#2



STORMSHIELD

Transformation numérique des entreprises :

Le début d'un nouveau cycle ?

Baromètre de la transformation numérique des entreprises
réalisé en collaboration avec l'Usine Digitale
Édition 2019

À l'occasion de la parution du premier baromètre de la cybersécurité Stormshield/L'Usine Digitale en décembre 2018, nous vous proposions une réflexion sur la sécurité dans le cadre de la transformation numérique des entreprises.

Un an plus tard, où en sommes-nous de cette question ? La transformation numérique est-elle encore un sujet ?
Une décennie que ce terme prétend décrire les mutations à l'œuvre dans nos sociétés et donc dans nos entreprises. Une vie à l'échelle d'Internet, qui a bouleversé notre rapport au temps.

Avant de tirer un trait peut-être hâtif sur l'expression, jetons un dernier regard au phénomène.

La métamorphose annoncée, qui devait amener les entreprises à plus de performance et de collaboration grâce à l'intégration du numérique, a-t-elle eu lieu ?

Comme souvent, ce livre blanc démontrera que « cela dépend » : si de grandes disparités subsistent, les entreprises continuent d'investir dans la numérisation de leurs métiers et de leurs offres.

Mais elles ne sont pas seules à gagner du terrain virtuel, les cyberattaquants, eux aussi, font leur transformation et les conséquences sont bien réelles.

Toujours plus ciblées et plus sophistiquées, les demandes de rançon, fuites de données, attaques par déni de service et autres cyberattaques se multiplient.

Ainsi, la moitié (48%) des directions SI, digitales et numériques que nous avons interrogées lors de cette enquête ont subi une ou plusieurs attaques au cours des douze derniers mois. C'est 13% de plus que l'an passé, ce qui illustre bien la pression croissante qui s'exerce sur la sécurité des écosystèmes informatiques.

Dans ce contexte, comment les **entreprises abordent-elles leurs projets numériques à l'aube de cette année 2020 ?** En particulier, sur la question toujours plus stratégique de la cybersécurité.

Bonne lecture.

Sommaire

04 **Préambule : peut-on encore parler de transformation numérique ?**

07 **Une maturité en question**

13 **Comment articuler transformation numérique et sécurité ?**

22 **Demain se prépare aujourd'hui**

27 **Conclusion**

Peut-on encore parler de transformation numérique ?

Selon les chiffres de l'édition 2019 de notre baromètre, la transformation numérique des entreprises est largement engagée.

Une proportion croissante de personnes interrogées déclare même que cette transformation a peu d'impact sur la sécurité de leurs systèmes d'information et sur leurs données (16% contre 5% en 2018).

Faut-il en déduire que les plus grands bouleversements sont derrière nous ? Doit-on encore parler de transformation numérique des entreprises ?

Points de vue croisés

Un processus en constante évolution pour Frédéric Leblond, Responsable Sécurité des Systèmes d'Information du Port Boulogne Calais

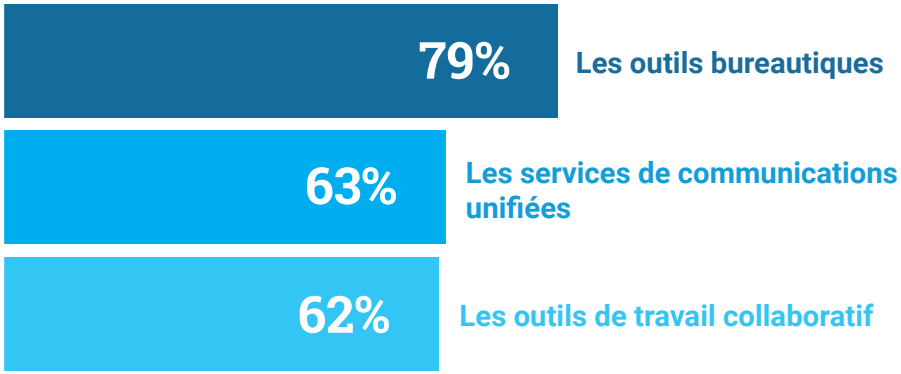
« La transformation numérique est un processus en constante évolution. Cela ne s'arrête pas aux infrastructures ou aux outils collaboratifs, la transformation rapproche les métiers et génère de nouvelles demandes et évolutions. »

Une mutation sans fin pour Nicolas Arpagian, Directeur de la Stratégie et des Affaires publiques de Orange Cyberdefense

« Il n'y a pas d'achèvement avec le numérique. Au-delà d'accélérer la transformation, il la rend donc continue. C'est pourquoi je préfère parler de mutation voire de rupture. Le vrai sujet, ce n'est pas que le numérique transforme les professions, c'est qu'il crée de nouvelles activités et de nouveaux métiers. »

