



Guide de la cybersécurité

édition 2016

***Transformation numérique et cybersécurité :
quand dirigeants et organisations doivent changer***

Evolutions réglementaires, innovations technologiques, enjeux culturels...
ils reviennent sur les principaux axes d'amélioration des entreprises pour les mois à venir.

MONACO

5 > 8 octobre 2016

2000 participants

4500 rendez-vous en one-to-one

160 ateliers et conférences

PROJETONS-NOUS ENSEMBLE

FONDEZ VOTRE BUSINESS SUR L'EXCELLENCE

Depuis 16 ans, Les Assises est l'événement incontournable le plus prisé de la scène professionnelle. Débats de haut niveau, échanges entre décideurs et leaders d'opinion, networking alliant business et convivialité. C'est le lieu de convergence de tout l'écosystème de la sécurité des systèmes d'information !



les assises

de la sécurité et des systèmes d'information

LinkedIn



YouTube

www.lesassisesdelasecurite.com

un événement
comeXposium
The place to be

DC
consultants

3

Marché

Transformation numérique et cybersécurité : n'oublions pas qu'elles sont inséparables

Le rôle du dirigeant n'a jamais été aussi important pour faire de la cybersécurité un sujet central dans la transformation de l'entreprise. Trois axes sont particulièrement à surveiller dans ce cadre.

Plus de 9 dirigeants sur 10, à la tête d'entreprises directement concernées par des cybermenaces admettent ne pas savoir interpréter un rapport de cybersécurité. D'après l'enquête qui évoque ce chiffre, menée par Goldsmiths (Université de Londres) pour Tanium et Nasdaq, le problème est qu'ils ne sont pas seuls. Parmi les dirigeants non-exécutifs et les cadres, 43% se sentent également démunis. Les DSI et les RSSI eux-mêmes ne sont pas épargnés : aux Etats-Unis, ils sont ainsi plus d'un sur cinq à faire les mêmes déclarations.

Cela pose la question de la justesse des choix stratégiques qui seront réalisés. « *Le dirigeant est dans une zone d'inconfort absolue* », note Olivier Ligneul, Chief Information Security Officer du groupe EDF et vice-président du Club des experts de la sécurité de l'information et du numérique (voir notre interview p.6). Comment aider le top management ? L'une des réponses est de sortir de la dissonance cognitive qui voudrait que la transformation numérique soit un sujet prioritaire pour l'entreprise,

au contraire de la sécurité numérique. Les deux sont indissociables comme le rappelle trois axes forts de transformation des organisations :

Les évolutions réglementaires

Beaucoup d'entreprises découvrent depuis quelques mois les changements impératifs qu'elles vont devoir mettre en place d'ici 2018 dans le cadre du Règlement européen sur la protection des données (voir p.14). D'autres acteurs ont depuis 2013 été confrontés à des évolutions majeures avec la Loi de Programmation Militaire. La parution en 2016 des arrêtés sectoriels contribuent à préciser l'action des acteurs industriels notamment (voir p.15). Et n'oublions pas d'autres dispositions, comme la directive NIS : si son impact paraît moindre que les précédentes, son périmètre s'avère beaucoup plus large. Aujourd'hui, les évolutions réglementaires concernent bien plus que les seules directions juridiques des entreprises : toute la gouvernance est impactée.

Les innovations technologiques

Elles sont bien sûr indissociables de la course effrénée entre « attaquants » et « défenseurs ». De plus en plus cependant, les champs qu'elles bouleversent sont variés : big data et *machine learning* pour faire face aux attaques ciblées

(voir p.16), administration facilitée pour l'ensemble des dispositifs de sécurité (p.17) ou encore travail de fond sur l'ergonomie des solutions afin de faciliter l'usage quotidien des collaborateurs (p.18)... Les points communs avec les évolutions technologiques « business » qui interrogent tous les acteurs de l'entreprise, sont innombrables.

Le changement de culture d'entreprise

Last but not least, l'évolution culturelle nécessaire autour de la sécurité dans les entreprises se lie intimement avec l'appropriation d'usages numériques globaux. Un peu de technologie, beaucoup de bons sens, est-on ainsi tenté de résumer (voir p.19) pour mieux accompagner les collaborateurs. Au-delà de leur sensibilisation sur certains vecteurs d'attaque, la montée en maturité se fait sur l'ensemble des comportements numériques, gages d'agilité et de résilience. Deux qualités que les entreprises voient comme des facteurs clés pour réussir dans un monde où numérique et business se recouvrent dorénavant presque entièrement. ■

Chiffres & Tendances

La cybersécurité, une priorité qui peine encore à s'imposer



83%

des entreprises se considèrent « exposées » aux cyberattaques

Dont

25%

se considèrent « très exposées »

Mais

31%

seulement placent la cybersécurité dans le top 10 de leurs priorités

Enjeux Cyber 2016 : La face cachée de la cyber - Deloitte 2016

L'impact réglementaire, connu mais mal maîtrisé



97%

des entreprises ont entendu parler du Règlement Européen sur la Protection des Données (GDPR)

Mais

57%

admettent qu'elles ne connaissent pas ou peu ce règlement

Facing the Cyber risk challenge - Lloyd's 2016

Le coût de la cybersécurité, sujet toujours douloureux



5 à 10%

du budget total de l'entreprise devraient y être consacré, selon Guillaume Poupard, directeur de l'ANSSI

Mais

C'est **MISSION (PRESQUE) IMPOSSIBLE** pour mesurer les coûts réels des cyberattaques selon l'ENISA, l'agence de l'Union Européenne pour la sécurité des réseaux et systèmes d'information. Les nombreuses études sur le sujet utilisent des méthodes et métriques trop variées pour dégager une vue unique.

