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 2011/II (juillet à décembre)

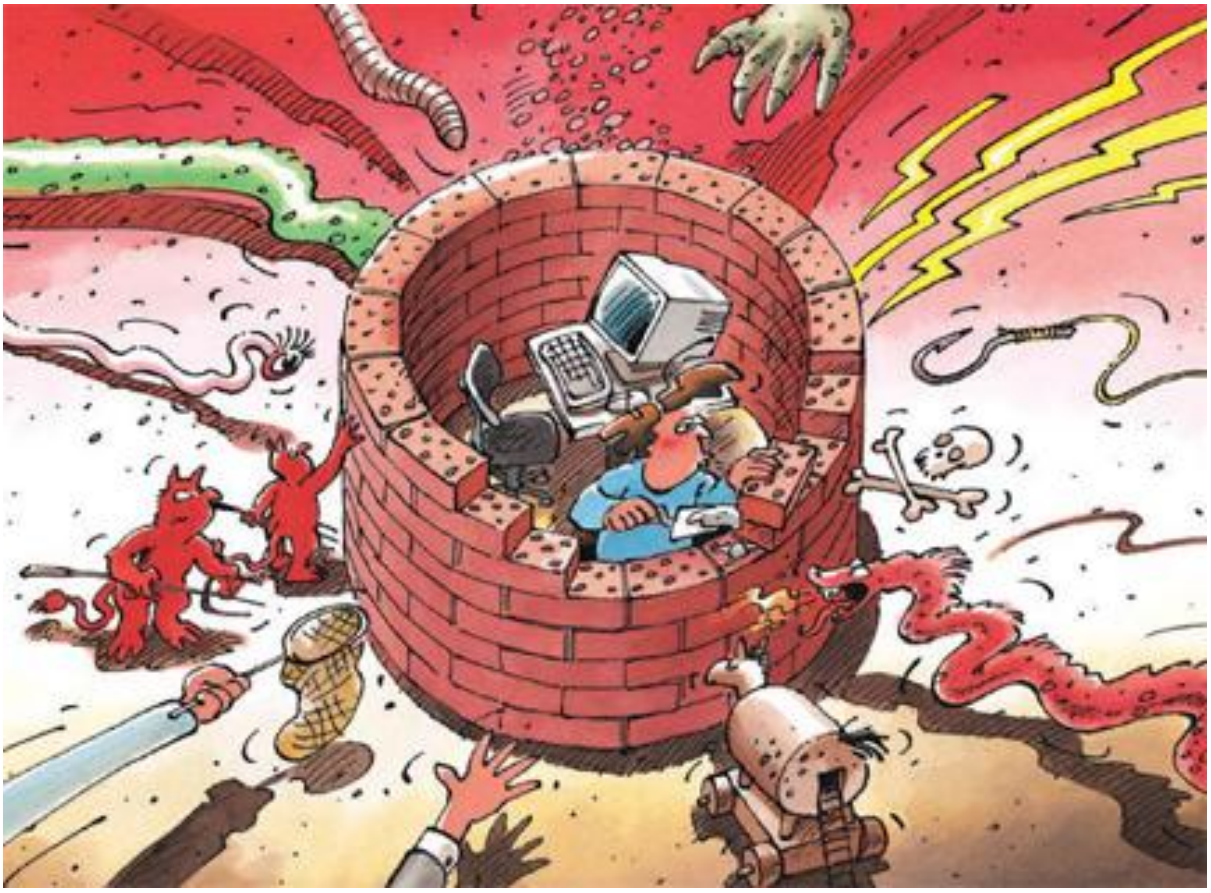


Table des matières

1 Temps forts de l'édition 2011/II

- **Attaques contre des fournisseurs de services de certification et effets**

  Une attaque lancée contre DigiNotar, organisme de certification néerlandais, a permis aux escrocs d'émettre abusivement plus de 530 certificats, notamment pour le domaine windowsupdate.com, qui héberge la fonction de mise à jour de tous les produits Windows de Microsoft, et pour différents domaines de Google.

  ► Situation sur le plan international: chapitre 4.1
  ► Tendances / Perspectives: chapitre 5.5

- **Cyberactivisme**

  L'intérêt des médias pour Anonymous s'est ravivé ces derniers mois, à la suite de diverses opérations menées dans le cyberespace. Qui se cache derrière Anonymous? Selon de nombreux témoignages, Anonymous ne serait pas une organisation à proprement parler, mais un mode de vie. Aucune forme spéciale de soutien n'est exigée, chaque activiste faisant, dans la mesure de ses moyens, ce qui lui paraît juste. D'où parfois des actions auxquelles une bonne partie du mouvement n'adhère pas et qui aboutissent à des déclarations contradictoires.

  ► Situation sur le plan international: chapitre 4.3
  ► Tendances / Perspectives: chapitre 5.2

- **«Bonne» et «mauvaise» surveillance d'Internet**

  L'analyse faite par le Chaos Computer Club du cheval de Troie appartenant aux autorités de poursuite pénale allemandes a soulevé – en Allemagne comme en Suisse – des débats animés sur son utilisation possible. En outre, WikiLeaks a commencé à publier, le 1er décembre 2011, de nombreux documents censés prouver que des entreprises de sécurité privées vendent des solutions TIC à des Etats autoritaires qui bafouent les droits de l'homme. Le vieux débat relancé à cette occasion met en lumière un réel problème lié à Internet, à la société en réseau et aux TIC. L'apparition de possibilités sans cesse nouvelles de communiquer, d'échanger des informations ainsi que de consulter des données en tout temps et de partout, n'est pas sans conséquences: les mesures prises à des fins de localisation et d'acquisition de l'information, et plus généralement le travail des autorités nationales chargées de la sécurité, sont toujours plus complexes.

  ► Situation sur le plan international: chapitre 4.7, 4.8
  ► Tendances / Perspectives: chapitre 5.3

- **Hameçonnage, escroqueries et ransomware en hausse**

  Un nouveau phénomène est apparu en Suisse durant l'été 2011, avec des appels téléphoniques d'escrocs se faisant passer pour des collaborateurs du service à la clientèle de Microsoft, afin d'accéder à l'ordinateur des victimes. L'hameçonnage a également redoublé ces six derniers mois, aux dépens surtout des fournisseurs de messagerie et des sociétés de cartes de crédit. Les criminels recourent à de nouvelles méthodes pour déjouer la désactivation des sites d'hameçonnage, afin de pouvoir sévir le plus longtemps possible. Au début de novembre, des maliciels émanant soi-disant du Département fédéral de justice et police (DFJP) ont été expédiés comme moyen de chantage (ransomware).

  ► Situation en Suisse: chapitre 3.1, 3.2, 3.3, 3.4, 3.5

2 Introduction

Le quatorzième rapport semestriel (juillet à décembre 2011) 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 derniers mois de l’année 2011. La situation nationale est analysée au chapitre 3 et la situation internationale au chapitre 4.

Le **chapitre 5** livre, sur des thèmes actuels, des analyses détaillées avec les tendances.

3 Situation en Suisse de l'infrastructure TIC

3.1 Appels de prétendus employés du service à la clientèle de Microsoft

Ces derniers temps, les appels téléphoniques d'escrocs se faisant passer pour des employés de Microsoft ou d'autres entreprises de support informatique se multiplient au niveau mondial, en Suisse aussi. Leurs auteurs parlent généralement anglais et prétendent venir des Etats-Unis, de Grande-Bretagne ou d'Australie. Ils signalent fréquemment des messages d'erreur qui leur seraient parvenus des ordinateurs de l'entreprise ou du particulier approchés. Les personnes appelées reçoivent p. ex. des instructions pour appeler le logiciel *Event-Viewer*[1], permettant de visualiser tous les événements survenus et les activités déployées par l'ordinateur. Or il faut savoir que même un système fonctionnant de manière irréprochable génère parfois des messages d'erreur. Selon l'âge et la configuration de l'ordinateur, la liste des messages d'erreur publiés dans le journal des événements peut être très longue, sans que le système présente le moindre problème. Les auteurs de tels appels de «support» recourent typiquement à ce programme afin de planter un décor plausible et d'effrayer leurs victimes. Ils visent ainsi à convaincre la personne contactée de leur livrer accès à leur ordinateur, en téléchargeant un programme d'accès à distance. Le cas échéant, l'escroc aura les mêmes possibilités de manipuler l'ordinateur qu'en étant directement assis devant lui (duplication/modification/suppression de données, installation de programmes, mise en place d'une «*porte dérobée*» pour s'introduire à volonté dans le système, etc.).

Parfois, les auteurs de ces appels proposent également de conclure un abonnement de support ou une garantie, et exigent à cet effet les données d'une carte de crédit ou une autre forme de paiement.

Les escrocs repèrent visiblement leurs victimes à l'aide des répertoires accessibles au public, comme le registre suisse du commerce ou les annuaires téléphoniques publics.

Il convient de rappeler que Microsoft n'appelle jamais spontanément pour résoudre des problèmes informatiques. Des précisions à ce sujet figurent sur le *blog* du responsable de la sécurité de Microsoft Suisse.[2]

Au cas où vous auriez laissé l'auteur d'un tel appel accéder à votre ordinateur, il est recommandé de le faire examiner et éventuellement nettoyer par un spécialiste. Il n'est pas pour autant garanti qu'un *maliciel* soit trouvé, ou les manipulations effectuées découvertes.

La méthode la plus sûre consiste à effacer entièrement le disque dur de l'ordinateur et à réinstaller le système d'exploitation. D'où l'importance de procéder régulièrement à la *sauvegarde* de toutes les données importantes sur un support externe, afin qu'elles ne soient pas perdues le jour où l'ordinateur rencontrera un problème.

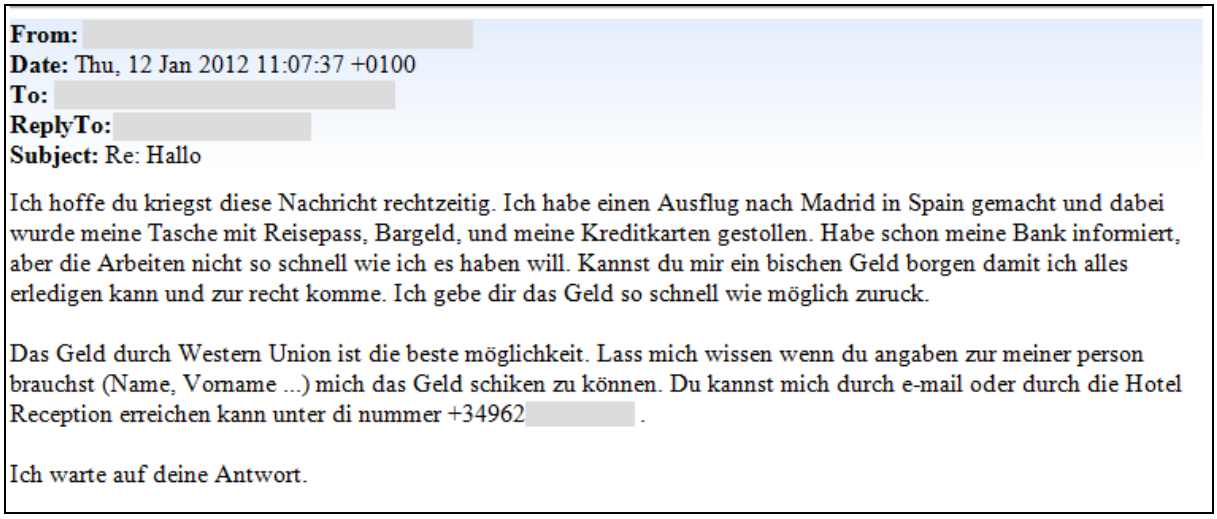
---

1 En français Observateur d'événements, programme du système Windows.

2 http://www.retohaeni.net/2011/07/microsoft-does-not-call-you/ (état: 23 février 2012).

3.2 Toujours plus de comptes de messagerie piratés

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI est fréquemment prévenue d'intrusions survenues dans des comptes de messagerie. Les escrocs modifient typiquement le mot de passe et d'autres données personnelles du compte (adresse alternative, numéro de Natel, etc.), afin que le propriétaire légitime n'y ait plus accès. Ils écrivent ensuite à tous les contacts du carnet d'adresses, ou à certains d'entre eux. Ces courriels sont généralement de faux appels au secours, expliquant que la personne se trouve bloquée à l'étranger, après s'être fait voler son argent et son passeport. Le destinataire est ensuite prié d'effectuer un versement d'argent.



From:
Date: Thu, 12 Jan 2012 11:07:37 +0100
To:
ReplyTo:
Subject: Re: Hallo

Ich hoffe du kriegst diese Nachricht rechtzeitig. Ich habe einen Ausflug nach Madrid in Spain gemacht und dabei wurde meine Tasche mit Reisepass, Bargeld, und meine Kreditkarten gestollen. Habe schon meine Bank informiert, aber die Arbeiten nicht so schnell wie ich es haben will. Kannst du mir ein bischen Geld borgen damit ich alles erledigen kann und zur recht komme. Ich gebe dir das Geld so schnell wie möglich zuruck.

Das Geld durch Western Union ist die beste möglichkeit. Lass mich wissen wenn du angaben zur meiner person brauchst (Name, Vorname ...) mich das Geld schiken zu können. Du kannst mich durch e-mail oder durch die Hotel Reception erreichen kann unter di nummer +34962 .

Ich warte auf deine Antwort.

Figure 1: Exemple de courriel envoyé à partir d'un compte piraté.

Outre les désagréments subis par le destinataire de tels courriels, le propriétaire de l'adresse électronique est lui aussi exposé à bien des déboires, car il n'a plus le contrôle de son compte et ne peut plus accéder à ses messages et à ses contacts. Cela peut avoir des effets dévastateurs et créer des situations gênantes dans le monde réel, si les données et les contacts n'ont fait l'objet d'aucune sauvegarde externe (*backup*) et si tous les contacts professionnels passaient par cette adresse électronique.

L'accès au compte de messagerie d'une tierce personne permet naturellement de commettre encore bien d'autres escroqueries. De nombreux services Internet sont accessibles par simple introduction du nom d'utilisateur et du mot de passe. En cas d'oubli ou perte de son mot de passe, le client peut en générer un nouveau en cliquant sur le lien «Mot de passe oublié». Il reçoit alors par courriel son nouveau mot de passe. Si un pirate parvient à accéder au compte de messagerie, il pourra aisément utiliser ce service afin d'accéder aux diverses prestations de service utilisées par la victime et d'en abuser à son profit.

Les conseils qui suivent permettent de limiter les dommages en cas de piratage de compte.

1. Faire une sauvegarde (*backup*) des contacts, afin de pouvoir se rabattre sur une adresse électronique alternative en cas d'incident. Cette précaution permet de prévenir très rapidement les contacts du risque de recevoir un courriel d'arnaque.
2. Choisir soigneusement son fournisseur de messagerie, a fortiori si la messagerie est utilisée dans un but professionnel.
3. En cas d'incident, chercher immédiatement à reprendre le contrôle du compte. Dans de rares cas, l'adresse alternative n'a pas été modifiée: le cas échéant, il est possible d'envoyer un mot de passe de remplacement à cette adresse électronique. Mais si l'adresse alternative a été modifiée, il faut lancer un processus de récupération

(*recovery*). La plupart des fournisseurs de messagerie mettent à disposition un formulaire spécial. Le tableau qui suit, qui n'est pas exhaustif, indique ce que proposent les principaux fournisseurs de messagerie:

Google	www.google.com/accounts/recovery/
Hotmail/ Live	https://account.live.com/resetpassword.aspx
Yahoo	https://edit.europe.yahoo.com/forgotroot
GMX	www.gmx.com/forgotPassword.html

La meilleure solution consiste toutefois à prévenir toute intrusion dans son compte. Veuillez lire à ce sujet nos recommandations pour le choix d'un mot de passe.[3] En outre, il faut garder à l'esprit qu'aucun prestataire sérieux n'invite par courriel ses clients à lui indiquer leur mot de passe. Ne cliquez par conséquent jamais sur un lien figurant dans un courriel pour accéder au site d'un fournisseur d'accès, d'un prestataire de services financiers, d'une société émettrice de cartes de crédit, etc.. Voir aussi nos informations concernant l'hameçonnage (*phishing*)[4]. Il faut toujours être sur ses gardes quand un site Web exige un mot de passe (voir chap. 3.3).

