Forum International sur la Cybercriminalité 2009 - Lille - 24 mars 2009

Autor(en): **Weck, Hervé de**

Objekttyp: **Article**

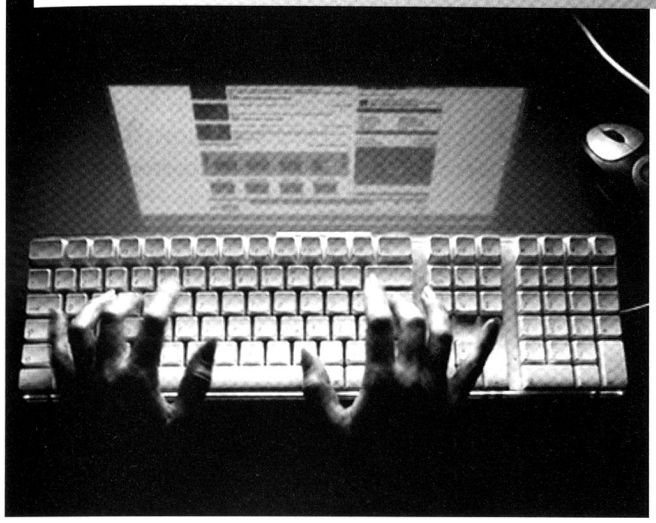
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2010)**

Heft 3

PDF erstellt am: **17.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-514429



La gendarmerie et l'armée française sont de plus en plus appelées à faire face aux menaces informatiques.

Sécurité

Forum International sur la Cybercriminalité 2009 - Lille – 24 mars 2009

Col Hervé de Weck

Ancien rédacteur en chef, RMS

Les atouts du télétravail (meilleure productivité, moindre impact environnemental, meilleure qualité de vie) incitent les entreprises à s'y intéresser, qu'il soit maîtrisé ou contraint. Les questions touchant à la sécurité des données restent, à juste titre, un des principaux freins à cette nouvelle façon de travailler.

Un état des lieux[1]

Il existe des solutions technologiques, toujours plus pointues, de sécurisation des réseaux privés virtuels (RPV ou VPN), mais elles doivent impérativement aller de pair avec un accompagnement des utilisateurs, afin qu'ils adoptent de bonnes pratiques. La mise en place d'un réseau RPV implique toute une série de choix, de la connectivité (nature du réseau, accès, authentification) à la réduction des fuites des données. Pour les télétravailleurs permanents ou fréquents, un protocole de protection des informations échangées (Ipsec) peut convenir. Pour les connexions occasionnelles, un protocole (dit SSL ou TLS) de protection des échanges sur Internet est préconisé. Ces recherches doivent englober les supports ultra-portables comme *iPhone* et *Blackberry* qui sont pour l'instant très peu protégés.

Les systèmes de sécurité des établissements bancaires reposent sur un ensemble de règles et de normes strictes ainsi que sur la triple dimension que constituent l'homme, l'organisation et les technologies. Des mesures préventives de protection des données et de sensibilisation de tous les acteurs permettent, en interne, de veiller au bon fonctionnement et à la bonne utilisation du système d'information. Le système de sécurité doit sans cesse s'adapter; de nouvelles techniques apparaissent, telles que le *phishing* ou les *keyloggers* qui menacent, entre autres, le monde bancaire. Même si les risques de fraudes venant de l'extérieur paraissent plus évidents que les risques venant de l'intérieur même de la structure, ces derniers s'avèrent tout aussi importants. Les cas des *traders* contournant à mauvais escient les systèmes de sécurité sont emblématiques. Dans 70% des cas, le risque vient de l'interne.

Seul un examen approfondi des identités et des diplômes du futur employé permet de s'assurer de ses bonnes intentions. Le crime organisé a compris que ce type d'attaques engendrait moins de risques que d'autres trafics. Grâce à la corruption, ils trouvent des complicités internes ou financent les études de jeunes gens brillants pour infiltrer les banques. Ce type de fraudes semble s'accroître, même si aucune donnée statistique ne peut confirmer cette tendance. En effet, les banques, par peur de ternir leur image, refusent généralement de porter plainte.

De nouvelles menaces stratégiques apparaissent avec le développement d'Internet et du cyberespace. D'origine étatique, criminelle ou terroriste, elles recouvrent un ample répertoire d'actions, depuis l'utilisation du déni de service jusqu'à la combinaison d'attaques physiques et informatiques. Pouvant atteindre les capacités économiques et militaires d'un pays, les attaques informatiques représentent un enjeu stratégique majeur pour les départements de défense, notamment parce qu'il est extrêmement difficile d'en identifier les auteurs. Si un État n'est pas identifié comme l'auteur d'une attaque, une riposte ne peut être légalement menée. De manière générale, les stratégies défensives sont privilégiées par rapport aux stratégies offensives, bien que l'armée américaine envisage de se doter de capacités offensives de lutte informatique. Actuellement, elles sont encore interdite et il n'est pas envisagé de les ouvrir aux acteurs privés. En France, des plans de vigilance et de réaction aux crises ont été mis en place pour faire face à ces nouvelles menaces informatiques. Cependant, il est encore nécessaire de développer les exercices de simulation et d'inciter les entreprises comme les individus à sécuriser leur système, pour en éviter l'utilisation par une tierce personne.