The cost of incident affecting CIIs - ENISA Août 2016

Pratiques

« La cybersécurité prend sa place au cœur de la nouvelle gouvernance des entreprises »

Interview d'Olivier Ligneul, vice-président du CESIN - CTO & group chief information security officer d'EDF

L'affirmation d'une culture de la sécurité numérique au sein des organisations va de pair avec la montée en puissance d'une culture du changement et de la transversalité chez les responsables de la sécurité des systèmes d'information. C'est l'un des messages portés par Olivier Ligneul, CISO du groupe EDF, récemment nommé vice-président du CESIN, le Club des experts de la sécurité de l'information et du numérique, qui revient sur l'évolution de la gouvernance des entreprises.

A quel point la transformation numérique des entreprises impacte-t-elle la façon dont elles gèrent aujourd'hui le sujet de la cybersécurité ?

Ce sont deux mutations initiées en parallèle. D'un côté, la gouvernance globale de l'entreprise est de plus en plus remise en question par de nombreux facteurs, parmi lesquels de nouvelles formes de concurrence et des changements majeurs de business models, mais également de nouveaux modes de travail, de nouveaux outils, des rapports hiérarchiques différents, etc. De l'autre, la fonction « cybersécurité » change également en

devenant toujours plus transversale. Elle adopte une vision très protéiforme : pour trouver sa place dans la nouvelle gouvernance de l'entreprise, elle cherche le bon équilibre pour ne pas être un frein, sans tomber non plus dans la superficialité.

Concrètement, qu'est-ce que cela implique ?

L'un des plus grands changements est que cette évolution oblige les « métiers » de l'entreprise à intégrer directement en leur sein le sujet sécurité. Le CESIN a constaté ces derniers mois une multiplication de créations de postes de RSSI et ceux-ci ne sont plus mis à l'écart du reste de l'activité de l'entreprise sous prétexte de la technicité. Le lien est au contraire de plus en plus fort.

Bien sûr, il n'y a pas de recette miracle en matière de gouvernance, chaque entreprise affine la position du curseur sécurité au sein de ses métiers... mais deux enjeux se croisent systématiquement. D'abord, la nécessité d'avoir un RSSI qui développe une vision homogène et globale du sujet cyber pour l'entreprise. Plus que jamais, il est nécessaire de se doter d'un référent sur des enjeux de sécurité par nature transversaux.

Les responsables de la sécurité ne peuvent plus être focalisés exclusivement sur un sujet particulier : c'est ce qui fait la joie des attaquants. On l'a bien vu lors de l'attaque sur l'Ukraine l'an dernier, si le système électrique du pays a été touché, à travers une agression sur le réseau industriel, il y a eu en même temps une attaque d'ampleur sur le secteur tertiaire, saturant les centres d'appel, afin d'empêcher les clients impactés d'appeler leur opérateur... Développer une vision de synthèse est devenu primordial. A l'opposé, on ne peut cependant plus se passer de responsabilités décentralisées, en local. Autrement dit, le RSSI devient un métier comme les autres ! En effet, il ne viendrait à l'idée de personne dans le cadre de la gouvernance d'une entreprise de prétendre qu'un directeur financier peut se passer de comptables, et vice-versa.

Cette nécessaire intégration du métier de la cybersécurité à tous les niveaux est-elle aujourd'hui bien prise en compte par les entreprises ?

Une fois que l'on a dressé ce portrait idéal, les interrogations restent évidemment nombreuses. Encore une fois, il n'y a pas de



modèle type que l'on pourrait copier-coller. Par contre, nous avons assisté ces dernières années à des prises de conscience parallèles, qui se répondent.

Les RSSI ont su prendre de plus en plus de recul. Ils ont conscience qu'ils ne peuvent plus se contenter d'être des ultra-spécialistes qui vont gérer les règles du pare-feu de l'entreprise. Ils savent qu'ils doivent se mêler au reste de l'or-

ganisation, avoir une démarche proactive et penser la sécurité comme un élément à part entière de la stratégie business. Et cet état d'esprit fonctionne : en 2016, le RSSI n'est plus celui qui déjeune en solitaire à la cantine !

Du côté des dirigeants, il y a clairement eu une prise de conscience généralisée de l'importance de la menace et de la nécessité à prendre le sujet en main. C'est la

« Les RSSI ne peuvent plus se contenter d'être les ultra-spécialistes qui gèrent les règles des pare-feux de l'entreprise »

Olivier Ligneul
vice-président du CESIN - CTO &
group chief information
security officer d'EDF

première étape pour voir ensuite les comportements évoluer et le sujet de la cybersécurité intégrer à part entière la nouvelle gouvernance de l'entreprise. En évoluant de concert, ces deux mondes ont commencé à échanger de plus en plus limpidement. Je pense qu'aujourd'hui, les RSSI parlent beaucoup plus aux directions générales qu'il y a de cela quelques mois. C'est un changement majeur pour les métiers de la cybersécurité, qui les rapprochent également d'autres acteurs aux responsabilités transversales comme le directeur des risques ou celui de la sécurité (physique, ndlr).

