الإتحـــاد العـــام لمقـــاولات المـــغرب
ⵜⴰⴹⴰⵎⵓⵏ ⵜⴰⵎⴰⵡⴰⵙⵜ ⵏ ⵜⵎⵓⵔⵜⵉⵜⵉⵏ ⵏ ⵍⵎⵖⵔⵉⴱ
Confédération Générale des Entreprises du Maroc
CGEM

CYBERSÉCURITÉ EN ENTREPRISE
GUIDE DE BONNES PRATIQUES

Préparé par la Commission Intelligence économique

ÉDITO

Cher(e)s Membres,

La réalisation de ce guide sur la cybersécurité, à destination des chefs d'entreprises marocains, nous a paru importante dans le contexte mouvant et incertain que nous traversons aujourd'hui du fait des répercussions du Covid-19 sur les entreprises.

Les chefs d'entreprises sont amenés à prendre des décisions stratégiques, financières, commerciales ou industrielles, au quotidien, et se trouvent ainsi exposés à des risques importants en cas de failles de protection dans leurs systèmes informatiques. Les cyberattaques, les intrusions et les vols de données sont aujourd'hui facilités par le télétravail, si le vecteur internet entre l'Entreprise et le Collaborateur n'est pas sécurisé par l'Entreprise.

Conscients que la cybersécurité est un sujet aux contours souvent peu ou mal maîtrisés par les chefs d'entreprises marocains, nous avons conçu ce guide comme un outil pratique destiné à permettre aux dirigeants de consolider leurs connaissances en matière de cybersécurité afin qu'ils soient en mesure de prendre les meilleures décisions pour leur stratégie numérique.

Ainsi, l'objectif de ce guide est de sensibiliser les entreprises marocaines aux nouvelles menaces et aux nouveaux enjeux qui imposent la mise en place d'une stratégie de cybersécurité moderne afin de répondre, au mieux, à la nécessité de protection de l'outil industriel, intellectuel, voire stratégique que représentent vos sociétés.

Nous espérons que ce guide vous sera utile et contribuera à la mise en place d'une stratégie de cybersécurité au sein de vos entreprises qui, liées les unes aux autres, contribueront à une plus grande sécurité de l'espace économique marocain.

Driss Benomar
Président
Commission Intelligence économique

TABLE DES MATIÈRES

INTRODUCTION

À l'échelle mondiale, le cybercrime est considéré comme l'un des risques les plus susceptibles de frapper les organisations au cours des 10 prochaines années.

Vu leur dépendance aux technologies de l'information et Internet, les entreprises, notamment les PME, sont devenues vulnérables à la cybercriminalité, ce qui fait de la cybersécurité une préoccupation croissante chez les entreprises.

Mais contrairement aux grandes organisations, la plupart des PME n'ont pas déployé un plan d'action de cybersécurité et ne disposent pas de ressources humaines et financières dédiées.

Le présent guide, élaboré par la Commission Intelligence économique de la CGEM, s'adresse aux chefs d'entreprises et leur permettra de :

- mesurer les enjeux pour l'entreprise et d'identifier les vulnérabilités spécifiques ;
- sensibiliser les collaborateurs ;
- entamer une démarche de cybersécurité au sein de l'entreprise.

Les recommandations contenues dans ce guide pratique aideront les PME à mieux se protéger contre la cybercriminalité, à avoir une longueur d'avance en termes de sécurité et de protection des données stratégiques et permettra, ainsi, d'éviter les pièges les plus courants.

CYBERSÉCURITÉ EN CHIFFRES

3 min Temps nécessaire pour casser un objet connecté selon les spécialistes

1,5 Million de victimes de fraude à la carte bancaire par an

62% le nombre d'entreprises ayant subi des attaques de phishing et d'ingénierie sociale en 2018

40% le taux de succès d'un ransomware (selon les éditeurs)

201 jours le temps moyen pour découvrir une cyberattaque

5% des dossiers des entreprises sont correctement protégés

71% des infractions étaient motivées financièrement et 25% étaient motivées par l'espionnage.

52% des violations comportaient du piratage, 28% impliquaient des logiciels malveillants et 33% incluaient du phishing ou de l'ingénierie sociale, respectivement.

.doc et .dot les principaux types de pièces jointes aux e-mails malveillants qui représentent 37%, le deuxième plus élevé étant .exe avec 19,5%.

Violations de données

4,1 Milliards d'enregistrements au 1er trimestre 2019

68% des chefs d'entreprise estimant que leurs risques de cybersécurité augmentent

I. DÉFINITIONS DE LA CYBERSÉCURITÉ ET DE SES ENJEUX DANS LE FONCTIONNEMENT DE L'ENTREPRISE

1. Qu'est-ce que la cybersécurité?

La cybersécurité se définit comme un ensemble de processus, de technologies et de pratiques visant à protéger les personnes et infrastructures numériques et les données accessibles via le cyberespace, contre les attaques, dommages et accès non-autorisés.

La cybersécurité a ainsi une importance stratégique afin d'avancer, avec confiance, dans l'ère numérique.

Les objectifs généraux en matière de sécurité sont les suivants :

- La disponibilité qui garantit l'accessibilité des systèmes d'information par les utilisateurs ;
- L'intégrité qui désigne l'authenticité des données ;
- La preuve qui garantit la non-répudiation d'une transaction avec possibilité de pouvoir auditer les résultats fournis ;
- La confidentialité qui prévient l'accès accidentel ou illicite à une information confidentielle.

1.1. Quelles sont les menaces informatiques?

La transformation digitale engagée par plusieurs entreprises remet en cause la sécurité de l'information et des systèmes. Les criminels et d'autres auteurs de cyber menaces malveillantes se servent des lacunes en matière de sécurité dans les entreprises, du manque de connaissance de la cybersécurité et des développements technologiques pour compromettre les cyber systèmes.

Ces cybercriminels volent des données personnelles et financières, des fonds, des éléments de propriété intellectuelle et des secrets commerciaux. Ils perturbent le quotidien et détruisent, parfois, les infrastructures dont dépendent les entreprises.

L'enjeu le plus important pour votre entreprise consiste à définir quels sont les biens, les menaces et les risques potentiels qui s'ensuivent et à les classer par ordre de priorité.

