LUTTE CONTRE LES RANÇONGICIELS :

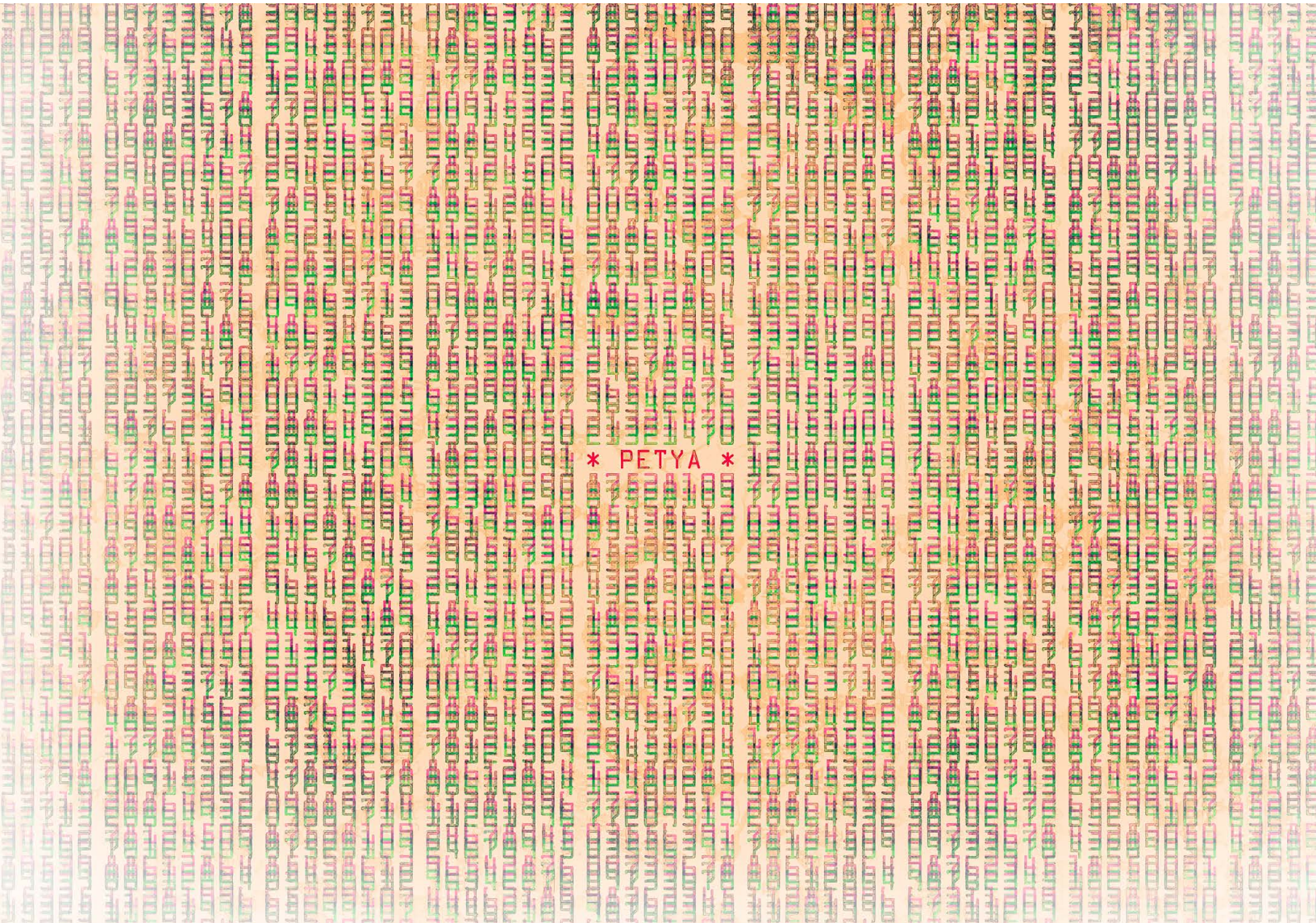
Stratégies pour protéger votre **entreprise** et vos **clients**

CYBERSCOUT® | Northbridge® Assurance

Voici la dure vérité à laquelle tout propriétaire d'entreprise doit faire face : si vous utilisez des ordinateurs, vous pouvez être la cible d'un rançongiciel, c'est-à-dire un type de maliciel qui chiffre les fichiers et dont se sert un malfaiteur pour ensuite exiger une rançon contre la clé de déchiffrement. Lorsqu'un tel type d'attaque frappe votre système, vos données et votre entreprise sont à la merci des pirates informatiques, et vous vous trouverez bien souvent démuni jusqu'à ce que vous payiez la rançon.

