Cybersécurité:

les menaces actuelles et leur évolution

Auteur
Stefan Frei, Security Architect, Swisscom

Août 2015

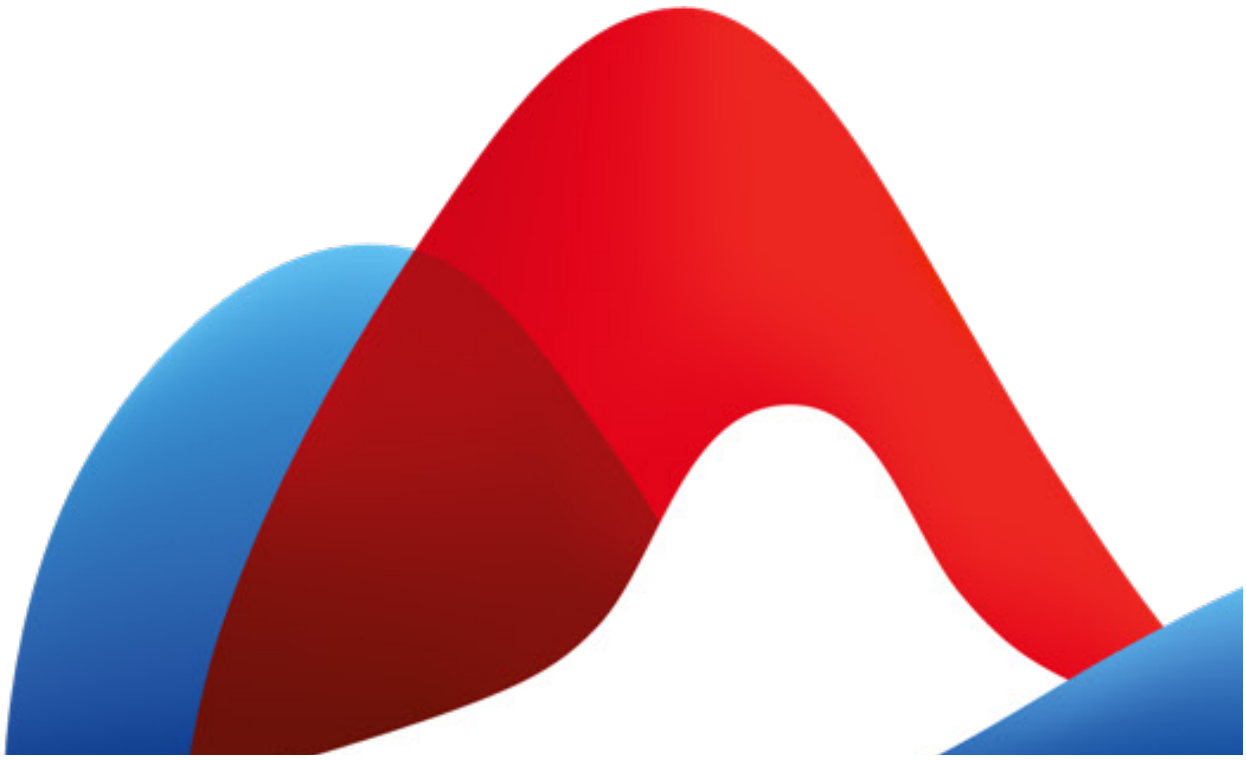

Table des matières

1 Introduction

Au cours des deux dernières décennies, le développement de nouvelles technologies, en particulier celles liées à Internet, a créé d'incroyables possibilités qui ont modifié durablement notre vie privée et professionnelle et qui continueront de le faire.
Les bouleversements générés par Internet peuvent être qualifiés de disruptifs. Ils ont des répercussions globales, comparables aux conséquences de la révolution industrielle et des innovations, par exemple la prospection de pétrole, l'invention de l'automobile ou l'introduction des antibiotiques.
Aujourd'hui, plus de trois milliards de personnes ont accès à Internet, ce qui correspond à 42% de la population mondiale en 2014[1]. La part de l'utilisation mobile ne cesse d'augmenter (94% de la population mondiale possède un téléphone mobile), tout comme le temps moyen que nous passons chaque jour sur Internet («always on»). La cybersécurité est devenue un facteur critique et continuera à gagner en importance dans la mesure où les gens seront de plus en plus connectés à leurs appareils.
Du point de vue de la société comme de l'économie, nous sommes toujours dans la phase précoce de l'adaptation de ces possibilités. Bien entendu, ces développements apportent également de nouvelles menaces et de nouveaux dangers. L'environnement de la sécurité Internet est marqué par une évolution fulgurante ainsi que des modifications de l'interface entre la technologie, l'économie et la société.

Dans le présent rapport, nous mettons en lumière la situation actuelle en matière de cybermenaces du point de vue de Swisscom et de la Suisse et, en tant qu'entreprise leader du marché des TIC en Suisse, donnons une estimation des développements attendus pour les 12 à 24 mois à venir.

2 Evolution de la situation en matière de cybermenaces

Aujourd'hui, Internet relie avec une intensité sans précédent les hommes, les machines, la technologie et l'économie. Les possibilités, mais aussi les menaces qui en résultent, sont la conséquence d'une multitude d'innovations technologiques ainsi que de nouvelles applications et services basés sur ces dernières. L'état actuel des menaces est complexe et évolue en permanence. Dans le cadre du présent travail, nous ne nous limiterons pas à l'extrapolation de menaces historiquement connues ou à certaines technologies. Notre objectif consiste, à partir de la dynamique et de l'évolution observées, à évaluer les menaces actuelles et à présenter l'évolution que nous entrevoyons au cours des 12 à 24 prochains mois.

[1] Internet World Statistics - http://www.internetworldstats.com/stats.htm

2.1 Situation – radar des menaces

Les menaces trouvent leur origine dans le développement constant de nouvelles technologies et de leur application et diffusion au sein de la société. Les menaces potentielles doivent être détectées de façon précoce et systématiquement répertoriées. Pour représenter l'état des menaces et leur évolution, nous utilisons un radar, voir Figure 2. Les thèmes et les menaces figurent sous forme de points sur le radar. Les points sur la Figure 2 reflètent la situation actuelle. La trace repérée montre pour chaque menace l'évolution que nous attendons au cours des 12 à 24 prochains mois.