1.2. Quelles sont les typologies des cyberattaques?

Une cyberattaque est un « acte malveillant commis envers un système informatique par l'intermédiaire d'un réseau informatique ». Le risque informatique est devenu l'une des préoccupations de la majorité des entreprises, quels que soient leur taille et leur secteur d'activité. Les menaces liées au piratage et à la perte de données sont les plus redoutées après le risque d'interruption d'activité.

Une prise de conscience seule n'empêche pas la multiplication des attaques. Selon une étude du cabinet EULER HERMES & DFCG parue en 2020, plus de 7 entreprises sur 10 ont subi au moins une tentative de fraude durant cette année.

Parmi les types d'attaques les plus répandues qui compromettent la sécurité de la PME, on trouve notamment :

- Déni de service (DoS – Denial of service) ;
- Hameçonnage (Phishing) ;
- L'Homme du milieu (Man-in-the-middle) ;
- Virus (Malware) ;
- Injection ;
- Ingénierie sociale ;
- Tunneling DNS ;
- Délit d'initié.

- **Déni de service (DDOS – Distributed Denial of Service)**

  Une attaque par déni de service est une tentative malveillante de déranger le trafic d'un serveur, service ou réseau, en bombardant la cible ou ses infrastructures environnantes avec un flot de trafic internet.

  Ces attaques exploitent un système de machines compromises, appelées zombies ou bots, qui effectuent des requêtes multiples vers l'adresse IP de la cible et empêchent les requêtes courantes de procéder. Cette armée de zombies peut être constituée d'ordinateurs et d'appareils en réseau.

- **Hameçonnage (Phishing)**

  L'hameçonnage est une des attaques les plus anciennes et connues qui vise à récupérer des données confidentielles des victimes tels qu'un nom d'usager, un mot de passe, des informations de carte de crédit ou encore des informations pour accéder au réseau.

  Cet acte malveillant repose sur l'ingénierie sociale pour manipuler les victimes et les pousser à effectuer une action telle que cliquer sur un lien téléchargeable ou télécharger un document. Le phishing s'amorce habituellement par un faux courriel d'une personne reconnue qui présente toutefois des différences avec un courriel original.

- **L'homme du milieu (Man-in-the middle)**

  L'attaque de l'homme du milieu s'apparente à l'hameçonnage traditionnel mais s'amorce avec des communications entre deux personnes qui peuvent être un particulier et sa banque ou encore un patron et l'un de ses employés.

  Un cybercriminel qui a intercepté les messages s'insère ensuite dans la conversation et envoie un message frauduleux à l'un des interlocuteurs. Il pourrait s'agir d'un courriel avec un lien vers un faux site très semblable à celui d'un fournisseur et qui demande les informations de connexion du client.
  Il existe de multiples façons pour les cybercriminels d'exécuter ces attaques, mais bien souvent, elles proviennent d'un réseau qui est mal protégé.

- **Logiciels malveillants (Malware)**

  Les virus informatiques sont, sans aucun doute, la forme d'attaque la plus connue, porte étendard des risques associés aux technologies d'information.
  Ils font partie de la famille des logiciels malveillants, communément appelés malwares, et n'en constituent qu'un faible pourcentage.

Actuellement, les virus purs ne représentent qu'une infime partie, comparativement à la majeure partie des malwares trouvés sur internet.
Parmi les logiciels malveillants les plus répandus, on retrouve le cheval de Troie, les cryptovirus, les adwares et les espiogiciels.

- **Injections**

  Les attaques par injections visent les sites et applications Web et sont reconnues comme étant le plus important risque de sécurité au niveau des applications sur internet.

  Ces injections consistent à entrer dans un programme à l'aide d'une requête qui est interprétée comme une commande par l'application visée. Cette action modifie l'exécution du programme et permet au cyberpirate d'accéder à une variété d'informations. Les plus connues sont les injections SQL et les Cross-Site Scripting (XSS), particulièrement dans les applications qui ne sont plus supportées. Ce qui montre l'importance, pour les entreprises, d'effectuer les mises à jour.

- **Ingénierie sociale « social engineering »**

  L'ingénierie sociale est l'art sombre de l'utilisation des interactions sociales pour tromper vos collaborateurs et les pousser à commettre une erreur de sécurité. Les attaques d'ingénierie sociale visent à franchir un obstacle de sécurité technique en manipulant leur victime pour révéler des informations privées (nom d'utilisateur, mot de passe, informations de carte de crédit, contrats, dossiers, etc.).

  Une attaque d'ingénierie sociale bien menée se terminera sans même que votre collaborateur ne sache ce qu'il s'est réellement passé. Les cybercriminels interagissent et posent des questions pour instaurer une relation de confiance dans le but de récupérer une quantité suffisante de renseignements de vos collaborateurs pour contourner les dispositifs de sécurité technique.

- **Tunneling DNS**

  L'attaque par Tunneling DNS utilise principalement le protocole DNS pour communiquer le trafic non DNS sur le port 53. Il envoie le trafic HTTP et autres protocoles comme les services VPN de tunnel DNS. Il est utilisé pour déguiser le trafic sortant en DNS, masquant les données qui sont généralement partagées via une connexion Internet. Pour une utilisation malveillante, les requêtes DNS sont manipulées pour exfiltrer les données d'un système compromis vers l'infrastructure de l'attaquant. Il peut également être utilisé pour les rappels de commande et de contrôle de l'infrastructure de l'attaquant vers un système compromis.

- **Délit d'initié**

  En informatique, le délit d'initié fait partie des menaces internes et se produit lorsqu'une personne qui détient des informations confidentielles, comme par exemple un mot de passe ou la clé de la salle des serveurs, s'en sert pour commettre un cybercrime. Cette personne peut également voler des données de l'entreprise ou vendre ces informations à des cybercriminels.

  À noter que les attaques internes représentent la principale menace pesant sur les organisations, dont 80 % sont confrontées au risque de voir des comptes utilisateurs compromis.
  Des employés peuvent mener à une cyberattaque contre leur entreprise par inadvertance, en ouvrant, par exemple, une pièce jointe infectée par un logiciel malveillant ou bien en tardant à corriger les failles de système.

1.3. Exemples de cyberattaques

En 2019, Airbus a été victime d'un incident de cybersécurité dans les systèmes informatiques de sa branche «aviation commerciale». Des données à caractère personnel ont été consultées, mais cette intrusion ciblait principalement des documents techniques relatifs à la certification des avions Airbus.

Cette infiltration s'est propagée via une première attaque dont l'un des fournisseurs d'airbus a été victime. L'attaque s'est donc produite en deux temps, sur plusieurs semaines, via un mode opératoire utilisé par un groupe de hackers qui opère depuis la Chine.

- En 2017, des pirates sont parvenus à faire émettre à leur profit 81 millions de dollars par virements de la Banque du Bangladesh. Par quel moyen ? Après avoir réussi à introduire un logiciel espion dans le réseau de la banque, ils ont patiemment observé pendant plusieurs mois, de l'intérieur, les processus internes jusqu'à identifier une méthode valable pour leur vol.

- Le cas de l'attaque NotPetya, survenue en 2017, qui a fait trembler le monde de la cybersécurité. Pour la première fois, un pays est la cible d'une action de sabotage de grande ampleur. En quelques heures, l'Ukraine, le pays ciblé, a vu peu à peu des pans de son économie se figer. Des dizaines, puis des centaines d'entreprises, n'ont pu accéder à leurs données. Il s'agissait d'un « wiper », c'est-à-dire un effaceur de données conçu dans l'unique but de détruire. Puis, de poste en poste, de réseau en réseau, NotPetya a commencé sa propagation qui a conduit à une guerre éclair. Très vite, il « envahit » l'Ukraine, puis traverse les frontières en empruntant les réseaux des filiales locales de groupes internationaux. On le retrouve en Russie et un peu partout en Europe.

- La compagnie aérienne britannique EasyJet a également été victime d'une cyberattaque « très sophistiquée » en mai 2020. Les pirates ont eu accès, grâce à celle-ci, aux adresses électroniques et aux informations de voyages d'environ 9 millions de clients. Pour 2 208 passagers, l'affaire était plus grave : leurs données de carte bancaire ont également été saisies par les auteurs de l'attaque.

- En Juin 2020, Honda a fait état d'une cyberattaque majeure au sein de ses serveurs internes. Victime de ransomware, le constructeur automobile japonais a dû arrêter une partie de sa production dans plusieurs de ses usines à travers le monde.

2. Enjeux de la cybersécurité

Vu l'ampleur des risques encourus, il est impératif, pour les PME, de se protéger contre la multitude d'attaques qu'elles peuvent subir.
La cybersécurité permet d'employer des méthodes préventives et de surveillance pour contrer les cyberattaques. Elle débute par l'implantation de bonnes pratiques au sein même de l'entreprise.

Ainsi, la cybersécurité permet d'améliorer :

- **la sécurité :** par la mise en place des contrôles axés sur les risques pour se protéger contre les menaces connues et émergentes et de se conformer aux règles et aux normes en la matière.

- **la vigilance :** par la détection des infractions et des anomalies grâce à une meilleure prise de conscience de la situation à l'échelle de l'entreprise.

- **la résilience :** par le développement de la capacité de reprendre les activités normales et de réparer les dommages subis par l'entreprise.

II. CADRE JURIDIQUE ET LÉGISLATIF DE LA CYBERSÉCURITÉ AU MAROC

Selon le rapport de Kaspersky, paru en juillet 2020, 13,4 millions de cyber-attaques ont été détectées entre avril et juin 2020 au Maroc (Période de confinement dû à la pandémie Covid-19).

Trois tendances majeures ressortent de ce rapport, à savoir : l'ingénierie sociale (techniques utilisées par les cybercriminels pour inciter des utilisateurs peu méfiants à leur envoyer leurs données confidentielles, infectant ainsi leurs ordinateurs avec des programmes malveillants), le Maroc est classé à la 32ème place mondiale, les menaces locales (48ème rang mondial) et le rôle des serveurs hébergés sur le territoire (61ème position mondiale).

Par ailleurs, l'Indice Global de la Cybersécurité (Global Cybersecurity Index) qui mesure le niveau de développement de chaque pays dans ce domaine et évalue l'engagement des pays en faveur de la cybersécurité dans cinq piliers stratégiques (juridique, technique, organisation, prise de conscience, savoir-faire et coopération internationale), place le Maroc au 93ème rang par rapport à 197 pays en 2018. Un positionnement quoiqu'en recul (49 en 2017).

Le Maroc est conscient de son classement parmi les pays les plus exposés à la menace électronique. Il s'est engagé, ces dernières années, dans le renforcement de ses capacités nationales de sécurité des systèmes d'information.

À partir de 2003, le Maroc a commencé à se doter d'un corpus législatif dédié à la protection contre les cybermenaces, avec, en premier lieu, la loi 07-03 intégrant des infractions relatives aux systèmes de traitement automatisé de données définies dans la Convention de Budapest.

En 2007, le pays se dote d'un cadre juridique portant sur la cryptographie, la signature électronique et la certification électronique avec la loi 53-05.

Le renforcement du cadre légal se poursuit en 2009 avec la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Inspirée des

législations européennes – ante RGPD – et française, cette loi a notamment pour objectif d'accompagner et de faciliter les échanges de données avec l'Europe compte tenu du développement de l'externalisation des services au Maroc.

Ces lois ont été complétées, depuis 2009, par plusieurs décrets et arrêtés dont les plus récents traitent plus particulièrement de la protection des systèmes d'information des infrastructures d'importance vitale (décret n° 2-15-712 fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale et arrêté n°3-44-18 fixant les critères d'homologation des prestataires d'audit privés des systèmes d'information sensibles des infrastructures d'importance vitale).

En complément de ce cadre législatif, le Maroc s'est doté, en 2012, d'une stratégie nationale en matière de cybersécurité articulée autour de 4 axes :

- **AXE 1 : Évaluer les risques pesant sur les systèmes d'information au sein des administrations, organismes publics et infrastructures d'importance vitale ;**
- **AXE 2 : Protéger et défendre les SI des administrations, organismes publics et infrastructures d'importance vitale ;**
- **AXE 3 : Renforcer les fondements de la sécurité des SI ;**
- **AXE 4 : Promouvoir la coopération nationale et internationale.**

Le 6 juillet 2020, la Chambre des Représentants a adopté **le projet de loi n° 05-20 relatif à la cybersécurité** dans le but de renforcer l'arsenal juridique en matière de lutte contre les cyberattaques et les cybercrimes, compte tenu des menaces croissantes auxquelles l'État, les institutions publiques et les entreprises font face.