Ces évolutions n'empêchent pas beaucoup de dirigeants d'avoir l'impression que le sujet de la cybersécurité est extraordinairement large et complexe... et que prendre les bonnes décisions est un véritable défi. Comment peuvent-ils s'assurer d'aller dans le bon sens ?

Il est certain que le champ des possibles est énorme. Le nombre de scénarii envisageables pour une cyberattaque ne se situe tout simplement pas dans un environnement « fini ». Intellectuellement, il est donc très difficile de prendre la mesure de ce qui est en train de se passer, de ce que cela représente pour son entreprise, et surtout, de ce que l'on peut faire pour assurer au mieux sa sécurité. C'est d'autant plus difficile qu'en face, les attaquants sont connus pour savoir s'adapter en permanence. Les variables sont donc nombreuses et on ne les maîtrise pas. C'est une zone d'inconfort absolue : le risque fait peur, la question de la confiance que l'on peut accorder aux très nombreux « sachants » - internes ou externes - se pose clairement... et l'efficacité des moyens humains et financiers que l'on

consacre à la sécurité n'est pas toujours visible de prime abord. Mais il en va de même pour de nombreux sujets, il ne faut pas en faire un blocage psychologique. Par nature, le métier du dirigeant est de piloter l'entreprise pour la faire croître, pour respecter ses valeurs, en faisant des choix qui ne sont pas toujours faciles, le tout dans un environnement incertain. L'important est donc de tracer le chemin entre la réalité actuelle du niveau de sécurité de son entreprise et un niveau cible idéal. Entre les deux, c'est une progression maîtrisée qu'il faut lancer.

Comment ?

L'un des principes qui pourra le plus venir en aide à un dirigeant est - cela peut paraître paradoxal - sa capacité à lâcher-prise. Cela revient à prendre en compte que l'on ne pourra jamais tout protéger parfaitement. Il faut donc choisir et souvent, renoncer. C'est là que la relation avec le RSSI révèle toute son importance : c'est le rôle de ce dernier de mettre en lumière ce qui est le niveau de protection minimum - pour tous - sous lequel l'entreprise ne peut pas descendre. A partir de cet essentiel, il sera plus simple de définir quels efforts et quels moyens complémentaires on pourra consacrer aux sujets que les dirigeants jugeront prioritaires.

Qu'en est-il de l'influence du dirigeant sur l'émergence d'une « culture de la cybersécurité » au sein de son entreprise ?

La priorité est d'éviter une approche de technicien, de prescripteur de la « bonne culture sécurité », qui s'avère très dommageable. A l'inverse, il y a des fondamentaux à rappeler, encore et encore. Le premier d'entre eux est l'exemplarité. C'est un point tout

à fait important pour le dirigeant. Il s'agit là de son comportement personnel, mais également, plus largement du fait que l'entreprise applique des règles uniformes pour tous et à tous les niveaux de la structure.

Mais la montée en puissance d'une culture de la sécurité au sein de l'entreprise, et notamment au sein du top management, ne se fera seulement si on assiste en parallèle à l'affirmation d'une culture du changement du côté des acteurs cyber, et du RSSI au premier rang d'entre eux. Cette culture du changement doit s'emparer des nombreux nouveaux usages amenés par la transformation numérique, de la complexité du rapport entre vie privée et vie professionnelle, des enjeux de liberté personnelle des collaborateurs, mais également de productivité... Internet l'a prouvé depuis 20 ans, les gains apportés par ces nouveaux usages sont supérieurs aux craintes que l'on peut avoir... à condition d'être prêt à avoir une vision de la sécurité dynamique, qui ne reste pas figée dans ses anciens credos. Entre contrôle centralisé et responsabilisation totale des individus, il existe un équilibre à acquérir.

Prenons l'image du Président des Etats-Unis : après des siècles d'ajustement, celui-ci n'a jamais été autant protégé qu'aujourd'hui et pourtant aucun président n'a jamais été autant communicant. Quand il se déplace, il est dans un véhicule avec un tel niveau de blindage, qu'il est complètement coupé du monde autour de lui... tout en restant ultra-connecté avec un niveau de services et de capacité à agir sans concession. Au-delà du caractère exceptionnel de ce que représente son rôle, c'est bien cette philosophie-là qui doit présider à une gouvernance moderne de la sécurité. ■

Pratiques

Retour sur une année de cyberattaques

Stuxnet, TV5Monde, Target... Certains noms résonnent encore au cœur des discussions entre spécialistes de la cybersécurité. Au-delà de la tentation qu'ont pu avoir certains offreurs de technologie de renforcer un « marketing de la peur » en surfant sur la médiatisation croissante des menaces, cette dernière a également contribué à renforcer la maturité de nombreuses organisations sur un sujet qu'elles laissaient auparavant de côté. Une montée en maturité qui sera sans doute encore aiguillée par les nouvelles attaques qui ne manqueront pas de faire la « Une ». Tour d'horizon de quelques événements qui ont d'ores et déjà fait de 2016 une année cyber mouvementée.

Black-out en Ukraine

Les tous derniers jours de l'année 2015 ont donné le ton : plusieurs centaines de milliers d'Ukrainiens ont été plongés dans l'obscurité pendant les fêtes, alors que le réseau électrique du pays était victime d'une série de cyberattaques coordonnées. C'est le cheval de Troie fort à propos nommé Black Energy, déjà connu, qui a été le vecteur principal de cette agression. Celle-ci a souligné une nouvelle fois les liens à risques qui s'établissent de plus en plus entre systèmes industriels et systèmes informatiques de gestion, offrant de nombreuses opportunités pour les criminels.

Casse du siècle au Bangladesh

Le 4 février 2016, la Banque Centrale du Bangladesh est victime d'un hold-up d'un genre nouveau, basé sur une approche sophistiquée : une forte expertise technique, associée à une excellente connaissance des usages de la banque, permettent aux attaquants

de subtiliser 81 millions de dollars en ciblant l'interface entre l'institution et le réseau d'échange inter-bancaire SWIFT. Dans la foulée, la banque empêche 850 millions de dollars supplémentaires d'être détournés. Jusqu'alors, SWIFT était considéré comme un système parfaitement sûr.

Aux Etats-Unis, le piratage s'invite au cœur de la campagne présidentielle

La multiplication des cyberattaques rythme les actualités de la campagne à couteaux tirés qui se joue entre Hillary Clinton et Donald Trump, mettant les sujets de la cybersécurité, de la responsabilité des individus et de la cyber-souveraineté au centre des débats. Coup sur coup, le public américain a ainsi pu voir des dizaines de milliers d'emails du DNC (Comité National Démocrate) être piratés, une tentative d'attaque sur les bases de données électorales ou encore la mise sur le marché par un groupe de hackers d'outils informatiques provenant de la NSA. Les cyberattaques se banalisent ainsi aux côtés des autres thèmes de la campagne comme l'immigration ou la lutte contre le terrorisme. Qu'en sera-t-il en France ?

Des cas de « Retour vers le Futur »

Des attaques ayant déjà eu lieu il y a plusieurs années peuvent avoir des conséquences bien réelles sur le présent. En septembre 2016, Yahoo - en pleine opération de rachat par l'opérateur télécom Verizon - publie une alerte sur le fait que les informations (noms, adresses email, téléphones, mots de passe) concernant 500 millions de ses utilisateurs lui ont été volées en 2014. Peu de temps avant, c'était Dropbox, la plateforme de stockage et d'échange de documents en ligne, qui a reconnu que 68 millions de ses utilisateurs s'étaient fait dérober leurs informations... en 2012. Bien que la valeur des données mises en vente sur Internet décroisse rapidement avec le temps, il n'est pas rare de voir circuler ainsi de nombreuses années plus tard le « butin » de pirates. En cause notamment, le temps mis par les entreprises pour se rendre compte qu'elles ont été compromises : il dépasse encore les 200 jours en moyenne.



Pratiques

Prise de conscience et montée en puissance cyber : les entreprises témoignent

Quelle que soit leur taille, toutes les organisations sont concernées par des problématiques de cybersécurité. Le numérique fait en effet aujourd'hui partie intégrante de leur activité, même si l'informatique n'est pas considérée comme leur cœur de métier et les entreprises tentent de faire les meilleurs choix pour faire face aux menaces. Trois d'entre elles décrivent leurs expériences.

« A aucun moment, nous nous sommes dit que nous allions payer la rançon demandée ! »

Véronique Brosseau, directrice du Cabinet BME est catégorique. Son entreprise, une TPE de 4 personnes spécialisée dans le secteur de la construction de bâtiments, a été ciblée durant l'été 2016 par un *ransomware* qui a bloqué tout son système informatique. Après 20 ans d'existence, l'entreprise était finalement confrontée à une cyberattaque qui, dans la perception de sa dirigeante, ne la concernait tout simplement pas. *« Nous avons bien entendu parler du sujet mais nous avons regardé de loin la médiatisation autour des attaques informatiques. Avec du recul, évidemment, je me dis que le problème n'avait rien à voir avec la taille de notre activité et que nous avons été pris dans quelque chose de plus large, qui ne nous visait pas spécifiquement »* témoigne-t-elle.

La TPE renforce sa résilience face aux ransomware

Le cas est représentatif de la prise de conscience qu'ont de plus en plus de dirigeants : si certaines affaires « cyber » parmi les plus médiatisées, espionnage, sabotage, détournement de fonds... sont le fruit d'attaques complexes et de technologies perfectionnées, tout un pan de l'économie est touché par une cybercriminalité beaucoup moins élitiste mais pas moins dommageable. TPE et PME, en pleine transformation numérique, se retrouvent au centre de la tempête.

Contrairement aux deux tiers des entreprises de toutes tailles confrontées à un problème de *ransomware*, le Cabinet BME a donc choisi de ne pas payer la rançon demandée. Du fait de la criticité des données prises en otage ou parfois en évaluant que le montant réclamé par leurs agresseurs est relativement faible (le montant moyen des rançons s'évaluent à environ 722 dollars, d'après une étude menée par l'éditeur japonais Trend Micro), beaucoup choisissent encore de céder. Les études spécialisées soulignent cependant que malgré une professionnalisation croissante des cybercriminels, le fait de traiter avec eux n'assure en rien de débloquer son système. De son côté, Véronique Brosseau, après une précédente més-

aventure, avait décidé d'organiser de manière beaucoup plus efficace son système de sauvegarde. Avec son habituel prestataire informatique, elle s'était donc équipée d'une solution proposée par l'éditeur français Woxoo. Ce parti-pris lui permettra lors de l'incident de reprendre son activité en 36h. A défaut d'avoir les moyens de mettre en place une protection digne des plus grands, la TPE a donc fait le choix de la résilience. Une décision de bon sens, alors que les entreprises de taille modeste ne peuvent tout simplement pas avoir une personne en charge de la sécurité à plein temps.

