AWK FOCUS

Juin 2013 Une publication d'AWK GROUP www.awk.ch

Du Global Village à Sin City?

André Arrigoni
Associé AWK Group

Il ne se passe pas un jour sans qu'on ne découvre de nouveaux sinistres, tentatives d'espionnage et autres vols de données. Il faut reconnaître que les mesures techniques préventives, qui sont souvent en décalage par rapport aux nouvelles menaces, et l'arsenal législatif ne sont que de peu d'efficacité par rapport aux risques de cette zone de non-droit que semble être le cyberespace.

Si Internet a incontestablement apporté d'immenses bénéfices, il devient aussi de plus en plus un foyer de nouvelles menaces et le terrain de jeu des criminels.

En outre, le web est de plus en plus entré dans le collimateur des forces armées et des services secrets. Dans de nombreux pays, des unités et services spécialisés pratiquent l'espionnage électronique via Internet – et ce, non seulement auprès d'institutions étatiques mais également d'entreprises privées.

Autrefois présenté comme *Global Village*, Internet s'apparente davantage à une mégapole dangereuse, dont les visiteurs feraient bien d'être sur leurs gardes!

Cordialement vôtre

Cybersécurité – tendances actuelles et mesures de protection

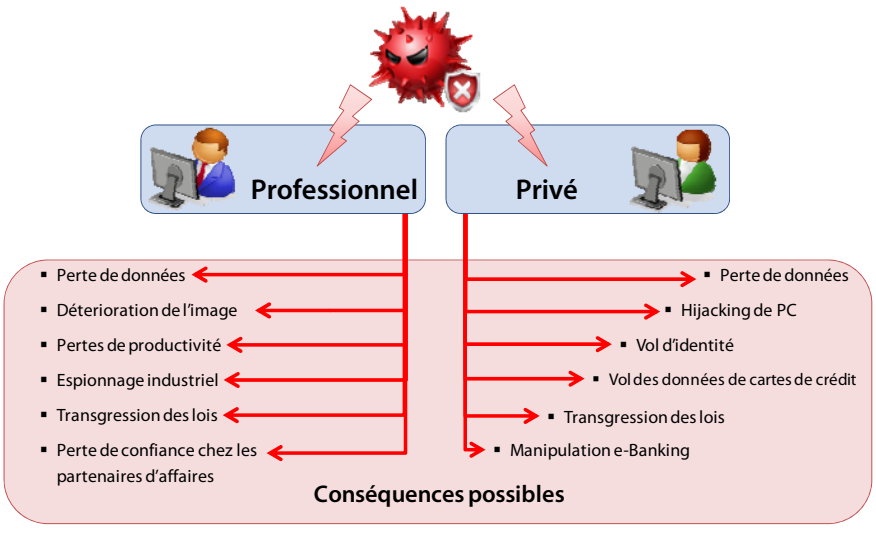
Les infrastructures d'information et de communication ont considérablement changé l'économie, l'Etat et la société. L'utilisation du cyberespace (Internet et les réseaux locaux qui y sont liés) apporte de multiples avantages et opportunités. Cependant, l'interconnexion numérique a également fait émerger de nouvelles menaces. Les infrastructures d'information et de communication sont détournées de leur usage à des fins criminelles, terroristes ou de renseignements. La cybersécurité doit donc trouver place dans la gestion des risques de notre société d'information moderne.

Dr Adrian Marti, Dr Philipp Grabher, Tarkan Bas

Un nombre croissant de services sont aujourd'hui proposés et utilisés par voie électronique. L'importance d'Internet ne cesse de croître pour L'Etat, l'économie et la société, accentuant notre dépendance à l'égard de cette infrastructure de communication critique.

Les menaces que les cyberrisques font peser sur les particuliers, les milieux économiques et les autorités étatiques sont bel et bien réelles:

- Des hackers infiltrent le réseau du DFAE (mai 2012) [1]
- Des centaines de milliers de données de patients ont disparu en Allemagne (octobre 2012) [2]
- Opération «Octobre rouge»: révélation d'une opération de cyberespionnage à grande échelle par Internet, portant atteinte à des représentations diplomatiques, organisations gouvernementales et instituts de recherche (janvier 2013) [3]



Cyberattaques et conséquences possibles

Normes et bonnes pratiques

ISO 27001:2005
Définit un système de management de la sécurité de l'information SMSI. Le point central est le processus d'amélioration continue, de même que les 134 points de contrôle destinés à piloter la sécurité de l'information.