La mauvaise nouvelle est que les crimes liés aux rançongiciels sont en hausse. Les pirates lancent davantage d'attaques de plus en plus sophistiquées et exigent des rançons plus élevées sans garantir qu'ils retourneront les données volées. Qu'arriverait-il à votre entreprise si vos données confidentielles étaient volées contre rançon? La triste réalité est que bon nombre d'entreprises seraient en grande difficulté.

En ce qui a trait aux rançongiciels, la prévention est la clé. En effet, le montant que vous seriez prêt à verser pour acquitter une rançon est probablement beaucoup plus élevé que l'investissement nécessaire à la mise en œuvre de mesures de prévention. Grâce au présent document technique et à nos programmes de cybersécurité personnalisés, vous pourrez peaufiner votre stratégie et mettre en place un plan d'action, ce qui contribuera à protéger votre entreprise contre les rançongiciels.



Vous êtes peut-être vulnérable, mais pas sans défense

Un rançongiciel peut être beaucoup plus néfaste que vous ne le croyez, puisque vos données sont au cœur de vos activités quotidiennes. Vous n'êtes pas certain de l'incidence d'une attaque sur votre entreprise?

Posez-vous les questions suivantes :

- Quelles seraient les répercussions sur vos relations avec les clients si vous deviez obtenir d'eux des copies de leurs données après une attaque par rançongiciel?
- Combien de temps votre entreprise pourrait-elle payer ses coûts d'exploitation en l'absence de revenus?
- Connaissez-vous les pratiques exemplaires à adopter pour protéger votre entreprise contre les rançongiciels et pour se rétablir après coup?

Les enjeux sont importants lorsque vous stockez des données; une seule atteinte peut entraîner des conséquences immédiates et durables. Heureusement, un plan d'action bien élaboré peut vous aider à vous remettre sur pied quelques heures après un incident.

La clé est d'élaborer un plan d'intervention complet et adapté aux besoins particuliers de votre entreprise. Voici les éléments principaux sur lesquels devrait être axé votre plan :

- **Formation des employés.** Encouragez vos employés à détecter et à déjouer les attaques criminelles, même si elles deviennent de plus en plus sophistiquées.
- **Processus d'audit.** Assurez-vous que votre plan de reprise est prêt à être utilisé par votre équipe d'intervention afin qu'elle puisse agir rapidement.
- **Recommandations technologiques.** Optimisez votre infrastructure informatique pour détecter et éliminer le plus de tentatives d'attaque possible.
- **Faites régulièrement des copies de sécurité.** Protégez vos données en en faisant régulièrement des copies de sécurité et en mettant leur intégrité à l'essai périodiquement.

Les menaces à la sécurité constantes et de plus en plus répandues dans le paysage numérique actuel signifient que vous devez vous concentrer sur votre plan d'intervention et être vigilant dans vos recherches. En restant au fait des tendances en matière de cybercriminalité et en sachant pourquoi et comment les criminels choisissent leurs moyens d'attaque, vous pourrez focaliser votre attention aux bons endroits et éviter une catastrophe financière.

En restant au fait des tendances en matière de cybercriminalité et en sachant pourquoi et comment les criminels choisissent leurs moyens d'attaque, vous pourrez focaliser votre attention aux bons endroits et éviter une catastrophe financière.

Profits élevés et faibles risques : voilà pourquoi les criminels aiment les rançongiciels

Puisqu'ils sont faciles à exécuter et rentables instantanément, les rançongiciels sont devenus les chouchous des pirates informatiques. Sur la scène commerciale, les attaques par rançongiciels se sont accrues dans les dernières années et, maintenant, elles semblent être devenues les moyens privilégiés de générer des revenus dans le Web invisible. Plusieurs raisons expliquent cette hausse de la popularité des rançongiciels.

En voici quelques-unes :

1. Efficacité

Chaque entreprise possède des renseignements particuliers qui sont essentiels à ses activités. L'incapacité d'accéder à ses données, l'interruption des activités rentables régulières qui s'ensuit et les dommages potentiels à sa réputation sont tous des facteurs qui incitent une entreprise à payer une rançon.

2. Faibles risques.

La plupart des rançons sont réclamées en cryptomonnaie, par exemple le bitcoin, les rendant ainsi impossibles à retracer.

De plus, il n'est pas nécessaire de vendre les données sur le marché noir pour réaliser un bénéfice : il suffit de réclamer la rançon directement à la victime. Les étapes et les interactions moins nombreuses réduisent la possibilité que les criminels se fassent prendre.

3. Facilité d'envoi.

Plus de 97 pour cent des courriels hameçons contiennent un rançongiciel. Le rançongiciel est conçu pour s'infiltrer dans l'ordinateur d'un utilisateur si celui-ci ouvre les pièces jointes ou les liens malveillants inclus dans un courriel.

4. Rentabilité.

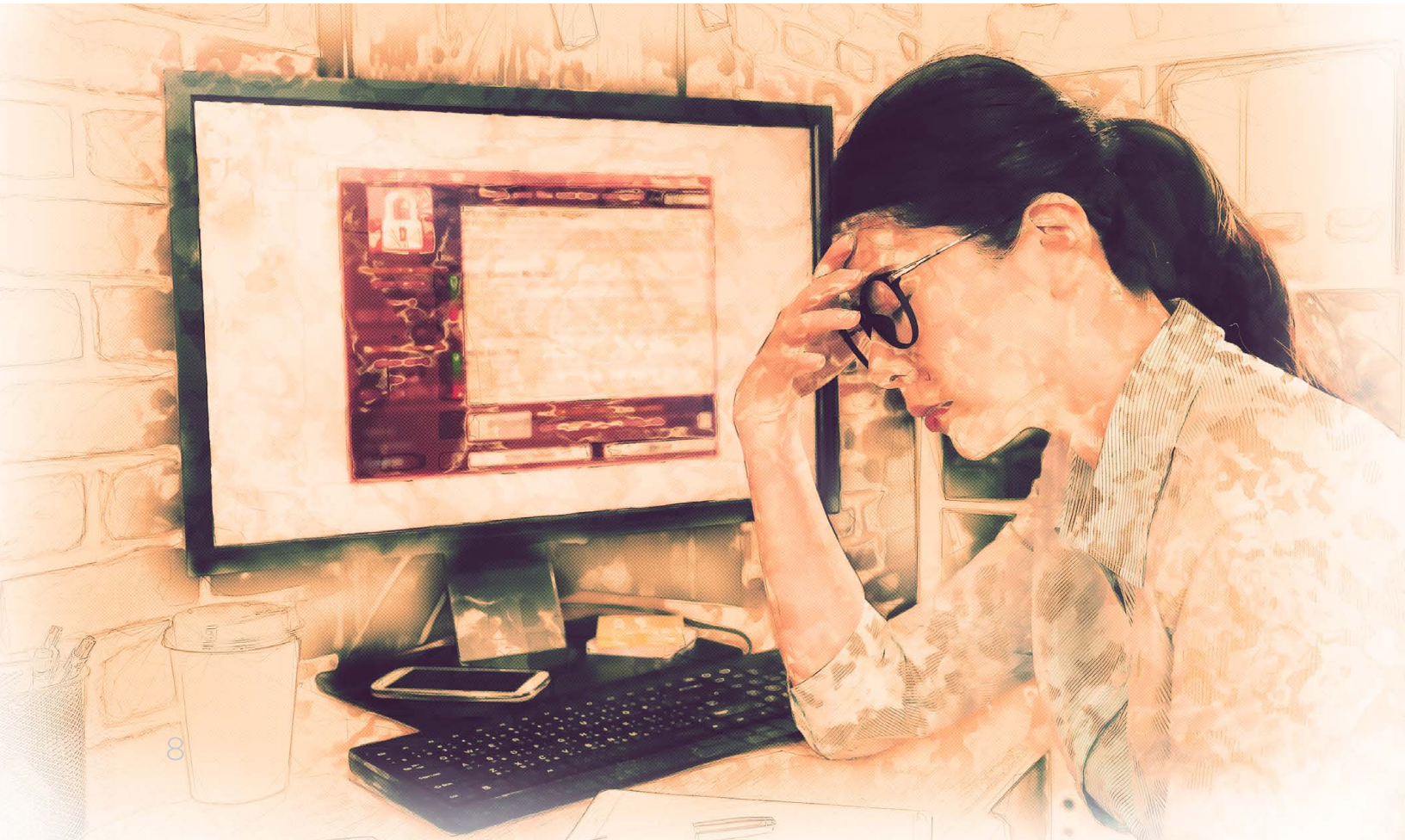
Le facteur de motivation le plus important est peut-être aussi le plus simple : les rançongiciels requièrent peu d'investissement de la part des criminels, mais peuvent toutefois générer de façon continue des montants d'argent considérables.

