ECO NEWS FLASH

OCTOBRE 2023 / N°15

Quand robustesse économique rime avec sécurité informatique

L'accélération de la digitalisation a fait de la sécurité informatique un enjeu économique vital. Alors que les experts du Forum Economique Mondial réunis à Davos en janvier 2023 évoquaient une « Cyber-Tempête » mondiale, cette préoccupation trouve aussi écho au Luxembourg. « Permettre une transformation sûre et fiable de l'économie des données » constitue en effet un des piliers de la feuille de route « Ons Wirtschaft vu muer » publiée en 2021 par le ministère de l'Economie, dans le but de faire du pays une économie compétitive et durable.

L'accroissement du risque de cyberattaques

Le 21ème siècle se caractérise par l'omniprésence de flux d'informations divers et variés communément nommés « Big Data ». Le recours croissant aux technologies digitales via par exemple le développement du télétravail, de l'e-commerce, des services en ligne, des appareils mobiles, des *smart technologies* ou encore des cryptomonnaies, s'est traduit par une multiplication des surfaces exposées aux cyberattaques. Ces dernières auraient en effet connu une augmentation mondiale de l'ordre de 80 % entre 2017 et 2022[1].

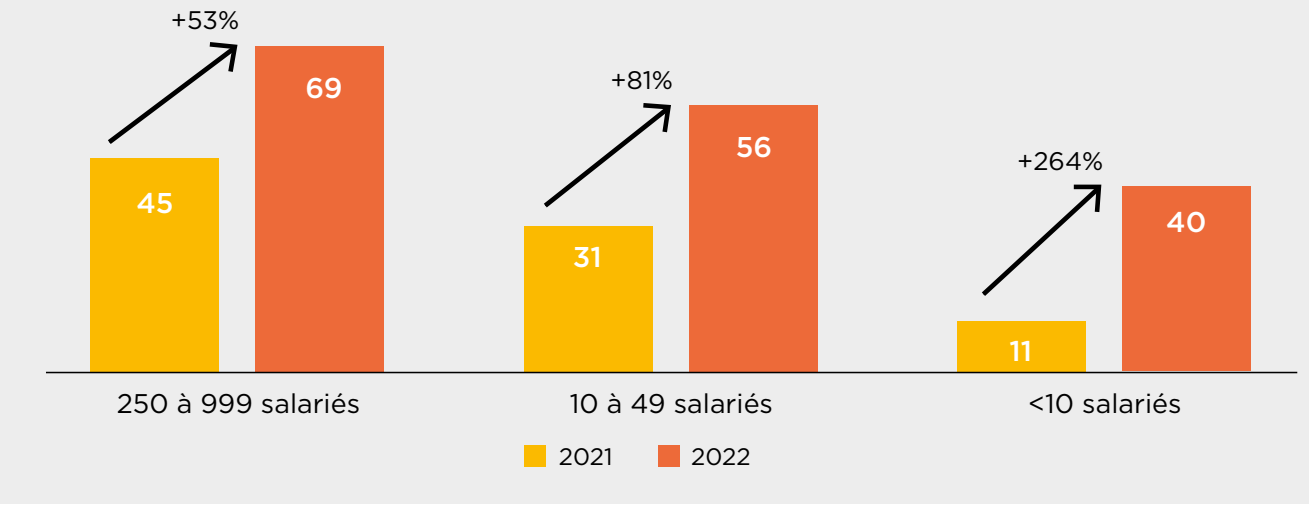
C'est ainsi que 83 %[2] des organisations auraient déjà subies une ou plusieurs violations de données au cours de leur existence. Selon le rapport 2022 de la société d'assurances Hiscox[3] (ci-après « enquête Hiscox »), le nombre de cyberattaques subies par une entreprise par an s'élève en moyenne à 190. Il existe néanmoins un écart important entre les plus grandes organisations et celles de taille plus modeste, puisque celles jouissant d'un revenu supérieur à 4,5 milliards d'euros peuvent connaitre jusqu'à 1.100 attaques en moyenne par an. En valeurs relatives cependant, force est de constater que les menaces informatiques s'accroissent plus particulièrement pour les plus petites structures. Entre 2021 et 2022, le nombre de cyberattaques s'est accru de 53 % pour les entreprises de 250 à 99 salariés, 81 % pour celles de 10 à 49 salariés et 264 % pour celles de moins de 10 salariés.

1 *Sonicwall (spécialiste en cybersécurité), « Cyber threat report », 2023.*

2 *Selon l'enquête internationale « Cost of a Data Breach » réalisée par IBM entre mars 2021 et mars 2022 sur un échantillon de 550 entités et publiée en 2022, dont majoritairement des ETI (entreprises de tailles intermédiaires, 250 à 4999 salariés) et multinationales.*

3 *Hiscox assurances, « Rapport sur la gestion des cyber-risques », 2022, enquête réalisée sur un échantillon de 5.181 professionnels en charge de la stratégie de cybersécurité de leur entreprise œuvrant majoritairement dans des TPE-PME (environ 60% des répondants) aux Etats-Unis, au Royaume-Uni, en France, en Allemagne, en Belgique, en Espagne, aux Pays-Bas et en Irlande.*