Les principaux chiffres 2019

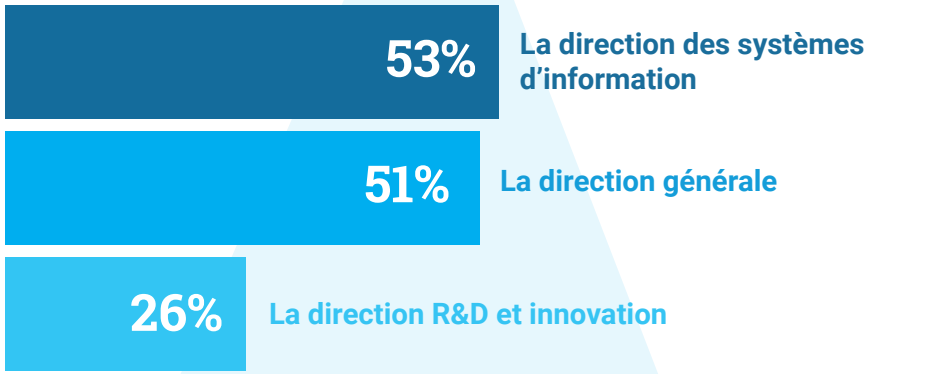
Quels sont les projets de transformation numérique les plus déployés ?



Les grandes entreprises, premières sur la donnée

On remarque que les grandes entreprises sont en avance sur le déploiement de projets de transfert et d'utilisation de la donnée (32% le prévoient contre 23% du total des répondants).

Qui initie les projets numériques au sein des entreprises ?

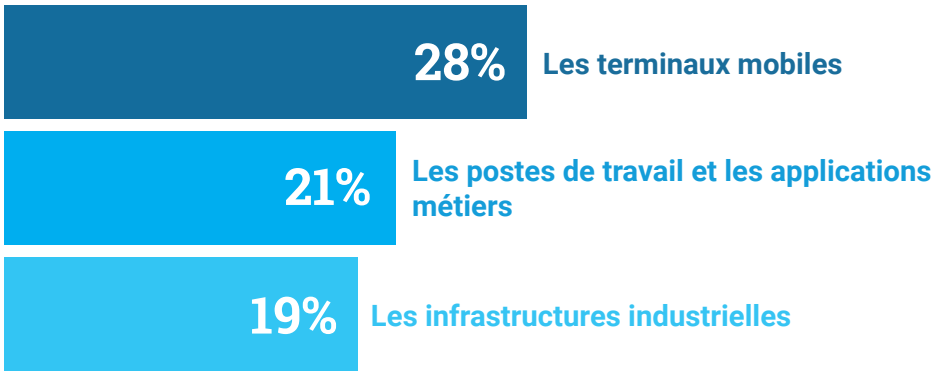


Des directions dédiées plus répandues au sein des grands groupes

37% des répondants issus de grandes entreprises ont cité la direction de la stratégie digitale (contre 25% sur l'échantillon total).

Les principaux chiffres 2019

Quels sont les éléments les plus vulnérables en matière de cybersécurité ?



La sécurité des terminaux mobiles et services de partage de documents, mieux gérée par les grandes entreprises

81% des personnes interrogées travaillant dans de grandes entreprises ont indiqué que les terminaux mobiles y étaient suffisamment sécurisés, contre seulement 51% de l'échantillon total. De même, elles sont 88% à se satisfaire de la sécurisation de leurs services de partage de documents (contre 64% dans les plus petites structures).

Quelles solutions de sécurité sont en place dans les entreprises ?



Plus d'1 entreprise sur 2
est équipée en antivirus, en antispam, en protection réseau et en VPN.



Plus d'1 entreprise sur 3
dispose d'une solution de chiffrement, de sandboxing ou encore d'une sonde de détection.

X5 Les Web Application Firewalls (WAF) et les Cloud Access Security Brokers (CASB) sont cités environ cinq fois plus que l'année dernière.

Partie 1

Une maturité en question

Malgré ces divergences de perception dans leur environnement, deux tiers (64%) des répondants estiment que leur entreprise a progressé en matière de transformation numérique en 2018.

Peut-on pour autant considérer qu'un seuil de maturité est atteint ?

Si la tendance globale paraît indiquer que oui, il faut prendre en compte la disparité des réalités vécues par l'échantillon.

Avancée de la transformation numérique : l'écart de perception se creuse

La moitié (48%) des directions SI, digitales et numériques s'estiment toujours en retard (soit une augmentation de dix points par rapport à l'année précédente !), alors que la proportion des directions métiers qui se déclarent « très en avance » grimpe de huit points pour atteindre 13%.

48%

des directions SI, digitales et numériques s'estiment toujours en retard

Faut-il en déduire que les directions SI, digitales et numériques sont plus critiques ?

