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 2012/I (janvier à juin)

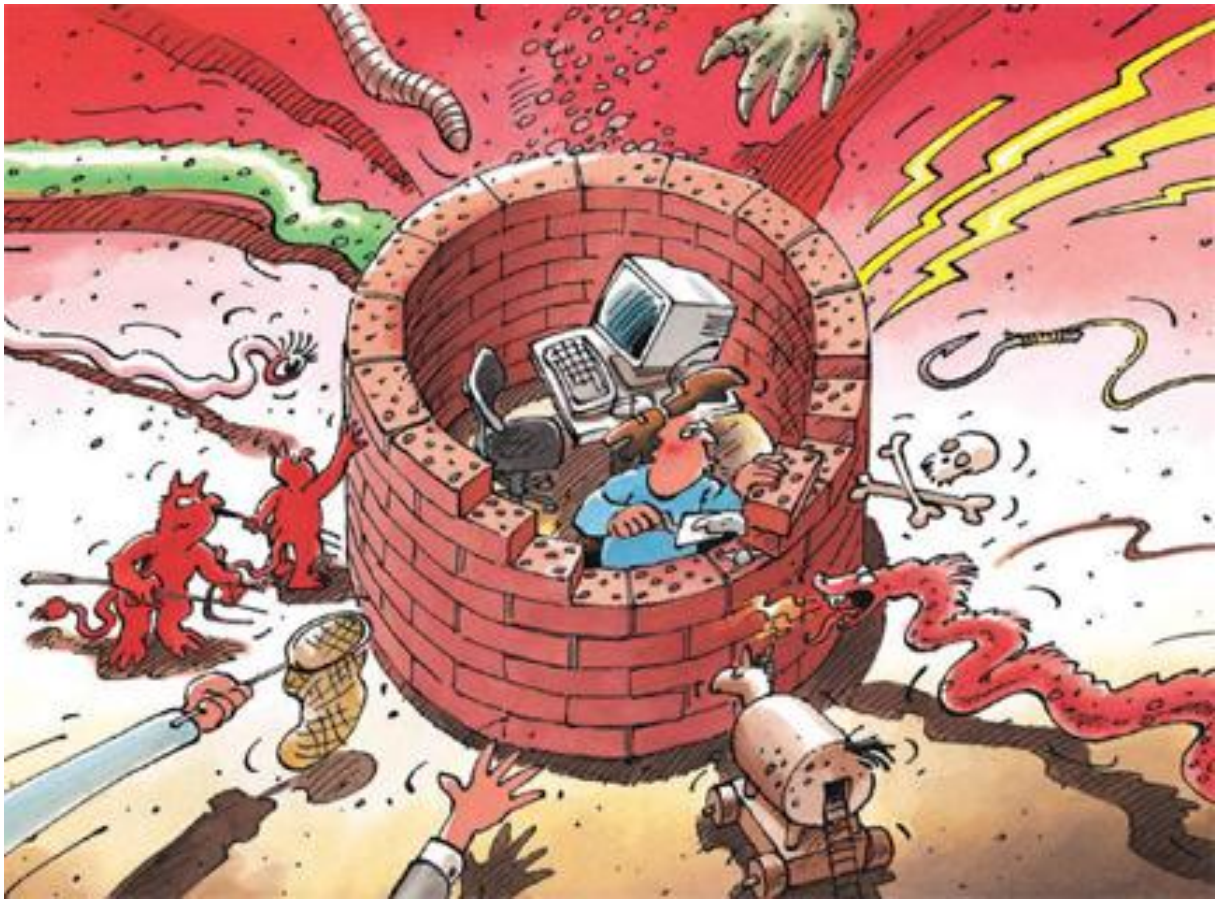


Table des matières

1 Temps forts de l'édition 2012/I

- **Piratage à grande échelle de mots de passe et de données de cartes de crédit**
  Au premier semestre 2012, des attaques de grande envergure ont à nouveau servi à dérober des données de clients (nom d'utilisateur et mot de passe en général), ainsi que des numéros de cartes de crédit à de grandes entreprises. Ces cas parfois très spectaculaires ne doivent toutefois pas faire oublier les attaques quotidiennes lancées contre de plus petites entreprises et leurs données, dont les médias ne parlent guère. Selon une étude de Verizon, plus de 75% des cyberattaques visent des sociétés employant moins de 1000 personnes.

  ► Situation sur le plan international: chapitre 4.5

  ► Tendances / Perspectives: chapitre 5.3

  Variantes de phishing
  La Suisse est tous les jours le théâtre d'attaques de phishing. Dans la plupart des cas, un courriel incite les clients à fournir les données de leur carte de crédit. Comme le montre un cas actuel, les escrocs dépouillent automatiquement les livres d'hôtes et les forums suisses, à la recherche d'adresses électroniques valables vers lesquelles ils envoient les e-mails de phishing. Le voice phishing, ou hameçonnage vocal, est courant en Suisse depuis une année: les victimes reçoivent un appel d'un soi-disant service de support informatique auquel elles sont invitées à livrer leurs données d'ouverture de session. Dès qu'ils se sont emparés des données d'accès à un compte de messagerie, les escrocs expédient de faux appels au secours à tous les contacts du carnet d'adresses piraté.

  Tous ces incidents exigent des entreprises de faire preuve de beaucoup de doigté dans leur communication avec leur clientèle. En cas de non-respect de certaines règles de base propres à la communication d'entreprise, les clients auront tôt fait de confondre une lettre d'information avec un courriel de phishing.

  ► Situation en Suisse: chapitre 3.2, chapitre 3.4, chapitre 3.5, chapitre 3.6

  ► Tendances / Perspectives: chapitre 5.4

  Cyberconflit au Proche-Orient
  L'existence du maliciel complexe Flame, utilisé pour attaquer et espionner des organisations dans plusieurs pays du Proche-Orient, a été rendue publique à la fin de mai 2012. Les analyses techniques menées par des entreprises de sécurité ont révélé des similitudes entre Flame, Stuxnet et Duqu.

  Le printemps arabe a déclenché des conflits ouverts, auxquels fait écho une utilisation agressive et offensive des technologies de l'information et d'Internet. D'où la paralysie temporaire de sites Web, de nombreux vols de documents étatiques ou privés, ainsi que l'usage de maliciels à des fins de sabotage.

  ► Situation sur le plan international: chapitre 4.1, chapitre 4.2

  ► Tendances / Perspectives: chapitre 5.2

- **Evénements dans le domaine des applications de vote électronique**
  A l'ère d'Internet, les citoyens attendent logiquement de l'Etat qu'il leur permette de se prononcer par voie électronique lors des votations et élections. Le e-voting comporte toutefois plusieurs différences de taille par rapport aux autres services électroniques comme le e-banking.

  ► Situation en Suisse: chapitre 3.7

  ► Tendances / Perspectives: chapitre 5.5

- **Stratégie nationale de protection contre les cyberrisques**
  Le Conseil fédéral a approuvé le 27 juin 2012 la stratégie nationale de protection de la Suisse contre les cyberrisques.

  ► Situation en Suisse: chapitre 3.9

2 Introduction

Le quinzième rapport semestriel (janvier à juin 2012) de la Centrale d’enregistrement et d’analyse pour la sûreté de l’information (MELANI) commente les grandes tendances et les risques liés aux technologies de l’information et de la communication (TIC), livre un aperçu des événements survenus en Suisse et à l’étranger, signale divers thèmes de la prévention et résume les activités des acteurs étatiques ou privés. Les termes techniques ou spécialisés (*écrits en italique*) sont expliqués dans un **glossaire (chapitre 6)** à la fin du rapport. Quant aux jugements portés par MELANI, ils figurent à chaque fois dans des encadrés en couleur.

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

Les **chapitres 3 et 4** passent en revue les pannes et les incidents, les attaques, la criminalité et le terrorisme visant les infrastructures TIC. Des exemples choisis illustrent les principaux événements des six premiers mois de l’année 2012. 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 Pannes informatiques du secteur privé et du public

Les fausses manipulations et les défaillances techniques comptent parmi les principales causes de pannes dans les infrastructures de l'information. Les systèmes critiques sont généralement conçus de manière redondante pour éviter toute défaillance. Comme l'ont montré certains incidents survenus dans le passé, les redondances portent généralement leurs fruits en cas de panne de matériel, alors qu'en cas de panne de logiciel le succès est incertain. Sachant que les systèmes redondants comportent plus ou moins le même logiciel et la même configuration, il n'est guère étonnant que lors de la commutation sur le système de secours, des problèmes de logiciel identiques à ceux du système principal apparaissent et que ce système se bloque à son tour.[1] Au premier semestre 2012 également, certaines pannes ont fait grand bruit en Suisse.

Panne informatique dans le canton de Berne

Le 8 mai 2012, une composante centrale du réseau informatique de l'administration cantonale bernoise est tombée en panne et a sérieusement entravé pendant plus de 24 heures les prestations de divers systèmes importants. Par exemple, l'Office de la circulation routière n'a plus été en mesure de répondre aux demandes de renseignements. L'Intendance des impôts a été privée de TaxMe, le service permettant de remplir sa déclaration d'impôt en ligne. De même, le système d'information sur les données relatives aux immeubles (GRUDIS), le *Géoportail*, les données sur le niveau des cours d'eau et des lacs ou encore le recueil des lois étaient indisponibles. Il n'y a toutefois eu aucune perte de données.

L'origine de la panne était une erreur logicielle dans l'infrastructure centrale de stockage (microcode). Cette erreur a notamment entraîné le dysfonctionnement des composants dédoublés du stockage ainsi que la suppression de la redondance de données dans un centre de calcul à distance.[2]

Succursales Coop privées de système de caisse

Le 4 avril 2012, toutes les succursales alémaniques de Coop ont rencontré des problèmes avec leurs systèmes de caisse. Ces derniers n'ont pu être utilisés pendant deux heures. Les magasins sont ainsi restés fermés, et la clientèle qui attendait a reçu des croissants gratuits. La panne était due à l'installation, pendant la nuit, d'une mise à jour logicielle défectueuse, que les tests n'avaient pas détectée.

Ouverture retardée de la Bourse suisse

Vendredi 13 janvier 2012, l'ouverture du négoce a été retardée à la Bourse suisse. Bien que l'erreur a pû être corrigée avant l'heure de négotiation habituelle, le processus de

---

1 MELANI rapport semestriel 2009/1, chapitre 4.6: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=fr (état: 31 août 2012).

2 http://www.be.ch/portal/de/index/mediencenter/medienmitteilungen.meldungNeu.html/portal/de/meldungen/mm/2012/05/20120509_1347_alle_dienstleistungensindwiederverfuegbar (état: 31 août 2012).

redémarrage de tous les partenaires commerciaux a pris plus de temps que prévu, ce qui a provoqué l'ouverture du marché à 12. L'exploitant de la Bourse suisse, SIX, a bien identifié la cause de la panne, mais n'a pas voulu la rendre publique. Selon le communiqué publié par SIX, seuls quelques participants n'ont pas pu exécuter leurs transactions en bonne et due forme. La décision de retarder l'ouverture du négoce a été prise pour ne pas porter préjudice à l'intégrité du marché.

Ce n'est pas la première fois qu'il a fallu interrompre le négoce suite à des problèmes techniques. Le 12 novembre 2009 déjà, la Bourse avait dû fermer ses portes à 15 heures.[3] Les pannes boursières peuvent néanmoins être qualifiées d'incidents rarissimes.

Ces exemples montrent clairement à quel point l'économie – mais aussi les administrations – sont tributaires du bon fonctionnement des TIC. De petites pannes peuvent déjà entraîner de sérieux dommages financiers. D'où l'importance de posséder une infrastructure TIC solide et, surtout, d'être en mesure de réparer au plus vite les dérangements. Selon une étude de 2005 menée par l'EPF de Zurich, une panne nationale d'Internet pendant une semaine pourrait causer en Suisse des pertes économiques se montant à 5,83 milliards de francs.[4] Comme une panne ne peut jamais être exclue, il est indispensable de prévoir pour de telles prestations de service une planification de la continuité opérationnelle.

3.2 Comptes de messagerie piratés – astuce face aux fournisseurs d'accès

On observe depuis plus de trois ans des intrusions dans des comptes de messagerie, commises à partir de données d'accès dérobées aux victimes. Les escrocs inspectent le compte piraté, puis écrivent à tous les contacts du carnet d'adresses ou à ceux paraissant le plus prometteurs. Ces courriels consistent généralement en faux appels à l'aide, dont l'expéditeur prétend être bloqué quelque part à l'étranger après s'être fait voler son argent et son passeport. Enfin, il demande de lui virer immédiatement de l'argent:

«J'espère que mon message t'atteindra rapidement. Excuse-moi de ne pas t'avoir signalé mon voyage en Espagne. Je suis à Madrid et j'ai des problèmes, car j'ai perdu mon porte-monnaie.»

Figure 1: Texte d'un courriel expédié par des escrocs à tous les contacts d'un compte de messagerie électronique compromis.

Les politiciens ne sont pas épargnés, comme le montre l'incident survenu au premier semestre 2012 à Verena Koshy de Köniz. Une personne qui se serait fait pirater son compte de messagerie a beau ne subir aucun préjudice financier direct, un tel incident est irritant et donne énormément de travail – a fortiori si l'on possède un vaste réseau et l'on a mémorisé de nombreux contacts. Beaucoup de personnes ont ainsi reçu un appel au secours censé venir de Madame Koshy. Si l'on découvre un tel incident, il faut s'empresser de prévenir ses correspondants et d'alerter son *fournisseur d'accès*, qui prendra les mesures nécessaires pour que la victime ait à nouveau accès à son compte. Les fournisseurs d'accès réagissent généralement dans un délai de 24 à 48 heures, et le compte piraté échappe ensuite au contrôle des escrocs.