Ce projet de loi permet au Maroc de fortifier son arsenal juridique en renforçant la sécurité des systèmes d'information des administrations de l'État, des collectivités territoriales, des établissements et entreprises publics et toute autre personne morale de droit public, ainsi que des opérateurs de télécommunications.

Ce texte de loi prévoit aussi les normes et dispositions de sécurité applicables aux infrastructures vitales et celles applicables aux exploitants de réseaux publics de télécommunications, aux

fournisseurs d'accès internet, de services de cybersécurité, de services numériques et aux éditeurs de plateformes en ligne.

Cette loi prévoit également la création de deux institutions. En premier lieu, il s'agit de la mise en place de la Commission stratégique de cybersécurité dont la mission sera, entre autres, de fixer les grandes orientations de l'État en matière de cybersécurité. La seconde institution "Autorité nationale de la cybersécurité", qui sera créée, aura pour mission, entre autres, d'exécuter les orientations fixées par la Commission.

En outre, pour assurer la gouvernance étatique de la cybersécurité, plusieurs organisations ont été créées au cours des dix dernières années :

- **Le Comité Stratégique de la Sécurité des Systèmes d'Information (CSSSI)**, créé en 2011 et présidé par le Ministre chargé de l'Administration de la Défense Nationale. La mise en oeuvre des orientations stratégiques revient principalement à la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), également créée en 2011.
- **L'Agence Nationale de Réglementation des Télécommunications (ANRT)**, chargée de la régulation et de la réglementation du secteur des télécommunications.
- **La Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP)** dont la responsabilité est de contrôler le respect de la législation en matière de protection des données personnelles.
- **Le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI)** qui porte la Campagne Nationale de Lutte Contre la Cybercriminalité.

Sans oublier la ratification de conventions internationales en matière de lutte contre la cybercriminalité et le terrorisme telles que la Convention de Budapest relative à la cybercriminalité.

Malgré cet arsenal juridique dont dispose le Maroc, il reste encore des efforts à faire en termes d'applicabilité. En effet, les tribunaux

continuent à se référer au droit commun pour incriminer des actes de cybercriminalité, question de commodité, au lieu de se référer aux nouvelles lois.

Un travail de sensibilisation doit également être mené pour maîtriser le phénomène et impliquer toutes les composantes de la société dans cette guerre numérique.

Le secteur privé, et particulièrement les petites et moyennes entreprises, reste relativement en retard en matière de stratégie, de formation et de sensibilisation à la cybersécurité à cause de multiples facteurs, non seulement en relation avec les budgets attribués à la sécurité des systèmes d'information ou de protection des données personnelles et professionnelles, mais également en l'absence d'une culture de cybersécurité.

Corpus juridique et légal pour combattre la cybercriminalité qui concerne les entreprises au Maroc :

- **Loi n°07-03** complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données (STAD) ;
- **Loi n°53-05** relative à l'échange électronique de données juridiques ;
- **Loi n° 09-08** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;
- **Décret n°2-15-712 du Joumada II 1437** (22 mars 2016) fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale ;
- **Loi n° 05-20** relative à la cybersécurité, qui renforce l'arsenal juridique du Maroc. En vertu de cette loi, le gouvernement pourra exercer, à l'aide de l'agence nationale de cybersécurité, un pouvoir de contrôle et de protection des systèmes informatiques et des données aussi bien des établissements publics que privés.

Malgré la présence d'un cadre juridique et législatif, les cybercriminels restent difficiles à pister. D'où l'importance, pour vos entreprises, de se doter de mesures de protection.

III. ÉVALUATION DES MENACES ET DES VULNÉRABILITÉS DE L'ENTREPRISE

Les cybercriminels profitent des vulnérabilités des systèmes informatiques, notamment des systèmes d'exploitation non corrigés, d'un mot de passe faible et d'une formation inadéquate des collaborateurs.

Les entreprises qui n'effectuent pas d'analyse des vulnérabilités et qui ne corrigent pas efficacement les faiblesses de leurs systèmes d'information s'exposent davantage à la compromission de leurs systèmes informatiques.

Pour protéger leurs actifs informationnels contre la menace grandissante de cyberattaques qui ciblent les vulnérabilités des systèmes, davantage d'organisations ont inclus des évaluations de la vulnérabilité dans leurs programmes de cybersécurité.

Ces évaluations permettent de déceler les vulnérabilités dans les systèmes informatiques. Les résultats de ces évaluations aident les organisations à localiser les risques de cybersécurité.

Quelques recommandations à suivre pour l'évaluation des menaces et des vulnérabilités :

- Utiliser périodiquement un outil automatisé pour évaluer les vulnérabilités de tous les systèmes du réseau. Remettre des listes de priorité renfermant les vulnérabilités les plus pressantes à chaque administrateur de système.

- S'abonner à un service de renseignement sur les vulnérabilités afin de demeurer au fait des nouvelles menaces et expositions au risque.

- Veiller à ce que les outils d'évaluation de la vulnérabilité utilisés soient périodiquement mis à jour et renferment les renseignements les plus à jour sur les vulnérabilités.

- Veiller à ce que les logiciels/applications informatiques soient mis à jour périodiquement à l'aide de correctifs de sécurité.

- Soumettre les correctifs essentiels à des essais avant de les faire passer au mode de production. Les menaces étant en constante évolution, il est recommandé que l'entreprise réalise un test d'intrusion au moins une fois par année ou dans les contextes suivants :

    - Avant le lancement de nouveaux produits et services ;
    - Après des modifications de votre infrastructure ;
    - Avant la fusion ou l'acquisition d'une entreprise ;
    - Lors de l'utilisation/du développement d'applications ;
    - Conformité aux normes réglementaires ;
    - Avant des contrats commerciaux importants.

Ces tests d'intrusion, également appelés « pentests », sont une évaluation des réseaux, systèmes informatiques et applications visant à identifier et à traiter les vulnérabilités de sécurité qui pourraient être exploitées par les pirates informatiques.

- Utiliser uniquement des systèmes d'exploitation et logiciels sans support par leur éditeurs.

- Utiliser le cloud comme solution pour éviter la perte des données sensibles, qui est un moyen simple d'utilisation pour les PME.

VI. MESURES INDISPENSABLES DE PROTECTION DES DONNÉES DE L'ENTREPRISE

La cybersécurité est d'abord une affaire de management, qui ne doit pas reposer sur une seule personne. Tout le monde est concerné. L'implication des dirigeants est la clé pour assurer la compréhension, la pondération des risques et la réussite des mesures nécessaires. Au même titre que le processus "métiers de l'entreprise", les processus de sécurité doivent être expliqués et communiqués aux services utilisateurs.

