Economies souterraines

Le capital intellectuel et les données d'entreprise sensibles
se monnaient désormais à prix d'or

Economies souterraines

Le capital intellectuel et les données d'entreprise sensibles se monnaient désormais à prix d'or

Sommaire

Avant-propos de Simon Hunt, VP et Directeur des Technologies, Endpoint Security, McAfee

La mondialisation et la banalisation des technologies de l'information ont conduit les entreprises à stocker des volumes croissants de données d'entreprise précieuses dans le nuage Internet. Cette évolution a motivé les cybercriminels à élaborer de nouveaux stratagèmes pour s'emparer de ces données très convoitées, tant de l'intérieur que de l'extérieur de l'entreprise.

Par le passé, les cybercriminels se concentraient sur les informations personnelles, notamment les numéros de carte de crédit et de sécurité sociale qu'ils revendaient ensuite au marché noir. Aujourd'hui, ces criminels ont compris que la vente des informations propriétaires d'une société à ses concurrents et aux gouvernements étrangers rapporte beaucoup plus. Par exemple, les documents juridiques d'une entreprise se monnaient beaucoup plus cher qu'une liste de cartes de crédit clients.

La cyberéconomie souterraine a évolué et concentre désormais ses efforts sur le vol du capital intellectuel de l'entreprise, sa nouvelle source de revenu. Le capital intellectuel se définit comme la valeur qu'une société génère grâce à sa propriété intellectuelle, notamment les secrets commerciaux, les plans marketing, les résultats de la recherche et du développement, et même le code source. Ainsi, l'opération Aurora lancée contre Google et au moins trente autres sociétés était une attaque sophistiquée conçue pour s'emparer du capital intellectuel desdites sociétés visées.

Plus récemment, une nouvelle attaque, appelée Night Dragon, s'en est prise aux compagnies pétrolières et gazières du monde entier. Pendant plusieurs mois, cette attaque a extrait de façon silencieuse et insidieuse des gigaoctets d'informations internes sensibles, notamment des informations propriétaires sur les champs pétrolifères, le financement des projets et les appels d'offres. Bien que ces attaques aient visé plus particulièrement le secteur de l'énergie, les techniques et les outils employés peuvent être tout aussi efficaces à l'encontre de n'importe quel autre secteur.

Plus que jamais, les solutions de protection des données revêtent une importance capitale pour protéger les entreprises contre les menaces internes et externes qui les guettent. WikiLeaks, par exemple, pose un nouveau risque aux entreprises dans la mesure où le personnel sera de plus en plus tenté de révéler les secrets de leur entreprise pour des raisons technologiques ou financières, pour améliorer la transparence ou simplement pour exposer ce qu'ils considèrent comme des actes répréhensibles. L'affaire WikiLeaks, largement relayée par les médias, a incité les sociétés à réexaminer sérieusement leur infrastructure afin d'identifier les ressources qui doivent rester confidentielles, celles qui relèvent du domaine public et celles qui doivent être protégées. Il devient de plus en plus difficile de contrôler les vecteurs d'intrusion en raison de la perméabilité croissante du périmètre due à l'extension des opérations sur les terminaux mobiles, dans le nuage Internet et chez des fournisseurs tiers. Une fois le réseau compromis, les cybercriminels excellent à extraire et à monétiser les données sur lesquelles ils ont mis la main.

Alors que les entreprises tentent de prévenir ces vols de capital intellectuel à grand renfort d'investissements en sécurité informatique, les attaques gagnent elles aussi en sophistication. Pour contrer ces menaces, les entreprises doivent non seulement implémenter des solutions et des technologies avancées mais aussi mettre en place de nouvelles stratégies et des formations. Et si les stratégies de sécurisation sont importantes, elles ne peuvent malheureusement pas résoudre, à elles seules, le problème.

Ce rapport évalue l'état de sécurité global des entreprises, lesquelles sont visiblement mal préparées pour se protéger des attaques sophistiquées lancées par l'économie souterraine. Il tente également de déterminer si les entreprises ont adapté leurs stratégies et approches en conséquence. Enfin, en guise de conclusion, le rapport présente différentes approches permettant de protéger le capital intellectuel pour limiter les pertes et profiter pleinement de la reprise économique à venir.

Introduction

Voici deux ans, McAfee publiait le rapport « Economies non sécurisées », la première étude mondiale sur la sécurité des économies de l'information. Cette étude menée à l'échelle internationale révélait que les sociétés du monde entier avaient perdu près de mille milliards de dollars en 2008 à cause des fuites de données, du coût des mesures correctives et du préjudice porté à leur réputation. Aujourd'hui, alors que l'économie mondiale montre des signes de relance, les entreprises portent un regain d'attention à leur capital intellectuel et tentent de quantifier les pertes imputables aux fuites de données et aux cyberattaques. Le capital intellectuel se définit comme la valeur qu'une société génère grâce à sa propriété intellectuelle, notamment les secrets commerciaux, les plans marketing, les résultats de la recherche et du développement et même le code source.

Internet a fait disparaître les frontières géographiques et la valeur des sociétés réside essentiellement dans leurs informations intangibles stockées de façon dématérialisée. Toujours en quête de nouvelles informations à voler, les cybercriminels cherchent à exploiter les failles et les problèmes, notamment le stockage à l'étranger, qui ont contribué à l'augmentation des vols de capital intellectuel et compliqué considérablement les poursuites judiciaires. Il arrive souvent que les sociétés ne se rendent même pas compte du vol de leurs informations tant les techniques utilisées sont sophistiquées.

