ESI® BENCHMARK REPORT

ÉDITION 2023

UNE ÉVALUATION DE PLUS DE
1,7 MILLION D'ATTAQUES
SIMULÉES DE SPEAR PHISHING
SUR DES EMPLOYÉS.

EMPLOYEE SECURITY INDEX

HORNETSECURITY

ESI® BENCHMARK REPORT
RAPPORT DE RÉFÉRENCE ESI® 2023

Chapitre 1: Sommaire exécutif

L'hameçonnage, un fléau qui se propage sans fin : le nombre de tentatives d'escroquerie avec de faux courriels continue d'atteindre des records. Les auteurs d'actes d'hameçonnage ciblent de plus en plus les entreprises, car c'est là qu'ils peuvent gagner le plus d'argent. Ils envoient des courriels qui n'éveillent aucun soupçon aux employés pour voler des informations sensibles, crypter des données ou, dans le pire des cas, paralyser l'ensemble des activités de l'entreprise.

Dans notre ESI® Benchmark Report (rapport de référence ESI®), nous vous présentons les dangers croissants de l'hameçonnage pour votre entreprise et des options de défense efficaces. L'accent est mis sur la formation et sur la sensibilisation à la sécurité de Hornetsecurity, grâce à laquelle vous pouvez former vos employés à adopter de meilleurs comportements en matière de sécurité et établir une culture de sécurité informatique durable. L'Employee Security Index (ESI®) breveté est au cœur même de nos solutions. Il offre un indicateur clé scientifiquement fondé pour mesurer et surveiller la sensibilisation à la sécurité.

Notre ESI® Benchmark actuel montre exactement comment cela fonctionne. Dans cette étude qui dresse un tableau transparent de la situation, nous avons évalué environ 1,8 million d'attaques de hameçonnage simulées contre des employés d'entreprises de toutes tailles et de tous secteurs et nous vous fournissons des recommandations importantes pour optimiser la sensibilisation à la sécurité de vos employés.

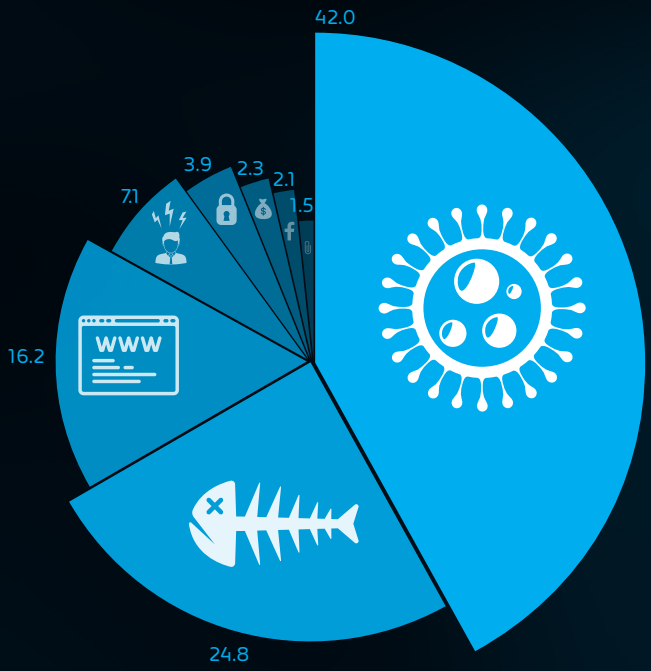
L'étude a surtout démontré que les entreprises de tous les secteurs atteignent un niveau de sécurité acceptable – qui correspond au moins à un ESI de 70 – en moyenne après seulement trois mois de formation sur la sensibilisation à la sécurité. En revanche, au fur et à mesure que la formation se poursuit, ils ont du mal à maintenir ce niveau. D'une part, cela est dû au fait que le niveau de difficulté des simulations d'hameçonnage augmente au fil du temps, alors que dans le même temps, de nouveaux employés intègrent constamment la formation. Les entreprises ont donc tout intérêt à opter pour une période de formation permanente.

Les résultats de l'étude ont également révélé que les scénarios d'hameçonnage les plus réussis exploitent la soumission aveugle à l'autorité des employés en tant que facteur psychologique. Les gestionnaires en particulier sont appelés à montrer l'exemple en matière de sécurité informatique. Ils doivent motiver les employés à participer à la formation sur la sensibilisation à la sécurité et à partager leurs expériences les uns avec les autres.

Chapitre 2 : Hameçonnage : en tête de liste pour les cyberattaques

L'hameçonnage est devenu une menace omniprésente. Le rapport fédéral sur la situation de la cybercriminalité de l'Office fédéral de la police criminelle allemande (BKA) a enregistré une augmentation significative du nombre d'hameçonnages en 2021 et a classé la fraude par courriels falsifiés comme l'un des types de cyberattaques les plus courants.[1]

Plus de 90 % des cyberattaques commencent désormais par un courriel d'hameçonnage. Le rapport Hornetsecurity sur les cybermenaces 2021-2022 a révélé que 40 % de l'ensemble du trafic du courrier électronique constitue une menace potentielle.[2] Il peut s'agir, par exemple, d'envois de masse aléatoires ou de courriels personnels de harponnage, pour lesquels une victime est espionnée pendant des semaines, voire des mois.



ATTACK STATISTIC	%
Andere	42.0
Phishing	24.8
URL	16.2
Ransom	7.1
Executable in archive/disk-image	3.9
Advance-fee scam	2.3
Brand Impersonation	2.1
Maldoc (malicious attachment)	1.5

Fig. 1 : The most popular email attack tactics in the 1st half of 2021

Graves conséquences pour les entreprises

Pour les entreprises concernées, un harponnage réussi peut entraîner des dommages financiers importants et une grave perte de confiance de la part des clients et partenaires. Dans des courriels qui semblent authentiques, les fraudeurs se font passer pour des supérieurs, des collègues ou des partenaires commerciaux afin d'inciter les employés à divulguer des données hautement sensibles ou à cliquer sur des liens et des pièces jointes malveillants. Ils demandent parfois aux employés de transférer de grosses sommes d'argent sur de faux comptes au nom de prétendus supérieurs. Dans d'autres cas, une attaque réussie peut servir de passerelle vers l'ensemble du réseau de l'entreprise.

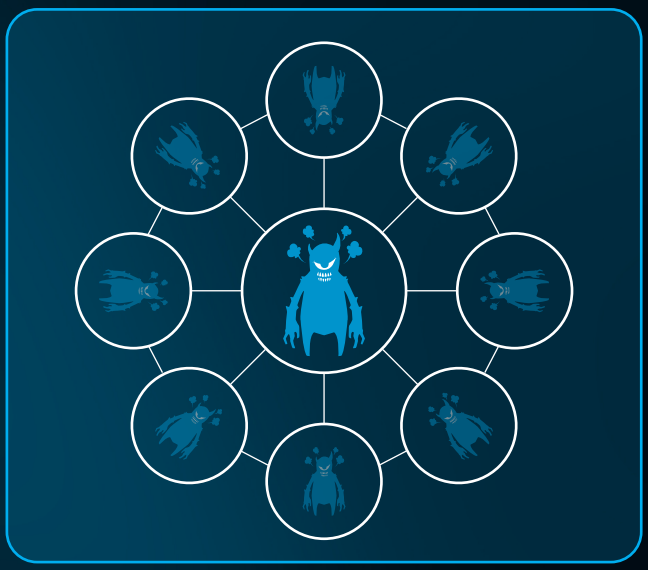
Fig. 2 : Dommages causés par la cybercriminalité aux entreprises en Allemagne, selon Bitkom.

Pas de répit en vue

Une diminution du nombre actuel d'actes d'hameçonnage n'est pas prévisible en raison de l'attractivité de cette pratique – bien au contraire. La pandémie du coronavirus s'est déjà révélée être un catalyseur désastreux, comme le montre le Microsoft Digital Defense Report 2021 (rapport Microsoft sur la défense numérique 2021).[3]

Selon ce rapport, de nombreux cybercriminels voient des opportunités dans l'exploitation des vulnérabilités qui résultent du nombre accru d'employés travaillant à domicile et des mesures de sécurité informatique insuffisantes des entreprises.

Une autre vague majeure d'hameçonnage a commencé avec le début de l'invasion de l'Ukraine par la Russie. Les cybercriminels se font notamment passer pour des institutions bancaires. Ils prétendent devoir vérifier si les clients respectent les sanctions de l'Union européenne (UE) contre la Russie – et accèdent à leurs informations de connexion via des sites Web bancaires fictifs. Ils n'ont besoin d'aucune connaissance en programmation pour falsifier les masques de saisie, mais peuvent utiliser des progiciels d'hameçonnage disponibles sur le Darknet (Web invisible) pour de petites sommes ou même gratuitement. Grâce à ces boîtes à outils, les fraudeurs peuvent désormais arriver à contourner l'authentification traditionnelle à deux facteurs (2FA), qui était auparavant considérée comme l'une des méthodes les plus efficaces pour protéger les comptes en ligne.



Gangs de fraudeurs actifs dans le monde entier

Les exemples montrent que les auteurs d'actes d'hameçonnage ont de moins en moins de scrupule et que leurs méthodes sont de plus en plus sophistiquées. Les actes délictuels sont de plus en plus commis par des gangs de fraudeurs organisés à l'échelle internationale qui comptent des centaines de membres et regroupent un large éventail de savoir-faire spécialisé afin de couvrir de manière professionnelle toute la chaîne des attaques. Selon le BKA, de plus en plus d'auteurs d'actes malveillants proposent même des attaques d'hameçonnage ciblées basées sur le modèle « crime-as-a-service » (crime en tant que service).

