Zeitschrift: Arbido

Herausgeber: Verein Schweizerischer Archivarinnen und Archivare; Bibliothek Information Schweiz

Band: - (2008)

Heft: 4: Informationswissenschaft: die Instrumente der Zukunft = Information documentaire: les outils du futur = Scienze della informazione: gli strumenti di domani

Artikel: La sécurité informatique

Autor: Brügger, Daniel

DOI: https://doi.org/10.5169/seals-769809

La sécurité informatique

Daniel Brügger, ingénieur en informatique, spécialiste de la sécurité IT

Le développement des réseaux, le stockage et le transfert de volumes d'informations de plus en plus importants, l'explosion du nombre d'utilisateurs, voilà qui nécessitent des systèmes (hardware et software) de plus en plus sophistiqués et performants. Mais qu'en est-il de la sécurité informatique? Comment préserver ces quantités phénoménales de données qui forment la richesse d'une entreprise ou d'une institution? Rappel de quelques principes que l'on sera de plus en plus contraint d'appliquer à l'avenir.

La sécurité informatique est un terme galvaudé, servi à toutes les sauces, quasiment un leitmotiv qu'on se lance en société comme: la sécurité, c'est très important! Ce à quoi quelqu'un répondra par: et de plus en plus! A ce moment-là, dans un mouvement solidaire, chacun hochera de la tête d'un air entendu, comme si cela coulait de source et... sans savoir du tout de quoi il retourne vraiment.

La sécurité informatique doit offrir toutes les techniques, mécanismes, architectures ou règles permettant de préserver le système d'information d'une entreprise. C'est aussi simple que ça.

Le système d'information

Encore un terme à la mode. Le système d'information est composé d'une multitude d'informations ainsi que du système lui-même. On pouvait s'en douter. L'information d'une entreprise, ce sont tous les fichiers créés, les courriels, les messages internes, les recherches et les commandes en ligne, les mémos, les fichiers Excel, Word, les schémas, les éléments financiers, les secrets de fabrication, les banques de données, etc. En ce sens, l'information d'une entreprise est son âme, son historique, sa valeur première.

Préserver cette valeur est donc absolument essentiel à la bonne marche de l'entreprise. Ne pas y penser, sous-estimer sa richesse ou remettre à plus tard les tâches de préservation de l'information signifierait mettre potentiellement en péril l'entreprise. En ce sens la responsabilité ultime revient toujours au management, aucune possibilité de se rabattre sur le méchant informaticien. La direction de l'entreprise doit mettre l'infrastructure, les outils et les personnes à disposition de son système d'informations avec pour but premier d'assurer sa défense! Plus loin encore, la direction doit s'assurer de la bonne application des mesures avec l'appui d'auditeurs si nécessaires.

Quels sont les risques?

Ils sont malheureusement innombrables. Tout d'abord, il faut impérativement se souvenir que 80% des attaques ou pertes de données sont réalisées depuis l'intérieur de l'entreprise. Le bandit masqué derrière son ordinateur existe, mais les personnages les plus dangereux vous côtoient à la cafétéria. Ou bien est-ce vous-même? Rassurez-vous, il s'agit très souvent d'erreurs de manipulations, de méconnaissances du système, de tentatives de découvertes ou encore de malveillance. Peu importe la façon, les données perdues peuvent malheureusement l'être de manière irrémédiable.

Si l'utilisateur est le risque majeur, bien d'autres événements peuvent avoir des répercussions catastrophiques. En voici une liste non exhaustive:

- Les personnes: mauvaise formation, faible prise de conscience de la sécurité, désinvolture, perte de donnée, divulgation d'informations confidentielles, non-respect des contrôles d'accès, fraude, vol, tentative d'accès ou d'attaque etc.
- Les équipements: défaillance, destruction de données, mauvaise résilience à la panne, mécanismes de sécurité faibles, etc.
- Les contrôles d'accès: contrôles d'accès peu respectés, pas de contrôle d'accès aux bâtiments, divulgation ou échange de mot de passe.
- Les éléments naturels ou environnementaux: le feu, les inondations, le vandalisme, les pannes d'électricité, etc.
- Les applications: mal structurées, elles entraînent des erreurs, des pertes de données, un ralentissement ou un arrêt de la production, des pannes intempestives.

Les mesures permettant d'écarter ou de réduire ces risques précités ne sont pas purement techniques. Elles doivent être à parts administrative et technique égales. Cela signifie qu'une formation adéquate des personnes, une sensibilisation à l'utilisation et aux mesures de sécurité est déjà un élément de réponse très important.

Ensuite, il existe évidemment une armada d'équipements de sécurité permettant de procéder de manière quasiment systématique. L'exemple de l'antivirus est des plus clairs:

- Dissuader: l'utilisateur signe une charte de l'utilisation de son accès à internet et des équipements informatiques de l'entreprise. En ce sens, accéder à un site pour le moins équivoque ou tenter d'installer un logiciel ne respecterait pas la première barrière dissuasive. Mon patron pourrait le savoir!
- Prévenir: empêcher l'événement! Le poste est équipé d'un antivirus mis à jour et empêche ainsi l'infection.
- Détecter: un virus tente d'infecter le poste, l'antivirus le détecte et l'identifie.

