Stopper les attaques informatiques avant qu’elles ne bloquent l’entreprise | Le Net Expert Informatique

Une récente étude de Gartner révèle que seulement 40 % des grandes organisations auront mis en place des plans de sécurité globaux afin de se prémunir contre les cyberattaques d'ici 2018. Cela signifie que 60 % des entreprises n'auront pas mis en place de stratégie d'ici trois ans, prenant un risque considérable face à des attaques de plus en plus sophistiquées qui pourraient atteindre un niveau supérieur au cours des prochaines années. Il ressort notamment de ce rapport que la priorité serait donnée à l'adoption de solutions de détection des attaques de manière réactive plutôt que proactive. Jean-François Pruvot, Regional Director France chez CyberArk, nous livre son analyse.

A l'heure où les cyberattaques sont de plus en plus nuisibles, les entreprises qui stockent des données sensibles figurent parmi les principales cibles. Le fait que la plupart des sociétés n'aient pas prévu de stratégie globale de sécurité d'ici à trois ans, et ce malgré les récentes attaques perpétrées contre de grands noms, témoigne souvent d'un manque de connaissances sur la manière de hiérarchiser les priorités dans le cadre de leurs programmes de sécurité ; cela laisse présumer que le hacker se trouve déjà à l'intérieur du réseau. Selon le général chinois Sun Tzu, dans son traité de stratégie militaire « L'art de la guerre », le succès de celle-ci repose sur la préparation mais également sur une bonne connaissance du terrain. Les entreprises doivent donc impérativement identifier l'ensemble des portes permettant d'accéder au « royaume IT », en particulier les comptes administrateurs ou à hauts pouvoirs qui conduisent à l'intégralité du système et des données qu'il renferme ; il est en effet impossible de protéger un espace sans connaître son étendue et ce qu'il contient.

La mise en place d'une stratégie globale de sécurisation de ces comptes et des systèmes d'information est donc indispensable pour limiter les vols et pertes de données, et se fait en plusieurs étapes clés.

Tout d'abord, partant du constat que la menace est peut-être déjà à l'intérieur, les RSSI doivent s'équiper d'outils de détection d'activités inhabituelles dans leurs systèmes. Cela leur permettra de contenir les menaces et de se prémunir contre l'infiltration progressive et malveillante de hackers dans le réseau en stoppant leur déplacement latéral. Une fois que les mesures de sécurité sont prises pour protéger les données, les comptes à privilèges difficilement détectables restent l'accès principal aux informations pour les pirates. Il est par exemple possible de les contourner pour pénétrer dans le système à l'aide de techniques de phishing classiques ; une fois à l'intérieur, le hacker peut s'y déplacer insidieusement et y installer des logiciels malveillants qui lui permettront de collecter autant de données que nécessaires sur des périodes pouvant se compter en années, et ce sans être détecté. Les comptes à hauts-pouvoirs qui ne sont pas suivis, gérés et protégés sont en effet l'une des vulnérabilités les plus répandues dans le cas de cyberattaques.

Enfin, une fois la stratégie établie, bien qu'il ne faille pas négliger la faille humaine, il est essentiel aujourd'hui que les entreprises ne se réfugient plus derrière cette excuse pour justifier les faiblesses des systèmes. En effet, que la menace vienne de l'intérieur ou de l'extérieur, les conséquences sont les mêmes pour les entreprises encore nombreuses à ne pas posséder les bases pour sécuriser leurs données ; elles doivent en effet commencer par mettre en place des correctifs, assurer leur mise à jour régulière, et surtout veiller au renforcement des contrôles sur les comptes à privilèges et administrateurs. Il est donc essentiel d'anticiper la présence de l'ennemi dans l'organisation et d'adopter ainsi une posture de gestion des risques concentrée sur la proactivité.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.infodsi.com/articles/158490/gestion-risques-stopper-attaques-avant-bloquent-entreprise.html