Europe : des menaces informatiques croissantes

Paris,
le 17 septembre 2001

Selon une étude réalisée par Evidian, spécialiste en sécurité informatique, les entreprises européennes sont particulièrement vulnérables aux attaques, notamment aux attaques internes: sabotage, escroquerie, espionnage, terrorisme…
La diversité des approches cultures entre pays européens s'avère également un facteur de risque.

Etude de la sécurité informatique auprès de 250 entreprises européennes

EVIDIAN
Secure e-Business Management

Introduction

Aujourd'hui, la sécurité informatique représente bien plus que quelques codes d'accès, du chiffrement de données et des procédures d'audit. L'attaque des plus grands sites de commerce électronique mondiaux, l'apparition quasi mensuelle de nouveaux virus destructeurs et des alertes régulières sur des affaires d'espionnage ont renforcé la perception de la vulnérabilité des systèmes d'information, et accru la demande pour les solutions de sécurité. Dans le monde, les consommateurs eux-mêmes considèrent que les problèmes de sécurité constituent le frein N°1 au développement du commerce et des échanges électroniques.

Les médias ont fait beaucoup pour mettre en avant les dangers du piratage informatique et attirer l'attention des entreprises sur la nécessité vitale de protéger leurs actifs informatiques. Mais, bien que des centaines de milliers de pare-feux et d'anti-virus aient été mis en place, tout cela rend-il les systèmes d'information vraiment plus sûrs ?

L'une des problématiques majeures pour une entreprise planifiant sa politique de sécurité doit être l'identification précise des types de menaces, et des domaines d'où celles ci sont susceptibles de venir.

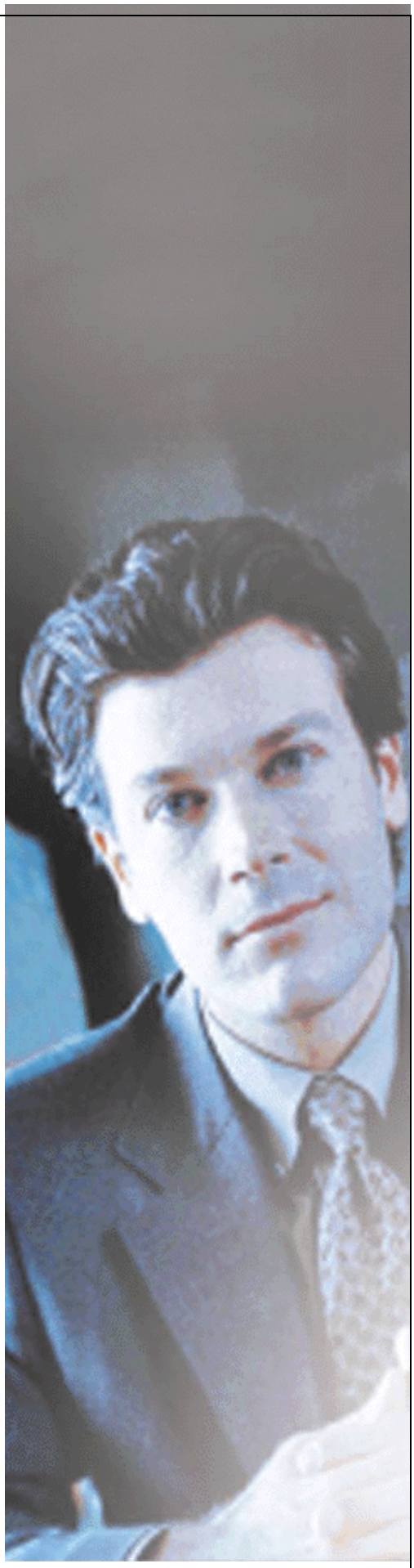
Le caractère spectaculaire et médiatique de nombreuses attaques a focalisé l'attention sur les menaces externes, et a conduit à l'explosion des ventes de solutions dédiées. Cependant, peu d'entreprises ont étudié si les piratages informatiques étaient réellement la source de la plupart des dommages, ou ont pris le temps d'étudier leurs différents marchés géographiques pour regarder si les menaces étaient les mêmes ou différaient nettement.