Bien que la situation géographique et la culture puissent jouer un rôle, notamment dans les pays où la frontière entre le monde des entreprises et les pouvoirs publics est floue, c'est la valeur des données qui détermine la société et le type d'informations pris pour cibles. Les visées et les motivations sont presque toujours financières.

La plupart des questions posées en 2011 sont similaires à celles soulevées deux ans plus tôt, mais le contexte économique est différent en cela qu'il est à la reprise et non plus dans une logique de récession. De quelle façon une reprise économique affecte-t-elle la capacité des entreprises à protéger leurs informations vitales ? Quels pays représentent la plus grande menace pour la stabilité économique des autres Etats ? Comment les cybercriminels vont-ils lancer des attaques d'envergure planétaire contre les entreprises ? De quelle façon la protection des actifs numériques peut-elle favoriser ou freiner la reprise économique mondiale dans l'année à venir ?

En collaboration avec des experts de la protection des données et de la propriété intellectuelle, McAfee et la SAIC (Science Applications International Corporation), une société FORTUNE 500® spécialisée dans les applications scientifiques, technologiques et d'ingénierie, ont tenté de répondre à toutes ces questions.

Après avoir interrogé plus de 1 000 décideurs informatiques aux Etats-Unis, au Royaume-Uni, au Japon, en Chine, en Inde, au Brésil et au Moyen-Orient, McAfee et la société SAIC ont mis au point une étude. Menée à bien par le bureau d'études international Vanson Bourne, celle-ci révèle les changements intervenus dans les attitudes et la perception de la protection de la propriété intellectuelle au cours de deux dernières années.

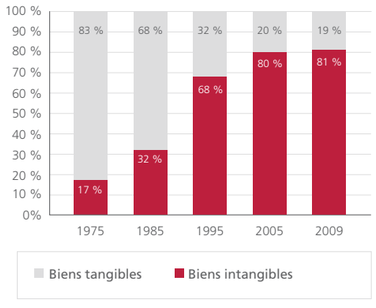
« Tout ce qui peut être monétisé peut devenir une cible de l'économie souterraine, qu'il s'agisse d'informations d'identification bancaires des clients ou des copies des bases de données des sociétés Fortune 100. »

Marcel van den Berg, Team Cymru

Section 1 : La valeur du capital intellectuel dans une économie en mutation

L'économie a connu un grand bouleversement au cours des vingt dernières années, dans la mesure où le capital intellectuel a remplacé les biens physiques comme principale représentation de la valeur d'une entreprise. Une analyse récente de la société Ocean Tomo Intellectual Capital Equity estime la valeur des biens intangibles à environ 81 % de la valeur des sociétés cotées au S&P 500, l'essentiel de cette valeur étant représenté par des technologies brevetées, des données propriétaires, des processus métier et des plans de mise sur le marché.

Composants de la valeur du marché S&P



SOURCE : OCEAN TOMO

Il est parfois difficile de quantifier la valeur du capital intellectuel car il est rarement évalué et il est souvent le fruit d'années d'investissements directs et indirects. En outre, la demande de l'économie souterraine lui attribue un prix qui ne reflète pas toujours correctement la valeur qu'il représente pour la société à laquelle il appartient. Ainsi, la formule du Coca-Cola ne vaut sans doute pas autant aujourd'hui pour un concurrent que le plan marketing de la société concernant sa nouvelle gamme de produits. Que représentent quelques millions de dollars par rapport aux milliards qu'une société concurrente peut économiser en recherche et développement grâce au vol des données propriétaires de Coca-Cola ? Marcel van den Berg, de la société Team Cymru, résume la menace ainsi : « Tout ce qui peut être monétisé peut devenir une cible de l'économie souterraine, qu'il s'agisse d'informations d'identification bancaires des clients ou des copies des bases de données des sociétés Fortune 100. »

Il arrive parfois que les gouvernements encouragent le vol des secrets commerciaux et, dans certains pays, les frontières entre le monde des entreprises et les pouvoirs publics sont floues. Si les coûts en recherche et développement sont minimes ou inexistants, les sociétés peuvent mettre plus rapidement des produits sur le marché et réaliser des bénéfices considérables grâce aux investissements consentis par d'autres entreprises. Le vol du capital intellectuel capital peut faire mourir une entreprise à petit feu et toutes les entreprises à travers le monde devraient s'en inquiéter.

En 2009, Walter Opfermann, un officiel allemand du service du contre-espionnage du Land du Baden-Württemberg, expert dans la protection des données, a déclaré que la Chine avait recours, pour s'emparer des secrets commerciaux, à un large éventail de méthodes « raffinées » —des espions traditionnels jusqu'aux écoutes téléphoniques et, de plus en plus souvent, à Internet[1]. Les secteurs les plus exposés aux attaques sont l'industrie automobile, les énergies renouvelables, la chimie, les communications, l'optique, la technologie des rayons X, les machines, les recherches sur les matériaux et l'armement. Les cybercriminels s'intéressent aux données de recherche et développement, aux techniques de gestion et aux stratégies de marketing.

Le vol du capital intellectuel capital peut faire mourir une entreprise à petit feu et toutes les entreprises à travers le monde devraient s'en inquiéter.

En Italie, en septembre 2010, un ancien ingénieur de Ferrari, Nigel Stepney, a été condamné à 20 mois de prison pour sa participation à des fuites de données d'entreprise confidentielles en 2007. Stepney a été déclaré coupable de sabotage, d'espionnage, de fraude sportive et de tentative de blessure grave pour avoir transmis certaines données techniques de Ferrari à l'écurie concurrente McLaren[2].