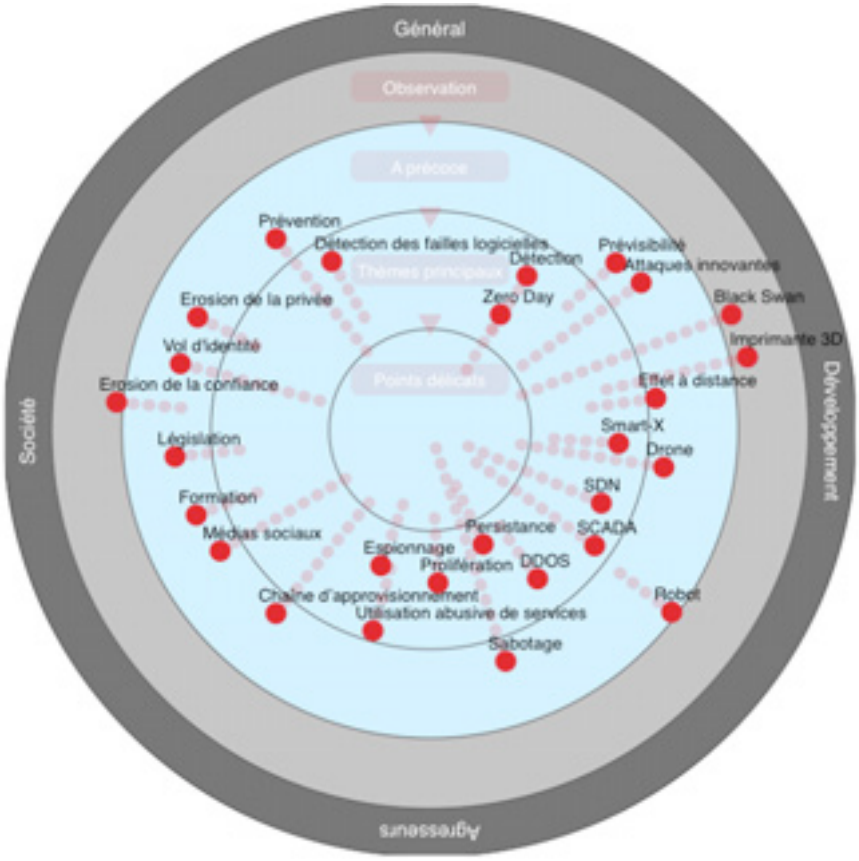

Figure 2 – Radar des menaces

Dans la Figure 2, nous distinguons quatre types de thèmes et de menaces, qui subdivisent le radar dans les segments *Général, Développement*, *Agresseurs* et *Société*:

Développement	Menaces résultant de l'évolution technologique, sans qu'elles ne soient induites spécifiquement par un agresseur ou un acteur spécifique.
Agresseurs	Menaces provenant de manière ciblée d'agresseurs.
Société	Menaces résultant de la mise en réseau croissante de la société.

Général	Menaces de nature générale et qui soit ne peuvent être affectées à aucune des catégories ci-dessus soit peuvent être affectées à plusieurs de ces catégories.

Il n'est pas toujours possible d'établir une séparation stricte dans ces quatre catégories.

Les nouvelles menaces ainsi que leur détection, leur évaluation ainsi que les contre-mesures suivent une évolution typique, qui est représentée sur le radar par les anneaux concentriques *Observation*, *Alerte précoce*, *Thèmes principaux* et *Points délicats*.

L'anneau extérieur *Observation* du radar contient des thèmes et développements susceptibles de devenir des menaces potentielles. Les thèmes figurant dans l'anneau *Observation* sont suivis systématiquement, mais avec des ressources limitées. L'anneau *Détection précoce* contient des menaces identifiées, qui pourraient devenir importantes au cours des prochaines années. Ces dernières sont examinées activement et approfondies en vue d'une meilleure compréhension du risque et de l'élaboration et de la préparation de contre-mesures. Les menaces figurant dans l'anneau *Thèmes principaux* sont actuelles. Des contre-mesures ont été engagées et mises en œuvre dans le cadre de projets et de processus réguliers.

Si l'évolution et le traitement des menaces ont lieu dans le cadre des trois phases décrites ci-dessus (*Observation*, *Détection précoce*, *Thèmes principaux)*, nous travaillons de manière proactive, de la détection systématique et précoce jusqu'au déploiement opérationnel de contre-mesures.

Les menaces qui apparaissent de façon inattendue ou celles qui évoluent plus rapidement que prévu sont traitées de manière réactive. Celles-ci figurent dans le radar dans l'anneau *Points délicats* situé le plus à l'intérieur.

Le radar fournit une vue d'ensemble et permet un relevé systématique de la situation ainsi que de l'évolution probable. Nous étudierons ci-après de manière approfondie ces évolutions ainsi que les différentes menaces.

3 Menaces liées à l'évolution

Les innovations technologiques, les nouvelles applications, l'utilisation différente d'Internet au sein de la société ainsi que le changement des conditions-cadres créent de nouvelle possibilités, mais aussi de nouvelles menaces. Certains des thèmes et des menaces du radar peuvent être dérivés de processus et de développements de niveau supérieur:

3.1 Complexité croissante de la société et d'internet

Notre société actuelle et l'utilisation d'Internet n'ont plus rien de commun avec les années 2000, lorsque la «bulle dot.com» a éclaté. Les années à venir devraient être tout aussi dynamiques et apporter une multitude d'innovations. La complexité du système Internet et de la société augmente rapidement et en permanence, avec un nombre croissant de nouvelles possibilités d'interaction et de combinaison entre l'homme, la machine, les services et divers processus de retour d'information. Une partie de ces nouvelles possibilités de combinaison et d'interaction entre l'homme et la machine («Devices»), qui voient le jour quotidiennement et en grand nombre, offrent fondamentalement de nouveaux scénarios d'attaque, que nous ne pouvons pas anticiper à partir d'une considération historique. En d'autres termes, nous devons distinguer les menaces prévisibles et modélisables («more of the same») des menaces qui sont en principe non prévisibles.

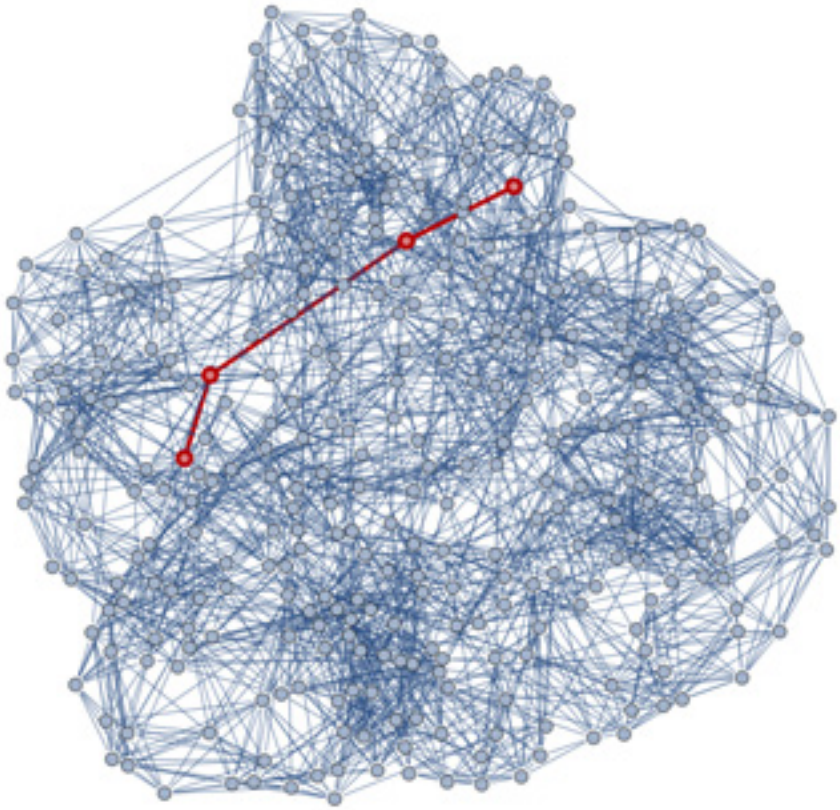

Figure 3 – Représentation simplifiée du système complexe Internet et société. Les personnes, les machines, les applications et les services capables d'interagir de manière diversifiée constituent des nœuds. Avec chaque nouveau nœud, le nombre de nouveaux moyens d'interaction possibles (représentés sous forme de lignes) entre les nœuds augmente de façon exponentielle.

