L'ESSENTIEL DE LA SÉCURITÉ NUMÉRIQUE POUR LES DIRIGEANTS

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 RÉPONSES ET LES CONSEILS DES GRANDS ACTEURS DE LA CYBERSÉCURITÉ

L'ÉDITION NUMÉRIQUE DE CET OUVRAGE EST DIFFUSÉE PAR LES ÉDITIONS
EYROLLES

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 de la sécurité numérique.
Leurs contributions, expertes, sont une chance précieuse pour bénéficier d'un guide qui couvre tous les sujets clés de la cybersécurité et propose des réponses pratiques.
Il a une ambition essentielle : être utile !

L'ESSENTIEL DE LA **SÉCURITÉ NUMÉRIQUE** POUR LES **DIRIGEANTS**

À L'INITIATIVE DE L'ASSOCIATION CEIDIG,
CONSEIL DE L'ÉCONOMIE ET DE L'INFORMATION DU DIGITAL

HAUT MANAGEMENT

Direction éditoriale :
Daniel Benabou

Collège éditorial :
présenté en 4e de couverture

Textes :
Nostromo,
Patrick Coquart, Guillaume Wallut

Conception graphique et maquette :
Juliane Cordes et Corinne Dury

Coordination :
Alice Nicolazo, Shake your Brand

Impression et façonnage :
Stipa, Montreuil

SOMMAIRE

DANIEL BENABOU
Directeur général d'IDECSI
Président du CEIDIG

UNE CLÉ DE SUCCÈS

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

Nous sommes fascinés par la fluidité des échanges et les possibilités exponentielles pour le développement et l'efficacité de nos entreprises. Comment bénéficier du meilleur de cette évolution ? Il y a plusieurs clés, dont une, encore peu visible et pourtant aujourd'hui si essentielle : 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 pas technique, elle est stratégique. Elle doit évidemment être un sujet de haut management. Partager les enjeux de ce mouvement est au fond l'une des ambitions de ce guide, que je suis très fier d'avoir initié et construit avec un collège de compétences si prestigieux.

PIERRE-HENRI DE MENTHON
Directeur délégué de la rédaction de CHALLENGES

LES ATOUTS FRANÇAIS

CHALLENGES EST HEUREUX DE CONTRIBUER, AVEC CE GUIDE, À UNE MEILLEURE CONNAISSANCE DES QUESTIONS DE SÉCURITÉ NUMÉRIQUE. ON PEUT SE DEMANDER POURQUOI UN HEBDOMADAIRE COMME LE NÔTRE S'INTÉRESSE À CE SUJET ET NE LE LAISSE PAS À SES CONFRÈRES DE LA PRESSE SPÉCIALISÉE.

Ce serait méconnaître les enjeux économiques de la cybersécurité. Une entreprise attaquée peut perdre des millions, son cours de bourse peut chuter, ses clients la quitter, ses dirigeants être limogés, ses salariés démotivés… Et puis, les *hackers* ayant toujours un temps d'avance, il reste à inventer les solutions de demain. Nous sommes persuadés que les entreprises françaises – grands groupes, PME ou start-up – ont des atouts pour être les champions de la sécurité numérique.

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

UNE PRIORITÉ STRATÉGIQUE

AU-DELÀ DE LA DIMENSION PUREMENT TECHNOLOGIQUE, PENSER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION, C'EST AUSSI CONSIDÉRER UNE COMPOSANTE ESSENTIELLE DES ENJEUX ÉCONOMIQUE, STRATÉGIQUE ET D'IMAGE RELEVANT DE VOTRE RESPONSABILITÉ DE DIRIGEANT D'ENTREPRISE.

Si la prise en compte de la sécurité numérique au sein des comités exécutifs progresse de manière significative, elle reste insuffisante et intervient trop souvent à l'issue d'un incident informatique grave. L'objectif de ce guide écrit à plusieurs mains est d'apporter la preuve par l'expérience qu'en matière de risque numérique, silence ne vaut pas absence, et de fournir aux dirigeants et responsables de la sécurité des systèmes d'information des outils à la croisée de leurs objectifs respectifs : la création de valeur à l'ère numérique d'une part et la confiance dans les systèmes d'information d'autre part. Certain que cet ouvrage résolument pratique fera écho à vos responsabilités, je vous en souhaite très bonne lecture !

ALAIN BOUILLÉ
Président du CESIN – Directeur de la sécurité des systèmes d'information Groupe Caisse des Dépôts

LE RSSI : L'HOMME-ORCHESTRE

La « sécurité informatique » est longtemps restée confinée dans un périmètre très technique forcément éloignée des préoccupations des dirigeants.
La sécurité désormais « de l'information » s'invite dorénavant dans l'agenda de nombreux Comex du fait d'une digitalisation partout en marche combinée à une cybercriminalité en augmentation exponentielle avec des effets le plus souvent dévastateurs pour les entreprises ciblées. Malgré tout, ces sujets restent complexes et les dirigeants se sentent souvent démunis lorsqu'ils doivent faire face à l'inéluctable crise cyber.
Pendant ce temps de plus en plus de responsables sécurité sont nommés et cette profession s'organise au sein d'associations comme le CESIN. Nous avons tenu à apporter notre contribution à ce guide qui, nous l'espérons, aidera le dirigeant à appréhender ce domaine de risques de plus en plus prégnant avec plus de sérénité.

VALÉRIE LEVACQUE
Présidente du GITSIS

STRATÉGIE CYBERSÉCURITÉ POUR L'ENTREPRISE NUMÉRIQUE

Pour les industriels de haute technologie que représente le GITSIS, la cybersécurité est un objectif prioritaire en regard de l'évolution des menaces actuelles. Sujet complexe à adresser, elle nécessite de disposer d'une vision stratégique globale sur : l'emprise croissante du numérique sur l'outil industriel ; l'évolution permanente des technologies et des usages (*Cloud*,…) ; la transformation de l'écosystème des entreprises et ses implications (entreprise étendue,…) ; les réglementations et leurs évolutions.
La sécurité numérique est encore trop souvent une affaire de spécialistes peu lisible pour les comités de direction.
Cet ouvrage qui leur est destiné leur apportera une vision synthétique de la réalité du risque actuel et de quelques repères clés.

OLIVIER VALLET
Membre du conseil d'administration
et Président du Comité Cybersécurité
de Syntec Numérique

LA SÉCURITÉ EST LA PREMIÈRE DES LIBERTÉS

En 2017, c'est la cybersécurité qui devrait être au sommet de nos préoccupations lorsqu'on parle de sécurité. Les entreprises y sont-elles aujourd'hui plus sensibilisées ? Très marginalement seulement.
Ce guide est donc vital pour les dirigeants et les entreprises françaises. Il va les aider à appréhender le phénomène, son accélération et il est un complément formidable des initiatives portées par l'État, les syndicats professionnels et les clubs. Ainsi, Syntec Numérique, premier syndicat professionnel du numérique, a mis la cybersécurité au sommet de son agenda en créant un comité dédié regroupant des entreprises spécialisées pour informer et échanger sur les bonnes pratiques.

