Boîte à outils pour les interventions d'urgence:

COMMENT RÉPONDRE À UNE ATTAQUE PAR RANSOMWARE EN 12 ÉTAPES

Chaque organisation doit partir du principe que, tôt ou tard, elle sera confrontée à une attaque par ransomware. La principale question est de savoir quand. Comme dit l'adage, mieux vaut prévenir que guérir!

Voici un guide sur les mesures à prendre lorsqu'un ransomware a frappé votre entreprise.

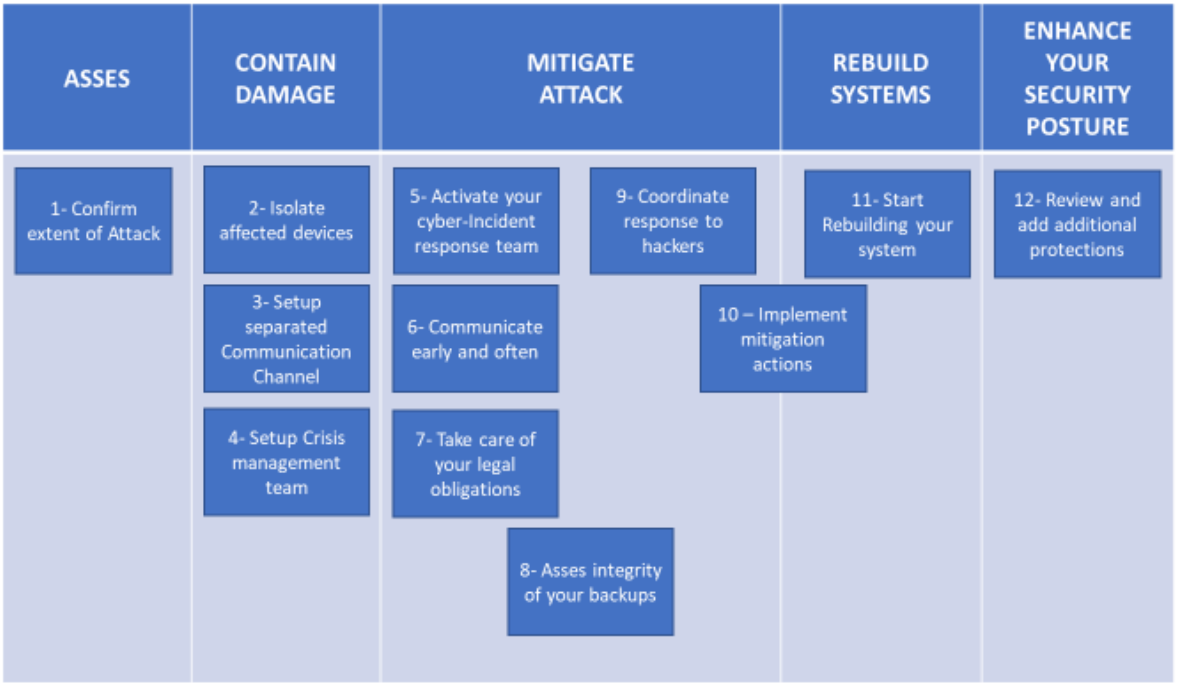
La préparation est essentielle pour faire face à une attaque par ransomware. L'objectif primordial est de faire en sorte que les organisations soient prêtes et n'aient pas à improviser une fois la catastrophe survenue, ce qui pourrait entraîner des erreurs supplémentaires et une perte de données majeure.

La préparation comprend la composition des équipes dont vous avez besoin (technique, crise, communication, etc.) et la manière de joindre ces personnes le plus efficacement. Dans la phase de préparation (par exemple, votre *playbook* est disponible, vous l'avez mis à l'épreuve par un exercice), assurez-vous d'inclure également un processus pour garder le tout à jour.

Les étapes décrites ci-dessous sont les étapes minimales que vous devrez suivre en cas d'attaque par un ransomware, si possible en appliquant vos plans de reprise d'activité (après sinistre), si ce n'est pas le cas, nous espérons que les directives ci-dessous mettront en évidence les actions importantes à entreprendre.

Se remettre d'une attaque par ransomware ne se fait pas en quelques heures et prend généralement des semaines ou des mois. Cependant, il est crucial de prendre des mesures dans les heures qui suivent une attaque confirmée.

Visuel: Étapes de haut niveau



1. Déterminer et confirmer l'ampleur de l'attaque par ransomware.

La reconstruction des systèmes n'est PAS la première étape de votre plan d'intervention.

Évaluez l'ampleur de l'attaque par ransomware en vous concentrant sur ce qui a été crypté et/ou potentiellement exfiltré. Il est essentiel de fournir une réponse à cette question pour activer un plan de réponse.

Ce plan d'intervention fournira également des indications utiles sur les questions internes et externes que vos dirigeants, vos employés et vos clients pourraient se poser.

Il est difficile de mettre en place un plan de réponse si vous ne connaissez pas l'ampleur de l'attaque. Essayez de documenter les données qui se trouvaient sur les machines cryptées et recherchez les données qui ont pu être exfiltrées.

