L'ESSENTIEL DE LA

SÉCURITÉ NUMÉRIQUE

POUR LES **DIRIGEANTS**
ET LES **DIRIGEANTES**

n°2 NOUVELLE ÉDITION 2021

LE MODE D'EMPLOI FACILE D'ACCÈS
POUR ÊTRE À JOUR ET MIEUX ÉCLAIRÉ FACE
AU NOUVEAU RISQUE NUMÉRIQUE

> LA RÉALITÉ DU RISQUE AUJOURD'HUI
> LES REPÈRES INDISPENSABLES ET LES CHIFFRES CLÉS
> LES CONSEILS DES GRANDS ACTEURS
DE LA CYBERSÉCURITÉ

avec

Challenges

L'ÉDITION NUMÉRIQUE DE CET OUVRAGE EST DIFFUSÉE PAR Éditions EYROLLES

« ENSEMBLE, PROTÉGEONS NOTRE ÉCONOMIE,
PROTÉGEONS NOS ENTREPRISES »

Quelle est la dimension du risque aujourd'hui ?
Que dois-je absolument savoir ?
Cet ouvrage a bénéficié d'une mobilisation unique de grands acteurs français du numérique et de la sécurité numérique.
Il a une ambition essentielle : être utile !

COMME L'ENVIRONNEMENT, LA SÉCURITÉ NUMÉRIQUE EST UN ENJEU SOCIÉTAL MAJEUR DE NOTRE TEMPS. DE GRANDS ACTEURS DU NUMÉRIQUE ET DE L'ÉCONOMIE, DES GRANDES ORGANISATIONS D'ENTREPRISES, LES GRANDES ÉCOLES SE SONT ASSOCIÉS POUR PORTER UNE ACTION D'INFORMATION AMBITIEUSE À LA HAUTEUR DE CET ENJEU.

- Agence nationale de la sécurité des systèmes d'information - ANSSI
- Association pour le Management des Risques et des Assurances de l'Entreprise - AMRAE
- Les Assises de la Cybersécurité
- Club des Experts de la Sécurité de l'Information et du Numérique - Cesin
- Conseil de l'économie et de l'information du digital - CEIDIG
- Magazine Challenges
- Association numérique des grandes entreprises et administrations publiques françaises - Cigref
- Conférence des grandes écoles - CGE
- Cinov Numérique
- Confédération des petites et moyennes entreprises - CPME
- Croissance Plus
- Cybermalveillance.gouv.fr
- Devoteam
- EGERIE
- Éditions Eyrolles
- France Digitale
- Gatewatcher
- Groupement Interprofessionnel pour les Techniques de Sécurité des Informations Sensibles - GITSIS
- IDECSI
- Linkbynet
- Medef
- Orange Cyberdefense
- Syntec Numérique

L'ESSENTIEL DE LA

SÉCURITÉ NUMÉRIQUE

POUR LES **DIRIGEANTS**
ET LES **DIRIGEANTES**

« ENSEMBLE, PROTÉGEONS NOTRE ÉCONOMIE,
PROTÉGEONS NOS ENTREPRISES »

à l'initiative de l'association CEIDIG,
Conseil de l'économie et de l'information du digital

HAUT MANAGEMENT

Direction de la publication,
Direction éditoriale :
Daniel Bénabou

Collège éditorial :
présenté en 4e de couverture

Rédaction :
Patrick Coquart, **Guillaume Wallut**

Coordination :
Éditions Cent Mille Milliards

Conception graphique et maquette :
Juliane Cordes, **Corinne Dury**

Impression et façonnage :
Stipa, Montreuil

SOMMAIRE

6 Enjeux et perspectives

14 PARTIE 1 **MIEUX COMPRENDRE LA RÉALITÉ DU RISQUE AUJOURD'HUI**
17 Êtes-vous une cible ?
18 Les grands types de menace
20 À quels impacts s'attendre ?
22 Demain a déjà commencé. 3 points clés à anticiper
24 Et en France ? Notre position, nos décisions, nos grandes initiatives
26 C'est arrivé tout près de chez vous… et ça se rapproche encore ! Un an de cyberattaques
28 Lise Charmel, 1er redressement judiciaire après une attaque informatique !
30 Lexique indispensable

32 PARTIE 2 **PROTÉGER SON ENTREPRISE : REPÈRES ET CONSEILS ESSENTIELS**
34 Se concentrer sur les points clés, 9 recommandations prioritaires
38 Quelle organisation ? Quels indicateurs ? Quel budget ?
40 Conseils pratiques à forte valeur ajoutée
42 Muscler sa défense grâce à ses collaborateurs
44 Les bonnes idées des entreprises pour améliorer leur cybersécurité
46 Point juridique flash
50 Carnet d'adresses

52 PARTIE 3 **DES ENTREPRISES ET DES EXPERTS FRANÇAIS : LEURS VISIONS, LEURS APPORTS**
54 La cybersécurité, un enjeu culturel, Devoteam
55 Maîtrise des risques cyber : un outil stratégique !, EGERIE
56 Comment se préparer efficacement contre une cyberattaque ?, Gatewatcher
57 Et vous, avez-vous sécurisé vos données dans le *cloud* ? Linkbynet
58 Un grand sujet pour toute l'entreprise, IDECSI
59 La cybersécurité, un indicateur de performance, Orange Cyberdefense

60 8 bons gestes pour se protéger

DANIEL BÉNABOU

Président, CEIDIG, Directeur général, IDECSI

UNE ÉCONOMIE MODERNE, EFFICACE

NOUS CONFIONS AU NUMÉRIQUE DE PLUS EN PLUS DE NOS FONCTIONS ÉCONOMIQUES ET SOCIALES.

Nous sommes fascinés par les possibilités exponentielles que cela offre pour le développement et l'efficacité de nos entreprises. Comment bénéficier du meilleur de cette évolution ? Une clé est essentielle, indispensable : la sécurité numérique. Elle apporte à l'entreprise la protection et l'environnement fort qui lui permettent de s'exprimer pleinement, sans frottement. **Liée à l'évolution du numérique, la cybersécurité n'est plus technique, elle est stratégique.** Elle est un sujet de haut management. Partager les enjeux de ce mouvement est l'une des ambitions de cette grande action d'information et de ce second guide, que je suis très fier d'avoir initié et construit avec un collège de compétences si prestigieux.

PIERRE-HENRI DE MENTHON

Directeur de la rédaction, Challenges

UN COMBAT ESSENTIEL

Sujet désormais majeur de la performance des entreprises, la cybersécurité demeure encore méconnue alors qu'elle s'adresse pourtant aussi bien aux très grands groupes qu'aux PME, aux TPE ou aux start-up. Toutes les organisations sont concernées par la menace potentielle d'une cyberattaque, avec les effets insoupçonnés sinon dévastateurs qu'elle engendre.

Challenges est heureux de contribuer à la diffusion de ce second guide de la sécurité numérique pour les dirigeantes et les dirigeants, toujours facile d'accès et plein de pertinence et de précisions. Aussi nous remercions les nombreux et prestigieux partenaires qui se sont activement associés à sa publication et assureront ainsi une diffusion massive des messages qu'il contient. Pour *Challenges*, « l'économie de demain est l'affaire de tous » : c'est dire si **l'évangélisation de la cybersécurité dans une époque d'incertitude et de complexité est un impératif pour la vitalité et l'excellence de tous les acteurs de notre économie**.

GUILLAUME POUPARD

Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

LE RISQUE NUMÉRIQUE EST LÀ ET LES ORGANISATIONS RISQUENT MALHEUREUSEMENT TRÈS GROS. DÉCIDEURS, AU VU DES IMPACTS POTENTIELS, LA CYBERSÉCURITE DOIT ENTRER DANS VOS PRIORITÉS DE PREMIER RANG !

La cybersécurité, c'est 99 % d'anticipation, de prévention et de bon sens. Dans ce domaine, la France dispose de spécialistes compétents et de confiance ; ce guide en est le reflet. Au sein même des organisations, des experts sont de plus en plus souvent capables de mettre en place des stratégies efficaces et pragmatiques. Mais seuls, ces derniers ne peuvent rien ! Je n'encouragerai par conséquent jamais assez les décideurs à se pencher sur ce sujet d'apparence austère et anxiogène car eux seuls sont à même de prendre *in fine* les décisions structurantes à la hauteur des risques numériques.

MYLÈNE JAROSSAY

Présidente du Cesin et Group Chief Information Security Officer LVMH

ALAIN BOUILLÉ

Délégué général du Cesin

LA COVID A ÉTÉ UNE ALLIÉE INATTENDUE DE LA TRANSFORMATION DIGITALE DES ENTREPRISES ET LA RÉVÉLATRICE DE NOUVEAUX CHALLENGES POUR LA CYBERSÉCURITÉ, DANS UN CONTEXTE TOUJOURS PLUS MENAÇANT.

Quand le confinement rime avec télétravail, les défis pour la cybersécurité sont nombreux. Il faut contacter et sécuriser à distance les environnements de travail des collaborateurs, détecter les dérives vers le *shadow IT* mais aussi les expositions de données sur des espaces de stockage *cloud* mal maîtrisés. L'entreprise doit traiter ces questions dans un climat où les cyberattaques redoublent de virulence. La crise sanitaire et les crises cyber se font par ailleurs écho sur les questions de dépendance. **Indéniablement, la réflexion sur la dépendance numérique de l'entreprise doit s'inscrire dans l'agenda des dirigeants** de manière proactive pour bâtir de nouvelles stratégies avant que le sujet ne s'y invite de force.

PHILIPPE COTELLE

Administrateur AMRAE - Head of Insurance Risk Management, Airbus Defence and Space

LA RÉSILIENCE DE L'ENTREPRISE PASSERA PAR LA BONNE ANTICIPATION ET GESTION DU RISQUE CYBER. LA MOBILISATION PAR LES DIRIGEANTS DE TOUTES LES PARTIES PRENANTES DE L'ENTREPRISE EST INDISPENSABLE FACE À UNE MENACE CYBER ORGANISÉE ET OFFENSIVE.

La crise a entraîné une digitalisation à marche forcée dans tous les secteurs. Cette irréversible dynamique et la dépendance accrue au numérique place l'entreprise en alerte face au risque cyber. Sa prévention devient une obligation. **La valorisation économique de l'entreprise dépendra de son investissement dans la résilience face à la menace.** Il est temps de se mettre tous autour de la table, avec la Sécurité, le Risk Management et le Business pour déployer un plan cohérent de gestion de risque, véritable atout confiance nécessaire au développement de l'entreprise.

JEAN-CLAUDE LAROCHE

Président du Cercle Cybersécurité du Cigref et DSI d'Enedis

LES CAPACITÉS DES CYBERCRIMINELS AUGMENTENT DÉSORMAIS PLUS RAPIDEMENT QUE LA CAPACITÉ DE LEURS VICTIMES À SE PROTÉGER. DANS CE CONTEXTE CRITIQUE, LES ENTREPRISES NE POURRONT PLUS FAIRE FACE SEULES À LA MENACE.

La sécurité dans l'espace numérique doit devenir un enjeu écosystémique. Si les grandes entreprises sont conscientes de l'impérieuse nécessité de se protéger, cela n'est plus suffisant. Ainsi, le Cigref propose que le régulateur européen définisse des normes de sécurité minimales applicables aux solutions et services numériques distribués sur notre marché. Il suggère par ailleurs que les États développent et renforcent leurs coopérations et les moyens nécessaires à la lutte contre la cybercriminalité.

JÉRÔME NOTIN

Directeur général, Cybermalveillance.gouv.fr

DE L'IMPORTANCE DES BONNES PRATIQUES

Le numérique est aujourd'hui dans toutes les entreprises. Bien utilisé, il permet d'absorber les crises que notre société peut connaître. Pour cela, le volet sécurité est essentiel et doit être utilisé comme un atout.

Outils collaboratifs, visioconférences, accès distants : ces nouveaux usages pour nombre d'entreprises permettent une adaptabilité forte dans le monde qui s'ouvre à nous. Mais nouveaux usages peut vouloir dire nouveaux risques. **Ce guide présente l'ensemble des enjeux de la cybersécurité et explique, par exemple, pourquoi la sensibilisation des collaborateurs est clé et comment le facteur humain peut et doit être un atout pour le chef d'entreprise.**

VALÉRIE LEVACQUE

Directeur Cyberdéfense ArianeGroup - Présidente du GITSIS

LES CYBERATTAQUES SE SONT INTENSIFIÉES CES DERNIERS TEMPS AVEC DES DOMMAGES DE PLUS EN PLUS IMPORTANTS POUR LES VICTIMES ET LEUR ÉCOSYSTÈME, QUELLES QU'EN SOIENT LES MOTIVATIONS (GUERRE DE L'INFORMATION, GAIN FINANCIER, NUISANCE…).

L'inéluctable accroissement de la surface d'exposition à ces menaces doit conduire à considérer la cybersécurité comme **un axe stratégique, à mobiliser les instances dirigeantes de nos entreprises, à s'organiser en conséquence pour apporter une réponse collégiale et solidaire** afin d'assurer la protection des données et la résilience de nos écosystèmes industriels. Cet ouvrage apportera aux dirigeants quelques réponses aux défis qu'ils doivent désormais considérer.