Spécialiste de la sécurité informatique, Evidian souhaitait évaluer combien la perception des différents types de menaces pouvait varier selon les différents pays européens. Evidian souhaitait également analyser combien le choix et la mise en œuvre de différents types de protection pouvait varier dans les différentes régions, et si le niveau de prise de conscience était le même..

Pour répondre à ces questions, 250 entreprises situées au Benelux, en France, en Italie, en Scandinavie, en Espagne et en Angleterre ont été interrogées. Ces entreprises provenaient de secteurs divers, allant de la finance à la distribution en passant par l'industrie et le secteur public. Les résultats, présentés en conclusion, sont révélateurs :

- Aujourd'hui, la sécurité n'est clairement n'est plus seulement une protection contre les risques mais une condition même de la survie des entreprises, alors même que les systèmes d'information sont vulnérables comme jamais auparavant.
- Trop souvent, les organisations se protègent seulement contre les barbares qui sont aux portes, en oubliant que les plus nombreux sont déjà dans la place.
- Même dans un monde globalisé, la sécurité est affaire de comportements. A ce titre, la prise en compte des différences culturelles entre pays reste essentielle.

Une synthèse de ces points clés est inclue à la fin de ce rapport, ainsi que quelques recommandations sur la façon dont ces points peuvent être utilisés pour aider les sociétés à réviser leur politique de sécurité. Ce que les résultats démontrent néanmoins, globalement, est que, lorsque il s'agit de la sécurité, une approche purement standardisée ne peut répondre à tous les risques.



L'étude et ses résultats

Les résultats de cette recherche ont été divisés en trois sections : les menaces, les solutions déployées et le degré de prise de conscience en matière de sécurité informatique dans chaque pays. Chaque région a été analysée séparément, et les résultats synthétisés pour donner une vue d'ensemble des pratiques de sécurité en Europe.

1.1 Quel est la plus grande menace pour votre entreprise en matière de sécurité ?

1/ D'où proviennent la majorité des infractions à la sécurité dans l'entreprise ?
2/ Quels domaines sont les plus affectés par ces infractions ?
3/ En termes de sécurité informatique, quelles sont les préoccupations majeures?

Résultats

D'un point de vue général, il apparaît clairement que c'est la menace interne qui prédomine. Alors que les médias popularisent généralement les attaques externes de pirates, plus spectaculaires et médiatiques, celles-ci ne représentent néanmoins que le sommet de l'iceberg, et moins de 30% des attaques. Les 70% restantes sont dues à des utilisateurs internes, liées tant à de simples erreurs accidentelles qu'au pur vandalisme ou terrorisme, à la fraude où à l'espionnage.

Au fait des pratiques et failles et de l'entreprise, des données et systèmes les plus sensibles, les utilisateurs internes constituent en outre une population particulièrement experte, dotée d'accès privilégiés aux systèmes d'information, et donc dangereuse. De l'employé frustré souhaitant se venger à bon compte à l'escroc désireux de s'enrichir, à l'espion à la solde d'un concurrent au terroriste infiltré, ils constituent une menace particulièrement sérieuse.

En quelques manipulation sur un système stratégique, un individu malveillant peu mettre à mal les données vitales d'une entreprise ou d'une nation, causer des dégâts considérables et la perte de milliards de dollars.

Cette menace est d'autant plus sérieuse que jamais les entreprises n'ont été aussi vulnérables. Désormais artère vitale du fonctionnement des entreprises, et –au delà – de l'économie mondiale au travers d'Internet et des réseaux de données (bourse, échanges bancaires électroniques…), les systèmes d'information sont un point névralgique, dont la mise à mal est à la fois dangereusement facile et peut avoir des conséquences catastrophiques.

Au vu des dégats catastrophique causés par de simples virus créés par des universitaires (le plus récent : Code Red, 10 milliards de dollars de dégats !), on imagine l'ampleur du désastre que pourrait causer une attaque délibérée par des individus infiltrés d'une organisation militaire – en cas de guerre – ou terroriste.

Cette menace est d'autant plus tangible que jamais l'expertise nécessaire pour mettre à mal un système d' information n'a été aussi répandue, avec des millions d'informaticiens experts et amateurs dans le monde, et des centaines de sites web publics consacrés aux techniques de piratage. Ceci met à la portée de très nombreux individus et organisations les techniques d'attaques informatiques les plus dangereuses.