1. Élaboration d'une stratégie Cybersécurité

La sécurité de l'information et des systèmes repose sur plusieurs volets et exige une approche de gestion intégrée. Les entreprises doivent instaurer une approche axée sur les risques pour mettre en place une stratégie de cybersécurité visant à éviter, atténuer, accepter ou transférer délibérément les risques que posent les cybermenaces.

L'objectif principal de la stratégie de cybersécurité doit être de rendre l'entreprise résiliente face aux risques de perte ou de compromission de l'information et des systèmes. Elle permet aussi d'établir et de tenir à jour un cadre approprié de gouvernance et de gestion des risques pour détecter et éliminer les risques auxquels sont exposés les réseaux et les services de communication.

Pour élaborer une stratégie en matière de cybersécurité, il ne suffit pas de vous préparer aux menaces que vous croyez connaître. Vous devez aussi envisager les menaces inconnues.

Les 3 étapes ci-après peuvent vous aider à créer une organisation qui exerce ses activités en toute sécurité, qui demeure vigilante face aux cybermenaces et qui peut faire preuve de résilience en cas d'attaque. Les entreprises qui suivent ces étapes essentielles peuvent devenir plus vigilantes, sécuritaires et résilientes.

1.1. Vigilance

Concentrez-vous sur ce qui importe : vos actifs attrayants et vos relations
Repérez vos interactions et vos actifs essentiels.

Évaluez le cyber risque de manière proactive
Renseignez-vous sur ce que vous devez chercher et sur la manière de détecter les menaces, qu'elles soient conventionnelles ou émergentes.

Mettez l'accent sur la sensibilisation pour établir une défense à plusieurs niveaux
Élaborez un cyber programme qui porte sur une combinaison de défenses englobant les aspects les plus cruciaux de votre organisation, de vos employés, de vos clients et de vos partenaires.

1.2. Sécurité

Fortifiez les protections de votre organisation
Établissez un plan pour corriger les failles, gérer les correctifs, concevoir des logiciels sécurisés et assurer la sécurité physique.

1.3. Résilience

Préparez-vous à l'inévitable
Concentrez-vous sur la gestion des incidents et la simulation pour « tester vos barrières » et votre réaction.

2. Cybersécurité en entreprise : 14 réflexes clés

- Impliquez le top management ;
- Sensibilisez les collaborateurs ;
- Élaborez une politique de sécurité et un code de conduite ;
- Gérez vos ressources informatiques ;
- Établissez des procédures avec vos partenaires ;
- Sécurisez votre site Internet ;
- Maîtrisez la diffusion des données relatives à votre société ;
- Choisissez les mots de passe avec soin ;
- Sécurisez l'accès à vos services bancaires ;

- Sécurisez votre matériel informatique et vos données ;
- Protégez votre connexion Internet ;
- Enquêtez sur le personnel et les menaces internes ;
- Sécurisez votre environnement physique et logique ;
- Protégez votre système d'information.

Réflexe 1 : Impliquez le top management

- Désignez un responsable de la sécurité de l'information ;
- Identifiez votre risque en matière de TIC et protégez votre entreprise pour l'avenir ;
- Respectez les exigences légales et réglementaires concernant la vie privée, le traitement des données et la sécurité ;
- Soyez conscient des cybermenaces et des vulnérabilités sur vos réseaux ;
- Définissez clairement les objectifs du monitoring du système et du réseau ;
- Identifiez les conséquences juridiques d'une fuite de données, d'une défaillance du réseau, etc. pour l'entreprise ;
- Procédez périodiquement à un audit des risques et de la sécurité ;
- Communiquez les résultats et le plan d'action au management.

Réflexe 2 : Sensibilisez les collaborateurs

- Sensibilisez chacun de vos collaborateurs à la cybersécurité de leur quotidien professionnel avec des exemples concrets ;
- Adoptez une charte informatique pour préciser à l'ensemble de vos collaborateurs les conditions d'utilisation du matériel informatique de l'entreprise, de la messagerie lors de déplacements professionnels ou encore pour l'utilisation mixte d'un matériel (usage professionnel et personnel) ;
- Développez des formations spécifiques pour les postes les plus exposés (ex : habilités aux paiements) et planifiez des séances de rappel car les fraudes évoluent régulièrement ;
- Mettez en place des protocoles et des consignes de sécurité, particulièrement pour les paiements et contrôlez la bonne application ;

- Si des mots de passe ou codes ont été révélés, changez-les immédiatement ;
- Surveillez régulièrement les comptes bancaires pour détecter des opérations frauduleuses et les contester.

Réflexe 3 : Élaborez une politique de sécurité et un code de conduite

- Créez et appliquez des procédures pour l'arrivée et le départ d'utilisateurs (personnel, stagiaires, etc.) ;
- Décrivez les rôles et les responsabilités en matière de sécurité (physique, du personnel et des TIC) ;
- Développez et diffusez un code de conduite pour l'utilisation des ressources informatiques ;
- Planifiez et exécutez des audits de sécurité ;
- Créez un schéma de classement et de traçabilité des informations sensibles ;
- Détruisez les documents sensibles à l'aide d'une déchiqueteuse ;
- Appliquez le Locked Print si disponible ;
- Développez un concept et un plan de formation à la cybersécurité.

Réflexe 4 : Gérez vos ressources informatiques

- Tenez un inventaire de l'ensemble des équipements TIC et des licences de logiciels ;
- Maintenez une carte détaillée et actualisée de tous vos réseaux et interconnexions ;
- Utilisez un instrument de gestion de configuration ;
- Définissez une configuration de sécurité de base ;
- Assurez-vous que les contrats et les accords de niveau de service (Service Level Agreements) disposent d'une clause de sécurité ;
- Implémentez un processus de contrôle du changement ;
- Implémentez un niveau uniforme de sécurité pour tous vos réseaux ;
- Auditez régulièrement toutes les configurations (y compris les serveurs, les pare-feux et les composants de réseau).

