STORMSHIELD



Transformation numérique des entreprises :

Et la sécurité dans tout ça ?

Baromètre réalisé en collaboration avec l'Usine Digitale

Décembre 2018

TRANSFORMATION NUMÉRIQUE

La transformation numérique des entreprises est forte de promesses en matière d'agilité, d'innovation, de productivité et de performance. Bouleversant tous les métiers et secteurs d'activité, elle métamorphose les modes d'organisation pour offrir à la fois plus de flexibilité, d'autonomie et de coopération.

La transformation numérique des entreprises devient alors incontournable et représente l'une des priorités majeures pour garantir compétitivité et croissance.

La mobilité, le cloud, l'Internet des Objets, l'intelligence artificielle, le big data ou encore les applications SaaS sont autant de sujets qui rendent les entreprises plus connectées, souples et évolutives. Mais toutes ces technologies qui ont également pour conséquence un éclatement des systèmes d'information et une myriade de nouvelles opportunités d'intrusion.

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 européen. Il est l'éditeur qui couvre le plus grand périmètre de protection parmi les détenteurs des Visas de Sécurité de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Comment les Directions Informatiques, les Directions Générales et les Directions Métiers appréhendent-elles cette transformation et les risques qu'elle engendre ? Comment peut-on protéger les actifs et données sensibles dans un environnement de plus en plus distribué et externalisé, face à des menaces de plus en plus sophistiquées ?

Telles sont les questions qui ont été posées à plus de 200 professionnels dans le cadre du baromètre « Transformation numérique des entreprises : et la sécurité dans tout ça ? » réalisé par Stormshield et l'Usine Digitale.

Parmi les **projets prioritaires de transformation numérique** relevés par le baromètre, ce livre-blanc met en avant trois domaines pour lesquels les entreprises interrogées ont montré une attention particulière en matière de vulnérabilité.

1

Tout d'abord, le **nomadisme des salariés** qui implique d'accéder aux données et ressources de l'entreprise en tout lieu (à domicile, en coworking ou sur le terrain) et qui représente par conséquent l'un des risques majeurs de vol d'informations, par négligence ou manque de protection.

2

Ensuite, les **services de partage de documents en mode cloud**, comme OneDrive ou Dropbox, qui permettent de stocker et d'échanger facilement des fichiers en dehors des zones maîtrisées par l'entreprise.

3

Enfin, le **déploiement de nouvelles technologies en interne**, notamment les objets connectés, qui présentent de nouvelles vulnérabilités et qui sont particulièrement difficiles à gérer en terme de cloisonnement et de contrôle des flux.

Les résultats du baromètre montrent que les entreprises sont lucides et identifient clairement l'impact majeur de la transformation numérique sur leur sécurité. Néanmoins, elles ont tendance à surévaluer les protections mises en place, principalement basées sur des technologies traditionnelles, qui ne sont plus suffisantes pour protéger l'ensemble des périmètres, des infrastructures et des données dans un environnement toujours plus ouvert et exposé.

Les entreprises face à la transformation numérique :

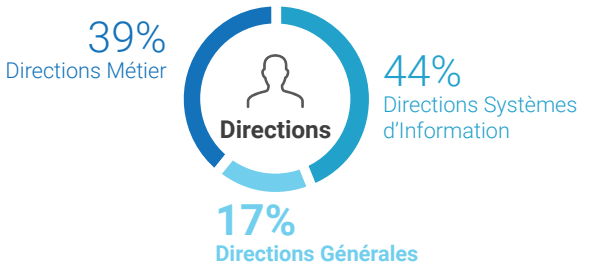
Quelques chiffres clés

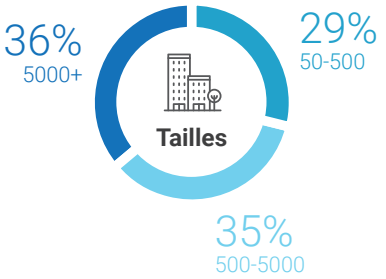
L'étude menée par Stormshield et l'Usine Digitale auprès de 200 répondants a permis de récolter à la fois la vision des Directions des Systèmes d'Information (44%), des Directions Métier (39%) et des Directions Générales (17%) quant à la transformation numérique de leur entreprise et à l'impact sur leur sécurité.