Au sein des cybergangs, certains « experts » sont chargés de rechercher des informations pouvant être trouvées sur les destinataires potentiels dans les réseaux sociaux et d'autres sources Internet, telles que les portails d'évaluation des emplois ou les sites Web des entreprises. Les utilisateurs assidus de médias sociauxsont des proies particulièrement faciles pour les auteurs d'acte de harponnage, comme le montre une étude conjointe de l'Université technique de Darmstadt et d'IT-Seal.4 Les fraudeurs sont heureux d'utiliser les données de profil de leurs victimes qui sont accessibles au public : données sur leur travail actuel, leur formation, leurs certificats, leurs loisirs ou leurs collègues pour créer des courriels de harponnage personnalisés.

Les membres du gang responsables de la conception descourriels malveillants jouent un rôle particulier. En plus de faire semblant d'être des initiés, ils doivent maîtriser les astuces psychologiques importantes pour tromper leurs victimes. Que ce soit la soumission aveugle à l'autorité, la curiosité, la volonté d'aider, le sentiment d'urgenceou la peur : quiconque s'appuie sur l'un de ces facteurs d'influence psychologique peut être à peu près certain que le destinataire du courriel suivra ses demandes sans réfléchir.

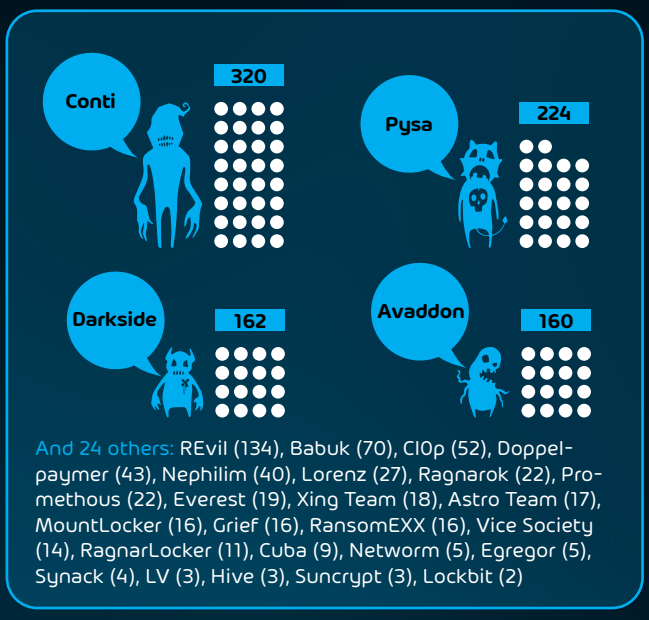


Fig. 3 : Les bandes de fraudeurs qui ont publié le plus de fuites de données personnelles volées ou extorquées

En savoir plus

Chapter 3 : Employee Security Index (ESI®) : la référence pour mesurer les progrès d'apprentissage

Hornetsecurity est un fournisseur de services de formation sur la sensibilisation à la sécurité regroupant des contenus, méthodes et outils de formation en une offre de services innovante. L'Employee Security Index (ESI®) breveté d'IT-Seal, appartenant au Groupe Hornetsecurity depuis mai 2022, est la principale marque distinctive. Cet indice fournit une référence scientifiquement fondée qui peut être utilisée pour mesurer et surveiller objectivement le comportement des employés en matière de sécurité.

Cette tâche n'est pas possible avec les méthodes de mesure employées jusqu'ici qui ne permettent aucune normalisation – et donc aucune possibilité de comparaison sur de plus longues périodes ou entre différents services, rôles et sites de l'entreprise.

À cela s'ajoute le risque que les problèmes de sécurité individuels, les erreurs ou les clics sur les courriels de harponnage soient surestimés ou sous-estimés et le fait que les entreprises n'ont finalement aucune visibilité sur le comportement de sécurité de leurs employés. Elles investissent donc souvent trop ou trop peu pour atteindre un niveau de sécurité approprié.

Le temps de préparation est crucial

Il en va autrement de l'ESI®, qui représente une méthode proche de la réalité et reproductible de mesure de la sensibilisation à la sécurité. Pour calculer l'ESI®, les attaques de harponnage sont divisées en différentes catégories (appelées « niveaux »), en fonction du temps que les cybercriminels doivent investir dans la préparation et l'exécution. Il s'agit, entre autres, de la collecte d'informations auprès de sources accessibles au public, la préparation technique, la copie de sites Web et la maintenance de l'infrastructure informatique nécessaire à une attaque d'hameçonnage. On distingue sept catégories, chacune correspondant à un temps de préparation d'une heure à plusieurs jours, voire semaines. L'ESI® individuel d'une entreprise est établi en fonction de la façon dont les employés réagissent aux simulations d'hameçonnage présentant divers degrés de difficulté.

Afin de pouvoir classer le niveau de sécurité d'une entreprise de manière standardisée, Hornetsecurity a défini des valeurs de tolérance pour un comportement de sécurité exemplaire par les groupes de test. Ces valeurs sont basées sur les « taux de réussite » du point de vue de l'intrus. Comme les « taux de réussite » de 0 sont illusoires (tout le monde fait des erreurs), les valeurs de tolérance se situent quelque part à la ligne de démarcation entre la sécurité et la faisabilité. Un groupe test modèle avec les « taux de réussite » les plus bas obtient au moins un ESI® de 90 sur une échelle de 0 à 100. Si un comportement critique se manifeste deux fois plus souvent, le groupe obtient un ESI® de seulement 80. Si le comportement se manifeste trois fois plus souvent, il n'atteint qu'un ESI® de 70. Les résultats inférieurs à 70 sont considérés comme critiques. Les valeurs de tolérance définies par Hornetsecurity sont en fonction de l'état actuel de la recherche et de l'expérience des simulations d'hameçonnage dans des entreprises issues des secteurs les plus divers.

L'ESI® offre ainsi aux entreprises une référence tangible et fiable pour comparer les différents groupes d'employés de manière standardisée. Qui est le plus sûr, le service commercial ou le service des ressources humaines, et comment la direction se compare-t-elle au service comptable? Ces informations sont précieuses lorsqu'il s'agit de définir de manière ciblée des mesures de formation continue.

Chapitre 4 :

ESI® BENCHMARK REPORT
PRINCIPAUX RÉSULTATS ET MEILLEURES PRATIQUES

Le rapport de référence actuel montre l'efficacité de l'ESI® pour mesurer et optimiser la sensibilisation des employés à la sécurité. À cette fin, environ 1,8 million d'attaques de harponnage simulées ont été évaluées. Ces attaques ont été menées entre mai 2019 et juin 2022 sur environ 140 000 utilisateurs de 350 entreprises de toutes tailles et de tous secteurs.

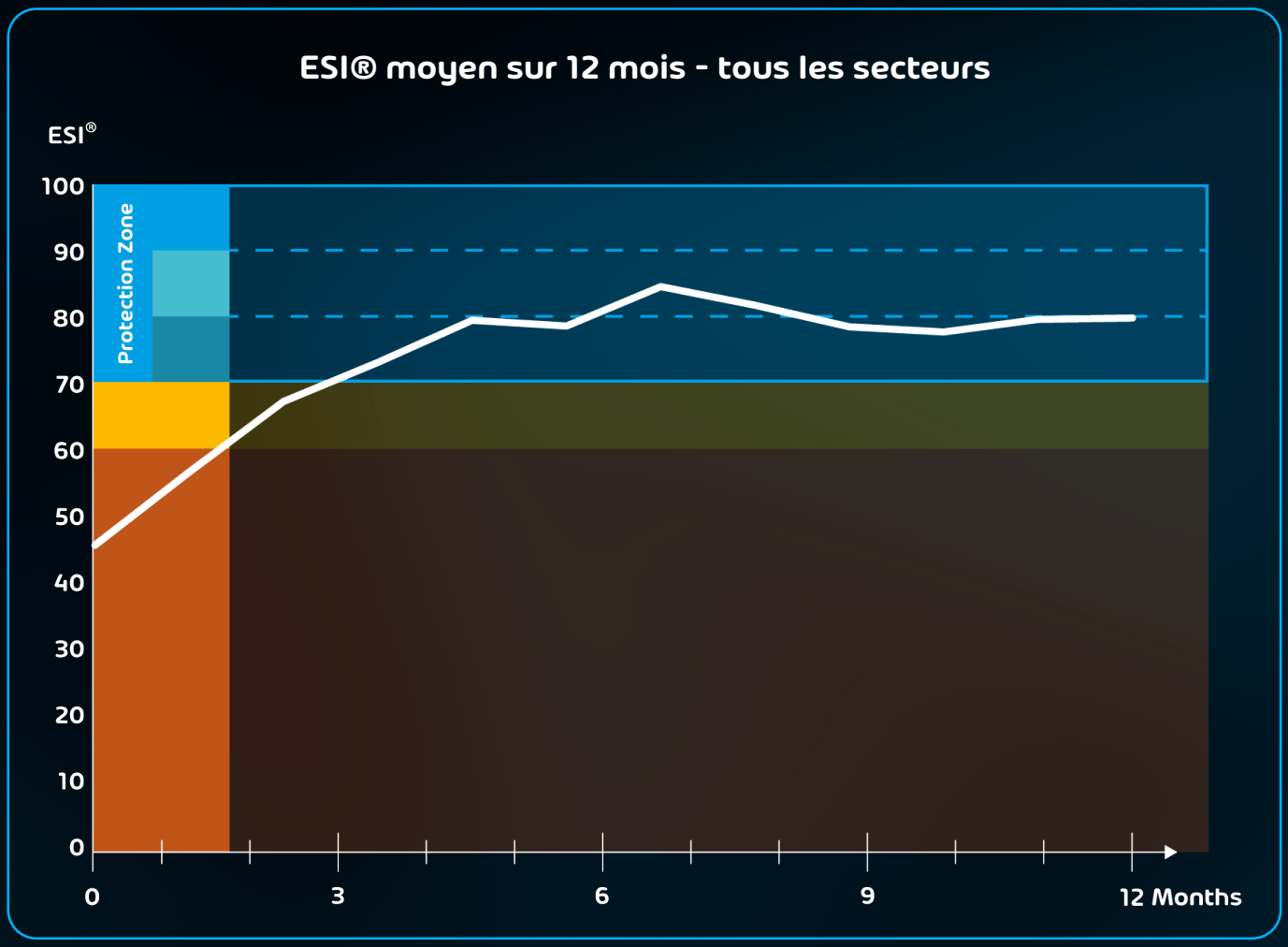
Le comportement des utilisateurs a été observé sur une période de formation de douze mois dans chaque cas. L'influence que des facteurs tels que l'appartenance à un secteur d'activité, la fonction et la position d'un employé dans l'entreprise ontsur les taux de clics apparaît ainsi clairement. Les effets de facteurs externes tels que l'évolution, les interruptions de formation et l'utilisation d'astuces psychologiques ont également été examinés. Les résultats de l'ESI® Benchmark fournissent des informations sur les mesures de formation de sensibilisation qui peuvent être utilisées pour atteindre une sensibilisation optimale à la sécurité parmi les différents groupes d'utilisateurs.