GÉRARD RIO
Fondateur des Assises de la sécurité et des systèmes d'information

UN MÊME OBJECTIF

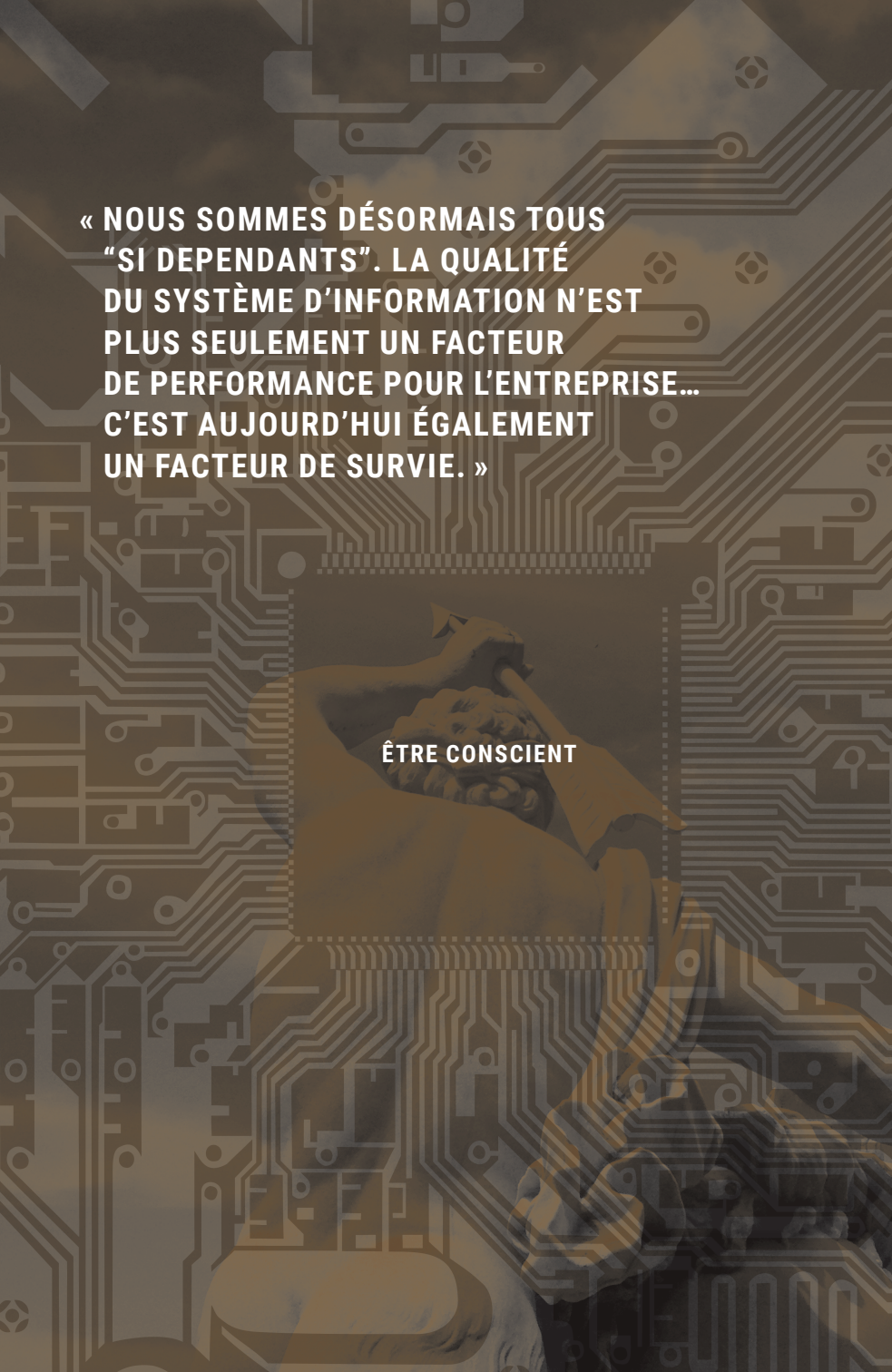
MAÎTRISER LES RISQUES NUMÉRIQUES, SENSIBILISER À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, ALERTER TOUT EN FAISANT COMPRENDRE LES ENJEUX… TELS SONT LES MESSAGES PORTÉS PAR CE GUIDE. DES MESSAGES QUE PARTAGENT DEPUIS TOUJOURS LES ASSISES DE LA SÉCURITÉ ET DES SYSTÈMES D'INFORMATION.

Nous sommes fiers de participer à ce guide sur la sécurité numérique à destination des dirigeants. D'abord en raison de la qualité des différents contributeurs qui en garantit le sérieux et l'expertise. Mais aussi car les messages véhiculés reflètent les objectifs que se fixent les Assises de la Sécurité depuis maintenant plus de 16 ans. À l'instar de cet ouvrage, les Assises se sont toujours considérées comme un outil de prévention. Et anticiper le risque est bien le propre du dirigeant d'entreprise.

PARTIE 1

MIEUX COMPRENDRE LA RÉALITÉ DU RISQUE AUJOURD'HUI

« NOUS SOMMES DÉSORMAIS TOUS “SI DEPENDANTS”. LA QUALITÉ DU SYSTÈME D’INFORMATION N’EST PLUS SEULEMENT UN FACTEUR DE PERFORMANCE POUR L’ENTREPRISE… C’EST AUJOURD’HUI ÉGALEMENT UN FACTEUR DE SURVIE. »



ÊTRE CONSCIENT

QUI EST **CONCERNÉ** ? QUI PEUT ÊTRE **CIBLÉ** ?

LA MENACE SE DÉMULTIPLIE. LES ENJEUX FINANCIERS DU CYBERCRIME SONT RENDUS ACCESSIBLES PAR UNE TECHNOLOGIE DE PLUS EN PLUS PERFORMANTE. CIBLÉES OU AUTOMATISÉES, LES ATTAQUES SONT MIEUX ORGANISÉES ET PLUS EFFICACES.

4 165

NOMBRE DE CYBERATTAQUES DÉTECTÉES EN FRANCE EN 2016

Source : The Global State of Information Security ® Survey 2017 de PWC

UNE ACTIVITÉ RENTABLE ET ORGANISÉE COMME UN MARCHÉ

La cybercriminalité s'est organisée, spécialisée, industrialisée et internationalisée. Elle attire des pirates qui agissent en véritables entrepreneurs. Avec leurs sous-traitants, leur R&D, leurs partenaires – parfois étatiques –, ils évoluent sur un marché mondialisé grâce à Internet et cachés dans des espaces dédiés très bien isolés (*dark web*). À partir d'organisations sans contraintes et sans règles, ils se spécialisent en productifs, pourvoyeurs de moyens d'attaque, en prospecteurs à la recherche de cibles et d'opportunités, ou en receleurs qui monnayent les valeurs acquises… Le cybercrime est d'autant plus lucratif que l'investissement initial est limité, le retour sur investissement très rentable, et le risque juridique quasi-nul pour des pirates bien organisés.

QUELLES ENTREPRISES SONT TOUCHÉES ?

Expressément visés ou non, il n'y a plus d'entreprises ni de secteurs épargnés. Comme pour n'importe quelle activité « commerciale », les *hackers* visent un segment de marché, en fonction de leurs moyens et de leur ambition. Certains attaquants s'intéressent aux grands

« IL FAUT ACCEPTER D'ÊTRE ATTAQUÉ. C'EST COMME TOMBER MALADE. L'IMPORTANT EST DE SE SOIGNER VITE ET BIEN. »

82 secondes

LE TEMPS QUI S'ÉCOULE ENTRE L'ENVOI D'UNE CAMPAGNE DE *PHISHING* ET LE PREMIER CLIC

Source : Data Breach Investigation Report 2015 de Verizon

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… Aujourd'hui, la menace a considérablement augmenté et la question n'est plus « Quelle est la probabilité que je sois attaqué cette année ? » mais « Combien de fois vais-je me faire attaquer ? ».

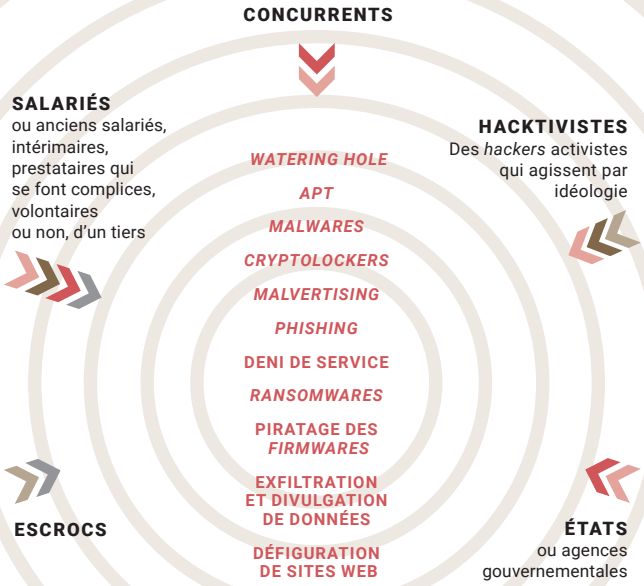
DES ATTAQUES PRÉPARÉES DONT LES DÉGÂTS PEUVENT ÊTRE CONSIDÉRABLES

Très dangereuses, elles s'appuient sur un travail méticuleux d'ingénierie sociale qui cherche à collecter des renseignements techniques et humains pour mieux cerner le profil et l'environnement professionnel de la cible. L'objectif est de rendre l'attaque furtive en la masquant derrière des contacts connus. La plupart du temps toutes les informations utiles sont disponibles sur les sites institutionnels des entreprises visées, mais également dans les médias et sur les réseaux sociaux.

DES ATTAQUES AUTOMATISÉES FACILES À RÉALISER

Simples à déclencher sur de larges périmètres grâce à des programmes informatiques disponibles sur Internet, les attaques automatisées sont lancées en masse. Comme les chaluts qui ramassent tout ce qu'ils trouvent, des logiciels automatiques captent dans leurs filets des victimes mal protégées et naïves. Opportunistes, ces attaques font désormais de toutes les entreprises des cibles qui trop souvent s'ignorent.

LES PRINCIPALES MENACES ACTUELLES



ATTAQUES COMMUNES
Quotidiennes, elles visent tout le monde : entreprises de toutes tailles, particuliers, administrations, sans distinction.

ATTAQUES CIBLÉES
Des agressions majeures qui visent une entreprise en particulier.

LES ATTAQUANTS	LES MOYENS
MOTIVATIONS / FINALITÉS	ESPIONNAGE · DÉSTABILISATION
FINANCIÈRE	DÉGRADATION · RÉPUTATION

DES ATTAQUANTS AUX **MOTIVATIONS MULTIPLES**

SI LA PRINCIPALE MOTIVATION DES ATTAQUANTS EST FINANCIÈRE, ELLE N'EST PAS LA SEULE. LE PROFIL DES ACTEURS, INTERNES OU EXTERNES, EST DIVERS. LEURS INTENTIONS LE SONT ÉGALEMENT.

LA PRINCIPALE MOTIVATION DES ATTAQUANTS : L'ARGENT… MAIS PAS SEULEMENT

L'appât du gain n'est pas la seule motivation des *hackers*. Certes, elle est essentielle et explique en grande partie la croissance de l'activité. Mais les attaques peuvent être également motivées par l'espionnage. Nullement réservé aux États, il peut être le fait d'un concurrent à la recherche d'informations confidentielles. L'attaquant peut aussi vouloir abîmer l'image d'une entreprise, la déstabiliser ou la manipuler. Et puis existe le « vandalisme cyber ». Ici le mobile est la dégradation. Quelquefois par vengeance, ou simplement pour mettre en avant la « performance » du *hacker* et asseoir sa réputation.

