GUIDE PRATIQUE

CYBERSÉCURITÉ

Comprendre, se préparer et savoir réagir en cas d'attaque

CHAMBER OF COMMERCE LUXEMBOURG

POWERING BUSINESS

FRANÇAIS

Sommaire

Une publication de la
Chambre de Commerce réalisée
en partenariat avec **MindForest** et
la **Luxembourg House of Cybersecurity**
Février 2023 (actualisation d'une brochure
éditée initialement en novembre 2021)

Introduction

Par son tissu économique, composé notamment d'acteurs du secteur banque/assurance et hébergeant également des institutions européennes traitant des données sensibles, le Luxembourg a considéré dès le début des années 2000 la cybersécurité comme la colonne vertébrale de son économie numérique.

Si bien que l'ensemble des entreprises et/ou institutions actives dans le secteur de la cybersécurité représente un écosystème* comptant plus de 370 acteurs, dont 30% ont la cybersécurité comme cœur de métier et 25% sont des startups.
Ensemble, ils forment un véritable maillage et travaillent en étroite collaboration afin de sensibiliser, protéger et réagir auprès des entreprises du pays en cas d'attaques.

Parmi ces acteurs, on retrouve la Luxembourg House of Cybersecurity, épine dorsale de la cyber-résilience au Luxembourg. Elle fait office de figure de proue à l'aide de ses deux centres, le *National Cybersecurity Competence Center* (NC3) et le *Computer Incident Response Center Luxembourg* (CIRCL), en proposant des conseils, des services, des formations dont peuvent bénéficier les entreprises du Grand-Duché.

Car hélas, la cybercriminalité est devenue un véritable business dans le monde entier. Le Luxembourg ne fait pas exception, comme en attestent les témoignages d'entreprises locales victimes d'attaques.

L'important dans ce cas est d'être préparé et d'avoir connaissance des risques et des impacts que pourraient avoir une cyberattaque sur son entreprise. Cela dans le but de protéger au mieux les données qui, perdues ou volées, peuvent mettre en péril la survie de celle-ci. Pour cela, des outils existent comme des exercices de simulation ou des tests de pénétration qui permettent d'anticiper les différents scénarios possibles et ainsi d'éviter au qu'ils ne se produisent.

Ce guide fournit quelques clés pour comprendre, se préparer et savoir comment agir en cas de cyberattaques.

* https://cybersecurity.lu

Faits et chiffres[1]

LE PHISHING[2]
(voir Les types de cyberattaques, p.12-13)
représente 2/3 des 1.114 incidents
identifiés au Luxembourg en 2020 par le CSIRT[3].
Viennent ensuite les attaques par déni de service (DDoS - visant à rendre indisponible un ou plusieurs services), l'usurpation d'identité, l'appel de numéros surtaxés.

LES CLIENTS DES BANQUES LUXEMBOURGEOISES
sont particulièrement visés par les campagnes de phishing, à défaut de pouvoir attaquer les établissements bancaires directement.
(voir Interview de Pascal Steichen ci-dessous).

LES VICTIMES DES CYBERATTAQUES AU LUXEMBOURG :
(selon les incidents reportés au CIRCL en 2020)


les particuliers : 54%


le secteur financier : 24%


les institutions : 12,5%


l'industrie : 9%

(1) Chiffres issus des seuls incidents reportés. Ils ne permettent donc pas de mesurer pleinement l'ampleur du phénomène.
(2) Phishing : attaque visant à récupérer des identifiants de connexion en vue de perpétrer une fraude.
(3) CSIRT : Computer Security Incident Response Team de POST Cyberforce, mis en place en 2020 afin de mieux combattre les cyberattaques détectées au Luxembourg.
(4) https://fit4cybersecurity.nc3.lu/
(5) CIRCL : Computer Incident Response Center Luxembourg, qui est une instance gouvernementale en charge de recueillir et d'analyser les tickets d'incident envoyés par les entreprises ou personnes victimes. https://www.circl.lu/opendata/statistics/#circl-operational-statistics

LES ENTREPRISES PEUVENT AUTO-ÉVALUER LEUR MATURITÉ vis-à-vis des moyens de protection mis en oeuvre pour limiter les risques, grâce à l'outil *Fit4Cybersecurity*[4] du National Cybersecurity Competence Center - NC3. Les réponses données au questionnaire, analysées par le NC3, permettent de constater que pour les TPE et PME :


80% **ont des mots de passe faibles,** facilement devinables ou laissés au choix des utilisateurs, sans protection

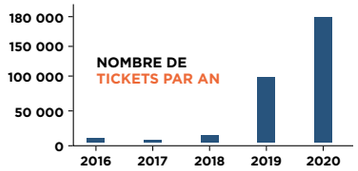

71% **ont des mesures insuffisantes** pour la protection des données personnelles et le respect du RGPD


70% **des TPE et 64% des PME ont des sauvegardes insuffisantes,** les laissant vulnérables à des cryptoransomwares


63% **des TPE et 56 % des PME n'utilisent pas de façon régulière les antivirus qu'ils possèdent, ne vérifient pas leurs mises à jour voire ne possèdent pas d'antivirus**


60% **des TPE et 54 % des PME ont des postes utilisateurs vulnérables** (absence de procédure d'autorisation de téléchargement de logiciels, machines non verrouillées, non mises à jour…)


55% **des TPE et 46 % des PME ne forment pas leurs collaborateurs aux logiciels utilisés, à la cybersécurité, ou à la sensibilité des données**



LE NOMBRE D'ATTAQUES EST EXPONENTIEL :
180.000 tickets d'incidents ont été ouverts auprès du CIRCL[5] en 2020, contre 100.000 en 2019 et 15.000 en 2018.
La part du phishing est croissante : de 16% des tickets en 2017, elle est passée à 71% des tickets en 2020 et 83% en 2021.

