SANS SECURITY AWARENESS

Guide de déploiement de la sensibilisation à la sécurité - Travailler de la maison en toute sécurité

Sommaire

En raison du coronavirus, de nombreuses organisations doivent permettre à leur personnel de travailler à partir de la maison. Ce peut être un défi car bon nombre de celles-ci n'appliquent aucune politique, ne sont pas dotées de la technologie ou n'ont pas la formation pour permettre le travail sécuritaire à distance. De plus, plusieurs employés ne sont pas familiers ou sont mal à l'aise avec l'idée de travailler de la maison. Le but de ce guide est de vous permettre de former rapidement ces personnes pour préserver la sécurité de tous autant que possible. Si vous avez des questions sur l'utilisation de ce guide, contactez-nous à l'adresse support@sans.org.

Considérant que votre personnel vit un stress important lié aux changements, et que votre organisation doit fort probablement gérer des limites de temps et de ressources, ce guide stratégique s'efforce d'offrir une formation aussi simple que possible. Nous recommandons que vous concentriez vos efforts sur les risques les plus importants qui pourraient avoir le plus gros impact, et qui sont décrits ci-dessous. Considérez-les comme un point de départ. Si vous désirez ajouter d'autres risques ou sujets, n'hésitez pas. Prenez en considération que plus vous ajoutez de comportements, procédures ou technologies à assimiler par votre personnel, moins ils pourront tout apprendre.

Comment utiliser ce guide

Nous recommandons que vous commenciez par lire le matériel dans ce guide et preniez connaissance des liens vers différents outils fournis pour vous donner un aperçu de ce qui est disponible. Vous découvrirez que pour chaque risque nous fournissons une variété d'outils que vous pouvez utiliser pour stimuler et former le personnel de votre organisation. Ces options vous permettent de choisir les méthodes que vous jugez les plus appropriées pour vos besoins et qui correspondent à votre culture d'entreprise. Après avoir lu ce document, lisez le Modèle de communication ainsi que la Fiche d'informations fournis avec cet ensemble pour une meilleure compréhension de votre objectif. Une fois les documents lus, vous devez considérer deux groupes clés.

1. **Équipe de sécurité** : Discutez avec votre équipe de sécurité pour développer une meilleure compréhension des risques-clés que vous tentez de gérer. Nous avons précisé dans ce guide ce que nous jugeons être prioritaire, soit les risques inhérents au travail à la maison, mais vous pourriez choisir de vous préoccuper de différents risques. Mais prudence, une erreur fréquente effectuée par les équipes de sécurité est de vouloir gérer tous les risques et de décourager ainsi les personnes avec de trop nombreuses politiques et exigences. Tentez de limiter au minimum les risques dont vous traiterez. Une fois que vous aurez ciblé et priorisé ces risques, confirmez les comportements qui contribueront à

gérer ces risques. Tel que mentionné précédemment, si votre organisation ne détient pas les ressources ou le temps pour exécuter ces tâches, tirez le maximum de l'information fournie ci-dessous.

2. **Communications** : Une fois que vous aurez identifié vos risques humains les plus importants et les comportements clés pour les gérer, joignez vos efforts à ceux de votre équipe de sécurité pour stimuler votre personnel et le former. Les programmes de sensibilisation à la sécurité les plus efficaces ont de forts partenariats avec leur équipe de communications. Si possible, vérifiez si vous pourriez impliquer une personne des communications dans votre équipe de sécurité. Lorsque vous échangez avec votre personnel, un des points majeurs qui incite à collaborer est que cette formation contribuera non seulement à leur protection au travail, mais aussi à la maison, pour eux-mêmes et leur famille.

Enfin, avec ces deux groupes vous tenterez de motiver votre personnel et de rendre la sécurité aussi simple que possible pour eux, les deux éléments clés pour un changement de comportement. Nous suggérons même de créer un comité consultatif composé de personnes clés qui fourniront des commentaires permettant de mettre le programme en route. En plus de votre équipe de sécurité et des communications, vous pourriez vous adjoindre des personnes du département juridique et des ressources humaines.

Fichiers numériques à télécharger MGT433

SANS Institute fournit une formation de deux jours MGT433 : Comment construire, maintenir et mesurer un programme de sensibilisation à la sécurité à forte incidence. Cette formation accélérée transmet toute la théorie, les habiletés, le cadre de travail et les ressources pour créer un programme de sensibilisation à la sécurité à haute incidence vous permettant de gérer et de mesurer efficacement votre risque humain. Dans ce guide nous permettons un accès gratuit aux fichiers numériques à télécharger pour les modèles et la planification des ressources. Bien que ce matériel peut excéder les besoins actuels de l'organisation, il peut être très utile pour de grandes entreprises ou des déploiements plus complexes.

Répondre aux questions du personnel

En plus de transmettre l'information à votre personnel et de le former, nous recommandons fortement une technologie quelconque ou un forum permettant de répondre aux questions des gens, en temps réel de préférence. Cette procédure peut comprendre un alias de messagerie, l'utilisation de Skype ou le site de clavardage Slack, ou un type de forum en ligne tel que Yammer. Une autre idée est l'hébergement d'une émission web que vous répétez plusieurs fois par semaine pour que les gens puissent choisir un moment qui leur convient pour l'écouter, et peut-être même pour poser des questions. L'objectif est de rendre la sécurité aussi facile d'accès que possible et d'aider les personnes qui ont des

questions. Voilà une occasion spéciale pour impliquer votre personnel et pour rendre la sécurité plus facilement applicable, tentez de tirer profit de cet outil. N'oubliez pas, pour que cette démarche soit efficace vous devriez consacrer une ressource pour modérer tout canal sécurisé et pour répondre activement aux requêtes.

Les risques et le matériel de formation

Nous avons ciblé trois risques principaux que vous devriez gérer pour votre personnel travaillant à distance. Il s'agit d'un point de départ et des démarches pour lesquelles vous tirerez le plus grand avantage. Chaque risque ci-dessous est rattaché à des liens vers de multiples ressources contribuant à transmettre le sujet et à la formation s'y rattachant. Nous fournissons de multiples outils de communication pour que vous puissiez choisir ceux qui auront le plus grand impact pour votre culture. De plus, presque tout le matériel est disponible en plusieurs langues. Si toutes ces options sont trop complexes et que votre temps est limité, nous recommandons que vous choisissiez et exploitiez simplement les deux sujets traités ci-dessous.

1. Fiche d'information sur le Travail à partir de la maison (comprise dans l'ensemble de déploiement).
2. Créer une vidéo sur la cybersécurité à la maison (Anglais) aussi disponible dans d'autres langues ici

Ingénierie sociale

Un des plus grands risques que courent les travailleurs à distance, tout spécialement en ces temps de changement dramatique et d'environnement d'urgence, sont les attaques d'ingénierie sociale. Les attaques d'ingénierie sociale sont une attaque psychologique dans lesquelles les criminels vous bernent pour vous pousser a faire une erreur, qui se fera plus facilement en ces temps de changements et de confusion. La solution est de former les gens au sujet de l'ingénierie sociale, pour savoir reconnaître les signes les plus fréquents d'attaques, et sur la façon de réagir lorsqu'une attaque est décelée. Assurez-vous de ne pas seulement mettre l'emphase sur les attaques par hameçonnage, mais aussi sur d'autres méthodes qui comprennent des appels téléphoniques, des messages textes, les médias sociaux ou de fausses nouvelles. Vous pouvez trouver le matériel requis pour la formation et le renforcement sur ce sujet dans notre dossier comportant le matériel traitant de l'ingénierie sociale. De plus, voici deux bandes-vidéo SANS sur la sensibilisation à la sécurité auxquelles vous avez accès, disponibles, encore une fois, en plusieurs langues.

- L'ingénierie sociale (Anglais) aussi disponible dans d'autres langues ici
- Hameçonnage (Anglais) aussi disponible dans d'autres langues ici

Mots de passe forts

Tel que précisé dans le Verizon DBIR annuel, les faibles mots de passe continuent d'être une des causes principales de brèches sur une échelle globale. Il y a quatre comportements clés contribuant à la gestion de ce risque, décrits ci-dessous. Vous pouvez trouver le matériel requis pour la formation et le renforcement sur ce sujet et sur ces quatre comportements dans notre dossier Mots de passe.

- Les phrases de passe (note, tant la complexité du mot de passe que son échéance sont morts).
- Utilisez des mots de passe différents pour tous vos comptes
- Gestionnaires de mots de passe
- L'authentification multi-facteurs (MFA en anglais). Souvent appelé authentification à deux facteurs, ou authentification en deux étapes

Systèmes à jour

Le troisième risque est d'assurer que toute technologie utilisée par votre personnel fonctionne avec les plus récentes versions de leur système d'exploitation, de leurs applications et des applis mobiles. Pour les personnes qui utilisent un appareil personnel, il peut être requis d'activer les mises à jour automatiques. Vous pouvez trouver le matériel requis pour la formation et le renforcement sur ce sujet dans notre dossier Maliciels ou dans le dossier Créer une cybersécurité à la maison .

D'autres sujets à considérer

- **Sans fil** : Sécuriser votre point d'accès sans fil. Ce sujet est traité dans le matériel Créer une cybersécurité à la maison aussi, veuillez regarder cette vidéo sur la création d'une cybersécurité à la maison (Anglais) aussi disponible dans d'autres langues ici.

- **RVP** : Qu'est-ce qu'un réseau virtuel privé (RVP) et pourquoi vous devriez en utiliser un. Nous recommandons le bulletin OUCH sur les RVP.

- **Travailler à distance** : Ceci touche les personnes qui travaillent à distance, mais NON à partir de la maison, tel que dans un café, un terminal d'aéroport ou un hôtel. Considérez utiliser notre vidéo de formation « Working Remotely » (Travailler à distance, en anglais) aussi disponible dans d'autres langues ici.

- **Enfants / Invités** : Pour renforcer l'idée que la famille / les invités ne devraient pas avoir accès aux appareils de travail, considérez la vidéo de formation pour Travailler à distance (Anglais) aussi disponible dans d'autres langues ici.

- **Détection / Réponse** : Voulez-vous que les personnes le rapportent s'ils croient qu'un incident s'est produit alors qu'il ou elle travaillait à partir de la maison? Si oui, que voulez-vous qu'ils rapportent et quand devraient-ils le faire? Ce sujet est traité dans notre matériel Piraté.

Bulletins OUCH

De plus, considérez l'utilisation des bulletins OUCH disponibles pour appuyer votre programme, chacun étant traduit dans plus de 20 langues. Ci-dessous sont donnés les bulletins OUCH qui, selon nous, contribueront le mieux à informer sur le travail sécuritaire à partir de la maison. Vous trouverez tous les bulletins dans les archives en ligne des bulletins OUCH sur la sensibilisation à la sécurité.

APERÇU

Four Steps to Staying Secure (Quatre étapes pour rester en sécurité)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Appliquer la cybersécurité chez soi)
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 (Fraudes personnalisées)
https://www.sans.org/security-awareness-training/resources/personalized-scams

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

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

Stop That Phish (Arrêtez ce courriel hameçon)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Être victime d'escroquerie dans les média sociaux)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

MOTS DE PASSE

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

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

ADDITIONNEL

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 (Objets connectés intelligents)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Conseils éclairs

Des conseils et des trucs que vous pouvez partager dans des formats de partage pratiques.

- Les mesures les plus efficaces que vous pouvez prendre pour sécuriser votre réseau sans fil à la maison est de changer le mot de passe par défaut fourni par l'administrateur, d'activer le chiffrement WPA2 et d'utiliser un mot de passe fort pour votre réseau sans fil.
- Pensez à tous les appareils connectés au réseau sans fil de votre maison, y compris les moniteurs pour bébé, les consoles de jeux, les téléviseurs, les appareils ménagers ou même votre voiture. Assurez-vous que ces appareils sont protégés par un mot de passe fort et/ou qu'ils fonctionnent avec la plus récente version de leur système d'exploitation.
- Une des façons les plus efficaces de protéger votre ordinateur à la maison est de vous assurer que votre système d'exploitation et vos applications sont à jour, avec les correctifs appropriés. Activez les mises à jour automatiques autant que possible.
- Enfin, le gros bon sens est votre meilleure protection. Si un courriel, appel téléphonique ou message en ligne vous semble étrange, inhabituel ou un peu trop attirant pour être vrai, c'est peut-être une attaque.
- Assurez-vous d'utiliser des mots de passe uniques séparés pour chacun de vos comptes. Difficile de mémoriser tous vos mots et phrases de passe? Considérez l'utilisation d'un gestionnaire de mots de passe pour les stocker de façon sécuritaire.

- L'authentification à deux facteurs est une des meilleures façons de sécuriser tout compte. L'authentification à deux facteurs est lorsque vous exigez un mot de passe ainsi qu'un code envoyé ou généré par votre téléphone intelligent. Les exemples de services qui utilisent l'authentification à deux facteurs comprennent Gmail, Dropbox et Twitter.
- Les attaques par hameçonnage visent à vous pousser à cliquer sur un lien malicieux ou à ouvrir une pièce jointe infectée dans un courriel. Soyez à l'affût de tout courriel ou message en ligne qui suscite un sentiment d'urgence, qui comporte des fautes d'orthographe ou qui s'adresse à vous avec la formule « Cher client ».

Mesures

Les mesures comportementales sont difficiles pour cette situation puisqu'il est plus difficile de mesurer comment les gens se comportent à la maison. De plus, certains de ces comportements ne sont pas spécifiques au travail (tel que de sécuriser leur appareil sans fil). Toutefois, vous pouvez mesurer l'engagement. Nous avons constaté que les sujets personnels ou émotifs comme ceux-ci peuvent être très stimulants, suscitant beaucoup plus d'intérêt que d'autres sujets. Ainsi, les mesures comme celles-ci peuvent être très représentatives.

- **Interaction** : À quelle fréquence est-ce que les gens posent des questions, publient des idées ou demandent de l'aide sur tout canal ou forum que vous hébergez?
- **Simulations** : Effectuez un type de simulation d'ingénierie sociale, telle que les attaques par hameçonnage, texte ou appel téléphonique.

Pour une liste de mesures beaucoup plus complète, téléchargez les matrices de mesures interactives de sensibilisation à la sécurité du forfait de téléchargement numérique MGT433.

Licence

Auteur de l'ensemble de déploiement

Lance Spitzner détient plus de 20 années d'expérience en sécurité dans la recherche en cyber menaces, dans la sécurité des architectures, la sensibilisation et la formation. Il a contribué à comprendre le domaine de la déception et de la cyber intelligence avec ses créations de réseaux leurres et la fondation du projet Réseau Leurre. En tant qu'instructeur SANS, il a développé les formations sur MGT433 : la sensibilisation à la sécurité et MGT521 : la culture de la sécurité. De plus, Lance a publié trois livres sur la sécurité, consulté dans plus de 25 pays et il a aidé plus de 350 organisations à construire des programmes de sensibilisation à la sécurité et de culture pour gérer le risque humain. Lance est un présentateur fréquent, un gazouilleur régulier (@lspitzner) et il travaille sur de nombreux projets de sécurité communautaire. Avant la sécurité de l'information, M. Spitzner a servi comme officier de blindé dans l'armée « Rapid Deployment Force » et a obtenu sa MBA de l'université de l'Illinois

Au sujet de SANS Institute

Le SANS Institute a été fondé en 1989 comme organisation coopérative de recherche et d'éducation. SANS est le plus fiable et de beaucoup, le plus grand fournisseur de formations sur la cyber sécurité et de certifications pour les professionnels des gouvernements et d'institutions commerciales partout au monde. Les instructeurs reconnus de SANS enseignent plus de 60 différentes formations dans plus de 200 événements de formations sur la cybersécurité en personne et en ligne. Le GIAC, une filiale de SANS Institute, valide les qualifications d'un praticien dûment qualifié dans plus de 35 certifications techniques pratiques en cyber sécurité. Le SANS Technology Institute, une filiale régionale indépendante accréditée, offre une maîtrise en cyber sécurité. SANS offre une myriade de ressources gratuites à la communauté Infosec y compris les projets de consensus, les rapports de recherches, et les bulletins; il opère aussi le système d'alerte précoce sur

internet - le Internet Storm Center. Au cœur de SANS se trouvent les nombreux praticiens de sécurité, qui représentent des organisations globales variées, des corporations aux universités, travaillant ensemble pour aider toute la communauté de l'information sur la sécurité. https://www.sans.org)