Pour Frédéric Leblond, Responsable Sécurité des Systèmes d'Information du Port Boulogne Calais, elles sont surtout plus réalistes : « *face à l'intensification des tentatives d'intrusion et à l'évolution très rapide des menaces, le RSSI est aux premières loges. Il est donc plus facile pour lui de suivre cette transformation et de jauger le niveau de protection de l'entreprise.* »

Une responsable de l'intelligence économique d'un grand groupe de l'énergie le reconnaît : « *en tant que direction métier, nous posons encore souvent un regard d'utilisateur sur ces questions. Il est difficile de se rendre compte de ce que cela représente quand on ne voit qu'une partie du tableau.* »

De son côté, Nicolas Arpagian, Directeur de la Stratégie et des Affaires publiques de Orange Cyberdefense, invite à se questionner sur le point de comparaison adopté entre les directions SI, digitales et numériques et les directions métiers : « *se comparer à des pairs n'est pas forcément suffisant. Une nouvelle concurrence est rendue possible par le numérique, qui crée de nouveaux services et des prestations inédites jusqu'alors. La vraie fragilisation peut venir de cette concurrence 'imprévue'* ».

État des lieux et priorités partagés au sein de l'entreprise

Malgré ces divergences de perception dans leur environnement, deux tiers (64%) des répondants estiment que leur entreprise a progressé en matière de transformation numérique en 2018.

Données et relation client à l'honneur, applications mobiles en perte de vitesse

Directions SI, digitales et numériques s'accordent avec leurs collègues des autres directions sur les trios de tête suivants en matière de projets de transformation numérique :

Projets déjà déployés	Projets en cours de déploiement	Projets en réflexion
• *travail collaboratif* • *outils bureautiques classiques* • *communications unifiées*	• *dématérialisation* • *plateformes métiers* • *digitalisation de la relation client*	• *utilisation de la donnée* • *plateforme métier* • *dématérialisation*

Autre point d'accord entre ces populations : 22% des répondants ne prévoient pas d'investir dans le déploiement d'applications mobiles, soit dix points de plus que l'an passé. Cette tendance est d'autant plus marquée chez les directions SI, digitales et numériques qui sont 33% à bouder ce genre de projets (soit une augmentation de 21 points).

Vers une intégration de la sécurité par défaut dans les projets numériques ?

6,5/10

c'est la note moyenne donnée par les répondants pour évaluer le degré de préparation de leur entreprise aux risques cyber induits par la transformation numérique. Cette donnée est stable par rapport à l'an dernier (6,6/10), mais on retrouve la même différence de perception entre directions SI, digital et numérique et directions métiers : les premiers donnent un 6,1 là où les seconds attribuent un 6,8/10.

L'OPPOSITION *SECURITY BY DESIGN* ET *BUSINESS FIRST* EST-ELLE TOUJOURS D'ACTUALITÉ ?

« *La Direction des Systèmes d'Information (DSI) et le Responsable de la Sécurité des Systèmes d'Information (RSSI) ont été impliqués dès que nous avons commencé à évoquer le développement d'un outil de gestion de l'information en interne. Même maintenant que l'outil est en place, il est régulièrement mis à jour et soumis à des tests* ».

Ce témoignage d'une responsable de l'intelligence économique dans l'industrie de l'énergie démontre que certaines entreprises intègrent bien la notion de risque cyber dès la conception de leurs projets numériques : c'est l'approche *security by design*.

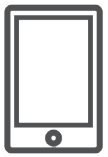
Elle serait très répandue dans les entreprises d'après les résultats de l'étude puisque 85% des répondants indiquent que la dimension sécurité est intégrée en amont du lancement des projets.

« *Culturellement, cette approche résonne beaucoup chez les acteurs des secteurs du transport, de la santé, des communications ou encore des services régaliens qui pensent à la sécurité avant tout,* confirme Rémi Decheron, Ingénieur commercial, Stormshield Data Security. *Alors que d'autres acteurs comme la banque sont plutôt orientés business first : ils ont longtemps privilégié la qualité de service, car l'information dans leur domaine a une durée de vie plus courte et nécessitait donc moins de sécurisation. C'était une façon de ne pas perdre en productivité.* »

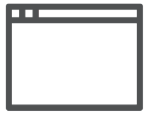
Mais sous l'impulsion de réglementations comme le RGPD et face à la pression de cyberattaques répétées, les deux approches tendent à se réconcilier.

« *Au-delà des différences de culture, de priorité et de rythme, toutes les entreprises cherchent aujourd'hui à sécuriser leur transformation numérique. Pour cela, nous leur proposons des outils qui s'inscrivent dans la démarche security by design et répondent à leurs exigences de sécurité maximale pour les uns, à leurs impératifs business pour les autres.* »

Il ressort également de l'étude que les quatre éléments les plus vulnérables en matière de cybersécurité sont :



les terminaux mobiles (28%)



les applications métier (21%)



les postes de travail (21%)



l'infrastructure industrielle (19%)

Dans ce contexte de maturité partielle et hétérogène, comment continuer à numériser nos modes et outils de travail, avec le meilleur niveau de sécurité possible ?