[3] http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Technische-Probleme-legen-Boerse-lahm/story/30392767 (état: 31 août 2012).

[4] http://www.ethz.ch (état: 31 août 2012).

Les escrocs avaient hélas eux aussi prévu qu'un blocage de compte et des mises en garde aux destinataires réduiraient leurs chances de succès. Ils ont par conséquent adopté des contre-mesures et modifié leur façon de procéder au cours des derniers mois: s'ils continuent à dérober les données de contact des comptes piratés, ils modifient entre-temps légèrement l'adresse de l'expéditeur – Meier devenant p. ex. Neier –, pour que les destinataires ne se doutent de rien. Les pirates auront préalablement créé une telle adresse pour commettre leur forfait. Contrairement au compte d'origine restitué à son propriétaire, ils continuent d'y avoir accès et peuvent ainsi communiquer avec les victimes jusqu'à ce que l'escroquerie ait abouti.

Autre nouveauté, les escrocs effacent tous les contacts et tous les courriels apparaissant dans les comptes piratés. Il s'agit d'empêcher le propriétaire d'origine de prévenir par la suite tous ses contacts. Cela peut être particulièrement gênant pour les victimes, qui n'ont généralement pas de sauvegarde (*backup*) de leur liste de contacts. Dans certains cas, le fournisseur parvient encore à sauver les données, mais bien souvent elles sont perdues à tout jamais.

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. L'adresse alternative a généralement été modifiée. Sinon, il est possible d'envoyer un mot de passe de remplacement à cette adresse électronique. En cas de modification de l'adresse alternative, 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	https://www.google.com/accounts/recovery/
Hotmail/ Live	https://account.live.com/resetpassword.aspx
Yahoo	https://edit.europe.yahoo.com/forgotroot
GMX	http://www.gmx.com/forgotPassword.html

3.3 Essor des chevaux de Troie demandeurs de rançons

MELANI avait déjà évoqué les *chevaux de Troie demandeurs de rançons* (*ransomware*) dans son précédent rapport semestriel[5]. Des maliciels utilisés comme moyen de chantage bloquent l'ordinateur de leur victime, avant d'exiger d'elle le versement d'une rançon. Cette forme de maliciel apparue en Allemagne au printemps 2011 arborait le logo de l'Office

[5] MELANI rapport semestriel 2011/2, chapitre 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 31 août 2012).

fédéral de la police criminelle, ce qui lui a valu le surnom de «BKA-Trojaner».[6] D'où un risque de confusion avec le *cheval de Troie des autorités de poursuite pénale allemandes*.

Les premières versions suisses de ce cheval de Troie ont été envoyées l'automne dernier au nom du Département fédéral de justice et police (DFJP). Un autre type de *cheval de Troie demandeur de rançon*, apparu au début de mars 2012, prétend provenir de la coopérative des auteurs et éditeurs de musique SUISA, qui gère les droits d'auteur en Suisse.[7] Depuis juin 2012, une version circule au nom d'un organisme fictif, le «Cyber Crime Investigation Department». Ce maliciel active même la webcam de l'ordinateur bloqué, afin de mieux intimider la victime.

Les maliciels exigent de leur victime le paiement d'une amende, généralement via le service de paiement en ligne Paysafe.

La société Paysafecard, émettrice des cartes à prépaiement utilisées par les escrocs, a réagi à cet abus et imprimé une mise en garde sur les cartes Paysafe.

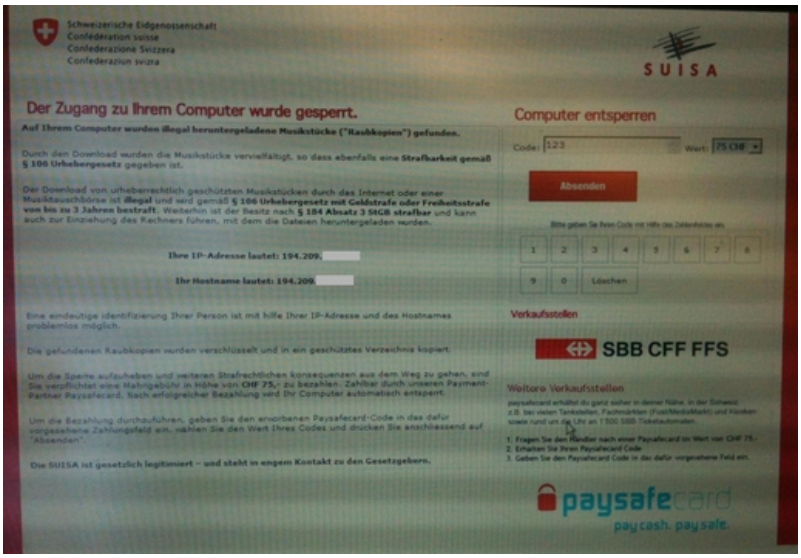


Figure 2: Cheval de Troie demandeur de rançon au logo de SUISA.

Figure 3: Cheval de Troie demandeur de rançon au logo de la Confédération suisse.

[6] Voir http://www.bka-trojaner.de: ce site présente les diverses versions du cheval de Troie (état: 31 août 2012).

[7] http://www.suisa.ch (état: 31 août 2012).

Depuis l'apparition en Suisse des premiers chevaux de Troie demandeurs de rançons, des cas d'ordinateurs bloqués sont régulièrement signalés à MELANI. L'infection provient généralement de portails vidéo ou de sites diffusant des contenus multimédia. On peut penser qu'elle se propage par des fichiers vidéo infectés ou par des logiciels corrompus de lecture vidéo.

Une infection avec blocage de l'ordinateur cause dans tous les cas des désagréments, surtout s'il s'agit d'ordinateurs professionnels dont de petites entreprises ont absolument besoin et que l'on ne peut se contenter de remplacer par d'autres.
MELANI a connaissance de tels cas.

MELANI connaît aussi des cas où le blocage a pu être aisément contourné: il est parfois possible d'y échapper en arrêtant le système, puis en le relançant sans liaison Internet.

3.4 Voice Phishing (Vishing)

La Suisse a été épargnée par le *voice phishing*, ou hameçonnage vocal, jusqu'à l'été 2011. Le dernier rapport MELANI a évoqué en détail cette arnaque toujours plus fréquente.[8] La technique des escrocs est presque toujours la même: un appel émanant d'une prétendue société de services informatiques (généralement Microsoft) annonce à la victime que son ordinateur envoie des messages suspects. A titre de preuve, la personne appelée reçoit des instructions pour appeler le logiciel *Event-Viewer* (observateur d'événements), qui signale tous les événements significatifs relatifs au système d'exploitation. 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 son ordinateur, en téléchargeant un programme d'accès à distance. Le cas échéant, ils auront les mêmes possibilités de manipuler l'ordinateur qu'en étant directement assis devant lui. Enfin, les escrocs cherchent généralement à vendre une licence de logiciel ou une prestation de service («nettoyage de système») et exigent à cet effet les données d'une carte de crédit.

Au cas où l'on aurait réagi à un tel appel téléphonique et révélé aux escrocs les données de sa carte de crédit, il est essentiel de la faire aussitôt bloquer.

Le cas échéant, il est difficile d'évaluer ce que les escrocs ont fait ou installé sur l'ordinateur. S'ils y ont téléchargé un programme d'accès à distance, ils auront les mêmes possibilités de manipuler l'ordinateur qu'en étant directement assis devant lui (duplication/modification/ suppression de données, installation de programmes, etc.). Les escrocs installent souvent aussi une «porte dérobée», pour s'introduire plus tard à volonté dans le système.

Après une telle mésaventure, il est recommandé de faire examiner son ordinateur 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 et à réinstaller le système d'exploitation. D'où l'importance de sauvegarder systématiquement au préalable ses données personnelles, afin d'éviter toute perte.

[8] MELANI rapport semestriel 2011/2, chapitre 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 31 août 2012).

En outre, une fois l'ordinateur nettoyé et réinstallé (ou en cas de changement d'ordinateur), il importe de modifier les mots de passe de tous les services Internet utilisés jusque-là.

Hameçonnage vocal au nom de Swisscom

En juillet 2012, un courriel a été mis en circulation au nom de Swisscom. Les victimes y étaient informées en français et en mauvais allemand que leur compte avait été suspendu. A la différence des courriels classiques de *phishing*, il fallait non pas indiquer son nom d'utilisateur et son mot de passe, mais appeler le numéro de téléphone indiqué pour en apprendre davantage. Le numéro en question, possédant le préfixe 0088, appartient à un opérateur de téléphonie par satellite. D'où une facture téléphonique salée en cas d'appel. MELANI ignore si les victimes ayant appelé ce numéro ont été invitées à révéler leur nom d'utilisateur et leur mot de passe. Pour les comptes email de Swisscom, ces messages de phishing ont été bloqués à temps.


Gesendet: Dienstag, 10. Juli 2012 01:19

Betreff: Sie haben 1 neue Nachricht / Vous avez 1 nouveau message

Ihr Konto ist gehemmt worden.

Für mehr Informationen erreichen Sie uns unter der Telefonnummer:
00881835211648 oder 00881835211650

Votre compte a été suspendu.

Pour de plus amples informations, vous pouvez appeler le numéro de téléphone:
00881835211648 ou 00881835211650

Figure 4: Courriels expédiés en juillet 2012 au nom de Swisscom.

3.5 Comment les cybercriminels accèdent aux adresses électroniques

Une adresse électronique peut aboutir de plusieurs manières à une base de données de polluposteurs. L'une de ces possibilités réside dans l'épluchage automatique d'Internet à la recherche d'adresses électroniques valables publiées sur des sites (forums, livres d'hôtes, etc.). Quand une adresse a abouti à une telle base de données, les criminels s'en servent à de multiples reprises et la revendent souvent à d'autres escrocs.

Les exploitants de forums ou livres d'hôtes sous-estiment souvent – ou refusent d'assumer – leur rôle dans ce contexte. En effet, les adresses électroniques figurent en toutes lettres dans la plupart des livres d'hôtes, où les criminels peuvent très facilement les extraire avec les outils nécessaires.

L'analyse d'une vague actuelle de courriels de phishing montre que ces sources sont bel et bien exploitées. En l'occurrence, les adresses électroniques utilisées par les escrocs ont permis de remonter aux livres d'hôtes de sites Internet suisses. Certains se sont révélés être une mine d'or pour les collecteurs d'adresses. A commencer par le site d'un musicien suisse, publiant en toutes lettres plus de 2700 adresses électroniques. Autre réel avantage pour les escrocs, ces adresses électroniques ont de fortes chances d'appartenir à des citoyens suisses ou du moins à des germanophones. De telles informations se prêtent à des envois de courriels de phishing ciblés et accroissent ainsi la probabilité que l'attaque fonctionne.

MELANI recommande de s'entourer des précautions suivantes lors de l'inscription d'adresses électroniques dans les livres d'hôtes et les forums:

Administrateurs de sites:

- Il est souvent superflu de publier l'adresse électronique, qui sert uniquement de moyen d'authentification pour l'administrateur de site. Le cas échéant, mieux vaut renoncer à une telle publication.
- Si une publication s'impose en vue d'une prise de contact, n'indiquez pas en toutes lettres les adresses électroniques. Vous avez différents moyens d'empêcher, p. ex. à l'aide de JavaScript, toute sélection automatique de vos adresses électroniques.
- La solution la plus efficiente consiste à ne pas publier l'adresse et à proposer à la place un formulaire Web (dûment sécurisé) permettant une reprise de contact.

Utilisateurs

- Ne communiquez votre adresse électronique qu'aux personnes nécessaires, et utilisez-la exclusivement pour la correspondance importante.

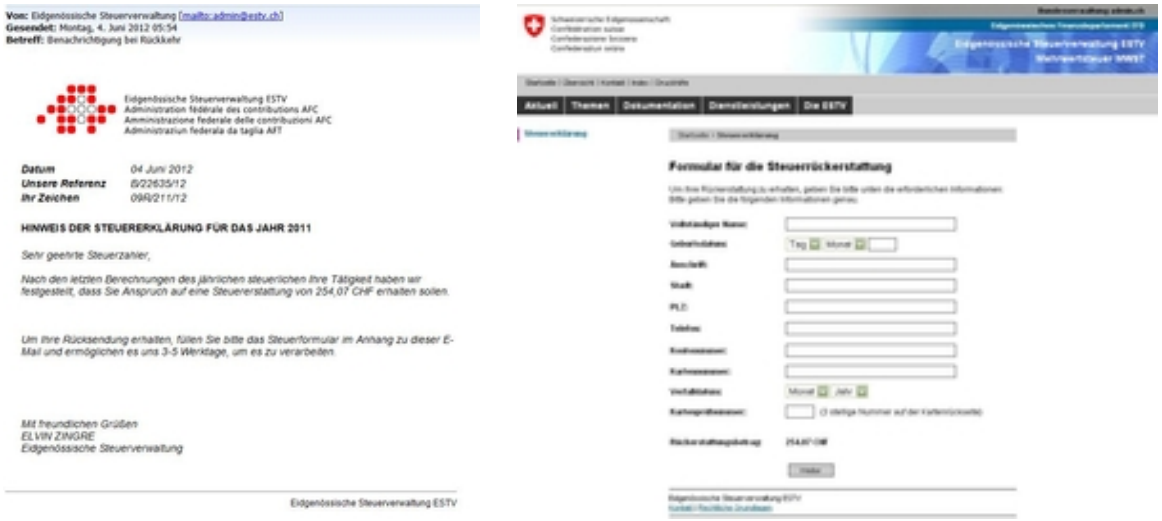
3.6 Courriels de phishing – prétendus remboursements d'impôts par l'AFC

Les escrocs usent d'astuce pour tromper la vigilance des autorités chargées de prévenir les attaques de *phishing*. MELANI en a déjà parlé dans le dernier rapport semestriel.[9] Une arnaque récente est décrite ci-après.

