CISOs CONNECT

en partenariat avec

AimPoint Group | W2Communications

Gros plan sur les ransomwares

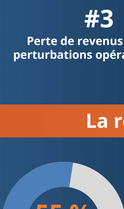
Ce que les RSSI en pensent

Afin de faire la lumière sur le battage médiatique qui entoure le sujet, nous avons interrogé en août 2021 plus de 250 responsables de la sécurité de l'information (RSSI) pour recueillir des témoignages directs sur leurs expériences en matière de ransomware, leurs préoccupations et leurs projets concernant la protection de leur entreprise.

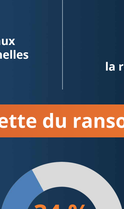
Aucun répit en vue

Global		Entreprises de taille moyenne (1 000 à 10 000 employés)
53 %	Touchées au moins une fois par une attaque de ransomware au cours des 12 derniers mois	66 %
69 %	S'attendent à être touchées au moins une fois par une attaque de ransomware dans les 12 prochains mois	80 %

Trois principaux secteurs d'activité s'attendant à être touchés par une attaque de ransomware au cours des 12 prochains mois



Construction et machines



Commerce de détail et biens de consommation durables

Production

Le coût de la rançon n'est PAS une préoccupation majeure

Impacts des ransomwares les *plus* préoccupants

#1
Exposition de données sensibles ou propriétaires

#2
Coût de la récupération/du retour à la normale des opérations

#3
Perte de revenus due aux perturbations opérationnelles

Impacts des ransomwares les *moins* préoccupants

#9
Perte de productivité des employés

#10
Coût du paiement de la rançon

#11
Coût des amendes pour non-respect de la réglementation/conformité

La roulette du ransomware

Le paiement de la rançon a permis une récupération ***TOTALE*** des données

Le paiement de la rançon a permis une récupération ***PARTIELLE*** des données

Le paiement de la rançon n'a permis ***AUCUNE*** récupération des données

1 sur 5 ..... des victimes d'attaque de ransomware ont eu un impact de ..... Plus de 5 M$

1 sur 20 ..... des victimes d'attaque de ransomware ont eu un impact de ..... Plus de 50 M$

Mesures de défense à portée de main

Contre-mesures techniques les plus importantes pour se prémunir contre les attaques par ransomware

Sauvegarde et récupération des données

Plateforme de protection des endpoints (EPP)

Sécurité de la messagerie électronique (avec détection de l'hameçonnage)

Sensibilisation et formation des utilisateurs

Principales contre-mesures techniques qui seront ajoutées aux défenses contre les ransomwares au cours des 12 prochains mois

Analyse du comportement des utilisateurs et des entités (UEBA)

Segmentation du réseau/Accès Zero Trust

Prévention des pertes/fuites de données (DLP)

Une lueur d'espoir… en quelque sorte

Il semble que la nature très médiatisée et à fort impact des ransomwares contribue à élever la cybersécurité au rang d'enjeu pour les conseils d'administration.

Principaux obstacles à la mise en place de défenses efficaces contre les ransomwares

Difficulté à mettre en œuvre les outils/technologies

Manque de personnel qualifié pour mettre en œuvre les solutions

Autres priorités conflictuelles

Obstacles les moins importants à la mise en place de défenses efficaces contre les ransomwares

Difficulté à justifier les demandes budgétaires correspondantes

Manque de soutien du conseil d'administration

Cliquez pour télécharger le rapport complet >>>>

zscaler