La prudence ne s'impose plus seulement quand l'expéditeur du courriel est inconnu, mais même lorsqu'il s'agit d'une personne connue. En cas d'événement insolite – surtout si une demande d'argent est formulée –, MELANI recommande d'essayer de joindre la personne par téléphone, de poser des questions dont elle seule connaît la réponse, de vérifier son identité ou de discuter avec des connaissances communes de la plausibilité de son récit.

En outre, il faut se garder d'ouvrir machinalement les annexes ou de suivre les liens de courriels dont l'expéditeur est connu – a fortiori si le courriel semble impersonnel et si son contenu n'est pas caractéristique des messages habituels de cet expéditeur.

3.3 Carte de vœux conçue pour dérober les mots de passe

Il est courant d'envoyer et de recevoir des cartes postales électroniques à l'époque des fêtes. Or toutes les cartes postales électroniques expédiées ne sont pas sérieuses. Deux cas particulièrement raffinés d'escroquerie, visant expressément des victimes suisses, ont été découverts pendant les fêtes de Noël.

Dans le premier cas, des courriels ont été envoyés au nom de Swisspostcard[5]. Ils indiquaient un expéditeur connu du destinataire, afin de l'inciter à cliquer sur un lien. Tout était fait pour lui donner l'impression d'avoir reçu une carte de Noël électronique, qu'il pourrait télécharger sur le site unsereweihnachtskarten.com.

[3] http://www.melani.admin.ch/themen/00166/00172/01005/index.html?lang=fr (état: 23 février 2012).

[4] http://www.melani.admin.ch/themen/00103/00203/index.html?lang=fr (état: 23 février 2012).

[5] SwissPostCard (Service de la Poste Suisse) permet de créer des cartes postales électroniques. Elles sont ensuite imprimées par la Poste, qui les achemine à bon port.

```
-------- Original-Nachricht --------
Datum: Mon, 26 Dec 2011 07:02:29 -0800
Von:
An:
Betreff: Du hast eine Weihnachtskarte erhalten!

Lieber,

Du hast eine Weihnachtskarte von "einem anonymen Absender" erhalten.

Was kannst Du tun?
Gehe zu: http://www.unsereweihnachtskarten.com?e=

Nachdem Du die Weihnachtskarte empfangen und gelesen hast, kannst du darauf antworten. Wenn du
eine Weihnachtskarte versenden möchtest, gehe zur genannten Webseite.


Viel Spaß,

Julia Emmrich
Unsereweihnachtskarten.com

Swiss Post International
swisspostcard.ch
```

Figure 2: Exemple de courriel d'hameçonnage prétendant que le destinataire a reçu une carte de Noël.

Un clic sur le lien ouvrait en arrière-plan le site original de Swisspostcard. Le premier plan était toutefois occupé par un formulaire, où la victime devait indiquer son nom d'utilisateur et le mot de passe de son compte de messagerie pour pouvoir télécharger sa carte de Noël. Les données d'accès saisies parvenaient directement aux escrocs, qui s'empressaient d'accéder audit compte. Tous les contacts de son carnet d'adresses recevaient par la suite un courriel d'*hameçonnage* du même type, afin de créer un effet boule de neige.

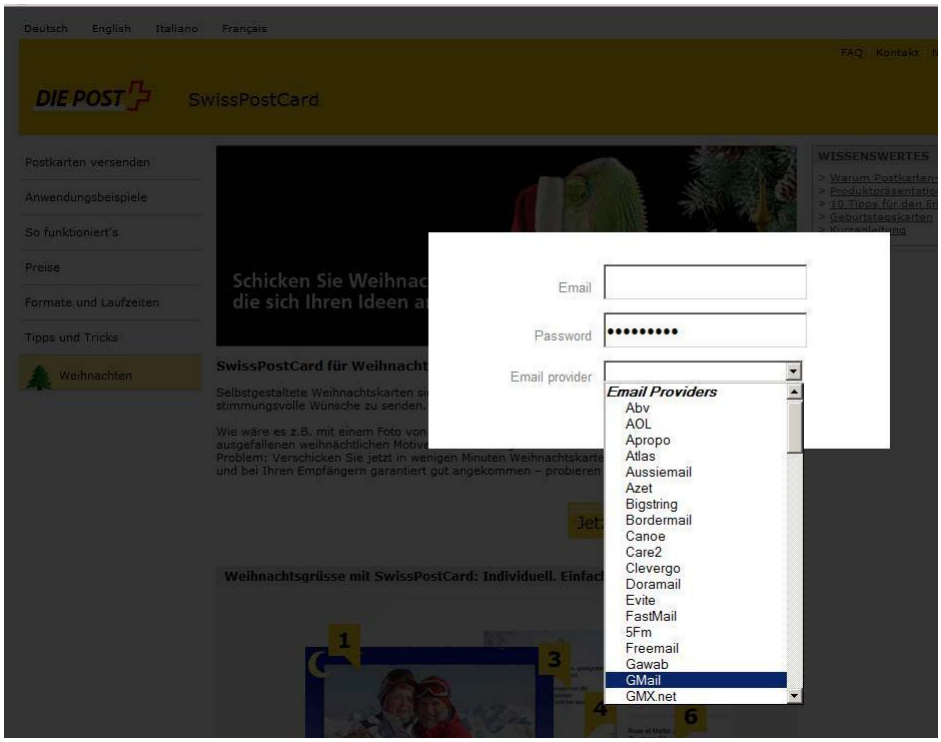


Figure 3: Site de phishing affichant en arrière-plan le site de Swisspostcard et invitant au premier plan la victime à saisir les données d'accès à son compte de messagerie.

Les escrocs récidivaient une semaine plus tard. Mais cette fois, leur courriel d'*hameçonnage* était envoyé non plus au nom de Swisspostcard, mais de Fleurop.

Le premier cas a permis d'établir une statistique du nombre d'accès. Quelque 25 939 personnes ont cliqué sur le lien, dont 4148 plusieurs fois, ce qui donne à penser qu'elles ont au moins essayé de communiquer leur nom d'utilisateur et leur mot de passe. Ainsi, 16 % des personnes auraient mordu à l'hameçon, sans qu'on sache toutefois combien ont réellement livré les données convoitées par les escrocs.

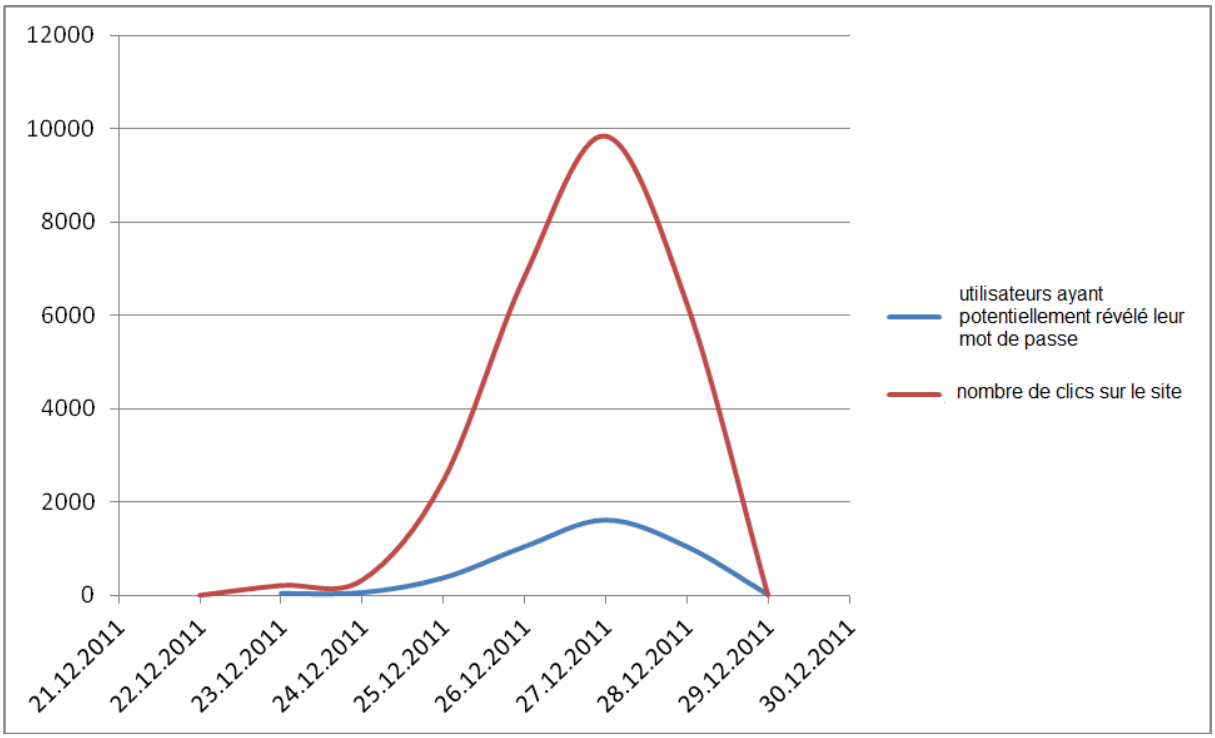


Figure 4: Accès au site d'hameçonnage «unsereweihnachtskarten.com». La ligne rouge indique le nombre de clics sur le site. La ligne bleue correspond aux utilisateurs ayant consulté plusieurs fois la page et donc lui ayant potentiellement révélé leur nom d'utilisateur et leur mot de passe.

Alors que les accès sont restés rares du 22 au 24 décembre 2011, en raison très certainement des festivités de Noël, leur nombre a augmenté en flèche le 25 décembre 2011 pour atteindre un pic le 27. Le site a été désactivé du réseau le 29 décembre.

Il ne suffit plus de se méfier des courriels d'expéditeurs inconnus. La prudence s'impose même lorsque le nom de l'expéditeur est familier. En particulier, il faut être sur ses gardes chaque fois qu'un site Web exige un mot de passe.

3.4 Attaques d'hameçonnage: progrès techniques

Des entités du secteur public, des organisations privées et des fournisseur de services Internet combattent contre les tentatives d'hameçonnage. La désactivation des sites d'hameçonnage est la plupart du temps une opération bien rodée. Entre-temps, ils sont presque tous neutralisés «en temps utile», c.-à-d. dans un délai allant de quelques minutes à un jour. Les cyberpirates cherchent par conséquent de nouvelles méthodes pour déjouer autant que possible la désactivation des sites d'hameçonnage.

Ainsi, la tentative d'*hameçonnage* décrite au chapitre 3.3 générait spécialement un lien par victime, et donc n'agissait qu'une seule fois. Concrètement, l'adresse électronique était encodée en *base64*. Si l'on cliquait une seconde fois sur le lien initial, un message d'erreur s'affichait. De même, la page d'accueil se contentait d'annoncer un message d'erreur. Cette précaution a compliqué la désactivation du domaine. Faute de preuve fournie par des tiers,

les autorités compétentes n'ont pas réagi, croyant de bonne foi qu'il n'y avait pas de site d'hameçonnage sous ce domaine. La réponse suivante d'un registraire le montre clairement:

Hello Sir,

Thank you for your email today and attention to this matter. After review we see that the subdomain you provided is not currently resolving to a phishing site at this time. If you have any further evidence of this domain being in breach of our registration agreement, please respond with it and we are happy to provide you with further assistance.

Thank you,

[redacted] Abuse Team

Figure 5: Réponse du registraire à une demande de MELANI visant à bloquer le domaine du site d'hameçonnage.

Une autre variante utilisée consiste à introduire un filtrage IP (p. ex. restrictions géographiques). Un site d'hameçonnage n'est ensuite joignable qu'à partir de certains domaines IP. Les visiteurs ayant d'autres adresses IP obtiennent un message d'erreur. Quiconque consulte le site avec la «mauvaise» adresse IP aura ainsi l'impression que le site a déjà été désactivé d'Internet.

Il faut toutefois savoir que la plupart des pages d'hameçonnage se dissimulent derrière des sites Web tout à fait normaux, sur un serveur Web qui a été compromis. A la différence des domaines exclusivement utilisés dans un dessein criminel, tant le propriétaire du site que le fournisseur d'hébergement ont ici la possibilité d'effacer le site. Mais comme les hébergeurs se contentent généralement de contrôles en ligne et n'examinent pas les répertoires des *serveurs* à la recherche des pages infectées, ils voyaient jusqu'ici dans le message d'erreur «*404 Not Found*» un indice sûr d'élimination de telles pages par le propriétaire.

3.5 En Suisse aussi: maliciel bloquant le PC et exigeant un paiement

Un *maliciel* mis en circulation au début de novembre en Suisse bloquait toutes les fonctions de l'ordinateur à des fins de chantage. Une fenêtre s'affichait à l'écran, avec un message semblant provenir du Département fédéral de justice et police (DFJP). L'utilisateur y était invité à s'acquitter d'une amende de 150 francs, sous prétexte que de la pornographie infantile et d'autres contenus illégaux auraient été retrouvés sur son ordinateur. Le message n'émanait bien entendu pas d'une autorité suisse.

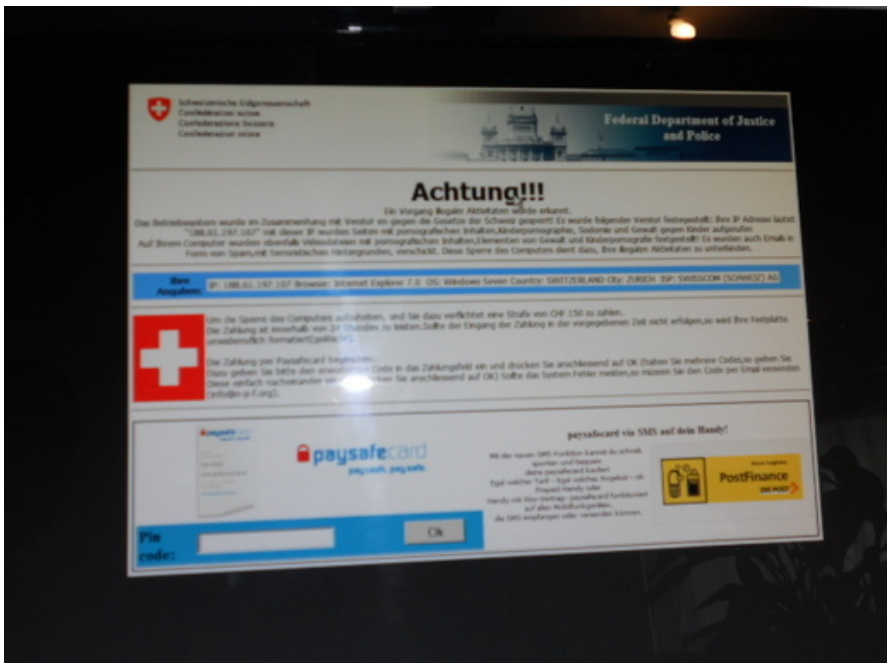


Figure 6: Capture d'écran d'un ordinateur infecté par un ransomware.

Dès mars et avril 2011, un *maliciel* affichait sur les ordinateurs infectés une mise en garde prétendument envoyée par l'Office fédéral de la police criminelle d'Allemagne. Il exigeait le versement d'une amende de 100 euros, en faisant valoir que des données illégales auraient été trouvées sur l'ordinateur infecté. En cas de non-paiement, l'ordinateur serait verrouillé et le *disque dur* reformaté. Des variantes de ce *ransomware* adaptées aux usages locaux ont été observées dans d'autres pays également.