NOMBRE MOYEN DE CYBERATTAQUES PAR AN SELON LA TAILLE DE L'ENTREPRISE

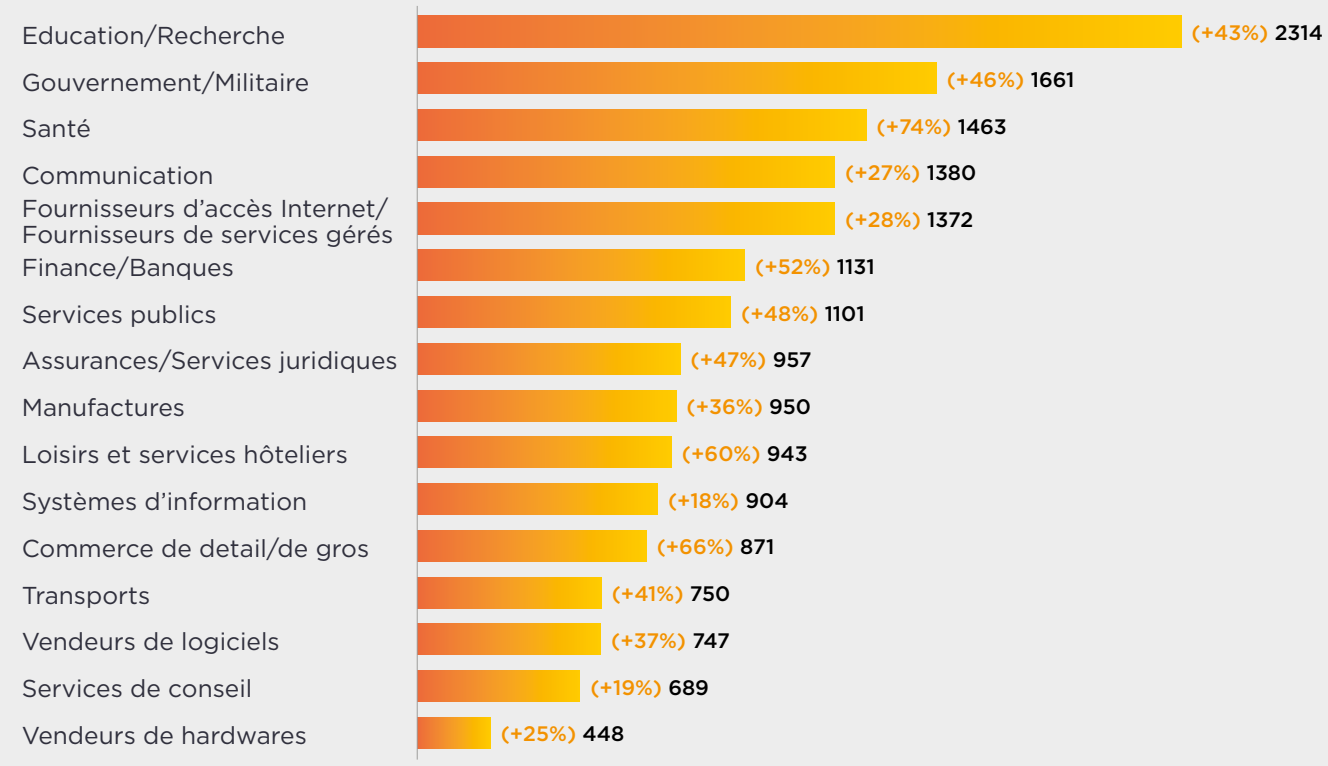


Source: Hiscox, Rapport 2022 sur la gestion des cyber-risques

Une menace pesant sur l'ensemble des secteurs de l'économie

Selon le rapport publié en 2023 par le fournisseur mondial de solutions de cybersécurité Check Point, le nombre de cyberattaques a connu une augmentation continue ces dernières années dans tous les secteurs d'activité de l'économie au niveau international.

NOMBRE MOYEN HEBDOMADAIRE DE CYBERATTAQUES PAR ORGANISATIONS ET PAR INDUSTRIES EN 2022 COMPARÉ À 2021



Source: Check Point 2023 Security report

Parmi ces derniers, les établissements d'enseignement et de recherche sont les plus menacés, avec une moyenne de 2.314 attaques par semaine et par organisation, soit une augmentation de plus de 43 % par rapport à 2021. La fermeture du Lincoln College (école américaine existant depuis plus de 150 ans, ayant survécu à de nombreux désastres, dont un incendie majeur en 1912, la grippe espagnole et la Grande Dépression), suite à une attaque informatique, est un exemple marquant du danger que représente ce type de menace.

En deuxième position des plus vulnérables, se trouvent les domaines gouvernementaux et militaires. Ces derniers ont connu une moyenne de 1.661 cyberattaques par semaine et par organisation en 2022, soit une augmentation d'environ 46 % par rapport à l'année précédente. L'Ukraine a par exemple été victime, en janvier 2022, d'une cyberattaque de grande ampleur qui a mis hors service plusieurs sites web de son gouvernement et de ses ministères. En juillet 2022, la Norvège et la Lituanie ont toutes deux été victimes d'attaques de déni de service distribué (DDoS[4]) à grande échelle. Le site internet du Parlement européen a quant à lui subi une attaque similaire (revendiquée par des groupes hacktivistes[5]) à la suite d'un vote déclarant la Russie comme État soutenant le terrorisme.

Le troisième secteur le plus touché, qui est aussi celui qui a enregistré la plus forte hausse de cyberattaques entre 2021 et 2022 (+74 %), est celui de la santé. Qu'il s'agisse d'hôpitaux, de cliniques ou de centres de recherche, les attaquants se concentrent plus particulièrement sur le secteur de la santé depuis le début de la pandémie de Covid-19. En mai 2022, les hôpitaux de l'intercommunale de soins de santé Vivalia en Belgique ont par exemple été victimes d'une attaque de type ransomware[6] de grande ampleur. 400GB de données (ex: informations sur les traitements, les prescriptions, les patients…) ont notamment été cryptées et rendues inaccessibles par les pirates informatiques, ce qui a significativement entravé la délivrance des services médicaux et conduit à la désactivation de 200 serveurs Windows et 1.500 postes de travail.

Dans le monde entier, les attaques informatiques engendrent ainsi des conséquences importantes sur tous les secteurs économiques. Elles peuvent perturber le fonctionnement des administrations et des organisations et découler sur des coûts tantôt humains, tantôt matériels ou financiers.

La vulnérabilité informatique: source d'innombrables coûts

Selon le «Global Data Protection Index 2022» publié par Dell Technologies, le coût moyen d'un cyber incident pour une entreprise a dépassé la barre du million de dollars américains en 2022. Les cyberattaques engendrent des coûts significatifs qui peuvent varier entre quelques milliers et plusieurs millions d'euros en fonction de variables telles que la taille de l'organisation, le secteur d'activité ou encore la nature et la gravité de l'attaque.

Les entreprises de grande taille sont celles qui ont des surfaces d'attaques potentielles les plus nombreuses, et qui sont donc les plus exposées aux cybermenaces engendrant des coûts importants. Ainsi, selon une enquête mondiale réalisée par IBM[7] en 2022 sur un échantillon majoritairement composé d'entreprises de tailles intermédiaires (250 à 499 salariés) et de multinationales, la facture d'une cyberattaque touchant des infrastructures critiques[8] peut par exemple s'élever jusqu'à 4,35 millions de dollars américains. A l'opposé, les dommages monétaires apparaissent comme moindres en valeurs absolues pour les structures de taille plus modeste. C'est ainsi que l'enquête Hiscox, dont 60 % des répondants sont des TPE (1 à 9 salariés) et des PME (10 à 249 salariés) estime le coût financier médian d'une cyberattaque à environ 9.000 euros pour la Belgique, 15.000 euros pour la France et 19.000 euros pour l'Allemagne.

4 Une attaque de déni de service distribué consiste à rendre un service indisponible, empêchant ainsi les utilisateurs légitimes d'y avoir accès.