ISO 27032
Définit les «Guidelines for Cyber-Security» avec des points de contrôle pour maîtriser les cyberrisques. La deuxième partie comprend des recommandations en matière de collaboration des diverses parties prenantes en vue d'augmenter la cybersécurité.

ITIL V5
L'IT Infrastructure Library s'est imposée comme une norme de fait pour la gestion des services informatiques opérationels. En matière de sécurité, l'ITIL traite de la gestion de la sécurité, de la gestion la continuité et de la gestion de la disponibilité.

CMM
Les Capability Maturity Models permettent de mesurer la maturité des processus et des organisations. Etant donné que la sécurité est très fortement liée à la maturité des organisations et des processus, les modèles de maturité s'appliquent parfaitement dans ce domaine.

Catalogue de protection de base du BSI et normes, ISF Good Practices, etc.
Il existe bon nombre de bonnes pratiques en matière de sécurité informatique et sécurité de l'information dont l'utilisation s'avère judicieuse dans le domaine de la cybersécurité.

Prévention: seules, les mesures de protection techniques ne suffisent pas

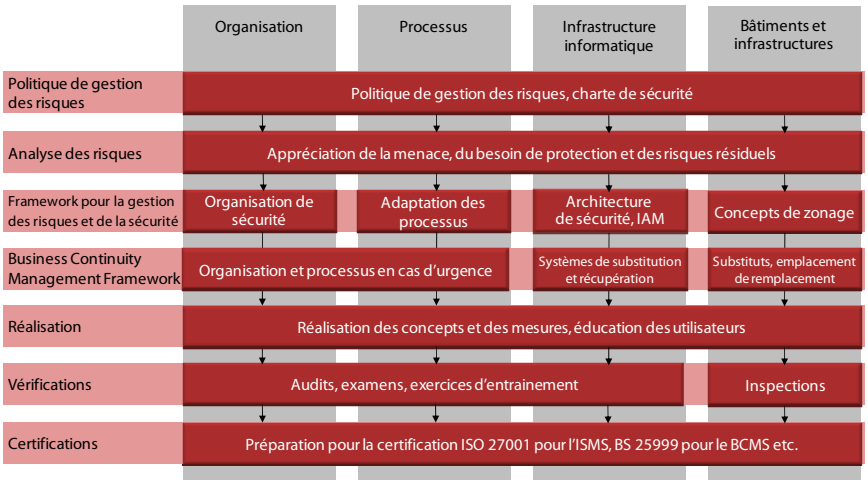
Il y a beaucoup de raisons qui expliquent l'efficacité des cyberattaques:

- Internet est une infrastructure ouverte, en perpétuelle mutation et dépourvue de toute instance de contrôle centralisée.
- L'interconnexion croissante des systèmes accentue la complexité et ne cesse de créer de nouvelles failles de sécurité.
- De nouvelles interfaces relient des systèmes jusqu'ici isolés avec Internet ouvert.
- La course effrénée à l'innovation et la pression concurrentielle font que les logiciels sont souvent mis en service, prématurément, avec des failles de sécurité.
- Les mesures de sécurité prises par les divers acteurs du cyberespace sont rarement concertées.
- Les utilisateurs sont souvent peu conscients de la question de la sécurité.

Pour améliorer la cybersécurité, il faut donc agir à plusieurs niveaux:

- Il faut constamment adapter et faire évoluer les cadres de référence de gestion des risques et de la sécurité, de même que les **normes** de sécurité (p.ex. ISO 27032 «Guidelines for Cybersecurity International Standard»).
- **Les exploitants d'infrastructures critiques** doivent intégrer le thème de la cybersécurité dans leurs réflexions sur les risques. Il est en particulier nécessaire d'instaurer, entre les partenaires du cyberespace, un échange d'informations efficace et réel, une coordination et une politique de traitement des incidents.
- **Les entreprises et les administrations** doivent affronter le risque de la cybercriminalité. Il convient de mettre en place et de mener une politique de gestion des risques et de la sécurité conformément aux bonnes pratiques en vigueur.
- Il ne suffit pas de se focaliser sur des mesures de nature technique pour faire face aux menaces provenant du cyberespace. **Les utilisateurs finaux** doivent être informés des règles de conduite à observer par le biais de formations et de campagnes de sensibilisation.

Le cadre de référence de la gestion de la sécurité chez AWK aide les responsables sécurité des entreprises à identifier les secteurs à risques et à définir les mesures préventives adaptées.