En cas d'apparition de ce message (ou d'un message analogue), MELANI recommande de faire analyser l'ordinateur infecté par un antivirus à jour en version *live CD* et d'éliminer le maliciel, ou de s'adresser à une entreprise d'informatique. Il est également conseillé de changer tous les mots de passe de l'ordinateur infecté.

3.6 Le monde politique dans le viseur des pirates

Plusieurs cyberincidents survenus au deuxième semestre 2011 ont concerné de près ou de loin des politiciens ou des partis politiques. Comme personnes publiques, les politiciens prêtent le flanc à ce genre d'attaques.

Pendant les élections au Conseil fédéral du 14 décembre 2011, un message publié sur Twitter au nom du conseiller national Andrea Caroni a annoncé la réélection d'Eveline Widmer Schlumpf – avant même que le résultat officiel du scrutin ne soit connu. Même s'il n'avait rien à voir avec ce compte Twitter, Andrea Caroni a dû rendre vraisemblable qu'il n'était pas l'auteur du micromessage (*tweet*). Il s'est ainsi rapidement créé un compte Twitter et a envoyé des informations sur l'incident. Cet exemple montre que dans Internet, chacun peut revêtir le rôle de son choix pour mettre en circulation toutes sortes de propos.

Le site Web de l'UDC a de nouveau été victime, le 3 août 2011, d'une attaque par déni de service distribué. En 2009 déjà, les sites des partis gouvernementaux avaient été attaqués et paralysés peu avant le scrutin populaire du 29 novembre 2009 «contre la construction de minarets». Ce nouvel incident a toutefois épargné les autres partis politiques.

La conseillère nationale Chantal Galladé a été confrontée à un tout autre problème. Faute d'avoir renouvelé à temps son domaine chantal-gallade.ch, celui-ci a été acquis par une

tierce personne qui y a placé de la publicité. Toutes les tentatives d'entrer en contact avec le nouveau propriétaire du site ont échoué. Celui-ci n'a pas daigné répondre. Entre-temps, Madame Galladé a enregistré un autre domaine.[6] Quant à l'ancien domaine, il n'accueille plus de publicité et a été mis en vente.

Un autre politicien avait montré sa carte d'identité à la caméra, lors d'une interview télévisée. Un inconnu en a fait une «copie» à partir de son ordinateur et a tenté de l'utiliser comme preuve d'identité pour créer un profil sur un portail de rencontres pour homosexuels. Mais le portail a pris contact avec le politicien pour lui demander s'il avait vraiment créé un tel profil. Le profil a été effacé aussitôt après sa réponse négative. Le bon travail et les précautions prises par le portail de rencontres ont permis d'étouffer l'affaire dans l'œuf.

3.7 Attaques massives de sites Web marchands

MELANI a constaté en août 2011, en Suisse aussi, une recrudescence d'*infections de sites web* aux dépens de boutiques en ligne. Les victimes étaient des sites Web marchands utilisant le logiciel de gestion osCommerce.

Les attaques ont été lancées via une *interface Admin* mal sécurisée. Les anciennes versions du logiciel renonçaient par défaut au contrôle classique des accès. Au lieu d'utiliser un mot de passe, le logiciel attribuait au répertoire du *panneau d'administration* un nom obscure ou/et il fallait sécuriser le répertoire à l'aide d'un fichier htaccess. Celui-ci (en anglais: hypertext access) peut être placé dans n'importe quel répertoire d'un site Web et sert à gérer les paramètres de configuration. De nombreux utilisateurs ont hélas négligé cette pratique. Pour y remédier, un contrôle des accès en tant qu'administrateur a été mis en place dans la version 2.2RC2 afin d'améliorer a posteriori le niveau de sécurité. Or en cas d'installation incorrecte, il était aisé de contourner cette mesure de sécurité sur un serveur Web Apache, par une *manipulation d'URL*.[7] Le pirate pouvait ainsi s'introduire dans l'administration et y installer le *code* de son choix. C'est ce qui s'est souvent produit en juillet/août 2011. Les boutiques Web piratées ont ensuite été utilisées pour propager des *infections de sites Web*. Selon le portail spécialisé gulli.com, les pirates auraient compromis 90 000 sites Web marchands.[8]

Dans le cas d'espèce, il était possible de se protéger en sécurisant tout le répertoire admin par le biais d'un fichier *.htaccess*. Un tel contrôle des accès, réalisé par le serveur Web lui-même, est indépendant de l'invite d'ouverture de session (login prompt) du logiciel de la boutique en ligne. Une marche à suivre détaillée est publiée sur le site heise.de[9]. De façon générale, il faut actualiser non seulement les logiciels des serveurs, mais également les applications installées, en l'occurrence celle de la boutique en ligne, et installer toutes les mises à jour de sécurité disponibles.

---

6 http://www.tagesanzeiger.ch/zuerich/region/Warum-Chantal-Gallad-fuer-Bikinis-wirbt/story/15004208 (état: 23 février 2012).

7 http://www.oscommerce.info/confluence/display/OSCOM23/%28A%29+%28SEC%29+Administration+Tool+Log-In+Update (état: 23 février 2012).

8 http://www.gulli.com/news/16740-zahlreiche-online-shopping-websites-kompromittiert-2011-08-01 (état: 23 février 2012).

9 http://www.heise.de/security/artikel/Schnellhilfe-fuer-osCommerce-Admins-1323536.html (état: 23 février 2012).

3.8 Faux sites immobiliers recrutant des agents financiers

Après une fraude à l'e-banking, il faut «blanchir» l'argent détourné. A cet effet, des *agents financiers* sont recrutés, par exemple via des bourses de l'emploi. Des sites Web spécialement créés à l'image de sites d'entreprises ordinaires comportent une rubrique «emplois vacants». Le profil d'emploi est toujours le même: la personne se fait envoyer de l'argent d'origine inconnue, qu'elle transfère sur des comptes désignés à l'avance. Ces «postes vacants» sont à chaque fois annoncés par *pourriel*.

Une forme particulièrement éhontée de recrutement d'agents financiers sévit aujourd'hui en Suisse. Elle repose sur les données d'entreprises inscrites au registre du commerce mais absentes d'Internet. Les sites publiés à leur nom par les escrocs prétendent appartenir à des entreprises actives au Tessin dans le secteur immobilier et rechercher des représentants régionaux pour transférer de l'argent de clients. Ces sites à l'apparence très professionnelle sont généralement des copies fidèles de sites existants. Le problème ici tient à ce que le mobile criminel n'est pas d'emblée visible – contrairement p. ex. aux sites d'*hameçonnage*. Les hébergeurs désactivent normalement très vite les sites criminels. Mais dans le cas d'espèce, il est très difficile de les convaincre d'agir. Et même quand ils le font, un site identique ne tarde pas à réapparaître sous un autre nom de domaine. Un groupe d'escrocs semble s'être fait une spécialité d'assurer la survie de ce genre de sites Web, afin de recruter un maximum d'agents financiers.

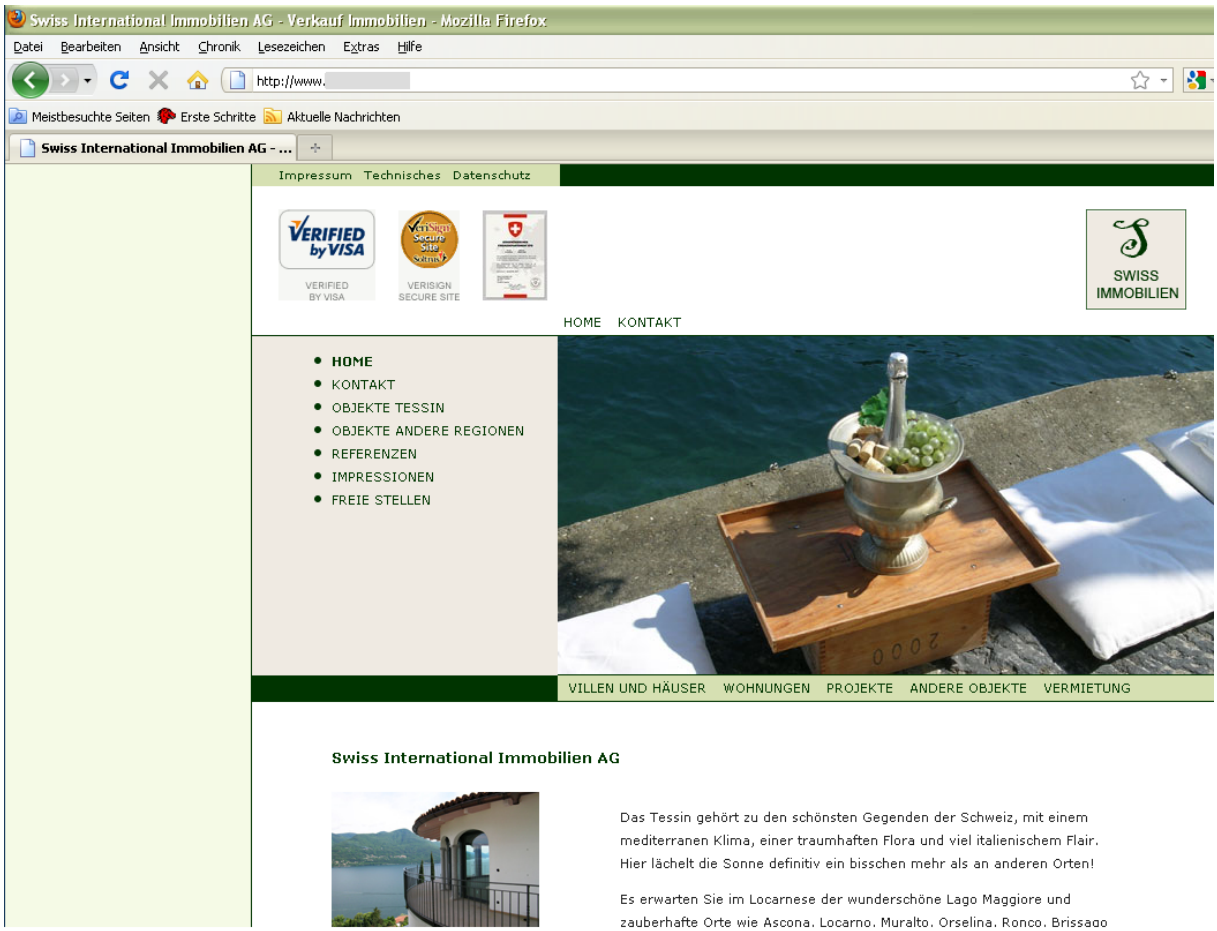


Figure 7: Exemple de site de recrutement d'agents financiers.

De telles offres ne sont pas seulement diffusées par pourriel ou sur des sites spécialement créés, mais se glissent aussi sur des portails d'emplois sérieux. Par principe, la prudence s'impose avec les transferts en espèces, à des inconnus, d'argent que l'on a reçu auparavant (volontairement ou par erreur). Dans tous les cas, il faut se méfier des offres

faisant miroiter des gains élevés. Le principe selon lequel il n'y a pas d'enrichissement légal sans effort vaut également dans le cyberespace. D'où la nécessité de ne jamais mettre son propre compte bancaire à disposition de tiers.

3.9 Systèmes de contrôle reliés à Internet – nécessité d'une sensibilité accrue aux enjeux de sécurité

Les moteurs de recherche de sites Web font partie du quotidien des internautes. Mais jusqu'à peu, on ignorait l'existence de moteurs de recherche permettant de trouver les *serveurs*, *routeurs*, *pare-feu*, imprimantes et autres appareils connectés à Internet. L'un d'eux, appelé SHODAN, existe depuis plusieurs années mais a acquis une grande notoriété suite à la publication de travaux de recherche consacrés aux systèmes *SCADA* reliés à Internet. Des chercheurs de l'Université de Cambridge ont voulu estimer le nombre de *systèmes de contrôle* industriels (SCI) reliés à Internet et particulièrement vulnérables. Leurs recherches[10] visaient à réfuter le mythe voulant que les systèmes de contrôle industriels ne soient pas connectés à Internet, et donc que la sécurité des infrastructures sensibles soit au-dessus de tout soupçon. Les chercheurs ont ainsi découvert que des dizaines de systèmes Siemens Simatic (proies recherchées par Stuxnet), de systèmes *SCADA* et de systèmes de gestion d'immeuble (*building management system, BMS*) sont reliés à Internet.

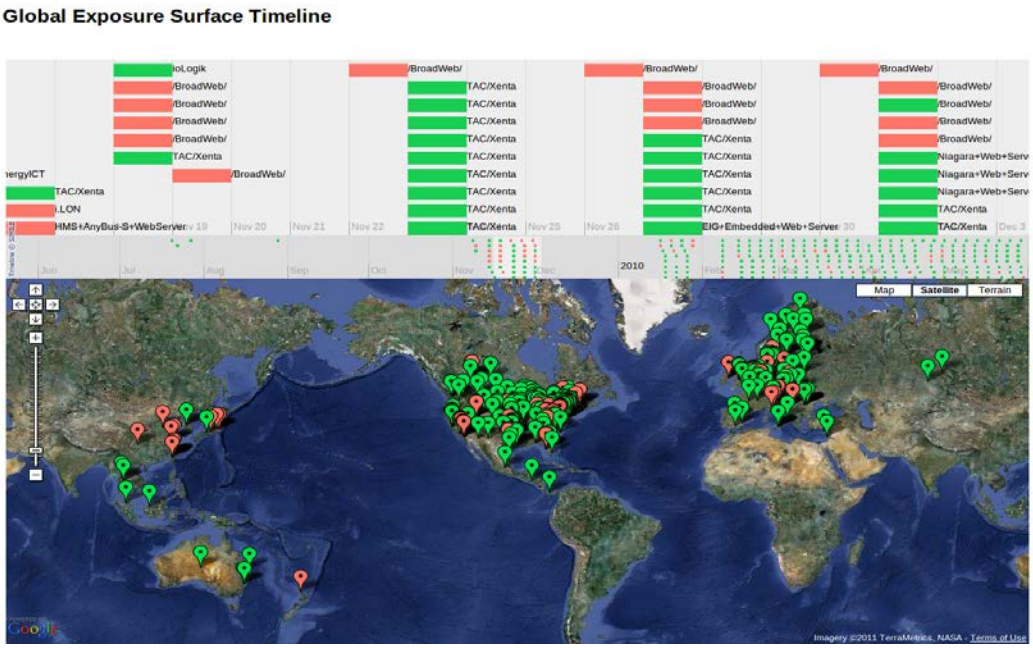


Figure 8: Analyse quantitative et visualisation des systèmes de contrôle industriels prêtant le flanc à des attaques (source: Eireann Leverett)[11]. Les systèmes marqués en rouge sont ceux pour lesquels un exploit existe déjà.

En Suisse, des recherches ont été menées pour identifier les 34 systèmes vulnérables. Il s'agissait généralement d'applications intervenant dans des systèmes de gestion d'immeuble (*BMS*). Leurs propriétaires avaient simplement omis de modifier le mot de passe par défaut des installations de commande. D'où la possibilité d'y accéder et d'en prendre le contrôle. MELANI a constaté, lors de ses vérifications, que les systèmes vulnérables ne faisaient pas partie d'infrastructures vitales, mais le plus souvent d'entreprises hôtelières ou de bureaux.

10 http://www.wired.com/images_blogs/threatlevel/2012/01/2011-Leverett-industrial.pdf (état: 23 février 2012).

11 http://cryptocomb.org/2011-Leverett-industrial.pdf (état: 23 février 2012).

