INTRINSEC
Innovative by design

RANSOMWARES

nos recommandations

Compte-tenu de la tendance actuelle des attaques par rançongiciels sur les entreprises françaises, nos équipes de détection et de réponse aux incidents de sécurité vous proposent quelques recommandations à mettre en place au sein de votre structure :

Les vecteurs d'infection principaux des rançongiciels sont la messagerie, l'accès internet, et enfin les supports amovibles (RETEX SOC, et confirmé par de nombreux rapports d'analyse d'attaque) ;

Les capacités de supervision SSI fournies par le SOC Intrinsec ne peuvent suppléer **à une bonne hygiène SSI du parc.**

Aussi, le SOC Intrinsec recommande aux entreprises de prendre en considération la publication du CIS : https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/#:~:text=Restrict%20Internet%20access.,least%20privilege%20and%20network%20segmentation.

Voici une première lecture de la couverture des mesures recommandées par le CIS, à adapter selon votre contexte :

Plan de réponse à incident :

- Mettre en place un dispositif de détection tel que le SOC Intrinsec ;
- les capacités de détection du SOC sont étroitement liées aux machines et équipements supervisés dans le SIEM, ainsi qu'à leurs capacités de journalisation/détection. La Matrice de détection **permet de visualiser les capacités de détection opérationnelles à l'instant T**.
- Répondre à l'incident en étant accompagné du CERT Intrinsec ou de votre CERT interne si vous en disposez.

Sauvegardes :

- Disposer d'un plan de sauvegarde opérationnel et suffisant : ce plan de sauvegarde est à la responsabilité de l'entreprise ;
- NB : **le SOC Intrinsec recommande que les sauvegardes soient testées régulièrement** ;

INTRINSEC
Innovative by design

RANSOMWARES

nos recommandations

Antivirus et antispam :

- Assurer leur déploiement à 100% sur votre parc, avec mise à jour plusieurs fois par jour ;
- Exploitation des alertes AV / AS : réalisable par le SOC Intrinsec ;
- NB : Concernant la détection des scripts et codes inconnus, le SOC Intrinsec **recommande la mise en place d'un EDR (ou à défaut, SYSMON).**
- Le SOC Intrinsec recommande également de **renforcer le filtrage antispam, et de rester vigilants quant aux messageries grand public telles que Gmail**, accédées sur un poste de travail de l'entreprise.

Désactiver les macros Office :

- Actions sous la responsabilité de l'entreprise ;
- Détection de macros Office malveillantes : réalisable par le SOC Intrinsec ;

Maintenir tous les systèmes à jour de correctifs (MCS) :

- Action sous la responsabilité de l'entreprise ;
- NB : **un MCS défaillant augmente la surface d'attaque du S.I**. et complique donc la tâche du SOC.

Restreindre l'accès Internet :

- S'assurer que tous les accès Internet passent par un **proxy filtrant ;**
- Traiter les détections passant par (ou contournant) les proxies : réalisable par le SOC Intrinsec ;

Appliquer le principe du moindre privilège :

- **Réduire les privilèges (notamment AD) de comptes qui n'en ont pas le besoin**
- Détecter des usages illégitimes de privilèges : réalisable par le SOC Intrinsec :

Valider l'accès et superviser l'activité de fournisseurs/tiers :

- Valider les bonnes pratiques de sécurité d'interconnexion avec des partenaires/tiers ;
- Détecter des incidents SSI inhérents à des accès partenaires/tiers : réalisable par le SOC Intrinsec ;

INTRINSEC
Innovative by design

RANSOMWARES

nos recommandations

Participer au partage d'informations de sécurité :

- Activer les fonctions « cloud » et « télémétrie » des solutions de sécurité en place.

Sensibiliser les utilisateurs à l'ingénierie sociale et au hameçonnage :

- Les pôles **conseil et évaluation d'Intrinsec peuvent vous accompagner** ;

Fermer les sessions (notamment navigateur) quand elles ne sont plus utilisées :

- Détection de sessions illégitimes : réalisable par le SOC Intrinsec ;

Mettre en place un signalement d'incident SSI :

- Le SOC Intrinsec peut fournir un service d'analyse de courriels suspects (hameçonnage, et courriels malveillants).

Des questions ? Nos équipes vous répondent et vous conseillent.

Besoin d'accompagnement ? Nos équipes peuvent couvrir vos besoins pour vous protéger contre les ransomwares :

- **Conseil - Accompagnement sur les actions dont vous avez la responsabilité**
- **Evaluation de votre niveau de cybersécurité**
- **SOC-Intrinsec**
- **Service de Vulnerability Check - Ransomwares**

CONTACTEZ-NOUS

CONTACT@INTRINSEC.COM