Lundi 4 juin 2012, des courriels de *phishing* ont été expédiés au nom de l'Administration fédérale des contributions (AFC). L'envoi faisait miroiter un remboursement d'impôt. Un formulaire *HTML* était annexé. Il fallait y indiquer ses coordonnées personnelles et les données de sa carte de crédit. A la différence des courriels classiques de *phishing*, qui invitent la victime à cliquer sur un lien et à saisir sur la page Web ainsi appelée des informations personnelles et les données de sa carte de crédit, la page *HTML* figurait directement en *annexe* du courriel. Une fois ouverte, elle s'installait localement sur l'ordinateur du destinataire. Un clic sur le bouton «continuer» avait pour effet d'envoyer le formulaire complété directement au pirate.

Cette approche présente un réel avantage pour l'escroc. Il n'aura pas besoin, pour placer sa page de phishing, d'un *serveur Web* piraté ou spécialement créé, qui risquerait d'être désactivé par les autorités chargées de la sécurité ou par l'*hébergeur*. Toutes les informations correspondantes figurent en effet dans l'*annexe*. Il suffit d'un script *PHP-Mailer*, que l'on trouve par milliers sans protection sur le réseau, pour expédier un tel message de phishing à toutes les adresses électroniques souhaitées. Il va de soi qu'il est plus difficile de bloquer ou détecter de tels publipostages.

[9] MELANI, rapport semestriel 2011/2, chapitre 3.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 31 août 2012).



Von: Eidgenössische Steuerverwaltung [mailto:admin@estv.ch]
Gesendet: Montag, 4. Juni 2012 05:54
Betreff: Benachrichtigung bei Rückkehr

Eidgenössische Steuerverwaltung ESTV
Administration fédérale des contributions AFC
Amministrazione federale delle contribuzioni AFC
Administraziun federala da taglia AFT

Datum 04 Juni 2012
Unsere Referenz IS/22635/12
Ihr Zeichen 09R/211/12

HINWEIS DER STEUERERKLÄRUNG FÜR DAS JAHR 2011

Sehr geehrte Steuerzahler,

Nach den letzten Berechnungen des jährlichen steuerlichen Ihre Tätigkeit haben wir festgestellt, dass Sie Anspruch auf eine Steuererstattung von 254,07 CHF erhalten sollen.

Um Ihre Rücksendung erhalten, füllen Sie bitte das Steuerformular im Anhang zu dieser E-Mail und ermöglichen es uns 3-5 Werktage, um es zu verarbeiten.

Mit freundlichen Grüßen
ELVIN ZINGRE
Eidgenössische Steuerverwaltung

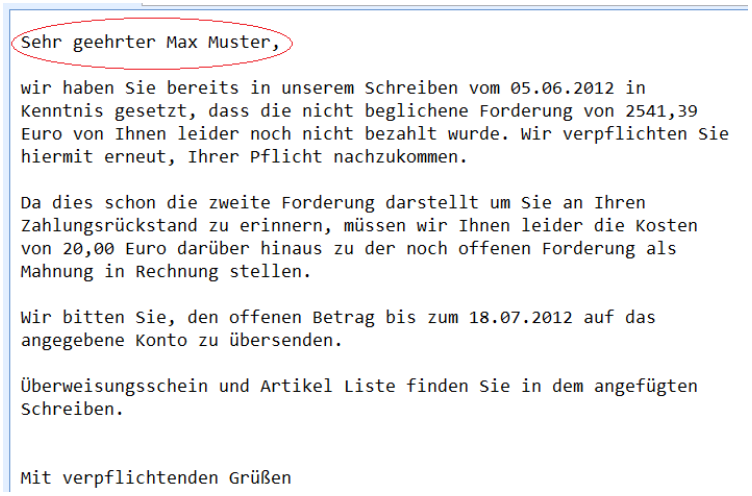
Eidgenössische Steuerverwaltung ESTV

Aktuell | Themen | Dokumentation | Dienstleistungen | Die ESTV

Formular für die Steuerrückerstattung

Figure 5: Courriel de phishing avec masque de saisie annexé.

Pendant longtemps, on aurait attendu des courriels de subversion psychologique qu'ils s'adressent personnellement au destinataire, afin d'inspirer confiance à la victime. Or étonnamment, cela n'a été le cas jusqu'ici qu'à titre exceptionnel. Une vague de pourriels envoyée en 2012 pour répandre un maliciel figurant dans l'*annexe* constitue un bon exemple d'utilisation de cette méthode:



Sehr geehrter Max Muster,

wir haben Sie bereits in unserem Schreiben vom 05.06.2012 in Kenntnis gesetzt, dass die nicht beglichene Forderung von 2541,39 Euro von Ihnen leider noch nicht bezahlt wurde. Wir verpflichten Sie hiermit erneut, Ihrer Pflicht nachzukommen.

Da dies schon die zweite Forderung darstellt um Sie an Ihren Zahlungsrückstand zu erinnern, müssen wir Ihnen leider die Kosten von 20,00 Euro darüber hinaus zu der noch offenen Forderung als Mahnung in Rechnung stellen.

Wir bitten Sie, den offenen Betrag bis zum 18.07.2012 auf das angegebene Konto zu übersenden.

Überweisungsschein und Artikel Liste finden Sie in dem angefügten Schreiben.

Mit verpflichtenden Grüßen

Figure 6: Exemple de courriel avec un logiciel malveillant et un appel personnel

En principe, aucune entreprise sérieuse ne sollicite l'envoi de mots de passe ni n'invite ses clients par courriel à vérifier ou actualiser leurs données de carte de crédit ou de compte et d'autres informations personnelles encore. De tels courriels émanent en règle générale d'escrocs. Ceux-ci imaginent régulièrement de nouveaux scénarios pour amener leurs destinataires à leur répondre sans réfléchir. Le chapitre 5.4 «Communication avec la clientèle à l'ère du *phishing*» approfondit cette question.

Ne suivez en aucun cas les instructions figurant dans des courriels suspects inattendus ou émanant d'expéditeurs inconnus, n'ouvrez pas leurs annexes et ne cliquez sur aucun hyperlien, mais effacez le message.

3.7 Evénements dans le domaine des applications de vote électronique

En effet, la démocratie directe est l'un des plus précieux acquis de la Suisse. La possibilité de voter par voie électronique (e-voting) est un enjeu d'actualité. Ses avantages sont évidents: la participation aux processus de formation de la volonté politique, aux votations populaires notamment, cesse d'être tributaire des horaires d'ouverture des locaux de vote et peut être garantie dans le monde entier.

Il n'est guère surprenant qu'outre la Suisse, de nombreux pays – comme la Norvège, l'Estonie ou la France – procèdent à des essais très prometteurs de vote électronique.

Des rumeurs de manipulation risquent toutefois d'ébranler la confiance accordée au vote électronique et d'en compromettre durablement l'essor. Or de banales attaques *DDoS* risquent déjà d'être lourdes de conséquences et de retarder, voire d'empêcher la tenue d'un scrutin démocratique. Le chapitre 5.5 revient plus en détail sur ce thème.

Au premier semestre 2012, les systèmes de vote électronique ont essuyé des péripéties dont plusieurs exemples sont exposés ci-dessous:

Vote surnuméraire lors d'un scrutin en ligne en Suisse

A l'issue de la votation fédérale du 11 mars 2012, on a appris que le vote d'un électeur inscrit dans le canton de Lucerne avait involontairement été enregistré deux fois, en raison d'une erreur de logiciel. L'anomalie avait aussitôt été décelée et les spécialistes avaient écarté le bulletin surnuméraire. Le communiqué concluait qu'il n'y avait jamais eu lieu de douter de l'exactitude du résultat final, et que le secret du vote avait été préservé en tout temps[10].

Attaque DDoS contre un scrutin du Nouveau Parti démocratique canadien

L'élection à la direction du Nouveau Parti démocratique canadien prévoyait une procédure en ligne à plusieurs tours. Des dizaines de milliers de membres du parti ont voté en ligne de chez eux. Or pendant l'élection, les serveurs ont subi une attaque *DDoS* qui a retardé les opérations. Le délai de vote a été reporté à plusieurs reprises, et il a même fallu interrompre et refaire un des tours de scrutin. Cet incident a sans doute découragé une partie des ayants droit de participer au scrutin.

Piratage d'un projet pilote d'e-voting à Washington D.C.

En mars 2012, des chercheurs de l'Université du Michigan ont signalé qu'il leur avait fallu très peu de temps pour désactiver les fonctions de sécurité d'un projet pilote de vote par Internet en phase de test à Washington D.C. En moins de 48 heures, ils avaient accédé aux commandes du serveur gérant les élections en ligne. Ils étaient parvenus à modifier tous les votes, ainsi qu'à identifier les électeurs réels. L'intrusion n'avait été détectée que deux jours plus tard, et encore seulement parce que les chercheurs avaient volontairement laissé un indice flagrant sur le serveur.

E-voting: règlement annulé par la Cour constitutionnelle autrichienne

La Cour constitutionnelle autrichienne a qualifié d'illégal le règlement sur le vote électronique adopté en 2009 par l'Union nationale des étudiants autrichiens (ÖH), qui ne définissait pas avec une précision suffisante les contrôles permettant de s'assurer du fonctionnement

[10] http://www.ge.ch/evoting/scrutin_20120311.asp (état: 31 août 2012).

irréprochable du système. Selon le ministère de l'Intérieur autrichien, la décision n'a pas de signification révolutionnaire, parce que le vote électronique pour les élections fédérales devrait d'abord être ancré en droit constitutionnel. Or la majorité constitutionnelle requise à cet effet est loin d'être assurée aujourd'hui en Autriche.[11]

3.8 Maliciel utilisant un certificat d'une société suisse

Plusieurs versions du maliciel Mediyes[12], apparues entre décembre 2011 et mars 2012, étaient signées par un *certificat avec clé privée de chiffrement* appartenant à une société du nom de Conpavi AG basée en Suisse centrale. Conpavi se présentait sur son site comme partenaire de la ville de Lucerne et de la haute école spécialisée bernoise pour des projets de cyberadministration.

La société anonyme Conpavi a beau exister et être inscrite au registre du commerce, son but est de fournir des services et de commercialiser des produits dans le secteur pharmaceutique. Elle n'a donc rien à voir avec la cyberadministration. S'agit-il pour autant d'une société écran créée à dessein par des escrocs, comme certains médias l'ont affirmé?[13]

La réalité est moins simple. Un coup d'œil à archive.org, projet d'archivage électronique mené par l'organisation *Internet Archive*, révèle que le site conpavi.ch a été créé en 2002.

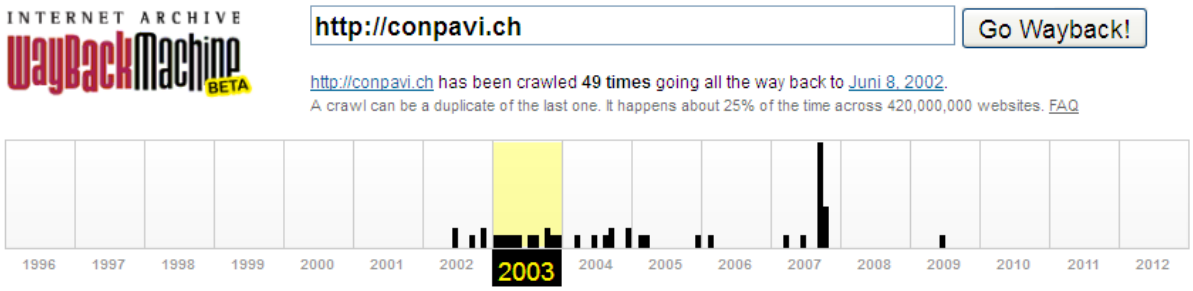


Figure 7: Indexation du site de la société Conpavi par archive.org.

Il ressort d'un examen plus approfondi du registre du commerce que l'entreprise a été créée le 20 mars 2000 sous le nom netauc et rebaptisée conpavi le 11 décembre 2001. Elle avait pour but de fournir des prestations liées aux moyens de communication électroniques, notamment de conseiller les collectivités publiques sur les questions touchant à Internet.[14] Le

---

11 http://www.heise.de/newsticker/meldung/Oesterreichs-Verfassungsgerichtshof-hebt-E-Voting-auf-1400214.html (état: 31 août 2012).

12 Le maliciel Mediyes repose sur le modèle de fraude au clic. Il intercepte les requêtes adressées par la victime aux moteurs de recherche Google, Yahoo et Bing, pour les rediriger vers un serveur d'un réseau de bannières publicitaires.