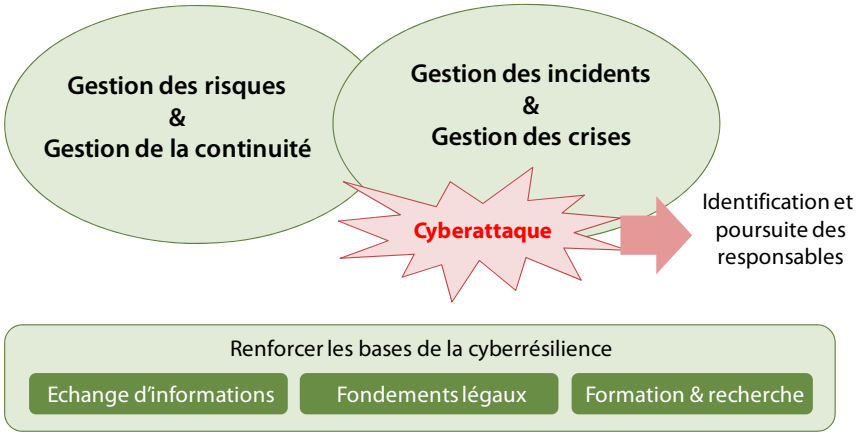
Cadre de référence de la gestion de la sécurité chez AWK

Cybersécurité: un Public Private Partnership au service de l'objectif

Le Conseil fédéral a approuvé le 27 juin 2012 la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) et chargé les départements de prendre en main l'application des mesures, à leur niveau respectif et en collaboration avec les autorités cantonales et les milieux économiques.

A travers la SNPC, le Conseil fédéral poursuit les objectifs stratégiques suivants:

- Déceler suffisamment tôt les menaces et dangers du cyberespace
- Accroître la capacité de résistance des infrastructures importantes dont dépendent la sécurité, la prospérité et la stabilité de la Suisse
- Réduire efficacement les cyberrisques, en particulier la cybercriminalité, le cyberespionnage et le cybersabotage



Eléments clés pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

AWK a soutenu l'unité de pilotage informatique de la Confédération dans l'élaboration du plan de mise en œuvre de la SNPC. Outre un plan d'action et un calendrier d'attribution des responsabilités, il s'agissait de créer chez tous les participants une compréhension commune de leurs rôles et la répartition des tâches en lien avec la gestion des risques, de la continuité, des incidents et des crises. L'intégration de la SNPC dans le contexte de la stratégie nationale de protection des infrastructures critiques (PIC) a été assurée. Conformément au modèle du *Public Private Partnership*, divers acteurs de la Confédération, des cantons et de l'économie privée ont été associés dans une approche transversale, afin qu'ensemble, ils puissent renforcer la capacité de résistance de la Suisse face aux cyberrisques.

La SNPC défend le principe de la responsabilité individuelle: chaque acteur est lui-même responsable d'analyser ses risques et ses vulnérabilités, et de mettre en place une gestion appropriée de la continuité et des crises.

Le 15 mai 2013, le Conseil fédéral a approuvé le plan de mise en œuvre SNPC et chargé le comité de pilotage SNPC de coordonner la concrétisation des mesures. Ce comité de pilotage a également la mission de suivre l'évolution des cyberrisques et de présenter des recommandations au Conseil fédéral sur le développement de la stratégie.

Les efforts internationaux en matière de cybersécurité

Union Européenne: l'UE a publié en février 2013 son dossier tant attendu consacré à la cybersécurité. Il comprend des directives et mesures destinées à «assurer un niveau commun élevé de sécurité des réseaux et de l'information dans l'Union». La stratégie de l'Union Européenne met l'accent sur le renforcement des composants techniques (produits TIC, etc.) pour accroître la sécurité et la cyberrésilience.

Allemagne: la stratégie de cybersécurité de l'Allemagne repose en premier lieu sur des moyens et mesures civiles, qui sont complétés par des mesures de l'armée.

Grande-Bretagne: le gouvernement britannique mobilise un budget de 650 millions de GBP pour établir un nouveau «National Security Cyber-Program». La mise en œuvre relève des services secrets britanniques GSHQ et doit intervenir dans les quatre prochaines années.