La Fédération Française de Tennis construit sa stratégie

Pas de responsable de la sécurité du système d'information non plus du côté de la Fédération Française de Tennis (FFT). Le directeur technique au sein de la DSI, Franck Labat se pose bien la question, mais n'a pas franchi le pas : *« En tant que fédération sportive, notre cœur de métier est loin d'être l'informatique... et pendant longtemps nous ne nous sommes pas posés la question d'une « stratégie de sécurité ». Mais le quotidien des entraîneurs, arbitres, gérants de club... laisse aujourd'hui une place de plus en plus importante aux outils collaboratifs et numériques. Cela change tout »*.



La FFT a pris en main sa stratégie de cybersécurité - CC BY 2.0 Chris Eason

La FFT a donc été confrontée ces derniers mois à une situation que connaissent de plus en plus d'entreprises de taille moyenne : par où commencer pour renforcer sa sécurité ? Et comment couvrir les spécificités de son activité avec des budgets raisonnables ? « *Le DSI a poussé le sujet au niveau de la direction. Le point de départ a été la conviction qu'il fallait agir. Ensuite, nous avons mené un audit pour, disons le crûment, « secouer le cocotier » et montrer les limites de notre fonctionnement actuel* » raconte Franck Labat. A partir de là, la fédération a dû faire des choix. En 2016, les réponses tactiques sur les sujets urgents ; plus tard,

en 2017, une montée en puissance généralisée pour augmenter le niveau global de sécurité. De quoi montrer des gains immédiats aux dirigeants, pour les convaincre de l'utilité de la démarche.

Implication des instances dirigeantes

En la matière, la FFT travaille par exemple avec l'éditeur américain Varonis pour optimiser la gestion et le contrôle des accès à ses données. Le directeur technique explique : « *A l'occasion d'un tournoi comme Roland-Garros, nos effectifs augmentent considérablement et nous devons mieux gérer ces accès saisonniers à nos données,*

tout en en profitant pour acquérir une bien meilleure visibilité sur nos infrastructures, nos usages en tant qu'organisation et ceux de nos collaborateurs, souvent isolés. »

Pour monter encore en puissance, la fédération va entamer une politique de communication intensive à l'intention de tous ses collaborateurs. « *Nous savons pertinemment que c'est le maillon le plus faible qui fait casser toute la chaîne de la sécurité. C'est le niveau minimum que nous devons augmenter, en introduisant une hygiène informatique de base et une première approche de la philosophie de la sécurité* ». Pour

ce faire, c'est un travail étroit avec les dirigeants qui est mené, afin que tout le management montre l'exemple sur les comportements du quotidien : verrouillage des téléphones mobiles, secret autour des mots de passe, liens permanents avec le département des ressources humaines... « *La direction générale est impliquée de A à Z. C'est essentiel pour assurer une continuité de la sécurité, du point de vue global jusqu'au système d'information lui-même* » remarque Franck Labat. « *Pour le reste, il faut trouver le bon équilibre... si je voulais vraiment toute la sécurité du monde, je couperais tous les accès à Internet et j'interdirais Facebook. Et je me retrouverais au chômage le lendemain* » plaisante-t-il.

Le Groupe SFA veut s'améliorer en permanence

L'engagement de la direction est également une constante pour le Groupe SFA. Comptant plus de 1000 salariés, 3 sites de production français et 25 filiales de distribution au niveau monde, cette entreprise industrielle est une ETI qui grandit encore et encore. Elle est également adossée à un groupe de presse avec des publications aussi connues que *Challenges* ou *Sciences et Avenir*. Frédéric Carricaburu, son DSI, explique que le sujet de la cybersécurité a toujours été sensible, afin d'assurer la protection des secrets industriels, des brevets, mais aussi des sources des journalistes. Depuis plusieurs années, c'est le directeur général adjoint en charge des aspects informatiques qui s'est fait le vecteur du changement, en poussant le comité de direction à ne pas se reposer sur les

investissements déjà réalisés. « *Quand on a déjà beaucoup de choses en place, se pose évidemment la question des choix qui seront vraiment utiles pour étendre le niveau de sécurité ! Il ne s'agit plus, contrairement à ce qui pouvait se faire il y a 10 ans, de choisir un énième pare-feu...* » témoigne le DSI.

D'autant plus que l'entreprise est confrontée à deux dynamiques qui se croisent. D'un côté, le périmètre de son système d'information s'étend et s'ouvre de plus en plus sur son écosystème. De l'autre, il n'est plus envisageable de bloquer les usages variés des utilisateurs. « *A force de vouloir mettre de la sécurité partout, cela devient rapidement ingérable, on se retrouve avec un chaos contreproductif* » insiste Frédéric Carricaburu, pour qui comprendre finement ce qui se passe sur les systèmes et se positionner dans une analyse proactive est la bonne réponse quand une entreprise commence à avoir un niveau de maturité respectable.