NOLWENN LE STER

Présidente du Comité Cybersécurité, Syntec Numérique
Head of Cybersecurity, Cloud Infrastructure Services France, Capgemini

LA CYBERSÉCURITÉ, UN RÉFLEXE EN DEVENIR

Syntec Numérique, syndicat professionnel des entreprises du numérique, a placé la cybersécurité au cœur de ses actions depuis 2015 et contribue à la sensibilisation du plus grand nombre.

Pour permettre aux entreprises de tirer parti des transformations digitales, les enjeux de la cybersécurité doivent être impulsés et portés par la direction générale, instillés et appliqués par la DSI et les autres métiers au cœur du sujet. Chacun a un rôle à jouer pour être efficace !

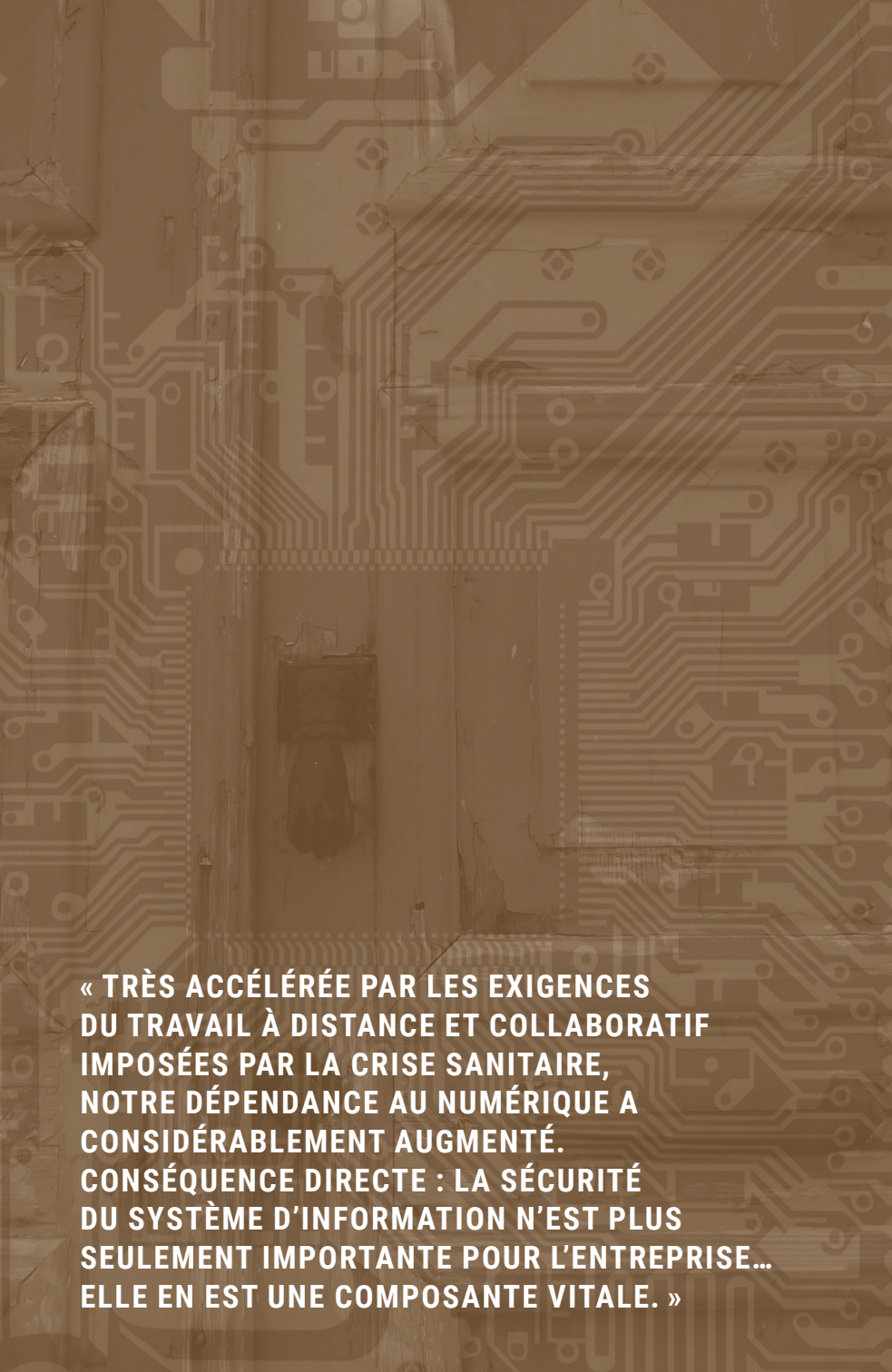
La seconde édition du guide constitue un outil formidable sur lequel peuvent s'appuyer les entreprises pour sensibiliser utilement leurs collaborateurs et directions métiers.

SOPHIE GUERIN

Directrice générale, DG Consultants

POURSUIVRE L'ÉVANGÉLISATION DE LA CYBERSÉCURITÉ

Il y a trois ans, lorsqu'est sorti le premier guide sur la cybersécurité à destination des dirigeants, l'objectif était clairement la pédagogie d'une population qui connaissait peu ou mal les cyber risques. Depuis, Wannacry, NotPetya, des vagues de *ransomware*… sont passés par là et, **si les dirigeants sont de plus en plus sensibilisés aux menaces, il est néanmoins indispensable de poursuivre l'évangélisation**. Tel est le but de cette nouvelle édition, une très belle initiative, à laquelle les Assises de la cybersécurité sont fières de participer.



« TRÈS ACCÉLÉRÉE PAR LES EXIGENCES DU TRAVAIL À DISTANCE ET COLLABORATIF IMPOSÉES PAR LA CRISE SANITAIRE, NOTRE DÉPENDANCE AU NUMÉRIQUE A CONSIDÉRABLEMENT AUGMENTÉ. CONSÉQUENCE DIRECTE : LA SÉCURITÉ DU SYSTÈME D'INFORMATION N'EST PLUS SEULEMENT IMPORTANTE POUR L'ENTREPRISE… ELLE EN EST UNE COMPOSANTE VITALE. »

ANNE-LUCIE WACK

Présidente de la Conférence des grandes écoles

LES GRANDES ÉCOLES PILIERS DE LA FORMATION SUR LA CYBERSÉCURITÉ

Dans le monde connecté d'aujourd'hui, les étudiant(e)s doivent être sensibilisé(e)s et formé(e)s à la cybersécurité et ses enjeux sociétaux, économiques et géopolitiques.

Cette filière n'est plus réservée aux écoles d'ingénieurs, elle irrigue les programmes des écoles de management, de l'ENA, et des autres spécialités. Nos étudiants sont les dirigeants de demain et doivent avoir la capacité de protéger les données de leurs organisations. 85% des diplômés des grandes écoles s'insèrent dans les activités liées au numérique dont la cybersécurité est un aspect central. Ces jeunes diplômés contribuent au développement de l'innovation dans la société par la création de start-up et de grands projets de R&D, pour porter l'offre française aux premiers rangs mondiaux.

THIBAUT BECHETOILLE

Président Croissance Plus

FAITES DU NUMÉRIQUE UN OUTIL DE CONFIANCE !

Sécurité numérique, souveraineté, résilience : autant de mots qui sont dernièrement revenus au cœur de l'actualité. Ces sujets sont cruciaux pour les entreprises en croissance.

En 2020, 9 entreprises françaises sur 10 ont fait face à une tentative d'intrusion informatique. Le numérique organise désormais les échanges et la valeur dans les organisations. Il ne doit donc plus être un facteur de risque mais un levier de confiance.

Pour y parvenir, ce guide que CroissancePlus est fier de soutenir vous propose des conseils pratiques et applicables. Bonne lecture !

FRANÇOIS ASSELIN
Président de la CPME

ENTREPRENEURS, VOUS POUVEZ ÊTRE LA CIBLE D'UNE CYBERATTAQUE, PUISEZ LES BONS RÉFLEXES DANS CE GUIDE POUR VOUS EN PRÉMUNIR

Alors que la transition numérique des TPE-PME a connu une accélération spectaculaire avec la crise, les chefs d'entreprise doivent se protéger des cyberattaques qui se multiplient. Les petites entreprises ne sont pas épargnées, loin s'en faut, et peuvent être mises en grande difficulté par ces piratages intempestifs de leurs données. C'est pour cela qu'au-delà de la prise de conscience, acquérir de bons réflexes est indispensable. La CPME est partenaire de ce guide pratique, un outil précieux pour poursuivre votre digitalisation en toute sécurité.

CHRISTIAN POYAU
MEDEF, co-Président de la Commission Mutations Technologiques et Impacts Sociétaux

CYBERSÉCURITÉ : TOUS CONCERNÉS !

L'année 2020 a démontré que la cybersécurité était l'affaire de toutes les entreprises, et que l'on n'est jamais trop petit pour être une cible ! Face aux multiples risques que représentent les menaces cyber, il est essentiel de se préparer en amont, d'adopter des bonnes pratiques et de diffuser une culture de la cybersécurité au sein de l'entreprise. C'est ce que le MEDEF propose via son test en ligne adapté à tous les niveaux de connaissance : en matière de virus, et notre actualité le démontre, se tester c'est se protéger et protéger les autres.

PARTIE 1

MIEUX COMPRENDRE LA RÉALITÉ DU RISQUE AUJOURD'HUI

ÊTES-VOUS UNE CIBLE ?
16

LES GRANDS TYPES DE MENACES
18

À QUELS IMPACTS S'ATTENDRE ?
20

DEMAIN A DÉJÀ COMMENCÉ. 3 POINTS CLÉS À ANTICIPER
22

ET EN FRANCE ? NOTRE POSITION, NOS DÉCISIONS, NOS GRANDES INITIATIVES
24

C'EST ARRIVÉ TOUT PRÈS DE CHEZ VOUS… ET ÇA SE RAPPROCHE ENCORE. UN AN DE CYBERATTAQUES
26

LISE CHARMEL, 1ER REDRESSEMENT JUDICIAIRE APRES UNE ATTAQUE INFORMATIQUE !
28

LEXIQUE INDISPENSABLE
30

ÊTRE CONSCIENT

POURQUOI NOS DONNÉES LES PLUS ANODINES ONT DE LA VALEUR ?

Toutes les données intéressent désormais les *hackers*, pas seulement les mots de passe ou les numéros de carte de crédit. Même les données « ordinaires » ont de la valeur, car associées entre elles, elles rendent bien plus crédibles les attaques des cybercriminels : un message contenant plusieurs informations vraies (dates de congés, logiciel utilisé, date de naissance…) incite à cliquer davantage en confiance et rend le piège plus difficile à déceler. Soyons vigilants quand nous communiquons des données. À qui ? Sont-elles indispensables ?

ÊTES-VOUS UNE **CIBLE** ?

INTERNATIONALES, PLUS NOMBREUSES, PLUS SOPHISTIQUÉES, LES CYBERATTAQUES VISENT NOS ENTREPRISES, NOS SYSTÈMES ET CONVOITENT NOS DONNÉES… MÊME LES PLUS ANODINES.

x 4

EN 12 MOIS, LE NOMBRE D'ATTAQUES DE TYPE RANÇONGICIEL POUR LESQUELLES L'AGENCE NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION A DÛ INTERVENIR. UNE ACCÉLÉRATION TRÈS INQUIÉTANTE.

ANSSI - Janvier 2021

LA FACE CACHÉE DU MONDE DES CYBERCRIMINELS : UNE ORGANISATION REDOUTABLE

La cybercriminalité continue de se perfectionner et s'organise désormais comme une véritable industrie, avec une grande multiplicité d'acteurs (investisseurs, fournisseurs, prestataires, sous-traitants, R&D…). Par exemple, des organisations commercialisent des modèles d'attaques et font appel à des sous-traitants pour les concevoir. Ils vont jusqu'à vendre les mises à jour de leurs logiciels malveillants ! Des exploitants mènent les actions pour leurs propres comptes, ou pour distribuer ensuite les données volées à d'autres cybercriminels.

À CHACUN SON MARCHÉ

Comme pour n'importe quelle autre activité « commerciale », les cybercriminels visent un segment de marché en fonction de leurs moyens et de leur ambition. Certains attaquants s'intéressent aux grands comptes, complexes à atteindre mais très rentables en cas de succès. D'autres aux PME, qui demandent moins d'efforts car souvent moins bien protégées. **Avec un tel niveau d'industrialisation et de quadrillage du marché, on comprend que tout le monde est ciblé.**

LES GRANDS TYPES DE **MENACES**

AVEC LA TRANSFORMATION DIGITALE, LA SURFACE D'EXPOSITION AU RISQUE A AUGMENTÉ ET COUVRE PLUSIEURS ASPECTS DE LA VIE DES ORGANISATIONS. LE CYBERCRIME BÉNÉFICIE LUI AUSSI D'UNE TECHNOLOGIE DE PLUS EN PLUS PERFORMANTE.

CIBLÉES OU AUTOMATISÉES, LES ATTAQUES SONT ORGANISÉES ET COUVRENT UN SPECTRE TRÈS LARGE

Ciblées, les attaques sont particulièrement dangereuses. Elles s'appuient sur un travail d'ingénierie sociale et une préparation méticuleuse qui les rendent très difficiles à identifier.
Automatisées, elles sont très opportunistes, ne visent personne et tout le monde à la fois. Elles sont particulièrement redoutables car diffusées en masse, elles impactent toutes les entreprises. Ici, une seule règle compte : la qualité et le niveau de dispositif de sécurité en place.