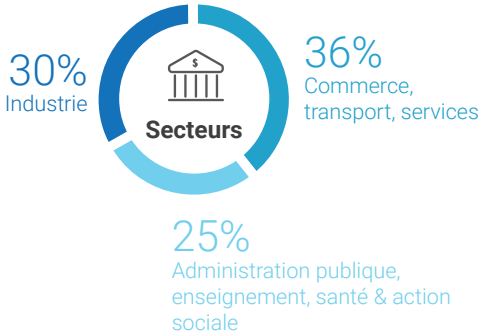
200

DSI, DG ET DIRECTIONS MÉTIERS
D'ENTREPRISES DE PLUS DE 50 SALARIÉS
EN FRANCE









L'enquête met en avant que **la transformation numérique des métiers est bel est bien engagée**, avec des perceptions cependant différentes selon la taille des entreprises et leur secteur d'activité.

Les entreprises de plus de 5 000 salariés se jugeant davantage « plutôt en avance » (39%) et celles du secteur public s'estimant « plutôt en retard » (51%). Cet écart de perception est également visible entre des Directions Métier plus optimistes (67% se considérant en avance ou à niveau) que les Directions des Systèmes d'Information (59%).



Sur l'ensemble des répondants, 27% des entreprises se jugent en avance et 31% se jugent à niveau en matière de transformation numérique.

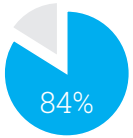
L'utilisation d'outils de **communication unifiée et de travail collaboratif est déjà une pratique courante** dans la plupart des entreprises.

Les nouvelles étapes de digitalisation concernent à présent l'utilisation de services SaaS (87%) et de nouveaux services numériques (83%), ou encore la numérisation de la relation client (81%) et la dématérialisation des process et nouvelles plateformes métiers (80%). En revanche, les entreprises sont plus frileuses sur les projets d'exploitation de la donnée, puisque 30% des DSI n'envisagent pas du tout de tels projets pour le moment.



Des outils de communication unifiée et de travail collaboratif déjà déployés dans près de 7 entreprises sur 10.

Toutefois, l'impact de ces nouveaux usages pour **la sécurité des systèmes d'information et des données reste difficile à mesurer** et les perceptions varient : 44% imaginent un impact positif, 37% ne parviennent pas à se prononcer, 14% redoutent un impact négatif et 5% n'envisagent aucun impact.



84% des répondants affirment que la transformation numérique a ou aura un impact fort sur la sécurité des systèmes d'information et des données.

Néanmoins, les répondants sont **confiants quant au niveau de préparation de leur entreprise** alors que les protections mises en place pour accompagner les projets de transformation numérique restent somme toute traditionnelles (antivirus à 78%, VPN IPsec ou SSL à 76%, appliances physiques et antispam à 70%) et que les budgets alloués à la sécurité dans ces projets restent méconnus pour 48% des personnes interrogées.

6,6/10

C'est la note moyenne que les entreprises accordent à **leur niveau de préparation face aux cyber-risques** que pose la transformation numérique.



Transformation numérique

Quand le gain d'efficacité pénalise la sécurité

Les professionnels interrogés confirment que les technologies numériques sont indispensables à la modernisation de leurs entreprises, mais ouvrent la porte à de nouvelles failles de sécurité.

« Nos employés ont désormais à disposition des téléphones mobiles, un extranet, une plateforme de réunion à distance… Et **notre préoccupation essentielle est devenue la sécurité des échanges d'informations** avec l'extérieur. Nous sommes alertés d'un risque d'attaque environ une fois par trimestre. »

— Professionnel d'une enseigne commerciale

SE TRANSFORMER POUR AMÉLIORER SON EFFICACITÉ OPÉRATIONNELLE...

Derrière cette appellation de transformation numérique, il y a la promesse de gagner en performance opérationnelle, d'économiser du temps, d'être plus réactif et donc plus efficace. **Et la révolution numérique aujourd'hui en marche transforme fondamentalement les process et les modèles économiques des entreprises.**

Avec les applications cloud, la DSI n'a plus à budgétiser l'achat de serveurs, ni à mobiliser et former du personnel pour leur maintenance. Les fournisseurs de plateformes ou d'applications cloud prennent en charge tous les aspects techniques et équiper de nouveaux salariés ou lancer des projets ne prend plus que quelques heures, au lieu de semaines, voire de mois auparavant. *« Le fait que les outils collaboratifs hébergés dans le cloud soient globalisés nous permet par ailleurs de travailler efficacement avec des partenaires situés dans d'autres pays »*, se félicite ce directeur dans le domaine du tertiaire.

Autre exemple d'efficacité avec les équipements mobiles et les accès distants sécurisés qui permettent de travailler n'importe où et d'intervenir à distance en disposant de toutes les informations ou applications nécessaires, en temps réel. Ou encore, les capteurs connectés qui permettent de détecter les anomalies d'un produit, d'une chaîne de production ou dans des locaux afin d'intervenir au plus vite avant que l'activité ne soit bloquée par un incident.