Plus de
97 pour cent
des courriels hameçons
contiennent un
rançongiciel.

Les escroqueries par rançongiciel évoluent (et rapidement)

Les profits générés par un rançongiciel peuvent varier selon la portée et l'intensité de l'attaque; cependant, des incidents récents ont révélé des résultats surprenants. L'attaque WannaCry survenue en 2017 a eu des effets désastreux partout dans le monde. Certains experts en évaluent les pertes financières éventuelles à 53 milliards de dollars américains.

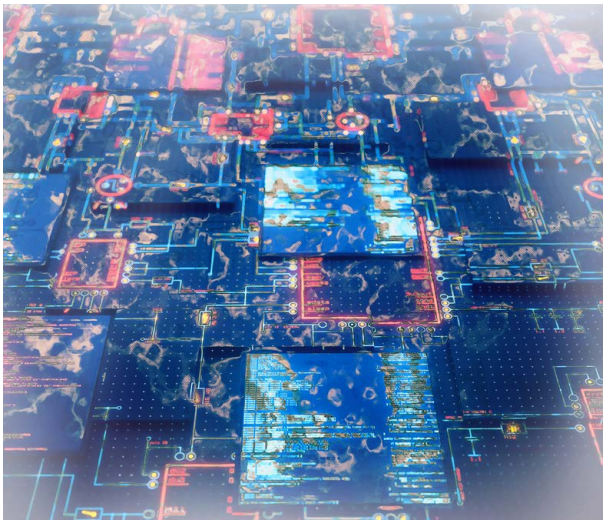
En fait, 35 % des dirigeants d'entreprise qui ont été confrontés à une attaque par rançongiciel révèlent que leur entreprise a finalement payé la rançon, et 20 pour cent de l'ensemble de ces entreprises ont versé plus de 40 000 $. En raison d'un faible nombre d'obstacles à l'accès aux données et des profits potentiels, les pirates informatiques utilisent de plus en plus les rançongiciels auprès des entreprises. En effet, ce type d'attaque a augmenté de 36 pour cent entre 2015 et 2016.



Les profits élevés générés par les premières versions de rançongiciels ont encouragé les pirates à investir dans des méthodes plus sophistiquées et incité d'autres personnes à se joindre à eux. De nos jours, les criminels sans compétence en informatique peuvent se tourner vers des plateformes Ransomware-as-a-service (RaaS) pour louer un logiciel malveillant moyennant un montant fixe.

Certaines versions de RaaS sont facilement déchiffrées, mais d'autres sont plus complexes, et les réseaux informatiques vieillissants pourraient ne pas faire le poids contre les plus récents maliciels.

Votre meilleure défense? Mettre à niveau votre système et vos pratiques en matière de protection des données pour mieux protéger votre entreprise contre la menace grandissante des rançongiciels.



Certaines versions de RaaS sont facilement déchiffrées, mais d'autres sont plus complexes, et les réseaux informatiques vieillissants pourraient ne pas faire le poids contre les plus récents maliciels.

Stratégies pour contourner les attaques par rançongiciel

La menace peut faire peur, mais il existe des méthodes éprouvées pour vous aider à protéger vos données. **Vos mesures de prévention devraient inclure les trois stratégies complémentaires suivantes :**

1. Encouragez les employés à détecter et à déjouer les tentatives d'attaques par rançongiciel.
2. Optimisez votre infrastructure informatique pour détecter et éliminer automatiquement les attaques par rançongiciel.
3. Passez en revue votre plan d'intervention en cas d'attaque réussie et mettez-le à l'essai.

Voici des pratiques exemplaires qui tiennent compte de ces stratégies et qui pourront vous aider à élaborer un plan de protection solide contre les cyberattaques.