Des agences de publicité en ligne proposent des fonctions de recherche aisées à intégrer à un site Web, pour permettre aux exploitants de sites intéressés d'afficher facilement de la publicité et de gagner ainsi de l'argent. Chaque fois qu'un visiteur effectue une recherche à partir d'un mot-clé, il voit apparaître, en plus du site désiré, une bannière publicitaire. Et s'il clique sur cette bannière, l'exploitant du site reçoit de l'argent.

C'est là-dessus qu'ont misé les escrocs. Ils ont utilisé les requêtes proposées pour faire s'afficher (sur le site Web spécialement créé par eux) de telles bannières et s'enrichir en cliquant automatiquement à l'arrière-plan sur l'hyperlien à caractère commercial s'y trouvant.

13 http://www.nzz.ch/aktuell/startseite/zuger_scheinfirmaauf_krummer_tour_im_internet-1.16001018 (état: 31 août 2012).

14 http://www.zefix.admin.ch (état: 31 août 2012).

16 juin 2009, Conpavi a été transformée en société fournissant des services et commercialisant des produits dans le secteur pharmaceutique. Or le site Web de l'ancienne société a été maintenu tel quel, avec la description de ses prestations. D'où d'une plate-forme idéale pour des criminels souhaitant commettre des escroqueries et obtenir des *certificats*. Quiconque n'avait pas examiné les faits en détail pouvait croire que l'entreprise existait encore et s'occupait de *cyberadministration*. C'est apparemment ce qui a permis de convaincre les organismes de certification d'émettre le *certificat* en cause.

Les escrocs cherchent par tous les moyens à rendre leurs agissements crédibles aux yeux de leurs victimes. Il arrive donc régulièrement qu'après une dissolution d'entreprise, ils s'emparent de sa raison sociale ou de son site Internet pour leurs malversations. Les liens menant à de tels sites Web continuent d'exister et une recherche via Google ne signale pas la présence d'activités suspectes. Bien souvent, les pirates récupèrent également le *nom de domaine,* une fois que la société l'a effacé ou a cessé d'en prolonger l'enregistrement. Ils héritent ainsi de la réputation que l'entreprise s'était acquise jusqu'à sa liquidation ou à son changement de but ou de raison sociale.

3.9 Adoption d'une stratégie nationale de protection contre les cyberrisques

A sa séance du 27 juin 2012, le Conseil fédéral a approuvé la stratégie nationale de protection de la Suisse contre les cyberrisques.[15] A cet effet il s'est notamment prononcé pour un renforcement, dès 2013, du personnel de MELANI au DFF et au DDPS. Ladite stratégie apporte également une réponse à diverses interventions parlementaires réclamant des mesures renforcées contre les cyberrisques.

Les objectifs stratégiques poursuivis par le Conseil fédéral sont les suivants:

- détection précoce des menaces et des dangers dans le cyberespace;
- augmentation de la capacité de résistance des infrastructures critiques;
- réduction efficace des cyberrisques liés en particulier à la cybercriminalité, au cyberespionnage et au cybersabotage.

La stratégie désigne les organes fédéraux responsables, dans le cadre de leur mission de base, de réaliser d'ici à fin 2017 les seize mesures proposées dans la stratégie. Ce processus fait appel à des partenaires choisis dans les milieux politiques, économiques et sociaux. Un organe de coordination basé au DFF vérifiera la mise en œuvre des mesures prévues et la nécessité de prendre d'autres dispositions afin de réduire les risques.

La collaboration active entre les secteurs privé et public, ainsi que la coopération avec l'étranger, sont déterminantes pour réduire les cyberrisques au strict minimum. L'échange permanent d'informations doit assurer la transparence et la confiance, tandis que l'Etat restreindra ses interventions aux cas où l'intérêt public est en jeu, selon le principe de subsidiarité.

Selon la stratégie formulée, la lutte contre les cyberrisques a sa place dans tout processus global d'affaires, de production ou administratif, et il convient d'y associer tous les acteurs – du personnel technique aux cadres dirigeants. Ainsi, il incombe à chaque entité politique, économique ou sociale d'identifier ses tâches et ses responsabilités dans le cyberespace, ainsi que de tenir compte des risques qui s'ensuivent dans ses processus, voire si possible

[15] http://www.news.admin.ch/message/index.html?lang=fr&msg-id=45138 (état: 31 août 2012).

de les neutraliser. Concrètement, les structures décentralisées de l'administration et de l'économie seront renforcées pour assumer ces tâches, en exploitant au mieux les ressources et les processus en place. Car il est nécessaire de collecter en permanence les informations de nature technique ou non, afin d'analyser et d'évaluer en détail les cyberrisques. Les résultats ainsi obtenus feront l'objet, dans la mesure du possible, d'un traitement centralisé et seront transmis aux acteurs concernés pour les soutenir dans leurs propres processus de gestion des risques.

La stratégie souligne que les cyberrisques sont essentiellement liés aux tâches et responsabilités assumées dans le cyberespace. D'où la nécessité de les envisager dans le cadre des processus existants de gestion des risques. Il s'agit en priorité de mettre à disposition des responsables de solides informations sur les cyberrisques, ainsi que de les sensibiliser à cet enjeu. A cet effet, le Conseil fédéral a chargé les départements de s'atteler à la mise en œuvre des mesures proposées, dans leurs domaines de compétences respectifs ou en partenariat avec les cantons et le secteur privé. L'éventail des mesures va de l'analyse des risques inhérents aux infrastructures TIC à la défense active des intérêts helvétiques au niveau international.

Autrement dit, le Conseil fédéral reconnaît qu'une bonne collaboration est généralement en place entre l'Etat et le secteur privé. Sa stratégie nationale de protection de la Suisse contre les cyberrisques vise à approfondir ces liens dans le cyberespace et à consolider les bases existantes, dans l'optique d'une réduction ciblée des cyberrisques. Il met ainsi l'accent sur les structures existantes et renonce à créer un organe central de pilotage et de coordination comme l'ont fait d'autres pays ou la collaboration est moins développée entre les différents acteurs impliqués. Il s'agira à la place d'intensifier les flux d'information et de diffuser au plus près des besoins des évaluations à jour des cyberrisques et des cybermenaces, afin de soutenir les autorités, les milieux économiques et les exploitants d'infrastructures critiques. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI sera renforcée à cet effet.

4 Situation internationale de l'infrastructure TIC

4.1 L'Iran dans le collimateur? Flame et Wiper

Le 28 mai 2012, Kaspersky Lab a annoncé la découverte d'un maliciel complexe, utilisé pour attaquer et espionner des organisations dans plusieurs pays. Ses fonctions incluent la collecte d'informations en tous genres. Par exemple, il peut surveiller le trafic réseau, enregistrer les frappes clavier, faire des copies d'écran ou des enregistrements audio, et même lire via *Bluetooth* les carnets d'adresses des téléphones mobiles situés à proximité, pour autant que leur fonction Bluetooth soit activée. Le maliciel du nom de Flame a sévi notamment au Moyen-Orient. Près de la moitié des infections attestées concernent l'Iran. Les premières versions datent de 2006 – autrement dit le réseau d'espionnage a agi dans l'ombre pendant plus de cinq ans. Notamment parce que les agresseurs n'infectaient que quelques dizaines de systèmes à la fois et veillaient toujours à supprimer Flame après s'être procuré des données sur les systèmes piratés. Et quand la découverte du maliciel par Kaspersky Lab a été rendue publique, ils ont logiquement désactivé l'infrastructure de contrôle de leur réseau d'espionnage pour effacer toute trace.

Plus de 80 *noms de domaine* ont été enregistrés durant l'attaque pour l'infrastructure de contrôle. Les serveurs utilisés se trouvaient un peu partout dans le monde, à Hong Kong, au Vietnam et en Turquie, mais aussi en Allemagne, en Grande-Bretagne ou en Suisse.

Flame s'est propagé par des clés USB et des réseaux locaux. En cas d'infection par clé USB, la faille de sécurité utilisée était la même que dans le cas de Stuxnet. Les analyses techniques menées par des entreprises de sécurité ont révélé d'autres similitudes entre Flame, Stuxnet et Duqu.[16]

Un maliciel du nom de Wiper, qui a perturbé en avril 2012 les réseaux de communication du ministère iranien du pétrole, espionné les données en circulation et anéanti les disques durs des systèmes infectés. Pour enrayer la progression de Wiper et à titre de mesure de sécurité, les systèmes informatiques du ministère du pétrole et de divers terminaux pétroliers iraniens ont été déconnectés d'Internet dans l'intervalle.

Ces attaques confirment que l'on n'est plus en présence d'activités d'espionnage isolées, mais que des efforts constants sont déployés pour accéder à certains systèmes, à des données et informations confidentielles, et que les pressions sur les données et systèmes sensibles augmentent chaque jour. Concrètement, il est possible d'exploiter pendant des années une infrastructure d'espionnage à l'insu de tous. On peut donc partir de l'idée qu'aujourd'hui déjà, d'autres logiciels d'espionnage sont en place et qu'ils sont soit utilisés en parallèle, soit gardés en réserve pour pouvoir continuer à épier et saboter les systèmes et réseaux déjà infiltrés, au cas où une attaque serait rendue publique. Voir aussi chapitre 5.2.

4.2 Cyberactivisme au Proche-Orient

De petites escarmouches ont éclaté en janvier 2012 entre des cyberpirates pro et anti-israéliens. Un pirate s'étant présenté comme saoudien et se faisant appeler «0xOmar» a publié des informations concernant les cartes de crédit de milliers d'Israéliens, qu'il s'était procurées en attaquant les banques de données de prestataires de services Internet. En réponse à cette action, un pirate israélien ayant choisi le pseudonyme d'«0xOmer» a publié des données sur des citoyens saoudiens. Le lendemain de l'appel d'un porte-parole du Hamas à protester contre l'occupation palestinienne en attaquant des sites Internet israéliens, les sites de la compagnie aérienne El Al et de la bourse israélienne étaient inaccessibles, ce qui a conduit en représailles à un assaut contre le site des bourses des Emirats Arabes Unis et d'Arabie saoudite. Suite à cet incident un téléprédicateur koweïtien a appelé via Twitter au cyber djihad contre Israël. Quelques jours plus tard, un pirate pro-israélien a publié les données d'accès à Facebook de plusieurs milliers d'Arabes, obligeant Facebook à réinitialiser les mots de passe des comptes en question. Après quelques autres cyberintrusions suivies de la publication des données pillées, et diverses atteintes à la disponibilité de sites Web, les hostilités ont finalement cessé à la mi-février.

Ces incidents montrent de façon exemplaire comment des acteurs non étatiques et même de simples quidams peuvent attiser des conflits politiques. Il suffit de joindre à la publication de données collectées lors d'une intrusion informatique une déclaration politique pour provoquer des réactions de la part de l'adversaire politique. De cette manière, des pirates peuvent se monter les uns contre les autres. Si dans le cas d'espèce un des camps était bien connu, l'autre l'était moins, et il a fallu s'en remettre pour la riposte à ses déclarations spontanées et non vérifiées. Au fil des événements, des doutes sont apparus sur la provenance réelle du provocateur «0xOmar» ce qui a conduit les pirates pro-israéliens à s'en prendre aussi à d'autres pays arabes et à l'Iran. Comme les agressions étatiques, le cyberactivisme soulève

[16] Voir MELANI, rapport semestriel 2010/2, chapitre 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=fr et MELANI, rapport semestriel 2011/2, chapitre 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 31 août 2012)

un problème d'imputabilité des faits. Tant que l'on n'a pas identifié clairement l'agresseur, on court le risque, en cherchant à rendre la pareille, de se tromper de cible et de punir en définitive un grand nombre d'innocents.

4.3 Anonymous promet de «fermer Internet» – rien ne s'est passé

Le 12 février 2012, Anonymous a annoncé son intention de paralyser Internet le 31 mars, en lançant des attaques contre les treize *serveurs racines DNS*. L'action visait à dénoncer tout à la fois les projets américains de loi pour lutter contre le piratage (Stop Online Piracy Act, SOPA), Wall Street, les politiciens irresponsables et les banquiers, ainsi que les abus en général. Cet appel a sans doute suscité l'intérêt des médias mais, comme l'avaient prédit les experts en sécurité, il n'a pas entraîné de perturbation significative du réseau.

Le système de noms de domaine (DNS) rend les services Internet plus conviviaux, puisqu'au lieu de l'*adresse IP* il suffit aux utilisateurs de composer un nom d'adresse (*URL*). Sans serveur *DNS*, Internet continuerait à fonctionner, mais il faudrait indiquer à la place des *URL* les *numéros IP*. Tout au sommet de la hiérarchie figurent les *serveurs racine*, qui renseignent sur le *Top-Level-Domain* ou domaine de premier niveau (p. ex. .com, .net, .ch).

Comme les *serveurs racines DNS* sont essentiels au bon fonctionnement d'Internet, divers mécanismes de sécurité sont en place. Ainsi, les treize *serveurs racines DNS* ne sont pas de simples serveurs. En réalité, il existe 259 serveurs de ce type, répartis à travers le monde et gérés par des exploitants différents afin d'augmenter la résilience des DNS.