Réflexe 5 : Établissez des procédures avec vos partenaires

- Établissez, pour vos collaborateurs, des protocoles précis pour la réalisation de toutes vos opérations bancaires ;
- Si une demande est inhabituelle ou concerne un changement d'IBAN, vérifiez directement auprès du partenaire en utilisant toujours les coordonnées et procédures habituelles de contact ;
- En cas de « rappel pour impayé », prenez le temps d'effectuer des vérifications sur la réalité de la prestation facturée et consultez les factures antérieures pour en vérifier la cohérence ;
- Contrôlez les informations diffusées sur votre entreprise, notamment sur Internet et n'échangez pas d'informations sensibles avec vos partenaires en dehors de circuits sécurisés ;
- Informez votre partenaire habituel (banque, comptable, etc.), dont semble provenir le message frauduleux pour lui signaler des tentatives de fraude utilisant son identité ;
- Surveillez régulièrement vos comptes bancaires pour détecter des opérations frauduleuses et les contester ;
- Nettoyez régulièrement votre système informatique.

Réflexe 6 : Sécurisez votre site Internet

- Installez un certificat de sécurité en «https» et choisissez un hébergement sécurisé avec une assistance 24h/24 ;
- Assurez-vous, auprès de votre banque ou de votre prestataire de paiement, de la sécurité des solutions de paiement proposées pour la vente à distance ainsi que des fonctionnalités de contrôle (plafond par carte, analyse de risque des transactions, scoring...) ;
- Limitez les risques d'impayés liés à l'usurpation d'identité/fraude à la carte bancaire par la mise en place d'un système d'authentification fort sur votre site (de type 3D Secure ou autre) ;
- Sécurisez les données de vos clients en les chiffrant, en changeant régulièrement les mots de passe, en mettant à jour vos antivirus...
- Conservez uniquement les données utiles de vos clients et évitez de stocker les numéros de carte bancaire.

Réflexe 7 : Maîtrisez la diffusion des données relatives à votre société

- Vérifiez que les contenus que vous publiez sur votre site /page sur les réseaux sociaux ne sont pas sensibles ; Contrôlez régulièrement les informations disponibles sur votre entreprise en saisissant son nom dans un moteur de recherche ;
- Sensibilisez vos salariés à ce risque spécifique, notamment en attirant leur attention sur les dangers des réseaux sociaux : informations, photos, etc. qui pourraient être utilisées de façon malveillante.

Réflexe 8 : Choisissez vos mots de passe avec soin

- Définissez un mot de passe unique pour chaque service, appareil, logiciel, application utilisé par votre entreprise. Il ne doit contenir aucune information professionnelle ou personnelle qui pourrait être découverte par un tiers ;
- Il doit combiner, si possible, des lettres (majuscules, minuscules), des chiffres et des caractères spéciaux ;
- Le mot de passe ne doit jamais être enregistré sur votre équipement.

Réflexe 9 : Sécurisez l'accès à vos services bancaires

- Ne divulguez pas votre identifiant et votre mot de passe de connexion. Ils sont strictement personnels ;
- Changez le mot de passe provisoire fourni par votre banque dès réception ;
- En cas de délégation à votre expert comptable ou à votre service financier par exemple : demandez à votre banque un code personnel pour chacun des utilisateurs et vérifiez que les opérations autorisées (consultation, virement, montants, etc.) sont conformes aux habilitations.
- Ne vous connectez pas depuis un appareil ou un réseau Wi-Fi public ;
- Pour votre navigation, tapez l'adresse du site de votre banque et ne suivez jamais un lien qui vous a été envoyé dans un courriel ;
- Suivez les consignes de sécurité pour votre matériel informatique et votre connexion.

Réflexe 10 : Chiffrez les disques de vos dispositifs et matériels informatiques (PC, tablettes, smartphones…)

- Chiffrez les données sensibles en les transformant en un code illisible qui ne peut pas être déchiffré facilement par les personnes qui n'y sont pas autorisées ; Mettez en place l'authentification pour tous les systèmes sensibles ;
- Verrouillez votre appareil dès que vous cessez de l'utiliser et activez l'authentification par code, schéma, empreinte, etc. de votre smartphone /tablette, en plus du code PIN ;
- Utilisez un antivirus régulièrement mis à jour et un système informatique de détection des menaces (EDR) ;
- Limitez la possibilité d'installation de logiciels aux seules personnes habilitées (votre référent informatique par exemple ou la personne désignée comme administrateur) ;
- Effectuez régulièrement des sauvegardes de vos données sur des supports externes (disques durs de préférence) stockés à un autre endroit ;
- Bannissez l'usage de logiciels et systèmes d'exploitation qui ne sont plus supportés par leurs éditeurs ;
- Limitez, pour vos collaborateurs ou vous-même, l'utilisation à des fins professionnelles des appareils privés souvent moins sécurisés ;
- N'introduisez pas de contenus en provenance de sources à la fiabilité inconnue (clé USB trouvée, sites internet, pièce jointe d'un courriel suspect, etc).
- En cas de perte ou de vol d'un terminal (tablette, ordinateur, téléphone…), changez immédiatement vos mots de passe (applications bancaires et non bancaires), y compris vos codes d'accès de messagerie électronique ;
- En cas de virus ou d'attaque, lancez votre antivirus et déconnectez votre appareil de votre réseau informatique pour éviter une propagation. N'effectuez aucune opération de banque à distance (connexion, virement, opposition…) jusqu'à désinfection de votre matériel ;
- Signalez les dysfonctionnements de votre ligne téléphonique à votre opérateur pour vous assurer que votre ligne n'a pas été détournée.

Réflexe 11 : Protégez votre connexion Internet

- Configurez votre réseau Wi-Fi en choisissant une clé de sécurité complexe (WPA2 ou WPA-AES) depuis l'interface de votre fournisseur d'accès ;
- Si vous mettez un réseau Wi-Fi à disposition de vos clients ou de vos partenaires, communiquez leur une clé de sécurité spécifique, différente de la clé principale ;
- Vérifiez la présence d'https devant l'adresse du site auquel vous vous connectez, icône d'une clé ou d'un cadenas dans la fenêtre du navigateur Internet ;
- Contrôlez l'adresse exacte du site et le fait qu'aucune autre fenêtre internet ne soit ouverte ;
- Ne transmettez pas d'informations sensibles et ne vous connectez pas à votre site de banque à distance depuis un ordinateur public ou connecté à un réseau Wi-Fi public ;
- En cas de suspicion d'utilisation de votre connexion, modifiez le mot de passe de votre réseau Wi-Fi en utilisant un autre terminal et un autre accès à internet (réseau de votre téléphone mobile par exemple) ;
- En cas de blocage de votre ordinateur et de demande de rançon, prévenez la police et ne payez pas : en effet, rien ne garantit que les pirates vous fournissent la clé qui permettra de déchiffrer vos fichiers ou de débloquer votre ordinateur. Pour éviter la propagation, déconnectez votre équipement du réseau mais sans l'éteindre ni le redémarrer ;
- Utilisez votre antivirus et des logiciels spécialisés de récupération des fichiers.