En voici une petite sélection.

HORNETSECURITY

IT-SEAL
Part of HORNETSECURITY group

Évaluation 1 : évolution moyenne de l'ESI®



Formation continue sur la sensibilisation nécessaire

L'évolution moyenne de l'ESI® sur douze mois montre clairement l'importance d'une formation continue sur la sensibilisation à la sécurité pour les employés. Un haut niveau de sécurité ne peut être maintenu sur une plus longue période que si les simulations de harponnage sont répétées régulièrement et adaptées en permanence aux dernières méthodes des attaquants.

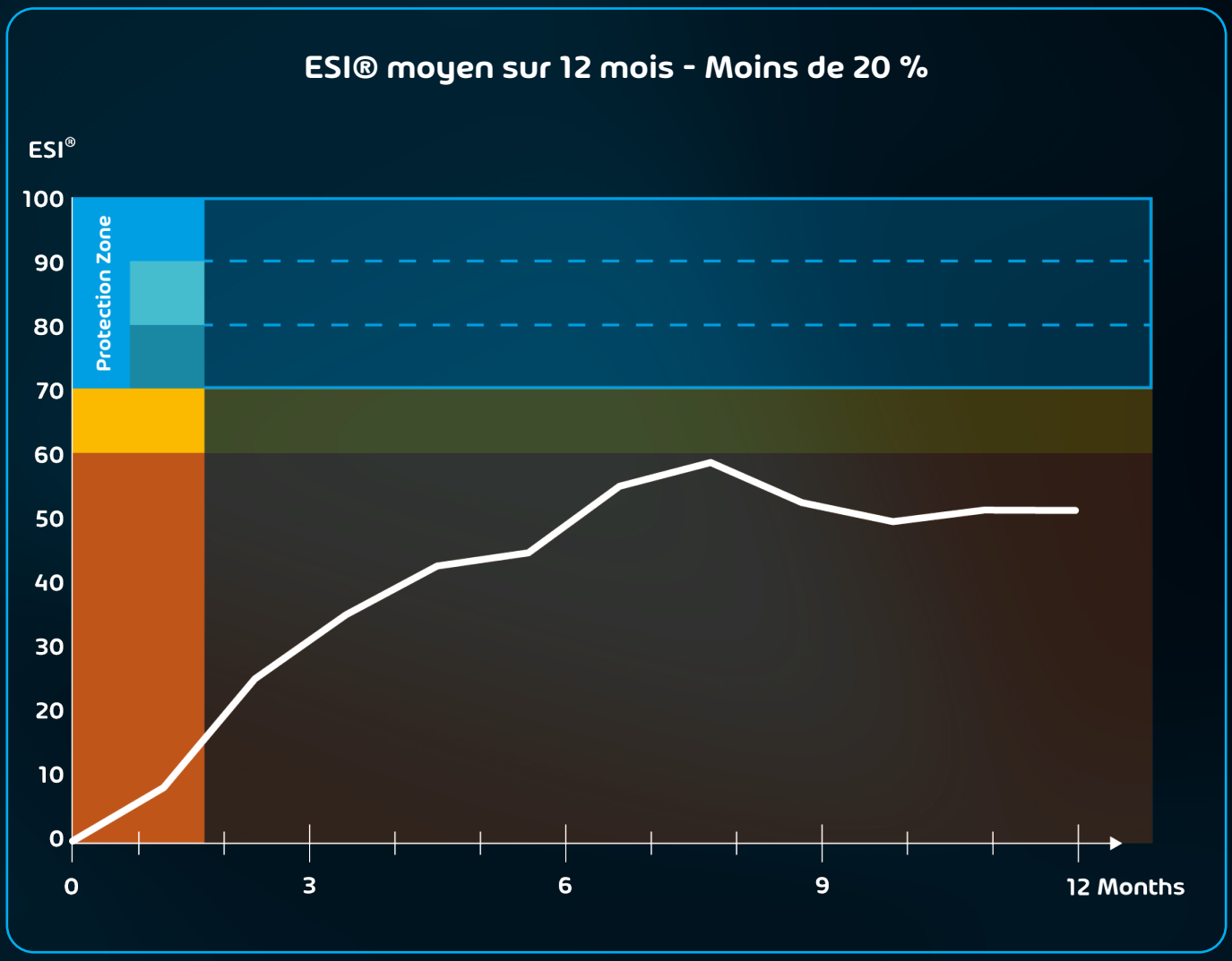
Comme le montre le graphique, la courbe ESI® monte fortement après le début de la formation de sensibilisation et atteint un niveau de sécurité acceptable après une moyenne de trois mois. Cependant, les entreprises et les organisations ont du mal à maintenir ce niveau sur le long terme. D'une part, cela est dû au fait que les employés oublient les leçons apprises dans les simulations de harponnage au fil du temps.

Pour que le personnel continue de « s'exercer », les entreprises et les organisations devraient donc miser sur des périodes de formation permanente. Ce n'est qu'en répétant régulièrement les attaques de harponnage simulées que l'on peut garantir que les employés reconnaissent l'importance des informations qu'ils reçoivent et les mémorisent pour toujours.

D'autre part, les entreprises embauchent constamment de nouveaux employés qui doivent être sensibilisés aux dangers de l'hameçonnage et formés à la reconnaissance des courriels malveillants. Grâce à des campagnes de sensibilisation continues, il est également possible d'intégrer de manière transparente les nouveaux employés dans les formations et de les encourager à assumer personnellement la responsabilité de la sécurité informatique.

En savoir plus

Évaluation 2 : ESI® chez les « moins de 20 % »



Zero formation selon le « principe de saupoudrage » !

Toute chaîne est aussi solide que son maillon le plus faible. L'évolution de l'ESI® du groupe des « moins de 20 % » montre que cette connaissance s'applique également au « pare-feu humain » pour se protéger contre les attaques de harponnage insidieuses. Il s'agit du groupe d'utilisateurs qui a les taux de clics les plus élevés sur les fausses attaques de harponnage.