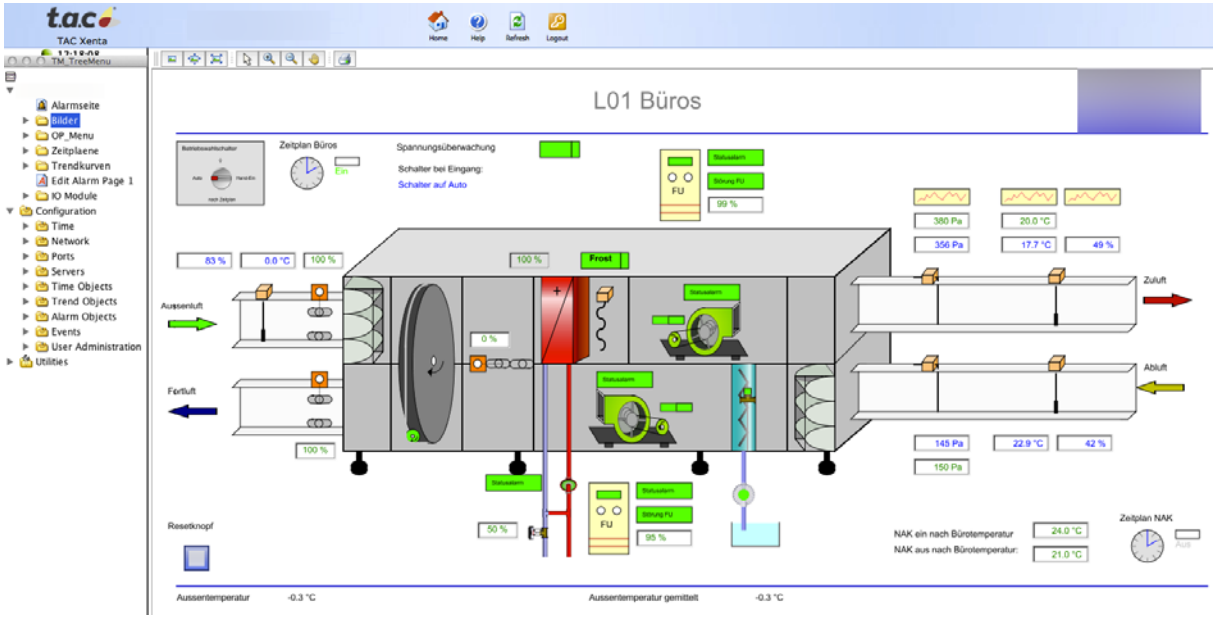


Figure 9: Exemple d'application du fabricant TAC (auj. Schneider Electric Buildings Germany GmbH) servant à la gestion d'immeuble.

Les cibles potentielles ont beau ne pas être vitales, le fait de ne pas modifier le mot de passe par défaut lors de l'installation d'un système de gestion d'immeuble (*building management system, BMS*) relié à Internet constitue une grave infraction aux prescriptions élémentaires de sécurité informatique. La possibilité, p. ex., d'accéder de l'extérieur au réseau de chauffage et de climatisation d'une entreprise et de le manipuler pourrait entraîner, le cas échéant, des problèmes majeurs. Le potentiel d'abus est d'autant plus grand qu'avec l'intégration des systèmes, l'intrus est susceptible d'accéder à d'autres applications de gestion internes, aux logiciels de décompte, etc. Par principe, les systèmes de contrôle industriels ne seront pas reliés à Internet. Si cela devait s'avérer indispensable, la prudence s'impose au niveau de la procédure définie. Une analyse détaillée figure au chapitre 5.1.

4 Situation internationale de l'infrastructure TIC

4.1 Attaque contre un organisme de certification néerlandais

Une attaque lancée contre DigiNotar, *organisme de certification* néerlandais, a abouti à l'émission frauduleuse, selon l'état actuel des connaissances, de plus de 530 *certificats*. Dont p. ex. des *certificats* de domaines appartenant à des services de renseignements: les pirates ont ainsi émis plusieurs *certificats* à chaque fois pour www.sis.gov.uk, www.cia.gov et www.mossad.gov.il. D'autres domaines ont fait les frais de cette escroquerie, dont windowsupdate.com, qui héberge la fonction de mise à jour de tous les produits Windows de Microsoft, et différents domaines de Google.

DigiNotar est un organisme délivrant des certificats numériques servant à garantir l'identité des sites Web visités et la communication cryptée (certificate authority, CA). Si de tels *certificats* ont été falsifiés, un internaute s'imaginera p. ex. être sur le site souhaité alors qu'il est relié à une infrastructure criminelle. Un pirate peut ainsi modifier le chemin d'accès aux données, s'emparer de documents cryptés et livrer à la place des données erronées. L'attaque lancée contre DigiNotar a abouti à la mise en circulation de *certificats* falsifiés – que les *navigateurs* et les ordinateurs croyaient authentiques. D'où la possibilité de décrypter la liaison sécurisée des comptes de messagerie électronique, ou de falsifier les mises à jour de Windows. Un *certificat* truqué n'y suffit toutefois pas, il faut encore rediriger l'envoi sur un *serveur* spécialement préparé. DigiNotar a apparemment découvert la fraude dès le 19 juillet 2011; Google s'est aperçu à fin août que ses services de messagerie subissaient des attaques de l'intermédiaire (*man-in-the-middle*) et a rendu l'incident public.

Microsoft a publié peu après, pour ses systèmes d'exploitation à partir de Windows XP et pour Internet Explorer, des mises à jour qui refusaient les *certificats racine* de DigiNotar et rangeaient l'organisme de certification compromis sur la liste des éditeurs non fiables. D'autres exploitants de *navigateurs*, comme Mozilla (Firefox) et Google (Chrome), ont entre-temps marqué comme non valables dans leurs programmes les *certificats* émis par DigiNotar.

Les faux *certificats* émis ont été employés, selon l'analyse des données faite par l'entreprise de sécurité mandatée, dont le rapport intermédiaire a été publié[12]. Près de 300 000 *adresses IP* auraient utilisé le *certificat* Google falsifié. 99 % de ces *adresses IP* appartenaient à des ordinateurs iraniens. Pour pouvoir capturer les données et les décrypter, le pirate devait encore intervenir directement dans leur cheminement, p. ex. auprès des fournisseurs d'accès Internet. Un cyberpirate iranien a revendiqué entre-temps cette agression et prétend avoir attaqué d'autres organismes de certification. On ignore jusqu'ici si ces attaques peuvent réellement lui être attribuées ou s'il s'agit, le cas échéant, d'un acteur étatique menant des activités d'espionnage.

La cyberattaque lancée contre DigiNotar a été fatale à cette entreprise. Selon sa société-mère Vasco, elle a cessé toute activité commerciale et a été liquidée. Peu après la révélation de l'incident, l'Etat néerlandais a repris le contrôle des activités opérationnelles de DigiNotar.

---

12 http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html (état: 23 février 2012).

Car outre ses propres c*ertificats*, DigiNotar était fournisseur des certificats PKI Overheid de l'Etat, et des indices laissaient croire que les systèmes de gestion utilisés à cet effet avaient aussi été compromis. Le certificat racine PKI Overheid n'a toutefois pas été retiré, pour ne pas compromettre la communication cryptée entre les systèmes informatiques. En outre, rien ne prouvait que de faux *certificats* aient été émis à l'aide de cette infrastructure. Tous les certificats délivrés par DigiNotar en tant que fournisseur de *certificats* PKI Overheid ont néanmoins été remplacés, par prudence, par de nouveaux *certificats* émanant d'autres organismes de certification.

Dans un autre cas, un cyberpirate a prétendu s'être introduit dans les systèmes de GlobalSign. Cet émetteur de certificats belge a alors retiré ses *serveurs* du réseau pendant une semaine et lancé une enquête. Il en est ressorti que le pirate ne s'était pas introduit dans un *serveur* servant à l'émission de certificats, mais dans un *serveur* hébergeant les pages Web publiques destinées au marché nord-américain. Selon GlobalSign, le serveur en question n'hébergeait ni application Web, ni données de clients.[13]

L'usage fructueux de *systèmes cryptographiques* à clé publique (public key cryptography) dépend de la fiabilité du fournisseur de services de certification choisi (*certification service provider, CSP*) et de l'infrastructure à clé publique (*public key infrastructure, PKI*)[14]. Aussi la robustesse des CSP et des PKI a-t-elle toujours été au cœur des préoccupations des techniciens préposés à la sécurité informatique. Ils recherchent notamment des scénarios empêchant toute contrefaçon des *certificats* (par exploitation d'une faible résistance aux collisions des fonctions de hachage[15]), ou encore l'usage abusif de certificats de signature de code. Dans ce dernier cas – comme l'a montré le ver Stuxnet –, un *certificat* usurpé permettrait p. ex. d'introduire dans un système d'exploitation des *maliciels*, sous forme de *logiciels pilotes* pourvus d'une signature numérique. En outre, les événements récents prouvent que les CSP risquent eux aussi d'être compromis par des escrocs cherchant à émettre de faux *certificats*. La tendance est apparemment de remonter à la source, pour ne pas devoir péniblement traquer les failles d'une procédure de cryptage en soi sûre.

4.2 SCADA – maliciels, cyberattaques et vulnérabilités

Les systèmes SCADA (Supervisory Control And Data Acquisition) servent à la surveillance et à la gestion des processus techniques (p. ex. approvisionnement en énergie et en eau). Au départ, ces systèmes ne ressemblaient que de loin aux TIC usuelles, ils étaient isolés des réseaux informatiques, utilisaient du matériel et des logiciels propriétaires et possédaient leur propre protocole de communication avec l'ordinateur central. Depuis quelques années, la commercialisation d'appareils relativement avantageux intégrant, comme technologie d'interface, le protocole Internet a changé la donne. Le recours aux TIC courantes et peu coûteuses s'est répandu, le revers de la médaille étant que les systèmes SCADA sont exposés aux menaces bien connues présentes sur Internet: les maliciels et les cyberpirates n'ont pas tardé à faire leur apparition.

---

13 http://www.zdnet.de/news/41558800/globalsign-comodohacker-hat-die-falschen-systeme-erwischt.htm (état: 23 février 2012).

14 En ce sens, les CSP et les PKI constituent le talon d'Achille de la cryptographie à clé publique.

15 Le secteur spécialisé Sécurité de l'UPIC a approfondi ce point dans ses considérations technologiques du 4 août 2010: «Technologiebetrachtung: Kollisionsresistenz und Brechung kryptografischer Hashfunktionen»: http://www.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de (état: 23 février 2012).

Symantec démasque Duqu, maliciel apparenté à Stuxnet

L'existence du *maliciel* Duqu, chargé d'espionner les ordinateurs des entreprises et des développeurs de systèmes de contrôle industriels (systèmes *SCADA*) a été révélée le 14 octobre 2011. Les données dérobées par ce biais pouvaient ensuite servir à lancer des attaques ciblées. Les composantes de base (pilotes) de ce nouveau *maliciel* sont reprises de Stuxnet.[16] A ceci près que le nouveau *maliciel* ne possède ni routine pour se propager, ni composantes *SCADA* pour manipuler p. ex. des systèmes de gestion. Afin de ne pas attirer l'attention, le *maliciel* ne s'active que 15 minutes après son installation. Son identification est d'autant plus difficile qu'il quitte le système infecté au bout de 36 jours. Différentes variantes de Duqu ont été observées. Dans un cas, un certificat dérobé à une société taïwanaise a servi à son installation; là encore, un parallèle peut être fait avec Stuxnet. Les autres variantes étaient apparemment dépourvues de signature numérique.

Les fonctions du *maliciel* comprennent l'enregistrement des frappes du clavier, l'analyse des informations échangées avec le réseau et des captures d'écran. Les informations recueillies sont dissimulées dans un banal fichier graphique en vue de leur transmission. Le pirate peut toutefois moduler à sa guise les fonctions susmentionnées, qui ne sont pas liées au *maliciel*. Duqu communique sous forme cryptée avec un *serveur command & control* possédant une *adresse IP* indienne: l'ordinateur infecté lui livre les données recueillies et prend auprès de lui de nouvelles instructions. Une variante antérieure aurait circulé en décembre 2010, les variantes récentes remontant à septembre et octobre 2011. Duqu aurait été localisé sur des ordinateurs de sept ou huit entreprises européennes, dont une *adresse IP* suisse.

Rumeurs d'attaques contre l'approvisionnement en eau

Une prétendue attaque électronique lancée au début de novembre 2011 contre le système d'alimentation en eau potable de Springfield/Illinois aux Etats-Unis a suscité tout un débat parmi les milieux spécialisés. Un pirate serait parvenu à s'infiltrer dans l'approvisionnement en eau et à saboter une pompe, à force de l'enclencher et de la déclencher. Comme peu de temps avant un ordinateur possédant une *adresse IP* russe avait semble-t-il accédé au réseau en question, les ragots allaient bon train. Quelques jours plus tard, le FBI et le Département de la sécurité intérieure (Department of Homeland Security, DHS) ont réfuté les comptes rendus de l'incident de Springfield. Il n'y avait aucun indice de cyberattaque. Le passage d'un rapport publié par la cellule d'analyse de la menace terroriste de l'Etat d'Illinois, à partir duquel de telles spéculations avaient été échafaudées, reposait sur des données non vérifiées. Rien n'indiquait que des données d'accès au système aient été dérobées, et l'on n'avait détecté aucune trace d'intrusion. Les accès à partir de la Russie provenaient d'un technicien dûment autorisé qui se trouvait en déplacement en Russie et qui se connectait au réseau à distance (conformément aux règles). La pompe connaissait des problèmes depuis longtemps et s'était plusieurs fois enclenchée et déclenchée, avant de cesser définitivement de fonctionner.

Un pirate probablement encouragé par ce fait divers s'est introduit le 18 novembre 2011 dans le service d'alimentation en eau potable de South Houston/Texas et a publié à titre de preuve des *captures d'écran (screenshot)* du système de gestion infiltré. Une personne ayant pour pseudonyme «pr0f» a expliqué sur le site pastebin.com les motifs de cette attaque: «L'heure est venue de montrer que les systèmes sensibles ne doivent pas être reliés à Internet. On ne doit pas craindre une vaste cyberguerre, mais plutôt les actes isolés d'individus qui, pour toutes sortes de motifs et sans êtres versés en informatique, sont susceptibles de s'en prendre à de tels systèmes».

---

16 Voir rapport MELANI 2010/2, chapitre 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=fr (état: 23 février 2012).

Piratage en 2007 et 2008 d'un satellite d'observation américain

Selon un article du magazine Bloomberg Businessweek[17], des attaques répétées auraient été décelées en 2007 et en 2008 contre les systèmes de gestion de deux satellites d'observation américains. De tels satellites servent à observer la terre, à comprendre le climat et à établir des cartes. Les pirates auraient pris le contrôle des opérations pendant plusieurs minutes. Bien qu'on ignore le déroulement exact des opérations, il se peut que des données aient été falsifiées. En théorie, il aurait été possible de modifier la trajectoire des satellites et même de les faire s'écraser au sol.

Préoccupations pour la sécurité du réseau du Dreamliner de Boeing

Selon un rapport de la FAA[18], le raccordement au réseau du nouveau Dreamliner de Boeing soulève des questions de sécurité. Apparemment, le réseau permettant aux passagers d'accéder à Internet en vol serait relié physiquement au réseau de contrôle et de navigation de l'avion, qui gère les fonctions relevant de la sécurité.

Boeing a tenu à préciser que le document de la FAA était trompeur et que le réseau destiné aux passagers n'était pas entièrement relié aux autres réseaux. A la séparation physique des réseaux s'ajoutaient des logiciels *pare-feu* et d'autres solutions ne pouvant être évoquées sur la place publique. Même s'il serait concevable d'échanger des données entre lesdits réseaux, les mécanismes de protection installés l'interdisaient absolument, en évitant que le service Internet du passager puisse accéder aux réseaux de contrôle et de navigation.

Toute liaison physique entre le réseau des passagers et le réseau de contrôle de l'avion rend le système de contrôle vulnérable aux cyberattaques. Boeing a reconnu le problème et souhaite tester et mettre en place une nouvelle solution.