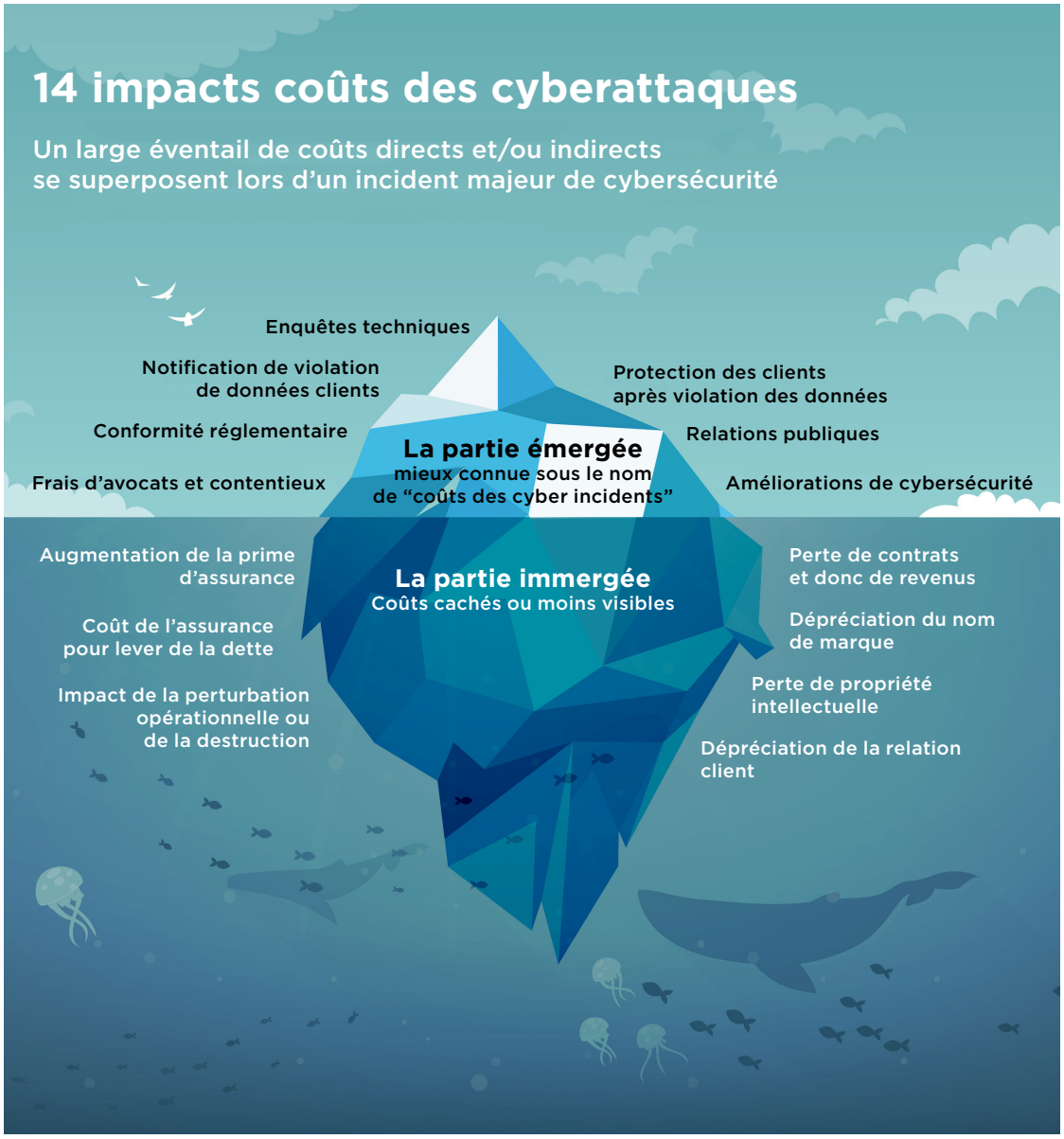
5 L'hacktivisme est une forme d'activisme numérique. Les hacktivistes exercent des violations de données sans but lucratif au nom d'idéologies politiques, sociales, religieuses ou anarchiques.

6 Pratique qui consiste à «prendre en otage» des données personnelles en les confisquant jusqu'à ce qu'une rançon soit versée par la victime de la cyberattaque.

7 IBM, «Cost of a Data Breach», 2022.

8 Les infrastructures critiques considérées par l'étude d'IBM comprennent les services financiers, la technologie, l'énergie, les transports, la communication, la santé, l'éducation et les industries des secteurs publics.

Les dommages liés à une cyberattaque sont néanmoins difficilement chiffrables car ils incluent à la fois des coûts directs (ex: coûts de l'enquête technique pour identifier l'origine de l'attaque, coûts de la sécurisation des données clients post-incidents…) et indirects (ex: impacts liés à la perturbation des activités, perte de la confiance client…). Comme ces derniers peuvent survenir des années suivant l'attaque informatique, ils risquent d'être sous-estimés, ce pourquoi le cabinet Deloitte les compare à la partie immergée d'un iceberg.



Source: Deloitte

L'enquête nationale[9] réalisée par la Luxembourg House of Cybersecurity (LHC) en 2023 et à laquelle la Chambre de Commerce a contribué, illustre parfaitement cette situation. En effet, 60% des PME luxembourgeoises ayant reporté un incident de sécurité informatique ont constaté une perte de temps de travail significative, car réallouée à la mitigation des conséquences et au rétablissement de l'entreprise. En outre, 11% ont vu leurs revenus directement impactés à la baisse.

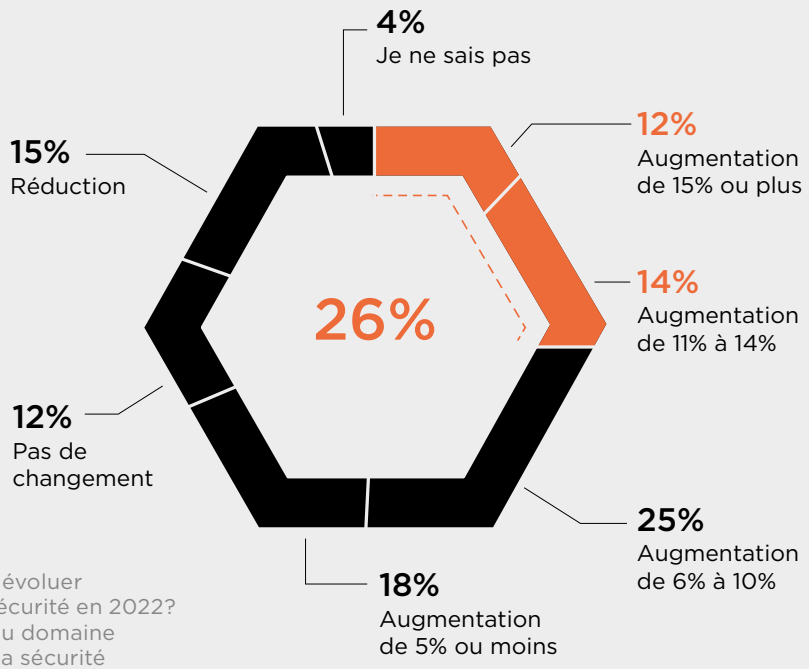
Pour éviter ce type d'incident, et parce qu'il vaut mieux prévenir que guérir, de plus en plus d'entreprises optent pour le renforcement de leur sécurité informatique.

9 Le rapport détaillant les résultats de l'enquête menée par la LHC à propos des défis et opportunités rencontrés par les PME dans le domaine de la cybersécurité devrait être publié fin 2023.

Des dépenses croissantes en la matière

Face à l'augmentation des vulnérabilités informatiques, les investissements des entreprises dans le domaine de la cybersécurité deviennent de plus en plus conséquents. C'est ainsi que l'enquête «2022 Global Digital Trust Insights» réalisée par PriceWaterhouseCoopers au niveau mondial, révèle que 69% des firmes interrogées en octobre 2021, prévoient une augmentation de leurs dépenses de sécurité informatique. Parmi celles-ci, plus d'un quart planifient une croissance à deux chiffres dans ce domaine.