1 425%

LE RETOUR SUR INVESTISSEMENT ESTIMÉ D'UN ***RANSOMWARE***

Source : 2015 Trustwave Global Security Report

LES ACTEURS DE LA MENACE : EXTERNES BIEN SÛR, MAIS AUSSI INTERNES

Avec des systèmes d'information connectés et accessibles de l'extérieur de l'entreprise, les collaborateurs de l'entreprise – ou ex-salariés – et prestataires peuvent être à l'origine de malveillances et de fuites. Volontairement ou à leur insu. Quant aux administrateurs informatiques, qui disposent de droits d'accès et de paramétrages élevés, ils peuvent facilement accéder aux contenus informatiques de l'entreprise ou être la cible privilégiée d'attaquants.

COMPRENDRE

« L'HABITUDE DE VIVRE DEPUIS TOUJOURS AVEC UN RISQUE OUVERT PEUT DONNER L'ILLUSION DE POUVOIR ÉVITER DE LE PROTÉGER. LE FAIT D'ACCEPTER UN RISQUE, DE "L'OUBLIER", N'ÉVITE PAS LES CONSÉQUENCES PARFOIS DRAMATIQUES DE SA RÉALISATION. »

LEXIQUE INDISPENSABLE

APT

Une *APT* (*Advanced Persistent Threat* ou menace persistante avancée) est un piratage informatique qui vise à placer du code malveillant personnalisé sur des postes de travail. Et ceci en restant inaperçu le plus longtemps possible.

DÉFIGURATION DE SITES WEB

L'attaque consiste à modifier le contenu d'un site Web, par exemple la page d'accueil qui peut alors devenir un écran noir, ou bien afficher les revendications politiques ou idéologiques des *hackers*.

DÉNI DE SERVICE

Une attaque par déni de service consiste à rendre indisponible un serveur, principalement en le saturant par un trop grand nombre de requêtes simultanées.

EXFILTRATION ET DIVULGATION DE DONNÉES

Les *hackers* s'infiltrent dans les réseaux pour s'emparer de données confidentielles et les publier. Leur objectif est de montrer que le site de leur victime est peu sécurisé, et de porter ainsi atteinte à son image.

MALVERTISING

Le *malvertising* (*malicious advertising*) utilise les publicités en ligne pour diffuser des logiciels malveillants.

MALWARE

Un *malware* (*malicious software* ou logiciel malveillant) est un programme informatique développé dans le but de nuire. Virus, vers, cheval de Troie sont des *malwares* très répandus.

PIRATAGE DE *FIRMWARES*

Les *firmwares* (micrologiciels intégrés dans du matériel informatique pour permettre au *hardware* d'évoluer en intégrant de nouvelles fonctionnalités) peuvent être piratés afin de rendre l'appareil inopérant ou de l'utiliser pour s'introduire dans un réseau.

PHISHING

Le *phishing* (ou hameçonnage) consiste à usurper une identité afin d'obtenir des renseignements personnels ou des identifiants bancaires pour en faire un usage criminel.

RANSOMWARE ET *CRYPTOLOCKER*

Un *ransomware* (ou rançongiciel) est un programme informatique qui bloque l'accès aux données tant qu'une rançon n'a pas été payée. Un *cryptolocker* (ou crypto-verrouilleur) est un *ransomware*, diffusé principalement par des courriels infectés, qui crypte les données de l'utilisateur. Une rançon est demandée (souvent en bitcoins) pour obtenir la clé de déchiffrement.

WATERING HOLE

Une attaque par point d'eau (*watering hole* en anglais) s'appuie sur les habitudes de navigation d'individus travaillant pour une entreprise cible. Un *hacker* peut par exemple trouver des informations sur un collaborateur grâce aux réseaux sociaux et les utiliser pour attaquer. S'il a repéré que sa proie préparait son mariage, il va ainsi placer un code malveillant sur les sites Web consacrés au mariage qui se propagera sur l'ordinateur de la personne cible, et ensuite sur le réseau de l'entreprise.

RETOUR SUR L'ATTAQUE DE **TV5 MONDE**

LA CHAÎNE DE TÉLÉVISION A ÉTÉ PIRATÉE. LES CONSÉQUENCES D'UNE ATTAQUE RÉUSSIE. QUELS ENSEIGNEMENTS EN TIRER ?

RAPPEL DES FAITS

8 avril 2015, 20h50. Les comptes Twitter et la page Facebook de TV5 Monde diffusent de la propagande en faveur de l'État islamique (Daech). Puis la page d'accueil du site Internet de la chaîne est piraté. La messagerie électronique ne fonctionne plus, et la diffusion de la chaîne s'arrête. Écran noir pour tous les téléspectateurs, partout dans le monde.

Le lendemain, 9 avril, vers 05h00 du matin, la chaîne diffuse à nouveau des programmes préenregistrés grâce à l'appui de l'ANSSI et d'acteurs spécialisés. Ce n'est qu'à 18h00 que le direct peut reprendre. Mais le fonctionnement de la chaîne reste perturbé pendant de longs mois encore. Les collaborateurs n'utilisent de nouveau Internet – avec un débit limité – qu'au mois de juillet. En octobre, la messagerie est encore souvent indisponible.

L'ORIGINE DE L'ATTAQUE

Tout aurait commencé quelques semaines plus tôt par un *phishing* intensif auquel quelques collaborateurs succombent. Parallèlement, un prestataire technique utilisateur du VPN est piraté. C'est donc par plusieurs portes d'entrée que les pirates investissent le système. TV5 Monde estime à six mois le temps de préparation nécessaire à l'attaque.

4,6 M€

LE COÛT DE L'ATTAQUE POUR TV5 MONDE EN 2015 (SOIT 5% DU CA). IL S'AGIT DU SEUL COÛT DE RECONSTRUCTION, HORS COÛTS D'INDISPONIBILITÉ, D'IMAGE, ETC. LA NOTE DEVRAIT DESCENDRE À 3,1 MILLIONS EN 2016, AVANT DE SE STABILISER À 2,5 MILLIONS D'EUROS ANNUELS.

« LES STATISTIQUES MONTRENT QUE 90 % DES ENTREPRISES FRAPPÉES PAR CE TYPE D'ATTAQUE FERMENT DANS LES DEUX ANS QUI SUIVENT. NOUS, NOUS FERONS PARTIE DES 10 % QUI SURVIVRONT, FORT HEUREUSEMENT. MAIS CELA VA NOUS DEMANDER UN CERTAIN NOMBRE D'ASTREINTES. »

Yves Bigot, PDG de TV5 Monde

POURQUOI CELA EST-IL ARRIVÉ ?

Selon l'ANSSI, TV5 Monde « avait fait le choix d'une sécurité limitée, ayant pour priorité la disponibilité de son système d'information. La chaîne a d'ailleurs reconnu un défaut d'anticipation de la menace ». Pour certains observateurs, les *hackers* ont aussi profité d'une architecture informatique dans laquelle la partie métier et la partie bureautique, connectée sur Internet, n'étaient pas séparées.

UN CHANGEMENT D'ATTITUDE

Le témoignage de la chaîne, écouté avec beaucoup d'attention par d'autres dirigeants, a permis de relayer les préoccupations de sécurité numérique auprès de ce secteur et a eu des vertus préventives certaines. Chaque nouveau projet intègre désormais un volet sécurité adapté.

UNE COMMUNICATION DANS TOUTES LES DIRECTIONS

TV5 Monde reconnaît qu'elle n'était pas préparée à une telle crise. Désormais, la chaîne dispose d'un plan de crise très précis, avec un volet communication externe. La communication a dû également s'intensifier à l'interne pour expliquer les interventions techniques et les raisons de leur durée. Et puis, la sensibilisation et la formation du personnel se sont accrues. C'est un travail répété sans cesse qui commence à porter ses fruits au bout d'un an et demi.

DES **ATTAQUES** TOUS AZIMUTS

DES CYBERATTAQUES ONT LIEU TOUS LES JOURS. LES MÉDIAS S'EN FONT DE PLUS EN PLUS L'ÉCHO, MÊME SI LA PLUPART DES CAS NE SONT PAS DIVULGUÉS.

YAHOO! VICTIME D'UN GIGANTESQUE VOL DE DONNÉES VOIT SON RACHAT COMPROMIS

Jeudi 22 septembre 2016, alors qu'il est en discussion en vue de son rachat par l'opérateur Verizon, Yahoo! annonce avoir été victime d'un piratage massif de plus de 500 millions de comptes. Le 14 décembre 2016, un nouveau piratage est révélé portant, cette fois, sur plus d'un milliard de comptes. Verizon, prêt à mettre 4,8 milliards de dollars sur la table, déclare : « Nous allons passer en revue l'impact de ce nouveau développement avant de tirer des conclusions définitives. »

DE GRANDS ACTEURS D'INTERNET BLOQUÉS AUX ÉTATS-UNIS PENDANT PLUSIEURS HEURES

Vendredi 21 octobre 2016, une cyberattaque menée en plusieurs vagues a sérieusement perturbé le fonctionnement d'Internet aux États-Unis. Des millions de personnes n'ont pu accéder à Twitter, Spotify, Amazon ou eBay. Les pirates, qui ont aussi paralysé le fonctionnement de Reddit, Airbnb, Netflix et les sites de plusieurs médias (CNN, New York Times, Boston Globe, Financial Times, The Guardian…), ont en fait attaqué la société Dyn, qui redirige les flux Internet vers les hébergeurs.

