HORNETSECURITY

EMPLOYEE SECURITY INDEX

LIVRE BLANC

Social Engineering (Ingénierie sociale) : l'utilisateur comme passerelle

Les attaques d'ingénierie sociale à l'échelle mondiale gagnent de l'ampleur avec la mise à niveau constante des mesures techniques de protection dans le domaine de la sécurité informatique : en 2013, 17 % des cyberattaques portaient encore l'empreinte de l'ingénierie sociale. Aujourd'hui, la grande majorité des attaques sont déjà préparées par l'ingénierie sociale. La propagation massive du logiciel malveillant Emotet et de ses successeurs a montré l'ampleur et la qualité de ces attaques : Emotet lit de manière ciblée les contacts et le contenu des courriels dans les boîtes aux lettres des systèmes infectés et utilise ces informations pour se propager. Ces courriels de spear phishing (harponnage) sont souvent difficilement reconnaissables pour le profane.

La sensibilisation à la sécurité (Security Awareness) permet de renforcer le « pare-feu humain »

Le facteur humain doit donc être pris en compte dans tous les concepts de sécurité de l'information – « Sensibilisation à la sécurité » est la devise. La sensibilisation à la sécurité décrit dans quelle mesure les collaborateurs connaissent l'importance de la sécurité de l'information dans leur entreprise ainsi que l'étendue de leur propre responsabilité en matière de sécurité et surtout la façon dont ils agissent en conséquence.

Diverses mesures peuvent être mises en place pour accroître la sensibilisation à la sécurité. Il est important de ne pas considérer les utilisateurs comme un risque, mais plutôt comme un maillon essentiel de la solution de sécurité informatique : « Tu es le pare-feu de votre entreprise ». Par conséquent, les employés doivent être impliqués, ne pas se sentir dépassés et, surtout, ils ne doivent pas être effrayés.

Cependant, la planification des activités de sensibilisation à la sécurité pose un certain nombre de défis :

- Comment assurez-vous que les mesures de sensibilisation à la sécurité sont efficaces et durables?
- Un retour sur investissement peut-il être indiqué? L'investissement en vaut-il la peine?
- Existe-t-il une référence ou une comparaison avec d'autres organisations dans des secteurs similaires?
- Les employés d'une organisation peuvent-ils être formés de manière plus ciblée qu'avec le « principe de saupoudrage »?

Avec l'Employee Security Index – en bref : ESI^{MD}– le comportement de sécurité des employés est rendu proche de la réalité, standardisé, reproductible et mesurable. Ce livre blanc explique en détail la méthode de calcul brevetée et présente une référence de plus de 60 entreprises européennes.

Classification des attaques comme base d'une méthode de mesure standardisée

Afin de rendre la sensibilisation à la sécurité mesurable, une simulation proche de la réalité des attaques de harponnage est un exercice indispensable. Il doit également être possible de procéder à des comparaisons entre les différentes attaques – c'est le seul moyen de mesurer la sensibilisation à la sécurité sur une plus longue période.

Nous classons donc les scénarios de phishing sous-jacents en différentes catégories. Le facteur décisif ici est le temps qu'un intrus doit investir dans la préparation et la mise en œuvre d'un scénario d'attaque. Il s'agit, par exemple, de la collecte d'informations (OSINT – Open Source Intelligence), la préparation technique, la copie des conceptions de sites Web ainsi que la mise à disposition de l'infrastructure. Les scénarios d'hameçonnage peuvent être divisés en sept catégories (appelées niveaux), qui nécessitent des temps de préparation différents.

Niveau	Exemple	Temps de préparation
1	Courriel de phishing de masse typique, tel que la confirmation de commande d'un portail d'achat bien connu.	Environ 15 minutes
2	Courriel prétendument envoyé par le directeur général ou la directrice générale(fraude utilisant la fonction du PDG).	Environ 1 heure
3	Courriel de spear phishing contenant des informations publiques sur l'entreprise, par exemple provenant de portails d'évaluation des emplois.	Environ 2 heures
4	Courriel de spear phishing faisant référence au service et au poste du destinataire, aux courriels de collègues directs ou de gestionnaires.	Environ 4 heures
5	Courriel usurpé d'un partenaire commercial qui n'a pas activé la fonction de protection contre l'usurpation d'adresses électroniques ou dont le compte a été piraté.	Environ 6 heures
6	Un partenaire commercial ou un collègue a été piraté : courriel d'un contact personnel répondant à une précédente conversation par courriel.	Environ 12 heures
7	Courriel de spear-phishing faisant référence à des sujets sur lesquels le destinataire travaille actuellement, par exemple une mise à jour de l'état d'un projet en cours dans lequel le destinataire intervient.	Plus que 20 heures

Tableau : Aperçu des temps de préparation

Indicateur de la sensibilisation à la sécurité : ESI^{MD} – L'Employee Security Index

Afin de mesurer le niveau de sensibilisation d'un groupe test, chaque employé participant est désormais la cible de scénarios d'attaque choisis au hasard dans différentes catégories. Le « taux de réussite » (du point de vue de l'intrus) est ensuite mesuré sur l'ensemble du groupe test.

Espérer un « taux de réussite » de 0 comme objectif relève de l'utopie – nous faisons tous des erreurs. C'est pourquoi nous définissons un groupe de test « modèle » qui se situe à l'interface entre la sécurité et la faisabilité. En fonction du temps de préparation que doit investir un intrus, nous définissons des valeurs de tolérance à l'intérieur desquelles le comportement de sécurité des employés peut encore être considéré comme « modèle ». Pour les catégories 1 à 7, ces valeurs de tolérance se situent entre 1,1 et 6,2 %.

Un groupe de test modèle avec exactement ces taux de réussite atteint une valeur ESI^{MD} de 90. Si un comportement critique se manifeste deux fois plus souvent, par ex. en cliquant sur un lien malveillant dans un courriel de phishing, le groupe obtient un ESI^{MD} de 80. Si le comportement se manifeste trois fois plus souvent, il n'atteint qu'un ESI^{MD} de 70. Les scores inférieurs à 70 sont considérés comme critiques (voir tableau 1).

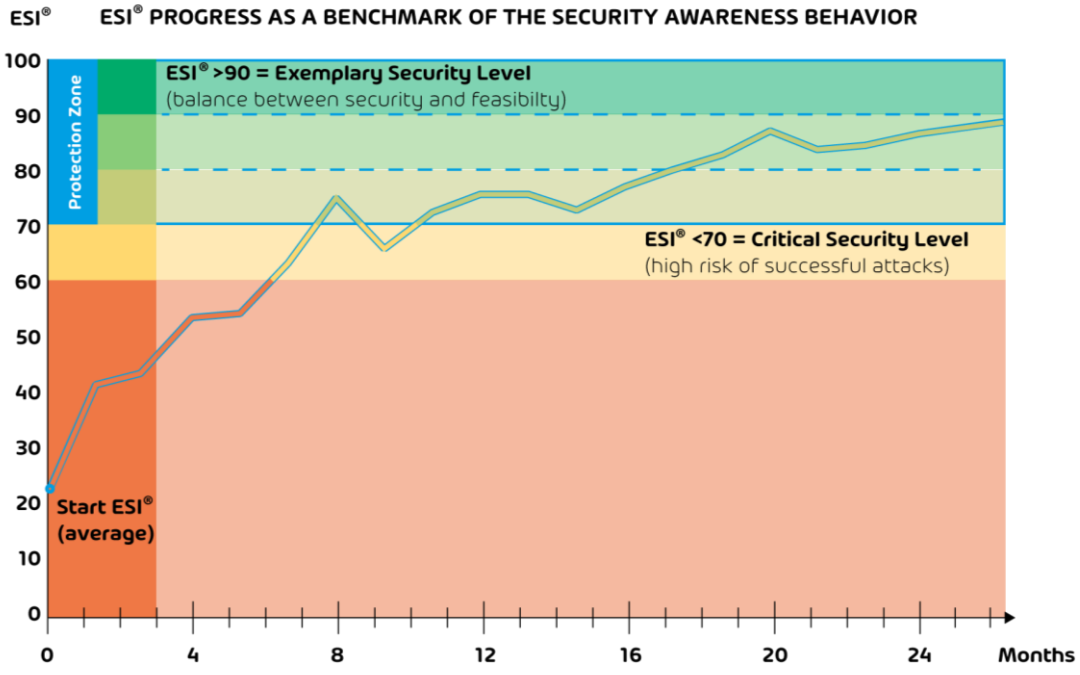

Tableau 1 : Un exemple de l'évolution de la méthode ESI^{MD} dans le temps comme référence de la culture sécurité

Voici les conclusions de l'étude sur l'ESI^{MD} auprès des entreprises européennes : la sensibilisation à la sécurité est faible – mais un succès d'apprentissage significatif est mesurable.

L'Employee Security Index est établi depuis mi-2018 dans le cadre de simulations de phishing dans des entreprises et des administrations internationales. Plus précisément, on mesure ici le taux de clics sur les liens et les fichiers joints. Parmi les exemples d'attaques simulées, on peut citer un prétendu message de la boîte aux lettres indiquant que la mémoire est pleine (catégorie 1), un courriel d'un collègue au hasard envoyant un lien vers un GIF amusant (catégorie 2) ou une demande du chef de service concernant une facture, fournie en pièce jointe (catégorie 4). La simulation de phishing a été réalisée de la manière la plus proche de la réalité possible : tous les participants ont subi des attaques de harponnage individuelles à des moments aléatoires.

Une évaluation de plus de 1,7 million d'attaques de phishing simulées donne un aperçu significatif du comportement de sécurité des employés d'entreprises de tous secteurs et de toutes tailles, comme le montre le tableau 2 sur une période de 12 mois.

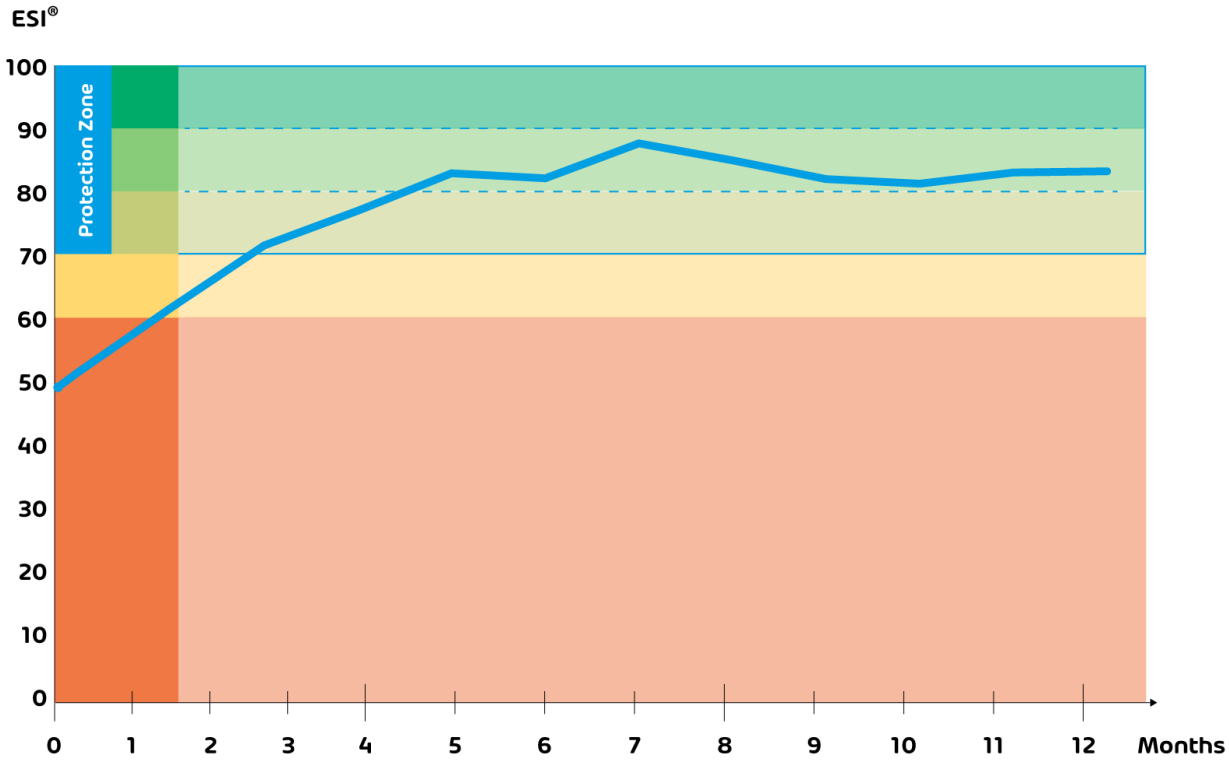

Tableau 2 : Détermination de l'ESI[MD] moyen à partir de la simulation de phishing

Formation continue sur la sensibilisation nécessaire

L'évolution moyenne de l'ESI[MD] montre clairement, dès les 12 premiers mois, pourquoi une formation continue est nécessaire pour maintenir un bon niveau de sécurité à plus long terme. Alors que la courbe ESI[MD] grimpe fortement au début et atteint rapidement un niveau de sécurité acceptable, à mesure que les scénarios de phishing deviennent plus sophistiqués, il devient beaucoup plus difficile de maintenir le

niveau – en particulier lorsque de nouveaux employés sont continuellement ajoutés ou que des groupes individuels et des employés interrompent la formation, comme on peut le voir sur le tableau 3.

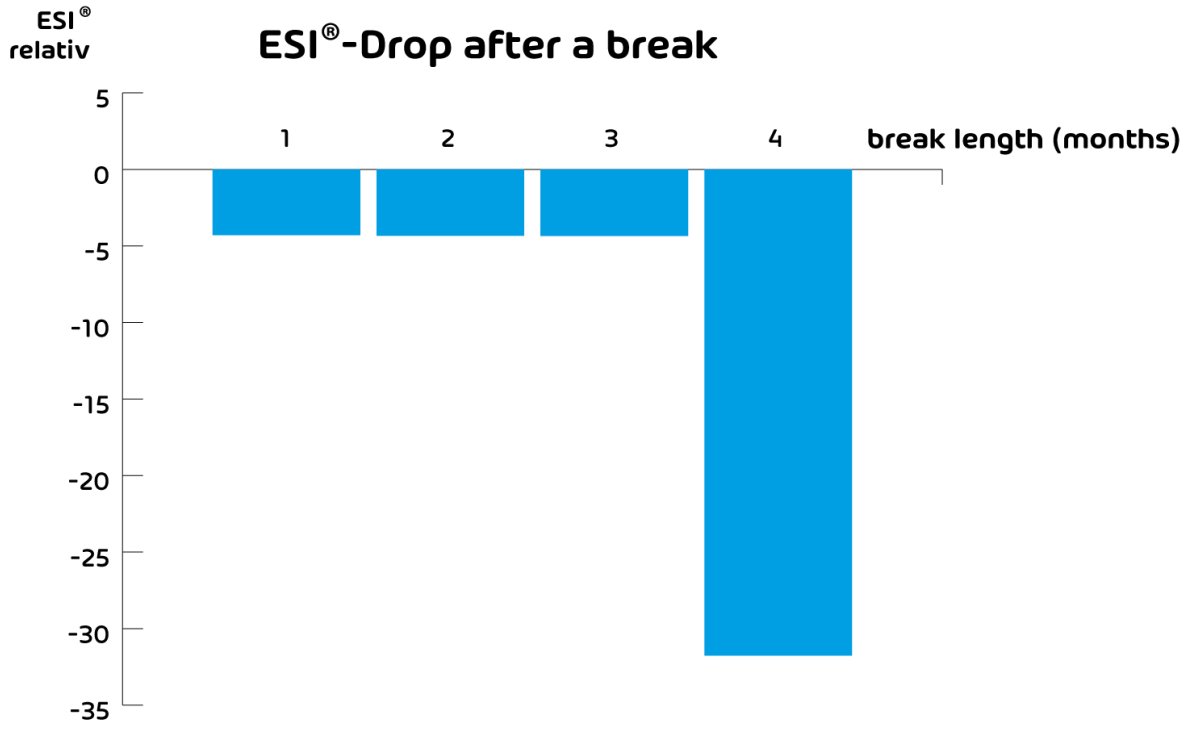

Tableau 3 : Baisse de l'ESI[MD] après une pause de la formation

Formation pour éviter les oublis

La sensibilisation est comme un muscle qui doit être régulièrement entraîné ou il se relâchera. On constate une nette baisse du comportement en matière de sécurité chez les groupes individuels ou collaborateurs qui interrompent la formation sur la sensibilisation et la reprennent plus tard. Sans formation, pendant les pauses, ils redeviennent plus négligents et ont déjà oublié des contenus d'apprentissage importants. La baisse de l'ESI[MD] dans ce graphique montre à quel point cet effet est effroyablement grand : après seulement le premier mois de pause, l'ESI[MD] chute de 5 points et se retrouve souvent déjà sous le niveau de sécurité cible. Après quatre mois, l'ESI[MD] a déjà perdu plus de 30 points et le niveau se retrouve presque au même niveau que celui du début de la formation sur la sensibilisation.

Instrument de contrôle servant de base à la prise de décision pour d'autres mesures de sensibilisation à la sécurité

L'ESI[MD] est donc un instrument de contrôle qui permet de surveiller en permanence la sensibilisation à la sécurité dans les entreprises. L'efficacité des différentes mesures de formation peut être vérifiée et les besoins spécifiques identifiés. La communication aussi bien avec la direction qu'avec le personnel est facilitée par une mesure tangible : une analyse quantitative de la sensibilisation à la sécurité permet d'effectuer une comparaison directe avec d'autres entreprises dans des secteurs similaires et peut donc être utilisée comme base de décision en matière d'investissements futurs.

Former les employés – de manière entièrement automatique avec le Security Awareness Service

Sensibiliser les employés à la sécurité est essentiel pour protéger efficacement une entreprise contre les cyberattaques. Les mesures techniques de sécurité à elles seules ne suffisent pas si les pirates savent exploiter les faiblesses humaines de manière ciblée.

Néanmoins, cette tâche représente un défi pour de nombreux responsables de la sécurité informatique, car la formation à long terme des employés peut prendre beaucoup de temps et mobiliser beaucoup de ressources. Notre service, Security Awareness Service prend en charge la majeure partie de ce travail pour vous.

En effet, notre service, Security Awareness Service forme vos collaborateurs sur la base des indicateurs ESI[MD], en fonction de leurs besoins et de manière entièrement automatisée pour une sensibilisation durable et efficace. Le programme de formation continue comprend une variété de méthodes pour cibler efficacement les employés : de la simulation de phishing en passant par la formation en ligne jusqu'aux courtes vidéos et supports de sensibilisation. Le résultat en est une culture de sécurité active et des employés bien informés qui connaissent et acceptent leur responsabilité vis-à-vis de l'entreprise. Le Awareness Engine constitue le cœur technologique du service Security Awareness Service et offre la bonne dose de formation pour chacun : chaque participant reçoit autant de formation que nécessaire et le moins possible.