Le capital intellectuel est de plus en plus vulnérable en raison de la convergence entre l'informatique et les activités d'entreprise. Les secrets commerciaux et les données propriétaires résident dans des bases de données et sont partagés par e-mail et via Internet. Le choix des cibles de l'économie souterraine a considérablement évolué ces dernières années. Si l'achat et la vente de cartes de crédit volées restent une activité très rentable, le capital intellectuel est devenu, depuis peu, une nouvelle source facile de gains importants.

Il est clair que les vecteurs et les cibles des attaques virtuelles lancées contre la société de l'information connectée actuelle se multiplient. Le Comité des crimes de haute technologie de l'Association du Barreau brésilien (Section de São Paulo) résume la situation ainsi : « Nous sommes face à des groupes spécialisés dans des attaques plus sophistiquées (dénis de service distribués) destinées à paralyser les réseaux, les services et l'infrastructure de base, ce qui entraîne des pertes de revenus et porte préjudice à l'image des grandes entreprises. D'autre part, nous avons des groupes qui cherchent à s'emparer d'informations sensibles et se livrent à de l'espionnage industriel. Les fuites de données des pouvoirs publics resteront une constante. »

Aujourd'hui, les cybercriminels s'intéressent aux contenus à des fins lucratives et ils disposent d'outils souples et rapides pour atteindre leurs objectifs. Dès qu'une vulnérabilité est identifiée, ils sont capables de mettre en place une opération de grande envergure quelques jours à peine après sa découverte. Ils développent un exploit et volent un maximum de données utiles dans des délais très courts. Des passeurs sont ensuite utilisés pour remettre les bénéfices (après prélèvement d'une commission) aux dirigeants du réseau clandestin.

La composante économique du stockage des données à l'étranger joue un rôle de plus en plus grand dans les décisions relatives aux données. Avec la baisse du prix du stockage des données à l'étranger, les sociétés prennent conscience de son intérêt sur le plan financier. Plus de la moitié des entreprises interrogées réévaluent les risques qu'impliquerait le traitement des données en dehors de leur pays d'origine (initialement motivé par la récession économique) alors qu'elles n'étaient que 40 % à le faire en 2008.

Les objets de messagerie décrivant la culture d'entreprise, les manuels de l'employé et les brevets représentent le type de données le moins protégé. Un quart ou plus des sociétés interrogées déclarent allouer un budget restreint ou nul à la protection de ces données. Les données relatives aux clients, aux fournisseurs, au personnel ainsi que les secrets commerciaux sont les informations les mieux protégées. Pourtant, des attaques telles que l'opération Aurora (entre autres) démontrent que les secrets commerciaux les mieux gardés ne sont pas à l'abri d'un pirate compétent, en dépit des systèmes de sécurisation traditionnels mis en place.

Tant la valeur des informations que le montant consacré à les protéger ont diminué au cours des deux dernières années. En 2008, les sociétés dépensaient environ trois dollars pour la protection d'un dollar de données à l'étranger. Ces dépenses en sécurité reviennent proportionnellement à 4,80 dollars pour chaque dollar de données, car bon nombre d'entreprises ont diminué leur volume de données stocké à l'étranger en maintenant les mêmes protections. Parallèlement, environ un tiers des entreprises cherche à augmenter le volume d'informations sensibles qu'elles stockent à l'étranger alors qu'elles n'étaient que 20 % il y a deux ans.

Certains pays ont une législation moins stricte en matière de notification et de confidentialité, ce qui peut constituer un atout. 80 % des entreprises qui stockent leurs informations sensibles à l'étranger sont influencées par les législations sur la confidentialité qui exigent la notification des divulgations de données aux clients. 70 % des entreprises qui stockent les informations sensibles à l'étranger choisissent des pays dont la législation leur confère davantage d'autonomie.

Les décisions prises en matière de protection des informations sensibles le sont souvent afin de respecter les réglementations du pays. Toutefois, seul un peu plus d'un tiers des entreprises estime que les réglementations de conformité imposées par leur pays d'origine sont utiles et s'attaquent véritablement au problème de protection du capital intellectuel de leur entreprise.

Section 2 : La protection des données sensibles

La cyberéconomie souterraine évolue tout comme le type de données pris pour cible. En outre, la sophistication croissante des attaques a conduit à un changement de l'approche en matière de protection des données. A présent, les sociétés doivent s'inquiéter non seulement d'un vol éventuel de leur capital intellectuel par la concurrence, mais aussi des fuites de données sensibles ou confidentielles dans les médias, comme dans l'affaire WikiLeaks.

En juillet 2010, Gordon M. Snow, Directeur-adjoint du FBI, a témoigné devant le sous-comité judiciaire de la Chambre américaine sur la criminalité, le terrorisme et la sécurité intérieure.

« L'impact du cybercrime sur les individus et le commerce peut être considérable, allant du simple désagrément à la faillite financière. L'importance des gains potentiels attire les jeunes criminels et a contribué à la création d'une importante économie souterraine connue sous le nom de "cyber-underground". Ce cyber-underground est un marché tentaculaire dominé par des règles et une logique très proches de celles régissant le monde des affaires légitime, à savoir un langage unique, des attentes codifiées quant au comportement de ses membres ainsi qu'un système de stratification basé sur les connaissances, les compétences, les activités et la réputation. »

Les nouvelles menaces sont caractérisées par une persistance et une sophistication élevées et les attaques touchent le monde entier. En novembre 2010, Postmedia News a révélé que 86 % des grandes sociétés canadiennes avaient subi une attaque, selon un rapport secret du gouvernement canadien. Le rapport révèle également qu'en deux ans, les activités de cyberespionnage ont doublé dans le secteur privé.