Au delà de cette perception commune de l'importance des menaces internes, l'étude a néanmoins permis de découvrir quelques disparités frappantes entre les pays.

La Grande Bretagne et l'Allemagne sont les pays le plus sensible aux attaques internes, délibérées et malveillantes.

Les entreprises au Benelux, en France, en Scandinavie et en Espagne estiment pour leur part qu'il y a plus de risques provenant de dégâts accidentels que de sabotages.

Au Benelux et en Espagne notamment, environ 45% des problèmes seraient causés accidentellement par le personnel alors que seulement 25% des dommages sont délibérés.

Le seul pays pour lequel la principale menace est nettement perçue comme externe est l'Italie. 35% des sociétés étudiées y estiment que les attaques externes délibérées sont la principale source de dommages.

L'Allemagne mentionne également une forte proportion d'attaques externes, donnant globalement une faible importance aux dégâts accidentels tant internes qu'externes ! Peut-être un signe de la rigueur germanique, considérant comme négligeables les risques d'erreurs et d'accident…

« D'où proviennent la majorité des infractions à la sécurité? »

	Interne/ Délibéré	Interne/ Accidentel	Externe/ Délibéré	Externe/ Accidentel	Autres
GB	70%	20%	5%	5%	-
Benelux	25%	45%	20%	10%	-
Allemagne	50%	10%	35%	5%	-
Italie	30%	20%	35%	10%	5%
Scandi.	10%	40%	20%	10%	20%
Espagne	25%	45%	25%	5%	-
France	15%	65%	15%	1.5%	1.5%

Concernant le domaine le plus vulnérable aux attaques, la disparité des réponses à travers les pays est plus grande encore, bien que la plupart des acteurs s'accordent sur l'importance des risques liées à l'Internet .

La majorité des sociétés en Italie, Bénélux, Scandinavie et France considèrent que le site web est l'élément le plus vulnérable de leur système d'information.

L'importance accordée à la sécurité internet/extranet est sans doute liée à l'importance stratégique et à la visibilité de ce domaine : site web, serveur e-commerce,… il s'agit du lien entre l'entreprise, ses partenaires, ses clients, le grand public… Subir une attaque au déni de service sur son serveur e-business, voir son site web défiguré ou sa base de numéros de cartes bancaires clients pénétrée est doublement pénalisant : en terme d'impact immédiat, mais aussi en terme d'image. Si elle est rendue publique, cette défaillance peut gravement altérer la confiance des partenaires et clients et – de facto – avoir des conséquences sur l'activité beaucoup plus négative que les dégâts directs liés à l'attaque.

En Allemagne et en Espagne c'est la sécurité de l'intranet qui préoccupe les dirigeants, ce qui renvoie aux dégâts causés par les employés. Enfin en Grande Bretagne, les entreprises se font plus de soucis pour les bases de données.

En moyenne, ce sont globalement les bases de données internes qui sont réputées subir le moins d'attaques, suivi bizarrement par l'extranet, dont les données sont pourtant sensibles (commerce électronique,…). L'extranet étant généralement un service internet sécurisé s'adressant à une population ciblée d'interlocuteurs (partenaires, employés nomades…), le faible risque perçu est sans doute lié à la confiance accordée à ces populations d'utilisateurs privilégiés.

Globalement, les résultats montrent que tous les domaines de l'entreprise – site web/e-commerce, extranet, intranet, bases de données internes…- sont l'objet d'une menace ou d'une autre. Ainsi les politiques de sécurité à mettre en place doivent nécessairement offrir une protection globale.

Veuillez dresser, puis classer par ordre croissant (1 étant le plus important) la liste des domaines subissant des attaques ou des dommages…

	Site web	Intranet	Extranet	Base de donnée
GB	3	2	4	1
Benelux	1	2	-	2
Allemagne	3	1	4	2
Italie	1	3	3	4
Scandinavie	1	-	2	2
Espagne	2	1	3	4
France	1	4	3	2

Par ailleurs, les 25O entreprises ont été interrogées sur le type de violation à la sécurité qu'elles redoutaient le plus.

Sans grande surprise, les virus sont considérés comme les plus dangereux par les entreprises du Benelux, d'Allemagne, d'Espagne et de France. Les intrusions externes sont généralement classées comme la seconde menace.

