Intermédiaires financiers et aïkido numérique

Leçon V: know your (cyber) enemy

Nos précédents articles portaient sur la manière d'appréhender les concurrents, les combattants et la technologie grâce à l'aïkido numérique. Revenons-en à présent au concept d'auto-défense, idéal pour parer à un nouveau type d'offensive, qui ne cesse de s'amplifier en terme de volume, comme de sophistication : les cyber-attaques.

« Know your enemy » est un principe qui prend tout son sens ici. Pour commencer, demandez-vous si votre ennemi se trouve au sein de l'entreprise ou en dehors. Parer à une menace provenant de l'intérieur est extrêmement difficile dans la mesure où les employés ont un accès élargi et légitime à vos actifs et à votre infrastructure. D'autant plus que cette situation est également très délicate à gérer du fait que personne ne veut traiter ses employés comme des suspects. Les raisons pouvant être à l'origine d'attaques d'employés sont multiples : erreur humaine, ignorance, frustration quant à l'évolution professionnelle ou l'environnement de travail, pour n'en citer que certains. Si des mesures techniques peuvent être prises pour atténuer le risque, conserver une culture d'entreprise saine et connaître vos collaborateurs n'en demeurent pas moins la meilleure ligne de défense. Il est essentiel d'adopter une communication claire et transparente.

Les assaillants provenant de l'extérieur poursuivent des objectifs différents, si bien que l'on peut, d'une manière générale, les diviser en trois grandes catégories:

1. Hackers : pas mus par des intérêts financiers, mais plutôt par la volonté de s'opposer à l'establishment, ou de flatter leur égo en jouant à David contre Goliath.
2. Criminels : recherchent généralement un rendement financier en recourant au vol de données/d'identité ou au chantage (p. ex. déni de service distribué (DDoS) ou cryptage de données) ou à l'espionnage industriel.
3. Terroristes : utilisent des moyens similaires aux hackers et aux criminels. Ils veulent ébranler des Etats, des entreprises ou des personnes.

Mode opératoire

L'interconnexion et la complexité croissantes de notre infrastructure mondiale ont créé des risques de vulnérabilité et ont changé les vecteurs de risque. Voici quelques exemples typiques :

Vol d'identité	Le mot de passe est d'abord piraté, puis le profil (p. ex. sur les réseaux sociaux) ou l'e-mail est détourné pour distribuer des messages (ou virus / cheval de Troie) ou faire chanter le propriétaire. La pratique du phishing en est un parfait exemple. Dans notre secteur, les ordres de paiement frauduleux en sont un cas typique.
Virus / cheval de Troie	Va de l'espionnage à l'intention de détériorer des données et/ou l'infrastructure sur des systèmes infectés ou d'utiliser (abusivement) un ordinateur (p. ex. botnet).
Vol de données	Piratage pour avoir accès au système afin de subtiliser des données qui sont soit vendues au marché noir, soit utilisées pour porter atteinte à l'ordre public ou en soutirer un bénéfice auprès du propriétaire. Dans les services financiers en particulier, le vol de données personnelles des clients est une menace à prendre très au sérieux – la situation financière des gens est un sujet très sensible qui requiert de déployer de très grands efforts pour les protéger contre les abus criminels.

DDoS	Le déni de service distribué pour ébranler des systèmes en envoyant un volume considérable de demandes à un serveur particulier.
Catastrophes naturelles	Panne d'électricité, incendie, inondation, tremblement de terre.

Protection des données précieuses – un facteur de la confiance des clients
Nous devons protéger les données de nos clients et de nos employés. Nous devons également protéger nos clients et leurs activités contre la fraude (p. ex. faux paiements). Et nous devons protéger nos systèmes de sorte à les maintenir opérationnels.

Les techniques à maîtriser sont si répandues que nous ne nous appesantissons pas à dessein. Face à toutes ces menaces, votre entreprise doit avoir un plan de Business Continuity Management (BCM) clair en place, qui repose sur l'identification et la priorisation des risques, ainsi que la mise en œuvre des mesures pour les atténuer. Mesures typiques : assurer une redondance géographique des systèmes informatiques, des postes de travail de secours équipés de la même technologie ainsi que des éléments plus procéduraux, tels que des listes de contacts. Des recommandations en matière de BCM sont synthétisées dans un document publié sur le site Web de l'Association suisse des banquiers (www.swissbanking.org). L'expérience nous a montré qu'avoir un plan était une bonne chose, mais qu'il valait mieux le mettre à l'épreuve. Exécuter un test de basculement pour voir s'il fonctionne vraiment dans la pratique et pas uniquement sur papier.

Questions clés pour votre prestataire d'accès informatique interne et externe
Pour déterminer le degré de solidité de vos défenses, vous pourriez poser dix questions essentielles à votre prestataire d'accès (interne ou externe) :

1. Quelle protection avez-vous pour faire face aux virus, cheval de Troie et autres formes de malicieux et spam?
2. Des pare-feux ont-ils été mis en place et quelles sont les règles actives?
3. Si vos systèmes ne sont pas protégés par une authentification à deux canaux, pourquoi et quels sont les risques?
4. Y a-t-il des systèmes de sauvegarde en place et quand le dernier test de basculement de système a-t-il été effectué avec succès?
5. Disposez-vous d'ordinateurs indépendants en cas de problème?
6. Quels sont les fichiers journaux disponibles et à quels niveaux sont-ils requis?
7. Une politique du moindre privilège est-elle définie et appliquée pour l'accès aux données?
8. Disposez-vous d'un inventaire logiciel, faisant état de l'âge, des dernières mises à jour et des données pertinentes? S'agissant des logiciels développés en interne, y a-t-il toujours au moins deux personnes disponibles qui comprennent le code?
9. Quel soin supplémentaire et quelles mesures sont indiqués lors de l'utilisation des services de cloud?
10. Quel est le degré d'efficacité du cryptage de vos données?

BCM et l'informatique ne sont pas des thèmes qui peuvent être délégués. Vous devez régulièrement procéder à votre propre évaluation du risque et impliquer les fournisseurs dans le processus. Faites-en un thème entrant systématiquement en ligne de compte.

Dernier point : une fois que vous avez passé du temps à gérer les cyber-risques pour votre entreprise, demandez-vous comment vous pourriez aider vos clients à protéger leur vie privée – en particulier lorsque leurs enfants utilisent les réseaux sociaux à leur guise… nous y reviendrons dans notre prochain article consacré aux réseaux sociaux.

Vous pouvez également vous référer à des check-lists existantes, telles que celle publiée par le Département fédéral des finances et celle de l'équipe UBS online security.

melani.admin.ch/melani/fr/home.html
ubs.com/ch/en/online-services/security.html#tips