ATTENTION À LA « BALLE PERDUE »

L'interconnexion grandissante entre les entreprises, les partenaires et les prestataires pose un sérieux problème d'effet domino en cas de compromission de l'un d'entre eux. Une entreprise peut ne pas être directement visée et pourtant être atteinte *via* l'un de ses partenaires victime d'une attaque, et voir ainsi ses systèmes contaminés. Pour éviter de devenir une victime collatérale, il est essentiel de s'intéresser à la sécurité des entreprises de son écosystème et d'exiger des garanties sur leur niveau de sécurité.

NOMBREUX ET AUX MOTIVATIONS MULTIPLES :

6 GRANDS PROFILS DES PRINCIPAUX ATTAQUANTS

- Les cybercriminels
- Les activistes
- Les États
- Les concurrents
- Les collaborateurs
- Les opportunistes

PRINCIPALES CYBERATTAQUES EN FRANCE

80 %
PHISHING OU *SPEAR PHISHING* (HAMEÇONNAGE CIBLÉ)

41 %
TENTATIVES DE CONNEXION (ESSAIS DE MOTS DE PASSE EN GRAND NOMBRE)

52 %
EXPLOITATION D'UN DÉFAUT DE CONFIGURATION (MAUVAIS PARAMÉTRAGE : ABSENCE DE MOT DE PASSE, DROIT ÉLEVÉ SUR UN SERVEUR…)

20 %
ATTAQUE PAR REBOND *VIA* UN PRESTATAIRE

3,6
TYPES D'ATTAQUES SUBIES EN MOYENNE PAR ENTREPRISE

Baromètre de la cybersécurité des entreprises, Cesin et OpinionWay, février 2021

LA « STAR » : LE COUPLE *RANSOMWARE/PHISHING*

Un seul clic et l'informatique est paralysée, les données sont *chiffrées*. Le principe est connu et pourtant il continue d'être sur le podium des compromissions les plus graves. Un e-mail usurpe le nom d'une entreprise de confiance et invite à cliquer sur un lien web ou à ouvrir une pièce jointe. Un programme malveillant se lance alors et chiffre toutes les données accessibles sur le système. La solution : compartimenter ce dernier et faire des sauvegardes régulières et indépendantes afin de récupérer ses données. Bien sûr, la sensibilisation des équipes est essentielle pour qu'elles augmentent leur vigilance et apprennent à détecter les fraudes et à ne pas cliquer sur n'importe quel lien.

QUAND LA MENACE VIENT DE L'INTÉRIEUR

- La négligence ou l'erreur « humaine ». Une mauvaise manipulation sur un dossier partagé à l'extérieur de l'entreprise donnera accès au système et ouvrira une fragilité.
- Les contournements des règles de sécurité.
- Le *shadow IT*, littéralement « informatique de l'ombre ». Il s'agit d'applications déployées par les collaborateurs ou les directions métiers sans l'aval ni le contrôle du service informatique et très souvent sans aucune sécurité (téléchargement d'application sur les smartphones, utilisation de services de partage de données…)
- Et, bien sûr, il y a la malveillance réalisée par des collaborateurs (indiscrétion, espionnage, vol de données…). Attention aux personnes qui disposent de droits élevés et accèdent facilement aux contenus numériques de l'entreprise : elles sont les cibles privilégiées des *hackers*.

À QUELS **IMPACTS** S'ATTENDRE ?

IMPACT INITIAL - PIC DE LA CRISE
premiers jours

EFFETS D'UNE CYBERATTAQUE ET COÛTS LIÉS

PERTES D'EXPLOITATION	• Arrêt du fonctionnement normal de l'entreprise, voire interruption d'activité sévère • Pertes de données indispensables au bon fonctionnement de l'entreprise • Arrêt des canaux de communication avec les clients/ fournisseurs • Perte de temps des équipes, démobilisation • Perte de clients, perte d'opportunités commerciales
COÛTS LIÉS À LA GESTION DE CRISE INFORMATIQUE	• Investigation, mobilisation d'expertise • Achat de matériel • Frais opérationnels de renfort (intérimaires métiers, saisies de données *a posteriori*, reconstruction de bases de données)
COÛTS LIÉS À LA COMMUNI-CATION	• Définition des messages, de la posture, communication auprès des collaborateurs, des clients, de l'écosystème, des autorités, des médias • Temps consacré à gérer les différentes interrogations
COÛTS JURIDIQUES	• Étude des impacts juridiques possibles • Gestion du dépôt de plainte de l'entreprise

LES CYBERATTAQUES PEUVENT COÛTER CHER, TRÈS CHER. C'EST MAINTENANT CONNU. IMPACTS DIRECTS, INDIRECTS, IMMÉDIATS OU DIFFÉRÉS, VOICI UNE ILLUSTRATION QUI DONNE LA DIMENSION ET DÉTAILLE L'ÉTENDUE DES CONSÉQUENCES POUR L'ENTREPRISE QUAND ELLE EST TOUCHÉE PAR UNE ATTAQUE.

À l'instar d'une explosion ou d'un tremblement de terre, l'entreprise traverse trois grandes phases qui s'inscrivent dans le temps. Il est peu probable d'échapper à une attaque sur le long terme. En s'y préparant ou en se protégeant, il est possible de diminuer les impacts, voire d'en éviter certains.

EFFET DE SOUFFLE *dans les mois qui suivent : de 1 à 3 mois*	**RÉPLIQUES** *effets rebonds de 6 mois à 3 ans*
• Dysfonctionnent interne • Activité en mode dégradé, ralentissement (désorganisation, rattrapages) • Frais de dédommagement	Révélation dans les médias, impacts dus aux changements organisationnels internes. Facteurs aggravants pour les activités B2C : visibilité négative de la marque, suite juridique GDPR
• Coût de reconstruction, de correction (peut monter jusqu'à 15 % du budget de la DSI) • Effet de rattrapage avec impact sur les pratiques internes - évolution des méthodes d'accès, conduite de changement qui peut être complexe...	
• Possibles rebonds à gérer en cas de fuite d'éléments nouveaux • Impact sur l'image dans le temps à suivre	
• Premières requêtes ou demandes des autorités • Audits complémentaires	• Suite des affaires judiciaires/juridiques • Coûts liés aux conseils et au temps consacré • Coûts des amendes éventuelles

Tableau réalisé avec le concours de Wavestone

DEMAIN A DÉJÀ COMMENCÉ. **3 POINTS CLÉS** À ANTICIPER

LA TRANSFORMATION NUMÉRIQUE S'ACCOMPAGNE D'UNE MUTATION PROFONDE DE L'ORGANISATION DES ENTREPRISES ET DES MODES DE COLLABORATION. LE TRAVAIL À DOMICILE, LE POUVOIR DES COLLABORATEURS SUR LES DONNÉES DE L'ENTREPRISE ET LA SOPHISTICATION DES ATTAQUES SONT TROIS ÉLÉMENTS DÉTERMINANTS.

1

ATTAQUES MASSIVES ET ULTRA SOPHISTIQUÉES : DU SUR-MESURE À GRANDE ÉCHELLE

Les e-mails malveillants contenant des fautes d'orthographe grossières et des logos mal reproduits sont de l'ordre du passé. Les cybercriminels progressent et les nouvelles technologies leur sont utiles pour réaliser des cyberattaques à la fois automatisées, massives et très personnalisées. Elles sont difficiles à identifier, et leur performance augmente considérablement. Elles font aujourd'hui déjà de nombreuses victimes. L'enjeu est de pouvoir disposer d'un outil de détection pour être immédiatement alerté en cas de compromission.

2

LE RÔLE GRANDISSANT DES COLLABORATEURS SUR LES DONNÉES ET LE SYSTÈME DE L'ENTREPRISE

Les nouvelles solutions de communication et de travail collaboratif ont transféré aux utilisateurs un pouvoir jusqu'alors réservé aux informaticiens de l'entreprise : le partage de données et de dossiers, l'attribution de droits d'accès plus ou moins élevés en interne voire en externe, etc. Limitées et très contrôlées auparavant, ces configurations se multiplient de façon exponentielle. Cette propagation des accès au système et aux données accroît d'autant plus l'exposition au risque.

3

L'ÉVOLUTION DES ORGANISATIONS ET DU TRAVAIL À DISTANCE

Et si, en 2020, la crise sanitaire avait été la répétition générale d'une mutation plus profonde du monde du travail ? Jusqu'au XVIIIe siècle, artisans, paysans, manufacturiers... travaillaient tous à domicile. Au XIXe siècle, le travail se déplace dans les usines. Le XXe siècle marque le règne de l'usine et des bureaux. Et au XXIe siècle... tout le monde retourne à la maison ! Avec un système d'information totalement étendu et très fragmenté, désormais porté par le *cloud* et avec des équipements mobiles dispersés, la sécurité numérique fait face à une nouvelle difficulté pour repenser ses modes de contrôle et de protection en profondeur.

UNE NOUVELLE FORME REDOUTABLE DE « CHEVAL DE TROIE » *VIA* LA COMPROMISSION D'UN LOGICIEL TRÈS UTILISÉ

La technique, très sophistiquée, consiste à infecter le logiciel d'un grand éditeur en y insérant un code malveillant. Les clients de l'éditeur sont automatiquement infectés à leur tour dès lors qu'ils lancent une mise à jour. Ce qui, comble de l'ironie, est indispensable pour bénéficier des nouvelles fonctionnalités mais surtout pour corriger les vulnérabilités et renforcer la sécurité du logiciel ! Très difficile à détecter et avec un rayonnement massif, ce type de menace engage à interroger les éditeurs sur l'intégrité de leur code. L'affaire Solarwinds a été un modèle du genre.

ET EN **FRANCE** ? NOTRE POSITION, NOS DÉCISIONS

LE RISQUE AUGMENTE, LA PLACE DE LA SÉCURITÉ NUMÉRIQUE AUSSI.

L'ARME CYBER EST DÉSORMAIS UNE ARME À PART ENTIÈRE

En janvier 2020, Florence Parly, ministre des Armées, présente la stratégie cyber de la France : le principe est assumé « d'utiliser l'arme cyber à des fins offensives, isolément ou en appui de nos moyens conventionnels ».

LA CYBERSÉCURITÉ AU CŒUR DE LA GÉOPOLITIQUE

Le cyberespace fait aujourd'hui partie des biens communs à l'humanité qu'il convient de réguler. Il devient donc un 5e espace stratégique, après les espaces maritime, aérien, orbital et fréquentiel.

LA SÉCURITÉ NUMÉRIQUE ENTRE À L'ÉCOLE

Depuis 2019, le ministère de l'Éducation nationale, de la Jeunesse et des Sports travaille sur l'intégration de programmes cyber, avec une première application envisagée dès le collège.

LE CYBER DEVIENT UN ENJEU ÉCONOMIQUE ET FINANCIER

100 % des rapports annuels des entreprises du CAC 40 contiennent maintenant un volet cybersécurité.

DES EXIGENCES RÉGLEMENTAIRES POUR LES ENTREPRISES

Après les OIV (opérateurs d'importance vitale), c'est aux 122 organismes et entreprises dont le service est considéré comme essentiel (OSE) de devoir garantir un niveau de sécurité minimal pour assurer leur protection (Directive européenne NIS – *Network and Information Security*).

LA CONFIANCE NUMÉRIQUE EN FRANCE :

2 134
ENTREPRISES

21
MILLIARDS D'EUROS DE CHIFFRE D'AFFAIRES

152
START-UP (+19 % EN UN AN)

+ 8,8 %
CROISSANCE MOYENNE ANNUELLE SUR 5 ANS, LA FILIÈRE FRANÇAISE QUI A LA PLUS FORTE CROISSANCE.

Observatoire de la confiance numérique 2020 ACN et radar Start up 2020 Wavestone

NOS GRANDES **INITIATIVES**

TOUS ENSEMBLE ! L'ÉLYSÉE INITIE LA CRÉATION EN FRANCE D'UN CAMPUS CYBER, UN LIEU UNIQUE EN EUROPE

Michel Van Den Berghe, CEO d'Orange Cyberdefense, est à la tête du Campus Cyber. L'ambition du projet a déjà été revue à la hausse, avec une 1ère réalisation d'un espace de plus de 26 000 m², situé à La Défense, dans le nouvel immeuble ERIA, et une extension est d'ores et déjà prévue près de Versailles.

PLUS DE 60 ORGANISATIONS RÉUNIES DANS UN SEUL LIEU POUR METTRE EN COMMUN LEURS COMPÉTENCES ET CONNAISSANCES ET PARTICIPER AU RAYONNEMENT DE LA FRANCE EN MATIÈRE DE CYBERSÉCURITÉ.

Sur une initiative du président de la République, le Premier ministre a confié à Michel Van Den Berghe une mission de préfiguration pour la création d'un campus dédié à la cybersécurité. L'objectif : rassembler entreprises, start-up, écoles et organisations publiques en un même lieu pour créer une synergie entre tous les acteurs ; augmenter les capacités de l'écosystème cyber et promouvoir l'excellence française en la matière. Volontairement animé par une structure dont la gouvernance repose sur un projet privé-public, le Campus Cyber développe une approche très entrepreneuriale et concrète. Start-up, industriels et entreprises se parleront directement et pourront travailler sur des projets communs.

Dès le second semestre 2021, près de 1 000 spécialistes mettront en commun leurs expertises et leurs idées en matière de cybersécurité. Leur objectif : mener à bien des projets concrets et opérationnels au profit de la société, de l'économie et de la compétitivité française. Des déclinaisons régionales du Campus sont prévues dans les années à venir.

Vous souhaitez en savoir plus et peut-être même rejoindre l'aventure ?
Contactez la « mission campus » :
contact@campuscyber.fr

C'EST ARRIVÉ TOUT PRÈS DE CHEZ VOUS… ET ÇA SE **RAPPROCHE** ENCORE.

LES ATTAQUES AUGMENTENT ET FONT CHAQUE JOUR DES VICTIMES DANS TOUS LES SECTEURS D'ACTIVITÉ ET DANS DES ENTREPRISES DE TOUTE TAILLE. CI-CONTRE, UN BREF APERÇU ILLUSTRANT L'ÉVOLUTION DES ATTAQUES CONNUES SUR UNE SEULE ANNÉE.

58 %

DES ATTAQUES SONT OPPORTUNISTES ET NE VISENT PAS UNE ENTREPRISE EN PARTICULIER.

Benchmark CERT-Wavestone, septembre 2019-août 2020

EN MOYENNE, IL FAUT

6 mois

À UNE ENTREPRISE POUR DÉTECTER UNE VIOLATION DE SES DONNÉES.

Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview

43 %

DES CYBERATTAQUES VISENT LES PETITES ENTREPRISES.

27 %

MOINS D'UN EMPLOYÉ SUR 3 A DÉJÀ REÇU DES INSTRUCTIONS DE SON EMPLOYEUR (TPE/PME) SUR LES MESURES DE SÉCURITÉ À PRENDRE AFIN DE TRAVAILLER DEPUIS SES APPAREILS PERSONNELS.

Étude Kaspersky, avril 2020

6

ENTREPRISES SUR 10 N'ONT PAS ALLOUÉ OU TRANSFÉRÉ DE BUDGET SPÉCIFIQUE POUR LUTTER CONTRE LA FRAUDE ET LA MENACE CYBER.

Étude fraude & cybercriminalité 2019, DFCG et Euler Hermes

41 %

DES ENTREPRISES N'ONT PAS DE PLAN D'URGENCE À ACTIVER EN CAS D'ATTAQUE.

Étude Bitdefender, juin 2020

UN AN DE CYBERATTAQUES

DÉCEMBRE
Dedalus / Agence européenne du médicament / Randstad Atlantic / Fareva / …

NOVEMBRE
Ville de Vincennes / Paris-Habitat / Les quotidiens *Paris-Normandie et Ouest-France* / Umanis / Scutum / Ville de Bondy / Siplec / Chambres d'agriculture de Nouvelle Aquitaine et de Centre-Val de Loire / Maisons Ty Breizh / …

OCTOBRE
Ville de Mitry-Mory / Ubisoft / Orléans Métropole / Sparflex / Verimatrix / Sopra Steria / …

ET LA MAJORITÉ N'EST PAS RENDUE PUBLIQUE…

SEPTEMBRE
Bouygues Telecom / SFR / CMA-CGM / Ville et Métropole de Besançon / Tribunal de Paris / Orpea / Gefco / Mr Bricolage / …

AOÛT
Leon Grosse / Groupe MOM (Materne & Mont Blanc) / Prismaflex International / Expanscience / Cabinet d'avocats Cornet Vincent Ségurel / Peugeot Motocycles / …

JUILLET
MMA / Spie / Conseil départemental 28 / Orange Business Services / Ademe / Rabot-Dutilleul / Doctolib / …

JUIN
France Télévisions / Logéal Immobilière / Fountaine-Pajot / Cadiou Industrie / …

MAI
Cooperl / Tarkett / Roger Martin / Porcher Industries / Bolloré Logistics / Hôpital de Fleurance-Lectoure / …

AVRIL
Cognizant / Champagne FM / Mairie de Toulouse / Toulouse Métropole / …

MARS
AP-HP / Mairie de Marseille / Métropole Aix-Marseille / Afpa / EssilorLuxottica / DMC / …

FÉVRIER
Région Grand-Est / Aro Welding Technologies / Bretagne Telecom / …

JANVIER
Bouygues Construction / …

LISE CHARMEL, 1ER **REDRESSEMENT JUDICIAIRE** APRÈS UNE ATTAQUE INFORMATIQUE !

VICTIME D'UN RANÇONGICIEL EN NOVEMBRE 2019, L'ENTREPRISE DE LINGERIE FÉMININE LISE CHARMEL N'A PAS EU D'AUTRE SOLUTION QUE DE SE PLACER EN REDRESSEMENT JUDICIAIRE. C'ÉTAIT LE SEUL MOYEN DE RETROUVER QUELQUES MARGES DE MANŒUVRE, TROIS MOIS APRÈS L'ATTAQUE.

FÉVRIER 2020

Le jeudi 27, le tribunal de commerce de Lyon prononce le placement de l'ensemble des entités françaises du groupe Lise Charmel en redressement judiciaire. Les dirigeants de l'entreprise sont soulagés, car c'est à leur demande que le tribunal a pris cette décision, pour pouvoir redémarrer l'activité dans les meilleures conditions, hors de toute pression financière. Un redressement « technique » en quelque sorte, selon les mots d'Olivier Piquet, directeur général.

MAIS COMMENT EN EST-ON ARRIVÉ LÀ ? RETOUR SUR TROIS MOIS ÉPROUVANTS.

NOVEMBRE 2019

Vendredi 8, à 7 heures du matin, les collaborateurs du service logistique sont empêchés de se mettre au travail. Leurs postes sont chiffrés et inopérants, comme ceux de l'ensemble du personnel, en France et dans le monde. Aucun fichier, aucune donnée

n'est accessible. L'ensemble de la chaîne, de la création à la production, en passant par la logistique et les boutiques, entièrement informatisée, est bloquée. Même le téléphone ne fonctionne plus.

DÉCEMBRE 2019

L'entreprise est toujours en état de choc. La rançon, exigée par les pirates en échange de la clé supposée permettre de déchiffrer les données n'a pas été payée. Les dirigeants ont fait le choix de reconstruire le système d'information. L'activité reprend doucement après plusieurs semaines d'arrêt complet.

JANVIER 2020

Après deux mois de paralysie plus ou moins totale, l'activité peut pleinement repartir. Mais le retard accumulé est considérable. Le manque à gagner et le coût de la reconstruction du SI se chiffrent certainement à plusieurs millions d'euros, même si l'entreprise préfère ne pas communiquer sur ce point.

MARS 2020

L'entreprise qui a porté plainte commence à mieux comprendre ce qui lui est arrivé grâce aux investigations de la police : **à l'origine du piratage, un simple clic dans un email reçu par un collaborateur sur sa boîte personnelle qu'il a consultée depuis un des postes de l'entreprise pendant la pause-déjeuner.**

OLIVIER PIQUET SOUHAITE PASSER DEUX MESSAGES À SES CONFRÈRES CHEFS D'ENTREPRISE :

1. Aucun système de sécurité n'est infaillible.

2. Préparez-vous donc au pire, en mettant en place un plan de relance pour pouvoir repartir de zéro.

Lise Charmel est une PME familiale spécialisée dans la création, la production et la distribution d'articles de corsetterie-lingerie et de balnéaire. L'entreprise emploie 1 150 collaborateurs dont environ 400 en France, principalement dans la région lyonnaise. Elle détient cinq marques, plutôt positionnées dans le haut de gamme : Lise Charmel bien sûr, née dans les années 1950, Éprise, Épure, Antinéa, et Antigel. Le groupe réalise près de 60 M€ de chiffre d'affaires.

LEXIQUE INDISPENSABLE

APT (ADVANCED PERSISTENT THREAT)
Forme typique d'attaque sophistiquée et très préparée, concentrée sur une organisation ciblée. Elle consiste à installer de façon très discrète des codes malveillants qui vont être actifs sur une longue période, dans le but, par exemple, de voler des données ou de provoquer des dysfonctionnements.

BACKDOOR
« Porte dérobée » dans un logiciel ou un matériel afin de transformer ce dernier en cheval de Troie à des fins d'espionnage ou de malveillance. C'est par exemple ce dont les États-Unis ont accusé Huawei.

BOTNET
Réseau constitué d'un grand nombre d'ordinateurs dont les cybercriminels ont pris le contrôle. Ils agissent alors comme des robots à l'insu de leurs propriétaires, exécutant les actes malveillants qui leur sont transmis : envoi d'emails en masse (spam), saturation d'un site web (deni de service DDoS)…

CRYPTOGRAPHIE
Consiste à coder, on dit « chiffrer », des documents ou des données afin de les rendre illisibles, incompréhensibles à toute personne ne disposant pas de la clé de déchiffrement. Cette technique permet de protéger les communications et les bases de données qui, même en cas d'accès malveillants ou de vol, se révéleraient quasiment impossibles à utiliser.

DARKNET / DARKWEB
Réseau internet caché où la navigation est anonyme. Il donne accès au *darkweb*, internet « parallèle », utilisé en particulier pour la communication des dissidents politiques, des activistes et des organisations criminelles. On trouve par exemple sur le *darkweb* des sites de vente d'armes, de stupéfiants et de données volées (CB, mots de passe…).

DDOS
(Distributed Denial-of-Service : attaque par déni de service distribué) Attaque contre un serveur, un site web ou une infrastructure en le/la submergeant par un trafic si important que son fonctionnement est perturbé, voire devient impossible.

EDR
(Endpoint Detection and Response) Placés sur les terminaux (postes de travail, serveurs), les EDR analysent et surveillent toutes les actions réalisées afin de repérer les commandes suspectes et de les bloquer.

FIREWALL
(Pare-feu) Solution de sécurité qui filtre les flux entrants sur le réseau informatique de l'entreprise afin de bloquer ou de mettre « en quarantaine » la présence d'éléments malveillants ou ne correspondant pas à sa politique de sécurité.

MALWARE
(*Malicious software* : logiciel malveillant) Programme informatique hostile qui, s'il réussit à s'installer, auto exécute des actions malveillantes sur le système informatique (virus, vers, cheval de Troie, *ransomware*, etc.).

PHISHING
(Hameçonnage) Technique frauduleuse d'envoi d'e-mails destinée à leurrer le destinataire en se faisant passer, par exemple, pour une entreprise connue afin de l'inciter à communiquer des données confidentielles (mots de passe, cartes bancaires…) ou à cliquer sur un lien corrompu pour installer un programme malveillant.

RANSOMWARE
(Rançongiciel) Programme malveillant souvent porté par un *phishing* (cf. plus haut), qui rend illisibles les données situées sur les postes ou les serveurs de l'entreprise en les chiffrant automatiquement. Les cybercriminels demandent le paiement d'une rançon contre l'envoi de la clé de déchiffrement.

SHADOW IT
Littéralement : informatique de l'ombre. C'est l'installation de logiciels et/ou la connexion de matériels sur le réseau de l'entreprise par des salariés ou des directions métiers, sans que ceux-ci ne soient ni connus, ni encore moins vérifiés et validés par la direction informatique. Le *shadow IT* est l'un des grands vecteurs de vulnérabilités.

VPN
(*Virtual private network*) Très utilisé pour les connexions et le travail à distance, un logiciel de VPN permet de créer un « tunnel » de connexion sécurisé entre les ordinateurs et le réseau de l'entreprise.

ZERO TRUST
Modèle de sécurité qui repose sur le principe qu'aucun accès d'utilisateur, y compris interne, n'est digne de confiance sur un réseau. Grâce à un processus strict de contrôle de l'identité, seuls les utilisateurs et les terminaux authentifiés et autorisés peuvent accéder au réseau, à leurs applications et à leurs données.

PARTIE 2

PROTÉGER SON ENTREPRISE : REPÈRES ET CONSEILS ESSENTIELS

SE CONCENTRER SUR LES POINTS CLÉS, 9 RECOMMANDATIONS PRIORITAIRES
34

QUELLE ORGANISATION ? QUELS INDICATEURS ? QUEL BUDGET ?
38

CONSEILS PRATIQUES À FORTE VALEUR AJOUTÉE
40

MUSCLER SA DÉFENSE GRÂCE À SES COLLABORATEURS
42

LES BONNES IDÉES DES ENTREPRISES POUR AMÉLIORER LEUR CYBERSÉCURITÉ
44

POINT JURIDIQUE FLASH
46

CARNET D'ADRESSES
50

SE CONCENTRER SUR LES POINTS CLÉS

9 RECOMMANDATIONS PRIORITAIRES

LA SÉCURITÉ NUMÉRIQUE SE PILOTE AVEC DES PRIORITÉS, COMME TOUTE AUTRE ACTIVITÉ DE L'ENTREPRISE. SI ELLE ENGAGE LES DIRIGEANTES ET DIRIGEANTS DANS LEURS CHOIX STRATÉGIQUES, ELLE RÉPOND SOUVENT À QUELQUES QUESTIONS DE BON SENS. EN VOICI 9, ESSENTIELLES. ELLES SONT SIMPLES, ÉVIDENTES ? TANT MIEUX !

01 QUELLES SONT NOS ACTIVITÉS LES PLUS INDISPENSABLES AU FONCTIONNEMENT DE L'ENTREPRISE ?

Cela semble sonner comme une évidence, mais il s'agit bien de faire cet exercice : quelles sont nos activités vitales ? Quel dispositif les protège et/ou nous garantit de pouvoir les faire fonctionner même en mode dégradé si elles étaient compromises. Ici, avec **un arbitrage éclairé des risques**, l'entreprise doit savoir quelles parties doivent être couvertes en priorité et quels contournements de secours peuvent être mis en place en cas d'indisponibilité. Il est indispensable de commencer par là.

02 AVONS-NOUS IDENTIFIÉ NOS DONNÉES SENSIBLES ?

Il en est de même avec les données : la disparition, le vol, la divulgation, l'indisponibilité de certaines d'entre elles peuvent causer un préjudice élevé. Ici aussi, avoir identifié **celles qui doivent rester confidentielles ou disponibles permet de déployer un dispositif de sécurité adapté** pour les protéger.

03 SOMMES-NOUS ACCOMPAGNÉS ? AVONS-NOUS ACCÈS À TOUTE L'EXPERTISE NÉCESSAIRE ?

Mettre en place un dispositif de sécurité performant et adapté exige un éventail de compétences et d'expertises difficilement disponibles dans l'entreprise. De même, en cas d'attaque, **l'aide d'un conseil expert** est souvent indispensable. Il peut permettre d'augmenter de façon déterminante la capacité et l'efficacité de la réaction. Identifier un partenaire pour accompagner son entreprise et ses collaborateurs en charge de la sécurité est donc aujourd'hui essentiel.

04 ENSEMBLE, ON DÉCIDE MIEUX : METTONS EN PLACE UN « CYBER-COMEX ».

De nombreux sujets de sécurité impactent directement l'activité et l'organisation de l'entreprise. Or, il s'agit d'arbitrer au mieux de l'intérêt du « business » et des métiers. Mettre en place **une gouvernance dédiée à la sécurité** augmente considérablement la capacité à tout envisager : Quel niveau de risque est acceptable ? Quelle modification des *process* est pertinente ? Quels investissements sont prioritaires ? Entouré d'un membre de la direction générale et de représentants métiers, la personne en charge de la sécurité prendra avec eux les décisions les plus adaptées. Ce cyber-comex se réunit sur son initiative, quand un sujet l'exige et, bien sûr, à fréquence régulière.

05 SAVONS-NOUS QUI PEUT FAIRE QUOI ET QUI FAIT QUOI SUR LES DONNÉES ?

La gestion des droits et des accès, la capacité de savoir qui peut faire quoi, qui a fait quoi sur quelles données est devenue essentielle. En insufflant **une culture de la sécurité** sur ce point dans l'entreprise, les risques de fuite de données seront fortement réduits. En particulier, la possibilité d'un accès aux systèmes par un compte non habilité ou compromis sera limitée.

06 SOMMES-NOUS PRÉPARÉS À UNE CRISE MAJEURE ?

La question se pose car il est aujourd'hui réaliste d'être victime d'une attaque lourde qui paralysera les systèmes d'information. Plusieurs entreprises citées dans les exemples de ce guide peuvent en témoigner. Après avoir répondu à la question 1, il est indispensable d'anticiper d'autres aspects : **la gestion de la crise elle-même et la communication. Un conseil : il faut s'entraîner.**

07 FOURNISSEURS, PRESTATAIRES ET PARTENAIRES : ÉVITONS LE MAILLON FAIBLE

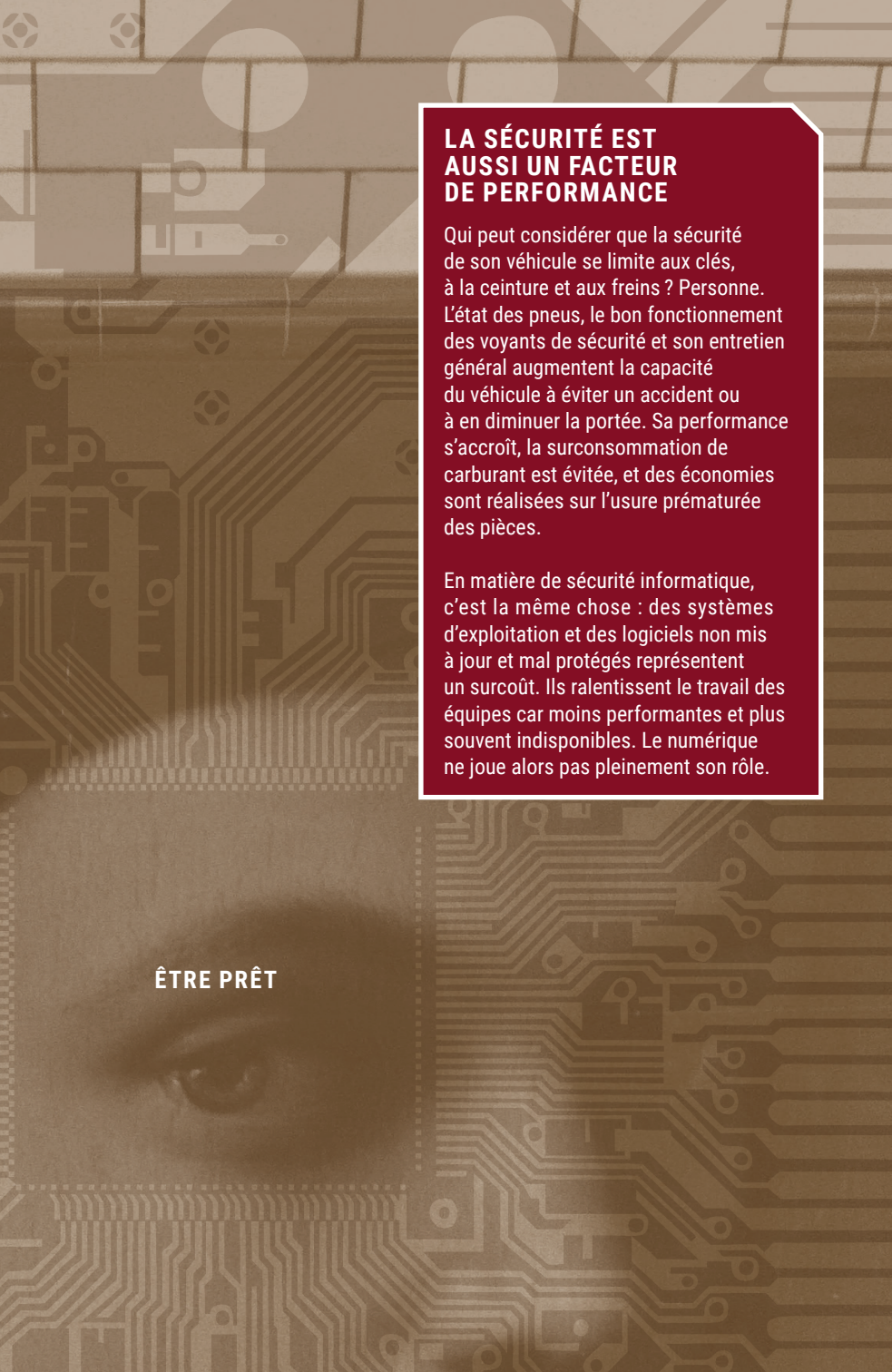
Tout comme les collaborateurs, les fournisseurs, les prestataires et les autres partenaires sont des portes d'entrée possibles pour les cyberattaquants. L'entreprise peut ainsi être visée à travers l'un d'eux ou être une victime collatérale. Avec la personne responsable de la sécurité numérique, il est nécessaire de passer en revue les données, les fichiers, les applications partagées et **les modes d'interconnexion avec les parties prenantes** afin de déterminer quelles procédures mettre en place pour se protéger. Il faut également solliciter le responsable juridique pour insérer une clause de cybersécurité dans les contrats.

08 SOMMES-NOUS ASSURÉS ? SOMMES-NOUS COUVERTS EN CAS DE CRISE CYBER ?

« Mon 1er conseil : assurez-vous. » C'est la recommandation claire de Dominique Cerutti, PDG du grand cabinet de conseil en ingénierie Altran, après une attaque majeure dont son entreprise a été victime fin 2019. Cela permet d'avoir accès rapidement à **tous les experts nécessaires – juridiques, techniques, communication –** et de couvrir la perte financière liée aux dégâts subis, à leur réparation, ainsi qu'à la baisse de revenus due à l'arrêt de l'activité. Il convient de vérifier les contrats actuels, d'étudier des polices spécifiques. C'est une mesure qu'il devient difficile d'ignorer et sans doute est-elle désormais vitale pour la plupart des entreprises, en particulier pour les PME.

09 QUI EST RESPONSABLE ET QUAND AI-JE ENTENDU PARLER DE SÉCURITÉ POUR LA DERNIÈRE FOIS ?

Et quand ai-je parlé de sécurité à l'entreprise ? À mes équipes ? La question cyber est-elle embarquée dans ma stratégie et dans mon quotidien ? Comment les membres du Comex vivent-ils cette question ? De quand date leur dernier *reporting* ? **Parler cyber avec les équipes**, c'est parler de notions vitales.



LA SÉCURITÉ EST AUSSI UN FACTEUR DE PERFORMANCE

Qui peut considérer que la sécurité de son véhicule se limite aux clés, à la ceinture et aux freins ? Personne. L'état des pneus, le bon fonctionnement des voyants de sécurité et son entretien général augmentent la capacité du véhicule à éviter un accident ou à en diminuer la portée. Sa performance s'accroît, la surconsommation de carburant est évitée, et des économies sont réalisées sur l'usure prématurée des pièces.

En matière de sécurité informatique, c'est la même chose : des systèmes d'exploitation et des logiciels non mis à jour et mal protégés représentent un surcoût. Ils ralentissent le travail des équipes car moins performantes et plus souvent indisponibles. Le numérique ne joue alors pas pleinement son rôle.

QUELLE **ORGANISATION** ?

IL EXISTE PLUSIEURS MODES D'ORGANISATION DE LA CYBERSECURITE DANS LES ENTREPRISES, SELON LES CONFIGURATIONS DE CHACUNE. DANS TOUS LES CAS, ELLE DOIT RÉPONDRE À QUELQUES PRINCIPES FONDAMENTAUX.

Bien sûr, il existe plusieurs modèles d'organisation, mais le besoin a évolué, et les organisations efficaces ont toutes 3 points communs :

- La cybersécurité est gérée comme un **élément transversal dans l'entreprise**. Elle concerne tout le monde, à tous les niveaux, depuis la conception d'un projet jusqu'à son exécution et la vente.
- **Mandat clair, proximité avec le Comex, liberté d'action :** appliquer ces trois grands principes garantit l'efficacité de la mission du responsable de la sécurité. Sa parole aura une meilleure portée, et le management conservera la main sur la politique de sécurité la plus adaptée à sa stratégie.
- **Une séparation des rôles** : les collaborateurs en charge de contrôler la sécurité et les dispositifs ne sont pas ceux qui doivent exécuter leur mise en place.

LE RISQUE ÉVOLUE, L'ORGANISATION AUSSI : L'APPARITION DU DIRECTEUR CYBERSÉCURITÉ

De plus en plus d'entreprises confient un rôle de premier plan à la personne en charge de la sécurité numérique en l'élevant au rang de directeur, avec parfois même une position de cadre dirigeant. Le responsable de la sécurité des systèmes d'information devient Directeur Cybersécurité, un peu comme quand les responsables du personnel sont devenus DRH à la faveur d'une adaptation aux enjeux d'une meilleure gestion des ressources humaines.

"SECURITY IS ALWAYS SEEN AS TOO MUCH UNTIL THE DAY IT'S NOT ENOUGH." **William H. Webster, ex-directeur du FBI**

(« LA SÉCURITÉ EST TOUJOURS CONSIDÉRÉE COMME EXCESSIVE, JUSQU'AU JOUR OÙ ELLE NE SUFFIT PAS. »)

QUELS **INDICATEURS** ?

La norme ISO 27001 et les 42 mesures d'hygiène de l'ANSSI sont le meilleur cadre pour demander un suivi et une comparaison de la situation de l'entreprise. Elles permettent aussi d'avoir un tableau de bord simple et clair.

Il est aussi important de mesurer l'écart entre la situation réelle de l'entreprise et les objectifs qu'elle s'est fixés. Pour suivre la progression, il est assez efficace de demander à la personne en charge de la sécurité de proposer un « *Security Score* », dont les composants peuvent s'appuyer sur les 3 indicateurs suivants :

- **Suivi des incidents** : « Sommes-nous attaqués ? Sur quoi ? Avec quelle intensité ? » Il est capital d'avoir une vision de tous les incidents dont l'entreprise est victime, même mineurs. Il faut donc les répertorier pour être capable d'évaluer leur impact et de savoir contre quoi se défendre.
- **Suivi des fragilités de son entreprise** : « Sommes-nous protégés ? Sur quoi ? » La sécurité est une question d'arbitrage, il est clé de connaître les vulnérabilités qui exposent l'entreprise et d'avoir conscience du risque associé. Cela aide également à mieux décider du dispositif à construire et de ses priorités.
- **Suivi des projets sécurité** : les grands projets qui couvrent précisément les fragilités de l'entreprise doivent être partagés. Leur avancement et leurs objectifs de réalisations doivent être suivis par la direction.

QUEL **BUDGET** ?

C'est la question que tout le monde attend ! Et elle est évidemment complexe. Il y a autant de réponses que de situations envisageables.
Tout d'abord, le plus important est d'identifier le budget dépensé : savoir combien l'entreprise investit chaque année.
Ensuite, un repère peut être utile : consacrer à la sécurité 5 à 10 % du budget informatique indique déjà un bon niveau de prise en compte du sujet.

PERTINENCE DU BUDGET

Dans tous les cas, il est essentiel de ne pas faire un arbitrage budgétaire « froid », seulement lié aux statistiques, qui serait déconnecté du contexte de l'entreprise, de son activité, de sa sensibilité au risque.
L'idéal, mais c'est un idéal presque indispensable, est de lier le budget à une analyse de risque. C'est le meilleur moyen d'investir un budget pertinent, en conscience des risques que l'entreprise considère acceptables et de ceux qui doivent être impérativement couverts.

DIRIGEANTES ET DIRIGEANTS DU COMEX

DIRECTION ACHATS, COMMERCIALE, COMMUNICATION, FINANCIÈRE, JURIDIQUE, LOGISTIQUE, MARKETING, RELATIONS PRESSE, RESSOURCES HUMAINES, SYSTÈMES D'INFORMATION, SECRÉTARIAT GÉNÉRAL, SUPPLY CHAIN, TECHNIQUE, TRANSFORMATION NUMÉRIQUE, WORKPLACE,…

CONSEILS PRATIQUES À FORTE VALEUR AJOUTÉE

VOICI UNE SÉLECTION DE POINTS D'ATTENTION PRIORITAIRES ET QUELQUES RÈGLES SIMPLES MAIS À FORT EFFET DE LEVIER POUR AUGMENTER SENSIBLEMENT LA PROTECTION ET SON *LEADERSHIP* SUR LE SUJET.

01 *SECURITY BY DESIGN* : LA SÉCURITÉ EST BIEN PLUS SIMPLE ET EFFICACE QUAND ELLE EST MISE EN PLACE DÈS LA NAISSANCE DES PROJETS

Qui construirait sa maison sans se préoccuper de sa sécurité, de la qualité de ses fondations, de la pérennité de sa structure ? S'interroger sur les questions de sécurité et associer très tôt la personne compétente de l'entreprise, c'est construire un projet sain, éviter les conséquences de fragilités laissées ouvertes. **Le coût est nettement moins élevé au départ qu'une fois le projet achevé.**

02 GESTION DES DROITS, « QUI PEUT FAIRE QUOI » : LA BONNE EXPLICATION

Qui peut accéder au CRM, au système RH, au dossier partagé de la direction du service ? Souvent vue comme une marque de confiance ou même comme un signe de position « sociale » dans l'entreprise, l'attribution des droits d'accès est souvent une question complexe à gérer pour les managers. Il s'agit en fait et uniquement de limiter l'exposition au risque. La question est donc : qui a besoin d'avoir quel type d'accès sur quelles données, quelles applications ? **Le niveau de droit accordé doit être cohérent avec le besoin de chaque collaborateur.** Ainsi, en cas d'attaque, de fraude ou d'usurpation des comptes, l'impact peut être considérablement réduit, voire nul, si l'utilisateur infecté dispose de droits limités. **Un manager responsable doit accepter de ne pas avoir de droits élevés s'ils ne lui sont pas indispensables.**

03 *SHADOW IT* : TELLEMENT SIMPLE… ET TELLEMENT RISQUÉ

La dernière application à la mode pour synchroniser les tâches de l'équipe ; le nouveau module de gestion d'événements « prêt à l'emploi » et si facile à connecter à la base de données… : **le digital offre mille raisons de se laisser tenter par de nombreuses applications. Celles-ci peuvent être un vecteur de compromission du système d'information.** Et leur notoriété ou leur cote ne sont pas la garantie de leur fiabilité d'un point de vue sécurité. La bonne approche n'est pas de s'en passer par principe mais d'interroger le service informatique et/ou la personne en charge de la sécurité. Ils vérifieront l'impact possible, aideront à paramétrer et à sécuriser l'application, sinon chercheront une alternative plus sûre.

04 IDENTIFIER LES POINTS CRITIQUES ET LES DONNÉES SENSIBLES DE SON SERVICE. LES COMMUNIQUER AU RSSI ET S'ASSURER DE LEUR SAUVEGARDE

De quoi a-t-on besoin pour travailler ? Quelles sont et où sont les données les plus sensibles ? Travailler avec son équipe sur ces questions et partager les résultats avec la personne en charge de la sécurité numérique est indispensable. C'est ensemble que sera mis en place un dispositif protecteur des données clés et de la continuité de l'activité en cas d'attaque.

05 DONNER L'EXEMPLE ET RENFORCER SON *LEADERSHIP*

« Donner l'exemple n'est pas le principal moyen d'influencer les autres, c'est le seul. » Cette citation (attribuée à Einstein, Gandhi ou encore A. Schweitzer) est parfaitement adaptée à la sécurité numérique. Un peu plus exigeante, portant aussi des enjeux majeurs pour la vie de l'entreprise, la sécurité numérique offre aux managers un moyen d'affirmer leur sens des responsabilités. **Montrer l'exemple, être clair et pédagogique sur le respect des règles**, c'est augmenter sa stature en étant fort sur une question stratégique.

06 RENCONTRER LA PERSONNE EN CHARGE DE LA SÉCURITÉ NUMÉRIQUE

Inviter la personne en charge de la sécurité numérique dans les réunions d'équipes, tous les 3 ou 6 mois : un point flash, un échange sur les difficultés rencontrées, les craintes… C'est un excellent moyen de faire évoluer favorablement ce sujet au sein de l'équipe. C'est aussi surtout une très bonne façon de nouer une relation privilégiée et constructive. Très utile quand, ensemble, il s'agira de trouver le meilleur équilibre entre sécurité et ergonomie pour la mise en place de solutions pour le département. Si l'entreprise dispose déjà d'un Risk manager il est bon de l'associer et d'avoir la même approche.

MUSCLER SA DÉFENSE GRÂCE À SES **COLLABORATEURS**

LONGTEMPS VUS COMME UN FACTEUR DE RISQUE, LES COLLABORATEURS DEVIENNENT L'UNE DES CLÉS ESSENTIELLES POUR AMÉLIORER LA SÉCURITÉ DE L'ENTREPRISE. PLUS AUTONOMES, ILS GÈRENT ET PARTAGENT DE PLUS EN PLUS DE DONNÉES. ILS SONT DAVANTAGE EXPOSÉS ET DOIVENT DONC FAIRE PARTIE DU SYSTÈME DE DÉFENSE. PLUS IMPLIQUÉS, ILS PEUVENT APPORTER UNE CONTRIBUTION DÉTERMINANTE.

PREMIERS BÉNÉFICIAIRES DE LA TRANSFORMATION DIGITALE MAIS AUSSI PREMIÈRES CIBLES DES CYBERCRIMINELS

Le rôle des salariés évolue à vitesse grand V. Ils sont désormais plus exposés, et de très nombreuses attaques avec des conséquences lourdes pour toute l'entreprise passent indifféremment par n'importe quel collaborateur (*phishing*, *ransomware*…). D'où l'importance de les engager tous pleinement.

« SENSIBILISER LES COLLABORATEURS À LA CYBERSÉCURITÉ ET LEUR DONNER DES MOYENS POUR QU'ILS SOIENT PLUS RESPONSABLES ET PLUS ACTIFS N'EST PLUS UNE OPTION »

QUE PENSENT-ILS AUJOURD'HUI ? QUEL RAPPORT ONT-ILS AVEC LA SÉCURITÉ DE LEURS DONNÉES ET CELLE DE L'ENTREPRISE ?

Sondage Ifop novembre 2019 – « Les Salariés et la Sécurité des données au travail »

Les points à améliorer :

- 45 % des collaborateurs se disent inquiets pour la sécurité de leurs données et des outils numériques utilisés dans le cadre de leur travail
- 1/4 déclarent même qu'ils n'utilisent pas ces derniers par crainte (quel gâchis !).

Le message est clair, ils ont besoin de mieux comprendre et d'avoir confiance.

Les points favorables : + de 80 %

- Ont conscience de l'enjeu sociétal de sécurité numérique et le placent au même niveau que d'autres grands enjeux comme l'écologie ou le développement durable.
- Disent avoir également conscience de la nécessité de leur implication pour que l'entreprise soit mieux protégée.
- Souhaitent avoir davantage de visibilité sur la sécurité et les accès à leurs données.

UN POTENTIEL À RENFORCER

Les utilisateurs finaux participent déjà à la détection de 25 % des attaques, devant **les services de détection cybersécurité** (24 %).

CERT-Wavestone, septembre 2019-août 2020

60 %

DES CYBERATTAQUES PEUVENT ÊTRE ATTRIBUÉES À DES COMPORTEMENTS HUMAINS INADÉQUATS*. PLUS ENGAGÉS, MIEUX FORMÉS, LES SALARIÉS SONT UN LEVIER DE DÉFENSE IMPORTANT.

*Accenture, « State of Cybersecurity Report 2020 »

DES MESURES À METTRE EN PLACE

Sensibiliser les collaborateurs à la cybersécurité et les former n'est plus une option. Si l'entreprise ne s'est pas emparée du sujet, il est possible de le faire à l'échelle des équipes. De nombreuses sociétés se sont spécialisées dans ce domaine et peuvent aider (formations, simulations d'attaques, conférences, *gaming*…)

Donner des moyens aux collaborateurs pour qu'ils soient plus responsables et plus actifs : des outils existent pour signaler un email suspect, leur permettre de contrôler les accès à leurs données.

LES **BONNES IDÉES** DES ENTREPRISES POUR AMÉLIORER LEUR CYBERSÉCURITÉ

VOICI QUELQUES BONNES PRATIQUES MISES EN PLACE DANS LES ENTREPRISES LES PLUS AVANCÉES POUR AMÉLIORER LA SÉCURITÉ ET LA CONSCIENCE SÉCURITÉ DE LEURS ÉQUIPES.

Les collaborateurs qui remontent une information aux équipes sécurité reçoivent **UN MAIL DE REMERCIEMENT PERSONNALISÉ DE LA DIRECTION GÉNÉRALE**.

UN CORRESPONDANT SÉCURITÉ NUMÉRIQUE, *LEADER* DU SUJET, DANS CHAQUE SERVICE.
Ce responsable « *security champion* », interlocuteur de la personne en charge de la sécurité dans l'entreprise, aide les autres membres de son service. Une responsabilité valorisée dans sa fiche de poste.

Créer **UNE CHARTE SÉCURITÉ**, c'est bien. Portée et **ASSUMÉE PAR LA DIRECTION MARKETING** c'est mieux. Elle véhiculera une autre image.

Pendant 1 an, cette équipe cyber a lancé un défi sous la forme d'**UN JEU : REPÉRER LES *PHISHINGS* PARMI LES MAILS REÇUS** quotidiennement.

« UN DOUTE SUR CE MAIL ? CLIQUEZ SUR CE BOUTON ! »
La direction a intégré un *plug-in* sur Outlook pour tous les postes internes. Les utilisateurs sont sensibilisés aux mails intrusifs et peuvent facilement signaler les mails suspects.

Les dirigeants profitent d'**UN *COACHING* CYBER PERSONNALISÉ ET RÉGULIER** d'1 heure ou 2 par trimestre.

Prendre en compte **LA COMPÉTENCE ET L'IMPLICATION SUR LA SÉCURITÉ DANS LES ÉVALUATIONS INDIVIDUELLES** : pas d'évolution possible sans validation de cette compétence.

L'entreprise donne à ses collaborateurs **UN CAHIER D'EXERCICES SUR LA CYBERSÉCURITÉ QUI S'ADRESSE AUSSI AUX ENFANTS**. Une bonne façon d'éveiller la conscience cyber des équipes en les invitant à améliorer la sécurité dans leur sphère privée.

Le cyber, c'est une question de culture d'entreprise. La direction de la communication l'intègre dans ses opérations. **CHAQUE MOIS, UN TÉMOIN VIENT PARLER, ACCOMPAGNÉ D'UN INTERVENANT CYBER**. Par exemple, le jardinier de Versailles est venu parler de la résilience des plantes…

La cybersécurité est un sujet transversal : tout le monde est concerné. **UNE CAMPAGNE DE SENSIBILISATION PORTÉE PAR LA DIRECTION DE LA COMMUNICATION** familiarise avec le sujet, infusé dans l'entreprise au même titre que tous les autres thèmes traités.

À propos de communication, les membres du Comex reçoivent **UNE NEWSLETTER MENSUELLE DÉDIÉE À LA CYBERSÉCURITÉ** avec la liste des attaques récentes afin de bien prendre conscience du danger qui s'approche. Pourquoi ne pas y ajouter la liste des partenaires et des fournisseurs de l'entreprise qui ont été victimes d'attaques ?

Une grande entreprise française organise chaque année en interne **UN RADIO-TROTTOIR, AVEC DES QUESTIONS LUDIQUES ET DES EXPLICATIONS PÉDAGOGIQUES**. Évidemment, des cadeaux récompensent les bonnes réponses.

POINT JURIDIQUE FLASH

LE RISQUE ÉVOLUE, LA LOI AUSSI. CE QU'IL FAUT SAVOIR.

LA MENACE ET LE RISQUE ÉVOLUENT SANS CESSE, ET LA LOI S'ADAPTE. À TEL POINT QU'ELLE CONCERNE UN NOMBRE CROISSANT D'ENTREPRISES. LE MESSAGE QUE VEULENT AINSI FAIRE PASSER LES AUTORITÉS EST CLAIR : LA NÉGLIGENCE EN MATIÈRE DE SÉCURITÉ NUMÉRIQUE N'EST PLUS PARDONNABLE.

