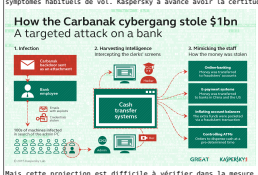
Comment les entreprises pourraient mieux se protéger des attaques informatiques de plus en plus sophistiquées ?

Comment les entreprises pourraient mieux se protéger des attaques informatiques de plus en plus sophistiquées ?

En 2013, un distributeur automatique de billets à Kiev s'est mis à délivrer des billets tout seul à certains moments de la journée qui semblaient être fortuits sans que personne n'ait à insérer une carte ou à presser un bouton. Les caméras de surveillance ont montré que l'argent qui avait été délivré a été raflé par des clients à qui la chance semblait sourire.

Cependant, quand l'expert en cybersécurité russe Kaspersky Labs a été appelé en Ukraine pour mener une enquête, il a découvert qu'il ne s'agissait là que de la partie émergée de l'iceberg. En effet, les ordinateurs internes de la banque, utilisés par les employés qui traitent des transferts quotidiens et qui tiennent la comptabilité, avaient été infiltrés par un logiciel malveillant qui permettait aux cybercriminels baptisé du même nom que leur logiciel Carbanak (basé sur le trojan Carbep) d'enregistrer chacun de leurs mouvements. Les recherches ont montré que le logiciel malveillant qui se cachait depuis des mois a envoyé des images et des vidéos a un groupe de cybercriminels pour lui permettre de déterminer comment la banque effectuait ses routines. « L'objectif étaient d'imiter leurs activités », expliquait Sergey Golovanov qui a mené les opérations d'investigations pour le compte de Kaspersky. « De cette façon, tout aurait ressemblé à une opération quotidienne normale » a-t-il rajouté par la suite. Ils commencent par ajouter virtuellement de l'argent sur un compte bancaire en modifiant le solde disponible, puis transfèrent toute la somme ajoutée vers le compte de destination, laissant le solde d'origine intact.

Dans un rapport que Kaspersky a publié il y a quelques jours déjà, l'entreprise a avancé que la portée de cette attaque s'étendait sur plus de 100 banques et autres institutions financières dans une trentaine de pays et cette série de vols pourrait en faire le plus gros casse de banque jamais réalisé et qui a en plus été menée sans les symptômes habituels de vol. Kaspersky a avancé avoir la certitude que près de 300 millions de dollars ont été dérobés à ses clients et que la somme total du casse pourrait atteindre le triple.



Mais cette projection est difficile à vérifier dans la mesure où les vols ont été limités à 10 millions de dollars par transaction, bien que certaines banques aient étés frappé plusieurs fois. De plus, dans certains cas, les transactions étaient plus modestes, sans doute pour éviter de déclencher des alarmes. La majorité des cibles étaient situées en Russie, mais il y en avait également plusieurs au Japon, aux Etats-Unis et en Europe. A cause d'une clause de non divulgation avec les banques qui ont été touchées, Kaspersky n'a pas eu le droit d'en établir une liste qui pourrait être portée au public. Des responsables à la Maison Blanche ainsi que du FBI, d'Interpol ou d'Europol ont été débriefés dessus mais ont avancé que cela prendrait du temps pour confirmer et évaluer les pertes.

Chris Dogget, le directeur général de Kaspersky en Amérique du Nord à Boston, a avancé que le groupe de cybers criminels Carbanak représente une augmentation de la sophistication des cyberattaques sur les entreprises financières. « C'est probablement l'attaque la plus sophistiquée du monde a vu à ce jour en termes de tactiques et des méthodes que les cybercriminels ont utilisé pour rester dissimulés », a-t-il déclaré. Les cybercriminels ont pris la peine d'étudier chaque particularité des banques ciblées tandis qu'ils établissaient de faux comptes en Chine et aux Etats-Unis qui pouvaient servir de destinations de transferts. En somme, une mécanique très bien huilée.

D'autres attaques qui ont également fait parler les médias comme celle qui a vu 76 millions de comptes clients de l'institution financière JPMorgan Chase être piratés ont poussé les banques à s'interroger sur la raison pour laquelle des pirates les considèrent comme des proies relativement facile. Pour pouvoir faire face aux menaces ou future menaces, certaines institutions ont estimé qu'elles devaient très vite colmater des failles non seulement dans la sécurité de leur système mais également dans celui des entreprises partenaires ou conseillères. Et si la réponse était toute autre ?