Avec l'interconnexion croissante, de nouveaux nœuds sont intégrés en permanence dans le système Internet et société. A partir des nombreux moyens d'interaction nouveaux et parfois surprenants qui apparaissent chaque jour, nous tirons les enseignements suivants quant à la situation en matière de menaces:

Nouvelles attaques innovantes	Les attaques qualitativement nouvelles, basées sur de nouveaux moyens d'interaction, vont augmenter. Celles-ci ne doivent pas forcément être exigeantes sur le plan technique. Une protection de base insuffisante des nouveaux systèmes et de leur mise en réseau ainsi qu'un manque de compréhension des interactions nouvellement créées autorisent de nouveaux chemins d'attaque toujours surprenants.
Prévisibilité	La prévisibilité des menaces diminuera. Les tendances et développements comme *Internet of Things*, *Smart Home*, *Smart Grid*, etc. se situent actuellement au premier plan de cette évolution et des menaces qui en résultent.
Prévention	Avec la diversité croissante des possibilités d'attaque, la prévention devient plus difficile. De plus, les attaques qualitativement nouvelles ne sont en principe pas prévisibles. Les systèmes de sécurité et les services existants peuvent uniquement offrir une protection contre des scénarios que ces systèmes modélisent déjà.
Effet à distance, cascades	Dans un système complexe comme celui représenté sur la Figure 3, des composants supposés distants sont également reliés entre eux et peuvent parfois interagir de diverses manières. Cela signifie que les attaques contre des composants distants du système (ou des composants auparavant isolés) peuvent subitement avoir une influence directe sur les propres composants. Par ailleurs, des interventions mineures (ou bien intentionnées) en un lieu du système risquent d'avoir des répercussions graves et imprévisibles à un tout autre endroit du système («cascades»). Nous prévoyons par conséquent un nombre accru d'attaques contre des sous-systèmes ou des fournisseurs dans le but de compromettre un objectif primaire. Nous prévoyons en outre que des défauts ou des attaques de moindre importance provoquent des dommages surprenants en raison d'une cascade.

Exemple destiné à illustrer ces mécanismes:
Les appareils GPS sont connus de tous et sont largement utilisés pour la localisation. Ce que l'on sait moins, c'est que d'innombrables services et appareils critiques sont tributaires des signaux GPS pour obtenir *l'heure exacte* et synchroniser les processus. Par

conséquent, une défaillance accidentelle ou ciblée du système GPS (p. ex. suite à une activité solaire extrême, une erreur de configuration ou une perturbation) n'aura pas seulement une incidence sur les systèmes liés à la navigation.

Exemple: en 2007, à San Diego aux Etats-Unis, suite à une défaillance des signaux GPS consécutive à un brouillage accidentel, *les téléavertisseurs d'urgence*, *les téléphones mobiles*, *les systèmes de gestion du trafic* et les *distributeurs automatiques de billets* sont tombés en panne dans toute la ville pendant deux heures.[2]
Les dépendances vis-à-vis du GPS pour la datation et la synchronisation de nombreux processus ont encore augmenté depuis cet événement. De nombreux services, qui à priori n'ont aucun rapport avec la navigation ou la localisation, peuvent être touchés:[3]

- Systèmes de communication, téléphone, mobile et réseaux de données
- Systèmes de distribution d'énergie («Power Grid»)
- Systèmes de transactions financières
- Synchronisation mondiale de transactions
- Systèmes répartis et capteurs

La prévisibilité des dommages potentiels en cas de défaillance d'un signal GPS est faible et les défaillances surviennent en cascade. La prévention est extrêmement difficile, étant donné que dans les systèmes montés à demeure, il n'est pas possible d'étendre simplement la portée des récepteurs GPS.
Avec du recul, il est facile d'expliquer les défaillances présentées, car les dépendances ont été identifiées dans le cas décrit. Mais il devrait être relativement difficile d'établir une liste exhaustive des dépendances actuelles de la synchronisation/datation GPS.

3.2 Dynamique d'innovation

En raison de l'innovation constante et de l'amélioration permanente des technologies existantes avec une chute simultanée des prix, le seuil d'entrée est abaissé pour de nombreux types d'attaque. Les mesures de sécurité qui sont basées

- sur la disponibilité limitée des technologies d'attaque,
- leurs prix élevés
- ou leur performances limitées

auront des effets de plus en plus limités au cours des prochaines années. Ainsi par exemple, des applications et attaques nouvelles et surprenantes sont prévisibles en raison de la disponibilité générale des imprimantes 3D, des drones aériens, des robots, etc.

[2] http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html
[3] http://www.gps.gov/applications/timing/

Imprimantes 3D	Les mesures de sécurité basées sur la complexité ou le caractère unique d'éléments mécaniques deviennent inappropriées. Il est de plus en plus souvent possible de copier facilement des clés mécaniques ou des outils spécifiques ou d'en établir de nouveaux. Dans de nombreux cas, le remplacement des éléments de sécurité est très complexe et coûteux et ne peut pas être maîtrisé rapidement ou à l'aide d'une mise à jour logicielle.
Drones aériens, robots	Les drones aériens tout comme les robots miniatures peuvent être commandés à distance, ce qui permet de surmonter en toute simplicité les barrières d'accès. Les hypothèses actuelles relatives à la protection physique des accès doivent être réexaminées. L'espionnage de zones accessibles physiquement en vue de la préparation d'attaques va se multiplier. Les systèmes d'accès qui empêchent l'entrée dans la zone protégée, mais qui autorisent sans restriction la sortie de l'intérieur vers l'extérieur (p. ex. portes de secours, protection contre l'incendie, sorties de garage) peuvent être contournés aisément grâce à des robots infiltrés.
Software Defined Radio (SDR)	Avec la diffusion de la radio logicielle (Software Defined Radios - SDR), tous les types de réseaux sans fil et de systèmes de contrôle sont accessibles de plus en fréquemment et facilement aux attaquants. Le sentiment de sécurité conféré par l'utilisation de protocoles non documentés s'érode. Les mesures de sécurité basées sur l'accès privilégié à l'équipement radio et aux bandes de fréquences deviennent par conséquent inappropriées. Les nouvelles attaques de tous types de systèmes de radiocommande et de communication (véhicules, bâtiments, trafic, commandes d'accès, WiFi, GSM, GPS, ...) s'intensifieront. Ainsi par exemple, des brouilleurs GPS sont proposés aujourd'hui pour moins de 100 dollars.

3.3 Internet et machines

En raison de l'interconnexion disponible partout et à tout moment et de la miniaturisation continue des composants, un nombre croissant de machines, d'appareils («Devices») et de capteurs de tous genres sont connectés à des réseaux. Cette évolution est rapide dans différents domaines. A côté des systèmes de contrôle qui pilotent les processus industriels et les flux énergétiques, les appareils et les capteurs qui régissent notre vie quotidienne se multiplient. Parmi les exemples notoires, on peut mentionner le tournant énergétique avec réseau intelligent «smart grid», la domotique «smart home», la gestion intelligente du trafic et les «smart cars» ainsi que les appareils portables («wearable devices») et la robotique («robotics»). Avec la diffusion croissante de ces technologies, le potentiel qu'elles représentent pour l'agresseur augmente également. Les dysfonctionnements ainsi que les attaques sur Internet entraîneront de plus en plus fréquemment des dommages non virtuels, avec des conséquences potentiellement fatales pour l'homme, l'environnement, la société et le matériel. Suite à l'interconnexion croissante, intentionnelle ou non, nous prévoyons au cours des prochaines années une multiplication des attaques dans ce domaine.

Systèmes de contrôle industriel ICS/SCADA	Les failles et les vecteurs d'attaque contre les systèmes ICS/SCADA se répandent à un rythme plus rapide que celui auquel leur protection peut être assurée. Les attaques ciblées et réussies contre ces systèmes de contrôle vont augmenter. Les systèmes de contrôle montés à demeure et accessibles, qui ne disposent pas d'un mécanisme intégré pour la mise à jour de sécurité du logiciel, ne peuvent pas être protégés ou ne peuvent l'être qu'à un coût très élevé. Par ailleurs, la durée d'utilisation de ces systèmes est nettement supérieure à celle des systèmes typiques des utilisateurs finals comme les PC, les tablettes et les téléphones mobiles. Parmi les systèmes de contrôle dont l'utilisation est critique aujourd'hui, nombre d'entre eux sont obsolètes et ont été construits à une époque où les menaces étaient comparativement insignifiantes. Ils sont donc extrêmement vulnérables et leur fonctionnement peut parfois être compromis par des attaques triviales.

Smart Home, Smart Grid, Smart Car, etc.,	Une forte concurrence, la chute des prix et la miniaturisation entraînent la diffusion de plus en plus rapide de tous types de systèmes et d'appareils «smart». Souvent, la sécurité joue un rôle mineur dans le design: • Méconnaissance des attaques complexes innovantes • Délai de commercialisation plus important que la sécurité • Mauvaise compréhension de la sécurité des différents composants ainsi que leur interaction • Absence de ressources pour garantir une réelle sécurité sur les appareils fortement miniaturisés En outre, ces systèmes sont de plus en plus fréquemment utilisés à des fins innovantes, non prévues au départ dans le cadre du design. Il en résulte une protection insuffisante des systèmes de contrôle ou de leur communication. Nous prévoyons une multiplication des attaques ainsi que de nouvelles défaillances spectaculaires, avec des dommages non virtuels.

3.4 Mises à jour de sécurité automatisées

Dans un environnement où les menaces sont en constante évolution, il est d'une importance capitale de pouvoir actualiser aisément un système à l'aide de mises à jour de sécurité. Les fabricants de systèmes d'exploitation et de logiciels à grande diffusion (Windows, navigateur Internet, App Stores, etc.) ont reconnu ce besoin et largement travaillé sur la convivialité et l'installation automatisée de mises à jour de sécurité. La Figure 4 donne un aperçu schématique de l'évolution des menaces et du développement de la protection au moyen de mises à jour de sécurité pour des ordinateurs typiques. Les mises à jour de sécurité permettent d'adapter régulièrement la protection aux nouvelles menaces.
Les systèmes de contrôle de tous genres (ICS/SCADA, Smart-X, etc.), qui ne disposent d'aucun mécanisme pour l'installation rapide et aisée des mises à jour de sécurité, deviennent de plus en plus vulnérables. Les menaces augmentent, et la protection inhérente s'érode, voir Figure 4. La situation est encore aggravée par le fait que ces systèmes sont généralement utilisés beaucoup plus longtemps que les PC.

Des mécanismes de mise à jour efficaces pour tous types de systèmes en réseau sont un préalable indispensable à un fonctionnement sûr et une durée d'utilisation prolongée.

L'absence de mécanisme de mise à jour de sécurité dans un produit ou un appareil en réseau doit être considérée comme un indicateur sûr pour de futures attaques ou défaillances.

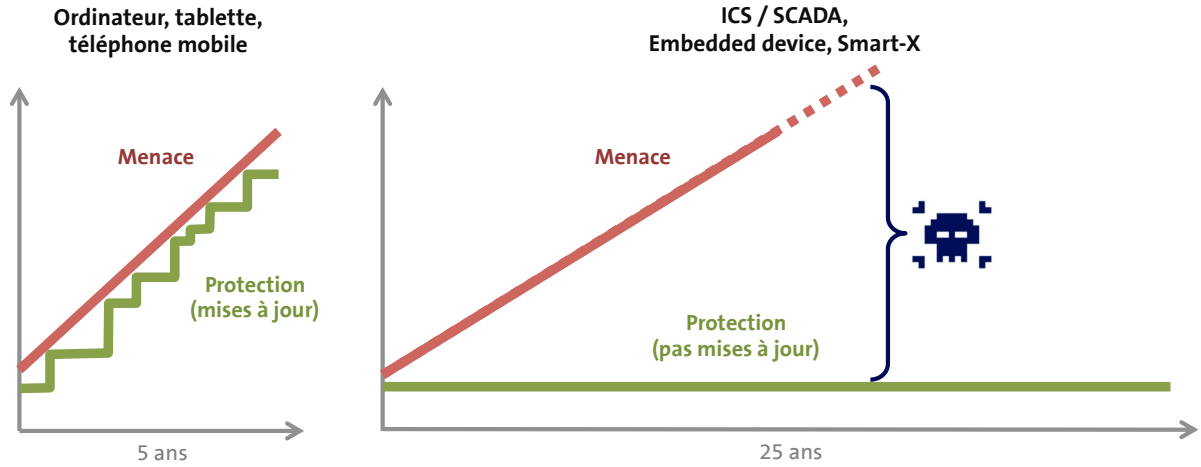

Figure 4 – Une durée d'exploitation prolongée sans possibilité de mises à jour de sécurité des systèmes ICS/SCADA entraîne une augmentation constante de la vulnérabilité.

3.5 Anciens systèmes (Legacy)

De nombreux systèmes informatiques ainsi que leurs applications sont utilisés bien au-delà de la durée de vie prévue par le fabricant. Ces systèmes ne sont plus pris en charge par ce dernier et utilisent des environnements d'exploitation et de développement ainsi que des protocoles de communication obsolètes. En outre, les mécanismes de protection intégrés tels que ceux que nous connaissons sur les ordinateurs personnels (p. ex. antimalware, exploit mitigation) ne sont pas disponibles dans la plupart des cas. En général, ces systèmes sont complexes et remplissent des fonctions critiques et spéciales – deux raisons pour lesquelles ils ne sont pas remplacés.
Dans le même temps, ces anciens systèmes sont soumis à la même pression en matière d'interconnexion directe et indirecte, à la fois en interne et en externe. Leur capacité de résistance aux attaques reste constante, alors que les menaces ne cessent d'évoluer, ainsi que le montre la Figure 4.

