Travailler ensemble
pour un monde meilleur

Comment protéger votre organisation contre les rançongiciels

Une stratégie de défense multidimensionnelle pour réduire le risque d'attaque par rançongiciel

Le nombre d'attaques réussies par rançongiciels a augmenté en 2019 et 2020, et cette tendance n'est pas près de s'arrêter. Des équipes d'EY ont analysé les méthodes courantes d'attaques par rançongiciel afin d'aider leurs clients à mieux prévenir ces attaques préjudiciables.

Il n'y a pas de produit ou de solution miracle capable de protéger entièrement une organisation contre les rançongiciels. Il n'est pas non plus possible d'esquisser une vaste stratégie de cyberdéfense en un seul document. Toutefois, les équipes d'EY peuvent passer en revue certains aspects bien précis ciblés par les attaquants dans le cadre de leur stratégie. Le présent document vise à établir des mesures de contrôle ou des pratiques de pointe qui, lorsque mises en œuvre, peuvent réduire le risque de réussite d'une attaque par rançongiciel contre votre organisation.

Contenu

Comment réduire les risques qu'un attaquant par rançongiciel accède à votre réseau

Les spécialistes en cybersécurité préconisent une approche multidimensionnelle (défense en profondeur) pour empêcher la réussite des attaques. Tous s'entendent pour dire que le renforcement de l'enveloppe externe est essentiel. Les organisations doivent réduire la surface d'attaque afin de devenir des cibles plus difficiles à exploiter. Il faut tenir compte des quatre volets ci-après.

1. Protégez-vous contre les menaces internes

Malgré tous les efforts que vous déployez pour renforcer l'enveloppe externe contre les menaces, votre travail n'est pas terminé tant que vous n'avez pas géré le risque lié à la cybersécurité le plus important pour une entreprise : le facteur humain. Les menaces internes ne sont pas toutes malveillantes. Les employés sont des êtres humains qui font des erreurs, malgré leurs efforts et leurs bonnes intentions. Les personnes mal intentionnées canalisent souvent leurs efforts pour hameçonner certains employés afin d'obtenir les justificatifs d'identité ou l'accès à un système nécessaire pour mener une attaque. Cette pratique a connu un plus grand succès au cours de la pandémie, alors que les attaquants ont commencé à exploiter l'anxiété suscitée par la COVID-19. Afin de réduire les possibilités de réussite des attaques par hameçonnage, mettez l'accent sur la formation et la mise à l'épreuve de vos employés.

- **Former le personnel.** Chaque année, procédez à une formation portant, au minimum, sur l'utilisation des ordinateurs, du courriel et d'Internet, ainsi que sur la manipulation et l'élimination des données, sur le signalement et le traitement des cyberincidents et sur d'autres règles de sécurité. Mettez régulièrement en œuvre des campagnes de sensibilisation à la sécurité à tous les échelons de votre entreprise afin d'intégrer la sécurité à votre culture organisationnelle. Ainsi, vos employés tiendront compte automatiquement de la sécurité dans chacune de leurs décisions, ce qui contribuera à assurer la sécurité de votre organisation.
- **Mettre à l'épreuve le personnel.** Mettez à l'épreuve vos employés de façon aléatoire, au moins tous les trimestres, afin de déterminer s'ils sont sensibles aux tentatives d'hameçonnage. Fournissez ressources et formations additionnelles aux employés qui ont des difficultés. Un test d'hameçonnage permet aux organisations d'envoyer à leurs employés un courriel qui semble réel, mais complètement faux, afin de mettre leurs utilisateurs à l'épreuve.
- **Mettre en œuvre une passerelle de messagerie électronique.** Déployez et configurez une passerelle de messagerie électronique pour analyser et bloquer les courriels malveillants, y compris les liens intégrés et les pièces jointes.
- **Mettre en œuvre un système de filtrage et de blocage des URL.** L'analyse et la notation du risque d'atteinte à la réputation peuvent réduire la probabilité de réussite des nombreuses tentatives d'hameçonnage et empêcher les liens malveillants de livrer leur charge et leur code d'exploitation.
- **Mettre en œuvre le SFP (Sender Policy Framework).** Réduisez les chances de courriels frauduleux en mettant en œuvre le SPF ou DMARC (Domain-based Message Authentication, Reporting, and Conformance). Reportez-vous à *CIS Control 7*[1] pour d'autres indications.