PROTECTION DES DONNÉES : LES SANCTIONS TOMBENT

Qui n'a pas entendu parler du RGPD ? Le règlement général sur la protection des données, entré en application le 25 mai 2018, nous le savons, impose des obligations de sécurité aux organisations gérant des données à caractère personnel. Ce que l'on sait moins, en revanche, c'est que la Commission nationale de l'informatique et des libertés (CNIL) a décidé de toucher au portefeuille, mais aussi à l'image et à la notoriété, des contrevenants. Depuis mai 2018, la CNIL prend, en moyenne, une délibération par mois pour sanctionner l'atteinte à la sécurité des données. Des sanctions qui peuvent être financières, et rendues publiques quand les manquements sont jugés suffisamment graves. Même si les sommes restent encore inférieures au regard des maximums prévus par la loi (jusqu'à 4 % du chiffre d'affaires annuel mondial), elles sont de plus en plus significatives.

AMENDES DÉSORMAIS APPLIQUÉES ET DE PLUS EN PLUS LOURDES :

> 22 M€ pour Bristish Airways et 18 M€ pour Mariott,

> Et déjà 250 000 € pour Bouygues Telecom et Optical center

> 400 000 € pour Sergic Immobilier et Uber

8 CONSEILS POUR SE PRÉPARER ET SE PROTÉGER JURIDIQUE-MENT

LES RECOMMANDATIONS DES AVOCATS SPÉCIALISÉS

1

Respecter la loi. C'est une évidence qui mérite cependant d'être rappelée.

2

Disposer d'un annuaire à jour de prestataires et de partenaires déjà identifiés : huissiers/juristes et avocats spécialisés qui ont les réflexes.

3

Verrouiller les contrats avec les sous-traitants et partenaires, et faire réaliser idéalement des audits pour vérifier qu'ils respectent les contrats et la réglementation.

4

La dimension cybersécurité doit dans ce sens être présente dans tous les actes juridiques.

5

Protéger sa propriété intellectuelle (savoir-faire, algorithmes, applications, code…).

6

S'assurer que les procédures internes formalisées sous forme de charte, code de conduite, etc. sont conformes à la réglementation.

7

Encadrer les transferts de données avec vos partenaires et vos prestataires, en particulier quand ils ne sont pas issus de l'Union européenne.

8

Déposer plainte en cas d'attaque.

99 %

L'ASSURANCE SE MET EN PLACE. D'APRÈS L'ÉTUDE DE L'ASSOCIATION DES ASSUREURS ANGLAIS*, 99 % DES RISQUES CYBER ASSURÉS ONT BIEN ÉTÉ INDEMNISÉS.

*The Association of British Insurers - octobre 2019

LA RESPONSABILITÉ PERSONNELLE DES DIRIGEANTS DE PLUS EN PLUS ENGAGÉE

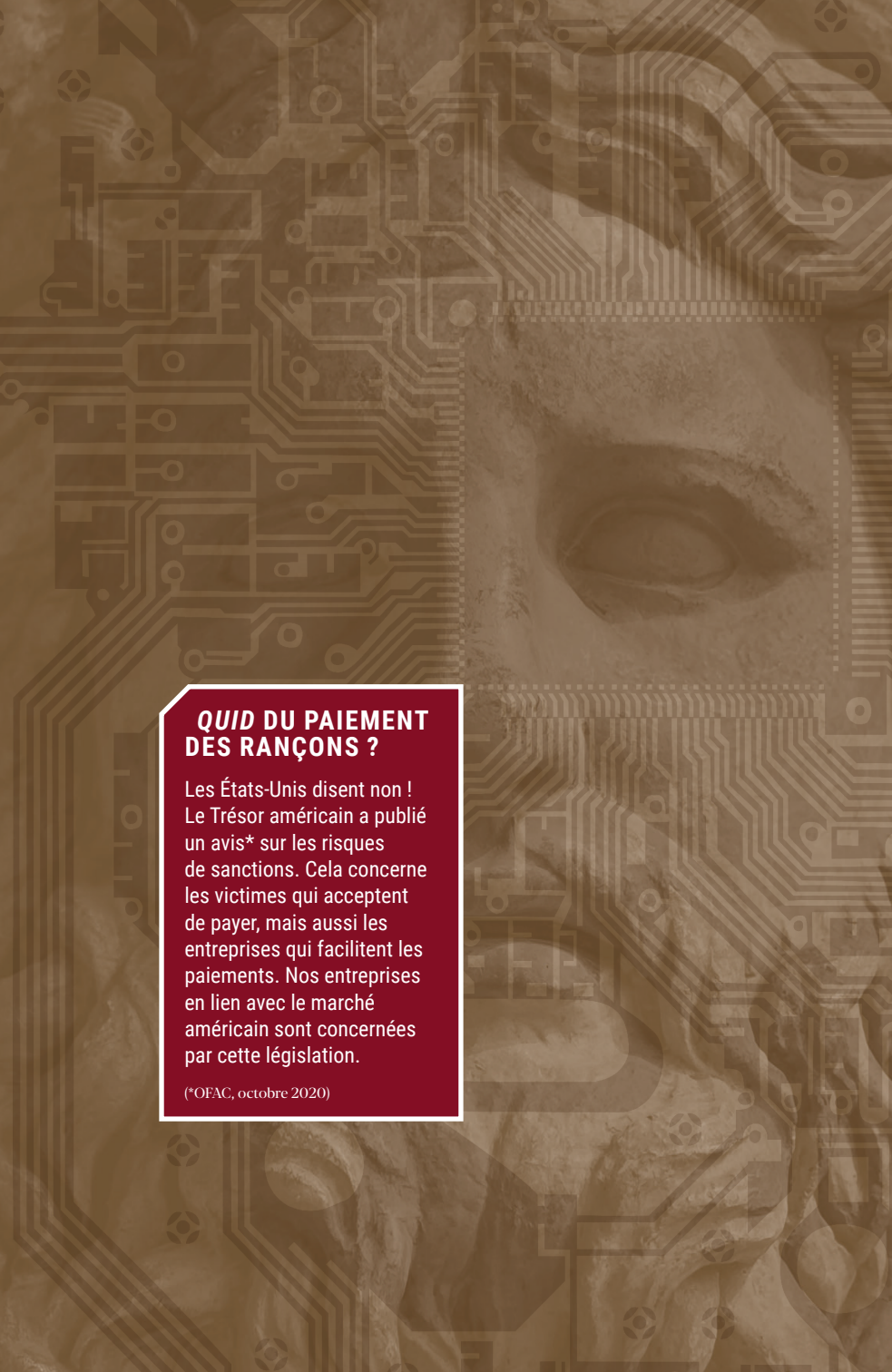
Deux points montrent une évolution sensible et invitent à prendre maintenant cette question très au sérieux.

D'abord, négliger la cybersécurité peut engager la responsabilité civile et pénale du dirigeant d'entreprise. Le juge pourrait en effet considérer que cela constitue une faute de gestion si les résultats de la société (voire sa pérennité) en étaient affectés.

Et, certaines compagnies d'assurances commencent à refuser désormais d'assurer les dirigeants et de couvrir la responsabilité civile des mandataires sociaux, si leur entreprise n'est pas elle-même assurée contre le risque de sécurité numérique.

OBLIGATIONS DE SE PROTÉGER : TOUTES LES ENTREPRISES BIENTÔT CONCERNÉES ?

D'abord imposée aux Organismes d'importance vitale, l'obligation de se protéger a été élargi aux organisations dont le service est considéré comme essentiel (OSE). La directive européenne NIS (*Network and Information Security*), moins connue que le RGPD, impose pourtant déjà à ces entreprises d'appliquer des règles de sécurité à leur SI et de déclarer tout incident à l'ANSSI. Elle leur impose aussi de prendre les mesures nécessaires pour garantir l'application de ces mêmes règles par leurs sous-traitants. Par conséquent, toute entreprise peut être concernée par cette directive même si elle n'est pas considérée comme OSE. Une nouvelle directive NIS 2 est en préparation : elle étendrait considérablement le champs des entreprises concernées !



QUID DU PAIEMENT DES RANÇONS ?

Les États-Unis disent non ! Le Trésor américain a publié un avis* sur les risques de sanctions. Cela concerne les victimes qui acceptent de payer, mais aussi les entreprises qui facilitent les paiements. Nos entreprises en lien avec le marché américain sont concernées par cette législation.

(*OFAC, octobre 2020)

CARNET D'**ADRESSES**

POUR S'INFORMER OU SE FORMER, ET EN CAS D'ATTAQUE, VOICI UNE SÉLECTION D'ADRESSES INDISPENSABLES

SSI.GOUV.FR
L'Agence nationale de la sécurité des systèmes d'information (ANSSI) assure la sécurité et la défense des systèmes d'information de l'État et des entreprises critiques en créant les conditions d'un environnement de confiance. Elle participe à la protection et à la défense du potentiel économique de la nation et assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

AMRAE.FR
Site de l'AMRAE, Association pour le Management des Risques et des Assurances de l'Entreprise, qui est l'association professionnelle de référence des métiers du risque et des assurances en entreprise. Elle propose notamment du contenu et des formations pour aider les organisations à mieux maîtriser leurs risques.

CERT.SSI.GOUV.FR
Site du centre gouvernemental de veille. Recense les alertes, menaces et incidents récents et fournit des indicateurs et des avis de sécurité.

CESIN.FR
Club des experts de la sécurité de l'information et du numérique. Association professionnelle de plus de 700 membres regroupant principalement des responsables sécurité d'entreprises. Lieu d'échange, de partage d'expérience. Le Cesin organise des rencontres, informe sur des alertes et propose des publications gratuites.

CIGREF.FR
Association représentative des plus grandes entreprises et administrations publiques françaises, exclusivement utilisatrices de solutions et services numériques, elle accompagne ses membres dans leurs réflexions collectives sur les enjeux numériques. Publie et offre régulièrement des documents et des rapports.

CLUSIF.FR
Club de la sécurité de l'information français. Cette association de promotion de la cybersécurité réunit entreprises et administrations autour du développement des bonnes pratiques pour la sécurité du numérique.

CNIL.FR
Autorité administrative indépendante française, la Commission nationale de l'informatique et des libertés (CNIL) est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Son site apporte des réponses pour comprendre ses droits, protéger les données et agir en cas de problème.

CYBERMALVEILLANCE.GOUV.FR
Site du gouvernement français pour aider les entreprises, les particuliers et les collectivités victimes de cybermalveillance, pour les informer sur les menaces numériques et leur donner les moyens de se défendre.

HEXATRUST.COM
Groupement d'entreprises françaises innovantes qui répondent aux grands enjeux et aux besoins des organisations publiques ou privées dans la protection contre les cybermenaces, la conformité réglementaire et l'accompagnement dans les grands projets de transformation digitale.

PHISHING-INITIATIVE.FR
Site créé par Orange Cyberdéfense pour vérifier ou dénoncer une adresse susceptible d'être à l'origine d'un *phishing*.

SYNTEC-NUMERIQUE.FR/ SECURITE-INFORMATIQUE
Membre de la Fédération Syntec (plus de 3 000 groupes et sociétés françaises spécialisés dans les professions du Numérique, de l'Ingénierie, du Conseil, de l'Événementiel et de la Formation Professionnelle), Syntec Numérique accueille des entreprises de services du numérique (ESN), des éditeurs de logiciels et des sociétés de Conseil en Technologies pour accompagner les entreprises dans leur transformation numérique.

PARTIE 3

DES ENTREPRISES ET DES EXPERTS FRANÇAIS : LEURS VISIONS, LEURS APPORTS

LA CYBERSÉCURITÉ, UN ENJEU CULTUREL
DEVOTEAM
54

MAÎTRISE DES RISQUES CYBER : UN OUTIL STRATÉGIQUE !
EGERIE
55

COMMENT SE PRÉPARER EFFICACEMENT CONTRE UNE CYBERATTAQUE ?
GATEWATCHER
56

ET VOUS, AVEZ-VOUS SÉCURISÉ VOS DONNÉES DANS LE *CLOUD* ?
LINKBYNET
57

UN GRAND SUJET POUR TOUTE L'ENTREPRISE
IDECSI
58

LA CYBERSÉCURITÉ, UN INDICATEUR DE PERFORMANCE
ORANGE CYBERDEFENSE
59

8 BONS GESTES POUR SE PROTÉGER
60

RENAUD TEMPLIER
Vice President - Trust & Cybersecurity, Devoteam

LA CYBERSÉCURITÉ, UN ENJEU CULTUREL

AUCUNE ENTREPRISE, QUELLE QUE SOIT SA TAILLE OU SON ACTIVITÉ, NE PEUT S'ESTIMER À L'ABRI DES CYBER-RISQUES. LE NUMÉRIQUE EST TROP OMNIPRÉSENT, TROP CRITIQUE, POUR QUE LA QUESTION NE SOIT PAS ABORDÉE DANS CHAQUE PROJET, PROCESSUS ET OUTIL INTERNES, ET CHAQUE SERVICE DIGITAL PROPOSÉ AUX CLIENTS. LA CYBERSÉCURITÉ DOIT ÊTRE L'AFFAIRE DE TOUS, TOUS LES JOURS, CAR LA MOINDRE BRÈCHE PEUT OUVRIR SUR UN GOUFFRE.