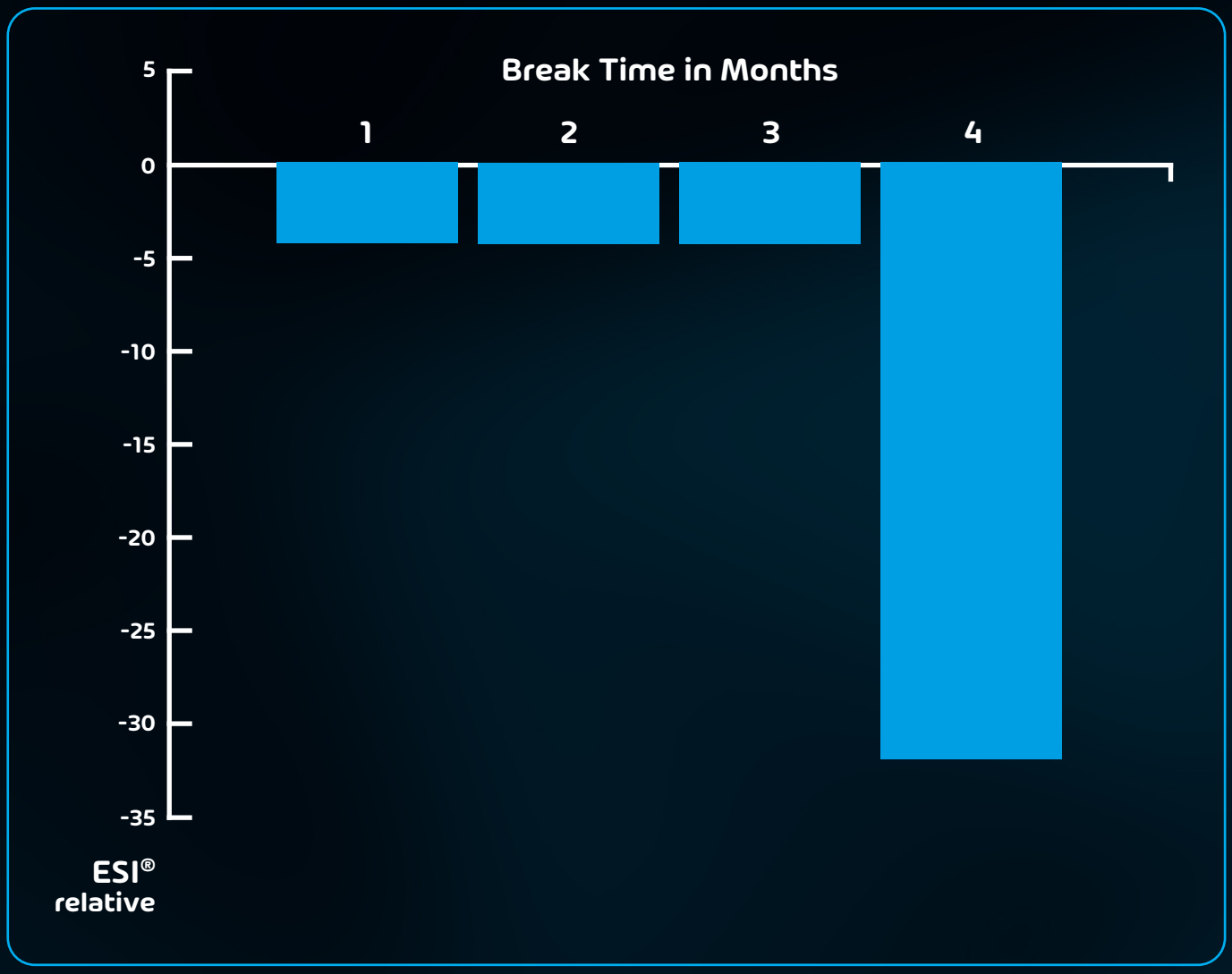
Il est vrai que l'on observe également chez le groupe des « moins de 20 % » un certain effet d'apprentissage dans les douze mois, comme le montre la courbe ci-dessus. Cependant, pendant cette période, le groupe ne peut pas atteindre une seule fois un niveau de sécurité adéquat, c'est-à-dire un ESI® d'au moins 70, et ce, malgré le fait que les « moins de 20 % » aient reçu la même formation sur la sensibilisation à la sécurité que leurs collègues.

Les résultats de l'enquête montrent clairement que les cours de formation à la sécurité ne doivent pas être répartis selon le principe de saupoudrage, mais doivent être adaptés aux besoins d'apprentissage individuels des employés. En effet, tous les utilisateurs n'apprennent pas de la même manière, aussi vite et aussi bien.

L'ESI® permet aux entreprises de répondre rapidement et facilement aux différents besoins de formation de leurs employés. Il offre un indicateur tangible et fiable pour documenter les progrès d'apprentissage personnels et en déduire l'utilisation ciblée de mesures de formation adaptées. Si des utilisateurs comme ceux du groupe des « moins de 20 % » affichent des taux de clics accrus, ils doivent être formés de manière plus intense.

En savoir plus

Évaluation 3 : baisse de l'ESI® après une pause



Pauses de formation pour une acquisition durable des connaissances

La sensibilisation des employés à la sécurité est comme un muscle qui se relâche sans exercice régulier. Si des groupes individuels ou des employés interrompent la formation pendant un certain temps, puis recommencent, on constate une nette baisse du comportement de sécurité. Ces utilisateurs semblent avoir oublié le contenu d'apprentissage important des simulations de harponnage et sont devenus beaucoup plus négligents dans le traitement des courriels entrants.

La baisse de l'ESI® dans ce graphique montre à quel point cet effet est fort, même si les groupe des « moins et plus de 25 % » – c'est-à-dire les groupes d'utilisateurs avec des taux de clics particulièrement élevés et particulièrement faibles – n'ont pas été pris en compte. Après le premier mois de pause de la formation, l'ESI® baisse de cinq points et se situe ainsi souvent à nouveau en dessous du niveau de sécurité cible. Après quatre mois sans formation de sensibilisation, l'ESI® a déjà reculé de plus de 30 points. Concrètement, cela signifie que les entreprises sont presque revenues à la case départ en ce qui concerne le comportement de sécurité de leurs employés.

Cependant, de courtes pauses dans la formation peuvent certainement aussi avoir un intérêt pédagogique et didactique pour l'entreprise. Une fois que certains groupes ou employés ont atteint le niveau de sécurité souhaité, ils doivent délibérément faire une pause d'une durée de deux à trois mois. En effet, il a été démontré qu'un contenu d'apprentissage, une fois acquis, a un effet plus durable sur le comportement de sécurité s'il est actualisé à nouveau après une certaine pause. Cela peut également prévenir une éventuelle « fatigue de sécurité » chez les employés.

En savoir plus

Évaluation 4 : secteur technologique par rapport à la moyenne

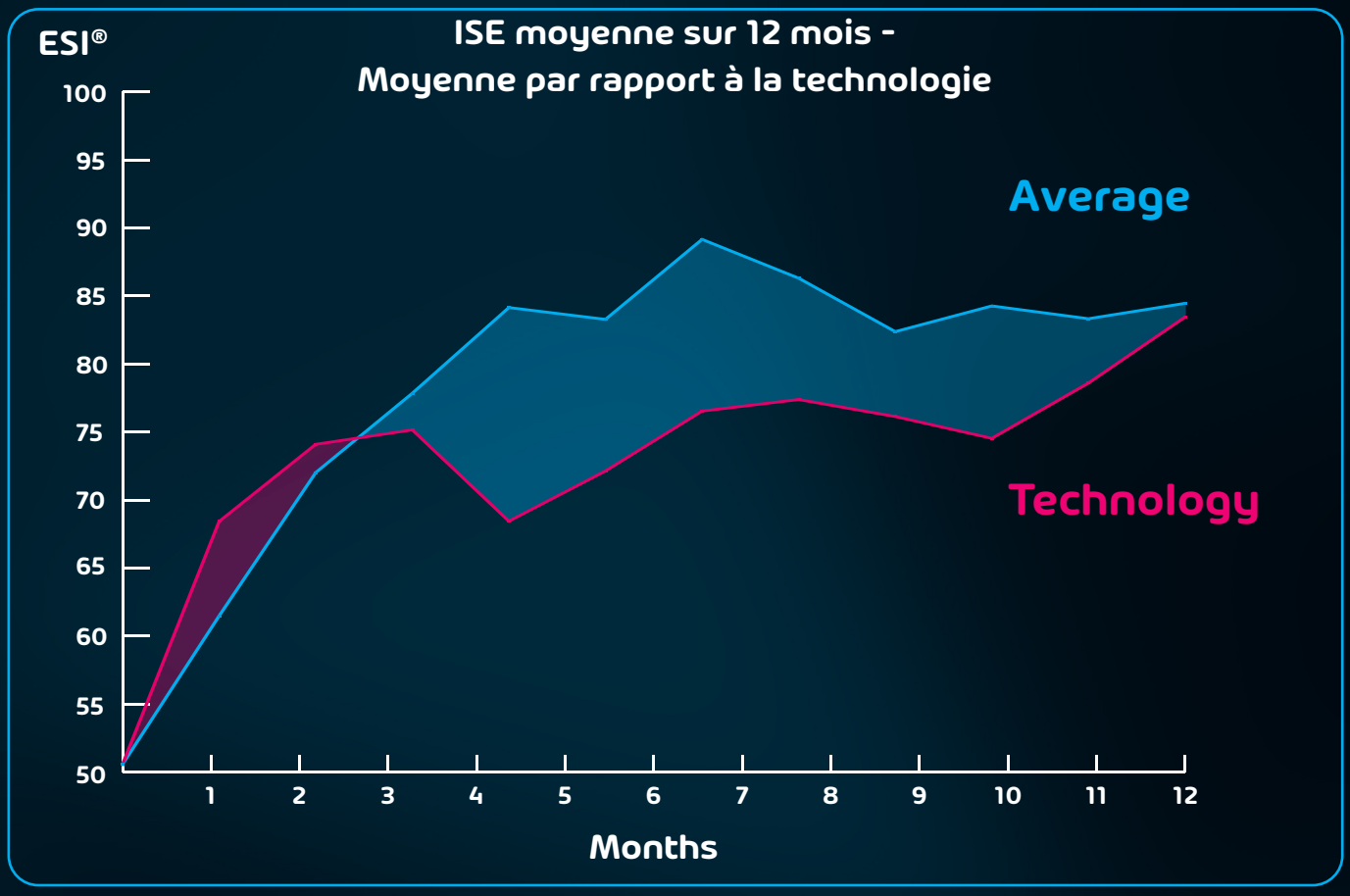


Fig. X : Secteur technologique vs. moyenne ESI® Evolution sur 12 mois

« Féru de technologie » avec un excès de confiance manifeste

En fait, on pourrait penser que les employés des entreprises informatiques sont beaucoup plus aptes à faire face aux cyberrisques que les membres d'autres industries. Cependant, cette hypothèse s'avère erronée, comme le montrent les courbes d'évolution ESI® ci-dessus. Ainsi, le secteur de la technologie affiche des taux de clics significativement plus élevés que la moyenne générale sur l'ensemble de la période d'étude.