1 « Email and Web Browser Protections », site Web du Center for Internet Security, https://www.cisecurity.org/controls/email-and-web-browser-protections/, accédé le 25 juillet 2020.

Il n'existe aucun système de protection de réseau parfait. Les méthodes d'attaque changent constamment, tout comme les surfaces d'attaque, et il est pratiquement impossible d'éviter systématiquement toutes les possibilités d'infiltrations. Il importe que les organisations partent du principe qu'un attaquant parviendra à déjouer les meilleurs mécanismes de défense. Heureusement, il existe des mécanismes de contrôle internes supplémentaires qui peuvent compliquer la vie d'un attaquant, et même l'arrêter.

Les objectifs d'un attaquant consistent à obtenir le contrôle du mécanisme responsable de la persistance et à accroître les privilèges d'accès. Par nature, les rançongiciels ne se propagent pas par eux-mêmes. Les attaquants ont besoin d'un accès et d'un effet de levier importants afin de propager les rançongiciels dans l'environnement informatique. Si des attaquants obtiennent l'accès à des justificatifs d'identité d'administration d'un système ou, pire encore, à des justificatifs d'identité d'administration d'un domaine, ils ont, en règle générale, réussi leur intrusion.

Avec ces justificatifs d'identité, les attaquants peuvent utiliser votre infrastructure pour perturber en grande partie vos systèmes informatiques, notamment en tirant parti des répertoires et stratégies de groupe, afin de déployer leur rançongiciel. Les organisations doivent tout faire pour protéger les comptes privilégiés et les accès administrateurs dans leur environnement. Sans privilèges, les attaques sont moins susceptibles d'avoir une incidence sur l'ensemble de l'organisation.

Malheureusement, dans de nombreuses organisations, il est trop facile d'obtenir un accès privilégié. Les trois étapes suivantes limitent considérablement la possibilité qu'une attaque donne à son auteur des droits d'accès administrateurs.

De nouvelles vulnérabilités et menaces émergent constamment. En plus d'appliquer les recommandations fournies, les organisations devraient penser à mettre en place un plan exhaustif d'information sur les menaces de façon à identifier rapidement les nouvelles menaces.

2. Protégez les systèmes et les applications exposés

Les organisations doivent aussi penser à protéger les systèmes et applications exposés à l'externe et donc vulnérables. Les systèmes exposés à l'externe présentant des vulnérabilités ouvertes sont des cibles attrayantes et faciles à exploiter. Les groupes d'attaquants par rançongiciels continuent de viser les vulnérabilités non corrigées des applications et des systèmes, notamment dans Windows Shares (SMB) (CVE-2020-0796), PulseVPN (CVE-2019-11510), F5 Big IP (CVE-2020-5902), Palo Alto Global Protect (CVE-2020-2034) et Citrix NetScaler (CVE-2019-19781). De nouvelles vulnérabilités et menaces sont découvertes constamment. En plus d'appliquer les recommandations fournies, les organisations devraient penser à mettre en place d'un plan exhaustif d'information sur les menaces de façon à identifier rapidement les nouvelles menaces.

- **Établir des configurations sécurisées.** Établissez, mettez en œuvre et gérez une configuration sécurisée pour chaque système du réseau. En cas d'incertitude, le Center for Internet Security (*CIS Control 5*[2]) peut fournir des directives sur les meilleures pratiques.
- **Appliquer des contrôles d'accès.** Revoir régulièrement les contrôles d'accès et confirmer les accès appropriés aux applications et systèmes exposés au public, y compris les unités de stockage en nuage.
- **Rechercher des vulnérabilités sur les systèmes.** Au moins une fois par trimestre, réaliser un balayage de vulnérabilités sur les systèmes et applications, et remédier aux vulnérabilités graves.
- **Corriger les systèmes.** Vérifier que vous disposez d'un processus pour tenir à jour les logiciels et micrologiciels des systèmes et applications exposés (processus de gestion des correctifs). De nombreuses vulnérabilités restent ouvertes aux attaques parce que les organisations n'ont pas de processus de correction systématique.
- **Sécuriser Windows SMB.** Ne jamais exposer Windows SMB à Internet. Les attaquants peuvent facilement trouver des vulnérabilités et compromettre les systèmes sous Windows en déployant des maliciels dans les systèmes de votre réseau interne grâce à cette exposition.

