

RANÇONGIELS : PRÉVENTION ET PROTECTION

PROTECTION EN TEMPS RÉEL

Le rançongiciel est une menace croissante depuis que des individus malveillants ont trouvé un moyen de monétiser des logiciels malveillants en paralysant des systèmes informatiques et en demandant le paiement d'une rançon pour les débloquer. Contrairement aux autres logiciels malveillants, qui doivent souvent rester cachés pendant de longues périodes pour fonctionner efficacement, le rançongiciel est conçu pour s'exécuter rapidement par spear phishing, sur des sites Web compromis et par le biais de téléchargements corrompus. Les établissements financiers sont particulièrement vulnérables à l'impact des rançongiciels qui peuvent menacer la capacité à transférer des fonds rapidement et efficacement, et parce que ces établissements sont des cibles considérées lucratives. Cependant, les individus malveillants ne respectent pas toujours leurs promesses : même en cas de paiement d'une rançon, certains cyberpirates ne suppriment pas le logiciel malveillant ou publient des données confidentielles.

- Investissez dans des systèmes de protection anti-logiciels malveillants qui s'adaptent à la veille sur les nouvelles menaces en temps réel.
- Évaluez la sécurité de tous les périphériques connectés aux réseaux qui hébergent des informations sensibles ou vitales. Connectez tous les systèmes non essentiels à un réseau distinct.
 - Soyez particulièrement vigilants lorsque vous apportez des périphériques IoT ou « intelligents » dans vos espaces de travail ; ces systèmes ont souvent des systèmes de sécurité plus faibles ou inexistantes et peuvent être ciblés comme points d'accès à des systèmes essentiels.
 - Pensez à sécuriser les configurations de travail à distance. Vérifiez que les outils de sécurité fonctionnent en dehors du réseau pour surveiller l'ensemble du trafic Web.
- Encouragez la formation des employés sur les attaques par hameçonnage et sur la nécessité de protection par mots de passe renforcés.
- Envisagez la mise en œuvre d'une authentification multifactorielle dans l'ensemble de votre organisation, si cela est réalisable.
- Procédez à la mise à jour régulière de tous les logiciels et systèmes. Modifiez les paramètres pour autoriser les mises à jour automatiques, si possible.
- Développez un plan d'intervention en cas d'incident et de gestion de crise afin de savoir comment traiter une attaque par rançongiciel et la perte de données précieuses.
- Préparez un plan de communication externe en cas d'attaque par rançongiciel.

SAUVEGARDES DE DONNÉES

- Investissez dans des systèmes de sauvegarde sécurisés et régulièrement mis à jour qui protègent vos données.
 - En cas d'utilisation de clés USB ou de disques durs, déconnectez physiquement ces périphériques des ordinateurs en réseau une fois les sauvegardes terminées.
 - En cas d'utilisation d'espace de stockage cloud, équipez les serveurs avec un cryptage de haut niveau et une authentification multifactorielle.
- Créez une copie en lecture seule des écritures comptables pour les pires cas de récupération d'urgence.
- Développez des systèmes qui effectuent une récupération des données et une correction automatiques.
- Élaborez des scénarios pour évaluer la durée de récupération des données critiques et des services de l'entreprise.

ENVIRONNEMENT RÉGLEMENTAIRE

- Évaluez les directives réglementaires et juridiques pertinentes en cas de rançongiciels dans votre environnement opérationnel.
 - Pensez aux directives nationales spécifiques. Élaborez un plan pour l'évaluation périodique des directives en constante évolution.
 - Pensez aux directives spécifiques au secteur financier.
 - Pensez aux exigences réglementaires et juridiques internationales.
- Évaluez les risques impliqués par le paiement d'une rançon. Dans certains cas, le paiement d'une rançon peut violer les régimes de sanctions existants en place contre des individus hostiles.
- Lien avec l'application des lois. Créez des connexions pour le partage rapide des informations dans l'éventualité d'une attaque.
- Évaluez les avantages et les inconvénients des politiques de cyber-assurance pour les rançongiciels.

Estimation de la préparation de votre organisation en cas de rançongiciels

Posez-vous les questions suivantes lorsque vous élaborez un plan de prévention et de protection contre les rançongiciels.

- Votre organisation procède-t-elle à des sauvegardes planifiées de manière régulière ?
 - Ces sauvegardes sont-elles déconnectées de votre réseau, via des systèmes de stockage cloud ou des clés USB et des disques durs ?
- Des périphériques non essentiels sont-ils connectés au réseau de votre organisation ?
 - Peuvent-ils être déplacés sur d'autres réseaux n'hébergeant pas de données sensibles ?
- Votre organisation connaît-elle les risques réglementaires et légaux impliqués par le paiement d'une rançon ?
 - Les directives juridiques sur ce sujet varient d'un pays à l'autre et sont fréquemment mises à jour.
- Votre organisation met-elle régulièrement à jour ses logiciels et ses systèmes ? Les mises à jour sont-elles automatisées ?
- Votre organisation dispose-t-elle d'un plan pour traiter les attaques par rançongiciels et la perte de données précieuses ?
- Votre organisation dispose-t-elle d'une politique de cyber-assurance ? Si c'est le cas, dans quelle mesure ce plan couvre-t-il les attaques par rançongiciels ?
 - Certains plans interdisent explicitement les paiements de rançons, alors que d'autres couvriront ces paiements dans le cadre de la politique d'assurance.