Regard de Pascal Steichen, directeur de la *Luxembourg House of Cybersecurity*

Quelles sont les tendances actuelles en terme de cyberattaques?
Le phishing s'est fortement développé, partout dans le monde, ces dernières années : c'est la contrepartie des progrès qui ont été faits pour renforcer les systèmes informatiques. Pour les petits criminels, le ticket d'entrée pour infiltrer les systèmes devient trop élevé, alors que l'humain, lui, n'a pas été « upgradé » et peut se faire usurper son identité.

De plus, l'email, qui est la porte d'entrée pour piéger les victimes, s'est généralisé. Nous sommes tous devenus dépendants de l'informatique, ce qui offre un terrain de jeu à l'échelle de la planète. Encore plus d'ailleurs avec le télétravail, ce qui n'a pas échappé aux *hackers*, qui ont axé leurs attaques sur les outils de visioconférence, les VPN, … et ont élargi leur spectre d'intervention à d'autres secteurs que la finance comme par exemple les hôpitaux, l'industrie. Heureusement, au Luxembourg, nous n'avons pas eu d'attaques majeures à déplorer sur nos hôpitaux ou nos sites gouvernementaux, comme ailleurs à l'étranger.

Est-ce que les petites entreprises intéressent les *hackers* ?
Les *hackers* font feu de tout bois… ils tentent systématiquement d'entrer partout où ils le peuvent, dans les grandes comme dans les petites entreprises, et pénètrent par la première porte qui s'ouvre. Toute entreprise peut donc être potentiellement victime.

L'avantage des PME est que la communication y est plus directe, et qu'un mail douteux peut être plus rapidement identifié.

Comment qualifieriez-vous la maturité des entreprises luxembourgeoises en matière de cybersécurité ?
Elles sont plutôt bien positionnées. Nous avons assisté à une véritable prise de conscience des risques liés à la cybercriminalité ces dernières années. Les entreprises sont de plus en plus nombreuses à nous solliciter pour nous demander conseil.

La question, hélas, n'est pas de savoir si on sera attaqué, mais quand. Il est même probable qu'on l'ait déjà été tout en l'ignorant, et la tâche est alors de diagnostiquer les traces éventuelles d'intrusion dans son système ou sur ses réseaux. Souvent, une intrusion peut avoir eu lieu des mois voire des années auparavant, et ne faire des dégâts visibles que bien plus tard.

Quelles sont vos recommandations ?
Il reste encore beaucoup à faire dans les entreprises pour sécuriser leurs infrastructures. Et les objets connectés, qui sont souvent mal protégés, offrent une surface d'attaque importante. Il faut plus que jamais rester vigilant et ne pas relâcher la sensibilisation de ses collaborateurs et de ses clients.

Les enjeux

Pour les organisations, les enjeux de la cybersécurité sont nombreux. Une cyberattaque a des conséquences à différents niveaux, de manière immédiate mais aussi sur la durée, et peut engendrer de nombreux coûts cachés.

Alors que les entreprises sont victimes de la cybercriminalité, elles restent responsables de leurs propres données et de leur protection. Entre la détection de la cyberattaque et le retour à une normalité complète, il peut s'écouler jusqu'à plusieurs années durant lesquelles l'organisation mettra en place un plan d'action pour réparer les dommages.

Image de l'entreprise

Les attaques de pirates informatiques peuvent avoir des conséquences importantes sur l'image, à long terme, de l'entreprise. Elles peuvent donner l'impression aux investisseurs que l'entreprise ne prend pas la cybersécurité suffisamment au sérieux, de même qu'elles peuvent impacter la confiance des clients, ce qui, à long terme également, peut mettre en péril les activités de l'entreprise.

Atteinte à la confidentialité

La confidentialité consiste simplement à s'assurer qu'aucune personne non autorisée n'accède aux données du système informatique ou aux dossiers papier. Elle a donc un lien direct avec le RGDP. Il s'agit ici des données personnelles mais aussi confidentielles.

Atteinte à la disponibilité

La poursuite continue des activités commerciales exige la disponibilité des données à tout moment. Cette disponibilité peut être altérée, par exemple, par un déni de service. Plus les opérations commerciales normales sont soutenues par l'informatique, plus les dommages financiers peuvent être importants si les données ne sont pas disponibles.

Enjeux légaux

Les conséquences juridiques sont extrêmement spécifiques à chaque secteur. Cependant, le RGDP établit un régime de protection des données personnelles à l'échelle européenne. Une violation de ce règlement peut coûter à l'entreprise contrevenante jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel du groupe.

Atteinte à l'intégrité

Le principe d'intégrité exige que l'on puisse garantir à tout moment que les données n'ont été ni modifiées ni supprimées. Un suivi continu des éventuels changements apportés à des données doit être mis en place. L'intégrité peut être impactée par des erreurs individuelles des employés et nécessite donc une formation à la manipulation des données.

Enjeux financiers

La perte de données sensibles, comme des secrets de fabrication ou des données clients, peut entraîner des dommages financiers :

- **directs :** frais de justice et d'avocat, relations publiques, amendes élevées, mise en conformité, notification de l'attaque aux clients, etc.
- **indirects :** baisse des ventes avec comme conséquence une baisse nette du chiffre d'affaires, perte de la confiance client, augmentation des primes d'assurance, dépréciation de la marque pouvant aller jusqu'à la révocation de la licence d'exploitation, etc.

Dans des domaines très réglementés, comme en particulier le secteur financier, des critères de qualité stricts sont fixés en matière de cybersécurité. S'ils ne sont pas respectés, des sanctions sévères sont appliquées (par la CSSF, l'ILR ou la CNPD pour le non respect de la protection des données).

Outre les conséquences possibles pour l'entreprise si la sécurité de l'information n'est pas prise en compte, les employés peuvent également être pris pour cible par les cybercriminels, par exemple en faisant du chantage avec des photos privées, qui peuvent aussi avoir des conséquences sur l'entreprise.

Témoignages
(Recueillis en novembre 2021)

Les sociétés **Felix Giorgetti** (construction) et **Victor Buck Services (VBS)** (service de traitement et d'édition d'informations) ont toutes les deux été victimes d'une attaque en 2020. Leurs responsables reviennent sur les circonstances et les conséquences de cet accident de sécurité.

