Cliquez sur ce lien pour la version française : Interview pour "Protect Letter" N° 47 de Trend Micro

Cybercrime: die Gefahren!

Interview mit Stéphane Koch, Competitive Intelligence & Information Security Advisor.

1. Wie hat sich aus Ihrer Sicht die Gefahrenlage im Internet in den letzten Monaten verändert?

Heutzutage stellt man immer öfter fest, dass die Attacken im Netz deutliche professioneller werden. Da Wirtschaftsinformationen für Unternehmen hohe Priorität haben, reizt es natürlich einige Leute, legale Wege zu umgehen und stattdessen mit cyberkriminellen Organisationen zusammenzuarbeiten. Im gleichen Mass wie sich Kommunikations- oder Speichertechnologien (z.B. smart phones, Skype, Bluetooth, GPS etc.) weiterentwickeln, gibt es auch immer mehr Möglichkeiten, Unternehmen oder Privatpersonen zu attackieren (bspw. Spyware). Selbst heutige Anwendersoftware und Protokolle, die auf dem neuesten Stand sind, sind nicht in der Lage, absolute Sicherheit zu gewährleisten.

2. Wo liegen heute die grössten Probleme bei Privatanwendern und KMUs?

Bei KMUs: Der Unterschied zwischen dem Potenzial einer Technologie einerseits und ihrem Verstehen andererseits ist oft gross, was dramatische Konsequenzen für die wirtschaftliche Situation des Unternehmens haben kann. Deshalb müssen die verschiedenen Informationskanäle, -quellen und -träger genauestens bekannt sein, um das Unternehmen schützen zu können.
Für Private: Die weite Verbreitung der ADSL-Anschlüsse macht den privaten Benutzer für Cyberkriminelle interessant. Ausserdem sind private Benutzer sehr attraktiv für potenzielle Attacken, weil sie Passwörter, Kreditkartennummern oder andere persönliche Informationen auf ihren Computern speichern und diese regelmässig benutzen ohne sie zu schützen. Komplizierte Attacken erscheinen immer mehr in diesem Umfeld in Form von Phishing, Pharming oder Angriffen im Stil von „Drive by pharming“. Hauptziel ist es natürlich, Informationen über Konten, die für die elektronischen Transaktionen dienen, herauszufinden.

3. Was ist Ihre Empfehlung an die Leser des Protect Letters?

In den letzten drei Jahren hat sich die Informations- und Kommunikationstechnologie enorm weiterentwickelt, weil die Bedürfnisse laufend zugenommen haben. Man sollte nicht ängstlich sein und sich den Vorteilen dieser Technologien verschliessen. Viel eher sollte man das eigene Verhalten dem Gefahrenpotenzial anpassen. Ausserdem sollten die Unternehmen Verantwortung übernehmen und ihre Mitarbeiter auf den auf dem Markt neusten Technologien ausbilden. Sicherheit ist ein dynamisches Modell, das sich jeden Tag ändert, sei es im privaten oder im

privaten Umfeld. Durch die Kombination von Technologie und menschlichem Verhalten wird der bestmögliche Grad an Sicherheit erreicht.

Über den Autor:
Stéphane Koch besitzt den Master Degree in Economic Crime Investigation und berät Unternehmen in „informational assets protections", „business marks protection" im Internet und anderen kritischen cybercrime Fällen. Er ist Mitglied des ThinkTank (Plattform für Cybercrime Experten), der mit der Swiss Security Exchange zusammenarbeitet. Zudem ist er im Geneva Forum of Security aktiv, führt regelmässig Seminare in Frankreich durch und unterrichtet an der EGE (Ecole de Guerre Economique) sowie der HEG (Haute Ecole de Gestion) in der Schweiz.