PLUS DE 25% DES ENTREPRISES S'ATTENDENT À UNE CROISSANCE À DEUX CHIFFRES DE LEUR BUDGET EN SÉCURITÉ INFORMATIQUE EN 2022

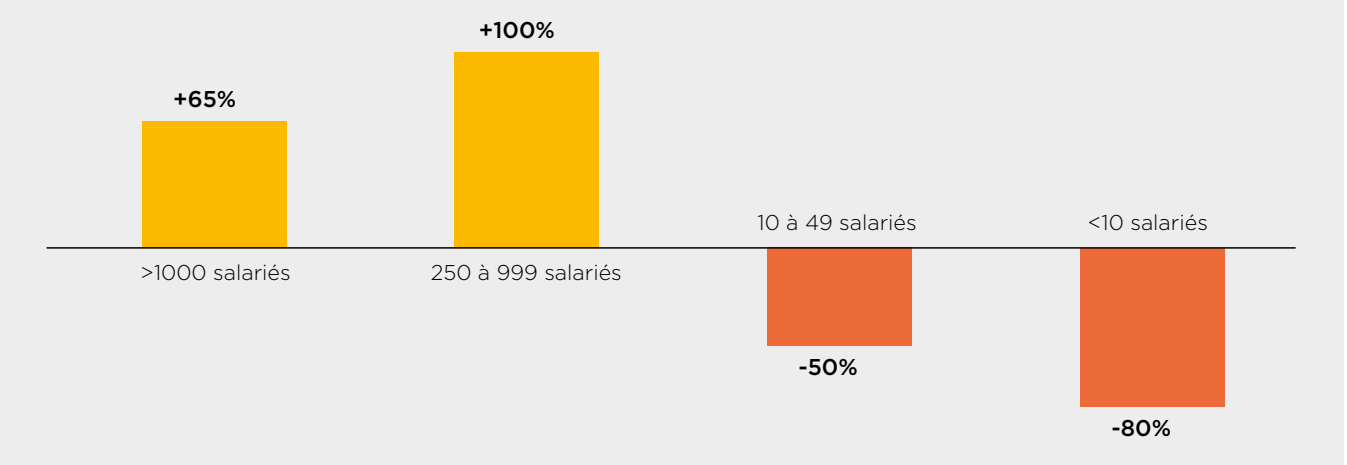


Question: Comment va évoluer votre budget de cybersécurité en 2022?
Base: 1.638 dirigeants du domaine de la technologie et de la sécurité

Source: Pwc, 2022 Global Digital Trust Insights, Octobre 2021.

Le coût associé au déploiement de mesures de cybersécurité est variable selon divers critères comme les exigences en matière de conformité et de réglementation, les solutions informatiques existantes, la complexité de l'infrastructure informatique, la sensibilité des données collectées, le secteur d'activité, ou encore la taille d'une entreprise. Si l'on se réfère à ce dernier élément, par exemple, un écart important est constaté entre les différentes firmes en termes de valeurs. L'enquête Hiscox permet d'observer qu'entre 2021 et 2022, les dépenses moyennes en cybersécurité des entreprises ont augmenté de 100% pour celles employant entre 250 et 999 personnes et de 65% pour celles employant plus de 1.000 personnes. A l'inverse, ces dépenses ont pratiquement été divisées par 2 pour les entreprises ayant entre 10 et 49 salariés et ont diminué de près de 80% pour les firmes de moins de 10 employés, bien que les conséquences d'une cyberattaque sont souvent plus critiques pour les structures de taille modeste. Ce phénomène est notamment le résultat d'évènements économiques tels que les retombées de la pandémie de Covid-19 ou encore la crise énergétique, qui ont particulièrement rogné la capacité des entreprises les plus modestes à alimenter leur budget informatique. En valeurs relatives néanmoins, ces petites entreprises suivent la tendance générale puisqu'elles allouent près de 20% de ce budget à la cybersécurité en 2022, contre 17% en 2021.

ÉVOLUTION DES DÉPENSES MOYENNES EN CYBERSÉCURITÉ DES ENTREPRISES ENTRE 2021 ET 2022



Source: Hiscox, Rapport 2022 sur le gestion des cyber-risques

Si assurer la cybersécurité dans les PME est en valeur absolue moins onéreux que dans les structures de plus grande taille, il n'en est rien en valeur relative. La mise en place de mesures de sécurisation nécessite généralement un pourcentage plus élevé du budget opérationnel pour les structures de taille modeste que pour les grandes entreprises. L'effet de volume permet par exemple à ces dernières de bénéficier de prix attractifs lors d'achat massif de dispositifs de sécurité. A l'opposé, certaines petites entreprises qui sont soumises à des mandats de conformité doivent mettre en œuvre certains contrôles de sécurité identiques à leurs homologues de plus grande taille, et ce malgré une clientèle moindre.

Une panoplie d'outils divers pour renforcer la sécurité informatique

Les postes de dépenses pour déployer une protection informatique sont divers. Parmi les plus courants, on compte par exemple la mise en place de formations de sensibilisation à la sécurité informatique pour les employés, le lancement d'un audit de cybersécurité, le déploiement d'un plan de réponse aux incidents, ou encore le renforcement et la maintenance des infrastructures et processus informatiques (ex: installation de pares-feux et anti-virus, mise à jour régulière des logiciels, politique de mots de passe forts, surveillance et détection des intrusions, sauvegarde régulière des données, etc.).

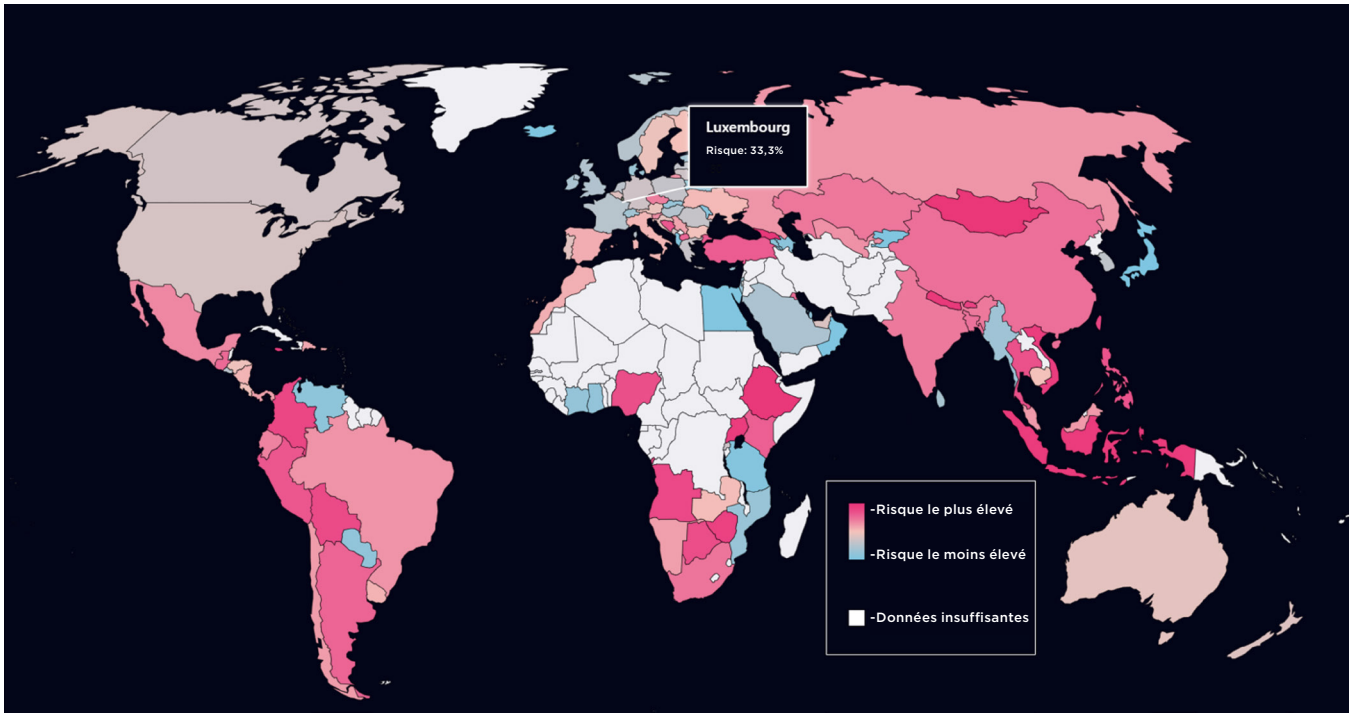
Parallèlement à ces mesures préventives, les entreprises sont également de plus en plus nombreuses à souscrire à une assurance dans le domaine de la cybersécurité. C'est ainsi qu'en 2022, 64% d'entre-elles, soit plus de la moitié, se sont protégées par ce biais selon l'enquête Hiscox.