2 « Secure configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers », site Web du Center for Internet Security, https://www.cisecurity.org/controls/secure- configuration-for-hardware-and-logiciels-on-mobile-devices-laptops-workstations-and-servers/, accédé le 25 juillet 2020.

3. Mettez en œuvre des solutions avancées de détection et interventions aux terminaux (EDR)

Les solutions avancées EDR font appel à des techniques proactives, comme l'apprentissage automatique et l'analyse comportementale pour identifier les menaces nouvelles ou complexes. Les solutions EDR permettent de détecter rapidement une attaque, d'en évaluer l'ampleur sur le réseau et d'isoler ou de mettre en quarantaine les systèmes touchés pour mettre fin à l'attaque. Ces techniques compliquent beaucoup la tâche des attaquants qui cherchent à s'installer dans votre réseau.

Quelle que soit la solution EDR retenue, envisagez fortement le déploiement de cette capacité sur tous les terminaux (systèmes d'utilisateurs finaux, serveurs, IdO).

- **Déployer l'EDR :** Déployez l'EDR sur l'ensemble des terminaux du réseau, en insistant sur les systèmes d'utilisateurs privilégiés et les infrastructures de serveurs. Travaillez avec le fournisseur retenu pour vous assurer que la solution EDR est configurée pour tirer pleinement avantage de ses capacités.

  Envisagez de mettre sur pied une équipe de surveillance de sécurité qui répondrait aux alertes EDR et qui serait chargée d'enquêter sur le trafic inhabituel et de mener une chasse proactive aux menaces afin de les détecter et d'y remédier plus rapidement. Cette équipe aiderait à protéger des actifs de l'organisation comme les données, les systèmes d'entreprise, la technologie opérationnelle et les marques.

  Dans l'impossibilité de faire appel à l'EDR (p. ex., systèmes de télésurveillance et d'acquisition de données [SCADA] et anciens systèmes), confirmez que ces systèmes sont isolés d'Internet et complètement séparés du reste du réseau. Quant aux technologies opérationnelles (TO), utilisez des diodes de données pour les communications à sens unique, comme pour la récupération de données et d'information sur des systèmes, appareils ou automates programmables industriels (API), et plus.

4. Sécurisez vos services réseau

L'une des méthodes les plus répandues pour obtenir l'accès à un environnement est d'exploiter des services réseau non sécurisés, particulièrement le protocole de bureau à distance (Remote Desktop Protocol ou RDP). Pour réduire le risque d'exposition attribuable aux services réseau non sécurisés, envisagez les étapes suivantes :

- **Désactiver les services superflus.** Réalisez une évaluation complète des systèmes exposés à l'extérieur, puis désactiver les services superflus et surveiller ceux qui restent.
- **Intégrer le renseignement sur les menaces.** Ayez recours au renseignement sur les menaces et priorisez les efforts de prévention et de détection. Utilisez des renseignements de fournisseurs pour prioriser l'identification et la correction des vulnérabilités communes. Mettez en œuvre les pratiques de pointe en matière de configuration de sécurité, améliorez les capacités de détection du centre d'opérations et de sécurité et augmentez la rigueur des évaluations internes et externes.

  Envisagez de mettre en place un portail de renseignement sur les menaces, qui se situe à l'extérieur de votre réseau et qui est mis à jour, parfois toutes les heures, avec des renseignements sur les adresses IP malicieuses et les domaines d'où proviennent de nombreuses attaques. Le portail bloque ensuite tout trafic entre votre réseau et ces sources malicieuses et élimine par le fait même les attaques qui pourraient provenir de ces sources.

Qu'arrive-t-il si un attaquant réussit à franchir mes lignes de défense extérieures?

- **Sécuriser les services de gestion à distance et RDP.** RDP a été conçu comme méthode de gestion facile des serveurs Microsoft Windows Servers à distance à partir d'un même réseau privé, et non sur Internet. Quand le RDP est exposé à Internet, les attaquants cherchent à l'exploiter, lui qui est souvent non sécurisé et négligé par les décideurs.

