CYBLEX TECHNOLOGIES

CYBERSÉCURITÉ : OÙ COMMENCER ?

Webinaire « Transformation digitale : Mettre en place la bonne méthode pour réussir »

07/07/2020

Castres-Mazamet Technopole BUSINESS INNOVATION CENTER

Chambres de Métiers et de l'Artisanat Tarn

CCI TARN

La Mêlée

SOMMAIRE

La cybersécurité en quelques mots …

CYBLEX
TECHNOLOGIES

Les PME et la Cybercriminalité

43%

Des cyberattaques visent les PME

700m €

Le coût additionné des attaques touchant les PME françaises

4/10

PME ont déjà subi une cyberattaque

André Thomas, patron d’une PME ayant déposé le bilan suite à une cyberattaque

Quels risques encourez-vous si vous ne vous préparez pas ?

- Une interruption d'activité
- Une baisse du chiffre d'affaires
  - baisse du carnet de commande,
  - honoraires d'avocats et frais de justice,
  - coûts de réparation matériel,
  - amende RGPD de 4% du CA…
- Une perte de données
- Une perte de propriété intellectuelle (brevets)
- Une perte de confiance auprès de vos clients et prospects

Les bonnes pratiques à suivre

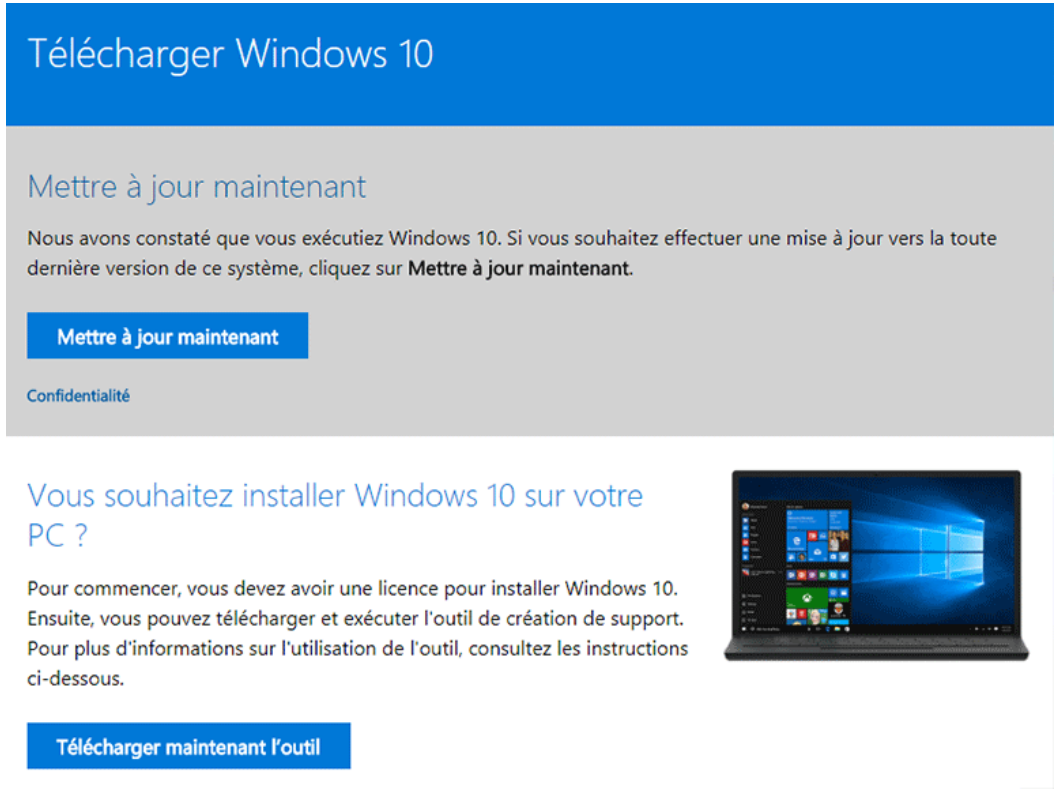
Un site = un mot de passe et comment s'en rappeler

- Etablissez des règles pour vos collaborateurs et sensibilisez-les
- Utilisez un gestionnaire de mots de passe CSPN (pas d'enregistrement dans le navigateur, ni de post-it, Excel, ou autres !)
- Moyens mnémotechniques
  - La méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » : ght5CDs%E7am ;
  - La méthode des premières lettres : « Allons enfants de la patrie, le jour de gloire est arrivé » : aE2lP,lJ2Géa!

