Les bonnes pratiques pour lutter contre la cybercriminalité

Les bonnes pratiques pour lutter contre la cybercriminalité

Les entreprises modernes sont très vite confrontées aux dangers que représente un modèle commercial actif en permanence. Les clients ont de plus en plus recours à des outils en ligne pour accéder à des comptes, à des services ou à de l'expertise.

Quant aux employés, ils souhaitent pouvoir se connecter à distance et à tout moment aux réseaux de leur entreprise. D'où l'aspiration à un accès quotidien plus simple et plus pratique. Mais cette souplesse a aussi son revers. Les hackers, qui l'ont également bien compris, créent par conséquent des virus et des logiciels malveillants, dans l'unique intention de nuire. À la lumière des récentes révélations de l'organisme britannique Office for National Statistics selon lequel plus de 5,8 millions d'incidents de cybercriminalité ont eu lieu l'an dernier, il est crucial que les entreprises protègent les données de leur personnel et de leurs clients contre la cybercriminalité.
Dans ce contexte, quelles sont les principales activités de cybercriminalité dont les entreprises ont à se prémunir, et que faire pour les combattre ?

La manipulation sociale (Social engineering)
A l'ère du numérique, les pratiques de manipulation sociale sont devenues un problème préoccupant. Du fait que l'internet offre aux fraudeurs un voile d'anonymat, il est important que les sociétés qui détiennent des données clients sensibles soient au courant des pratiques les plus répandues parmi les hackers qui utilisent la manipulation sociale.
Le phishing aussi appelé hameçonnage, est peut-être la forme la plus connue de piratage de fraude par abus de confiance. Il recouvre les tentatives de fraudeurs qui généralement déploient de multiples moyens pour acquérir des données sensibles telles que les noms d'utilisateur, les mots de passe et les détails de paiement en se faisant passer pour une personne connue ou des organismes de confiance par courrier électronique ou une autre forme de communication numérique. Récemment, les cas de hameçonnage beaucoup plus ciblé, où les hackers se présentent comme des personnes de confiance, sont à la hausse. En cas de succès de l'attaque, les données des clients ou les documents sensibles d'une entreprise et donc sa réputation – sont en danger.
En effet, la recherche par Get Safe Online indique que la fraude liée au phishing a contribué aux organisations britanniques qui ont perdu plus de 1 milliard de livres sterling au cours de la dernière année en raison de la cybercriminalité.
Selon l'enquête, réalisée avec Opinion Way et dévoilée en exclusivité par Europe 1, 81% des sociétés française ont été ciblées par des pirates informatiques en 2015.
Le vishing et le smishing sont les variantes du phishing passant respectivement par les communications téléphoniques et SMS. Dans un cas comme dans l'autre, le principe est de récupérer les données sensibles de vos clients ou de votre entreprise. Compte tenu de l'impact dévastateur que peut avoir l'utilisation de la manipulation sociale par les cybercriminels sur les entreprises modernes, les dirigeants d'entreprise et les responsables informatiques doivent être très attentifs à ce type d'activités.