FELIX GIORGETTI

Paul Feider
Directeur Administratif, Commercial et Financier

Jean-Marc Sertic
Responsable IT et Organisation.

VICTOR BUCK SERVICES

Edith Magyaricks
CEO

LES PREMIERS SIGNES DE L'ATTAQUE

Felix Giorgetti : Le 17 janvier 2020, nous n'avions plus accès à nos documents ni à nos applications. Nous avons vite compris que nous étions victimes d'un *ransomware*. **Les analyses ont révélé qu'il s'était infiltré dans nos systèmes dès l'automne 2019.** Les *hackers* nous ont demandé de transférer 500.000 dollars en bitcoins sur un compte, avec un ultimatum de 4 jours, sinon ils augmenteraient la rançon à 1 million de dollars.

VBS : Nos systèmes ont fait l'objet d'un sabotage en août 2020. Pendant une semaine, nous n'y avions plus accès et ne pouvions plus servir nos clients. Par effet domino, cette attaque a eu des conséquences pour eux.

LES CONSÉQUENCES SUR LES CLIENTS ET L'ENTREPRISE

Felix Giorgetti : Nous ne pouvions plus mener à bien nos activités les plus élémentaires, soutenues par l'informatique : communiquer, accéder aux plans pour travailler sur les chantiers et aux données pour émettre des factures. **Il a fallu plusieurs mois pour que notre système soit à nouveau complètement opérationnel.** Avec l'aide de notre service informatique et de consultants externes, nous l'avons progressivement remis en état : séparer notre réseau interne du réseau externe, transférer les données de manière sélective et sous contrôle strict, tout en opérant des changements pour accroître la sécurité.

VBS : Heureusement, à ce jour, les investigations n'ont montré aucune fuite de données clients, mais ceux-ci ont dû mettre en place dans l'urgence des solutions de repli. **La plupart nous ont témoigné leur soutien et nous sont restés fidèles une fois la situation rétablie, mais certains ont mis plus de temps à prendre une décision pour leur reconnexion.** Il y a eu un impact certain sur les revenus de 2020, dû à cet arrêt d'activité avec certains clients. Cet impact perdure en 2021 puisque certains clients ne sont revenus qu'au cours de cette année-ci.

LES PREMIÈRES RÉACTIONS

Felix Giorgetti : Nous avons immédiatement contacté le CIRCL et la police, puis notre fournisseur d'accès internet.
Nous avons « débranché » toutes les connexions internet pour que l'attaque ne se propage pas dans nos systèmes. Le *ransomware* avait aussi attaqué certaines sauvegardes dans notre *cloud*, mais heureusement pas le *backup* du système. Nous avons donc pu récupérer nos données.

VBS : Dès le début, nous avons joué la carte de la transparence avec nos collaborateurs autant que nos clients. **Il n'y a aucune honte à être victime d'une attaque.** Cela peut arriver à tout le monde. Nous avons justement voulu parler de notre expérience malheureuse afin qu'elle puisse servir à d'autres. Car il est souvent question des intrusions venant de l'extérieur, mais il est trop peu connu que les collaborateurs, par négligence ou manque de sensibilisation, peuvent être les vecteurs des menaces.

LES MESURES MISES EN ŒUVRE À PLUS LONG TERME

Felix Giorgetti : Nous avons beaucoup investi dans la sécurité de nos systèmes, formé le personnel, introduit des règles plus strictes en matière de mots de passe et mis en place un concept de *backup* plus ciblé. En outre, nous avons limité l'accessibilité de notre système informatique à certaines heures, ce qui nous permet de mieux monitorer les activités sur les serveurs et d'agir plus rapidement si l'un des indicateurs fait soupçonner une attaque.

VBS : Parmi les mesures mises en œuvre, nous avons sensibilisé nos collaborateurs, quel que soit leur poste dans l'entreprise, aux comportements à risques qui peuvent engendrer des failles. Chacun doit comprendre qu'il a sa part de responsabilité.

LES CONSEILS AUX ENTREPRISES

Felix Giorgetti : La leçon à tirer est que cela peut arriver à n'importe qui, quelle que soit la taille de l'entreprise. Il faut trouver le bon équilibre entre sécurité et opérationnalité ; le pragmatisme est le maître mot. De plus, un concept de *backup* sophistiqué est indispensable pour disposer d'un plan B en cas d'urgence et ainsi minimiser la perte d'activité et les dommages financiers. Il est important que les gens parlent de ce sujet et que d'autres entreprises témoignent. **Dans la lutte contre la cybercriminalité, nous pouvons apprendre beaucoup les uns des autres.**

VBS : Notre entreprise, du fait de son activité, disposait déjà d'un *framework* solide en matière de cybersécurité, ce qui n'est pas à la portée de toutes les PME. **Sans trop investir, il est possible de prioriser afin de sécuriser les activités cruciales, et de pouvoir ainsi continuer son activité et limiter l'impact.** C'est un vrai sujet pour les chefs d'entreprise, qui doivent avoir un minimum de connaissances sur la cybersécurité et les risques encourus, et ainsi éviter tous les incidents qui peuvent l'être.

L'humain, maillon faible de la sécurité

« L'humain peut être une faille, mais il peut aussi être le premier rempart aux intrusions, à condition d'avoir été sensibilisé et formé. Pour les petites entreprises, la sensibilisation des collaborateurs pour éveiller leur vigilance face aux mails douteux est le moyen le plus efficace, et le moins coûteux pour faire face aux menaces.»

