zscaler

THE RESILIENCE FACTOR

Les entreprises doivent prêter plus d'attention à la cyber-résilience

Un nouveau rapport de Zscaler, intitulé **« Déverrouiller le pouvoir de la résilience : pourquoi être « Resilient by design » est le prochain impératif de cybersécurité »**, souligne qu'une hiérarchisation plus pertinente des priorités et qu'un investissement plus important s'imposent pour garantir que les stratégies de cyber-résilience soient adaptées aux inévitables scénarios de défaillance futurs.

PRINCIPALES CONCLUSIONS

Dans un contexte de menaces en constante évolution et d'un environnement opérationnel de plus en plus versatile, la continuité d'activité est en péril.

45 % des entreprises ont subi un **scénario de défaillance majeur** au cours des 6 derniers mois

60 % des entreprises s'attendent à affronter un scénario de défaillance majeur au cours des **12 prochains mois**

Les responsables informatiques se sentent bien préparés à ces scénarios de défaillance.

49 % des responsables informatiques estiment que leur infrastructure informatique est **hautement résiliente**

78 % qualifient l'approche de leur entreprise en matière de cyber-résilience de **mature**

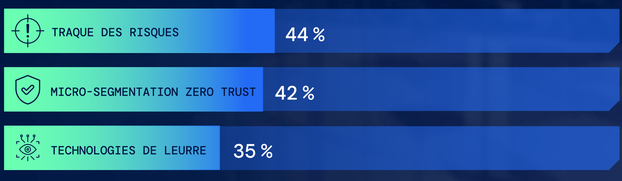
94 % estiment que leurs mesures actuelles de cyber-résilience sont **efficaces**

Cependant, un examen plus approfondi révèle des incohérences, des lacunes et des pratiques peu efficaces.

SEULEMENT **45 %** des responsables informatiques déclarent que leur stratégie de cyber-résilience est **à jour** face à l'essor de l'IA.

40 % admettent **ne pas avoir réévalué** leur stratégie de cyber-résilience au cours des 6 derniers mois.

Moins de la moitié des entreprises utilisent tous les outils de sécurité proactifs suivants.



Les dirigeants d'entreprise se montrent peu investis, ce qui constitue une problématique.

SEULS 39 % des responsables informatiques estiment que la cyber-résilience est une priorité absolue pour les dirigeants d'entreprise.

49 % s'accordent à penser que le budget alloué à la cyber-résilience ne répond pas à des besoins en constante évolution.

SEULS 36 % déclarent que la stratégie de cyber-résilience est intégrée dans la stratégie globale de résilience de leur entreprise.

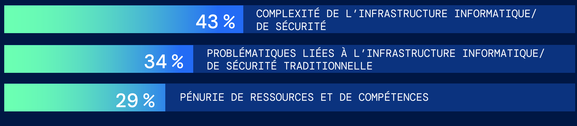
SEULS 44 % déclarent que le DSSI/RSSI est impliqué dans la planification de la résilience.

Un changement de culture s'impose pour lever les principaux freins au déploiement d'une stratégie de cyber-résilience robuste.

60 % des responsables informatiques estiment que leur entreprise accorde une priorité excessive à la prévention dans sa stratégie de cybersécurité.

57 % déclarent que leurs dirigeants continuent de penser d'un échec de la cybersécurité est lié à l'accès initial obtenu par un acteur malveillant.

Les trois principaux freins à une meilleure résilience :



Intégrer d'emblée la cyber-résilience dans la stratégie d'entreprise.

Les responsables informatiques voient le lien entre une stratégie de cyber-résilience robuste et de meilleures performances d'entreprise, mais peinent à obtenir des résultats dans le cadre de leurs efforts actuels.

56 % constatent une **réduction** des pertes de données.

53 % observent une restauration **plus rapide** après un incident.

49 % font état d'une détection et d'un confinement **accélérés** des incidents.

Le contexte économique actuel exige que les entreprises accordent davantage d'attention à la cyber-résilience, qu'elles financent davantage ce projet, l'actualisent plus fréquemment et qu'elles en attendent davantage. Un changement fondamental d'approche et de mentalité s'impose pour faire de la cyber-résilience un élément essentiel de la stratégie de sécurité, pris en compte dès sa conception. C'est le principe même de la notion de **« Resilient by Design »**.

Pour en savoir plus sur la mise en œuvre d'une approche « Resilient by design », rendue possible par la plateforme Zero Trust Exchange, cliquez ici. Consultez le rapport.

MÉTHODOLOGIE

En décembre 2024, Zscaler a chargé Sapio Research de mener une enquête auprès de 1 700 responsables informatiques sur 12 marchés (Australie, France, Allemagne, Inde, Italie, Japon, Pays-Bas, Singapour, Espagne, Suède, Royaume-Uni et Irlande, États-Unis). Ces professionnels IT évoluent dans des organisations qui comptent plus de 500 collaborateurs issues de tous les secteurs d'activités.

À PROPOS DE ZSCALER

Zscaler (NASDAQ : ZS) aide les entreprises à accélérer leur transformation numérique en renforcant leur agilité, leur efficacité, leur résilience et leur sécurité. Sa plateforme Zero Trust Exchange™, conçue sur les principes du SASE, protège des milliers de clients contre les cyberattaques et la perte de données en assurant une connexion sécurisée entre utilisateurs, dispositifs et applications partout dans le monde. Avec plus de 160 centres de données répartis à l'échelle mondiale, Zero Trust Exchange™ s'impose comme la plus grande plateforme de sécurité cloud native.

zscaler