Mais face aux cybermenaces, il n'existe pas de solution universelle. En fonction des risques et du contexte propres à chaque entreprise, la parade passe par une combinaison de mesures techniques, fonctionnelles et organisationnelles. Mais aussi, par des mesures de politique de conformité aux normes et à la réglementation. Autant de bonne pratiques qui doivent s'inscrire dans la continuité des usages quotidiens. Et c'est pourquoi la cybersécurité constitue désormais un enjeu culturel.

Nécessaire moteur du changement, le top management doit lui-même prendre ce virage, car la réponse aux attaques passe généralement par des décisions rapides et fortes au plus haut niveau. C'est aussi la raison pour laquelle des exercices grandeur nature sont indispensables afin de sensibiliser toute l'organisation et d'en valider les réflexes.

Cheville ouvrière de la transformation, le RSSI est l'artisan du dialogue entre l'aspect technologique de la cybersécurité et cette dimension culturelle, opérationnelle. Pour cela, il doit pouvoir compter sur des partenaires pour qui, à l'image de Devoteam, ces deux aspects sont indissociables.

devoteam

JEAN LARROUMETS
Président et Fondateur, EGERIE
PIERRE OGER
Directeur général et Fondateur, EGERIE

MAÎTRISE DES RISQUES CYBER : UN OUTIL STRATÉGIQUE !

Alors que la survie de certaines entreprises est en jeu dans la crise mondiale que nous traversons, le numérique est un atout laissant entrevoir l'avenir plus sereinement. Comme toute opportunité, il porte aussi en lui de nouvelles menaces et le management des risques cyber se hisse désormais à un niveau stratégique. Face à des opérations de déstabilisation dont les impacts sur les activités des organisations sont de plus en plus critiques, il est primordial d'aborder la cybersécurité au travers d'une gestion des risques anticipée, collaborative et automatisée. Cette démarche permet ainsi de prendre, malgré la pression permanente, des décisions éclairées, et de répondre aux exigences de conformité réglementaire, d'innovation et de performance opérationnelle.

EGERIE
INTEGRATED CYBERRISK MANAGEMENT

JACQUES DE LA RIVIÈRE
Président, co-fondateur, Gatewatcher

COMMENT SE PRÉPARER EFFICACEMENT CONTRE UNE CYBERATTAQUE ?

Soyons clair : il est impossible de bloquer toutes les tentatives d'intrusion dans un SI. De fait, la détection, souvent négligée par les entreprises, est devenue un élément central dans la stratégie de cyberdéfense. L'enjeu est simple : repérer une attaque le plus tôt possible afin d'en limiter les dommages. Les *hackers* commencent par une collecte d'informations sur l'entreprise : adresses IP, recherches web, fouille des poubelles de l'entité, *social engineering*… Ils se mettent alors à exploiter les failles repérées lors de la brèche initiale. Une fois dans le système, ils maintiennent leurs accès pendant la phase de persistance. Ils effectuent alors des mouvements latéraux (exécution d'un code afin de récupérer les identifiants des équipements clients et la cartographie du réseau client). Enfin, a lieu la phase de malveillance : c'est le coup porté à l'entreprise (perte financière, vol de données…). Afin de limiter les risques, il devient essentiel de mener une stratégie de défense en profondeur, en protégeant les couches matérielles et hautes des SI. Pour garantir la cybersécurité du pays, l'ANSSI impose des obligations de détection aux Opérateurs d'Importance Vitale à travers la Loi de programmation militaire. À l'échelle européenne, la directive NIS impose des normes aux Opérateurs de Service Essentiels. Certaines entreprises innovantes comme Gatewatcher se distinguent en apportant une capacité de détection qui permet de prévenir les cyberattaques très rapidement.

GATEWATCHER

DAVID HOZE
Directeur de Linkbynet Cybersecurity

ET VOUS, AVEZ-VOUS SÉCURISÉ VOS DONNÉES DANS LE *CLOUD* ?

LA PLUPART DES ENTREPRISES MIGRENT LEURS DONNÉES ET LEURS APPLICATIONS DANS LE *CLOUD*. CETTE TENDANCE DE MARCHÉ SE GÉNÉRALISE ET S'ACCÉLÈRE. ET POURTANT, ENCORE TROP PEU D'ENTRE ELLES ONT MIS EN PLACE LES SOLUTIONS DE SÉCURITÉ PERMETTANT D'ASSURER LA RÉSILIENCE ET LA PROTECTION DES DONNÉES MIGRÉES. QU'ATTENDONS-NOUS POUR NOUS PROTÉGER ?

Les experts en cybersécurité le savent bien : le nombre d'attaques informatiques explose, et la cybermenace, qu'elle soit étatique, mafieuse ou crapuleuse, augmente de façon exponentielle.

Et pourtant, les solutions *cloud* offrent des perspectives de protection et de résilience des données et des applications extrêmement puissantes. Si tant est qu'elles soient activées et bien configurées.
Encore trop peu d'entreprises les mettent en place. Souvent par méconnaissances des solutions, ou bien par peur de perdre en agilité.
Pourtant, les grands *clouders* de la planète ne lésinent pas sur les solutions de protection, et redoublent de réactivité face aux cyber-menaces.
Bien accompagnée en amont, une entreprise peut assurément renforcer la sécurité de sa transformation digitale. Encore est-il nécessaire de choisir judicieusement ses experts et d'y associer une démarche de qualité, de pragmatisme et d'agilité. C'est le crédo de l'entité CyberSécurité de Linkbynet, un des leaders européens de la sécurité dans le *cloud*.

LINK BYNET CYBER SECURITY

DANIEL REZLAN
Président, IDECSI

UN GRAND SUJET POUR TOUTE L'ENTREPRISE

Il y a suffisamment d'enjeux, de sujets et de difficultés dans la gestion de nos entreprises, pour ne pas s'exposer trop ouvertement à un risque aujourd'hui si critique. L'accélération exponentielle des attaques, la variété des menaces exigent que nous passions de la conscience du risque, nous l'avons aujourd'hui, à sa maîtrise. Notre implication pleine et attentive de dirigeants est donc maintenant indispensable. Nous n'éviterons pas d'être la cible d'une attaque majeure.

Nous ne pouvons donc pas éviter de nous protéger. La pression est telle qu'il semble illusoire de penser que, seuls avec nos équipes informatiques et sécurité, nous pourrons porter un système de défense et d'alertes suffisant. Dès lors, faisons de cette question centrale un grand sujet *corporate*, qui engage toute l'entreprise, ses managers et ses collaborateurs. La sécurité numérique est d'ailleurs l'un des rares sujets communs où tous les collaborateurs peuvent apporter une contribution. Et elle est ici si précieuse. Consolidée, cette contribution apporte une ressource considérable à la protection de l'entreprise. Activons-la !

IDECSI
Enterprise Security

FRÉDÉRIC ZINK
Managing director France,
Orange Cyberdefense

LA CYBERSÉCURITÉ, UN INDICATEUR DE PERFORMANCE

L'intensification des usages numériques, les interconnexions techniques croissantes avec les partenaires, clients/sous-traitants et le déploiement des automates multiplient les risques cyber.
S'il est hors de question de renoncer à cette numérisation, les comités de direction doivent disposer des informations leur permettant d'apprécier les enjeux de cybersécurité : connaissance des obligations légales, cartographie du patrimoine informationnel et évaluation précise du niveau de sécurité de leur société. Qui passe par l'adoption d'une capacité efficace de détection des incidents de sécurité. Cela concerne les entités de toutes tailles puisque les centres de supervision (SOC) peuvent être proportionnés au périmètre à protéger.
En connaissant mieux leur organisation, et les usages qui sont faits des systèmes d'information, les dirigeants sont plus à même de déceler les points d'amélioration. De quoi intéresser les managers bien au-delà de la communauté IT. De même, les donneurs d'ordre externes, les investisseurs et les analystes sont de plus en plus intéressés par des informations concernant l'état de la sécurité, les mesures mises en place pour identifier les pannes ou les attaques, et les moyens actionnables pour remédier à la situation de crise.
Il convient de leur fournir des données précises et pertinentes pour ne pas être identifié comme le maillon faible de la chaîne économique. Cela explique la tendance à systématiser la mention de la cybersécurité parmi les indicateurs de performance des entreprises.

Orange Cyberdefense

DIRIGEANTS MAIS AUSSI UTILISATEURS.

8 BONS GESTES POUR SE PROTÉGER

ET PROTÉGER NOS DONNÉES PROFESSIONNELLES ET PERSONNELLES

1

DÉFINIR UN MOT DE PASSE DISTINCT POUR CHAQUE COMPTE

Couper les passerelles et cloisonner évite l'effet domino qui permet d'accéder à tous les comptes avec un seul mot de passe.

2

SAUVEGARDER RÉGULIÈREMENT

Conserver une copie des données est une mesure élémentaire, en entreprise comme à la maison.
Cette sauvegarde doit être indépendante afin de ne pas être touchée en cas de problème.

3

EFFECTUER LES MISES À JOUR DES LOGICIELS

C'est un principe fondamental. Les attaquants recherchent les postes dont les logiciels n'ont pas été mis à jour pour exploiter une faille non corrigée.

4

NE PAS SE CONNECTER AU WIFI PUBLIC

Privilégier une connexion 4G aux réseaux de bornes Wifi publiques, pas sécurisées : smartphones, tablettes ou ordinateurs peuvent être épiés et leurs données récupérées.

5

NE PAS TRANSFÉRER DES DONNÉES PROFESSIONNELLES SUR UN COMPTE PERSONNEL

Pour éviter toute contamination, ne pas héberger des données professionnelles sur des équipements personnels (smartphones, clé USB…), ni brancher un support personnel sur un terminal professionnel.

6

NE PAS CLIQUER SUR DES PIÈCES JOINTES, DES LIENS OU DES MESSAGES VENANT D'ÉMETTEURS INCONNUS OU NON-ATTENDUS

Même si la tentation est grande : « En cas de doute, il n'y a pas de doute ! » Un soupçon sur un message provenant d'une personne connue ? Appeler celle-ci pour confirmation !

7

ÉTEINDRE SES ÉQUIPEMENTS LE SOIR

Éteindre les terminaux limite les intrusions et fait du bien à la planète.

8

EN CAS DE SUSPICION D'ATTAQUE, SE DÉCONNECTER DU RÉSEAU

Quelque chose d'anormal se produit sur un poste de travail ? Le déconnecter du réseau pour éviter une propagation mais le maintenir sous tension pour ne pas perdre les informations utiles à l'analyse de l'attaque, et alerter les équipes de sécurité et le support informatique.

LE COMITÉ ÉDITORIAL REMERCIE CHALEUREUSEMENT POUR LEUR CONCOURS ET LEUR CONTRIBUTION AU CONTENU :

- Henri d'AGRAIN, Délégué Général, Cigref
- Antoine ANCEL, Directeur Cyber Sécurité Opérationnelle Groupe, SNCF
- Gérôme BILLOIS, Associé cybersécurité et confiance numérique, WAVESTONE
- Olivier DALOY, Information Systems Security Director, FAURECIA
- Émilie DUMÉRAIN, Déléguée juridique et aux usages Cybersécurité, SYNTEC NUMÉRIQUE
- Cyril HAZIZA, Group Chief Information Security Officer, KERING
- Olivier ITEANU, Avocat, ITEANU AVOCATS
- Arnaud MARTIN, Directeur de la Cyber Sécurité Groupe CAISSE DES DÉPÔTS
- Carlos MARTIN, Directeur Sécurité de l'Information, LA BANQUE POSTALE
- Garance MATHIAS, Avocat Associée Fondateur, MATHIAS AVOCATS
- Patrick MÉNEZ, Deputy Group Chief Security Officer, AXA
- Clara MORLIERE, Chargée de Mission, Cigref
- Philippe NETZER-JOLY, Group Chief Cyber Security Officer, ARKEMA
- Christian POYAU, Président de la commission « Mutations technologiques et impacts sociétaux », MEDEF
- Nadège REYNAUD, Cybersecurity Expert, CESIN
- Daniel REZLAN, Président, IDECSI, Coprésident, CEIDIG
- Alain ROGULSKI, Group Chief Information Security Officer, SODEXO
- Loïs SAMAIN, RSSI, EDF HYDRO
- Betty SFEZ, Avocate Associée, SOLEGAL
- Marc TOURNIER, Responsable de la Sécurité des Systèmes d'information Groupe, ERAMET
- Michel VAN DEN BERGHE, CEO ORANGE CYBERDEFENSE

AINSI QUE LES GRANDES ORGANISATIONS DU MONDE DE L'ÉCONOMIE ET DE L'ENTREPRISE, DES GRANDES ÉCOLES FRANÇAISES, POUR LEUR IMPLICATION ESSENTIELLE DANS LA DIFFUSION DU GUIDE :

MEDEF

cpme CONFÉDÉRATION DES PME

CONFÉRENCE DES GRANDES ÉCOLES

Croissanceplus Grandir ensemble

FRANCE DIGITALE

Quelle est la dimension du risque aujourd'hui ?
Que dois-je absolument savoir ?
Cet ouvrage a bénéficié d'une mobilisation unique de grands acteurs français du numérique et de la sécurité numérique. Il a une ambition essentielle : être utile !

AVEC LA CONTRIBUTION ET LE SOUTIEN DE