Pascal Steichen,
Directeur,
Luxembourg House of Cybersecurity

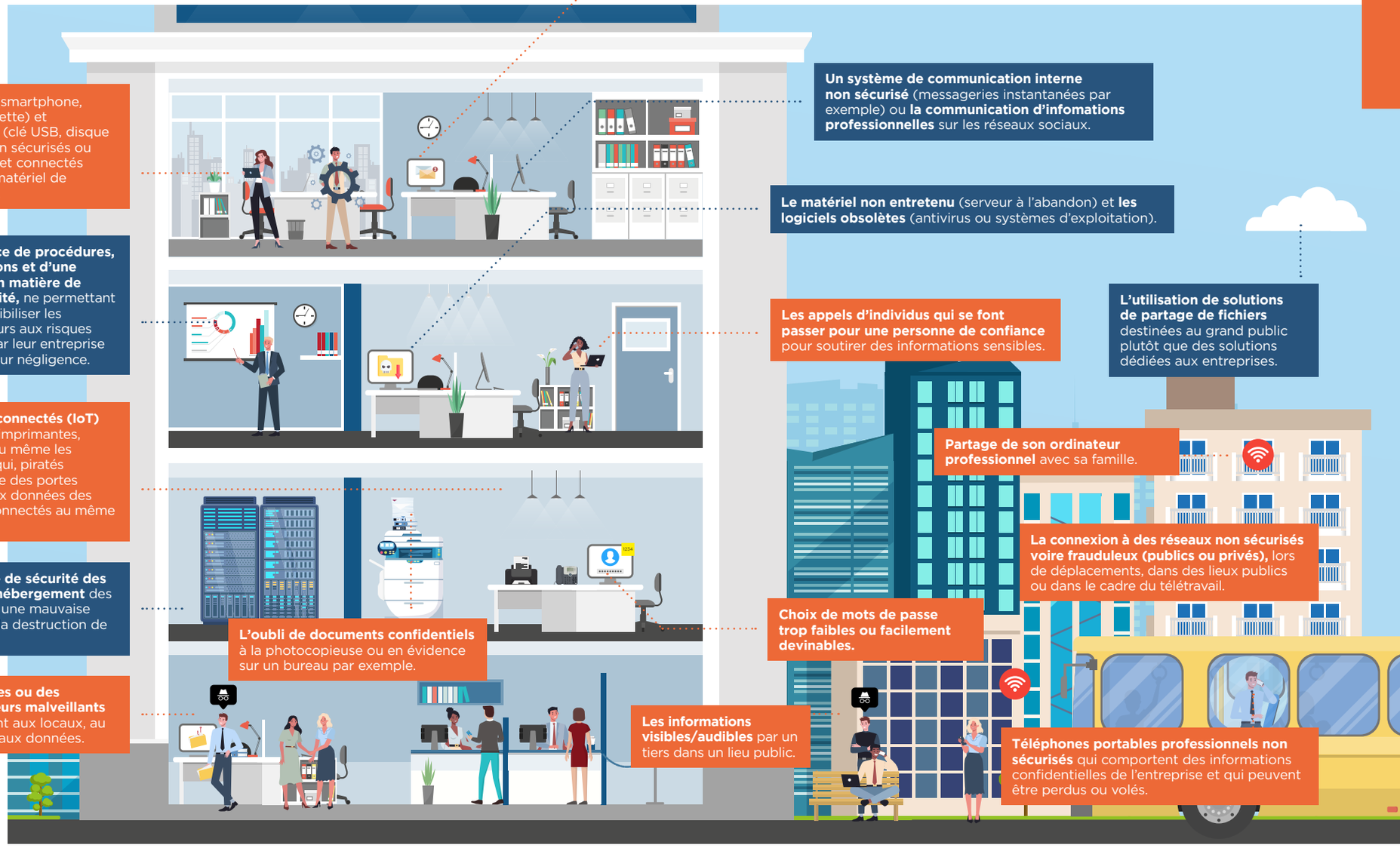
Hélas, trop souvent, les petites entreprises se croient épargnées car pas suffisamment alléchantes pour des *hackers*. C'est une erreur ! Les *hackers* peuvent passer par elles, moins bien protégées et souvent fournisseurs de grands groupes, pour atteindre indirectement ceux-ci. Sensibiliser les employés permet d'augmenter la résilience de son organisation, même si ce n'est pas la réponse à tout.

LÉGENDE

- Erreur humaine
- Manquement de l'entreprise

**BYOD = Bring Your Own Device, pratique qui consiste à utiliser ses équipements personnels dans un contexte professionnel.*

*** Téléphones connectés à internet*



L'ouverture de mails professionnels ou privés malveillants ou frauduleux ou **les téléchargements de données hasardeuses, de fichiers corrompus ou de logiciels malveillants** sur le réseau de l'entreprise ou bien sur l'équipement professionnel depuis un réseau externe.

Le BYOD* (smartphone, laptop, tablette) et accessoires (clé USB, disque dur, etc) non sécurisés ou corrompus et connectés au réseau/matériel de l'entreprise.

Un système de communication interne non sécurisé (messageries instantanées par exemple) ou **la communication d'infomations professionnelles** sur les réseaux sociaux.

Le matériel non entretenu (serveur à l'abandon) et **les logiciels obsolètes** (antivirus ou systèmes d'exploitation).

Une absence de procédures, de formations et d'une politique en matière de cybersécurité, ne permettant pas de sensibiliser les collaborateurs aux risques encourus par leur entreprise du fait de leur négligence.

Les appels d'individus qui se font passer pour une personne de confiance pour soutirer des informations sensibles.

L'utilisation de solutions de partage de fichiers destinées au grand public plutôt que des solutions dédiées aux entreprises.

Les objets connectés (IoT) comme les imprimantes, les VoIP** ou même les ampoules, qui, piratés peuvent être des portes ouvertes aux données des appareils connectés au même réseau.

Partage de son ordinateur professionnel avec sa famille.

La connexion à des réseaux non sécurisés voire frauduleux (publics ou privés), lors de déplacements, dans des lieux publics ou dans le cadre du télétravail.

Un manque de sécurité des espaces d'hébergement des données et une mauvaise gestion de la destruction de celles-ci.

L'oubli de documents confidentiels à la photocopieuse ou en évidence sur un bureau par exemple.

Choix de mots de passe trop faibles ou facilement devinables.

Des externes ou des collaborateurs malveillants qui accèdent aux locaux, au matériel et aux données.

Les informations visibles/audibles par un tiers dans un lieu public.

Téléphones portables professionnels non sécurisés qui comportent des informations confidentielles de l'entreprise et qui peuvent être perdus ou volés.