Anciens systèmes et protocoles	Nous tablons sur une recrudescence des attaques contre des systèmes et protocoles obsolètes. Avec la diffusion de connaissances spéciales sur ces systèmes, les risques augmentent également.

Interconnexion et API	Les anciens systèmes sans contact extérieur direct sont de plus en plus fréquemment reliés à une superstructure moderne au travers d'interfaces API. De ce fait, ces systèmes, leurs données ainsi que des fonctions auparavant isolées sont exposées vis-à-vis de l'extérieur. Nous prévoyons une diffusion encore plus large des API ainsi que des protocoles et de la communication machine-machine, allant au-delà des zones de protection actuelles. Il en résultera notamment de nouveaux vecteurs d'attaque innovants. Nous attendons également une augmentation des violations de données, ce qui aura pour effet d'exposer des systèmes d'exploitation auparavant isolés.

3.6 Complexité des logiciels

En dépit de grands progrès et d'investissements importants dans le développement de logiciels sécurisés, l'industrie ne parvient pas à créer et à commercialiser des logiciels intrinsèquement sûrs. Sur dix grands développeurs de logiciels, seulement quatre ont pu réduire le nombre de failles dans leurs produits au cours des douze derniers mois par rapport à la moyenne des cinq années précédentes. La Figure 5 montre l'évolution des failles logicielles sur les vingt dernières années.

Failles logicielles	Nous attendons toujours un grand nombre de failles, qui concernent pour l'essentiel des produits ayant de grandes parts de marché. Les systèmes qui ne sont pas considérés directement comme des ordinateurs (p. ex. systèmes de contrôle, SmartX, capteurs) ne seront pas épargnés.

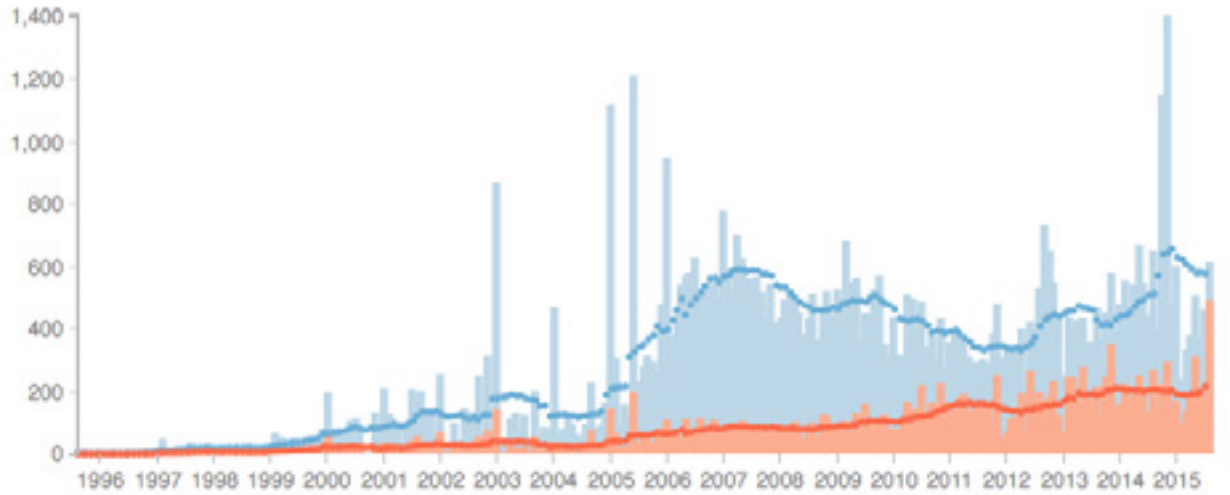

Figure 5 - Failles publiées par mois, 1995 à 2015. En rouge: Failles des dix plus grandes entreprises. Les lignes indiquent la moyenne sur les douze mois précédents.[4]

Des mécanismes de mise à jour efficaces, capables d'actualiser un grand nombre de systèmes concernés, revêtiront une importance croissante. L'absence de tels mécanismes dans un produit ou un appareil interconnecté doit être considérée comme un indicateur sûr pour de futures attaques ou défaillances.

4 Menaces par des agresseurs

Les menaces décrites dans la partie précédente sont le résultat du développement d'Internet, de la technologie et de la société, sans qu'un acteur particulier ne planifie, pilote ou lance une menace.

Nous examinerons cependant, dans la quatrième partie, les menaces émanant d'acteurs.

Nous distinguons cinq groupes d'acteurs ayant différents objectifs, moyens et méthodes. Ces groupes sont énumérés à la Figure 7.

[4] http://techzoom.net/BugBounty/SecureSoftware

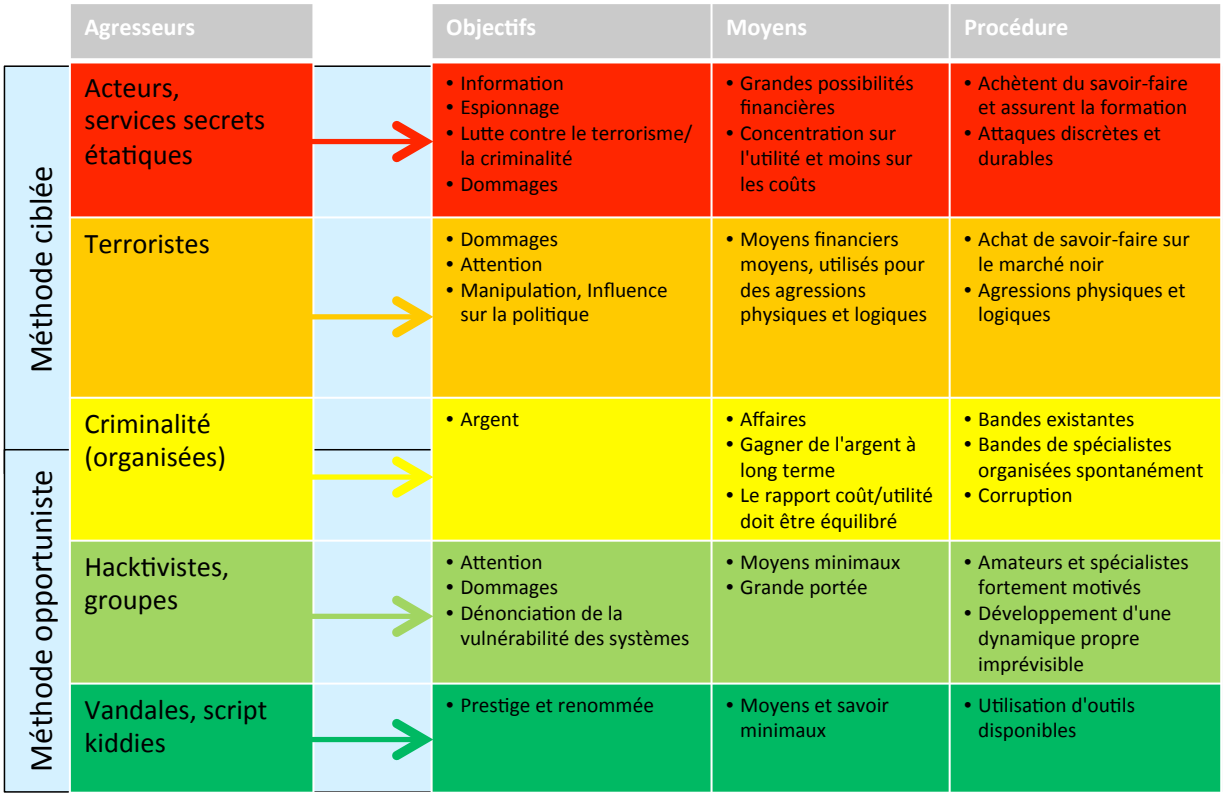

Figure 7 – Classification des agresseurs

Nous distinguons par ailleurs les acteurs qui procèdent *de manière opportuniste* des acteurs *qui procèdent de manière ciblée*, la transition étant parfois floue.