Cela peut être attribué au fait que les gens surestiment souvent leurs propres capacités, en particulier lorsqu'il s'agit de sujets quisont liés à leur secteur d'activité professionnelle. Dans l'industrie informatique, une telle vision peut comporter des dangers considérables pour la sécurité informatique. Cela concerne non seulement votre propre entreprise, mais également ses clients. Il existe de nombreux fournisseurs de logiciels et de centres de données dans le secteur informatique qui développent et exploitent des applications pour d'autres entreprises.

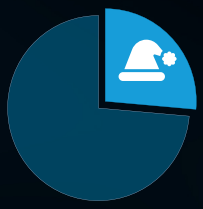
Dans ce cas également, l'ESI® aide à compenser les déficits spécifiques au secteur en matière de comportement de sécurité. Les entreprises informatiques reçoivent ainsi un chiffre clé fiable pour déterminer le niveau de sécurité et les progrès d'apprentissage des employés et pour en déduire l'utilisation ciblée des mesures de formation continue. De cette façon, la formation de sensibilisation peut être systématiquement adaptée aux besoins d'apprentissage accrus des employés de l'informatique.

En savoir plus

Évaluation 5 : les cinq principaux scénarios de harponnage et leurs facteurs psychologiques

1. Autorité de l'expéditeur et curiosité

La direction informe par courriel d'un nouvel organigramme, qui montre les responsabilités dans l'entreprise. Il est téléchargeable sur l'intranet.
taux de réussite de 28 %

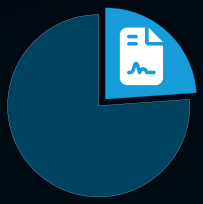


2. Autorité de l'expéditeur et curiosité

Scénario de Noël : la direction offre ses livres préférés de l'année en cours à tous les employés.
taux de réussite de 28 %

3. Crainte des conséquences désagréables

Le destinataire est informé que son compte de messagerie est plein. Un lien peut être utilisé pour remédier à la situation.
taux de réussite de 24 %



4. Sens du devoir et crainte des conséquences désagréables

Le destinataire sera invité à signer de nouvelles directives sur le travail à domicile.
taux de réussite de 24 %

5. Curiosité et crainte

Le destinataire reçoit un message indiquant que des voitures ont été endommagées dans le parc de stationnement de l'entreprise. Il doit regarder des photos pour vérifier si sa voiture est concernée ou non.
taux de réussite de 24 %

Les « points de déclenchement » ne sont pas les mêmes pour tous les destinataires

Les causes qui font que certaines personnes se font piéger par un courriel de harponnage dépendent de nombreux facteurs différents : niveau de stress et de formation de l'utilisateur, capacité de concentration, conception des courriels, lignes d'objet et autres.

Cependant, les facteurs d'influence psychologiques auxquels chaque personne réagit différemment sont d'une importance capitale. De ce fait, il y a des utilisateurs qui ont tendance à se soumettre aveuglément à l'autorité et qui cliquent immédiatement sur chaque courriel semblant provenir de leur chef d'équipe ou de la direction. En revanche, les réactionsd'autres employés sont de plus en plus liées à des facteurs humains tels que la volonté d'aider ou le sens du devoir.

La curiosité, la peur, une foi aveugle en l'autorité, la volonté d'aider, la vanité et de nombreux autres sentiments sont autant de facteurs d'influence psychologique importants pour les escrocs. Ils les utilisent consciemment et souvent dans des combinaisons individuelles afin de tromper leurs victimes potentielles. Pour s'assurer que les employés font exactement ce qu'on leur demande, les attaques de harponnage ciblent intelligemment leur système de réflexion rapide, par opposition à la réflexion lente et rationnelle du psychologue et lauréat du prix Nobel Daniel Kahneman dans son ouvrage à succès.[2]

Des simulations d'hameçonnage efficaces doivent donc toujours cibler les facteurs d'influence auxquels un utilisateur s'avère particulièrement sensible. Ainsi, au cours de la formation, les employés apprennent à s'armer de façon consciente contre les ruses psychologiques des attaquants auxquelles ils sont particulièrement vulnérables.

Chapitre 5 : Précautions à prendre par les entreprises : il faut agir rapidement

Comme le montrent les explications, les risques croissants d'hameçonnage obligent les entreprises à agir rapidement. Il faut savoir que même les technologies de sécurité informatique les plus avancées ne suffisent pas à elles seules à vous protéger contre le harponnage. En effet, si les services informatiques parviennent aujourd'hui à intercepter chaque jour des millions de courriels frauduleux, nombre d'entre eux arrivent dans la boîte de réception des employés.

Par conséquent, les entreprises devraient considérer la responsabilisation des employés à leur rôle de pare-feu humains comme une priorité. Cette exigence est également étayée par une étude en cours de la Bitkom Digital Association, selon laquelle la majorité des cybercriminels exploitent le « facteur humain » comme le maillon supposément le plus faible de la chaîne de sécurité.[1]

Une stratégie de sécurité informatique qui intègre les trois éléments centraux d'une culture de sécurité est la plus efficace : état d'esprit – compétences – ensemble d'outils. Voici ce que cela signifie concrètement : les employés doivent être sensibilisés à la menace que représentent les courriels de harponnage, formés à les reconnaître et soutenus pour se défendre au moyen de mesures techniques et organisationnelles adaptées.

Mindset

Motivation et communication ouverte

· Comprendre la menace

· Mettre l'accent sur la responsabilité personnelle

· Outils de communication pour toutes les parties prenantes

Skillset

Acquérir des compétences et des connaissances

Simulation de phishing

· E-Learning

· Séminaires en ligne

· Formation en présentiel

· Matériel de sensibilisation

Toolset

S'impliquer activement et intervenir

Tableau de bord en direct

· Gestionnaire de mots de passe

· Chaînes de messages de sécurité

· Bouton de signalement - Outlook Add-In

État d'esprit : éveillez un sentiment de sécurité face aux dangers

La plupart des employés ont une confiance aveugle dans les technologies de sécurité informatique. Les courriels entrants sont ouverts sans hésitation et les demandes qu'ils contiennent sont suivies, d'autant plus que les messages semblent provenir de sources dignes de confiance. Les entreprises sont donc bien avisées d'engager un processus de réflexion en faisant appel à la responsabilité personnelle et à l'auto-efficacité des employés. Ils doivent savoir que leur engagement et leur attention sont cruciaux pour le bon fonctionnement de toute l'entreprise.

En préparation à la formation sur la sensibilisation à la sécurité, des campagnes d'information initiées par la direction et soutenues par les cadres et le personnel de sécurité informatique sont recommandées. L'expérience a montré que les faits et les chiffres concernant les incidents de sécurité dans leur propre secteur laissent une impression durable sur les employés. Un exemple est l'entreprise d'ingénierie mécanique austro-chinoise FACC, qui a perdu environ 43 millions d'euros lorsqu'un comptable est tombé dans le piège de faux courriels du prétendu patron de l'entreprise. Il a transféré cette somme à des escrocs sur Internet qui lui ont fait croire qu'il s'agissait de transactions strictement confidentielles pour un achat d'entreprise.

Les campagnes d'information développent un impact maximal lorsqu'elles utilisent différents canaux et incluent des réunions d'équipe, des vidéos et des circulaires par courriel.

Compétences : encourager les décisions intuitives

Les formations sur la sensibilisation à la sécurité suivantes ne doivent pas se limiter aux formations classiques en présentiel, aux cours d'apprentissage en ligne et aux webinaires. En effet, ces formes d'apprentissage ne transmettent que des connaissances purement théoriques sur les attaques d'hameçonnage. Les simulations pratiques de harponnage se sont révélées efficaces pour aiguiser les sens des utilisateurs dans leur travail quotidien. Celles-ci utilisent des informations réelles sur les employés et l'entreprise pour simuler des attaques réelles. Si un employé tombe dans le piège d'un courriel malveillant, il atterrit directement sur une page explicative interactive avec des informations sur les caractéristiques suspectes du message : des lettres inversées dans la ligne d'adresse aux faux sous-domaines en passant par les liens et pièces jointes douteux.

Si les simulations de harponnage sont si efficaces, c'est qu'elles encouragent les décisions impulsives des employés responsables des clics spontanés sur les courriels. Dans son ouvrage à succès « Schnelles Denken, langsames Denken », le psychologue et prix Nobel Daniel Kahneman distingue ce système de pensée humain instinctif et émotionnel de sa capacité de prise de décision rationnelle et logique.2 De plus, les attaques de harponnage simulées constituent le « moment le plus propice à l'apprentissage » d'un employé. En l'informant de son comportement potentiellement dangereux au bon moment, il est formé de manière particulièrement efficace à la détection des attaques – et sera à l'avenir plus prudent avec les courriels entrants.