  Si vous utilisez RDP, ou tout autre service de gestion à distance, il faut le configurer pour qu'il se situe derrière une passerelle d'accès à distance ou un réseau privé virtuel (VPN), et préférablement mettre en place une authentification à deux facteurs. Limitez l'accès aux personnes qui en ont besoin et assurez une surveillance pour détecter des accès ou des comportements inhabituels.

Dans l'impossibilité de placer le RDP derrière une passerelle :

- Limitez l'accès à ceux qui en ont besoin
- Mettez en place une authentification solide, idéalement à deux facteurs
- Configurez-le pour une authentification à l'échelle du réseau, qui exige une authentification des utilisateurs avant qu'une session RDP puisse être établie
- Mettez en place le blocage de comptes pour limiter les attaques par force brute
- Limitez l'accès en établissant des règles de pare-feu qui ne permettent le RDP qu'à partir d'une liste d'adresse IP de confiance
- Mettez en place un processus de détection et interventions aux terminaux sur le serveur RDP et surveillez les connexions au moyen d'une solution de gestion des informations et des événements de sécurité (SIEM)

1. Identifiez les comptes privilégiés

Vous devez savoir qui peut accéder à quoi sur votre réseau. Déterminez où les droits d'administrateurs sont disponibles et identifiez les employés qui ont des accès administrateurs. Fouillez en profondeur. Il est facile d'oublier des privilèges administratifs sur des systèmes isolés, des appareils réseau, l'IdO ou d'autres systèmes. Il suffit d'un seul compte administrateur oublié, en configuration par défaut, ou toute autre forme de mot de passe faible, qu'un attaquant peut exploiter pour obtenir l'accès.

- Faites l'inventaire des systèmes sur votre réseau et identifiez les comptes administrateurs ou privilégiés
- Déterminez quelles personnes ont accès à chaque compte et demandez-vous si ces personnes en ont besoin pour faire leur travail.
- Déterminez la raison d'être de chaque compte de service, et demandez-vous quels services il exécute, à quels systèmes il a accès et à quelle fréquence il y a accès.
- Identifiez les mots de passe faibles et communs, et ceux qui sont partagés par plusieurs utilisateurs privilégiés et comptes de services. Changez les mots de passe pour qu'ils soient différents et plus complexes.

2. Adoptez une politique sur les comptes privilégiés

Une fois que vous avez identifié les accès administratifs et privilégiés de votre environnement et déterminé qui utilise ces accès, vous devez définir une politique pour votre organisation.

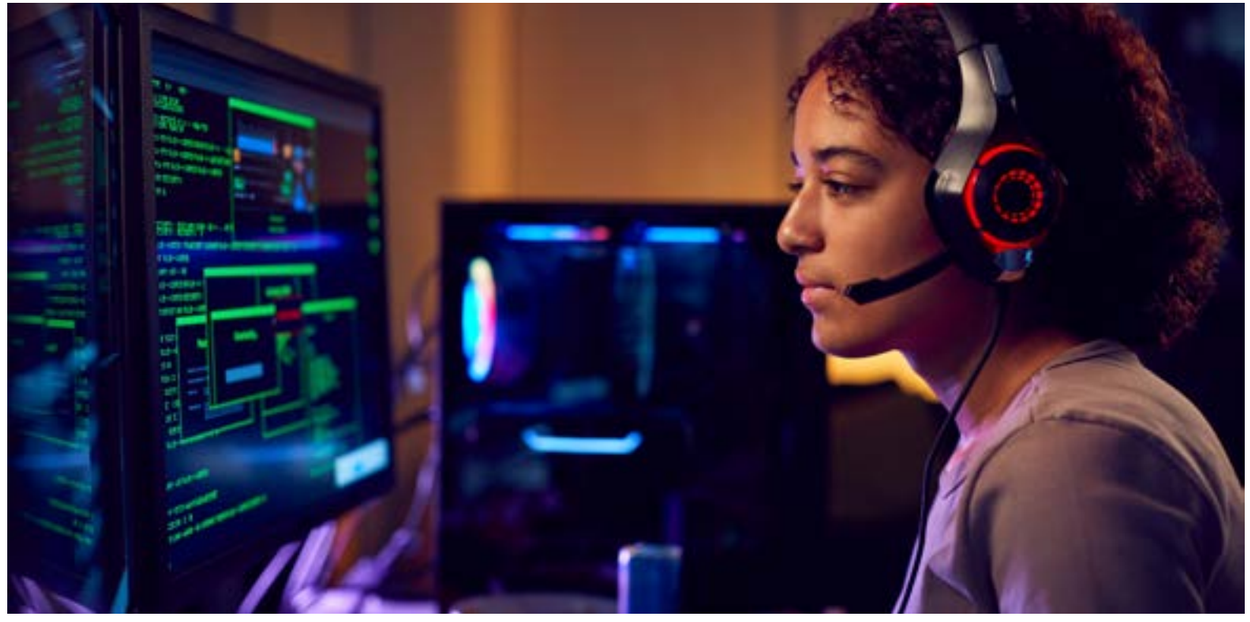
Vous pouvez inspirer votre politique des pratiques de pointe présentées dans *CIS Control 4*[3]. Les pratiques suivantes sont essentielles pour réduire le risque qu'une attaque ne compromette les justificatifs d'identité pour l'accès administrateur.