L'analyse de long terme pour mieux « se comprendre »

Avec DarkTrace, une start-up britannique fondée en 2013 par des anciens de l'univers du renseignement et des chercheurs en mathématique, le groupe SFA s'est donc mis à observer l'ensemble de son système en temps réel. L'approche de la jeune entreprise, qui a levé 65 millions de dollars durant l'été et se revendique du système immunitaire humain, s'appuie sur du machine learning et des mathématiques bayésiennes pour affiner en permanence la compréhension de ce qui se passe dans l'écosystème numérique de l'entreprise.

« *Nous n'avons pas mis cette solution en place pour apporter une réponse immédiate à un problème déjà identifié, comme c'est souvent le cas en matière de cybersécurité* » note Frédéric Carricaburu. « *Nous sommes dans l'analyse de plus long terme. On est parti du principe que nous étions déjà sans doute compromis d'une façon ou d'une autre. Nous avons donc commencé par une détection de presque tous les événements, pour ensuite réduire progressivement la sensibilité des alertes* ». Progressivement, l'apprentissage automatique reconnaît quels sont les « usages » normaux de l'entreprise et identifie les anomalies, signes potentiels d'une attaque.

Mais une solution logicielle, aussi bien conçue soit-elle, ne fait pas tout. Le DSI du Groupe SFA entend par ailleurs continuer à augmenter la sensibilité de toutes les parties prenantes de l'entreprise à la diversité des menaces : « *Sans se laisser bloquer par la peur, il ne faut pas que l'on puisse se dire que les cyberattaques n'arrivent qu'aux autres. Nous allons donc continuer à sensibiliser, grâce à des moyens innovants comme des serious games, notamment dans nos usines. Et auprès de nos directeurs également, en attirant plus que jamais l'attention sur les risques d'arnaque au président par exemple* ». Une nouvelle fois, le rôle du dirigeant est mis en avant : même dans les plus grandes organisations, il suffit ainsi que l'un d'entre eux soit conscient des enjeux et convaincu qu'il lui faut agir, pour pouvoir rapidement faire naître ces mêmes convictions chez ses pairs. ■

Zoom

Vecteurs d'attaques : que surveiller en priorité ?

Le mélange entre capacités technologiques et ingénierie sociale rend la variété des attaques possibles sur une entreprise presque sans limite. Retour sur certaines des fragilités les plus courantes dans les organisations.

Les points d'entrée dans les systèmes de l'entreprise et la nature informatique des menaces ne sont qu'une partie de l'équation que doivent prendre en compte les responsables dans les organisations pour acquérir la vision la plus complète de leur cybersécurité. Autrement dit, la notion de cyberattaque est plus large que de mettre face à face une technologie malicieuse et une conséquence malheureuse sur le système d'information : entre les deux, des hommes, des usages, des erreurs, des combinaisons de menaces et de problèmes, contribuent à faire de la protection de l'entreprise un sujet à la fois transversal et loin d'être simpliste.

Trois modèles pour une majorité de menaces

Ceci étant dit, les attaques les plus insidieuses et complexes, dites « APT » pour Advanced Persistent Threat, ne représenteraient que 0,4% de la totalité des opérations malicieuses, selon le Data Breach Investigation Report 2016 mené par Verizon. Ce « grand espionnage » vise en priorité les grandes entreprises et notamment les Opérateurs d'Importance Vitale.

Pour les autres, le même rapport évoque que 93% des compromissions de données se déroulent en quelques minutes à peine et que la grande majorité des entreprises seront avant tout confrontées aux deux ou trois types de menaces qui visent leur secteur d'activité en particulier.

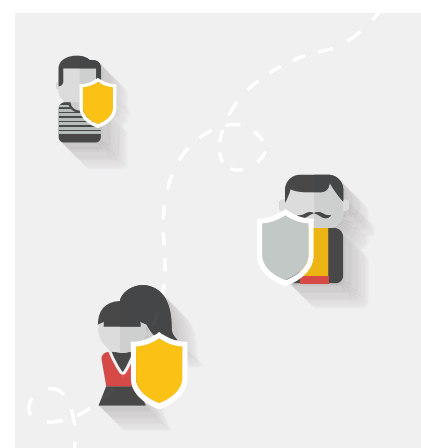
Ainsi, dans le secteur du divertissement, les incidents sont presque exclusivement concentrés sur des attaques par déni de services (ddos), alors que dans celui de la santé ce sont les vols et pertes de terminaux physiques, les utilisations abusives d'accès en interne et des erreurs non-intentionnelles du personnel qui représentent les trois-quarts des problèmes. Dans le commerce de détail, les attaques ddos, celles sur des applications web et les intrusions de points de vente/paiement représentent 9 incidents sur 10. Autrement dit, chaque activité peut déjà identifier assez facilement ses propres démons.

Des emails au potentiel destructeur

Toutes catégories confondues, l'email reste cependant l'un des points d'entrée privilégiés dans l'entreprise, que ce soit de manière indéterminée à travers des campagnes qui toucheront au hasard des millions de personnes, ou au contraire de façon extrêmement ciblée, en s'adressant spécifiquement à un individu, généralement

en ayant emprunté préalablement l'identité d'une de ses connaissances.

