



CASES articles

Le World Wide Web – Quels sont les risques ?

Représentons-nous un risque ?

Pour plus de sécurité, adoptez les réflexes CASES !

Sommes-nous réellement non-vulnérables ?

Virus, vers, chevaux de Troie, espionnage industriel, escroqueries, utilisation abusive de données ou pannes suite à des tempêtes – les menaces sur le réseau Internet semblent être légion. Mais que cela signifie-t-il réellement ? Quel est le véritable sens du terme « risque » dans notre société de communication moderne ? Quelles menaces nous guettent après tout ? Surfer sur l'Internet, avoir un ordinateur rien que pour les enfants ou un petit réseau pour l'entreprise, – est-ce réellement risqué ? Pas grand-chose à craindre, à priori... C'est en tout cas ce que pensent de nombreux utilisateurs. Le facteur humain est pourtant responsable de bon nombre de vulnérabilités et celles-ci permettent aux menaces de se concrétiser et entraînent des préjudices. Les entreprises et les utilisateurs privés préfèrent bien souvent ignorer cet état de fait. Avoir connaissance des dangers est pourtant une condition sine qua non pour espérer réduire les risques.

L'été est généralement propice aux cambriolages et c'est alors l'occasion qui fait le larron. Une clé laissée sous un pot de fleurs, dans la boîte à lettres ou même glissée sous la paillasson est rapidement découverte par les cambrioleurs. Ils connaissent ces petites astuces et, après quelques minutes seulement, peuvent déambuler tranquillement dans votre maison. Les préjudices alors subis comprennent des pertes financières directes. Très vite, il est également nécessaire de procéder à des travaux de remise en ordre ou de réparation ; il faut por-



ter plainte auprès de la police et effectuer les autres démarches administratives tout aussi longues et fastidieuses. En outre, la peur d'un éventuel retour des cambrioleurs persiste bien souvent de longs mois après.

Qu'est-ce qu'un risque ?

L'exemple du cambriolage permet très aisément de définir le risque, et ensuite de le transposer au monde virtuel. Dans un premier temps, il convient de parler de la « menace » : le cambrioleur. Il n'est pas possible d'influencer sur cette menace, c'est une éventualité toujours présente. Ensuite, il y a une « vulnérabilité ». Dans notre exemple, il s'agit de la clé abandonnée. C'est cette vulnérabilité qui permet au cambrioleur d'accéder à la maison rapidement et silencieusement, et à l'insu des voisins. Sans elle, le voleur aurait probablement renoncé au cambriolage : il aurait en effet été forcé de casser une fenêtre

ou de crocheter la serrure, ce qui aurait pu attirer l'attention du voisinage. Les « conséquences » possibles sont également évidentes : le voleur peut emporter des objets de valeur, mais aussi, selon son état d'esprit, faire des dégâts par pur vandalisme.

Dans notre exemple, le risque résulte donc d'une « vulnérabilité », d'une « menace » et a de nombreuses « conséquences ». Ceci permet d'établir une définition générale et de la représenter sous la forme d'une équation : $\text{risque} = \text{vulnérabilité} \times \text{menace} \times \text{conséquences}$. Le propriétaire de la maison parti en vacances aurait pu éviter cette vulnérabilité. Il aurait du confier la clé à son voisin. L'élément correspondant de l'équation aurait tendu vers la valeur « 0 ». Comme une équation multipliée par la valeur « 0 » est égale à « zéro », le risque aurait également été égal à « zéro ». Le propriétaire de la maison peut également influencer partiellement sur l'importance des conséquences.

Un système d'alarme permet par exemple de signaler rapidement la présence de cambrioleurs. Les objets de valeur peuvent être conservés dans un coffre-fort. Ces mesures permettent de limiter les conséquences éventuelles et donc de limiter le risque global. Ce qui est valable pour le monde réel s'applique également au monde virtuel, tant pour les utilisateurs privés que pour les entreprises. La définition du risque est ainsi également transposable à l'Internet.