... MAIS DEVOIR MIEUX MAÎTRISER LA SÉCURITÉ

Toutes ces nouvelles opportunités offertes par la numérisation **s'accompagnent d'un ensemble de nouveaux défis de sécurité** qui nécessitent un meilleur encadrement. La transformation numérique ne peut aller de pair sans une sécurité accrue et une confiance sur le long terme. Parce que les équipements et les données sortent du périmètre interne de l'entreprise et parce que les nouveaux dispositifs connectés échappent aux procédés de protection traditionnels, les organisations se doivent de changer profondément leur approche de la sécurité numérique.

« Nous nous retrouvons avec des automates interrogeables par le système d'information de l'entreprise. Du point de vue de la DSI, ce ne sont pas des choses acceptables. De plus, notre problématique est de sécuriser cela avec des interlocuteurs qui ne sont pas formés aux problématiques de l'industrie », se désole ainsi ce prestataire pour l'industrie.

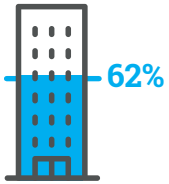
Ce livre blanc présente des cas concrets liés au changement de posture que doivent adopter les entreprises concernées par la transformation numérique.



Salariés nomades

Les terminaux ne sont plus abrités par l'enceinte de l'entreprise

L'accroissement du travail des salariés en dehors des murs de l'entreprise est pour 62% des répondants la principale problématique à surmonter en matière de sécurité.



Avec des équipements mobiles et des données de l'entreprise circulant au-delà du traditionnel pare-feu, les solutions de chiffrement s'imposent pour éviter les vols ou pertes de données.

SÉCURISER LES ACCÈS DISTANTS

Depuis septembre 2017, en France, le télétravail est devenu un droit inscrit dans le Code de travail[1]. Cette nouvelle condition réglementaire nécessite la mise en place d'un système d'accès distant au système d'information pour les entreprises qui n'en disposaient pas encore. En effet, l'ouverture du système d'information depuis l'extérieur peut vite devenir un trou béant en termes de sécurité si des mécanismes de protection adaptés ne sont pas déployés. **Authentification des employés en situation de mobilité, application de règles d'accès sur les ressources mises à disposition et protection des communications** pour assurer leur confidentialité sont les briques de base d'un accès distant sécurisé.

Pour répondre à cet enjeu, 76% des entreprises interrogées ont mis en place un système d'accès distant via VPN (Virtual Private Network) dans le cadre de leur transformation numérique.

Stormshield adresse cette problématique en attribuant à l'utilisateur un accès VPN qui lui permet de travailler depuis l'extérieur comme s'il était physiquement dans l'entreprise et qui chiffre sa connexion pour éviter qu'elle soit mise sur écoute. Cette fonctionnalité supporte l'authentification des collaborateurs, la définition de politiques d'accès (utilisateurs, plages horaires, ressources mises à disposition) ainsi que le chiffrement des communications.

Les appliances physiques et virtuelles Stormshield Network Security (SNS) offrent deux types de VPN :

- VPN SSL qui présente l'avantage d'être souple à utiliser et simple à déployer,
- VPN IPsec qui apporte un niveau de confiance plus élevé puisque le code associé est audité dans le cadre de la qualification ANSSI.

PROTÉGER LES DONNÉES DES TERMINAUX

42% des DSI estiment qu'il faudrait mieux sécuriser les terminaux – PC, tablettes ou smartphones – dont les utilisateurs se servent lorsqu'ils sont en situation de mobilité ou en télétravail.

« ***Le problème posé par le nomadisme des salariés est lié au fait qu'en dehors du périmètre de ses sites géographiques, l'entreprise n'encadre plus les procédures de contrôle. L'équipement est exposé au vol, à la perte, à l'espionnage et les données sensibles qu'il héberge peuvent se retrouver dans les mains d'un inconnu ou d'une personne malveillante*** », explique Matthieu Bonenfant, Directeur Marketing chez Stormshield.

En complément de la mise en place de réseaux privés virtuels, le contenu du disque dur de l'appareil client doit être chiffré, de sorte qu'un malfaiteur qui se retrouverait en sa possession ne puisse pas l'examiner. Ce mécanisme de protection est nécessaire mais pas suffisant. « ***Les constructeurs de terminaux et PC professionnels proposent souvent cette option. Néanmoins, ce chiffrement ne résiste pas à un espion qui dispose des logiciels adéquats pour le pirater*** », indique Jocelyn Krystlik, Data Security Business Unit Manager chez Stormshield.

