Études stratégiques

Les principes essentiels de la sécurité à destination des Directeurs des Systèmes d'Information (DSI)

S'engager dans l'innovation en toute confiance

IBM

Chaque jour, de nouveaux flux d'informations circulent au sein des entreprises, pour alimenter des processus d'analyse instantanée et susciter des décisions plus intelligentes. Employés, clients et sous-traitants sont tous en interaction, comme jamais auparavant, grâce à une multitude de technologies. Cependant, la prolifération et la superposition de ces réseaux créent des problématiques considérables. D'où une complexité incroyable et des points d'attaque potentiels quasiment illimités. Les DSI (directeurs des systèmes d'information) sont confrontés à une frustration croissante – et s'interrogent. Une sécurité robuste est-elle encore possible à une époque hyper-connectée ? La réponse est positive, même si la démarche impose des changements fondamentaux en termes de processus et d'attitudes. IBM a mis en œuvre sa propre stratégie interne et défini les dix axes essentiels nécessaires pour assurer une sécurité intelligente au 21ème siècle.

Alors que le soleil se lève sur Londres, une directrice commerciale se réveille, ouvre son smartphone et s'aperçoit qu'une énorme opportunité d'affaire est annoncée en Malaisie. L'information déclenche une cascade de messages. Avant l'heure du petit déjeuner, six membres de l'équipe mondiale se retrouvent en téléconférence, dont un par Skype depuis Lyon. Trois intervenants sont en ligne sur leurs téléphones portables. Au cours de la journée, les emails se multiplient autour de la planète, pour partie au travers du réseau de l'entreprise, et les autres sur Gmail et Yahoo. Le soir même, à Londres, l'affaire est conclue. Et dans les heures qui suivent, certains des participants échangent leurs profils sur LinkedIn.

91 %

des utilisateurs professionnels de smartphones se connectent à la messagerie électronique de l'entreprise, mais seul un sur trois d'entre eux possède un logiciel de sécurité sur son équipement.

Source : Kaspersky Labs
http://usa.kaspersky.com/sites/usa.kaspersky.com/files/Enterprise%20 Mobile%20Survey.pdf

Aujourd'hui, personne n'ignore que les managers peuvent instantanément mobiliser l'intelligence de leurs équipes et d'immenses volumes de données pour prendre des décisions plus pertinentes et plus rapides. Cependant, les capacités extrêmes de ces réseaux interconnectés – en termes de vitesse, d'ouverture, de facilité d'accès et d'omniprésence – s'accompagnent d'innombrables vulnérabilités. En outre, la sécurisation d'un réseau d'entreprise devient infiniment plus complexe avec la prolifération de l'information liée à l'activité de milliers d'équipements et le succès des services web offerts à tous. Selon une étude de Kaspersky Labs, 91 % des utilisateurs professionnels de smartphones se connectent à la messagerie électronique de l'entreprise, mais seul un sur trois d'entre eux possède un logiciel de sécurité sur son équipement. Dans cet environnement, la facilité d'accès bénéficie à chacun de nous – et bien trop souvent aussi aux organisations criminelles.

Les réseaux criminels considèrent aujourd'hui les ordinateurs et les équipements mobiles reliés en réseau comme un actif de premier plan. C'est en infectant ces équipements au moyen de logiciels malveillants extrêmement difficiles à détecter qu'ils développent leurs bases d'opérations. Pour les délinquants, les réseaux d'entreprises regorgent de trésors numériques, notamment les mots de passe, les identifiants d'utilisateurs, les secrets professionnels et les informations personnelles. Ils ciblent également les actifs stratégiques, aussi bien au sein des

ministères que des réseaux de communication. Certains d'entre eux vont jusqu'à stopper les activités des entreprises. Selon une étude Gartner, 20 à 30 % des ordinateurs personnels du public ont été infectés par des agents « botnet » et des logiciels malveillants, et peuvent jouer le rôle d'une infrastructure pour des actions criminelles. Alors que de nombreuses entreprises envisagent l'utilisation des équipements personnels de leurs collaborateurs dans le cadre professionnel, le potentiel d'infection constitue une très sérieuse préoccupation.

