Les plus grands risques de cybersécurité contre lesquels les propriétaires d'entreprises doivent se protéger

Devolutions

TOUT LE MONDE EST EXPOSÉ AUX CYBERMENACES

Vous pensez peut-être que seules les grandes entreprises doivent être vigilantes en matière de cybersécurité. Malheureusement, tout le monde est exposé aux cybermenaces. Voici donc certaines des plus grandes menaces contre lesquelles vous devriez protéger votre entreprise.

Rançongiciel

Un rançongiciel (ou ransomware en anglais), c'est l'équivalent numérique – vous l'aurez compris par son nom – d'une fraude où les hackers demandent une rançon. Une seule erreur de sécurité suffit pour que votre entreprise soit paralysée pendant des semaines alors que vous travaillez à trouver une solution à cette crise.

Le rançongiciel chiffre tous les fichiers sur vos serveurs et ordinateurs, vous empêchant de faire votre travail ou de récupérer les fichiers. Pour restaurer vos fichiers, vous devez payer les fraudeurs.

La version la plus célèbre d'attaques par rançongiciel, NotPetya, était une attaque organisée contre des entreprises essentielles à l'économie et aux infrastructures de l'Ukraine. Elle visait notamment les gares routières, les banques et les réseaux électriques. Les pirates informatiques moins ambitieux peuvent cibler des entreprises ou des ordinateurs privés dépourvus de mesures de sécurité suffisantes.

Les pirates peuvent entrer dans votre système si, par exemple, vous n'avez pas d'antivirus à jour ou si vous êtes victime d'une tentative d'hameçonnage.

Attaque d'un point d'extrémité

La tendance à utiliser son propre appareil (ordinateur, cellulaire, tablette, etc.) au travail présente des avantages, mais elle apporte également son lot de défis. En effet, il est beaucoup plus facile pour les pirates informatiques d'infiltrer le portable de l'employé que d'entrer dans un système fermé. Une fois que l'employé arrive au bureau et se connecte à vos serveurs, le virus peut se propager rapidement. C'est pourquoi il est primordial de sensibiliser vos employés sur les protocoles de sécurité s'ils apportent leurs propres appareils au travail.

Attaque d'un tiers

Vous êtes à l'affût des bonnes pratiques en cybersécurité et votre site web est bien protégé, mais ce n'est peut-être assez pour repousser les pirates informatiques. Un logiciel tiers peut constituer une faille permettant la propagation des logiciels malveillants. Si vous utilisez un plugiciel compromis ou si votre hôte n'est pas suffisamment sécurisé, il peut s'agir d'une porte d'entrée pour les logiciels malveillants.

Attaques de type cross-site scripting

Les attaques de type cross-site scripting (XSS) peuvent faire perdre à vos clients des informations privées et sensibles, par exemple des informations bancaires, tout en permettant aux pirates d'accéder au panneau d'administration de votre site web. Sur les deux fronts, c'est mauvais pour les affaires : il y aura un impact financier et un impact sur votre réputation. En nettoyant les entrées sur votre site web et en vous assurant que la sortie soit chiffrée, vous empêcherez la plupart des attaques XSS.

Piratage des banques de données

Plus tôt cette année, Facebook, le plus grand réseau social de la planète, avait été assez négligent pour laisser plusieurs gigantesques bases de données sans protection par mot de passe, provoquant la fuite des informations personnelles de plus de 400 millions d'utilisateurs. Même si votre organisation n'est peut-être pas si négligente, une mauvaise protection de la base de données peut amener des tiers à accéder à des données extrêmement sensibles.

Après un tel incident, il peut être difficile de rebâtir une réputation et réparer les dommages causés à votre entreprise. « Nos serveurs hébergent des informations qui, si elles sont publiées, peuvent être dévastatrices pour la carrière de nos clients. C'est la raison pour laquelle nous nous assurons de toujours disposer d'une sauvegarde et de chiffrer les données sensibles des utilisateurs afin d'empêcher les pirates d'y accéder », a affirmé Jessica Neilsen, PDG de l'agence de rédaction professionnelle Essay Writer.

Créer un mot de passe fort qui ne soit pas une date ou le nom d'une personne, c'est également une bonne idée. Il faudrait mille ans pour déchiffrer un mot de passe composé de 8 chiffres et de lettres, et il n'est pas difficile de le créer.

Minage de cryptomonnaie

Ce type de menace (en anglais cryptojacking) n'est pas facile à reconnaître. Les pirates n'essaient pas d'avoir accès à votre base de données; ils veulent simplement utiliser les ressources de votre appareil pour miner de la cryptomonnaie.

Bien que cette menace puisse sembler inoffensive, miner de la cryptomonnaie requiert beaucoup d'énergie, ce qui peut, avec le temps, surcharger vos serveurs. Cela ralentira considérablement votre site web, ce qui entraînera une baisse des revenus au fur et à mesure que les pirates se graisseront la patte… sur votre dos.

Pour vous protéger contre cette menace, vous devez vous assurer que votre site web n'est pas une bonne cible pour l'injection SQL et informer vos employés du danger potentiel lié au minage de cryptomonnaie.

Hameçonnage

L'hameçonnage est l'une des techniques de piratage les plus anciennes et les plus efficaces. Il exploite l'humain (et ses erreurs), beaucoup moins fiable que n'importe quel code. La plupart des menaces figurant sur cette liste utilisent l'hameçonnage pour accéder à votre système. Il est donc essentiel de savoir comment prévenir les stratégies d'hameçonnage pour la sécurité de votre entreprise. La première chose que vous devriez expliquer à vos employés est de toujours savoir qui est derrière le courriel qu'ils ouvrent et qu'il ne faut jamais cliquer sur des liens ou ouvrir des fichiers suspects.

Menaces de l'intérieur

Vous serez peut-être surpris d'apprendre que la plupart des menaces à la sécurité proviennent de personnes en qui vous avez confiance, et non de pirates informatiques. Les anciens employés frustrés, les employés actuels aux intentions malveillantes ou les employés dont le portable personnel est piraté peuvent s'avérer aussi dangereux qu'une mauvaise protection de votre site web.

Cela signifie qu'un gestionnaire que vous venez d'embaucher ou un ingénieur en logiciel que vous avez licencié peut, volontairement ou involontairement (c'est-à-dire par négligence ou par ignorance), conduire votre entreprise à une crise de sécurité. Vous devez travailler sur les procédures d'intégration et de désaffectation de vos employés pour vous assurer que votre personnel ne se transforme pas en menace pour la sécurité.

Conclusion

Les risques de cybersécurité sont très réels, que vous possédiez une petite ou une grande entreprise. Protégez-vous des menaces décrites dans cet article et vous limiterez la majorité des risques liés au web.