Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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

Sûreté de l'information

Situation en Suisse et sur le plan international

Rapport semestriel 2012/II (juillet – décembre)

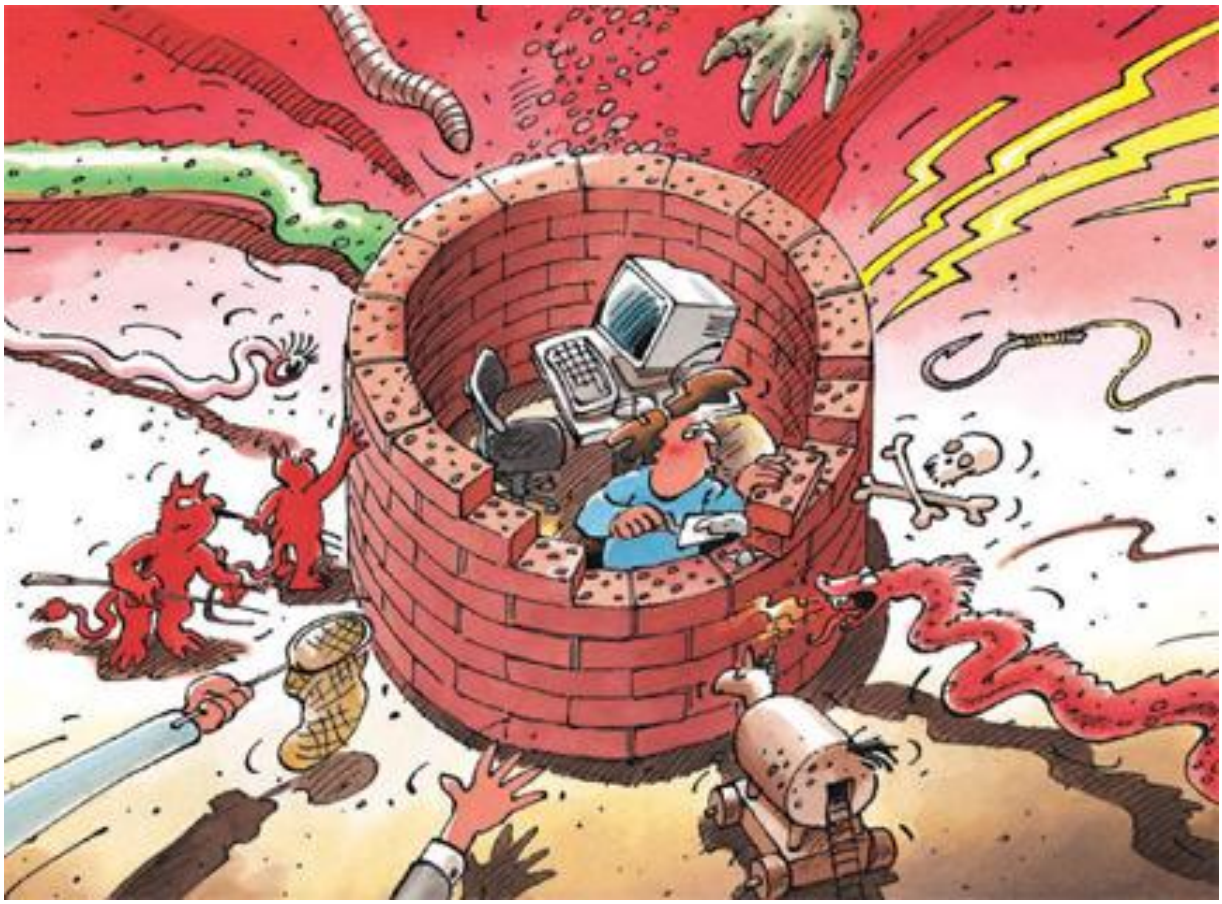


Table des matières

1 Temps forts de l'édition 2012/II

- **Augmentation des cas de phishing**
  Le phishing classique, soit l'envoi de courriels incitant par divers stratagèmes la victime à livrer des données personnelles, est en plein essor. Les pirates se sont surtout concentrés sur les données des cartes de crédit. Or un nouveau mode opératoire s'est ajouté aux nombreuses tentatives assez rudimentaires de fraude à la carte de crédit par phishing, prenant aussi pour cible au deuxième semestre 2012 la clientèle suisse du e-banking.
  ► Situation en Suisse: chapitre 3.1

- **DDoS – attaques massives contre diverses banques américaines**
  Les attaques par déni de service distribué (DDoS), lancées pour paralyser un service d'information, font désormais partie des principaux risques encourus par les réseaux. Dès septembre 2012, des attaques DDoS parfois massives ont été signalées contre diverses banques américaines. D'autres attaques DDoS ont fait les gros titres.
  ► Situation en Suisse: chapitre 3.7
  ► Situation sur le plan international: chapitre 4.2

- **Cyberconflit au Proche-Orient – Mise à jour**
  Lors de ses analyses du maliciel Flame, le fabricant russe d'antivirus Kaspersky Lab a découvert un autre maliciel, qu'il a baptisé Gauss. Il s'agit du premier cas connu où un logiciel d'espionnage raffiné, probablement d'origine étatique, s'en prend aux opérations bancaires en ligne. Les ordinateurs infectés par ce cheval de Troie se trouvaient principalement au Liban, suivi d'Israël et des territoires palestiniens.

  Une infection par maliciel a paralysé la société pétrolière étatique saoudienne Saudi Aramco. Peu après, le producteur de gaz naturel qatari RasGas a dû couper son réseau interne du monde extérieur. Même en l'absence de confirmation officielle, divers experts pensent que RasGas a été victime de la même cyberarme. Ces experts occidentaux soupçonnent l'Iran, dont les exportations énergétiques font les frais des sanctions internationales, de vouloir empêcher les Etats arabes d'augmenter leur production pétrolière et gazière.
  ► Situation sur le plan international: chapitre 4.1, chapitre 4.2

- **Dépendance des TIC dans la vie de tous les jours – toujours et partout**

  Depuis plusieurs années, les cyberattaques ne se limitent plus aux ordinateurs et aux serveurs. Tout système informatique risque d'en faire les frais. Entre autres exemples, des cyberpirates sont en mesure d'ouvrir la serrure électronique d'une chambre d'hôtel. La dépendance actuelle de la société face aux TIC comporte de nombreuses facettes.
  ► Situation en Suisse: chapitre 3.4
  ► Situation sur le plan international: chapitre 4.3, chapitre 4.6

- **Réglementation versus liberté – Comment accroître la sécurité d'Internet?**
  Internet ne fait l'objet d'aucune réglementation étatique et reste un espace de liberté, soumis principalement à des normes techniques et à des directives administratives (appelées «policies»). Il existe toutefois une puissante coalition de pays aspirant à une réglementation d'Internet. Très attachés à leur souveraineté, ces Etats cherchent à étendre leur pouvoir de contrôle sur le cyberespace.
  ► Situation sur le plan international: chapitre 4.9
  ► Tendances / Perspectives: chapitre 5.3

2 Introduction

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

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

Les **chapitres 3 et 4** passent en revue les pannes et les incidents, les attaques, la criminalité et le terrorisme visant les infrastructures TIC. Des exemples choisis illustrent les principaux événements des six derniers mois de l’année 2012. La situation nationale est analysée au chapitre 3 et la situation internationale au chapitre 4.

Le **chapitre 5** livre des tendances et présente les développements attendus.

3 Situation en Suisse de l'infrastructure TIC

3.1 Phishing – tendances actuelles

Le *phishing* classique, soit l'envoi de courriels incitant par divers stratagèmes la victime à livrer des données personnelles, est en plein essor. Les pirates se sont généralement concentrés sur les données des cartes de crédit. Aux nombreuses tentatives assez rudimentaires de fraude par phishing sont venues s'ajouter, au deuxième semestre 2012, des attaques par *voice phishing*, elles aussi dirigées contre la clientèle suisse du e-banking. A la différence des *maliciels* s'en prenant aux applications de e-banking, de telles attaques n'exigent qu'une infrastructure rudimentaire et sont à la portée même des non-spécialistes. Il suffit généralement d'un ordinateur et/ou d'un téléphone.

3.1.1 Attaques combinées de phishing et de voice phishing

Un nouveau mode opératoire a fait son apparition en automne 2012 dans les escroqueries par phishing. Des courriels d'hameçonnage prétendent qu'une banque aurait installé un nouveau système de sécurité, afin de mieux protéger ses comptes de e-banking. Un soi-disant employé de la banque prendra contact par téléphone avec la victime et l'assistera dans les démarches nécessaires. La victime est par conséquent priée d'indiquer, outre ses données personnelles, son numéro de téléphone.

Puis les victimes reçoivent des escrocs – ce qui ne s'était encore jamais vu en Suisse – un appel les invitant, sous prétexte d'améliorer les mesures de sécurité, à révéler leur mot de passe et le second élément de sécurité. La victime est par exemple priée de saisir un code sur son lecteur de cartes et de communiquer le résultat affiché au pirate. Ce dernier peut ainsi se connecter au compte de e-banking et effectuer un paiement. A supposer que le système prévoie une *signature de transaction*, l'escroc se renseigne à nouveau selon la même méthode. Les auteurs des appels font preuve d'un grand professionnalisme et maîtrisent notamment le suisse-allemand.

3.1.2 Sites de phishing avec protocole https

Il était à prévoir que tôt ou tard, les escrocs se mettraient à utiliser des sites de phishing basés sur un protocole sécurisé (pages https). Les premières vagues de courriels renvoyant à de tels sites sont apparues en automne 2012. Un lien URL débutant par https:// *(hyper text transfer protocol secure)* indique que les informations du site font l'objet d'une transmission sécurisée.

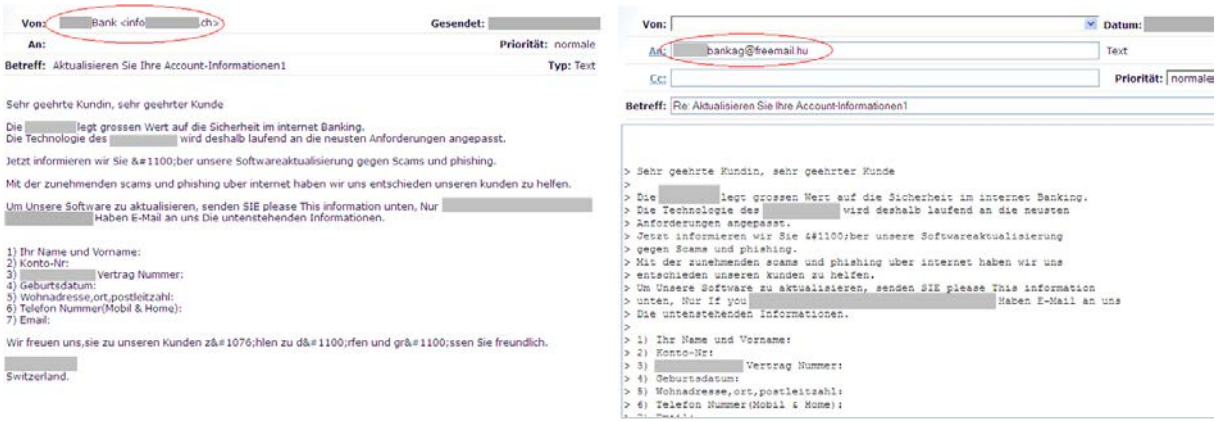
Le cas échéant, les escrocs ne possédaient pas de *certificat* spécial et s'étaient contentés d'utiliser le *certificat* d'un site piraté. Il ne s'agit toutefois pas d'une tendance générale, et de tels cas sont restés isolés.

Figure 1: site de phishing avec protocole sécurisé.

3.1.3 Toujours plus de courriels de phishing sans site ad hoc

Comme l'expliquait déjà le dernier rapport semestriel MELANI[1], les escrocs cherchent également à accéder aux données de leurs victimes sans site de phishing classique, enregistré sur un serveur Web. Deux méthodes sont employées à cet effet. La première consiste à joindre au courriel une page de phishing, sous forme de formulaire HTML. Cette page HTML est créée localement sur l'ordinateur du destinataire, à l'ouverture du message. Une fois les champs du formulaire complétés et le bouton «Envoi» appuyé, les données parviennent «directement» au pirate.

La seconde méthode est encore plus simple. Le formulaire y fait partie intégrante du courriel. Il suffit dès lors d'une adresse électronique spécialement conçue pour l'escroquerie. Les pirates profitent encore de la possibilité de définir pour chaque courriel une adresse de réponse différente de celle d'où il semble provenir. Ainsi, ce n'est qu'en appuyant sur le bouton de réponse que la victime, qui croyait être en contact avec un établissement financier, peut voir où le courriel est réellement envoyé.



[1] MELANI rapport semestriel 2012/1, chapitre 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: 28 février 2013).

Figure 2: courriel de phishing avec adresse de réponse spécialement préparée. Le courriel semble émaner du service d'information d'une banque suisse, mais la réponse ira en réalité à une adresse créée auprès d'un fournisseur hongrois de services de messagerie gratuits.

Ces deux méthodes dispensent le pirate de compromettre un serveur Web ou d'exploiter son propre serveur afin d'héberger son site de phishing. En effet, de tels sites sont rapidement désactivés, une fois l'escroquerie signalée aux autorités de sécurité ou à l'hébergeur.

