Décalage des incitants

Motivés par les forces du marché, les cybercriminels distancent désormais les professionnels de la sécurité.

Un décalage en trois dimensions

Le décalage entre la cybercriminalité et la réponse des équipes de sécurité est complexe. Il intervient à plusieurs niveaux : entre les pirates et les professionnels de la sécurité, entre la stratégie et l'implémentation, et entre les dirigeants et les exécutants des entreprises.

Cybercriminels

Agiles et rapides

Les incitants des pirates trouvent leur origine dans un marché fluide et décentralisé, favorisant l'agilité et la rapidité d'adaptation.

contre

Professionnels de la sécurité

Entravés par la bureaucratie

Les professionnels de la sécurité sont entravés par la bureaucratie et par un modèle décisionnel descendant.

Stratégie

90 %

Plus de 90 % des entreprises ont défini une stratégie de cybersécurité.

contre

Implémentation

Moins de 50 %

Moins de la moitié des entreprises ont implémenté leur stratégie dans son intégralité.

Cadres

Mesure différente du succès

Les cadres dirigeants qui conçoivent les stratégies de cybersécurité mesurent le succès différemment des responsables de l'implémentation.

contre

Exécutants

Efficacité limitée

Les exécutants qui mettent les stratégies en pratique sont limités par les cadres dirigeants.

L'ampleur du décalage

Bien que les risques de cybersécurité constituent plus que jamais une source de préoccupation pour les entreprises, il existe diverses lignes de fracture au niveau de la gestion des risques et des incitants proposés aux équipes, ainsi que des failles inhérentes au décalage entre les modes opératoires des pirates et la marge de manœuvre dont disposent les professionnels de la sécurité.

76 %

Pour 76 % des répondants, les risques de cybersécurité figurent désormais parmi les trois principaux facteurs de risque.

54 %

54 % des cadres dirigeants interrogés sont davantage préoccupés par l'impact sur la réputation que par les effets réels d'un incident de cybersécurité.

83 %

83 % des répondants continuent de faire état de dommages dus à des compromissions de la cybersécurité.

5 x plus

Les opérateurs étaient cinq fois plus nombreux à estimer qu'aucun incitant n'existe en matière de cybersécurité.

Idées/argent

Les cybercriminels de haut niveau volent des idées, tandis que les criminels de bas étage dérobent de l'argent.

51 %

Seuls 51 % des experts en informatique interrogés en Russie avaient trouvé un emploi dans le secteur informatique légitime.

42 %

42 % des vulnérabilités sont exploitées par les criminels dans les 30 jours suivant leur détection.

Enseignements à tirer du marché criminel

Rapprochement entre le marché criminel et les professionnels de la sécurité

Amélioration de la transparence

La généralisation du partage d'informations peut contribuer à réduire les coûts encourus par les équipes de sécurité en réduisant la duplication, et à faire connaître les technologies et pratiques offrant des améliorations significatives de la sécurité.

Ajustement des incitants

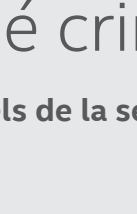
Pour renforcer la motivation à tous les échelons, des dirigeants aux opérateurs, des incitants tels que des primes et des distinctions honorifiques doivent être proposés aux employés et aux responsables qui assurent une protection performante.

Exploitation des forces du marché

L'externalisation et le recours à des travailleurs indépendants peuvent contribuer à réduire les coûts, à renforcer la concurrence et à favoriser la généralisation de meilleures pratiques innovantes.

Ouverture de l'accès au marché

L'extension du vivier de compétences, par exemple en ouvrant la porte aux jeunes générations et aux experts en TIC étrangers qui basculent souvent dans la cybercriminalité, peut contribuer à pallier la pénurie de compétences en cybersécurité pour les entreprises, en plus de priver les marchés criminels de ces talents.



Utilisation des divulgations publiques

Une réaction accélérée aux divulgations publiques de vulnérabilités par la mise en œuvre de pratiques de correction plus efficaces et le remplacement plus rapide des anciens systèmes peut renforcer la sécurité et augmenter le coût des attaques pour les cybercriminels.

Réduisez le décalage.
Suivez l'exemple des pirates.
Adaptez-vous pour prospérer.

Pour obtenir le rapport complet :
www.mcafee.com/misaligned.

intel Security

2504_0217_info-misaligned-incentives-cybercriminals-defenders