En sus du chiffrement matériel par défaut, l'éditeur recommande d'utiliser le logiciel Stormshield Data Security (SDS). Celui-ci place les fichiers sensibles dans un container avec un chiffrement supplémentaire. Outre une version pour PC, SDS existe aussi pour les smartphones et tablettes. Il prend la forme d'un navigateur alternatif au système qui permet, une fois que l'utilisateur s'est authentifié, de manipuler les fichiers contenus sur le terminal comme ceux hébergés sur un service de stockage cloud.

« Les fichiers sécurisés par SDS ne sont pas accessibles par les outils traditionnels, mais SDS peut en revanche accéder à tous les périphériques. Il devient ainsi possible de chiffrer directement une photo prise, une fonction très appréciée dans l'industrie où les prises de vues servent à évaluer des pièces critiques », conclut Jocelyn Krystlik.

(1) L'Ordonnance n° 2017-1387 du 22 septembre 2017 relative à la prévisibilité et la sécurisation des relations de travail (JO du 23 septembre 2017) impose que tout refus de télétravail à un salarié doit être motivé par l'entreprise..



Partage de documents

Le défi de protéger les données confidentielles sur une place publique

Même si les services de partage de documents en ligne améliorent les échanges et facilitent l'agilité des collaborateurs, la confidentialité des informations ne doit pas pour autant échapper au contrôle de l'entreprise.

Aujourd'hui, ces outils de partage cristallisent les craintes des DSI qui considèrent à 48% que de telles applications SaaS présentent un risque élevé.



UN PARTAGE EN LIGNE TROP FACILE D'ACCÈS

Parmi les nouvelles fonctions collaboratives, les services de partage de documents en ligne tels que OneDrive, Google Drive ou encore Dropbox sont tout particulièrement montrés du doigt, puisque les entreprises estiment qu'ils font partie des éléments de transformation dont le niveau de protection devrait être amélioré en priorité.

« *Il y a une urgence à sécuriser le partage et le stockage en ligne car les Directions Métiers des entreprises, et notamment celles des industriels, veulent en bénéficier tout de suite. Il faut en effet savoir qu'elles obtiennent pour ce type de services des tarifs groupe très attractifs comparativement au coût actuel de leurs serveurs de fichiers. En revanche, elles ne peuvent pas accepter que leurs données se retrouvent en clair sur une plateforme exploitée par un tiers et accessible par n'importe qui* », relève Jocelyn Krystlik, Data Security Business Unit Manager chez Stormshield.

DONNER LE CONTRÔLE À L'UTILISATEUR TOUT EN MAÎTRISANT LA SÉCURITÉ

Les fournisseurs de services de partage en mode cloud proposent généralement de chiffrer les données pour que seuls les utilisateurs disposant des bons droits d'accès puissent les lire. Mais Jocelyn Krystlik souligne un problème : « *Ces droits d'accès ne sont administrables que par les responsables de la sécurité, ce qui génère une surcharge de travail et une latence non négligeable dans le traitement des demandes* ». Or, pour que la collaboration reste agile, il faut que ce soit l'utilisateur lui-même, en tant que propriétaire de la donnée, qui puisse attribuer des accès aux collaborateurs de son choix.

« *À l'inverse, il n'est pas non plus question de laisser les salariés partager leurs documents sur des plateformes dont l'entreprise n'a pas la main mise, sans mettre en place des garde-fous. Il faut donc que l'utilisateur accède aux fonctions d'autorisation depuis sa machine, mais que tous les relevés d'activité remontent sur le tableau de bord de surveillance des équipes de sécurité* », explique-t-il.

Pour résoudre cette situation, l'éditeur propose l'outil SDS (Stormshield Data Security), intégré aux principaux clients de messagerie et services de partage cloud. SDS présente toutes les fonctions de gestion des accès à la donnée (niveau de criticité des données, sélection des collaborateurs autorisés...) depuis l'interface de l'utilisateur. SDS est basé sur un mécanisme de chiffrement de fichiers de bout en bout, depuis le terminal de l'expéditeur jusqu'à celui du destinataire. De leur côté, les administrateurs définissent les identités et les règles d'usage sans pouvoir accéder aux données.



Évolutions technologiques et Internet des Objets

Se protéger face à l'inconnu

La transformation numérique des entreprises implique des évolutions technologiques continues et le déploiement d'objets connectés. La course effrénée à l'innovation pousse trop souvent les éditeurs et constructeurs à privilégier la miniaturisation, les performances et la réduction des cycles de développement au détriment de la sécurisation de leurs produits. Ces composants techniques sont donc parfois mal maîtrisés et intègrent nativement peu de mécanismes de sécurité (mises à jour automatiques, authentification, chiffrement des communications…).

