CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Stratégie face aux rançongiciels

Comment se préparer, réagir et se remettre d'une attaque d'un rançongiciel

© Cyber Readiness Institute 2020 | guide@cyberreadinessinstitute.org

D'ici 2021

"toutes les 11 secondes"

une nouvelle organisation sera victime de logiciel de rançon, selon l'étude de marché Cybersecurity Ventures.[1]

Stratégie face aux rançongiciels

Payer ou ne pas payer? Cette question est souvent la première que beaucoup d'organisations se posent après avoir été victimes d'une attaque par un logiciel de rançon (ransomware en anglais).

Malheureusement, le choix n'est pas simple. De nombreuses organisations ne savent tout simplement pas comment se protéger contre les rançongiciels. Ce guide est destiné à fournir une feuille de route aux organisations (par exemple les petites et moyennes entreprises, les gouvernements nationaux et locaux) pour se protéger contre cette menace croissante.

[1] umbrella.cisco.com/blog/2019/12/17/ransomware-defense-for-dummies-2nd-edition

Toutes les organisations courent le risque d'avoir leurs précieuses données - sur les clients, les employés, les opérations - chiffrées par un acteur malveillant afin que l'organisation perde son accès. **Une attaque de type "ransomware" est menée par un acteur malveillant prenant en otage les données d'une organisation contre une rançon.** Les acteurs malveillants peuvent accéder aux données d'une organisation par divers moyens, y compris par l'hameçonnage (phishing) et par des logiciels sans correctifs de sécurité. Les correctifs sont délivrés par les sociétés développant des logiciels afin de contrer les vulnérabilités se trouvant dans leurs programmes ; de nombreux utilisateurs ne parviennent pas à télécharger les correctifs, ce qui signifie que les vulnérabilités peuvent être exploitées.

Une organisation qui se prépare aux dangers informatiques peut être résiliente face à une attaque de logiciel de rançon en prenant des mesures préventives (par exemple, en créant une sauvegarde des données critiques), en élaborant et en testant un plan de réponse contre

ÉTAPE 1

Préparer

ÉTAPE 2

Répondre

ÉTAPE 3

Récupérer

Préparer

Assurez-vous que votre entreprise sauvegarde régulièrement ses données; le stockage des données dans un cloud est un outil couramment utilisé pour les sauvegardes. Si vos employés sauvegardent des informations confidentielles sur leurs propres ordinateurs, votre organisation doit également fournir des instructions claires à vos employés sur la manière de sauvegarder régulièrement leurs données. Les éléments clés pour se protéger contre les logiciels de rançon comprennent:

- Priorisez les données les plus critiques pour votre organisation et les sauvegarder. Assurez-vous que vous puissiez réinstaller à partir des sauvegardes, qui sont souvent dans un coud, et que les sauvegardes soient testées fréquemment.
- La détection précoce est importante, alors assurez-vous que votre personnel sait comment signaler un éventuel incident lié à un logiciel de rançon ou un comportement inhabituel du réseau.
- Conclure, si possible, un contrat avec un vendeur qui peut fournir du soutien en cas d'incident. Établir un contrat, avant qu'un incident ait lieu, afin que vous puissiez immédiatement avoir accès au vendeur

Comme les acteurs malveillants utilisent souvent l'hameçonnage pour infecter un système avec des logiciels de rançon, il est crucial d'avoir une stratégie contre l'hameçonnage. Effectuer des tests d'hameçonnage réguliers afin que les employés puissent détecter un e-mail de *phishing* avant de cliquer sur un lien ou des pièces jointes et, si possible, utiliser un logiciel *anti-phishing*.

Mettez à jour votre logiciel avec les derniers correctifs de sécurités. Cette mesure préventive essentielle rendra plus difficile l'accès à votre système pour les acteurs malveillants.

Élaborer une stratégie à l'échelle de l'organisation concernant les attaques contre rançon. Il est beaucoup plus facile d'avoir ces discussions lorsque la pression pour fournir une réponse n'est pas imminente. Les questions à considérer sont: Quelles sont les données les plus importantes pour votre organisation ? Votre assurance couvre-t-elle les logiciels de rançon ? Êtes-vous d'accord de payer une rançon ? Si oui, savez-vous comment utiliser les bitcoins et autres crypto-monnaies?