Depuis un peu plus d'un an, les entreprises ont notamment été confrontées à la montée en puissance notable des ransomware, qui rendent inaccessibles un système en le chiffrant, après qu'un utilisateur ait ouvert une pièce-jointe infectée. Ces prises d'otage numériques ont tout simplement explosé. Le phishing, qui renvoie à partir d'une url, à l'allure tout aussi officielle que l'email qui la contient, vers une page web contrefaite, afin de subtiliser des informations personnelles, est également en forte progression. Ces emails n'ont, par ailleurs, pas cessé de voir leur qualité et donc leur efficacité augmenter. En visant n'importe quel collaborateur dans l'entreprise, ces menaces sont devenues parmi les plus visibles au sein des écosystèmes professionnels. ■

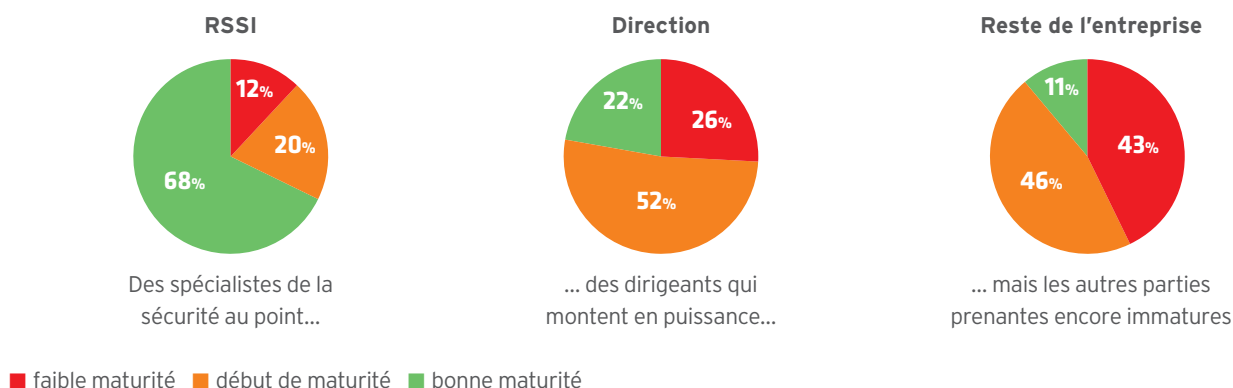


Sondage

Quelle est la maturité perçue des entreprises en matière de cybersécurité ?

Près de 80 spécialistes, fournisseurs de solutions et prestataires de services de sécurité, ont accepté de partager leur perception de la maturité des entreprises sur leur marché. Quelques enseignements :

Quel est le niveau de maturité des acteurs de l'entreprise ?



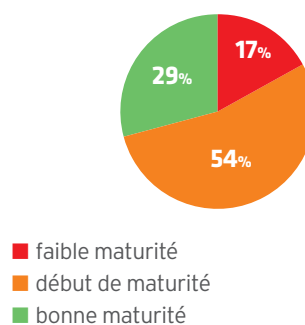
Qui doit être le moteur du changement ?



Mention spéciale à la direction juridique

Les évolutions réglementaires sont connues mais posent encore des difficultés.

Maturité sur les nouvelles réglementations



Des disparités importantes en matière de maîtrise des technologies de sécurité



Sécurité des réseaux et infrastructures
Bien maîtrisée



Sécurité des applications et des données
Mal maîtrisée



Sécurité des usages mobiles
Mal maîtrisée

Sondage

Quelles devraient être les priorités des entreprises en 2017 selon les prestataires ?

« Profitez des projets de transformation digitale, ou bien encore des projets DevOps pour intégrer la sécurité plus profondément dans votre architecture et dans vos process » **Arnaud Cassagne**, directeur des opérations, Optalia

« Rapprochez-vous de vos RSSI et des besoins métiers » **Jean-François Tesseraud**, CISO/RSSI, Systemis

« En 2017, préparez-vous à... 2018 et l'entrée en vigueur du Règlement Européen sur la Protection des Données (RGPD) » **Laurent Heslault**, directeur des stratégies de sécurité, Symantec

« Formez les utilisateurs aux bons usages et pratiques en matière de cybersécurité et sensibilisez aux enjeux... encore et encore » **Simon Roger**, président directeur général, TheGreenBow

« Réalisez des tests d'intrusions, renforcez votre détection des incidents, recrutez des compétences pour analyser, réagir et améliorer » **Gabriel Leperlier**, head of continental Europe advisory services GRC/PCI, Verizon

« Améliorez la gestion des identités : établissez une cartographie complète des données de l'entreprise et des collaborateurs y ayant accès, et gérez les droits au quotidien par des campagnes de contrôles impliquant l'ensemble des métiers de l'entreprise » **Moullan Chakir**, country manager, 8MAN

« Assurez-vous que vos responsables sécurité coopèrent au quotidien avec votre DSI » **Patrice Denos**, responsable département security management, Nedap

LE SECTEUR VU COMME LE PLUS INSPIRANT EN MATIÈRE DE CYBERSÉCURITÉ



Banques & Assurances

CEUX QUI DOIVENT ENCORE FAIRE DES EFFORTS IMPORTANTS



Tourisme & Loisirs



Medias



Enseignement



Collectivités territoriales

50 acteurs de la cybersécurité à suivre

Le jeune marché de la cybersécurité continue son évolution rapide. Sous la pression des nouvelles réglementations, les Opérateurs d'Importance Vitale (OIV) consentent à des investissements importants. Les PME et ETI, elles, prennent conscience de leur dépendance au numérique et de la nécessité de mettre en place ou d'améliorer leur stratégie de sécurité. Pour répondre à ces besoins variés, de produits et de services associés, c'est une myriade d'acteurs, de toute taille, pure-players ou non, qui se sont positionnés ces dernières années. Le marché attend encore les grandes consolidations qui clarifieront de nombreux pans de leurs activités.

Alliancy le mag vous fait découvrir 50 acteurs qui ont répondu à son enquête et qui proposent d'accompagner les dirigeants et leurs entreprises dans leur transformation, en toute sécurité.

🛡️ Sécurité des réseaux & infrastructures

🛡️ Sécurité applicative & des données

🛡️ Sécurité mobile

🛡️ Audit & recherche

🛡️ Conseil & politique de sécurité

Ⓢ Prix de l'Innovation des Assises de la Sécurité 2016

	🐦	🛡️	🛡️	🛡️	🛡️	🛡️
6cure	@6cure	●				
8MAN	@PN8MAN	●	●		●	
ACENSI Cybersecurity	@acensigroup	●	●	●	●	●
Advens	@advens	●	●	●	●	●
aleph-networks	@alephnetworks1	●	●			●
Arbor Networks	@arbornetworks	●	●			●
Avencis	-	●	●	●	●	
Bitdefender	@BitdefenderPro	●	●	●		●
Brainloop	@brainloopinc		●	●	●	
Brainwave	@brainwave_fr		●		●	
CDC Arkhineo	@CDC_Arkhineo		●			
Cisco	@CiscoSecurity	●	●	●	●	●
Citrix	@CitrixFrance	●	●	●		●
CS	-	●	●		●	●
DenyAll	@DenyAllSecurity		●			●
EfficientIP	@efficientip	●	●	●		●
Enki	@ENKI_SECURITY	●	●	●	●	●
ESET	@ESET_France	●	●			●
Fortinet	@Fortinet	●	●	●	●	●
GB&Smith	@gbandsmith	●	●		●	
Gemalto	@GemaltoSecurity	●	●	●	●	●
Harmonie Technologies	@HarmonieSSI		●	●	●	●
iGuard	@iGuard_france	●	●	●		
iTrust	@iTrust_France	●	●		●	●
Kaspersky Labs	@kasperskyfrance	●	●	●		●
Keeex	@KeeexTwt		●			●

	🐦	🛡️	🛡️	🛡️	🛡️	🛡️
Nedap	@Nedapfr	●			●	●
Nomios	@NomiosFR	●	●	●		●
NTT Com Security	@NTTComSec_FR	●	●	●	●	●
OpenMinded Consulting	@openminded_c	●	●	●	●	●
Optalia	@newlode	●	●	●	●	●
Orange Cyberdefense	@orange cyberdef	●	●	●	●	●
Pradeo	@Pradeo_France		●	●		
PrimX Technologies	@ltsecurfeed	●	●	●		
Schneider Electric	@SchneiderElecFR	●			●	
Siemens	@siemens_france	●				●
Solucom	@risk_insight	●	●	●	●	●
Sophos	@SophosFrance	●	●	●		
Symantec	@SymantecEMEA	●	●	●	●	●
Systemis	@systemisgroup	●	●	●	●	●
TheGreenBow	@TheGreenBow	●	●	●		
ThreatQuotient	@threatquotient	●	●			●
Cryptosense Ⓢ	@cryptosense	●	●			
Trovolone	@Trovolone	●	●	●		●
VadeSecure	@Vade_Retro_Tech	●				●
Varonis Systems	@VaronisFR		●	●	●	●
Verizon	@VZEntreprise	●	●	●	●	●
Wooxo	@wooxo_		●	●	●	●
YesWeHack	@bountyfactory	●	●	●		●
Zscaler	@zscalerFR	●	●	●	●	



Un oubli ? Vous souhaitez figurer dans la prochaine liste « 50 acteurs de la cybersécurité à suivre » ? Faites-nous signe : redaction@alliancy.fr

Transformation numérique et cybersécurité : quand dirigeants et organisations doivent changer

Quels que soient leur secteur d'activité et leur taille, les entreprises ont aujourd'hui compris que leur compétitivité, leur proposition de valeur et leur pérennité passaient par une transformation de fond avec le numérique. Mais cette transformation peut-elle se penser sans sécurité ? Le bon sens rappelle immédiatement que non. Les problématiques de cybersécurité ont connu ces dernières années une médiatisation qui les a fait sortir du seul domaine des experts. Et pour assurer l'efficacité, l'agilité et la résilience de leurs entreprises, les dirigeants eux-mêmes ont aujourd'hui tout intérêt à monter au créneau, aux côtés de leurs responsables de la sécurité des systèmes d'information. Entre les évolutions de culture d'entreprise, l'intégration de nouvelles technologies dans le fonctionnement quotidien de l'organisation et la pression grandissante des réglementations, les occasions se multiplient pour aligner vision de la transformation numérique et stratégie de sécurité. Les témoignages d'entreprises et conseils d'experts réunis dans ce guide présentent certaines des pistes les plus intéressantes du moment pour accélérer ces changements.

Et pour aller plus loin :



Découvrez notre centre de ressources
sécurité numérique sur :
[www.alliancy.fr/ressource/securite-
numerique-les-contenus-a-lire-absolument](http://www.alliancy.fr/ressource/securite-numerique-les-contenus-a-lire-absolument)

WWW.ALLIANCY.FR