Partie 2

Assurer la sécurité de sa transformation numérique

37%

c'est le nombre de projets numériques pilotés par la direction générale dans les grandes entreprises

L'étude révèle que les directions générales sont plutôt impliquées dans les projets de cybersécurité, notamment dans leur pilotage (30% sur l'échantillon total).

Pour Nicolas Arpagian, Directeur de la Stratégie et des Affaires publiques de Orange Cyberdefense, c'est indispensable à la réussite des projets :

« *L'intégration de la dimension sécurité dans les projets numériques dépend du management. Il faut que la hiérarchie soit réellement impliquée, car cela représente un investissement de la part de l'entreprise. Les salariés peuvent émettre des propositions mais c'est au manager de donner les moyens de les concrétiser.* »

La sécurité comme responsabilité collective de l'organisation

Sécuriser le numérique n'est pas un exercice solitaire. Les sondés ont en moyenne cité 3,4 acteurs à l'initiative des projets numériques et 2,2 acteurs impliqués dans leur pilotage.

D'ailleurs, pour mieux prendre en compte les défis de la cybersécurité, 61% des répondants envisagent ou ont mis en place des changements organisationnels, comme la création d'une direction de la stratégie digitale par exemple.

Une montée en puissance des directions de la stratégie digitale

Les DSI sont toujours celles qui portent le plus les projets de cybersécurité et, plus l'entreprise est petite, plus elles sont en première ligne (59% dans les PME contre 50% dans les grandes entreprises).

Elles restent également majoritairement à l'initiative des projets numériques (53%), mais ce chiffre est en recul de 16 points par rapport à l'année dernière. Cela s'explique par la création dans de nombreuses entreprises de directions dédiées, souvent dénommées « direction de la stratégie digitale ». Ces nouvelles entités pilotent par exemple 1 projet numérique sur 4 au sein des entreprises de taille intermédiaire (ETI) et sont à l'origine de presque 4 projets sur 10 dans les grandes entreprises.

DSI

Les DSI sont toujours celles qui portent le plus les projets de cybersécurité

La direction juridique, nouvel interlocuteur sur les questions de cybersécurité

Un cadre réglementaire européen renforcé en matière de cybersécurité a été posé, notamment avec l'adoption du Règlement Général sur la Protection des Données (RGPD) et du Cybersecurity Act, respectivement en 2018 et en 2019.

En plus de faire avancer la prise de conscience autour des enjeux de cybersécurité, le RGPD a permis de donner une valeur « tangible » aux données personnelles, en fixant par exemple une amende à 4% du chiffre d'affaires globalisé pour les entreprises prises en faute dans la protection des données qu'elles traitent. Ce nouveau règlement a également obligé les entreprises à caractériser les données qu'elles manipulent et à définir un calendrier pour se mettre en conformité.

Face à ces évolutions juridiques et à des réglementations « qui se chevauchent parfois » d'après Frédéric Leblond, la direction juridique est de plus en plus impliquée lors du déploiement de projets numériques. 60% des répondants disent la solliciter souvent, voire systématiquement, contre 46% l'année dernière. Sur la population des directions SI, digitales et numériques, on observe une progression du même ordre (57% vs 47% en 2018) et un recul de dix points des profils qui ne font jamais appel à ce service.

« La politique du groupe à ce niveau est assez récente, mais nous avons désormais une direction chargée de la transformation numérique et une personne à la direction juridique dédiée à la question de la cybersécurité. Chaque direction métier peut être force de proposition, mais les décisions sont prises de concert, avec le conseil de la DSI et de la protection de l'information, sur les moyens techniques et la conformité. »

Responsable de l'intelligence économique d'un grand groupe de l'énergie

La direction sécurité, une alliée plus qu'un frein aux projets numériques

À mesure que la compréhension des enjeux de cybersécurité progresse, la perception de la fonction sécurité évolue également : elle est tour à tour décrite comme un conseiller, un « gendarme protecteur » ou un soutien par les interrogés.

De la même façon, la prise en compte des problématiques de sécurité ne représente pas un frein au développement des projets numériques pour 82% des sondés travaillant en ETI et 71% dans les grandes entreprises. En revanche, c'est encore la perception de près de 40% des PME interrogées.

Les ressources humaines, un rôle clé dans la cybersécurité

L'implication, facteur clé de succès de la sensibilisation

La sensibilisation aux bonnes pratiques arrive en tête des leviers cités pour faire face aux défis de la cybersécurité. 72% des personnes interrogées déclarent que des initiatives dans ce sens sont en place dans leur entreprise.