Un rapport publié en mars 2010 par Forrester Research montre que les connaissances propriétaires et les secrets d'entreprise ont deux fois plus de valeur que les données d'autrui qu'il est nécessaire de conserver et de protéger—comme les dossiers médicaux, les informations de carte de crédit et les renseignements clients.

« Les secrets représentent deux tiers de la valeur du portefeuille d'informations des sociétés. En dépit de la multiplication des obligations réglementaires imposées aux entreprises, les données d'autrui sous leur responsabilité ne représentent pas les actifs les plus précieux des portefeuilles d'informations des entreprises. En comparaison, les connaissances propriétaires et les secrets d'entreprise ont une valeur deux fois supérieure. Comme l'illustrent clairement les dernières attaques lancées contre les entreprises, les secrets sont des cibles privilégiées en matière de vol des données[3]. »

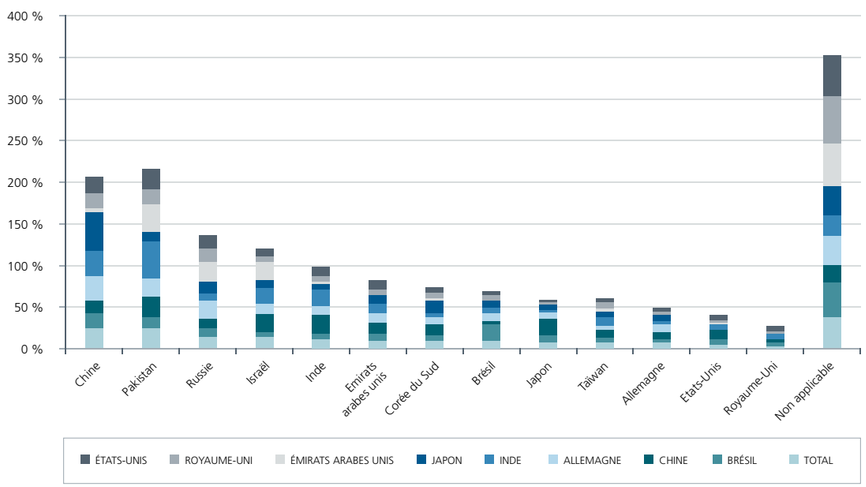
« En fait, les stratégies ne font pas l'objet d'audits suffisamment réguliers de la part des responsables, ce qui multiplie les possibilités de commettre des opérations illégales. »

Le Comité des crimes de haute technologie de l'Association du Barreau brésilien (Section de São Paulo)

Bien que près de 90 % des entreprises stockant des informations sensibles à l'étranger réalisent des analyses formelles du risque, un pourcentage en hausse depuis 2008, les sociétés continuent de stocker des données dans des pays à haut risque. Même s'il est difficile d'attribuer la responsabilité d'une attaque à un pays spécifique, la Chine, la Russie et le Pakistan sont considérés comme les Etats les moins sûrs en matière de stockage des données. C'était déjà le cas en 2008. Les pays jugés les plus sûrs étaient le Royaume-Uni, l'Allemagne et les Etats-Unis, ce qui est toujours vrai en 2010.

Bon nombre d'entreprises n'évaluent pas les menaces et les risques aussi souvent qu'elles le devraient. Plus d'un quart des entreprises évaluent deux fois par an, voire moins, les menaces ou les risques auxquels leurs données sont exposées. Plus de la moitié d'entre elles fixent elles-mêmes la fréquence des évaluations des risques au lieu de suivre les recommandations des auditeurs ou les exigences réglementaires.

Figure 1. Votre société a-t-elle évité d'entretenir des relations commerciales avec ces pays ?



Comme le fait remarquer le Comité des crimes de haute technologie de l'Association du Barreau brésilien (Section de São Paulo) : « La grande majorité des sociétés de divers secteurs manquent de contrôle sur leurs stratégies de sécurisation des informations ; de plus, les différents services de l'entreprise tardent souvent à communiquer entre eux lorsque des incidents de sécurité se produisent. En fait, les stratégies ne font pas l'objet d'audits suffisamment réguliers de la part des responsables, ce qui multiplie les possibilités de commettre des opérations illégales. Il semblerait que les actes malveillants posés au sein des entreprises ne sont pas sanctionnés. Les sociétés doivent s'améliorer sur ce point, notamment par une formation permanente visant à protéger leur capital intellectuel. »

En Chine, au Japon, au Royaume-Uni et aux Etats-Unis, les entreprises dépensent en moyenne plus d'un million de dollars par jour pour leurs systèmes informatiques. Aux Etats-Unis, en Chine et en Inde, elles consacrent en moyenne plus d'un million de dollars par semaine à la sécurisation de leurs informations sensibles stockées