Illustration : Martin Vidberg pour la CNIL

Ne remettez pas vos mises à jour à plus tard

- Mettez à jour vos logiciels de façon régulière
- Organisez des mises à jour automatiques
- N’utilisez que les sites internet officiels des éditeurs logiciels pour vos mises à jour

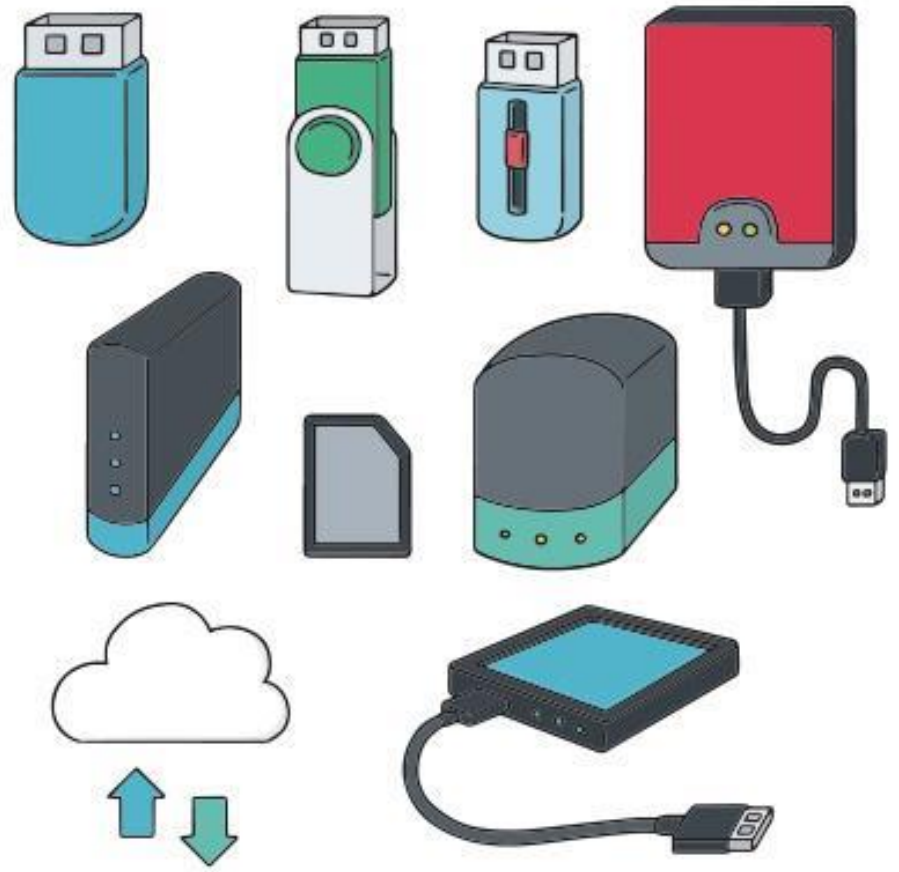


N’est pas administrateur qui veut

- Gérez soigneusement les identités et les accès
- Mettez à jour votre liste de collaborateurs, stagiaires et prestataires
- Distinguez comptes administrateurs et utilisateurs

Effectuez des sauvegardes régulières

- Quotidiennes ou hebdomadaires
- Sur support externe ou Cloud
- Pour le Cloud, assurez-vous que votre contrat avec l'hébergeur couvre les risques d'attaques sur ses systèmes et l'impact sur vos données
- Chiffrez vos données avec un logiciel de chiffrement en les sauvegardant



