

# 6 conseils pour éviter la contamination du réseau par des ransomwares | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



**6 conseils pour #éviter la contamination du réseau par des ransomwares**

**6 conseils pour éviter la contamination du réseau par des ransomwares** Une étude réalisée par Bitdefender aux États-Unis montre que les APT (Advanced Persistent Threats), le spear phishing et les ransomware sont les types d'incidents les plus craints dans les entreprises.

Cette étude montre, en effet, qu'en termes d'importance, les APT (techniques complexes d'intrusion réseau) sont en tête des préoccupations : 19,7% des managers interrogés les estiment difficiles à gérer.

Les ransomware arrivent en seconde position (13,7%) avec les rootkits. Ces derniers préoccupent plus les DSI que les menaces 0-day.

Le Spear Phishing (des e-mails soigneusement préparés, destinés à des individus spécifiques au sein de l'entreprise) sont mentionnées par à peu près 13% des personnes interrogées. Reste qu'il s'agit là d'une des techniques les plus utilisées pour pénétrer la sécurité de l'entreprise et diffuser des malwares.

Quant aux incidents générés par le BYOD (Bring Your Own Device, l'utilisation de son appareil personnel dans le cadre du travail) et aux vulnérabilités zero-day, ils semblent moins inquiétants, puisque 11,3% des personnes interrogées voient le BYOD comme un risque potentiel pour leur entreprise, tandis que 10,3% des managers pensent que les attaques zero-day sont sources de menaces pour la sécurité de leur entreprise.

BitDefender fait donc 6 recommandations pour que les entreprises puissent limiter les risques d'infection :

1. Mettre en garde les employés contre les nouvelles menaces et leur expliquer comment déceler un e-mail de spear phishing et d'autres attaques d'ingénierie sociale.
2. Installer, configurer et maintenir à jour la solution de sécurité de l'entreprise.
3. Bloquer l'exécution de certains programmes vecteurs d'infections, comme par exemple des logiciels de téléchargement illégal ou de P2P au bureau.
4. Utiliser un pare-feu pour bloquer les connections entrantes vers des services qui n'ont pas lieu d'être publiquement accessibles via Internet.
5. S'assurer que les utilisateurs aient les droits les plus faibles possible pour accomplir leurs missions. Lorsqu'une application requiert des droits d'administrateur, il faut être certain que l'application soit légitime.
6. Activer la restauration système afin de retrouver les versions précédentes des fichiers qui ont été chiffrés, une fois que la désinfection a eu lieu.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.itrmobiles.com/index.php/articles/157764/6-conseils-eviter-contamination-reseau-ransomwares.html> :