20 à 30 %

des ordinateurs personnels grand public abritent des logiciels malveillants et fonctionnent en partie pour des réseaux criminels.

Source : http://www.computerweekly.com/opinion/CW-Security-Think-Tank-How-to-prevent-security-breaches-from-personal-devices-in-the-workplace

Un seul ordinateur infecté peut provoquer des dommages considérables. L'un des exemples les plus spectaculaires à ce jour est Stuxnet, un ver informatique extrêmement sophistiqué conçu pour perturber les logiciels et les équipements industriels. Au cours du printemps 2009, ce logiciel malveillant a commencé à se diffuser au travers des machines, principalement en Iran. Un utilisateur, semble-t-il, l'avait introduit en utilisant une clé USB contaminée. Conçu pour attaquer des machines utilisant un logiciel Siemens, ce ver informatique a provoqué des ravages sur de nombreux systèmes industriels.

Les enseignements pour les responsables de la sécurité au sein des entreprises sont clairs. Si un ver informatique peut s'introduire dans des secteurs d'activité hautement protégés en Iran et ailleurs, il n'aura aucune difficulté à identifier une issue dans les équipements de professionnels, répartis dans le monde entier, utilisant Twitter, Facebook ou Skype et communiquant par SMS. De plus, si un logiciel malveillant peut paralyser un équipement industriel, comment ne pas imaginer qu'il soit possible d'interrompre le fonctionnement d'une chaîne logistique, de modifier la circulation routière et d'endommager des réseau d'alimentation électrique, parmi d'autres catastrophes possibles ? La réponse est simple : c'est possible.

Pour faire face à ces défis de plus en plus pressants, les entreprises se doivent de disposer d'une **nouvelle génération de responsables de la sécurité.** Ces dirigeants doivent être naturellement en phase avec les innombrables menaces technologiques existantes, mais également être conscients des enjeux stratégiques. Quelles sont les informations pouvant être partagées de manière élargie ? Qui doit avoir accès à certains éléments stratégiques, et comment les protéger ? La conjugaison de ces défis techniques et stratégiques conduit à une complexité incroyable. S'il peut être tentant d'y répondre au moyen de solutions tout aussi complexe, les plus visionnaires des dirigeants d'entreprises savent qu'une telle escalade est intenable, inabordable et, au final, stérile.

La seule réponse possible est d'accepter un changement fondamental de la manière dont l'entreprise fonctionne. La première étape consiste à **étendre la sphère d'influence des actions de sécurité au sein de l'entreprise,** en englobant le personnel technique, leurs machines, mais aussi toutes les personnes appartenant à l'organisation, et toutes celles en relation professionnelle avec elle. La solution est simple : chaque personne constituant une faille potentielle représente également une partie de la solution. En résumé, le succès résulte d'une prise de conscience sérieuse et durable, c'est-à-dire d'**une culture intégrant la notion de risque.**

Une culture intégrant la notion de risque exige davantage que la disponibilité d'une technologie de pointe et va bien au-delà de l'application de meilleures pratiques. Il s'agit d'une manière inédite de réfléchir, fondée sur une approche pragmatique au travers de laquelle la sécurité s'appuie sur des décisions et des procédures justifiées, à tous les niveaux de l'entreprise. Il s'agit de remanier l'ensemble des pratiques de traitement de l'information, depuis le comité de direction jusqu'aux stagiaires de passage. Dans une culture intégrant le risque, les procédures de protection des données constituent une seconde nature, tout comme nous bouclons notre ceinture de sécurité ou nous stockons des allumettes en lieu sûr.

Il s'agit d'une manière inédite de réfléchir, fondée sur une approche pragmatique au travers de laquelle la sécurité s'appuie sur des décisions et des procédures justifiées, à tous les niveaux de l'entreprise.