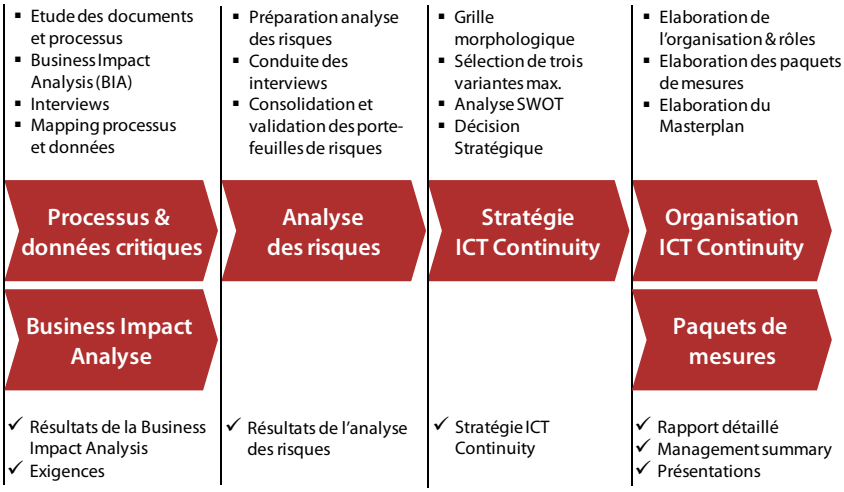
USA: le département américain de la Défense envisage d'augmenter massivement l'effectif du département de la cybersécurité en 2014, qui passera de 900 collaborateurs actuellement à 4900 collaborateurs. En outre, il est prévu de classifier à l'avenir les cyberattaques graves comme actes de guerre.

En situation de crise: l'ICT Continuity garantit le maintien des processus d'affaires stratégiques

Les processus d'affaires essentiels dans l'entreprise sont plus que jamais tributaires de la disponibilité de l'infrastructure TIC. Les attaques ciblant l'infrastructure TIC sont généralement coordonnées par delà les frontières, si bien que les législations nationales ne peuvent les combattre que partiellement.

Les attaques par déni de service (Denial-of-Service - DOS) représentent actuellement l'une des principales menaces qui pèsent sur l'infrastructure TIC d'une entreprise. Un flot de requêtes submerge l'infrastructure TIC jusqu'à ce que celle-ci tombe en panne. Les solutions techniques pour riposter à de telles attaques s'avèrent hélas souvent insuffisantes.

Pour se préparer aux cas les plus critiques, il convient de mener une analyse ICT Continuity. Ce processus permet de déceler et de traiter suffisamment tôt les impacts potentiels des défaillances de l'infrastructure TIC qui représentent une menace pour l'entreprise. Le résultat se présente sous la forme d'un catalogue de mesures qui, en situation de crise, rendent possible la poursuite des processus stratégiques pour l'activité, ou leur reprise dans un délai prédéfini. Cette démarche est de nature à améliorer de façon décisive la stabilité d'une entreprise.



Méthode AWK en matière d'ICT Continuity Management

AWK a déjà épaulé de nombreuses organisations et entreprises en matière d'ICT Continuity Management. L'Association des entreprises électriques suisses (AES) en est un exemple probant: AWK a prêté son concours à l'élaboration d'une recommandation de la branche [4] pour les infrastructures TIC critiques des entreprises de production et distribution d'énergie. L'objectif était de renforcer la capacité de résistance de l'approvisionnement en électricité face à des cyberattaques et de garantir ainsi au mieux, en situation de crise, la sécurité d'approvisionnement pour l'Etat, les infrastructures critiques, l'économie et les particuliers.

Sources:
[1] Des hackers s'en prennent au DFAE, www.computerworld.ch, mai 2012
[2] Disparition de données de patients de la clinique Mittelbaden, www.haufe.de, octobre 2012
[3] Opération Octobre rouge, www.kaspersky.com, janvier 2013
[4] Association des entreprises électriques suisses, Recommandation de la branche pour le marché suisse de l'électricité au sujet de l'ICT Continuity, www.strom.ch, décembre 2011

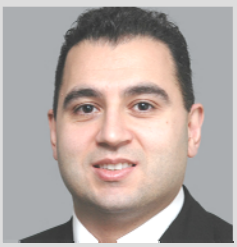
Les auteurs

Adrian Marti
Responsable de secteur, Dr. phil. nat., EMBA, CISM, CRISC

Adrian Marti est responsable du domaine de compétence « sécurité de l'information » chez AWK

Philipp Grabher
Consultant, PhD Computer Security, Dipl.-Ing.

Philipp Grabher est expert en cryptographie et protocoles de sécurité chez AWK



Tarkan Bas
Senior Consultant, Dipl. El.-Ing. ETH, CISM, CISA

Tarkan Bas est expert en Risk Assessments et Security Audits chez AWK

A propos d'AWK Group

Avec 130 collaborateurs, AWK est l'une des principales sociétés de consulting suisses pour les technologies de l'information.

Nous travaillons dans toute la Suisse à partir de nos sites de Zurich, de Berne et de Bâle.

Nos prestations de services comprennent le consulting, l'ingénierie et la gestion de projet.

AWK GROUP
Consulting | Engineering | Project Management