Menaces

La multitude des utilisateurs de la toile fait du média Internet un endroit lucratif pour les cybercriminels. Il est certain que parmi les 1,2 milliard d'utilisateurs se dissimulent également des individus aux desseins malveillants. Les catastrophes naturelles, pannes d'électricité ou défaillances des réseaux de communications sont également des éléments qui échappent au contrôle de l'utilisateur. La complexité atteinte de nos jours par les technologies, les réseaux et les applications, ainsi que leur interconnexion, est bien souvent responsable de la fragilité des systèmes face aux menaces.

Vulnérabilités

Certains types de vulnérabilités représentent un risque considérable pour les structures informatiques et de communication. Pour les entreprises, ceux-ci peuvent être classés en trois catégories : les vulnérabilités d'ordre organisationnel, technologique et physique. Cette répartition s'applique également à l'utilisateur privé.

Vulnérabilités d'ordre organisationnel

Pour les entreprises, les vulnérabilités d'ordre organisationnel comprennent par exemple l'absence de gestion de la sécurité des ressources informatiques. L'utilisation inadéquate des moyens disponibles, comme les mots de passe par exemple, peut également être citée. Sans incitation à le faire, les utilisateurs sont peu enclins à modifier leur mot de passe régulièrement. Des documents écrits, décrivant les procédures et les règles à appliquer pour certains processus, tels que les sauvegardes par exemple, font également souvent défaut. Si

ce genre de procédure existe, il n'est alors pas rare de constater que les collaborateurs en ignorent tout. Les risques auxquels sont soumis les systèmes ne font que rarement l'objet d'évaluations. Les mesures de sécurité existantes sont alors souvent totalement inadaptées par rapport aux risques réels.

Les utilisateurs privés connaissent également des vulnérabilités d'ordre organisationnel. Anti-virus, pare-feu, patches, sauvegardes, mots de passe, mises à jour incessantes et paramètres – les utilisateurs privés prennent-ils vraiment toutes les mesures de sécurité qui s'imposent ? Combien mettent correctement en œuvre les patches correctifs, un pare-feu ou des mots de passe ? Quand le mot de passe a-t-il été modifié pour la dernière fois ? Ici encore, les mesures de protection sont bien souvent inadaptées par rapport aux risques. Un système anti-virus est-il vraiment suffisant pour protéger les données financières présentes sur un ordinateur portable ? Que se passe-t-il si l'ordinateur est volé ? Ou s'il venait à être infecté par un malware, comme un cheval de Troie par exemple ? Les utilisateurs privés tolèrent de nombreuses vulnérabilités. La comparaison avec la clé cachée sous un pot de fleurs se révèle ici fort à propos.

Vulnérabilités d'ordre technologique

Quiconque ayant pu examiner les codes d'un logiciel en connaît la complexité et sait que des vulnérabilités peuvent apparaître. Les causes peuvent être multiples : manque de temps, structuration insuffisante, absence de considérations relatives à la sécurité. Si l'interaction de plusieurs programmes devient nécessaire, la complexité et la probabilité de voir apparaître des vulnérabilités s'en trouvent multipliées. L'interdépendance de l'alimentation électrique, des réseaux de télécommunications, des appareils et des applications génère des faiblesses supplémentaires. À cela viennent s'ajouter des éléments comme des fournisseurs, des producteurs et des clients, le tout engendrant un ensemble extrêmement complexe, avec de nombreuses vulnérabilités potentielles. Les mises à jour de certains programmes, effectuées à la hâte et sans période de test suffisante en augmentent encore le nombre. En outre, la

complexité des règles d'accès et des filtres rend difficile pour une entreprise de conserver une vision d'ensemble et cela génère encore d'autres vulnérabilités.