Les problèmes rencontrés par les systèmes *SCADA* ont une explication historique. C'était à l'origine des systèmes propriétaires et autonomes, fonctionnant en réseau fermé. A la rigueur, seul le fabricant pouvait y accéder de l'extérieur, via un modem à composition automatique (*dial-up modem*), à des fins de maintenance. Ces systèmes ne comportent dès lors guère de fonctions de protection contre les attaques électroniques. Or ces derniers temps, les systèmes *SCADA* sont toujours plus en réseau, ils font appel à des protocoles et des technologies standardisés, sont parfois accessibles via Internet, voire ont été repérés par des moteurs de recherche spéciaux (voir moteur de recherche SHODAN au chapitre 3.9). Stuxnet a également montré que même un système cloisonné ne suffit pas à garantir la sécurité. Dès lors que des données peuvent être transférées, p. ex. via une *clé USB*, des *maliciels* risquent d'y entrer clandestinement. La présence de Stuxnet dans les médias a éveillé l'intérêt de nombreux experts de la sécurité pour les systèmes de supervision industrielle et les solutions *SCADA*. Entre-temps, toute une série de lacunes de sécurité ont été identifiées dans ces produits. Les recherches ont notamment montré des méthodes permettant de commander à distance des systèmes, d'en importer ou d'y télécharger toutes sortes de données, d'y introduire et exécuter des *codes* nuisibles, ou encore de les alimenter en fausses données auxquelles ils réagiront en donnant les commandes aberrantes voulues par les pirates.

17 http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html (état: 23 février 2012).

18 Federal Aviation Administration, autorité aéronautique américaine, http://www.faa.gov (état: 23 février 2012).

4.3 Anonymous

Le 27 juillet 2011, la police britannique a arrêté sur l'archipel écossais des Shetland un jeune homme de 19 ans, soupçonné d'être le porte-parole des groupes Anonymous et LulzSec. D'autres participants à ce mouvement de cyberprotestation ont été interpellés notamment aux Etats-Unis, en Grande-Bretagne, aux Pays-Bas, en Espagne et en Turquie. De telles arrestations sont à chaque fois suivies d'attaques dirigées contre les sites Web des corps de police ou des gouvernements impliqués. C'est ce qui s'est produit au début de juillet, après une action coordonnée des polices italienne et tessinoise durant laquelle 15 personnes soupçonnées d'activisme ont été arrêtées en Italie. De même, un Italien de 26 ans considéré comme le cerveau de la branche italienne d'Anonymous a été arrêté au Tessin où il résidait. Le collectif Anonymous avait notamment attaqué les sociétés italiennes Eni, Finmeccanica et Unicredit. D'autres institutions comme la Poste italienne, le Sénat, la Chambre des députés ou le site du ministre-président Berlusconi étaient dans son collimateur. Suite à ce coup de filet, des cyberactivistes ont annoncé avoir dérobé et publié sur Internet des données de *serveurs* de la cyberpolice italienne (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastructure Critiche, CNAIPIC). Cette autorité étatique est chargée de la protection de l'intégrité et du maintien de la disponibilité des infrastructures informatiques vitales en Italie. Le groupe Anonymous a beau avoir rejeté, en la qualifiant de faux, une lettre décrivant l'opération comme une mesure de rétorsion, il semble y avoir un lien entre ces deux événements.

En juillet 2011 également, des cyberactivistes ont signalé s'être introduits dans un *serveur* de l'OTAN et y avoir copié de nombreux documents. A titre de preuve, ils ont publié deux documents PDF de 2007 et 2008. Le vol aurait été commis à l'aide d'une *injection SQL*. Une autre action a consisté à publier le nom, l'adresse et la date de naissance de 25 000 politiciens autrichiens. Cette action visait à dénoncer l'obligation de conservation des données relatives aux communications électroniques, instaurée en avril 2011 en Autriche.

Mais l'action qui a eu le plus grand retentissement est sans aucun doute l'attaque lancée en fin d'année contre les données de clients de l'entreprise américaine Strategic Forecast (Stratfor). Cette société spécialisée dans les analyses internationales de la sécurité livre à ses clients des rapports sur des enjeux brûlants de la sécurité géopolitique, comme le terrorisme, les bouleversements politiques ou les changements de pouvoir dans des pays spécifiques. Cette cyberattaque a permis de dérober des fichiers d'adresses électroniques, des données d'utilisateur, des mots de passe et des informations sur des cartes de crédit. L'action visait notamment à effectuer, avec les données de cartes de crédit volées, des versements à des organisations de bienfaisance et, par là, à «redistribuer plus d'un million de dollars au profit d'œuvres charitables». Or des paiements non autorisés ont également été réalisés à l'aide des cartes de crédit. Les activistes ont d'ailleurs rendu un mauvais service aux organisations de bienfaisance – de tels paiements générant de lourds frais administratifs pour toutes les parties. Dans un premier temps, Anonymous a revendiqué cette action baptisée LulzXmas, avant que paraisse sur Internet, en son nom, un démenti qu'Anonymous a par la suite désavoué. Enfin, un communiqué a exposé les «vraies» raisons de l'attaque, soit révéler les contacts entretenus avec les services secrets et l'industrie d'armement.

Des cyberactivistes du monde entier militent, sous la bannière Anonymous, pour un Internet libre et exempt de tout contrôle étatique. Anonymous a beau dire et répéter être un collectif de militants égaux en droits, quelques personnes y tiennent le rôle de meneurs. Il s'agit probablement d'utilisateurs versés en informatique, qui motivent leurs troupes en leur révélant des possibilités d'action. Quiconque le souhaite peut y exercer cette fonction – à court terme aussi. Une analyse de la structure des membres figure au chapitre 5.2.

4.4 Un acteur étatique aurait espionné pendant des années des systèmes informatiques, dont ceux de l'ONU à Genève et du CIO

L'entreprise de sécurité McAfee a publié le 3 août 2011 des informations relatives à une attaque coordonnée visant des entreprises, des autorités publiques et des organisations. Elle avait découvert sur un serveur de contrôle appartenant aux pirates, grâce à une erreur de configuration, des fichiers journaux (*log file*) répertoriant toutes les intrusions commises depuis 2006. L'analyse de ces fichiers a permis de savoir à qui ces agresseurs s'en étaient pris et combien de temps leurs attaques avaient duré. McAfee parle de l'une des plus grosses affaires d'espionnage à ce jour. Depuis 2006, 72 entreprises, organisations et gouvernements, dont le siège genevois des Nations Unies et le siège lausannois du Comité international olympique (CIO), ont été épiés de manière systématique. La plupart des réseaux piratés se trouvent toutefois aux Etats-Unis. Il s'agit de sociétés de communication par satellite, d'entreprises de sécurité et même d'un fabricant de panneaux solaires. Aucun nom concret d'entreprise n'a filtré. Des services gouvernementaux américains, canadiens, indiens, vietnamiens et taïwanais sont également concernés. Quant à la nature des renseignements dérobés, l'entreprise de sécurité s'est contentée de dire que «les informations pillées constitueraient une grave menace économique, si elles devaient tomber entre les mauvaises mains.»[19]

Pour cette opération, les pirates ont utilisé des méthodes d'infection traditionnelles, comme l'envoi de courriels ciblés et des liens spécialement préparés. Leurs victimes ont reçu des courriels personnalisés comportant de fausses adresses d'expéditeur. Il suffisait d'un clic sur le lien indiqué pour qu'un *maliciel* se charge et s'installe. En outre, un canal aboutissant au serveur de contrôle était mis en place.

Il semble probable qu'un acteur étatique soit à l'origine de cette cyberattaque, étant donné l'absence de marché pour ce genre d'informations. Le fait que le serveur de contrôle n'ait pas été mieux protégé montre soit que les pirates ne sont pas non plus irréprochables dans la sécurisation de leurs infrastructures, soit qu'ils s'en moquent parce qu'ils ont assez d'autres alternatives. Cette attaque d'espionnage rappelle une fois de plus l'intérêt durable qu'éveillent les données et informations, et les pressions croissantes que subissent chaque jour les données sensibles. Tout indique que d'autres réseaux d'espionnage sont en cours de mise en place, voire sont opérationnels sans avoir encore été découverts.

Ainsi l'envoi de courriels ciblés se poursuivra. C'est ce que montre p. ex. l'attaque lancée en juillet 2011 contre des entreprises d'armement. En l'occurrence, les escrocs ont adressé à des collaborateurs triés sur le volet des courriels formulés de manière professionnelle, qui annonçaient une conférence de l'Institut américain d'aéronautique et d'astronautique (AIAA). Ce document classé «secret» invitait ses destinataires à transmettre jusqu'au 30 juillet une contribution scientifique pour cette manifestation.[20] Les escrocs se réfèrent fréquemment à une conférence dans leurs courriels de subversion psychologique.

Rappelons que les multinationales ne sont pas seules visées par l'espionnage économique, mais que les petites et moyennes entreprises novatrices constituent des proies recherchées.

---

19 http://www.spiegel.de/netzwelt/web/0,1518,778126-8,00.html (état: 23 février 2012).

20 http://www.heise.de/security/meldung/Gezielte-Angriffe-auf-Ruestungskonzerne-dauern-an-1282837.html (état: 23 février 2012).

La Chine est régulièrement soupçonnée d'être à l'origine de ce genre d'opérations, ce que le gouvernement chinois dément à chaque fois. En effet, il est difficile de déterminer sans hésitation possible les auteurs d'une cyberattaque, dont les seules traces sont généralement les *adresses IP*. Si une *adresse IP* vient de Chine, cela ne prouve pas pour autant que le pirate soit lui aussi chinois. Il est relativement aisé de louer dans n'importe quel pays des *serveurs* pour lancer des attaques, à seule fin de dissimuler le pays d'origine de l'agression. Et même si l'attaque venait réellement de Chine, on ne sait pas pour autant qui en est l'instigateur. Selon un article du Wall Street Journal les services secrets américains ont identifié une vingtaine de groupes pirates chinois, dont émaneraient la plupart des cyberattaques lancées contre les Etats-Unis.[21] Même si selon un rapport douze d'entre eux communiquent avec l'Armée populaire de libération de Chine, il sera très difficile de prouver que le gouvernement chinois ait ordonné les attaques. A cela s'ajoute que plusieurs Etats seraient en mesure de lancer de vastes opérations de cyberespionnage.

4.5 Cyberattaques diverses

Au deuxième semestre aussi, des opérations concertées de piratage et d'espionnage informatique ont été menées ou rendues publiques. La liste d'exemples qui suit n'a aucune prétention à l'exhaustivité:

Attaque d'espionnage contre la Chambre américaine du commerce

Selon le Wall Street Journal, des pirates chinois auraient aménagé au moins six portes dérobées dans le réseau informatique de la Chambre américaine du commerce. C'est ainsi que l'organisation faîtière de l'économie américaine basée à Washington a peut-être fait l'objet d'un espionnage systématique pendant des mois entiers. La faille de sécurité a été découverte et comblée dès mai 2010, mais ce n'est qu'au premier semestre 2011 que l'incident a été rendu public.[22]

Nouvelle attaque visant les services en ligne de Sony

Après l'attaque lancée au semestre précédent contre des données de clients de Sony, des pirates se sont à nouveau introduits, en octobre 2011, dans les comptes d'utilisateurs des services en ligne PlayStation Network (PSN) et Sony Entertainment Network (SEN). Ils auraient ainsi accédé à 93 000 comptes, mais Sony les aurait verrouillés et les données des cartes de crédit n'auraient couru aucun danger. Contrairement au premier cas, l'attaque n'avait pas été lancée directement contre Sony: la tentative d'accès aux comptes reposait sur des informations obtenues d'une autre manière. L'explication est simple: beaucoup d'utilisateurs se servent du même mot de passe pour plusieurs services, voire pour tous. Prévenus par courriel, les titulaires des comptes n'ont pu réutiliser leur compte qu'à l'issue d'un processus d'authentification. Sony s'est engagé à rembourser les personnes lésées, au cas où des achats auraient été réalisés frauduleusement sur son réseau.

---

21 http://online.wsj.com/article_email/SB10001424052970204336104577094690893528130-lMyQjAxMTAxMDEwMjExNDIyWj.html; voir aussi le rapport complet du service de contre-espionnage des Etats-Unis (Office of the National Counterintelligence Executive, NCIX): www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (état: 23 février 2012).

22 http://www.spiegel.de/netzwelt/netzpolitik/0,1518,805052,00.html (état: 23 février 2012).

Cyberattaques contre des réseaux sud-coréens

Les données de 35 millions d'internautes ont été dérobées lors d'une cyberattaque menée en Corée du Sud. Les autorités nationales ont révélé à fin juillet que l'agression émanait d'ordinateurs ayant une *adresse IP* chinoise et avait pris pour cibles la plate-forme en ligne Nate et le réseau social Cyworld. Entre autres données obtenues illégalement figuraient des numéros de téléphone, des numéros de sécurité sociale ainsi que des adresses électroniques et des mots de passe. La police sud-coréenne a expliqué que les investigations dureraient probablement plusieurs mois.[23]

4.6 Désactivation du réseau de zombies DNS-Changer

Une infection provoquée par le *maliciel DNS*-Changer manipulait le *système DNS* afin que le *navigateur* redirige à leur insu les internautes sur des pages spécialement préparées, lorsqu'ils voulaient consulter des sites Web populaires.

Le FBI a arrêté en novembre 2011 les administrateurs criminels de ce *réseau de zombies*. Les serveurs de noms de domaine (*DNS* server) piratés ont été remplacés par des serveurs fonctionnant correctement et gérés par le FBI, pour éviter toute nouvelle manipulation.

Ces *serveurs* auraient dû être déconnectés le 8 mars 2012, mais le FBI a prolongé le délai jusqu'au 9 juillet 2012. A partir de cette date, les ordinateurs infectés ne pourront plus résoudre de nom de domaine et les utilisateurs concernés ne pourront par conséquent plus consulter de site Web. D'où de sérieux problèmes à prévoir, selon l'usage fait de l'ordinateur.

SWITCH[24] et les autorités allemandes ont conçu des tests en ligne permettant à chacun de savoir en un instant si son ordinateur a été infecté par le *maliciel DNS*-Changer[25].

Selon les informations dont dispose MELANI, le FBI aurait notamment identifié en une semaine 20 500 *adresses IP* suisses. Cela ne signifie pas qu'il y ait autant de systèmes infectés, car il s'agit le plus souvent d'*adresses IP* dynamiques. Des milliers d'ordinateurs suisses pourraient néanmoins être infectés par le *maliciel DNS*-Changer.

4.7 Chevaux de Troie des autorités de poursuite pénale

Le 8 octobre 2011, le Chaos Computer Club (CCC)[26] a déclaré s'être procuré le cheval de Troie utilisé par les autorités de poursuite pénale allemandes. Ce cheval de Troie sert aux enquêteurs allemands à surveiller à la source les télécommunications. Il intercepte les communications téléphoniques par Internet, soit les conversations par *voice over IP* (*VoIP*), avant leur cryptage au niveau de l'émetteur ou après leur décryptage chez le récepteur.

Dans la discussion qui a suivi, ce cheval de Troie a souvent été assimilé à tort aux programmes d'espionnage des services de renseignements et aux opérations de mise sur écoute à grande échelle. Or il faut bien se garder de confondre les bases juridiques applicables aux différents types d'interventions.

---

23 http://www.tagesanzeiger.ch/digital/internet/Hacker-greifen-suedkoreanische-Netzwerke-an/story/31054597 (état: 23 février 2012).

24 http://www.dns-check.ch (état: 23 février 2012).

25 http://www.dns-ok.de (état: 23 février 2012).

26 http://www.ccc.de (état: 23 février 2012).