1 Actes en ligne du 3e Colloque: http://pourconvaincre.blogspot.com

Le téléphone portable : gestion au sein de l'entreprise

Le téléphone portable devient un outil d'importance croissante dans l'entreprise. Les *smartphones*[15] permettent aux employés de travailler à distance et en toutes circonstances. Les *Mobile device management* (*MDM*) contrôlent à distance l'ensemble des terminaux mobiles d'une entreprise. La géolocalisation, au moyen des cartes *SIM*, de systèmes *GPS* intégrés à un téléphone ou à un véhicule, donne plus de réactivité à l'entreprise. Elle permet le suivi en temps réel de ses marchandises. Les téléphones *Near field communication* (*NFC*), reconnaissant les puces *RFID*, améliorent et rendent plus rapides les échanges d'informations entre l'entreprise et ses employés.

A terme, ils pourront intégrer dès leur conception des applications monétiques, billettiques, ou de *smartposters*. D'autres applications peuvent lui être ajoutées en fonction des besoins spécifiques des entreprises. Ces nouvelles technologies, amenées à se développer, représentent néanmoins un renforcement des risques environnementaux et sécuritaires. En stockant et en transmettant davantage d'informations, un téléphone infiltré est une menace non négligeable pour l'entreprise. Le renouvellement continu des parcs téléphoniques produit une grande quantité de terminaux mobiles qui sont recyclés ou revendus et dont la destruction des données constitue un enjeu critique.

L'internet de demain : quelles menaces et quels risques?

L'interconnexion croissante des systèmes et la grande disponibilité de l'information provoquent une augmentation de plus en plus imprévisibles et une professionnalisation des menaces informatiques. Les organisations privées concurrencent la puissance numérique des Etats qui se préparent par ailleurs à l'éventualité de guerres virtuelles. Dans le futur, l'interaction entre mondes virtuel et réel permettra aux menaces informatiques de provoquer des morts réelles et au cyberterrorisme de se développer. Pour y faire face, il faut responsabiliser l'ensemble des acteurs de la chaîne d'échanges informatiques et non plus seulement l'utilisateur final ou les directeurs d'entreprise. Ces derniers gardent néanmoins une obligation de sécurisation de leurs systèmes, notamment pour les assurances prenant en charge les risques numériques.

L'usurpation d'identité étant la principale vulnérabilité d'Internet, il faut favoriser l'émergence de systèmes permettant d'identifier l'auteur et le contenu de toute source d'information. Une *constitution numérique* permettrait de garantir un minimum d'éthique dans l'utilisation d'Internet. Les entreprises et les États doivent établir quelles sont les données essentielles à leur fonctionnement pour en renforcer la protection. Certains appuient la création d'une police internationale d'Internet ou sa prise en charge, soit par une *haute autorité des robots*, soit par des applications autonomes pouvant détruire automatiquement les fichiers illégaux.

Le chef d'entreprise engage sa responsabilité en matière pénale dès lors qu'il fournit une connexion Internet à ses salariés. La consultation ou le téléchargement par un salarié de contenus interdits – images pédo-pornographiques ou vidéos sous copyright – relève de la responsabilité du chef d'entreprise. La nomadisation (portables, Wi-Fi) multiplie les risques et les vols. Dans une situation de guerre de l'information, les pertes d'informations sont préjudiciables et profitent au concurrent. Pour cette raison, il convient de mettre en place une stratégie de sensibilisation des salariés: le management des risques. L'exemple américain invite à considérer les chartes d'utilisation qui peuvent être signées par les employés mais qui doivent être expliquées, de manière à ce que les droits et les devoirs de l'utilisateur en entreprise soient bien compris. Suite à une attaque, déposer plainte est un excellent moyen pour la justice de capitaliser les informations et d'évoluer. Malheureusement, de nombreuses entreprises préfèrent taire ces actes, qu'ils soient internes ou externes. Les cyberdélinquants le savent et ils profitent de la situation.

La veille permet d'accéder au Web invisible, celui auquel nous n'avons pas accès par les moteurs de recherche traditionnels. Ainsi, il est possible aujourd'hui d'observer de façon automatisée les pratiques des concurrents, les grandes tendances sociétales, les comportements des clients et des acteurs institutionnels. La veille consiste à identifier les sources d'informations pertinentes, organiser les recherches, sauvegarder les informations obtenues, les analyser, les synthétiser et les diffuser aux bons interlocuteurs. Le veilleur ne doit pas laisser de traces de son passage, au risque de se voir fermer l'accès aux informations ou de livrer des données utiles aux sites visités. Pour cela, il peut changer les adresses IP utilisées et l'heure de lancement des automates de veille, effacer ses logs.

La veille sécuritaire consiste à s'informer de façon permanente sur le fonctionnement des outils de sécurité, à lancer l'alerte si un comportement anormal est identifié et à prendre rapidement des contre-mesures. Les outils de veille sécuritaire sont souvent mal utilisés par les entreprises. L'enjeu central de la veille est le traitement et la classification des très nombreuses informations obtenues. La surveillance doit être permanente et les capacités de réaction rapides.

Les entreprises s'engagent de façon croissante dans la lutte contre la cybercriminalité et le renforcement de leur sécurité. Leurs investissements dans ce domaine ne semblent pas être remis en cause par la crise économique actuelle. Leur priorité reste la bonne application des standards classiques de sécurité, ainsi que les actions de sensibilisation visant à réduire les comportements à risques. D'autres mesures de sécurité sont adoptées, telles que la cybersurveillance, l'authentification unique ou la suppression des ports USB des ordinateurs.

Les attaques internes représentent la principale source de menaces, bien que les entreprises se préparent également à l'éventualité d'attaques massives qui nécessitent

une plus grande coopération entre acteurs internes et externes, entre acteurs publics et privés. La législation en France encourage le renforcement des politiques de sécurité, notamment par l'adoption de Plan de continuité d'activités et de Plan de reprise d'activité. Certaines entreprises souhaitent la mise en place d'authentifications et de certifications officielles pour les différents acteurs en contact avec les réseaux électroniques. Le contrôle de l'application de la législation, ainsi que sa clarification et son adaptation au contexte national et européen sont vivement souhaités.

H.W.

Nouvelles brèves

Armes russes

Le Sri Lanka, dont le budget de la défense annuel est d'1,7 milliard de dollars, a emprunté à la Russie 300 millions USD ce mois de février, afin d'acquérir des armes et du matériel de guerre. L'an dernier, des contrats pour 200 millions ont été annulés avec la Chine et le Pakistan – afin de « réchauffer » les relations du Sri Lanka avec l'Inde, leur principal adversaire.

La Russie renoue donc avec la tradition soviétique des ventes d'armes contre emprunt, souvent à un taux très généreux, afin d'augmenter son influence en Asie ou en Afrique. Rappelons que la chute de l'Empire soviétique est, pour une large part, due à l'endettement et à la politique de fournitures militaires.

http://www.strategypage.com/htmw/htproc/articles/20100214.aspx

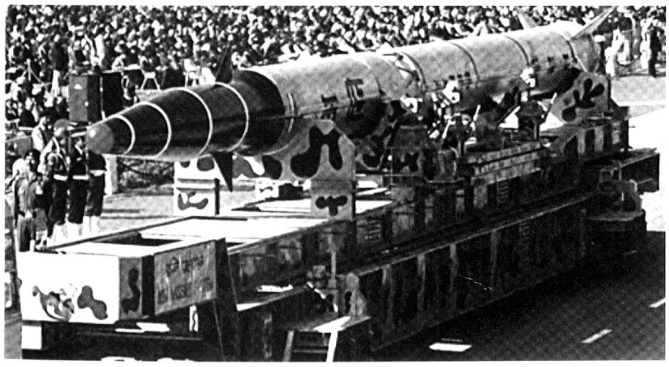
Nouvelles brèves

Dissuasion indienne

Le 7 février, l'Inde a testé avec succès le 4e et dernier test de sa fusée intermédiaire (IRBM) *Agni* III. L'engin à deux étages pèse 50 tonnes et atteint une altitude de 350 km ; il transporte une charge de 1,5 tonne : assez pour emporter une ogive nucléaire. L'*Agni* I atteint les 700 km, l'*Agni* II 2'500 et l'*Agni* III a une portée de 3'500 km. Une Ve version de cet engin est en cours de développement. Il est clair que les versions I et II visent le Pakistan. La version III est destinée à dissuader la Chine. Une future version V serait destinée à être pointée vers la Russie.

http://www.strategypage.com/htmw/hticbm/articles/20100210.aspx

Le missile indien *Agni I*, d'une portée de 700 km.



La Russie est dépendante de ses exportations d'armement. Ici, un Su-30 indien durant un vol d'entraînement en Grande Bretagne, escorté parun Eurofighter *Typhoon* et un *Tornado* F.3.