ET SI VOTRE ADRESSE EMAIL FIGURAIT PARMI DES DONNÉES PIRATÉES ?

Le site haveibeenpwned.com recense l'ensemble des listings hackés et diffusés…

EN **FRANCE**, L'ÉTAT AUSSI **S'ORGANISE** ET SE DOTE DE FORCES CYBER

LA MULTIPLICATION ET LA COMPLEXITÉ DES CYBERATTAQUES N'ONT PAS ÉCHAPPÉ À L'ÉTAT FRANÇAIS. DÈS 2008, LE LIVRE BLANC SUR LA DÉFENSE ET LA SÉCURITÉ NATIONALE S'EST EMPARÉ DE LA QUESTION.

4 400

RÉSERVISTES VIENDRONT RENFORCER LA CYBERDÉFENSE D'ICI 2019

« L'ÉMERGENCE D'UN NOUVEAU MILIEU, D'UN CHAMP DE BATAILLE CYBER, DOIT NOUS AMENER À REPENSER PROFONDÉMENT NOTRE MANIÈRE D'ABORDER L'ART DE LA GUERRE. »

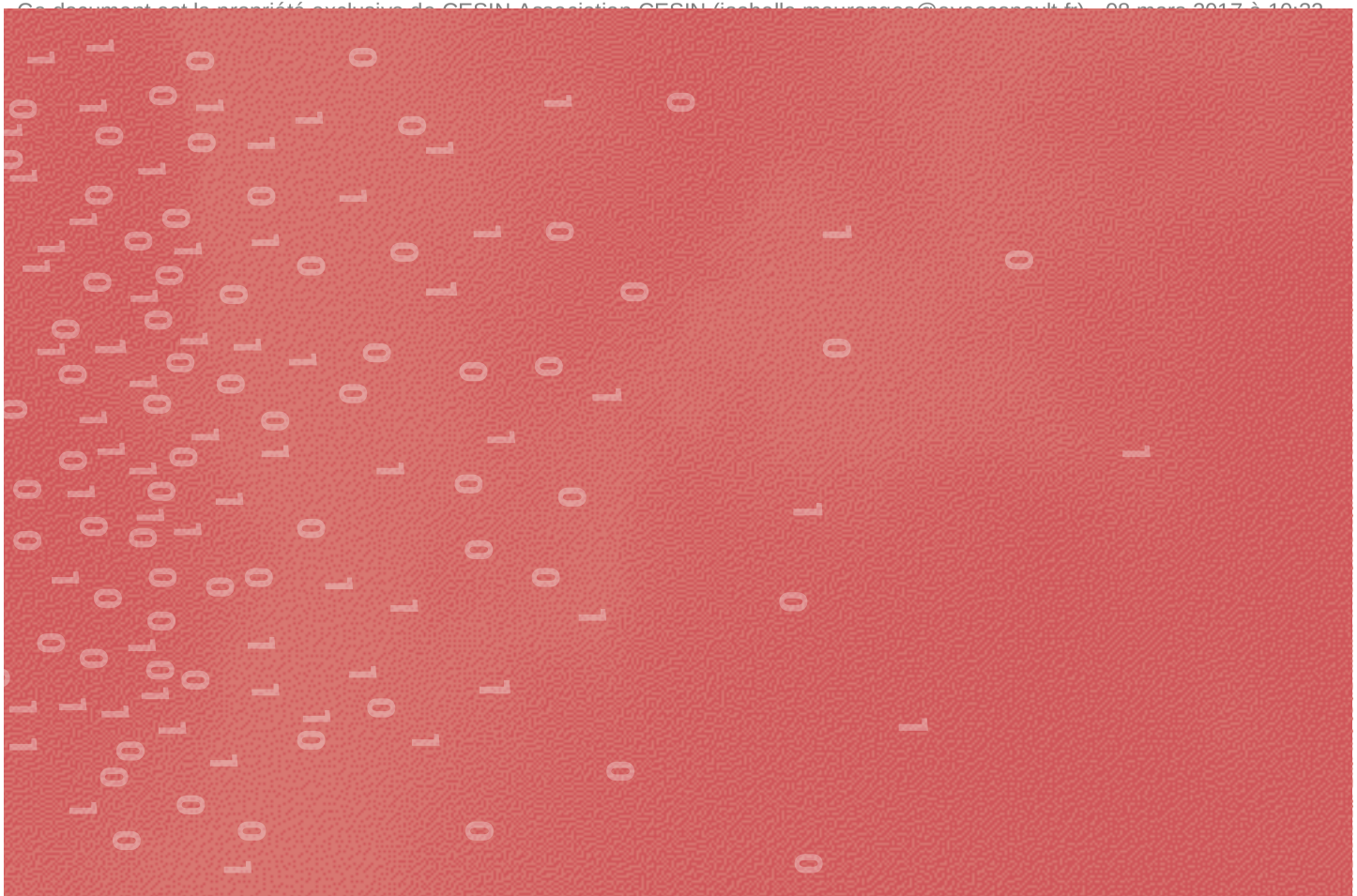
Jean-Yves Le Drian
Ministre de la Défense

C'est ainsi qu'a été créée l'Agence nationale de sécurité des systèmes d'information (ANSSI) en juillet 2009. Rattachée au Premier ministre, ses attributions ont été renforcées en 2011 : l'agence est depuis lors l'Autorité nationale en matière de défense et de sécurité des systèmes d'information.

Au ministère de la Défense, le poste d'Officier général chargé de la cyberdéfense coordonne l'action dans ce domaine et sert d'interface principale en cas de crise cyber. L'état-major « Cybercom » dispose d'une équipe de 2 600 « combattants du numérique » et s'appuie sur 600 experts de la Direction générale pour l'armement (DGA).

Depuis 2014, le ministère de l'Intérieur bénéficie aussi d'un poste de préfet chargé de la lutte contre les cybermenaces. Il coordonne notamment l'action des forces de police et de gendarmerie en la matière.

Quant au ministère des Affaires Étrangères, il développe des coopérations internationales sur les questions de cybersécurité, tant au niveau bilatéral qu'au sein des organisations internationales.



PARTIE 2

PROTÉGER SON ENTREPRISE : REPÈRES ET CONSEILS ESSENTIELS

SE CONCENTRER SUR **LES POINTS CLÉS** : 10 QUESTIONS POUR MIEUX APPRÉHENDER LA CYBERSÉCURITÉ

LA CYBERSÉCURITÉ S'INSCRIT DANS UNE VISION STRATÉGIQUE ET A DES IMPACTS IMMÉDIATS SUR LES BUDGETS ET LES RÈGLES D'USAGE DES SYSTÈMES D'INFORMATION. S'Y INTÉRESSER, C'EST DÉJÀ FAIRE UN PROGRÈS SIGNIFICATIF : LA CYBERCRIMINALITÉ PEUT AUSSI METTRE EN PÉRIL L'EXISTENCE DE N'IMPORTE QUELLE ORGANISATION OU AFFECTER DURABLEMENT SON FONCTIONNEMENT ET SES RÉSULTATS. VOICI UNE PREMIÈRE SÉRIE DE QUESTIONS POUR VÉRIFIER QUE L'ON A BIEN PRIS LA MESURE DU SUJET.

5 QUESTIONS POUR FAIRE LE POINT

1 *Qui est mon RSSI ?*

Le connaissez-vous ? L'avez-vous rencontré ? Même si le poste n'existe pas dans votre entreprise, quelqu'un assure ou doit avoir la responsabilité de la sécurité des systèmes d'information. À qui reporte-t-il ? Quel est le périmètre de ses responsabilités ? Lui montrer votre intérêt est très significatif.

2 *Depuis quand n'ai-je pas entendu parler de cybersécurité ?*

Mettre le thème à l'agenda du Comex est simple à faire et essentiel. D'abord informatif, ce sujet fait monter en compétence le top management qui aura une approche plus pertinente et plus impliquée. Un point trimestriel, même rapide, est déjà un bon rythme. Votre RSSI peut aussi venir présenter des cas de cyberattaque relayés par la presse en montrant comment votre entreprise est concernée ou aurait réagi.

3 *Quand ai-je parlé de cybersécurité à toute l'entreprise ?*

De quand date votre dernier message pour sensibiliser vos équipes à ce sujet ? Sont-elles au courant des principaux risques ? Assez simple à mettre en place, une campagne régulière d'information et de sensibilisation peut éviter une catastrophe en tenant tout le monde en éveil afin d'adopter les bons comportements.

59 %

DES ENTREPRISES ONT AUGMENTÉ LEURS DÉPENSES DE CYBERSÉCURITÉ EN 2016

Source : The Global State of Information Security ® Survey 2017 de PWC

4 *Quelle est l'intensité des attaques subies par mon entreprise ?*

Toutes les entreprises subissent des attaques sur leurs systèmes d'information. Êtes-vous au courant du volume et de la fréquence de celles qui concernent votre entreprise ? Savez-vous si vos équipes ont déjà empêché avec succès une attaque majeure ?

