Les Cahiers du Digital

#8

La cybersécurité

Enjeux pour l'économie wallonne, les PME industrielles et le secteur des cryptomonnaies

HEC LIÈGE
Management School - Liège Université

La collection *Les Cahiers du Digital* a pour but de présenter au public les enjeux majeurs de la transformation numérique en s'appuyant sur la contribution d'expert·es qui détiennent une connaissance de terrain reconnue en la matière.

Rédigés dans un style clair et abordable, et approfondissant chacun une thématique spécifique, ces cahiers s'adressent non seulement à nos étudiant·es, mais également à tout·e lecteur·trice désireux·se de s'informer sur ces enjeux, quel que soit son domaine d'expertise.

TABLE DES MATIÈRES

Les auteur·es **5**

Avant-propos **7**

Chapitre 1 - La cybersécurité et les PME **11**

Introduction 11

Qu'est-ce que la cybersécurité ? 12

PME et cybersécurité : carnet de route 13

TOP 5 des cyberattaques ciblant les PME 15

PME wallonne de demain : what's next ? 17

Conclusion 18

Chapitre 2 - Décrypter la cybersécurité pour mieux lutter contre les cybermenaces **21**

Introduction 21

La menace universelle de la cybercriminalité 21

PME et industries : des cibles faciles 22

La principale faille de sécurité…c'est vous ! 25

IA et cybersécurité, menace ou opportunité ? 26

Chapitre 3 - Règlements de Comptes à O.K. Corral : Bitcoin, Blockchain & Cybersécurité **31**

Introduction 31

Les concepts fondamentaux 31

Le cas du Bitcoin 34

La science du test logiciel 35

Résultats 38

Conclusion 39

Ressources utiles **43**

prix du mémoire en transformation digitale

Votre mémoire/TFE de Master :

- s'intéresse à la transformation digitale des organisations ou aux évolutions socio-économiques liées au numérique ?
- traite d'un enjeu numérique susceptible de contribuer au redéploiement économique de la Wallonie, même de manière indirecte ?
- a été défendu dans un des établissements d'enseignement supérieur de la Fédération Wallonie-Bruxelles ?

Donnez plus d'impact à votre mémoire/TFE !

memoire.bydw.be

Avec le soutien de la Wallonie — digital wallonia .be — LOUVAIN School of Management — Solvay Brussels School — HEC LIÈGE — Warocque — UNIVERSITÉ DE NAMUR

Les auteur·es

Jeremy Grandclaudon, Nina Hasratyan, Axel Legay & Lisa Lombardi

Jeremy Grandclaudon est expert en cybersécurité pour l'Agence du Numérique (ADN), où il responsable de la stratégie en cybersécurité pour la région wallonne via le programme Cyberwal by Digital Wallonia. Il a occupé diverses fonctions (chef de projet, responsable de programme, gestion d'incidents..) en cybersécurité depuis 2010. Ayant débuté dans le secteur privé, notamment dans le secteur bancaire chez ING mais aussi pour différents cabinets de conseil, il s'est ensuite orienté vers la recherche. Il a contribué, entre autres, au projet européen SPARTA pour la mise en place des NCC et de schémas de certification.

Nina Hasratyan est Cheffe de Projets pour Cyberwal by Digital Wallonia, la stratégie de cybersécurité de la Région Wallonne. Elle travaille également en tant que responsable des services de cybersécurité et de conseil en stratégie chez Approach Cyber. Les postes précédents incluent celui de responsable cyber et risque chez HeadMind Partners, responsable politique à la European Cyber Security Organisation (ECSO) et co-créatrice et coordinatrice opérationnelle de la Fondation Women4Cyber. En effet, alors qu'elle travaillait à l'ECSO, elle a contribué à la cocréation de Women4Cyber, et aujourd'hui elle est membre du Women4Cyber Council, l'entité de conseil stratégique de la Fondation. En 2022, Nina a été sélectionnée pour figurer dans la liste « Santander-CIDOB 35 Under 35 Future Leaders ».

Axel Legay est professeur à l'UCLouvain, où il dirige le laboratoire de cybersécurité et de vérification formelle. Il a obtenu son doctorat en informatique à l'Université de Liège. Il a également occupé un poste de post-doctorant à Carnegie Mellon sous la supervision d'Edmund M. Clarke (laureat du prix Turing). Il s'intéresse particulièrement à l'intégration de techniques d'intelligence artificielle dans les processus de validation de sécurité. Il est un fondateur et contributeur majeur du model checking statistique (une variante statistique du model checking largement utilisée dans l'industrie) qu'il a appliqué à divers problèmes de sécurité et de sûreté. Depuis 2021, Axel Legay dirige le programme de recherche CyberExcellence. Il est membre du conseil numérique du gouvernement wallon et des esprits numériques du gouvernement fédéral. Il est également président du conseil fédéral de la politique scientifique et a été désigné "Wallon de l'année" en 2023.

Lisa Lombardi est passionnée par l'entrepreneuriat, le développement des PME et le numérique. Elle occupe actuellement le poste de conseillère au sein de l'Union Wallonne des Entreprises (UWE), où elle met son expertise au service des entreprises wallonnes pour les aider à développer leur activité et à relever les défis du monde numérique en leur proposant des conseils personnalisés et un soutien concret, ou encore en animant des conférences et ateliers sur des thématiques liées à l'entrepreneuriat, aux PME et au numérique. Lisa assure également depuis son lancement le pilotage de l'axe « sensibilisation & accompagnement » du programme régional wallon pour la cybersécurité, Cyberwal by Digital Wallonia.

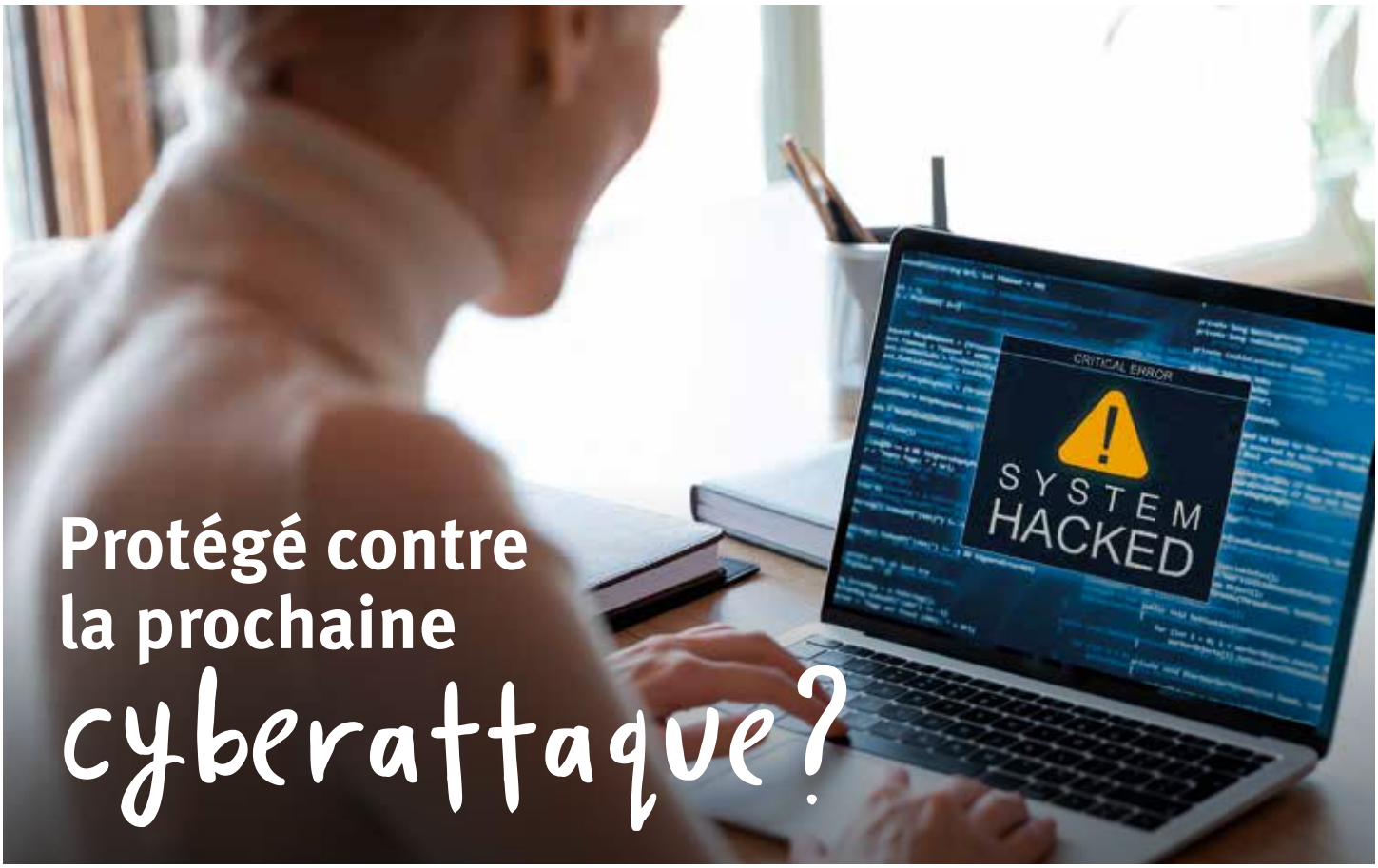
Jean-Philippe Parmentier

Jean-Philippe Parmentier est le directeur de l'INFOPOLE, un cluster qui regroupe plus de 120 entreprises et acteurs spécialisés dans le numérique. Il vise au développement et au rayonnement du secteur numérique wallon par la stimulation de l'innovation, la connexion des acteurs entre eux ou avec les autres secteurs de la demande et par la mise en avant de ces acteurs qui excellent dans leurs domaines mais sont trop peu connus ou reconnus. Avec son équipe, leurs membres et partenaires, l'INFOPOLE est un contributeur important dans la mise en œuvre de la stratégie Digital Wallonia.

Benoît Donnet & Vincent Jacquot

Benoit Donnet a obtenu son doctorat en informatique à l'Université Pierre et Marie Curie en 2006 et a effectué un postdoctorat jusqu'en 2011 à l'Université catholique de Louvain. Il a rejoint en 2011 l'Institut Montefiore de l'Université de Liège, où il a été nommé successivement Professeur assistant et Professeur associé. Ses recherches portent sur les mesures d'Internet, la modélisation des réseaux, la sécurité des infrastructures informatiques, les nouvelles architectures Internet et l'enseignement de l'informatique.

Vincent Jacquot a obtenu son master en informatique à l'Université de Liège en 2021. Après un court passage de 2 ans dans l'industrie, Vincent est revenu à Liège en 2023 pour y faire un doctorat. Ses recherches portent sur la sécurité des blockchains, systèmes décentralisées et smart contracts.



Protégé contre la prochaine cyberattaque ?

Ethias Cyber Security vous aide à y voir plus clair

L'actualité le montre régulièrement : la probabilité pour une organisation d'être victime d'une cyberattaque ou d'un virus est l'un des risques opérationnels majeurs du 21e siècle sur le plan informatique. **Le nombre de signalements de tentatives de phishing – fraude en ligne au moyen de faux courriels, sites ou messages – continue sa progression en Belgique.** Cette tendance à la hausse se confirme d'année en année : 10 millions de cas signalés sur la plate-forme safeonweb.be en 2023 (6 millions en 2022).

L'impact potentiel des cyberattaques est devenu chaque jour de plus en plus évident. Ces menaces sont non seulement capables de perturber les cyber-infrastructures, mais elles détruisent également l'intégrité, la disponibilité et la confidentialité des informations que nous enregistrons, analysons et échangeons sous forme numérique ; sans parler des risques financiers, réputationnels ou de confidentialité qu'elles englobent.

Ethias Cyber Security, une offre de services innovante

A travers différents niveaux d'analyse, l'objectif est de :

- vous accompagner dans la **sécurisation maximale** de votre environnement digital,
- définir avec vous les priorités,
- mettre en place les mesures appropriées pour r**éduire les failles potentielles** et les impacts liés aux actifs d'information.

Grâce au recours à des experts dans le domaine de la cyber prévention, Ethias Cyber Security propose un **service complet** intégrant notamment :

- un audit de la politique de prévention déjà existante,
- un accompagnement dans la mise en œuvre d'une politique de prévention,
- l'élaboration d'un plan de continuité des activités,
- l'élaboration d'un plan de gestion des incidents.

Découvrez notre catalogue de services sur solutions.ethias.be

Steve PIRET, Key Account Manager
rue des Croisiers 24 - 4000 LIÈGE
0474 42 71 87 - 04 220 31 31
steve.piret@ethias.be
ethiasservices@ethias.be

ethias Services

Ethias Services SA | Rue des Croisiers 24 | 4000 LIÈGE
RPM Liège TVA BE 0825.876.113 | IBAN : BE03 0688 9413 2384 | BIC : GKCCBEBB
Document publicitaire. Ne constitue pas une obligation contractuelle. E.R. : Yves Mélot

Avant-propos

Nicolas Neysen

Dans le monde interconnecté et numérique d'aujourd'hui, la cybersécurité émerge comme un impératif incontournable pour les entreprises, transcendant les frontières géographiques et les secteurs d'activité. Les avancées technologiques rapides et la prolifération des données numériques ont révolutionné la manière dont nous travaillons, communiquons et interagissons. Cependant, cette révolution numérique s'accompagne d'une face sombre, celle des cybermenaces, qui ne cessent de croître en complexité et en nombre.

Au vu de l'importance de la thématique, le Digital Lab ne pouvait ignorer cette réalité et c'est pourquoi il a été décidé de lui consacrer un numéro afin de jeter un coup de projecteur sur les enjeux cruciaux qui gravitent autour de la question, notamment vis-à-vis de l'économie wallonne.

Les entreprises wallonnes, parmi lesquelles les PME constituent l'épine dorsale de l'économie régionale (99.6% de toutes les entreprises), ne sont pas immunisées contre ces risques. Au contraire, elles deviennent des cibles de choix pour les cybercriminels en raison de leur vulnérabilité relative et de leur potentiel lucratif. Les statistiques révèlent une tendance inquiétante : les cyberattaques ont doublé entre 2019 et 2020, touchant jusqu'à 60 % des entreprises wallonnes, avec des conséquences parfois dévastatrices allant de pertes financières à la compromission de la réputation, en passant par une mise en danger de la confidentialité des données. Ce constat sera notamment approfondi dans le premier article de ce cahier. Ce dernier plonge en effet dans la réalité des PME en Wallonie, exposant les risques spécifiques auxquels elles sont confrontées et proposant des solutions pratiques pour renforcer leur posture de sécurité.

La cybersécurité ne se résume toutefois pas à des chiffres alarmants. C'est aussi une question de conscience et de préparation proactive. Les entreprises wallonnes doivent reconnaître l'urgence de la situation et entreprendre des actions concrètes pour se prémunir contre ces menaces omniprésentes. Cela implique non seulement des investissements dans des technologies de pointe – pas nécessairement onéreuses – et des stratégies de défense robustes, mais également un changement de mentalité et une sensibilisation généralisée à tous les niveaux de l'organisation. L'importance du facteur humain est d'ailleurs au cœur du second chapitre. Celui-ci explore en profondeur les différentes formes de cybermenaces, mettant en lumière les raisons de leur prolifération et offrant des stratégies concrètes pour contrer ces attaques, en mettant dès lors l'accent sur le rôle crucial de l'humain dans ce processus.

Enfin, ce cahier se clôture par une analyse critique de la technologie Blockchain sous l'angle de la cybersécurité. Bien que souvent perçue comme une innovation numérique révolutionnaire, la technologie de la blockchain et son application la plus emblématique, le Bitcoin, ne sont pas à l'abri des défis et des vulnérabilités. Contrairement à l'image largement répandue d'une technologie inviolable et infalsifiable, les auteurs apportent des preuves qui révèlent des failles potentielles et des risques inhérents à cette infrastructure décentralisée. Ce chapitre adopte donc un regard critique sur la blockchain et le Bitcoin, démystifiant au passage ces technologies souvent confondues l'une avec l'autre. Concrètement, les auteurs montrent comment une cyberattaque pourrait être montée contre l'infrastructure du Bitcoin pour voler de l'argent.

Au travers de ce cahier, nous espérons donc à nouveau offrir une perspective utile et pertinente, en croisant les regards des praticiens et experts de terrain d'une part, et des chercheurs universitaires d'autre part. À travers une exploration des principaux défis et des solutions existantes en matière de sécurité informatique, ce numéro vise à éclairer le lectorat dans un domaine qu'il n'est pas toujours simple d'appréhender.

Nous vous en souhaitons une bonne lecture !

Digital Transformation | Innovation | Change

HEC LIÈGE Management School - Liège Université | DIGITAL LAB

FORMATION

PROTÉGER SON ENTREPRISE DES ATTAQUES CYBER-CRIMINELLES

Les enjeux liés à la cybersécurité n'ont jamais été aussi importants qu'en ce moment. On le sait, la crise du Covid-19 a fortement contribué à l'augmentation des attaques criminelles sur Internet. Sécuriser un système d'information, c'est assurer l'intégrité, la confidentialité et l'accès à des données qui y sont stockées. Cette formation a pour but de montrer comment à la fois protéger ses données, mais aussi détecter des attaques potentielles et y faire face efficacement.

BÉNÉFICES POUR VOUS ET VOTRE ENTREPRISE

Pour moi

- Comprendre les cyberattaques au travers d'exemples d'attaques dites sociales (fishing) et techniques (backdoor) ainsi que leur combinaison.
- Distinguer les notions de vulnérabilité, de menace et d'attaque.
- Identifier les types de menaces, leurs objectifs, et le fonctionnement du marché des pirates.

Pour mon entreprise

- Anticiper les risques et impacts potentiels sur l'entreprise et sur la personne de l'employé.
- Évaluer son degré de maturité actuel face à la menace cybercriminelle.
- Disposer en interne de collaborateurs sensibilisés aux risques en matière de cybersécurité.

NOS EXPERTS

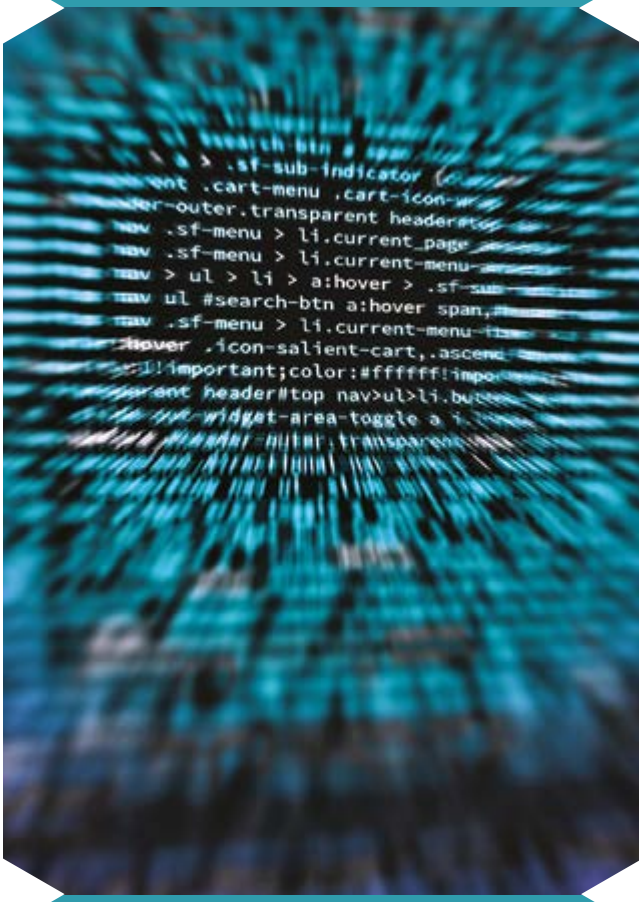
Axel Legay, professeur de cybersécurité à l'école polytechnique de l'UCLouvain. En tant qu'expert internationalement reconnu, il a été chargé à la fin du printemps 2020 de la mise en place de l'application de traçage digital en Belgique, dans le cadre de la lutte contre le Covid-19. Axel Legay est auteur ou co-auteur de plus de 300 articles scientifiques dans le domaine de la cybersécurité et de l'Internet des objets.

Sébastien Lugan, ingénieur et docteur en sciences de l'ingénieur. Il est chercheur senior à l'UCLouvain. Spécialiste en déploiement, sécurisation, supervision et audit des réseaux de communication, il encadre des cours de réseaux de communications à l'École Polytechnique de Louvain.

VERS LE SITE

HEC LIÈGE Management School - Liège Université | EXECUTIVE EDUCATION

EQUIS ACCREDITED · AACSB ACCREDITED · Qfor



Durée : 7 heures

Liège

CEO, CTO, Responsables IT, Cadres expérimentés, entrepreneurs, indépendants, chercheurs.

Français

Expert

Présentiel

Sophie Dumont
T. +32(0)4 232 73 79
s.dumont@uliege.be

La cybersécurité et les PME

CHAPITRE 1

Chapitre 1 - La cybersécurité et les PME

Jeremy Grandclaudon, Nina Hasratyan, Axel Legay & Lisa Lombardi

Introduction

La notion de « cybersécurité » est sur toutes les lèvres. Que l'on soit un citoyen, une PME, un service public, une ASBL ou une grande multinationale, nous faisons tous face aux mêmes dangers à partir du moment où nous sommes utilisateurs de produits digitaux.

Selon des chiffres de l'Union Wallonne des Entreprises (UWE), 99,6% des entreprises wallonnes sont des PME (petites et moyennes entreprises[1]), qui elles-mêmes emploient plus de 78% des salariés du secteur privé wallon (soit près de 579.000 personnes[2]). Mais nos PME sont-elles prêtes à faire face aux cybermenaces ? Se sont-elles posé les bonnes questions ? La prise de conscience de sa vulnérabilité face à la cybercriminalité et la réalisation que la cybersécurité concerne tout le monde, du plus petit au plus grand, est un processus long et ardu. Or, les cybercriminels n'attendent pas et sont au contraire à l'affût. D'autant plus que 2024 est une année cruciale pour la Belgique : élections fédérales, élections régionales, élections européennes, présidence belge du Conseil de l'Union européenne… La Belgique sera sous le feu des projecteurs, attirant l'attention sur ceux qui la composent et ses PME n'y feront pas exception.

Il est certain que le nombre de cyberattaques va de pair avec l'accélération de la digitalisation observée depuis la pandémie de Covid-19. À titre de référence, la Police fédérale constatait qu'en 2020, le nombre de cyberattaques avait doublé par rapport à l'année précédente[3] alors qu'en parallèle, la Fédération des Entreprises de Belgique (FEB) estimait qu'entre 40% et 60% des entreprises wallonnes auraient été victimes d'une cyberattaque[4].

Les conséquences peuvent être désastreuses : financières, économiques, réputationnelles, sociétales, sécuritaires. Les entreprises touchées peuvent subir une, plusieurs ou toutes ces conséquences en même temps. Selon le dernier sondage fait par Proximus, environ 38% des cyberattaques entraînent un arrêt d'activité pour les entreprises belges[5]. Dans la même lignée, l'OCDE, dans une étude réalisée en 2021[6], mentionne qu'une cyberattaque couronnée de succès impacte généralement plus lourdement les entreprises de plus petite taille que les grandes entreprises, ces dernières disposant de plus de ressources pour supporter les coûts liés à la récupération de leur système, les pertes financières occasionnées par un arrêt d'activité momentané ou pour faire face à une perte de crédibilité[7].

Toutefois, le critère des ressources ne suffit pas comme justification quant au manque de mesures de sécurité prises par les PME. La

1 Union Wallonne des Entreprises, « Les entreprises wallonnes en 12 questions », Edition 2020. https://www.uwe.be/wp-content/uploads/2020/10/Entreprise-2020.pdf (consultée le 6 décembre 2023).

2 Union Wallonne des Entreprises, « Les entreprises wallonnes en 12 questions », Edition 2023. https://indd.adobe.com/view/9e2e86b0-356f-48e8-9038-4d504a71195f (consultée le 6 décembre 2023).

3 Police Fédérale, « Statistiques de criminalité 2021 ». https://www.police.be/5998/fr/presse/statistiques-de-criminalite-2021#:~:text=En%202021%2C%20pas%20moins%20de,n%27a%20pas%20eu%20lieu (consultée le 6 décembre 2023).

4 CCILB, « Les cyberattaques deviennent de plus en plus courantes ». https://www.ccilb.be/fr/news/1911-cyber-attquaque-assurance#:~:text=Selon%20les%20donn%C3%A9es%20de%20la,en%20un%20an%20%C3%A0%20peine. (consultée le 6 décembre 2023).

5 Proximus, « Enquête : Comment les entreprises gèrent-elles la cybersécurité ». https://cybersecurity.proximus.be/rapport-d-enquete2021/rapport-denquete-cybersecurite (consultée le 6 décembre 2023).

6 OECD, « OECD Studies on SMEs and Entrepreneurship : The digital transformation of SMEs . https://www.oecd-ilibrary.org/industry-and-services/the-digital-transformation-of-smes_bdb9256a-en (consultée le 6 décembre 2023).

7 SPF Économie, « La cybersécurité au sein des PME belges ». https://economie.fgov.be/fr/themes/entreprises/pme-et-independants-en/digitalisation-des-pme/la-cybersecurite-au-sein-des (consultée le 6 décembre 2023).

> Une cyberattaque couronnée de succès impacte généralement plus lourdement les entreprises de plus petite taille que les grandes entreprises.

cybersécurité n'est pas qu'une question de moyens techniques. Il s'agit de processus de résilience et de consolidation continus, ainsi que d'un ensemble de bonnes pratiques à mettre en place.

Si, comparé aux PME, les grandes entreprises ont plus des ressources pour se relever d'une cyberattaque, le degré de préparation en amont est une toute autre affaire. Parfois, il suffit de quelques gestes faciles et pratiques à mettre en place pour rendre la tâche des cybercriminels plus difficile.

Qu'est-ce que la cybersécurité ?

Avant même de considérer les ressources nécessaires pour se préparer à d'éventuelles cyberattaques, il est surtout crucial de comprendre ce qu'est la cybersécurité et ce qu'elle englobe.

Selon le Center for Cybersecurity Belgium (CCB[8]), l'agence de la cybersécurité belge dépendant du Cabinet du Premier Ministre[9], « la cybersécurité est le résultat d'un ensemble de mesures de sécurité qui doivent minimiser le risque d'accès perturbé et non-autorisé aux systèmes d'information et de communication (TIC)[10] ».

Mais qu'entend-t-on par un « ensemble de mesures » exactement ? Toujours selon ce rapport du CCB, cela englobe à la fois des protections techniques que des précautions organisationnelles. « L'expérience a démontré que seule une approche holistique à la cybersécurité peut permettre à une entreprise ou organisation d'augmenter ses chances de protection et de minimiser la possibilité de se faire attaquer. »

Ainsi, poussant le raisonnement plus loin dans sa stratégie, le CCB mentionne que la « cybersécurité englobe toutes les mesures raisonnables et acceptables destinées à protéger les TIC des citoyens, des entreprises, des organisations et des pouvoirs publics contre les cybermenaces. Il s'agit de la protection des systèmes (tels que le matériel, les logiciels et les infrastructures connexes), des réseaux, ainsi que des données qu'ils contiennent[11] ».

Pour atteindre un degré de protection suffisant, les mesures techniques requièrent la recherche et la mise en place des outils le plus performants sur le marché – et cela ne signifie pas nécessairement des coûts astronomiques car il existe de nombreuses solutions *open source* accessibles gratuitement – tels que des logiciels pour une authentification multi-facteurs, un anti-virus ou anti-malware, etc. Les mesures organisationnelles impliquent la mise en place d'une gouvernance solide à l'échelle de l'entreprise couvrant les différentes politiques et procédures que cette dernière établit afin d'homogénéiser et de systématiser ses efforts de cybersécurité. Cela nécessite également de se pencher sur un autre point majeur qui est la sensibilisation de tout le personnel à de bonnes pratiques de cyber-hygiène[12].

8 Centre for Cybersecurity Belgium (CCB). https://ccb.belgium.be/fr (consultée le 20 décembre 2023).

9 CCB, « Stratégie Cybersécurité Belgique 2.0 2021-2025 ». https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_FR_DP2.pdf (consultée le 20 décembre 2023).

10 *Ibid.*

11 *Ibid.*

12 Note de l'éditeur: La cyberhygiène est un principe fondamental en matière de sécurité de l'information et, comme le montre l'analogie avec l'hygiène personnelle, équivaut à la mise en place de mesures de routine simples pour minimiser les risques liés aux cybermenaces. Source : European Union Agency for Network and Information Security (ENISA). *Review of Cyber Hygiene practices*. 2016. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport (consulté le 15 avril 2024). Traduit de l'anglais par l'éditeur.

PME et cybersécurité : carnet de route

Le message le plus important est donc que les PME doivent entamer leur démarche en vue de se cybersécuriser, si pas dès leur création, alors le plus rapidement possible, car les mesures techniques et organisationnelles doivent faire partie intégrante de leur fonctionnement journalier. En somme, être proactifs, plutôt que réactifs. Oui, mais comment ? Par où commencer ?

> Les PME doivent entamer leur démarche en vue de se cybersécuriser, si pas dès leur création, alors le plus rapidement possible.

Pour cela, plusieurs acteurs en Wallonie œuvrent, ensemble, à la mise en place et à la facilitation de programmes de sensibilisation et d'accompagnement.

Cyberwal by Digital Wallonia

Comme cheffe de file, porteuse du programme Cyberwal by Digital Wallonia (Cyberwal by DW[13]), la stratégie en matière de cybersécurité de la Région wallonne, l'Agence du Numérique (AdN) œuvre à la mise en place de différents événements, campagnes, projets et outils, ainsi qu'à la centralisation de différentes offres de formations en cybersécurité en Wallonie. C'est surtout au travers de son Pilier 1 « Sensibilisation et outillages[14] » que Cyberwal by DW offre aux PME un « parcours de cybersécurité » fait de cinq étapes majeures :

1. s'informer/se former et se familiariser avec les termes et enjeux de la cybersécurité ;
2. définir ses objectifs de cybersécurité et son périmètre, à savoir ce qui doit être protégé ;
3. mettre en place des mesures organisationnelles en prévoyant un premier plan d'action, en attribuant des rôles et en mettant par écrit les procédures-clés (type politique de sécurité) ;
4. faire un état des lieux en faisant des analyses de risques et de maturité, pour pouvoir mieux identifier ses cyberattaques en cas d'incident ;
5. mettre en place d'autres mesures organisationnelles et des mesures techniques en fonction de l'état des lieux pour aller plus loin dans la démarche.

Ce guide contient les 5 étapes-clés du parcours de cybersécurité qui serviront de ligne directrice aux PME. Chacune de ces étapes a des possibilités infinies, une vaste documentation disponible en ligne, et une fois les premières étapes franchies, les PME pourront faire appel à des experts en cybersécurité au travers du programme Chèque-entreprises[15]. Grâce à ce programme, la Région intervient à hauteur de 75% dans l'aide aux PME qui décident de faire appel à des prestataires de services en cybersécurité[16].

UWE : Commission Numérique

Cyberwal by DW n'agit pas seul ; il centralise tout un réseau de partenaires privilégiés sur l'ensemble de la Wallonie, dont l'Union wallonne des Entreprises (UWE)[17]. L'UWE, qui compte 6.000 entreprises membres de toutes tailles et émanant de tous secteurs, implantées dans les quatre coins de la Wallonie, agit comme la courroie de transmission des grandes législations et projets wallons et travaille avec ses membres à bâtir des positions reflétant les réelles attentes des

13 Cyberwal by Digital Wallonia. https://www.digitalwallonia.be/cyber (consultée le 8 janvier 2024)

14 Digital Wallonia, « Cyberwal by Digital Wallonia. Pilier 1. Sensibilisation et accompagnement ». https://www.digitalwallonia.be/fr/publications/cyberwalbydw-sensibilisation/ (consultée le 8 janvier 2024).

15 Chèques-entreprises Cybersécurité. https://www.cheques-entreprises.be/cheques/cybersecurite/ (consultée le 8 janvier 2024).

16 Digital Wallonia, « Aides à la transformation numérique : le dispositif des chèques-entreprises ». https://www.digitalwallonia.be/fr/publications/aides-transformation-numerique/ (consultée le 8 janvier 2024).

17 Union Wallonne des Entreprises (UWE). https://www.uwe.be/ (consultée le 6 décembre 2023).

entreprises. En tant que cheffe de file du pilier « Sensibilisation » de Cyberwal by DW, l'UWE déploie des efforts de coordination et de mise en œuvre d'actions visant à informer le plus possible les entreprises wallonnes des menaces liées à la cybercriminalité. Au travers de sa Commission Numérique[18], elle favorise l'échange d'expériences et de conseils entre responsables d'entreprise afin de conscientiser et d'outiller un maximum de CEO wallon·nes.

Conseils pratiques

De manière très pratique et en lien avec le parcours de sécurité évoqué précédemment, voici quelques conseils concrets afin d'augmenter la résilience de sa PME :

1. **Sensibiliser le personnel** : Les membres du personnel sont souvent la première ligne de défense contre les cyberattaques. Il est important de les sensibiliser aux risques de sécurité informatique et de leur fournir une formation régulière sur les bonnes pratiques de cybersécurité.
2. **Mettre en place une politique de sécurité informatique**: Les PME doivent élaborer une politique de sécurité informatique claire et la communiquer à tout le personnel. Cette politique doit inclure des mesures de sécurité telles que l'utilisation de mots de passe forts, la mise à jour régulière des logiciels et la sauvegarde régulière des données.
3. **Utiliser des outils de sécurité**: Les PME doivent utiliser des outils de sécurité tels que des antivirus, des pare-feu et des logiciels de détection des intrusions pour protéger leurs systèmes informatiques.
4. **Effectuer des sauvegardes régulières des données**: Les PME doivent effectuer des sauvegardes régulières de leurs données pour éviter de perdre des informations importantes en cas d'attaque.
5. **Mettre en place des procédures d'urgence**: Les PME doivent élaborer des procédures d'urgence pour faire face aux cyberattaques. Ces procédures doivent inclure des plans de continuité des activités et des plans de reprise après sinistre.
6. **Faire appel à des experts en cybersécurité**: Les PME peuvent faire appel à des expert·es en cybersécurité pour les aider à élaborer une politique de sécurité informatique efficace et à mettre en place des mesures de sécurité appropriées.

Les membres du personnel sont souvent la première ligne de défense contre les cyberattaques. Il est important de les sensibiliser aux risques de sécurité informatique

18 UWE, « Commission Numérique ». https://www.uwe.be/participez-a-la-nouvelle-commission-numerique-de-luwe/ (consultée le 6 décembre 2023).

TOP 5 des cyberattaques ciblant les PME

Si de nombreuses PME sont encore réfractaires aux mesures de cybersécurité qu'elles devraient mettre en place pour protéger leurs activités, c'est parce qu'elles sont convaincues d'être trop petites pour attirer l'attention des acteurs malveillants et pensent passer sous leur « radar ». Malheureusement, c'est une ligne de pensée entièrement erronée qui leur donne un faux sentiment de sécurité.

Cependant, le risque zéro n'existe pas – c'est l'une des règles d'or de la cybersécurité. En effet, si, auparavant, mener une cyberattaque réussie requérait des compétences pointues de la part des cybercriminels, aujourd'hui, la situation a bien changé grâce à de nombreuses offres de services disponibles gratuitement sur le *dark web*. Cela augmente le nombre d'acteurs malveillants, et par corrélation les chances pour toute entreprise de se faire attaquer. A titre d'exemple, « l'employé moyen d'une petite entreprise de moins de 100 salariés pourrait subir 350 % d'attaques de *social engineering* de plus qu'un employé d'une grande entreprise[19] ».

Si certaines cyberattaques sont grandioses et font les titres dans les médias (c'est le cas notamment avec les grandes entreprises), dans la réalité il en faut beaucoup moins pour qu'une cyberattaque impacte les activités d'une entreprise et la continuité de son business. En 2023, une société américaine a publié le top 6 des cyberattaques les plus communes ciblant les PME[20]. Si la dernière attaque du top 6 est plus pointue, les 5 premières restent des notions connues et dangereuses pour toute entreprise.

Ransomware (ou rançongiciels)

Selon la définition du CCB[21], « un ransomware est un logiciel malveillant (malware) qui encrypte les données des utilisateurs dans l'idée de leur restituer leurs données ultérieurement en échange d'une rançon. Dans les cas extrêmes, le ransomware bloque l'accès au système informatique en encryptant également des données vitales au bon fonctionnant dudit système. Le ransomware n'est pas un phénomène nouveau, mais la menace qu'il représente a connu une croissance exponentielle au cours de ces dernières années ». Il serait logique de penser que les acteurs malveillants préféreraient s'attaquer à de larges entreprises pour des plus grosses sommes d'argent. Toutefois, ces dernières coopèrent rarement. Alors que le triste constat est que ces acteurs savent que les PME vont payer pour récupérer leurs données, car l'alternative serait la faillite.

Attaques contre la chaîne d'approvisionnement

Dans notre monde ultra-connecté, la cybersécurité ne s'arrête pas aux frontières numériques de l'entreprise mais continue avec les partenaires tiers. Le CCB définit cette problématique de la manière suivante [22]: « La sécurité de la chaîne d'approvisionnement consiste en la sécurisation des actifs et des services tout au long du cycle de vie d'un système (conception, développement, élaboration, conditionnement, assemblage, distribution, intégration au système, gestion opérationnelle, entretien et mise hors service) ».

Dans ce genre d'attaques, les PME sont, en général, les victimes indirectes d'une attaque contre une large entreprise dont elles sont l'un des fournisseurs. Et, à nouveau, si une cyberattaque contre une large entreprise

19 Barracuda, « Pourquoi la cyber-résilience est-elle importante pour les PME et comment y parvenir ? ». https://fr.blog.barracuda.com/2023/05/22/why-cyber-resilience-matters-smbs (consultée le 20 décembre 2023).

20 Jumpcloud, « 6 Common Cyberattacks That Threaten SMEs ». https://jumpcloud.com/blog/common-sme-cyberattacks (consultée le 20 décembre 2023).

21 CCB, « Ransomware Protection et prévention ». https://ccb.belgium.be/sites/default/files/Ransomware_2019_FR.pdf (consultée le 13 décembre 2023).

22 CCB, « Lignes directrices « gestion sécuritaire de la chaîne d'approvisionnement » - Supply Chain Proces – 2020 ». https://ccb.belgium.be/sites/default/files/Supply%20Chain%20Proces%20FR%20-%20Lignes%20directrice%20gestion%20s%C3%A9curitaire%20de%20la%20chaine%20dapprovisionnement%20edition%202020.pdf (consultée le 23 novembre 2023) .

peut lui faire mal, elle peut généralement s'en remettre, contrairement à une PME, pour laquelle cela signifierait devoir mettre la clé sous la porte.

Phishing et ses variantes

Ce type d'attaque est un classique indémodable et défini comme suit par le SPF Économie[23] : « Le phishing est une fraude en ligne par laquelle des escrocs usurpent l'identité d'une personne, d'une entreprise, d'une organisation bien connue de tous (banques, fournisseurs d'énergie, opérateur téléphonique...) ou encore d'une institution publique comme b-post ou le SPF Finances par exemple. Ils envoient des messages (via SMS, e-mails ou réseaux sociaux) en leur nom afin d'extorquer des informations personnelles, des données bancaires ou de contaminer un ordinateur avec un virus ou un logiciel malveillant ».

C'est l'une des attaques privilégiées des acteurs malveillants car elle est facile à déployer et s'appuie sur l'erreur humaine. Or, les PME avec des ressources restreintes sont en majorité peu sensibilisées aux principes de cyber-hygiène, et leur personnel est donc plus vulnérable et plus susceptible de tomber dans le piège d'une attaque d'ingénierie sociale.

Exploitation de vulnérabilités dans les logiciels

Une vulnérabilité informatique est un défaut de sécurité, présent à la conception ou après une mise à jour et qui peut se situer dans une application, un logiciel ou dans un composant matériel. Ces failles peuvent aussi provenir des utilisateurs et de leur façon de se servir des outils informatiques. Très souvent, les vulnérabilités exploitées dans les logiciels sont connues et publiées. Toutefois, si les grandes entreprises ont des procédures de gestion des correctifs[24] connues et bien implémentées, une grande majorité des PME n'applique pas ces règles de cyber-hygiène de base. Ce qui fait qu'elles continuent à utiliser des logiciels avec un potentiel vulnérable, les rendant elles-mêmes vulnérables à des cyber-attaques.

Piratage de comptes

Si un système est trop simple ou mal configuré, des attaquant·es pourraient facilement y avoir accès après avoir simplement piraté le compte d'un·e utilisateur·rice/employé·e. Le piratage des comptes peut se faire de nombreuses manières, y inclus grâce à un logiciel de vol de mots de passe, l'ingénierie sociale[25], ou en achetant sur le *dark web* les identifiants de comptes précédemment piratés. Une fois un compte piraté, l'attaquant·e peut simplement naviguer dans tout le réseau de l'entreprise ou organisation sous le nom de l'utilisateur·rice dont l'identité a été usurpée, rendant ce genre d'attaques difficilement détectables.

Ces différents types d'attaques et leurs impacts démontrent que leurs conséquences peuvent être désastreuses pour toute PME qui en serait victime. Toutefois, un autre dénominateur commun est qu'elles pourraient aussi facilement être évitées (ou rendre la tâche des attaquants beaucoup plus ardue) en mettant en place de simples mesures préventives, comme celles décrites précédemment.

23 SPF Économie, « Phishing ». https://economie.fgov.be/fr/themes/protection-des-consommateurs/arnaques-la-consommation/formes-darnaques/vous-avez-recu-un-message/vous-avez-recu-un-message-dun#:~:text=Le%20phishing%20est%20une%20fraude,le%20SPF%20Finances%20par%20exemple. (consultée le 22 novembre 2023) .

24 Note de l'éditeur: La gestion des correctifs ou, en anglais, « *patch management* », est le processus d'identification, d'acquisition, d'installation et de vérification des correctifs pour les produits et les systèmes. Les correctifs corrigent les problèmes de sécurité et de fonctionnalité des logiciels et des microprogrammes. Source: Souppaya, Murugiah., & Scarfone, K. (2012). *Guide to enterprise patch management technologies (draft) recommendations of the National Institute of Standards and Technology* (Revision 3, draft.). U.S. Dept. of Commerce, National Institute of Standards and Technology. https://www.govinfo.gov/content/pkg/GOVPUB-C13-PURL-gpo28901/pdf/GOVPUB-C13-PURL-gpo28901.pdf (consulté le 15/04/2024). Traduit de l'anglais par l'éditeur.

25 Note de l'éditeur : Le *social engineering* est une technique utilisée par les cybercriminels pour tromper les individus afin de leur soutirer des informations confidentielles. Source : https://www.digitalwallonia.be/fr/agenda/social-engineering-comment-proteger-vos-employes-et-votre-entreprise/ (consultée le 15 avril 2024).

PME wallonne de demain : what's next ?

Si aujourd'hui, la majorité des PME ne se pense pas concernée par la cybersécurité, la donne est déjà en train de changer. L'Union européenne œuvre en continu pour la mise en place de législations en cybersécurité afin de faire de ses États-Membres des acteurs majeurs de la cybersécurité. En 2016 déjà, l'UE votait pour l'implémentation de la Directive NIS[26], transposée dans la loi belge en 2019[27], couvrant la sécurité des Opérateurs de Services Essentiels. En 2022, la Directive NIS 2[28] a été votée, avec pour vocation de remplacer la Directive NIS de 2016. Sa portée sera beaucoup plus conséquente car le nombre de secteurs a été élargi de sept à quinze, et couvre non seulement les OES (*Original Equipment Suppliers*) mais également toute entreprise, y inclus PME, qui est enregistrée comme fournisseur d'un opérateur important ou d'un opérateur essentiel, y compris critique. La Directive NIS 2 n'est pas la seule législation qui va concerner les PME. Voici trois textes législatifs qui sont en cours de finalisation dans les institutions européennes et qui devront être suivis de manière rapprochée : le *Cyber Resilience Act* (CRA[29]), le *Data Act*[30], et le *Artificial Intelligence Act* (AI Act[31]).

Mais entre les cyberattaquants et des exigences de conformité de plus en plus lourdes, comment les PME peuvent-elles sortir leur épingle du jeu ? A quoi peuvent-elles aspirer pour devenir la PME idéale en termes de cybersécurité en Wallonie ? Nous avons déjà évoqué cinq

L'Union européenne œuvre en continu pour la mise en place de législations en cybersécurité afin de faire de ses États-Membres des acteurs majeurs de la cybersécurité.

26 Parlement européen, « Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ». https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148 (consultée le 08/01/2024).

27 Le Moniteur Belge, « Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique », 7 avril 2019. https://www.ejustice.just.fgov.be/doc/rech_f.htm (consultée le 08/01/2024).

28 Parlement européen, « Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union ». https://eur-lex.europa.eu/eli/dir/2022/2555 (consultée le 08/01/2024).

29 Parlement européen, « Horizontal cybersecurity requirements for products with digital elements ». https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act (consultée le 08/01/2024).

30 Parlement européen, « Data act ». https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act (consultée le 08/01/2024)

31 Parlement européen, « Artificial intelligence Act ». https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence (consultée le 08/01/2024).

bonnes pratiques dans cet article, première étape dans le parcours en sécurité d'une PME, mais il faut pouvoir aller plus loin.

Afin de mettre en place ces notions, dans un deuxième temps, les PME peuvent aussi s'appuyer sur des boites à outils comme « la Boîte à outils de cybersécurité pour petites entreprises » de la GCA[32]. Ce type de boite à outils permet aux entreprises de passer d'un concept parfois nébuleux (surtout dans son implémentation) à une série d'outils concrets, gratuits et facilement disponibles : comment dresser son inventaire IT, comment sécuriser sa messagerie ou mettre en place une stratégie de sauvegarde efficace, entre autres. Grâce à cette deuxième étape, la PME peut commencer à mettre en place des solutions concrètes et réduire son exposition aux risques cyber.

La troisième étape consiste dans la systématisation de cette démarche afin de s'appuyer sur un cadre plus formel comme le « *CyberFundamentals Framework*[33] » (CyFun), proposé par le CCB afin de répondre à trois objectifs essentiels pour la sécurité d'une entreprise :

- protéger les données ;
- réduire de manière significative le risque des cyberattaques les plus courantes ;
- accroître la cyber-résilience d'une organisation.

Il existe quatre niveaux de complexité dans le CyFun – *Small*, *Basic*, *Important*, *Essential* – qui comprennent chacun un nombre de contrôles incrémentaux selon le niveau, afin de permettre aux entreprises et organisations de faire une évaluation de leur maturité. Ainsi, ce n'est pas nécessairement la taille de l'entité qui va déterminer le niveau du CyFun à utiliser, mais le niveau de maturité. Dans le cas qui nous occupe, une PME n'ayant aucun contrôle de sécurité en place devra commencer par le niveau *Small* afin de mettre en place les fondamentaux de la cybersécurité avant même de penser à des choses plus poussées. A l'inverse, une PME, tout aussi petite, mais qui a un certain nombre de contrats et qui est fournisseur d'un opérateur important ou opérateur essentiel, identifié comme tel dans le cadre de la Directive NIS 2, devra avoir un niveau de maturité et de contrôles mis en place suffisamment élevés et consolidés pour lui permettre de maintenir son statut de fournisseur.

Conclusion

Dans cet article, nous avons pu examiner la résilience des PME wallonnes face aux principales cyberattaques et les différentes ressources à leur disposition pour améliorer leur posture en cybersécurité.

A cet effet, il est particulièrement important de remettre l'accent sur les activités de sensibilisation, surtout si elles sont relayées via des acteurs de confiance, car elles jouent un rôle essentiel en aidant les PME dans leurs démarches de cybersécurité et permettent d'établir un climat de confiance et de partage d'information.

Il est essentiel pour toute entreprise de se préparer à l'éventualité d'une cyberattaque, aussi bien pour limiter les coûts que pour mieux y résister, plutôt que de jouer à la politique de l'autruche et la subir de plein fouet. Comme mentionné en amont, pour réduire au maximum ce risque, il existe de nombreuses ressources, certaines présentées ici, qui permettent de mieux s'outiller pour répondre aux défis modernes en cybersécurité. Toutes ces initiatives ont un coût, visible et invisible, et les PME n'ont pas des ressources illimitées. C'est pourquoi il existe en Wallonie des possibilités de financement destinés à aider les entreprises à franchir le pas et/ou à continuer leurs efforts en matière de cybersécurité.

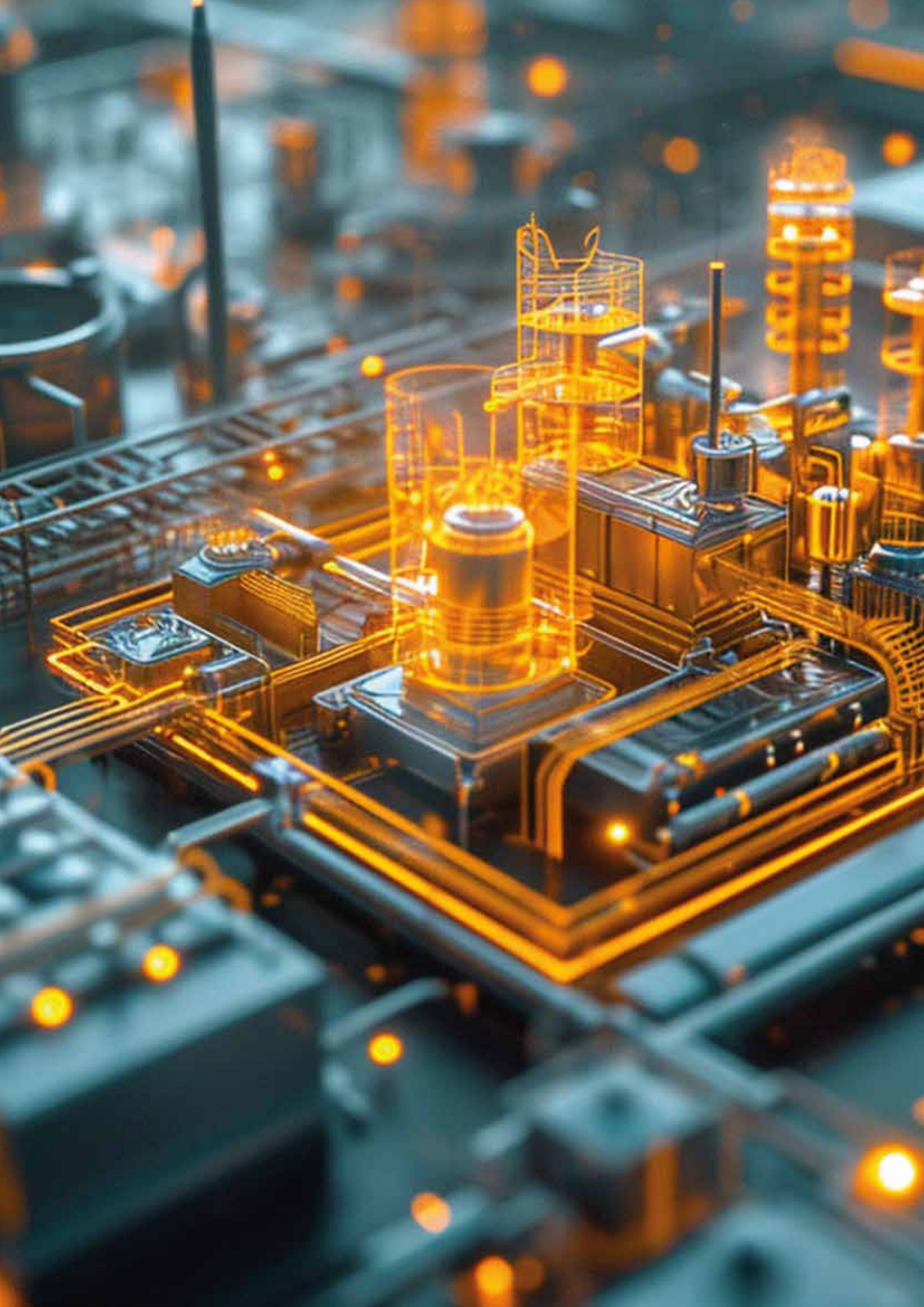
D'année en année, le nombre de cyberattaques ne fait que croître ; le temps des hésitations est révolu. La cybersécurité est l'affaire de tous.

32 Global Cyber Alliance (GCA), « Boîte à outils de cybersécurité pour petites entreprises » . https://gcatoolkit.org/fr/petites-entreprises/ (consultée le 10 janvier 2024).

33 CCB, « CyberFundamentals Framework ». https://atwork.safeonweb.be/fr/tools-resources/cyberfundamentals-framework (consultée le 08/01/2024).

Décrypter la cybersécurité pour mieux lutter contre les cybermenaces

CHAPITRE 2



Chapitre 2 - Décrypter la cybersécurité pour mieux lutter contre les cybermenaces

Jean-Philippe Parmentier

Introduction

Dans un monde et une société de plus en plus connectés, la cybersécurité est devenue une préoccupation majeure pour tout le monde : citoyen·nes, entreprises et services publics. Malgré cela, les cyber-attaques se multiplient, elles pleuvent de toutes parts, elles sont de plus en plus importantes et frappent tout le monde, sans distinction. Cela suscite de la stupeur, de l'incompréhension et surtout beaucoup de questions, comme par exemple : « pourquoi y a-t-il de plus en plus d'attaques alors que nous sommes – en théorie – de mieux en mieux protégés ? », « quelle est la part de responsabilité de l'Humain par rapport aux failles techniques ? », « par où commencer pour me protéger ? », « l'IA va-t-elle nous aider à lutter contre les menaces ou au contraire empirer les choses ? », etc.

Ce chapitre vise à répondre à ces différentes questions en apportant un éclairage sur la réalité des menaces de cybersécurité qui pèsent sur tout le monde. La première partie présentera les principales raisons de l'explosion des menaces. Notamment, elle mettra en évidence la vulnérabilité particulière des PME et du secteur industriel et les conséquences qu'elle peut avoir sur leur santé ou survie.

La seconde partie se penchera sur le rôle de « l'Humain », qu'il ou elle soit citoyen·ne, employé·e ou responsable d'entreprise. Une meilleure compréhension de son rôle et de ses moyens d'actions est cruciale pour le transformer en premier rempart pour limiter et contrer les attaques comme le *social hacking*.

Enfin, la troisième partie abordera brièvement le rôle de l'IA dans la création de nouvelles menaces. Elle s'attardera davantage sur les opportunités que peuvent représenter ChatGPT et consorts en tant qu'alliés dans la lutte contre la cybercriminalité.

La menace universelle de la cybercriminalité

Piraterie : une histoire vieille comme le monde

Les premiers actes de piraterie maritime remontent à l'Antiquité et ont évolué à travers le temps pour prendre différentes formes : Illyriens, Vikings, corsaires, Barberousse, Barbe Noire pour les plus célèbres. La piraterie maritime persiste encore aujourd'hui, notamment dans les eaux du Golfe d'Aden et de la mer Rouge, utilisant des moyens techniques et technologiques qui rivalisent avec ceux d'une armée conventionnelle. Cette piraterie moderne représente une menace sérieuse dont les armateurs de bateaux peinent à se prémunir totalement.

Il en est de même pour les voleur·ses et cambrioleur·ses qui ont traversé les époques et ont − à peu de chose près − toujours touché tout le monde : riches propriétaires, diligences, transports de fonds, banques, musées, voitures, commerces, château, villas, maisons, appartements, facteur·ices, pensionné·es, jeunes ados, etc. N'épargnant personne, pas même les plus modestes, ils visent tantôt de véritables trésors, tantôt des sommes plantureuses, tantôt des butins dérisoires.

Avec les différentes évolutions technologiques qui ont conduit à la dématérialisation des valeurs et titres de propriété, à la dépendance accrue aux outils numériques, à l'essor de l'économie de la donnée, à la multiplication des transactions en lignes et dématérialisées, les pirates, toujours assoiffés par l'appât du gain (de préférence facile et à faible risque), ont trouvé dans cet univers numérique un nouveau terrain de jeu qui leur offre un nombre incalculable d'opportunités : vol de données ou d'identifiants, usurpation d'identité, blocage de

systèmes, extorsion de fonds, arnaques à la carte de crédit, rançons, etc.

Une menace grandissante

Les chiffres et les statistiques en matière de cybersécurité mettent en lumière le fait que les attaques et les menaces sont de plus en plus nombreuses et de mieux en mieux élaborées. Ils soulignent l'omniprésence des cybermenaces et la probabilité élevée que nous serons toutes et tous touchés un jour. Dès lors, autant s'y préparer !

En effet, selon Statbel[1] et Proximus[2] qui ont réalisé tous les deux des études récentes sur des panels significatifs d'entreprises de toutes tailles :

- Une entreprise sur trois a connu un incident de cybersécurité en 2022. Ce chiffre est d'une sur quatre pour les PME
- Le nombre d'attaques est en augmentation de 37% depuis 2019
- 70% des PME sont préoccupées par les menaces et incidents en cybersécurité
- 22% des attaques proviennent du *social engineering*, 15% via des *ransomwares*
- 33% des attaques-touchent des ordinateurs fixes et individuels
- 1/3 des incidents empêchent les membres du personnel de travailler durant quelques heures/jours, et dans 1 cas sur 5, cela les empêche de travailler pendant plusieurs semaines/mois.
- 37% des incidents coûtent plus de 10.000€, et dans 10% des cas cela grimpe à plus de 100.000€

Ces chiffres permettent d'objectiver quelque peu une réalité que nous connaissons à travers le prisme des médias, où il est rare qu'une semaine se passe sans qu'une cyberattaque ne fasse les gros titres. Cependant, cette réalité médiatique n'est que la partie émergée de l'iceberg. Car bon nombre de structures

> Une entreprise sur trois a connu un incident de cybersécurité en 2022. Ce chiffre est d'une sur quatre pour les PME.

touchées préfèrent ne pas ébruiter les ennuis rencontrés et garder l'anonymat pour ne pas nuire à leur réputation.

Ce nombre relativement élevé de personnes ou d'entreprises touchées confirme ce que nous constatons de manière très fréquente parmi nos proches sur les réseaux sociaux qui sont régulièrement victimes de hacking de leurs comptes ou de leurs boîtes de messagerie. En plus de cela, il faut ajouter les arnaques en ligne, qui se font plus discrètes, les victimes préférant généralement, elles aussi, garder l'anonymat.

PME et industries : des cibles faciles

Les PME sont-elles plus vulnérables ?

De manière générale, les PME sont en moyenne moins avancées en termes de maturité numérique que les plus grandes entreprises. Ce retard se confirme également dans le domaine de la cybersécurité. Elles sont donc potentiellement plus vulnérables et constituent des proies plus faciles que les grandes entreprises. Comme indiqué ci-dessus, les chiffres montrent que, pour le moment, les PME sont un peu moins touchées que les plus grandes entreprises.

Par ailleurs, les pirates ont généralement tendance à s'attaquer aux maillons les plus vulnérables d'une chaîne. Les PME, étant en en contact avec de plus grandes entreprises (fournisseurs, sous-traitants, partenaires, etc.),

1 Proximus (2022), L'impact de la cybersécurité sur les entreprises du Benelux. https://cybersecurity.proximus.be/rapport-d-enquete-2022/des-resultats.

2 Statbel (2022), enquête sur la sécurité dans les entreprises.

peuvent donc servir de point d'accès idéal pour toucher ces dernières. De même, avec l'évolution et le renforcement du niveau général de la sécurité des entreprises, en particulier celles de plus grande taille, les PME les moins sécurisées deviennent des cibles de choix car elles sont des proies plus faciles. Il serait donc présomptueux et très dangereux de penser qu'elles sont à l'abri de cette menace.

Enfin, comme le montre une étude de l'OCDE[3], une cyberattaque réussie menace plus lourdement la continuité des entreprises de plus petite taille car celles-ci ont moins de ressources financières pour faire face aux coûts directs et indirects de l'attaque : arrêt des activités ou perte de crédibilité.

Se préoccuper de leur cybersécurité est donc un enjeu très important pour les PME, en particulier pour celle qui ont un (trop) faible niveau de protection et de sécurité.

Pourquoi les entreprises industrielles sont-elles particulièrement touchées ?

Les entreprises avec une activité industrielle présentent des caractéristiques et un profil spécifique qui les rendent particulièrement vulnérables. C'est la raison pour laquelle elles sont soumises à un grand nombre d'attaques et ce nombre est en augmentation constante depuis plusieurs années. Passons à présent en revue quelques éléments expliquant leur plus grande vulnérabilité.

1. La transition vers une Industrie 4.0

En se transformant pour coller au modèle de l'industrie 4.0[4], les industriels ont connecté et interconnecté l'ensemble de leurs systèmes et équipements. Ils recourent de manière intensive à des appareils connectés de type Internet des Objets (ou IoT pour *Internet of Things*) pour piloter, surveiller, monitorer et contrôler leur système de production. L'utilisation d'ordinateurs, de tablettes et autres équipements portables, de robots et de cobots, de machines-outils connectées s'est généralisée sur les sites de production. Ces technologies ont également permis à des partenaires d'intervenir à distance ou au personnel de piloter et de gérer l'usine depuis des sites extérieurs à celle-ci.

Ces transformations profondes de leur manière de fonctionner ont mis fin, de manière irréversible, à ce fonctionnement « en vase clos », qui les avaient relativement épargnés jusque-là des attaques. Cette connectivité accrue et l'accroissement du nombre et de

Cette connectivité accrue et l'accroissement du nombre et de la diversité des équipements ont eu pour conséquence d'augmenter de manière significative la surface d'exposition des industries aux cybermenaces.

3 OCDE (2021), The digital Transformation of SMEs, studies on SMEs and Entrepreneurship. https://www.oecd.org/publications/the-digital-transformation-of-smes-bdb9256a-en.htm.

4 Pour plus d'informations sur l'Industrie 4.0 et ses enjeux, voir les Cahiers du Digital #1 et #2 disponibles en français et en anglais sur www.digitallab.be/publications.

la diversité des équipements ont eu pour conséquence d'augmenter de manière significative la surface d'exposition des industries aux cybermenaces et de les rendre particulièrement vulnérables car elles n'y étaient pas correctement préparées.

2. La rencontre entre l'IT et l'OT

Bien que les acronymes soient proches, l'IT (*Information Technology*) et l'OT (*Operational Technology*) appartiennent à des mondes très différents. Tout d'abord, ils ont évolué au fil du temps de manière indépendante et avec des objectifs bien distincts : les systèmes IT se concentrent sur la gestion de l'information que l'on retrouvera dans l'entreprise mais généralement en dehors des sites de production. Pour faire simple et de manière un peu caricaturale dans « les bureaux » (ex : finance, stock, *supply chain*, gestion des clients, etc.). L'OT, quant à lui, se concentre sur la gestion et le contrôle des processus de production.

Chacun de ces deux mondes comprend ses propres outils, ses propres modes de fonctionnement et ses propres contraintes. L'IT aura une préférence pour des systèmes plus agiles, plus rapide, plus adaptables tandis que l'OT mettra l'accent sur la robustesse, la disponibilité continue et la sécurité des processus de production. Cette opposition de style se marque également au niveau de leurs champs lexicaux respectifs[5].

Compte tenu de ces différences quasiment « philosophiques », ces deux « mondes » ont/avaient jusqu'à présent des approches très différentes de la cybersécurité. Aujourd'hui, pour protéger de manière efficace les sites industriels, de nouvelles pratiques et méthodes doivent voir le jour. Des efforts mutuels de collaborations doivent naître au sein des équipes afin que celles-ci agissent comme une équipe unifiée, avec une approche plus globale de la cybersécurité.

3. Des infrastructures vieillissantes et obsolètes

La majorité des industries utilise des systèmes informatiques et des équipements industriels qui ont été mis en place il y a de nombreuses années, c'est-à-dire bien avant l'existence des premières cyberattaques industrielles. Cette situation de relative obsolescence, d'évolution technologique limitée et de rareté des mises à jour découle directement du mode de fonctionnement de l'OT, mais aussi, plus globalement, du besoin de l'industrie de produire en continu – l'état d'esprit général étant « tant que ça marche bien, surtout on ne touche à rien ! ».

Dès lors, comme le montre une étude d'Agoria[6], il n'est pas rare que les responsables ne sachent pas quel est l'âge approximatif des plus anciens PLC (31% des cas), utilisent des PLC (ou automate programmable industriel) qui ont dix ans ou plus (35%) ou laissent tourner des systèmes d'exploitation sous de vieux Windows (25%, dont 3% de MS-DOS, 9% de Windows 2000 et 13% de Windows XP, soit une entreprise sur 4 avec un OS vieux de plus de 20 ans). Enfin, 48% d'entre eux ne procèdent jamais, ou rarement, à des mises à jour de leur système.

4. Un manque de connaissance et de compétences en cybersécurité industrielle

Comme nous l'avons détaillé ci-dessus, le monde industriel était jusqu'à présent peu ou moins concerné par la cybersécurité. De ce fait, il souffre d'un manque de culture, de stratégie ou de sensibilisation aux bonnes pratiques pour diminuer les risques.

En témoignent les chiffres de l'étude Agoria :

- 64% des répondant·es indiquaient ne pas avoir de politique de sécurité pour l'OT alors qu'ils en ont une pour l'IT.

5 Pour l'OT : Scada, PLCs, DCS, RTU, MES, PAC, PID, IACS, ICS, etc. Pour l'IT : IP, Infra, VPN, Cloud, SQL, ERP, CRM, Java & Python, web-based, etc. Nous ne détaillons pas l'ensemble de ces abréviations ici. Elles sont données à titre illustratif pour faire comprendre au lectorat qu'il s'agit quasiment de deux langues et donc de deux mondes différents.

6 Agoria (avril 2021), La sécurité Industrielle dans l'industrie manufacturière. https://www.agoria.be/fr/etude-Cyber-securite-dans-industrie-manufacturiere

- 55% des répondant·es n'envisageaient pas de norme relative à sécurité OT.
- 45% ne tiennent pas compte des recommandations et des risques de sécurité partagés par leurs équipementiers.

> 45% des responsables d'entreprises ne tiennent pas compte des recommandations et des risques de sécurité partagés par leurs équipementiers.

On peut toutefois supposer que ces chiffres sont aujourd'hui différents et qu'ils évoluent positivement, même s'ils restent préoccupants. Les attaques récentes dans le secteur industriel, couplées aux différentes initiatives des acteurs privés et publics, ainsi que le développement d'une offre de cybersécurité industrielle ont permis de sensibiliser le secteur et d'augmenter le niveau de compétences. Cependant, malgré ces initiatives et améliorations, le niveau de cybersécurité reste « trop » faible dans le secteur.

5. Manque de vision stratégique

Enfin, élément non négligeable, certains pointent le sous-investissement dans la cybersécurité comme cause principale des difficultés du secteur. Ce phénomène résulte, en général, d'un manque de vision stratégique ou d'un manque d'intégration de cette thématique à la stratégie globale de l'entreprise. Dès lors, la cybersécurité est davantage vue comme un coût non productif que comme un investissement garantissant la continuité des opérations et le bon fonctionnement de l'usine.

Les conséquences d'une attaque dans le domaine industriel peuvent être particulièrement lourdes. La moindre interruption d'une ligne de production peut entraîner des pertes conséquentes de chiffre d'affaires. Par ailleurs, un arrêt (même très court) peut nécessiter une relance complète des installations, ce qui prend du temps, génère des rebuts et/ou nécessite une série de vérifications. Ces pertes ou manques à gagner, peuvent mettre l'entreprise en grande difficulté financière en cas d'arrêt prolongé, ou pire, l'entraîner vers la faillite. Cela a notamment été le cas pour des entreprises comme Asco, Picanol group, Mondelez, Renault-Nissan, Norsk Hydro qui ont fait l'objet d'attaques et ont été mises à l'arrêt pendant plusieurs jours/semaines/mois. Leurs valorisations financières ont subi de très nettes diminutions dans les jours et mois qui ont suivi ces attaques.

Ces conséquences financières sont parfois « un moindre mal » comparativement à celles liées aux risques de divulgation de secrets de fabrication, la dégradation de la réputation de l'entreprise ou des dommages encore plus graves comme des accidents industriels mettant en danger l'intégrité physiques des ouvriers.

La principale faille de sécurité…c'est vous !

Un bon système de cybersécurité repose sur plusieurs piliers : la mise en place d'une politique de sécurité, la protection (technique) des systèmes et des réseaux, ainsi que la gestion des actions et la détection des vulnérabilités.

Un pilier fondamental et souvent négligé est la bonne formation et la sensibilisation du personnel aux bonnes pratiques et aux risques cyber. Ils sont la première ligne de défense de l'entreprise. Une grande majorité des attaques trouvera sa réussite en exploitant une faille humaine dans le dispositif de protection : divulgation d'identifiants et d'accès, partage d'informations sensibles ou données non protégées, utilisation de mots de passe trop peu robustes, clic sur des liens malveillants ou téléchargement de logiciels corrompus.

Le *social hacking* est un terme générique utilisé pour décrire l'ensemble des menaces qui tentent d'abuser des personnes en profitant de leur crédulité ou manque de vigilance. Ces menaces ont généralement pour objectif d'usurper une identité, des données personnelles, des données bancaires, des codes d'accès, etc.

Le *phishing*[7] (ou « hameçonnage ») est une technique par laquelle le·la cybercriminel·le tente d'obtenir des informations confidentielles. Dans la très grande majorité des cas, il·elle utilisera un e-mail pour arriver à ses fins. Des SMS et des appels téléphoniques, voire même des QR Codes, sont aussi utilisés pour mener ce type d'attaque. En général, le message contient un lien vers un site web frauduleux ayant l'apparence d'un site légitime où vous devez encoder vos logins et mots de passe, votre numéro de carte de banque, etc. Informations que les pirates récupéreront pour accomplir leurs méfaits.

Certains e-mails contiennent une pièce jointe ou demandent le téléchargement d'une application. Dans ce second mode d'action, le pirate installera un virus pour accéder à votre ordinateur. Cela lui permettra, en fonction de ses objectifs, de collecter toutes vos données personnelles, de bloquer votre appareil, d'accéder à vos différents comptes ou bien encore de se propager à travers le réseau et les applications utilisées par votre entreprise. Plus récemment, les pirates utilisent des messages envoyés via MS Teams ou utilisent l'envoi d'e-mail/invitation à travers les agendas partagés pour envoyer une URL ou des fichiers infectés.

L'ingéniosité n'a pas de limite et se renouvelle sans cesse. La vigilance est plus que jamais de rigueur. De plus, avec l'essor de l'IA générative, les pirates évoluent et se professionnalisent. Leurs e-mails sont de plus grande qualité, davantage personnalisés à votre situation, les rendant dès lors plus difficilement détectables.

IA et cybersécurité, menace ou opportunité ?

L'intelligence artificielle (IA) générative connaît un développement spectaculaire ces derniers mois. Une grande série d'outils très simples à utiliser ont ainsi vu le jour. ChatGPT, bien entendu, mais aussi Google Bard, Midjourney, Dall-E, HeyGen, Adobe Firefly, etc. Ces outils sont capables de générer du contenu de plus en plus réaliste, y compris pour des utilisations malveillantes. Que ce soit en matière de diffusion de *fake news*, *deep fake*, mails de *phishing* ou autres arnaques en tout genre, l'usage de l'IA générative est de nature à produire des contenus davantage crédibles, rendant plus que jamais difficile la distinction entre le vrai et le faux.

Le *phishing* (ou « hameçonnage ») est une technique par laquelle le·la cybercriminel·le tente d'obtenir des informations confidentielles.

De multiples autres utilisations frauduleuses voient le jour. Elles concernent également des dimensions plus techniques où les pirates vont

7 Pour plus de détails et d'informations : https://safeonweb.be/fr/apprenez-reconnaitre-les-e-mails-frauduleux

tenter d'entrer dans les systèmes ou de les pirater en générant des virus ou malwares, en analysant les failles des codes et systèmes, en générant des attaques plus sophistiquées, etc.

Ceci dit, bien que ces outils puissent être à l'origine de nouvelles attaques ou les renforcer, ils peuvent également contribuer à s'en prémunir et à augmenter le niveau de cybersécurité des personnes et des organisations. En voici quelques exemples :

- **Détection des tentatives de *phishing*** : Par l'analyse des e-mails et messages reçus, de leur contenu tant sur le fond que sur la forme, des modèles d'IA peuvent être entrainés spécifiquement pour détecter ce type de menace. L'utilisation de l'IA permet d'identifier des « patterns » ou caractéristiques communes à travers les milliers d'e-mails reçus (URL ou e-mail « exotiques », fautes d'orthographe, type de demande, etc.). Elle permet aussi de prendre des actions *ad hoc* en fonction de la menace : blocage d'URL, suppression de pièce jointe, désactivation des accès ou plus simplement signalement aux personnes en charge de la sécurité informatique.

- **Détection de « *fake news* », « *deep fake* » et autres faux contenus** : De manière similaire à ce qui est fait pour le *phishing*, l'IA permet de détecter des contenus (texte, audio ou vidéo) qui auraient été falsifiés. Cette détection se base sur plusieurs éléments :
  - des anomalies ou incohérences : ombre ou reflet incohérents avec la prise de vue, déformation des objets, visage ou partie du corps (par ex : une main à 6 doigts), objet ou personne qui ne sont pas en lien avec le reste de l'image, etc.
  - des incohérences techniques : compression d'image particulière, succession de pixels trop uniformes ou au contraire trop différents,
  - l'analyse des métadonnées du fichier : information sur l'appareil utilisé, ses paramètres, les angles ou la focale utilisés, la date et heure, etc. Par une analyse poussée de ces informations et leur recoupement, certains modèles d'IA peuvent détecter des images ou vidéos falsifiées

- **Identification des failles dans du code et dans des systèmes IT** : L'IA peut être utilisée de manière proactive et en amont des attaques, pour analyser en profondeur du code, pour détecter des failles de sécurité, des erreurs de programmation ou des configurations lacunaires qui pourraient être exploitées par des cybercriminels.

- **Détection des virus** : Par l'analyse du comportement d'un système IT ou d'un processus, par l'identification de comportements suspects ou par l'analyse de la signature des virus connus (comme le font aujourd'hui la plupart des antivirus), un modèle d'IA entrainé spécifiquement à cette tâche peut, sur base de ces connaissances et ses capacités d'apprentissage en temps réel, identifier et détecter des virus existants et même identifier de nouveaux virus qui sont jusque-là encore inconnus.

- **Monitoring de l'activité d'une entreprise** : L'IA a la capacité d'analyser des grandes quantités de données, de les croiser et peut, même en cas de signaux dits « faibles », identifier des tentatives de hacking. Des modèles ont aujourd'hui la capacité d'analyser un grand nombre de paramètres pour identifier des activités suspectes en se basant sur des journaux d'activités, des logs, des connexions ou tentatives de connexions, les IP utilisées, l'utilisation de la bande passante ou l'utilisation de ressources physiques (CPU, GPU, mémoire, réseaux, etc.), les comportements des machines et des utilisateur·ices, etc.

Outre ces capacités importantes pour détecter des menaces, l'IA permet aussi de réagir en temps réel pour contrer les menaces ou en limiter les impacts négatifs en activant ou désactivant des accès ou systèmes, en changeant des paramètres, en bloquant des ports ou adresses IP, en désactivant des comptes ou utilisateurs, etc.

Une fois de plus, il s'agira d'une course perpétuelle entre « policier et voleur ». Ces

derniers tenteront à chaque fois d'avoir un coup d'avance pour commettre des attaques et arnaques sans se faire prendre. Pour les « policiers » et les victimes, il s'agira, sur base de leurs (mauvaises) expériences et apprentissages, de détecter les tentatives de fraude et de tout faire pour limiter les impacts négatifs de ces attaques. Et idéalement, de les éviter en adoptant une véritable politique de cybersécurité[8].

8 Vous ne savez pas par où commencer ? Une liste de ressources utiles pour améliorer votre cybersécurité vous est proposée en page 43.

Règlements de Comptes à O.K. Corral : Bitcoin, Blockchain & Cybersécurité

CHAPITRE 3

Chapitre 3 - Règlements de Comptes à O.K. Corral : Bitcoin, Blockchain & Cybersécurité

Benoît Donnet et Vincent Jacquot

Introduction

En 2008, une alternative au système bancaire, rédigée par une personne se présentant sous le pseudonyme de «Satoshi Nakamoto», était proposée[1]. Cette alternative, nommée Bitcoin[2], consiste en un système de paiement digital. Ce système permet à deux individus de s'échanger de l'argent sans impliquer la participation d'une autorité centrale, mais en passant par un livre de compte distribué, la *blockchain*[3].

Peu de gens avaient alors réalisé que cette alternative serait l'étincelle à l'origine d'une succession d'innovations technologiques. Aujourd'hui, le Bitcoin s'invite dans toutes les discussions : des boursicoteurs[4] du dimanche s'échangeant leurs astuces aux plus hautes sphères politiques, en passant par le monde criminel. Cependant, force est de constater que les termes « *blockchain* », « cryptomonnaie », « Bitcoin » et autres sont malheureusement souvent utilisés de manière interchangeable.

Dans cet article, nous proposons de démystifier ces termes, mais aussi de rendre accessibles les concepts techniques sur lesquels Bitcoin est bâti, à savoir : la *blockchain*, les algorithmes de consensus, le minage, les signatures digitales, etc.

Nous souhaitons également dissiper certaines prétendues vérités au sujet du Bitcoin. Souvent perçu comme inviolable, Bitcoin n'en reste pas moins sensible aux cyberattaques. Nous verrons notamment, comment une cyberattaque pourrait être montée contre l'infrastructure du Bitcoin pour voler de l'argent.

> Souvent perçu comme inviolable, Bitcoin n'en reste pas moins sensible aux cyberattaques.

Les concepts fondamentaux

Au commencement était la fonction de hachage

Il serait impossible de décrire convenablement les composants sur lesquels est bâti le Bitcoin sans parler des *fonctions de hachage*. Ces fonctions, dans le sens mathématique du terme, permettent d'assigner une valeur, appelée résumé ou encore hachage, à des données de taille arbitraire. Formulé autrement, une fonction de hachage condense n'importe quelle quantité de données en un nombre. Un exemple, illustrant la fonction de hachage MD5, est fourni ci-dessous. Cette fonction attribue un nombre (voir *output*) compris entre zéro et 2^{128} -1 à toute donnée passant par cette fonction (*input*). Par exemple : en hachant la phrase « Le monde se divise en deux catégories », on obtient la valeur 242.764.306.336.737.911.699 .793.470.266.177.972.672.

Mais le concept ne se limite pas à condenser l'information contenue dans une phrase, il est possible de hacher une image, un film, un programme, etc. En d'autres termes, n'importe quelle représentation binaire d'une information peut être hachée (voir figure1).

1 Nakamoto Satoshi, « Bitcoin: A Peer-to-Peer Electronic Cash System. », Livre blanc, Organisation Bitcoin, octobre 2008, disponible à l'adresse suivante : https://bitcoin.org/bitcoin.pdf (consultée le 10 janvier 2024).

2 Mot anglais résultant de la contraction de *bit*, la plus petite unité de données en informatique, et de *coin*, pièce de monnaie.

3 En français : chaîne de blocs

4 Personne impliquée dans l'achat ou la vente de petites quantités mobilières en Bourse.

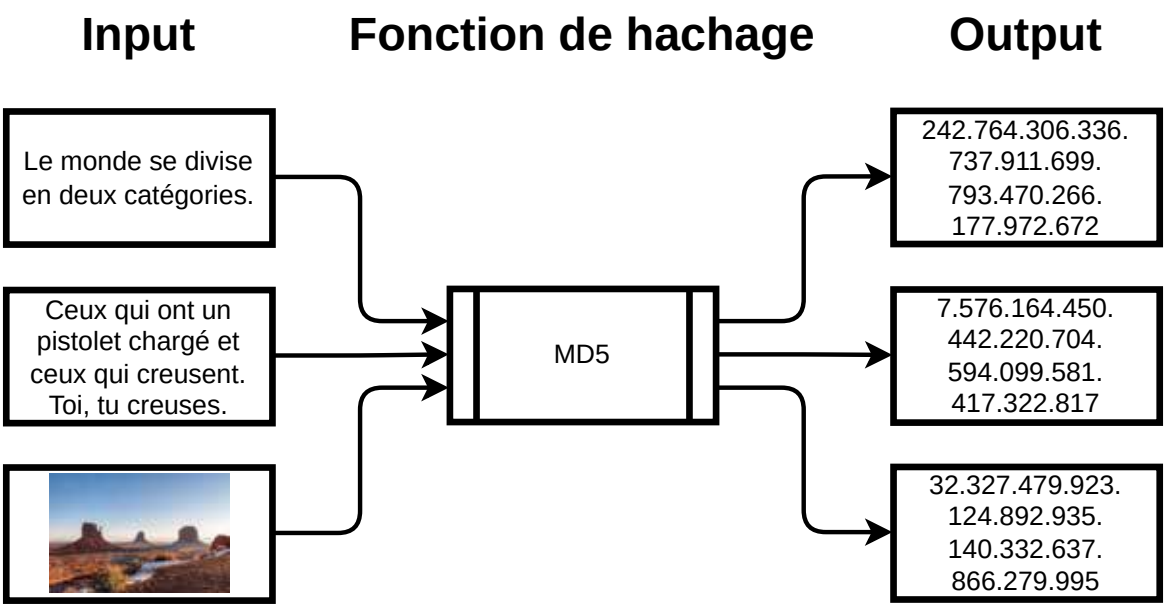


Figure 1

Si l'on considère le fait que la valeur de sortie est restreinte à un intervalle (c'est-à-dire un nombre fini de valeurs possibles) et que les valeurs d'entrée sont non restreintes (on peut générer une infinité de textes différents), il apparaît évident qu'il existe nécessairement des valeurs d'entrée différentes qui produisent la même valeur de hachage. Ce phénomène est appelé *collision*.

Une bonne fonction de hachage doit satisfaire de nombreuses propriétés que nous omettons volontairement dans cette publication, afin de nous concentrer sur deux propriétés essentielles à la compréhension de ce qui suit.

1. Tout changement, même infime, dans la valeur d'entrée doit générer une valeur de sortie complètement différente. Dans notre exemple, la modification d'un seul pixel de l'image étant hachée, doit produire une valeur de hachage complètement différente.
2. Étant donnée une valeur de hachage h et une fonction de hachage $hash$, il doit être difficile (au sens mathématique du terme) de trouver des données $data$ tel que $hash(data) = h$. Cela signifie qu'il doit être difficile de trouver une donnée qui permette de générer une collision.

Ensuite vint la blockchain

La *blockchain* est une structure de données stockant l'information en différents blocs et protégeant l'intégrité de celle-ci à l'aide des fonctions de hachage. Dans le cadre de données, l'intégrité peut être définie comme la capacité à garantir que celles-ci n'ont pas été modifiées par d'autres personnes que son auteur. Prenons l'exemple illustré ci-dessous. Les données ont été réparties entre 3 blocs. En plus de contenir des données, chaque bloc contient la valeur de hachage du bloc précédent. Par exemple, le bloc 1 contient la valeur de hachage des données du bloc 0: H_1. De même, le bloc 2 contient la valeur de hachage des données du bloc 1 et de H_1. Et ainsi de suite (voir figure 2).

L'inclusion de ces valeurs de hachage permet de vérifier l'intégrité des données. Prenons l'exemple illustré ci-dessous et supposons qu'une tierce partie ait modifié les données dans le bloc 0, cette modification peut être aisément détectée grâce à la valeur de hachage stockée dans le bloc 1. En effet, de par les propriétés exposées précédemment, il doit être pratiquement infaisable pour cette tierce personne de modifier les données du bloc 0 sans en changer la valeur de hachage.

Néanmoins, le lecteur averti remarquera que cette tierce personne pourrait alors modifier

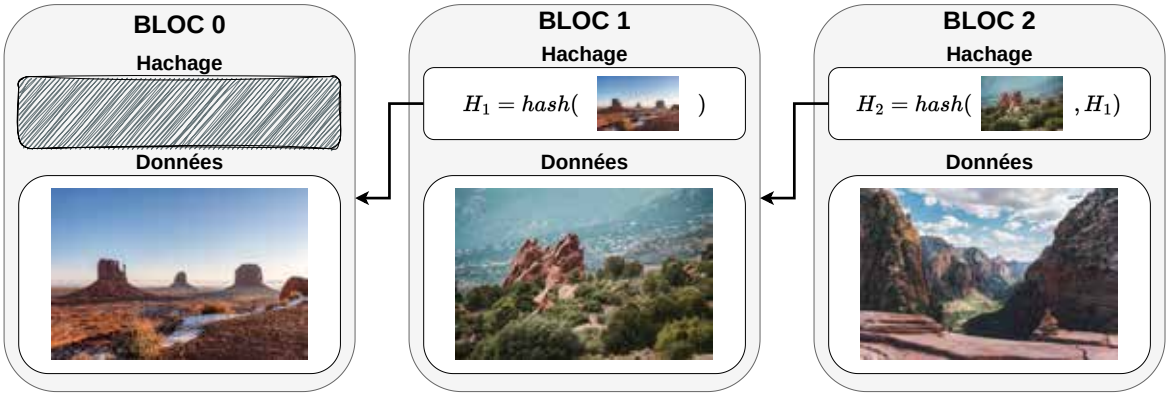


Figure 2

la valeur H_1 afin d'occulter cette modification dans le bloc 0. Ce faisant, H_2 et la valeur de hachage du bloc 1 ne correspondraient plus, l'obligeant ainsi à modifier le bloc 2 et tous les blocs suivants (voir figure 3).

Finalement, il est important de noter que les *blockchains* ne sont pas inhérentes au concept de crypto-monnaie, de décentralisation ou de Bitcoin. En effet, d'après Alan Sherman *et. al.*[5], cette structure de données trouverait ses origines dans une publication de David Chaum datée de 1982[6].

Signature numérique

Afin de conclure cette section sur les concepts fondamentaux, attardons-nous sur le concept de *signature numérique* qui est un mécanisme permettant d'authentifier l'auteur d'un document électronique. Une signature numérique comporte des propriétés analogues à celles d'une signature manuscrite sur un document papier :

- elle doit permettre au lecteur d'authentifier la personne ayant apposé sa signature ;
- elle doit être infalsifiable, personne ne doit pouvoir reproduire la signature d'un autre ;

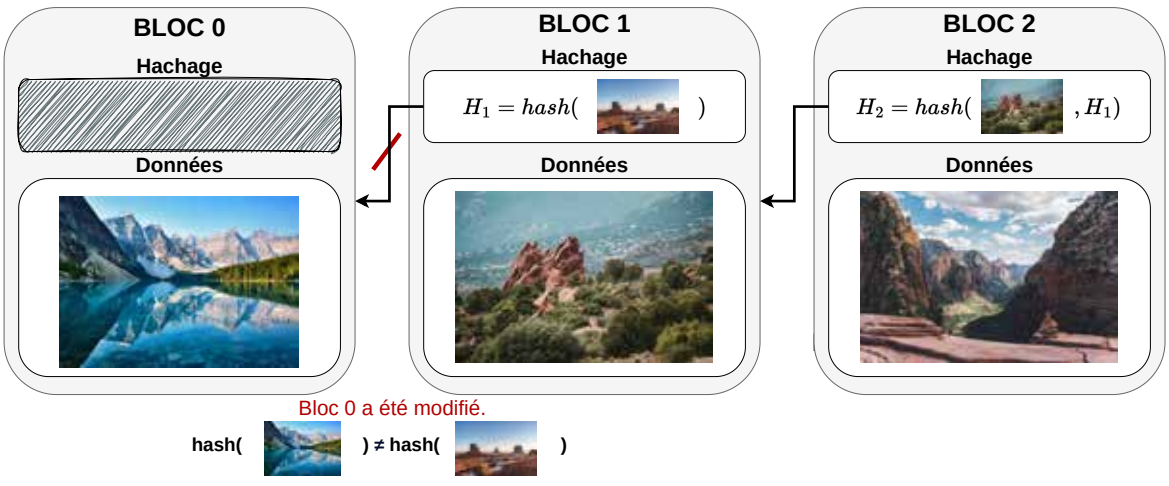


Figure 3

5 Sherman Alan Theodore, Javani Farid, Zhang Haibin and Golazewski Enis, « On the Origins and Variations of Blockchain Technologies », IEEE Security & Privacy, 2019, vol. 17, n° 1, pp. 72-77.

6 Chaum David Lee, « Computer systems established, maintained and trusted by mutually suspicious groups », Thèse de doctorat, 4 avril 1982, Berkeley.

- elle ne peut pas être ré-utilisable, une signature sur un document ne peut pas être déplacée sur un autre document ;
- une fois signé, le document ne doit plus pouvoir être modifié ;
- finalement, une personne ayant signé ne peut pas renier sa signature.

Si ce concept vous semble abstrait, imaginez-vous faire un virement sur l'application bancaire de votre choix. Ce virement comportera votre signature numérique. Une tierce personne ne peut en aucun cas produire une signature numérique valide. De même, à supposer que cette tierce personne récupère votre signature numérique pour un virement en particulier, ce dernier ne peut la réutiliser pour signer d'autres virements.

Le cas du Bitcoin

Le Bitcoin[7] est la première monnaie décentralisée (₿), c'est-à-dire ne requérant pas la participation d'une autorité centrale chargée de veiller au bon fonctionnement du processus. En effet, toute personne est libre de télécharger et de faire tourner un programme, appelé *client*. Ce client est chargé, entre autres, de se connecter à d'autres clients, de diffuser les transactions financières et de vérifier ces dernières. Les transactions financières sont collectées et stockées dans une *blockchain* publique, appelée *registre*.

Une des propriétés garanties par Bitcoin est l'immuabilité des transactions financières : dès lors qu'une transaction financière a été publiée dans le registre, il doit être impossible de la modifier. Tel que mentionné à la sous-section précédente, l'utilisation d'une *blockchain* n'est pas suffisante pour garantir la propriété d'immuabilité des transactions contenues dans celle-ci. Sans mécanisme supplémentaire, un·e utilisateur·rice malveillant·e pourrait modifier une transaction dans un bloc et modifier toutes les valeurs de hachage des blocs suivants pour obfusquer sa modification.

Pour la création d'un nouveau bloc, les clients doivent atteindre un consensus. Il existe plusieurs algorithmes de consensus mais celui utilisé par le Bitcoin est le *minage*. Ainsi, pour créer un bloc, un client doit résoudre un puzzle mathématique. Ce puzzle étant entièrement basé sur la notion d'aléatoire, chaque client n'a qu'une faible probabilité de le résoudre[8]. Cette probabilité est directement proportionnelle à sa puissance de calcul mise à l'œuvre. Ainsi, si une personne malveillante souhaitait modifier un bloc en particulier, celle-ci serait enjointe de déployer une puissance de calcul considérable afin d'en modifier les suivants.

Finalement, intéressons-nous à la manière dont Bitcoin représente une transaction. Une transaction est essentiellement composée de un ou plusieurs *inputs* et de un ou plusieurs *outputs*. Prenons l'exemple de la transaction à droite dans la figure 4 proposée ci-dessous. Cette transaction est composée de 2 *inputs* et 2 *outputs*. Un *output* représente l'endroit où est stockée une quantité de bitcoins. Chaque *output* définit un ensemble de conditions pour pouvoir être dépensé. Nous reviendrons plus amplement sur ce sujet dans la sous-section suivante. Il est à noter qu'un *output* étant dépensé l'est toujours entièrement, il n'est pas possible d'utiliser une fraction de l'argent contenu dans celui-ci. À l'inverse, les *inputs* ont pour but de dépenser l'argent contenu dans des *outputs*. Toujours dans notre exemple, les deux *inputs* dépensent donc 2 *outputs* définis dans des blocs précédents et qui n'avaient pas été dépensés jusqu'à présent. Les fonds contenus dans ces 2 *outputs*, respectivement 0,05882892 et 0,13218618 bitcoins, sont répartis entre les deux *outputs* de la transaction. Finalement pour qu'une transaction soit validée, la quantité de bitcoins contenue dans tous les *outputs* doit nécessairement être inférieure à la quantité amenée grâce aux *inputs*.

Un grand pouvoir implique de grandes responsabilités

Revenons sur la manière dont Bitcoin vérifie qu'un *input* est bel et bien autorisé à dépenser un *output*. Bitcoin définit un langage de script,

7 *Op. cit.* « Bitcoin: A Peer-to-Peer Electronic Cash System. »

8 C'est la résolution de ce puzzle mathématique qu'on appelle communément « minage ».

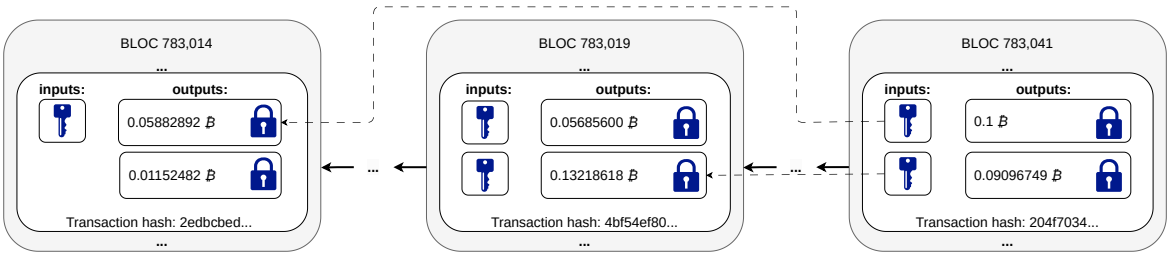


Figure 4

à savoir un langage pouvant être interprété par une machine. Ce langage est sobrement baptisé Script[9] et permet aux utilisateur·rices d'exprimer les conditions sous lesquelles leur argent peut être dépensé. Dans la vaste majorité des cas, la condition se résume à la présentation d'une signature digitale. L'*output* contient donc du code rédigé en Script qui vérifie la validité de cette signature. À l'inverse, l'*input* doit contenir cette signature.

Néanmoins, les capacités de Script ne se limitent pas à la vérification de signatures. En effet, il est possible de définir toute sorte de conditions, par exemple[10] :

- un *output* appartenant à plusieurs individus et requérant la signature d'un certain nombre d'entre eux;
- un *output* proposant un puzzle mathématique à résoudre;
- un *output* bloqué jusqu'à une certaine période dans le temps;
- etc.

> Dès lors que l'on s'attelle à la traduction d'objectifs dans un langage de programmation, ou bien dans un langage de script, on s'expose à l'introduction d'erreurs dans celle-ci.

Selon Alan J. Perlis, « *there are two ways to write error-free programs; only the third one works*[11] [12] ». Dès lors que l'on s'attelle à la traduction d'objectifs dans un langage de programmation, ou bien dans un langage de script dans le cas qui nous occupe, on s'expose à l'introduction d'erreurs dans celle-ci.

Puisque les transactions sont publiques, est-il possible d'analyser la *blockchain* afin de trouver des *outputs* non dépensés et n'étant pas correctement protégés de telle sorte que n'importe qui pourrait réclamer l'argent s'y trouvant ?

La science du test logiciel

Notre question de recherche consiste donc en la recherche d'erreurs contenues dans du code rédigé en Script. Fort heureusement pour nous, les informaticiens ayant été très rapidement confrontés à cette problématique, une panoplie de techniques ont été développées à cette fin. En effet, les développeurs ont mis au point des techniques plus ou moins élaborées pour tester leur logiciel. À titre d'exemple, supposons que nous souhaitions tester un programme prenant deux nombres en entrée.

Une première méthode un peu naïve consiste à exécuter le programme avec différentes valeurs d'entrée et vérifier que celui-ci s'exécute correctement et renvoie la valeur de sortie attendue. Néanmoins, il n'est pas possible de prouver qu'un programme est correct grâce à cette méthode. En effet, il faudrait tester

9 Communauté Bitcoin, « Script », Documentation, Bitcoin Wiki, décembre 2010, disponible à l'adresse suivante : https://en.bitcoin.it/wiki/Script (consultée le 10 janvier 2024).

10 *Ibid*.

11 « Il y a deux manières d'écrire des programmes sans erreurs ; seule la troisième fonctionne ». Traduit de l'anglais par les auteurs.

12 Perlis Alan J., « Special Feature: Epigrams on programming », ACM SIGPLAN, septembre 1982, vol. 17, n° 9, pp. 7–13.

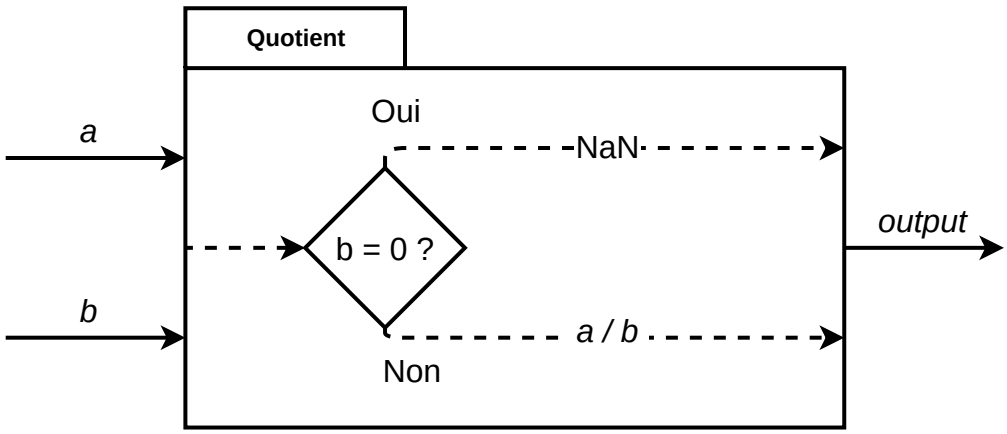


Figure 5

chaque valeur d'entrée possible pour ce faire. Comme l'écrivait Dijkstra en 1970, « *program testing can be used to show the presence of bugs, but never to show their absence*[13] [14] ».

L'exécution symbolique à la rescousse de Bitcoin

Une autre technique permet de pallier partiellement cette lacune : l'exécution symbolique. Prenons le cas suivant et illustré dans la figure ci-dessous. Ce programme prend en entrée deux nombres *a* et *b* réels et en calcule le quotient *a/b*. Le programme renvoie une valeur d'erreur spéciale *NaN* (« *not a number*[15] ») si *b* est égal à 0 (voir figure 5).

Plutôt que d'exécuter le code à l'aide de valeurs concrètes, on exprime le code sous forme d'expressions mathématiques et/ou logiques. Dans notre cas, la valeur de sortie pourrait être formulée comme étant :

$$valeur_{sortie} = Si(b \neq 0), Alors \frac{a}{b}, Sinon\ NaN$$

Tout l'intérêt réside dans le fait qu'il existe tout un pan de l'informatique et la logique mathématique s'intéressant à l'étude de ce genre d'expressions : la satisfiabilité modulo des théories. À l'aide d'un *solveur*, c'est-à-dire un programme capable d'interpréter ce genre d'expressions, il est possible d'interroger le modèle représentant le programme. Par exemple, il y a-t-il des valeurs d'entrée telles que la valeur de sortie soit égale à douze ?

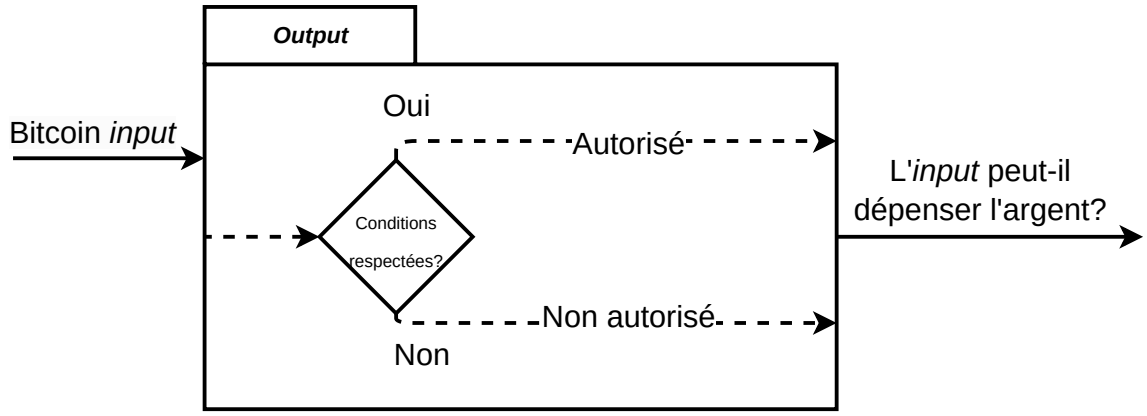


Figure 6

13 « Les tests de programmes peuvent être utilisés pour montrer la présence de bugs, mais jamais pour montrer leur absence ». Traduit de l'anglais par les auteurs.

14 Dijkstra Edsger W., « Notes On Structured Programming », EWD249, avril 1970, Section 3 ("On The Reliability of Mechanisms").

15 En français : pas un nombre.

Revenons à du concret et tentons de voir comment cette technique peut nous aider à trouver des *outputs* vulnérables. Les conditions incluses dans ces derniers agissent comme un programme qui prendrait en entrée un *input* Bitcoin. La valeur de sortie, quant à elle, indique si l'*input* est autorisé ou non à dépenser l'argent contenu (voir figure 6).

Notre méthodologie

La première étape, voir illustration ci-dessous, consiste à déployer un client Bitcoin afin de télécharger la *blockchain*. Cette étape est triviale et ne requiert que quelques jours. La seconde implique l'écriture d'un petit script afin d'extraire les *outputs* de la *blockchain* (voir figure 7).

Ayant toutes nos données prêtes, nous pouvons nous atteler à l'analyse de celles-ci. Grâce à l'exécution symbolique, nous pouvons traduire les conditions spécifiées dans un *output* comme étant des expressions logiques. À notre connaissance, il n'existe aucun exécuteur symbolique pour le langage Script. Nous en avons donc implémenté un[16].

Ensuite, à l'aide d'un solveur, il est possible de rechercher des valeurs pour lesquelles nous serions autorisés à prendre les fonds stockés. Bien évidemment, tout solveur mathématique a ses limites, notamment aucun solveur n'est capable de contrefaire une signature digitale. Néanmoins, ceux-ci sont parfaitement capables de résoudre des puzzles mathématiques. Bon nombre de solveurs mathématiques existent

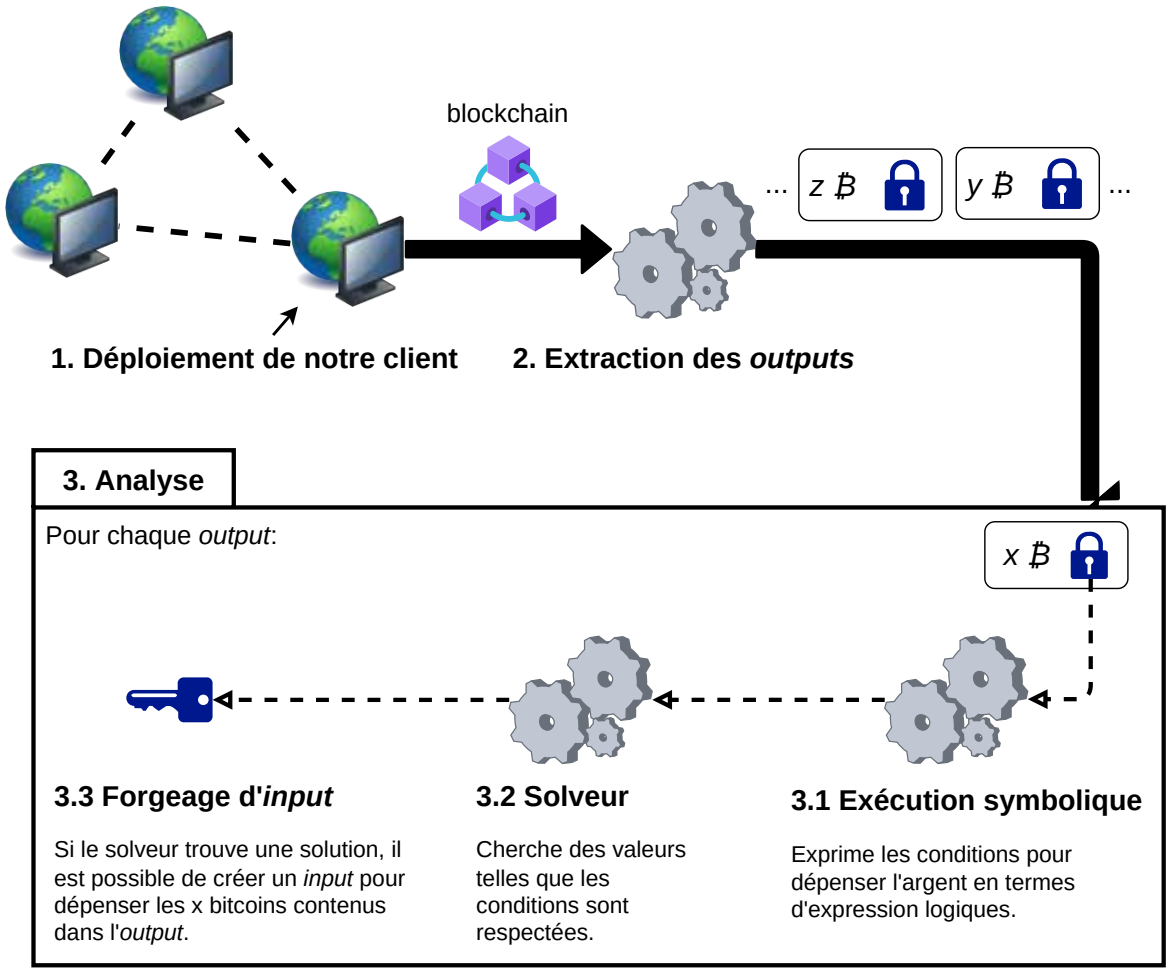


Figure 7

16 Jacquot Vincent, Donnet Benoit, « Symbolic Executor », Code source, Université de Liège, janvier 2023, disponible à l'adresse suivante : https://gitlab.uliege.be/blockchains/bitcoin/symbolic_execution (consultée le 22 janvier 2024).

déjà, nous avons opté pour celui développé par Microsoft : Z3[17].

Dans l'éventualité où Z3 trouve une solution, nous sommes donc en possession de valeurs nous permettant de prendre l'argent contenu dans cet *output*, révélant ainsi une faille de sécurité dans les conditions protégeant les fonds.

Résultats

Bitcoin, une crypto-monnaie inviolable ?

Notre analyse de la *blockchain* s'étend du premier bloc publié le trois janvier 2009 au bloc 775.000 publié le quatre février 2023. Sur les centaines de millions de transactions passées au microscope, nous avons découvert 373.926 instances d'*outputs* étant vulnérables. Grâce à notre exécuteur symbolique, nous sommes en mesure d'apporter la preuve formelle de ces vulnérabilités. Nous savons également que ces vulnérabilités auraient pu être exploitées pour voler 55,36 ₿, ce qui équivaut à un peu plus de 2 millions d'euros en date du quinze janvier 2024[18]. De plus, notre exécuteur symbolique a été capable de prouver que 9.357 instances contenaient des conditions irréalisables. L'argent contenu dans ces dernières est donc bloqué et ne pourra jamais être dépensé. Finalement, nous estimons dans l'article complet que nous avons publié en septembre 2023 qu'un peu plus 1.304 ₿ seraient toujours vulnérables à l'heure actuelle[19].

Néanmoins, ces résultats sont à mettre en comparaison avec l'état global de la *blockchain*. Celle-ci comprend plus de 2 milliards d'*outputs* et les 19 millions de ₿ en circulation à l'heure d'écrire ces lignes[20].

Dans l'écrasante majorité des cas, nous pouvons considérer l'argent comme étant bien protégé. Néanmoins, le prix du Bitcoin étant assez élevé, ces vulnérabilités restent des cibles attrayantes pour des hackers. Et ce, d'autant plus que le processus d'attaque peut être entièrement automatisé et ne requiert qu'un investissement personnel très limité de la part de personnes mal intentionnées : à savoir un ordinateur connecté à Internet et un peu d'argent pour payer les frais de transaction lors du vol.

Quelques cas concrets de vulnérabilités

Dans cette section, il nous a semblé pertinent de fournir quelques exemples concrets trouvés. Afin d'éviter toute incitation à des actions illégales, tous les échantillons proposés ici sont des *outputs* dont les fonds ont d'ores et déjà été dépensés. Ceux-ci permettent d'illustrer les raisons à l'origine de ces vulnérabilités. En effet, les différents *outputs* étant sensibles aux attaques peuvent être groupés en plusieurs catégories.

La première regroupe les puzzles et défis mathématiques. Dans le premier exemple proposé ci-dessous (figure 8), il suffit de trouver 2 nombres a et b tels que leur somme est égale à quatre et leur différence à 2. Bien qu'étant trivial, ce simple système d'équations à deux inconnues fut utilisé pour protéger 0,0101 ₿ répartis en 4 outputs[21] : l'équivalent d'environ 393 euros[22]. L'exemple suivant (figure 9) implique l'utilisation d'une fonction de hachage en particulier : SHA-1[23]. Pour débloquer les quelques 2,4998322 ₿ (97.336 €) contenus

17 Microsoft Research Team, « Z3: An efficient SMT solver », Documentation, Microsoft, mars 2008. https://www.microsoft.com/en-us/research/project/z3-3/ (consultée le 22 janvier 2024).

18 Employés de Coin Market Cap, « Bitcoin Price », Métriques, Coin Market Cap. https://coinmarketcap.com/currencies/bitcoin/ (consultée le 15 janvier 2024).

19 Jacquot Vincent, Donnet Benoit, « CHAUSSETTE: A Symbolic Verification of Bitcoin Scripts », septembre 2023, International Workshop on Cryptocurrencies and Blockchain Technology (CBT)

20 Employés de chez Blockchain.com, « Total Circulating Bitcoin », Métriques, *Blockchain.com*. https://www.blockchain.com/fr/explorer/charts/total-bitcoins (consultée le 15 janvier 2024).

21 Employés de BlockStream, « Bitcoin Stream Explorer », Métriques, BlockStream. https://blockstream.info/address/3PTNXWr3E3VdndyHvfJSVdFkK2AzcfAKJz (consultée le 15 janvier 2024).

22 Cette conversion (₿ => €) et les suivantes ont été faites sur base du prix en date du 15 janvier 2024 : 1 ₿ = 38937 €.

23 Communauté Wikipédia, « SHA-1 », Documentation. https://fr.wikipedia.org/wiki/SHA-1 (consultée le 15 janvier 2024).

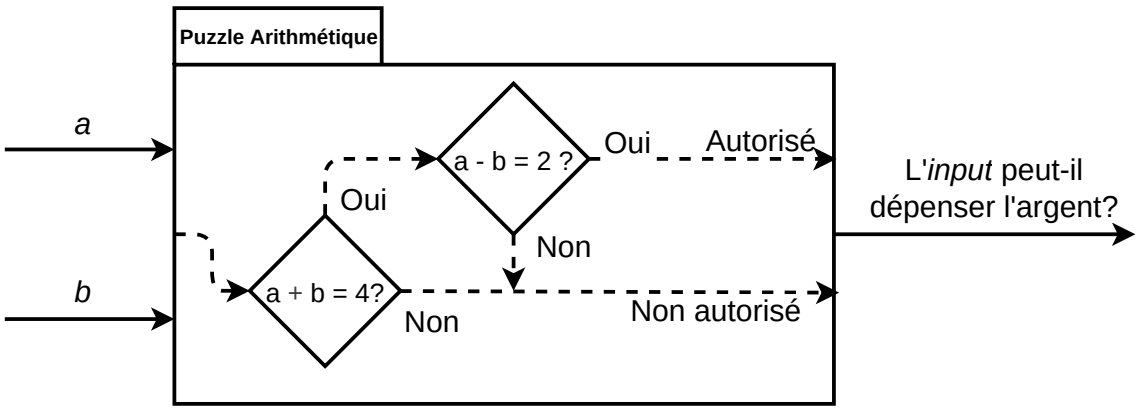


Figure 8

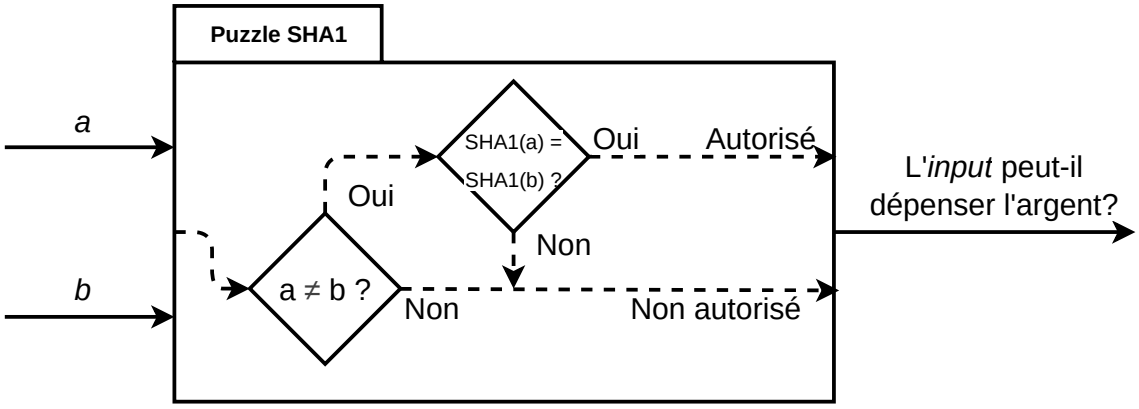


Figure 9

dans 23 outputs[24], il était requis de fournir deux nombres distincts en entrée produisant une collision, c'est-à-dire dont la valeur de hachage est la même.

La seconde raison à laquelle nous pouvons imputer la présence de failles de sécurité est possiblement d'origine humaine. Par exemple, nous pouvons citer ces 398 outputs[25] qui n'étaient tout simplement pas verrouillés et ne restreignent pas l'accès aux 0,31459225 ₿ (12.249 €) stockés. Finalement, nous pouvons également citer le cas du logiciel P2Pool[26] qui permet à des utilisateurs de joindre collectivement leurs efforts pour participer au minage de blocs. Un bug semble à l'origine de la création de 182 outputs impossibles à dépenser[27].

Conclusion

Malgré sa réputation d'être inviolable, Bitcoin, à l'instar de tout protocole ou logiciel, peut comporter des failles de sécurité. De nombreux articles se sont déjà attelés à décrire et quantifier de potentielles attaques. Pour n'en citer que quelques-unes :

- les attaques Sybil[28] : un utilisateur malveillant déploie de nombreuses identités virtuelles afin de manipuler le réseau ;

24 Employés de BlockStream, « Bitcoin Stream Explorer », Métriques, BlockStream. https://blockstream.info/address/37k7toV1Nv4DfmQbmZ8KuZDQCYK9x5KpzP (consultée le 15 janvier 2024).

25 Employés de BlockStream, « Bitcoin Stream Explorer », Métriques, BlockStream. https://blockstream.info/address/3MaB7QVq3k4pQx3BhsvEADgzQonLSBwMdj (consultée le 15 janvier 2024).

26 Communauté Bitcoin, « P2Pool », Documentation, Bitcoin Wiki. https://en.bitcoin.it/wiki/P2Pool (consultée le 15 janvier 2024).

27 Communauté de Bitcoin Talk, « P2Pool », Discussion, Bitcoin Talk. https://bitcointalk.org/index.php?topic=67158.0 (consultée le 15 janvier 2024).

28 Communauté de Bitcoin, « Weaknesses », Documentation, Bitcoin Wiki. https://en.bitcoin.it/wiki/Weaknesses (consultée le 15 janvier 2024).

- les attaques par déni de service[29] : saturation d'un ou plusieurs clients par la quantité d'informations à traiter, par exemple en publiant des transactions dont la vérification requiert d'importantes ressources ;
- ou finalement les attaques des 51%[30]. Celle-ci repose sur l'hypothèse qu'un groupe contrôle la majorité de la puissance de calcul allouée au processus de minage. Ce groupe aurait donc la capacité d'altérer la blockchain.

À notre connaissance, nous sommes les premiers à avoir quantifié le potentiel des attaques par exécution symbolique sur l'entièreté du réseau Bitcoin dans notre article publié en septembre 2023[31]. Cette démarche s'inscrit dans la lignée de nombreux précédents travaux par d'autres chercheurs s'attelant à améliorer la sécurité de ces technologies émergentes. Nous avons détecté et prouvé que 55 ₿ auraient pu être dérobés dans le passé. De plus, nous avons fourni une estimation quantifiée des vulnérabilités qui pourraient toujours être d'actualité.

Finalement, l'entièreté de nos outils développés dans le cadre de nos recherches est libre d'accès. Nous espérons que ceux-ci pourront être utilisés par la communauté dans le but de bâtir un réseau plus sûr pour tous.

Ce travail est soutenu par le projet CyberExcellence financé par la Région wallonne, sous le numéro 2110186.

29 *Ibid.*

30 Communauté de Wikipédia, « Attaque des 51% », Documentation, Wikipédia. https://fr.wikipedia.org/wiki/Attaque_des_51_%25 (consultée le 15 janvier 2024).

31 *Op. cit.* « CHAUSSETTE: A Symbolic Verification of Bitcoin Scripts ».


Digitise.
Optimise.
Empower.
Innovate.
Co-create.
Working at AG,
adventure guaranteed.
AG.BE/JOBS
Supporter of your life

La cybersécurité : enjeux pour l'économie wallonne, les PME industrielles et le secteur des cryptomonnaies
Les Cahiers du Digital - N°8
Digital Lab - HEC Liège Management School - Liège Université

Auteur·es : Benoît Donnet, Jeremy Grandclaudon, Nina Hasratyan, Vincent Jacquot, Axel Legay, Lise Lombardi, Jean-Philippe Parmentier
Date de publication en ligne : Avril 2024
Coordination : Nicolas Neysen & Mireille Meyer
Design, traduction & communication : Roxanne Thonnard
Crédits images : Cover & p.10: ©sonatik/Adobe Stock; p.14: ©Caphira Lescante/AdobeStock, p.17: ©Bartek/Adobe Stock, p.20: ©Rathnayakamudalige/Adobe Stock, p.23: ©Zaleman/Adobe Stock, p.26: ©Philip Steury/Adobe Stock, p.30: ©Omar/Adobe Stock, pp.32-33: ©Cayetano Gil/Unsplash, ©John Lee/Unsplash, ©Sean Foster/Unsplash, ©Fineas Anton/Unsplash

Avec le soutien de :

Ressources utiles

Les essentiels

Tout savoir sur le programme de Cybersécurité de la Wallonie	https://digitalwallonia.be/cyberwal/
Pour les personnes et pour les entreprises	www.safeonweb.be
Pour les entreprises, PME et autres organisations	https://mapmecybersecurisee.be/ *Une série de conseils, d'outils et ressources (audit rapide de sécurité, formation en ligne) pour améliorer votre cybersécurité.* https://www.cybersecuritycoalition.be *Outils de sensibilisation, de bonnes pratiques et guide pour améliorer votre cybersécurité.*

Sensibiliser aux bonnes pratiques

https://www.cybersecuritycoalition.be/fr/resource/cyber-security-kit/
https://surfersanssoucis.safeonweb.be/fr/modules/1
https://safeonweb.be/fr/surfez-en-toute-securite

Pour débuter

Quick wins	https://atwork.safeonweb.be/fr/tools-resources/quick-wins
Les bases	https://www.cybersecuritycoalition.be/fr/resource/cyber-security-basics-pour-les-starters/
Les cyberfondamentaux pour les TPE et PME	https://atwork.safeonweb.be/sites/default/files/2023-06/cyfun_small_f_20230301.pdf
Pour vous protéger efficacement	https://safeonweb.be/fr/surfez-en-toute-securite

Auto-diagnostic pour TPE, PME et indépendants

https://atwork.safeonweb.be/fr/tools-resources/self-assessment
https://mapmecybersecurisee.be/quickscan
https://economie.fgov.be/fr/cyberscan
https://www.cybersecuritycoalition.be/fr/resource/pme-security-scan/

Se former

Webinaires	https://atwork.safeonweb.be/fr/tools-resources/videos-webinars
Webinaire et formation	https://www.agoria.be/cyberstart/fr
Atelier cybersécurité	https://cyber4sme.be/

Mettre en place un plan de cybersécurité

Guide et documents de référence	https://atwork.safeonweb.be/fr/tools-resources/policy-templates *Documents de référence couvrant l'ensemble des points clés de la cybersécurité* https://atwork.safeonweb.be/fr/tools-resources/cyberfundamentals-framework *Des cadres de références adaptés au niveau de risques des entreprises*
Financement et ressources	https://atwork.safeonweb.be/fr/tools-resources/mesures-de-soutien *Mesures de soutien au niveau EU, BE et des régions* https://www.cheques-entreprises.be/cheques/cybersecurite/ *Chèques entreprises* https://www.digitalwallonia.be/fr/programmes/cyberwal-by-digital-wallonia/ *Programme Cyberwal by Digital Wallonia*

En cas d'attaque

Si vous avez un problème	https://safeonweb.be/fr/au-secours
Signaler un incident ou recevoir de l'aide	https://www.cert.be/fr/signaler-un-incident-0
Guide de premier secours	https://ccb.belgium.be/fr/cert/premiers-secours-en-cas-de-cyberattaque
Guide de gestion des incidents	https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-FR.pdf

Trouver un·e expert·e

Agoria	https://www.agoria.be/fr/services/expertise/digitisation/cybersecurity/cybersecurity-redline
Infopole	https://clusters.wallonie.be/infopole/fr/vous-cherchez-un-expert-numerique-lancez-un-appel-competences

CONTACT

www.digitallab.be
digitallab@uliege.be

HEC LIÈGE
Management School - Liège Université
DIGITAL LAB