SANS SECURITY AWARENESS

Guide de déploiement de la sécurité – Le télétravail en toute sécurité

Résumé

Conséquence du Coronavirus, de nombreuses entreprises doivent effectuer la transition vers le télétravail pour leurs employés. Cela représente une vraie gageure car elles manquent de politiques, de technologies et de formation pour assurer la sécurité de leurs employés à distance. En outre, de nombreux employés sont inquiets à l'idée de travailler chez eux et ne savent pas comment s'y prendre. Ce guide a pour but de vous aider à former rapidement ces employés en matière de sécurité. Si vous avez des questions relatives à l'utilisation de ce guide, veuillez nous contacter à support@sans.org.

Vos employés subiront vraisemblablement un stress important et devront s'adapter à des changements ; de plus, votre entreprise ne dispose pas de délais et de ressources infinis : ce guide stratégique propose donc la formation la plus abordable possible. Nous vous conseillons de vous concentrer sur les risques importants, qui auront le plus d'impact, décrits ci-dessous. Ce sera pour vous un point de départ. Si vous souhaitez intégrer des risques ou sujets complémentaires, n'hésitez pas à le faire. Attention, plus vous exigez de vos employés qu'ils adoptent de nouveaux comportements, procédures et technologies, plus ils risquent d'échouer à tout mener de front.

Comment utiliser ce guide

Nous vous conseillons de commencer par lire ce guide et consulter les liens vers les différentes ressources fournies pour avoir une idée de ce qui est disponible. Vous découvrirez que nous proposons pour chaque risque toutes sortes de ressources, que vous pouvez utiliser pour former vos employés. Cela vous permettra de choisir les modalités les plus efficaces, selon vous, en fonction de vos besoins et de votre culture. Quand vous aurez lu ce document, passez au Modèle de communication et à la fiche d'information joints dans ce kit pour mieux comprendre ce que vous tenterez d'accomplir. Une fois ces documents lus, vous devrez vous coordonner avec deux groupes clés :

1. **L'équipe de sécurité** : coordonnez-vous avec votre équipe de sécurité pour mieux comprendre quels sont les risques les plus importants auxquels vous serez confrontés. Dans ce guide, nous avons identifié les risques les plus courants auxquels sont exposés des employés travaillant de chez eux, mais vous serez peut-être exposés à d'autres risques. Attention, les équipes de sécurité font souvent l'erreur d'essayer de gérer tous les risques et saturent les employés de procédures et de prescriptions. Essayez de limiter au maximum le nombre de risques dont vous parlerez. Une fois que vous aurez identifié et hiérarchisé ces risques, déterminez quels seront les comportements à même d'y faire face. Comme nous l'avons déjà mentionné, si votre entreprise n'a pas le temps ou les ressources nécessaires, vous pouvez utiliser ce qui suit.

2. **Communications** : une fois que vous aurez identifié les principaux risques humains et les comportements clé à adopter pour y faire face, associez-vous avec votre équipe de communication pour former vos employés dans ce sens. Les formations sur la sécurité les plus efficaces sont celles qui s'effectuent en étroite collaboration avec l'équipe de communication. Si possible, vous pouvez même intégrer une personne de l'équipe de communication à votre équipe de sécurité. Lorsque vous communiquez avec vos employés, vous pouvez les impliquer efficacement en insistant sur le fait que cette formation de sécurité leur permettra de créer un environnement cyber-sécurisé chez eux, donc de les protéger et de protéger leurs proches, en plus de leur servir au travail.

Au bout du compte, en travaillant avec ces deux équipes, vous vous efforcez de simplifier au maximum les questions de sécurité pour vos employés et de motiver ces derniers, ce qui constitue les deux éléments clés de tout changement de comportement. Nous vous conseillons même de créer un conseil consultatif composé d'employés clés dont les retours et suggestions vous aideront à lancer le programme. En plus de vos équipes de sécurité et de communication, il serait judicieux de vous associer à d'autres services, comme les ressources humaines et le service juridique.