3.1.4 Premier nom de domaine suisse révoqué à la demande de MELANI

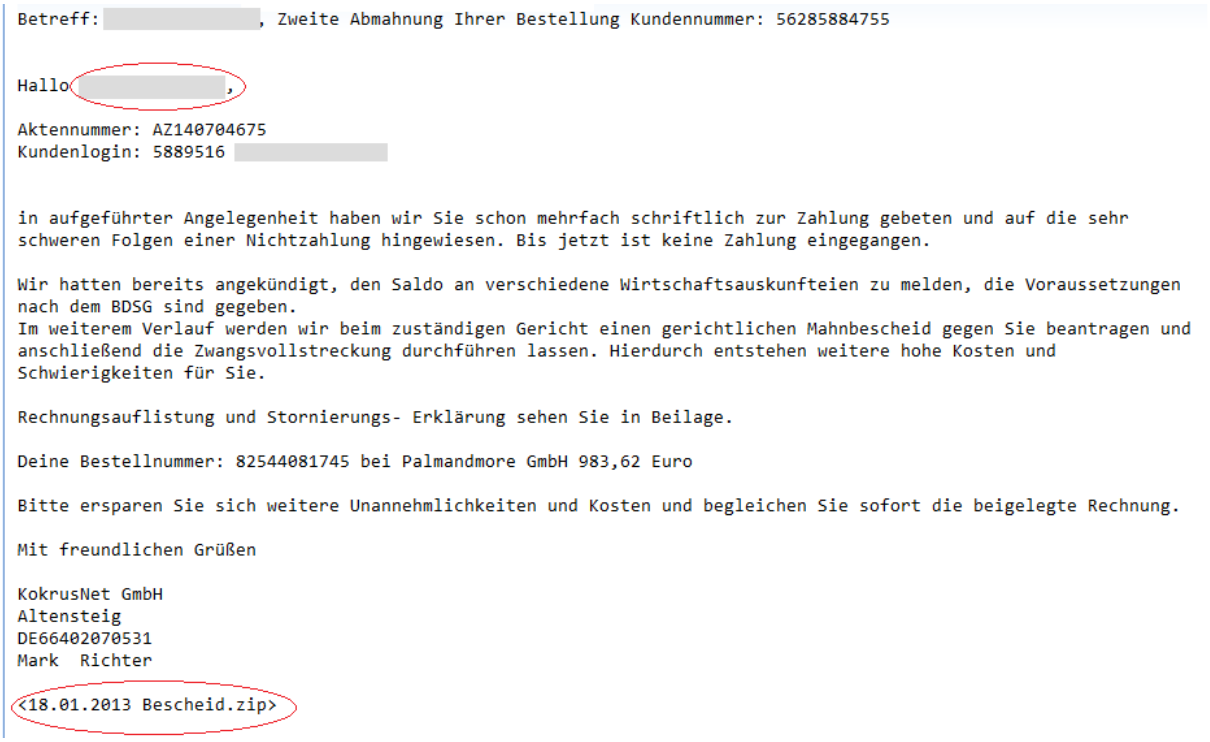
Afin de combattre toute utilisation abusive des noms de domaine se terminant par « .ch » et de protéger les internautes de risques particulièrement graves, la révision de l'ordonnance sur les ressources d'adressage dans le domaine des télécommunications (ORAT, RS 784.104; en vigueur depuis le 1er janvier 2010) a introduit un nouvel article, en vertu duquel le registre «.ch» (SWITCH) doit bloquer un nom de *domaine* et supprimer l'assignation y relative à un serveur de noms si un service de lutte contre la cybercriminalité reconnu par l'Office fédéral de la communication (OFCOM) a présenté une demande de blocage, ou s'il existe un soupçon fondé de présumer que le nom de domaine en question est utilisé de manière illicite. Concrètement, il doit être utilisé soit pour accéder par des méthodes illicites (*phishing*) à des données sensibles, soit pour diffuser des logiciels malveillants (*malware*). SWITCH peut prendre de son propre chef cette mesure de prévention des menaces et la maintenir durant cinq jours ouvrables au maximum. SWITCH a déjà souvent recouru à cette possibilité, notamment pour protéger les visiteurs de sites Web piratés. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a récemment dû faire usage de cette compétence pour la première fois.

Un site de phishing possédant un nom de domaine se terminant par « .ch » a été signalé à MELANI en décembre 2012. Il avait été exclusivement conçu pour cette attaque et il ne s'agissait pas – comme c'est souvent le cas – d'un site compromis, où les pirates hébergent normalement leur page de phishing dans un sous-répertoire. MELANI a alors décidé de prolonger le blocage de cinq jours opéré par SWITCH de 30 jours supplémentaires, tout en chargeant SWITCH de procéder à la vérification de l'identité du titulaire du nom de domaine. Comme celui-ci n'a pas répondu, le nom de domaine a été révoqué.

3.2 Fausses factures avec maliciel en annexe

Depuis plusieurs mois, toujours plus de courriels se référant à une commande, une livraison ou une facture (fictives) et dont l'expéditeur a été falsifié sont en circulation. MELANI reçoit chaque semaine plusieurs annonces dans ce sens. Les expéditeurs cherchent à intimider le destinataire, en lui annonçant des rappels impliquant des frais et d'éventuelles poursuites judiciaires, pour l'amener à ouvrir l'annexe. Cette dernière contient un maliciel, se trouvant généralement dans un fichier zip.

Dans les cas connus de MELANI, ces courriels ont fait l'objet d'un envoi personnalisé, et donc appelaient le destinataire par ses nom et prénom. L'adressage personnel tend à se répandre, car les courriels frauduleux semblent ainsi plus dignes de confiance.



Betreff: , Zweite Abmahnung Ihrer Bestellung Kundennummer: 56285884755

Hallo ,

Aktennummer: AZ140704675
Kundenlogin: 5889516

in aufgeführter Angelegenheit haben wir Sie schon mehrfach schriftlich zur Zahlung gebeten und auf die sehr schweren Folgen einer Nichtzahlung hingewiesen. Bis jetzt ist keine Zahlung eingegangen.

Wir hatten bereits angekündigt, den Saldo an verschiedene Wirtschaftsauskunfteien zu melden, die Voraussetzungen nach dem BDSG sind gegeben.
Im weiterem Verlauf werden wir beim zuständigen Gericht einen gerichtlichen Mahnbescheid gegen Sie beantragen und anschließend die Zwangsvollstreckung durchführen lassen. Hierdurch entstehen weitere hohe Kosten und Schwierigkeiten für Sie.

Rechnungsauflistung und Stornierungs- Erklärung sehen Sie in Beilage.

Deine Bestellnummer: 82544081745 bei Palmandmore GmbH 983,62 Euro

Bitte ersparen Sie sich weitere Unannehmlichkeiten und Kosten und begleichen Sie sofort die beigelegte Rechnung.

Mit freundlichen Grüßen

KokrusNet GmbH
Altensteig
DE66402070531
Mark Richter

<18.01.2013 Bescheid.zip>

Figure 3: Exemple de fausse facture personnalisée, avec maliciel en annexé (Bescheid.zip).

3.3 Systèmes de contrôle non protégés contre les intrusions en ligne

La sécurité des systèmes de contrôle industriels (SCI) est un thème toujours plus souvent abordé non seulement par les experts en sécurité, mais aussi par les médias.[2] Selon l'Industrial Control System *CERT* (ICS-CERT) américain, qui a lancé une mise en garde à fin octobre[3], les attaques contre de tels systèmes sont en hausse. Cet avertissement était dû à l'offre toujours plus abondante d'outils permettant aux criminels de repérer de tels systèmes et de s'y introduire. Il n'est même pas nécessaire de posséder des connaissances spéciales. L'outil le plus connu est indiscutablement le moteur de recherche SHODAN, qui existe depuis plusieurs années et qui permet de repérer les systèmes *SCADA*, dont il a déjà été

[2] http://www.br.de/fernsehen/das-erste/sendungen/report-muenchen/report-februar-102.html (état: 28 février 2013).

[3] http://ics-cert.us-cert.gov/index.html (état: 28 février 2013).

question dans un précédent rapport[4]. Ce moteur de recherche a permis à l'ICS-CERT de localiser plus de 500 000 systèmes. Outre SHODAN, il existe par exemple un projet du nom d'ERIPP (Every Routable IP Project).

De nombreux exploitants de systèmes de contrôle industriels ont mis l'accent jusqu'ici sur un fonctionnement stable, négligeant la sécurité des manipulations. Sans doute beaucoup ignorent-ils que leurs systèmes sont reliés à Internet. En outre, de nombreux fabricants programment par défaut, dans l'application, des mots de passe universels leur permettant d'accéder aux systèmes même en cas de perte des données d'accès. Si elle garantit la poursuite d'une exploitation stable en cas d'oubli du mot de passe, une telle solution constitue toutefois un vecteur d'attaque. En août 2012, le chercheur en sécurité informatique Justin W. Clarke a rendu public un autre cas critique. Il a découvert dans le système d'exploitation propriétaire Rugged OS, utilisé dans les centrales électriques ou dans la surveillance du trafic, une *clé RSA* secrète pourvue d'un code fixe. Une fois la clé connue, il devient possible de décrypter et d'épier le trafic sécurisé du réseau. L'ICS-CERT, organisme de sécurité américain, a alors émis une mise en garde.[5]

Phil Kernick, expert australien des questions de sécurité, a identifié un autre problème. Presque tous les incidents *SCADA* qu'il a examinés impliquaient des maliciels. Ces derniers n'avaient pourtant pas été spécialement conçus contre les systèmes SCADA. Il s'agissait p. ex. de *maliciels* couramment utilisés contre le e-banking. Or une fois infectés, les systèmes SCADA ne présentaient plus un fonctionnement stable et tombaient parfois en panne, avec les graves conséquences qui s'ensuivent. La raison tient généralement à l'absence de séparation stricte entre les réseaux de contrôle et les réseaux Office. De même, la possibilité (offerte p. ex. au personnel ou aux partenaires externes) de raccorder des périphériques de sauvegarde USB ou des ordinateurs mobiles s'avère souvent problématique, faute la plupart du temps des nécessaires politiques de sécurité pour les utilisateurs et/ou de mesures techniques de protection.

En principe, il ne faudrait relier les machines à Internet que si c'est indispensable à leur bon fonctionnement. Le cas échéant, il s'agit bien entendu de suffisamment protéger de tels systèmes, à l'aide de pare-feu et de mots de passe forts. Et pour éviter toute propagation de maliciels des ordinateurs de bureau aux systèmes SCADA, on veillera à séparer ces deux réseaux.

Alors même que MELANI avait déjà signalé, dans son rapport semestriel 2011/2, la présence en Suisse de 34 systèmes vulnérables identifiés par le moteur de recherche SHODAN, de tels cas se sont reproduits durant l'année sous revue. Soit les systèmes en question ne possédaient aucun mot de passe, soit ils avaient conservé celui d'origine, qu'il aurait fallu modifier lors de la mise en service. Même si ces cibles potentielles ne sont généralement pas considérées comme sensibles, quiconque installe un système de pilotage relié à Internet sans modifier son mot de passe d'origine néglige un principe élémentaire en matière de sécurité informatique. Quant à l'entreprise dont le réseau de chauffage ou de climatisation serait accessible en ligne et manipulable, elle s'expose à de mauvaises surprises.

En outre, les possibilités d'accéder, à la faveur de leur intégration partielle, à d'autres applications administratives internes, tels les logiciels de facturation, augmentent le potentiel

[4] Voir rapport MELANI 2011/2, chapitre 3.9: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 28 février 2013).

[5] http://ics-cert.us-cert.gov/pdf/ICS-ALERT-12-234-01.pdf (état: 28 février 2013).

d'abus. Par principe, les systèmes de contrôle industriels ne devraient pas être reliés à Internet. Et si cela devait s'avérer indispensable, une extrême prudence s'impose.

3.4 Panne des feux de circulation dans le canton de Vaud

Une panne informatique du système vaudois de gestion du trafic survenue le 16 juillet 2012 a gêné la circulation et provoqué un gigantesque bouchon sur l'autoroute, entre Lausanne et Chexbres. Vers 16 heures, la division de la police vaudoise chargée de la surveillance du trafic a constaté des problèmes techniques. Peu après, le système a cessé de réagir et la signalisation a été mise hors service. C'est ainsi que dans le tunnel de Flonzaley, la bande de gauche est restée bloquée et n'a pu être rouverte au trafic, provoquant ainsi un bouchon de 15 kilomètres. Seule l'intervention manuelle d'un technicien a permis de normaliser peu à peu la situation du trafic entre Lausanne et Chexbres à partir de 19h30. La panne informatique proprement dite n'a été résolue qu'à 01h40 du matin.

En outre, la transmission des alarmes des tunnels des autoroutes vaudoises a elle aussi été interrompue. En cas d'incendie ou d'accident, le système d'alarme du tunnel n'aurait pas fonctionné. Les caméras de surveillance avaient beau continuer à fournir des images, il n'était pas possible de les déplacer. C'est ce qui a conduit à déployer les forces de police aux emplacements stratégiques.[6]

Même s'il s'agissait d'une panne et non d'une cyberattaque, cet incident montre clairement à quel point la société actuelle dépend des TIC. La signalisation routière recourt elle aussi toujours plus aux TIC pour gérer les flux croissants du trafic, alors que l'infrastructure reste inchangée. De tels systèmes sont toutefois conçus pour afficher, en cas de dysfonctionnement, une lumière clignotante jaune. Le scénario où tous les usagers de la route auraient le feu vert, qui aboutirait à des accidents, est ainsi exclu.

3.5 Panne chez Ricardo

Le 28 octobre 2012, le site d'enchères en ligne ricardo.ch a connu de graves problèmes informatiques. Une erreur apparue dans la banque de données a empêché près d'un tiers des clients de miser, et cela pendant plusieurs heures. Par conséquent, les produits se sont généralement écoulés bien en dessous de leur valeur, puisque les ventes se sont faites malgré cette panne. Or il est bien connu que dans une vente aux enchères, les dernières minutes sont les plus lucratives. Ricardo.ch a fait savoir qu'en raison de l'expiration du délai pour surenchérir, les produits «devaient dans tous les cas être cédés au plus offrant».

Deux semaines plus tard et en raison sans doute des nombreuses protestations reçues de clients, le discours avait changé. Dans l'évaluation initiale, on était parti de l'idée que les offres en question seraient automatiquement prolongées, ce qui n'avait pas toujours été le cas. Ricardo.ch rappelait désormais que dans de telles circonstances, les vendeurs ne sont en principe pas liés par le contrat et qu'ils peuvent s'adresser à son service à la clientèle[7] : Ricardo s'est montré conciliant avec ses clients, et a remboursé à certains des sommes plus élevées.

---

6 http://www.vd.ch/autorites/departements/dse/police-cantonale/medias/communiques-de-presse/articles/disfonctionnement-reseau-informatique-gerant-la-signalisation-routiere-sur-les-autoroutes-vaudois/ (état: 28 février 2013).

7 http://blog.ricardo.ch/2012/11/teilausfall-von-ricardo-ch-am-28-oktober-2012/ (état: 28 février 2013).