Le CCC a reproché aux autorités de poursuite pénale, après avoir analysé leur cheval de Troie, de ne pas avoir limité ses fonctions à l'enregistrement des conversations, mais d'avoir aussi prévu des possibilités de lecture et de transmission des données enregistrées sur l'ordinateur. Il était ainsi possible de connaître le contenu du *navigateur Web* à l'aide de captures d'écran. En outre, une possibilité d'accès à distance permettait de télécharger toutes sortes de fonctions. Le CCC a également critiqué le mode de cryptage: la communication sortante faisait l'objet d'un simple *cryptage symétrique*, la communication entrante étant dépourvue de tout cryptage. Ce n'est pas anodin, car apparemment les données et les instructions ne sont pas traitées sur des *serveurs* allemands, mais sur des serveurs étrangers. Le cheval de Troie comporterait en outre des failles de sécurité dont des tiers seraient susceptibles de tirer parti pour accéder eux-mêmes à l'ordinateur surveillé.

En Suisse aussi, l'incident a lancé un débat sur l'utilisation de chevaux de Troie par les autorités de poursuite pénale. La Police judiciaire fédérale y a recouru dans quatre cas – trois fois dans la lutte contre le terrorisme, une fois contre le crime organisé. Le canton de Zurich s'est servi dans au moins un cas d'un cheval de Troie contre des trafiquants de drogue[27]. En apprenant l'existence de ce cheval de Troie, le parti pirate suisse a saisi le Ministère public de la Confédération d'une plainte contre l'utilisation de logiciels d'espionnage dans la lutte contre le terrorisme et le crime organisé. Le Ministère public de la Confédération a toutefois refusé d'entrer en matière.[28]

Avant même l'ère d'Internet, les autorités de poursuite pénale pouvaient déjà écouter les conversations téléphoniques de personnes suspectes, avec l'autorisation d'un juge. Les fournisseurs de services de télécommunication ont en effet l'obligation légale de laisser les autorités de poursuite pénale pratiquer cette forme de surveillance.[29]

L'essor de technologies de communication alternatives confronte les autorités de poursuite pénale à de nouveaux défis. A l'instar de la téléphonie par Internet (p. ex. Skype), où il n'y a plus d'opérateur téléphonique classique pour acheminer les conversations par le réseau. La communication s'y fait de manière cryptée, et la surveillance n'est possible qu'aux terminaux. La procédure pénale autorise l'usage de dispositifs techniques à des fins de surveillance.[30] Dans le cas de la téléphonie par Internet, il peut s'agir d'un programme qui s'infiltrera dans l'ordinateur de la personne suspecte, afin d'y surprendre la communication avant son cryptage et de la transmettre aux autorités de poursuite pénale.

Les bases juridiques actuelles[31] sont-elles suffisantes en Suisse pour ce genre de surveillance? La jurisprudence et les milieux politiques sont divisés sur la question.[32] D'autant plus que lors des débats, les confusions sont fréquentes entre poursuite pénale et service de renseignements, entre surveillance téléphonique et perquisitions en ligne d'ordinateurs. D'une part, il s'agit d'examiner sous l'angle du droit les entités impliquées et les diverses mesures en place. D'autre part, il convient de limiter les fonctionnalités des logiciels aux interventions admises, ainsi que d'exclure toute modification de ces fonctions ou tout abus des méthodes prévues. Il n'est pas acceptable qu'un logiciel d'écoute dûment

27 http://www.nzz.ch/nachrichten/politik/schweiz/trojaner_im_fall_stauffacher_eingesetzt_1.12994241.html (état: 23 février 2012).

28 http://www.aargauerzeitung.ch/schweiz/anzeige-der-piratenpartei-zu-spionage-software-bleibt-ohne-folgen-115718001 (état: 23 février 2012).

29 Voir la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT): http://www.admin.ch/ch/f/rs/c780_1.html (état: 23 février 2012) et son ordonnance http://www.admin.ch/ch/f/rs/c780_11.html (état: 23 février 2012).

30 Art. 280 du code de procédure pénale suisse: http://www.admin.ch/ch/f/rs/312_0/a280.html.

31 Le code de procédure pénale suisse n'est en vigueur que depuis le 1er janvier 2011. Jusque-là, chaque canton ainsi que la Confédération avaient leur propre droit de procédure.

32 L'usage de logiciels de surveillance n'est possible en Suisse que dans le cadre d'une poursuite pénale. Les services de renseignement ne sont pas autorisés à s'en servir à titre préventif.

autorisé pour enregistrer les conversations VoIP permette aussi, p. ex., de faire des captures d'écran ou d'intercepter des courriels. La situation devient réellement problématique si l'on ne peut exclure tout risque que des tiers non autorisés prennent connaissance des données collectées, voire procèdent à des manipulations des logiciels utilisés. Car la sécurité doit primer en cas de recours à ce genre de moyens.

Il convient de rappeler enfin la présence d'obstacles de taille à une surveillance téléphonique «normale», voire à une surveillance de la téléphonie par Internet: en Suisse, elle n'entre en ligne de compte qu'avec l'autorisation d'un juge, pour certains délits graves et si «les mesures prises jusqu'alors dans le cadre de l'instruction sont restées sans succès ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance».[33] Le principe de proportionnalité doit être respecté ici, comme à chaque atteinte aux droits fondamentaux.

4.8 Ventes de logiciels de surveillance et d'investigation montrées du doigt par WikiLeaks

WikiLeaks a commencé à publier le 1er décembre 2011, en collaboration avec de grands journaux du monde entier, des documents censés prouver que les solutions de sécurité, de surveillance et d'investigation informatique ne sont pas seulement vendues aux Etats démocratiques, mais que de juteuses affaires sont également conclues avec des Etats bafouant le droit. La grande majorité de ces documents sont des brochures de vente, des présentations publiques et des listes de prix d'une centaine de sociétés spécialisées dans les solutions globales de sécurité, la sécurité TIC et l'investigation informatique, dont DigiTask et Siemens en Allemagne, FoxIT aux Pays-Bas, Dreamlab Technologies SA en Suisse et Hewlett Packard aux Etats-Unis.

Des documents rendus publics après la chute de plusieurs régimes du monde arabe ont révélé l'existence d'offres concrètes, soumises par certaines de ces entreprises aux anciens potentats. Après la chute du gouvernement égyptien, on a ainsi appris que le groupe anglo-allemand Gamma avait vanté ses produits au régime Moubarak. En Libye, le gouvernement Kadhafi aurait utilisé pour son «Public Safety System and Passport Network» les solutions sur mesure de la société française Amesys.[34] La Syrie emploierait elle aussi des logiciels de surveillance développés par des entreprises TIC occidentales. Outre un logiciel du fabricant allemand Utimaco, qui relie les lignes téléphoniques sous écoute aux ordinateurs de son centre de surveillance, des logiciels d'archivage de messagerie de la société américaine NetApp y sont utilisés. Quant aux techniques de surveillance des réseaux de communication, elles proviendraient de la société française Qosmos. Aucun de ces fabricants n'aurait toutefois directement approvisionné la Syrie.[35]

Dans ce nouveau «scoop», WikiLeaks et divers groupes de défense de la liberté de l'information rappellent qu'un tel transfert technologique au profit d'Etats non démocratiques est non seulement répréhensible sur le plan moral et éthique, mais qu'en plus la participation fournie à la surveillance et donc à l'oppression de la population de ces pays a coûté des vies humaines. Il est vrai qu'ils dénoncent de manière générale la vente de tels produits aux autorités de poursuite pénale, aux services de renseignement et aux armées des pays occidentaux. WikiLeaks souligne clairement dans son éditorial que l'usage de telles solutions

---

33 Art. 269 du code de procédure pénale suisse: www.admin.ch/ch/f/rs/312_0/a269.html (état: 23 février 2012).

34 http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html (état: 23 février 2012).

35 http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html (état: 23 février 2012).

de surveillance des TIC et le marché qui en résulte sont fondamentalement destructeurs, et qu'il manque des dispositions légales permettant de contrôler de telles «armes» numériques. Les entreprises critiquées par WikiLeaks sont actives dans la surveillance informatique et la sauvegarde des données (computer forensics, *lawful interception, data retention*; voir aussi chapitre 5.3).

Il est révélateur que les documents publiés sous l'étiquette «Spy Files» ne concernent que des fournisseurs occidentaux. On n'y trouve pas une seule mention des entreprises asiatiques montantes dont les programmes sont destinés à une surveillance totale, à des missions de renseignement ou plus généralement à la sécurité intérieure, et qui se sont spécialisées dans l'identification des utilisateurs, dans les mesures de censure et la surveillance des réseaux sociaux ou des liaisons cryptées (HTTPS). Or ces nouveaux venus sur le marché de la sécurité n'ont guère de scrupules à vendre des logiciels de sécurité aux Etats intéressés, sans se soucier de l'ordre public qui y règne.

4.9 Stratégies et exercices

Nouvelle stratégie européenne pour la sécurité des réseaux

L'Union européenne a annoncé pour l'année prochaine une «grande stratégie européenne pour la sécurité des réseaux européens». Une lettre aux ministères compétents des Etats membres invite dans un premier temps à passer en revue les «capacités de sécurité» de chaque pays. L'UE estime devoir renforcer son action politique dans ce domaine et entend conférer à l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[36] un rôle-clé dans l'élaboration de sa stratégie.[37]

Exercice de cyber-crise allemand

Le 30 novembre et le 1er décembre 2011, le Ministère fédéral de l'intérieur d'Allemagne a testé pour la première fois la gestion d'une crise nationale déclenchée par des cyberattaques, avec les Länder de Hambourg, Thuringe, Saxe, Hesse et Basse-Saxe notamment. L'opération s'est déroulée dans le cadre de l'exercice LÜKEX (Länder Übergreifende Krisenmanagement-Übung/EXercise), organisé tous les deux ans sur un thème différent afin d'entraîner la collaboration entre plusieurs services fédéraux, les états-majors de crise des Länder ainsi que des entreprises choisies. Le scénario imaginé cette année a confronté les états-majors de crise de l'Etat fédéral et des Länder à une série d'incidents affectant tant les administrations que le secteur privé (attaques massives de *pourriel*s, programmes malveillants, saturation intentionnelle des systèmes). Au total, 2500 personnes provenant de douze Länder se sont prêtées au jeu.

L'exercice visait à tester la coordination entre l'Etat fédéral et les Länder en matière d'analyse des causes des attaques informatiques, ainsi que les mesures de prévention aux échelons tant politique qu'administratif. En outre, il s'agissait de vérifier la coordination des mesures de protection de la population et des réseaux tant commerciaux qu'étatiques, de même que la collaboration entre les organisations publiques et non gouvernementales, à l'échelon fédéral comme dans les Länder. L'exercice fera l'objet d'une évaluation détaillée au cours des prochains mois, avec tous les participants. Le but est d'optimiser la planification de crise et les processus de gestion.[38]

La Suisse, représentée en particulier par des acteurs de la chancellerie fédérale et de la Stratégie nationale pour la protection de la Suisse contre les risques cybernétiques, participait avec un statut d'observateur à l'exercice LÜKEX. Des exercices de conduite stratégique similaires à LÜKEX sont réalisés en Suisse. Le prochain aura également pour thème une attaque cybernétique contre la Suisse. Le Conseil fédéral veut pouvoir vérifier la stratégie nationale de défense cybernétique et, notamment, son concept d'application. L'exercice se déroulera en quatre parties, entre septembre 2012 et mai 2013. Il est destiné

---

36 http://www.enisa.europa.eu (état: 23 février 2012).

37 http://www.heise.de/security/meldung/Neue-EU-Strategie-fuer-Sicherheit-in-den-Netzen-angekuendigt-1394814.html (état: 23 février 2012).

38 Communiqué de presse du Ministère fédéral de l'intérieur d'Allemagne: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/12/luekex.html?nn=109632 (état: 23 février 2012).
Aperçu des exercices précédents: https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/IT-Krisenreaktionszentrum/Uebungen/Beispiele/beispiele_node.html (état: 23 février 2012).

aux états-majors de crise des départements fédéraux ainsi qu'à d'autres organes ad hoc au sein de l'administration fédérale.[39]

Cyber Atlantic

Figure 10: Logo de Cyberatlantic 2011.

Le premier exercice conjoint de cyber-sécurité entre l'UE et les Etats-Unis a été réalisé le 3 novembre 2011 à Bruxelles. D'une durée d'un jour, cet exercice sur table intitulé Cyber Atlantic 2011 avait pour but de déterminer comment l'UE et les Etats-unis coopéreraient en cas de cyberattaques sur leurs infrastructures d'information critiques. Deux scénarios prévoyaient une cyberattaque furtive et ciblée (*advanced persistent threat, APT)* et une perturbation d'un système *SCADA* dans le secteur énergétique. Plus de 20 Etats membres de l'UE ont été impliqués dans cet exercice, dont seize activement. Cyber Atlantic 2011 s'inscrit dans le cadre d'un engagement de l'UE et des Etats-Unis en matière de cybersécurité, déclaré le 20 novembre 2010 au sommet de Lisbonne.[40] La Suisse a participé, avec le statut d'observateur, à l'exercice Cyber Atlantic 2011, qui lui a permis d'acquérir des connaissances utiles pour la coordination internationale des efforts en cas de cyberincident.

39 http://www.news.admin.ch/message/index.html?lang=fr&msg-id=43517 (état: 23 février 2012).

40 http://www.enisa.europa.eu/media/press-releases/le-premier-exercice-conjoint-de-cyber-securite-entre-lue-et-les-etats-unis-a-ete-realise-aujourdhui-le-3-novembre-2011 (état: 23 février 2012).

5 Analyses approfondies et tendances

5.1 SmartGrid et domotique

Comme indiqué aux chapitres 3.9 et 4.2, les *systèmes SCADA* (supervisory control and data acquisition) servent essentiellement à la gestion des centrales électriques ou des systèmes de transport, mais s'emploient toujours plus dans les maisons, les bureaux ou les hôtels, à des fins de gestion du chauffage, de la climatisation et des stores. Des logiciels d'application (*app*) permettent même de commander les installations récentes à partir de tablettes tactiles et de smartphones. Le désir de s'en servir non seulement dans le réseau local protégé, mais de partout via Internet est bien légitime. Dans les appartements de vacances notamment, un système de commande à distance est pratique, p. ex. pour enclencher le chauffe-eau ou rendre la température agréable avant son arrivée, ou simplement pour contrôler à distance que la cuisinière et toutes les lumières aient été éteints et que le chauffage fonctionne de manière irréprochable.

Or là aussi, il faut penser aux questions de sécurité. Les systèmes sont directement reliés à Internet, et donc encourent en principe les mêmes risques que les systèmes informatiques. Comme indiqué au chapitre 3.9, diverses installations de commande d'hôtels ou d'entreprises reliées à Internet avaient conservé leur mot de passe d'origine, par négligence de leur propriétaire. D'où la possibilité pour des tiers d'y accéder et d'en prendre le contrôle. Ce qui paraît anodin à première vue peut avoir de graves conséquences, p. ex. si une personne malveillante coupe le chauffage en plein hiver dans une maison vide, voire désactive le système d'alarme géré par un système domotique.

Les contacts avec les systèmes *SCADA* se développeront dans un autre secteur également. Les bouleversements liés à la sortie à long terme du nucléaire obligeront les entreprises d'approvisionnement énergétique à rechercher des possibilités de garantir la stabilité énergétique, au fur et à mesure que l'énergie de bande d'origine nucléaire se raréfiera et que l'apport irrégulier de courant éolien ou solaire augmentera. Les réseaux de distribution intelligents (*smart grid*) aideront à résoudre le problème. Dans un premier temps, il s'agira de détecter la consommation d'énergie directement auprès du consommateur, afin d'accroître la stabilité du système. Ces données seront transmises à une centrale. Alors qu'une part importante de la consommation de courant fait encore l'objet d'estimations et de valeurs empiriques, il deviendra possible de la cerner précisément et de garantir une meilleure stabilité du système. Or si ces données devaient tomber entre les mauvaises mains ou un compteur électrique intelligent (*smartmeter*) être piraté, une personne mal intentionnée pourrait p. ex. déterminer, à partir de la consommation de courant, si le propriétaire des lieux est chez lui et même manipuler sa facture.