MGT433 Pack de téléchargement numérique

SANS Institute propose la formation de deux jours MGT433 : Comment élaborer, maintenir et évaluer un programme de sensibilisation à la sécurité à grand impact. Cette formation intensive fournit tout le nécessaire en matière de théorie, compétences, structure et ressources afin d'élaborer un programme de sensibilisation à grand impact et d'évaluer vos risques humains. Dans le cadre de ce guide, nous vous donnons accès au Pack de téléchargement numérique de la formation, avec modèles et ressources de planification. Si ces ressources dépassent vraisemblablement les besoins de cette initiative, elles pourront être utiles aux sociétés plus importantes ou aux déploiements plus complexes.

Répondre aux questions des employés

En plus d'alerter et d'entraîner vos employés, nous vous conseillons fortement d'utiliser une technologie ou un forum vous permettant de répondre aux questions des gens, en temps réel de préférence. Par exemple, un alias de messagerie électronique dédié, Skype, un canal de conversation Slack ou un forum en ligne, comme Yammer. Autre possibilité, vous pouvez héberger une émission vidéo sur la sécurité, plusieurs fois par semaine afin que chacun puisse la regarder quand cela lui convient, en direct, voire même pose des questions. Il s'agit pour vous de rendre la sécurité abordable et de répondre aux questions des gens. C'est une fabuleuse occasion d'impliquer vos employés et de promouvoir la sécurité. Essayez d'en profiter. Pour que ce soit efficace, n'oubliez pas que vous devez affecter une personne à la modération de tout canal de sécurité et au traitement actif des questions.

Ressources concernant les risques et la formation

Nous avons identifié trois principaux risques que vous devez prendre en compte pour vos employés travaillant à distance. Ce sera notre point de départ, et ce qui vous sera vraisemblablement le plus utile. Chacun des risques ci-dessous est assorti de liens vers diverses ressources qui vous aideront à communiquer et former vos employés. Nous fournissons de nombreuses ressources de communication afin que vous puissiez choisir celles qui auront le plus grand impact en fonction de votre culture. De plus, l'immense majorité de nos ressources sont traduites en plusieurs langues. Si vous trouvez tout ceci trop compliqué et si votre temps est compté, nous vous conseillons de déployer uniquement les deux ressources ci-dessous.

1. Fiche d'information Le télétravail en toute sécurité (incluse dans votre kit de déploiement).
2. Créer un Environnement Cyber-Sécurisé à la Maison (Anglais) également disponible ici dans d'autres langues

Ingénierie Sociale

En cette période de grands bouleversements et d'urgence, les attaques d'ingénierie sociale représentent le plus grand danger auquel sont confrontés les employés en télétravail. L'ingénierie sociale est une attaque psychologique par laquelle un criminel incite sa victime à commettre une erreur, profitant de la période de changements et de confusion. Il s'agira surtout d'expliquer aux employés ce qu'est l'ingénierie sociale, comment détecter les indicateurs d'une attaque d'ingénierie sociale et comment réagir le cas échéant. Attention de ne pas vous focaliser uniquement sur les attaques par e-mail de hameçonnage et d'évoquer d'autres méthodes : appels téléphoniques, textos, réseaux sociaux et fake news. Vous trouverez les ressources nécessaires pour former vos employés et renforcer leurs connaissances à ce sujet dans notre dossier Ressources de support pour l'ingénierie sociale. Voici également deux liens vers des vidéos SANS sur la sécurité, elles aussi fournies dans plusieurs langues.

- Ingénierie sociale (Anglais) également disponible dans d'autres langues ici
- Hameçonnage (Anglais) également disponible dans d'autres langues ici

Mots de passe forts

Comme l'indique le Rapport d'enquête annuel sur les compromissions de données (DBIR) de Verizon, les mots de passe faibles restent à l'origine de la plupart des violations de données dans le monde. Les quatre comportements clés pour faire face à ce risque sont listés ci-dessous. Vous trouverez les ressources nécessaires pour former vos employés et renforcer leurs connaissances à ce sujet dans notre dossier Mots de passe.

- Phrases de passe (attention, complexité des mots de passe et expiration des mots de passe sont inactifs).
- Utilisez un mot de passe unique pour chacun de vos comptes
- Gestionnaires de mots de passe
- AFM (Authentification à facteurs multiples). Souvent appelée authentification à deux facteurs ou vérification en deux étapes

Systèmes mis à jour

Troisièmement, vous devez vous assurer que vos employés utilisent des technologies à jour : système d'exploitation, applications et applications mobiles. Les personnes utilisant des appareils personnels devront ainsi activer les mises à jour automatiques. Vous trouverez les ressources nécessaires pour former vos employés et renforcer leurs connaissances à ce sujet dans les dossiers Maliciels et Créer un Environnement Cyber-Sécurisé à la Maison.

Sujets supplémentaires à aborder

- **Wi-Fi** : sécuriser votre point d'accès Wi-Fi. Vous trouverez ces informations dans Créer un Environnement Cyber-Sécurisé à la Maison. Consultez également la Vidéo Créer un Environnement Cyber-Sécurisé à la Maison (Anglais) également disponible dans d'autres langues.

- **VPN** : qu'est-ce qu'un VPN et pourquoi vous devez en utiliser un. Nous vous conseillons la lettre d'information OUCH sur les VPN.

- **Travailler à Distance** : Ceci s'adresse aux personnes qui travaillent à distance, mais PAS depuis leur domicile (café, terminal d'aéroport, hôtel). Pensez à utiliser notre vidéo Travailler à distance (Anglais) également disponible dans d'autres langues ici.

- **Enfants / Invités** : Pour insister sur l'idée que les proches et invités ne doivent pas accéder aux appareils de travail, pensez à utiliser la vidéo Travailler à distance (Anglais) également disponible dans d'autres langues ici.

- **Détection / Réaction** : Souhaitez-vous que les employés estimant avoir connu un incident pendant qu'ils travaillaient de chez eux le signalent ? Si oui, que voulez-vous qu'ils signalent, et à quel moment ? Vous trouverez les réponses à ces questions dans Piraté.

Lettres d'information OUCH

De plus, pensez à utiliser les lettres d'information OUCH mises à la disposition du public dans le cadre de votre programme. Elles sont toutes traduites dans plus de vingt langues. Les lettres d'information OUCH susceptibles de compléter votre initiative Le télétravail en toute sécurité sont listées ci-dessous. Vous trouverez toutes les lettres d'informations dans les Archives des lettres d'informations de sécurité OUCH en ligne.

PRÉSENTATION

Four Steps to Staying Secure (Quatre mesures pour se protéger)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Créer un Environnement Cyber-Sécurisé à la Maison)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

INGÉNIERIE SOCIALE

Social Engineering (Ingénierie Sociale)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (Messagerie / Hameçonnage par SMS)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Arnaques personnalisées)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Usurpation d'Identité d'un Directeur)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (Attaques / arnaques par téléphone)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Bloquer le hameçonnage)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Arnaques via les réseaux sociaux)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

MOTS DE PASSE

Making Passwords Simple (Créer des mots de passe simplement)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (Verrouiller sa connexion)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

RESSOURCES SUPPLÉMENTAIRES

Yes, You Are a Target (Oui, vous êtes une cible)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Appareils domestiques intelligents)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Conseils rapides

Des astuces à partager dans un format facile à utiliser.

- La mesure la plus efficace pour sécuriser votre réseau sans fil domestique consiste à modifier le mot de passe administrateur par défaut, activer le chiffrement WPA2 et utiliser un mot de passe fort pour votre réseau sans fil.
- Pensez bien à tous les appareils connectés à votre réseau domestique : baby phones, consoles de jeu, TV, appareils ménagers, voire même votre voiture. Assurez-vous que tous vos appareils sont protégés par un mot de passe fort et/ou dotés d'un système d'exploitation à jour.
- Pour protéger efficacement votre ordinateur à domicile, vous pouvez vous assurer que son système d'exploitation et ses applications sont à jour. Activez la mise à jour automatique si possible.
- Au bout du compte, faire preuve de bon sens est votre meilleure défense. Si un e-mail, appel téléphonique ou message en ligne vous semble étrange, suspect ou trop beau pour être vrai, c'est peut-être une attaque.
- Utilisez un mot de passe unique pour chacun de vos comptes. Vous oubliez vos mots/phrases de passe ? Pensez à utiliser un gestionnaire de mots de passe pour les stocker en toute sécurité.
- La vérification en deux étapes constitue l'un des meilleurs moyens de sécuriser un

compte. La vérification en deux étapes consiste à exiger un mot de passe et un code envoyé vers votre appareil mobile ou généré par celui-ci. Parmi les services compatibles avec la vérification en deux étapes, on trouve Gmail, Dropbox et Twitter.

- Le hameçonnage est une attaque consistant à tenter de vous faire cliquer sur un lien malveillant ou ouvrir la pièce jointe d'un e-mail. Méfiez-vous de tout e-mail ou message en ligne créant un sentiment d'urgence, comporte des fautes d'orthographe ou commence par « Cher client. »

Données

Il est difficile d'évaluer les comportements dans cette situation car il est moins aisé de les mesurer quand les employés sont chez eux. En outre, certains de ces comportements ne sont pas liés au travail proprement dit (sécuriser un périphérique Wi-Fi, par exemple). Cela dit, vous pouvez mesurer la motivation. Nous avons déterminé que les sujets personnels et jouant sur les émotions suscitent la motivation et beaucoup plus d'intérêt que les autres. Les données suivantes peuvent donc s'avérer utiles.

- **Interactions** : à quelle fréquence les employés posent-ils des questions, publient-ils leurs idées ou demandent-ils de l'aide sur l'un des canaux sécurisés ou forums que vous hébergez ?
- **Simulations** : effectuez des simulations d'ingénierie sociale, par exemple hameçonnage ou attaques par texto ou appel téléphonique.

Vous trouverez une liste exhaustive des données mesurables en téléchargeant le Security Awareness Metrics Matrix du Pack de téléchargement numérique MGT433.

Licence

L'auteur du kit de déploiement

Lance Spitzner a 20 ans d'expérience dans le domaine de la sécurité : recherches en menaces cyber, architecture, sensibilisation et formation à la sécurité. Pionnier dans le domaine de la fraude et du renseignement lié à la cybercriminalité, il a créé les pots de miel et fondé le projet Honeynet. En tant que formateur SANS, il a développé les formations MGT433: Security Awareness et MGT521: Security Culture. Il a également publié trois livres sur la sécurité, fait office de consultant dans plus de 25 pays et aidé plus de 350 organisations à élaborer des programmes sur la sécurité des données afin de gérer leurs risques humains. Très présent sur Tweeter (@lspitzner), Lance effectue régulièrement des présentations et contribue à de nombreux projets sur la sécurité de la communauté. Avant de se consacrer à la sécurité des données, M. Spitzner a été officier de char dans la Rapid Deployment Force de l'armée et obtenu une maîtrise en administration des affaires à l'Université d'Illinois.

À propos de SANS Institute

Fondé en 1989, SANS Institute est un organisme collaboratif de recherche et de formation. SANS est le fournisseur de formations et de certifications en cybersécurité pour professionnels œuvrant au sein de gouvernements et institutions commerciales le plus estimé et le plus important au monde. Les formateurs SANS dispensent plus de 60 formations différentes dans plus de 200 événements de formation à la cybersécurité et en ligne. Le GIAC, filiale de SANS Institute, valide les compétences des professionnels par le biais de plus de 35 certifications en cybersécurité techniques interactives. Le SANS Technology Institute, filiale indépendante accréditée au niveau régional, propose des diplômes de maîtrise en cybersécurité. SANS fournit une multitude de ressources gratuites à la communauté InfoSec, comme des projets de consensus, rapports de recherche et lettres d'informations. Il fait également fonctionner l'Internet Storm Center, premier système de surveillance d'Internet. Au cœur de SANS, on trouve de nombreux experts en sécurité représentant toutes sortes d'organisations mondiales (entreprises, universités...) travaillant main dans la main pour aider la communauté de la sécurité de l'information toute entière. (https://www.sans.org)