kaspersky

Les bonnes pratiques et conseils pour se protéger des ransomwares

Bonnes pratiques

Afin de mettre toutes les chances de votre côté, nous vous invitons très fortement à prendre connaissance des recommandations suivantes (en anglais) :

- Comprendre les causes qui participent à la désactivation des modules de protection.
- Renforcer la sécurité et réduire la surface d'attaque d'un ransomware.
- Maîtriser le principe de fonctionnement d'une contamination par ransomware.

Conseils génériques

Kaspersky

1. Assurez-vous que les produits Kaspersky sont bien en dernières versions (Kaspersky Life Cycle).
2. Assurez-vous que tous les systèmes Endpoint sont bien protégés.
3. Assurez-vous qu'il ne soit pas possible d'arrêter ou de désinstaller la protection.
4. Vérifiez régulièrement vos exclusions.
5. Assurez-vous que les modules suivants sont bien activés et fonctionnels :
   - Détection comportementale
   - Réparation des actions malicieuses
   - Protection contre les Exploits
   - Prévention des intrusions
   - Kaspersky Security Network
6. Assurez-vous d'appliquer les recommandations évoquées dans les bonnes pratiques.
7. Mettez en place des rapports automatiques quotidiens qui seront analysés régulièrement. Toutes les informations suspicieuses doivent faire l'objet d'une analyse.
8. Envisagez la mise en place et l'activation du module de contrôle d'applications.

Conseils génériques

Tiers

1. Informez et sensibilisez vos équipes sur ce qu'est un ransomware et sur ce que cela implique pour votre organisation en cas d'attaque.
    - Renforcez les politiques de l'entreprise concernant l'interdiction de partager ou de révéler les identifiants utilisateur.
    - Privilégiez l'utilisation des comptes utilisateurs pour les usages courants.
    - Informez les utilisateurs qui n'utilisent pas régulièrement des macros de ne jamais les activer dans des documents Microsoft Office.
    - Informez les utilisateurs sur la prudence à avoir avec les pièces jointes non sollicitées.
2. Assurez-vous que les patchs Microsoft soient bien appliqués au plus tôt et fréquemment.
3. Assurez-vous que les patchs des logiciels tiers (navigateur internet, clients mails, lecteurs PDF, outils de compression utilitaires et plug-ins tels que Java, Flash…) soient bien appliqués.
4. Assurez-vous que les patchs des applications de sécurité périmétriques (VPN/Firewall, … etc.) soient bien appliqués.
5. Réalisez régulièrement des analyses des ports ouverts et des vulnérabilités sur votre réseau. Ne laissez pas de ports non obligatoires, exposés sur Internet. Par exemple, verrouillez l'accès RDP et tous les autres protocoles de gestion à distance de votre organisation.
6. Obligez à utiliser des mots de passe robustes et si possible mettez en œuvre l'authentification à deux facteurs surtout pour des connections en provenance de l'extérieur de votre réseau (VPN, RDP, SSH, etc.).
7. Si ce n'est pas encore le cas, pensez à utiliser un proxy pour la navigation Internet de votre entreprise ainsi qu'un système de filtrage d'URL.
8. Equipez le serveur de messagerie de votre entreprise d'un logiciel de protection avancé (anti-spam, anti-phishing, antivirus de pièces jointes…), sachant que le vecteur d'attaque préféré des hackers est l'email.
9. Désactivez tous les services inutiles et vulnérables.
10. Assurez-vous de renforcer la sécurité autour des outils Powershell, VBS etc …
11. Centralisez les journaux de sécurité sur une plateforme de gestion des incidents et failles de sécurité (SIEM), mais aussi vérifiez et analysez fréquemment les informations des journaux.
12. Un système de sauvegarde automatique et régulier doit être inclus dans votre plan de protection face à la cybercriminalité. Si possible, gardez en une copie hors ligne ou hors site.
13. Prévoyez un Plan de Reprise d'Activité (PRA) en cas d'attaque.
14. Faites évaluer et vérifiez vos capacités de réaction face aux incidents.
15. Surveillez et mesurez constamment l'efficacité globale de votre stratégie de sécurité via des audits et/ou tests d'intrusion – le ransomware n'est que la partie émergée de l'attaque.

kaspersky