Comme pratiquement n'importe quelle entreprise, ricardo.ch exclut toute responsabilité en cas de problème technique. C'est donc généralement au client à assumer le risque. Ainsi, les conditions générales de Ricardo.ch précisent que l'entreprise n'assume de responsabilité que pour une indisponibilité passagère de son site web, une défaillance de certaines ou de toutes les fonctions du site ou pour des dysfonctionnements de ce dernier résultant du dol ou de la négligence grave de sa part. En cas de négligence légère, ricardo.ch n'assume en particulier aucune responsabilité pour des problèmes techniques en raison desquels des offres ou des offres d'enchères seront acceptées ou traitées tardivement ou de manière erronée.[8] Or en cas d'incident, a fortiori quand de l'argent est en jeu, les conditions générales subissent généralement de fortes pressions publiques. Et bien souvent, les entreprises renoncent à les faire valoir et se montrent conciliantes, pour éviter que leur réputation ne soit mise à mal.

3.6 Attaque DDoS contre le site Inside Paradeplatz

Le site Web «Inside Paradeplatz» a été paralysé à deux reprises en trois mois, à cause d'une attaque par déni de service distribué (DDoS). En juin déjà, des inconnus s'en étaient pris au site et lui avaient envoyé des milliers de requêtes à la seconde, le rendant temporairement inaccessible. L'incident s'est reproduit au début de septembre, mais pour une durée bien supérieure à la première attaque, qui avait été repoussée au bout d'un jour et demi. En outre, le site personnel de l'exploitant a apparemment été compromis en parallèle à la seconde attaque et a subi une infection par *drive-by download*.[9] Selon l'exploitant, quiconque recherchait ce site via Google et cliquait sur son hyperlien voyait s'afficher une mise en garde dans ce sens. Toujours selon ce dernier, l'agresseur visait à l'empêcher de diffuser des informations par un autre canal. Ces indices font penser à une attaque ciblée. Or en pareil cas, il est très difficile de découvrir l'agresseur, qui veille à brouiller les pistes.

Les attaques *DDoS* comptent désormais parmi les principaux dangers guettant les réseaux. Le chapitre 4.2 offre un bref tour d'horizon des attaques DDoS survenues à l'étranger. L'attaque décrite ci-dessus ne correspond toutefois guère au schéma habituel des attaques DDoS. Le fait que le site privé de l'exploitant ait également subi une infection par *drive-by download* autorise toutes les spéculations. La raison invoquée par l'exploitant, à savoir que les pirates cherchaient à empêcher par l'infection du site que des informations ne soient diffusées par un autre canal, n'est pas entièrement convaincante. Car pour y parvenir, il aurait suffi à l'agresseur de lancer une attaque DDoS contre ce site privé également.

Une autre possibilité est que les escrocs visaient à infecter de façon ciblée les ordinateurs des personnes faisant partie de l'entourage de l'exploitant avec un maliciel, afin d'accéder à des informations. En effet, la probabilité est grande que les connaissances de l'exploitant se rendent d'abord sur son site privé, afin d'apprendre pourquoi son site officiel a cessé de fonctionner.

[8] http://www.ricardo.ch/ueber-uns/Portals/ch-ueber-uns/Docs/downloads-pdf-de/AGB_DE.pdf (état: 28 février 2013).

[9] http://insideparadeplatz.ch/2012/08/28/inside-paradeplatz-im-visier-von-hackern/ (état: 28 février 2013).

3.7 Un cadeau d'Apple ou une arnaque potentielle?

Un *SMS* rédigé en mauvais allemand, qui faisait miroiter à ses destinataires un cadeau d'Apple, a été mis en circulation en novembre 2012. MELANI suppose, sur la base des nombreuses réactions lui étant parvenues, que le SMS a été envoyé à grande échelle. Il contenait un code et un lien. Les noms de domaine étaient tous formés sur le même modèle et indiquaient «.cc» comme domaine de premier niveau (*top level domain*).

Figure 4: SMS annonçant un prétendu gain.

Pour recevoir un iPhone 5 gratuit, il fallait inscrire sur le site Web indiqué le code transmis par SMS. Des analyses ont montré que même en introduisant n'importe quel chiffre, le visiteur était redirigé vers un site. Ce simple constat donnait une piètre image du SMS, qui n'était au fond qu'un prétexte pour obtenir du destinataire une manipulation spécifique.

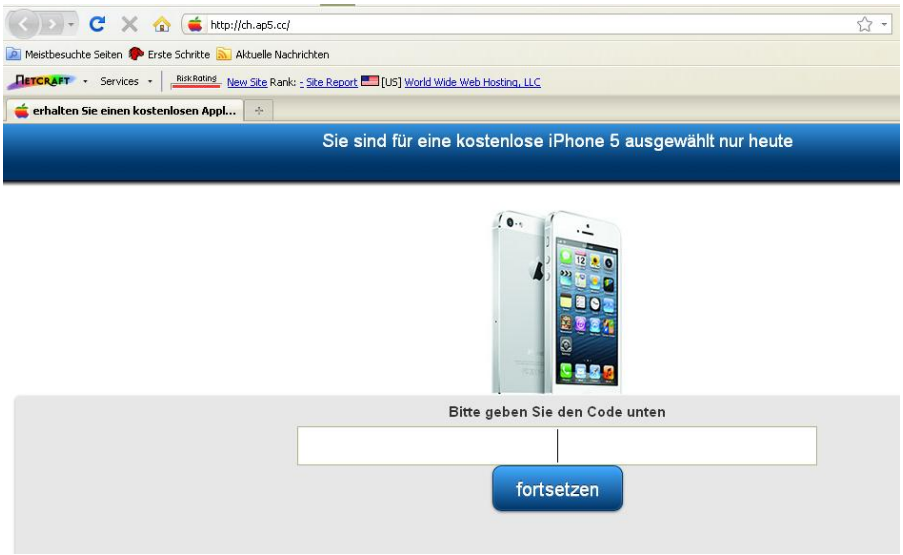


Figure 5: Page où il fallait inscrire le prétendu code gagnant.

Après avoir inscrit le code gagnant, la victime était redirigée sur le site d'une plate-forme d'enchères online appelée «Ziinga». Il faut y indiquer ses nom et prénom, son adresse et son sexe, et accepter les conditions générales de Ziinga. Une telle demande ne surprendra guère la personne persuadée d'avoir gagné un iPhone. Or l'acceptation des conditions générales aboutissait à l'abonnement le plus cher («platine») à 89.99$ par mois.

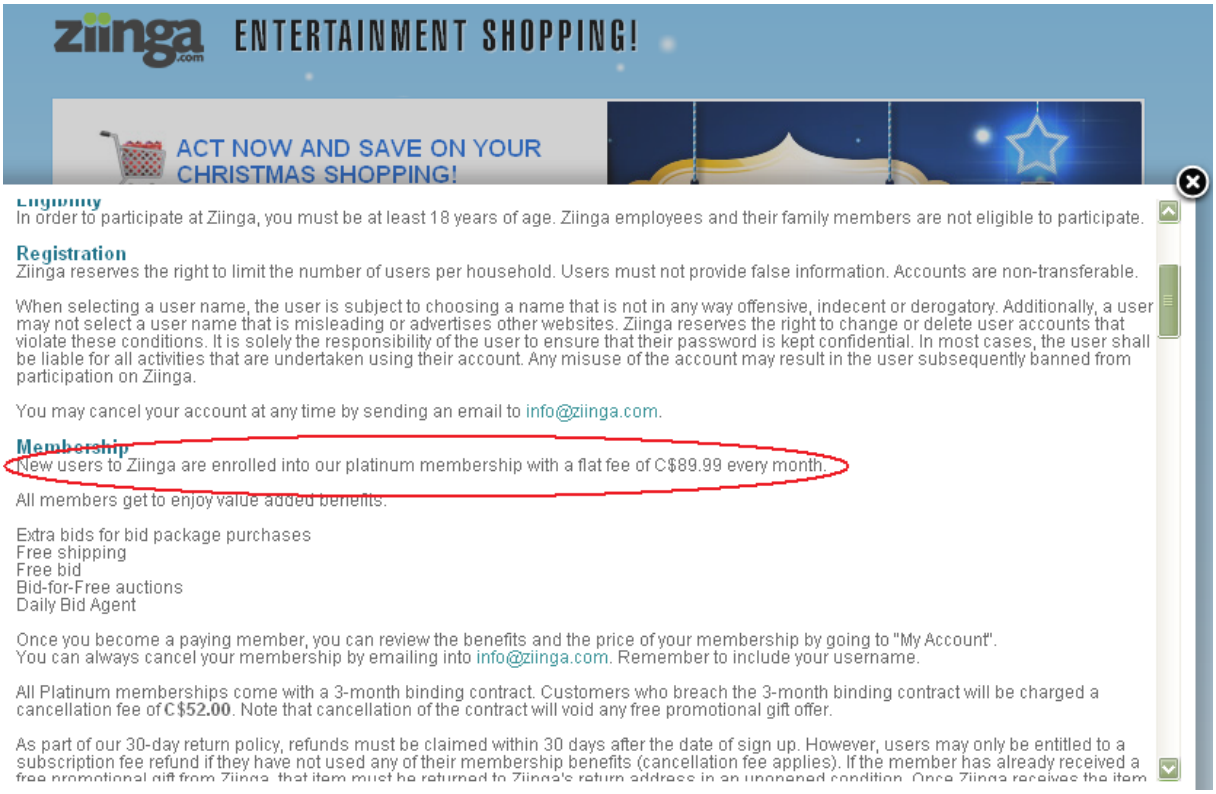


Figure 6: Conditions générales de Ziinga (état: 30 novembre 2012).

Ziinga est mentionné sur Wikipedia. Bien qu'il soit signalé comme «non neutre», l'article est informatif. Des utilisateurs ont déploré que la cotisation facturée aux membres fasse l'objet d'une publication cachée dans les conditions générales[10]. Et si une résiliation est en tout temps possible, une taxe de de £ 28 (USD 52) est perçue. Dans le cas d'espèce, Ziinga s'est toutefois distancié des SMS envoyés et a exclu toute collaboration. Il reste à savoir qui, en dehors de Ziinga, avait intérêt à ce que de tels SMS soient expédiés. Le véritable auteur de l'envoi n'a pu être identifié. Quant aux sites indiqués, ils ne contenaient aucun maliciel.

L'envoi pourrait aussi avoir eu pour but de vérifier la validité des numéros de téléphone mobiles. Chaque lien envoyé était en effet unique et renfermait un code associé au numéro appelé. En cliquant sur ce lien, le destinataire signalait à l'expéditeur que son téléphone était en service. Comme de surcroît il fallait indiquer une adresse électronique, il devenait même possible de relier le numéro de téléphone mobile à l'adresse électronique. De telles données sont susceptibles soit de servir à mener des attaques de phishing ciblées, soit d'être revendues aux milieux intéressés.

[10] http://en.wikipedia.org/wiki/Ziinga#Controversy (état: 28 février 2013).

3.8 Réapparition du piratage téléphonique[11]

Le piratage téléphonique (*phreaking*), pratique remontant aux premiers centres de relais automatiques des compagnies téléphoniques, a culminé dans les années 1970 jusqu'au milieu des années 1990. L'invention du phreaking est attribuée à un individu se faisant appeler «Cap'n Crunch». Il s'agissait de s'introduire dans des systèmes téléphoniques, afin p. ex. de lancer des appels gratuits. Les raccordements fixes et, désormais aussi, les systèmes *VoIP* de particuliers ainsi que les systèmes téléphoniques d'entreprises de toute taille sont concernés. Si l'attaque aboutit, les systèmes téléphoniques piratés pourront servir à diverses formes d'escroqueries.

Les pirates accèdent aux systèmes téléphoniques notamment par leurs logiciels de maintenance. Ces derniers sont fréquemment protégés par un simple numéro *PIN* standard. Mais les escrocs parviennent régulièrement aussi à s'introduire dans des systèmes téléphoniques protégés et soigneusement entretenus. Afin de rester anonymes et de brouiller les pistes, ils procèdent p. ex. par usurpation d'identité (*spoofing*). Concrètement, ils dissimulent leur propre numéro et affichent celui d'une autre personne. Tant la technique correspondante que les numéros PIN standard sont disponibles sur Internet.

Le mode opératoire le plus fréquent fait appel aux numéros de service à valeur ajoutée. De tels numéros permettent d'offrir une prestation de service payée par l'appelant, avec un supplément de prix sur les taxes de télécommunication (à l'instar des numéros 0900 en Suisse). Dans cette variante, l'escroc commence par s'introduire dans le système téléphonique d'une entreprise. Grâce à cette prise de contrôle, il peut ensuite relier les lignes de l'installation téléphonique à un numéro de service à valeur ajoutée créé par lui. Et pour que la victime ne s'en aperçoive pas trop vite, les attaques se font en dehors des heures de travail. Comme dans cette variante les escrocs accaparent de nombreuses lignes téléphoniques, la probabilité d'être découvert serait bien plus grande aux heures de bureau. L'attaque principale est souvent précédée d'essais de moindre importance. Les numéros surtaxés en cause sont généralement exploités dans des pays où il est très difficile de remonter aux auteurs des infractions.

Une autre variante prend pour cibles les systèmes de paiement en ligne. Divers points de vente, comme les kiosques ou les stations-service, proposent des cartes à prépaiement. Les escrocs usurpent par *spoofing* un numéro de service du fabricant et contactent certains de ses points de vente. Croyant parler à un représentant du fournisseur habituel, le personnel révélera les codes et informations des cartes à prépaiement. Les escrocs s'empresseront ensuite de vider les cartes en ligne. De tels dommages sont irréversibles. Les auteurs de ce genre de *piratage téléphonique* ont besoin d'informations d'initié. En plus de connaître le numéro de service de l'entreprise, ils doivent maîtriser les processus techniques et le système de support.

Par ailleurs, les systèmes *VoIP* piratés permettent de mener des attaques de phishing téléphonique (*vishing*, voir chapitre 3.1).