5 *Suis-je exposé personnellement ?*

Au cœur de la stratégie de votre entreprise, vous êtes une cible de choix, et votre présence médiatique concentre l'intérêt des *hackers*, qui mesurent votre maturité et votre appétence pour la cybersécurité. Le premier moyen de vous protéger est donc de commencer par appliquer les règles et consignes préconisées, elles-même respectées par vos collaborateurs. Ces derniers seront d'autant plus motivés par votre exemplarité.

« SI UN COMEX N'A PAS ENTENDU PARLER DE CYBERSÉCURITÉ DEPUIS TROIS MOIS, C'EST QU'IL Y A UN PROBLÈME. »

5 QUESTIONS À POSER À SON RSSI

Les décisions stratégiques ou budgétaires ont forcément un impact sur la sécurité des systèmes d'information de l'entreprise : la cybercriminalité peut être un frein au déroulement des activités métier, la cybersécurité peut constituer un avantage concurrentiel dans la génération de valeur. Interroger en amont son RSSI est le meilleur moyen de savoir dans quel cadre agir.

1 *Quelles sont nos cinq plus grandes vulnérabilités ?*

Il est impossible de se protéger à 100 % contre toutes les menaces. Vous interroger sur les cinq plus grands risques que votre SI fait peser sur votre activité vous permettra de confirmer ou d'invalider vos décisions. Interrogez-vous également sur les vulnérabilités qui vous inquiètent et que vous aimeriez couvrir (*Cloud*, *Shadow IT*…), et partagez-les avec votre RSSI.

2 *La dernière cyberattaque était-elle dans notre cartographie des risques ?*

Avez-vous validé la cartographie et connaissez-vous les risques pris par votre entreprise ? Les attaquants profitent de l'effet de surprise et du manque de préparation de leur cible : savoir si la dernière attaque subie était envisagée vous poussera à vous interroger sur les risques que vous acceptez de prendre. Suivez aussi l'actualité des grandes cyberattaques et interrogez-vous : quelle serait la résilience de votre entreprise face à de telles attaques ? Êtes-vous prêts ?

205 milliards

NOMBRE D'EMAILS ÉCHANGÉS CHAQUE JOUR DANS LE MONDE EN 2015 (HORS SPAM)

Source : Radicati group, 2016

3 *De quand date notre dernier audit de sécurité ?*

En matière de cybersécurité, les audits et les tests d'intrusion sont essentiels. Ils révèlent les failles critiques et permettent de les corriger à temps : si vous optez pour des solutions dans le *Cloud*, êtes-vous en conformité avec la matrice des risques de votre entreprise ? Comment gérez-vous le *Shadow IT* et les usages non répertoriés de vos équipes qui ont trouvé en ligne ce que le SI ne leur propose pas ? Les menaces évoluent sans cesse, auditer régulièrement votre sécurité s'impose…

SHADOW IT

LE *SHADOW IT* DÉSIGNE LES MATÉRIELS ET LOGICIELS UTILISÉS DANS L'ENTREPRISE À L'INSU DE LA DSI ET DU RSSI.

4 *Sommes-nous préparés à une cybercrise ?*

Personne n'est jamais vraiment préparé à affronter une crise. Mais des exercices d'évacuation en cas d'incendie sont souvent organisés. Pourquoi ne pas faire de même avec le SI ? L'avez-vous déjà fait ? Avez-vous aussi un plan en cas d'attaque majeure ?

5 *Comment sommes-nous juridiquement protégés ?*

En cas de mauvaise protection du SI, votre responsabilité civile et pénale en tant que dirigeant peut être engagée. Surtout en cas de divulgation de données personnelles… Connaissez-vous votre exposition ? En avez-vous parlé avec votre RSSI, votre responsable juridique ou votre conseil extérieur ?

QUELLE **ORGANISATION** ?

UN RSSI EST SOUVENT RATTACHÉ À LA DSI. LA QUESTION N'EST PAS DE LE PLACER DANS OU EN DEHORS DE CELLE-CI MAIS LÀ OÙ IL AURA LES MOYENS D'AGIR EFFICACEMENT. À CONDITION D'APPLIQUER TROIS PRINCIPES : MANDAT CLAIR, PROXIMITÉ AVEC LE COMEX, LIBERTÉ D'ACTION. SA PAROLE AURA UNE MEILLEURE PORTÉE, ET LE MANAGEMENT CONSERVERA LA MAIN SUR LA POLITIQUE DE SÉCURITÉ LA PLUS ADAPTÉE À SA STRATÉGIE.

Dans certains organigrammes, le RSSI peut être rattaché à un membre de la direction générale, à la DSI, à une direction des risques voire à la DRH. L'important est de déterminer à quelle place il a le plus de chances d'être efficace. Trois principes encadrent sa mission :

- **un mandat clair :** délégations de pouvoir, responsabilités juridiques et opérationnelles, pouvoir d'imposer des choix techniques et organisationnels, de faire des arbitrages.
- **un niveau hiérarchique proche des instances dirigeantes :** il dépend directement d'un membre du comité de direction pour accélérer les prises de décisions.
- **une transversalité :** tous les métiers de l'entreprise sont concernés par la sécurité des systèmes d'information, pas seulement la DSI avec qui la coopération est constante.

66 %

DES RSSI SONT À LA DSI TANDIS QUE 22 % SONT DÉSORMAIS À LA DIRECTION DES RISQUES.

Source : baromètre Opinionway-Cesin, 2016

« LA SÉCURITÉ EST UNE FAÇON D'ÊTRE, ET NON PAS LA RAISON D'ÊTRE D'UNE ÉQUIPE CYBER. »

DES COMPÉTENCES DE PLUS EN PLUS RECHERCHÉES

Il est essentiel de bien choisir ses experts pour s'entourer dans sa propre entreprise, mais les compétences sont rares, disputées… et chères ! La cybersécurité est une « discipline » encore jeune et en pleine expansion, et le système éducatif peine aujourd'hui à former des experts en nombre suffisant.

TOUS LES MÉTIERS SONT CONCERNÉS PAR LA CYBERSÉCURITÉ

La cybersécurité n'est pas seulement une affaire de spécialistes. Bien au contraire, elle doit être intégrée dans tous les projets de l'entreprise. Un dialogue constant doit donc s'instaurer entre les équipes métiers et les experts de la sécurité numérique.

LE RSSI : RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Il définit et met en œuvre la stratégie et la politique de sécurité de l'entreprise. Certains RSSI ont vu leur titre évoluer en Responsable de la sécurité de l'information. Ce qui tend à prouver que la *data* devient le nerf de la guerre numérique.

COMMENT DÉFINIR LE **BON BUDGET** ?

COMBIEN ÇA COÛTE ? COMMENT SAVOIR SI L'ON DÉPENSE ASSEZ OU TROP ? COMMENT ÉVALUER EN FONCTION DE LA STRATÉGIE DÉCIDÉE ? QUESTIONS SOUVENT POSÉES MAIS SANS RÉPONSE SIMPLE…

Plusieurs acteurs de la cybersécurité, dont l'ANSSI, s'accordent sur des éléments de *benchmarking* : de 3 % à 10 % du budget informatique doit être consacré à la cybersécurité. Un *benchmarking* à affiner en se comparant à des entreprises du même secteur d'activité et de même taille, sachant qu'être dans la moyenne n'est pas la garantie d'une protection optimale…
Quel que soit son montant, ce budget comporte trois postes principaux :

- **la cyberdéfense** (protection, détection, réaction)
- **le maintien en condition des moyens techniques**
- **l'évolution des moyens techniques et des processus**

… Et un quatrième qui optimise les trois premiers : l'engagement de la direction et les campagnes d'information et de sensibilisation.

3 à 10 %
LE BUDGET INFORMATIQUE CONSACRÉ À LA CYBERSÉCURITÉ

« LA SÉCURITÉ DES SYSTÈMES D'INFORMATION PARTICIPE À LA CRÉATION DE VALEUR, COMME LES AUTRES ACTIVITÉS DE L'ENTREPRISE. »

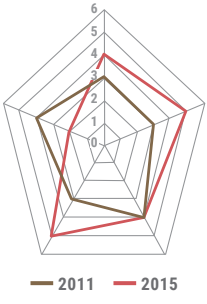
ET LE *CLOUD* ? *

Le *Cloud* est une révolution pour les organisations, avec un enjeu fort de développement économique. Confier à un tiers la gestion en réseau des données réduit les budgets informatiques, mais c'est aussi accroître les risques. L'ANSSI propose un nouveau référentiel pour sécuriser le secteur et le faire évoluer en confiance.

* Voir page 45 : 10 recommandations pour maîtriser le *Cloud*

QUEL **TABLEAU DE BORD** ? QUELS **INDICATEURS** SUIVRE ?

LE TABLEAU DE BORD CYBERSÉCURITÉ MESURE NOTAMMENT L'ÉCART ENTRE LA SITUATION RÉELLE ET LES OBJECTIFS DE L'ENTREPRISE EN FONCTION DES RISQUES ACCEPTÉS. IL COMPORTE AU MOINS CINQ SUJETS : STRATÉGIE, CONFORMITÉ, FINANCE, OPÉRATIONNEL, RH.