Interview pour "Protect Letter" N° 47 de Trend Micro

1. Comment ce sont développés, d'après vous, les dangers/risques/attaques du cybercrime ces derniers mois?

On assiste à une professionnalisation des attaques et à une mise en relation d'organisations criminelles qui ne se côtoyaient pas forcement par le passé. De plus, la valeur intrinsèque que peuvent représenter les informations économiques des entreprises, a poussé nombre d'individus - possédant des connaissances et une maîtrise technologique poussée - à franchir la frontière de la légalité, soit pour commercer avec des organisations criminelles, soit pour entreprendre des actions criminelles par eux-mêmes. A ce titre, les spywares (logiciels espions) représentent un risque majeur pour les entreprises et les particuliers. Dans le même temps, on assiste à une multiplication des technologies de communication et des supports de gestion et de stockage de données (smart phones, téléphonie internet, Wifi, Bluetooth, Blackberry, GPS, PDA, lecteurs MP3, clés USB, etc…). Il en résulte une perception de plus en plus floue de la frontière entre les outils de l'entreprise et ceux du particulier, ainsi que de la séparation entre les données à caractère privé et professionnel, qui viennent à transiter sur ces différents supports. La plupart des programmes et des protocoles utilisés par ces outils de nouvelle génération ne sont pas encore totalement sécurisés, ni même leur utilisation - dans le contexte des options disponibles - maîtrisée par leurs détenteurs. Ce qui rend d'autant plus difficile la sécurisation du périmètre informationnel des acteurs concernés.
L'explosion des connexions ADSL privée à fait du particulier une cible intéressante pour les cybercriminels. En effet, en plus des données stockées sur les ordinateurs des particuliers (cartes de crédit, et mots de passe de comptes web), il faut aussi prendre en compte les ressources que représentent ceux-ci pour la commission d'acte illégaux, que cela soit pour du spamming à grande échelle, ou pour de l'hébergement de contenu pédophile, par exemple. Dans cet environnement complexe, de nouvelles attaques, plus insidieuses voient le jour, faisant suite aux actions de Phishing, le Pharming ou les attaques de type « Drive by pharming » on fait leur apparition chez les particuliers. Le but principal étant d'obtenir les informations des comptes servant au paiement des transactions électroniques.

2. Où se trouvent actuellement les plus gros problèmes pour les utilisateurs privés et les PME?

Pour les PME : Le décalage entre la compréhension que l'on a des technologies utilisées, et leurs potentiels réels, peut avoir des conséquences importantes sur l'environnement stratégique et concurrentiel des entreprises, et de facto, leur puissance économique. Il est donc nécessaire de penser aux avoirs dématérialisés de l'entreprise en termes de patrimoine informationnel. L'interdépendance croissante aux divers acteurs par lesquels l'information passe, et la fragilisation des infrastructures de transport des données ou celles de l'énergie, accroissent le spectre du risque tout en le rendant plus difficilement maîtrisable. À ce titre, il faut prendre en considération les différents vecteurs et "véhicules" de l'information participants à l'exercice de l'activité professionnelle, et inclure ceux-ci dans le périmètre informationnel de l'entreprise. Car, qu'il soit de nature humaine ou technique, chaque dysfonctionnement peut entraîner de graves conséquences sur la réputation des entreprises concernées.
Pour les particuliers, il est difficile de les dissocier de leur statut d'employés, qu'ils occupent un poste au sein d'une entreprise ou parce qu'ils sont leur propre patron. La raison à cela se trouve dans le fait que les entreprises sont globalement mieux sécurisées qu'auparavant, et par conséquent, le domicile privé représente actuellement le maillon faible en termes de sécurité. Il faut aussi ajouter que l'accroissement de la bande passante et l'évolution des technologies de l'information et de la communication (TIC), ont multiplié les possibilités de travailler de manière délocalisée, ou d'accéder à distance à tous les types de services on-line. De plus, ce qui touche la réputation d'un individu, peut facilement avoir des conséquences sur celle de l'entreprise qui l'emploi. L'avènement des réseaux sociaux online et des services de type « web 2.0 » ou autres outils de création et de partage d'information, ont mis à disposition, sur le Net, une quantité énorme de données à caractère privé ou même confidentiel. Les erreurs de configuration des intranets ou le traitement amateurs de documents d'entreprise sont venus enrichir la masse d'information en circulation - celle-ci étant accessible, par tout un chacun, par le biais des outils de recherche. Le principal défi, sera donc de réussir à « ancrer » une « conscience » de la sécurité, comme étant une problématique globale et transversale, dans le comportement social de l'individu, qu'il soit chômeur, employé, entrepreneur, ou directeur.