Le *piratage téléphonique (phreaking)* nécessite des connaissances techniques. Même si des instructions détaillées sont publiées en ligne, il faut constamment s'adapter aux nouvelles prescriptions de sécurité et ajuster son approche, ce qui peut demander des compétences de programmation. En outre, pour s'introduire dans des systèmes téléphoniques sécurisés et protégés, il faut disposer d'informations détaillées sur l'organisation de l'entreprise prise pour

[11] Ce sous-chapitre se base sur un rapport aimablement mis à disposition de MELANI par l'Office fédéral de la police (fedpol).

cible, sur ses processus et son personnel (connaissances d'initié). Tout indique toutefois qu'à l'avenir, le *piratage téléphonique* sera toujours plus simple et s'étendra à de nouveaux domaines. On peut s'attendre à ce que les *smartphones* soient davantage pris pour cible. Après avoir pris le contrôle d'un téléphone mobile, les pirates en profiteront par exemple pour souscrire à des services *SMS* payants.

3.9 Deuxième exercice paneuropéen «Cyber Europe 2012» – nouvelle participation de la Suisse

Le 4 octobre 2012, plus de 500 professionnels de la cybersécurité ont participé à Cyber Europe 2012. Ce deuxième cyberexercice paneuropéen, basé sur des activités de communication et de coordination déployées au niveau tant national qu'européen, visait à améliorer la capacité de résistance (résilience) des infrastructures d'information critiques. Cyber Europe 2012 a ainsi constitué une étape marquante dans les efforts consentis pour renforcer au niveau européen la coopération, l'état de préparation et la réaction en matière de cybercrise.

Cyber Europe 2012 avait trois objectifs:

- tester l'efficacité et les capacités d'évolution des procédures standard réglant la coopération des pouvoirs publics en Europe;
- explorer la coopération entre les acteurs publics et privés en Europe;
- identifier les lacunes et défis quant à la façon de traiter les incidents cybernétiques à grande échelle en Europe.

29 Etats membres de l'UE/AELE étaient impliqués dans la manifestation; 25 d'entre eux ont participé activement à l'exercice, tandis que les quatre autres étaient présents en tant qu'observateurs. En outre, diverses institutions de l'UE étaient engagées. Soit au total 339 organisations, représentées par 571 acteurs. Conformément à une recommandation de Cyber Europe 2010 duquel ils étaient absents, des acteurs du secteur privé ont pris part à l'exercice (dont pour la Suisse deux entreprises télécom et deux du secteur financier). Les acteurs publics et privés ont coopéré au niveau national, tandis que les pouvoirs publics mettaient en place une coopération transfrontalière.[12]

Le scénario de l'exercice consistait à simuler une série de cyberincidents à grande échelle, affectant tous les pays participants: des adversaires fictifs s'associaient pour déstabiliser l'Europe, principalement au travers d'attaques *DDoS* contre des services publics électroniques. Les services touchés étaient des services d'e-government et des services financiers (e-banking, etc.). Ces cyberincidents – un défi pour les participants des secteurs public et privé – impliquaient une collaboration internationale.

L'exercice «Cyber Europe 2012» a permis de tester, comprendre et évaluer les mécanismes européens de cybercoopération en place. Il a également intensifié la coopération en vue de la gestion des cyberincidents.

Expériences et conclusions:

[12] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/ENISA_2012_00490000_DE_TRA.pdf (état: 28 février 2013).

- Tous les pays participants se sont pleinement impliqués durant l'exercice, où de nombreuses interactions bilatérales et multilatérales ont eu lieu au niveau international.
- Des procédures opérationnelles et des outils de communication standardisés ont permis aux divers pays de bien évaluer la situation au cours de la cybercrise simulée.
- Les procédures opérationnelles n'ont pas toujours été adaptables comme souhaité au grand nombre de pays participants.
- Il est crucial que les protagonistes connaissent bien les procédures opérationnelles, pour obtenir une capacité de réaction rapide et efficace à travers toute l'Europe.
- En Suisse, les contacts ont bien fonctionné avec les participants du secteur privé. La difficulté tenait plutôt à la grande quantité d'informations à traiter.
- La présence d'infrastructures techniques adéquates et stables ainsi que d'outils de pointe s'avère cruciale pour garantir une coopération efficace et sans accrocs.
- «Cyber Europe 2012» a contribué à établir la confiance entre les pays, ce qui est capital lorsqu'il s'agit de déployer des activités efficaces et rapides pour limiter les risques d'une cybercrise réelle. L'exercice a favorisé la mise en place de nouvelles relations et renforcé celles déjà en place.

4 Situation internationale de l'infrastructure TIC

4.1 Cyberconflit au Proche-Orient – mise à jour

4.1.1 Gauss: cheval de Troie espionnant le e-banking

Lors de ses analyses du maliciel Flame[13], le fabricant russe d'antivirus Kaspersky Lab a découvert un autre maliciel, qu'il a baptisé Gauss. Flame et Gauss se sont avérés très proches par leur architecture, la structure de leurs modules, leurs instructions de base et leur manière de communiquer avec le *serveur Command & Control*. Ces similitudes frappantes ont conduit à attribuer la paternité des deux maliciels au même laboratoire.

Selon les indices découverts, Gauss serait en activité depuis septembre 2011 et aurait espionné des dizaines de milliers d'ordinateurs jusqu'à sa découverte en juin 2012. La majorité des ordinateurs infectés se trouvaient au Liban, suivi d'Israël et des territoires palestiniens.

Les fonctionnalités de Gauss lui permettent de dérober les mots de passe pour Internet, les identifiants des systèmes de e-banking, les *cookies* de navigation et certaines données de configuration des systèmes infectés. Le maliciel était spécialement programmé pour intercepter les données liées aux comptes ouverts auprès de banques libanaises.

[13] Voir sur Flame le rapport MELANI 2012/1, chapitre 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: 28 février 2013).

Il s'agit du premier cas connu où un logiciel d'espionnage raffiné, probablement d'origine étatique, possède les caractéristiques d'un cheval de Troie spécialisé dans le e-banking. Or à la différence de ses prédécesseurs exploités par des cybercriminels, Gauss n'effectue pas d'opérations bancaires au préjudice de ses victimes, et se limite à espionner les transactions bancaires effectuées à partir de l'ordinateur infecté.

4.1.2 Shamoon: espionnage et sabotage de sociétés pétrolières et gazières

Le 15 août 2012, une infection par maliciel a paralysé des ordinateurs du réseau interne de Saudi Aramco, société pétrolière étatique saoudienne. Un logiciel baptisé Shamoon a collecté pour l'agresseur, sur les systèmes infectés, des informations relatives aux fichiers avant d'effacer ces derniers et de réécrire le secteur de démarrage principal (*Master Boot Record, MBR)*. D'où la nécessité de réinstaller les ordinateurs devenus inutilisables. Aux dires de Saudi Aramco, plus de 30 000 ordinateurs de son réseau interne ont été infectés – mais l'incident n'aurait perturbé ni la production de pétrole, ni les activités de négoce. Tous les appareils concernés ont pu être remis en état.

Peu après, le producteur de gaz naturel qatari RasGas a dû couper son réseau interne du monde extérieur. Même en l'absence de confirmation officielle, divers experts pensent que RasGas a également été victime de Shamoon.

Le mode de fonctionnement de Shamoon rappelle Wiper [14], maliciel découvert au printemps 2012 et qui avait sévi en Iran. L'analyse de Shamoon indique toutefois que l'auteur n'est pas le même que pour Wiper.
Comme une opération d'une telle ampleur requiert d'importants efforts, la participation d'un Etat, ou du moins un soutien étatique, paraît probable. Divers experts occidentaux soupçonnent l'Iran, dont les exportations énergétiques font les frais des sanctions internationales, de vouloir empêcher les Etats arabes d'augmenter leur production pétrolière et gazière.

[14] Voir au sujet de Wiper le rapport MELANI 2012/1, chapitre 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: 28 février 2013).

4.1.3 Hacktivisme au Proche-Orient

Outre les deux cas spectaculaires susmentionnés, le Proche-Orient a été le théâtre de diverses cyberattaques de moindre envergure au deuxième semestre 2012. En voici un bref aperçu:

- En août, la plate-forme de blogs de l'agence de presse Reuters a été sabotée à deux reprises, et son compte Twitter @ReutersTech une fois. Les pirates ont ainsi publié de fausses dépêches sur la situation au Proche-Orient, dans un but de propagande.

- En août également, des courriels ont été envoyés de façon ciblée à des dissidents syriens, pour les inviter à télécharger un programme de sécurité du nom d'Anti Hacker, censé les protéger d'intrusions malveillantes. Il s'agissait en réalité d'un logiciel d'espionnage.[15]

- Un groupe (autoproclamé) de hackers pakistanais a protesté en septembre contre le film «Innocence of the Muslims» en défigurant divers sites Internet. A la mi-novembre, ce groupe s'en est notamment aussi pris à des sites israéliens. Le collectif Anonymous a choisi le même moment pour lancer son opération Israël (OpIsrael). Il s'agissait de protester contre le gouvernement israélien, qui avait annoncé son intention de couper les moyens de communication dans la bande de Gaza.

- Anonymous a déclaré la «guerre» au régime d'Assad en Syrie, accusé d'avoir coupé les liaisons Internet avec l'étranger.[16]

- Un groupe de pirates a usurpé, pour son activité de propagande pro-palestinienne, plusieurs comptes d'utilisateur du vice-premier ministre israélien. Ce forfait n'a apparemment pas été commis au titre de l'opération Israël d'Anonymous, mais constitue un acte indépendant de solidarité avec la Palestine.

- En raison d'une mise en garde contre une vaste attaque ciblée visant la police israélienne, les ordinateurs de la police ont été temporairement déconnectés par précaution d'Internet. Les fonctionnaires ont été sensibilisés à l'importance de ne jamais raccorder de périphérique USB à leur ordinateur de service. Le réseau informatique interne de la police a toutefois fonctionné – seuls les échanges de courriels avec les autorités ont été impossibles pendant un certain temps.

- L'Agence internationale de l'énergie atomique (AIEA) a signalé que les coordonnées personnelles de chercheurs avaient été dérobées lors d'une cyberattaque, puis publiées sur Internet. Les pirates ont menacé de divulguer d'autres informations sensibles, si les meurtres de scientifiques nucléaires iraniens se poursuivaient – ces dernières années, plusieurs chercheurs ont été tués en Iran lors d'attentats que le gouvernement iranien a attribués à Israël et aux Etats-Unis.

- L'entreprise de sécurité Symantec a découvert le ver informatique Narilam, qui paraît s'intéresser surtout aux entreprises basées en Iran. Analyses à l'appui, il ne se livre pas à

---

15 https://www.eff.org/deeplinks/2012/08/syrian-malware-post (état: 28 février 2013).

16 http://www.youtube.com/watch?v=olZzqa6nwos; http://www.youtube.com/watch?v=xdmlPhWIAuw (état: 28 février 2013).

des activités d'espionnage, mais attaque des bases de données (p. ex. de comptabilité) du monde de l'économie, pour y modifier des données ou supprimer des champs.[17]

Diverses hypothèses ont été émises quant aux auteurs de ces attaques. Mais il sera difficile de démontrer si elles proviennent d'organisations étatiques, de pirates patriotes ou de sympathisants d'un groupement spécifique, et d'identifier les soutiens dont leurs auteurs ont bénéficié.

4.2 Attaques DDoS – motifs, auteurs et victimes

Dans le cyberespace, les attaques par déni de service distribué ou attaques DDoS (*Distributed Denial of Service*), consistant à inonder la victime de messages envoyés simultanément par de nombreux systèmes, poursuivent des buts différents. Il en a déjà été question dans de précédents rapports.[18] Au début, il s'agissait de purs actes de vandalisme. Les motivations ont changé entre-temps. On observe par exemple des attaques DDoS servant d'instrument de vengeance, visant à nuire à la concurrence, relevant du racket ou poursuivant des mobiles politiques. Alors que les attaques de moindre importance sont généralement tues et ne parviennent pas à la connaissance du public, on trouve régulièrement des attaques DDoS de grande envergure visant à attirer l'attention des médias. Les sites ou serveurs Web font partie des cibles privilégiées. Mais les serveurs de messagerie, les *serveurs DNS*, les *routeurs* et les *pare-feu*, ou d'autres types de services Internet ne sont pas épargnés. Les attaques lancées au deuxième semestre 2012 contre les banques américaines représentent indiscutablement un saut qualitatif. D'autres attaques DDoS ont également fait grand bruit.

4.2.1 Attaques DDOS visant des banques américaines

Depuis septembre 2012, des attaques par déni de service distribué (DDoS) parfois massives ont été signalées contre diverses banques américaines, à commencer par la Bank of America, Citigroup et Wells Fargo. Si aucun vol de données n'a été signalé jusqu'ici, l'accès en ligne aux établissements touchés a régulièrement été impossible.

Le volume de données mobilisées pour ces attaques a parfois dépassé 60 GB/s. Diverses sources les ont d'emblée attribuées à l'Iran et pensent qu'au lieu d'émaner de milieux criminels, elles seraient d'origine étatique, ou du moins que le gouvernement les soutient ou les tolère. Un article du New York Times signale ainsi, sans citer de nom, que des membres du gouvernement américain soupçonnent fortement l'Iran.[19] Cette thèse n'a toutefois pu être confirmée à ce jour. Seules la persistance de ces attaques et la difficulté de les circonscrire accréditent la thèse d'une implication étatique. Il faut bien admettre qu'en pareil cas, les preuves sont difficiles à réunir et, expérience à l'appui, une grande prudence s'impose en raison des enjeux politiques de part et d'autre. L'Iran a toujours catégoriquement nié toute implication dans ces attaques.

Divers experts croient pouvoir expliquer les attaques par l'embargo économique américain décrété contre l'Iran et y voient des mesures de rétorsion. Le groupe Izz ad-Din al-Qassam

---

17 http://www.symantec.com/connect/blogs/w32narilam-business-database-sabotage (état: 28 février 2013).

18 Voir rapport MELANI 2010/2, chapitre 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=fr (état: 28 février 2013).

19 http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=1& (état: 28 février 2013).

Cyber Fighters, qui a d'emblée revendiqué les attaques, a invoqué comme motif la diffusion de vidéos de Mahomet.[20] Or là aussi, le hacktivisme a été soupçonné de servir de prétexte pour dissimuler les intentions véritables.[21]

Les attaques émanaient également d'ordinateurs suisses. Il s'agissait généralement de serveurs Web à bande large, compromis par les pirates. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a informé leurs exploitants.

