Considérez ces dix étapes cruciales pour prévenir et détecter les attaques de rançongiciels

Les attaques de rançongiciels représentent un problème mondial sérieux qui s'aggrave; en fait, elles sont souvent considérées comme la principale cybermenace à laquelle sont confrontées les entreprises aujourd'hui.[1] Les statistiques sur les rançongiciels sont stupéfiantes:

- **Les dommages causés aux entreprises et aux organisations devraient s'élever à 20 milliards $ en 2021[2].**
- **Les rapports mondiaux sur les rançongiciels font état d'une augmentation de plus de 715 % entre 2019 et 2020[3]**
- **Les paiements consécutifs aux attaques par rançongiciel ont augmenté en valeur de 60 % depuis 2019[4].**

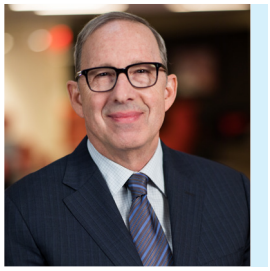
Les rançongiciels occasionnent une crise qui ne fera qu'empirer à mesure que les acteurs de la menace continueront à se perfectionner et à acquérir de l'expertise. Les auteurs de crimes par rançongiciels agissent souvent avec la discipline et l'approche d'une entreprise traditionnelle légitime, mais avec une intention criminelle. Heureusement, il existe des stratégies que les entreprises peuvent adopter pour réduire le risque d'être victimes d'une attaque par rançongiciel.

Considérez ces dix technologies et processus pour aider à prévenir et à détecter une attaque par rançongiciel. Chacune de ces étapes concorde étroitement avec la façon dont les agresseurs créent et accomplissent leur activité criminelle. Bien que certaines soient coûteuses, la mise en oeuvre proactive de ces mesures dès maintenant peut atténuer les coûts de pertes d'exploitation, de l'atteinte à la réputation, de la réaction aux incidents ou du paiement consécutif à une attaque par rançongiciel.

1. **Formation de sensibilisation à l'hameçonnage**, pour apprendre aux employés et aux utilisateurs finaux à repérer les courriels d'hameçonnage et à reconnaître les signaux d'alerte pour réduire le nombre de clics sur les courriels malveillants que de nombreux agresseurs par rançongiciel utilisent pour pénétrer un réseau.
2. **Désactivation de l'accessibilité du bureau à distance directement à partir de l'Internet**, pour empêcher les agresseurs par rançongiciel de forcer brutalement les services Protocole de bureau à distance orientés Internet pour pénétrer un réseau.
3. **Filtrage des URL et bac à sable correctement configurés pour les pièces jointes des courriels**, afin d'empêcher les logiciels malveillants contenus dans les courriels de rançongiciel de s'exécuter ou de passer inaperçus.
4. **Solution avancée de détection et de réaction des points terminaux (« EDR »)**, pour détecter et éventuellement mettre en quarantaine les rançongiciels et autres logiciels malveillants avancés, ainsi que pour faciliter la criminalistique d'entreprise en cas d'attaque.
5. **Outil avancé de détection des logiciels malveillants qui inspecte le trafic réseau**, afin d'identifier les rançongiciels et autres lots malveillants ou d'examiner le trafic réseau circulant sur le circuit.
6. **Services de compte à 16 caractères et plus, et mots de passe d'administrateur de domaine** pour empêcher les rançongiciels et autres criminels de pirater des noms et mots de passe d'administrateur faibles. Dans l'idéal, ces mots de passe forts devraient faire l'objet d'une alternance régulière à l'aide d'un outil de gestion des accès privilégiés (PAM). Les cyberattaquants par rançongiciel utilisent ces identifiants piratés pour se déplacer latéralement et déployer leur rançongiciel.
7. **Outils de détection des mouvements latéraux.** Après être entrés dans la place avec un rançongiciel, les cybercriminels se déplacent généralement latéralement en utilisant des références informatiques compromises. La détection de ce mouvement latéral anormal permet habituellement de mettre fin à l'attaque avant le déploiement du rançongiciel.
8. **Plateforme de gestion d'information et d'événements de sécurité (SIEM) correctement configurée**, regroupant les journaux d'événements, de sécurité, de pare-feu et autres. Il est très difficile de riposter à une attaque de rançongiciel et de s'en remettre sans SIEM, car la visibilité à partir des journaux locaux non centralisés est souvent mauvaise.
9. **Fonction de surveillance continue de la sécurité**, qui assure une surveillance continue et une chasse aux menaces à l'aide des journaux et des alertes collectés.
10. **Verrouillage du déploiement de logiciels et des outils d'accès à distance** (comme SCCM, PDQ et PsExec) pour un petit ensemble de comptes privilégiés avec une authentification à plusieurs facteurs lorsque cela est possible. Une fois qu'ils ont obtenu des privilèges élevés, les criminels commandent généralement des comptes SCCM/PDQ/PsExec pour propager l'exécutable du rançongiciel à travers le réseau.