Il est intéressant de noter que dans les pays ayant un fort taux d'utilisation d'Internet, comme l'Allemagne et la Scandinavie, les intrusions externes sont nettement perçues comme très dangereuses.

Chose intéressante, les entreprises anglaises sont beaucoup moins préoccupées par les virus que par les sabotages, qui représentent pour elles la plus grande menace.

Une statistique également intéressante est le grand nombre d'entreprises italiennes préoccupées par les impacts de la fraude financière. Ce type de crime est nettement perçu comme soit très répandu soit créant l'impact le plus dévastateur en Italie.

Globalement, la menace la plus faiblement perçue est celle provenant des employés, ce qui vient en contradiction avec les chiffres des attaques, majoritairement internes. Une fois de plus, on constate une focalisation de l'attention sur les menaces externes, qui ne sont ni les plus nombreuses, ni les plus dangereuses.

Cette situation est inquiétante, car elle illustre une relative impréparation des entreprises à lutter contre les menaces internes, pourtant les plus potentiellement menaçantes.

Veuillez dresser la liste des types de dangers qui vous préoccupent le plus, dans l'ordre croissant (1 étant la plus grande priorité)

	Virus	Sabotage	Accès des employés	Accès externe	Fraude financière
GB	5	1	4	3	2
Benelux	1	2	4	5	3
Allemagne	1		3	2	
Italie	4	5	2	2	1
Scandi.	2	5	4	1	3
Espagne	1	5	3	2	4
France	1	3	2	2	4

1.2 Quels solutions de sécurité utilisez-vous ?

Chaque pays perçoit différemment les menaces liées à la sécurité. Ces différences se répercutent-elles dans les méthodes et technologies utilisées pour les combattre ?

1/Quelle solutions de sécurité utilisez vous en ce moment ?
2/Combien dépensez-vous par an pour réparer les dégâts causés par les atteintes à la sécurité ?

Résultats

On s'attendrait à ce que le type de sécurité déployé par les entreprises réponde aux problèmes qui les préoccupent le plus. Étonnement, les résultats de cette partie de l 'étude révèlent que la corrélation entre ces deux éléments est faible !

Comme on pouvait s'y attendre, avec une crainte généralisée des virus, les pare-feux, associés à des anti-virus, sont de loin les produits les plus utilisés. Cependant, il ne semble pas que les entreprises se sentent vraiment concernées en ce qui concerne la protection de leur système contre les violations internes.

La meilleure façon de protéger les systèmes d'information internes est de systématiser les mesures de contrôle d'accès, utilisant une authentification des utilisateurs par login/mot de passe, carte à puce ou certificat électronique, et la limitation des droits d'accès aux domaines accrédités. Si ces techniques sont largement utilisées en France, Grande Bretagne et Scandinavie, la sécurité d'accès interne aux applications semble être une préoccupation moins partagée dans les autres pays.

La technologie la moins diffusée est celle des certificats électroniques (PKI), ce qui est normal compte tenu de la relative jeunesse de cette technologie.

Ici aussi, la prédominance est données aux mesures de protections dites de « périmètre » (pare-feu,…), c'est à dire protégeant l'entreprise contre l'extérieur, au détriment des mesures de contrôle généralisée, pourtant essentielles pour la protection interne.

Listez les différents outils de sécurité utilisés, dans l'ordre croissant

	Firewall /anti virus	Mot de passe/ Log-in	Chiffrement (sauf PKI)	PKI	Clé/Cart e à puce
GB	1	1	-	-	-
Benelux	1	2	4	5	3
Allemagne	2	3	1	5	4
Italie	1	2	4	5	3
Scandinavie	1	1	-	3	4
Espagne	1	2	4	3	5
France	1	1	3	4	5

En ce qui concerne le montant des dépenses annuelles consacrées à la réparations des infraction à la sécurité, il semblerait que ce soit les entreprises françaises qui déboursent le plus (ou qui clament le faire !) en Europe. En moyenne, le montant de ces dépensent s'élèverait à 500 000$ par an contre une moyenne allant de 50000$ à 250000$ dans le reste des pays d'Europe.