Le Luxembourg: un des pays où le risque de cybermenaces reste le plus faible

Selon le rapport publié en 2023 par le fournisseur mondial de solutions de cybersécurité Check Point, le risque d'occurrence d'attaques informatiques n'est pas le même dans tous les pays. Si la cybersécurité est un défi mondial, certains pays peuvent être plus ou moins fréquemment ciblés selon des facteurs tels que par exemple, leur rôle géopolitique, leur puissance économique, leur niveau de développement technologique ou encore la quantité de données qu'ils possèdent. En effet, les motivations d'une cyberattaque sont diverses, allant de la recherche de gains financiers à l'espionnage industriel, en passant par le terrorisme, l'hacktivisme ou la cyberguerre[10].

10 La cyberguerre consiste à utiliser les ordinateurs et Internet pour mener des offensives dans le cyberespace (ex: sabotage d'équipements, perturbation des infrastructures sensibles, désinformation...)

NIVEAU DE RISQUE DE CYBERMENACES DANS LE MONDE



Source: Check Point 2023 Security report

La plupart des zones les plus susceptibles d'être visées par des cyberattaques sont localisées en Asie (et notamment dans la partie Sud-est), en Amérique du Sud et dans certains pays africains. Parmi les territoires à plus hauts risques (en rouge sur la carte), on compte notamment la Mongolie (100 %), l'Ethiopie (95,3 %), le Népal (77,6 %) et l'Indonésie (69,5 %).

Les 3 pays considérés comme les moins risqués (en vert sur la carte) sont le Japon (15,8 %), l'Islande (16,4 %) et Oman (18,4 %).

Le Luxembourg est quant à lui évalué à 33,3 % et constitue un des pays où le risque est le plus faible dans l'Union européenne, après la Slovaquie (30,1%), le Danemark (31,3 %), la Suisse (32,4 %) et l'Estonie (32,5 %).

Le Luxembourg : un écosystème de cybersécurité bien positionné au niveau mondial

A côté du risque d'occurrence d'attaques informatiques, il convient aussi d'observer des niveaux de cybersécurité différents selon les pays. A cette fin, on peut se référer au Global Cybersecurity Index qui a été calculé suite à une enquête réalisée en 2020 dans 169 pays et publié en 2021 par l'International Telecommunication Union (ITU)[11]. Cet indicateur mesure en effet l'engagement des pays en faveur de la cybersécurité au niveau mondial, sur la base de cinq piliers (mesures juridiques, mesures techniques, mesures organisationnelles, développement des capacités et mesures coopératives), agrégés dans un score global.

Dans ce classement pour le moins serré, le Luxembourg obtient un index de 97,41 qui le porte 13ème au niveau mondial sur 194 pays (les 3 premiers étant les Etats-Unis avec un score de 100, le Royaume-Uni et l'Arabie Saoudite tous deux à 99,54), et 7ème au niveau du continent européen sur 47 pays (les champions étant le Royaume-Uni à 99,54, l'Estonie à 99,48 et l'Espagne à 98,52).

11 Agence des Nations Unies spécialisée dans les technologies de l'information et de la communication.

GLOBAL CYBERSECURITY INDEX 2020 - EXTRAIT DU CLASSEMENT MONDIAL

Pays	Score	Classement
États-Unis	100	1
Royaume-Uni	99,54	2
Arabie Saoudite	99,54	2
Estonie	99,48	3
Corée (Rép. de)	98,52	4
Singapour	98,52	4
Espagne	98,52	4
Russie	98,06	5
Emirats Arabes Unis	98,06	5
Malaisie	98,06	5
Lituanie	97,93	6
Japon	97,82	7
Canada	97,67	8
France	97,6	9
Inde	97,5	10
Turquie	97,49	11
Australie	97,47	12
Luxembourg	**97,41**	**13**
Allemagne	97,41	13
Portugal	97,32	14
Lettonie	97,28	15
Pays-Bas	97,05	16
Norvège	96,89	17
Ile Maurice	96,89	17
Brésil	96,6	18
Belgique	96,25	19
Italie	96,13	20

Source: ITU, Global Cybersecurity Index v4, 2020

GLOBAL CYBERSECURITY INDEX 2020 - EXTRAIT DU CLASSEMENT EUROPÉEN

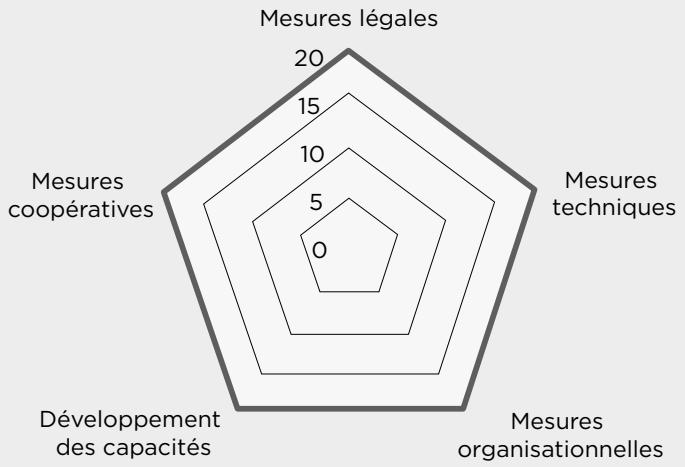
Pays	Score	Classement
Royaume-Uni	99,54	1
Estonie	99,48	2
Espagne	98,52	3
Lituanie	97,93	4
France	97,6	5
Turquie	97,5	6
Luxembourg	**97,41**	**7**
Allemagne	97,41	7
Portugal	97,32	8
Lettonie	97,28	9
Pays-Bas	97,05	10
Norvège	96,89	11
Belgique	96,25	12
Italie	96,13	13
Finlande	95,78	14
Suède	94,59	15
Grèce	93,98	16
Autriche	93,89	17
Pologne	93,86	18
Danemark	92,6	19
Croatie	92,53	20

Source: ITU, Global Cybersecurity Index v4, 2020

Selon le Global Cybersecurity Index 2020, les points forts du Luxembourg résident dans l'existence d'un cadre juridique approprié pour traiter les questions de cybersécurité et de cybercriminalité («mesures légales» dans l'encadré ci-après), ainsi que dans la disponibilité d'institutions (exemple: organisme national chargé des cyberincidents) et d'outils techniques (ex: cadre national de surveillance, d'alerte et de réaction aux incidents) relatifs à ce domaine («mesures techniques» dans le graphique ci-après).

L'axe où il y aurait le plus de marge de progression à réaliser serait celui concernant les mesures organisationnelles («mesures organisationnelles» dans l'encadré ci-après). En d'autres termes, il s'agit de développer une stratégie nationale solide en matière de cybersécurité, un plan global de mise en œuvre des mesures et des outils pour en évaluer les résultats.

INDICE MONDIAL DE CYBERSÉCURITÉ 2020 - PROFIL DU LUXEMBOURG



Niveau de développement
Pays développé
Pays sans littoral

Domaines de points forts relatifs
Mesures légales et techniques

Domaines de croissance potentiels
Mesures organisationnelles

Score global	Mesures légales	Mesures techniques	Mesures organisationnelles	Développement des capacités	Mesures coopératives
97.41	20.00	19.54	18.98	19.48	19.41

Source: ITU, Global Cybersecurity Index v4, 2020

Certaines mesures organisationnelles ont commencé à être développées au Grand-Duché. La 1ère stratégie nationale de cybersécurité a été instaurée en 2012 et a été mise à jour 3 fois (en 2015, en 2018 et en 2021) pour inclure les nouveaux développements en termes de sécurité informatique. Chaque itération a donné lieu à un renforcement des dispositifs de cybersécurité luxembourgeois. C'est ainsi, par exemple, qu'ont été successivement introduits la Computer Emergency Response Team[12] (CERT), l'Agence nationale de la sécurité des systèmes d'information[13] (ANSSI), le Cybersecurity Competence Center[14] (C3) et le Comité interministériel de coordination en matière de cyberprévention et de cybersécurité.

À côté de ces mesures, on constate néanmoins qu'il existe actuellement encore peu d'outils permettant d'avoir des statistiques plus précises sur l'état de la cybersécurité au Luxembourg. C'est dans ce contexte que le présent document de travail propose un entretien avec Pascal Steichen (CEO de la LHC, agence publique placée sous l'autorité du Ministère de l'Économie et qui a pour mission d'accroître la cyber résilience nationale) dans lequel ce dernier partage son expérience opérationnelle qui permettra au lecteur de mieux cerner la position et progression du Grand-Duché dans sa quête de résilience digitale.

12 La CERT est une équipe chargée de la sécurité informatique et de la réponse aux incidents y relatifs au Luxembourg.

13 L'ANSSI a pour principale mission de veiller à la mise en œuvre de la politique générale de sécurité de l'information de l'Etat.

14 La C3 est une initiative étatique visant à renforcer la sécurité informatique nationale et à promouvoir le développement de compétences dans ce domaine. Ses activités incluent la Recherche & Développement, la formation, les activités de sensibilisation, l'assistance aux entreprises et institutions ou encore la promotion de l'écosystème de cybersécurité luxembourgeois, pour ne citer que quelques exemples.

Entretien avec Pascal Steichen,
CEO de la Luxembourg House of Cybersecurity (LHC)

1. *Quel est le rôle de la LHC ?*

La LHC a pour mission d'accroître la résilience cyber de l'économie luxembourgeoise. L'agence couvre le spectre complet de la cybersécurité grâce à ses deux centres d'expertise.

Le Centre national de compétence en matière de cybersécurité (NC3) a pour objectif de renforcer l'écosystème national face aux menaces et risques cyber, en développant les compétences et les capacités en matière de cybersécurité, de manière à contribuer au développement de la base industrielle de cybersécurité du pays et à renforcer l'autonomie stratégique de l'Union européenne dans ce domaine. Le Centre de réponse sur incident informatique (CIRCL) a pour rôle de fournir une réponse systématique aux menaces et incidents liés à la sécurité informatique. Le CIRCL est la CERT[15] pour le secteur privé, les communes et les entités non gouvernementales au Luxembourg. Il est fortement impliqué dans le partage d'intelligence sur la menace cyber et contribue à la recherche en la matière.

2. *Comme l'a souligné la rencontre annuelle du Forum économique mondial à Davos en janvier, la sécurité informatique est devenue un enjeu économique vital. Pourquoi ?*

La digitalisation rapide de l'économie, et de la société en général, accélérée par la pandémie de Covid-19, crée une dépendance quasi-totale envers la technologie. Dans ce contexte, la prise en compte de la sécurité au cœur des activités d'une entreprise est un gage de qualité mais, bien plus, une nécessité pour sa survie. La complexité de la sécurité de l'information augmente à mesure que son spectre d'application évolue. Les enjeux sont trop importants pour ignorer les risques liés à la cybersécurité et les organisations doivent prendre les mesures nécessaires pour garantir leur succès.

3. *Comment se positionne l'écosystème de cybersécurité luxembourgeois par rapport aux autres économies au niveau de l'Union européenne et au niveau mondial ?*

Selon l'index GCI (Global Cybersecurity Index), le Luxembourg est bien positionné à l'échelle internationale. Le développement de l'écosystème a été majoritairement piloté, les premières années, par les besoins du secteur financier et le portail national CYBERSECURITY Luxembourg recense aujourd'hui plus de 300 fournisseurs de services et/ou produits.

Le Luxembourg occupe un rôle central dans le développement de la politique cybersécurité européenne. Pour ne citer que quelques exemples, les négociations du règlement général européen sur la protection des données (RGPD) se sont effectuées sous la houlette d'une Commissaire luxembourgeoise, la directive NIS a été validée sous la présidence luxembourgeoise du Conseil de l'Union européenne, ou encore, le Luxembourg détient la première présidence du Centre européen de compétences en cybersécurité depuis février 2022.

4. *Quelles sont les principales préoccupations relatives à la cybersécurité au Luxembourg ?*

Notre rapport « Cyber Threat Landscape Luxembourg – 2021-2022 » permet de mieux comprendre les menaces actives au Luxembourg sur la période examinée et les mesures existantes pour s'en prémunir. En 2021-22, les préoccupations principales s'articulaient autour des points suivants : le flux continu de vulnérabilités, l'abus continu de serveurs précédemment compromis, et les attaques contre les fournisseurs de services informatiques et les acteurs du secteur de la banque de détail. Les 4 menaces les plus observées concernaient les attaques de rançongiciel[16] (ransomware), les créations de logs non sécurisés pour exécuter des codes à distance sur des hôtes ciblés (Vulnérabilité Log4j), les détournements de DNS[17] et enfin le phishing[18].

15 La CERT est une équipe chargée de la sécurité informatique et de la réponse aux incidents y relatifs au Luxembourg.

16 Un rançongiciel (ou ransomware) est un logiciel informatique malveillant conçu par les pirates pour forcer les victimes à payer une rançon pour que leurs données soient déchiffrées.

17 Le DNS (Domain Name System) est un service qui fait le lien entre les noms de domaines des sites internet et les adresses IP qui leur sont associées.

18 Le phishing (ou hameçonnage) est une pratique consistant à obtenir du destinataire d'un courriel d'apparence légitime, la transmission de ses coordonnées bancaires ou identifiants de connexion pour réaliser un vol d'argent.

5. *Quelles mesures prioritaires faudrait-il mettre en place pour renforcer l'écosystème de cybersécurité au Luxembourg ?*

L'offre de services/produits de l'écosystème luxembourgeois est très complète, avec seuls quelques rares services manquant à l'appel. Ces manques, bien identifiés, sont pris en compte par des programmes de développement de startups (une mission initiée par le Ministère de l'Économie et confiée à la Luxembourg House of Cybersecurity). En parallèle de cela, la sensibilisation continue reste un effort clé et décisif pour le renforcement et le développement des compétences de l'écosystème. Le plus grand challenge actuel, et futur, réside dans la montée en compétences cyber de secteurs encore peu informatisés ou hors secteur tertiaire, utilisateurs d'IoT[19], comme par exemple, l'industrie, la santé, l'énergie, etc.

6. *Quelles sont les forces et faiblesses de l'écosystème luxembourgeois de cybersécurité ?*

L'écosystème est très pluridisciplinaire, mais peu spécialisé. En effet, l'offre de services se veut très complète tandis que celle des produits demeure encore trop éparse, avec peu de startups spécialisées. De plus, de par la taille du pays, la scalabilité des entreprises est limitée. Enfin, de façon globale et unanime, le secteur de la cybersécurité fait face à un manque de professionnels qualifiés pour faire face aux menaces émergentes.

