Protéger nos Communes Numériques : Enjeux et Solutions en Cybersécurité

La cybersécurité est un enjeu majeur pour notre société et l'une des priorités pour le Luxembourg.

A connaître

Cybersecurity.lu – le portail national pour tous
Accédez à toute l'expertise nationale et prenez connaissance des acteurs présents dans votre commune

Notions importantes

Cyber hygiène : appliquez les règles de base pour garantir votre sécurité en ligne
Réseaux sociaux : utilisez-les prudemment !

Boîte à outils

- **Pandora :** un doute sur un fichier ? Ne l'ouvrez pas, testez-le et accédez même à son contenu !
- **Luxchat :** utilisez Luxchat pour vos conversations privées, en toute intimité !
- **SPAMBEE :** un spam ? Signalez-le !

Bourgmestre

- Diffusez et rappelez régulièrement les bons conseils et bonnes pratiques d'hygiène en ligne
- Nommez des responsables sécurité en interne

Checklist des 7 indispensables pour les utilisateurs :

Phishing – Posez-vous les bonnes questions :
- o Le **contexte** de l'email correspond-il à une **situation familière** ?
- o Au premier doute, demandez l'avis d'un expert interne ou externe et si le doute se confirme, rapportez-le via **SPAMBEE[1]**

Mots de passe – Comment renforcer leur robustesse ?
- o **12+ caractères** différents ****
- o Activez l'**authentification à double facteur**
- o Utilisez un mot de passe différent par service
- o Consignez-les dans un gestionnaire de mot de passe (ex : Passbolt, Padloc, Dashlane, ...)

Envoi d'informations sensibles – utilisez les bons moyens !
- o Evitez de transmettre des informations sensibles par email mais **favorisez des systèmes d'échange dédiés tels que Luxchat[2]**

Destruction des données – détruire simplement ne suffit pas !
- o **Faites vider ou détruire** les données de tout support physique[3] non utilisé par un **professionnel**
  - Support papier = shredder
  - Support numérique = acteurs tels que LabGroup, Streff, Blancco

Télétravail/mobilité et travail hors du bureau – redoublez de vigilance !
- o Ne vous connectez pas à un **réseau WiFi non sécurisé** (ex. réseaux WiFi publics)
- o Activez votre **VPN professionnel** (fourni par votre organisation)
- o Vérifiez qui peut **voir votre écran**

Mises à jour – ne les oubliez pas !
- o **Mettez à jour vos machines** (laptops, GSM, tablettes) et **applications** (applications bureau et en provenance de stores) dès que possible

Intelligence artificielle – soyez critique !
- o Ne divulguez **pas d'information confidentielle dans une requête IA** (ex. ChatGPT, Gemini, etc)
- o **Méfiez-vous** des messages, images, vidéos ou des documents que vous recevez, même s'ils paraissent réels, surtout sur les **réseaux sociaux**

[1] https://spambee.lu/
[2] https://www.luxchat.lu/
[3] Y compris téléphones, montres connectées, écouteurs/casques connectés, routeurs, kit mains libres, IoT, etc

Checklist des 7 indispensables pour les CISO (Responsables Sécurité) :

Pour être résilient, il faut connaître ses risques

- **Fit4Cybersecurity**
  - évaluez la maturité de votre sécurité de l'information
- **Cybersecurity Observatory**
  - anticipez les menaces cyber, adaptez vos stratégies
- **MONARC**
  - évaluez vos risques
- **Statistiques d'incidents**
  - signalez votre incident sur le site web de CIRCL pour informer tout le monde des risques

Wifi – une connexion sécurisée

- **Sécurisez** votre Wifi
- **Vérifiez** l'éventuelle présence de réseaux **Wifi malicieux**

Politique de backup – l'arme fatale contre les ransomware

- Backups **déconnectés, délocalisés, chiffrés, journaliers et retenus**
- **Testez** vos backups et assurez-vous que toutes les données y sont bien incluses
- **Dimensionnez** vos backups selon vos besoins, et demandez les moyens pour le faire

Shadow IT – savez-vous qui agit dans l'ombre ?

- Assurez-vous de connaître tous les **équipements connectés à votre réseau** et qu'ils respectent vos règles

Monitoring/Détection – mieux vaut prévenir que guérir

- Détecter un incident = mieux que de devoir le gérer
- Parle à un expert pour mettre en place un système de détection d'intrusion

Charte utilisateur – bien communiquer en interne pour plus d'efficacité

- Rédigez vos règles de façon simple, compréhensible pour que chacun puisse les comprendre
- Faites signer ce document aux utilisateurs pour vous assurer qu'ils les aient bien lu et les appliquent dès que possible
- Trustbox

ROOM #42 DO[N'T]PANIC **– préparez-vous au pire**

- Mettez votre **Business Continuity Plan** à l'épreuve d'une cyberattaque

Liste des contacts clés :

Autorités

RGPD :
CNPD
(+352) 26 10 60 -1
info@cnpd.lu

Directive NIS :
ILR INSTITUT LUXEMBOURGEOIS DE RÉGULATION
(+352) 28 228 380
niss@ilr.lu

En charge des applications informatiques des communes

sigi
(+352) 35 00 99-1
contact@sigi.lu

SYVICOL Syndicat des Villes et Communes Luxembourgeoises
(+352) 44 36 58 - 1
info@syvicol.lu

Pour accroître votre résilience cyber

LHC/NC3

LHC Luxembourg House of Cybersecurity
nc3.lu National Cybersecurity Competence Center LUXEMBOURG
+352) 274 00 98 601
info@lhc.lu / info@nc3.lu

Gestion d'incidents

CIRCL – CERT (Computer Emergency Response Team) pour le secteur privé, les communes et les entités non gouvernementales au Luxembourg

circl.lu Computer Incident Response Center LUXEMBOURG
(+352) 2478 8444
info@circl.lu

POLICE LËTZEBUERG
– pour déposer plainte

Citoyens

BEE SECURE
Helpline: 8002 1234

Digital Inklusioun fir all Alter
GoldenMe
(+352) 661 529 913

Groupe de travail
National Plattform fir d'Reduktioun vu Katastropherisiken

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires intérieures