Une question sur le nombre d'atteintes à la sécurité relevées dans chaque entreprise a aussi été incluse dans le questionnaire. Le chiffre le plus élevé semble se trouver dans les entreprise anglaises et allemandes qui reportent un nombre de 50 à 100 violations par an. Cependant, selon les experts en sécurité d 'Evidian, ce chiffre serait en réalité à multiplier par 5.

En effet, les entreprises rechignent généralement à communiquer sur les attaques dont elles font l'objet, de peur d'ajouter aux conséquences directes de ces attaques des conséquences néfastes sur leur image et sur la confiance que leur accorde leurs partenaires et clients.

En outre, de nombreuses attaques ne sont pas détectées. Sans systèmes de protection et de détection d'intrusions, de nombreuses entreprises ne peuvent même pas repérer l'ensemble des attaques dont elles sont l'objet, si celles ci n'ont pas de conséquence immédiatement et nettement perceptibles.

Ainsi, des défauts de qualité de service des systèmes d'information (transactions erratiques, données altérées…) pourront souvent passer pour de simples défaillances de systèmes et logiciels, alors qu'ils peuvent aussi être causés par des attaques. De plus, si ils sont souvent difficilement detectables, fraude et espionnage peuvent causer des dégâts considérables.

Une étude ICSA récente montre ainsi que les entreprises mettant en place une politique de sécurité dénombrent plus d'attaques. La raison en est simple : les entreprises qui ne mettent pas en œuvre de politique de sécurité renforcée ne sont pas moins frappée, dans une proportion sans doute bien plus importante, mais elles ne le détectent pas !

Cette situation crée une situation paradoxale. Sans protection réelle, l'entreprise ne peut pas quantifier les attaques dont elle est l'objet et – se croyant indemne – attend de voir venir. La sanction économique, à terme, peut être désastreuse…

Quel est le montant moyen annuel dépensé par les grandes et moyennes entreprises pour sécuriser leurs systèmes d'information

	>$50000	$50000-$99999	$100000-$249999	$250000-$499999	>$500000
GB		✓			
Benelux		✓			
Allemagne			✓		
Italie		✓			
Scandi.		✓			
Espagne	-	-	-	-	-
France					✓

1.3 Prise de conscience

Evidian souhaitait enfin évaluer le niveau général de prise de conscience sur la sécurité, dans les entreprises européennes.

1/ Quel est votre budget annuel pour la sécurité informatique?
2/Quels secteurs dépensent le plus pour la protection de leur système informatique ?
3/Pensez-vous que des crainte relatives à la sécurité retiennent certains utilisateurs d'utiliser les services en ligne ?
4/ En termes d'importance, à quel rang classez-vous la sécurité informatique de votre entreprise ?

Résultats

Tout comme elles sous-estiment souvent le nombre d'attaques auxquelles elles sont confrontées chaque année, les entreprises ont parfois aussi tendance à surestimer le montant dépensé dans la sécurité.
Néanmoins, aucune des entreprises interrogées n'a dépensé plus de 3 millions de $ annuel, même si quelques budget informatiques dépassaient les 30 millions de $. La plupart des entreprises en Grande Bretagne, au Benelux, en Espagne et en France dépensent moins de 1 million de $ par an.

En Italie, Scandinavie et Allemagne, ces dépenses sont légèrement en hausse (en moyenne entre de 1$ à 3 millions).

Sans grande surprise, c'est le secteur de la finance (banque/assurance) qui dépense le plus dans la sécurité. En moyenne, les entreprises de ce secteur dépensent 15% de plus que leurs rivaux les plus proches dans les pays étudiés, excepté pour la France. Les secteurs de l'industrie disposent également de budgets sécurité conséquents en Grande Bretagne, en Allemagne et en Espagne.

Malgré des dépenses de sécurité relativement peu élevées, plus de 85% des entreprises interrogées ont admises que la sécurité était d'une grande ou même très grande importance.

Enfin, il a été demandé aux entreprises si elles pensaient que la crainte d'un certain manque de sécurité retient les utilisateurs de se servir des services en ligne.
Plus de 90% des entreprises interrogées ont convenu que c'etait bien le cas.

Profils d'entreprise

Comment une grande ou moyenne entreprise gère-t'elle la sécurité dans chacun des pays où l'étude a été réalisée ?
L'étude a permis d'établir des profils types :

? ? ? ?

