Cybercriminalité : ne laissez pas les hackers faire la loi | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LENETEXPERT.fr | RGPD CYBER LE NET EXPERT MISES EN CONFORMITÉ | SPY DETECTION Services de détection de logiciels espions | LE NET EXPERT FORMATIONS | LE NET EXPERT ARNAQUES & PIRATAGES

Le Net Expert INFORMATIQUE
Protection des données personnelles
Sécurité Informatique - Cybercriminalité

vous informe...

Cybercriminalité : ne laissez pas les hackers faire la loi

Sécurité ne veut pas dire complexité. Il vaut mieux déployer des outils basiques, que pas d'outil du tout. Il faut également changer la façon d'appréhender la sécurité. Par exemple, le RSSI ne doit pas être une fin en soi, mais le point de départ pour avoir un plan d'action efficace et les solutions adéquates. Il va également faire le lien entre vulnérabilité des systèmes et impact sur le business.

La bataille du hacking est de plus en plus féroce, mais avec les bons outils et quelques bonnes pratiques les entreprises peuvent gagner la guerre contre la cybercriminalité

C'est une réalité, nous ne pouvons pas éviter les failles de sécurité. Les cybercriminels développent sans cesse de nouveaux outils pour déjouer les mesures de sécurité mises en place par les départements informatiques des entreprises. Certains hackers vont même jusqu'à communiquer publiquement des informations sur la manière de hacker des données, banalisant ces pratiques hautement dangereuses pour les entreprises.

Dans ce contexte, les attaquants peuvent tenter et retenter de s'introduire dans les dispositifs de sécurité de l'entreprise et indiquer à leurs pairs ce qui a fonctionné ou non, jusqu'au jour où ils arriveront à leurs fins. Ce n'est, en effet, qu'une question de temps et de patience, des ressources qui font rarement défaut aux hackers.

Les RSSI : un point de départ et non une finalité en soi

Bien que les risques d'attaques cybercriminelles soient de plus en plus nombreux et les hackers de plus en plus doués pour détourner les systèmes de sécurité, il est toujours mieux d'avoir une politique de sécurité, même basique, que pas de protection du tout ! Cette affirmation semble évidente, mais aujourd'hui nombreuses sont les entreprises qui ne possèdent toujours aucune solution ou politique pour protéger leur organisation.

Embaucher un responsable de la sécurité informatique (SSI – Responsable de la Sécurité des Systèmes d'Information) représente déjà un grand pas pour une entreprise. Ce référent sécurité tranquillise les actionnaires et témoigne d'une réelle volonté de mettre la sécurité informatique dans la liste des priorités de l'entreprise.

Loin d'être une mesure suffisante en elle-même, cette mesure doit être la première brique pour poser les fondations d'un système de protection durable, résistant et évolutif. Les hackers tenteront, encore et encore, à chercher une faille de sécurité… jusqu'à ce qu'ils la trouvent ! Et tel est précisément le problème : une équipe de sécurité doit réussir chaque jour à maintenir les mauvais éléments à l'écart. Un attaquant, lui, ne doit réussir qu'une seule fois.

Traduire les problématiques techniques pour qu'elles parlent aux métiers

En réalité, les entreprises ont besoin d'un responsable de la sécurité qui soit capable de communiquer aussi bien sur l'impact économique que sur les implications des choix organisationnels en matière de sécurité et de technologie. Les responsables de la sécurité ont trop souvent tendance à se lancer dans des discussions hautement techniques et aborder des sujets difficiles à appréhender pour la plupart des dirigeants.

Pour accomplir leur mission et avoir un véritable impact sur l'activité, les responsables de la sécurité à tous les niveaux, soutenus par l'industrie de la sécurité, doivent être en mesure de transposer les conversations techniques sur les vulnérabilités du réseau en une discussion sur les coûts ou les opportunités pour l'entreprise proprement dite. Une fois ce pas franchi, l'entreprise peut prendre des décisions fondées concernant l'impact de ses choix.

Une nouvelle définition de la notion sécurité

Les outils proposés par les éditeurs assurent un certain degré de protection contre les pirates. Les solutions technologiques constituent le socle de la sécurité informatique en entreprise et se doivent donc d'être adaptées aux différents défis auxquels l'entreprise peut être potentiellement exposée. De nos jours, il ne s'agit cependant plus de s'attendre à ce que les logiciels soient des remèdes miracles contre les attaquants.

Il s'agit bel et bien d'améliorer les pratiques de sécurité et de permettre aux équipes qui en sont chargées de s'investir dans la mise en œuvre de procédures abouties. Aucun dispositif de sécurité n'est inviolable, c'est un fait. Il faut cependant se poser les bonnes questions, voire LA bonne question : « Parmi ce que nous surveillons déjà, que pouvons-nous utiliser pour réduire le risque à l'égard de notre activité ? »

Dans la plupart des cas, la clé réside dans une meilleure exploitation des outils existants et non dans l'acquisition de nouveaux outils, un message qui réjouira toujours le conseil d'administration. Le plus gros défi n'est pas nécessairement d'accroître la sécurité, mais de la rendre plus intelligente.

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : http://www.lesechos.fr/idees-debats/cercle/cercle-119704-cybercriminalite-ne-laissez-pas-les-hackers-faire-la-loi-1072763.php