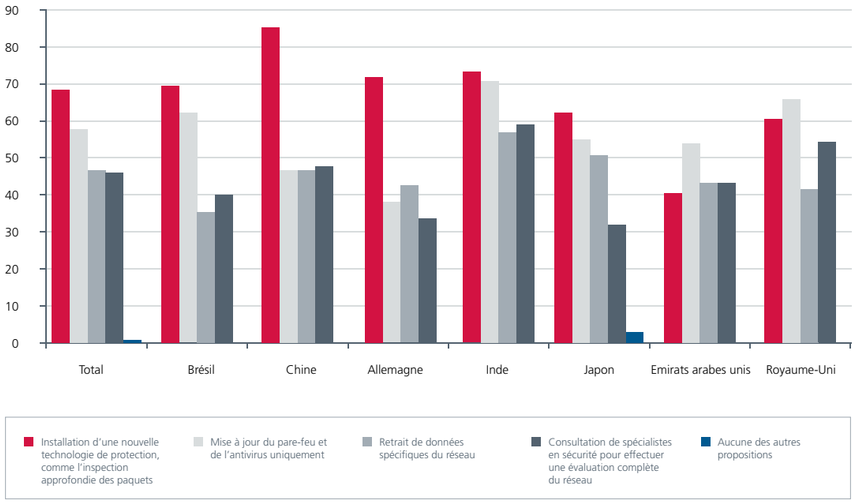
Plus d'un quart des entreprises évaluent deux fois par an, voire moins, les menaces ou les risques auxquels leurs données sont exposées.

En Chine, au Japon, au Royaume-Uni et aux Etats-Unis, les entreprises dépensent en moyenne plus d'un million de dollars par jour pour leurs systèmes informatiques.

à l'étranger. Près de la moitié des sociétés interrogées prévoient d'augmenter le budget de sécurité informatique consacré aux mises à niveau matérielles et logicielles ainsi qu'à l'hébergement externe des données et d'autres services. Plus de la moitié d'entre elles estiment que leur investissement en protection des informations sensibles augmentera, alors que 5 % seulement cherchent à diminuer leurs dépenses.

En dépit de la hausse des dépenses en sécurité informatique, les solutions implémentées sont souvent réactives. Lorsqu'elles décident de prendre des mesures de protection, les sociétés installent souvent de nouvelles fonctions ou technologies telles que l'inspection approfondie des paquets, comme l'ont déclaré près de deux tiers d'entre elles. Les solutions les plus prisées pour la protection des données sensibles restent l'utilisation des logiciels antivirus, des pare-feux et des systèmes de détection/prévention des intrusions (IDS/IPS) puisque quatre sociétés sur cinq les ont implémentées.

Figure 2. Mesures prises pour corriger les failles de sécurité et protéger les systèmes à l'avenir



Il est intéressant de constater que près de la moitié des répondants ont déclaré être prêts à « retirer du réseau certaines données » afin d'éviter toute fuite. Ici, la sécurité des données est jugée plus importante que la disponibilité ou l'utilisation des informations.

La sécurisation des équipements mobiles reste un défi pour 62 % des entreprises. En matière de gestion de la sécurité des informations, le problème majeur auquel les sociétés sont confrontées est la nature changeante des attaques, suivie de près par la multiplication des équipements et des services, notamment les supports amovibles, les smartphones et les sites de réseau social. La mobilité continue de favoriser la productivité et l'efficacité du personnel, une tendance qui ne cesse de croître. Parallèlement, les entreprises s'intéressent de près aux moyens de communication sociaux pour exploiter leurs multiples avantages. Ces deux tendances font monter en flèche le niveau de risque auquel s'exposent les sociétés en matière de fuites de données. Si l'on ajoute à cela la nécessité pour une entreprise de partager des données critiques avec ses partenaires clés, il est impératif de revoir et de renforcer les stratégies traditionnelles en matière de cybersécurité. « Il est probable que les cybercriminels se concentrent tout particulièrement sur le développement de techniques d'exploitation des smartphones en raison de leur omniprésence et de leurs fonctionnalités. Selon toute probabilité, les services dématérialisés seront également au centre des convoitises non seulement pour le vol de données mais aussi pour les ressources et l'infrastructure bon marché qu'elles représentent dans le cadre des pratiques cybercriminelles », a déclaré Marcel van den Berg de la société Team Cymru.

La sécurisation des équipements mobiles reste un défi pour 62 % des entreprises.

Selon toute probabilité, les services dématérialisés seront au centre des convoitises non seulement pour le vol de données mais aussi pour les ressources et l'infrastructure bon marché qu'elles représentent dans le cadre des pratiques cybercriminelles.

Section 3 : Incidence accrue des cybermenaces sur les activités de l'entreprise

La large couverture médiatique de certains incidents suscite des inquiétudes croissantes quant aux fuites de données confidentielles, surtout émanant du personnel interne. En 2008, trois personnes étaient condamnées pour le vol des plans de marketing de Coca-Cola[4] et un an plus tard, un ancien programmeur de Goldman Sachs était arrêté pour avoir dérobé le code informatique utilisé dans des opérations pour compte propre[5].

« Une seule erreur, même commise de bonne foi par un employé, peut avoir des conséquences dramatiques », explique Dinesh Pillai, Président de Mahindra Special Services Group, une importante société indienne spécialisée dans le conseil en gestion des risques de sécurité. « La manipulation d'un employé par ingénierie sociale peut entraîner des fuites de données critiques, des pertes financières et un préjudice pour l'image de l'entreprise, voire même une interruption des opérations métier de celle-ci. La plupart des technologies actuelles ont recours à des algorithmes prédéfinis pour détecter une anomalie. Toutefois, les réseaux clandestins possèdent des compétences et des techniques bien supérieures qui leur permettent d'identifier des voies et moyens de s'introduire dans les systèmes. »

En outre, selon le Comité des crimes de haute technologie de l'Association du Barreau brésilien (Section de São Paulo), il est rare que la menace interne soit simplement « accidentelle » : « D'après nos observations, la menace interne la plus importante provient de professionnels que l'on peut considérer comme des "intrus". Ces derniers occupent des postes peu importants et se livrent à des pratiques d'appropriation de données sensibles et d'ingénierie sociale ».