Pour que cet effet d'apprentissage perdure, les attaques de harponnage simulées doivent être répétées en continu et adaptées aux nouvelles méthodes d'attaque. Autrement, ce qui a été appris est vite oublié, comme le psychologue Dr. Hermann Ebbinghaus l'a découvert dès 1885.3 Selon la courbe d'oubli d'Ebbinghaus, le contenu d'apprentissage doit être répété plusieurs fois avant d'être mémorisé de façon permanente. En fonction de la fréquence de répétition, le cerveau reconnaît l'importance de l'information et la mémorise pour toujours. Après cela, la formation sur la sensibilisation à la sécurité doit devenir un processus continu si on veut qu'elle aitun effet durable.

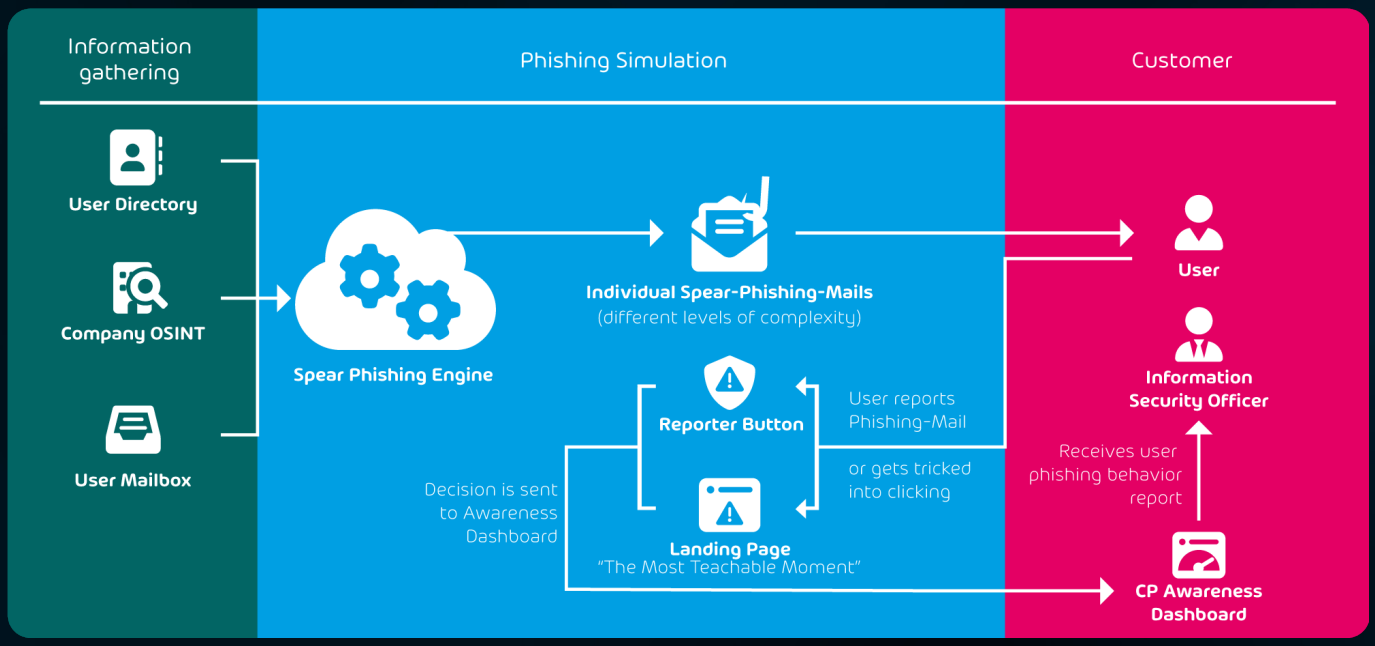


Fig. 4 : Spear phishing simulation process

En savoir plus

Ensemble d'outils : la cerise sur le gâteau de toute stratégie de lutte contre l'hameçonnage

Avec le bon ensemble d'outils, les entreprises peuvent compléter leurs défenses contre le harponnage. Les gestionnaires de mots de passe, faciles à intégrer dans l'environnement de travail informatique et permettant le stockage et la gestion centralisés des identités numériques, présentent un grand avantage. Les gestionnaires de mots de passe aident à empêcher les employés d'utiliser toujours les mêmes données de connexion pour plus de commodité. Si les auteurs d'actes de harponnage parviennent à voler un seul mot de passe, ils ne peuvent plus l'utiliser automatiquement pour accéder à tous les autres comptes d'un utilisateur.

Afin de mettre un terme à l'utilisation croissante de 2FA, les entreprises devraient passer à FIDO2 (Fast Identity Online).4 FIDO2 propose une procédure 2FA innovante dans laquelle l'inscription à un service en ligne est cryptée et ne peut pas être piratée, même avec les méthodes d'attaque de haute technologie actuelles.

Un autre outil utile est le « bouton reporter » qui peut être intégré directement dans Microsoft Office. Il aide les employés à identifier et à signaler les courriels suspects. Sur simple pression d'un bouton, les utilisateurs reçoivent des informations utiles indiquant si un courriel peut être falsifié et, si nécessaire, le transmettent au responsable de la sécurité informatique pour un examen plus approfondi.

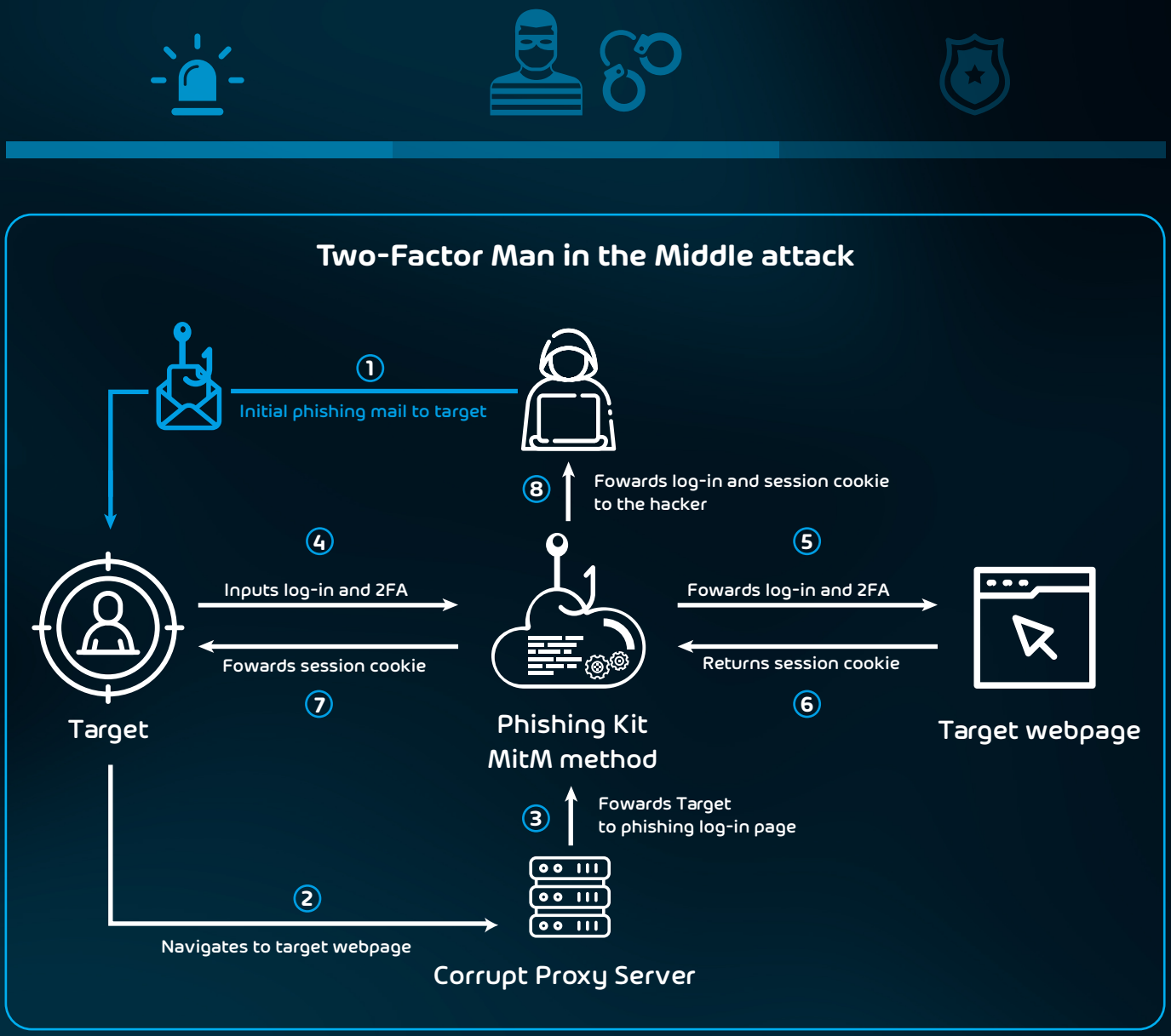


Fig. 5 : Construction d'une attaque de type Man in the Middle contre les authentifications 2FA

En savoir plus

La formation sur la sensibilisation à la sécurité de Hornetsecurity offre une solution complète

Hornetsecurity a développé une solution complète pour dispenser une formation de sensibilisation à la sécurité, qui combine des formats d'apprentissage innovants tels que la formation en ligne, le « Moment le plus propice à l'apprentissage » et la ludification avec l'une des simulations de harponnage les plus avancées. Dans le cadre de cours d'apprentissage en ligne classiques, de courtes vidéos et de jeux-questionnaires, les participants reçoivent des informations importantes sur les cyberrisques croissants et sur la meilleure façon de s'en protéger, ainsi que leur entreprise.