À ce sujet, Nicolas Arpagian, Directeur de la Stratégie et des Affaires publiques de Orange Cyberdefense souligne l'importance d'allier enseignement théorique et pratique : « *dans le cadre d'une action de sensibilisation au hameçonnage chez un de nos clients, nous envoyons une campagne de phishing avant et après la formation de façon à mesurer son efficacité.* »

Impliquer les collaborateurs à travers des cas pratiques issus de leur quotidien permet à chacun de se sentir concerné quel que soit son rôle dans l'entreprise et de se rendre compte que l'entreprise est un « *corps social interconnecté* ».

Néanmoins, Frédéric Leblond identifie deux freins à ces actions de formation : le premier concerne le budget, parfois difficile à obtenir, et le second, le choix de la méthode. « *Alors même que la sensibilisation est quelque chose de très important. C'est en parlant et en montrant la sécurité que l'on progressera sur le sujet.* »

Sur ce deuxième point, beaucoup d'initiatives fleurissent, des ateliers aux newsletters en passant par des démonstrations live de white hats, ces hackers éthiques qui mènent par exemple des tests d'intrusion pour assurer la sécurité de systèmes.

La dimension sécurité semble également de plus en plus souvent intégrée lors des formations aux nouveaux outils de transformation numérique (en hausse de neuf points à 48%).

Les spécificités du recrutement en cybersécurité

Au-delà de la sensibilisation de l'ensemble du personnel, 48% des répondants ont ou prévoient de recruter des profils experts en cybersécurité. Cette proportion monte à 67% dans les grandes entreprises.

Pour Sylvie Blondel, Directrice des Ressources Humaines chez Stormshield, la première étape pour attirer des candidats compétents en cybersécurité est de diffuser une offre d'emploi qui affiche clairement les attentes de l'entreprise à ce niveau.
L'enjeu est ensuite d'arriver à vérifier que la personne possède certaines « soft skills » comme l'engagement, la responsabilité ou encore la fiabilité en plus de son bagage technique.

48%

des répondants ont ou prévoient de recruter des profils experts en cybersécurité

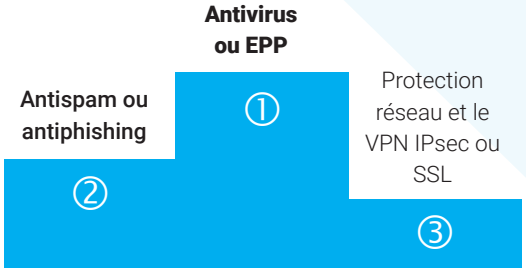
« *C'est un processus collaboratif et complet : il y a un entretien avec les RH mais également des entretiens et des tests techniques très poussés, qui sont pilotés par les managers et qui impliquent une partie de l'équipe d'accueil pour faciliter l'intégration. Ce profil de poste revêt une forte dimension éthique ; c'est pourquoi nous recherchons des gens à la fois passionnés, convaincus du sens de leurs actions et responsables.* »

Le support indispensable de la technologie

Au-delà des évolutions organisationnelles évoquées et des actions menées sur le front de la sensibilisation ou du recrutement, la réponse aux défis de cybersécurité posés par la transformation numérique est aussi technologique.

Des solutions de sécurité désormais « classiques », adoptées par plus de la moitié des entreprises

Au classement des solutions en place les plus populaires, l'antivirus ou EPP se classe en 1re place (60%), talonné par l'antispam ou antiphishing (59%). La protection réseau et le VPN IPsec ou SSL se partagent la troisième place du podium (54%).



Près de

75%

des personnes interrogées citent le déploiement ou les projets de déploiement de nouvelles solutions de sécurité.

L'essor des applications web booste le WAF

Parmi ces solutions, le Web Application Firewall (WAF)[1] affiche une belle progression : 41% des répondants déclarent l'avoir mis en place contre 8% l'an dernier sous l'effet de la multiplication des applications web comme Google Docs, Office 365 ou encore Gmail. Les grandes entreprises en sont particulièrement friandes puisqu'elles l'auraient adopté à 61%.

« *Les solutions de WAF analysent par exemple le contenu des pages web ou contrôlent des protocoles de transfert tels que http ou https. Elles offrent aussi une protection contre les attaques comme l'injection SQL ou le cross-site scripting (XSS) qui ciblent spécifiquement les applications web. Enfin, elles peuvent également contrôler des données pour s'assurer de la conformité à la politique de sécurité* », précise Stéphane Prévost, Product Marketing Manager chez Stormshield.

[1] Par rapport à un pare-feu classique, le WAF contrôle spécifiquement l'accès aux applications web et en assure la protection.

