaruga Carlo	21.03.2014	CN	DFAE	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143240
Mo	14.3236	Vitesse d'accès à Internet proposée dans le cadre du service universel. Passer au haut débit	Candinas Martin	21.03.2014	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143236
Mo	14.3011	Réduction des coûts grâce à une procédure électronique de déclaration en douane	Commission de l'économie et des redevances CN	24.03.2014	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143011
Mo	14.3293	Redevance sur les supports vierges	Commission de l'économie et des redevances CN	08.04.2014	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143293
Ip	14.3379	Sécuriser les sites Internet suisses par des entreprises suisses	Derder Fathi	08.05.2014	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143379
Ip	14.3351	Médecine personnalisée. Créer une banque nationale de données biologiques au lieu de laisser proliférer des banques de données privées étrangères	Schmid-Federer Barbara	08.05.2014	CN	DFI	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143351
Ip	14.3341	Swisscom. Passage planifié de la téléphonie analogique à la téléphonie par Internet pour tous les raccordements du réseau fixe	Glättli Balthasar	08.05.2014	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143341
Ip	14.3409	Droit minimum d'accès numérique	Recordon Luc	05.06.2014	CE	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143409
Mo	14.3423	Positionner la Suisse en tant que plate-forme internationale en matière de gouvernance Internet	Noser Ruedi / Groupe libéral-radical	10.06.2014	CN	DFAE	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143423
Po	14.3532	Administration fédérale et logiciels ouverts. Etat des lieux et perspectives	Graf-Lischer Edith	19.06.2014	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143532
Po	14.3658	Rapport sur les conséquences et les mesures à prendre face aux plate-formes Internet d'échange de services, particulièrement dans le domaine du logement et du transport	Sommaruga Carlo	20.06.2014	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143658
Ip	14.3630	Prescriptions en matière de publicité. Reprise automatique du droit européen	Müller Thomas	20.06.2014	CN	DFAE	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143630

6 Glossaire

Access control list (ACL)	Une liste de contrôle d’accès (access control list, ACL) contient des instructions permettant aux systèmes d’exploitation ou aux programmes de limiter l’accès à certaines données ou fonctions.
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Advanced Persistent Threat (APT)	Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L’agresseur est disposé à investir beaucoup de temps, d’argent et de savoir-faire dans ce genre d’attaque ciblée et furtive, et dispose d’importantes ressources.
Attaque DoS	Attaque par déni de service (denial of service). Vise à rendre impossible l’accès à des ressources, ou du moins à le restreindre fortement aux utilisateurs.
Automate programmable industriel (API)	Un automate programmable industriel (en angl. programmable logic controller, PLC), est un dispositif électronique programmable destiné à la commande de processus industriels par un traitement séquentiel. Depuis plusieurs années, de tels dispositifs remplacent dans la plupart des domaines le pilotage par des réseaux logiques câblés.
Backup	Un backup (sauvegarde des données) désigne la duplication de données, dont la restauration permettra de retrouver les données perdues.
Barre d’adresse	En inscrivant l’URL dans la barre d’adresse du navigateur, l’internaute obtient la page Internet souhaitée.
Bit/Byte	Le byte est la plus petite unité de mesure de la quantité de données stockées ou transmises. Un byte est composé de 8 bits.
Cache	La mémoire cache (mémoire tampon) sert à stocker les données auxquels un système fait le plus souvent appel, afin de réduire les temps d’attente du microprocesseur.
Certificat	Un certificat numérique est un enregistrement de données numériques qui confirme des propriétés déterminées de personnes ou d’objets et permet d’en contrôler l’authenticité et l’intégrité par des méthodes cryptographiques. Le certificat numérique contient notamment les données nécessaires à son contrôle.

Certificate Authority (autorité de certification)	Une autorité de certification est une organisation délivrant des certificats numériques. 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.
Chat	Le «chat» désigne en informatique la conversation entre plusieurs personnes connectées en même temps à un réseau, qui échangent des messages s'affichant en temps réel sur leur écran.
Cheval de Troie	Les chevaux de Troie sont des programmes qui, de manière larvée, exécutent des actions préjudiciables tout en se présentant à l'utilisateur comme des applications ou des fichiers utiles.
Chiffrement du transport	Cryptage des données lors de l'acheminement entre deux serveurs, ou entre l'utilisateur et son fournisseur de messagerie.
Clé privée / clé publique	La cryptographie à clé publique est une méthode de chiffrement asymétrique. Elle repose sur l'utilisation d'une clé publique (diffusée) et d'une clé privée (gardée secrète) qui permettent l'une de coder le message, l'autre de le décoder.
Cloud computing	L'informatique dans les nuages (cloud computing, cloud IT) est une notion propre aux technologies de l'information. Les TIC ne sont plus gérées et mises à disposition par l'utilisateur, mais acquises d'un ou plusieurs prestataires. Les applications et les données ne se trouvent plus sur l'ordinateur local ou au centre de calcul de l'entreprise, mais dans le nuage (cloud). L'accès à ces systèmes à distance s'effectue par un réseau.
Code Review	La revue de code désigne l'examen systématique du code source d'un programme, afin d'en détecter et d'en corriger les erreurs.
Codec vidéo	Un codec vidéo désigne une paire d'algorithmes capables de convertir des signaux vidéo en signaux numériques ou l'inverse, soit de compresser ou décompresser des données.
Computer Network Operation (CNO)	Les opérations dans les réseaux informatiques constituent une méthode de guerre nouvelle, visant à obtenir l'infodominance sur l'adversaire.
Content Management System (CMS)	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).
Defacement	Défiguration de sites Web.
Diffie-Hellmann	Le procédé d'échange des clés de Diffie et Hellman autorise deux correspondants à convenir d'une clé de chiffrement (clé secrète).
DNS	Système de noms de domaine (Domain Name System). Le DNS rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP les utilisateurs composent un nom (p. ex. www.melani.admin.ch).
DNS Amplification/Reflection Attack	Attaque par déni de service (attaque Denial of Service, DoS), utilisant des serveurs DNS publics comme amplificateurs.
Exploit Code	(Exploit) Programme, script ou ligne de code utilisant les failles de systèmes informatiques.
Fingerprint	En informatique, les empreintes digitales (fingerprint) reposent souvent sur des fonctions de hachage servant à identifier un fichier.
Force brute	La méthode «brute force» consiste à tester, une à une, toutes les combinaisons possibles pour découvrir le mot de passe ou la clé.
Hardware Security Module (HSM)	Un module de sécurité matériel (hardware security module, HSM) est un dispositif connecté à un ordinateur hôte, dont l'objet est de créer un environnement sécurisé résistant aux intrusions en assurant les contrôles d'authentification et les processus cryptographiques.
HTTP Strict Transport Security	HTTP Strict Transport Security (HSTS) est un mécanisme permettant à un serveur Web de déclarer à un agent utilisateur qu'il doit interagir avec lui par une connexion sécurisée.
HTTP-Request	HyperText Transfer Protocol. Protocole de transfert d'hypertexte. Norme pour la transmission de documents HTML (par exemple sur Internet).
HTTPS	Protocole pour une transmission sûre, c'est-à-dire chiffrée, de documents HTML dans un réseau (p.ex. Internet).
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.
Ingress Filtering	Un filtrage d'entrée protège les réseaux, en supprimant le trafic entrant indésirable.
Internet Service Provider (ISP)	Internet Service Provider. Fournisseur de services Internet. Sociétés offrant, généralement contre rémunération, différentes prestations pour l'utilisation ou l'exploitation de services Internet.
Least Privilege	Principe consistant en l'octroi de droits d'accès restreints au système et à ses ressources, afin que l'utilisateur ne puisse accomplir que les tâches nécessaires à l'exercice de ses fonctions.
Malicious Code	Programme malveillant (maliciel). Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie).
Métadonnées	Les métadonnées ou métainformations sont des données renseignant sur la nature de certaines autres données.
NTP	Protocole permettant de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure (Network Time Protocol, NTP).
OPC Server	OLE for Process Control (OPC) est une technique destinée à l'interopérabilité des systèmes industriels, permettant d'accéder aux données de terrain de dispositifs d'usine.
OpenSSL	OpenSSL est un logiciel libre de chiffrement basé sur la bibliothèque SSLeay, qui implémente le protocole TSL (Transport Layer Security) et son prédécesseur SSL (Secure Sockets Layer).
OTP	Un mot de passe unique (one-time password, OTC) n'est valable que pour une session ou une transaction. Un OTP déjà utilisé n'est plus valide.
Patch	Rustine. Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d'erreurs et remédie ainsi p.ex. à une lacune de sécurité.
Peer To Peer	Peer to Peer Architecture de réseau où tous les postes de travail ont les mêmes possibilités de communication (à l'inverse des réseaux client/serveur). P2P sert fréquemment aux