Aux dires des banques américaines, les attaques DDoS se poursuivraient, mais avec des conséquences moins graves. Les pannes auraient même diminué durant les premières semaines de janvier, malgré l'annonce par les pirates de nouvelles attaques en début d'année. Des observateurs y voient la preuve que les établissements financiers ont amélioré entre-temps leur capacité de repousser de telles attaques.[22] Ainsi, la statistique du trafic des treize principales institutions américaines établie en janvier 2013 révèle une accessibilité pendant 97 % du temps, contre 95 % durant la première phase des attaques. (1% correspond à environ 15 minutes).

Au-delà des précautions techniques, les attaques DDoS exigent notamment des mesures d'organisation et de communication notamment. Que communique une entreprise et de quelle manière? Il s'agit là incontestablement d'un facteur décisif. Une stratégie de communication peut s'avérer une première mesure contre les effets des attaques DDoS. A contrario, une communication irréfléchie est susceptible de déclencher une nouvelle attaque DDoS. D'où l'importance d'évaluer à l'avance les risques et effets d'une communication à grande échelle.

Les précautions techniques constituent assurément le deuxième facteur décisif. Il est bien plus simple d'effectuer des préparatifs en amont que sous les feux d'une cyberattaque. A fortiori pour les entreprises dont l'existence dépend directement de prestations de service ou de ventes en ligne. Normalement, le fournisseur de transit possède l'expérience requise et a la possibilité de fournir des solutions adéquates, afin de repousser les attaques DDoS.

Les mesures précitées valent en particulier pour les infrastructures vitales. Au cas où une attaque DDoS toucherait tout un secteur économique voire plusieurs secteurs, les échanges d'informations entre entreprises revêtent une très grande importance. Car ils permettent d'éviter les attaques, ou du moins d'en prévenir les effets. MELANI garantit un tel échange d'informations pour les exploitants d'infrastructures critiques en Suisse.

4.2.2 Attaque DDoS contre un fournisseur d'électricité allemand

Les serveurs du fournisseur d'électricité allemand «50 Hertz Transmission» ont subi pendant plusieurs jours une attaque DDoS. L'entreprise raccorde près d'un tiers de l'Allemagne au réseau électrique. L'attaque n'a toutefois perturbé à aucun moment l'approvisionnement électrique, car les pirates s'en étaient pris non aux systèmes de gestion (*SCADA*), mais «seulement» aux serveurs Web de l'entreprise. L'attaque a également perturbé la communication par courriel. 50 Hertz a réagi en déconnectant ses serveurs du réseau.

---

[20] http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0 (état: 28 février 2013).

[21] http://blogs.techworld.com/war-on-error/2013/01/iran-v-usa---the-worlds-first-cyberwar-has-started/index.htm (état: 28 février 2013).

[22] http://www.bankinfosecurity.com/are-banks-winning-ddos-battle-a-5434 (état: 28 février 2013).

Selon les médias, l'attaque a utilisé des milliers d'*adresses IP* d'Europe orientale, de Russie notamment[23]. On ignore toutefois si l'auteur venait de la région ou s'il s'est contenté d'y louer un réseau de zombies, et quels étaient ses motifs.

Les pressions économiques poussent toujours plus à l'uniformisation des systèmes, et le pilotage à distance et l'exploitation sans personnel s'étendent de composantes isolées aux sous-stations entières. Il est vrai que dans la plupart des cas, les réseaux administratifs et de pilotage demeurent strictement séparés. Mais la présence d'une technologie de réseau homogène incite fréquemment à relier les réseaux commerciaux et ceux de contrôle, pour simplifier les processus administratifs. Or il faut se rappeler qu'ils n'ont pas les mêmes besoins de sécurité, et prévoir des possibilités adéquates pour les systèmes SCADA.

Par ailleurs, les entreprises d'approvisionnement électrique ne sont pas seulement exposées à une attaque contre leur système SCADA. En effet, les systèmes livrant des informations nécessaires au maintien de la stabilité du réseau jouent aussi un rôle essentiel. Or ces systèmes sont toujours plus souvent reliés au réseau administratif, ce qui en fait une cible potentielle de cyberattaques.

4.2.3 Attaques DDoS en Suède contre des serveurs étatiques ou bancaires

Au début d'octobre, diverses entreprises ou autorités suédoises ont subi des attaques DDoS. Outre des banques, les sites des chemins de fer suédois (SJ) et de l'agence de presse TT ainsi que des serveurs de la Défense ont été touchés. Ces attaques faisaient probablement suite à la demande d'extradition de Julian Assange. Trois jours plus tard, la même mésaventure est arrivée aux serveurs de la Banque centrale suédoise, du Parlement et des services de renseignement (Säpo). L'opération avait été annoncée cette fois par Anonymous, qui entendait protester contre la justice suédoise. Les magistrats s'en étaient pris aux plates-formes de téléchargement de films et autres contenus selon le protocole *BitTorrent*.

[23] http://www.welt.de/wirtschaft/energie/article111369975/Russische-Hacker-attackieren-Stromnetzbetreiber.html (état: 28 février 2013).

4.2.4 Attaques contre l'infrastructure DNS

L'infrastructure DNS est toujours plus souvent la cible d'attaques. Le système de noms de domaine (*DNS*) rend les services Internet plus conviviaux, puisqu'au lieu de l'*adresse IP* il suffit aux utilisateurs de composer un nom d'adresse (*URL*). Tout au sommet de la hiérarchie figurent les *serveurs racine*, qui renseignent sur le *Top-Level-Domain* ou domaine de premier niveau (p. ex. .com, .net, .ch). Outre ces serveurs racine, chaque fournisseur d'accès dispose de serveurs DNS, qui mettent en cache de telles informations pour leurs clients.

La société Deutsche Telekom s'est débattue entre le 3 et le 6 septembre 2012 contre une attaque massive visant son infrastructure DNS. Elle est toutefois parvenue à la repousser, et aucune défaillance n'a été constatée.

Au début de 2013, SWITCH a également subi une attaque contre son infrastructure DNS. Là encore, l'agression a été déjouée.[24] Ce n'était d'ailleurs pas la première opération du genre. Cette cyberattaque contre l'infrastructure «.ch» n'était pas une fin en soi, mais un simple moyen d'attaquer des serveurs Web basés aux Etats-Unis. La méthode dite de réflexion ou amplification DNS (*DNS amplification attack*) consiste à forcer un serveur de noms à répondre à de petits paquets d'information par des paquets beaucoup plus volumineux. En théorie, une requête de 60 octets peut susciter une réponse de plus de 3000 octets. Il ne reste plus qu'à rediriger ces longues réponses vers la cible visée. Grâce à cette astuce, les agresseurs ont besoin d'une plus petite infrastructure (réseau de zombies) pour générer un gigantesque flux de données.

Les attaques DDoS figurent parmi les principaux dangers des réseaux. Ce n'est pas tant le nombre d'attaques qui augmente que leur complexité. On observe toujours plus d'attaques contre les protocoles DNS.[25] SWITCH a écrit dans son blog qu'aujourd'hui, le protocole DNS est le plus utilisé pour les attaques DDoS. En outre, les *serveurs DNS faisant autorité* seraient privilégiés, à la place des *résolveurs de DNS* publics précédemment utilisés.[26]

4.3 Faille des terminaux de points de vente

Jusqu'ici, les pirates se concentraient sur les terminaux de points de vente acceptant le paiement par carte de crédit (*point of sale, POS)* et recouraient principalement aux méthodes classiques de *skimming*, consistant à installer du matériel sur les terminaux pour pouvoir copier les bandes magnétiques et les codes *PIN*. Ce mode opératoire a également servi dans les commerces suisses.[27] Une nouvelle lacune de sécurité, publiée au début de juillet 2012 par les experts allemands en sécurité Thomas Roth et Karsten Nohl de SRLab, a toutefois révélé l'existence d'un autre danger encore.

Les experts en sécurité ont découvert une faille critique dans les terminaux de cartes «Hypercom Artema Hybrid» du fabricant Verifone. Le lecteur de cartes subit une attaque par *débordement de tampon* (*buffer overflow*) visant sa *pile (stack)*, dans un but de prise de contrôle de son processeur d'application. Le pirate bénéficiera ensuite d'un accès en ligne

---

[24] Cette attaque fera l'objet d'un rapport détaillé dans le rapport semestriel 2013/1.

[25] http://www.all-about-security.de/security-artikel/applikations-host-sicherheit/applikationen-web-services/artikel/14953-ddos-angriffe-bleiben-groesste-gefahr-fuer-netzwerke/ (état: 28 février 2013).

[26] http://securityblog.switch.ch/2012/12/04/ddos-angriffe-durch-reflektierende-dns-amplifikation-vermeiden/ (état: 28 février 2013).

[27] Voir rapport MELANI 2011/1, chapitre 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=fr (état: 28 février 2013).

au terminal, qui lui permettra de contrôler le champ de saisie et l'affichage, et donc de copier le numéro PIN et les données de la bande magnétique. Autrement dit, un agresseur potentiel n'a plus besoin d'accéder directement à l'appareil – un accès *TCP/IP* au terminal faisant l'affaire. Il n'est même pas nécessaire d'accéder physiquement au réseau de l'entreprise concernée. Des escrocs peuvent aussi se procurer un tel accès en introduisant un maliciel sur l'ordinateur d'un collaborateur. Ils y parviendront naturellement encore plus facilement si le terminal de cartes est directement accessible par Internet, et donc s'il possède une *adresse IP publique*.

Des attaques locales directement effectuées sur l'appareil à travers l'interface série ou l'interface JTAG sont également possibles. Avec JTAG on opère en aval du niveau du logiciel. L'accès à travers l'interface JTAG se déroule directement au niveau du processeur, c'est pourquoi la faille ne peut pas être corrigée entièrement à l'aide d'une mise à jour du logiciel. [28]

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a pris connaissance rapidement de cette faille de sécurité. Elle a transmis l'information aux entreprises chargées de l'exploitation de ces terminaux en suisse, qui ont adopté les mesures qui s'imposaient.

4.4 Attaques visant des institutions européennes

Selon une enquête de l'agence Bloomberg publiée en juillet, un groupe d'espions chinois se serait introduit dans le système informatique du Conseil européen. Ce groupe, baptisé «Byzantine Candor», aurait ainsi pu s'emparer du courrier électronique d'Herman Van Rompuy et d'autres hauts responsables européens. Selon l'article de Bloomberg, les pirates seraient liés à l'armée populaire de libération chinoise et auraient été identifiés grâce au travail d'un collectif américain composé d'universitaires, d'entreprises et de spécialistes en sécurité informatique. En plus du Conseil européen, au moins 20 entreprises auraient été victime des pirates. Ces cibles auraient toutes en commun de disposer de technologies susceptibles d'offrir un avantage compétitif à la Chine en matière économique. Selon Bloomberg, Byzantine Condor ne serait qu'un exemple d'une véritable industrie chinoise du cyberespionnage. L'UE ne s'est pas exprimée officiellement sur ces attaques.

Le nombre d'incidents similaires rendus publics a fortement augmenté depuis deux ans (voir rapports MELANI 2011/1 et 2011/2)[29]. En décembre 2010, divers médias avaient déjà évoqué les activités d'espionnage prêtées au groupe Byzantine Candor ainsi que ses liens possibles avec l'armée chinoise, suite à la publication par Wikileaks d'une dépêche américaine secrète de 2008 dans ce sens. Il y était question de la recrudescence des activités d'espionnage déployées par la Chine depuis plusieurs années. Plus récemment, en février 2013, l'entreprise de sécurité américaine Mandiant a publié un rapport attribuant diverses activités d'espionnage déployées au cours des dernières années, le plus souvent contre des entreprises américaines, à l'unité 61398 de l'armée chinoise.[30] Les autorités

[28] http://www.golem.de/news/verifone-ec-kartenterminals-in-deutschland-gehackt-1207-93144.html (état: 28 février 2013).

[29] Voir rapport semestriel MELANI 2011/1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=fr (état: 28 février 2013). Voir rapport semestriel MELANI 2011/2: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 28 février 2013).

[30] Le rapport semestriel 2013/1 reviendra en détail sur ce thème.

chinoises nient toutefois catégoriquement l'existence de ce genre d'activités de cyberespionnage.

4.5 Entrée en service du CERT-UE et du Centre européen de lutte contre la cybercriminalité (EC3)

Suite à une phase pilote d'une année suivie d'une évaluation, le *CERT* (*computer emergency response team*) de l'Union européenne est entré en service le 11 septembre 2012. La mission principale de cette structure est de protéger les institutions européennes contre les cyberattaques. Le CERT est constitué de spécialistes IT et sécurité issus des principales institutions européennes. Il sera amené à collaborer avec les CERT des pays membres, de même qu'avec diverses entreprises de sécurité. Il convient ici de rappeler que la Commission a été l'objet de plusieurs attaques informatiques au cours des dernières années[31 et 32], ce qui explique en partie la nécessité de disposer d'une telle structure.

Le Centre européen de lutte contre la cybercriminalité (EC3) a été inauguré le 11 janvier 2013, dans les locaux d'Europol à La Haye. Il entend être le point focal au sein de l'Union européenne dans la lutte contre la cybercriminalité. Selon Cecilia Malmström, commissaire européenne chargée des affaires intérieures, le EC3 «accroîtra fortement la capacité de l'UE à lutter contre la cybercriminalité et à défendre un Internet libre, ouvert et sûr». Le centre et ses compétences ont fait l'objet d'une présentation détaillée dans un précédent rapport MELANI[33].

4.6 Sésame ouvre-toi: piratage des serrures électroniques d'hôtels

En juillet 2012, un pirate de 24 ans a expliqué aux participants à la conférence Black Hat de Las Vegas comment déverrouiller sans peine certaines serrures électroniques de chambres d'hôtel. La méthode consiste à rechercher à l'aide du connecteur de programmation de la serrure, qui apparemment n'est pas protégé contre les intrusions, le code passe-partout enregistré sans cryptage sur la puce de contrôle. Selon les médias, cette faille concernerait principalement les serrures électroniques de la marque Onity.