- Adoptez des exigences de mots de passe uniques et solides pour les accès administrateurs sur chaque système, ou des limites quant à où et à quand ces accès peuvent être utilisés.
- Ne donnez des accès administrateurs ou privilégiés qu'aux personnes qui en ont besoin pour leur travail. Pour ce faire, vous pouvez instaurer, dans votre solution de gestion des identités numériques, des contrôles additionnels qui identifient les rôles administratifs et privilégiés, appliquent la politique que vous avez définie et facilitent une vérification régulière pour le maintien des accès. Si vous avez une solution de gestion des identités numériques et que ce n'est pas déjà fait, travaillez avec votre fournisseur pour mettre en œuvre cette capacité.
- Restreignez l'accès aux systèmes pour utilisateur final. Les employés ne doivent pas se connecter à leur poste de travail avec un compte administrateur. Il convient de verrouiller ces systèmes avec une solide politique de sécurité, notamment en limitant l'accès à l'éditeur du registre dans les systèmes pour utilisateur final sous Windows.
- Vérifiez que les justificatifs d'identité disposant de privilèges élevés sont uniques et protégés par un mot de passe solide. S'il peut être plus simple d'utiliser le même mot de passe pour les accès administrateurs sur tous les systèmes et pour tous les justificatifs d'identité administrateurs de l'entreprise, il sera aussi plus facile pour un attaquant de faire des ravages une fois qu'il aura réussi à compromettre un seul compte privilégié.
- Les comptes de services sont souvent négligés. Assurez-vous que les comptes de services sont configurés pour disposer seulement des privilèges qui sont vraiment nécessaires pour accomplir le travail auquel ils servent. Un attaquant peut se servir d'un compte de services négligé pour se déplacer latéralement dans l'environnement, malgré les meilleures pratiques adoptées pour les comptes administratifs et les comptes privilégiés.

Pour les comptes privilégiés des différents actifs de TI, applications et infrastructure, vous pouvez envisager une solution centralisée de gestion des mots de passe, ou un coffre-fort des mots de passe, qui permet :

