

ÉTUDE

Le facteur humain dans la cyberdéfense

Pourquoi la sanction échoue, et ce qui fonctionne à sa place

L'utilisateur est régulièrement présenté comme le maillon faible de la sécurité. Cette formule est commode et contre-productive : elle désigne un coupable là où il faudrait décrire un système. Ce document propose une autre lecture, et la méthode qui en découle.

Le problème n'est pas l'inattention

Les messages d'hameçonnage qui aboutissent ne sont pas grossiers. Ils reprennent une chaîne de traitement réelle : une facture attendue, une demande hiérarchique, une notification d'un outil effectivement utilisé dans l'entreprise. Ils arrivent au moment où la personne est en train de faire exactement ce que le message lui demande de faire.

Autrement dit, la victime ne se distrait pas de son travail : elle le fait. Un dispositif de sensibilisation qui traite l'événement comme une faute d'attention passe à côté de son objet.

Pourquoi la sanction est contre-productive

Sanctionner le clic produit un effet mécanique et prévisible : les gens cessent de signaler. Or le signalement est la seule source d'information précoce dont dispose une organisation sur ce que reçoivent réellement ses collaborateurs.

Une organisation qui punit le clic obtient des statistiques de clic flatteuses et un délai de détection dégradé. Elle a amélioré son indicateur et affaibli sa défense.

Le raisonnement vaut au-delà de l'hameçonnage. Toute règle de sécurité qui rend le travail impossible est contournée, et le contournement devient une pratique tacite que personne ne documente — donc que personne ne sécurise.

Ce qui fonctionne

Rendre le signalement plus rapide que le doute

Un bouton de signalement dans le client de messagerie, une réponse systématique à celui qui signale, y compris quand le message était légitime. L'objectif n'est pas d'obtenir zéro clic : c'est d'obtenir un signalement en quelques minutes plutôt qu'une découverte en quelques semaines.

Simuler pour enseigner, pas pour classer

Les campagnes de simulation ont une valeur pédagogique réelle à deux conditions : que le résultat individuel ne soit pas transmis à la hiérarchie, et que la personne qui clique reçoive immédiatement une explication utile plutôt qu'un rappel à l'ordre. La bonne question après un clic n'est pas « pourquoi avez-vous cliqué », mais « qu'est-ce qui, dans ce message, ressemblait à votre quotidien ».

Adapter le contenu au poste

La comptabilité est exposée à la fraude au virement, la direction à l'usurpation d'identité, l'informatique à la compromission de comptes à privilèges, l'accueil aux supports amovibles et aux visiteurs. Une sensibilisation générique traite tout le monde comme personne.

Réduire ce qui repose sur la vigilance

La mesure la plus efficace consiste à diminuer le nombre de décisions laissées au jugement individuel : authentification à plusieurs facteurs, filtrage des pièces jointes, bannière signalant les messages externes, double validation des changements de coordonnées bancaires. Chaque décision retirée à l'utilisateur est une décision qu'il ne peut plus rater.

Mesurer autre chose que le taux de clic

Le taux de clic est un indicateur pauvre : il varie avec la difficulté du message envoyé et se manipule facilement. Trois indicateurs disent davantage de la solidité réelle d'une organisation.

- Le taux de signalement, et surtout sa progression dans le temps
- Le délai entre la réception d'un message malveillant et son premier signalement
- La proportion de collaborateurs ayant signalé au moins une fois — un taux de signalement porté par dix personnes n'est pas une culture de sécurité

En résumé

Le facteur humain n'est pas une faiblesse à corriger, c'est un capteur à activer. Une organisation où les gens signalent vite détecte vite. Cela suppose de renoncer à la logique de faute, d'outiller le signalement, et d'accepter que le bon indicateur ne soit pas le plus flatteur.

Ce document a une vocation informative et ne constitue pas un conseil juridique. Pour situer votre exposition réelle et vos priorités, échangez avec un expert ASEVIO : www.asevio.com/contact