Un autre pirate a présenté – à partir de l'exemple susmentionné – une application particulièrement efficace de cette méthode. Il a expliqué en détail sur son blog comment fabriquer un appareil permettant de s'introduire dans une chambre d'hôtel «protégée» par un système électronique. Et comme l'appareil a la forme et la taille d'un stylo, son possesseur ne risque pas d'attirer l'attention sur lui.

Une mise à jour des serrures n'est possible qu'à condition d'en changer le circuit imprimé (*platine*). Or le fabricant ne rembourse pas les frais correspondants, qui sont à la charge des hôtels. Il propose à la place une variante gratuite, soit un couvercle empêchant d'accéder au

---

31 Voir rapport semestriel MELANI 2012/1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: 28 février 2013).

32 Voir rapport semestriel MELANI 2011/1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=fr (état: 28 février 2013).

33 Voir rapport semestriel MELANI 2012/1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: 28 février 2013).

connecteur de programmation. Plus de quatre millions de serrures de portes seraient concernées au niveau mondial.[34]

La faille de sécurité était apparemment connue depuis longtemps. La personne l'ayant découverte l'a rendue publique de peur que les autorités et les services secrets n'en fassent usage à leur tour.

Depuis quelques années déjà, les ordinateurs personnels ou les serveurs ne sont plus les seules cibles de tentatives de piratage. Tout système informatique est susceptible d'être attaqué. L'utilisation d'une faille de sécurité afin d'ouvrir sans problème une porte d'hôtel contrôlée par un système électronique n'est qu'un exemple de ce principe. Cette possibilité devrait par conséquent être systématiquement prise en compte lors de la conception de tout produit intégrant une procédure d'identification basée sur des systèmes électroniques.

En s'introduisant dans une chambre d'hôtel, une personne non autorisée pourrait prendre connaissance de données confidentielles. Peu importe ici que ces données se trouvent sur un ordinateur portable, sur une clé *USB* ou sur papier. L'affaire soulève une autre question brûlante, soit la nécessité pour les entreprises de préciser comment leurs employés doivent protéger leurs données sensibles lors d'un voyage de service. Il faut p. ex. sensibiliser les collaborateurs concernés et prendre les mesures d'usage (comme le cryptage des données sur support informatique).

4.7 Appareils connectés au réseau mobile – grande variété et faible conscience des enjeux de sécurité

Le réseau mobile fait également l'objet d'une attention soutenue de la part des spécialistes en sécurité. En juillet 2012, un chercheur allemand a fait une démonstration des failles de sécurité pouvant potentiellement toucher ce réseau et les appareils s'y trouvant.[35] Une requête dans la base de données du RIPE lui a tout d'abord permis de sélectionner des adresses IP attribuées par les opérateurs aux appareils connectés au réseau mobile. Un simple balayage de ports a ensuite permis de récupérer diverses informations. Le premier enseignement concerne la grande variété des équipements présents sur ce réseau: routeurs GSM/GPRS, caméras, compteurs de consommation énergétique (smart meter), lecteurs de codes-barres, systèmes de gestion du trafic routier. Dans certains cas, il a même été possible d'obtenir les données de localisation de l'appareil, sans devoir s'identifier préalablement. Le chercheur n'a cependant pas tenté de se connecter à ces terminaux pour les exploiter à distance.

Le but de l'expérience était de démontrer les implications potentielles de la grande quantité d'appareils qui sont présents sur les réseaux et faciles à identifier. En effet, il est possible dans ces conditions d'y chercher des failles de sécurité pour tenter de prendre le contrôle des appareils. Une personne mal intentionnée pourrait ainsi avoir accès à des appareils utilisés dans un cadre domestique, dans l'espace public, voire dans un environnement industriel.

[34] http://www.t-online.de/computer/sicherheit/id_58856082/hacker-knacken-hotel-tueren-binnen-sekunden.html (état: 28 février 2013).

[35] http://www.heise.de/security/meldung/Scan-in-Mobilfunknetzen-foerdert-tausende-ungeschuetzte-Geraete-zu-Tage-1653619.html (état: 28 février 2013).

Par souci d'économies, toujours plus de systèmes critiques possèdent une liaison GSM/GPRS – à l'instar des systèmes *SCADA*, des terminaux de cartes de crédit ou des distributeurs automatiques de billets.

4.8 App Stores

Les grands fournisseurs mondiaux de contenus pour smartphones ont créé pour leurs propres clients des boutiques en ligne permettant d'acheter diverses applications (*apps*). D'où naturellement la question de savoir quels avantages ou inconvénients ces plates-formes présentent du point de vue de la sécurité.

App Store iOS
L'App Store iOS est la plate-forme lancée en 2008 par Apple. Pour avoir accès à ce marché, soit pour y proposer ses applications, chaque fournisseur doit impérativement se soumettre aux procédures de vérification internes d'Apple[36]. Ce n'est qu'après une analyse que son application sera admise dans la plate-forme Apple. Un tel processus doit notamment servir à vérifier le fonctionnement des applications. Si elle ne remplit pas les critères fixés par Apple, l'app ne sera pas proposée. Beaucoup de ces critères se rapportent à la sécurité de l'appareil de l'utilisateur final. Par exemple, une application ne sera pas proposée si elle installe et exécute des programmes supplémentaires, si elle prend connaissance de données protégées voire transmet sans autorisation préalable de telles données à des tiers.

Dans le cas de l'«App Store iOS», l'utilisateur final s'en remet entièrement à Apple pour les questions de sécurité. Or quelle est l'efficacité de cette solution? Il est certes rare que des applications malveillantes apparaissent dans le système Apple. Mais il a pu arriver que les processus de vérification soient contournés. Le cas le plus connu est peut-être celui de Charlie Miller, chercheur dont Apple avait contrôlé et accepté l'application. Or elle enfreignait la règle de base de ne télécharger ou exécuter aucun code supplémentaire[37]. Quand Miller a rendu son exploit public, Apple lui a retiré sa licence de développeur. Un ancien collaborateur d'Apple du nom de Mike Lee s'est récemment exprimé, dans une interview, sur la structure mise en place par Apple pour ses vérifications[38]. Lee estime que l'équipe engagée par Apple pour analyser les apps est sous-dotée. En outre, l'examen de beaucoup d'applications serait monotone et dénué d'intérêt. Cela tiendrait tant à leur contenu (souvent pornographique) qu'au fait que beaucoup d'apps sont des copies ou de simples mises à jour d'applications existantes. Cette monotonie risque d'entraîner des fautes d'inattention, comme dans le cas de «Find and Call» (trojan:iOS/Fidall). Cette app était en mesure de dérober la liste de contacts et de la transférer à un serveur.

Play Store (Android)
Comme signalé le semestre dernier[39], Google mène une autre politique pour ses applications. Selon cette approche, la sécurité est avant tout l'affaire de l'utilisateur final. Cette politique permet aux utilisateurs de télécharger Android de n'importe quel site. Il n'est pas nécessaire de passer par Play Store, soit la boutique officielle. Google vise néanmoins à offrir des applications sûres aux clients passant par sa propre plate-forme. D'où l'introduction

---

36 https://developer.apple.com/appstore/guidelines.html (état: 28 février 2013).
37 http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (état: 28 février 2013).
38 http://www.businessinsider.com/heres-why-it-really-sucks-to-be-an-app-reviewer-for-apple-2012-7#ixzz1zaB9ki4H (état: 28 février 2013).
39 Voir rapport MELANI 2011/2, chapitre 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 28 février 2013).

au début de 2012 du système Bouncer. Ce système analyse automatiquement toutes les applications du Play Store, à la recherche de programmes malveillants. Deux chercheurs – Charlie Miller mentionné plus haut et Jon Oberheide – ont toutefois révélé en juillet qu'il était possible de duper Bouncer et d'infecter un smartphone Android[40] avec une app spécialement préparée.

Google cherche à concilier sécurité et flexibilité. D'un côté, l'offre de prestations de service doit être aussi ouverte et flexible que possible, ce qui séduit naturellement les criminels. De l'autre, Google vise à procurer à l'utilisateur final un maximum de sécurité.

Amazon Appstore (Android):
Amazon a lancé au premier semestre 2011 sa propre boutique d'applications pour Android, avant de commercialiser à fin 2011 sa propre tablette. Cette tablette nouvelle génération est basée sur une version modifiée du système Android 4.0 (Ice Cream Sandwich), ne donnant accès qu'à la boutique en ligne d'Amazon. Les experts ont émis des réserves sur la sécurité de ladite boutique. Ils ont notamment déploré que les utilisateurs d'Android possédant une tablette d'une autre marque doivent activer l'option «Autoriser l'installation des applications provenant de sources inconnues» pour accéder à la boutique Amazon. Les restrictions de téléchargement étant ainsi assouplies, le risque d'installer une app malveillante à partir d'un site n'étant pas digne de confiance existe. Le rapport F-Secure du deuxième trimestre 2012[41] rappelle d'ailleurs que la plupart des applications malveillantes pour Android émanent de «marchés parallèles» à la plate-forme Google Play Store. Au même trimestre, F-Secure signalait la première infection par *drive-by download* conçue pour Android. Autre sujet d'étonnement, l'entreprise de sécurité TrustGo a conclu, dans son rapport basé sur l'analyse de 2,2 millions d'apps provenant de 187 marchés[42], que Play Store et Amazon Appstore n'occupent que les 4e et 5e places en matière de sécurité. Selon le même rapport, les cinq boutiques en ligne Android «les plus dangereuses» se trouveraient toutes en Chine.

Dans des systèmes fermés comme celui d'Apple, la sécurité de l'utilisateur final est entre les mains du fabricant. Ceci présente l'avantage de confier les tâches de sécurité complexes à une entreprise ayant les connaissances et la marge de manœuvre nécessaires. Comme déjà indiqué, il est rare que des applications malveillantes circulent dans le système d'Apple. Le revers de la médaille, c'est que les clients de l'App Store doivent faire confiance à l'entreprise et n'ont aucun moyen de contrôler ce qui se passe dans leur propre système.

D'un autre côté, des attaques ont déjà abouti contre le système de sécurité du Play Store, et Amazon demande aux utilisateurs de sa boutique de modifier leurs paramètres de sécurité afin que des applications puissent être téléchargées en dehors de leur marché d'origine. Or des escrocs placent leurs apps malveillantes sur différents marchés Android ou sur divers sites Web, en les faisant passer pour des applications légales. Des milliers de programmes malveillants sont ainsi en circulation sur les divers marchés. Et même si Android fournit les informations nécessaires afin de vérifier si les applications possèdent les droits requis, cette possibilité n'est que rarement utilisée. En effet, le facteur sécurité est secondaire pour l'utilisateur habituel, qui désire que l'installation de son app soit aussi rapide et simple que possible. L'exploitant du marché doit également garder à l'esprit cet aspect, de façon à offrir un degré de sécurité élevé.

40 http://jon.oberheide.org/files/summercon12-bouncer.pdf (état: 28 février 2013).
41 http://www.f-secure.com/weblog/archives/MobileThreatReport_Q2_2012.pdf (état: 28 février 2013).
42 http://www.trustgo.com/images/en-GB/trustgo_q4_mobile_mayhem.pdf (état: 28 février 2013).

4.9 Obligation de signaler les cas de piratage et contrôle du réseau – arguments pro et contra

Plusieurs pays dont la France, les Etats-Unis et l'Allemagne ont annoncé préparer la mise en place d'un devoir d'annonce des cyberattaques graves. De même, la Commission européenne a exprimé, dans sa cyberstratégie pour l'Union européenne, sa volonté d'accroître la sécurité d'Internet en instaurant un régime de déclaration obligatoire pour les entreprises fournissant des prestations de service d'importance nationale. Un devoir existe déjà pour les prestataires de télécommunications, depuis l'adoption par l'UE de son «Paquet Télécom».

Les milieux économiques, les fournisseurs d'accès Internet et l'industrie en particulier s'opposent à une telle façon de procéder de peur, le cas échéant, de retombées négatives sur la marche des affaires et de dégâts d'image. Le fardeau administratif est par ailleurs jugé excessif. Il faudrait en outre définir en détail ce que l'on entend par une attaque ou une faille de sécurité. Les entreprises et les exploitants d'infrastructures critiques misent plutôt sur une collaboration librement consentie, en fonction des besoins, avec les autorités.

Les avantages ou inconvénients respectifs du devoir d'annonce et de l'échange facultatif d'informations sont loin de faire l'unanimité, dans les pays qui en débattent. Ainsi, la mise en place d'un régime d'échange facultatif des données est un processus de longue haleine, basé sur la confiance et donc qui demande du temps. Des résultats sont rarement visibles du jour au lendemain. Or une fois un tel partenariat en place, la qualité des échanges est généralement meilleure. Dans un régime d'obligation d'annonce, les informations sont par définition échangées dès le début. Mais elles sont enserrées dans un étroit corset légal, privant de marge de manœuvre les autorités et les entreprises. Au risque que les informations échangées soient peu utiles. Et expérience à l'appui, les discussions préalables à l'adoption d'une loi sur les télécommunications, afin de définir le degré d'exhaustivité et la forme des informations à fournir, prennent également beaucoup de temps.

Il n'est pas possible de dire dans l'absolu laquelle des variantes est préférable. La réponse dépend fortement de la structure et de la taille du pays. Dans un grand pays, qui compte davantage d'acteurs et d'entreprises, la mise en place de rapports de confiance constitue certainement un plus grand défi. En Suisse, l'échange facultatif d'informations a été établi dans le cadre d'un partenariat public privé (PPP).

5 Tendances / Perspectives

5.1 Failles des navigateurs – stratégie à deux navigateurs et autres possibilités

Il est aujourd'hui généralement d'usage d'installer régulièrement, de préférence automatiquement, les mises à jour de sécurité des systèmes d'exploitation et des applications. On rencontre néanmoins régulièrement des *failles «zero day»*, soit des lacunes pour lesquelles il n'existe pas encore de mise à jour de sécurité. Presque tous les jours, de telles failles de sécurité sont identifiées dans toutes sortes d'applications. Les *navigateurs* Internet ne font pas exception à la règle. Selon la gravité de la vulnérabilité découverte, il peut être judicieux de changer de navigateur jusqu'à ce que le fabricant ait résolu le problème.