Faites régulièrement des copies de sécurité de vos données

Si vos données sont chiffrées par une tierce partie, vos copies de sécurité seront peut-être le seul moyen de les récupérer. Vous devrez établir la plus grande période de temps sans sauvegarde avec laquelle vous êtes à l'aise et, ensuite, sauvegarder vos données en conséquence. Alors, si vous ne voulez pas perdre plus d'une journée de données, faites des copies de sécurité toutes les 24 heures; c'est aussi simple que cela.

Protégez vos copies de sécurité en vous assurant qu'elles ne sont pas reliées ni aux ordinateurs ni aux réseaux qui contiennent les données copiées. Par exemple, vous pouvez les stocker dans le nuage ou dans un centre de données. Notez toutefois que certains rançongiciels peuvent s'infiltrer dans une plateforme de sauvegarde infonuagique si le système est configuré de façon à effectuer des copies de sécurité en continu. Communiquez donc avec votre fournisseur pour savoir comment il s'y prend pour atténuer ce risque.

Vous devez non seulement faire des copies de sécurité de vos données, mais aussi avoir la certitude qu'elles fonctionneront comme prévu. Mettez donc à l'essai l'intégrité de vos copies de sécurité de façon périodique afin de vous assurer de pouvoir vous y fier lorsque vous en aurez besoin.

Concentrez-vous sur la sensibilisation et la formation

La majorité des attaques par rançongiciel réussissent à duper les utilisateurs en les incitant à cliquer sur les pièces jointes et les liens malveillants inclus dans un courriel. Montrez à vos employés comment reconnaître les courriels hameçons; rappelez-leur d'éviter de cliquer sur des bannières ou des liens sans en connaître la nature, la destination et la provenance; et dites-leur de visiter seulement des sites fiables. Il est essentiel que les membres de votre équipe soient sur la même longueur d'onde en ce qui concerne les pratiques exemplaires de sécurité informatique.

Si vous proposez un bulletin d'information à vos employés ou à vos clients, faites-leur part des plus récents types d'attaques par rançongiciel. Même si une infime partie de votre personnel est informé des menaces actuelles, cela pourrait être suffisant pour éviter une attaque dévastatrice.

Utilisez des logiciels anti-programmes malveillants de dernière génération

Dans certains cas, ces types de programmes peuvent détecter un rançongiciel avant qu'il n'arrive dans votre système. Assurez-vous que ces programmes sont mis à niveau automatiquement et qu'ils effectuent des analyses régulièrement.

Gardez vos logiciels à jour

Moins vous avez de bogues, plus il sera difficile d'infecter votre système. Mettez à jour tous vos systèmes d'exploitation périphériques, vos logiciels et vos micrologiciels à mesure que des failles sont découvertes, y compris Adobe Flash, Java et certains navigateurs Web. Pour y arriver facilement, vous pouvez utiliser un système de gestion des correctifs centralisés.

Mettez en place des normes de protection en matière de technologies de l'information (TI)

Votre équipe des TI est une première ligne de défense importante. Voici quelques mesures que peuvent prendre vos experts en TI pour contribuer à protéger votre entreprise :

- Autoriser les systèmes à exécuter seulement les programmes connus et conformes à la politique de sécurité.
- Éviter que les programmes ne s'exécutent dans des emplacements où les rançongiciels s'infiltrent souvent, comme des fichiers temporaires contenant des navigateurs Web populaires ou des programmes de compression/décompression, y compris ceux situés dans le dossier AppData/LocalAppData.
- Désactiver les macros dans les documents envoyés par courriel. Si possible, utiliser la suite Microsoft Office.
- Utiliser un logiciel de visionnement pour ouvrir les documents de la suite Office envoyés par courriel plutôt que les logiciels de la suite Microsoft Office.
- Catégoriser et segmenter les données selon leur valeur et leur utilité. Par exemple, les données de recherche de nature délicate ou les données de l'entreprise ne devraient pas être stockées sur le même serveur ou le même segment de serveur que celui d'un environnement de courrier électronique. Configurer les pare-feu afin qu'ils bloquent l'accès aux adresses IP malveillantes.
- Désactiver le protocole d'accès à distance (Remote Desktop Protocol ou RDP) s'il n'est pas utilisé.
- S'assurer qu'un virus ne peut s'infiltrer dans aucun lecteur mappé. Certains types de rançongiciels, comme VirLock et Locky, peuvent accéder aux lecteurs réseau partagés et les chiffrer, permettant ainsi au virus de se propager à l'échelle de l'entreprise.
- Resserrer la politique en matière de courriels. Renforcer les filtres antipourriels pour éviter que des courriels hameçons et les fichiers exécutables n'atteignent les utilisateurs et pour authentifier les courriels entrants afin de prévenir l'usurpation par courriel.
- Mettre en place un programme de test de l'hameçonnage. Envoyer régulièrement des courriels hameçons factices aux employés. Voir combien d'entre eux se font prendre et se servir de ces résultats pour former les employés et leur rappeler la marche à suivre.

