Le rapport des RSSI

Le point de vue des RSSI

Préparé par CISOs Connect en collaboration avec AimPoint Group et VV2 Communications, le CISOs Report (rapport des RSSI) se détache des gros titres et du battage médiatique d'un secteur hyperactif pour révéler les plus grandes préoccupations des responsables de la cybersécurité d'aujourd'hui, les plus gros problèmes auxquels sont confrontées leurs équipes, et les priorités et plans qu'ils mettent en place pour protéger efficacement leurs entreprises.

Un constat clé : la mise en œuvre d'un modèle de sécurité Zero Trust constitue la priorité des RSSI modernes.

Niveau de risque actuel pour les cyberattaques : EXTRÊME

75 %
touchées par au moins une cyberattaque ayant causé des préjudices matériels au cours des 12 derniers mois

57 %
touchées par plus d'une cyberattaque ayant causé des préjudices matériels au cours des 12 derniers mois

67 %
considèrent que le paysage des menaces est plus inquiétant aujourd'hui qu'il y a un an

Les cybermenaces les plus préoccupantes

- Ransomware
- Hameçonnage/ spear phishing
- Attaques contre la chaîne d'approvisionnement

Faiblesses et impacts qui préoccupent le plus les RSSI

Les plus grandes vulnérabilités

#1
Faiblesses de la sécurité des tiers (c'est-à-dire des partenaires connectés)

#2
Logiciels/ systèmes non corrigés

#3
Failles de sécurité cloud

Conséquences d'une attaque réussie

#1
Exposition de données PII/clients

#2
Temps d'indisponibilité des infrastructures/services critiques

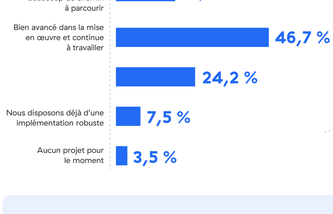
#3
Atteinte à la marque ou à la réputation

Les impacts externes préoccupent particulièrement les RSSI actuels, car les conséquences des défaillances dans ces domaines ont des répercussions vont bien au-delà du périmètre de l'entreprise.

La voie à privilégier

En réponse à l'expansion de la surface d'attaque et au paysage inexorable des menaces, une écrasante majorité d'entreprises adoptent désormais un modèle de sécurité Zero Trust.

Quel est la situation de votre entreprise concernant un modèle de sécurité Zero Trust ?



96,5 %
Pourcentage de RSSI qui misent sur un modèle de sécurité Zero Trust pour améliorer la posture de sécurité de leur entreprise

L'identité est le nouveau périmètre

La redistribution des ressources (applications, systèmes et utilisateurs) de l'intérieur de l'entreprise physique vers l'extérieur (pensez au cloud et au télétravail) a miné le périmètre traditionnel du réseau, le rendant inefficace en tant que limite de confiance. Un résultat important, et un principe clé de Zero Trust, est que l'identité est devenue le nouveau périmètre. Les changements opérés par les RSSI pour tenir compte de cette nouvelle réalité sont notamment :

- **Investissement dans des solutions destinées à atténuer le risque d'exposition des informations d'identification/identités**
- **Augmentation de l'inspection des appareils des utilisateurs avant d'accorder l'accès**
- **Investissement dans une MFA de nouvelle génération qui fournit une expérience utilisateur sans heurt**
- **Accélération de la mise en œuvre d'un modèle de sécurité Zero Trust**

Principaux investissements technologiques

Pourcentage de répondants prévoyant d'investir dans chaque technologie au cours des 12 prochains mois :

63 %
réseau/ micro-segmentation

56 %
plateforme SSE (security service edge)

53 %
Plateforme de protection des applications cloud natives (CNAPP)

41 %
tromperie / défense active

Comment Zscaler peut vous aider

Zero Trust Exchange de Zscaler permet une transformation sécurisée du cloud et protège vos utilisateurs, applications et charges de travail, peu importe où ils se trouvent. Alimenté par le plus grand cloud de sécurité au monde, Zscaler stoppe les menaces grâce à une approche à quatre niveaux :

Minimisez les surface d'attaque
Rendez les applications invisibles sur Internet et impossibles à exploiter

Empêcher l'intrusion
Bloquez les attaques grâce à l'inspection complète inline et aux informations sur les menaces fournies par le plus grand cloud de sécurité au monde

Éradiquer le mouvement latéral
Connecter les utilisateurs directement aux applications sans jamais exposer le réseau

Arrêter la perte de données
Prévenir le vol de données et l'exposition accidentelle sur les appareils gérés et non gérés, le cloud public et les SaaS

Rendez-vous sur www.zscaler.fr pour découvrir comment Zscaler peut aider votre entreprise à réduire les risques, et pourquoi nous avons été classés parmi les leaders du Magic Quadrant™ de Gartner® pour le SSE (Security Service Edge).

Télécharger le rapport complet

Copyright © 2022, CISOs Connect.
Tous droits réservés.

CISOs CONNECT