La décision doit être prise sans attendre. La sécurité des entreprises approche rapidement d'un point de non retour. Voyons de quoi il s'agit. Dans les milieux criminels, les professionnels ont supplanté les amateurs. D'où la montée des menaces. Parallèlement, les entreprises ont gagné en productivité et se composent de collaborateurs « autonomes », grâce à la large diffusion de torrents de données numériques indispensables aux activités (opérationnel, marketing, commercial, service client). D'où la multiplication des vulnérabilités. En effet, la quasi-totalité de l'activité d'une entreprise est aujourd'hui gérée au travers du numérique, et une intrusion peut avoir pour conséquence la déstabilisation de l'ensemble de la structure. En d'autres termes : les délinquants sont plus compétents, ont à leur disposition d'innombrables portes numériques pour s'introduire dans l'entreprise, et dans ses trésors cachés.

Face à de tels enjeux, envisager une approche nouvelle de la sécurité peut s'avérer dissuasif, voir même déroutant. Alors que les produits et les services de sécurité ne manquent pas, nos clients nous font souvent part de leur déception concernant le marché, qu'ils perçoivent comme ballotté au rythme des unes des médias, en cherchant du sens à la plus récente crise liée à la sécurité, ou pour répondre aux obligations légales de conformité. La plupart d'entre eux ne savent pas comment aborder le problème ou à qui faire confiance, et décrivent la sécurité et la conformité comme un investissement impossible à mesurer, dont le retour sur investissement est douteux et qui offre l'attractivité d'un dos d'âne sur une autoroute. Cette confusion est souvent source d'indécision, voir de renoncement à l'innovation sous l'effet de la peur.

Sans aucun doute, la protection d'une entreprise est un engagement fort et continuel. En outre, modifier une culture est difficile. Cependant, cette démarche est essentielle. Bénéficier d'une sécurité à toute épreuve est le prix à payer pour maintenir l'activité, sachant que cette démarche est tout à fait à la portée d'une entreprise.

Chez IBM, notre mission est de chercher de manière constante le juste équilibre entre l'indispensable innovation et la nécessité de maîtriser les risques. La réponse complète d'IBM à ces enjeux réside dans la technologie, les processus et l'application de règles. Ce qui se traduit par 10 pratiques essentielles. Dans les mois qui viennent, est prévue la diffusion d'une série de livres blancs abordant ces pratiques de manière plus détaillée. En voici un résumé succinct :

Principes essentiels de la sécurité - Le point de vue d'IBM

1. Construire une culture intégrant la notion de risque

L'idée est élémentaire. N'importe lequel d'entre nous peut infecter l'entreprise, par exemple en cliquant sur une pièce jointe douteuse, ou en oubliant d'installer un correctif de sécurité sur un smartphone. Ce qui veut dire que la mise en œuvre de la sécurité au sein d'une entreprise doit inclure tous les collaborateurs. Construire une culture intégrant la notion de risque implique de préciser les risques et les objectifs et de communiquer à leur sujet. Cependant, le changement le plus important est culturel. Pensez à la réaction immédiate d'horreur que nombre d'entre nous peuvent avoir à la vue d'un adulte discutant sur son téléphone mobile alors que son enfant court dans une rue. Nous devons avoir la même intolérance, dans une entreprise, lorsque nos collègues négligent les questions de sécurité. Il appartient bien entendu aux managers de conduire ce changement de manière déterminée, dans l'ensemble de la hiérarchie, et ce, tout en mettant en place des outils pour suivre la progression de la démarche.

2. Gérer les incidents et y répondre

Supposons que deux incidents de sécurité similaires se produisent, l'un au Brésil, l'autre à Paris. Il est possible qu'il existe un lien entre eux. Mais sans la sécurité intelligente nécessaire pour les relier, il est possible qu'un élément important, susceptible d'indiquer un incident potentiel, passe inaperçu. Il est essentiel d'élaborer une action à l'échelle de l'entreprise pour mettre en œuvre des outils d'analyse intelligente et des capacités de réponse automatique. Grâce à un système automatisé et unifié, une entreprise peut surveiller ses opérations et réagir rapidement.