Méthode opportuniste	Les acteurs utilisent les possibilités d'Internet, soit parce que l'occasion se présente de manière fortuite, soit parce que la cible est mal protégée.
Méthode ciblée	Les acteurs ont un objectif clairement défini, qu'ils poursuivent résolument et de manière typique, avec des ressources considérables (finances, expertise, personnel, matériel). Ces agresseurs sont souvent persévérants en ce sens que la poursuite de l'objectif se fait également sur une période prolongée et par le biais de divers canaux parallèles.

4.1 Acteurs et services secrets étatiques

De tout temps, les Etats et les services secrets ont fait de l'espionnage et du sabotage. Le cyberespionnage et le cybersabotage font de plus en plus fréquemment partie des stratégies militaires de défense et d'attaque. Certains Etats procèdent actuellement au développement massif de leurs cybercapacités offensives et défensives.
A la différence des cybercriminels et d'autres agresseurs, les Etats peuvent se procurer un accès direct aux parties critiques de l'infrastructure Internet («Internet Backbone») et

forcer, de par la loi, les fournisseurs de services ou les fabricants à la surveillance ou à la coopération. Les activités étatiques vont de la surveillance systématique et étendue du trafic Internet à l'introduction cachée de logiciels malveillants dans le matériel et les logiciels des systèmes cibles d'autre pays (ou de concurrents).
Elles ont pour objectif d'une part de recueillir des informations, et d'autre part, de préparer la possibilité d'un sabotage par des implants cachés («backdoors», «kill switches»). En particulier au nom de la lutte contre le terrorisme et pour le contrôle de l'opposition, des données sont interceptées de façon massive et systématique sur Internet.
Les agresseurs étatiques disposent d'énormes ressources et de la persévérance nécessaire pour atteindre un objectif par le biais de plusieurs canaux d'attaque et sur de longues périodes.

Chaîne d'approvisionnement Supply Chain	Nous devons partir du principe que des parties de l'infrastructure critique de notre pays sont déjà compromises. A l'avenir, l'intégrité des objets à livrer sera de plus en plus menacée et devra être remise en question.
Espionnage industriel	Une grande partie de la valeur ajoutée de notre pays résulte de l'exploitation des droits de propriété intellectuelle et industrielle. Nous prévoyons une recrudescence des attaques à des fins d'espionnage industriel.
Sabotage/préparation	Les services secrets mettront en œuvre de plus en plus souvent des kill switches ou d'autres mesures afin de préparer un sabotage en cas de besoin. Sont concernés à la fois les produits matériels et logiciels. Une telle fonctionnalité peut se manifester par exemple dans des «failles logicielles» ou des comptes d'accès intégrés à des «fins de maintenance». Il est parfois difficile d'attribuer clairement un défaut à une mesure intentionnelle d'un adversaire. Le matériel peut être livré doté de sécurités et de points de rupture, de manière à ce qu'une fonction correspondante puisse être activée ou désactivée à distance par des impulsions logicielles.
Télécommunication mobile, WiFi	Les réseaux de communication mobile et les réseaux WiFi feront de plus en plus l'objet d'attaques actives ou passives (sniffing, jamming, spoofing, SS7, ...).
APT/Zero Day	Les attaques techniquement sophistiquées vont augmenter, alors que dans le même temps, la possibilité de les détecter va se réduire.

4.2 Terrorisme

Tout comme les criminels, les terroristes font eux aussi appel aux possibilités d'Internet. Leur objectif n'est pas de nature financière, mais consiste à susciter ou multiplier l'attention en faveur de leur cause et à manipuler et influencer les milieux politiques et la société. En d'autres termes, il s'agit d'occasionner un maximum de dommages afin de susciter la plus grande attention possible et répandre la peur et la terreur par des scénarios entièrement réels.

Utilisation abusive de services	L'utilisation abusive de services établis à des fins de propagande et de recrutement (p. ex. hébergement, médias sociaux, communication) est amenée à augmenter.
DDOS	Les attaques distribuées par déni de service (Distributed Denial of Service - DDOS) en vue d'une démonstration de force ou pour entraîner un maximum de dommages vont se multiplier.
Evénements	Les grandes manifestations ou conférences sur des sujets sensibles feront de plus en plus fréquemment l'objet de cyberattaques. Celles-ci toucheront également de façon accrue les fournisseurs et les prestataires qui participent à ces manifestations.
Médias électroniques	Nous attendons une multiplication des attaques ciblées contre tous types de médias très populaires (TV, radio, web, médias sociaux). Il s'agit là d'objectifs appropriés pour diffuser de la propagande, semer la panique et faire des démonstrations de force.
Comptes utilisateur critiques	Nous prévoyons une multiplication des attaques contre les comptes utilisateur individuels ayant de nombreux membres (Facebook, Twitter, blogs, ...).

Les grandes manifestations ou les services s'adressant un vaste public (p. ex. stations TV, retransmission de grands événements comme par exemple une coupe du monde de football), constituent des plateformes idéales pour les attaques terroristes. Outre ces services, des comptes individuels (p. ex. Twitter, Facebook, etc.), qui ont une forte audience, sont également menacés plus fréquemment. Nous estimons que ce type de services et de comptes feront plus souvent l'objet d'attaques ciblées.

4.3 Criminalité organisée

La criminalité et la criminalité organisée font partie des phénomènes les plus anciens de la société. L'histoire nous apprend que les criminels s'approprient et mettent à profit très rapidement les nouvelles technologies.
Les criminels procèdent avec professionnalisme pour atteindre leurs objectifs financiers, à la fois de manière ciblée et opportuniste.
Divers groupes criminels se spécialisent dans des domaines particuliers, par exemple la recherche de points faibles, le développement de logiciels malveillants, la vente/location d'outils, la gestion de botnets, le recrutement de money mules, la création d'e-mails de phishing, etc. Criminalité traditionnelle et cybercriminalité se complètent et se confondent.
Du fait de cette répartition du travail, des «services» et «outils» de haute qualité, qui peuvent en principe être achetés ou loués par tout un chacun, sont mis à disposition.