La méthode préconisée par Anonymous, soit une attaque par déni de service (*DNS Amplification Attack*), amène les serveurs de noms à réagir à certains brefs paquets de requêtes par de très longs paquets. En théorie, une requête de 60 octets peut susciter une réponse de plus de 3000 octets. Il ne reste ensuite qu'à rediriger ces longues réponses vers les *serveurs de noms DNS*, afin de les surcharger et donc de les paralyser. Or ces serveurs possèdent des capacités gigantesques pour gérer les pics de trafic. D'où la garantie que le *DNS* continue à fonctionner même si deux tiers des serveurs racines devaient tomber en panne. Une panne de *serveur de noms DNS* devrait en outre se prolonger pour faire s'effondrer Internet, sachant que les fournisseurs d'accès ont tendance à mettre en cache les données *DNS* pour réduire le trafic réseau. Les *serveurs de noms DNS* sont toutefois soumis à une surveillance permanente. En cas d'anomalie, le trafic malveillant entrant serait immédiatement bloqué. La dernière attaque de grande envergure remonte à 2007 et avait pris pour cible deux des treize *serveurs de noms DNS*. Mais comme les autres fonctionnaient normalement, aucune perturbation significative n'était apparue.

Anonymous se renierait en partant à l'assaut d'Internet, après s'être souvent dit opposé à toute attaque contre les médias. Une attaque dont toute la communauté des internautes ferait les frais serait contre-productive pour Anonymous, qui se mettrait ainsi à dos des sympathisants. En outre, pour mener à bien une telle opération, il faudrait procéder à des tests préalables de l'outil mentionné par Anonymous et pouvoir compter sur un nombre élevé de volontaires. Or comme lors du projet d'attaque contre Facebook de novembre 2011, divers activistes ont déjà pris leurs distances avec cet appel.

Les liens informels au sein d'Anonymous se traduisent par une absence de coordination au niveau tant de la communication que des cyberattaques plus ou moins spectaculaires effectuées. 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, chacun peut en principe publier des communiqués au nom d'Anonymous pour susciter l'intérêt des médias.

Anonymous épie une conférence téléphonique entre Scotland Yard et le FBI

Des activistes d'Anonymous ont surpris une conférence téléphonique confidentielle entre la police londonienne Scotland Yard et le FBI, son homologue américain. Anonymous avait apparemment réussi à intercepter un courriel renfermant les données d'accès à cette conférence téléphonique. Les activistes avaient ensuite publié le contenu de la conférence, sur YouTube notamment.
Outre diverses questions sans importance, cette conférence téléphonique avait abordé les modalités des enquêtes en cours contre Anonymous et LulzSec, p. ex. les dates des arrestations prévues. Anonymous a publié non seulement le fichier audio de la conférence, mais aussi les données d'accès à cette conférence téléphonique. Des poursuites pénales ont été engagées.[17]

4.4 Protestations contre l'ACTA – sur Internet aussi

Le projet de ratification de l'accord ACTA (Anti-Counterfeiting Trade Agreement) a suscité au début de 2012 un tollé de protestations dans différents pays. Cet accord commercial anti-contrefaçon est un projet de traité multilatéral de droit public. Les nations signataires visent à établir un nouveau cadre juridique pour la lutte contre l'imitation frauduleuse de produits et les violations de droits d'auteur.

Ces protestations visant à faire capoter l'accord ACTA ont essentiellement consisté en manifestations traditionnelles, qui ont atteint leur paroxysme à la journée d'action européenne du 11 février 2012. De nombreuses actions de protestation ont également été signalées sur Internet (la liste ci-dessous n'ayant aucune prétention à l'exhaustivité):

République tchèque

En République tchèque, 27 000 enregistrements concernant des membres du principal parti gouvernemental (ODS) ont été volées et publiées. Outre leur adresse privée, ces données contenaient le numéro de téléphone des membres du parti. La ratification de l'accord ACTA a été suspendue jusqu'à nouvel avis le 6 février 2012.

Pologne

Des attaques *DDoS* ont temporairement paralysé divers sites Web du gouvernement polonais. Elles auraient eu pour auteurs la branche polonaise d'Anonymous et le groupe de cyberpirates Polish Underground. Des activistes ont en outre remplacé le site d'origine de la commune de Kraszevice par un slogan anti-ACTA[18]. Là encore, le gouvernement à décidé de remettre à plus tard la ratification de l'ACTA.

Etats-Unis

Dans le sillage des actions de protestation contre l'ACTA, Anonymous a visiblement aussi saboté plusieurs sites de la Commission fédérale du commerce américaine (FTC). Sept sites auraient fait les frais de l'opération – mais non le site principal.

Grèce

Vendredi 3 février 2012, des membres du collectif Anonymous s'en sont pris au Ministère grec de la justice. Ils dénonçaient aussi bien les mesures d'économies que la participation de

---

17 http://www.spiegel.de/netzwelt/web/anonymous-attacke-hacker-veroeffentlichen-fbi-gespraech-mit-scotland-yard-a-813224.html (état: 31 août 2012).

18 http://www.kraszewniki.pl/ (état: 31 août 2012).

la Grèce à l'accord ACTA. Leurs revendications se sont affichées pendant quatre heures sur le site du ministère. Les pirates informatiques ont fixé au gouvernement un ultimatum de deux semaines pour se retirer de l'accord ACTA, le menaçant sinon de nouvelles attaques.

Slovénie

La branche slovène d'Anonymous avait momentanément paralysé plusieurs sites Web, dont ceux du principal parti gouvernemental (SDS) et d'autres partis, lors des actions de protestation contre l'ACTA. D'où le gel de la ratification du traité, le 7 février 2012.

En Suisse, les protestations ont été beaucoup plus discrètes. Sans doute aussi parce que les citoyens disposent d'autres instruments politiques, avec le référendum et l'initiative. Il y a bien eu des manifestations à petite échelle, à Zurich surtout – mais ni grand défilé ni cyberattaques comme dans d'autres pays européens. Alors même que la Suisse avait participé à la conception ainsi qu'à la négociation de l'accord ACTA, le Conseil fédéral a signalé le 9 mai 2012 qu'il ne le signerait pas pour le moment.

Les protestations liées à l'accord ACTA montrent une fois de plus que la contestation s'exprime toujours plus dans le monde virtuel. Elles témoignent également de la réelle sensibilité des citoyens aux questions touchant à Internet. Toute limitation ou réglementation est accueillie avec d'autant plus de scepticisme qu'Internet reste perçu comme une zone de liberté, voire de non-droit et donc d'impunité.

4.5 Vols à grande échelle de mots de passe et de données de cartes de crédit

Les attaques à grande échelle contre des entreprises connues se sont poursuivies au premier semestre 2012. Des données de clients ont été dérobées à cette occasion (noms d'utilisateur et mots de passe, parfois aussi données de cartes de crédit).

La semaine du 4 au 8 juin 2012, plus de six millions de valeurs *hash SHA*-1 liées aux mots de passe du réseau social professionnel en ligne LinkedIn ont été publiées sur des forums Internet. *SHA*-1 est une fonction de hachage cryptographique très répandue générant, à partir de n'importe quel texte, un code hash à 160 bits (empreinte). Il est souvent possible de reconstruire le mot de passe à partir de la valeur hash. De nombreux mots de passe ont déjà été publiés en toutes lettres. Les documents parus avaient beau ne pas indiquer l'adresse électronique (qui joue le rôle de nom d'utilisateur) – tout indique que ces données étaient également tombées aux mains du pirate.

Quelques heures seulement après l'annonce de cet incident, de premiers sites d'hameçonnage invitaient à «vérifier» les mots de passe LinkedIn.

Accès à la banque de données de Zappos, filiale d'Amazon

Des inconnus ont accédé aux données personnelles de 24 millions de clients américains de Zappos, filiale d'Amazon, dérobant au passage la valeur hash de leur mot de passe. Par chance, seuls les quatre derniers chiffres des cartes de crédit étaient enregistrés dans la banque de données attaquée. Aux dires de Zappos, les escrocs n'ont pas réussi à

s'introduire dans les serveurs où étaient enregistrées les autres informations relatives aux paiements et les numéros complets des cartes de crédit.[19]

Pillage des données de cartes de crédit de Global Payments

L'exploitant de cartes de crédit Global Payments a eu moins de chance. Il s'est fait subtiliser les données de plus de 1,5 million de cartes de crédit. Tout a commencé par une cyberattaque contre une entreprise de taxis new yorkaise.[20] Les pirates étant parvenus à accéder à un compte d'administrateur de cette société, ils ont dupliqué pendant plusieurs mois les données des cartes de crédit. Ils se sont toutefois bien gardés de s'en servir tant que durait leur collecte. Ils ont ainsi évité que la victime ne découvre l'escroquerie et n'adopte des mesures de sécurité qui auraient réduit leur butin.

450 000 noms d'utilisateurs et mots de passe dérobés à Yahoo! Contributor Networks

Yahoo a été victime au premier semestre 2012 d'une cyberattaque. Le groupe de pirates «D33Ds Company» a dérobé et publié en ligne les données d'utilisateurs et mots de passe de 450 000 usagers de la plate-forme d'édition de contenu Yahoo! Contributor Networks[21]. La victime a déclaré avoir immédiatement comblé la faille de sécurité de son système informatique. Le collectif «D33Ds Company» a fait savoir que la banque de données était mal sécurisée et les mots de passe non chiffrés. L'attaque visait à donner une leçon aux administrateurs de banques de données, afin de les tirer de leur léthargie.

Publication de 50 000 noms d'utilisateurs et mots de passe de Twitter

Plus de 50 000 noms d'utilisateurs et mots de passes de comptes Twitter ont été publiés le 9 mai 2012. Twitter a promis de réinitialiser les mots de passe des comptes piratés. On ignore toujours d'où provenaient les données et qui les a divulguées. La qualité des données était médiocre, à en juger par les nombreuses inscriptions à double, par les comptes obsolètes ou renfermant des données erronées (fake accounts).[22]

Piratage de comptes GMX

Au moins 3000 comptes appartenant à des clients du fournisseur de messagerie GMX ont été piratés. On a d'abord cru à une *attaque par force brute*. Or cette méthode ne convient guère aux prestations de service en ligne, sachant qu'une opération d'une telle envergure serait très vite démasquée. Selon toute vraisemblance, les pirates étaient en possession de noms d'utilisateurs et de mots de passe. GMX a confirmé que des noms d'utilisateurs et des mots de passe avaient été introduits de façon très ciblée. On ignore toutefois comment les mots de passe ont été dérobés. Il pourrait s'agir de mots de passe subtilisés dans un autre contexte – auprès d'autres prestataires de services – puis «testés» sur des comptes GMX.[23] Et comme beaucoup de gens reprennent le même mot de passe pour tous les services utilisés sur Internet, une telle façon de procéder paraît logique.

Selon Firehost, les attaques de sites Internet par *injection SQL* ont augmenté de 69% entre avril et juin 2012.[24] Une *injection SQL* consiste à envoyer des requêtes manipulées à une banque de données. Elle aboutit généralement grâce à une interface mal programmée et négligeant de contrôler les requêtes entrantes, ou encore grâce à une faille de sécurité. D'où

[19] http://online.wsj.com/article/BT-CO-20120116-706917.html (état: 31 août 2012).

[20] http://blogs.gartner.com/avivah-litan/2012/03/30/new-credit-card-data-breach-revealed/ (état: 31 août 2012).

[21] http://www.focus.de/digital/internet/datenbank-muehelos-geknackt-hacker-veroeffentlichen-zugangsdaten-von-450-000-yahoo-nutzern_aid_781269.html (état: 31 août 2012).

[22] http://www.spiegel.de/netzwelt/web/twitter-passwoerter-im-netz-a-832171.html (état: 31 août 2012).

[23] http://www.zeit.de/digital/datenschutz/2012-07/gmx-passwort-account (état: 31 août 2012).

[24] http://www.heise.de/newsticker/meldung/Deutlicher-Anstieg-der-SQL-Injection-Angriffe-1651041.html (état: 31 août 2012).

la possibilité d'espionner les données des clients, de manipuler des boutiques en ligne ou d'effacer de grandes quantités de données. Une attaque couronnée de succès, la perte de données de clients et l'atteinte à la réputation qui s'ensuit peuvent coûter très cher, voire ruiner une entreprise. Là aussi, il est utile d'actualiser régulièrement le logiciel de son site et de bien se protéger contre toute attaque extérieure.

Il est devenu indispensable d'utiliser des mots de passe différents pour chaque service en ligne. Le gain de sécurité est énorme, même si l'on doit noter quelque part (sur du papier) ces mots de passe pour s'en souvenir.

4.6 SCADA – mise à jour

Un groupe de prestataires de services de sécurité a publié en janvier 2012 des failles de sécurité de composantes de systèmes de contrôle industriels. Ce geste a mis en émoi tant les fabricants que les exploitants. Car les découvreurs de ces vulnérabilités n'avaient pas informé au préalable les fabricants pour leur permettre de combler d'emblée la lacune de sécurité. Ils ont préféré s'adresser directement au grand public. Cette façon de procéder leur a valu des critiques de différents côtés.

Les chasseurs de vulnérabilités ont d'abord voulu montrer aux exploitants d'infrastructures critiques à quel point il est facile de compromettre des systèmes *SCADA*. Ensuite, ils ont visiblement voulu donner une leçon aux fabricants. Le groupe s'était visiblement déjà aperçu que les fabricants, tout en connaissant certaines lacunes de sécurité depuis des années, ne s'empressent pas de les corriger mais retardent le plus longtemps possible leur publication et les mises à jour requises.[25] A leur décharge, il faut dire que les mises à jour de systèmes *SCADA* ne sont pas comparables à celles d'ordinateurs. L'actualisation d'un système de contrôle comporte toujours un risque de dysfonctionnement qui, le cas échéant, pourrait être lourd de conséquences.