« Un certain nombre d'entreprises placent leurs employés directs et indirects sous une surveillance renforcée. Dans de nombreux cas, il s'agit de professionnels qui subissent des pressions de la part de bandes criminelles sévissant dans leur communauté défavorisée. Ces bandes demandent aux employés de leur procurer des informations sensibles, par exemple les dates de passage des services de courrier, des terminaux électroniques, les plannings d'approvisionnement, des mots de passe de sécurité internes et externes et bien d'autres données d'entreprise, en échange de la sécurité de leur famille. »

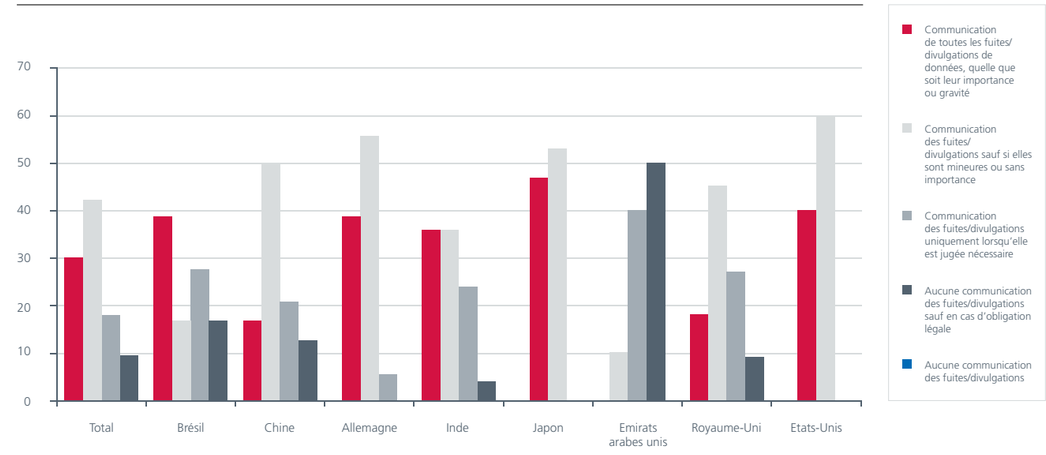
Par conséquence, comme dans l'étude précédente, c'est l'impact sur la réputation qui préoccupe le plus les entreprises. Près de la moitié des entreprises ont déclaré qu'il s'agit de leur première préoccupation concernant des divulgations de données sensibles ou de propriété intellectuelle. Aujourd'hui, une société qui perd une recette secrète, un plan de mise sur le marché ou un autre secret capital hésite à signaler l'incident en raison du tollé potentiel que cela pourrait provoquer au sein de sa clientèle et de son actionnariat et de la réaction défavorable que cela pourrait occasionner sur les marchés. Dans la mesure où la couverture médiatique d'une divulgation peut nuire à la réputation d'une marque et au cours de son action, elle est rarement rendue publique.

Une entreprise sur sept n'a pas signalé de divulgations et/ou de fuites de données aux agences et autorités gouvernementales externes ou aux actionnaires. Seules trois sociétés sur dix signalent toutes les divulgations/fuites de données intervenues, alors qu'une entreprise sur dix communique uniquement ces incidents si elle est légalement tenue de le faire. A l'heure actuelle, 60 % des entreprises « sélectionnent » les divulgations/fuites qu'elles signalent, en fonction de leur impact potentiel.

L'admission d'une vulnérabilité importante peut attirer d'autres pirates informatiques. Par conséquent, peu d'entreprises souhaitent porter à la connaissance du public leur perte de capital intellectuel.

Les activités liées aux fusions et acquisitions, aux partenariats, à la commercialisation de produits sont autant de cibles potentielles de vol de la part des réseaux criminels de l'économie souterraine. Près d'un quart des entreprises a vu une fusion et acquisition ou la commercialisation d'un produit interrompue ou retardée par une divulgation de données ou une menace crédible

Figure 3. Déclaration des divulgations de données



de divulgation. Environ la moitié des sociétés ont été confrontées à une divulgation de données peu importante et près d'un quart à une divulgation de données au cours de l'année écoulée, des pourcentages supérieurs à ceux observés en 2008.

Qui plus est, les divulgations de données coûtent cher. En moyenne, ce type d'incident coûte aujourd'hui aux entreprises plus de 1,2 million de dollars contre moins de 700 000 dollars en 2008.

C'est probablement la raison pour laquelle seul un quart des entreprises effectue une analyse post-mortem d'une fuite ou divulgation, et la moitié seulement prend des mesures pour y remédier et protéger les systèmes après un incident avéré ou une tentative d'intrusion. Plus de 50 % des entreprises ont décidé à un moment ou à un autre de ne pas entreprendre d'enquête sur un incident de sécurité à cause du coût qu'entraînerait cette investigation. Les entreprises tendent plutôt à analyser et à régler une divulgation de données mineure en interne au lieu de faire appel à une assistance externe. Cette absence d'enquête signifie que les vecteurs potentiels d'attaques n'ont pas été circonscrits et que la menace persiste ou qu'une nouvelle intrusion reste possible. Le personnel interne concerné n'est pas identifié et les incohérences ne sont pas analysées afin de mettre au jour une menace plus importante. L'absence de mesures correctives expose les sociétés au risque de divulgations ultérieures.