Si l'étude montre un bon niveau de confiance des entreprises concernant la protection des infrastructures (87% considèrent que leurs réseaux sont bien protégés), elle révèle aussi que l'adaptation de la sécurité aux évolutions technologiques permanentes touchant leur système d'information est un sujet d'inquiétude. Alors, comment sécuriser ces nouveaux équipements, depuis peu intégrés au réseau IT ?



LES OBJETS CONNECTÉS COMME AUTANT DE POINTS D'ENTRÉE

Caméras de surveillance, sondes et capteurs, outillages connectés, véhicules et systèmes autonomes rendent aujourd'hui les bâtiments, les villes et les usines intelligentes. **Ces objets connectés constituent un des piliers de la transformation numérique** car ils créent le lien entre le monde physique et le monde numérique. Leur développement exponentiel est un véritable challenge pour la sécurité numérique.

« Ce sont des environnements IoT que l'on ne connaît pas, que l'on ne sait généralement pas aussi bien sécuriser que des serveurs ou des PC, mais qui constituent pourtant des cibles d'attaques pour les pirates », indique Matthieu Bonenfant, Directeur Marketing chez Stormshield.

Citons pour exemple le tristement célèbre Botnet Mirai, qui avait réussi à prendre le contrôle de 500 000 objets connectés, essentiellement des caméras de videosurveillance, en utilisant leurs identifiants et mots de passe par défaut. En 2016, les équipements infectés par Mirai avaient été coordonnés pour déclencher deux cyberattaques géantes contre le fournisseur de services cloud OVH et le service DynDNS, dont dépendent de nombreux sites web comme GitHub, Twitter, Netflix ou Airbnb. Techniquement, les pirates à la manœuvre pouvaient tout aussi bien dérober les données de ces équipements, images de vidéosurveillance comprises.



AGIR AU NIVEAU DU FIREWALL

Pour éviter que les objets connectés ne se retournent contre leur propriétaire ou ne soient détournés de leur usage, Matthieu Bonenfant préconise de **mettre en place le principe de « Zero Trust »** en isolant par filtrage ces composants du reste du système d'information. La segmentation du réseau en zones de confiance permet de contrôler toutes les connexions entre zones ou avec Internet. ***« Dans le cadre des objets connectés, il est possible de savoir quels types de connexions sont réalisés de manière légitime. La bonne pratique est donc ici de fonctionner par listes blanches et de n'autoriser que certaines actions comme la connexion d'un objet vers sa plateforme cloud de management. Ainsi, le détournement d'un tel objet connecté pourra être plus facilement maîtrisé »***, détaille-t-il.

Stormshield propose de résoudre cette problématique avec sa gamme de firewalls Stormshield Network Security (SNS). L'avantage de cette solution est qu'une seule appliance est capable de créer jusqu'à 50 zones physiques différentes et de filtrer tous les échanges entre ces zones. Par ailleurs, les boîtiers haut-de-gamme SNS sont évolutifs, puisque leur châssis permet d'acquérir des modules de connectique additionnels au fur et à mesure que des zones sont ajoutées sur le réseau. « C'est un des principes induit par la transformation numérique : pour gagner en agilité, il est important de pouvoir adapter dynamiquement son investissement en fonction des besoins immédiats », conclut Matthieu Bonenfant.

STORMSHIELD

Leader européen de la cybersécurité et filiale à 100% d'Airbus CyberSecurity, Stormshield propose des solutions communicantes et intelligentes pour anticiper les attaques et protéger les infrastructures numériques.

Sa mission : assurer la cybersécurité et la protection des données des organisations, de leurs collaborateurs et de leurs clients.

Son expertise se décline en trois gammes de produits complémentaires pour une sécurité sans failles :

- Protection des réseaux informatiques et industriels (Stormshield Network Security).
- Protection des postes et serveurs (Stormshield Endpoint Security).
- Protection des données (Stormshield Data Security).

L'interaction de ces trois gammes de produits renforce le niveau de protection des environnements IT, OT et cloud quel que soit le point d'attaque.

Ces solutions de pointe et de confiance sont certifiées au plus haut niveau européen (EU Restricted, NATO Restricted, ANSSI EAL3+/EAL4+).

Présents dans plus de 40 pays via un réseau de partenaires distributeurs, Stormshield assure la protection des informations stratégiques d'entreprises de toutes tailles, d'administrations publiques et d'organismes de défense partout dans le monde.

www.stormshield.com



Version 1.0 - Copyright Stormshield 2018