La grande différence avec les logiciels ordinaires tient à ce que les fournisseurs SCADA ne sont guère habitués à réparer les failles de sécurité, tandis que les exploitants mettent rarement à jour leurs composantes logicielles. Comme leurs processus fonctionnent en permanence, ils ne peuvent procéder à des actualisations qu'au cours de plages de maintenance spécifiques. En outre, les possibilités de tester par avance les effets des correctifs de sécurité (*patchs)* sur le processus d'ensemble sont restreintes. Le principe «don't touch a running system» s'applique, d'autant plus que les dérangements et les pannes ont tôt fait d'engendrer des coûts élevés.

Au départ, les systèmes *SCADA* 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. Ces dernières années, l'afflux sur le marché d'appareils relativement avantageux intégrant, comme technologie d'interface, le protocole Internet a changé la donne. Ces composantes ont beau ne pas être le plus souvent (encore) reliées à Internet, elles facilitent l'intrusion, via des ordinateurs portables ou des *clés USB*, de maliciels dans ces systèmes fonctionnant en réseau fermé. Et comme les composantes *SCADA* ne sont pas conçues pour des solutions de sécurité comme les *pare-feu* ou les *antivirus*, les pirates ayant réussi à accéder au réseau ont le champ libre.

[25] http://www.heise.de/security/meldung/Sicherheitsexperten-setzen-Hersteller-von-Industriesteuerungen-unter-Druck-1418292.html (état: 31 août 2012).

Risque de cyberattaque contre des installations ferroviaires américaines

Selon un rapport de la Transportation Security Administration (TSA), l'agence américaine contrôlant la sécurité des moyens de transport, un dérangement des voies ferrées survenu le 1er décembre 2011 au nord-ouest des Etats-Unis provenait apparemment de deux intrusions commises avec des adresses IP non américaines. Il en est résulté des retards de quinze minutes. L'incident s'est répété le lendemain, mais sans provoquer de dérangement. Les causes exactes de ces intrusions n'ont pas été rendues publiques. Le Département américain de la sécurité intérieure (Department of Homeland Security, DHS) a toutefois souligné qu'une attaque ciblée pouvait être exclue. Les données des trois adresses IP à l'origine de l'agression ont été mises à disposition d'autres entreprises de transport, tant aux Etats-Unis qu'au Canada.[26]

Implants défaillants

L'exemple suivant montre que les grands systèmes ne sont pas seuls exposés à une cyberattaque lourde de conséquences, mais que les petits systèmes encourent eux aussi de sérieux dangers. Dans une récente étude, des experts en sécurité ont analysé les risques que comportent les implants médicaux. Sans surprise, il en est ressorti que les stimulateurs cardiaques p. ex. présentent de sérieux risques sur le plan de la sécurité. Comme chacun sait, les porteurs de stimulateurs cardiaques doivent se tenir à l'écart des appareils à fort rayonnement électromagnétique. Lors d'un test, des chercheurs ont bloqué un défibrillateur implantable en le bombardant d'ondes radio. Ils ont également décelé d'autres vulnérabilités préoccupantes. Ainsi, des liaisons *WiFi* servant aux mises à jour comportaient des failles qu'ils ont pu exploiter. Dans le pire des cas, une désactivation était possible (p. ex. pompes à insuline), avec des conséquences fatales pour la victime.[27]

4.7 Création d'un Centre européen de lutte contre la cybercriminalité

La Commission européenne a proposé le 28 mars 2012 de créer au sein d'Europol, l'Office européen de police basé à La Haye, un nouveau Centre européen de lutte contre la cybercriminalité. Aujourd'hui déjà, Europol coordonne le travail des forces de police nationales dans le domaine de la criminalité organisée transfrontière et facilite les échanges entre les polices des Etats membres.

Le centre, qui concentrera ses efforts sur la lutte à l'échelle européenne contre la cybercriminalité, entrera en activité le 1er janvier 2013. Il centralisera les informations ou expériences, soutiendra les investigations criminelles et encouragera les solutions et les actions de sensibilisation au niveau européen en matière de cybercriminalité. En outre, la création d'un groupe d'experts interdisciplinaire est prévue afin d'œuvrer plus efficacement contre les cybercrimes et la pédopornographie.[28]

Le formidable essor de la communication puis des transactions commerciales via Internet est allé de pair avec une explosion des cas d'escroquerie et autres délits en ligne. Les investigations révèlent souvent la présence de centaines de victimes, disséminées aux

[26] http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/ (état: 31 août 2012).

[27] http://www.pcwelt.de/news/Sicherheitsrisiko-Medizinische-Implantate-als-Zielscheibe-fuer-Hacker-5708296.html (état: 31 août 2012).

[28] https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417 (état: 31 août 2012).

quatre coins du monde. De même, les escrocs dont on parvient à remonter la trace sont généralement basés dans plusieurs pays, et donc leurs forfaits relèvent de différentes juridictions. Les forces de police nationales ne sont plus en mesure de mener isolément des enquêtes aussi vastes et complexes, et les traditionnelles demandes d'entraide judiciaire sont lentes et pèchent par manque d'efficience. Aucun délit ne présente un caractère aussi résolument international que les cybercrimes. D'où la nécessité d'une approche coordonnée, commune et supranationale pour les réprimer efficacement. C'est précisément à ce niveau que le Centre européen de lutte contre la cybercriminalité vise à proposer ses services.

4.8 Désactivation d'un réseau de zombies Zeus

Microsoft a saisi le tribunal de district de New York, en coopération avec plusieurs prestataires de services financiers, soit l'Information Sharing and Analysis Center (FS-ISAC), l'Electronic Payments Association (NACHA) et le spécialiste en sécurité de l'information Kyrus. Le 23 mars 2012, des US-Marshals, agents fédéraux américains, ont perquisitionné deux bâtiments de Pennsylvanie et de l'Illinois. Plusieurs *serveurs Web* soupçonnés d'être mêlés aux agissements d'un réseau de zombies Zeus ont été saisis. Microsoft a innové sur le terrain juridique, pour rendre la perquisition possible. En lieu et place d'un procès pénal, son choix s'est porté sur le dépôt, avec des organisations du secteur financier, d'une plainte civile contre les exploitants du réseau de zombies Zeus. Microsoft a d'abord porté plainte contre inconnu. Puis en juillet, deux noms mêlés au réseau de zombies Zeus ont été publiés. Yevhen K. et Yuriy K sont entre-temps en prison en Grande-Bretagne.[29]

La procédure adoptée ne prétendait pas démanteler le réseau de zombies. Car il est loin d'être simple de désactiver un réseau de la complexité de Zeus. Il s'agissait plutôt d'occasionner du travail et des frais aux exploitants de tels réseaux criminels – dans l'espoir qu'ils cessent d'être une affaire lucrative.

Les réactions à la perquisition n'ont toutefois pas toutes été positives. Ainsi FoxIT, prestataire de services de sécurité néerlandais, a publié quelques remarques critiques sur cette opération Microsoft.[30]

4.9 Infections par «drive-by download» – rôle des bannières publicitaires

A la mi-mai 2012, des escrocs ont exploité une faille d'*OpenX*, logiciel d'affichage et de gestion des bannières publicitaires, pour diffuser des maliciels via le site www.wetter.com. On ignore combien de temps l'infection a été active. Le cas échéant, des maliciels ont été installés à l'insu des visiteurs. Le CERT.at a connaissance de différentes variantes de programmes malveillants ainsi répandus, dont un *cheval de Troie demandeur de rançon* (*ransomware*).[31] Voir plus haut le chapitre 3.3 consacré à la question, ainsi que le rapport semestriel MELANI 2011/2, chapitre 3.5[32].

---

29 http://www.golem.de/news/botnet-microsoft-nennt-zwei-mutmassliche-betreiber-von-zeus-1207-92930.html (état: 31 août 2012).

30 http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/ (état: 31 août 2012).

31 http://www.cert.at/warnings/all/20120516.html (état: 31 août 2012).

32 Voir MELANI, rapport semestriel 2011/2, chapitre 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 31 août 2012).

Les infections de sites Web sont en ce moment le vecteur de diffusion de maliciels le plus répandu. Les serveurs centraux, mettant du contenu à disposition de différents sites Web, jouent ici un rôle central. Dans le cas de la publicité en ligne notamment, mais aussi des services statistiques, la moindre page compromise peut être lourde de conséquences.

La manière dont les annonceurs et autres fournisseurs de contenus en ligne utilisent le logiciel choisi par eux revêt donc une très grande importance. Là encore, tous les programmes doivent être constamment actualisés. Le cas échéant, un site ne peut prétendre offrir une plus grande sûreté que celle de son maillon faible. Et bien souvent, il s'agit d'offres de tiers, de contenus injectés sur le site et échappant de ce fait à tout contrôle de l'exploitant.

5 Tendances / Perspectives

5.1 Usage mixte (professionnel/privé) des TIC – un risque pour la sécurité?

Alors qu'autrefois, une distinction stricte était opérée entre vie privée et vie professionnelle, la limite est désormais perméable. Tandis que les employeurs attendent de leurs collaborateurs qu'ils soient joignables en dehors des heures de bureau ou qu'ils travaillent aussi le soir en période de stress (à leur domicile), ces derniers utilisent aussi les TIC à des fins privées. Ils consultent p. ex. leurs messages privés ou cultivent leurs réseaux sociaux. Par ailleurs, la course aux appareils dernier cri est constante. Pourquoi un collaborateur se contenterait-il d'un téléphone mobile sans fonctions supplémentaires, alors qu'il utilise à titre privé un *smartphone*? Si l'entreprise ne réagit pas, il s'acquittera tôt ou tard de tâches professionnelles avec son appareil personnel, ou d'autres idées lui traverseront l'esprit pour modifier des processus de travail selon ses vœux ou besoins. Il s'agit évidemment d'un nouveau défi pour les responsables informatiques. Car dès que des ordinateurs sont utilisés non plus dans le réseau interne (contrôlé) mais à l'extérieur, de nouveaux risques apparaissent.

Les échanges de données entre ordinateurs privés et professionnels, p. ex. par *clé USB* ou par CD, constituent un risque supplémentaire. Expérience à l'appui, les pirates se servent volontiers de *clés USB* lors d'attaques ciblées visant à s'introduire dans des réseaux d'entreprises. Concrètement, l'agresseur infecte l'ordinateur privé (mal protégé) d'un collaborateur pour se glisser discrètement de là, par le biais d'un support de sauvegarde externe, sur son ordinateur professionnel. Pour compliquer les choses, les recherches sont beaucoup plus difficiles en cas d'incident impliquant un ordinateur privé, faute d'enregistrement systématique des activités de cet ordinateur en ligne. Alors qu'une entreprise victime d'un envoi ciblé de maliciels peut vérifier a posteriori si le courriel est arrivé à destination et a été ouvert, ce n'est guère possible dans les réseaux privés.

Cette évolution montre de façon exemplaire l'importance d'un concept de sécurité intégral. Au-delà des questions classiques relatives aux TIC, il aborde des questions d'organisation. Qui a accès à quelles données? Les collaborateurs savent-ils quelles données peuvent quitter le réseau d'entreprise, ou quels appareils peuvent être pris et raccordés au travail? Suffit-il de bloquer les ports *USB* dans le périmètre de sécurité, ou devrait-on également y interdire les téléphones mobiles? Plus généralement, on est amené à se demander s'il ne vaudrait pas mieux remettre à grande échelle de tels outils de travail et en autoriser l'usage privé. Même s'il en résulte un surcroît de travail administratif pour l'employeur, le contrôle des appareils et des applications installées est ainsi garanti, vu qu'ils lui appartiennent et sont soumis à ses contrôles.

Bien qu'indispensables, les mécanismes techniques de sécurité n'offrent pas une protection à 100 %. Il faudra désormais mettre l'accent sur la protection de l'information et ne plus se contenter de protéger les ordinateurs et les réseaux où sont stockées les informations. Autrement dit, la gestion de l'information et des données, la classification de l'information, etc. joueront un rôle de plus en plus important. En outre, une véritable analyse des risques s'impose pour adapter à la valeur réelle de l'information la sécurité tant des canaux de distribution que des droits d'accès et des lieux de stockage. Tout canal ou lieu de stockage n'offre pas la même sécurité, de même que certains documents sont plus sensibles que d'autres. Trop souvent, les TIC sont assimilées à un simple facteur de coûts, et les directions d'entreprises n'y voient qu'une fonction logistique et de support. En réalité, la sûreté de l'information dépend dans une large mesure des TIC, qui ont à ce titre leur place dans le processus commercial et stratégique de la gestion des risques. Concrètement, la sûreté de l'information doit faire partie intégrante du concept de sécurité, au même niveau de priorité stratégique que la protection des bâtiments et des personnes, ou encore le contrôle de gestion financière.