Diffusion des outils et services (prolifération)	Les outils d'attaque ainsi que les services destinés à la gestion de systèmes compromis deviennent de plus en plus raffinés et répandus.
Attaques complexes	Les attaques complexes et à plusieurs niveaux (p. ex. par DDOS) vont se multiplier. Les attaques de phishing seront plus raffinées sur le plan psychologique et parfaitement adaptées à la victime quant à la représentation, au contenu et au moment choisi («spearphishing»).
Camouflage, empêchement de la détection	Les logiciels malveillants et les outils d'attaque deviennent plus raffinés dans leur capacité à échapper à la détection par les produits de sécurité.
Persistance	Les points faibles sont plus fréquemment recherchés et exploités systématiquement et les attaques correspondantes sont commercialisées et proposées à des personnes désireuses d'acheter.

4.4 Hacktivistes

Les hacktivistes ont une mission, généralement dans le contexte d'un thème émotionnel. Pour coordonner une procédure, ils peuvent constituer ou trouver rapidement par les médias sociaux (souvent spontanément) de grands groupes de personnes partageant les mêmes idées. L'objectif de l'attaque est soit déterminé par le sujet (pollueurs, gouvernements, sociétés dominantes, ...), soit défini spontanément. Les acteurs sont fortement motivés et possèdent également un savoir professionnel dans leurs rangs. Une dynamique propre incontrôlable se créée facilement au sein du groupe.

Médias sociaux	Nous attendons une recrudescence de campagnes spontanées ou d'attaques coordonnées par le biais des médias sociaux contre des objectifs ayant un rapport direct ou indirect avec le sujet déclencheur.

4.5 Vandales, skript kiddies

Les vandales et les skript kiddies sont des attaquants non professionnels qui, par ennui ou besoin de se faire valoir, réalisent des attaques et des «expériences» à l'aide d'outils facilement disponibles. Ils n'ont aucun objectif particulier, mais la possibilité d'acquérir un certain prestige, avec des moyens et un savoir minimal, grâce à des cyberattaques. Aussi le choix de la cible et le moment de l'attaque doivent-ils plutôt être qualifiées d'aléatoires.
De telles attaques sont à considérer comme un bruit de fond permanent sur Internet et à traiter en conséquence. La protection de base de tous les systèmes interconnectés doit pouvoir repousser de telles attaques de manière automatisée. Avec la disponibilité accrue des informations et des outils d'attaque simples à utiliser, ces attaques ne vont pas diminuer, et la protection de base devra être contrôlée et adaptée en permanence.

5 Menace résultant de la mise en réseau de la société

5.1 Perte de repères

Des innovations techniques et de nouvelles applications Internet sont introduites à un rythme extrêmement rapide. Des acteurs de niche peuvent devenir en quelques années des fournisseurs dominants, ce qui constitue une menace pour les modèles commerciaux existants et les hypothèses de sécurité actuelles. Cela pose des exigences élevées aux personnes et à l'économie, car des secteurs entiers peuvent être remis en question du jour au lendemain (p. ex. entreprises de taxi vs. Uber, hôtels vs. AirBnB). Par nature, il n'y a pas de grandes chances de pouvoir, à long terme, lutter contre cette évolution, s'y soustraire ou renverser la tendance.

«**Because there is no army that can hold back an economic principle whose time has come»**
John Donovan, AT&T

Il existe par ailleurs un risque qu'en tant qu'économie et société, dans la recherche du droit applicable et de la formation, nous ne soyons plus en mesure de résister à la dynamique introduite par Internet, ce qui aura des répercussions fatales pour les futures générations.

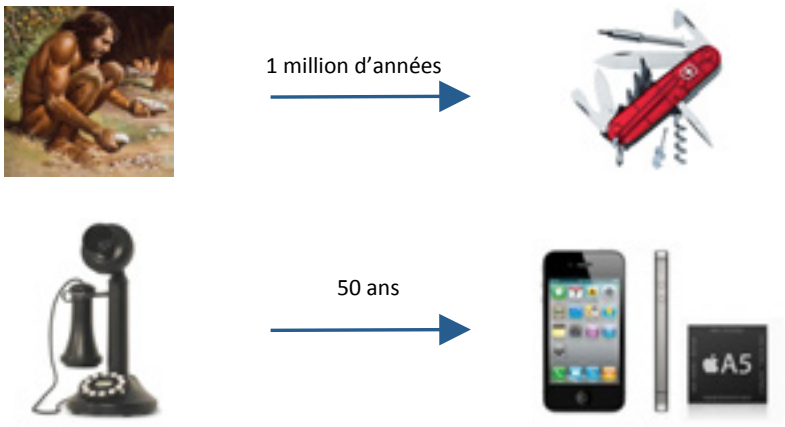

Figure 8 – Les nouvelles technologies sont introduites à un rythme toujours plus rapide, ce qui pose des défis majeurs à l'individu et à la société.

Nous devons apprendre rapidement, à tous les niveaux, à maîtriser de manière adéquate cette grande dynamique et agilité à l'ère d'Internet. Les développements comme le «cloud computing», la «shared economy», l'enseignement à distance, etc. exigent de nouvelles façons de penser afin d'évaluer correctement les avantages et les risques. Pour éviter de s'exposer de manière irréfléchie à des dépendances non souhaitées, il faut que ces risques et possibilités soient identifiés de façon précoce et que l'on dispose des mécanismes permettant d'exploiter le potentiel.
Les choses familières cèdent la place aux nouveautés, l'existant change en permanence. Il devient plus difficile de s'y retrouver dans cette diversité et ce flux d'informations.

Formation	Notre système de formation est encore toujours conçu pour acquérir avant tout des aptitudes telles que celles requises à la première phase de l'industrialisation.[5] Le risque en tant que société et économie, est que nous ne soyons pas en mesure de suivre l'évolution.

[5] https://www.youtube.com/watch?v=Optk-gYgFo8

Politique, recherche du droit applicable	La recherche du droit applicable peut difficilement suivre les développements rapides de l'ère de l'Internet. Les connaissances et la compréhension des tenants et aboutissants du cyber-environnement sont rares, avec le risque de voir adopter des lois non adéquates ou des lois déjà totalement obsolètes au moment de leur introduction. Le débat mené actuellement au sujet des logiciels d'intrusion dans le cadre de *l'arrangement de Wassenaar* illustre à la perfection ce défi.[6]
L'être humain	Avec l'augmentation rapide de la complexité et de la diversité des services, des possibilités d'interaction et de combinaison, l'être humain est de plus en plus sollicité voire dépassé. C'est vrai à la fois pour l'administrateur des systèmes TIC et pour les utilisateurs finaux. Cela ouvre une multitude de nouveaux espaces pour les agresseurs. La complexité est l'ennemi majeur de la sécurité, tant du point de vue technique que du point de vue humain et social.

5.2 Erosion de la sphère privée

Pour s'identifier vis-à-vis des services et des autorités, chacun dispose d'un nombre fini, mais faible, d'attributs personnels. Le nombre de services Internet utilisés quotidiennement et à l'avenir ne cesse d'augmenter. Lors de chaque fuite de données auprès d'un service ou d'une autorité quelconque, tous les attributs d'identification d'une personne disparaissent progressivement. Les attributs tels que *l'adresse e-mail, le mot de passe* et *les questions de sécurité* peuvent être modifiés relativement facilement après une fuite de données. Les attributs statistiques comme par exemple *le numéro de sécurité sociale, la date de naissance, le lieu de naissance, le sexe, le domicile,* etc. se modifient difficilement voire pas du tout. En raison de cette évolution et des nombreuses informations personnelles pouvant être consultées via les médias sociaux («OSINT»), les attributs personnels ne peuvent pas être tenus secrets à long terme[7].