Élaboration d'un plan d'intervention

Il arrive qu'un rançongiciel perce les moyens de défense d'une entreprise; toutefois, il est possible de neutraliser une attaque ou d'en limiter les répercussions si vous agissez sur-le-champ.

Vous devriez avoir un plan d'intervention en place pour contribuer à limiter les dommages et tracer la voie vers un rétablissement rapide. Les 48 premières heures sont particulièrement importantes. C'est pourquoi nous présentons dans un autre document technique quelques mesures que vous pouvez prendre pour gérer ce problème : trouvez-les ici!

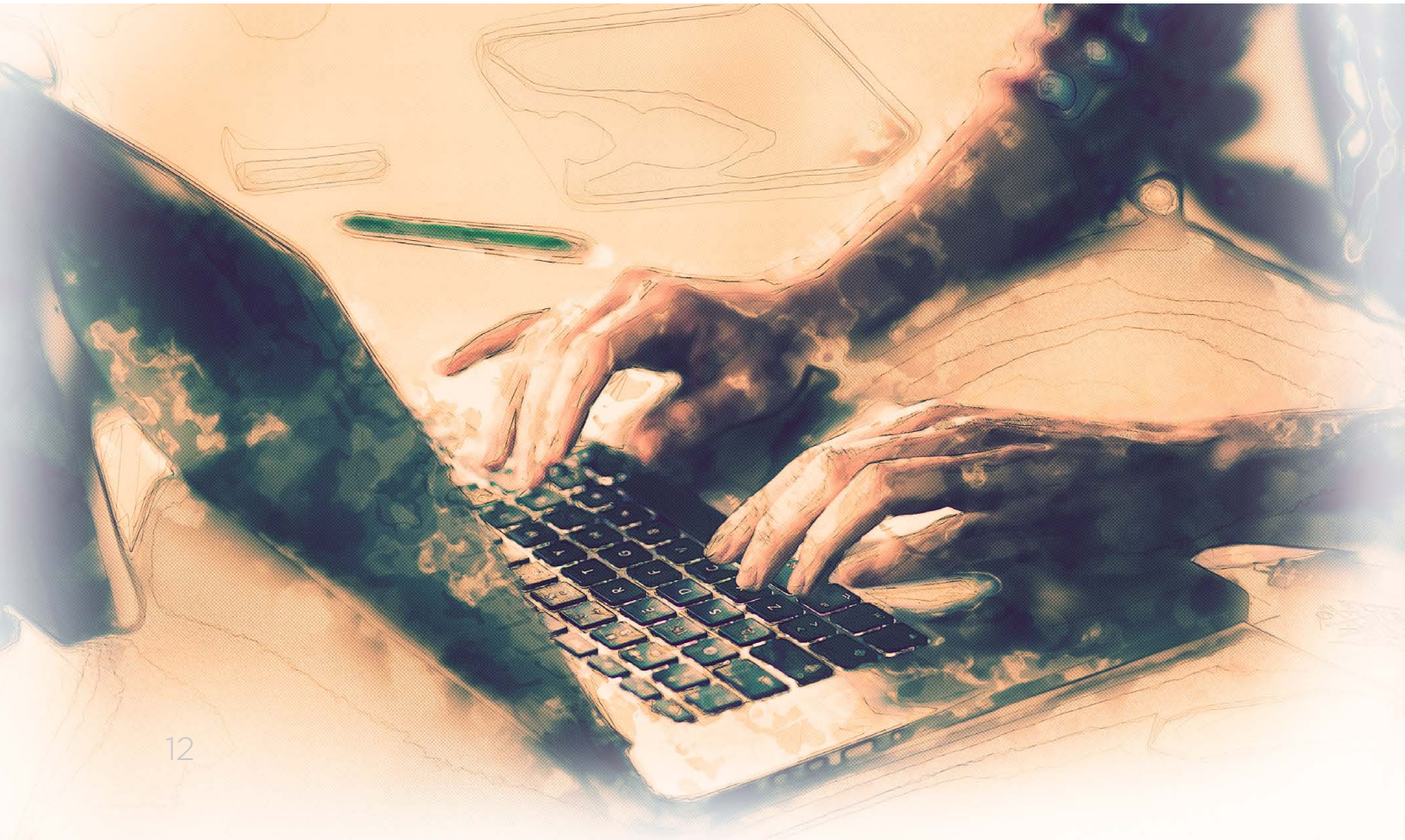
Comment faire pour reprendre le contrôle de la situation?