Les types de cyberattaques

Le Social Engineering
(Ingénierie Sociale)
Des techniques de manipulation psychologique sont utilisées au téléphone, en contact direct, par email ou sur les réseaux sociaux pour qu'une personne divulgue des informations sans s'en rendre compte.

Le ransomware
Un ransomware locker est un logiciel malveillant qui prend en otage la machine et la rend inaccessible. Souvent, cela ne touche pas les données, mais incite l'utilisateur à payer pour récupérer l'utilisation de sa machine.

Le cryptoransomware
(type de *ransomware* le plus connu) chiffre silencieusement les données, les rendant petit à petit inaccessibles, cible toutes autres machines connectées au réseau, recherche les *backups* et demande à payer une rançon pour recouvrir les données perdues.

Le malware (logiciel malicieux)
C'est un programme développé pour nuire à un système informatique.

Il en existe plusieurs types :

Le virus : accomplit une tâche malicieuse sur la machine de la victime (voler des données, les rendre inaccessibles, les modifier) et se transmet à toute machine compatible qui se connecte à la machine infectée. Il est souvent transmis via pièce jointe, ou média de stockage.

Le Cheval de Troie : souvent sous forme d'un logiciel, il ouvre un canal pour qu'un attaquant puisse faire ce qu'il veut sur la machine.

Le spyware : envoie des données sur ce que fait l'utilisateur d'une machine (sans le prévenir) pour une utilisation commerciale ou d'espionnage.

Différents signes qui peuvent permettre de détecter une tentative de cyberattaque :
- Adresse email étrange ou incorrecte
- Fautes d'orthographe ou de syntaxe
- Lien ne correspondant pas à une adresse connue ou au contexte
- Fichier joint au format particulier (Word avec des macro, zip,...)
- Demande d'informations trop sensibles comme identifiant, mot de passe

Les bons réflexes après la détection d'une cyberattaque :
- Contactez le support informatique de votre entreprise en cas de doute (en interne ou votre prestataire externe)
- Reportez l'incident au CIRCL
- Contactez votre banque (si risque d'accès aux comptes bancaires)
- Changez les mots de passe
- Déconnectez les appareils du réseau, avec ou sans fil
- Faites appel à des experts *(voir Les acteurs, p.16-17)* pour vous aider à rétablir la situation et à vous protéger à l'avenir

Ne pas oublier
- Communiquez vers vos collaborateurs et vos clients, jouez la transparence
- Sensibilisez et formez vos collaborateurs pour augmenter la résilience de votre entreprise
- Faites des sauvegardes régulières et hors ligne de vos données

Le phishing
Le cybercriminel se fait passer pour un tiers de confiance ou joue sur les faiblesses humaines (gentillesse, pitié, appât du gain, curiosité, libido, peur, paresse, etc.), incitant à l'ouverture d'une pièce jointe, d'un site web, à la communication d'un mot de passe, avec pour conséquence l'installation d'un malware ou la perte de données.

L'arnaque au président
Le collaborateur pense être en contact avec une personne du top management de sa société ou de la société mère. L'attaquant recherche des informations sur les réseaux sociaux pour trouver une victime potentielle (profil supportant mal la pression). Après plusieurs échanges pour établir la confiance, il demande un virement et/ou le transfert de documents de manière urgente et confidentielle.

Un mot de passe mal protégé
Certaines attaques consistent à deviner un mot de passe en essayant toutes les combinaisons possibles de caractères pouvant former le mot de passe, en s'aidant de dictionnaires de mots prédéfinis et qui peuvent être adaptés pour cibler une victime (combinaison de prénom+date de naissance par exemple)

Le déni de service
Le fraudeur tente de perturber le fonctionnement normal du serveur, service ou network ciblé, en le submergeant par un flot de traffic internet.

Étapes pour protéger votre entreprise

ÉTAPE 1
Faire régulièrement un état des lieux

Procéder à des auto-diagnostics de la maturité de votre entreprise, de votre exposition aux risques, de la sécurité de vos données.
(voir Les outils et solutions, p.20-21)

Faire auditer votre système informatique pour voir s'il y a déjà des traces d'intrusion.

Inventorier :

- les accès existant à vos informations sensibles (collaborateurs, prestataires externes...), y compris les données physiques (dossiers)
- les appareils connectés au réseau (attention aux appareils apportés par des collaborateurs) et assurez-vous de leur fiabilité
- les informations les plus sensibles et vitales pour votre entreprise, et sécurisez-les
- les actifs attrayants, qui pourraient susciter la convoitise (portefeuille clients, documents financiers, données personnelles,..) et veillez à la conformité avec le RGPD
- les mesures de protection existantes (antivirus, pare-feu)

ÉTAPE 2
Prévenir les risques

Mettre en place une stratégie de cybersécurité (*security policy*) et dresser un plan d'urgence avec des processus et des procédures clairs, mis à jour régulièrement. Les expliquer aux collaborateurs et s'assurer qu'ils soient lus et bien compris, par exemple en faisant signer un document.

Créer une structure interne de support et une gestion des incidents (en fonction de la taille de l'organisation).

Connaître les acteurs/institutions clés en matière de cybersécurité. *(voir Les acteurs, p.16-17)*

Assurer une mise à jour régulière des logiciels et des systèmes d'exploitation.

S'assurer de la mise en place d'un *backup* régulier et déconnecté du réseau (pour ne pas être infecté en cas d'intrusion).

Prendre en compte les différentes configurations de travail (présentiel/virtuel, en déplacement).

Changer et faire changer régulièrement les mots de passe.

ÉTAPE 3
Sensibiliser et former les collaborateurs

Sensibiliser aux principales menaces existantes au travers de formations internes ou développées par des experts. *(voir Les outils et solutions, p.20-21)*

Expliquer le plan d'urgence et les processus existants, les tester dans la mesure du possible.

Réaliser des mises en situations/simulations.
(voir Les acteurs, p.16-17)

Faire des rappels et mises à jour réguliers.

Mettre en place un guide de bonnes pratiques pour les collaborateurs comprenant toutes les informations clés.