INDICATEUR SOUS FORME DE GRAPHE AVEC GRADUATION DU NIVEAU D'ENGAGEMENT DE L'ENTREPRISE DANS LES CINQ SUJETS TRAITÉS :

- Maturité de l'organisation
- Protection du dirigeant
- Sensibilité du patrimoine informationnel
- Exposition aux menaces cyber
- Niveau de résilience du SI

25 %

POURCENTAGE D'ENTREPRISES AYANT MIS EN PLACE UN TABLEAU DE BORD SSI

Source : Enquête MIPS du CLUSIF sur des entreprises de plus de 200 salariés, 2016

LA CYBERSÉCURITÉ CONTRIBUE AUSSI À LA RENTABILITÉ DE L'ENTREPRISE

Chaque jour, elle arrête des milliers de *spams*, sécurise des téléchargements, élimine des *phishings*, nettoie des milliers de mails infectés… Elle doit donc avoir un budget, des objectifs et des indicateurs, au même titre que les ventes, la trésorerie ou la performance RH.

LES INDICATEURS RENSEIGNENT SUR L'ÉTAT ET LES TENDANCES DE LA SSI

Ils mesurent les risques en fonction de leur maturité. Cinq sujets sont vitaux :

1. **Stratégie** : mise en œuvre de la politique de sécurité, dangerosité des risques, évolution de leur cartographie.
2. **Conformité** : mise en conformité réglementaire et normative, respect des engagements contractuels.
3. **Finance** : budget, retour sur investissement (coûts des incidents, pertes de CA évitées…).
4. **Opérationnel** : incidents avec identification des causes, audits et tests de vulnérabilité, taux de disponibilité des services, mises à jour (systèmes, logiciels), taux de réduction du *Shadow IT*.
5. **RH** : actions de sensibilisation, formations, compétences des équipes en charge.

POINT JURIDIQUE FLASH

LE RISQUE ÉVOLUE, LA LOI AUSSI. LES POUVOIRS PUBLICS ONT PRIS LA MESURE DU DANGER EN MATIÈRE DE CYBERSÉCURITÉ. DES DISPOSITIONS LÉGALES ENCADRENT DÉSORMAIS LES ORGANISATIONS, DES PLUS GRANDES AUX PLUS PETITES.

LA DIRECTIVE EUROPÉENNE *NIS* ENTRE EN VIGUEUR EN MAI 2018

L'Union européenne a adopté le 6 juillet 2016 la directive *NIS* (*Network and Information Security*). Elle instaure des règles et impose aux États de s'organiser et de coopérer.

EN FRANCE, LES OIV DOIVENT DÉJÀ RESPECTER PLUSIEURS MESURES DE SÉCURITÉ

Un opérateur d'importance vitale (OIV) est une entreprise ou une organisation qui exploite ou utilise des installations jugées indispensables à la survie de la Nation. La loi lui impose de renforcer la sécurité de ses systèmes d'information afin d'être mieux protégé contre les actes malveillants. Des obligations qui auront un impact sur ses sous-traitants.

20 M€

OU 4 % DU CA ANNUEL MONDIAL, L'AMENDE MAXIMALE PRÉVUE EN CAS DE NON RESPECT DE LA RÉGLEMENTATION EUROPÉENNE SUR LES DONNÉES PERSONNELLES

DES NORMES ISO POUR LA SÉCURITÉ NUMÉRIQUE

Les normes internationales, telles que la série ISO/CEI 27000, ont pour ambition de rendre la toile plus sûre. Elles fournissent un cadre pour le partage d'informations, la collaboration, la gestion des incidents. Elles peuvent aider à protéger la vie privée et à se prémunir contre les attaques.

DES LABELS ET DES CERTIFICATIONS

La CNIL délivre des labels à des produits et procédures. De quoi identifier plus aisément ceux qui garantissent un haut niveau de protection des données personnelles. De même, l'ANSSI peut certifier le niveau de sécurité de matériels et logiciels, en s'appuyant sur des tests d'intrusion.

EN CAS D'ATTAQUE, L'ENTREPRISE PEUT-ELLE SE DÉFENDRE ?

En cas de piratage, le bon réflexe est de se tourner vers l'ANSSI et vers les services spécialisés de police et de gendarmerie. Peu de sanctions sont cependant prononcées, les pirates étant souvent à l'abri dans des pays non coopératifs… Il est donc préférable d'anticiper : la loi y contribue.

LE RESPECT DES DONNÉES À CARACTÈRE PERSONNEL : UNE NOUVELLE CONTRAINTE ?

Le règlement européen de protection des données à caractère personnel du 27 avril 2016 entrera en application en mai 2018. Toutes les données qui permettent d'identifier un individu devront être protégées. Un règlement qui s'inscrit dans la continuité de la loi française « Informatique & Libertés » et qui vise à améliorer la confiance dans les systèmes numériques et leurs nouveaux usages.

« SI NOUS N'AVONS PAS CONSTATÉ D'ATTAQUES VISANT À DÉTRUIRE DES SYSTÈMES INFORMATIQUES INDUSTRIELS, CE N'EST PAS POUR AUTANT QUE NOUS N'EN AURONS PAS DEMAIN, CAR CETTE SITUATION EST TECHNOLOGIQUEMENT MATURE. L'OBJECTIF EST D'ANTICIPER. »

Ces pages ont été réalisées avec le concours de Me Eric Caprioli (Caprioli Associés), Matthieu Grall (CNIL) et Me Betty Sfez (Cabinet Sfez Avocats)

10 BONS GESTES POUR SE PROTÉGER

CES RECOMMANDATIONS CONCERNENT AUSSI BIEN LA VIE PROFESSIONNELLE QUE L'ESPACE PRIVÉ, QU'IL EST PRÉFÉRABLE DE NE PAS MÊLER. IL CONVIENT AUSSI DE PROTÉGER SON IDENTITÉ NUMÉRIQUE, SURTOUT POUR LES PAIEMENTS EN LIGNE, ET D'APPLIQUER LA MÊME PRUDENCE À TOUS LES ÉQUIPEMENTS : *SMARTPHONE*, TABLETTE, ORDINATEUR FIXE OU PORTABLE, OBJET CONNECTÉ…

01
DÉFINIR UN MOT DE PASSE DISTINCT POUR CHAQUE COMPTE

Chaque porte a sa clé : chaque compte bénéficie donc de son propre mot de passe. Couper les passerelles et cloisonner évite l'effet domino qui permet d'accéder à tous les comptes avec un seul mot de passe.

02
SAUVEGARDER RÉGULIÈREMENT

Conserver une copie des données est une mesure élémentaire, en entreprise comme à la maison.

03
EFFECTUER LES MISES À JOUR DES LOGICIELS

C'est un principe d'hygiène fondamental. Les attaquants recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser une faille non corrigée.

04
ÉVITER DE SE CONNECTER AU WI-FI PUBLIC

Les réseaux de bornes wi-fi publiques ne sont pas sécurisés : quelqu'un peut s'y connecter, épier les utilisateurs et récupérer leurs données. Il est donc préférable de privilégier une connexion 4G ou une solution d'accès sécurisé proposée par la DSI, quand c'est possible.

05

ÉVITER DE TRANSFÉRER DES DONNÉES PROFESSIONNELLES SUR UN COMPTE PERSONNEL

Autant que possible, pour éviter toute contamination, ne pas héberger des données professionnelles sur des équipements personnels (*smartphone*, clé USB…) ni brancher un support personnel sur un terminal professionnel.

06

S'ABSTENIR DE COMMUNIQUER SES MOTS DE PASSE

Donner à son assistant(e) plutôt une délégation sur sa messagerie afin qu'il ou elle reçoive celle-ci sur son propre poste.

07

ÉVITER DE CLIQUER SUR DES PIÈCES JOINTES, DES LIENS OU DES MESSAGES INCONNUS

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 !

08

RESTER PRUDENT EN PRÉSENCE DU PUBLIC

Idéalement, se prémunir des vues indiscrètes sur les écrans mobiles (il existe des filtres de protection), ne jamais se séparer des appareils, n'emporter que les données nécessaires à la mission, surtout à l'étranger (voire utiliser une connexion sécurisée).

09

ÉTEINDRE SES ÉQUIPEMENTS LE SOIR

Éteindre les terminaux limite les intrusions.

10

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

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

PARTIE 3

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

RENAUD TEMPLIER
Directeur Risque et Sécurité chez DEVOTEAM

LA CYBERSÉCURITÉ AU CŒUR DES PRÉOCCUPATIONS DE LA DIRECTION GÉNÉRALE

QU'IL S'AGISSE DE RÉPONDRE AUX OBLIGATIONS LÉGALES, D'ANTICIPER LES ATTAQUES MALVEILLANTES OU PLUS POSITIVEMENT DE DÉVELOPPER LA CONFIANCE DES CLIENTS, LA CYBERSÉCURITÉ RENTRE DÉSORMAIS DE MANIÈRE INDÉNIABLE DANS LE GIRON DES DIRECTIONS GÉNÉRALES.

La cybersécurité influe sur l'organisation de l'entreprise : il est indispensable de sécuriser les données, d'assurer la continuité de l'activité et la conformité par rapport aux réglementations (*General Data Protection Regulation*, *Solvency, Supervisory Review and Evaluation Process*, Loi de Programmation Militaire, etc.).