Discuter et convenir d'une stratégie à l'échelle de l'organisation concernant les attaques par rançongiciel. **Il est beaucoup plus facile d'avoir ces discussions**

Ces données sont-elles **essentielles à vos opérations?**

Votre organisation a-t-elle déterminé à l'avance qu'il est **acceptable de payer une rançon?**

Votre assurance **couvre-t-elle les rançongiciels?**

Répondre

Si un employé ou l'organisation est confronté à une demande de rançon, votre organisation doit d'abord évaluer la légitimité de la demande de rançon en contactant votre responsable informatique. Si elle est légitime,Deux scénarios possibles sont présentés:

1. **Votre organisation dispose de sauvegardes qui fonctionnent. Vous n'avez pas besoin de vous inquiéter pour la rançon. Vous restaurez complètement vos données et vous vous remettez au travail.**

2. **Les données qui sont retenues en otage sont nécessaires et il n'y a pas de sauvegardes fonctionnelles.**

   a. Vérifiez si les données existent ailleurs dans l'organisation (par exemple, fichiers en cache, courrier électronique) afin que vous puissiez "enregistrer" les données pour remplacer celles qui sont retenues en otage

   b. Si vous ne pouvez pas accéder aux données ailleurs, posez les questions suivantes:

   - Les données sont-elles essentielles à vos opérations?
   - Votre organisation a-t-elle déterminé à l'avance qu'elle est d'accord pour payer une rançon?
   - Est-ce que votre assurance le couvre?

Récupérer

L'incendie est éteint et il est temps de reprendre les activités habituelles. L'ampleur de l'attaque par rançon et la gravité de son impact sur vos opérations quotidiennes déterminera le temps et les efforts nécessaires pour vous en remettre. Utilisez l'incident comme une expérience d'apprentissage pour renforcer l'importance des principes de préparation au numérique, comme la sensibilisation aux correctifs de sécurité et à l'hameçonnage.

En veillant à ce que vos logiciels soient toujours mis à jour avec les derniers correctifs de sécurité, vous rendrez la pénétration de votre système plus difficile. De même, la mise en place d'une formation régulière sur l'hameçonnage minimise l'erreur humaine et les points d'entrée potentiels dans votre système. Comme pour toute violation de la sécurité, informez toutes les parties concernées, réinitialisez les identifiants et les mots de passe de tous les appareils compromis, mettez à jour le logiciel sur tous les appareils et réinstallez vos données à partir de sauvegardes une fois que la menace du logiciel rançon a été neutralisée.

Il est particulièrement important de s'assurer que correctifs de sécurité soient toujours à jour après l'attaque. Si les données ont été restaurées, certaines vulnérabilités étaient corrigées, avant l'apparition du logiciel de rançon, peuvent réapparaître.

Le programme de préparation au numérique Cyber Readiness Program comprend des informations détaillées et des modèles afin de vous aider à créer vos propres stratégies et plan d'intervention pour se préparer, réagir et se remettre d'une attaque de logiciel de rançon. Inscrivez-vous gratuitement sur **BeCyberReady.com**.

Pour lire des exemples réels de la façon dont des entreprises et des municipalités ont répondu à une attaque de logiciels de rançon, veuillez consulter les **Cyber Readiness News.**

Le programme de préparation au numérique **Cyber Readiness Program** comprend des informations détaillées et des modèles afin de vous aider à créer vos propres stratégies et plan

Guide de décision pour les demandes de rançon

PREPARER

Avez-vous établi un ordre de priorité de vos données et de vos systèmes afin de savoir ce qui est le plus

Avez-vous plan d'intervention concernant les rançons?

Identifiez ce qui est le plus précieux. Allez sur **BeCyberReady.com**

Élaborer un plan de réaction aux incidents concernant les logiciels de rançon. Allez sur **BeCyberReady.com** pour accéder à un modèle

L'avez-vous testé dans

Sauvegarder votre système et toutes les données.

Félicitations.

Testez votre sauvegarde pour vous assurer que vous pouvez récupérer vos données - surtout les

Vous feriez mieux d'espérer que vous n'aurez pas d'attaque de rançon.

RÉPONDRE

Isolez l'incident et supprimez le ou les ordinateurs infectés du réseau. Ensuite, continuez.

Excellent travail.

Disposez-vous d'un support

Pouvez-vous ou votre support informatique créer une

Avez-vous une assurance contre

Votre stratégie couvre-t-elle les

Vos données sont irrécupérables...

RECUPERER

Vous êtes de retour dans les affaires! Inscrivez-vous pour le progamme gratuit Cyber Readiness Programme sur **BeCyberReady.com** afin d'empêcher les attaques de nouveaux logiciels de rançon à l'avenir..

guide@cyberreadinessinstitute.org