Les acteurs de la cybersécurité au Luxembourg

PREMIER MINISTRE

STRATÉGIE NATIONALE

Comité interministériel de coordination en matière de cyberprévention et cybersécurité

SECTEUR PUBLIC

Haut-Commissariat à la protection nationale

Responsable de la protection des infrastructures critiques et coordination de la lutte anti-terroriste

GOVCERT.lu

Point de contact unique dédié au traitement des incidents informatiques affectant les systèmes d'information du gouvernement et d'opérateurs d'infrastructures critiques (privé et publique) définis opérant au Luxembourg

CYBERSECURITY LUXEMBOURG
cybersecurity.lu

L'écosystème de confiance offrant une expertise étendue en matière de cybersécurité

+ DE 330 ACTEURS

- **319** sociétés privées
- **37** entités publiques
- **9** associations

25% DE STARTUPS

30% DONT LA CYBERSÉCURITÉ EST LE COEUR DE MÉTIER

SECTEUR PRIVÉ

LHC Luxembourg House of Cybersecurity

Epine dorsale de la cyber-résilience au Luxembourg.

LHC vise à capitaliser et à développer la collaboration, l'innovation, les compétences et le renforcement des capacités.

SE PROTÉGER ET PRÉVENIR LES CYBERMENACES & TESTER ET AMÉLIORER SA CYBER-RÉSILIENCE

nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

Le Centre national de compétences en matière de cybersécurité (NC3) a pour objectif de renforcer l'écosystème luxembourgeois face aux menaces et risques cyber, en développant les compétences et les capacités en matière de cybersécurité, de manière à contribuer à développer la base industrielle de la cybersécurité dans le pays, et à renforcer l'autonomie stratégique de l'Union européenne.

DÉTECTER ET RÉAGIR FACE AUX INCIDENTS CYBER

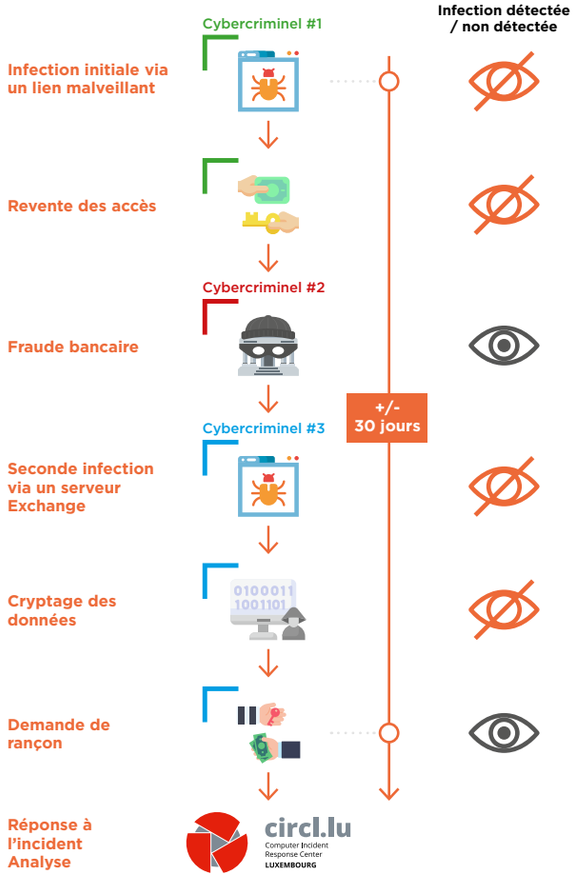
circl.lu
Computer Incident Response Center
LUXEMBOURG

Le *Computer Incident Response Center Luxembourg* (CIRCL) est une initiative gouvernementale visant à fournir un dispositif de réponse systématique aux menaces et incidents de sécurité informatique.
Le CIRCL est le CERT pour le secteur privé, les communes et les entités non gouvernementales au Luxembourg.

Coup d'oeil sur un processus d'infection

Considérons ci-après l'exemple de vulnérabilités identifiées sur certains serveurs Microsoft Exchange en février-mars 2021. Une situation qui a concerné un certain nombre d'entreprises luxembourgeoises. Dès les vulnérabilités rendues publiques, le CIRCL a notifié les organisations pour lesquelles il avait identifié un serveur Exchange vulnérable[1], et susceptible d'entraîner le vol ou la destruction de données ou la compromission des infrastructures. **C'est pourquoi, il est recommandé aux entreprises de fournir au CIRCL un point de contact, leur nom de domaine et adresse IP afin que ce dernier puisse les notifier lors de ses recherches proactives de vulnérabilités.**

En prenant pour base cet exemple, découvrez ce qu'il se passe avant, pendant et après une infection. L'exploitation d'une vulnérabilité par un premier attaquant, si elle n'est pas détectée pendant un certain temps, permet à plusieurs autres attaquants potentiels de l'exploiter.



[1] Ce qui ne veut pas dire que la vulnérabilité était exploitée et le serveur infecté.

270 serveurs Microsoft Exchange identifiés vulnérables au Luxembourg et **30 d'entre eux infectés en une semaine** en mars 2021.

Des vulnérabilités apparaissent régulièrement sur des produits ICTs. **Comment éviter qu'un tel cas se produise ?** Réaliser et tenir à jour un inventaire de tous les équipements exposés sur internet et effectuer leur maintenance ou s'assurer qu'elle soit faite dans les délais requis si confiée à un tiers.

Se préparer à faire face à une telle situation. Avoir un maximum d'éléments préparés en avance, comme un scénario de crise et des éléments de communication tels qu'un communiqué de presse (à adapter en fonction de la situation) permet d'éviter d'agir sous l'effet de la panique.

Auto-évaluation

Dans mon entreprise...