Un parc de solutions très hétérogène en fonction de la typologie d'entreprise

Selon les résultats de l'étude, le chiffrement des e-mails serait ainsi une réalité dans 1 grande entreprise sur 2 contre 1 PME ou ETI sur 3. De la même façon, 52% des répondants issus de grandes entreprises disent utiliser l'authentification à double facteur (2FA) contre moins de 20% en ETI ou en PME. Autre exemple avec les solutions SOAR (Security Orchestration, Automation and Response), en place dans un tiers des grandes entreprises et moins de 10% des ETI et PME.

CASB

Le CASB a la cote auprès des grandes entreprises

Les *Cloud Access Security Brockers* (CASB) sont des solutions qui contrôlent les accès au cloud. En 2019, près de 20% des répondants déclarent l'avoir déployé au sein de leur entreprise contre 4% en 2018. Cette croissance est essentiellement portée par les grands groupes qui l'ont adopté à 41% contre 18% des ETI et 7% des PME).

Pourquoi les grandes entreprises le plébiscitent-elles?

« *Cette solution s'inscrit dans la tendance actuelle des entreprises et du monde informatique à recourir à des services cloud au sein des entreprises et du monde informatique pour ne pas avoir à maintenir des services en interne* », explique Stéphane Prévost, Product Marketing Manager chez Stormshield.

« *En premier lieu, le CASB permet de gérer les accès à une application par population. Il sécurise également les données en utilisant des tokens. Et protège l'espace cloud des menaces, puisqu'il contrôle ce qui y est déposé et par qui. Enfin, le CASB peut répondre en partie à la problématique posée par la shadow IT car il donne de la visibilité sur qui utilise quoi.* »

La dimension budgétaire de la cybersécurité

Nous l'avons vu, sécuriser la transformation numérique exige des moyens humains et matériels. Et donc des investissements.

« *Lors de la mise en place de nos outils de travail collaboratif, nous avons fait le choix d'une sécurisation en deux temps, avec à chaque fois un budget compris entre 1 et 10% du montant global du projet* », déclare Frédéric Leblond, Responsable Sécurité des Systèmes d'Information du Port Boulogne Calais.

Cette part de 1 à 10% du budget d'un projet numérique allouée à la sécurité semble traduire une certaine vérité, partagée par près de la moitié des répondants. Seuls 20% d'entre eux dépenseraient davantage. Interrogées sur la question, les directions SI, digitales et numériques sont près d'un quart à déclarer dépenser plus de 10% pour la sécurité des projets numériques. Soit une augmentation de six points en un an.

Il est à souligner tout de même que plus de 40% de l'échantillon se dit incapable de répondre à cette question, faute d'information. Ce qui indique clairement que le sujet reste sensible, voire confidentiel, même en interne.

Les budgets moyens ne seraient donc a priori pas très élevés. Mais moins d'un tiers (27%) des répondants se disent préoccupés par le manque de moyens financiers pour prévenir le risque à l'avenir. Le secteur public constitue une exception sur ce point puisque cette proportion grimpe à 45%.

Paradoxalement, sur le total de l'échantillon, 10% seulement citent les ressources financières comme axe d'amélioration pour la cybersécurité de leur entreprise.

Partie 3

Demain se prépare aujourd'hui

Le manque de moyens financiers n'est donc pas la préoccupation majeure des répondants à l'étude. La difficulté à définir le rôle de chacun dans le processus de sécurisation non plus, puisqu'elle n'est invoquée que par 27% de l'échantillon, en recul de 15 points par rapport à l'année dernière.

Mais alors, quels sont les défis de cybersécurité qui occuperont les entreprises dans les années à venir ?

Enjeux géopolitiques qui interfèrent dans les choix technologiques, automatisation, augmentation de la surface d'attaque avec l'ouverture d'environnements auparavant fermés sur Internet, partage d'informations sur le cloud, intensification de la réglementation, les sujets de préoccupations ne manquent pas à l'aube de l'année 2020.

Mobilité et cloud sont dans tous les esprits

Au premier rang des défis à venir en matière de cybersécurité, l'accroissement de la mobilité des salariés est cité par près de la moitié (45%) des répondants, devant la méconnaissance des utilisateurs. L'utilisation du cloud partage quant à elle la troisième place du tableau avec l'évolution rapide des systèmes d'information.

~1 sur 2

des répondants place l'accroissement de la mobilité des salariés au premier rang des défis

Pour la responsable de l'intelligence économique dans le secteur de l'énergie « *le cloud pose de vraies questions du point de vue de la sécurité de l'information. La problématique est d'arriver à partager la donnée aux personnes en droit de la connaître tout en se protégeant de la maladresse comme de la malveillance.* »

Qu'il s'agisse de projets d'industrie du futur ou de transformation numérique plus généralistes, la demande de partage de l'information dans le cloud augmente. Et le besoin de protection des données sensibles et/ou à caractère personnel avec elle.