Pour les entreprises interrogées, ce sont les fuites de données accidentelles ou délibérées commises par des employés qui représentent la principale menace. Le respect (ou l'inobservation) des procédures de sécurité par les employés est considéré comme le défi majeur posé à la sécurité des informations d'une entreprise. Il devance d'autres problèmes, notamment l'hétérogénéité des systèmes ou le manque de sécurité des systèmes des partenaires de la chaîne logistique. Il apparaît clairement que les stratégies n'ont pas endigué les fuites de données, contraignant les sociétés à choisir des solutions technologiques robustes et innovantes pour assurer la mise en œuvre de leurs directives.

Une entreprise sur dix communique uniquement les divulgations ou fuites de données si elle est légalement tenue de le faire.

Section 4 : Des solutions et des stratégies concertées

Pour de nombreuses entreprises, les décisions prises en matière de gestion des risques et de la sécurité sont davantage motivées par le respect strict des normes de conformité que par la nécessité de protéger leur capital intellectuel. Ces entreprises ne sont pas toujours conscientes qu'une divulgation de données peut avoir un impact considérable sur les activités et la productivité, et se traduire par un ralentissement du développement de produits ou d'une procédure de fusion et acquisition.

Il faut une approche concertée en matière d'implémentation de stratégies et de solutions avancées pour que la situation évolue réellement. Ces stratégies doivent être mises en œuvre en parallèle avec des technologies d'inspection approfondie des paquets, de prévention des fuites de données, de surveillance avancée des menaces, d'analyse, voire de mesures telles que le retrait de certaines données du réseau.

Sans compter que la distinction entre menaces externes et internes tend à s'estomper. « Des pirates compétents peuvent infiltrer un réseau, s'emparer d'informations d'identification valides et disposer d'une grande liberté d'action, au même titre qu'un membre du personnel. Il est impératif de posséder des stratégies de défense contre ces menaces internes combinées. Les entreprises doivent se doter d'outils de protection contre les menaces internes capables de prédire les attaques », déclare Scott Aken, Vice-Président de la division Cyber Operations chez SAIC.

Tom Kellermann, Vice-Président de la division Security Awareness pour Core Security Technologies, cite l'absence de calendriers bien définis pour les tests d'intrusions et l'application de mesures correctives comme principale faille dans les stratégies de cybersécurité de nombreuses sociétés. En outre, une authentification faible, une sécurité perméable et une technologie de détection des intrusions inadéquate dans les environnements sans fil ne font qu'aggraver le problème.

Pour Tom Kellermann, il faut réévaluer régulièrement les fonctions d'analyse post-mortem et d'intervention en cas d'incident. « Les menaces persistantes avancées illustrent tout particulièrement la nécessité de mettre en place un système d'intervention de crise qui inclut le mapping des chemins des attaques. Les fournisseurs de services managés tiers, notamment les sociétés d'hébergement et d'infrastructure dématérialisée doivent être soumis à des obligations contractuelles qui leur imposent de tester leur sécurité et de respecter des normes plus strictes en matière de cybersécurité, sous peine de devenir une brèche béante par laquelle les prédateurs n'ont plus qu'à s'infiltrer », déclare Tom Kellermann.

« La plupart des entreprises considèrent toujours la sécurité comme un problème lié au périmètre. Mais dans la mesure où ce périmètre ne cesse de s'étendre avec l'arrivée des terminaux mobiles et de l'informatique dématérialisée, la tâche d'un service de sécurité informatique devient de plus en plus complexe », ajoute Scott Aken.

Certaines tendances émergentes font évoluer la façon dont les sociétés se protègent contre les attaques sophistiquées et les fuites internes :

Inspection approfondie des paquets – La technologie d'inspection approfondie des paquets est une solution très souple qui vient compléter l'architecture de sécurité existante en effectuant une analyse complète en ligne et en temps quasi réel de tous les paquets (niveaux 2-7), c.-à-d. sans perte de paquets. Les applications logicielles installées au-dessus de la couche matérielle permettent de mettre en place n'importe quelle stratégie basée sur des règles pour retirer certaines données des paquets quittant le réseau, mais aussi pour éliminer tout type d'exploit du trafic entrant.

Sécurité du réseau basée sur le comportement humain – Ces solutions ont une longueur d'avance sur les pirates internes ou externes dans la mesure où elles détectent les intentions par l'analyse des activités intervenant sur le réseau. Elles n'utilisent pas des signatures, la détection d'anomalies ou l'analyse heuristique : elles reposent sur la présence de comportements humains communs à toutes les manœuvres trompeuses sur un réseau afin de les bloquer avant que les données ne quittent le réseau.

Outils de détection des menaces internes – De récentes innovations dans les technologies de détection des menaces internes ont permis de créer des suites d'outils qui peuvent être déployés sur les systèmes afin de surveiller simultanément des centaines ou des milliers d'utilisateurs internes, dans le but d'effectuer un suivi de leurs activités et d'y identifier des caractéristiques de nature à déclencher des alertes. En établissant un profil des activités suspectes en temps réel, ces solutions peuvent interrompre la connexion en cas de suppression non autorisée de données ou d'activités inhabituelles et critiques.