1. Les employés reçoivent des formations à la sécurité et à la protection de l'information
❒ Oui, ils en ont eu une il y a déjà quelque temps
❒ Oui, ils en ont régulièrement
❒ Non, jamais

2. Chacun sait à qui s'adresser en cas de questions ou problèmes liés à la sécurité de l'information
❒ Oui, cela fait partie d'une procédure communiquée et affichée
❒ Oui, je crois
❒ Non, je ne pense pas

3. Pour se connecter à distance à l'entreprise, les employés disposent de règles (choix de connexion WiFi ...) et d'un accès protégé (VPN – Virtual Private Network)
❒ Oui
❒ Non

4. Les mots de passe doivent répondre à une structure définie (12 caractères ou plus, au moins une majuscule, une minuscule, un chiffre, un caractère spécial) et sont changés régulièrement
❒ Oui
❒ Non

5. Les ordinateurs sont soumis à des droits d'administration ou à des consignes, qui empêchent les utilisateurs d'installer un logiciel d'une source non validée ou certifiée
❒ Oui
❒ Non

6. Les *backups* concernant toutes les données importantes sont faits et vérifiés régulièrement par des tests de restauration.
❒ Oui
❒ Non

7. Il faut éviter de travailler sur son matériel informatique personnel au sein de l'entreprise.
❒ Oui
❒ Non

Vous avez répondu « non » à au moins une question ou vous souhaitez tester votre maturité à la sécurité de l'information ? Nous vous recommandons de passer le diagnostic *Fit4Cybersecurity* du CASES (**https://fit4cybersecurity.cases.lu/**) pour obtenir un score et des recommandations qui vous aideront à augmenter la maturité de votre entreprise en matière de cybersécurité.

Les outils et solutions
(liste non exhaustive)

Une palette d'outils est à la disposition des entreprises pour se préparer au mieux à parer une attaque : auto-diagnostics pour se situer et recevoir des recommandations en fonction de son profil, applications, services, vidéos, formations…
Voir aussi le site https://lhc.lu ainsi que la plateforme https://cybersecurity.lu qui référence tous les acteurs de la cybersécurité au Luxembourg.

Aucune solution logicielle n'est indiquée ici car le choix est pléthorique. Un logiciel pourrait donner la fausse impression à une entreprise d'être protégée, alors que la protection comprend de multiples paramètres.

La *Luxembourg House of Cybersecurity* héberge un *Cyber Desk* destiné à vous mettre en relation avec le bon interlocuteur : que vous ayez besoin d'aide, de conseils ou que vous souhaitiez discuter d'un sujet ou d'un projet lié à la cybersécurité, des experts compétents sont là pour vous. Plus d'informations : https://lhc.lu/service/cyber-desk

Communication et sensibilisation

Trustbox par le NC3 (https://nc3.lu/pages/trustbox.html) : outils et matériel permettant d'accroître la sensibilisation et de renforcer les connaissances et réflexes des employés de l'entreprise.

Mise en situation réelle

ROOM#42 par le NC3 (https://room42.lu/) : un bureau reconstitué pour simuler une situation d'attaque, identifier les réactions des employés et leur enseigner comment réagir.

Formations

Des formations pour tous les niveaux (du débutant au responsable IT), de la sensibilisation à l'analyse technique de ce qui se produit lors d'une cyberattaque, dans toutes les langues, pour une durée de quelques heures à plusieurs jours.

Voir :
- **www.cybersecurity.lu/education**
- **www.lifelonglearning.lu**
- **www.houseoftraining.lu**
- **www.keyjob.lu**
- **www.circl.lu/services/training/**

Outils d'auto-diagnostic (gratuits, anonymes et en ligne)

***Fit4Cybersecurity* du NC3 (https://fit4cybersecurity.nc3.lu/) :** permet d'évaluer la maturité de son entreprise en matière de cybersécurité et de recevoir des recommandations en fonction des résultats. *(voir Auto-évaluation, p.19)*

***Fit4Contract* du NC3 (https://fit4contract.nc3.lu/) :** est un outil d'auto-évaluation conçu pour aider les clients à revoir leurs contrats avec leurs fournisseurs. En cas d'incident, un bon contrat peut faire la différence, si les responsabilités de chaque partie prenante sont clairement définies. *Fit4Contract* aide à négocier un contrat qui protègera mieux l'entreprise en cas de problème de sécurité de l'information.

***Fit4Privacy du NC3* (https://fit4privacy.nc3.lu/) :**
outil d'auto-évaluation en ligne, anonyme, donnant des recommandations concrètes quant aux étapes clés de la protection des données.

Services

Threat Observatory Platform par le NC3 (https://nc3.lu/pages/observatory.html) : vise à fournir à ses utilisateurs des informations sur les menaces émergentes en matière de cybersécurité, afin de faciliter leurs processus de décision concernant les stratégies de prévention à entreprendre.

MONARC par le NC3 (https://nc3.lu/pages/monarc.html) :
outil et méthode permettant une évaluation des risques optimisée, précise et reproductible.

MISP par le CIRCL (https://www.circl.lu/misp/) :
plateforme de partage d'informations relatives aux menaces, servant aussi à optimiser l'application des contre-mesures et améliorer la prévention et la détection des logiciels malveillants.

URL abuse par le CIRCL (https://www.securitymadein.lu/services/urlabuse/) :
possibilité de soumettre des URL suspects afin de les faire analyser.

Lookyloo par le CIRCL (https://lookyloo.circl.lu/) : interface web qui permet aux utilisateurs de capturer et soumettre une page de site web.

Pandora par le CIRCL (https://pandora.circl.lu/submit) :
service en ligne gratuit permettant d'examiner en toute sécurité des fichiers ou des documents reçus par un tiers.

Typosquatting Finder par le CIRCL (https://typosquatting-finder.circl.lu/) :
service gratuit et public permettant de trouver rapidement des domaines typosquattés afin d'évaluer si un adversaire utilise des faux domaines existants.

Testing Platform par le NC3 (https://nc3.lu/pages/testing-platform.html) :
contient les outils et les services qui aideront les organisations à effectuer des tests de base sur leurs infrastructures les plus couramment exposées, à commencer par les serveurs de messagerie et les serveurs web.
La *Testing Platform* consacre tout un volet au pentesting.
Des hackers sous contrat pénètrent les systèmes informatiques afin d'identifier les brèches par lesquelles les cybercriminels pourraient s'immiscer, et font des recommandations pour les réduire.
Plusieurs sociétés proposent ce service.
Voir **https://www.cybersecurity.lu/privatesector?taxonomy_values=85**

Le *pentesting* pour identifier les failles de son système

Propos recueillis auprès de Jean-Marie Bourbon, service Sécurité Offensive de POST.
Parmi les 50 experts en cybersécurité de son département Cyberforce, POST compte neuf « *pentesters* », qui mettent leurs talents de *hackers* au service de leurs clients, afin de simuler une attaque, identifier les failles et faire des recommandations pour mieux se protéger.