GB

- Dépense de moins de 1 million de $ par an dans la sécurité

Dépense entre 100000$ et 249999$ par an dans la réparation des dégâts causés

- 70% des dégâts sont causés par des attaques délibérées.
- La base de données est l'élément le plus sujet à ces attaques
- La plus grande préoccupation est le sabotage
- Protections favorite : pare-feu et login/mot de passe.
- Pour la direction, la sécurité est très importante

Benelux

- Dépense de moins de 1 million de $ par an dans la sécurité
- Dépense entre 50000$ et 99999$ par an dans la réparation des dégâts causés
- 45% des dégâts proviennent d'accidents causés par des employés
- Les sites web sont les plus sujet à ces attaques
- La plus grande préoccupation est les virus
- Protections favorite : pare-feu et login/mot de passe.
- Pour la direction, la sécurité a une importance moyenne

Allemagne

- Dépense entre $1 et 3 millions de $ par an dans la sécurité
- Dépense entre 100000$ et 249999 millions de $ dans la réparation des dégats causés
- 50% des dégats sont causés par des attaques délibérées.
- L'intranet est le plus sujet à ces attaques
- La plus grande préoccupation est les virus
- Protection favorite : pare-feu et chiffrement
- Pour la direction la sécurité a une très grande importance

Espagne

- Dépense moins de $1 million par an dans la sécurité
  - Les dépenses varient d'années en années
  - 45% des dégâts proviennent des accidents internes
  - L'intranet est le plus sujet aux attaques
  - Les virus sont le souci numéro un
- Protections favorite : pare-feu / anti virus
  - Selon la direction, la sécurité est très importante

Italie

- Dépense entre 1$ et 3 millions de $ par an dans la sécurité
- Dépense entre 50000$ et 99999 millions de $ dans la réparation des dégats causés
- La plus grande préoccupation est la fraude financière
- Protections favorite : pare-feu
- Pour la direction la sécurité a une grande importance

France

- Dépense moins de $1 million par an dans la sécurité
- Dépense plus de à $500,000 par an en réparation
- 65% des dégâts proviennent des accidents internes
- Le site web est le plus exposé aux attaques
- Les virus sont le souci numéro un
- Protections favorite : pare-feu et login/mot de passe.
- Selon la direction, la sécurité est très importante

Scandinavie

- Dépense de $1 à 3 million par an dans la sécurité
- Dépense entre $50,000 et $99,999 par an pour la réparation des dégâts causés
- 40% des dégâts proviennent des accidents internes
- La base des données est la plus exposée aux attaques
- L'accès non autorisé par un employé est le souci numéro un.
- Protections favorite : pare-feu / anti virus
- Pour la direction, la sécurité est très important

Conclusion

L'étude démontre une prise de conscience croissante, mais encore insuffisante dans le domaine de la sécurité. Elle met aussi en avant le fait qu'il existe une confusion certaine quant à la meilleure façon de lutter contre les attaques. Enfin, elle souligne la variété des menaces liées à la sécurité et des différents moyens de les combattre.

1- **Aujourd'hui, la sécurité n'est plus seulement une protection contre les risques mais la condition même de la survie des entreprises, et de l'accès au marché.** Quelques semaines de transactions boursières aberrantes d'un seul employé ont pu précipiter il y a quelques années une entreprise aussi importante que la banque Barings à la faillite. Une attaque délibérée de systèmes d'information vitaux pourraient avoir des conséquences toutes aussi catastrophiques. Sur une entreprise, comme sur un groupement économique ou une nation, dont les artères économiques vitales (système boursier et bancaire…) pourraient être durement frappés. En outre, il en va de l'efficacité opérationnelle des entreprises, mais aussi de leur capacité à créer la confiance chez leurs clients et partenaires. A ce titre, la sécurité devient aujourd'hui bien plus qu'une protection ou une assurance contre les attaques : c'est la condition sine-quoi-none pour pouvoir s'insérer durablement dans l'économie en réseau de demain. Cependant, si la securité est perçue comme une nécessité stratégique pour les entreprises et leurs dirigeants, les budgets sont encore souvent limités. Selon les estimations d'IDC, plus de 79% des moyennes et grandes entreprises consacrent moins de 10% de leur budget informatique à la sécurité. Alors que les menacent croissent rapidement, il importent que les mesures de protections soient à la hauteur des enjeux.