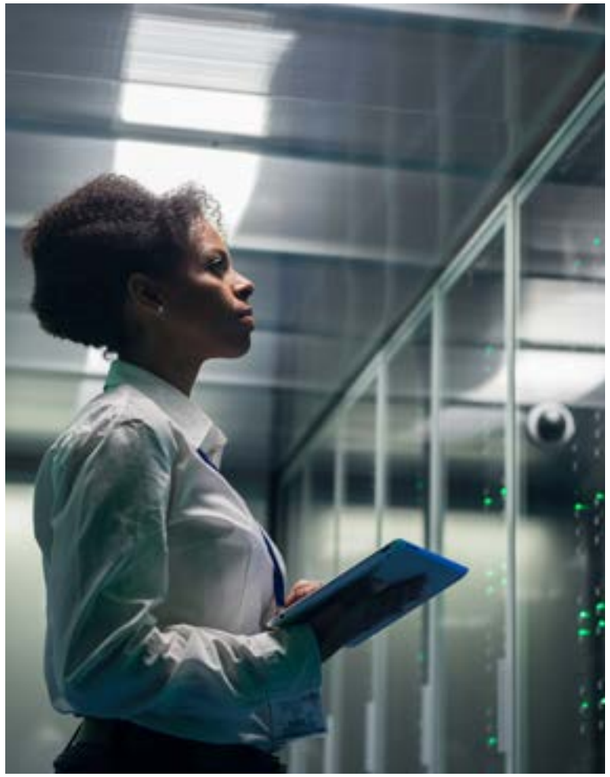
- De stocker de façon sécurisée et centralisée les identifiants privilégiés et de randomiser les mots de passe
- D'avoir une trace d'audit de l'activité privilégiée
- D'analyser les comportements des utilisateurs et les menaces liés à l'activité privilégiée

3 « Controlled Use of Administrative Privileges», site Web du Center for Internet Security, https://www.cisecurity.org/controls/controlled-use-of-administrative-privileges/, accédé le 25 juillet 2020.



- D'appliquer automatiquement les normes et politiques sur les comptes privilégiés
- De gérer et contrôler les comptes de services
- De faire l'abstraction des mots de passe des comptes privilégiés des utilisateurs finaux grâce à la capacité de gestion des sessions.
- D'adopter l'authentification multifactorielle pour les comptes privilégiés et les comptes administrateurs. Pour un attaquant qui obtiendrait le mot de passe d'un compte administrateur, il serait très difficile, sinon impossible, de tirer un réel avantage en raison de l'authentification multifactorielle.
- D'empêcher les personnes qui ont un accès administrateur de se connecter à leur poste de travail d'employé avec des privilèges élevés. Chaque employé, y compris ceux des TI, se verrait attribuer un compte utilisateur normal sans privilèges ou avec des privilèges réduits pour leur poste de travail normal. Autrement dit, les employés doivent disposer d'un accès utilisateur leur permettant seulement d'accomplir les tâches nécessaires à leur travail. Il ne doit pas être permis aux employés de se connecter avec un accès administrateur à leur poste de dans le cadre des activités quotidiennes normales.
- Limitez l'utilisation de privilèges administratifs aux tâches qui nécessitent des privilèges élevés. Idéalement, mettez en place une solution de gestion des accès privilégiés, qui fait que les employés doivent demander les privilèges élevés. Ces privilèges doivent être approuvés et demeurent en vigueur pour une période donnée. Les solutions de gestion des accès privilégiés peuvent être très efficaces pour empêcher un attaquant de compromettre un identifiant s'il tombait sur un ordinateur sur lequel un employé s'est connecté avec des privilèges élevés.
- Si vous n'avez pas déjà de solution de gestion des accès privilégiés, envisagez de limiter les tâches et les accès administrateurs à un serveur tremplin ou à un poste de travail à accès privilégié. Les postes de travail à accès privilégié sont isolés d'Internet, sécurisés et privés de fonctionnalités utilisateurs comme les courriels externes. Ils sont réservés aux accès administrateurs. Il ne faut pas laisser un compte administrateur connecté en continu à un poste de travail, quel que soit le système.
- N'utilisez pas descriptions faciles à identifier pour les comptes privilégiés. Souvent, les organisations utilisent des identifiants communs comme « ADM » pour désigner les comptes administrateurs (p. ex. : « adm - joe01 »). Ces identifiants sont pratiques et faciles à utiliser, mais ils attirent aussi l'attention des attaquants qui fouillent les environnements à la recherche de comptes privilégiés et qui concentreront leur attaque sur ces comptes, notamment en essayant de trouver le mot de passe ou en compromettant les postes de travail.

3. Surveillez votre environnement pour détecter des comportements inhabituels des utilisateurs privilégiés



Une fois que vos accès privilégiés sont protégés, surveillez-les pour détecter des comportements inhabituels, ce qui est particulièrement important pour détecter et contrer non seulement les attaques par rançongiciels, mais aussi toute autre forme de cyberattaque.