Pourquoi faire des tests d'intrusion si on a des logiciels pour se protéger ?
Avant de corriger une vulnérabilité il faut la mettre en évidence.
Prendre le rôle d'un cybercriminel en simulant les techniques utilisées lors d'une cyberattaque pour éprouver les vulnérabilités dune entreprise est le meilleur moyen pour la protéger. Car hélas, avoir un antivirus, des machines à jour ou former ses employés ne constitue pas une garantie suffisante contre les intrusions. Les méthodes classiques ont atteint leurs limites et l'actualité le montre sans cesse.

Le *pentester* étudie les possibilités qui lui sont offertes pour pouvoir pénétrer le système informatique d'une organisation : un accès distant est-il proposé ? Est-il seulement protégé par un mot de passe ? Quels sont les obstacles et comment pourraient-ils être contournés ?
Il est même possible de tenter de rentrer physiquement dans un bâtiment pour aller jusqu'à la salle des serveurs ou le bureau du dirigeant pour y brancher un boitier ou soustraire des documents,... C'est beaucoup plus facile qu'on pourrait le penser, il suffit d'y aller au culot.

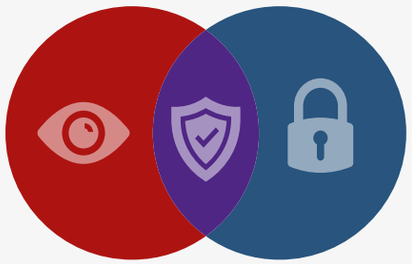
Pour une petite entreprise, 3 à 4 jours de consultance technique peuvent suffire pour dresser un bilan des vulnérabilités les plus aisément exploitables, identifier les risques et obtenir des recommandations pour limiter la surface d'attaque offerte aux criminels.

Les recommandations faites ne consistent pas à acheter des solutions coûteuses, loin de là. Changer une configuration, faire une mise à jour ainsi que diverses actions relativement simples suffisent dans la plupart des cas.

Des logiciels *open source* gratuits existent aussi, il suffit de savoir ce dont on a besoin. Et puis il faut former son équipe IT à avoir les réactions appropriées face à une attaque, pour ne pas faciliter les intrusions dans le système en prenant des mesures inappropriées.

Afin de former le personnel IT du client nous proposons des exercices appelés « *Adversary Simulation* » permettant de simuler une menace réelle, ainsi que d'évaluer objectivement et factuellement l'exposition d'une société aux risques d'intrusions.

CONFIGURATION CLASSIQUE D'EXERCICE
DE SIMULATION D'UNE ATTAQUE.
Les rouges sont les attaquants, les bleus l'équipe IT qui contre les attaques. La purple team est une équipe mixte, qui permet de comprendre les tactiques des rouges.



Red Team (offensive)
Simule une menace en utilisant une approche réaliste pour évaluer les réactions des personnes et l'efficacité des procédures et technologies utilisées pour défendre l'entreprise.

Purple Team (but commun)
Travaille pour comprendre les techniques, tactiques et procédures employées par les attaquants afin d'améliorer sa posture.

Blue Team (défensive)
Répond à l'intrusion, contient et identifie la menace, monitore.

Pourquoi les cybercriminels attaqueraient-ils une petite entreprise ?
Une PME peut être prestataire d'un grand groupe ou d'un organisme gouvernemental, par exemple. Les cybercriminels passeront par elle, car elle est souvent moins bien protégée, pour atteindre leur cible ultime. C'est ce qu'on appelle la « *supply chain attack* ».

Quels conseils donneriez-vous à une petite entreprise ?
Ne pas se fier entièrement à une solution qui pourrait donner la fausse impression d'être protégé. Les solutions existantes ne protègent que des attaques connues, or il en apparaît tous les jours de nouvelles, qui ne laissent aucune chance de se défendre et pour lesquelles il n'existe aucun patch correctif. Il faut se méfier de la seule protection périmétrique et mettre le plus d'obstacles possibles pour limiter la surface d'attaque. Ce n'est pas parce qu'on ne voit rien qu'il ne se passe rien. Le ver peut être dans le fruit et attendre avant de se déclarer.

Investir dans la sécurité, c'est comme prendre une assurance : cela coûte et ne rapporte pas directement. Mais cela permet de limiter les impacts d'une attaque qui elle, pourrait conduire à une rupture d'activité, à l'exposition, à des sanctions et dans certains cas, comme nous l'avons déjà vu malheureusement, à la cessation pure et simple des activités de l'entreprise.

Qui peut m'aider ?

Pour se protéger, prévenir et analyser les cyber-risques :
info@nc3.lu

Pour tester et améliorer sa cyber-résilience :
info@nc3.lu

Pour rapporter ou réagir à un incident cyber :
https://www.circl.lu/report/

Pour reporter un incident de sécurité, 3 options :

- **Remplir un formulaire anonyme en ligne :**
  https://www.circl.lu/contactform/
- **Envoyer un email de préférence chiffré en GPG/PGP :**
  info@circl.lu
- **Appeler le :**
  (+352) 247 88444

Pour un contact avec la *Luxembourg House of Cybersecurity* et être orienté vers le département qui correspond le mieux à vos besoins :
info@lhc.lu

Pour obtenir une liste d'outils mis à disposition par le CIRCL et le NC3 :
https://circl.lu/services/
https://nc3.lu/

Pour en savoir plus sur le *ransomware*, attaque la plus fréquente sur les PME :
https://circl.lu/pub/tr-57/

Pour consulter la liste exhaustive de tous les acteurs qui gravitent autour de la cybersécurité :
https://cybersecurity.lu