Réflexe 12 : Mettez en place une gouvernance des données stricte

- Mettez sur pied une équipe pluridisciplinaire ;
- Examinez les processus de filtrage de sécurité préalable à l'embauche ;
- Élaborez des politiques et des processus de recrutement ;
- Mettez en place un processus des activités de formation et d'éducation ;

- Surveillez les comportements douteux ou perturbateurs dès le processus d'embauche et appliquez des mesures d'intervention adéquates.
- Mettez une distinction entre les fonctions et les privilèges mini-minimums.

Réflexe 13 : Sécurisez votre environnement physique et logique

- Déployez des pare-feux nouvelle génération avec des fonctionnalités comme émulation et extraction des menaces, anti-phishing, anti-bot et anti-ransomware ;
- Exigez l'authentification à double facteur pour tout accès à distance ;
- Fractionnez le réseau interne de l'organisation pour faire en sorte que les utilisateurs n'aient accès qu'aux services dont ils ont besoin à des fins professionnelles ;
- Mettez en œuvre une solution de contrôle d'accès au réseau afin d'empêcher des systèmes informatiques inconnus de communiquer avec le réseau de l'organisation.

Réflexe 14 : Protégez votre système d'information

- Mettez en œuvre des processus de sauvegarde et de recouvrement et effectuez périodiquement des sauvegardes de vos systèmes ;
- Mettez en œuvre une politique pour contrôler tous les accès à des supports amovibles ;
- Analysez tous les supports pour éliminer les programmes malveillants avant de les importer sur l'ordinateur de l'organisation ;
- Mettez un processus de validation des solutions avant de les intégrer dans votre système d'information ;
- Contrôlez le flux d'entrée/sortie de matériels.

V. TÉLÉTRAVAIL : SÉCURISEZ LES ÉCHANGES CONTRACTUELS

La globalisation, les risques sanitaires, les catastrophes naturelles, ont poussé les organisations à privilégier le télétravail pour leurs collaborateurs. Ce mode de travail impose une vigilance constante afin de garantir la protection de l'information stratégique face aux attaques des cybercriminels.

Dans le contexte mondial actuel, bien que l'adoption de solutions numériques ait joué un rôle important dans la réduction du risque de contracter le virus Covid-19, en permettant aux gens de continuer à travailler et à étudier, elle a néanmoins accru les défis de la cybersécurité.

Ceci concerne particulièrement les personnes qui travaillent à domicile car si les entreprises ont souvent des défenses de cybersécurité installées dans les bureaux et sur les ordinateurs de l'entreprise, il n'en est pas toujours de même pour les employés travaillant à distance.

Ainsi, Le confinement de millions de salariés à travers le monde pour se protéger du Covid-19 a suscité un nombre sans précédent de cyberattaques et de tentatives d'intrusions numériques.

La pandémie a créé un environnement idéal pour les cybercriminels car la majorité des employés travaille dans des conditions moins familières, moins sécurisées et les entreprises n'étaient pas préparées à ce genre de situation étant donné que le basculement a dû se faire dans l'urgence. Cette pandémie a ouvert la porte à des acteurs malveillants qui ont recours à l'hameçonnage par courriel « phishing » et au piratage psychologique « social engineering ».

Les cybercriminels profitent des peurs générées par la pandémie pour pousser les utilisateurs à cliquer sur des pièces-jointes ou des liens malveillants pour s'infiltrer.

Les sociétés qui opèrent en mode télétravail engagent leur survie en cas de cyberattaques car cela engendre des risques sérieux de sécurité de type hameçonnage, chiffrement illicite par rançongiciels, le vol des données et l'escroquerie par des faux ordres de virement. Aujourd'hui, le télétravail n'est plus un confort mais parfois une obligation légale, comme c'est le cas durant la période de crise Covid-19. Il est au cœur des efforts fournis contre la pandémie. L'entreprise a l'obligation de préparer des mécanismes de travail à distance qui puissent être efficaces pour ralentir la propagation du Covid-19.

Les entreprises doivent s'adapter et engager des actions en déployant les mesures nécessaires, à savoir :

- Définir et mettre en œuvre une politique de télétravail avec une charte de sécurité pour les équipements des télétravailleurs ;
- Sensibiliser ses collaborateurs de façon périodique aux procédures, politique, chartes sécurité et risques cyber ;
- Sécuriser et réaliser un inventaire des équipements et accès extérieurs ;
- Déployer des solutions pour renforcer la politique de gestion des accès, mots de passe et les mises à jour de sécurité systèmes.
- Assurer exclusivement des accès à distance chiffrés (HTTPS, VPN) avec authentification forte à deux ou trois facteurs.
- Durcir la sauvegarde des actifs informationnels, ordinateurs des collaborateurs et les conserver hors ligne.
- Déployer une solution de cryptage sur les ordinateurs mobile des collaborateurs contre la perte ou vol des équipements.
- Superviser en permanence les accès externes et les systèmes sensibles 24/24 et 7/7 via des solutions SIEM ;
- Centraliser le traitement des incidents de sécurité et adopter un comportement de résilience ;
- Mettre en place une solution qui centralise la stratégie de protection des données (DLP) face aux menaces avec une visibilité à l'échelle de l'entreprise ;
- Évaluer vos collaborateurs pour vérifier le niveau de vigilance et l'application des mesures de sécurité ;

- Veiller sur l'application stricte des consignes de sécurité sur l'ensemble des utilisateurs sans exception ;
- Sensibiliser les employés sur la façon de détecter et de gérer les attaques de phishing ;
- Appliquer des mesures de sécurité obligatoires sur les postes nomades (Antivirus avec fonction Firewall, gestionnaire des correctifs, etc.) ;
- Envisager la gestion des applications et appareils mobiles (MDM) pour faciliter la mise en place d'un certain nombre de mesures de sécurité dans l'immédiat ;
- Vérifier et mettre à jour tous vos systèmes de façon périodique ;
- Limiter l'accès des employés aux informations protégées et n'utiliser que des dispositifs et des services autorisés et validés par l'entreprise.