5.2 Cyberconflit au Proche-Orient

Dans le sillage du printemps arabe, des documents ou indices rendus publics après la chute des premiers gouvernements ont confirmé que certains Etats arabes recouraient à des technologies occidentales de pointe pour surveiller sur le Web les opposants au régime. Même les pays épargnés par les troubles disposeraient de programmes et d'infrastructures leur permettant de contrôler les communications à grande échelle. La vente de telles solutions informatiques est en plein essor. Le rapport semestriel 2011/2[33] a déjà abordé cette problématique complexe, où il faut se garder de toute vision manichéenne et réductrice. Les incidents survenus dans des foyers de crise et de conflit au Proche-Orient rappellent d'ailleurs que dans le secteur des TIC, le champ des acteurs et des ressources va bien au-delà de la surveillance des communications:
Le maliciel Stuxnet et ses modules annexes ont ainsi démontré la redoutable efficacité des instruments TIC, quand leur développement a bénéficié de ressources suffisantes et de l'appui étatique et sert à des fins de sabotage ou d'espionnage. Comme expliqué au chapitre 4.2, des groupes non étatiques sont aussi impliqués, sur le terrain virtuel, dans les conflits au Proche-Orient. Or il est difficile de savoir précisément qui se cache derrière ces mouvements de protestation, dans quelle mesure ils reçoivent du pouvoir un soutien autre qu'idéologique, et comment leur rivalité aboutit à une escalade. Ils maîtrisent les multiples facettes du vol de données, jusqu'à la défiguration de sites Web (defacement) appréciée de tous les pirates, en passant par les attaques par déni de service. Les avantages d'Internet sont également exploités sur le plan organisationnel et pour la propagande. Ainsi, des activistes de toutes provenances s'organisent via Facebook, Twitter et d'autres médias analogues, ou publient sur Internet, pour étayer leurs déclarations et leurs revendications, des vidéos et des photos prises à l'aide d'un téléphone mobile dont il est impossible de reconstituer de façon concluante le contexte réel.

Il n'est donc guère surprenant que des tentatives en tous genres soient faites pour infiltrer non seulement les comptes électroniques des adversaires, mais aussi leurs groupes dans les réseaux sociaux, afin de connaître les activités projetées, l'identité des protagonistes et encore d'autres informations utiles. Par exemple, il était déjà de notoriété publique avant le printemps arabe que les dissidents vivant à l'étranger étaient exposés à des attaques informatiques ciblées. Les membres de régimes autoritaires et leurs proches s'exposent eux-

[33] Voir MELANI, rapport semestriel 2011/2, chapitre 5.3: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 31 août 2012).

mêmes à être importunés par des activistes ou des services de renseignement étrangers, comme le rappelle la publication des achats effectués par Bashar al-Assad sur son compte iTunes.[34]

La demande croissante de technologies de surveillance (centrale), les actes de sabotage informatique, la publication d'images de propagande, et jusqu'aux efforts visant à discréditer des individus sur la base de courriels personnels dérobés, témoignent de l'exploitation systématique des moyens et méthodes informatiques par les acteurs d'une région instable et traditionnellement en proie aux tensions.

Les troubles, crises et conflits au Proche-Orient existaient déjà bien avant le printemps arabe. Mais les manifestations et les désordres ont donné à ces affrontements en coulisses une nouvelle dimension, tandis que d'autres difficultés jusque-là maîtrisées se révélaient au grand jour. Quant aux TIC, elles étaient utilisées au Proche-Orient avant ces incidents et débordements, tant pour la communication et la surveillance (centrale) de ce secteur que pour les systèmes *SCADA*, ou encore pour soutenir les processus de production et d'affaires. L'éclatement du conflit lors du printemps arabe a toutefois encouragé un usage agressif et offensif des TIC, d'Internet en particulier.

Des cas de paralysie temporaire de sites Web, de vol de documents étatiques ou privés ou d'usage de maliciels à des fins de sabotage sont régulièrement rendus publics. Sans parler de la diffusion massive par les service Web 2.0 d'annonces, de vidéos ou bribes d'information concernant la situation sur place – chacune des parties au conflit recourant à cette technique et les vérifications sur place ou la traçabilité de l'information étant souvent impossibles. Pour aggraver les choses, les outils TIC sont souvent relativement bon marché et ont une portée considérable, ce qui en rehausse l'attrait pour tous les protagonistes.

Autrement dit, le cyberconflit mené à plusieurs niveaux au Proche-Orient est en premier lieu un effet secondaire des affrontements concrets et des réalités locales. D'où l'importance de ne pas ramener les cyberincidents à des événements isolés, comme le font volontiers les médias, mais de les resituer dans leur contexte général, déterminant pour pouvoir porter une appréciation complète sur ce qui a été montré, ce qui s'est produit et ce qui a été annoncé.

5.3 Vol de données: beaucoup de petites entreprises et peu de grandes visées

Les attaques menées contre les clients de grandes entreprises, notamment contre leurs données de cartes de crédit, font souvent les gros titres. Outre les événements actuels présentés au chapitre 4.5, il est utile de rappeler ici les nombreuses attaques passées, comme la perte de données de clients subie par Sony l'année dernière, le pillage systématique, dès 2005 et pendant 18 mois, de plus de 45 millions de numéros de cartes de crédit appartenant à la chaîne de magasins anglo-américaine TJX, ou encore l'incident dont a été victime le fabricant de cartes de crédit Heartland en 2009.

Il ressort toutefois d'une étude réalisée par l'entreprise de sécurité américaine Verizon[35], sur la base de données des services secrets américains (US Secret Service) et des polices tant australienne que néerlandaise et irlandaise, que les attaques contre les grandes entreprises

[34] http://www.guardian.co.uk/world/2012/mar/14/assad-itunes-emails-chris-brown (état: 31 août 2012).
[35] http://securityblog.verizonbusiness.com/category/ask-the-data/ (état: 31 août 2012).

sont restées minoritaires en 2011. Sur les 855 incidents signalés, qui ont compromis 174 millions jeux de données, seule une faible partie concernent de grandes entreprises. D'où l'importance de ne pas perdre de vue, sous l'influence de quelques cas certes spectaculaires, les cyberattaques visant quotidiennement de plus petites entreprises dont les médias ne parlent pas. Dans plus de 75 % des cas, les attaques ont pris pour cibles des entreprises occupant moins de 1000 salariés.

Alors que les grandes entreprises sont bien préparées face aux cyberrisques et disposent généralement d'une équipe de sécurité informatique et d'un responsable de la sécurité (CSO), cette sensibilité fait encore défaut à bien des PME. Trop d'entreprises continuent à traiter avec insouciance les données de leur clientèle. Or à quoi bon sécuriser la transmission des commandes via https, si les données des cartes de crédit sont ensuite stockées sans cryptage sur un ordinateur?

Une partie des cybercriminels en profitent sans pitié, opérant selon le principe de la moindre résistance et recherchant les cibles les plus «faciles». Leurs méthodes d'attaque sont largement automatisées et testent systématiquement les lacunes de sécurité ou erreurs de configuration connues des sites Web ou des banques de données, afin de dérober ensuite les données stockées. Il peut donc être globalement plus fructueux de pirater non pas une seule grande entreprise mais plusieurs petites entreprises Elles ont beau offrir un moindre butin – moins de données-clés –, il est plus facile de s'y introduire.

Les grandes entreprises ne devraient toutefois pas se croire en sécurité. Car à plus long terme, les efforts consentis par certains criminels bien formés et possédant un solide bagage technique portent aussi leurs fruits. En matière d'espionnage, la notion d'*advanced persistent threat* (APT) s'est établie et implique principalement des acteurs étatiques qui ne sont pas à l'affût d'un avantage financier immédiat. Or si au bout du compte le profit est au rendez-vous, une attaque ciblée préparée pendant des mois par des professionnels peut aussi en valoir la peine pour les criminels. Mais à la différence de l'espionnage étatique, l'appât du gain joue un rôle central dans leur cas.

5.4 Communication avec la clientèle à l'ère du phishing

«Aucune entreprise sérieuse ne demande par courriel des données d'ouverture de session ou des mots de passe.» Telle est la réponse standard donnée par MELANI aux personnes lui envoyant un courriel dont elles ignorent s'il émane ou non de l'expéditeur indiqué. Cette règle, simple de premier abord, met parfois les entreprises dans l'embarras, à l'ère de la communication électronique avec la clientèle. Comment lui faire savoir qu'un courriel n'émane pas d'escrocs? Surtout, une communication désinvolte risque de rendre les clients imprudents, le jour où ils recevront un courriel d'arnaque.

Vérifications d'e-Bay auprès de la clientèle

L'exemple ci-dessous est révélateur du dilemme où se trouvent les entreprises:
eBay envoie ponctuellement à ses membres des courriels de contrôle, quand un compte n'a plus été consulté pendant une longue période. Il est clair qu'une telle mesure s'impose pour éviter au fil des ans une multiplication des comptes dormants.
Même sans exiger directement le nom d'utilisateur et son mot de passe, le courriel éveille la méfiance de bien des destinataires, surtout si comme dans le cas d'espèce, le compte d'utilisateur venait d'être utilisé pour une transaction.

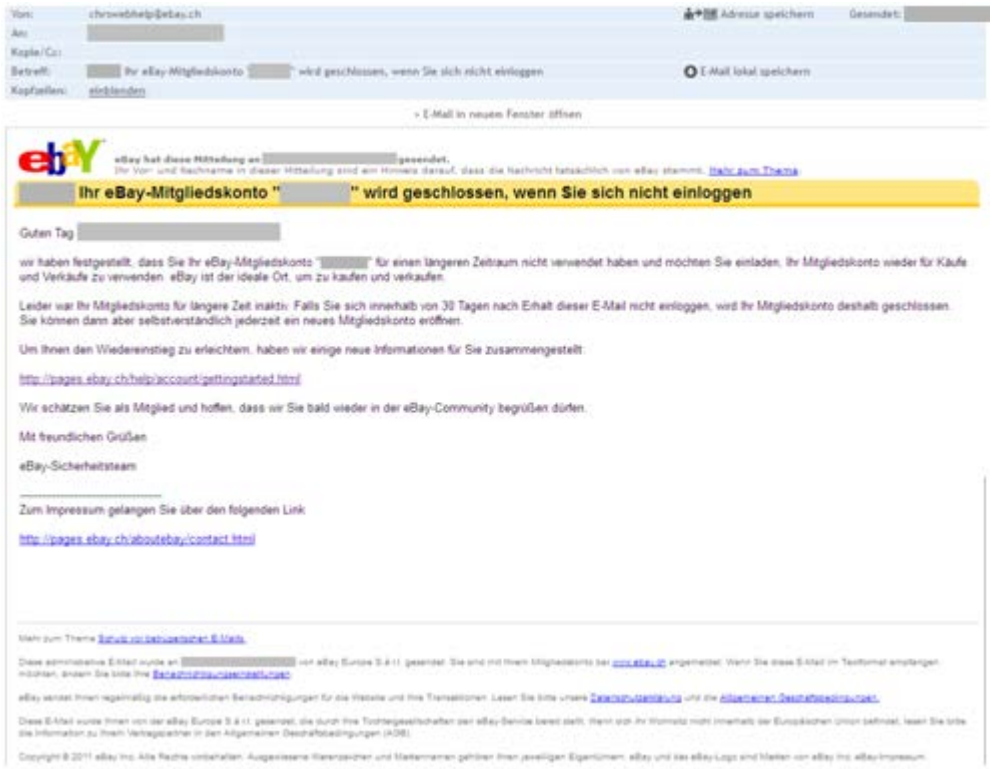


Figure 8: Courriel d'e-Bay destiné à contrôler l'identité des clients.

Modification des conditions générales de Paypal

Un autre cas soumis à MELANI concernait une modification de conditions générales communiquée par Paypal dans un courriel à la fin de juin 2012. Même si le message ne contenait pas de lien à une page d'ouverture de session, le simple fait de recevoir à l'improviste un courriel de Paypal a gêné certains utilisateurs.

Newsletter de Suisse Tourisme

Un courriel expédié par Suisse Tourisme le 31 mai 2012 a suscité des questions. Car les liens qu'il renferme renvoient non pas au domaine de Suisse Tourisme, mais à un autre serveur suisse du nom de «crm.stnet.ch». Les liens étaient en outre compliqués et longs, ce qui a poussé des destinataires à faire vérifier par MELANI si ce courriel était authentique.

Figure 9: Courriel promotionnel de Suisse Tourisme comportant des liens au domaine stnet.ch

Réinscription à la lettre d'information de MELANI

MELANI n'échappe pas à ce genre de problème. La lettre d'information de MELANI ayant migré en juin 2012 sur le portail d'information de la Confédération et faute de pouvoir y transférer, pour des raisons techniques, la banque de données avec les adresses électroniques enregistrées, il a fallu informer tous les abonnés que s'ils voulaient continuer à la recevoir, ils devaient se réinscrire à la lettre d'information MELANI.

Une telle opération est complexe et doit être soigneusement planifiée. Elle a donc fait l'objet d'un premier courriel de MELANI, définissant le moment exact où la réinscription serait annoncée. Le courriel à ce sujet a été expédié au format texte exclusivement et ne contenait qu'un lien conduisant au domaine MELANI, par analogie aux lettres d'information antérieures. Les nouveaux abonnés n'ont jamais dû indiquer leur mot de passe (il fallait en choisir un nouveau). En outre, l'envoi était clairement mentionné sur la page d'accueil du site de MELANI. Cette procédure a malgré tout suscité des réactions d'abonnés – peu nombreuses il est vrai. Le cas échéant, il est utile de répondre rapidement aux questions posées par les clients juste après l'envoi d'une lettre d'information, afin de dissiper autant que possible l'inquiétude. Dans le cas d'espèce, il y avait aussi un potentiel d'amélioration, consistant p. ex. à utiliser dans le courriel un lien aboutissant à une page sécurisée (https).

