6.3. PME et cybersécurité dans le cadre du conflit russo-ukrainien : 7 conseils pour faire face aux menaces

Les cyberattaques peuvent avoir des conséquences très lourdes (atteinte à l'image et à la réputation, pertes de revenus...) pour les entreprises, particulièrement pour les PME en ce compris les indépendants et TPE.

Dans le cadre des tensions internationales actuelles, les principales attaques identifiées sont des attaques de type « déni de service distribué (DDoS) » et du (spear)phishing (e-mails destinés à subtiliser des informations sensibles).

Comment faire face aux menaces ?

Suivez ces sept conseils pour assurer votre sécurité informatique.

1. **Établissez une courte liste de vos services numériques les plus critiques**

Avoir une vue d'ensemble de vos services numériques vous permet de déterminer les services à protéger en priorité. Pour vos services numériques les plus critiques, examinez s'il vous est possible d'obtenir une redondance ainsi qu'une sauvegarde de vos données et applications critiques.

Contactez si besoin un service informatique externe pour protéger ce qui vous est essentiel.

2. **Privilégiez la double authentification (ou Multi Factor Authentification - MFA)**

La double authentification (Multi Factor Authentification - MFA) est un procédé qui permet de renforcer la sécurité de ses comptes en agissant comme une protection supplémentaire en cas de vol de votre mot de passe. Ainsi pour accéder à vos comptes, vous pouvez combiner un mot de passe avec un code reçu sur votre GSM.

Certains processus, comme se connecter à une session Microsoft sur votre ordinateur par exemple, requièrent l'emploi de mots de passe. Adoptez une politique de mots de passe forts (longs, avec des caractères différents, signes, chiffres...).

3. **Sauvegardez vos données et vos applications critiques (back-up, copies)**

Pensez à stocker (back-up, copie) vos données les plus critiques et à les protéger de manière « non connectée » à internet si possible.

4. **Augmentez la fréquence de vos scans de sécurité (antivirus)**

Munissez-vous d'un antivirus (antimalware) et faites tourner régulièrement vos scans de sécurité complets.

5. **Définissez une procédure de gestion des incidents**

Concevez un plan de gestion des incidents dans lequel vous définissez le rôle de chaque membre du personnel en cas de cyberattaque.

Pour vous aider à disposer d'un plan de gestion des incidents, téléchargez le template « Gestion des incidents » dans la section « PME » du site Digital Reaction Plan (1)

6. **Apprenez à connaître les principales menaces et à savoir comment réagir si besoin**

Les principales attaques identifiées pour l'instant dans le cadre des tensions internationales sont majoritairement des attaques de type « déni de service distribué » (en anglais Distributed Denial of Service - DDoS) » et du (spear)phishing (e-mails destinés à subtiliser des informations sensibles).

- Pour se préparer à lutter contre une attaque par déni de service distribué (DDoS), consultez notre page « Cybersécurité : comment protéger votre PME des attaques par déni de service distribué (DDoS) ? (2) ». Vous pouvez également suivre les conseils du CERT.be (3).

- Pour se préparer à lutter contre le phishing, à pouvoir le détecter et à augmenter votre niveau de cyberrésilience, consultez la fiche pratique « Phishing » sur le site Digital Reaction Plan (1) et faites suivre les messages suspects à : suspect@safeonweb.be.

7. **Prévoyez la communication de crise**

Si vous maîtrisez la communication, vous maitrisez également les risques pour la réputation de votre entreprise. Consultez la fiche « Communication de crise » sur Digital Reaction Plan (1).

Plus d'infos

- Pour des conseils généraux sur la cybersécurité, consultez le site du Centre pour la Cybersécurité Belgique (CCB) (4).
- Pour des conseils et des avertissements récents sur les problèmes de sécurité en ligne, consultez le site du Cert.be, la Federal Cyber Emergency Team (5).
- Retrouvez les principales menaces sur le site de l'European Union Agency for Cybersecurity (ENISA) (en anglais) (6).
- Suivez les alertes du CERT-EU News Monitor (en anglais) (7).
- Pour plus d'infos sur les menaces, consultez la rubrique « Software and Tools » de la Malware Information Sharing Platform (MISP) (en anglais) (8).

(1) https://www.digitalreactionplan.be/fr/documents-et-telechargements
(2) https://economie.fgov.be/fr/themes/line/securite-de-linformation/cybersecurite-et-pme/cybersecurite-comment-proteger
(3) https://www.cert.be/fr/paper/ddos-protection-et-prevention
(4) https://ccb.belgium.be/fr
(5) https://cert.be/fr
(6) https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
(7) https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html
(8) https://www.misp-project.org/tools/

Dernière mise à jour : 18 mars 2022

SPF Economie – ECONEWS du jeudi 7 avril 2022