Les 10 bonnes pratiques de la cybersécurité

NORGAY SMB
ICEA + ANSCOM

Quelques chiffres

50%

Entreprises françaises **victimes d'une cyberattaque**

69%

Entreprises victimes sont des **TPE / PME**

>50%

Entreprises **investissant dans leur cybersécurité**

70%

Entreprises Ayant une **cyber-assurance**

94%

Logiciels malveillants **délivrés par e-mail**

50k€

Coût moyen d'une attaque

70M€

Rançon la plus élevée au monde !

90%

Brèches de cybersécurité causées par une **erreur humaine**.

Sources : ANSSI / CESIN / CNIL

NORGAY SMB
ICEA + ANSCOM

Évaluez votre informatique

Conseil 👍

Comprenez quelles informations vous devez protéger et où elles se trouvent, ainsi que tout le matériel et les logiciels en jeu. Il est essentiel de connaître l'inventaire que vous détenez, sa valeur, les menaces auxquelles il est confronté et d'évaluer où des améliorations sont nécessaires.

Quelle est votre dépendance à l'informatique ?
Exemple : Une usine qui produit 24/7 et dont l'outil de production est piloté par l'informatique aura une forte dépendance.

Notre solution ▸ L'audit de sécurité informatique

En quoi consiste un audit de sécurité informatique ?

Un audit de sécurité informatique est une analyse des risques encourus par une entreprise en termes de piratage et d'intrusion. Il permet de déterminer les failles du système et les solutions à mettre en place pour y remédier.

NORGAY SMB
ICEA + ANSCOM

2

Gestion des droits utilisateurs

Conseil 👍

Ne donnez l'accès administrateur aux systèmes d'exploitation et aux applications qu'à ceux qui en ont vraiment besoin. Vérifiez régulièrement la liste des administrateurs et mettez à jour les niveaux de privilèges en fonction des besoins de l'organisation.

Les comptes administrateurs, s'ils sont compromis, peuvent donner aux criminels les « clés du royaume », alors assurez-vous de disposer d'un processus pour supprimer (ou désactiver) ces comptes lorsqu'ils ne sont plus nécessaires.

Notre solution ▸ Faire l’inventaire des données

Faire l’inventaire des données qui sont disponibles dans votre système d’information.

Créer des groupes d’utilisateurs et y appliquer des droits d’accès en fonction des besoins de chaque groupe.

NORGAY SMB
ICEA + ANSCOM

Antivirus et EDR

Définition ✏️

Un virus est un programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire.

Il existe différents types de virus comme le rançongiciel, le cheval de Troie, le logiciel espion… Les virus peuvent s'infiltrer dans un système informatique par l'ouverture d'un message (mail, MMS, chat), d'une pièce jointe ou d'un clic sur un lien frauduleux, par exemple. Il peut aussi s'introduire en naviguant sur un site malveillant, en s'installant dans un appareil ou un logiciel non mis à jour, par l'absence d'utilisation d'un antivirus, l'installation d'une application piratée, etc.

Notre solution ▸ Antivirus et EDR

Les programmes antivirus centralisés pour les terminaux restent une couche de protection précieuse. Chaque virus, une fois qu'il est découvert est inscrit dans une base de données. Cette base de données est partagée entre tous les antivirus. On appelle cette base de données, une base de signature de virus. Les antivirus analysent en permanence ces bases de données pour trouver des virus.

Mais quid des virus qui n'ont pas encore été découverts ? On appelle ce genre de virus « Zero day ». Pour cela les antivirus ont ajouté une nouvelle fonctionnalité d'étude comportementale des programmes exécutés sur un ordinateur. Dès qu'un programme exécute une commande qu'il n'est pas censé faire, l'antivirus cloisonne le programme. Cette nouvelle fonctionnalité est appelé EDR (Endpoint Detection and Response).

Stratégie de mot de passe et MFA

RoboForm

Définition ✏️

Concrètement, l'authentification consiste à prouver que les utilisateurs sont bien ce qu'ils prétendent être. L'authentification multi facteur (MFA) va plus loin en exigeant des utilisateurs de fournir deux facteurs (catégories) d'authentification ou plus, avant que leur accès soit autorisé.

Un pirate ou un utilisateur non autorisé peut voler un mot de passe ou l'acheter sur le dark web, mais la probabilité qu'il ait accès à un second facteur d'authentification est très faible et requiert beaucoup plus d'efforts. Par conséquent, la MFA stoppe la plupart des acteurs malveillants avant qu'ils ne puissent pénétrer dans vos systèmes et accéder à vos données.

Notre solution ▸ MDP et authentification multi facteur

Stratégie de mot de passe et authentification multi facteur

- Inciter les utilisateurs à ne pas avoir un même mot de passe pour différents services
- Obliger les utilisateurs à avoir des mots de passe complexes
- Imposer une fréquence de renouvellement de mot de passe
- Bloquer les accès après plusieurs tentatives infructueuses
- Utiliser un coffre fort de mots de passe
- Mise en place de l'authentification multi facteur

NORGAY SMB
ICEA + ANSCOM

5

Anti-Spam

Définition ✏️

L'hameçonnage ou phishing est un mail frauduleux destiné à tromper la victime pour l'inciter à communiquer des données personnelles (identifiants, mots de passe etc..) et/ou bancaires en se faisant passer pour un tiers de confiance.

Notre solution ▸ L'anti-spam

L'anti-spam est un logiciel qui vise à détecter et à bloquer les e-mails potentiellement dangereux dans les boîtes de réception des utilisateurs.

Les protocoles anti-spam déterminent ce qu'est un message non sollicité et non désiré (spam) ; dans de nombreux cas, le spam fait la publicité d'un produit, qui peut être légitime (mais toujours non désiré) ou malveillant.

Cet outil offre une solution de filtrage totale, capturant les courriers indésirables et les virus avant même que les e-mails n'atteignent les serveurs. Cela garantit que votre boîte de réception reste propre et vous évite de passer des heures à traiter manuellement les courriels non sollicités.

Pare-feu

Définition ✏️

L’intrusion dans un système informatique (serveur, réseau…) se définit comme l’accès illicite à ce système par un pirate, ce qui peut entraîner le vol, voire la perte totale, des informations du système touché.

Notre solution ▸ Le pare-feu

Pièce maîtresse de la sécurité de votre réseau, un pare-feu est un appareil de protection qui surveille le trafic réseau entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

7

Sauvegarde

Définition ✏️

L’un des objectifs de la cybersécurité est d’éviter une perte de données.

La perte de données fait référence à divers scénarios qui entraînent une perte d'informations. Cela peut inclure le vol, les erreurs humaines, les logiciels malveillants, les cyberattaques, les virus, les pannes de courant, etc. En réalité les données peuvent être perdues pour de nombreuses raisons, la plupart du temps évitables.

Notre solution ▸ La sauvegarde 3 2 1

3 ▸ Créer 3 copies de données minimum. Stocker vos données sur trois copies minimise considérablement le risque potentiel de perte de données.

2 ▸ Stocker vos copies de données sur 2 supports de stockage différents.

1 ▸ Stocker 1 copie de données hors site.

NORGAY SMB
ICEA + ANSCOM

Formation des utilisateurs

Définition ✏️

Il n'y a pas une seule personne au monde qui ne fasse jamais d'erreurs. En fait, faire des erreurs est une partie essentielle de l'expérience humaine - c'est ainsi que nous grandissons et apprenons. Pourtant, dans le domaine de la cybersécurité, les erreurs humaines sont bien trop souvent ignorées.

D'après une étude IBM, l'erreur humaine est la cause principale de 95% des brèches de cybersécurité. En d'autres termes, si l'erreur humaine était entièrement supprimée, 19 brèches de sécurité sur 20 n'auraient peut-être pas eu lieu du tout !

Notre solution ▸ La formation

½ journée de formation pour les utilisateurs reprenant les grands thèmes de la cybersécurité ainsi qu'une mise en situation.

Ayez un plan

Conseil 👍

Soyez prêt en cas d'incident ou de violation. L'urgence de la situation après la violation peut conduire à des étapes manquées ou à l'engagement de mauvaises ressources.

Avoir un plan de reprise (testé) après sinistre pour garantir que vous pouvez reprendre vos activités dans un délai acceptable vous offre une tranquillité d'esprit.

Choisir entre PCA (Plan de continuité d'activité) et PRA (Plan de reprise d'activité) en fonction de votre dépendance à l'outil informatique.

Contrairement au PCA qui est là pour empêcher tout arrêt de l'activité de l'entreprise, le PRA va décrire l'ensemble des procédures nécessaires à un redémarrage au plus vite du système informatique.

Notre solution ▸ La formation

Norgay SMB vous aide à mettre en place un PCA ou PRA en fonction de vos besoins.

NORGAY SMB
ICEA + ANSCOM

10

Surveillance active

Conseil 👍

Même si vous avez mis en place une armée de systèmes de cybersécurité, celle-ci ne sert à rien si elle n'est pas dirigée et contrôlée.

Vous devez superviser votre système d'information pour être alerté dès la moindre anomalie. Cette surveillance peut être faite par vos équipes spécialisées en interne ou par les équipes d'un prestataire externe.

Notre solution ▸ La formation

Un contrat de maintenance CATE

Le contrat de maintenance informatique permet d'assurer le support technique aux utilisateurs et de maintenir le système d'information en conditions opérationnelles.

NORGAY SMB
ICEA + ANSCOM

Ils nous font confiance…

… Et ils sont plus de 700 !

En savoir plus

Sébastien JAEGLE
Responsable commercial infrastructure

s.jaegle@norgaysmb.fr
06 35 27 59 71

www.norgaysmb.fr

+33 (0) 3 20 714 714 / +33 (0) 3 21 60 57 30

support@norgaysmb.fr

NORGAY SMB
ICEA + ANSCOM