Les grands groupes s'interrogent sur les mégadonnées (Big data) et l'Internet des objets (IoT)

Les grandes entreprises s'intéressent davantage aux challenges posés par le développement du Big data (52%) et de l'IoT (49%) que les ETI (respectivement 22% et 16%) et les PME (35% et 26%). En revanche, elles partagent avec les ETI une préoccupation plus élevée que les PME concernant le développement de l'intelligence artificielle (44% contre 40%).

Pour Stéphane Prévost, les objets connectés étant « *développés par des entreprises non spécialistes de la cybersécurité, celle-ci n'est pas intégrée dans les produits. Le piratage de ces objets pour mener des attaques par déni de service (DDoS) par exemple est un vrai sujet de préoccupation. C'est pourquoi le Cybersecurity Act, adopté en juin 2019, prévoit un certificat européen afin que les entreprises puissent s'approvisionner chez des fabricants certifiés.* »

Le renforcement de la réglementation préoccupe plutôt les PME

Les petites et moyennes entreprises sont en effet 41% à classer le cadre réglementaire dans les « défis cyber » à venir contre 28% des ETI et 34% des grandes entreprises.

Pour Nicolas Arpagian, « *2020 sera l'année de la concrétisation d'un certain nombre d'engagements liés à la législation. Pour beaucoup d'entreprises, cela signifie poursuivre la mise en conformité avec le RGPD. Pour d'autres organismes, désignés opérateurs de service essentiels (OSE) suite à la définition de ce statut par la directive européenne NIS, il s'agit aussi d'appliquer les règles de sécurité qui leur incombent. Mais toutes doivent garder à l'esprit qu'elles sont des structures vivantes et veiller à maintenir cette conformité au gré des évolutions de l'organisation.* »

41%

des répondants classent le cadre réglementaire dans les « défis cyber » à venir

L'automatisation comme réponse au manque de compétences en matière de cybersécurité ?

La méconnaissance des utilisateurs sur les questions de cybersécurité se classe en 2e position des préoccupations des entreprises (42%). Nous avons déjà évoqué le recrutement et la montée en compétence des équipes pour y remédier. Toutefois, la tentation est grande d'automatiser la sécurité pour la confier à des technologies de protection et de détection. Il peut s'agir d'éviter certaines erreurs humaines ou de dégager du temps aux personnels informatiques pour des tâches à plus forte valeur ajoutée.

Cyber sécurité 2e

position des préoccupations des entreprises

Quoi qu'il en soit, l'automatisation, rendue possible par le développement d'API et de connecteurs ouverts, est une des pistes pour plus de sécurité et une administration facilitée des systèmes.

Vers une meilleure prise en compte de l'expérience utilisateur ?

24%

ont cité l'amélioration de l'expérience utilisateur des solutions de sécurité

Parmi les défis à venir, 24% des répondants ont cité l'amélioration de l'expérience utilisateur des solutions de sécurité. Bien souvent en effet, quand un collaborateur choisit de passer par un autre outil que celui recommandé par la DSI de son entreprise, c'est que ce dernier ne remplit pas un ou plusieurs critères « d'usabilité[2] » : utile, utilisable, navigable, accessible et/ou compréhensible.

« *Comment faire adhérer l'utilisateur à la cybersécurité et à ses outils ? C'est un enjeu de taille pour les entreprises comme pour les éditeurs de solutions de cybersécurité, puisque l'expérience utilisateur peut être un critère déterminant dans le choix d'une solution* », selon Rémi Decheron, Ingénieur commercial, Stormshield Data Security.

Puisque la cybersécurité est l'affaire de tous, il faut tendre à développer « l'usabilité » des outils de cybersécurité afin de favoriser leur adoption par tous.

[2] L'usabilité c'est « le degré selon lequel un produit peut être utilisé, par des utilisateurs identifiés, pour atteindre des buts définis avec efficacité, efficience et satisfaction, dans un contexte d'utilisation spécifié ».

Pourquoi les EDR et Next-Gen EPP séduisent particulièrement les grandes entreprises ?

Les directions SI, digitales et numériques de grandes entreprises semblent conquises par les solutions de détection et de réponse des terminaux (EDR pour Endpoint Detection and Response) qui promettent de leur apporter de la visibilité sur une éventuelle attaque en cours.

« *Dans les cas d'attaques sophistiquées, les hackers cherchent à rester le plus longtemps possible 'sous le radar' pour explorer tranquillement l'infrastructure dans laquelle ils ont pénétré. Pour ce faire, ils vont lancer d'autres commandes qui sont autant d'indices qu'une attaque est en cours* », d'après Stéphane Prévost, Product Marketing Manager chez Stormshield.

Ce sont ces signaux faibles que les outils d'EDR détectent. Ils sont aussi capables de donner des indications de remédiation.