Les points suivants devraient être pris en compte lors de l'envoi de lettres d'information:

- Envoyer autant que possible des courriels au format texte.
- Veiller à la régularité des envois.
- N'introduire que de rares liens, et encore seulement à son propre domaine. Si possible, utiliser des liens conduisant à des pages sécurisées (https) et en informer le destinataire.
- Ne pas créer d'hyperlien vers des pages Web exigeant le nom d'utilisateur et le mot de passe, ou d'autres données encore.
- Signaler la lettre d'information sur la page d'accueil du site Web ou y placer directement l'hyperlien correspondant, pour que le destinataire ait la possibilité de saisir à la main l'adresse principale, puis d'y cliquer sur la lettre d'information.
- Appeler les clients par leur prénom et nom, si ces informations sont connues.

5.5 Vote électronique en Suisse – expériences réalisées

Le projet helvétique «Vote électronique» a démarré en 2000. Ce terme définit en Suisse l'exercice des droits politiques par voie électronique (participation à une élection ou une votation, signature d'initiatives et de référendums).

Le premier essai pilote a été réalisé en 2003 dans une petite commune genevoise, où un nombre limité de citoyens ont eu la possibilité de participer à des scrutins communaux par voie électronique. Cet essai pilote a rencontré un écho international: de prestigieux journaux en ont parlé, en Suisse comme à l'étranger.

Depuis 2003, le Conseil fédéral a approuvé plus de 100 essais de vote électronique au niveau fédéral. Il sera utilisé pour la 115 fois lors de la votation populaire fédérale du 25 novembre 2012. Mais si l'on tient compte des nombreux autres essais au niveau communal et cantonal et de ceux réalisés à l'occasion d'élections, le nombre d'essais de vote électronique effectués en Suisse est bien plus important.

En dépit de toutes ces tentatives, seulement des incidents mineurs avec peu d'effet (voir l'exemple dans la section 3.7) sont connus. Le vote par voie électronique est-il pour autant sûr en Suisse? La brève analyse qui suit vise à répondre à cette question:

A l'heure actuelle, seul un nombre limité d'électeurs suisses sont autorisés à voter par voie électronique. Entre-temps, ce droit a certes été étendu aux Suisses de l'étranger. Il est malgré tout peu probable à l'heure actuelle, pour plusieurs raisons, qu'un essai défectueux de vote électronique influence le résultat final:

- La taille de l'électorat est choisie de façon à ce que même en cas de résultat très serré, on puisse partir de l'idée qu'une panne partielle ou totale du système électronique n'aurait avec une probabilité aucune influence sur le résultat final.

- La fermeture des urnes électroniques doit toujours précéder celle des urnes physiques le samedi avant le dimanche des votations. Cette mesure vise à permettre, p. ex. en cas de panne totale des systèmes électroniques (suite à un effondrement sur le plan suisse des liaisons Internet ou a cause d'une attaque DDoS), de donner aux électeurs la possibilité d'exprimer leur voix physiquement, dans un local de vote.

Outre ces mesures d'organisation, il existe toute une série de mesures techniques visant à garantir le respect des principes inscrits dans la loi fédérale sur les droits politiques et dans l'ordonnance sur les droits politiques (unicité, anonymat et confidentialité du vote).

Or qu'en est-il si une grande partie de la population fait usage de cette prestation de service? En cas d'usage à grande échelle du vote électronique dans toute la Suisse, les mesures susmentionnées cesseraient de déployer leur effet:

- Une attaque contre l'urne électronique est certainement peu probable. Les suffrages validés y sont stockés sous forme cryptée jusqu'au dépouillement. La brève période où un vote électronique est possible ne devrait donc pas suffire pour décrypter et falsifier les suffrages, même en cas d'*attaque par force brute*. Même une cyberattaque réussie n'aurait vraisemblablement pas d'influence sur l'issue d'un scrutin. Car les limites en vigueur (aucun essai ne pouvant concerner plus de 10 % des électeurs au niveau fédéral) ont été définies pour que même une défaillance totale du e-voting ou des manipulations des bulletins électroniques n'affectent pas le résultat final.

- En revanche, il n'est évidemment pas exclu qu'un jour ou l'autre, une attaque contre un système de vote électronique porte ses fruits. On pourrait penser p. ex. à une attaque *DDoS* contre les systèmes électroniques, visant à empêcher les Suisses de l'étranger d'exprimer leur voix à temps.

- Le principal problème réside certainement dans des unités d'entrée peu sûres (systèmes clients) accouplé à l'absence de traçabilité et de possibilité de preuve. De nombreux vecteurs d'attaque utilisés contre les applications de e-banking pourraient directement, voire sous une forme plus rudimentaire, prendre pour cible le vote électronique. Car les mesures de protection mises en place dans le e-banking – procédure d'authentification et de surveillance des transactions – sont inapplicables ici. D'où une menace réelle, le client étant indiscutablement le talon d'Achille du vote électronique.[36] Si un maliciel s'installe sur l'ordinateur d'un électeur, il pourrait manipuler à volonté le suffrage exprimé. Par exemple, le code malicieux introduit dans le navigateur veillera à transformer tout paramètre «oui» envoyé au serveur de vote électronique en «non» avant son cryptage. Le maliciel serait également en mesure de manipuler l'image de sécurité transmise en retour par le serveur après le décryptage, de façon à ce que l'électeur ne s'aperçoive de rien. Un tel scénario d'attaque serait préoccupant s'il était utilisé à grande échelle pour manipuler un

[36] https://www.e-voting-cc.ch/index.php/de/workshops/workshop09/programm09/87 (état: 31 août 2012).

maximum de suffrages.[37] Les technologies modernes de e-voting, basées notamment sur le principe de vérifiabilité, permettent d'ailleurs d'identifier de bonne heure de telles intrusions.

La vérifiabilité sert à constater les manipulations des suffrages. A supposer qu'un virus modifie une voix sur l'ordinateur d'un électeur, un système vérifiable le lui signalerait. Dans un premier temps, l'affichage à l'écran d'un code par objet (ou par candidat aux élections) pourrait remplir cette fonction. L'électeur ayant voté comparerait les codes reçus en retour avec les codes personnels faisant partie de son matériel de vote. Et comme les codes sont différents pour chaque objet (ou candidat) et pour chaque électeur, le virus ne «saurait» pas quel code afficher pour tromper l'électeur.

La différence essentielle entre le e-voting et le e-commerce se situe au niveau de la tolérance aux erreurs. Alors qu'un certain pourcentage d'escroqueries est acceptable pour les activités commerciales par voie électronique et que les entreprises – qui réalisent des économies par l'entremise d'Internet – sont d'accord d'en assumer le coût, le vote par voie électronique doivent refléter la volonté de l'électorat. Toute autre attitude affaiblirait la confiance dans la démocratie.

Une extension du cercle des électeurs au vote électronique doit être subordonnée à l'introduction de la vérifiabilité.

[37] http://data.rrb.zh.ch/appl/rrbzhch.nsf/0/C12574C2002FAA1FC1257942004EB439/$file/Evaluation_E-Voting_Z%C3%BCrich.pdf (état: 31 août 2012).

6 Glossaire

Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Annexe	Une annexe (angl.: attachment) est un fichier accompagnant le texte d'un courriel.
Attaque DDoS	attaque par déni de service distribué (Distributed Denial-of-Service attack) Attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux systèmes.
Attaque par force brute	Méthode d'attaque consistant simplement à tester toutes les solutions/tous les mots de passe possibles pour trouver la bonne combinaison.
Backup	Un backup (sauvegarde des données) désigne la duplication de données, dont la restauration permettra de retrouver les données perdues.
Bluetooth	Technologie permettant d'établir une communication sans fil entre deux équipements terminaux, mise en œuvre surtout dans les téléphones mobiles, les ordinateurs portables, les PDA (assistants numériques personnels) et les périphériques d'entrée (p.ex. la souris).
Certificat numérique	Attestation qu'une entité (personne, ordinateur) possède une clé publique (PKI).
Cheval de Troie demandeur de rançon	Maliciel bloquant l'ordinateur pour exiger de son propriétaire le versement d'une rançon (ransomware).
Cheval de Troie des autorités de poursuite pénale allemandes	Logiciel utilisé par la police en Allemagne, dans le cadre d'une instruction pénale, afin p. ex. d'épier la téléphonie par Internet (VoIP).
Cyberadministration	La cyberadministration (e-government) désigne l'utilisation des technologies de l'information et de la communication entre les administrations (fédérale, cantonales, communales, etc.) ainsi qu'entre ces institutions et leurs usagers (particuliers, entreprises) pour simplifier le traitement des processus.
DNS	système de noms de domaine (Domain Name System). Le DNS rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP les utilisateurs composent un nom (p. ex.

	www.melani.admin.ch).
DNS Amplification Attack	Attaque par déni de service (attaque Denial of Service, DoS), utilisant des serveurs DNS publics comme amplificateurs.
Domaines	Tout nom de domaine (p. ex. www.exemple.com) est associé par l'intermédiaire d'un serveur DNS (Domain Name System) à son adresse IP, laquelle permet d'établir une connexion réseau entre ordinateurs.
E-Commerce	Le e-commerce, ou commerce électronique, désigne l'ensemble des activités commerciales effectuées par l'entremise d'Internet.
Event-Viewer	Observateur d'événements: programme signalant les événements significatifs relatifs au système d'exploitation Windows, classés comme erreur, avertissement ou informations.
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.
Fonction de hachage MD5	L'algorithme MD5 (message digest 5) génère une série de chiffres de même longueur, quelle que soit la longueur du texte soumis. Les fonctions de hachage s'emploient dans trois domaines: - cryptographie; - systèmes de banques de données. Les fonctions de ha-chage permettent d'effectuer des recherches efficaces dans une grande masse de données. - sommes de contrôle. Chaque fichier reçoit une valeur hachée. Toute modification est un indice de manipulation.
Géoportail	Plate-forme en ligne dédiée aux informations géographiques.
HTML	HyperText Markup Language Langage de balisage hypertexte. Le HTML permet de créer des pages Web. Il sert à en définir les caractéristiques (p.ex. la structure des pages, la présentation, les liens sur d'autres pages, etc.). Du fait que le HTML est constitué de caractères ASCII, l'édition d'une page HTML peut s'effectuer avec un traitement de texte usuel.

Injection SQL	Une injection SQL exploite une lacune de sécurité liée aux banques de données SQL, dès lors que le concepteur du site Web néglige de contrôler les variables utilisées dans les requêtes SQL. Le pirate cherche à exécuter des requêtes non prévues, pour modifier les données voire contrôler le server.
Internet Archive	Projet de bibliothèque numérique, indexant à intervalles réguliers un maximum de contenus de sites Web pour en accélérer la diffusion. Les clichés des pages Web effacées continuent à pouvoir y être consultés.
logiciels antivirus	Les logiciels antivirus protègent vos données contre les virus, les vers et les chevaux de Troie.
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).
OpenX	OpenX est un logiciel au code source ouvert (open source) permettant de gérer l'affichage des bannières de publicité en ligne.
Patch	Rustine. Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d'erreurs et remédie ainsi p.ex. à une lacune de sécurité.
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.
PHP-Mailer	Programme PHP offrant la possibilité d'envoyer du texte à l'aide d'une fonction d'envoi de messages. Le PHP est un langage de script utilisé pour la réalisation de sites ou applications Web dynamiques.
Porte dérobée	Une porte dérobée (en anglais: backdoor) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un pirate d'accéder secrètement à un programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.

Ransomware	Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate crypte ou efface des données et ne fournit la clé nécessaire pour les sauver qu'après le versement d'une rançon.
Recovery	Action de régénérer des données qui ont été perdues ou contaminées; récupération de données
Remote Administration Tool	Un RAT (Remote Administration Tool, outil de télémaintenance) est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur.
Serveur racine DNS	Les serveurs de noms racines ou serveurs racines (root server) répondent aux requêtes qui concernent les noms de domaine de premier niveau (.com, .net, .ch…). Ils renferment la liste des serveurs (nom/adresse IP) ayant autorité sur tous les domaines de premier niveau.
SHA	Secure Hash Algorithm (algorithme de hachage sécurisé) Le terme SHA désigne un groupe de fonctions de hachage stan-dardisées utilisées en cryptographie. Elles servent au calcul d'une valeur de vérification univoque pour toutes sortes de données élec-troniques.
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.).
Spoofing	Usurpation d'identité électronique, dans le but d'obtenir un accès non autorisé dans un réseau.
Systèmes SCADA	Supervisory Control And Data Acquisition Systèmes servant à la surveillance et à la gestion de processus techniques (p. ex. approvisionnement en énergie et en eau).
Top-Level-Domains	Tout nom de domaine dans Internet est formé d'une série de signes séparés par des points. Le domaine de premier niveau ou de tête (TLD) désigne le dernier élément de cette série et se situe au niveau hiérarchique le plus élevé du nom. Par exemple, si le nom de domaine d'un ordinateur ou d'un site est de.example.com, le TLD sera «com».
URL	Uniform Resource Locator Adresse d'un document Web composée du nom du protocole,

	du nom du serveur et du nom de fichier avec son chemin d’accès (exemple : http://www.melani.admin.ch/test.html).
USB Memory Stick	Clé mémoire USB. Petit dispositif de stockage des données connecté à l'interface USB d'un ordinateur.
Voice Phishing	Variante de l’hameçonnage par courriel (phishing), où le pirate invite la victime par téléphone à lui communiquer ses données d’accès.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.