Menaces internes
A l'instar de la manipulation sociale qui peut porter préjudice aux entreprises de l'extérieur, il est légitime de se méfier également des menaces internes. Votre personnel peut disposer de privilèges d'accès aux données sensibles et en faire usage pour nuire à votre entreprise. Les employés mis à l'écart, les prestataires présents ou le personnel de maintenance sur site pourraient également représenter un danger pour votre société.
Les problèmes posés par les activités malveillantes des initiés ne sont pas toujours visibles immédiatement mais ils ne sauraient pour autant être ignorés. Prenons le cas d'un employé qui vient d'être licencié ou de perdre son poste dans une entreprise pour une autre raison. Il est possible que cette décision provoque chez lui de la colère et l'amène à vouloir exprimer son ressentiment envers son ancienne société. S'il possède toujours les droits d'accès au stockage partagé ou à des documents, il a la possibilité de modifier, supprimer ou falsifier les données ultrasensibles. De même, un prestataire exerçant sur le site et auquel un mot de passe temporaire a été attribué sans restrictions pour une courte durée peut représenter un danger. Qu'il s'agisse de corruption ou de communication de données financières, d'informations clients ou bien de droits d'authentification, les agissements de tels escrocs peuvent faire des ravages sur les entreprises de toutes tailles.
Cependant, comme c'est le cas avec les dangers de la manipulation sociale, le fait de connaître et de mesurer la menace potentielle des initiés malveillants peut permettre de faire un grand pas en avant dans la prévention des activités de cybercriminalité visant les entreprises. Les responsables informatiques et les dirigeants d'entreprises doivent rester vigilants en accordant aux utilisateurs des droits d'accès limités à leurs besoins et se méfier des récentes évolutions des techniques frauduleuses pour protéger leur entreprise contre les intentions malveillantes des cybercriminels.

Comment riposter
La lutte contre la cybercriminalité devrait dominer les débats et les plans stratégiques des dirigeants d'entreprise dans les années à venir. Pour optimiser leurs chances de l'emporter, les entreprises peuvent prendre plusieurs mesures.
1. Abandonnez la technique des mots de passe, trop simple, au profit d'un système d'authentification forte en entreprise : Les hackers qui dérobent le nom d'utilisateur et le mot de passe d'un employé peuvent la plupart du temps parcourir le réseau sans être repérés et charger des programmes malveillants ou bien voler ou enregistrer des données. Pour protéger les systèmes et les données, les entreprises ont besoin d'un système d'authentification forte qui ne repose pas exclusivement sur une information connue de l'utilisateur (mot de passe). Au moins un autre facteur d'authentification doit être utilisé, par exemple un élément que possède l'utilisateur (ex. un jeton d'ouverture de session informatique) et/ou qui le caractérise (ex. une solution d'identification biométrique ou comportementale). Il est également envisageable d'abandonner totalement les mots de passe et d'associer cartes, jetons ou biométrie.
2. Profitez de la commodité accrue d'un modèle d'authentification forte mobile : Les utilisateurs sont de plus en plus désireux d'une solution d'authentification plus rapide, plus transparente et plus pratique que celle offerte par les mots de passe à usage unique (OTP), les cartes d'affichage et autres dispositifs physiques. Désormais, les jetons mobiles peuvent figurer sur une même carte utilisée pour d'autres applications, ou être combinés sur un téléphone avec des dispositifs d'identification unique pour accéder à des applications cloud. Il suffit pour l'utilisateur de présenter sa carte ou son téléphone à une tablette, à un ordinateur portable ou à un autre périphérique pour s'authentifier sur un réseau, après quoi l'OTP devient inutilisable. Plus aucun jeton à mettre en place et à gérer. L'utilisateur final n'a qu'un seul dispositif à porter et n'a plus besoin de garder en mémoire ou de taper un mot de passe complexe.
3. Utilisez une stratégie de sécurité informatique par niveaux qui garantit des niveaux d'atténuation des risques appropriés : Pour une efficacité optimale, les entreprises ont intérêt à adopter une approche de la sécurité par niveaux, en commençant par authentifier l'utilisateur (employé, associé, client), puis en authentifiant le dispositif, en protégeant le navigateur et l'application, et enfin en authentifiant la transaction en recourant à l'intelligence basée sur les fichiers signatures si nécessaire. La mise en œuvre de ces niveaux nécessite une plateforme d'authentification polyvalente et intégrée dotée de moyens de détection des menaces en temps réel. Cette plateforme, associée à une solution antivirus, apporte le plus haut degré de sécurité possible face aux menaces actuelles.

Chip Epps est Vice President, Product Marketing, IAM Solutions de HID Global
…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Les bonnes pratiques pour lutter contre la cybercriminalité Chip Epps, HID Global*