2. Isolez les appareils affectés

Isolez les appareils touchés autant que possible pour éviter toute propagation.

Lorsqu'un ransomware frappe, il est essentiel d'isoler autant que possible les appareils touchés pour éviter toute propagation. Il faut partir du principe que les attaquants sont déjà bien implantés dans votre environnement au moment où l'attaque par ransomware est lancée. Il est donc essentiel d'agir rapidement pour en limiter l'impact.

Commencez par isoler les appareils infectés et les enlever du réseau. Débranchez les câbles réseau, arrêtez les connexions réseau (y compris les réseaux Wi-Fi). Si votre réseau le permet et est correctement segmenté, vous pouvez également déconnecter le segment de réseau infecté.

N'éteignez PAS les appareils infectés, évitez d'arrêter les systèmes. Il se peut que des logiciels malveillants non activés aient aussi été installés. Le fait de disposer d'un système en fonctionnement peut également vous aider à demander l'aide d'une société de réponse aux incidents pour mener des enquêtes détaillées.

Ne commencez pas les opérations de récupération tant que l'étendue de l'attaque n'est pas connue, ce qui inclut la méthode, le moment, les systèmes impactés.

3. Mettre en place un canal de communication séparé

Supposons que les outils de communication de votre entreprise (s'ils sont encore fonctionnels) soient compromis.

Les communications sensibles sur l'évolution de l'incident doivent se faire sur un canal séparé et sécurisé. Supposez que vos systèmes de messagerie (s'ils sont encore fonctionnels) ont également été violés et que l'attaquant y a accès, ce qui signifie que la communication sur votre réseau doit être limitée au strict minimum. Analysez quels systèmes pourraient être utilisés pour communiquer en interne et en externe. Mettez en place un canal de communication sécurisé avec votre équipe technique et votre équipe de direction.

Il est conseillé d'installer p.ex. Signal ou d'utiliser temporairement un système de conférence externe (outil de communication sécurisé) et de créer des groupes séparés. Vous pourriez ainsi créer un groupe constitué des responsables techniques, un groupe incluant les responsables de la communication et un groupe orienté *leadership*. La moitié du travail pour faire face à un incident de ransomware sera consacré à la coordination et à la communication.

4. Mettre en place une équipe de gestion de crise

L'équipe de gestion de crise coordonnera toutes les activités nécessaires pour remettre vos systèmes informatiques dans un état opérationnel, mais s'occupera également des priorités commerciales et informatiques, de la communication et des aspects juridiques.

Mettez en place une équipe de gestion de crise (parfois appelée équipe de continuité des activités) qui s'accordera sur les professionnels de l'entreprise, la stratégie de communication, les questions juridiques et aidera à résoudre les conflits de priorité lorsque le rétablissement des fonctions de l'entreprise devra être abordé.

Cette équipe doit coordonner toutes les communications internes et externes, en veillant à ce que l'organisation parle d'une seule voix pendant la crise.

L'équipe de gestion de crise doit comprendre les principales parties prenantes de l'entreprise, votre Délégué à la protection des données (DPO), les services de communication, le service juridique et un représentant de l'IT.

Désignez un gestionnaire de crise qui assurera la liaison entre votre ou vos équipes techniques et l'équipe de gestion de crise.

En fonction de la taille de l'organisation, vous pouvez envisager d'avoir deux équipes de gestion de crise, l'une pour les aspects commerciaux et l'autre pour les aspects informatiques opérationnels (la dernière faisant directement rapport à la gestion de crise commerciale).

5. Activez votre équipe de réponse aux cyberincidents

Demandez l'aide professionnelle de cyberspécialistes, tels que des experts en criminalistique, qui peuvent vous aider à déterminer comment l'incident s'est produit et à éviter qu'il ne se reproduise.

Vérifiez si la réponse aux incidents fait partie de votre contrat d'assurance. Vérifiez si vous disposez d'une expertise interne, sinon engagez une équipe professionnelle de réponse aux incidents pour vous aider à évaluer le vecteur d'attaque initial et le point d'entrée et permettre une atténuation appropriée.

6. Communiquer tôt et souvent

Communiquez tôt et souvent, tenez vos employés en interne, vos fournisseurs, vos prestataires de services et vos clients au courant. Cacher cette attaque n'est généralement pas une bonne idée car cela peut nuire à la réputation de votre marque.

Soyez aussi transparent que possible vis-à-vis de vos employés, des parties prenantes, des clients ou des utilisateurs, et de la presse au sujet de l'attaque. Même si vous n'avez pas toutes les réponses, il est important d'informer toutes les parties prenantes. Plus d'informations: https://www.cert.be/fr/la-communication-de-crise-en-cas-de-cyberattaque .

Lorsque vos systèmes de communication ne sont pas disponibles, envisagez des solutions temporaires comme la création d'une page web de communication ou des systèmes de notification de masse par SMS.

7. S'occuper de vos obligations légales

Les acteurs du ransomware ne souhaitent pas seulement que vous payiez la rançon pour décrypter les systèmes, mais ils ont aussi souvent exfiltré des données et menacent de les vendre ou de les rendre publiques si vous ne payez pas.