Dans le cas des attaques d'hameçonnage simulées, le Spear-Phishing-Engine (moteur de harponnage), également breveté, entre en jeu, ce qui garantit une apparence authentique des attaques d'hameçonnage. Le Spear-Phishing-Engine utilise des technologies innovantes Open Source Intelligence ou OSINT (renseignements provenant de sources disponibles publiquement) qui génèrent automatiquement des scénarios d'hameçonnage spécifiques à l'entreprise, au service et à l'employé. Des données d'entreprise accessibles au public (par exemple, à partir de portails d'employeurs) et d'autres sources sont utilisées pour le contenu d'hameçonnage.

De cette manière, des courriels de harponnage proches de la réalité peuvent être préparés avec, par exemple, une demande du chef de service concernant une facture, fournie en pièce jointe. Dans d'autres courriels, les escrocs se font passer pour des collègues ou des employés et évoquent une prétendue discussion technique. Pour approfondir davantage, le destinataire du courriel reçoit un lien « intéressant » qui mène en fait directement au logiciel malveillant. Les exemples montrent que le stratagème des auteurs d'actes de harponnage est toujours le même. Ils creusent profondément dans leur boîte à malice psychologique et sont si habiles à cibler les émotions de leurs victimes potentielles que, sans même réfléchir, ces dernières font exactement ce que les cybercriminels leur demandent de faire.

SECURITY AWARENESS SERVICE

En savoir plus

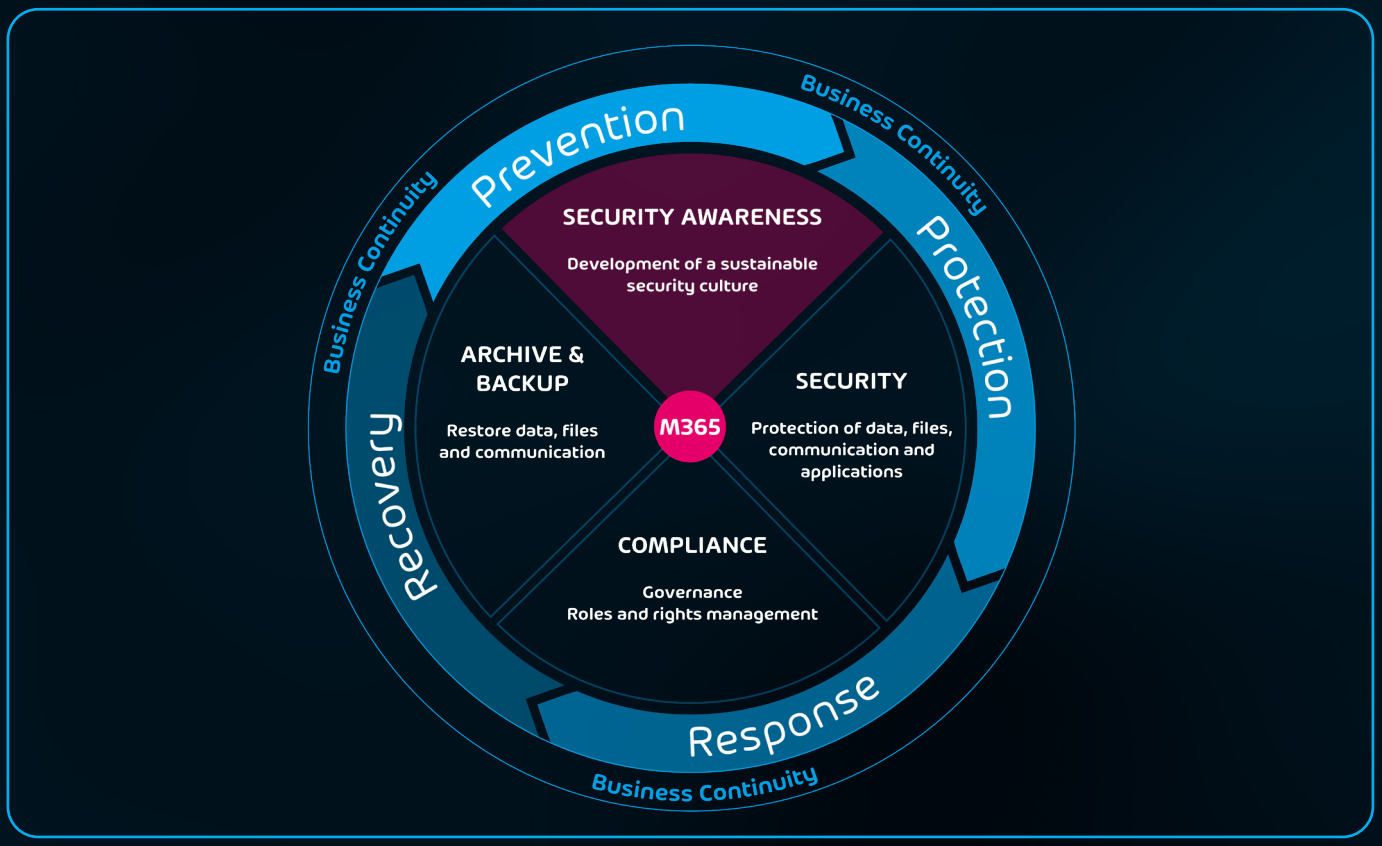


Abb. 6 : La sensibilisation à la sécurité dans le cadre de la continuité d'activité d'Hornetsecurity

En savoir plus

Service en mode du pilote automatique

Au début de la formation sur la sensibilisation à la sécurité, un niveau de sécurité d'au moins ESI® 70 doit être visé, qui sera ensuite progressivement augmenté. L'Awareness Engine est utilisé pour atteindre les différents ESI® souhaités. Ce moteur utilisant l'intelligence artificielle permet une formation en mode pilotage automatique, et interrompt et lance automatiquement les attaques de harponnage simulées – en utilisant les indicateurs ESI® et en fonction des besoins. Au lieu d'une formation uniforme selon le principe de saupoudrage, chaque participant reçoit autant de formation que nécessaire et le moins possible. Les entreprises économisent du temps, de l'argent et de précieuses ressources humaines, car elles n'ont pas à s'occuper de la mise en œuvre et du contrôle de la formation.

Les attaques d'hameçonnage simulées contre les différents employés sont répétées et réactualisées à intervalles définis. Les gestionnaires et les responsables de la sécurité informatique peuvent s'informer sur l'évolution permanente de la sensibilisation des indicateurs ESI® via leur propre système frontal, l'Awareness Dashboard, qui, comme toutes les autres solutions de Hornetsecurity, est intégré au Control Panel. Les résultats de la formation de sensibilisation peuvent y être consultés à tout moment. Les employés eux-mêmes peuvent suivre leurs progrès d'apprentissage individuels dans le User Panel. Il s'agit de la plate-forme d'apprentissage de la Security Awareness Service, à laquelle tous les participants ont leur propre accès pour consulter leurs résultats de formation et de tests individuels.

La formation continue mène à un succès durable

Déjà plus de 1 000 entreprises de tous les secteurs et de toutes les tailles font confiance à la technologie de sensibilisation éprouvée d'IT-Seal, qui appartient au groupe Hornetsecurity.

Afin d'obtenir un effet à long terme et durable, de nombreux clients optent pour une durée permanente de la formation sur la sensibilisation. D'une part, cela permet d'empêcher que le niveau ESI® une fois atteint ne baisse à nouveau. Au lieu de cela, le sujet de la sensibilisation à la sécurité peut être ancré longtemps dans la mémoire des participants. D'autre part, il est ainsi possible de continuer à intégrer régulièrement les nouveaux employés dans les formations à la sécurité.

Chapitre 6 : Succès client – quels sont les avantages de la Security Awareness Service pour les clients

Les attaques de harponnage réussies peuvent avoir des conséquences fatales pour les entreprises, qu'elles proviennent du secteur financier, de l'industrie des assurances ou de l'industrie manufacturière. Comment deux entreprises renommées renforcent leurs défenses à l'aide de Security Awareness Service.

En tant que chef de file des fournisseurs de solutions bancaires (multibanques) en ligne et mobiles en Allemagne, Star Finanz mène ses activités dans l'environnement hautement réglementé du secteur financier. L'entreprise doit souvent traiter des données financières et transactionnelles sensibles provenant de clients finaux et d'entreprises. Afin de les protéger du harponnage, des formations à la sécurité interne ont déjà été organisées par le passé pour les employés.

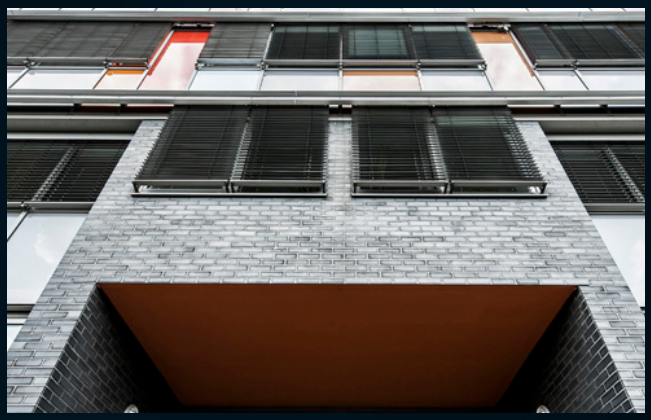
Cependant, face au caractère de plus en plus sophistiqué des attaques d'hameçonnage, il s'avère nécessaire de faire appel à un fournisseur de services de formation professionnelle. La solution Security Awareness Service de Hornetsecurity a été choisie parce que c'est une solution complète de formation de sensibilisation à la fine pointe de la technologie en matière d'attaques. À cela s'ajoute l'ESI® Benchmark innovant, qui permet de mesurer objectivement la sensibilisation à la sécurité des employés.