- Si vous utilisez une solution de gestion des accès privilégiés, vous avez peut-être déjà la capacité de surveiller l'utilisation des privilèges et de détecter des comportements anormaux. Malgré tout, vous devriez penser à communiquer avec votre fournisseur pour trouver d'autres façons de faire le suivi de l'utilisation des accès privilégiés.
- Il y a des solutions et des fournisseurs qui permettent de surveiller en profondeur les comportements anormaux dans les différents systèmes de votre environnement. L'EDR en est un exemple. Passez en revue les contrôles que vous avez déjà pour détecter des comportements inhabituels et demandez-vous s'ils ont des failles. Reportez-vous à *CIS Control 6*[4] pour plus de détails sur les meilleures pratiques à cet égard.

  Une gestion solide des accès privilégiés et des accès administrateurs constitue l'une des méthodes les plus efficaces pour limiter la capacité d'un attaquant à récolter des données ou à lancer une attaque par rançongiciel dans votre environnement.

4 « Maintenance, Monitoring, and Analysis of Audit Logs », site Web du Center for Internet Security, https://www.cisecurity.org/controls/maintenance-monitoring-and-analysis-of-audit-logs/, accédé le 25 juillet 2020.

J'ai été infecté par un rançongiciel. Qu'est-ce que je fais?

Même en suivant les meilleures pratiques, rien ne garantit que votre organisation ne sera jamais touchée par une attaque par rançongiciel. C'est pourquoi il faut développer un bon niveau de résilience opérationnelle et de redondance qui limitera les dommages et qui assurera une reprise rapide après un tel incident perturbateur. Les éléments suivants peuvent vous aider à établir cette une résilience opérationnelle.

Sauvegardez et sécurisez vos données importantes

Assurez-vous d'avoir un processus de sauvegarde sécurisée de vos données importantes. Malheureusement, dans bien des cas de rançongiciel, l'attaquant aura désactivé, effacé ou crypté les sauvegardes. Si un rançongiciel crypte vos données, il est probable qu'il n'existe aucune clé publique de décryptage, et vous aurez à décider si vous acceptez de payer une forte rançon pour en obtenir une. Or, l'Office of Foreign Assets Control du U.S. Department of Treasury a adopté des mesures qui pourraient vous empêcher de payer la rançon à certains groupes.

- Implantez un processus de sauvegarde sécurisé visant à conserver plusieurs copies, dont certaines le sont de manière sécuritaire et hors ligne. Vous pouvez utiliser les sauvegardes traditionnelles sur bande comportant un service de stockage hors site, des solutions basées sur l'informatique en nuage ou d'autres méthodes. Dans tous les cas, confirmez que l'accès à vos sauvegardes est restreint et sécurisé. Le fait de limiter vos sauvegardes de données à un seul système connecté à votre réseau est un risque important qui pourrait permettre à l'attaquant de porter atteinte à vos capacités de les récupérer.
- Mettez continuellement à l'épreuve la capacité de votre organisation à récupérer rapidement ses sauvegardes. Mettez à l'épreuve votre capacité à restaurer différents systèmes et données essentielles au moins deux fois par année. Malheureusement, de nombreuses organisations apprennent au cours d'une attaque de rançongiciel que ce qu'elles pensaient être un système robuste de sauvegarde de leurs données est trop lent ou qu'elles ne peuvent pas du tout l'utiliser pour restaurer leurs données.

Reportez-vous à *CIS Control 10*[5] pour d'autres indications sur les pratiques exemplaires en matière de définition et de mise à l'épreuve de votre processus de sauvegarde et de restauration des données.

5 « Data Recovery Capability », site Web du Center for Internet Security, https://www.cisecurity.org/ controls/data-recovery-capability/, accédé le 25 juillet 2020.

Créez un plan d'intervention

Lorsqu'une organisation dispose d'un plan déterminé – et qu'elle le met en pratique à maintes reprises – elle est moins susceptible d'être en proie à la panique et de prendre des mesures tardivement qui peuvent exacerber une attaque de rançongiciel et accroître les dommages et les coûts.