VI. CYBER ASSURANCE

La cyber assurance est une couverture des dommages aléatoires et quantifiables se produisant dans le monde numérique : destruction, perte, altération, divulgation, ou accès non autorisé à des données informatiques.

Un événement Cyber peut avoir différentes causes : accidentelle, erreur humaine, criminalité, malveillance ou défaillance matérielle ou logicielle.

La police d'assurance cyber peut couvrir les axes d'indemnisation des frais engagés suite un événement et prendre en charge des réclamations présentées par les tiers.

Il est important de savoir que l'assurance liée aux infractions à la sécurité des données en vertu des polices commerciales traditionnelles est un nouveau produit au Maroc. L'assurance traditionnelle ne couvre pas toutes les catégories de risques et pertes éventuels.

Quand vous êtes à l'étape de sélection d'un assureur en la matière, il importe de savoir que cette sous-spécialité cyber-risque demeure à l'étape de l'élaboration, il n'existe donc pas de clauses standards au sein du secteur.

Une pratique exemplaire consiste à examiner minutieusement les dispositions des polices d'assurance générale de la société en ce qui concerne les demandes de règlement pour infractions à la sécurité des données et à la protection des renseignements personnels.

Dans le cadre d'une stratégie de cybersécurité, il convient de déterminer le type et la portée de la protection qui correspond le mieux aux intérêts de l'entreprise et de chercher une police d'assurance traditionnelle adaptée qui englobe tous les risques auxquels un cyber incident pourrait exposer l'entreprise.

CONCLUSION

Aujourd'hui, l'entreprise ne dispose quasiment plus de fonctions essentielles indépendantes de son système d'information, ce qui l'expose à des risques majeurs entravant son activité et son image.

Les entreprises marocaines sont-elles protégées face à une éventuelle cyberattaque ? La réponse est hélas non pour la majorité d'entre elles car il y a un décalage entre le niveau de sécurité de l'entreprise et la sophistication des attaques qui évoluent rapidement avec les nouvelles technologies.
Ce retard peut être expliqué par plusieurs facteurs, notamment l'absence d'information, de compétences internes, de procédures de contrôle, des contraintes budgétaires et le manque de sensibilisation des collaborateurs.

Ainsi, le dirigeant d'entreprise doit considérer non seulement la sécurité numérique sous l'angle technologique mais bien intégrer la composante stratégique et d'image de la sécurité. On voit malheureusement que beaucoup de dirigeants prennent souvent en compte la sécurité numérique au détour d'un incident informatique grave. Or, ce manque de clairvoyance et de stratégie peut entraîner de grandes pertes à l'entreprise.

Aux entreprises de mettre les moyens en oeuvre pour se protéger. En ce sens, la cybersécurité répond à cet enjeu de protection et de confiance pour assurer le niveau adéquat d'investissement qui couvre les risques cyber, à condition qu'elle soit considérée dans le cadre d'une approche globale de gestion intégrée.

En conclusion, à l'entreprise d'utiliser les solutions qui s'offrent à elle contre la cybercriminalité, souvent très accessibles, pour se prémunir efficacement et lui garantir une vraie sécurité contre d'éventuelles menaces cybernétiques.

ANNEXE

VOCABULAIRE IT DE SÉCURITÉ

Déni de service (Dos) : Action ayant pour effet d'empêcher ou de limiter la capacité d'un système à fournir le service attendu, en sur-sollicitant le service au delà de ses capacités (ex : saturer un site web de requêtes pour le mettre hors service).

Disponibilité : Assurer l'accès et l'utilisation lorsque c'est nécessaire.

Exigences : Caractéristiques réelles prouvant l'identité d'un tiers et/ ou du respect de conformité normatif et législatif en vigueur.

Exfiltration : Sortie de données de l'entreprise de manière non autorisée.

Failles logicielles : Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système.

HTTPS : HTTP sécurisé, protocole par lequel un navigateur va tout d'abord construire un tunnel TLS (Transport Layer Security) pour protéger les informations échangées avec le serveur. Cela permet notamment de protéger l'identification et l'authentification d'un utilisateur.

Intégrité : Conservation des qualités et caractéristiques originelles d'une donnée ou d'un système, sans altération.

Menace : Cause potentielle d'un accident, à fin malveillante, s'appuyant sur une ou plusieurs vulnérabilités.

Obsolescence : Système ou protocole vieillissant, périmé, désuet.

Porte dérobée : une porte dérobée est un accès secret à un logiciel, permettant à l'éditeur ou au mainteneur informatique d'y accéder plus rapidement. L'introduction malveillante d'une porte dérobée peut transformer le logiciel en «Cheval de Troie».

Pare feu : Un pare feu est un outil permettant de protéger un ordinateur ou un réseau connecté à un autre réseau ou à internet. Il protège des attaques externes (filtrage entrant) et souvent de connexions

illégitimes à destination de l'extérieur (filtrage sortant). Le pare feu est souvent installé sur une machine dédiée dans une architecture réseau conçue pour cela.

Patrimoine immatériel : Ensemble des informations, données, connaissances et brevets détenus par une organisation.

Plan de continuité : Définition d'un plan d'action permettant de continuer l'activité (PCA) l'entreprise, éventuellement de manière réduite, lorsqu'elle subit despannes ou des attaques. Voir résilience.

Plan de reprise : Définition d'un plan d'action permettant à l'entreprise, après panne ou interruption d'activité (PRA) attaque, de revenir à un niveau normal attendu de production.

Politique de sécurité : Définition de la stratégie de protection de l'entreprise mise en place suite à une analyse de risque. La politique de sécurité inclut des moyens techniques (pare-feu, antivirus, annuaire d'entreprise), leur configuration, et les règles de bon comportement des utilisateurs, particulièrement en cas d'incident. Intrusion Attaque réussie.

Résilience : Capacité à faire face à une situation perturbante telle qu'une panne ou une attaque informatique et de continuer à fonctionner.

Risque : Possibilité qu'une vulnérabilité conduise à un préjudice sur le fonctionnement de l'entreprise.

Système d'information : Ensemble de matériels et de logiciels fournissant les services numériques d'une entreprise.

Violation d'accès : Accès non autorisé aux données ou aux services.