Cela étant, la cybersécurité a aussi un impact direct sur le business : tous les clients doivent se sentir dans un environnement de confiance et être rassurés sur le respect de leur vie privée et de l'utilisation de leurs données.

Il est impossible d'empêcher l'avènement de cyberattaques. En partant de ce postulat, les entreprises doivent opérer une réelle transformation de leur sécurité informatique et s'assurer de la résilience de leur système d'information. Cette transformation doit être gérée et pilotée grâce à l'engagement des dirigeants, avec des outils efficaces et de la gouvernance mise en œuvre. L'utilisation de tableaux de bords concis permet d'accélérer la prise de décision.

Du conseil à la conformité, Devoteam, acteur majeur du conseil en technologies innovantes et management pour les entreprises, accompagne ses clients du CAC 40 afin de les aider à définir une stratégie globale d'amélioration à coût maîtrisé.

devoteam

JEAN-NOËL DE GALZAIN
Président d'HEXATRUST

EN QUALITÉ DE DIRIGEANT, QUELLES SONT VOS RESPONSABILITÉS EN MATIÈRE DE SÉCURITÉ NUMÉRIQUE ?

Banque, assurance, industrie, santé… les entreprises de tous les secteurs doivent respecter la réglementation en vigueur (Directive NIS, RGPD, LPM…). Votre responsabilité de dirigeant et celle de votre entreprise sont engagées dans la protection des données personnelles de vos clients. En cas de pertes ou de fuites de données, les pénalités peuvent atteindre 4 % du CA mondial ou 20 millions d'euros ainsi que de l'emprisonnement en cas d'incident.

Le groupement Hexatrust s'est fixé l'objectif de réunir les meilleurs éditeurs de solutions de cybersécurité et de confiance numérique « made in France » dans un portfolio de 9 solutions essentielles, autour d'un label de confiance, pour les faire connaître aux dirigeants, aux DSI et aux RSSI. Ces solutions sont innovantes, déployées à l'international, souvent certifiées et qualifiées par l'ANSSI. Elles permettent d'aborder la cybersécurité de manière pratique et professionnelle, dans une approche partenariale au cœur des enjeux auxquels vous avez à faire face.

Il est donc naturel pour Hexatrust de s'associer à cette initiative en vue de promouvoir la cybersécurité auprès des dirigeants d'entreprise ou d'organisation publique. La sensibilisation des utilisateurs est une partie de la réponse. La mise en œuvre d'une politique de sécurité ensuite n'en est que plus bénéfique, dans un climat de confiance.

Alors surtout n'hésitez pas à nous solliciter, et bâtissons ensemble une transformation numérique cybersécurisée et durable…

DANIEL REZLAN
Président d'IDECSI

PROTÉGER LES DIRIGEANTS EUX-MÊMES

COMMENT SAVEZ-VOUS QUE PERSONNE NE LIT VOS MAILS ? ÊTES-VOUS GARANTI DE L'INTÉGRITÉ DE VOS ÉCHANGES ET DE CEUX DE VOTRE COMITÉ DE DIRECTION ? QUELQU'UN UTILISE-T-IL VOTRE MOT DE PASSE ? ÊTES-VOUS PRÉVENU SI UN ACCÈS INDISCRET OU MALVEILLANT SE PRODUIT SUR VOTRE COMPTE, SUR LES APPLICATIONS QUE VOUS UTILISEZ ?

Les dirigeants et le haut management sont au cœur de la stratégie et des informations clés de l'entreprise. Leurs données, leurs accès sont naturellement une cible très privilégiée de malveillances ou d'indiscrétions internes et/ou externes. Or, comment être certain qu'aucun accès ou paramétrage illégitime n'est actif en ce moment sur leur compte mail par exemple ? Ou sur celui du directeur financier, du DRH ou même du DSI ? Penser la sécurité numérique de son entreprise c'est à notre avis penser d'abord à garantir l'intégrité des comptes les plus sensibles.

Ce constat est à la genèse de la création d'Idecsi : apporter une solution adaptée aux dirigeants, c'est-à-dire sans aucune contrainte, immédiatement opérationnelle et couvrant tous les risques.

Cela s'appuie sur plusieurs exigences : adapter le bon niveau de sécurité pour chaque collaborateur en fonction de la nature des données qu'il échange, offrir une protection personnalisée couvrant en priorité les applications les plus sensibles, et mettre l'utilisateur au cœur du dispositif. Chacun peut même recevoir les informations qui le concernent sur son smartphone. Ce sont ces orientations stratégiques fortes qui animent notre action, avec l'ambition pour Idecsi d'être le plus utile aux dirigeants et aux managers de la sécurité.

IDECSI

MICHEL VAN DEN BERGHE
Président d'ORANGE CYBERDEFENSE

LA SÉCURITÉ EST LA CONDITION INDISPENSABLE D'UNE TRANSFORMATION NUMÉRIQUE RÉUSSIE

ALORS QUE LES ENTREPRISES DE TOUS LES SECTEURS MISENT SUR LA TRANSFORMATION NUMÉRIQUE POUR ABORDER LES NOUVELLES FORMES DE CONCEPTION, DE PRODUCTION ET DE CONSOMMATION, LES PROCESSUS AINSI CRÉÉS DOIVENT S'APPUYER SUR UNE POLITIQUE DE SÉCURITÉ QUI PROTÈGENT LEURS ACTIFS ESSENTIELS.

La sécurité n'est pas une fin en soi. Elle doit trouver sa place au sein des organisations pour accompagner le travail des métiers. Dans cet esprit, nos équipes Audit & Conseil adaptent leurs analyses et recommandations aux spécificités juridiques et techniques de chaque société. C'est en étant à l'écoute des besoins propres à chaque entité que l'intégration des outils et des procédures de sécurité s'effectuera dans les meilleures conditions. Lorsqu'une attaque survient, cela permet d'en limiter l'impact et un retour sans délai à une situation normale. Cette approche partenariale est indispensable pour que la diffusion croissante des technologies dans les organisations se déroule de la manière la plus performante possible. Les équipements de sécurité venant renforcer le savoir-faire des métiers en le protégeant contre les piratages ou les tentatives de blocage (saturation d'accès par déni de service, chiffrement contre rançon…). L'évolution constante de la menace exige un suivi précis des techniques présentes sur le Net : notre *CERT* (*Computer Emergency Response Team*) et notre laboratoire d'épidémiologie analysent et intègrent en continu les logiciels malveillants détectés sur notre réseau, et ceux de nos partenaires académiques et industriels.

Orange
Cyberdefense

STÉPHANE DAHAN
Directeur Général de SECURIVIEW

LA SURVEILLANCE DE VOTRE RÉSEAU RESTE LE MEILLEUR REMPART CONTRE LES CYBERATTAQUES

93%, C'EST LE POURCENTAGE DES GRANDES ENTREPRISES VICTIMES D'UNE CYBERATTAQUE DANS LE MONDE. 51% C'EST L'AUGMENTATION DE CES ATTAQUES CONTRE LES ENTREPRISES FRANÇAISES EN 2015 QUI ENTRENT DANS LE TOP 5 DES SOCIÉTÉS VISÉES. SE CACHENT ENCORE CELLES QUI IGNORENT QU'ELLES SONT VICTIMES.

Ransomware, attaques aux présidents, espionnage, exfiltration de données, vols de brevets…, autant de cyberattaques entrées aujourd'hui dans notre vocabulaire quotidien. Nous sommes désormais loin des actes de piratages qui n'apportaient que de la gloire à leurs auteurs. Les enjeux économiques font aujourd'hui espérer bien plus aux cybercriminels qui les commettent. Ces délits, remontés de jour en jour par les médias les plus généralistes, ne permettent plus de se cacher derrière l'ignorance en laissant ces aspects aux « sachants » de votre entreprise.

Depuis les années 90, une course folle à l'équipement n'a cessé de faire augmenter vos dépenses de protection et pourtant les actes malveillants n'ont jamais été aussi nombreux. Sans une expertise et une intelligence humaine pour les exploiter et les analyser, vous resterez vulnérable. Nous conseillons un rééquilibrage du budget dédié à la cybersécurité en transférant des fonds alloués à de la pure protection vers de la détection et de la riposte. Les *SOC* (*Security Operation Center*) sont aujourd'hui nécessaires pour organiser votre défense et vos ripostes. Ils sont à l'*IT* ce qu'ont été les centres de télésurveillance aux systèmes d'alarmes dans les années 80. Aujourd'hui, tous les utilisent et nul ne les remet en cause.