Dans un second temps, des appareils comme les lave-vaisselle ou les lave-linge pourraient être reliés au *smart grid* et contrôlés par lui. Ainsi, le consommateur final signalerait à la centrale qu'il souhaite enclencher son lave-linge. La centrale de commande déciderait du moment le plus opportun pour le mettre en marche.

Il est bien clair qu'un tel système doit être soigneusement protégé, car de fausses manipulations pourraient entraîner, le cas échéant, de graves pannes de courant. Dans le pire des cas, l'approvisionnement énergétique risque un effondrement complet.

5.2 Anonymous – avantages et inconvénients d'une structure ouverte

Anonymous a refait parler de lui ces derniers mois, lors de diverses opérations menées dans le cyberespace. Sur la liste de ses victimes figurent de prestigieuses entreprises, à l'instar de Sony, de la Bank of America ou de la société de sécurité Stratfor (voir chapitre 4.3), et même des organisations criminelles comme la mafia mexicaine de la drogue Los Zetas.

En Suisse c'est surtout l'opération Payback (en franç. représailles) qui a fait des vagues. Même Postfinance en a fait les frais, lors d'une cyberattaque motivée par le blocage du compte de Julian Assange, fondateur de WikiLeaks. Or qui se cache derrière Anonymous et ces attaques? Selon de nombreux témoignages, Anonymous n'est pas une organisation ou un groupe à proprement parler, doté de statuts, d'un règlement d'affiliation et de cotisations à payer. Anonymous représente plutôt une idée ou un mode de vie[41]. Aucune forme spéciale de soutien n'est exigée, chaque «anon» faisant ce qui lui paraît juste. L'avantage d'une telle définition est que les inhibitions à rejoindre Anonymous sont faibles et qu'ainsi, des meneurs peuvent tirer parti d'un mouvement d'humeur contre une entreprise ou un pays, avant même que les participants à de telles actions n'en aient mesuré les conséquences. Mais ce genre de structure n'est pas sans danger – notamment pour la cohérence du mouvement. Comme chaque «anon» décide lui-même de ce qu'il considère approprié, il arrive que soient annoncées ou réalisées des actions auxquelles ne souscrivent pas la majorité, a fortiori la totalité des membres d'Anonymous.

Un exemple illustre bien ce risque de dérive. Anonymous avait annoncé son intention d'attaquer Facebook le 5 novembre 2011 – pour qu'«un maximum d'utilisateurs tournent le dos à Facebook».[42] Les médias en ont abondamment parlé – pourtant il ne s'est rien passé le 5 novembre. L'annonce a lancé un vaste débat non seulement dans la presse, mais aussi dans les rangs d'Anonymous. D'autres «anons» y ont vu les divagations d'un loup solitaire et ont qualifié le projet d'«imaginaire», alors même qu'il y avait de bonnes raisons aux yeux d'Anonymous de lancer une telle opération. Le nom de l'auteur du projet a ensuite été publié, mesure constituant le pire châtiment au sein d'Anonymous.[43]

Les justifications, les démentis et les contre-démentis se sont également enchaîné lors de l'attaque visant Stratfor. Alors que dans un premier temps Anonymous avait revendiqué l'action appelée LulzXmas et invité à faire des versements à de bonnes œuvres à l'aide des données des cartes de crédit dérobées, un démenti a bientôt circulé dans Internet au nom d'Anonymous, avant d'être lui-même démenti. Selon un communiqué ultérieur, l'attaque visait à révéler les contacts noués avec les services secrets et l'industrie d'armement.[44] Le cas Stratfor met en lumière un aspect moins reluisant: des criminels mus par des mobiles purement financiers et sans visions généreuses se servent d'Anonymous comme d'un écran de fumée pour masquer leurs agissements. Les données des cartes de crédit n'ont pas seulement servi à transférer un million de dollars à des organisations charitables. Elles ont aussi été publiées en ligne, où elles étaient librement accessibles à tous les criminels (et au reste du monde) et utilisables à toutes sortes de fins.

---

41 http://www.format.at/articles/1131/524/303276_s1/format-chat-anonymous-mitglied-tvxor (état: 23 février 2012).

42 https://www.taz.de/!81221/ (état: 23 février 2012).

43 http://www.golem.de/1111/87543.html (état: 23 février 2012).

44 http://www.n-tv.de/technik/Hacker-Angriff-gibt-Raetsel-auf-article5086791.html (état: 23 février 2012).

Les liens informels au sein d'Anonymous se sont traduits par une série de cyberattaques non coordonnées, plus ou moins spectaculaires. Comme la structure d'Anonymous ne prévoit ni affiliation ni porte-parole officiel, et que personne ne porte la responsabilité d'ensemble de ce mouvement, un chacun peut en principe lancer des attaques ou publier des communiqués au nom d'Anonymous. Il est par conséquent vain de discuter, après une cyberattaque ou la publication de données, pour savoir s'il s'agit ou non d'Anonymous. Et les lettres de revendication ou les démentis n'ont guère de valeur probante non plus.

5.3 «Bonne» et «mauvaise» surveillance d'Internet

L'analyse qu'a faite le Chaos Computer Club du cheval de Troie appartenant aux autorités de poursuite pénale allemandes, y c. la publication de toutes ses fonctionnalités, a soulevé des débats animés sur son utilisation possible non seulement en Allemagne, mais en Suisse aussi. En outre, WikiLeaks a commencé à publier, le 1er décembre 2011, toutes sortes de documents censés prouver que des entreprises de sécurité privées vendaient des solutions TIC à des Etats autoritaires bafouant les droits de l'homme. Beaucoup de ces solutions, qui relèvent de l'interception légale (*lawful interception*) et de l'investigation informatique, permettent aux autorités d'écouter ou d'enregistrer les conversations des citoyens par Internet ou téléphone mobile, ou d'espionner les données enregistrées sur leurs ordinateurs.

Le vieux débat relancé à cette occasion met en lumière un réel problème lié à Internet, à la société en réseau et aux TIC. L'apparition de possibilités sans cesse nouvelles de communiquer, d'échanger des informations ainsi que de consulter des données en tout temps et de partout, n'est pas sans conséquences: les mesures prises à des fins de localisation et d'acquisition de l'information et, plus généralement, le travail des autorités nationales de sécurité deviennent d'autant plus compliqués. Cette évolution implique par exemple, si un juge a ordonné l'écoute des communications par Skype, l'usage de solutions informatiques – comme des programmes étrangers – sur l'ordinateur des suspects. Les Etats menant une politique répressive à l'égard des opposants politiques n'ont pas tardé à réagir à l'essor des possibilités de communication tant nationales qu'avec l'étranger, en renforçant leurs contrôles centralisés sur les réseaux internes et sur les liaisons internationales. A cet effet, ils utilisent en partie les mêmes produits ou solutions informatiques que les Etats de droit respectueux des individus. La raison tient à ce que sur le plan technique, tant Internet que les ordinateurs et les réseaux fonctionnent partout de la même manière, et donc les solutions mises au point peuvent servir dans n'importe quel pays, indépendamment du contexte juridique.

Les produits informatiques ne sont soumis à aucun contrôle des exportations sur le plan juridique, hormis certaines restrictions frappant le commerce des solutions de cryptage. Une telle mesure serait d'ailleurs difficilement réalisable. D'une part, les solutions logicielles montrées du doigt par WikiLeaks sont presque toujours des biens à double usage (*dual use items*), d'autre part elles consistent en *code* de programme et peuvent donc être transférées en tout temps d'un endroit à l'autre, faute d'existence physique. Ironie du sort, un régime d'exportation obligerait à un contrôle systématique d'Internet et des flux de données.

Comme toutes sortes d'opérations se font toujours plus en ligne, les autorités étatiques chargées de la sécurité sont logiquement à la recherche de solutions informatiques sous une forme ou l'autre. C'est pour elles l'unique manière de continuer à remplir leur mission dans le cadre de l'Etat de droit. Il n'existe certes pas de ligne de séparation nette indiquant à partir de quand l'emploi de telles solutions est illégal selon la conception occidentale de l'Etat. Mais chaque pays est libre d'édicter, pour sa propre industrie des TIC, des règles contraignantes sur le négoce des solutions informatiques, ainsi que de préciser dans sa législation dans quels cas ses autorités peuvent recourir à de tels produits. En Suisse, les travaux correspondants ont déjà été entrepris voire menés à terme, lors de la révision de la

loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[45] et d'autres lois.

5.4 Sécurité à l'ère de la communication mobile – comment protéger son smartphone?

Selon les dernières statistiques[46], plus de quatre millions de téléphones mobiles sont utilisés en Suisse, dont 1,5 million de *smartphones*[47]. Deux systèmes d'exploitation dominent le marché, au niveau mondial comme en Suisse: près d'un appareil sur deux vendu en Suisse est équipé d'iOS d'Apple, alors qu'Android de Google détient 27 % du marché. Ces deux systèmes d'exploitation sont également les plus répandus parmi les tablettes tactiles.

On observe dans ce contexte une convergence croissante entre les systèmes d'exploitation des appareils mobiles et les systèmes d'exploitation «classiques» des ordinateurs de bureau (*desktop*). Il suffit de penser au nouveau système d'exploitation Mountain Lion d'Apple, qui renferme diverses fonctions d'iOS, ou à Windows 8, dont l'interface graphique sera identique au bureau et en version mobile[48]. Ces statistiques montrent qu'on est actuellement dans une phase transitoire, où les systèmes *desktop* sont repris par les systèmes mobiles. Une analyse d'iOS et d'Android aidera à mieux comprendre quel en est l'enjeu pour la sécurité:

- Le système d'exploitation d'Apple est un système propriétaire, ne fonctionnant que sur le matériel de cette société. A moins d'avoir manipulé son iOS[49], un utilisateur peut installer uniquement des applications provenant de l'iTunes-Store, ou à la rigueur des applications internes[50], à condition de participer au programme pour développeurs iOS en entreprise. En effet, chacun peut élaborer des applications pour le système iOS. Avant toute mise sur le marché[51], elles doivent d'abord avoir été analysées et acceptées par Apple. Les applications porteront ensuite la signature d'Apple et seront proposées dans l'iTunes-Store. L'utilisateur n'est toutefois pas habilité à consulter les droits conférés à une application.
- Le système Android repose sur une plate-forme libre (*open source*) utilisant un noyau Linux, et convient au matériel de n'importe quel fabricant. Les applications sont principalement distribuées par Google Play Store (Avant il s'applelait Android Market[52]) – un clic suffit pour leur installation à partir de n'importe quel site[53]. Tout un chacun peut également développer des applications pour Android. A la différence d'Apple, il n'est pas prévu de processus d'examen, et le développeur *signe* lui-même ses applications. L'utilisateur final peut consulter les droits de l'application (à condition de passer du site à Google Play Store; il est caractéristique que les

45 http://www.admin.ch/ch/f/rs/c780_1.html (état: 23 février 2012).
46 http://weissbuch.ch/wb11press.html (état: 23 février 2012).
47 Un smartphone est un téléphone mobile doté de fonctions avancées comme la navigation Web ou le traitement des données personnelles. Les autres téléphones mobiles modernes ne disposent que de quelques fonctions supplémentaires (feature phone). D'où leur moindre complexité.
48 Le prochain système d'exploitation Windows 8 Metro semble avoir renoncé au bouton Démarrer cher aux utilisateurs de Microsoft: http://arstechnica.com/microsoft/news/2012/02/discoverability-windows-8-and-the-disappearance-of-the-start-button.ars (état: 23 février 2012).
49 Dans l'univers iOS, l'opération porte le nom de «jailbreaking» (débridage).
50 Une entreprise peut p. ex. mettre au point son propre App Store à l'aide du programme «iOS Developer Enterprise»: https://developer.apple.com/programs/ios/enterprise/ (état: 23 février 2012).
51 https://developer.apple.com/appstore/guidelines.html (état: 23 février 2012).
52 Le Android Market a été modifié en Google Play le 7 mars 2012
53 Cette procédure porte le nom de «sideloading», ou transfert local direct.

applications installées sur les smartphones ne signalent pas directement les droits requis).

Symantec a récemment publié un rapport[54] sur la manière dont les deux systèmes d'exploitation s'y prennent pour garantir la sécurité de l'utilisateur final. Ce rapport s'articulait en cinq grands points:

1. **Contrôle traditionnel des accès:** besoin p. ex. d'un mot de passe pour accéder au téléphone, ou possibilité pour l'appareil de refuser tout accès après un certain temps d'inactivité.
2. **Provenance des applications:** la *signature numérique* fait principalement foi ici.
3. **Cryptage:** cryptage des données en cas de vol ou perte de l'appareil.
4. **Bac à sable (*sandboxing*):** tentative d'isoler les applications afin qu'elles n'aient accès qu'aux processus requis et ne puissent modifier le système.
5. **Droits des applications:** les applications n'obtiennent que les droits dont elles ont absolument besoin pour remplir leurs fonctions.

Selon le rapport de Symantec, les différences entre les systèmes sont frappantes. Elles tiennent essentiellement à la provenance des applications. Les deux philosophies diffèrent radicalement à ce sujet. Apple assume la responsabilité[55] des applications à installer, sur le plan de la sécurité. Le modèle *open source* d'Android permet par contre aux utilisateurs d'installer n'importe quelle application, mais ni leur fonctionnement ni les droits requis ne sont soumis à des contrôles approfondis et à des restrictions sévères. Il suffit de se rendre sur l'Android Market pour trouver dès la première page des jeux qui exigent des autorisations superflues pour fonctionner. A l'instar p. ex. du droit d'envoyer ou recevoir des *SMS*, de faire des téléphones ou d'accéder aux données personnelles enregistrées sur l'appareil[56].

Autre point sensible, la protection contre les *maliciels* offerte par les appareils mobiles diffère considérablement de celle qui nous est familière par les ordinateurs de bureau. D'où la nécessite de revoir entièrement la protection des appareils mobiles, ou de reprendre les bonnes vieilles solutions des systèmes *desktop*:

- Antivirus:
  Le système d'exploitation des appareils mobiles n'est pas équipé par défaut d'une protection antivirus. Sur iOS, seul Apple est en mesure d'offrir une telle protection, car un antivirus devrait avoir accès à toutes les applications, ce qui n'est pas le cas des applications installées. Elles en sont empêchées par un bac à sable (*sandboxing*) et parce que les droits sont cédés de manière restrictive. Sur Android, les seuls antivirus efficaces sont payants. L'application gratuite de Creative Apps a beau être l'antivirus le

---

54 http://www.symantec.com/podcasts/detail.jsp?podid=b-a-window-into-mobile-device-security (état: 23 février 2012).

55 Dans un cas au moins, révélé par le chercheur américain Charlie Miller, il a été possible de désactiver le dispositif de sécurité de l'App Store et d'y publier une application potentiellement dangereuse: http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (état: 23 février 2012).

56 Un exemple intéressant vient d'Uloops, application permettant de composer des morceaux de musique. Dans la présentation qu'ils en donnent, les développeurs signalent que cette application a accès au statut téléphonique et à l'identité. Elle peut ainsi importer des informations comme le numéro de série du téléphone, le modèle et la marque, le nom d'utilisateur, le mot de passe et l'adresse électronique, sans oublier quantité de données personnelles.
https://market.android.com/details?id=net.uloops.android&feature=featured-apps#?t=W251bGwsMSwxLDIwMywibmV0LnVsb29wcy5hbmRyb2lkIl0 (état: 23 février 2012).

plus répandu, elle n'aurait reconnu aucun des 172 *virus* testés selon une étude réalisée par AVTest[57].