Il existe des obligations légales de notification aux autorités telles que le DPA/GBA/APD en cas de suspicion de violation de données (généralement dans les 72 heures).
https://www.autoriteprotectiondonnees.be/citoyen/agir/contact (site web disponible en NL et FR). Impliquez votre délégué à la protection des données (DPO).

L'équipe juridique et/ou le DPO peuvent également déposer une plainte auprès de la police locale.

8. Évaluez l'intégrité de vos sauvegardes

Vérifiez que les attaquants n'ont pas compromis également la sécurité et l'intégrité de votre système de sauvegarde.

Si le système de sauvegarde est sécurisé, ce qui signifie que vous disposez d'une copie indépendante et vérifiée de vos données, éviter le paiement d'un ransomware est la meilleure option. Vous devez donc avoir la confirmation que les sauvegardes n'ont pas été compromises ou consultées (des sauvegardes immuables sont indispensables).

9. Coordonnez votre réponse aux pirates

Par principe, vous ne devez PAS payer de rançon à des organisations criminelles.

Le Centre pour la Cybersécurité Belgique (CCB) déconseille fortement le paiement d'une rançon. Il peut y avoir des situations dans lesquelles le paiement est la seule option restante, mais gardez à l'esprit que les attaquants sont très probablement intéressés par le gain financier et que toutes les opportunités de vous extorquer plus d'argent seront évaluées par ces acteurs.

Soyez prudent lorsque vous interagissez avec l'attaquant, l'embauche d'un négociateur professionnel n'est pas une solution miracle. Il existe de nombreux cas connus de montants de rançon qui ont été doublés après l'embauche d'un négociateur et n'oubliez jamais qu'il n'y a aucune garantie que les clés de déchiffrement seront reçues.

10. Mettre en œuvre des mesures d'atténuation

Mettez en place des services (minimums) de surveillance de la sécurité (service SOC), activez la détection aux points de terminaison (*Endpoint détection*). Patchez, réinitialisez, mettez à jour les systèmes vulnérables connus touchés par l'attaque. Mettez en place l'authentification multi-facteurs.

N'ouvrez pas la connectivité Internet à tous les utilisateurs, concentrez-vous d'abord sur les utilisateurs nécessaires au rétablissement de vos opérations informatiques pour vos fonctions de gestion de crise. Appliquez des correctifs, réinitialisez, mettez à jour les systèmes vulnérables connus touchés par l'attaque. Effectuez une réinitialisation complète de tous les mots de passe et mettez en place, si ce n'est déjà fait, une authentification multifactorielle. Concentrez-vous d'abord sur les comptes et services privilégiés (comptes administrateurs, services administrateurs).

Mettez en œuvre des services de surveillance de la sécurité (service SOC), activez une solution de détection des points d'accès aux systèmes critiques (*Endpoint Detection*) tels que les systèmes d'authentification et d'autorisation, les systèmes ouverts à l'Internet. Le but est d'avoir une (meilleure) visibilité sur les activités qui se déroulent sur votre réseau.

11. Commencez à reconstruire vos systèmes

Corrigez, mettez à jour, reconstruisez et réinitialisez votre système d'authentification, mettez en œuvre l'authentification multifactorielle.

Ne restaurez pas un système en vous basant sur des sauvegardes proches ou postérieures à l'attaque. Agissez d'abord sur les points précédents et ensuite, seulement ensuite, commencez les activités visant à reconstruire votre système à partir des sauvegardes.

Veillez à ne pas réinfecter les systèmes propres pendant la restauration. Une fois le système restauré, veillez à vérifier qu'il ne reste rien de malveillant sur celui-ci avant de le réintégrer dans votre réseau. Reconstruisez vos systèmes en fonction d'un ordre de priorité des services critiques. Restaurez d'abord les serveurs puis les terminaux. Il est également recommandé de conserver une copie de vos données cryptées, un outil de décryptage gratuit pour votre souche de ransomware pourrait être disponible à l'avenir.

Supprimer ou isoler complètement les anciens systèmes et protocoles.

12. Examinez et ajoutez des protections supplémentaires pour prévenir une future attaque.

Bien que l'accent doive être mis sur l'assainissement à la suite de l'attaque et sur la reconstruction de l'infrastructure, les dirigeants de l'entreprise doivent être conscients qu'une nouvelle attaque est possible.

Prenez le temps d'analyser et de documenter l'attaque en détail, mettez en place de nouveaux contrôles, processus, procédures et solutions pour prévenir une attaque ultérieure.

Webinar disponible en français et en néerlandais: https://www.youtube.com/watch?v=r0Iraugn-wo

La brochure de CERT.be sur le ransomware est disponible en français et en néerlandais.

Contact

CERT.be
Federal Cyber Emergency Team
Rue de la Loi, 16
1000 Bruxelles
info@certbe

Centre pour la Cybersécurité Belgique
Rue de la Loi, 16
1000 Bruxelles
info@ccb.belgium.be

Disclaimer

Editeur responsable

Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur
Rue de la Loi, 16
1000 Bruxelles