7. *La cybersécurité est un domaine encore souvent considéré comme trop complexe pour certaines entreprises, dont celles qui entament à peine leur processus de digitalisation. Les PME, notamment, ont souvent peu de ressources humaines, monétaires et temporelles à investir dans le renforcement de leur sécurité informatique.*

a. Dans un environnement où de nombreux flux d'information sont interconnectés, est-ce que cela ne risque pas de menacer la sécurité de l'ensemble des entreprises, petites et grandes ?

En 2023, il n'y a plus d'arguments entendables à l'encontre d'un investissement en cybersécurité, et ce, peu importe la taille de l'entreprise et le secteur d'activité. Il s'agit d'une simple question de survie pour l'entreprise. La LHC est là pour démystifier la complexité souvent perçue de la cybersécurité. L'agence a pour objectif de la rendre appréhendable pour tout type d'entreprise et de secteur et d'accompagner les premiers pas de la mise en place d'une stratégie de cyber résilience. L'expertise de l'écosystème est ensuite à disposition pour couvrir les différents besoins. La mise en relation de l'offre et la demande est notamment rendue possible par le biais du portail national www.cybersecurity.lu, où un registre de tous les acteurs en cybersécurité peut être consulté.

b. Comment s'assurer que l'ensemble des entreprises luxembourgeoises soient bien protégées ?

La collaboration, la coopération et l'échange d'informations en sont les éléments clés. La cybersécurité est un sport collectif, dans lequel le partage d'information n'est pas à craindre, au contraire, il est crucial pour permettre au secteur d'évoluer en corrélation avec la menace.

8. *Parlez-nous de quelques projets novateurs relatifs à la connaissance de l'état de l'offre et de la demande en matière de cybersécurité sur lesquels la LHC œuvre actuellement.*

Je souhaiterais mettre en avant 2 projets. Dans le 1er, nous travaillons sur le développement d'un « Observatoire de la cybersécurité », lequel est un outil central pour la prise de décision, en permettant la maîtrise des menaces cyber qui opèrent sur son secteur d'activité ainsi que les mesures existantes et fiables pour y faire face. Le 2ème projet en cours, réalisé en collaboration avec plusieurs partenaires dont la Chambre de Commerce, est le lancement de la 1ère enquête nationale sur le thème de la cybersécurité. Focalisée sur les PME, elle a pour objectif de mieux connaître et appréhender leurs besoins réels en matière de sécurité informatique et, à termes, de proposer des solutions concrètes et efficaces pour protéger les acteurs les plus vulnérables. Les résultats sont sortis fin octobre 2023.

9. *Quel conseil général donneriez-vous aux entreprises en matière de sécurité informatique ?*

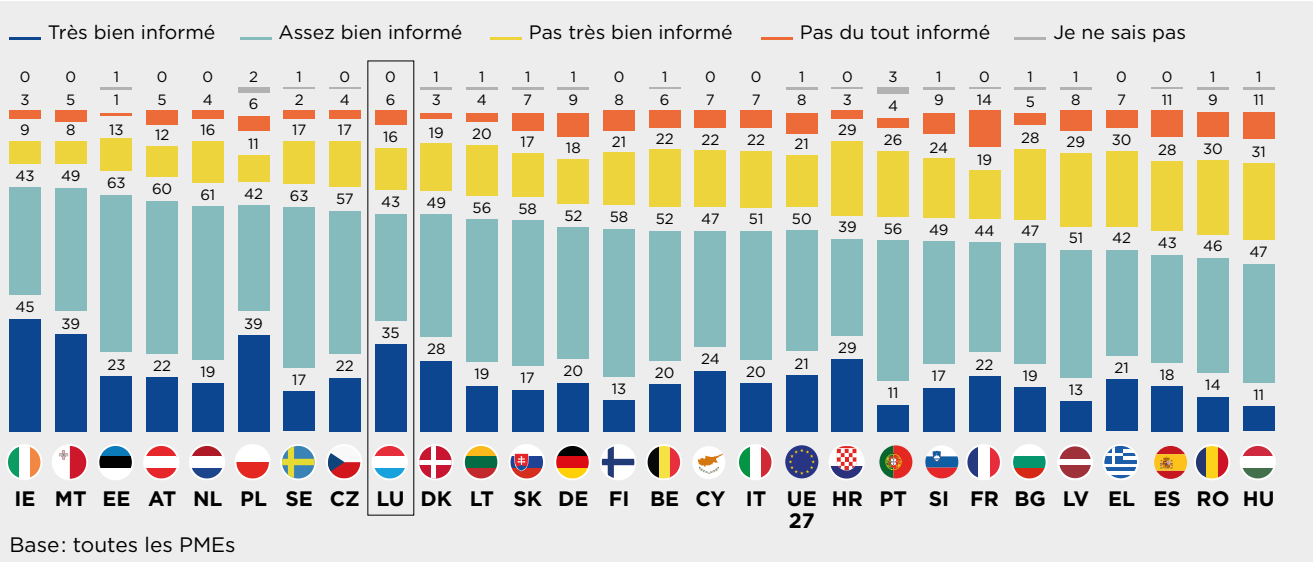
Nous évoluons dans une « data-driven economy ». Pour que la cybersécurité puisse se développer à la même vitesse et échelle, et soutenir ce modèle, la connaissance des menaces et des besoins en sécurité de l'information est indispensable.

19 *L'IoT, aussi connue sous le nom d'Internet des objets (Internet of Things en anglais) désigne l'existence d'objets connectés à Internet, tels que les objets dits "intelligents" (ex: montres et thermostats connectés, assistants vocaux…)*

Des progrès à faire en termes de sensibilisation par rapport à la sécurité informatique

Selon l'Eurobaromètre Flash 496 «SMEs and Cybercrime» publié par la Commission européenne en mai 2022 et basé sur des données recueillies entre novembre et décembre 2021, le Luxembourg (où les PME représentent 99% des entreprises) a un niveau de sensibilisation aux risques de cybersécurité relativement bon. Il se situe en effet en 8ème position dans l'Europe des 27 avec 78% des dirigeants de PME qui ont déclaré être «très bien» ou «assez bien» informés sur le sujet, contre une moyenne de 71% constatée dans la zone européenne.

DANS QUELLES MESURES VOUS SENTEZ-VOUS BIEN INFORMÉ PAR RAPPORT AUX RISQUES DE CYBERCRIMES? (% UE27)