3. Quels sont vos conseils aux lecteurs du Protect Letter - concernant la cybercriminalité ?

Si l'utilisation des TICS a connu une telle croissance ces derniers trois ans, ce n'est pas à cause des effets d'annonce et de l'apport du marketing, c'est en réponse à l'expression d'un réel besoin. Il ne faut donc pas tomber dans la paranoïa par rapport aux risques présents, et interdire, ou s'interdire les avantages que représente l'utilisation de ces technologies. Il faudrait plutôt envisager de changer des comportements et des cultures…. Et que les entreprises prennent enfin la responsabilité de sensibiliser et de former leurs employés à une utilisation maîtrisée des technologies disponibles sur le marché, elles en ont les moyens et le pouvoir. Elles seront largement payées en retour par une diminution des erreurs et pannes dû à une mauvaise gestion et utilisation des systèmes d'information. Mais, ne nous arrêtons pas en si bon chemin, la culture interne de la sécurité au sein des entreprises doit aussi changer. Trop de structures sont encore segmentées en départements qui ont de la peine à collaborer entre eux. La communication, les ressources humaines et le service informatique sont naturellement unis par les mécanismes liés au traitement et à la circulation de l'information au sein de l'entreprise. Il faut bien être conscient que si la collaboration et le partage de connaissance peinent à se mettre dans le secteur privé, ce n'est pas le cas dans les milieux criminels, ou le B2B du crime organisé est déjà bien rodé. Cela étant dit, il serait simpliste de jeter la pierre aux seules entreprises et individus, les fabricants de logiciels et d'ordinateurs, tout comme les gouvernements ont aussi leur part de responsabilité. Que cela soit par la mise sur le marché de produits dont la fiabilité n'est pas assurée, ou par le laxisme de certaines autorités politiques face à des lobbies dont les objectifs sont purement mercantiles. Il n'est donc pas étonnant que nombre de failles de sécurité soient découvertes et communiquées dès la commercialisation des produits. On a tendance à créer des marchés là où l'on devrait régler, et légiférer sur des problèmes : le spamming en est la parfait illustration. Le problème, c'est que ces opportunités économiques se font au détriment des entreprises et des individus.
Au final, la réponse sera philosophique, Socrate disait que le savoir c'est savoir que l'on ne sait rien, il en va de même avec les TIC, La sécurité est un modèle dynamique, qui chaque jour se redéfinit. Les vérités d'hier peuvent être à la base des erreurs d'aujourd'hui. Il faut savoir remettre en cause ses connaissances et garder un sens critique par rapport à ses acquis. Que cela soit pour le professionnel ou pour le particulier, la sécurité repose sur des mesures techniques et humaines, basée sur la connaissance d'un environnement.

Stéphane Koch

Bio :

Professionnel : Membre du think tanks "Swiss Security Exchange". Stéphane koch est spécialisé dans les aspects liés à la gestion stratégique de l'information. Consultant pour un groupe européen de communication en matière de stratégie internet, il effectue aussi, sur le marché Suisse, des missions de conseil et de formation dans les domaines de la sécurité économique, de la gestion de la réputation et de la protection du patrimoine informationnel de l'entreprise et de sa marque sur Internet.

Enseignement : Membre du comité scientifique des études postgrades HES en Intelligence économique et veille stratégique (IEVS), il intervient aussi en tant que formateur et en tant qu'expert pour le Centre suisse d'enseignement du marketing, de la publicité (SAWI), l'Institut Suisse de Relations Publiques (SPRI), la Geneva School of Diplomacy et dans diverses filières des Hautes Ecoles Spécialisées (HES-SO). Depuis 2003, il dispense à l'EGE, une série de cours sur la gestion offensive et défensive de l'information et la protection du périmètre informationnel et de la réputation sur Internet