Des progrès d'apprentissage tangibles mesurables

À ce jour, des simulations d'attaques de harponnage et des formations en ligne pour les employés de Star Finanz sont menées en continu. « De grands progrès d'apprentissage ont été réalisés et le niveau de sécurité du personnel a augmenté de manière significative », conclut André Haase, architecte principal de la sécurité chez Star Finanz.

Pour des raisons de protection des données, il est très avantageux pour Star Finanz que Hornetsecurity traite les informations des clients en Allemagne. De ce fait, toutes les mesures de formation sont compatibles avec le Règlement général sur la protection des données (RGPD) de l'Union européenne (UE). De plus, en utilisant les mesures de sécurité reconnues de la Security Awareness Service, l'entreprise peut poser un jalon important pour une éventuelle certification ISO 27001.

Pour André Haase, il ne fait aucun doute que la Security Awareness Service sera maintenue afin d'obtenir un effet durable de la formation sur la sensibilisation.



André Haase
Senior Security Architect - Star Finanz

En savoir plus

Succès client – quels sont les avantages de la Security Awareness Service pour les clients

Si une entreprise manufacturière est touchée par une attaque d'hameçonnage, toute la chaîne de production peut être paralysée. Il en résulte des pertes de profits sans compter que la confiance des clients et la compétitivité s'en trouvent également diminuées.

Kirchhoff & Lehr, spécialiste de la technologie de profilage connu dans toute l'Europe, ne peut se permettre de tels dysfonctionnements. En plus d'une large gamme de produits, le fabricant s'est fait un nom grâce à un haut niveau de qualité, de fiabilité de livraison, mais aussi grâce à l'excellent rapport qualité-prix de ses produits. Lorsque le nombre de courriels malveillants a explosé pendant la crise du coronavirus, l'entreprise cherchait une solution pour sensibiliser les employés aux attaques d'hameçonnage

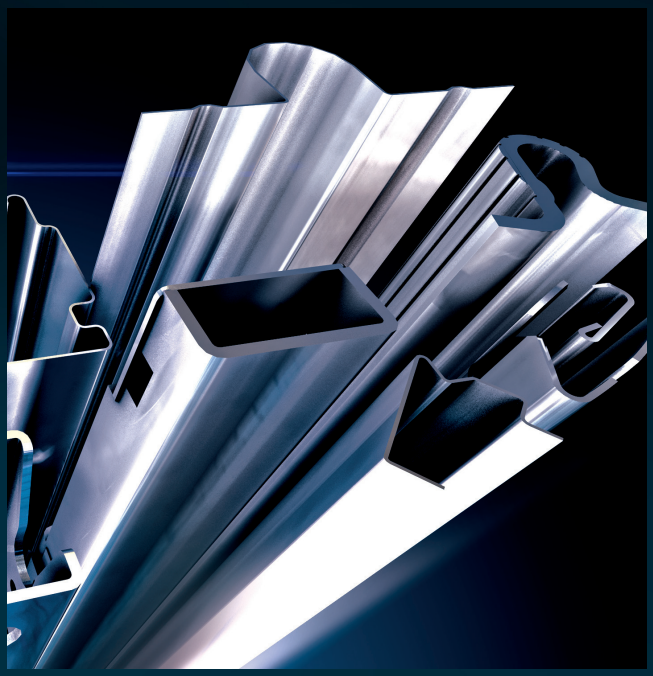
La formation devient permanente

Peu de temps après, les responsables ont décidé de faire de la formation de sensibilisation à la sécurité un exercice permanent pour le personnel administratif. « Cela est principalement dû aux simulations de harponnage, qui offrent un avantage pédagogique et didactique élevé », souligne Robert Batz, responsable informatique chez Kirchhoff & Lehr.

Avant le début de la formation de sensibilisation, les employés ont été informés conformément aux règles de protection des données et leur consentement demandé. Depuis lors, ils reçoivent régulièrement des courriels d'imitation de harponnage. De plus, leur sensibilisation à la sécurité est renforcée par le bouton Reporter inclus dans la Security Awareness Service. Si un utilisateur reçoit un courriel suspect, il peut le transmettre directement au service informatique pour une vérification technique.

Après seulement quelques mois, la hausse de l'ESI® montre clairement que les employés font de grands progrès dans la détection des attaques d'hameçonnage. Afin qu'ils puissent rester dans la pratique et que les nouveaux employés puissent également en bénéficier, les formations sont prolongées bien au-delà de la durée du contrat initialement convenu.

Robert Batz, le directeur informatique, en est persuadé : « Nous avons reçu des commentaires exceptionnels concernant la formation sur la sensibilisation, nos employés ont reconnu leur responsabilité en tant que pare-feu humain. »



Robert Batz
Le directeur informatique - Kirchhoff & Lehr GmbH

En savoir plus

Chapitre 7 : Résumé et perspectives

Malgré l'utilisation des dernières technologies de sécurité informatique, il ne peut y avoir de sécurité à 100 %. Cependant, des mesures efficaces sont désormais à la disposition des entreprises pour limiter les effets des cyberattaques. Cela garantit que les activités se poursuivent sans interruption, que les attaques sont rapidement contrées et – si le pire devait arriver – tous les systèmes, fichiers et données peuvent être restaurés rapidement. De plus, la continuité globale des activités garantit que les entreprises misentt également sur la sécurité en matière de conformité. Elles peuvent ainsi prendre les mesures appropriées afin de se protéger contre les poursuites pénales et les atteintes à leur réputation en cas de cyberattaque.

La Security Awareness Service est destinée aux utilisateurs particuliers

Hornetsecurity propose actuellement les solutions les plus avancées pour la sécurité, la sauvegarde et la conformité des courriels qui couvrent tous les aspects du cycle de sécurité informatique d'un point de vue technique : de la prévention et de la protection à la réponse et à la récupération.

Cependant, la plupart des cyberattaques visent toujours le « maillon le plus faible qu'est l'humain » et, en fin de compte, même les systèmes et les outils les plus sécurisés sur le plan technique ne le sont que si les utilisateurs les utilisent avec prudence.

Avec la Security Awareness Service, Hornetsecurity intègre le facteur humain dans sa propre solution de cybersécurité et l'intègre activement dans le cycle de sécurité informatique. La formation continue sur la sensibilisation à la sécurité de Hornetsecurity prépare systématiquement les employés aux cyberrisques croissants. Au fil du temps, ils apprennent à reconnaître et à contrer efficacement même les attaques d'hameçonnage les plus sophistiquées. Ils maîtrisent les mesures nécessaires pour prévenir les incidents de sécurité aux conséquences graves en amont et assurer la continuité des activités à tout moment.

De plus, Hornetsecurity accompagne les entreprises au début de la formation sur la sensibilisation à la sécurité pour développer la consciencede la sécurité souhaitablechez leurs employés. C'est le seul moyen pour que l'ensemble des compétences acquises, en combinaison avec les processus et outils d'accompagnement, puisse contribuer au développement d'une culture de la sécurité activement pratiquée et durable.

HORNETSECURITY

En savoir plus

Références

1 Federal Criminal Police Office (BKA): Bundeslagebild Cybercrime 2021, mai 2022

2 Hornetsecurity: Cyber Threat Report Edition 2021/2022, janvier 2022

3 Microsoft: Microsoft Digital Defense Report 2021, octobre 2021

4 Anjuli Franz and Evgheni Croitor, Darmstadt Technical University (TU): Who bites the Hook?

Investigating Employees' Susceptibility to Phishing: A randomized Field Experiment, 2021

5 Daniel Kahneman: Thinking, Fast and Slow, 2012

6 L'économie allemande ciblée : plus de 220 milliards d'euros de dégâts par an, 5 août 2021

7 Daniel Kahneman: Thinking, Fast and Slow, 2012

8 Wikipedia: Hermann Ebbinghaus

9 FIDO-Alliance: Authentification FIDO – Une vision sans mot de passe

À propos du groupe Hornetsecurity

Hornetsecurity est un fournisseur de premier plan de sécurité et de sauvegarde de la messagerie électronique en nuage, qui sécurise les entreprises et les organisations de de toutes tailles dans le monde entier. Son portefeuille de produits primés couvre tous les principaux domaines de la sécurité du courrier électronique, notamment le spam notamment le filtrage des spams et des virus, la protection contre le phishing et les ransomwares, ainsi que l'archivage et le cryptage conformes à la loi. l'archivage et le cryptage. À cela s'ajoutent la sauvegarde, la réplication et la récupération des courriels, des points d'extrémité et des machines virtuelles. Le produit phare est la solution de sécurité cloud la plus complète du marché pour Microsoft 365. Avec plus de 450 employés répartis sur 12 sites, l'entreprise, dont le siège social est situé à Hanovre, en Allemagne, dispose d'un réseau international de partenaires. Basée à Hanovre, en Allemagne, dispose d'un réseau international de plus de 5 000 partenaires de distribution et MSP, ainsi que de 11 centres de données redondants et sécurisés. Plus de 50 000 clients utilisent les services premium, dont Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA et CLAAS.

HORNETSECURITY