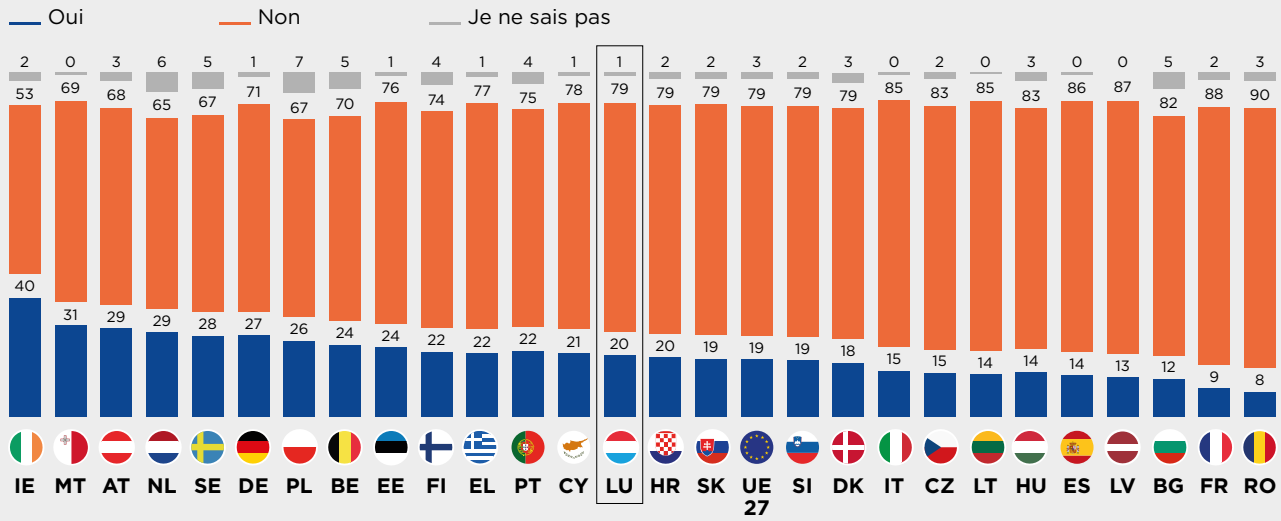
Base: toutes les PMEs

Source: Commission européenne, Eurobaromètre Flash 496 «SMEs and Cybercrime»

Comme une faille de cybersécurité chez une entité peu protégée peut être exploitée pour contaminer tout un système (fournisseurs, clients, partenaires commerciaux, administrations...), il est vital de renforcer la robustesse de la sécurité informatique à son maillon le plus vulnérable. Dans ce cadre, le Luxembourg pourrait renforcer sa résilience par rapport aux cyberattaques en améliorant le niveau de sensibilisation des entreprises qui se sont déclarées «pas très bien» (16%), voire «pas du tout» informées (6%) à ce sujet.

En outre, 79% des PME luxembourgeoises ont déclaré ne pas avoir, durant les 12 mois précédant l'enquête, fourni de formation ou de programme de sensibilisation à la cybersécurité à leurs employés. Cela fait ainsi pressentir l'existence potentielle d'un écart entre le niveau de sensibilisation à la cybersécurité perçue par les dirigeants et le niveau réel constaté sur le terrain.

DANS LES 12 DERNIERS MOIS, VOTRE ENTREPRISE A T'ELLE DISPENSÉ UNE FORMATION OU SENSIBILISÉ SES EMPLOYÉS AUX RISQUES LIÉS AUX CYBERCRIMES? (% PAR PAYS)



Source: Commission européenne, Eurobaromètre Flash 496 «SMEs and Cybercrime»

Pour aider le Luxembourg à renforcer sa cybersécurité afin qu'il reste compétitif dans un monde digitalisé, la Chambre de Commerce mène de front de nombreuses initiatives que cela soit sur le plan de la sensibilisation ou de l'acquisition de compétences.

Les initiatives de la Chambre de Commerce pour faire du Luxembourg une économie digitale résiliente

Pour aider les entreprises à renforcer leur résilience dans un monde digital, la Chambre de Commerce propose de nombreuses ressources et services dans le domaine de la cybersécurité. Dans le cadre des élections législatives de 2023, elle a par exemple publié le livret «Poser les fondations d'une data-driven economy compétitive et innovante», où elle a analysé l'état de la digitalisation au Luxembourg et proposé plusieurs recommandations. L'une d'elle[20] consiste à accélérer le développement d'un programme de type «Fit4» spécifiquement dédié à la cybersécurité et aux PME par le biais d'un partenariat public-privé, dans le but d'aider celles-ci à établir un diagnostic en matière de cybersécurité et de renforcer leur protection tout en finançant une partie de leurs dépenses.

20 Cette recommandation a été reprise par la Luxembourg House of Cybersecurity en tant qu'action à mettre en place dans la conclusion de son rapport «A Comprehensive Market Study on Cybersecurity Challenges and Opportunities within Luxembourg's SME sector».

LES SERVICES OFFERTS PAR LA CHAMBRE DE COMMERCE EN MATIÈRE DE CYBERSÉCURITÉ

 PUBLICATIONS	• **Livret élections 2023** « Poser les fondations d'une data-driven economy compétitive et innovante » • **Guide pratique** sur la cybersécurité • **Articles thématiques** divers (magazine MERKUR, presse)
 CONFÉRENCES & WORKSHOPS	• **Conférences Cybersecurity4Success** de l'Enterprise Europe Network (EEN) (en 2021 et 2022) • **Workshop « E-forum 2023 »** de la House of Entrepreneurship sur la sécurisation de l'e-commerce et la protection contre les fraudes en ligne (octobre 2023) • Accompagnement à des **foires** et **salons** (ex: Forum international de la cybersécurité)
 FORMATIONS & CONSEILS	• **Conseils** de la House of Entrepreneurship • **Formations en cybersécurité** de la House of Training (plus d'une vingtaine disponibles)
 RECHERCHE & ADVOCACY	• **Avis** relatifs aux **projets de lois** et aux **règlements grands-ducaux** • Participation à des **groupes de travail** relatifs à la cybersécurité • Participation à l'**enquête nationale** «A Comprehensive Market Study on Cybersecurity Challenges and Opportunities within Luxembourg's SME Sector» de la House of Cybersecurity (octobre 2023)
 PROMOTION DU LUXEMBOURG	• **Pavillon national** au **Forum international de la cybersécurité** à Lille (avril 2023) en collaboration avec la House of Cybersecurity et le ministère de l'Economie.

Messages clés

1. Le recours croissant aux technologies digitales s'est traduit par une multiplication des surfaces exposées aux cyberattaques qui ont connu une augmentation mondiale de l'ordre de 80 % entre 2017 et 2022[21].
2. Les attaques informatiques engendrent des coûts significatifs qui peuvent varier entre quelques milliers et plusieurs millions d'euros en fonction de variables telles que la taille de l'organisation, le secteur d'activité ou encore la nature et la gravité de l'attaque.
3. En matière de cybersécurité, le dicton « mieux vaut prévenir que guérir » s'applique, car se rétablir d'une attaque peut se révéler plus coûteux qu'investir dans des dispositifs robustes de défense.
4. L'écosystème luxembourgeois de cybersécurité est relativement bien positionné au niveau mondial, mais peut cependant être renforcé. Le facteur humain constitue notamment un risque majeur en termes de vulnérabilité informatique, puisqu'environ 2 tiers des cyberattaques constatées au Grand-Duché se révèlent être du « phishing ». Malgré cela, selon l'Eurobaromètre Flash 496 « SMEs and Cybercrime » publié par la Commission européenne en mai 2022 et basé sur des données recueillies entre novembre et décembre 2021, 79 % des PME luxembourgeoises ont déclaré ne pas avoir, durant les 12 mois précédant l'enquête, fourni de formation ou de programme de sensibilisation à la cybersécurité à leurs employés.
5. Pour aider les entreprises à renforcer leur résilience dans un monde digital, la Chambre de Commerce mène des initiatives diverses et variées et propose de nombreuses ressources dans le domaine de la cybersécurité.
6. La cybersécurité constitue un enjeu économique voué à gagner en importance dans les économies actuelles qui sont de plus en plus digitalisées. En tant que telle, elle ne peut plus être omise des stratégies des entreprises quels que soient leur taille et leur secteur d'activité.

Auteure : **Hoai Thu Nguyen Doan,** Affaires économiques, Chambre de Commerce
hoaithu.nguyen@cc.lu

21 Sonicwall (spécialiste en cybersécurité), « Cyber threat report », 2023.