Apprenez-en davantage sur la façon dont les Solutions pour la cybersécurité d'Aon peuvent aider votre entreprise en visitant **aon.com/cyber-solutions**

Empower Results®



À propos de l'auteur

Eric M. Friedberg

Coprésident Stroz Friedberg, une entreprise d'Aon

Eric M. Friedberg est cofondateur et co-président de Stroz Friedberg, LLC, une société de cyberconseil et de services techniques acquise par Aon plc en 2016. Monsieur Friedberg possède 30 ans d'expérience des secteurs public et privé dans les domaines du droit, de la lutte contre la cybercriminalité, de la cybergouvernance, de la sécurité informatique, de la criminalistique, des enquêtes et de l'investigation informatique. Son expertise est recherchée par les conseils d'administration, les comités de vérification, les cadres de haut niveau, les cabinets d'avocats et les tribunaux.

Personnes-ressources des Solutions pour la cybersécurité

Eric Friedberg
Coprésident Stroz Friedberg, une entreprise d'Aon
+1 212.981.6536
eric.friedberg@aon.com

AMÉRIQUES

Christian E. Hoffman
Chef de la direction, Solutions pour la cybersécurité, Amérique du Nord
+1 212.441.2263
christian.hoffman@aon.com

Beatrice Conner
Directrice générale, Services de consultation
+1 214.377.4567
beatrice.conner@aon.com

Chad Pinson
DFIR, Enquêtes et Gestion de la mobilisation
+1 214.377.4553
chad.pinson@aon.com

Brent Rieth
Directeur de pratique, É.-U., Erreurs et omissions/ Cybercourtage
+ 1 312.381.3141
brent.rieth@aon.com

Ady Sharma
Vice-président, Exploitation commerciale cybersécurité, Canada
+1 416.263.7876
ady.sharma@aon.ca

Katharine Hall
Vice-présidente principale, directrice de la pratique cyber, Canada
+1 780.423.9820
katharine.hall@aon.ca

LATAM

Temo Garcia
Courtier principal et cyberchampion
É.-U./Amérique latine
+1 312.381.4398
temo.garcia@aon.com

EMEA

Onno Janssen
Chef de la direction, EMOA
+49 (4) 03.605.3608
onno.janssen@aon.com

Richard Hanlon
Chef des services commerciaux
+353 1 266.6443
richard.hanlon@aon.ie

APAC

Michael Parrant
Directeur de la pratique de Cyber assurance
+6 (141) 333.9783
michael.j.parrant@aon.com

Andrew Mahony
Directeur régional
+6 (58) 428.1965
andrew.mahony@aon.com

Chris McLaughlin
Directeur
+61 29253.7792
chris.mclaughlin@aon.com

Sources

1. **https://www.inc.com/adam-levin/ransomware-is-number-one-cyber-threat-this-year-heres-what-you-can-do.html**
2. **« 2019 Cybersecurity Almanac », Cisco and Cybersecurity Ventures, 2019.**
3. **Bitdefender's Mid-Year Threat Landscape Report 2020, page 14**
4. **Coveware Ransomware Marketplace Report, August 3, 2020**

Au sujet des Solutions pour la cybersécurité : Les Solutions pour la cybersécurité d'Aon offrent une approche globale de la gestion des cyberrisques, des compétences inégalées en investigation, ainsi que des technologies exclusives qui aident les clients à repérer et à quantifier les cyberrisques, à protéger les actifs essentiels et à se rétablir après des cyberincidents.

À propos d'Aon : Aon plc (NYSE : AON) est le principal fournisseur mondial d'une vaste gamme de solutions pour la gestion du risque, des régimes de retraite et des programmes de santé. Nos 50 000 employés de 120 pays génèrent des résultats pour les clients grâce à des données et des analyses exclusives produisant des points de vue permettant de réduire la volatilité et d'améliorer le rendement.

Empower Results®