Quant aux plateformes de protection de postes nouvelle génération ou Next-Gen EPP, elles combinent les capacités de détection de l'EDR et la capacité de blocage d'un EPP classique (antivirus, anti-malware, etc.). Elles sont plutôt destinées aux entreprises pouvant investir dans des équipes cyber, seules capables d'analyser les signaux remontés par l'EDR.

Quelles seront les solutions de sécurité phare de 2020 ?

24% des directions SI, digitales et numériques prévoiraient de déployer un outil de gestion des accès privilégiés (PAM pour *Privilege Access Management*) dans l'année à venir et 18% mentionnent l'implémentation d'une solution de sandboxing.

Là encore, les projets sont très variables d'une typologie d'entreprise à l'autre : alors qu'une ETI sur cinq réfléchit à déployer un outil de gestion des identités et des accès (IAM pour *Identity and Acces Management*), les PME investissent davantage dans le chiffrement des e-mails (27%) et les grands groupes plébiscitent les EDR et Next-Gen EPP (38%).

Conclusion

Une nouvelle ère pour la cybersécurité des entreprises

La maturité correspond à « l'étape ultime d'un processus de croissance ». Une entreprise mature sur les questions de transformation numérique et de cybersécurité aurait donc digitalisé toute son offre, ses processus et mis en place tous les outils nécessaires pour les sécuriser ?

Ce serait sans compter sur la nouvelle donne inhérente à ce nouvel environnement : avec le code, rien n'est figé dans le marbre.

La nouvelle constante, c'est le changement. La transformation n'est plus un chemin linéaire, mais une façon de fonctionner. Quant aux menaces de demain, elles n'ont pas encore été inventées ; comment alors envisager de s'en protéger dès maintenant ?

Il existe bien un palier, franchi par beaucoup d'entreprises aujourd'hui : passer de la prise de conscience à l'action pour sécuriser la transformation numérique. Mais parler de maturité n'est sans doute pas le terme qui correspond le mieux à la phase dans laquelle nous entrons.

Nicolas Arpagian, Directeur de la Stratégie et des Affaires publiques de Orange Cyberdefense, préfère parler de « séquence de la responsabilité ». « *Par le passé, ceux qui avaient conscience du risque prenaient des mesures de sécurité pour se protéger. Puis ce risque s'est diffusé au sein des organisations au rythme de l'intensification de la numérisation des activités. Aujourd'hui, nous entamons un 3e stade d'évolution dans lequel nous nous protégeons aussi afin de ne pas être tenus pour responsables au regard des nouvelles législations et des obligations contractuelles qui se renforcent. De la même manière, les acteurs de la communauté financière (assurances, investisseurs, agences de notation…) commencent à demander des comptes sur l'état de la cybersécurité.* »

Que l'heure soit venue de la maturité ou de la responsabilité, trois attitudes fondamentales s'imposent aux entreprises qui ne souhaitent pas prendre le train en marche :

Intégrer le réflexe sécurité

Face à des menaces toujours plus présentes, les entreprises doivent continuer à investir dans des solutions de cyberprotection et de détection des menaces. L'approche security-by-design et l'automatisation ne doivent pas faire oublier la dimension humaine de la cybersécurité.

Accepter le risque

La détermination des cyberattaquants, motivés par des enjeux colossaux, rend l'attaque inéluctable : tôt ou tard, toutes les entreprises peuvent en être victime, quels que soient les moyens investis. Néanmoins, il est possible de travailler en amont à la cyberrésilience de l'organisation pour lui permettre d'en limiter l'impact.

Se penser comme un écosystème

Oui, toutes les entreprises sont concernées. Les hackers ciblent aujourd'hui n'importe quel maillon de la chaîne logistique pour atteindre leur cible. Il est donc impératif d'avoir une vision globale de notre écosystème numérique, incluant les prestataires, les fournisseurs, les clients et tous les interlocuteurs de l'entreprise. **La cybersécurité est devenue une responsabilité collective pour les organisations privées comme publiques.**

Sources et références

Baromètre de la cybersécurité 2019 Stormshield / L'Usine Digitale

Méthodologie :

Questionnaire auto administré en ligne, rempli entre le 1er juillet et le 26 août 2019 par 233 décideurs issus des décideurs issus de directions SI / digitales / numériques et de directions métiers, de tous secteurs d'activité et de toutes tailles d'entreprise.



STORMSHIELD

Leader européen de la cybersécurité et filiale à 100% d'Airbus CyberSecurity, Stormshield propose des solutions de confiance, certifiées et qualifiées au plus haut niveau. Cet éditeur couvre le plus grand périmètre de protection parmi les détenteurs de visas de sécurité de l'ANSSI (agence nationale de la sécurité des systèmes d'information).

www.stormshield.com