- Pare-feu:
  A ce jour, aucune étude n'a été consacrée aux *pare-feu* des appareils mobiles.
- Mises à jour du système d'exploitation et des applications:
  seuls Apple et quelques fabricants de matériel proposant Android fournissent des mises à jour régulières pour les appareils dont le système d'exploitation n'a pas été modifié (donc sans débridage [*jailbreak*] ni ajustement de la mémoire morte [*ROM*]). La plupart des producteurs de matériel utilisant Google ne sont pas en mesure d'offrir cette prestation. Par conséquent, les éventuelles lacunes de sécurité persisteront jusqu'à ce que l'utilisateur ait acheté un nouvel appareil.

L'utilisateur est ainsi confronté à un dilemme: soit il décide de faire confiance à Apple et de faire partie d'un système fermé[58] n'offrant guère de «liberté», soit il opte pour un système *open source* avec ses avantages et inconvénients[59], son caractère ouvert et son peu de restrictions.

5.5 Conséquences des attaques de fournisseurs de services de certification[60]

L'usage en toute sécurité de systèmes de chiffrement à clé publique (cryptographie à clé publique) repose à chaque fois sur la sécurité offerte par les CSP et les PKI[61]. Par conséquent, la sécurité des CSP et des PKI est un thème dont les techniciens de la sécurité se sont toujours occupés. Ils s'intéressent en particulier à des scénarios qui comportent des certificats falsifiés (via des failles de la résistance aux collisions des fonctions de hachage cryptographique[62]), ou qui se basent sur l'utilisation abusive de certificats de signature de code. Dans le second cas, comme l'a montré le ver Stuxnet, un tel certificat permet p. ex. d'introduire des maliciels dans un système d'exploitation, sous forme de logiciels de pilotage porteurs d'une signature numérique. Or les récentes attaques contre des CSP ont révélé que le piratage d'un CSP dans le but d'émettre de faux certificats représente une réelle menace. Il devient possible de lancer des attaques MITM (*man-in-the-middle*, attaque de l'intermédiaire) de grande envergure, avec de faux certificats pour serveur SSL/TLS. Il aura dès lors le contrôle complet des données transmises, qu'il décryptera à volonté pour en prendre connaissance.

L'émission – comme dans les cas étudiés ici – de faux certificats amène à un double constat:

---

57 http://www.av-test.org/fileadmin/pdf/avtest_2011-11_free_android_virus_scanner_english.pdf (état: 23 février 2012).

58 Outre les avantages et inconvénients respectifs de l'architecture iOS et du modèle de marché, il convient de signaler d'autres surprises, comme l'envoi des coordonnées GPS. Ces données sont transmises à Apple lors de chaque copie de sécurité, à l'insu de l'utilisateur: http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking/ (état: 23 février 2012).

59 Même dans ce cas, d'autres facteurs que l'architecture et le modèle de marché doivent être pris en compte. Android laisse aux fournisseurs de services Internet la possibilité de modifier le système opérationnel ou d'installer des applications avant la mise en vente. Cela vaut p. ex. pour un logiciel développé par Carrier IQ, installé par défaut sur certains appareils Android. Il enregistre en détail le comportement des utilisateurs et communique ces informations à son concepteur: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/ (état: 23 février 2012).

60 Extrait du rapport technique du même nom téléchargeable sous http://www.melani.admin.ch/dokumentation/00123/01132/index.html?lang=fr

61 En ce sens, les CSP et les PKI sont le talon d'Achille de la cryptographie à clé publique.

62 Ce point est approfondi p. ex. dans les considérations technologiques du 4 août 2010 intitulées «Technologiebetrachtung: Kollisionsresistenz und Brechung kryptografischer Hashfunktionen» : http://www.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de

- Premièrement, tous les mécanismes en place de révocation de certificats fondés sur des listes noires (interrogation d'une CRL et/ou requêtes OCSP) sont impuissants face à de tels certificats. Un faux certificat (c.-à-d. émis de façon illégitime) n'est pas nécessairement identifiable comme tel. Pour cela, il faudrait être en mesure de distinguer les certificats autorisés (c.-à-d. émis légitimement) des autres.
- Deuxièmement, il est apparu que le modèle de confiance (centralisé et hiérarchisé) basé sur la recommandation UIT-T X.509 pose problème. Car si dans ce modèle un CSP ou une autorité de certification racine (Root CA) sont compromis, toutes les entités se référant à cette CA en font les frais (au pire des cas tous les internautes). Du point de vue de la sécurité, tout le monde est logé à la même enseigne et la probabilité qu'une Root CA soit compromise est proportionnelle à la longueur de la liste.

Les remarques qui précèdent montrent l'importance des précautions visant à prévenir au mieux, dans l'état actuel des choses, les attaques MITM. Comme il n'existe que peu d'approches pour s'en protéger, on essaiera de rendre ce genre d'attaque aussi difficile et coûteuse que possible pour l'agresseur. A cet effet, il importe de déterminer s'il est possible ou non d'apporter des changements au modèle de confiance.

- A défaut de pouvoir modifier le modèle de confiance, il est recommandé soit de travailler avec des listes vides de Root CA dignes de confiance, soit de ne sélectionner que certaines Root CA. Google offre déjà cette possibilité depuis la version 13 de Chrome («Public Key Pinning»). Une liaison avec le serveur de noms de domaine (DNS) s'impose ici, si l'on souhaite généraliser cette approche à tous les domaines.
- S'il est possible d'apporter des modifications au modèle de confiance, de nouvelles approches entrent en ligne de compte. Il faudrait prévoir un modèle de confiance où l'impact de la compromission serait circonscrit localement. Un tel modèle devrait impérativement être répandu à large échelle et accepter les relations de confiance dynamiques . Des chercheurs de l'université Carnegie Mellon ont par exemple montré que les attaques ont généralement une portée locale. D'où la possibilité de reconnaître les faux certificats selon la localisation géographique des services de notariat.

Comme tout système socio-technique, un CSP a ses points faibles et ses vulnérabilités qu'exploitent (de manière plus ou moins ciblée) des attaques malveillantes. Les procédés et mécanismes cryptographiques utilisés sont moins en cause ici que les interfaces avec les processus d'émission et de délivrance de certificats. Des agressions seraient envisageables et réalisables à ce niveau, comme le prouvent les derniers incidents en date. La comparaison avec un faussaire est ici éclairante: l'escroc peut soit falsifier des billets de banque soit – ce qui est plus compliqué – s'introduire dans un centre d'impression de billets pour émettre de vrais billets avec les machines en place. Il va de soi que la seconde possibilité est plus difficile à réaliser, mais d'autant plus lucrative. Une attaque analogue a abouti entre-temps dans le domaine des PKI et selon toute vraisemblance, ce genre d'attaque se renouvellera. Il vaut donc la peine de tenir compte d'une telle éventualité dans les réflexions sur l'aménagement des futures PKI.

6 Glossaire

.htaccess	.htaccess (en anglais: hypertext access) est un fichier pouvant être placé dans tout répertoire de site Web et servant à gérer les paramètres de configuration.
404 Error Page	Une page d'erreur s'affiche, par exemple, en cas de clic sur un lien Internet obsolète ou suite à une requête portant sur une URL qui n'existe pas. La plupart des navigateurs affichent la page standard fournie par le serveur Web;. L'administrateur de site peut installer individuellement les pages d'erreur.
AcceptPathInfo	Paramètre de configuration du serveur Web Apache.
AdminPanel, interface d'administration	Interface graphique où l'administrateur peut gérer et contrôler les paramètres.
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.
Agent financier	Un agent financier est un intermédiaire légal effectuant des opérations de courtage en devises. Depuis peu, cette notion s'utilise aussi à propos de transactions financières illégales.
Apache Web Server	Logiciel de serveur libre, à code source ouvert, produit par l'Apache Software Foundation; il s'agit du serveur HTTP le plus populaire du Web.
Autorité de certification	Une autorité de certification est une organisation délivrant des certificats numériques. Un certificat numérique peut être vu comme un passeport dans le cyberespace et s'utilise pour identifier par une clé publique une personne physique ou morale. Il est signé par l'autorité de certification, qui atteste ainsi du lien entre l'identité physique et l'identité numérique.
Backup	Un backup (sauvegarde des données) désigne la duplication de données, dont la restauration permettra de retrouver les données perdues.
Base64	Base64 est un codage de l'information utilisant

	64 caractères, choisis pour être disponibles sur la majorité des systèmes. Il permet de transmettre n'importe quel document binaire (application, vidéo, etc.) en pièce jointe en le codant à l'aide de caractères classiques.
Biens à double usage	Produits, y c. les logiciels et les technologies, susceptibles d'avoir une utilisation tant civile que militaire (de l'angl. dual use); notion employée surtout lors du contrôle des exportations.
Blog	Un blog est un type de site Web censé donner régulièrement (web log signifie journal de bord sur le Web) le point de vue de son auteur sous forme de billets (courts textes) ou d'articles (textes plus longs) sur une multitude de sujets.
Bot / Malicious Bot	Du terme slave «robota», signifiant travail. Programme conçu pour exécuter, sur commande, certaines actions de manière indépendante. Les programmes malveillants (malicious bots) peuvent diriger à distance les systèmes compromis et leur faire exécuter toutes sortes d'actions.
Browser	Logiciel utilisé essentiellement pour afficher les différents contenus du Web. Les navigateurs les plus connus sont Internet Explorer, Opera, Firefox et Safari.
Capture d'écran	(en angl. screenshot) Copie du contenu graphique actuel de l'écran.
Certificat numérique	Attestation qu'une entité (personne, ordinateur) possède une clé publique (PKI).
Certificat pour serveur SSL/TLS	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.
Certificat racine	Certificat servant à valider tous les certificats subalternes.
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.
Certification Service Provider (CSP)	Voir Autorité de certification.
Code	Instructions donnant à l'ordinateur les ordres à

	exécuter.
Compteur électrique intelligent	Un compteur électrique intelligent (en angl. SmartMeter) indique à l'utilisateur sa consommation effective d'énergie établie à des intervalles suffisamment courts et transfère ces données à l'entreprise d'approvisionnement en énergie.
Cryptographie symétrique	En cryptographie symétrique, la même clé s'utilise pour chiffrer et déchiffrer les données, (contrairement à la cryptographie asymétrique).
Data Retention	Terme désignant la conservation des données personnelles, requise par les autorités à des fins d'analyse de trafic et de surveillance des télécommunications.
Desktop	Un «desktop computer» ou «desktop» est un ordinateur de bureau.
Dial-Up	Signifie "appeler un numéro" et désigne l'établissement d'une liaison avec un autre ordinateur par l'intermédiaire du réseau téléphonique.
Disque dur	(en angl. hard disk) Support magnétique de stockage des données numériques, constitué de plusieurs plateaux de forme circulaire.
DNS-système	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).
Event-Viewer	Observateur d'événements: programme signalant les événements significatifs relatifs au système d'exploitation Windows, classés comme erreur, avertissement ou informations.
Exploit	(Exploit) Programme, script ou ligne de code utilisant les failles de systèmes informatiques.
Fichier journal	Un fichier journal (log file) regroupe de façon chronologique l'ensemble des événements survenus sur un système informatique. Une ligne est consacrée à chaque action.
Firewall	Un pare-feu (firewall) protège les systèmes informatiques en surveillant et, éventuellement refusant, les connexions entrantes ou sortantes. Un pare-feu personnel (personal firewall ou desktop firewall) est en revanche installé pour protéger un ordinateur unique; il est directement installé sur le système à protéger, c'est-à-dire sur

	votre ordinateur.
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.
Infrastructure à clé publique (Public Key Infrastructure)	Système de gestion des clés de chiffrement et des certificats numériques.
Interception légale	(de l'angl. lawful interception) Terme désignant la possibilité qu'ont les Etats de surveiller à la source les télécommunications (conversations, correspondance, images, vidéos, etc.).
Jailbreak	Le jailbreaking (de l'anglais: évasion), ou débridage, est une opération consistant à outrepasser une restriction à l'utilisation des produits Apple, à l'aide de logiciels adéquats.
Live CD	Un live CD (CD autonome) contient un système d'exploitation exécutable sans installation, qui se lance au démarrage de l'ordinateur.
Malicious Code	Programme malveillant. 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). Voir aussi malware
Man-in-the-Middle attack	Man-in-the-Middle attack, attaque de l'intermédiaire Attaque où le pirate s'immisce dans le canal de communication de deux partenaires pour lire ou modifier les données échangées.
Manipulation d'URL	Les manipulations d'URL permettent à un pirate d'amener un serveur Web à lui délivrer des pages auxquelles il n'est pas censé avoir accès.
Open Source	Open Source est une palette de licences pour des logiciels dont le code source est accessible au public, dans une optique de développement communautaire.
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 de contrôle qui traduit les commandes d'un logiciel afin de permettre à l'ordinateur de communiquer avec un périphérique.
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.
Pourriel (Spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de polluposteur (spammer) et ses envois de pollupostage (spamming).
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.
Recovery	Action de régénérer des données qui ont été perdues ou contaminées; récupération de données.
Restrictions géographiques	Filtre de géo-blocage basé sur l'adresse IP de l'internaute et empêchant d'accéder à certains services en ligne depuis certains pays.
ROM	Read Only Memory. Mémoire dans laquelle les données sont accessibles en lecture, mais pas en écriture.
Root CA	Autorité de certification racine (AC racine), autorité de plus haut niveau dans l'infrastructure à clé publique, certifiant les autorités de certification subalternes.
Router	Dispositif intelligent 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.
Sandboxing	(de l'angl. sandbox signifiant bac à sable) Mécanisme permettant l'exécution de logiciels avec moins de risques pour le système d'exploitation. Souvent utilisé pour du code non

	testé ou de provenance douteuse.
Server	Système informatique offrant à des clients certaines ressources, telles que de l'espace mémoire, et des services (p.ex. courrier électronique, Web, FTP, etc.) ou des données (serveur de fichiers).
Serveur Command & Control	La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C).
Signature numérique	Mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie à la signature manuscrite.
Smart grid	L'expression «smart grid» désigne un réseau de distribution (d'électricité) intelligent, où les donnée de différents appareils (compteurs des consommateurs, etc.) parviennent au producteur grâce aux technologies informatiques. Des ordres peuvent aussi être donnés à ces appareils, selon le réglage du 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.
SQL-Injection	Une injection SQL exploite une lacune de sécurité liée aux banques de données SQL, dès lors que le concepteur du site Web néglige de contrôler les variables utilisées dans les requêtes SQL. Le pirate cherche à exécuter des requêtes non prévues, pour modifier les données voire contrôler le server.
Système de contrôle	Voir SCADA
Système de cryptage	Technique ayant pour but de chiffrer un message, c.-à-d. de le rendre inintelligible pour ceux à qui il n'est pas destiné. La cryptographie permet d'assurer la sécurité des transactions et la confidentialité des messages.
Système de gestion d'immeuble	(en angl. building management system, BMS) Application permettant de visualiser et gérer différents circuits ou sous-réseaux (éclairage, climatisation, intrusion, etc.) à l'aide d'une

	interface utilisateur unique.
Systèmes SCADA	Supervisory Control And Data Acquisition Systèmes servant à la surveillance et à la gestion de processus techniques (p. ex. approvisionnement en énergie et en eau).
Tweet	Court message transmis sur la plate-forme de communication Twitter.
USB	Universal Serial Bus Bus série permettant (avec les interfaces physiques) de raccorder des périphériques tels qu'un clavier, une souris, un support de données externe, une imprimante, etc. Il n'est pas nécessaire d'arrêter l'ordinateur pour brancher ou débrancher un appareil USB. Les nouveaux appareils sont généralement (selon le système d'exploitation) reconnus et configurés automatiquement.
Virus	Programme informatique d'autoréplication, doté de fonctions nuisibles, qui s'installe en annexe d'un programme ou fichier hôte pour se propager.
VoIP	Voice over IP, téléphonie par le protocole Internet (IP). Protocoles souvent utilisés: H.323 et SIP.
X.509	X.509 est une norme de cryptographie UIT pour les infrastructures à clé publique, reposant sur un système hiérarchique d'autorités de certification.