– Réagir: la mesure de protection du poste de travail est lancée, le virus est effacé ou isolé si cela n'est pas possible. Le poste et donc ses données sont préservés.

Les risques du futur?

Si l'exemple du virus a presque un côté amusant, chacun en ayant été un jour ou l'autre victime, les enjeux de la sécurité informatique ont atteint un tel niveau que le rapprochement avec la sécurité d'un pays au sens strict devient évident. A l'heure du terrorisme qui prend d'ores et déjà la forme électronique, les nations doivent prévoir des techniques de défense appropriée. Cela n'a rien d'utopique ou d'alarmiste, l'actualité nous donne raison jour après jour.

Des cas de prise d'otage d'information ont été révélés. Une entreprise ou une institution fait l'objet d'une attaque ciblée. Un dossier ou carrément un disque sensible est crypté et l'on ne peut plus du tout y accéder. Les attaquants contactent ensuite la société et lui proposent la clé permettant de décrypter les données contre une rançon. Simple et efficace. Les cibles sont des organismes financiers ou des sociétés à forte capitalisation sur leur image. Si la rançon n'est pas versée, une divulgation dans les médias de l'attaque est organisée, entraînant immanquablement un très fort déficit d'image pour la société cible.

Plus impressionnant encore fut l'attaque en avril 2007 envers un pays, l'Estonie en l'occurrence. Le pays décide le déplacement d'une statue d'un soldat russe dans un parc en banlieue. Vainqueur des nazis pour les uns, oppresseurs pour les autres, le fait de toucher à un symbole engendre les foudres des hackers russes. En quelques heures, les sites gouvernementaux, banques, médias ou encore services d'urgence subissent une attaque par déni de service. Les sites sont submergés de requête amenant à un arrêt complet de leur service respectif. L'attaque est si impressionnante et déstabilisante pour le pays qu'elle ne peut pas raisonnablement n'être que le fait d'individus isolés. D'aucuns n'y vont pas par quatre chemins, la Russie démontre ici sa force de frappe dans ce qui s'appelle dorénavant le «war game». Pour la petite histoire, un an plus tard c'était au tour de la Lituanie d'être la victime désignée pour des motifs quasiment similaires.

Au sein de l'OTAN, plusieurs pays ont signé ce printemps un accord visant à la création d'un centre de cyberdéfense. Il est reconnu que la criminalité informatique ne tient pas compte des frontières et qu'une collaboration entre pays est indispensable. L'Estonie a demandé la qualification juridique des événements susmentionnés en acte de terrorisme. A noter également que l'Union européenne dispose depuis 2004 de sa propre agence de sécurité informatique, l'ENISA (European Network and Information Security Agency) dont le but est simple et fondamental à la fois, à savoir: «Contribuer à moderniser l'Europe et à assurer le bon fonctionnement de l'économie numérique et de la société de l'information.»

Contact: dab@oxygen-company.com

Références:

– **Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), rapports semestriels**
– **Shon Harris, CISSP All-in-one, 4th edition**
– **Divers sites internet avec recoupement d'informations**
– **http://www.enisa.europa.eu/**

ABSTRACT

Informatiksicherheit

Firmen produzieren viel Information. Diese ist nicht nur leeres Datenmaterial, sondern gleichsam die «Seele» und die Geschichte des Unternehmens. Wer sich über die Wichtigkeit dieses Fundus' im Klaren ist, wird die Sicherheit ganz gross schreiben.

80% der Angriffe auf Daten werden intern verursacht. Das muss nicht willentlich geschehen. Oft sind Unwissen, Fehlmanipulationen oder Unachtsamkeit der Grund für Datenverluste.

Neben dem Personal können auch fehlerhaftes Material, mangelhafte Zugangssicherheit (ins Gebäude, ins System), «natürliche» Katastrophen (z.B. Feuer, Wasser) oder schlecht strukturierte Software für Verluste verantwortlich zeichnen.

Es gibt eine Reihe von technischen und administrativen Vorkehrungen, welche die Informatiksicherheit erhöhen.

Die Vorkehrungen reichen von Antivirenprogrammen über verschiedene präventive Massnahmen bis hin zu Personalschulungen.

Künftig werden Vorkehrungen auf nationaler Ebene an Wichtigkeit gewinnen (Stichworte Terrorismus, Hackerangriffe, «Geiselnahme» von Informatikdaten, die gegen Lösegeld wieder «freigegeben» werden). Wichtig ist in diesem Zusammenhang die internationale Zusammenarbeit. Die NATO («cyber-defense») und auch die EU (ENISA – European Network and Information Security Agency) sind daran, entsprechende Strukturen aufzubauen.