Ce qui n'est qu'une simple formalité pour un ordinateur privé peut s'avérer un vrai casse-tête dans le monde professionnel. Car à la différence des ordinateurs privés, il est souvent délicat pour une entreprise de changer de navigateur. Par exemple faute d'avoir prévu une stratégie à deux navigateurs. Cela est fréquemment le cas, afin que le service chargé des TIC ne doive assumer la maintenance que d'un seul navigateur.

En cas de grave faille de sécurité, des données confidentielles voire secrètes risquent aussi d'être menacées. Il est par conséquent judicieux de parer à toute éventualité, dans la vie privée comme dans le cadre professionnel, afin de pouvoir au plus vite se rabattre sur un navigateur de rechange.

Les possibilités suivantes seraient envisageables dans le monde professionnel (l'énumération n'étant pas exhaustive):

Equipement de tous les postes avec au moins deux navigateurs
Tous les postes de travail d'une entreprise comportent au moins deux navigateurs. En cas de nécessité, le personnel sera prié de ne plus utiliser le navigateur problématique jusqu'à nouvel avis. Il serait également possible, le cas échéant, d'agir directement via le serveur mandataire (*proxy*), en empêchant ce navigateur d'accéder à Internet. Mais une telle solution serait coûteuse, en obligeant à assurer la maintenance de plusieurs navigateurs. Quant aux utilisateurs, ils hésiteraient souvent sur le navigateur à utiliser.

Equipement ponctuel d'au moins deux navigateurs
Seuls les postes de travail ayant impérativement besoin d'Internet seront équipés de plusieurs navigateurs. A supposer que l'un d'eux présente une faille de sécurité, il ne sera plus utilisable et il faudra en changer. Le grave inconvénient de cette solution tient à ce qu'en cas d'urgence, une partie du personnel serait momentanément privée d'accès à Internet. Même si cela ne joue peut-être pas un rôle important pour leur travail, les utilisateurs concernés risquent de se sentir infantilisés ou discriminés.

Liste blanche
Tous les départements de l'entreprise signalent au service TIC les *URL* dont ils ont absolument besoin même en cas d'urgence. Les liens correspondants seront inscrits sur une liste blanche. En cas de faille de sécurité, tous les URL absents de cette liste seront bloqués. Une telle mesure permettrait de faire l'économie d'un second navigateur. Le risque de dommages sera réduit au minimum, puisque seuls des URL bien précis resteront accessibles. Tout risque n'est pas pour autant écarté. D'où la nécessité d'installer au plus vite les mises à jour de sécurité, afin de pouvoir renoncer au blocage temporaire des URL absents de la liste blanche.

Indépendamment de toute décision prise au sujet des TIC privées ou professionnelles, ce serait une illusion de croire que d'autres navigateurs seraient plus sûrs. Tôt ou tard, tout navigateur finit par présenter une faille de sécurité. Et si l'un d'eux ne comporte aucune lacune connue à un moment donné, il n'est pas pour autant fiable à 100%. La prudence et le bon sens sont par conséquent toujours de mise sur Internet.

5.2 Aperçu des cyberstratégies

A ce jour, plus d'une vingtaine de pays ont publié une stratégie complète de cybersécurité. La plupart des Etats considèrent les menaces venant du cyberespace comme un des grands défis du 21e siècle et, en réponse à l'augmentation du nombre de cyberincidents (p. ex. Stuxnet, Duqu, Flame et Ghostnet), intègrent toujours plus la cybersécurité dans leur stratégies nationales de politique de sécurité (p. ex. France, Pays-Bas et Grande-Bretagne).

Toutes les cyberstratégies ont pour point commun de considérer l'usage des technologies de l'information et de la communication (TIC) comme un facteur de progrès économique et de bien-être social. En même temps, elles érigent en priorité nationale l'amélioration de la capacité de résistance (résilience) des infrastructures vitales, et donc la réduction au minimum des cyberrisques.

Transversalité des cyberenjeux
Il s'avère essentiel de coordonner les activités étatiques, qu'elles soient de nature politico-stratégique ou technique et opérationnelle. Car la maîtrise des cyberrisques est conçue comme une tâche transversale, et divers services ou acteurs ont désormais dans leur mission de base des aspects cybernétiques à prendre en compte. A cet effet, certains pays ont créé des centres de cyberdéfense (p. ex. Allemagne et Pays-Bas).

Partenariat public privé
Comme la majeure partie des prestations d'infrastructure publiques sont en mains privées, la collaboration entre l'Etat et le monde économique est essentielle. La plupart des stratégies soulignent le besoin d'intensifier et d'institutionnaliser cette collaboration. De nombreuses cyberstratégies partent de l'idée qu'il faut accroître la sécurité du cyberespace non à l'aide de prescriptions et d'interventions étatiques sur le marché, mais sur une base facultative, en renforçant la coopération (p. ex. Suisse, Grande-Bretagne et Pays-Bas).

Coopération internationale
Une réduction efficace des cyberrisques nécessite une collaboration internationale accrue. Toutes les cyberstratégies aboutissent au même constat. Or rares sont les pays qui décrivent en détail comment l'on pourrait ou devrait améliorer et institutionnaliser la collaboration au niveau international. Les Etats-Unis font exception, avec leur cyberstratégie affichant sa vocation internationale. La Grande-Bretagne aussi encourage, à travers la Conférence de Londres sur le cyberespace lancée en 2011, le dialogue international pour définir des règles de conduite internationales dans le cyberespace. De même, les organisations internationales (p. ex. Union européenne, G8, Nations Unies, Organisation pour la sécurité et le développement en Europe) ont un rôle important à jouer dans l'élaboration de règles de conduite. Tant l'Allemagne que l'Australie misent sur les systèmes communs de détection précoce et sur la désignation d'interlocuteurs chargés de la communication en cas de crise.

Avec sa «Stratégie nationale de protection de la Suisse contre les cyberrisques», notre pays mise davantage, pour la maîtrise des cyberrisques, sur la collaboration entre les acteurs publics et privés. Le modèle de partenariat public privé (PPP) n'est pas nouveau pour la Suisse où, depuis la privatisation de divers services publics – p. ex. dans le secteur des télécommunications –, les autorités étatiques soutiennent, selon le principe de subsidiarité,

les processus de sûreté de l'information spécifiques aux infrastructures critiques. Ainsi, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI, créée en 2004, informe les exploitants de telles infrastructures sur les incidents et menaces propres au cyberespace, contribuant par là à la gestion des risques des entreprises. MELANI comporte une structure comparable aux centres de cyberdéfense mis en place à l'étranger. En outre, la coopération mise en place ainsi que le mandat de MELANI vont au-delà des efforts déployés dans beaucoup d'autres pays.

Cette collaboration avec l'économie a fait ses preuves et fonctionne bien. La «stratégie nationale de protection de la Suisse contre les cyberrisques» renforce les structures décentralisées en place. Contrairement à d'autres Etats, la Suisse renonce à se doter d'un organe central de pilotage et de coordination.

5.3 Réglementation versus liberté – Comment rendre Internet plus sûr?

Lancé comme projet de l'agence ARPA (Advanced Research Projects Agency) du ministère de la Défense américain, Internet s'est peu à peu imposé comme plate-forme d'information et d'offres et a évolué de son rôle de réseau à but purement scientifique vers une infrastructure des superlatifs à usage commercial. Les chiffres parlent d'eux-mêmes: alors que seules 500 000 personnes se servaient d'Internet en 1991, près de 2,5 milliards d'individus sont dans ce cas aujourd'hui. Et l'on estime qu'en 2020, jusqu'à 5 milliards de personnes – soit env. 60 % de la population mondiale – seront raccordées à Internet.

Internet ne fait l'objet d'aucune réglementation étatique et reste un espace de liberté soumis principalement à des normes techniques et à des directives administratives (appelées «policies»). En leur qualité d'organisations non gouvernementales, l'ICANN (Internet Corporation for Assigned Names and Numbers) et l'ISOC (Internet Society) affinent constamment ces prescriptions techniques et administratives et permettent aux acteurs politiques et économiques, au monde scientifique et à la société civile de collaborer à la gestion d'Internet. Les gouvernements occidentaux approuvent ce modèle de gouvernance multipolaire, jugé apte à garantir la liberté d'information.

Il existe toutefois une puissante coalition de pays aspirant à une réglementation d'Internet. Très attachés à leur souveraineté, ces Etats cherchent à étendre ou assurer leur pouvoir de contrôle sur le cyberespace.

La Conférence mondiale des télécommunications internationales organisée à fin 2012 à Dubai (CMTI 12) par l'Union internationale des télécommunications (UIT, agence des Nations Unies) prévoyait d'étendre à Internet le champ d'application du Règlement des télécommunications internationales (International Telecommunication Regulations, ITR). Le fait que 55 Etats sur 144 n'aient pas signé le nouveau traité, qui pourtant ne portait pas sur la régulation concrète d'Internet et se limitait à préciser des questions d'interprétation en la matière, est symptomatique de l'absence de consensus au sein de la communauté internationale quant à la répartition des compétences liées à la régulation d'Internet.

Les multinationales comme les fabricants de logiciels, les moteurs de recherche et les réseaux sociaux, mais aussi l'industrie de la musique et du film, exercent une influence à ne pas sous-estimer. Ces sociétés ont tout intérêt à ce que l'évolution d'Internet ne nuise pas à la bonne marche de leurs affaires. De telles entreprises mènent également un lobbying actif pour freiner la réglementation ou au contraire pour combler le vide réglementaire qui leur coûte cher ou qui limite leurs propres opportunités sur le marché.

5.4 Traces sur Internet – données laissées lors de la visite d'un site Web

L'information est la nouvelle valeur monnayable sur Internet. Cette phrase est toujours plus d'actualité à propos des informations personnelles récoltées en ligne. Des programmes sans cesse améliorés et la puissance de calcul croissante des processeurs permettent d'exploiter de manière toujours plus raffinée de grandes quantités de données, qui acquièrent ainsi une valeur commerciale. Même si en pareil cas l'individu en tant que tel disparaît dans la masse de données, de nombreux utilisateurs quotidiens d'applications électroniques se demandent quelles données sont récoltées sur eux, et dans quel but elles sont traitées et sauvegardées.

Toutes sortes de prestataires en ligne s'intéressent de près au comportement des internautes, afin d'afficher des annonces publicitaires mieux ciblées et d'en mesurer l'impact concret. A commencer par Google, dont la publicité est «personnalisée» en fonction des requêtes saisies par l'utilisateur. Les entreprises insérant la publicité en ligne tirent leurs revenus des clics effectués par les utilisateurs sur de tels liens. Par conséquent, toute information leur permettant de placer leur publicité de manière ciblée, selon les intérêts des utilisateurs, a une valeur monétaire. La bannière publicitaire ne provient généralement pas du site lui-même, il s'agit d'une page dans la page (balise *IFrame*), publiée par une régie publicitaire. Les balises IFrame de ladite agence publicitaire renferment encore de petits scripts qui collectent des données telles que l'adresse IP, le *domaine*, le *navigateur*, l'heure locale ou le système d'exploitation.[43] Plus les bannières publicitaires et donc les collecteurs d'informations figurent sur de nombreuses pages, plus ils permettent d'établir un profil d'utilisation détaillé. A condition bien sûr que l'utilisateur ait été reconnu sur chacune des pages visitées. Cette tâche incombe aux *cookies* (ou témoins de connexion). Les témoins de connexion ne sont pas nuisibles en soi: ils servent à attribuer les réglages personnalisés à chaque utilisateur, pour ne pas devoir redéfinir ces paramètres à chaque visite ou sur chaque page. Les régies publicitaires ont rapidement découvert le profit à tirer de cette technique, qu'elles ont intégrée dans leurs bannières publicitaires.

Une étude publiée en 2010 par le Wall Street Journal portait sur 50 des pages les plus consultées. L'ordinateur test avait enregistré durant l'opération 3180 témoins traceurs (*tracking cookie*), provenant généralement d'entreprises publicitaires. Les informations de ces témoins sont affinées par d'autres renseignements comme le lieu de domicile, afin de dresser un profil aussi précis que possible de l'utilisateur.[44]

Ces données demeurent certes plus ou moins anonymes, à l'exception de l'adresse IP. Mais tout change si par recoupement avec des données personnelles, les entreprises identifient les propriétaires des profils d'utilisation. Le bouton «J'aime» de Facebook est régulièrement évoqué en rapport avec cette thématique. Par analogie aux bannières publicitaires, un profil d'utilisateur peut être établi à partir des boutons Facebook de diverses pages. Avant même que l'on ait cliqué sur un tel bouton, des données sont transmises à Facebook.[45] A supposer que l'utilisateur soit connecté à ce moment, Facebook aurait la possibilité d'attribuer la page consultée directement à la personne. Et comme la longévité des témoins de connexion peut atteindre deux ans, cela resterait encore longtemps possible.

---

43 http://de.wikipedia.org/wiki/DoubleClick (état: 28 février 2013).

44 http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html (Stand: 28. Februar 2013).

45 http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html (état: 28 février 2013).

Aux traces laissées involontairement viennent s'ajouter les données publiées volontairement, p. ex. sur Facebook, Xing ou d'autres plates-formes de médias sociaux. Chacun doit être bien conscient des données qu'il souhaite communiquer ou non. Mais le risque tient aux recoupements possibles entre les données collectées en arrière-plan et celles ayant été spontanément indiquées.

Les nouvelles technologies éveillent toujours les convoitises. Comme la navigation tend à se déplacer des ordinateurs «normaux» vers les *smartphones*, l'affichage de la publicité varie de plus en plus selon la localisation. Par conséquent, les données *GPS* joueront à l'avenir un rôle croissant. Une première étape a été franchie quand Telefonica a signalé qu'il utiliserait des géodonnées à des fins commerciales. Au début d'octobre 2012, cet opérateur mobile a créé la division Telefonica Dynamic Insight. Cette société est chargée de traiter et d'analyser des informations – dont des géodonnées d'opérateurs Telecom – présentant un intérêt commercial. Elles doivent p. ex. permettre de prévoir l'afflux de personnes en fonction de la météo, du jour et de l'heure. De telles informations aideront notamment les entreprises à planifier les horaires de leur personnel et leurs achats, ou les communes à contrôler les flux de personnes.