La protection des données privées mises à la disposition de tiers devient de plus en plus difficile. Les attaques qui, par l'utilisation de données personnelles et privées, mettent en confiance la personne visée pour l'inciter à entreprendre certaines actions, continuent d'augmenter, à la fois en nombre et en raffinement.

[6] https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation
[7] http://techzoom.net/Publications/Papers/databreach

Usurpation d'identité	L'érosion croissante de la sphère privée entraînera une augmentation des attaques telles que l'usurpation d'identité. Ces attaques deviennent plus sophistiquées (plus personnelles) et leur détection par les personnes concernées devient de plus en plus difficile, voire impossible.
Utilisation abusive de données	Le volume élevé et toujours croissant de données personnelles et de métadonnées disponibles auprès de l'Etat, de tiers et de prestataires de services augmente le risque d'utilisation abusive et de surveillance.
Voie à sens unique	Les données personnelles, même si elles ne sont divulguées *qu'une seule fois* (volontairement ou involontairement), ne peuvent pas être retirées. Une fuite de données ou un faux pas suffit pour compromettre pour *toujours* la sphère privée. C'est pourquoi nous devons partir du principe que la plupart de nos données personnelles (p. ex. contacts) ne peuvent pas rester confidentielles. De nombreuses applications demandent par exemple à l'utilisateur un accès à ses coordonnées lors de leur lancement. Si par erreur, on répond ne serait-ce qu'une fois par «oui» à la question, la fuite des données ne peut plus être annulée.

5.3 Erosion de la confiance

Le flux d'information continu et l'utilisation abusive de plus en plus fréquente d'informations privées et personnelles entraînera, d'une manière générale, l'érosion de la confiance dans les services et informations.

Erosion de la confiance	La détection des attaques, lancées avec des méthodes raffinées et en utilisant des données personnelles et privées, deviendra plus difficile. Ces attaques augmenteront et seront de plus en plus souvent couronnées de succès.

6 Résumé

Les nouvelles technologies entraînent toujours une certaine insécurité au départ. Leur adaptation et leur bon usage constituent un processus qui prend du temps. Nous devons identifier les risques que nous pouvons repousser individuellement (en tant qu'utilisateur ou organisation) ainsi que les menaces qui existent ou sont inhérentes au système et celles qui ne peuvent être traitées durablement qu'au niveau de la société ou dans le cadre d'une coopération internationale.

Enseignements tirés de ces réflexions:

- La sécurité Internet est avant tout un problème de gestion de la complexité. La prise en compte de la technologie seule ne suffit pas à la compréhension des menaces.
- La prévention à cent pour cent est une illusion. Les entreprises tout comme les autorités doivent partir du principe que leur infrastructure sera compromise (ou qu'elle l'a déjà été).
- Les organisations doivent veiller à ce qu'une compromission déjà existante soit détectée et maîtrisée dans les meilleurs délais.
- Une compromission avérée doit être traitée dans le cadre d'un processus défini et éprouvé et non d'un processus d'exception.
- L'absence de mécanismes de mise à jour logicielle efficaces pour un produit ou un appareil en réseau doit être considérée comme un indicateur sûr pour des attaques et défaillances ultérieures.
- Nous estimons que les attaques ciblées se multiplieront et que leur nature ainsi que le moment de leur survenue seront imprévisibles.

7 Glossaire

0-Day/Zero-Day Exploit	Exploit software connu avant ou lors de la première divulgation d'une faille de sécurité. En d'autres termes, l'exploit est disponible avant que le développeur du logiciel ne dispose d'un patch de sécurité.
API	Application Programming Interface Interface de programmation permettant aux programmes d'échanger directement des données avec un langage commun (machine-machine).
Backdoor	Porte dérobée permettant d'accéder à un ordinateur en contournant la protection d'accès.
Botnet	Réseau avec grand nombre d'ordinateurs compromis, dont le contrôle central est assuré par un botmaster.
Defacement	Introduction de contenus indésirables sur un site Internet piraté.
DOS, DDOS	Déni de service (Denial of Service - DOS) Un système est paralysé par un grand nombre de demandes. Déni de service distribué (Distributed Denial of Service - DDOS) L'attaque DOS (attaque par déni de service) est lancée simultanément depuis un grand nombre de systèmes répartis (p. ex. un botnet). Il n'est plus possible de bloquer l'agresseur.
Exploit	Programme, code ou séquences d'instructions permettant d'exploiter les failles d'un logiciel.
Exploit Mitigation	Terme générique désignant les techniques utilisées pour empêcher ou rendre plus difficile l'exploitation des failles des systèmes.
GPS	Global Positioning System Système mondial de navigation par satellite, permettant de déterminer à un moment précis une position géographique.
ICS	Industry Control System Désignation générale des systèmes de contrôle industriel, voir SCADA.
TIC	Abréviation correspondant à technologies de l'information et de la communication, pour le secteur de l'informatique et des télécommunications.
Jamming	Brouillage intentionnel de la radiocommunication.
Kill switch	Logiciel caché, qui peut également réagir à un ordre provenant de l'extérieur et qui perturbe le fonctionnement d'un système ou le rend inutilisable.

Malware	Logiciel malveillant qui exécute des fonctions dommageables et non souhaitées.
Money Mule	Des criminels incitent des personnes à percevoir de l'argent de «clients» et à le transférer, par le biais d'un service de transfert, après déduction d'une commission. La personne (money mule) croit travailler pour une organisation légitime.
OSINT	Open Source Intelligence Collecte d'informations en utilisant exclusivement des sources accessibles au public.
Patch Mise à jour de sécurité	Remplacement du code programme du logiciel défectueux afin d'éliminer les failles de sécurité.
Phishing	Avec le phishing, les utilisateurs sont incités à divulguer des données sensibles (le plus souvent par des e-mails contenant des messages trompeurs).
SCADA	Supervisory Control And Data Acquisition System Systèmes de surveillance et de contrôle de processus techniques (p. ex processus industriels).
Faille	Faille ou vulnérabilité matérielle ou logicielle, par laquelle les pirates peuvent avoir accès à un système.
SDR	Software Defined Radio Emetteurs et récepteurs haute fréquence universels qui assurent le traitement des signaux par logiciel et qui sont par conséquent adaptables par l'utilisateur à différents protocoles et applications.
SmartGrid	Réseau électrique intelligent SmartGrid comprend l'interconnexion et la gestion des producteurs d'électricité, des systèmes de stockage, des consommateurs d'électricité ainsi que des réseaux de transmission et de distribution d'énergie.
SmartHome	Habitat intelligent Terme générique désignant la gestion en réseau et partiellement automatisée de l'énergie, de la maintenance et de la sécurité dans les appartements et les maisons.
Médias sociaux	Sites Internet sur lesquels les utilisateurs échangent des informations par le biais de profils établis par leurs soins (p. ex. Facebook, Twitter, LinkedIn, Xing).
Spearphishing	Attaques de phishing ciblées et personnalisées.
Spoofing	Tentatives de tromperie dans les réseaux en vue de masquer son identité.