2- **Trop souvent, on se protège seulement contre les barbares qui sont aux portes, en oubliant que les plus nombreux sont déjà dans la place.** Si les risques liés aux technologies internet sont uniformément perçus (virus, attaques de pirates…), il s'avère néanmoins que seulement peu entreprises développent une politique complète pour lutter contre les attaques les plus dangereuses, les attaques internes. Or, s'ils offrent un haut niveau de protection contre les attaques provenant des sources externes, pare-feux web et anti-virus ne sont pas efficaces contre les attaques internes soit délibérées soit accidentelles. La solution est pourtant relativement simple : compartimentation des différents services de l'entreprise par pare-feux internes, et surtout accentuation des politiques de gestion de contrôle d'accès interne (authentification, contrôle d'accès et gestion des accréditations individuelles). Dans un monde en réseau, la sécurité, aujourd'hui, ne doit plus seulement être réfléchie en seule matière de périmètre interne/externe. Elle doit être universelle.

3- **Même dans un monde globalisé, la sécurité est affaire de culture et de comportements. A ce titre, la prise en compte des différences culturelles entre pays reste un paramètre important.** Il apparaît nettement que les menacent diffèrent en nature et en intensité selon les pays et les cultures. Une entreprise cherchant à établir une politique de sécurité efficace a besoin de consulter chacun de ses bureaux locaux et d'être sure que ces politiques couvrent toutes les éventualités. Les italiens sont plus préoccupés par la fraude. En Grande-Bretagne, ce sont les sabotages dus à des employés ou des ex-employés qui sont redoutés, alors que dans les pays scandinaves ce sont les erreurs involontaires. Ainsi, l'étude démontre une fois de plus qu'il est essentiel de « penser globalement et agir localement ». Une politique de sécurité globale ne peut fonctionner que si elle est définie au départ internationalement, c'est à dire adaptable dans tous les pays. Et non pas si elle est une politique de sécurité américaine, française, allemande, britanique ou italienne, appliquée uniformément.

Avant tout, mettre en place une réelle sécurité est une affaire de comportements et d'organisations. Les solutions techniques ne sont qu'un moyen. C'est leur utilisation effective et leur mise en oeuvre qui importent. Que sert il de protéger étroitement le serveur internet ou les bases de données clients des attaques externes si un seul employé malveillant, parmi des milliers d'autres, a libre accès pour les détruire ? Pourquoi gérer étroitement les accréditations de chacun si on laisse les utilisateurs afficher le mémo de tous leurs mots de passe bien en vue sur leur bureau ? Comment pouvoir développer en toute quiêtude ses activités d'e-commerce alors que de nombreuses données sensibles sont placées sur des serveurs en libre accès ? Peut-on se permettre d'oublier de désactiver les droits d'employés démissionnaires ou licenciés aux bases de données sensibles de l'entreprise jusqu'à plus d'un an après leur départ, alors même qu'ils ont intégrés des sociétés concurrentes, comme cela arrive quotidiennement dans des milliers d'entreprises ?

Même si une politique est dirigée par le siège central, elle a besoin d'être assez flexible pour prendre en compte les dangers de tous types et de toute provenance. Et surtout, elle a besoin d'être respectée et appliquée partout, prenant en compte les sensibilités de chacun.

Comme Internet l'a amplement démontré, nous vivons dans un monde largement interconnecté !

A propos d'Evidian

Evidian est le principal éditeur européen de logiciels d'administration sécurisée pour les entreprises et les telecommunications (authentification unique et contrôle d'accès, gestion des utilisateurs et des PKI, pare-feu…).

Choisi parmi les plus grandes entreprises européennes, Evidian a reçu en 2000 et de nouveau en 2001 les trophées mondiaux des meilleurs logiciel de contrôle d'accès et de gestion des politiques de sécurité, décernés par « Secure Computing Magazine », première revue internationale consacrée à la sécurité informatique. Implantée en France, Evidian est présente à travers l'Europe et les Etats Unis.

Pour de plus amples informations sur Evidian et ses produits, visitez le site Web www.evidian.com ou adressez un courrier électronique à info@evidian.com .