	échanges de données.
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 falsifiées.
Pilote (informatique)	Programme destiné à permettre à l'ordinateur de communiquer avec un périphérique.
PingBack	Un PingBack est une fonction qui permet à un site d'exiger une notification chaque fois que d'autres sites postent un lien vers lui.
Port	Elément d'adresse assurant l'attribution des connexions TCP et UDP et des paquets de données aux clients et serveurs par les systèmes d'exploitation
Porte dérobée	Une porte dérobée (en anglais: backdoor) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un pirate d'accéder secrètement à un programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.
Ransomware	Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate crypte ou efface des données et ne fournit la clé nécessaire pour les sauver qu'après le versement d'une rançon.
Remote Administration Tool	Un RAT (Remote Administration Tool, outil de télémaintenance) est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur.
Remote Procedure Call (RPC)	Méthode de communication standard utilisée pour établir des liaisons à distance entre des systèmes informatiques en réseau, au moyen de protocoles spécialisés.
Réseau de zombies	Réseau d'ordinateurs infectés par des programmes malveillants (bots). Un pirate (le propriétaire du réseau de zombies) les contrôle complètement à distance. Un réseau de zombies peut compter de quelques centaines à des millions d'ordinateurs compromis.
Router	Dispositif assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un router s'utilise par exemple dans un

	réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
Serveur de commande et contrôle	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 de commande et contrôle (C&C).
Service de transmission en continu (streaming)	Principe utilisé pour l'envoi en continu et la lecture de flux audio ou vidéo par le réseau.
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.).
SMS	Short Message Service. Service de messages courts. Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile.
SNMP	SNMP (Simple Network Management Protocol) est un protocole de communication permettant aux administrateurs réseau de gérer et superviser les équipements (par ex. routeur, serveur, commutateur, imprimante, ordinateur, etc.).
Social Engineering	Les attaques d'ingénierie sociale utilisent la serviabilité, la bonne foi ou l'incertitude des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.
Spearphishing	Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
SSH FileTransfer Protocol	Secure Shell Protocole permettant grâce au chiffrement des données d'ouvrir une session (login) sécurisée sur un système informatique accessible par l'intermédiaire d'un réseau (p.ex. Internet).
SSL	Secure Sockets Layer Protocole permettant de communiquer en toute sécurité sur Internet. SSL s'emploie aujourd'hui p. ex. pour les transactions financières en ligne.
Tunneling	La tunnellisation (tunneling) est l'encapsulation de données d'un protocole réseau dans un autre afin qu'elles circulent sans être épiées ou bloquées.
URL	Uniform Resource Locator. Adresse d'un document Web composée du nom du protocole, du nom du

	serveur et du nom de fichier avec son chemin d'accès (exemple : http://www.melani.admin.ch/test.html).
User Datagram Protocol (UDP)	UDP est un protocole réseau simple, sans connexion, faisant par-tie de la couche de transport de la famille de protocoles Internet. UDP a pour tâche de délivrer à l?application correcte les données échangées par Internet.
Virus	Programme informatique d'autoréplication, doté de fonctions nuisibles, qui s'installe en annexe d'un programme ou fichier hôte pour se propager.
VPN	Virtual Private Network Réseau privé virtuel. Permet, par le chiffrement du trafic de données, d'établir une communication sécurisée entre ordinateurs à travers un réseau public (p.ex. Internet).
Watering Hole attack	Attaque du trou d'eau, attaque ciblée par un maliciel n'infectant que des sites supposés être visités par un groupe spécifique d'utilisateurs.
Webmail	Une messagerie web (webmail) est une interface web rendant possible l'émission, la consultation et la manipulation de courriers électroniques directement sur le Web depuis un navigateur.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.