Les applications des smartphones ont de beaux jours devant elles. Or jusqu'ici, la transparence laisse à désirer sur les données transmises aux fournisseurs d'applications en ligne. En outre, les nouvelles techniques comme la reconnaissance faciale intéressent vivement la branche publicitaire. Autrement dit, il y a peu de chance qu'à l'avenir, il soit plus aisé aux utilisateurs de décider quelles données les concernant peuvent ou non être traitées voire transmises à des tiers (autodétermination en matière d'information).

A l'heure actuelle, la plupart des gens savent que sur Internet, la prudence s'impose avec les données personnelles. Car à l'arrière-plan, de nombreuses données sont collectées sur les habitudes de navigation, généralement dans le but d'afficher la publicité adéquate, et ainsi de gagner un maximum d'argent.

Les fabricants de navigateurs ont mis au point des réglages pour éviter que des entreprises commerciales n'obtiennent des informations sur les habitudes de navigation. Une première restriction désactive la fonction «Accepter les cookies tiers». Outre le règlement d'autres paramètres de la vie privée, ce blocage peut être effectué sur tout navigateur. Firefox et Internet Explorer (les numéros de versions sont indiqués ici[46]) offrent en outre l'option «Do not Track», qui invite un site Web par *«opt-out»* à ne pas établir de profil de navigation. Il convient encore de mentionner ici le module d'extension (*add-on*) de Firefox «Ghostery»[47], qui déjoue autant que possible, à l'aide d'une liste noire, toute tentative de traçage. Or ni cette procédure ni aucune autre ne saurait garantir à 100 % qu'aucune donnée ne soit collectée et, le cas échéant, agrégée à d'autres.

[46] http://ie.microsoft.com/testdrive/browser/donottrack/default.html (état: 28 février 2013).

[47] http://www.ghostery.com/ (état: 28 février 2013).

5.5 Données de sociétés tierces sur les propres pages d'une entreprise – un problème pour la sécurité?

Beaucoup de sites Web affichent de la publicité. Or cette publicité provient très rarement de l'entreprise elle-même, mais d'une société tierce qui en assure la production et la gestion (voir aussi chap. 5.4). Hormis la publicité, beaucoup d'autres contenus sont injectés par des fournisseurs externes – service statistique, service affichant les actualités ou les cours boursiers, etc. En l'occurrence, on n'a pas affaire à une simple image, mais en général à une page dans la page (*IFrame*) pleinement fonctionnelle, possédant les mêmes droits que le site principal. Les portails d'information en particulier utilisent de telles fonctions, car ils ont besoin d'intégrer des informations tirées de différents sites.

Figure 7: URL de sociétés tierces publiant du contenu et utilisant Javascript sur le site Web de deux quotidiens suisses. Le programme NoScript utilisé bloque les pages de tiers utilisant Javascript et les signale comme telles.

La figure 7 montre les divers contenus étrangers s'affichant sur le site Web de deux quotidiens suisses. Tous deux se procurent leurs contenus publicitaires auprès de tiers. Parfois les mêmes entreprises ou serveurs se chargent de la livraison des contenus. Ces serveurs revêtent donc un rôle central. A supposer que l'un d'eux soit compromis, les conséquences pourraient être dramatiques et, au pire des cas, une bonne partie des ordinateurs de la population suisse seraient infectés. Ces dernières années, divers incidents de ce genre sont survenus à une moindre échelle. A la mi-mai 2012, un *maliciel* s'était répandu via une bannière publicitaire du site wetter.com[48]. Des sociétés suisses ont déjà connu pareille mésaventure et ont diffusé à leur insu des maliciels, à partir d'une bannière publicitaire accueillie sur leur site.

Indépendamment de tous les avantages et des économies qu'une centralisation des contenus Web peut lui offrir, toute entreprise devrait être bien consciente des risques qui s'ensuivent. Non seulement les ordinateurs des internautes visitant son site Web risquent une infection par maliciel, mais en cas d'incident l'entreprise touchée s'expose à une perte de confiance.

[48] Voir rapport MELANI 2012/1, chapitre 4.9: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: 28 février 2013).

Il faut donc absolument définir, en amont déjà, comment procéder au cas où du contenu de tiers serait compromis. L'entreprise a-t-elle accès à ces contenus, ou peut-elle les modifier ou les supprimer en cas de nécessité? Il importe surtout de définir par avance les contacts pour la sécurité informatique avec les entreprises tierces, afin de pouvoir rapidement joindre les bonnes personnes et adopter les mesures appropriées en cas d'incident.

5.6 Fiabilité de la chaîne logistique

A fin avril 2012, Sunrise a annoncé son projet de confier à Huawei, pour les cinq prochaines années, l'exploitation et l'entretien de ses réseaux mobile et fixe. Ce prestataire chinois assume l'entière responsabilité opérationnelle de Sunrise depuis le 1er septembre 2012. Au début de février 2013, Swisscom a conclu à son tour un partenariat avec Huawei. Limité à huit ans, le mandat porte sur l'extension du réseau à fibre optique jusqu'aux bâtiments (Fibre to the Street, FTTS). L'arrivée de sociétés étrangères sur le marché suisse des télécommunications constitue-t-elle une menace pour la sécurité nationale? Cette question se pose par rapport à l'accès à des informations sensibles et aux possibilités de sabotage des infrastructures de l'information qu'une telle position autorise.

Même si aucun incident de ce genre n'est connu à ce jour, il n'est pas complètement exclu que la participation d'entreprises étrangères au déploiement ou à la maintenance de réseaux suisses de télécommunication ne puisse être exploitée par des services de renseignements étrangers. Toutefois, les entreprises télécom passant des contrats au niveau mondial n'ont aucun intérêt à participer à de telles pratiques. Car si un tel cas était rendu public, non seulement elles n'inspireraient plus confiance et leur réputation serait mise à mal, mais elles s'exposeraient à des sanctions sous forme d'interdiction d'accès à certains marchés.

Il n'est jamais exclu qu'un Etat cherche à étendre son influence, a fortiori si le contexte politique international devait évoluer. Et comme tout composant électronique possède des micrologiciels (*firmware*), il serait possible par la suite d'y placer des *maliciels*. L'alternative à la confiance absolue accordée à un fabricant consiste à utiliser toutes les possibilités de contrôle, en procédant pour chaque produit ou mise à jour de logiciel à des analyses, aussi longues que coûteuses, du *code source* et à des tests de sécurité. L'idéal réside dans un bon dosage de ces deux approches. Les analyses des risques et des vulnérabilités font partie du b.a.-ba de toute stratégie d'entreprise. Elles devraient par conséquent se focaliser moins sur le pays d'origine du fabricant que sur les possibilités de prévoir plus tard d'autres mesures de sécurité, indépendamment de l'appareil utilisé.

6 Glossaire

0-day-exploit	Exploit paraissant le jour même où une faille de sécurité est rendue publique.
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Adresse IP publique	Adresse IP reconnue et adressable normalement dans le réseau.
Advanced Research Projects Agency Network (ARPANet)	Le réseau Arpanet est l'ancêtre d'Internet. Il a été développé dès 1962, à la demande des forces aériennes américaines, par une petite équipe de chercheurs placée sous la direction du Massachusetts Institute of Technology et du ministère de la Défense.
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 DoS	attaque par déni de service (denial of service). Vise à rendre impossible l'accès à des ressources, ou du moins à le restreindre fortement aux utilisateurs.
BitTorrent	BitTorrent est un protocole de transfert de données pair à pair permettant de distribuer rapidement de grandes quantités de données.
Certificat numérique	Attestation qu'une entité (personne, ordinateur) possède une clé publique (PKI).
Circuit imprimé (platine)	Support, généralement sous forme de plaque, destiné à regrouper des composants électroniques pour réaliser un système plus complexe. Les appareils électroniques en possèdent généralement un ou plusieurs.
Code source	Instructions originales d'un programme écrites dans un langage lisible par l'homme et devant être compilées (traduites) pour être lues par un ordinateur.
Computer Emergency Response Team (CERT)	Le terme CERT (ou CSIRT, Computer Security Incident Response Team) désigne un organisme chargé de la coordination et de l'adoption de mesures liées aux incidents relevant de la sécurité informatique.
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.
Cryptage RSA	Du nom de ses inventeurs Rivest, Shamir et Adleman. Méthode de cryptage avec clé publique introduite en 1978. RSA est une procédure asymétrique.
Débordement de tampon	Fréquente faille de sécurité des logiciels, dont les pirates profitent pour glisser dans la mémoire tampon des codes permettant de faire exécuter des programmes d'accès (en anglais buffer overflow).
Defacement	Défiguration de sites Web.
Système de noms de domaine (Domain Name System, DNS)	Le DNS rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP les utilisateurs composent un nom (p. ex. www.melani.admin.ch).
DNS Amplification Attack	Attaque par déni de service (attaque Denial of Service, DoS), utilisant des serveurs DNS publics comme amplificateurs.
Domaines	Tout nom de domaine (p. ex. www.exemple.com) est associé par l'intermédiaire d'un serveur DNS (Domain Name System) à son adresse IP, laquelle permet d'établir une connexion réseau entre ordinateurs.
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.
Firmware	Microprogrammes. Instructions enregistrées dans une puce pour commander un appareil (p.ex. numériseur, carte graphique, etc.). Elles sont en général modifiables par des mises à jour.
General Packet Radio Service (GPRS)	Le general packet radio service (service général de radiocommunication par paquets) est un service de transmission numérique des données par ondes radioélectriques, offert sur un réseau mobile de type GSM et utilisant la commutation de paquets.
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.
Global System for Mobile Communications (GSM)	Le réseau GSM (Global System for Mobile Communications, au départ Groupe spécial mobile) constitue un standard de téléphonie mobile entièrement numérique, permettant de transmettre la voix ainsi que des messages texte (SMS) ou multimédia.

HyperText Transfer Protocol Secure (https)	Protocole pour une transmission sécurisée, c'est-à-dire chiffrée, de données HTML dans un réseau (p. ex. Internet).
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.
Lecteur de codes-barres	Un lecteur de codes-barres (barcode scanner) est un appareil utilisé pour décoder et transmettre différents codes-barres. Des technologies de lecture optique ou par faisceau rouge ou infrarouge sont utilisées.
Programme/logiciel malveillant	Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie). Voir aussi malware
Master Boot Record (MBR)	Le secteur de démarrage principal (Master Boot Record) est le premier bloc de données (d'une taille de 512 octets) du disque dur. Le MBR contient la table de partition du support de données ainsi qu'une routine d'amorçage servant à charger le système d'exploitation présent sur l'une des partitions.
Navigateur / Browser	Logiciel utilisé essentiellement pour afficher les différents contenus du Web. Les navigateurs les plus connus sont Internet Explorer, Netscape, Opera, Firefox et Safari.
Opt out	L'option d'exclusion (opt out) désigne en marketing direct la possibilité donnée aux clients inscrits d'office sur une liste établie à des fins de promotion ou de publicité de s'en désinscrire.
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 sites 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.
Pile (stack)	Mise en œuvre particulière d'un ensemble de protocoles de communication réseau.

Numéro d'identification personnel (PIN)	Un numéro d'identification personnel est un code numérique secret permettant d'obtenir l'accès à une machine et d'y effectuer l'opération désirée.
Piratage téléphonique	Le piratage téléphonique (phreaking) consiste à percer les systèmes téléphoniques, afin notamment de ne pas payer la conversation ou de rester anonyme.
Point of sale (POS)	Un terminal EFT/POS est un terminal de point de vente (POS, point of sale) acceptant le paiement sans numéraire (EFT, electronic funds transfer).
Proxy	Programme servant d'intermédiaire pour accéder à un autre réseau, en collectant les requêtes et en les transmettant vers l'extérieur à partir d'une même adresse.
Réseaux IP Européens (RIPE)	Le RIPE NCC (Réseaux IP Européens – Network Coordination Centre) est un registre régional gérant l'attribution des ressources (adresses IP et numéros d'AS notamment) en Europe et dans une partie de l'Asie, dont le Moyen-Orient.
Résolveur de DNS	Un résolveur (resolver) est un module logiciel simple installé sur un ordinateur client DNS. Il sert d'interface entre l'application du client et les serveurs de noms, en effectuant des requêtes de résolution de noms.
Routeur	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un routeur s'utilise par exemple dans un réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
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).
Serveur DNS faisant autorité	Un serveur DNS faisant autorité est responsable d'une zone. Ses informations concernant cette zone sont par conséquent réputées sûres.
Signature de transaction	Elément de sécurité supplémentaire du e-banking. Quand le client donne un ordre de paiement, il recevra p. ex. par SMS un code sur son téléphone mobile. La banque n'exécutera le paiement qu'une fois ce code saisi dans son système de e-banking.
Skimming	Le skimming (litt. écrémage en anglais) désigne une attaque par 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.

Smart Meter	Un Smart Meter (compteur intelligent en français) est un compteur électrique de nouvelle génération, qui identifie la consommation énergétique de l'utilisateur de manière détaillée et peut transmettre ces données à l'entreprise chargée de la distribution.
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.).
Short Message Service/Service de messages courts (SMS)	Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile.
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).
TCP/IP (Transmission Control Protocol / Internet Protocol)	Ensemble de protocoles de communication conçu pour la transmission des données sur Internet.
Top-Level-Domains (TLD)	Tout nom de domaine dans Internet est formé d'une série de signes séparés par des points. Le domaine de premier niveau ou de tête (TLD) désigne le dernier élément de cette série et se situe au niveau hiérarchique le plus élevé du nom. Par exemple, si le nom de domaine d'un ordinateur ou d'un site est de.example.com, le TLD sera «com».
Uniform Resource Locator (URL)	Adresse d'un document Web composée du nom du protocole, du nom du serveur et du nom de fichier avec son chemin d'accès (exemple : http://www.melani.admin.ch/test.html).
Universal Serial Bus (USB)	Norme servant (avec les interfaces physiques) à 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.
Usurpation d'identité (spoofing)	Technique consistant à remplacer son identité par celle d'une autre personne, afin d'agir anonymement.
Voice phishing	L'hameçonnage par téléphone est une pratique criminelle d'ingénierie sociale consistant à communiquer avec des gens par téléphone pour leur dérober des informations personnelles. Cette fraude tire habituellement parti des avantages de VoIP.
Voice over IP (VoIP)	Téléphonie par le protocole Internet (IP). Protocoles souvent utilisés: H.323 et SIP.