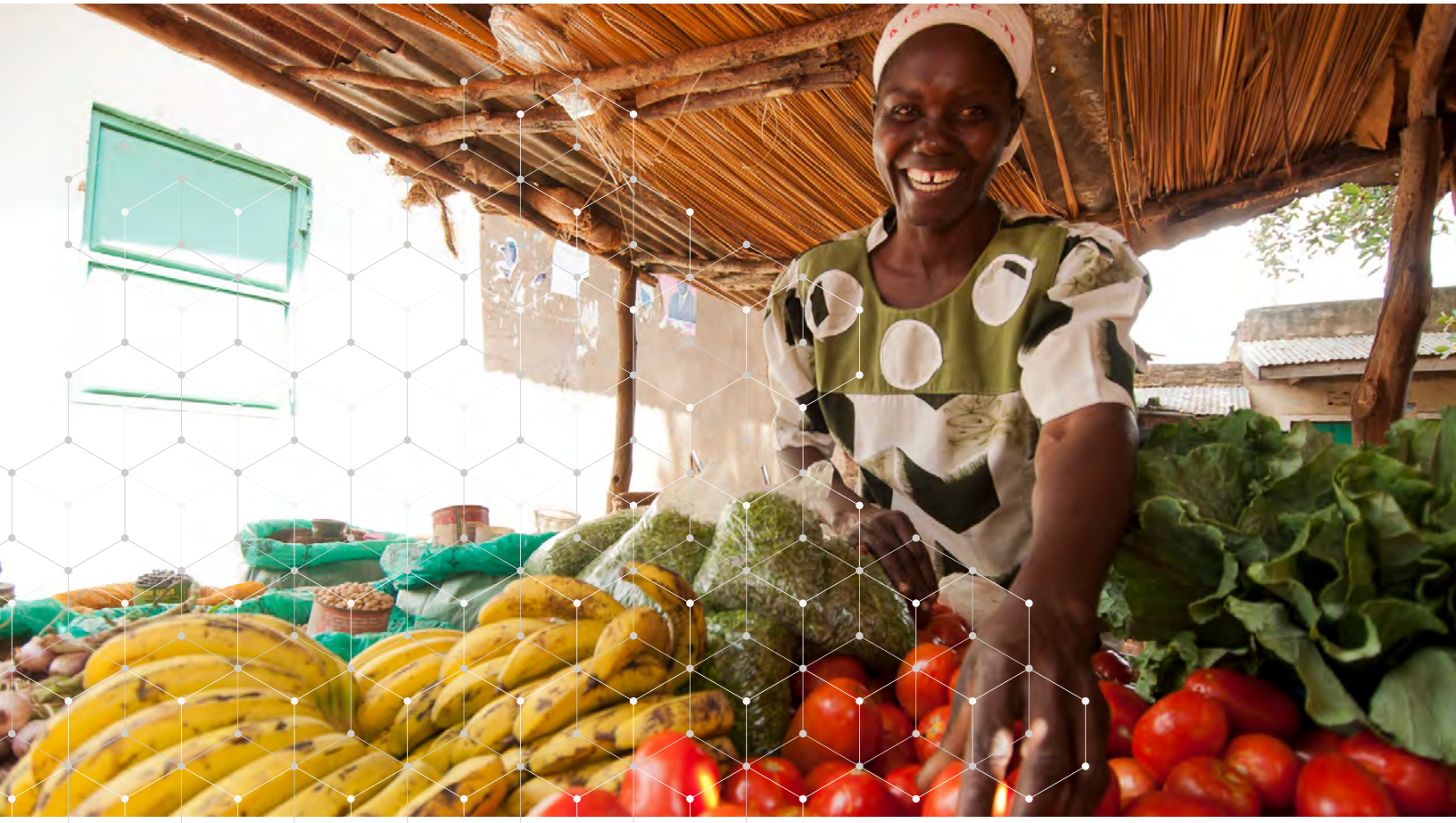
USAID
FROM THE AMERICAN PEOPLE

Guide de la cybersécurité pour les petites et moyennes entreprises



2ÈME PARTIE : PROTÉGER VOTRE ENTREPRISE

MENTIONS

Le Guide de la cybersécurité pour les petites et moyennes entreprises a été élaboré avec le soutien du Centre pour le développement économique et commercial (EMD) du Bureau pour le développement, la démocratie et l'innovation (DDI) relevant de l'Agence américaine pour le développement international (USAID). Il a été en grande partie rédigé par Daniel Vazquez dans le cadre du projet Activité Commerce et Compétitivité mise en œuvre par Resonance Global. Clare Sullivan, du Cyber SMART Research Center de l'Université de Georgetown, ainsi que Jeremy Ravenelle, Evan Legé et Anne Szender McCarthy du projet Activité Commerce et Compétitivité, y ont également contribué.

Ce document a été produit pour être révisé par l'Agence américaine pour le développement international. Il a été préparé par Activité Commerce et Compétitivité, sous numéro de contrat AID-OAA-C-17-00110. Son contenu relève de la seule responsabilité de l'auteur et ne reflète pas nécessairement les opinions de l'USAID ou du gouvernement américain.

TABLE DES MATIÈRES

GLOSSAIRE DES TERMES

Logiciel antivirus : programme qui surveille un ordinateur ou un réseau pour détecter ou identifier les principaux types de codes malveillants et pour prévenir ou contenir les incidents malveillants, parfois en supprimant ou en neutralisant le code malveillant.[1]

Crypto-monnaie : monnaie numérique dans laquelle les transactions sont vérifiées et les enregistrements conservés par un système décentralisé utilisant la cryptographie plutôt que par une autorité centralisée.[2] Les exemples incluent Bitcoin, Ethereum, Monero, etc.

Cyberattaque : attaque via le cyberespace qui cible l'utilisation du cyberespace par une organisation, dans le but de perturber, désactiver, détruire ou contrôler de manière malveillante un environnement ou une infrastructure informatique, de détruire l'intégrité des données ou voler des informations contrôlées.[3]

Cybersecurité : activité, processus, capacité ou état par lequel les systèmes d'information et de communication et les informations qu'ils contiennent sont protégés et/ou défendus contre les dommages, l'utilisation, la modification non autorisée ou l'exploitation.[4]

Déni de service distribué (DDoS) : forme de cyberattaque dans laquelle l'attaquant rend la machine, le site Web ou le réseau cible indisponible pour ses utilisateurs en inondant la cible de demandes dans le but de surcharger le système.

Cryptage : le processus de transformation de texte en texte chiffré.[5]

Pare-feu : capacité qui limite le trafic réseau entre les réseaux et/ou les systèmes d'information.[6]

Firmware : programmes informatiques et données associées qui peuvent être écrits ou modifiés automatiquement pendant l'exécution.[7]

HTTPS : regroupement du protocole de transfert hypertexte (HTTP) avec le protocole Secure Sockets Layer (SSL)/ Transport Layer Security (TLS). Le TLS est un protocole d'authentification et de sécurité largement implémenté dans les navigateurs et les serveurs Web.[8]

Logiciel malveillant : logiciel qui compromet le fonctionnement d'un système en exécutant une fonction ou un processus non autorisé.[9]

Modem : appareil qui convertit les données numériques devant être transmises sur un réseau, tel qu'un appareil permettant à un réseau domestique ou professionnel de se connecter avec un fournisseur de services Internet (FAI).

Authentification multi-facteurs : authentification utilisant deux ou plusieurs facteurs différents pour réaliser l'authentification. Les facteurs incluent : quelque chose que vous connaissez (mot de passe ou code PIN) ; quelque chose que vous possédez (dispositif d'identification cryptographique ou jeton) ; ou quelque chose que vous êtes (par exemple, données biométriques).[10]

Routeur : sur un réseau, appareil qui détermine le meilleur chemin pour transmettre un paquet de données vers sa destination[11], comme un appareil qui émet un signal Wi-Fi, par exemple.

Secure Sockets Layer (SSL) : assure la confidentialité et l'intégrité des données entre deux applications communicantes. Il est conçu pour encapsuler d'autres protocoles, tels que HTTP.[12]

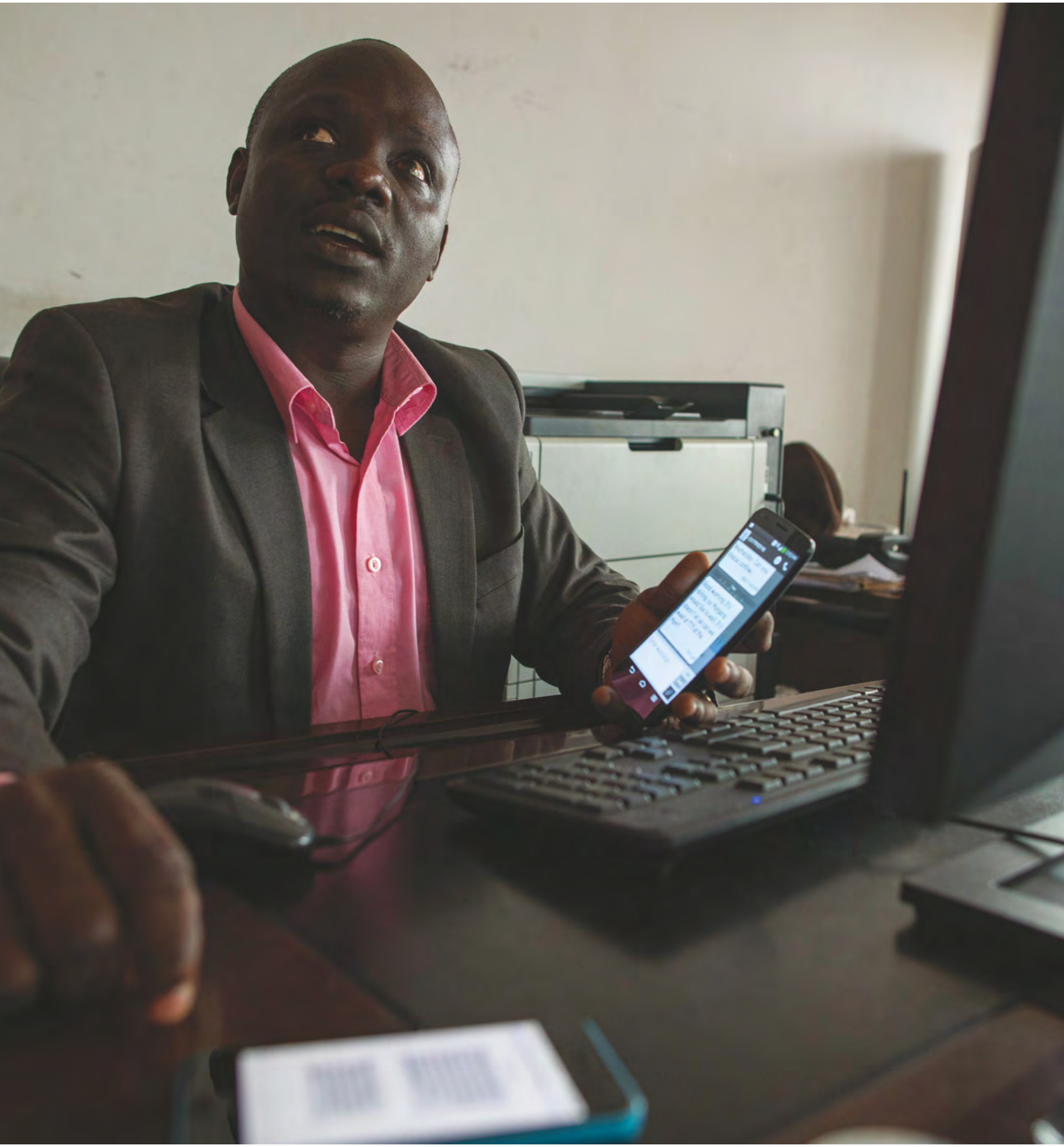
Service Set Identifier (SSID) : le nom d'un réseau Wi-Fi.

Wi-Fi Protected Access 2 (WPA2) : protocole de sécurité utilisant des mots de passe pour sécuriser les réseaux Wi-Fi.

LISTE D'ABRÉVIATIONS

DDoS	Déni de service distribué
FAI	Fournisseur d'accès à Internet
FSC NIST	Cadre de cybersécurité de l'Institut national des normes et de la technologie
IdO	Internet des objets
IP	Protocole Internet
PCI	Industrie des cartes de paiement
SSID	Réseau sans fil Wi-Fi (Service Set Identifier)
SSL	Couche de sockets sécurisée (Secure Sockets Layer)
TI	Technologie de l'information
WPA	Accès protégé par Wi-Fi
WPS	Configuration protégée par Wi-Fi

1 https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
2 https://www.oed.com/
3 https://csrc.nist.gov/glossary
4 https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
5 https://csrc.nist.gov/glossary
6 https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
7 https://csrc.nist.gov/glossary
8 https://www.healthit.gov/faq/what-does-https-web-address-mean
9 https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
10 https://csrc.nist.gov/glossary
11 https://csrc.nist.gov/glossary
12 https://www.oed.com/



INTRODUCTION

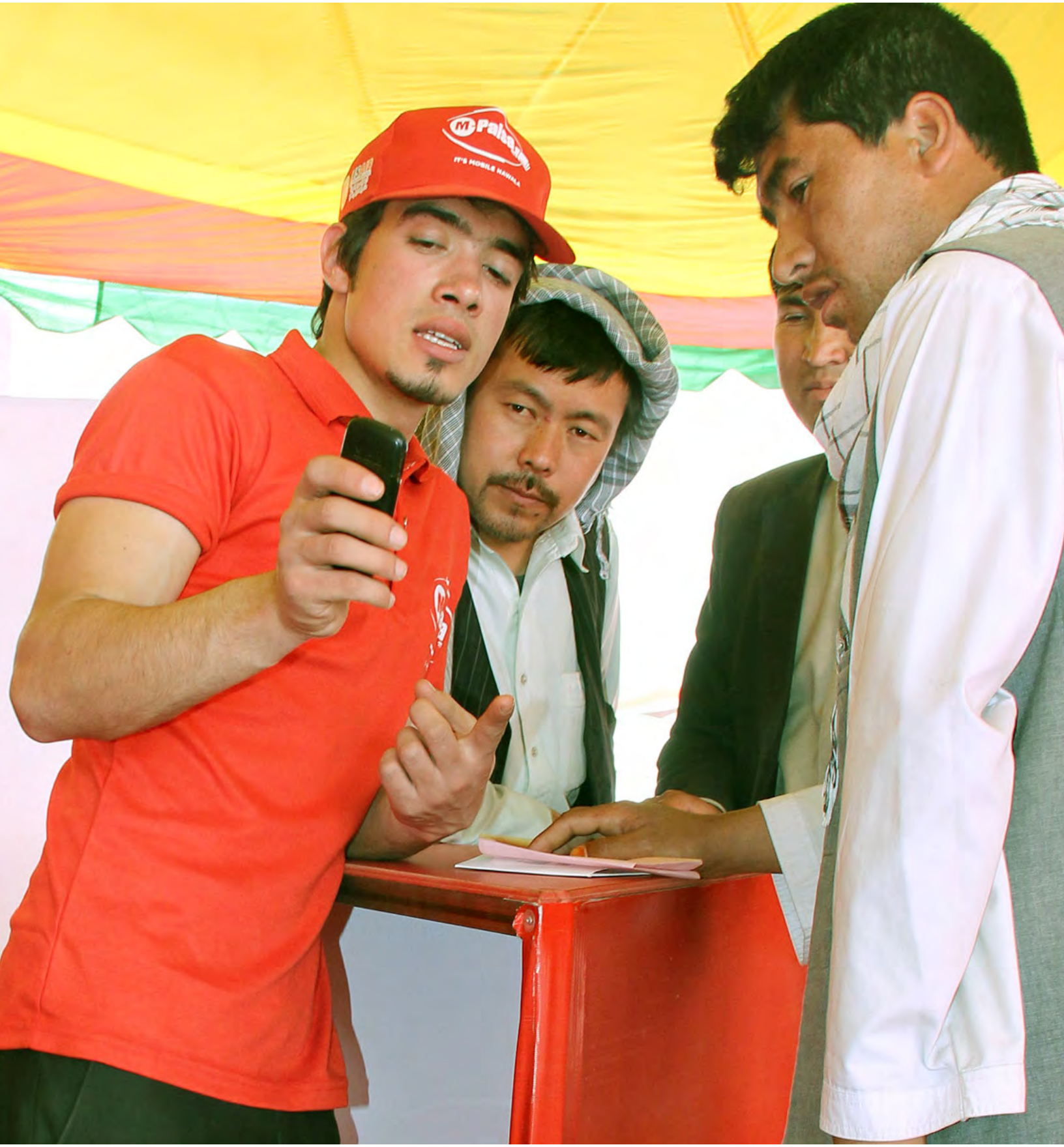
La deuxième partie du *Guide de la cybersécurité pour les petites et moyennes entreprises* offre des stratégies permettant aux propriétaires de petites entreprises de protéger leur organisation contre les menaces de cybersécurité, afin de les aider à se familiariser avec ces stratégies. Pour de plus amples informations, les propriétaires de petites entreprises devraient consulter des ressources plus élaborées sur Internet ou demander l'avis d'un professionnel de l'informatique.

D'un point de vue commercial, il peut être logique d'aborder la cybersécurité dans une perspective de conformité légale. Cela peut être un premier pas dans la bonne direction, mais les entreprises doivent partir du principe que l'innovation et les nouvelles technologies dépassent rapidement les réglementations. Les entreprises peuvent prendre des mesures relativement simples pour réduire considérablement la probabilité et l'impact des cyberattaques. Malgré de bonnes pratiques préventives, il est tout de même probable qu'au moins une attaque réussisse, ce qui oblige l'entreprise à devenir plus résiliente et à établir sa capacité à se remettre d'une telle violation.

L'importance d'un bon leader

Toutes les entreprises se posent la question de savoir qui devrait diriger le service de cybersécurité. L'article du *Harvard Business Review* sur la nécessité de repenser le leadership en matière de cybersécurité soutient que cette personne doit manager et être responsable de la cybersécurité, et doit être « une voix influente dans la stratégie commerciale, les décisions technologiques et la gestion des risques d'entreprise », plutôt que quelqu'un qui ne possède que des compétences techniques.[13] Les entreprises doivent intégrer la connaissance de la cybersécurité et les bonnes pratiques dans toute l'organisation, en couvrant tous les aspects : aspect technique, stratégie de planification commerciale, et individus, y compris les clients, fournisseurs et employés.

13 https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is



© FAIDA

COMMENT DÉMARRER

De nombreuses entreprises ont mis des mesures de cybersécurité en place dans le cadre d'une sécurité informatique complète pouvant considérablement réduire les risques d'attaque. Ces actions, connues sous le nom de « pratiques de cyber-hygiène », sont relativement simples, effectuées de manière régulières et peuvent avoir un impact positif sur la sécurité numérique des entreprises. Les meilleures pratiques de cyber-hygiène comprennent :

1. Former les employés à faire confiance mais vérifier ;
2. Installer des logiciels antivirus et antimalware réputés et les maintenir à jour ;
3. Utiliser des pare-feux et les vérifier régulièrement ;
4. Définir des mots de passe robustes et les modifier fréquemment.
5. Utiliser une authentification multi-facteurs ;
6. Mettre le/les logiciel(s) à jour régulièrement ;
7. Crypter toutes les données sensibles ;
8. Sécuriser les connexions Wi-Fi ;
9. Surveiller les systèmes de paiement ;
10. Sécuriser le site Web de l'entreprise ;
11. Empêcher les téléphones portables d'être des cibles ;
12. Conserver des sauvegardes de toutes les données ;
13. Ne pas oublier que la sécurité physique fait partie de la cybersécurité ;
14. Se renseigner sur les cyber-assurances ; et
15. Envisager d'embaucher un professionnel de l'informatique.

FORMER SES EMPLOYÉS

Pour qu'une entreprise réussisse, ses employés doivent être formés, et cette formation doit inclure une connaissance de la cybersécurité. Des nouveaux employés ou formations doivent initier les employés aux compétences et systèmes nécessaires à leurs fonctions, y compris la cybersécurité basique. La formation continue et les certifications ou mises à jour annuelles préparent les employés à l'évolution de l'environnement commercial et doivent également couvrir les mises à jour des politiques, stratégies et tactiques de cybersécurité pour limiter les menaces émergentes.

1. Former les employés à faire confiance mais vérifier

En règle générale, les employés ne doivent avoir accès qu'aux ressources et informations nécessaires à l'exercice de leurs fonctions. Afin de déterminer cet accès, l'entreprise doit connaître les données, les systèmes, les appareils, etc. et en connaître leur but. Les entreprises doivent si possible créer des profils d'utilisateurs, c'est-à-dire des comptes qui limitent l'accès à des ressources spécifiques au sein de l'entreprise. Lorsque cela n'est pas possible, la meilleure action suivante consiste à définir des restrictions et à protéger l'accès aux dossiers ou fichiers par mot de passe dans le cadre de la fonctionnalité des

systèmes d'exploitation. Il est également primordial de mettre fin à l'accès une fois qu'un employé quitte l'entreprise. Cela atténuera le risque de menaces internes. Si une entreprise désire se protéger grâce à des contrôles robustes, il existe de nombreuses solutions informatiques qui peuvent faciliter la création et la gestion des profils d'utilisateurs. Les administrateurs peuvent en parler avec un professionnel de l'informatique et doivent envisager de contacter le service d'assistance de leur système d'exploitation pour connaître les méthodes de contrôle d'accès appropriées.

ABONNEMENTS GRATUITS OU PAYANTS

De nombreuses sociétés de sécurité réputées proposent des versions gratuites de leurs programmes antivirus et pare-feu. Compte tenu du niveau de risque de l'entreprise, ces versions peuvent être une défense suffisante pour les entreprises à faible risque. Pour celles qui présentent un risque plus élevé, des abonnements payants premium peuvent être nécessaires pour fournir des fonctionnalités ou une assistance supplémentaires.

LIMITER LES RISQUES : COMPTES UTILISATEURS

Une fois qu'une entreprise a pris connaissances de ses données et des risques associés, elle doit définir qui a accès à quelles données. Pour cela, elle doit :

- **Dresser une liste complète** des comptes utilisés pour accéder à tous les services, appareils, applications, adresses e-mail, services cloud, bases de données, téléphones, tablettes, appareils Internet des objets (IdO), systèmes d'entreprise, etc. il faut connaître et enregistrer leurs utilisateurs, y compris les fournisseurs externes qui y ont accès.
- **Identifier chaque utilisateur et les flux de données auxquels il/elle a accès, et imposer l'utilisation de mots de passe différents pour chaque fonction ou système,** particulièrement pour les informations limitées.
- **Demander aux utilisateurs de ne pas partager leurs comptes et de protéger les données critiques par mot de passe.**

2. Installer des logiciels antivirus et anti-malware réputés

La solution la plus courante pour se protéger contre les logiciels malveillants est un logiciel antivirus. Les systèmes d'exploitation Microsoft Windows, Google Chrome et Mac disposent déjà d'un logiciel antivirus intégré qui fonctionne contre la plupart des menaces[14] et qui possède une fonctionnalité de base qui détecte et supprime les logiciels malveillants, lorsque ces systèmes sont mis à jour. Malgré les avantages de ces programmes intégrés, les attaquants peuvent facilement créer des programmes malveillants qui contournent ces protections. Il est recommandé d'inclure une protection antivirus supplémentaire sur les appareils informatiques de l'entreprise et de s'assurer qu'elle est régulièrement mise à jour.[15]

CONFIGURATION DU PARE-FEU

Testez le pare-feu lorsque vous mettez le plan de cybersécurité de l'entreprise en place. Cela aidera à s'assurer qu'il est correctement configuré et qu'il fonctionne. Bien qu'il existe plusieurs outils gratuits en ligne qui peuvent aider à effectuer des tests, il est prudent de travailler avec un professionnel de l'informatique qui pourra interpréter les résultats techniques et résoudre les problèmes identifiés.

3. Utiliser des pare-feux

Les pare-feux sont des dispositifs ou programmes qui contrôlent le flux d'informations ou le trafic entre les réseaux (trafic réseau) d'un réseau externe à l'entreprise, au sein

du réseau interne de l'entreprise ou entre des dispositifs ayant des configurations de sécurité différentes.[16] Les pare-feux peuvent être intégrés dans le routeur fourni par le fournisseur d'accès Internet (FAI) ou dans des programmes antivirus spécifiques. Un pare-feu est une défense essentielle pour une entreprise. En fonction du niveau de risque, les entreprises doivent envisager de mettre à niveau les pare-feux et de les compléter avec d'autres solutions, telles que celles qui cryptent le trafic ou surveillent de près les informations échangées avec et au sein du réseau de l'entreprise.

4. Définir des mots de passe robustes

Les mots de passe simples composés d'un seul mot que l'on utilisait par le passé ne sont plus efficaces pour la protection des comptes. Les attaquants disposent désormais d'outils capables de décrypter les mots de passe en moins d'une heure. Pour plus de sécurité, il faut définir des mots de passe contenant des phrases courtes avec des chiffres et caractères spéciaux pour les rendre plus complexes, plus longs et plus difficiles à deviner, tels que **#Sl33pWe11**, **Sc0r3G0a1!** ou **K0mbuchaP0w3r***.

LIMITER LES RISQUES : PROTECTION PAR MOT DE PASSE

Les mots de passe doivent toujours être complexes, conservés en lieu sûr, confidentiels et changés régulièrement. Les employés écrivent souvent leur mot de passe sur une note attachée à leur ordinateur ou placée près de leur zone de travail, menaçant la sécurité des données. Les « portefeuilles » numériques peuvent crypter les mots de passe de manière sécurisée.

Les entreprises doivent avoir un mot de passe pour chaque système ou site Web et doivent s'assurer qu'ils sont changés régulièrement ou au moins une fois par an. Si un site autorise des mots de passe plus longs (20 caractères ou plus), les utilisateurs peuvent créer des phrases de mot de passe complètes, comme « Je voudrais de longues vacances ! »

Les interfaces administratives des systèmes permettent généralement de personnaliser les exigences de mot de passe, y compris la fréquence de leur modification. Les entreprises doivent utiliser ces fonctionnalités pour créer des spécifications de mot d e passe fonctionnels.

14 https://www.av-test.org/en/antivirus/home-windows/

15 Des journaux réputés, comme *PC Magazine*, testent fréquemment les logiciels antivirus gratuits et les pare-feux, et dressent des rapports accessibles par le public. En voici quelques exemples : https://www.pcmag.com/picks/the-best-free-antivirus-protection

16 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

5. Utiliser l'authentification multi-facteurs

L'utilisation de l'authentification multi-facteurs s'est propagée ces dernières années. L'authentification multi-facteurs oblige les utilisateurs à fournir au moins deux moyens de vérification pour accéder à un compte, une application ou un système. Il peut s'agir d'une combinaison d'un mot de passe ou d'une information spécifique à l'utilisateur légitime et d'un code généré et envoyé par le système (par e-mail, SMS ou appel téléphonique) à l'utilisateur. De nombreuses plates-formes technologiques, y compris les fournisseurs d'authentification unique, les systèmes de paiement et les comptes utilisateurs, utilisent désormais l'authentification multi-facteurs. Si possible, les entreprises doivent s'assurer qu'il est activé pour les comptes internes (employé) et externes (client), selon le cas.

6. Mettre le/les logiciel(s) à jour régulièrement

Grâce aux mises à jour, les développeurs corrigent ou « patchent » les problèmes, y compris les vulnérabilités de sécurité des applications, des programmes ou des systèmes d'exploitation. Ces mises à jour doivent être installées dès que possible. Les entreprises doivent garder à l'esprit que seuls les développeurs peuvent corriger ces vulnérabilités. Si le problème ne peut pas se détecter, l'entreprise sera vulnérable, même si tous ses systèmes informatiques sont constamment mis à jour. Il s'agit d'un risque auquel il faut se préparer, mais la mise à jour régulière du logiciel d'entreprise pourra atténuer ce risque.

7. Crypter toutes les données sensibles

Le cryptage des données rend le contenu lisible uniquement pour ceux qui ont les clés ou les mots de passe permettant d'ouvrir ou de décrypter les données. Des fichiers individuels ou des appareils entiers, y compris des disques durs cloud, peuvent être cryptés. Il existe de nombreuses solutions de cryptage disponibles, Microsoft et Apple proposant des outils de chiffrement intégrés, tels que BitLocker[17] et FileVault[18] respectivement. L'inconvénient de ces outils est que si la clé ou le mot de passe est perdu, les données ne peuvent pas être récupérées. Assurez-vous de faire une copie de la clé dans un endroit sûr ou d'avoir un moyen de mémoriser en toute sécurité le mot de passe associé.

8. Sécuriser les connexions Wi-Fi

Les appareils Wi-Fi sont fournis par les FAI sous forme de boîtiers dotés d'un « modem » (appareil qui connecte l'entreprise au réseau du fournisseur) et d'un « routeur » (appareil qui diffuse le signal Wi-Fi dans l'entreprise) combinés en un seul dispositif. En règle générale, un technicien installe ce boîtier lors de l'installation Internet initiale et l'appareil reste intacte jusqu'à ce que le FAI le modifie ou qu'il tombe en panne et doive être remplacé. Les FAI achètent ces appareils en grandes quantités, et leurs exigences de sécurité pour les consommateurs ne correspondent pas nécessairement aux exigences d'une entreprise individuelle. Les appareils devront probablement être adaptés pour répondre aux exigences de cybersécurité d'une entreprise. Pour augmenter la protection d'un routeur, certaines mesures peuvent être effectuées à peu de frais ou gratuitement :

a. **Changer le mot de passe permettant l'accès aux paramètres du routeur.** Le routeur dispose d'une interface qui permet aux administrateurs de modifier la configuration de l'appareil. Les routeurs sont livrés avec un mot de passe générique ou attribué par le FAI permettant d'accéder à leurs paramètres. En suivant les instructions de l'appareil, les administrateurs peuvent remplacer le mot de passe générique par un nouveau mot de passe robuste. Ils doivent conserver ce nouveau mot de passe en lieu sûr et ne le partager qu'avec les personnes concernées.

b. **Mettre le logiciel du routeur du FAI de l'entreprise régulièrement à jour.** Le « Firmware » est le système d'exploitation du routeur. Grâce aux paramètres du routeur, les administrateurs peuvent vérifier et installer les mises à jour au besoin, conformément au plan de cybersécurité de l'entreprise. Ils doivent également planifier le renouvellement de l'assistance pour l'appareil en identifiant la date de fin de prise en charge.

c. **Toujours activer la sécurité, ou protocole de cryptage,** pour vous connecter au Wi-Fi et changer le mot de passe d'accès fréquemment. Si le routeur peut prend en charge un réseau invité, les administrateurs doivent l'activer et l'utiliser pour toute personne ou tout élément n'ayant pas besoin d'accéder aux systèmes informatiques de l'entreprise, y compris les invités, les fournisseurs externes et les appareils IdO privés. Les protocoles de cryptage Wi-Fi sécurisent la connexion entre le routeur et l'appareil qui s'y connecte, comme un ordinateur portable, mais ne sécurisent pas les communications Internet. Cela nécessite de modifier fréquemment le mot de passe du réseau invité. Le cryptage Wi-Fi évolue en permanence avec le Wi-Fi Protected Access (WPA) et son remplacement plus sécurisé, le WPA2, désormais couramment pris en charge par les appareils. Les entreprises doivent activer le protocole le plus récent possible et remplacer le mot de passe Wi-Fi par défaut (également appelé « phrase de chiffrement ») par un mot de passe robuste et unique, même si le mot de passe par défaut semble difficile à décrypter. Le WPA2 accepte une plage de 8 à 63 caractères, ce qui devrait être suffisant pour accepter les mots de passe réseau, tels que **HautLesMainsPeaudeLapin,HautLesMainsPeaudeLapin,HautLesMainsPeaudeLapin**. En réalité, les mots de passe Wi-Fi professionnels sont souvent partagés avec des tiers. Il est donc recommandé de les modifier régulièrement dans le cadre du plan de cybersécurité de l'entreprise et de s'assurer que le mot de passe interne, non invité, est sécurisé et non publié publiquement.

d. **Désactiver les connexions Wi-Fi faciles,** comme la technologie Wi-Fi Protected Setup (WPS) à bouton unique. Si le routeur n'est pas sécurisé, toute personne ayant physiquement accès au routeur pourra utiliser cette fonction pour se connecter au réseau.

e. **Changer le nom du réseau Wi-Fi.** Le Service Set Identifier (SSID) correspond au nom du réseau Wi-Fi. Remplacez le SSID par défaut par un SSID ne révélant aucune information personnelle et ne fournissant pas d'informations sur l'appareil, telles que la marque et le modèle du routeur ou le FAI, afin de limiter les attaques.

17 https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

18 https://support.apple.com/en-us/HT204837

f. **Se renseigner sur les conséquences de changement des paramètres du routeur.**
L'activation ou la désactivation d'une fonctionnalité peut faciliter les attaques ou limiter la fonctionnalité de l'appareil.

g. **Tester.** Quelles que soient les modifications appliquées au routeur, il faut toujours exécuter des tests pour voir si tout fonctionne comme prévu.

h. **Ajouter votre propre routeur.** Les petites entreprises disposent souvent de routeurs grand public, les FAI réservant les appareils sophistiqués aux gros clients. Une petite entreprise peut améliorer sa sécurité Wi-Fi et son contrôle sur la fonctionnalité du routeur en ajoutant son propre routeur connecté au routeur/modem fourni par le FAI. Les administrateurs peuvent contacter le FAI pour discuter de la mise en place de cette configuration ou rechercher des options auprès d es fabricants.

9. Surveiller les systèmes de paiement

Selon le type d'entreprise, les paiements s'effectueront de différentes manières, via un point de vente, le site Web de l'entreprise, une application ou un site marchand tiers, par exemple. Chaque option comporte des défis en matière de cybersécurité. Le Conseil des normes de sécurité de l'industrie des cartes de paiement (PCI), une organisation qui élabore des normes de sécurité liées aux méthodes de paiement, a créé des guides complets[19] sur les risques de ces différents systèmes, y compris les terminaux de paiement connectés à Internet ou les applications de paiement. Ces guides offrent également des conseils sur les mesures à prendre pour atténuer les risques. De nombreuses mesures concernent la cyber hygiène (la mise à jour des logiciels et l'utilisation de mots de passe robustes, par exemple), car les systèmes de paiement sont des appareils connectés. Le cryptage des données des cartes de paiement transmises vers le système de paiement et dans les systèmes marchands est primordial.

10. Sécuriser le site Web de l'entreprise

Un site Web est un outil permettant d'interagir avec les consommateurs, de fournir des services ou de vendre des produits, et il détermine l'identité numérique d'une entreprise. Pour bien sécuriser cet outil, il faut connaître les propriétés techniques du site, l'écosystème informatique dans lequel il est géré et l'endroit où le site est enregistré ou hébergé. De nombreuses entreprises utilisent des services cloud offrant des outils de création de sites Web faciles. Ces solutions facilitent la création et la gestion du site et délèguent une partie de la responsabilité de la protection et de la surveillance de l'infrastructure informatique au fournisseur d'hébergement. Cependant, les sites Web peuvent être à risque s'ils sont mal codés par l'outil de construction, les plug-ins, les extensions ou les services tiers mal configurés ou présentant des vulnérabilités.

SÉCURITÉ PHYSIQUE

La cybersécurité offre une protection dans le monde numérique, mais la cybersécurité et la sécurité physique se superposent. Toute personne ayant accès à un terminal de paiement peut l'altérer. Lorsqu'un pirate a un accès physique à un routeur, il peut voler les identifiants de connexion au réseau de l'entreprise. Ce guide ne traite pas des procédures de sécurité physique, mais les entreprises doivent garder à l'esprit qu'une stratégie de cybersécurité complète et réussie doit inclure la sécurité physique des locaux, des réseaux et des appareils..

LIMITER LES RISQUES : SÉCURITÉ DU SITE WEB

Allouez les ressources nécessaires à la sécurité du site Web de l'entreprise selon l'importance du site Web et les risques associés. Il faut :

1. **Être exigeant avec les identifiants de connexion de l'administrateur.** Limitez le nombre de personnes ayant des privilèges administrateur.
2. **Utiliser un hébergeur de site Web et un logiciel réputé pour la création et gestion du site.**[20] Les entreprises fiables auront de bonnes solutions de sécurité, comme les pare-feux, les antimalwares, la surveillance et la prévention de déni de service distribué (DDoS))[21] qui protègent les sites hébergés et les fonctionnalités évolutives.
3. **Mettre à jour le logiciel du site régulièrement.** Cela inclut la plate-forme, le logiciel du site Web et tous les programmes additionnels codés dans le site, comme les plug-ins, les extensions et les intégrations tierces.
4. **Utiliser des protocoles HTTPS.** Cela nécessite l'installation de certificats Secure Sockets Layer (SSL) qui cryptent les informations entre le site Web et l'utilisateur.
5. **Exiger des mots de passe robustes si le site permet aux utilisateurs de créer des comptes,** et activer les fonctionnalités de verrouillage des comptes après plusieurs tentatives de connexion infructueuses.
6. **Créer un « cyber pen » autour des fichiers téléchargeables par les utilisateurs.** Cela nécessite de mettre en place des mesures pour garantir la sécurité des fichiers, notamment les antivirus et antimalwares autorisés. Il est conseillé de limiter le type et la taille des fichiers acceptés pour le téléchargement et d'avoir un programme qui vérifie le type de fichier et s'assure que le fichier est téléchargé dans un emplacement sûr en dehors du dossier où les informations sensibles sont stockées ou des accès aux fichiers du site.
7. **Sauvegarder régulièrement le site Web, y compris toutes ses données. La fréquence des sauvegardes dépend de l'importance des données,** mais idéalement, les sauvegardes doivent être effectuées quotidiennement. Si possible, les entreprises devraient disposer d'un service de sauvegarde automatique. Si le site Web et ses données sont essentiels à l'entreprise, les organisations doivent envisager de faire des sauvegardes redondantes et de conserver les données de sauvegarde à différents endroits pour y avoir accès en cas de catastrophe naturelle ou politique, ou de cyberattaque.

19 https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf

20 Les entreprises telles que Wix, Squarespace ou Weebly sont réputées mondialement pour la qualité de leurs produits et services. Il peut y avoir des entreprises nationales ou régionales qui offrent des produits similaires.

21 Le déni de service distribué (DDoS) est une forme de cyberattaque qui submerge un serveur cible de demandes, ce qui finit par amener le serveur à rejeter les demandes réelles, et par désactiver le site Web.

22 https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

23 https://support.apple.com/guide/icloud/erase-a-device-mmfc0ef36f/icloud

24 https://support.google.com/accounts/answer/6160491?hl=en

11. Empêcher les téléphones portables d'être des cibles

Le nombre d'utilisateurs de smartphones ne cesse d'augmenter, on estime qu'il y aurait plus de 3,4 milliards d'utilisateurs aujourd'hui dans le monde.[22] De nombreux utilisateurs apportent les appareils sur leur lieu de travail ou utilisent ceux fournis par leurs employeurs. La différence entre les appareils mobiles et les ordinateurs de travail, c'est la quantité de données personnelles et professionnelles pouvant être enregistrée, et le fait qu'ils soient connectés en permanence. Leur portabilité les expose également à un risque plus élevé de perte ou de vol. Un pirate qui peut accéder à un téléphone, soit physiquement, soit en l'infectant avec un logiciel malveillant, peut pénétrer le réseau d'une entreprise. Gardez à l'esprit qu'une entreprise a plus de contrôle sur les appareils mobiles qu'elle fournit à ses employés que sur les appareils personnels utilisés dans un environnement professionnel.

LIMITER LES RISQUES : SÉCURISER LES APPAREILS MOBILES

Les entreprises peuvent améliorer la sécurité des appareils mobiles en suivant les pratiques générales de cyber-hygiène (mettre à jour les applications et les systèmes d'exploitation, installer des programmes fiables, configurer des connexions sécurisées, utiliser des réseaux Wi-Fi fiables, etc.). De plus, certaines précautions ne s'appliquent qu'aux smartphones. Les entreprises doivent :

1. **Acheter des appareils dont les données peuvent être effacées à distance et qui utilisent des fonctionnalités de sécurité renforcées.** Les téléphones sont souvent effacés grâce à une interface Web gérée par le fabricant ou le développeur. Apple[23] et Android ont tous deux cette fonctionnalité.[24] Une sécurité renforcée permet à l'utilisateur de crypter toutes les informations stockées sur son téléphone avec une sauvegarde sur le cloud ou sur un ordinateur personnel, un mot de passe robuste ou des informations biométriques étant nécessaires pour déverrouiller le téléphone. Les entreprises doivent utiliser toutes ces fonctionnalités.
2. **Utiliser et mettre à jour le système d'exploitation du fabricant.** Les utilisateurs remplacent souvent le système d'exploitation d'origine par un système créé par une communauté de développeurs. Ce processus est appelé « rooting » ou « jailbreaking ». Vu que la sécurité d'un système d'exploitation rooté et jailbreaké n'est pas garantie, ces appareils ne doivent pas avoir accès au réseau de l'entreprise ou à des données sensibles.
3. **Éviter de cliquer sur des liens suspects, notamment par SMS ou dans les applications de texte ou de messagerie.** Comme nous l'avons vu dans la section précédente, les liens compris dans les messages peuvent être utilisés pour diffuser des logiciels malveillants et lancer une attaque.
4. **Être vigilant sur les applications et limiter les données auxquelles les applications peuvent accéder.** Les chercheurs analysent régulièrement les

applications pour localiser les problèmes de sécurité, comme lors du récent débat impliquant TikTok et WeChat.[25] Il faut éviter d'utiliser les applications trouvées hors des magasins officiels du système d'exploitation (Google Play ou Apple Store, par exemple) et restreindre les données auxquelles les applications peuvent accéder après l'installation. Les entreprises doivent limiter l'accès des applications à d'autres ressources, telles que leur adresses, contacts, dossiers de fichiers, informations provenant d'autres applications ou appareils photo.

5. **Désactiver les fonctions lorsque vous ne les utilisez pas.** Les smartphones utilisent de nombreuses façons de se connecter, en plus des réseaux cellulaires, comme le Bluetooth, le Wi-Fi et l'AirDrop. Chaque méthode est potentiellement attaquable. Les administrateurs ne doivent activer ces fonctionnalités qu'en cas de besoin.
6. **Supprimer.** Une fois qu'un téléphone portable a été déconnecté du réseau d'une entreprise, toutes les données liées à l'entreprise doivent être supprimées. Le téléphone doit, si possible, être complètement effacé.

12. Conserver des sauvegardes de toutes les données

La plupart des entreprises dépendent aujourd'hui des données et des systèmes de technologie de l'information (TI). Lors de la mise en plan d'un plan de cybersécurité et de la création de sauvegardes, les entreprises doivent comprendre le fonctionnement des systèmes et prioriser les sauvegardes pour les informations les plus sensibles et les systèmes critiques. Plus l'entreprise mûrit, plus les administrateurs doivent envisager d'obtenir des systèmes sophistiqués qui aident à rétablir les opérations rapidement à la suite d'un incident.

Certaines entreprises pensent que le stockage cloud gratuit ou abordable fournit une sauvegarde adéquate. Bien que la plupart offrent un système de sauvegarde, si le stockage cloud est synchronisé avec un ordinateur, une attaque contre le système, le fichier ou le service cloud d'origine peut s'étendre aux données enregistrées, de sorte que ce type de protection peut ne pas être suffisant. Les entreprises doivent tirer pleinement parti des solutions cloud gratuites et réputées pour la protection de leurs données, mais elles doivent connaître les limites de ses solutions, comme leur incapacité à effectuer des sauvegardes de certains types et tailles de fichiers, l'incompatibilité avec les noms de fichiers et le risque de perdre des données entre la dernière et la prochaine sauvegarde.[26] Prenons l'exemple d'une petite entreprise qui produit des vidéos. Ses fichiers sont très volumineux, difficiles et relativement lents à sauvegarder sur les services cloud. Perdre des jours ou des semaines de données non enregistrées peut être très coûteux. Dans certains pays, les solutions gratuites ne sont pas suffisantes pour être conforme avec les réglementations..[27]

LES COÛTS D'UNE PERTURBATION

En 2014, le cabinet d'études mondial Gartner a constaté que le coût moyen des temps d'arrêt des entreprises était de 5 600 $ par minute. Pour une entreprise, ce coût peut être inférieur, selon les caractéristiques de l'organisation, du pays et du secteur, mais il est raisonnable d'estimer que sans plan de cybersécurité, les coûts de remise en ligne de l'entreprise s'élèveront à plusieurs jours de coûts opérationnels, même dans le meilleur des cas.

25 https://www.vox.com/recode/2020/8/11/21363092/why-is-tiktok-national-security-threat-wechat-trump-ban

Une sauvegarde adéquate doit sauvegarder les programmes et les systèmes d'exploitation en plus des données. Elle doit créer une copie ou une image complète de toutes les informations sur les disques durs utilisés par les ordinateurs de l'entreprise. En cas d'incident, cette image peut être rechargée sur un ordinateur propre ou neuf, ce qui réduit le temps de récupération.[28] À l'aide d'un logiciel spécialisé, les sauvegardes peuvent être enregistrées localement (sur le stockage de l'ordinateur), sur des disques ou des supports externes, sur un service cloud ou dans un système hybride utilisant à la fois le stockage local et cloud.

LIMITER LES RISQUES : SAUVEGARDER LES DONNÉES

Les entreprises doivent sauvegarder leurs données souvent, et si possible de manière automatique. Si l'entreprise ne dispose pas d'un système de sauvegarde automatique, elle doit consacrer le temps nécessaire à la sauvegarde complète manuelle. C'est important lorsque l'on considère le niveau de tolérance à la perte de données applicable à une entreprise. Les systèmes d'exploitation Microsoft et Apple, ainsi que de nombreux systèmes d'exploitation mobiles, offrent une fonctionnalité de sauvegarde qui peut être utilisée comme point de départ.

Les sauvegardes peuvent être corrompues ou perdues, ou le support utilisé pour les enregistrer peut devenir obsolète, il est donc sage de faire plusieurs copies en utilisant différents supports. Une copie doit être conservée hors site pour la protéger d'un incident catastrophique, comme un incendie ou l'effondrement d'un bâtiment, et toutes les copies doivent être cryptées.

Certaines entreprises peuvent souffrir d'un manque d'interconnexion ou de standardisation de leurs systèmes. Les employés n'ont pas forcément le même ordinateur ou le même système d'exploitation, et les informations peuvent être réparties sur des ordinateurs et des appareils adaptés aux fonctions individuelles des employés. Le comptable dispose par exemple de toutes les informations comptables, le responsable marketing dispose de toutes les informations marketing, etc. Dans ce cas, la création de sauvegardes manuelles peut être la seule option possible, à moins que l'entreprise ne soit prête à investir dans une infrastructure informatique capable de prendre en charge tous les dispositifs.

13. Ne pas oublier que la sécurité physique fait partie de la cybersécurité

Les équipements informatiques physiques comprennent de nombreux risques. La connexion, la déconnexion, le redémarrage et le chargement font partie des nombreuses actions qu'un attaquant peut entreprendre pour faciliter ou lancer une cyberattaque lorsqu'il a un accès physique aux appareils de l'entreprise. Les ordinateurs contenant les informations professionnelles les plus sensibles doivent être conservés dans un endroit sûr, comme une armoire ou un bureau verrouillé. Un routeur ne doit pas être laissé sans sécurité dans une zone à accès libre. Les entreprises doivent être sûres que les appareils connectés industriels nécessitent des clés pour fonctionner. Afin de déterminer les appareils critiques, une entreprise doit au minimum savoir de quels appareils elle dispose, leur utilisation et le type d'informations qui y sont stockées.

La plupart des entreprises ont déjà des protocoles de sécurité physique solides en place, et les mesures dépendent du type d'entreprise et de son emplacement. Il est important d'inclure les équipements cyber dans la sécurité physique de l'entreprise.

VÉRIFIER LA CYBER-HYGIÈNE

Les entreprises doivent identifier les pratiques et politiques appropriées en matière de cyber hygiène. Les administrateurs peuvent examiner les points 1 à 13 de cette section et déterminer les conseils les plus pertinents pour leurs types de données et de systèmes. Ils doivent également déterminer si l'entreprise utilise ces conseils au mieux, puis identifier les domaines nécessitant une amélioration ou mise à jour.

14. Se renseigner sur les cyber-assurances

Sur certains marchés, les compagnies d'assurance proposent des polices qui couvrent les pertes résultant d'une cyberattaque, comme une interruption du réseau ou une violation de données. La cyber assurance ne doit pas être considérée comme un substitut à la cybersécurité. Lorsqu'elle est disponible, cette assurance peut être un outil précieux permettant de limiter les dommages et renforcer les cyberdéfenses, mais elle n'élimine pas tous les risques et ne couvre pas toutes les conséquences et coûts des cyber incidents.

Lorsqu'elles décident d'acheter un type assurance, les entreprises doivent tenir compte de son profil de risque et non des types d'assurances d'autres entreprises, même similaires. Prenons l'exemple d'une entreprise qui offre une livraison garantie dans les délais. Si une cyberattaque l'empêche de livrer les produit dans les temps, l'entreprise aura un risque accru de mise en cause de la responsabilité par rapport à ses concurrents.

26 Lorsqu'il y a un incident, même si une entreprise fait des sauvegardes régulières, elle perd toujours une partie de ses données. Si une sauvegarde est effectuée quotidiennement à la fermeture des bureaux le vendredi et qu'une attaque se produit à la fin d'un lundi, l'écart serait de 72 heures.

27 https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

28 *PC Magazine* passe régulièrement en revue les services de sauvegarde et les évalue en fonction de différents critères de référence. https://www.pcmag.com/picks/the-best-online-backup-services

LIMITER LES RISQUES :
ASSURANCE POUR LES ENTREPRISES

Les entreprises disposant de polices d'assurance professionnelles doivent contacter leur assureur pour savoir si les cyberattaques ou les pertes produites par un cyber incident, telles que la perte de données en raison d'un vol par un employé, sont couvertes. Les entreprises peuvent également se renseigner sur une assurance cyber supplémentaire et si, dans le cadre de la police d'assurance, l'assureur offre un soutien pour améliorer les pratiques de cybersécurité à l'assuré. Ces services sont parfois offerts afin de réduire les risques pour l'assureur. Lorsqu'elles discutent avec un assureur et lorsqu'elles envisagent l'achat d'une police d'assurance, les entreprises doivent se rappeler des points suivants :

- Il existe des coûts associés à la récupération des données, y compris le temps du personnel et l'achat potentiel de nouvel équipement. Les données peuvent également être considérées comme un élément de valeur.
- Un incident affectant l'entreprise ou les données peut se produire dans le système de l'entreprise, dans un système tiers ou pendant le transfert de données. Les données des systèmes de fournisseurs tiers peuvent ne pas être couvertes par une assurance standard.
- Des acteurs étrangers sont souvent à l'origine d'attaques. Cela peut inclure des groupes parrainés par un gouvernement ou des groupes provenant d'états voyous qui souhaitent provoquer un chaos général et des perturbations, sans nécessairement nuire à une entreprise en particulier. Les entreprises doivent connaître les incidents, y compris les « cas de force majeure », qui sont couverts ou non par leur assurance.
- Les attaques peuvent nuire à la réputation d'une entreprise et engager la responsabilité légale. Des services juridiques, informatiques ou professionnels peuvent être nécessaires pour en gérer les conséquences. Les entreprises doivent clarifier et comprendre les responsabilités potentielles en matière de paiement d'amendes et d'indemnisations, ainsi que toute autre obligation découlant d'un cyber incident.
- Lorsque des données personnelles sont compromises, les lois peuvent exiger que l'entreprise fournisse une notification immédiate aux personnes et aux entreprises concernées, en plus du remboursement de l'argent perdu et des frais encourus, ainsi que d'autres dédommagements. Les entreprises doivent vérifier si ces exigences sont couvertes par leur assurance.
- Les compagnies d'assurance ont des directives qui diffèrent pour ce qui est des logiciels de rançon ou de l'extorsion. Les entreprises doivent connaître les politiques et procédures requises, particulièrement s'il y a lieu d'agir, et comment. Les compagnies d'assurance peuvent définir les conditions liées à la cybersécurité de manière différente. Les entreprises doivent pouvoir comprendre ce que propose ces compagnies en fonction des conditions qu'elles leurs offrent.

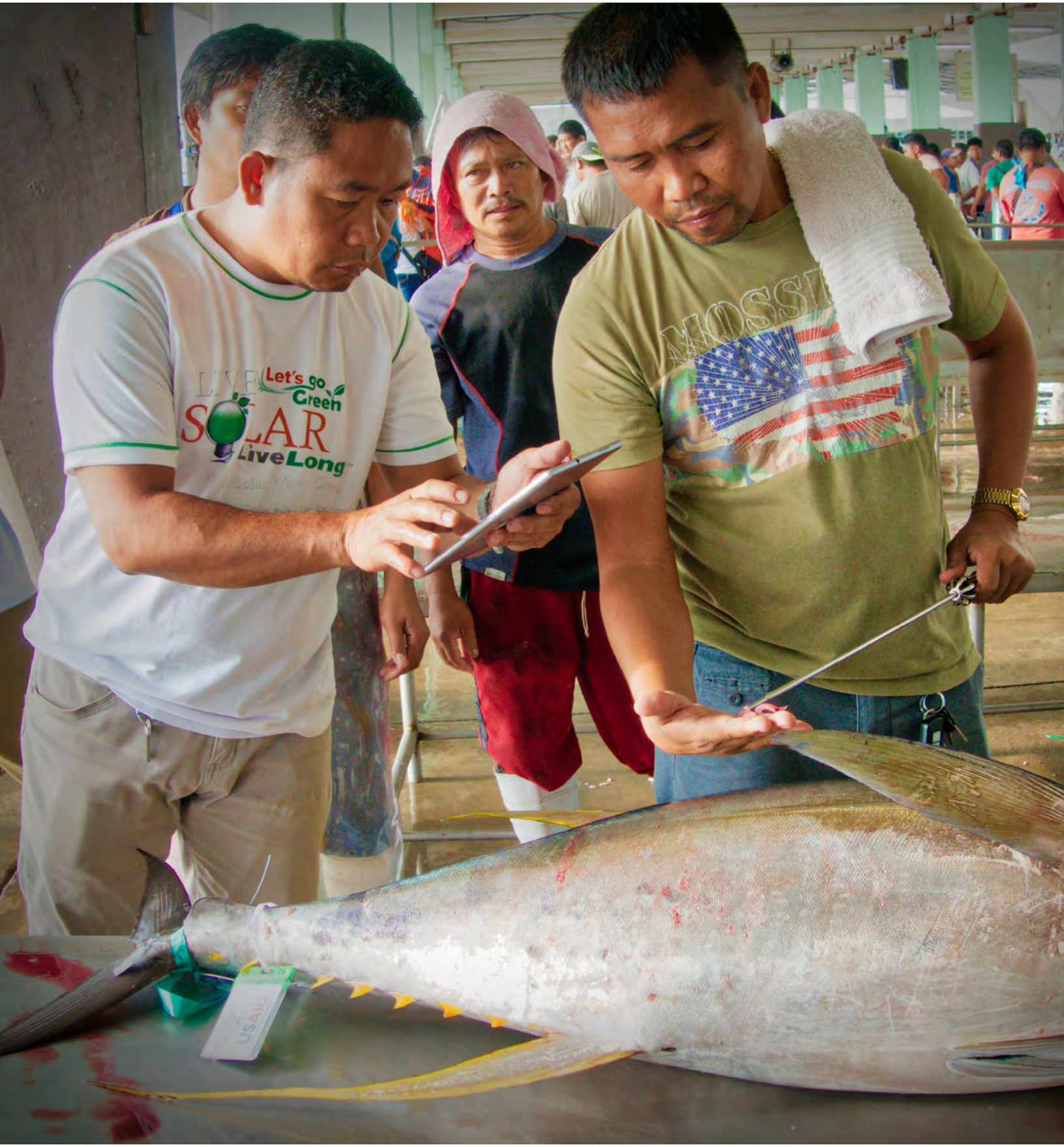
- Il existe des éléments ou des risques que la cyber-assurance ne couvrira pas, tels que les pertes futures potentielles ou le coût de l'amélioration des systèmes de sécurité. Une entreprise doit garder à l'esprit que ces dépenses doivent être couvertes en cas d'incident.

Compte tenu de ces points, les entreprises doivent déterminer si une assurance cybersécurité leur est nécessaire. Si c'est le cas, le plan de reprise d'activité doit inclure les étapes de collecte des informations requises pour déposer une réclamation dans le cadre de la police d'assurance cyber choisie.

15. Envisager d'embaucher un professionnel de l'informatique

Les sections de ce guide peuvent aider une entreprise à développer un plan de cybersécurité solide et la guider pour ce qui est de la croissance, des modifications et de l'adoption de nouvelles technologies. À un moment donné, il peut être nécessaire d'embaucher un professionnel de l'informatique, soit en tant que consultant, soit en tant qu'employé. Dans ce cas, les propriétaires de petites entreprises et leur personnel peuvent acquérir une compréhension fondamentale de la cybersécurité grâce à ce guide, ce qui leur permettra de choisir le meilleur type d'assistance pour leur entreprise.

Il est très important de connaître les risques pour l'entreprise, les actions à entreprendre pour réduire les risques immédiats et la méthode à implanter permettant d'atteindre les objectifs de réduction des risques dans un cadre commercial. Pour rappel, le cyber est un risque opérationnel qui peut avoir des conséquences importantes pour une entreprise et ses clients. La sensibilisation à la cybersécurité peut aider une entreprise à s'améliorer. La transformation n'a pas besoin d'être immédiate, elle peut être planifiée de manière que des objectifs soient atteints régulièrement au fil du temps. Il est cependant important d'établir une culture d'entreprise incluant la sensibilisation à la cybersécurité, de connaître les mesures entreprises pour faire face au cyber-risque et d'identifier les actions permettant d'améliorer la cybersécurité de l'entreprise.



© MELINDA DONNELLY FOR USAID/OCEANS

DANS LE CAS D'UN INCIDENT DE CYBERSÉCURITÉ

Une entreprise doit toujours réagir rapidement en cas de cyberattaque ou d'incident de cybersécurité. La vitesse de cette réaction peut faire la différence entre des dommages mineurs ou une perturbation majeure. Un administrateur doit tout d'abord informer les personnes concernées. Cela peut inclure le personnel interne ayant un rôle spécifique ou des consultants externes pouvant fournir des services spécialisés nécessaires, tels que la sécurisation des opérations, l'arrêt d'une violation de données, les analyses informatiques, la correction des vulnérabilités, la rédaction de mémorandums juridiques pour les rapports et les communications avec les autorités compétentes ou les intervenants, tels que les clients et les fournisseurs. Ils vont déterminer les obligations juridiques nécessaires selon le type d'incident. Les gouvernements ou les entités gouvernementales peuvent réglementer la notification des failles de sécurité de manière différente, ce qui est particulièrement le cas quand des données personnelles sont impliquées.

Rétablir les opérations

Lors d'un cyber événement, il peut être nécessaire de mettre les ordinateurs et l'équipement réseau hors ligne pour empêcher tout accès ultérieur aux systèmes de l'entreprise et pour éviter la propagation de logiciels malveillants sur des équipements non infectés.

Les entreprises doivent suivre les conseils des professionnels de l'informatique, du fournisseur d'antivirus et/ou du fournisseur de sauvegarde. Les sauvegardes complètes du système, comme indiqué ci-dessus, sont souvent le meilleur moyen pour restaurer les systèmes à leur état non affecté et pour rétablir les opérations commerciales. Les entreprises doivent pouvoir identifier la source de l'attaque afin que la vulnérabilité ne soit pas exploitée à nouveau, ce qui entraînerait une nouvelle atteinte aux systèmes de l'entreprise.

Les étapes des opérations de restauration dépendent de la nature de l'incident, de l'activité et des données concernées.

Gérer les communications de manière efficace

Après qu'une entreprise ait été la cible d'une cyberattaque, la stratégie de communication doit passer en mode urgence. Ce qui est annoncé publiquement sur le moment peut être essentiel pour survivre à une attaque, conserver la confiance et la réputation de l'entreprise et minimiser la responsabilité légale. L'institut de génie logiciel de l'université de Carnegie Mellon a élaboré un guide pour communiquer efficacement lors de la

DANS LE CAS D'UNE CYBERATTAQUE

Les administrateurs doivent disposer d'une liste papier des contacts d'urgence en cas d'incident de cybersécurité. Ils doivent s'assurer que ces contacts ne dépendent pas des systèmes de messagerie ou de téléphone de l'entreprise. L'administrateur doit également vérifier que chaque personne connaît ses responsabilités en cas de cyber incident.

Le cas échéant, l'administrateur peut contacter le processeur de paiement de l'entreprise et collecter toutes les informations nécessaires à la reprise des activités.

SE PRÉPARER AUX CYBERATTAQUES

Les entreprises peuvent simuler un cyber incident pour tester le temps de réponse de l'entreprise et pour déterminer si chaque employé connaît son rôle. Utilisez des sauvegardes pour vous entraîner aux opérations de restauration.

29 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651816

INSTITUT NATIONAL DES NORMES ET DE LA TECHNOLOGIE

NIST, par son acronyme anglaise, développe des normes, des directives, des meilleures pratiques et d'autres ressources en matière de cybersécurité. Ils sont une excellente ressource pour les grandes et les petites entreprises.

- Coin de la cybersécurité des petites entreprises
- Guide de démarrage rapide du cadre de cybersécurité
- Guides de cybersécurité à tout faire
- Guide pour répondre à un cyber incident

gestion des incidents,[29] expliquant comment communiquer lors d'un incident. Ce guide fait également référence aux communications dans le cadre de cybersécurité (CSF) de l'Institut national des normes et de la technologie (NIST), ce qui facilite leur intégration dans la communication globale de l'entreprise.

Pour communiquer efficacement lors de la gestion des incidents, les entreprises doivent élaborer un plan de communication en suivant le guide et les dix points principaux de Carnegie Mellon.[30] Les entreprises doivent :

1. Penser la communication en tant qu'initiative stratégique.
2. Avoir un plan de communication réactif.
3. Considérer le message, la réputation et les intervenants de l'entreprise comme des facteurs clés dans l'élaboration des plans de communication.
4. Dans le plan de communication, définir et déterminer les éléments clés suivants :
   - Établir l'objectif ;
   - Identifier le public concerné ;
   - Définir les rôles et les responsabilités ;
   - Comprendre et standardiser le message ;
   - Déterminer et établir des chaines de communication ; et
   - Définir les méthodes de distribution du message.
5. Former et tester le plan sans cesse. Assurez-vous que le plan fonctionne et, comme pour le plan de réponse aux incidents, testez-le au préalable afin qu'il soit prêt pour la gestion des incidents.

Le partage d'informations et la communication avec le public et/ou les clients conviennent à la plupart des scénarios, mais il est important que les entreprises se mettent en rapport avec les forces de l'ordre locales et les autorités compétentes avant de communiquer publiquement. La méthode et le contenu peuvent varier selon le scénario. La gestion des médias doit également être prise en compte car les médias pourraient parler de l'incident, il est donc important de comprendre les motivations des médias et de l'entreprise, et de les harmoniser.

NOTIFIER LES AUTORITÉS

Lorsque des délits commis sur l'Internet, comme le piratage, les rançongiciels, etc., se produisent, il faut agir rapidement pour minimiser les dégâts causés à l'entreprise et limiter la responsabilité légale en cas de problèmes de conformité. Chaque juridiction a des exigences liées aux déclarations et des délais spécifiques, de sorte que les entreprises doivent contacter les autorités locales avant tout incident pour connaître les exigences qui s'appliquent à leur type d'organisation. Cela inclut les exigences légales spécifiques et les conseils sur l'instant où il faut impliquer les autorités après des menaces ou des demandes de rançon. Les cyber délits peuvent faire l'objet d'enquêtes et de poursuites qui diffèrent des autres crimes, les entreprises doivent donc informer toutes les autorités compétentes susceptibles de superviser l'incident. Il est préférable de

connaître ces informations à l'avance afin que le personnel clé connaisse les exigences liées aux déclarations.

En général, les entreprises doivent s'attendre à fournir des informations exactes et complètes sur l'attaque et les parties impliquées, y compris :

- Le type d'incident, quand il a été détecté et ce qui s'est passé.
- Si des transactions financières ont été impliquées, telles qu'une rançon. Les agences gouvernementales exigeront probablement les numéros et noms des titulaires de compte, les dates et les montants des transactions, les destinations des transactions, etc.
- Des copies des communications entre l'attaquant et la victime.
- Tout autre renseignement relatif au piratage signalé, y compris le nom et les informations de contact des organisations et individus dont les données ont été exposées.

Les administrateurs doivent être conscients que les attaquants utilisent des techniques leur permettant de pénétrer et de demeurer dans un réseau sans être détectés jusqu'au lancement d'une attaque. Il peut donc se passer du temps entre la violation initiale et des activités illégales. L'accès aux données commerciales les plus critiques peut être piraté, mais l'entreprise peut en prendre connaissance plus tard, lorsque les clients appellent au sujet de débits non autorisés sur leurs cartes de crédit, par exemple. Les entreprises doivent documenter toutes les circonstances et leurs chronologies pour pouvoir fournir un rapport complet de l'incident. Cela peut inclure les connexions au réseau, les registres de trafic, les adresses IP (Internet Protocol), les sites Web concernés, les demandes de transfert électroniques, etc. Un professionnel de l'informatique pourra aider à rassembler toutes ces informations. En cas de doute, les entreprises doivent ajouter toutes les informations possibles au dossier d'incident. Des informations qui paraissent insignifiantes peuvent être cruciales selon les circonstances. Si un professionnel de l'informatique est embauché, il doit vérifier que l'attaquant n'est plus présent sur le réseau, et assurer la liaison avec les autorités pour l'enquête sur l'incident et pour la préservation des preuves.

NOTIFIER LE FOURNISSEUR D'ACCÈS

Les attaques récentes suivent un modèle de « réseau en étoile », car les attaquants violent les systèmes développés par les fournisseurs pour cibler leurs clients. Si l'attaque utilise des prestataires de services, tel qu'un processeur de paiement, pour effectuer des paiements non autorisés, ou implique le service de stockage de données d'un fournisseur, les entreprises doivent informer les fournisseurs concernées et consulter les autorités de façon conjointe, afin de limiter les dégâts et accélérer le processus de récupération. Une entreprise peut également faire partie d'une chaîne d'approvisionnement qui a été entièrement ou en partie exposée lors d'un cyber incident. L'entreprise doit alors informer les partenaires en aval et en amont de l'incident et doit partager les informations pertinentes avec eux.

30 https://insights.sei.cmu.edu/blog/top-10-considerations-for-effective-incident-management-communications/

CREER UNE COMMUNICATION DYNAMIQUE

Les entreprises doivent rédiger un modèle de message initial destiné aux consommateurs, clients et fournisseurs en cas d'attaque exposant leurs données. Ils doivent adapter ce message aux types de données client et fournisseur collectées et stockées dans l'entreprise et s'assurer qu'il est conforme aux exigences légales.

FAIRE DES COPIES PAPIER

À l'aide des informations compilées dans ce guide, les entreprises doivent préparer un dossier d'urgence de cybersécurité contenant des copies papier de tous les documents préparés pour la cber atténuation et les éventualités. Elles doivent s'assurer que le dossier est accessible même si les systèmes informatiques sont inutilisables en cas d'incident informatique.

Les administrateurs doivent discuter de ces plans avec les prestataires de services et les fournisseurs pour mieux se préparer aux attaques, afin que chacun connaisse le processus de signalement d'un incident, les informations nécessaires à l'obtention d'aide et la manière de rétablir les opérations. Ils doivent documenter ce processus dans le cadre de la stratégie de cybersécurité de l'entreprise.

NOTIFIER LES CLIENTS ET LES CONSOMMATEURS

Afin de garantir à toutes les personnes concernées que leurs intérêts sont protégés et que les impacts immédiats et à long terme de l'incident sont minimisés, il faut une divulgation rapide et honnête, des conseils d'experts et une coordination avec les autorités.

Les notifications doivent généralement répondre à des exigences légales ou réglementaires. Lors de la première notification aux autorités, les entreprises doivent savoir si les lois ou réglementations imposent une notification spécifique des parties concernées, connaître les caractéristiques de ces notifications et le délai accordé pour les exécuter. Il est important que les interactions ne compromettent pas les enquêtes des autorités, il faut donc être extrêmement vigilant quant à leur participation au calendrier et au contenu des communications de l'entreprise.

Lors de l'élaboration de communications, les entreprises doivent inclure les informations suivantes :

- Une explication simple et honnête de l'incident ;
- Une explication sur les données compromises et l'impact de la violation sur les clients et fournisseurs, sur le moment et à l'avenir ;
- Un rappel des lois ou réglementations applicables et des agences impliquées dans le dossier ;
- Les mesures entreprises pour se remettre de l'incident et pour protéger les intérêts des clients et des fournisseurs ;
- Des conseils sur ce que les clients et les fournisseurs peuvent faire pour se protéger si leurs données ont été compromises ou utilisées à mauvais escient ;
- Les coordonnées d'un interlocuteur pouvant répondre aux questions ;
- Les moyens par lesquels les clients et les fournisseurs seront tenus informés des développements (par exemple, via e-mail, site Web de l'entreprise, etc.), conformément aux exigences légales.

RÉSEAUX SOCIAUX

Les entreprises doivent présumer que l'incident sera partagé sur les réseaux sociaux. Le plan de communication doit inclure une composante sur l'utilisation efficace des médias sociaux. Les points décrits ci-dessus s'appliquent aux communications sur les réseaux sociaux, mais les informations publiées sur ces réseaux sont susceptibles de devenir connues publiquement, au-delà du groupe de clients ou de fournisseurs concernés.

Tirer des leçons de l'incident

Une fois les opérations rétablies, les entreprises doivent faire le point sur ce qui s'est passé, ce à quoi les attaquants ont pu accéder et sur l'efficacité du plan de réponse. Elles peuvent ensuite examiner les mesures de sécurité en place et chercher des méthodes pour les renforcer afin d'empêcher qu'une attaque similaire ne se reproduise, ainsi que tout type d'attaque pour laquelle l'entreprise n'est pas préparée. (Voir « Catégories de menaces », dans la 1ère partie de ce guide). Les entreprises doivent déterminer ce qu'il faut mettre en place à l'avenir pour améliorer la réponse aux incidents, en se penchant sur la façon dont la violation a été découverte, comment elle a été communiquée, en interne et en externe, et comment elle a été résolue. Il sera plus facile de se préparer aux incidents futurs grâce à une connaissance précise des coûts (financiers, réputationnels et opérationnels, entre autres) d'une attaque et des mesures nécessaires à la prévention de cette attaque.

APPRENTISSAGE

À la suite de chaque incident et au moins une fois par an, les entreprises doivent réviser et développer leur plan d'intervention et formation du personnel afin de documenter ce qui a été appris et les éventuels changements à mettre en œuvre.

CONCLUSION

Les étapes décrites dans ce guide ne nécessitent pas un haut niveau d'expertise ou de grandes dépenses, mais nécessitent de la réflexion et une planification afin d'être mises en œuvre. Bien qu'il s'agisse d'actions basiques peu onéreuses que toute petite entreprise est en mesure de mettre en place, les étapes pourront être intégrées à des stratégies plus sophistiquées à mesure que l'organisation mûrit dans sa compréhension du cyber et que l'entreprise se développe. Plus la cyber technologie se développe et évolue, plus de nouvelles menaces vont apparaître et plus de nouvelles ressources seront disponibles pour les entreprises. En attendant, les points abordés dans ce guide vous offrent une approche et un plan de base solides permettant de renforcer la cybersécurité et la résilience de votre petite entreprise.

USAID
FROM THE AMERICAN PEOPLE