- Lorsque vous élaborez le plan d'intervention en cas d'incident de cybersécurité de votre organisation, assurez-vous qu'il comprend tous les rôles liés à votre intervention – internes et externes – qui peuvent être concernés, y compris les principales personnes-ressources en matière de soutien et les fournisseurs. Le plan devrait définir les responsabilités pour chaque rôle et les étapes générales à suivre afin d'établir, de contenir, de corriger et de rétablir les choses à la suite d'un incident de cybersécurité.
- Tenez compte du rôle des fournisseurs et des ressources externes dans votre plan d'intervention. Outre les fournisseurs informatiques tiers, vous aurez peut-être besoin de l'aide de fournisseurs spécialisés en cybersécurité et en criminalistique, de conseillers juridiques en matière de cybercriminalité, ainsi que de conseillers en communications ou en relations publiques. Il est souvent possible d'établir une relation avec ces fournisseurs avant une attaque par rançongiciel, dans le cadre d'un mandat de représentation, qui établit les conditions contractuelles, les tarifs prénégociés et les capacités proactives qui améliorent votre capacité à faire face à un cyberincident. Une fois qu'une organisation est identifiée et qu'un mandat est en place, ajoutez cette entreprise et ses personnes-ressources à votre plan d'intervention en cas d'incident.
- Mettez votre plan d'intervention en pratique. Faites des exercices de simulation, où tout le personnel nécessaire peut reproduire, en toute sécurité, une véritable attaque par rançongiciel. Cet exercice vous permet de confirmer que les outils, processus, méthodes et personnes sont prêts. Plus une organisation s'exerce, plus elle trouvera de moyens pour améliorer son plan, former son personnel et réduire la panique si une attaque se produit.

Reportez-vous à *CIS Control 19*[6] pour d'autres indications sur les pratiques exemplaires en matière de définition et de mise à l'épreuve de votre processus de sauvegarde et de restauration des données.

6 « Incident Response and Management », site Web du Center for Internet Security, https://www.cisecurity.org/controls/incident-response-and-management/, accédé le 25 juillet 2020.

Comment l'équipe d'EY peut vous aider

Les attaques par rançongiciel peuvent s'avérer coûteuses et dommageables et elles font preuve de plus en plus de sophistication. Les organisations doivent se tenir activement au courant des derniers schémas d'attaque, tenir compte des vulnérabilités et mettre à jour leurs plans d'intervention.

Les Services de consultation en cybersécurité d'EY peuvent vous aider à mettre en œuvre votre stratégie de gestion des risques liés aux rançongiciels grâce à des approches personnalisées pour votre organisation, notamment :

- Service de renseignements sur les cybermenaces
- Gestion et planification des cyberrisques
- Résilience des entreprises
- Gestion des identités et des accès
- Gestion des accès privilégiés
- Détection des menaces actives et intervention
- Exercices de planification d'intervention en cas d'incident

Communiquez avec nous pour en savoir davantage sur la façon dont votre organisation peut se protéger contre les attaques par rançongiciel.

Yogen Appalraju
Leader, Cybersécurité, EY Canada
yogen.appalraju@ca.ey.com
+1 416 932 5902

Chandra Majumdar
Leader, Gestion des cybermenaces, EY Canada
chandra.majumdar@ca.ey.com
+1 416 941 1833

Atul Ojha
EY Canada Digital Identity Co-Leader
atul.ojha@ca.ey.com
+1 416 932 4335

Omer Arshed
Coleader, Identité numérique, EY Canada
omer.arshed@ca.ey.com
+1 416 943 3800

Keith Mularski
Leader, Renseignements sur les cybermenaces, EY Amériques
keith.mularski@ey.com
+1 412 644 0612

EY | Travailler ensemble pour un monde meilleur

La raison d'être d'EY est de bâtir un monde meilleur, de créer de la valeur à long terme pour les clients, les gens et la société, et de renforcer la confiance à l'égard des marchés financiers.

S'appuyant sur les données et la technologie, les équipes diversifiées d'EY présentes dans plus de 150 pays instaurent la confiance au moyen de la certification, et aident les clients à prospérer, à se transformer et à exercer leurs activités.

Que ce soit dans les services de certification, de consultation, de stratégie, de fiscalité ou de transactions, ou encore, au sein des services juridiques, les équipes d'EY posent de meilleures questions pour trouver de nouvelles réponses aux enjeux complexes du monde d'aujourd'hui.

3749339
DE 00

ey.com/ca/fr