La raison principale pour laquelle les cybercriminels voient de grandes entreprises ainsi que leurs partenaires principaux comme des proies relativement faciles est une déconnexion alarmante entre les membres du conseil de l'administration de l'entreprise et leurs services informatiques. Le rapport « exposer les fissures de la cybersécurité : une perspective mondiale » publié par l'Institut Ponemon l'année dernière a mis en évidence le fait que les professionnels de la sécurité se trouvent « inefficaces, isolés et dans l'obscurité » lorsqu'ils font face aux cybermenaces. Après avoir interrogés 4 880 professionnels expérimentés de la sécurité informatique provenant de 15 pays, le rapport a découvert :

- un déficit dans l'efficacité des solutions en matière de sécurité;
- un décalage entre les dirigeants de l'entreprise et la valeur perçue de la perte des données ;
- une visibilité limitée dans les activités cybercriminelles.

De plus, le panel a avancé que près de la moitié des cadres dirigeants siégeant au conseil d'administration ont une faible compréhension de la question de sécurité. Mais le problème semble encore plus profond. Il faut réaliser que les départements informatiques ont également leur part de responsabilité dans cette déconnexion qui a pris de l'ampleur entre eux et le C.A.

Cette situation est imputable en partie à ce legs du temps où les dirigeants d'une société naviguaient pour la plupart en zone totalement inconnue en ce qui concerne l'informatique. Mais elle est également le résultat d'une impasse émotionnelle qui existe désormais entre les chefs de services informatique qui défendent ce qu'ils considèrent comme leurs fiefs personnels sans réaliser que la cybersécurité a des impacts à tous les niveaux des opérations de l'entreprise. Le cantonnement de la cybersécurité fait de cette manière peut cultiver la complaisance au sein des entreprises, berçant les dirigeants dans une douce illusion selon laquelle leurs cyberdéfenses sont impénétrables.

Une image plus réaliste serait pour le PDG de comprendre que son entreprise peut être piratée (si ce n'est pas déjà le cas). A moins qu'une entreprise n'effectue régulièrement des tests de pénétration sur ses défenses numériques, il est probable qu'une partie de ses données soit compromise à son insu.

Les départements informatiques peuvent penser à tort que la cybersécurité n'est qu'un problème qui relève de l'informatique, mais elle concerne en réalité d'autres domaines, y compris les ressources humaines. Plusieurs violations de données, par exemple, ne sont pas issues d'un piratage externe mais plutôt interne, parfois il s'agit de l'œuvre d'un employé mécontent ou malhonnête ou même d'un ancien employé. Des estimations avancent que près d'un ex-employé sur trois en Angleterre a encore accès à des données détenues par leur ancien employeur.

Aussi, la première mesure à prendre serait déjà de déterminer quelles données peuvent être compromises et par qui. Pour ce faire, les chefs d'entreprise pourraient appuyer des enquêtes menées en interne par les équipes informatique puisqu'elles ont la capacité de voir à leurs « angles morts ».

Parfois, un intrus peut avoir pénétré le système d'information d'une entreprise pendant des mois, voire des années, avant qu'elle n'en prenne conscience. Dans un tel cas de figure, les dégâts peuvent être difficiles à quantifier. Par exemple, s'il s'agit d'un concurrent, il peut avoir acquis des stratégies commerciales en examinant ses documents confidentiels quasiment en temps réel. S'il s'agit d'un cyber-pirate, il peut utiliser les informations obtenues pour détourner des fonds de l'entreprise. Quoiqu'il en soit, il existe des logiciels de prochaine génération qui permettent de retracer l'historique complète de chaque document, afin que l'entreprise puisse avoir connaissance de l'utilisation des données voire même de l'utilisateur.

Si aucune donnée sensible n'a été violée, il n'y a pas de raison de penser qu'elles ne le seront pas à l'avenir. Ce qui signifie qu'il faut développer une stratégie de gestion de crise afin de limiter les dommages qui pourraient être causés par une violation significative des données. Sans une stratégie efficace, il est possible de vous retrouver en train de payer des primes d'assurance voire perdre la confiance de vos partenaires et de vos clients.

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données personnelles, Denis JACOPINI est en mesure de prendre en charge, en tant qu'intervenant de confiance, externe à l'entreprise, la sensibilisation de vos salariés au risque informatique et à la cybercriminalité afin de les informer des risques, des conséquences et des bonnes pratiques de l'informatique au quotidien.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.developpez.com/actu/81729/Comment-les-entreprises-pourraient-elles-mieux-se-proteger-des-attaques-informatiques-de-plus-en-plus-sophistiquees/