Vous devrez reprendre le contrôle de votre système aussitôt que possible. Effacez les disques durs, restaurez vos systèmes et téléchargez des versions propres de vos fichiers à partir d'une copie de sécurité non infectée. Enfin, effectuez une analyse antivirus.

Avec qui devriez-vous communiquer?

Selon la gravité de l'attaque et la taille de votre équipe d'experts internes, vous devrez peut-être faire appel aux entités suivantes :

- **Autorités policières.** Si les autorités policières doivent analyser vos ordinateurs ou vos serveurs, vous devrez peut-être vous procurer temporairement de l'espace serveur pour restaurer vos systèmes.



- **Fournisseurs de service.** Communiquez avec vos fournisseurs de services informatiques et de services de cybersécurité, le cas échéant.
- **Conseillers juridiques.** Les spécialistes en droit peuvent vous aider à établir si la protection des données a été compromise, et à prendre les mesures appropriées pour informer les parties touchées et remédier à la situation.
- **Votre assureur.** Votre assureur peut aller au-delà du simple traitement de votre demande de règlement. Vous devriez pouvoir compter sur lui pour vous aiguiller vers des conseillers juridiques ou en matière de violation des données, des professionnels spécialisés en TI et d'autres experts qui vous aideront à régler votre problème et à vous remettre sur pied.

Assurez-vous que votre plan d'intervention est plus qu'un simple exercice technique. Rappelez-vous que les administrateurs de réseau et les ingénieurs en logiciels n'ont pas la responsabilité de gérer les répercussions délicates et dispendieuses découlant de la résolution d'un problème informatique, comme aviser les clients et les employés conformément aux mandats juridiques ou communiquer avec les médias et les autorités policières. Veillez à avoir des experts dans chaque domaine.

Rappelez-vous que les administrateurs de réseau et les ingénieurs en logiciels n'ont pas la responsabilité de gérer les répercussions délicates et dispendieuses découlant de la résolution d'un problème informatique, comme aviser les clients et les employés conformément aux mandats juridiques ou communiquer avec les médias et les autorités policières.

Façons dont nous pouvons vous aider

Maintenant que vous savez tout le mal qu'un rançongiciel peut causer, et que la menace de ce genre d'attaques continuera sans doute de croître, vous pouvez mettre en place des mesures plus ciblées pour rester maître de la situation. Bien qu'il soit important de protéger votre entreprise autant que possible, la bonne assurance pourrait venir à votre rescousse si vos efforts ne s'avéraient pas suffisants.

Les assurances des cyberrisques ne sont pas toutes pareilles. En effet, sans un partenariat adapté à votre entreprise, vous pourriez devoir assumer les frais juridiques, les amendes, les coûts de réparation et les frais d'interruption des activités résultant d'un incident majeur. De plus, les rançongiciels étant devenus plus complexes et généralisés, une seule attaque du genre pourrait vous causer d'importants problèmes financiers.

En partenariat avec CyberScout, Northbridge Assurance a mis au point un programme d'assurance des cyberrisques complet et polyvalent. En plus de protéger vos finances en cas de violation des données, votre police vous donne accès à de vastes cyberressources préventives, à une aide réactive et à des conseils personnalisés pour veiller à ce que ce genre d'incident ne se reproduise jamais. Après tout, la gestion des risques s'exerce en continu, et Northbridge prend cette gestion très au sérieux, notamment en vous offrant des polices multirisques qui placent la réussite à long terme de votre entreprise au centre des priorités.

Northbridge Assurance | CYBERSCOUT®