Analyse post-mortem avancée – Chaque terminal numérique, ordinateur, téléphone portable laisse une trace ou une empreinte numérique qui peut être mise au jour à l'aide d'une analyse sophistiquée des réseaux et des ordinateurs. Des services et des outils logiciels permettent de découvrir et d'extraire du contenu critique mais aussi d'identifier des comportements d'utilisateurs et des caractéristiques uniques. La connaissance des failles et des vulnérabilités qui ont conduit à une attaque est la première étape dans la prévention d'une attaque ultérieure.

Analyse avancée des logiciels malveillants – Il est désormais possible d'identifier des logiciels malveillants de type « jour zéro » qui utilisent ou utiliseront des exploits réseau pour attaquer un réseau. Une fois détecté, le logiciel malveillant peut être capturé à des fins d'analyse et de réponse.

Conclusion

Bien qu'il soit impossible d'éliminer toutes les failles de sécurité informatique, les entreprises peuvent limiter considérablement les risques associés aux fuites des données confidentielles. Elles recherchent des solutions pour surveiller les mouvements des informations sensibles et endiguer les fuites de données potentielles, qu'elles soient intentionnelles ou non. Et ces solutions existent.

Il est possible d'installer des appliances sur le réseau afin d'enregistrer et de classifier toutes les interactions avec Internet. De même, il existe des équipements capables d'explorer les données structurées et non structurées stockées afin de rechercher et de découvrir l'emplacement où les entreprises conservent leurs données sensibles. Bien que ces équipements ne constituent pas des nouveautés à proprement parler, ils sont continuellement mis à jour et intègrent toujours plus de fonctionnalités prédictives basées sur le comportement humain. Des technologies telles que l'inspection approfondie des paquets, l'analyse du comportement humain et le chiffrement sont autant de solutions qui ne cesseront de se généraliser et de gagner en efficacité dans les années à venir.

Aujourd'hui, les entreprises vont plus loin qu'une mise en conformité simpliste et s'efforcent de protéger les données plus sensibles, notamment les documents de conception, les schémas techniques, les plans de lancement des produits, les formules pharmaceutiques, en bref leur capital intellectuel. Ces documents sont bien plus complexes que de simples numéros de sécurité sociale ou de carte de crédit et exigent des solutions de protection avancées.

Scott Aken pense que la protection de l'entreprise commence par une prise de conscience et par la connaissance des éléments qu'elle tente de protéger.

« La plupart des entreprises consacrent des sommes colossales à la protection des parties moins critiques de leur réseau alors que leur richesse essentielle, le capital intellectuel, reste sans défense. L'analyse approfondie des ressources hébergées sur le réseau alliée à une stratégie de défense en profondeur efficace, le tout mis en œuvre par du personnel correctement formé peuvent devenir de formidables alliés dans la protection des données d'une entreprise. »

Contributeurs

Scott Aken, Vice-Président de la division Cyber Operations, SAIC

Jenifer George, Cyber Portfolio Manager, SAIC

Marcel van den Berg, chef d'équipe du projet Business Intelligence, Team Cymru

Simon Hunt, Vice-Président et Directeur des Technologies de la division Endpoint Security, McAfee

Tom Kellermann, Vice-Président de la division Security Awareness, Core Security Technologies

Dinesh Pillai, Président, Mahindra Special Services Group

Erasmo Ribeiro Guimarães Junior, Secrétaire et membre du Comité des crimes de haute technologie, Association du Barreau brésilien (Section de São Paulo)

Marco Aurélio Pinto Florêncio Filho, Vice-Président du Comité des crimes de haute technologie, Association du Barreau brésilien (Section de São Paulo)

Coriolano Aurélio de Almeida Camargo Santos, Président du Comité des crimes de haute technologie, Association du Barreau brésilien (Section de São Paulo)

Références :

1 *http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage*

2 *http://f1grandprix.motorionline.com/condannato-nigel-stepney-patteggia-1-anno-e-8-mesi/*

3 *http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf*

4 *http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf*

5 *http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aSDxSdMlPTXU*

A propos de McAfee

McAfee, filiale à part entière d'Intel Corporation (NASDAQ : INTC) est la plus grande entreprise au monde entièrement dédiée à la sécurité informatique. Elle propose dans le monde entier des solutions et des services proactifs et réputés, qui assurent la sécurisation des systèmes, des réseaux et des périphériques mobiles et qui permettent aux utilisateurs de se connecter à Internet, de surfer ou d'effectuer leurs achats en ligne en toute sécurité. Grâce au soutien de son système hors pair de renseignement sur les menaces, Global Threat Intelligence, McAfee crée des produits innovants au service des particuliers, des entreprises, du secteur public et des fournisseurs de services, pour les aider à se conformer aux réglementations, à protéger leurs données, à prévenir les perturbations dans le flux des activités, à identifier les vulnérabilités ainsi qu'à surveiller et à améliorer en continu leurs défenses. McAfee consacre tous ses efforts à trouver des solutions novatrices afin d'assurer à ses clients une protection irréprochable.

www.mcafee.com/fr

A propos de la société SAIC

SAIC est une société FORTUNE 500® spécialisée dans les applications techniques, scientifiques et d'ingénierie qui exploite sa connaissance approfondie de ces domaines pour résoudre des problèmes d'importance capitale pour les Etats-Unis et le reste du monde, en matière de sécurité, d'énergie, d'environnement, d'infrastructures critiques et de santé.

SAIC : From Science to Solutions®
Pour plus d'informations, visitez le site à l'adresse www.saic.com

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr