Annexe 3

Diffusion sans restriction

(version numérique disponible sur les sites Internet du SGDSN et du gouvernement)

VIGIPIRATE

SÉCURITÉ DU NUMÉRIQUE SENSIBILISATION DES DIRIGEANTS

Cette fiche s'adresse aux dirigeants d'entreprises privées ou de collectivités territoriales et vise à les aider à appréhender la question de la sécurité du numérique à travers quelques exemples et recommandations pratiques.

1 Cela pourrait vous arriver...

Les scénarios proposés ci-dessous illustrent quelques exemples (parmi d'autres) de menaces de nature cyber pesant sur les organisations et relevant de la responsabilité de leurs dirigeants.

Usurpation d'identité / hameçonnage

Le hameçonnage consiste à usurper l'identité de l'expéditeur dans le but de duper le destinataire qui est invité à ouvrir une pièce-jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette 1ère machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation.

Arnaud reçoit une demande d'ajout de contact sur LinkedIn de la part de son supérieur hiérarchique pendant la période des fêtes de fin d'année. Ce dernier est en congés et souhaite lui transmettre des documents car il n'a pas accès à sa boîte mail momentanément. Mais ce qu'Arnaud ne sait pas, c'est que la personne qui s'adresse à lui n'est pas son supérieur mais un groupe d'attaquants ayant usurpé son identité. En transmettant à ce collaborateur un simple document contenant une charge malveillante, ils ont pu compromettre les équipements de l'entreprise connectés à Internet et exfiltrer des données sensibles en relation avec une importante négociation commerciale de nature confidentielle. Dès le lendemain, les informations fuitent dans la presse, conduisant ainsi à la rupture de la négociation au profit d'une entreprise concurrente.

Rançongiciel

Le rançongiciel est un programme malveillant chiffrant tout ou partie des données stockées sur un ordinateur ou accessibles par un réseau. L'objectif est de proposer à la victime de récupérer ses données en échange du paiement d'une rançon.

Guillaume est dirigeant d'entreprise. Nous sommes vendredi après-midi avant le début des congés de fin d'année et Guillaume avait déjà autorisé ses employés à partir exceptionnellement à 15h00. Son responsable sécurité lui indique qu'une mise à jour de l'ensemble des postes de travail doit être réalisée mais ne pourra pas être effective avant 15h00. Guillaume décide de fermer l'entreprise comme prévu et de reporter l'opération de mise à jour.
Le 2 janvier, les ordinateurs de tous les employés affichent un écran noir porteur d'un message exigeant d'eux le paiement d'une rançon en échange de la récupération de leurs données. Les employés ne pouvant plus travailler, l'activité de l'ensemble de l'entreprise et de ses sous-traitants est à l'arrêt et mise en péril.

Les conséquences pour votre entreprise peuvent être graves :
perte financière importante, atteinte à l'image de l'organisation, etc.

2 S'emparer de la question de la sécurité numérique

5 questions pour faire le point

- Depuis quand n'ai-je pas entendu parler de cybersécurité ?
- Mon entreprise est-elle une cible d'intérêt pour des attaquants ?
- Ai-je pris toutes les précautions pour protéger mes informations et les échanges avec mes partenaires et mes collaborateurs ?
- Quel est la part du budget consacrée à la sécurité informatique ?
- Ai-je déjà parlé de cybersécurité à mes collaborateurs ?

5 questions à poser à mon RSSI

- Quelles sont nos principales vulnérabilités ?
- Quels sont les moyens de protection actuellement en place pour lutter contre les attaques et codes malveillants ?
- A-t-on déjà fait un audit de sécurité des SI ?
  A-t-on déjà fait une analyse de risques ?
  Dispose-t-on d'une cartographie des SI ?
- Sommes-nous préparés si une crise d'origine cyber survenait ?
- Disposons-nous d'une couverture juridique et nos contrats d'assurance intègrent-ils le risque cyber ?

SÉCURITÉ DU NUMÉRIQUE
SENSIBILISATION DES DIRIGEANTS

Vous êtes au cœur de la stratégie de gestion des informations clés de l'entreprise. Vos données personnelles sont autant d'informations potentiellement convoitées par des individus aux intentions malveillantes. Soyez notamment vigilant à l'égard de possibles usurpations de votre identité sur les réseaux sociaux et maîtrisez les informations sur votre entreprise qui circulent sur Internet.

Sensibiliser vos employés aux bonnes pratiques

Vos employés doivent être sensibilisés voire formés aux bonnes pratiques de l'informatique et devenir acteur de la sécurité numérique de leur entreprise.

Analyser les risques et protéger les systèmes d'information sensibles

Il est essentiel de savoir quels sont les systèmes d'information les plus cruciaux pour le bon fonctionnement de votre entreprise afin de pouvoir traiter les risques susceptibles de les fragiliser.

Préparer votre entreprise à une attaque informatique

Assurez-vous de disposer d'un plan de réaction aux incidents de sécurité (notamment un processus de sauvegarde régulier des données critiques) et testez-le. En particulier, établissez une chaîne de remontée d'incidents connue des employés afin de reconnaître au plus tôt une tentative d'attaque.

Organiser un exercice simulant une attaque

Un exercice de gestion de crise permet de vérifier la solidité des procédures mises en place dans votre organisme et de les corriger si nécessaire.

3 Vous pensez avoir été victime d'une attaque

Qui prévenir ?

Dirigeant d'une entreprise (TPE, PME) ou d'une collectivité territoriale, il est recommandé de vous rendre sur la plateforme numérique www.cybermalveillance.gouv.fr afin d'être mis en relation avec des prestataires de proximité susceptibles de vous assister techniquement. Vous pouvez également déposer plainte auprès d'un service de la Police nationale ou de la Gendarmerie nationale ou adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

4 Documents de référence

Guide des bonnes pratiques de l'informatique
https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf.pdf
Guide d'hygiène informatique (à l'attention des DSI)
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
MOOC (Massive Open Online Course) SecNumacadémie de l'ANSSI
https://www.secnumacademie.gouv.fr
En cas d'incident
https://www.ssi.gouv.fr/en-cas-dincident/

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr