BSF NEWSPAPER
L'ACTUALITÉ / TECH' / BUSINESS / RÉGION
DU XXI ÈME SIÈCLE

NUMÉRO SPÉCIAL
CYBERSÉCURITÉ

COMBATTRE UN SPECTRE PROTÉIFORME !

LEXIQUE
PARLEZ-VOUS CYBER ?

Page 4

TECH'
LOIN DES YEUX, PRÈS DES ATTAQUES

Page 4

NOUVEAU MÉTIER
LE HACKER ÉTHIQUE

Page 4

A LA UNE !

Alors que nous sommes au cœur de l'ère numérique, la question n'est pas de savoir si nous serons attaqués, mais plutôt quand et comment nous y répondrons. La cybersécurité n'est pas seulement une ligne de défense, c'est une stratégie essentielle !

Un chiffre fait peur : on estime que presque une entreprise sur deux fait faillite dans les 18 mois suivant une cyberattaque, ce qui met en évidence le risque existentiel que ces attaques représentent pour les PME.

Autres chiffres qui font trembler : Le coût moyen des fuites de données a augmenté significativement de **15 %** en trois ans. **47 %** des sociétés victimes d'un ransomware ont choisi de payer la rançon, soulignant l'impact dévastateur de ces attaques sur les entreprises. **36 %** des cadres supérieurs sont susceptibles de tomber dans le piège du phishing, deux fois plus que les salariés ordinaires.

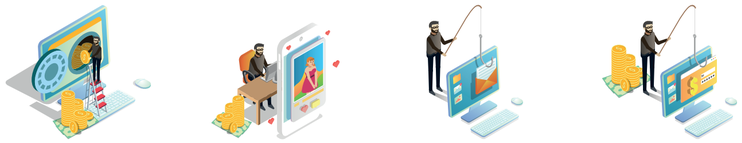
Quant à la forme des attaques, cela ressemble plutôt à un spectre protéiforme qui plane au dessus du monde numérique. Une cyberattaque peut être envisagée comme une invasion silencieuse, souvent invisible jusqu'à ce que le dommage soit fait.

Ces attaques prennent de nombreuses formes, chacune avec son propre arsenal de destruction. Les virus et les vers se propagent à travers le réseau, détruisant et dupliquant.

Les ransomwares prennent en otage vos précieuses données, demandant une rançon pour leur retour. Les attaques par déni de service (DDoS) submergent les systèmes, les rendant inopérants. Et la liste continue, chaque variante étant une créature adaptée à exploiter les faiblesses de notre monde numérisé.

Cybersécurité : Le terme cybersécurité est construit à partir du préfixe « cyber », d'origine grecque, réapparu au milieu du xxe siècle avec le mot cybernétique, ce dernier concernant l'étude des processus de contrôle et de communication chez l'être vivant et la machine.

« 36 % des cadres supérieurs sont susceptibles de tomber dans le piège du phishing, deux fois plus que les salariés ordinaires »



Suite de l'article **A la une**

Mais qui est derrière ces attaques ? Les hackers, souvent vus comme les maraudeurs du monde numérique, ne sont pas un bloc monolithique. Leurs motivations, comme leurs méthodes, varient considérablement.

Les "white hats" sont les chevaliers du royaume numérique, piratant pour renforcer la sécurité et protéger les citoyens du net. Les "black hats", en contraste, sont les brigands, cherchant à exploiter, voler, et semer la discorde pour leur propre gain ou pour celui de commanditaires obscurs.

Puis, il y a les "grey hats", des vigilants qui naviguent dans une zone grise, parfois en protecteurs, parfois en prédateurs, selon le code qu'ils choisissent de suivre.

Bref, le temps est venu de voir le verre à moitié plein en parlant cybersécurité face aux attaques. Pour résumer, la cybersécurité représente un ensemble essentiel de pratiques, de technologies et de politiques conçues pour protéger les réseaux, les ordinateurs, les programmes et les données, les dommages ou les accès non autorisés.

Pour les entreprises, cela signifie adopter une posture proactive et former les employés aux meilleures pratiques de sécurité et mettre en place des politiques strictes de gestion des données.
Mais plus que cela, il faut intégrer une culture de la sécurité, où chaque collaborateur comprend sa responsabilité dans la protection de l'entreprise contre les menaces numériques. ■

L'INFORMATIQUE FANTÔME

L'informatique fantôme désigne l'utilisation non autorisée de logiciels, matériels ou ressources informatiques dans une entreprise sans l'approbation ou la surveillance du service informatique.

Cela inclut l'utilisation de services de stockage cloud personnels, de logiciels de communication non approuvés ou d'appareils personnels connectés au réseau de l'entreprise.

Bien que souvent adoptée pour améliorer la productivité, cette pratique expose à des risques de sécurité, car les systèmes non surveillés peuvent être vulnérables aux attaques.

Les entreprises tentent de gérer ces risques en intégrant ces technologies à leurs protocoles de sécurité standard plutôt que de les interdire complètement. ■

Cyb' LE DIAGNOSTIC CYBERSÉCURITÉ DU GROUPE BSF

Les cabinets d'expertise comptable sont devenus des acteurs clés de la cybersécurité pour les entreprises.

À ce titre, le Groupe BSF vous propose **CYB'**, un diagnostic des risques "cybersécurité" sur mesure, aux vertus pédagogiques. C'est un état des lieux précis qui permet d'identifier et recenser vos données critiques les plus sensibles aux cyberattaques.

Ce diagnostic met en évidence les insuffisances et failles pouvant se présenter dans vos procédures de sécurité. Plus concrètement, le diagnostic s'appuie sur les principaux points suivants.

- État des lieux de l'écosystème informatique.
- Consultation de la documentation et des procédures.
- Examen des dispositifs mis en place au sein des systèmes d'information.
- Réalisation de la cartographie des risques en matière de cybersécurité.
- Analyse de la police d'assurance afin de déterminer les risques couverts et mesurer leurs incidences sur l'entreprise et les tiers en cas d'incidents.

Le Groupe BSF fort de sa déontologie professionnelle liée à son activité d'expert-comptable, réalise ce diagnostic en toute indépendance et dans un climat de totale confiance.

Suite aux conclusions de mission, vous serez au fait des points-clés à traiter pour votre cybersécurité et disposerez d'un plan d'action détaillé à présenter à votre prestataire technique.

ÉCOUTEZ AYMERIC BOUTEILLER PRÉSENTER L'OFFRE CYB' DE BSF

Scannez moi

NOUS CONTACTER
Mail : cyb@bsf.fr
Numéro de tél. : 05 57 59 02 02

LEXIQUE
PARLEZ-VOUS CYBER ?

Attaque par déni de service (DDoS)
Tentative de rendre une machine ou un réseau indisponible pour ses utilisateurs prévus, souvent en surchargeant le service avec un flux excessif de demandes.

Phishing
Technique d'escroquerie utilisée pour tromper les utilisateurs afin qu'ils divulguent des informations personnelles, comme des mots de passe ou des détails de cartes de crédit.

Malware
Logiciel malveillant conçu pour endommager ou réaliser des actions non autorisées sur un système informatique. Cela inclut les virus, les chevaux de Troie, les spywares, et les ransomwares.

Ransomware
Type de malware qui chiffre les fichiers de l'utilisateur, rendant les données inaccessibles, et demande une rançon pour leur déchiffrement.

Spyware
Logiciel espion conçu pour s'infiltrer dans un dispositif informatique (ordinateurs, smartphones…) afin de collecter des informations sur lui ou sur ses activités.

Zero-Day
Vulnérabilité logicielle qui est inconnue du fabricant du logiciel ou du public jusqu'à ce qu'elle soit exploitée par un attaquant.

Hameçonnage (Spear Phishing)
Forme de phishing plus ciblée, où l'attaquant personnalise l'attaque pour une victime ou un groupe spécifique.

Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
Dispositifs ou applications qui surveillent les réseaux ou les systèmes pour des activités malveillantes ou des violations de politique et peuvent bloquer ou signaler ces activités.

Botnets
Réseaux de dispositifs informatiques infectés par des logiciels malveillants et contrôlés à distance par un attaquant.

White Hat
Hacker éthique qui utilise ses compétences en cybersécurité pour identifier et réparer les vulnérabilités des systèmes informatiques dans le but de les protéger contre les attaques (lire aussi Pentester).

Black Hat
Hackers malveillants qui exploitent les failles de sécurité dans les systèmes informatiques sans autorisation, souvent dans des buts illicites tels que le vol d'informations, la fraude, ou la création de botnets.

Pentester (Testeur d'intrusion)
Professionnel de la cybersécurité qui réalise des tests de pénétration sur des systèmes informatiques, des réseaux ou des applications web.

VOUS ABONNER GRATUITEMENT AU BSF NEWSPAPER DIGITAL

groupe-bsf.fr/bsfnewspaper/

TECH

LOIN DES YEUX, PRÈS DES ATTAQUES

Une étude réalisée par SoSafe, une entreprise spécialisée dans la sensibilisation à la cybersécurité souligne les préoccupations croissantes liées à l'aug mentation du travail hybride et du télétravail en matière de cybersécurité.

Une majorité écrasante de spécialistes en cybersécurité (neuf sur dix) considère que l'essor du travail à distance a exacerbé les risques pour les entreprises, avec 75 % d'entre eux attribuant directement ces risques accrus au télétravail.

Le télétravail est en effet une porte ouverte au phishing. Cette menace exploite souvent des emails ou messages semblant légitimes pour tromper les employés distants, moins encadrés par les mesures de sécurité des bureaux.

Les cybercriminels ciblent des données sensibles telles que mots de passe, informations financières ou identifiants professionnels, causant des dommages financiers et réputationnels importants.

Quelques exemples de vulnérabilité :

Les outils de communication en visio - Les espaces de travail à domicile peu protégés - L'utilisation d'ordinateurs et portables personnels à des fins professionnelles - Le sentiment, à distance d'être moins concerné par les procédures de sécurités appliquées dans l'entreprise. ■

NOUVEAU MÉTIER

LE HACKER ÉTHIQUE

La cybersécurité ne cessera de nous surprendre ! Preuve en est, ce nouveau métier, le "hacker éthique"…

"Hacker éthique", aussi connu sous le nom de pentester ou consultant en sécurité informatique, désigne les professionnels de la cybersécurité dont la mission est de détecter et d'exploiter les vulnérabilités des systèmes informatiques, des réseaux et des applications.

« Contrairement aux cybercriminels, les hackers éthiques agissent avec permission »

Leur objectif est d'améliorer la sécurité en identifiant et en réparant les failles avant qu'elles ne soient exploitées par des hackers malveillants.

Contrairement aux cybercriminels, les hackers éthiques agissent avec permission et dans un cadre légal strict, souvent sous contrat ou salariés d'entreprises spécialisées en sécurité informatique.

La carrière de hacker éthique exige un large éventail de compétences techniques en informatique, notamment dans les domaines des réseaux, des systèmes d'exploitation et de la programmation.

Une compréhension approfondie des méthodes d'attaque et des techniques de défense est également essentielle.

Les certifications professionnelles, comme le Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), ou encore le GIAC Security Essentials (GSEC), sont hautement valorisées dans le secteur et peuvent attester des compétences et des connaissances spécialisées dans le domaine de la cybersécurité. ■

3 QUESTIONS À

J.F. CHEVASSU / ADISTA

Dans le passé lorsque Adista a commencé, qu'était la cybersécurité ?

Adista existe depuis une vingtaine d'année, la cybersécurité se focalisait alors sur la défense du périmètre réseau avec des pare-feux. Les infrastructures informatiques étaient dans les entreprises, ce qui délimitait nettement les frontières du système d'information et simplifiait sa sécurisation.

Aujourd'hui qu'en est-il de la cybersécurité ? Qu'est ce qui a changé ?

La révolution numérique de ces dix dernières années a fait exploser le volume de données. Les systèmes d'information sont désormais hybrides. On s'appuie de plus en plus sur des applications métiers, des outils ou des capacités de calcul dans le Cloud tout en conservant certaines données, informations sensibles ou applications développées en interne au sein de ses propres serveurs. Ce qui compte aujourd'hui c'est l'accès à ces données, possible de partout, à n'importe quelle heure et depuis n'importe quel appareil. Cela élargi considérablement la surface d'exposition aux risques cyber, dans un contexte géopolitique tendu et face à une cybercriminalité de plus en plus structurée. Les entreprises doivent appliquer des stratégies dites « Zero Trust » basées sur le principe : never trust, always verify (ne faites aucune confiance, vérifiez toujours).

Qu'elles pourraient être les préoccupations cyber de demain ?

Demain, les préoccupations en matière de cybersécurité seront probablement dominées par les risques associés aux intelligences artificielles génératives et à la prolifération des objets connectés. Ces technologies pourraient engendrer de nouvelles menaces, telles que les deepfakes, plus complexes et difficiles à contrer. ■

GROUPE BSF / ACCOMPAGNER LES DIRIGEANTS DANS LEURS PRISES DE DÉCISION

DONNÉES FINANCIÈRES, FISCALES, JURIDIQUES, SOCIALES & COMPTABLES

Contact / infos-bsf@bsf.fr

Directeur de rédaction / Groupe BSF
Ligne éditoriale / Stephan Pluchet (Agence Elem nt) /
Rédacteur / Olivier Leguistin (Cotc Communication)
Création graphique / Stephan Pluchet / Agence Elem nt
agenceelement.com / stephan@agenceelement.com
Crédits photos / AdobeStock / I**mpression** / Proformats