Sécurisez l’accès Wi-Fi de votre entreprise

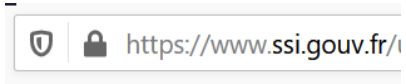
- Modifiez l’identifiant de connexion et le mot de passe par défaut, puis changez-le régulièrement
- Utilisez le protocole de chiffrement WPA2 ou WPA-AES et activez-le.
- Modifiez la clé de connexion par défaut et changez-la régulièrement
- Activez le pare-feu de votre box
- Ayez une box dédiée aux connexions des tiers de passage dans vos bureaux (prestataires, clients, invités…)

Phishing, malwares : méfiez-vous de vos emails

- Sensibilisez vos collaborateurs
  - Vérifier lors du survol du lien hypertexte
  - Quand demande d'identifiants, vérifier la barre d'adresse
  - Ne téléchargez rien d'inhabituel sans scanner d'abord avec un antivirus
  - En cas de doute, contactez directement l'émetteur via les contacts trouvés sur Internet et non ceux fournis dans le mail
- Renforcez les protocoles Métier (contrôles d'identité, confirmations multiples avant paiement, etc.)
- Installer un antispam phishing

Ouvrez l’œil avant de payer sur Internet

- Vérifiez que le site a bien un cadenas et une adresse en https://



- Vérifiez l’orthographe du site
- Demandez un moyen de paiement en ligne sécurisé à votre banque

Séparer les usages personnels des usages professionnels

AU BUREAU

- Evitez :
  - le BYOD.
  - L'envoi d'emails pro, vers la boîte email perso
  - La connection d'une clé USB perso sur un moniteur pro
- Réduisez l'accès des données critiques à certains collaborateurs seulement
- Chiffrez vos données, en cas d'exfiltration illégale, elles ne pourront pas être lues
- Mettez en place l'audit par l'activation de journaux et leur surveillance
- Si vous en avez les moyens, installez des outils de détection de fuites de données

EN CAS DE TÉLÉTRAVAIL

- Incitez vos collaborateurs à :
  - Utiliser un VPN si ils travaillent de chez eux ou à distance
  - Sécuriser leur wifi personnel
  - Arrêter ou mettre en veille leurs ordinateurs quand ils ne sont pas devant
  - Ne pas laisser les enfants jouer avec

Que faire en cas d’incident ?

Quels recours si vous êtes attaqué ?

Isolez le système

Déconnectez immédiatement le poste d'internet et du réseau

Ne payez pas !

Ne payez pas la rançon exigée. Ca reviendrait à financer des cybercriminels, sans garantie de retrouver vos données.

Faites une restauration

Effectuez ou faites effectuer une restauration du poste victime.

Alertez les autorités

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Portez plainte au commissariat de votre domicile et sur Cybermalveillance.gouv.fr

Pour aller plus loin

Évaluez votre sécurité

I - Sensibiliser et former		STANDARD	RENFORCÉ
1	Former les équipes opérationnelles à la sécurité des systèmes d'information		
2	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique		
3	Maîtriser les risques de l'infogérance		

II - Connaitre le système d'information		STANDARD	RENFORCÉ
4	Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau		
5	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour		
6	Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs		
7	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés		

Faites le point sur ce que vous avez déjà et ce qu'il vous manque avec l'outil de suivi de l'ANSSI et leurs 42 mesures d'hygiène informatique

Références

- Témoignage André Thomas, patron d'une PME qui a déposé le bilan après une cyberattaque
- Guide des bonnes pratiques de l'informatique – ANSSI
- Guide d'hygiène informatique – ANSSI
- Cyberattaques : le patron d'une TPE témoigne
- S'évaluer sur le site de Cyber'occ
- A Small Business No Budget Implementation of the SANS 20 Security Controls – SANS Institute [anglais]

Vous avez des questions ?
Contactez nous !

Christophe VENDRAN

cvendran@cyblextechnologies.fr
Tel : 06 44 51 29 04

Castres·Mazamet Technopole
BUSINESS INNOVATION CENTER

CCI TARN

Chambres de Métiers et de l'Artisanat
Tarn

La Mêlée

MERCI

Rejoignez-nous sur