Dix astuces pour empêcher une cyberattaque

Une cyberattaque peut toucher n'importe quelle entreprise. Vous pouvez cependant vous protéger en prenant quelques mesures de précaution.

Sauvegarder les données
Définissez un processus réglant la sauvegarde régulière de vos données. Évaluez la quantité de données en nombre de jours que vous pouvez supporter de perdre et stockez en conséquence une copie supplémentaire de votre sauvegarde séparément (offline) et hors murs (offsite). Assurez-vous de conserver les sauvegardes antérieures durant plusieurs mois.

Régler l'utilisation des informations de l'entreprise
Demandez-vous exactement quelles informations vous voulez publier par exemple sur votre site internet ou sur les réseaux sociaux. En principe, aucune information confidentielle ne devrait être transmise par voie anonyme (p.ex. téléphone ou courriel).

Sensibiliser le personnel à l'utilisation des courriels
Cultivez une saine méfiance face à des liens ou des annexes de courriel dont l'expéditeur/l'expéditrice vous est inconnu(e). N'hésitez pas à lui poser des questions lorsque quelque chose vous paraît inhabituel et incitez votre personnel à faire de même.

Utiliser des mots de passe sûrs
Les mots de passe devraient comporter à la fois lettres, chiffres et caractères spéciaux, soit douze signes au minimum. Misez sur une authentification à deux facteurs dès que possible. Évitez absolument d'utiliser les mêmes mots de passe pour plusieurs applications! Pour ce faire, ayez recours à un gestionnaire de mots de passe et générez un mot de passe par application.

Régler l'accès aux données
Votre personnel ne devrait normalement disposer d'aucun droit d'administrateur.

Utiliser un ordinateur séparé pour les payements
Pour vos payements, utilisez un ordinateur séparé sur lequel vous ne pouvez pas surfer sur internet ni recevoir de courriels. Réglez clairement les processus concernant le trafic des payements (p.ex. le principe du double contrôle et la signature collective) et discutez avec votre banque des mesures de sécurité possibles.

Procéder à des mises à jour de sécurité
Assurez-vous que des mises à jour de sécurité s'effectuent automatiquement sur l'ensemble des ordinateurs et serveurs de votre réseau.

Protéger le réseau
Vous devriez utiliser un pare-feu (firewall) personnel sur chaque ordinateur. De plus, protégez le réseau entrepreneurial contre les incursions venant d'internet à l'aide d'un pare-feu.

Répartissez votre réseau entrepreneurial en différents secteurs, par exemple la production, les ressources humaines et la comptabilité. Il n'y a aucune raison que le personnel des ressources humaines ait accès à votre site de production.

Sécurisez l'accès extérieur à votre réseau à l'aide d'une authentification à deux facteurs ou installez une liaison plus sûre via un réseau privé virtuel (VPN).

Installer une protection antivirale
Assurez-vous qu'un logiciel antivirus soit installé sur chaque ordinateur et le protège en temps réel.

Se montrer prudent(e) avec les services de cybernuage
Les données sensibles et les secrets commerciaux ne devraient jamais être archivés non cryptés dans le cybernuage.

Vous trouvez plus de détails dans notre brochure «Empêcher la cybercriminalité: mode d'emploi à l'intention des petites et moyennes entreprises» ou sur www.melani.admin.ch

En collaboration avec la Police cantonale bernoise et MELANI