3. Protéger les espaces de travail

Les cyber-criminels sondent en permanence les faiblesses des systèmes. Un poste de travail, un ordinateur portable ou un smartphone constituent autant d'accès potentiels pour des attaques malveillantes. Les paramètres de ces équipements ne doivent en aucun cas être laissés à la discrétion des personnes et des groupes autonomes. Ils doivent tous être sous le contrôle d'une gestion centralisée en vérifiant leur bonne application. Les flux de données circulant dans l'entreprise doivent être classifiés, en fonction de profils de risque et acheminés exclusivement vers les cercles d'utilisateurs concernés. Sécuriser le personnel de l'entreprise revient à éloigner le chaos pour instaurer la confiance.

4. Sécurité intégrée dès la conception

Imaginez que les constructeurs automobiles fabriquent des voitures sans ceintures de sécurité, ni airbags, mais les ajoutent ensuite, en fonction de craintes ou d'accidents. Nous jugerions la démarche illogique et démesurément coûteuse. De manière analogue, l'une des vulnérabilités majeures des systèmes d'information – par ailleurs sources de gaspillage financier – réside dans la mise en œuvre de services, dans un premier temps, puis l'intégration ultérieure de fonctions de sécurité. La seule solution viable consiste à intégrer la sécurité dès la phase initiale, et de procéder à des tests automatisés et périodiques permettant de vérifier la conformité, D'où découle une réduction des coûts. Si l'intégration d'une fonction de sécurité dans une application représente un surcoût de 40 €, sa mise en place ultérieure peut multiplier ce coût par 100, c'est-à-dire 4 000 €.

5. Maintenir les systèmes en ordre

Il est très fréquent que des utilisateurs continuent à se servir de logiciels obsolètes, car ils les connaissent et les utilisent facilement. Cependant, gérer les mises à jour de ces logiciels disparates est pratiquement impossible. En outre, les éditeurs de logiciels interrompent parfois l'application de correctifs lorsque les programmes sont dépassés. Ce que n'ignorent pas les cyber-criminels. Dans un système sécurisé, les administrateurs peuvent assurer le suivi de chaque programme exécuté, avec la garantie qu'il a été mis à jour et en disposant d'un système complet pour installer des mises à jour et des correctifs dès leur diffusion.

6. Contrôler les accès réseau

Prenons l'exemple de la criminalité urbaine. Les opérations de police seraient bien plus faciles si chaque véhicule circulant dans la ville portait une balise radio unique et ne roulait que sur quelques voies, balisées par des capteurs. Il en est de même pour les données. Les entreprises capables de canaliser des données dûment enregistrées au travers de points d'accès contrôlés pourront plus facilement cibler et isoler des logiciels malveillants.

7. Assurer la sécurité des environnements Cloud

Le Cloud Computing offre des gains potentiels d'efficacité considérables. Ce qui ne va pas sans quelques risques. Lorsqu'une entreprise transfère certains services informatiques vers un environnement de Cloud Computing, elle peut être amenée à en côtoyer d'autres – parmi lesquelles éventuellement des spécialistes des techniques de l'escroquerie. Dans un certain sens, un environnement Cloud pourrait ressembler à un hôtel fréquenté partiellement par des clients porteurs du virus de la peste bubonique. Pour réussir dans un tel environnement, les clients doivent disposer des outils et des procédures nécessaires pour s'isoler des autres et surveiller toute menace éventuelle.

8. Surveiller l'environnement proche

Prenons le cas d'un sous-traitant qui a besoin d'accéder à un système. Comment pouvez-vous vous assurer qu'il dispose des bons mots de passe ? L'indiquer sur un bloc-notes ? L'envoyer dans un message ? Improviser, c'est prendre des risques. La culture de la sécurité doit aller bien au-delà des limites de l'entreprise et établir les bonnes pratiques que doivent appliquer ses sous-traitants et ses fournisseurs. Il s'agit en fait d'un processus similaire à celui du contrôle qualité mis en place il y a quelques décennies. Avec une logique identique : la sécurité, tout comme l'excellence, doit être omniprésente dans l'ensemble de l'écosystème. Les effets dévastateurs de la négligence d'une entreprise peuvent entraîner des bouleversements dans des secteurs entiers de la société.

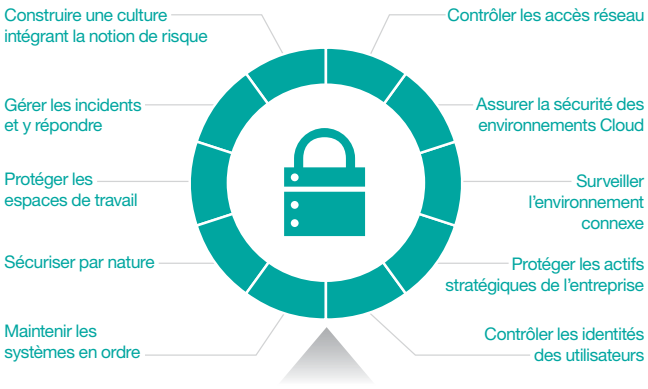
9. Protéger les actifs stratégiques de l'entreprise

Il existe, au sein de l'entreprise, un lieu particulier et précieux, contenant ses actifs les plus critiques, comme par exemple des données techniques et scientifiques, des documents décrivant d'éventuelles opérations de fusion et d'acquisition, ou des informations financières confidentielles relatives aux clients. Une entreprise se doit de procéder à un inventaire en adoptant un traitement particulier pour ses données critiques. Chaque élément jugé comme prioritaire doit être protégé, repéré et crypté comme si la survie de l'entreprise en dépendait. Et c'est parfois le cas.

10. Contrôler les identités des utilisateurs

Supposons que vous embauchiez une intervenante à temps plein. Six mois après, elle bénéficie d'une promotion. L'année suivante, un concurrent surgit et la recrute. Comment le système doit-il traiter cette personne au cours d'une période donnée ? Il doit d'abord lui accorder un accès limité aux données, puis ouvrir davantage de possibilités d'accès, pour finalement les lui retirer. Ce processus consiste à gérer le cycle de vie des identités. Et il est vital. Les entreprises qui négligent cet aspect naviguent dans le brouillard et s'exposent à des intrusions. Pour répondre à ce risque, une entreprise se doit de mettre en œuvre des systèmes méticuleux permettant d'identifier les utilisateurs, de gérer leurs autorisations et de les leur retirer après leur départ.

Comment s'engager dans l'innovation en toute confiance ?



Équilibrer gestion des risques et innovation

Poursuivre le dialogue

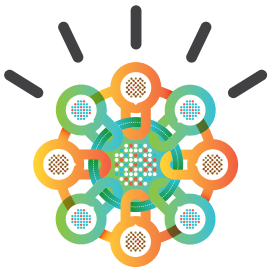
Pour consulter d'autres articles, obtenir des informations supplémentaires ou partager vos points de vue avec d'autres responsables de la sécurité, visitez les sites : **ibm.com/smarter/cai/security et ibm.com/security/fr**.

À propos de l'auteur

Kristin Lovejoy est directrice, chargée du risque informatique, Office of the CIO, IBM. Vous pouvez la contacter à l'adresse : **klovejoy@us.ibm.com**.

À propos de l'IBM Centre for Applied Insights

L'IBM Centre for Applied Insights s'appuie sur les compétences d'experts des contenus et des outils d'analyse pour contribuer à ouvrir la voie de nouvelles sources de création de valeur pour les clients d'IBM. Le Centre réalise des études et crée des ressources et des outils dans une approche pragmatique avec pour objectif de susciter l'action au sein des entreprises.



IBM France
17 Avenue de l'Europe
92275 Bois Colombes Cedex

CIE03116-FRFR-00