SECURIVIEW
NEXT GENERATION SOC

LAURENT GIOVACHINI
Directeur Général Adjoint du Groupe SOPRA STERIA

LA CYBERSÉCURITÉ EST DEVENUE UNE NÉCESSITÉ, POUR LES ORGANISATIONS COMME POUR LEURS DIRIGEANTS EUX-MÊMES

Pour rester compétitives, les entreprises doivent accélérer leur transformation digitale, tout en garantissant la protection de leur patrimoine d'informations. La cybersécurité apporte le socle de confiance indispensable à cette mutation.
Les dirigeants l'ont bien compris. De plus en plus sensibles aux risques d'entreprise induits par une menace croissante, ils augmentent en grande majorité leurs investissements en cybersécurité.
Les États également. Ils renforcent la réglementation pour surveiller les infrastructures critiques et protéger les données personnelles. Ces obligations engagent les directions générales, qui exercent de plus en plus souvent la responsabilité directe de la cybersécurité pour leurs organisations.
Sopra Steria, leader de la transformation digitale et offreur global en cybersécurité, est à leurs côtés pour les aider à relever ce défi. Opérateur de confiance, reconnu par l'ANSSI comme par l'ensemble de l'écosystème cyber, Sopra Steria assure la sécurité numérique de grands clients sensibles dans les secteurs de la défense, de l'aéronautique, de la banque, des transports ou encore de l'énergie.
La négligence humaine reste toujours la principale source de risques, avec de lourds impacts potentiels pour les dirigeants. Acteur d'une sensibilisation essentielle, je vous invite à suivre, comme je m'efforce de le faire, les précieux conseils de ce guide !

sopra steria

XAVIER LEFAUCHEUX
Vice-Président Europe du Sud de WALLIX

PROTÉGER VOS ACTIFS SENSIBLES EN DIMINUANT LES RISQUES D'ATTEINTE À LA SÉCURITÉ

En tant que dirigeant d'entreprise vous avez la responsabilité de conduire la transformation numérique de votre organisation. Cette responsabilité s'accompagne d'obligations légales qui vous engagent pénalement et financièrement. Alors, comment gérer les risques provenant du cyberespace ? Il existe un cadre réglementaire relatif à la protection des données et la sécurité des systèmes d'information (RGPD, Loi de Programmation Militaire) qui implique désormais la traçabilité des activités des utilisateurs « à privilèges » sur le système d'information, avec un délai de mise en conformité qui court jusqu'en 2018.

La protection des actifs sensibles de votre entreprise commence donc par la gestion des accès à votre SI, qui héberge vos applications et données sensibles, par vos employés « privilégiés » ayant des droits d'accès et vos prestataires externes, ainsi que par la gouvernance des mots de passe. Wallix est le concepteur de la solution logicielle « WAB Suite » qui offre un point de contrôle unique pour identifier les utilisateurs à risque, surveiller l'accès aux ressources et prévenir les fuites de données, et pour gérer les mots de passe de l'entreprise. Première solution du marché totalement certifiée CSPN par l'Agence nationale de la sécurité des système d'information (ANSSI), elle vous permet de répondre à vos obligations de mise en conformité. Le WAB a été choisi par plus de 400 sociétés et organisations publiques dans le monde pour protéger l'accès à leurs actifs sensibles.

WALLIX
TRACE, AUDIT & TRUST

LES **10 CONSEILS DU CESIN** POUR **APPRÉHENDER LE *CLOUD***

L'EXTERNALISATION DES DONNÉES DANS LE *CLOUD* EST AUJOURD'HUI UNE PRATIQUE BANALE. MAIS CETTE SOLUTION, QUI OFFRE DE GRANDS AVANTAGES, PEUT ÉGALEMENT PRÉSENTER DES RISQUES. C'EST POURQUOI LE CESIN A ÉMIS UNE SÉRIE DE RECOMMANDATIONS POUR LES PROJETS *CLOUD*.

1. Estimez la valeur des données que vous comptez externaliser ainsi que leur attractivité en termes de cybercriminalité.
2. S'il s'agit de données sensibles voire stratégiques pour l'entreprise, vous devrez valider le principe de leur externalisation.
3. Évaluez le niveau de protection de ces données en place avant externalisation.
4. Adaptez vos exigences de sécurité dans le cahier des charges de votre appel d'offre en fonction du résultat du point 1.
5. Effectuez une analyse de risque du projet en considérant les risques inhérents au *Cloud*.
6. Exigez un droit d'audit ou de test d'intrusion de la solution proposée.
7. À la réception des offres, analysez les écarts entre les réponses et vos exigences.
8. Négociez, négociez.
9. Faites valider votre contrat par un juriste. Si vous êtes une entreprise française, ce contrat doit être rédigé en français et en droit français.
10. Faites un audit ou un test d'intrusion avant démarrage du service et assurez-vous du maintien du niveau de sécurité de l'offre dans le temps.

85 %

DES ENTREPRISES STOCKENT DES DONNÉES DANS LE *CLOUD*

Source : baromètre Opinionway-Cesin, 2016

www.cesin.fr

SITES UTILES

33700 et **www.33700.fr**
Un numéro et un site pour signaler les SMS et MMS abusifs.

cert.ssi.gouv.fr
Le site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques.

#CyberVigilant
Un fil d'information sur Twitter, et de conseil pour se protéger efficacement.

www.hoaxbuster.com
Un site d'information sur les *hoax* (canulars) et rumeurs en circulation sur le Web francophone.

www.internet-signalement.gouv.fr
Un portail mis en place par les pouvoirs publics français pour transmettre des signalements de contenus ou de comportements illicites rencontrés sur Internet.

phishing-initiative.fr/contrib
Un service qui permet de dénoncer l'adresse d'un site de *phishing* francophone.

www.pointdecontact.net
Un service français de signalement en ligne de tout contenu choquant rencontré sur Internet.

www.signal-spam.fr
Une plate-forme nationale de signalement des *spams*.

LES ORGANISMES QUI PEUVENT VOUS AIDER

AFCDP
Association française des correspondants à la protection des données personnelles
www.afcdp.net

AFPI
Association française des prestataires de l'Internet
www.afpi-france.com

ANSSI
Agence nationale de la sécurité des systèmes d'information
www.ssi.gouv.fr

BEFTI
Brigade d'enquêtes sur les fraudes aux technologies de l'information
01 55 75 26 19

CDSE
Club des directeurs de sécurité des entreprises
www.cdse.fr

CESIN
Club des experts de la sécurité de l'information et du numérique
www.cesin.fr

CESYF
Centre expert contre la cybercriminalité français
www.cecyf.fr

CHECY
Centre des hautes études du cyberespace
www.checy.org

CIGREF
Club informatique des grandes entreprises françaises
www.cigref.fr

CLUSIF
Club de la sécurité de l'information français
www.clusif.fr

CNIL
Commission nationale de l'informatique et des libertés
www.cnil.fr

CYBERLEX
Association du droit et des nouvelles technologies
www.cyberlex.org

GITSIS
Groupement interprofessionnel pour les techniques de sécurité des informations sensibles
www.gitsis.asso.fr

HEXATRUST
Groupement d'entreprises françaises, éditrices et intégratrices de solutions innovantes dans les domaines de la sécurité des systèmes d'information, de la cybersécurité et de la confiance numérique.
www.hexatrust.com

IHEDN
Institut des hautes études de défense nationale
www.ihedn.fr

INHESJ
Institut national des hautes études de la sécurité et de la justice
www.inhesj.fr

OCLCTIC
Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication
01 49 27 49 27

SYNTEC NUMERIQUE
Syndicat professionnel des entreprises du numérique.
www.syntec-numerique.fr

QUIZ

**DÉTENDEZ-VOUS, PROFITEZ DE CE TEST (FACILE !)
POUR FAIRE LE POINT SUR VOS CONNAISSANCES**

01

LES INITIALES RSSI SIGNIFIENT…

- ☐ Républiques Socialistes et Soviétiques d'Ingouchistan
- ☐ Responsable des Systèmes de Sécurité Informatique
- ☐ Responsable de la Sécurité des Systèmes d'Information
- ☐ Je n'en sais rien

02

YAHOO! A ÉTÉ VICTIME…

- ☐ de Google
- ☐ d'un piratage de plus de 500 millions de comptes
- ☐ euh non, d'un piratage de plus d'1,5 milliard de comptes, en fait
- ☐ de négligence

03

UN BUDGET DE CYBERSÉCURITÉ REPRÉSENTE QUEL POURCENTAGE DU BUDGET INFORMATIQUE ?

- ☐ de 25 à 50 %
- ☐ de 10 à 25 %
- ☐ de 3 à 10 %
- ☐ Beaucoup trop

04

QUI CONNAÎT AUSSI LE MOT DE PASSE DE MA MESSAGERIE PROFESSIONNELLE ?

- ☐ Personne
- ☐ Mon assistant(e)
- ☐ Le responsable informatique
- ☐ J'aimerais bien le savoir

05

EXISTE-T-IL UNE NORME POUR LA CYBERSÉCURITÉ ?

- ☐ Non, il n'y en a pas encore…
- ☐ Oui, la norme ISO/IEC 27001-2013
- ☐ Oui, la norme ANSSI/OIV 2009
- ☐ Surtout pas, il y a assez de normes comme ça

06

33700 EST…

- ☐ le nombre de *spams* reçus chaque mois par la rédaction de *Challenges*
- ☐ le code postal de Mérignac, qui n'a rien à faire ici
- ☐ le n° de téléphone à contacter pour signaler les SMS et MMS abusifs
- ☐ le code de déblocage du mobile de Mark Zuckerberg

07

QU'EST-CE QU'UN *MALWARE* ?

- ☐ Le contraire du *bonware* (qu'on reconnaît au bruit qu'il fait quand il s'en va)
- ☐ Un habitant du Malawi
- ☐ Un Tupperware comportant un défaut
- ☐ Un programme informatique développé dans le but de nuire

RÉPONSES : Bien sûr, vous trouverez les réponses dans les pages de ce guide…

ISBN : 978-2-212-85439-8
Eyrolles, 2017