Pour les utilisateurs privés, de nouvelles vulnérabilités peuvent par exemple faire leur apparition lors de l'installation de programmes supplémentaires. Les vulnérabilités existantes, plus l'arrivée de ces dernières permettront peut-être à des tiers d'accéder au système d'exploitation de l'utilisateur. Lorsqu'une application ne fonctionne pas, de nombreux utilisateurs ont tendance à désactiver leur pare-feu. La vérification de réglages ou la recherche d'une éventuelle autre source d'erreur est souvent omise, faute de connaissances ou de temps.

Vulnérabilités d'ordre physique

Les entreprises peuvent être durement touchées par la défaillance d'un logiciel, d'un matériel informatique ou d'une banque de données. Une mauvaise climatisation ou une interruption de l'alimentation électrique peuvent être à l'origine de ce genre de panne. Il s'agit de vulnérabilités qui, pour la plupart, pourraient être évitées. Les pannes de composants individuels entraînant la défaillance de systèmes importants sont également à considérer comme des vulnérabilités, tout comme l'absence de contrôles d'accès. Cette absence peut entraîner des manipulations ou des erreurs humaines. Un incendie volontaire ou l'effacement d'une banque de données peuvent causer des dommages considérables. Si les copies de sauvegarde sont stockées dans le centre de calcul même par exemple, un éventuel incendie peut provoquer la perte irrémédiable des données et des applications. La répartition inadéquate des ressources, comme la mémoire de travail par exemple, peut également mener à l'effondrement d'un système. Des conséquences fatales peuvent aussi être provoquées par un câblage confus et non documenté.

Pour les utilisateurs privés, il convient de veiller à ce que les appareils soient protégés de la pluie, du soleil, du froid et de la poussière. Laisser un ordinateur dans une voiture ou dans le jardin peut très bien aboutir au vol. L'accès de tous les membres de la famille à un seul et même ordinateur

constitue également une vulnérabilité importante. Les parents connaissent-ils les pages Internet que consultent leurs enfants ? Ou les jeux qu'ils téléchargent ? Que se passe-t-il lorsque l'ordinateur a été infecté par des malwares à cette occasion ? Cela peut-il avoir des conséquences sur les virements bancaires effectués sur Internet ? L'absence de copies de sauvegarde ou leur stockage inadapté peut également avoir des conséquences graves. Par exemple, Combien de temps faudrait-il pour recréer les documents importants qui se trouvaient dans l'ordinateur ? Que peut représenter la perte de toutes ses photos-souvenirs pour une personne ? Et que se passe-t-il lorsque toutes les analyses, les documents de travail et l'original d'un mémoire sont irrémédiablement perdus deux semaines à peine avant la date prévue pour sa

présentation ? Chaque utilisateur devrait se poser ce genre de question.

La réduction des vulnérabilités contribue de façon décisive à la diminution des risques auxquels sont exposés les utilisateurs des applications et moyens de communication électroniques actuels. Ce sont bien souvent les utilisateurs mêmes qui sont à la base de ces faiblesses et ce sont également eux qui peuvent les neutraliser partiellement ou même complètement.

L'exploitation des vulnérabilités par les cybercriminels peut entraîner des pertes financières substantielles. Ces pertes peuvent par exemple être générées par la destruction ou le vol de données critiques, ou même par la mise hors service d'un système informatique complet. La remise en ques-

tion de la crédibilité de l'entreprise lorsque des données confidentielles sont dévoilées peut également avoir des conséquences préjudiciables. Les utilisateurs privés peuvent d'ailleurs également être durement touchés par la publication de données personnelles. Les enfants relatant les disputes conjugales de leurs parents sur l'Internet sont par exemple assez nombreux de nos jours. Il faut également tenir compte de la perte de temps : lorsqu'il s'agit de la recherche fastidieuse d'une faille de sécurité ou la restauration de données détruites par exemple.

Une liste actuelle reprenant les vingt vulnérabilités technologiques les plus fréquentes peut être consultée sur la page Internet de l'institut de sécurité de l'information SANS: www.sans.org.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu