Avis d'expert

Guide pratique pour la cyberdéfense des ETI

Rédigé par Charles Préaux
Professeur des universités associé à l'université de Bretagne sud
Directeur de la formation d'ingénieurs en cyberdéfense à l'ubs/ENSIBS

Actualisé par Nicolas Lacourte
Solution manager Cybersécurité

nxo

Sommaire

> Le grand enjeu du XXI siècle est la numérisation de notre monde et l'enjeu de l'enjeu est la confiance dans cette numérisation en termes de liberté et d'égalité

Executive summary

Avec l'évolution croissante du numérique, on constate que les entreprises et notamment celles de taille intermédiaire, subissent de plus en plus de cyberattaques : 80% des entreprises françaises ont été touchées en 2018 selon une étude réalisée par le Cesin (Club des experts de la sécurité de l'information et du numérique) et Opinionway (entreprise de sondage). La sécurité du système d'information représente une préoccupation pour les ETI mais pas une priorité car bien souvent, elle ne savent pas comment aborder ce nouveau problème ni combien investir raisonnablement.

Conscient de cette réalité, NXO a souhaité mettre à disposition ce libre blanc pour sensibiliser et accompagner les ETI dans une démarche plus sécurisée. A travers 4 chapitres, le livre blanc donne aux dirigeants les outils pour :

- Comprendre les termes employés dans le domaine « cyber »
- Connaitre le panorama de la menace et des vulnérabilités concernant leurs systèmes
- Identifier les enjeux majeurs de la cyberdéfense de leur entreprise
- Mettre à disposition une démarche d'auto diagnostic du niveau du dirigeant d'autant plus simple

Ce guide se veut pratique et tend à montrer le rôle central du dirigeant dans la mise en place d'une politique de sécurité pour se prémunir des attaques et en limiter les conséquences.

Toutes les clés sont réunies pour permettre au dirigeant d'acquérir une vision claire et précise du domaine, ainsi il sera capable de transformer ce frein en véritable atout business.

Source : https://www.ouest-france.fr/economie/entreprises/entretien-cyberattaques-les-pme-et-eti-constituent-le-maillon-faible-6662295

Constat général

Ce guide pratique pour la cyberdéfense des entreprises de petite taille et de taille intermédiaire (ETI) se veut pédagogique et simple d'accès dans la mesure où ces entreprises sont d'abord et avant tout centrées sur leurs activités cœur de métier. En effet, la problématique de la cyberdéfense est rarement au centre de leurs préoccupations bien qu'elle les préoccupe de plus en plus

Ces entreprises constatent la dépendance croissante de leurs activités au fonctionnement des systèmes d'information ou des systèmes de production qui sont immergés et interconnectés au cyberespace. Il s'agit d'un espace où la complexité et la virtualité sont reines, où les enjeux sont assez mal cernés et la cyber menace est omniprésente. La protection des savoirs et des données numériques est devenue une impérieuse nécessité face à une cybercriminalité toujours plus performante et inventive. La cyberdéfense est une partie essentielle de l'entreprise numérique. Les organisations doivent apprendre à vivre avec des niveaux de risques acceptables.

En fait, tous les ingrédients sont réunis actuellement pour que les dirigeants d'entreprise retardent le moment de s'engager dans la voie de la cyberdéfense de leurs intérêts vitaux dans une économie numérique mondiale grandissante. En fait, elles ne savent pas vraiment comment aborder ce nouveau problème, ni combien investir raisonnablement. Il est indispensable que les dirigeants d'entreprise discernent si la cyberdéfense de leurs entreprises est un frein couteux et peu rentable ou une force qui pousse au développement.

LES DIRIGEANTS HÉSITENT À ENGAGER LEURS ENTREPRISES DANS LEUR CYBERDÉFENSE

D'une manière générale, les entreprises de type ETI hésitent à investir dans la prévention, dans la protection ou dans la cyberdéfense de leurs systèmes car elles ne savent pas bien poser le problème pour le résoudre. Elles ne savent pas trop si l'anticipation est nécessaire. Elles sont déconcertées par les diverses réglementations et par les offres et solutions. Elles se demandent comment faire ? Faut-il tout traiter en interne et combien faut-il investir raisonnablement pour cela ? Faut-il s'assurer pour déléguer les risques ? Faut-il sous-traiter ? Comment s'y retrouver dans le dédale des discours des consultants ou des vendeurs de solutions ? Tout cela est-il réellement efficace lorsque l'on constate que les cyberattaques ne cessent de croître ?

De nombreux documents disponibles en France égarent le dirigeant :

- Les directives de Bruxelles (par ex : GDPR : directive sur la protection des données personnelles),
- Les divers textes de lois et décrets en cyber sécurité,
- Le livre blanc de la défense et de la sécurité nationale de 2013,
- Le livre blanc de l'ENISA : « Comment tirer les leçons des incidents de sécurité touchant les systèmes de contrôle industriels/les systèmes SCADA ? »,
- Les documents d'orientation (par ex : Stratégie nationale pour sécurité du numérique),
- Les divers dispositifs (par ex : PPST: Dispositif de protection du potentiel scientifique et technique de la nation),
- Les politiques de sécurité (par ex : la PSSI : Politique de Sécurité des Systèmes d'information),
- Les référentiels (par ex : le RGS de l'ANSSI : Référentiel Général de Sécurité),
- Les instructions interministérielles (par ex : l'IGI 1300),
- Les nombreux guides et recommandations fort pertinents de l'ANSSI (par ex : les 40 règles du guide d'hygiène informatique),
- Les méthodologies d'analyse de risques (par ex : EBIOS, MEHARI, …)
- Le document de « anticipation, stratégie contre la cybercriminalité » du ministère de l'intérieur,
- Les nouvelles plateformes (par ex l'Acyma qui permet en cas d'incident de mettre en relation des victimes et des entreprises compétentes)

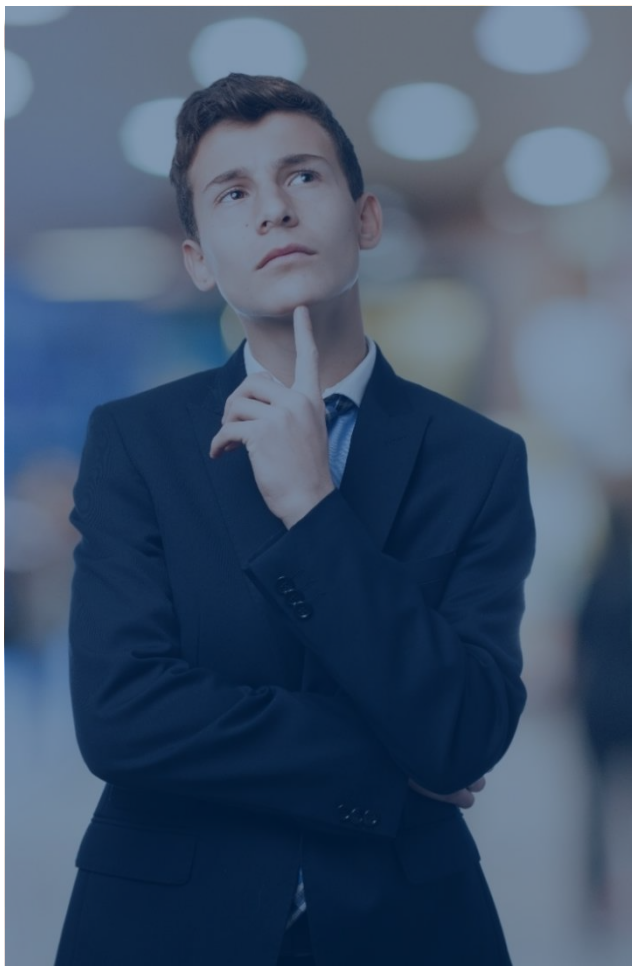
LES DIRIGEANTS HÉSITENT À ENGAGER LEURS ENTREPRISES DANS LEUR CYBERDÉFENSE (SUITE)

L’abondance, la diversité et le temps qu’il faut pour les lire, les comprendre et surtout savoir ce qu’il faut en faire n’est pas vraiment compatible avec la charge de travail d’un dirigeant d’entreprise. C’est lorsque les cyberattaques perturbent ou paralysent le fonctionnement des systèmes de l’entreprise, nuisent à l’image de l’entreprise ou à ses intérêts vitaux, que le désarroi du chef d’entreprise l’amène à prendre des décisions dans l’urgence d’une gestion de crise. Or, ce n’est certainement pas le moment idéal pour conduire une réflexion posée et rationnelle à moindre cout.

Ainsi, il y a peu d'anticipation et surtout du « curatif d’urgence » qui pousse les entreprises à réagir et s'équiper. Il y a aussi une assez mauvaise perception des risques « cyber », de ce qu'il faut protéger.

Les entreprises disent alors : c’est trop compliqué, trop couteux, bien qu’elles aient conscience du risque. Bref les dirigeants doutent à engager leurs entreprises dans leur cyberdéfense.

LES DIRIGEANTS TERGIVERSENT : « LA CYBERDEFENSE EST-ELLE UN ATOUT POUR LA CREDIBILITE DE MON ENTREPRISE ? »



On constate que les entreprises ont des difficultés à s'impliquer dans la cyber protection et la cyberdéfense de leurs systèmes alors qu'elles sont de plus en plus sensibilisées et conscientes des risques liés aux cyberattaques. Les témoignages d'autres entreprises victimes de cybercriminalité peuvent inquiéter.

En fait certains dirigeants d'entreprise pensent que ce sont des démarches trop complexes et des investissements inutiles et que ces sujets concernent principalement la DSI ou l'administrateur système et réseau mais pas vraiment le niveau de la direction.

A ce stade, on doit se poser la question essentielle suivante : la cyberdéfense peut-elle devenir une force pour la crédibilité et la pérennité de l'entreprise ?

LES DIRIGEANTS TERGIVERSENT : « LA CYBERDEFENSE EST-ELLE UN ATOUT POUR LA CREDIBILITE DE MON ENTREPRISE ? » (SUITE)

Il y a plusieurs pistes pour tenter de répondre à cette question :

- A l'instar de la démarche qualité ISO 9000, une entreprise peut améliorer la confiance de ses clients par la maitrise de l'information dans ses processus de production et de relations clients**.** La prise en compte de la cyberdéfense peut devenir une opportunité pour le développement des entreprises car comme pour la qualité elle rassure le client. Elle contribue à diffuser une culture de confiance.

- Une entreprise, qui connait la dépendance numérique de ses systèmes et qui sait protéger ses savoirs, ses données numériques et les échanges automatisés avec ses partenaires, fournisseurs et clients, aura intérêt à protéger et à défendre son activité de production et de commercialisation pour protéger son business et fidéliser la confiance de ses clients. La cyberdéfense devient alors un avantage commercial en sachant communiquer sur la maitrise du numérique et sur la capacité à s'adapter à la numérisation des nouveaux métiers pour des nouveaux marchés.

- Les entreprises doivent se plier, année après année, à des contraintes réglementaires et juridiques de plus en plus nombreuses. Par exemple, elles doivent satisfaire des obligations sur la protection des données personnelles. En effet, depuis le 25 mai 2018, la protection des données personnelles est renforcée par le Règlement Général sur la Protection des données (RGPD ou GDPR en anglais). Elle impose notamment de tenir un registre des traitements mis en œuvre et de notifier les failles de sécurité aux autorités et aux personnes concernées. Pour toutes les données sensibles, une étude d'impact devra être menée : caractéristiques du traitement, risques et mesures adoptées. Une obligation lourde, assortie d'une sanction s'élevant de 2 à 4% du chiffre d'affaire mondial, à laquelle toutes les entreprises devront se soumettre.

LES DIRIGEANTS TERGIVERSENT : « LA CYBERDEFENSE EST-ELLE UN ATOUT POUR LA CREDIBILITE DE MON ENTREPRISE ? » (SUITE)

Pour relever le défi de la cyberdéfense de leurs entreprises, les dirigeants d'entreprise doivent réaliser que la cyberdéfense peut être un atout compétitif.

Ils ont aussi besoin :

✓ De comprendre les termes employés dans le domaine « cyber », c'est l'objectif du chapitre 1 de ce guide pratique,

✓ De connaitre le panorama de la menace et des vulnérabilités concernant leurs systèmes, c'est l'objectif du chapitre 2,

✓ D'identifier les enjeux majeurs de la cyberdéfense de leurs entreprises, c'est l'objectif du chapitre 3,

✓ D'une démarche d'auto diagnostic du niveau du dirigeant d'autant plus simple à mettre en œuvre que leur temps est compté : c'est l'objectif du chapitre 4.

Synthèse

Face aux doutes et aux interrogations des dirigeants des ETI, ce guide pratique propose 4 pistes de réflexion :

01
LA CYBERDÉFENSE, UN FACTEUR DE PÉRENNITÉ

Il est de la responsabilité du dirigeant de décider de protéger et de cyber défendre les systèmes de son entreprise pour améliorer la confiance de ses clients, celle de ses collaborateurs et pour organiser la pérennité de son entreprise compte tenu du niveau des menaces actuelles. (cf. chapitre 2 sur les enjeux et 3 sur les menaces et vulnérabilités).

02
EFFECTUER UN AUTO-DIAGNOSTIC

Le dirigeant doit **conduire lui-même un auto diagnostic** en termes de cyberdéfense de son entreprise. C'est l'affaire de quelques minutes qui lui apprendront des notions clés sur le niveau réel de protection numérique et de cyberdéfense de son entreprise (cf. chapitre 4).

03
LANCEMENT D'UNE DÉMARCHE DE PILOTAGE STRATÉGIQUE DU RISQUE « CYBER »

Le dirigeant doit lancer une démarche de pilotage stratégique de prise en compte du risque « cyber » en trois étapes (cf. chapitre 5). Il peut la réaliser avec un collaborateur de confiance (RSSI, DSI, …). **Il est de la responsabilité du dirigeant de décider, face aux risques, des traitements à opérer et des responsabilités en charge des traitements.**

04
ORGANISER UNE SURVEILLANCE PERMANENTE DU SI

L'entreprise doit **organiser une surveillance permanente de ses systèmes en assurant le maintien en condition de sécurité et en permettant de détecter au plus vite les incidents**. Elle doit conduire une analyse détaillée des évènements intervenant dans le système afin de réagir rapidement en cas d'attaque (cf. Conclusion).

Chapitre 1 : décryptage du domaine « cyber »

L'objectif de ce premier thème est de donner quelques définitions pour avoir des repères clairs dans le domaine du « cyber ». Beaucoup de personnes pensent que le domaine du « cyber » est celui de la sécurité informatique.

En fait, le domaine du « cyber » est pluridisciplinaire car il intègre :

- La sécurité de l'information,
- La sécurité de l'informatique (tout ce qui traite l'information),
- La sécurité des composants électroniques,
- La sécurité des réseaux de communication,
- La sécurité du spectre électromagnétique,
- La sécurité des systèmes et les réseaux de production industrielle,
- La sécurité du big data,
- La sécurité des objets connectés,
- Le volet juridique et le volet éthique spécifique au domaine du « cyber ».

MENACE, VULNERABILITE, ATTAQUE, RISQUE

Face à la diversité des menaces, des vulnérabilités et des attaques et surtout face à la difficulté de les appréhender car elles sont principalement virtuelles donc nos sens humains sont quasi inopérants (on ne peut pas toucher, voir, sentir, écouter…), il est donc important de comprendre les concepts de menace, vulnérabilité, attaque, risque et évènements redoutés.

Le terme « système » dans la suite du document intègre les systèmes et réseaux informatiques et les systèmes et réseaux de production industrielle.

MENACE

Il s’agit d’un danger potentiel qui existe dans l'environnement du système indépendamment de celui-ci. (Exemple : menace potentielle d’orage).

Il y a trois familles de menaces intentionnelles :

Menaces actives : dommage ou altération du système

ex: modification des tables d'un routeur, de la configuration d'un système

Menaces passives :

- Divulgation non autorisée d'information sans que le système soit modifié
- Contrefaçons, atteinte aux fonctionnalités
- écoute de ligne, atteinte aux données, désinformation
- Fraude, indiscrétions

Menaces physiques :

- Vol, sabotage, destruction, incendie
- Détournement

VULNERABILITE

Il s’agit d’une **faiblesse du système** qui le rend sensible à une menace (exemple : trou dans la toiture)

Il existe des vulnérabilités humaines, d’organisation et techniques. Les CERT *(Computer Emergency Response Team, Équipe d'intervention en cas d'urgence informatique)* capitalisent les vulnérabilités techniques connues.

ATTAQUE

Il s’agit du chemin qui permet à une menace d'exploiter une vulnérabilité. C'est une action malveillante qui consiste à contourner les fonctions et mécanismes de sécurité d'un système (exemple : l’orage est avéré et la pluie tombe sur la maison)

RISQUE

Le risque est une combinaison de chaque menace M pouvant exploiter des vulnérabilités V :

∑ (M i * ∑ V ij) (exemple : inondation de la maison)

GESTION DES RISQUES

La gestion des risques est un processus itératif de pilotage, visant à maintenir les risques à un niveau acceptable pour l'organisme.

La gestion des risques inclut typiquement l'appréciation, le traitement, la validation du traitement et la communication relative aux risques.

CONFIDENTIALITE, INTEGRITE ET DISPONIBILITE DES BIENS ESSENTIELS

Les **biens essentiels** sont les informations et les fonctions considérées comme importantes ou sensibles pour l'entreprise dont on appréciera les besoins de sécurité en terme de confidentialité, d'intégrité et de disponibilité.

Evènement redouté : Un évènement redouté est un scénario de menace potentielle représentant une situation crainte par l'entreprise vis-à-vis de ses biens essentiels et analyse de la gravité des impacts. (Exemple de scénario : si l'orage survient et que le toit de la maison n'est pas étanche alors l'inondation de la maison arrivera)

La **confidentialité** est un principe d'observation au niveau système. La confidentialité est la prévention de divulgation non autorisée d'information. Une information confidentielle ne doit être divulguée qu'aux acteurs qui sont autorisés à la connaître. Il peut être nécessaire de définir des niveaux d'habilitation pour les acteurs et des besoins d'en connaître relatifs aux informations confidentielles. (Par exemple : diffusion restreinte, confidentiel personnel, confidentiel médical, confidentiel industrie, confidentiel défense, …)

L'intégrité est un principe d'action au niveau système. L'intégrité est la prévention de modification(s) non autorisée(s) d'information ou de programme. Une information ou un programme ne doit être modifié que par les acteurs qui ont le droit de le faire et dans le respect des règles de gestion du système d'information.

La disponibilité est un principe d'action au niveau système. La disponibilité est la prévention d'un déni de service non autorisé. L'accès aux ressources du système (programmes, informations) doit être garanti aux acteurs quand ils en ont besoin.

CYBER ESPACE

Le cyberespace peut être défini comme un *« domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés ».*

Le cyberespace est un « univers virtuel de la cognition humaine » qui s'appuie sur l'Internet. Il n'y pas vraiment de définition académique du cyberespace. Personne n'a conçu ni réalisé le cyberespace. Personne ne peut vraiment revendiquer sa paternité.

Le cyberespace est un espace mondial virtuel.

Pour simplifier, on peut modéliser le cyberespace comme étant constitué de quatre couches :

COUCHE N°1

Infrastructure mondiale liée à l'interconnexion des réseaux et des ordinateurs qui constituent un maillage de la planète (Internet)

COUCHE N°2

de millions de communications numériques assurées en permanence par des milliards de microprocesseurs qui équipent les réseaux du pouvoir, les systèmes économiques, les systèmes d'armes, militaires, les satellites, les téléphones, les PDA, les télévisions, les systèmes bancaires et boursiers, les systèmes de contrôles industriels (SCADA), les infrastructures de transport aérien, ferroviaire et routier, les systèmes de production de l'énergie, les systèmes de santé, les systèmes d'approvisionnement des grandes surfaces,…

COUCHE N°3

D'un ensemble d'usages et de données numérisées (Big data) constituant un espace mondial informationnel.

COUCHE N°4

L'internaute qui exploite les usages et les données numériques

Le cyberespace peut être analysé par cinq nouvelles propriétés de la cognition humaine :

TRANSFORMATION DE L'ESPACE-TEMPS

Ubiquité : communication peut être établie vers ou reçue de n'importe où et à tout moment

Instantanéité : l'interaction à travers un environnement communicant n'introduit pas de délai supplémentaire : quasi temps réel

Absence de frontière ou déterritorialisé : indifférent à la position géographique des participants (transfrontalier)

TRANSFORMATION DE LA FRONTIÈRE ENTRE LE RÉEL ET LE VIRTUEL

Dématérialisé : constitué de paquets d'électrons voyageurs et non de matière solide

Mise en réseau généralisée à échelle mondiale

Virtualisation : Ce nouvel espace de la cognition humaine ne peut pas être appréhendé uniquement par les 5 sens humains (vue, toucher, odorat, ouïe, goût). Il est principalement virtuel, comme le sont les menaces, les vulnérabilités, les attaques donc les risques. On l'appréhende indirectement par ses effets

NOUVEL ESPACE DE RISQUE

Cette mise en réseau généralisée génère de nouveaux comportements de délinquance : substitutions d'identité, usurpation, CID, authentification, répudiation, anonymisation, cybercriminalité…

ABSENCE DE PATERNITÉ

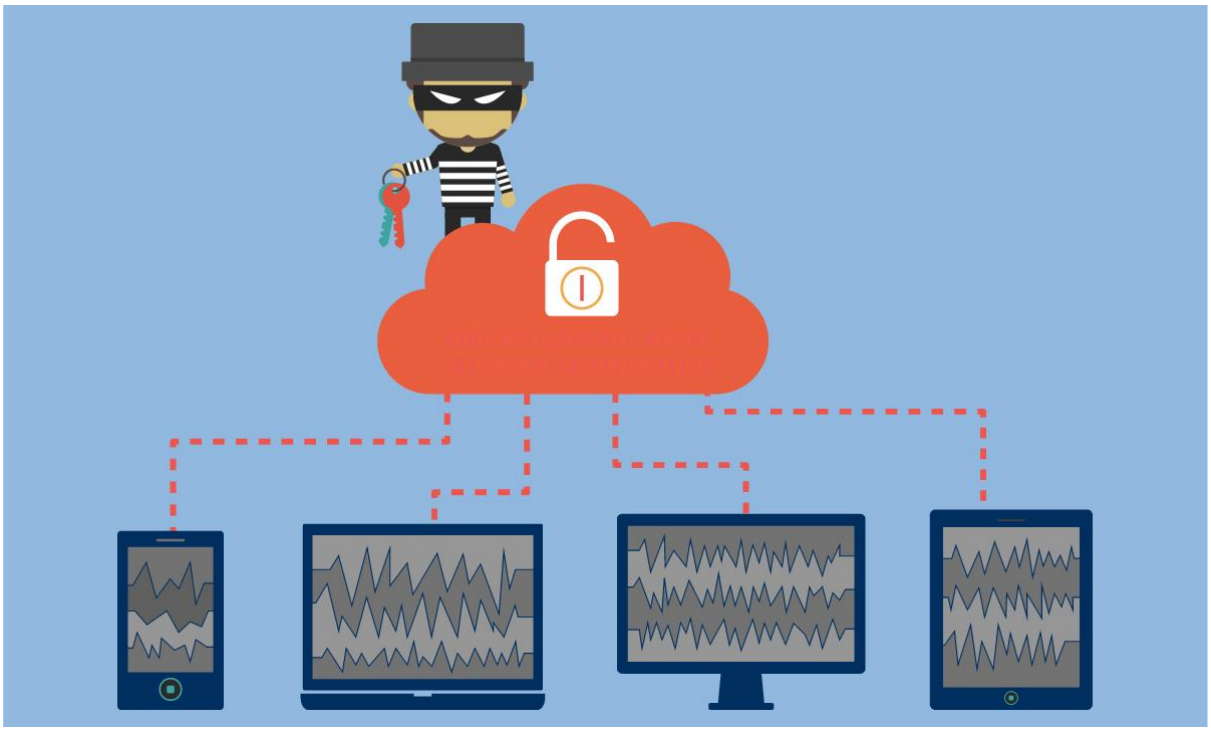
Personne n'a décidé, n'a conçu, ni réalisé le cyberespace

ABSENCE DE MAITRISE ET DE GOUVERNANCE

Personne ne maitrise le cyberespace car il combine des dimensions : internationale, physique, logique, électromagnétique, spatiale, psychologique, cognitive et juridique

CYBER LUTTE

C’est une démarche d’agression systémique dans le cyberespace pour rechercher un effet à obtenir sur une cible.



Un agresseur met en œuvre, d’abord, des stratégies de recherche d’information sur la cible pour la connaitre et identifier ses vulnérabilités et, ensuite, recherchera tous les moyens humains, organisationnels et techniques possibles et efficaces pour atteindre la cible. Enfin, l’agresseur va concevoir, réaliser et mettre en œuvre le vecteur offensif pour traiter la cible et obtenir l’effet escompté. Le cyber lutte est donc un espace d’affrontement numérique entre systèmes offensifs et systèmes défensifs où l’avantage opérationnel est à l’attaquant.

Le respect des lois et de l’éthique reste un sujet d’autant plus délicat à traiter que le périmètre du cyberespace est celui du monde, il s’affranchit donc des frontières.

SECURITE DES SYSTEMES D'INFORMATION

C'est l'ensemble des mesures techniques et organisationnelles visant à protéger un système d'information et à lui permettre de résister à des menaces potentielles susceptibles de compromettre la confidentialité, l'intégrité et la disponibilité de ses informations et des services que ces systèmes offrent.

La SSI est construite à priori par :

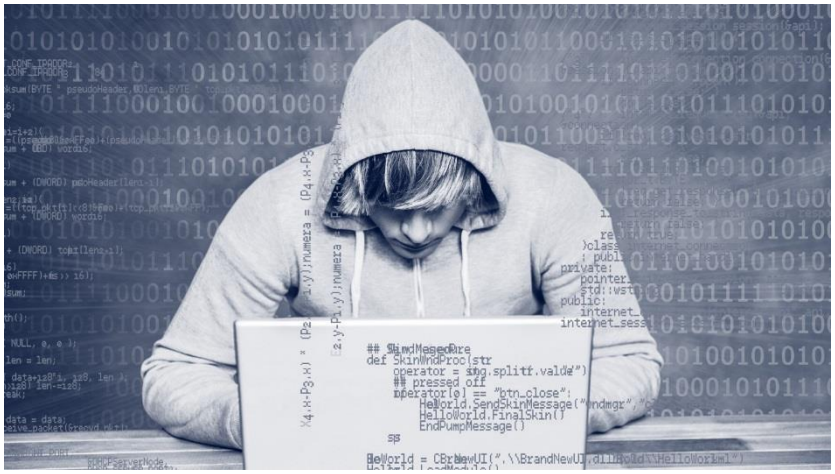
- des méthodes d'analyse de risque (EBIOS, MARION, MEHARI, …) en phase amont de l'ingénierie des systèmes d'information en prenant en compte des menaces et vulnérabilités potentielles et présumées
- une politique de SSI (PSSI) pour protéger la cible de sécurité (ensemble des informations et fonctions sensibles)
- des techniques d'ingénierie des systèmes d'information intégrant des exigences et objectifs de sécurité, des composants et architectures de sécurité, des évaluations et audits de sécurité

Dans les faits, la SSI est positionnée en phase de construction (Build) des systèmes, donc il s'agit d'une :

- capacité de protection statique (ou passive) des systèmes d'information
- capacité de spécification, de conception, de réalisation et de qualification de systèmes de confiance

CYBER CRIMINALITÉ

C’est l’ensemble des actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d’information comme moyens de réalisation d’un délit ou d’un crime, ou les ayant pour cible.



La cybercriminalité intègre deux volets :

LE VOLET TECHNIQUE POUR L’INVESTIGATION NUMERIQUE

est assuré par l’analyse de la menace et par des méthodes d’investigation numérique (« Forensic ») pour rechercher des éléments de preuves ou tenter d’établir la preuve. On peut définir le « Forensic » comme un ensemble de protocoles et de mesures permettant de rechercher des éléments techniques sur un conteneur de données numériques en vue de répondre à un objectif technique en respectant une procédure de préservation du conteneur »: localisation et interprétation de traces numériques

LE VOLET JURIDIQUE POUR L’INSTRUCTION ET LA REPRESSION

s’appuie sur l’arsenal juridique en France sur l’autorité judicaire et sur les experts judicaires en sécurité

CYBER DEFENSE

La cyberdéfense peut se définir comme la défense ou la protection dynamique (et active) des infrastructures critiques ou vitales connectées au cyberespace.

Ces infrastructures concernent les systèmes d'information, les systèmes de communication et les systèmes industriels des Opérateurs d'Infrastructures Vitales (OIV) de notre pays qui sont maintenant massivement interconnectés à l'Internet, menacés de ce fait par l'arsenal des risques qu'il véhicule.

La cyberdéfense est l'ensemble des activités opérationnelles et dynamiques pouvant être conduites dans un contexte de gestion de crise afin de décider du mode opératoire au sein des systèmes à protéger ou d'intervenir dans le cyberespace pour **garantir la défense et la résilience** des systèmes face à des cyber attaques ou des systèmes d'attaques avérées.

Dans les faits, la cyberdéfense est positionnée en phase de d'exploitation et de supervision (RUN) des systèmes, donc elle regroupe :

UNE CAPACITÉ DE DÉFENSE AVEC

- la protection dynamique et permanente des systèmes (systèmes d'information et systèmes de production)
- la gestion de crise cybernétique (centres opérationnels de la cyberdéfense : SOC)
- la défense active en profondeur avec une capacité de lutte dans le cyberespace dans le respect de la loi

UNE CAPACITÉ DE RESILIENCE

(continuité des services : PCA, PRA, plan de secours, dévolution…)

La cyberdéfense :

- prend en compte la **protection globale de la chaine de confiance du numérique**
- s'appuie sur le cycle de vie suivant : **Prévention / Détection / Réaction (civil) ou Veille / Alerte / Réponse (militaire)**

CYBER DEFENSE

Le SGDSN/ANSSI est l'autorité nationale en cyberdéfense : doctrine et la politique nationale. Les 12 secteurs d'activités d'importance vitale sont définis par le SGDSN:

Secteurs Étatiques

ACTIVITÉS CIVILES DE L'ETAT
ACTIVITÉS MILITAIRES DE L'ETAT ACTIVITÉS JUDICIAIRES
ESPACE ET RECHERCHE

Secteurs de la protection des citoyens

SANTÉ,
GESTION DE L'EAU,
ALIMENTATION

Secteurs de la vie économique et sociale de la nation

ENERGIE
COMMUNICATION ÉLECTRONIQUE AUDIOVISUEL ET INFORMATION TRANSPORTS
FINANCE
INDUSTRIE

Il est important de comprendre que la cyberdéfense d'une entreprise (RUN des systèmes), qui est une aptitude de protection dynamique, permanente et résiliente des systèmes massivement connectés au cyberespace, ne peut exister que s'il y a eu lors de la phase d'ingénierie de ces systèmes (BUILD des systèmes) une étude de sécurité pour protéger le patrimoine informationnel (biens essentiels) de l'entreprise (Sécurité des Systèmes d'Information : SSI).

Il faut savoir que sans construction de la SSI préalable, il ne peut pas y avoir de cyberdéfense d'un système.

CYBER DEFENSE

On peut distinguer quatre niveaux de maturité dans la cyberdéfense de son entreprise:

01 CYBERDÉFENSE BASIQUE (B)

(mesures basiques de première nécessité)

02 CYBERDÉFENSE STRUCTURANTE (S)

(mesures structurantes de protection)

03 CYBERDÉFENSE DYNAMIQUE (D)

(mesures de sécurité dynamique)

04 CYBERDÉFENSE RESILIENTE (R)

(mesures de continuité d'activité et d'amélioration continue)

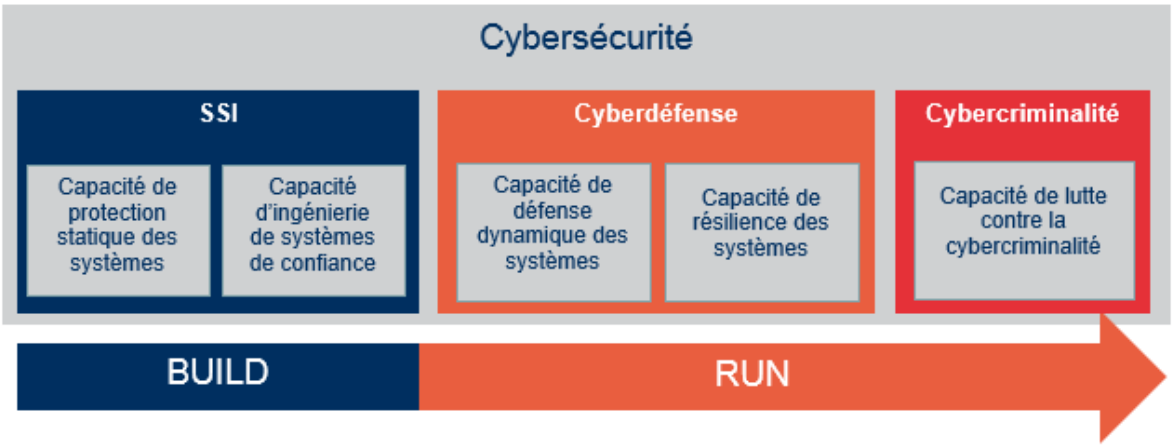
Enfin, pour évaluer la cyberdéfense d'une entreprise, il faut se mettre dans la peau d'un agresseur pour auditer, depuis l'extérieur, la résistance des dispositifs défensifs des systèmes de sa propre entreprise (approche Pentest ou audit actif).

CYBER SECURITE

C'est l'état recherché pour un système lui permettant de résister à des évènements potentiels et/ou avérés issus du cyberespace susceptibles de compromettre sa confidentialité, son intégrité ou sa disponibilité de ses informations et des services que ces systèmes offrent.

Dans les faits, la cyber sécurité regroupe :

- la protection statique des systèmes face à des menaces potentielles donc la SSI
- la protection dynamique et résilience des systèmes face à des menaces avérées donc la cyberdéfense
- la lutte contre la cybercriminalité (volet répressif)

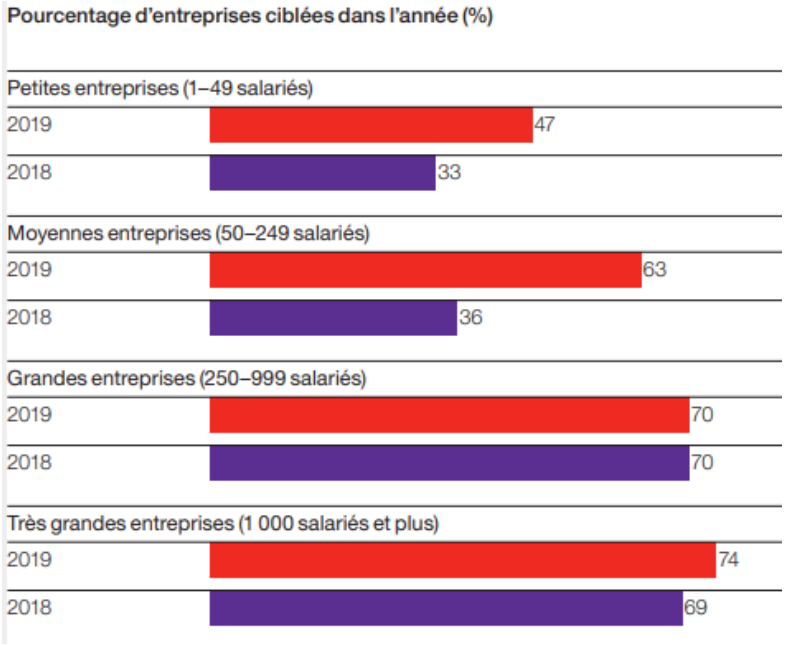


Chapitre 2 : panorama des menaces et des vulnérabilités des ETI en 2019

UN ETAT DES LIEUX DES PME ET ETI EN 2019

Il est difficile d'avoir des données fiables en terme de sécurité des PME et ETI en France car il n'y a pas de recensement officiel. L'état des lieux est donc basé sur une étude Hiscox 2019 qui nous montre que le rique Cyber est important quel que soit la dimension de l'entreprise.

Si les entreprises de grande taille restent celles qui sont le plus susceptibles d'être touchées, la proportion d'entreprises de moins de 50 employés ayant déclaré un cyber-incident est passée de 33% à 47%. Ce chiffre a progressé de 36% à 63% pour les entreprises de taille moyenne (50-249 employés).



D'autres sources, provenant de la déclaration des fournisseurs d'accès internet, indiquent des chiffres plus inquiétants : on peut estimer que pour 100 entreprises matures sachant gérer la sécurité numérique, il y a 2000 entreprises qui sont seulement conscientes des risques sans le gérer et 400 000 entreprises fragiles car démunies : ce sont principalement les PME et ETI.

Selon ces sources, les PME et ETI nationales sont en danger numérique car seulement une sur 4000 serait protégée !

Source : https://www.hiscox.fr/courtage/sites/courtage/files/documents/rapport_hiscox_gestion_cyber_risques.pdf

UN ETAT DES LIEUX DES PME ET ETI EN FRANCE

Il faut savoir qu'il y a des données personnelles et sensibles un peu partout dans les entreprises et que l'annuaire central d'entreprise (Active directory ou LDAP) et les Smartphones de l'encadrement restent les objets les plus convoités par les cyberattaques.

Il ne faut pas perdre de vue que le fournisseur d'accès Internet est la première ligne défensive de l'entreprise car elle est connectée à l'Internet par son intermédiaire. Il est donc important de connaitre les services de sécurité que le fournisseur met en œuvre pour protéger l'entreprise (anti spam, anti virus, IDS, IPS, anti DDOS…).

Près de la moitié (46 %) des incidents de sécurité informatique sont causés par les salariés au sein de l'entreprise.

Selon l'étude IFOP d'octobre 2019, seuls 32% des dirigeants d'ETI estiment que leur entreprise est tout à fait préparée pour affronter une crise cyber mais 89% des sondés se disent préparés et ce, quel que soit le niveau estimé d'exposition au risque...

Cependant, parmi les 32% « certains d'être préparés à affronter une attaque cyber », 53% considèrent être faiblement voire nullement exposés au risque cyber...

Ceci est d'autant plus étonnant que les mesures et les moyens à mettre en œuvre pour affronter une crise cyber supposent un niveau de maturité élevé quant à l'appréhension de ce risque et des investissements à réaliser pour le maîtriser...

LES MENACES

Le recensement et l'analyse de la menace sont aussi des sujets complexes à cerner. On peut noter les informations suivantes :

Certains groupes français annoncent qu'ils détectent plusieurs dizaines de cyberattaques /seconde

35% des incidents de cybersécurité sont dus à des collaborateurs internes à l'entreprise. (source PWC)

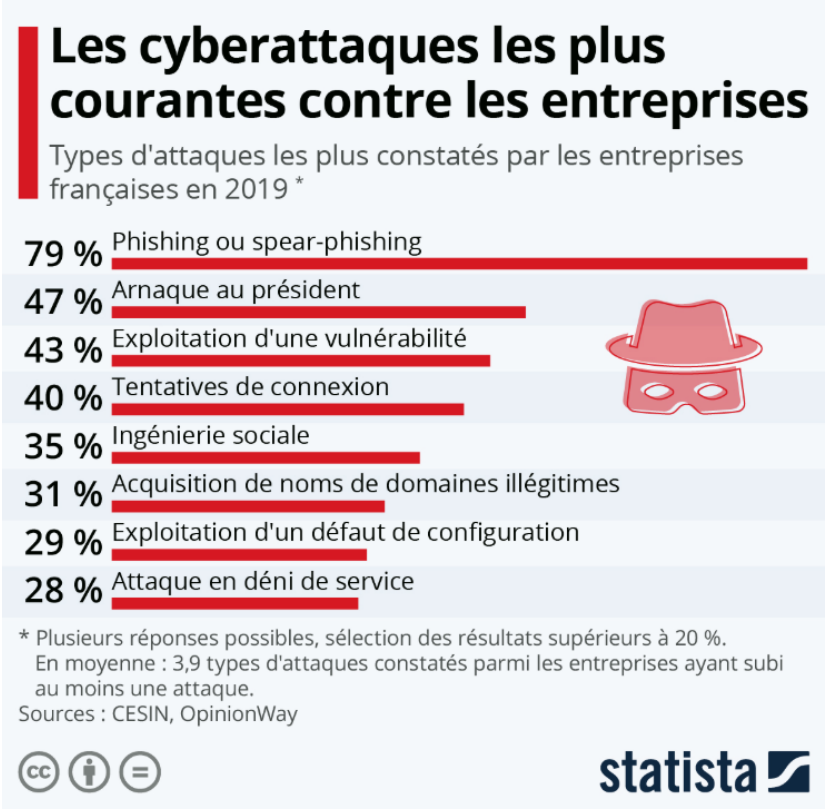
Il faut en moyenne 7 mois à une entreprise pour détecter une violation de données, et 75 jours pour reprendre une activité normale et sécurisé après une attaque

91 % des cyber-attaques démarrent par un E-Mail

Plus de 30% des infections par Ransomwares sont liés à des mots de passe faibles.

81 % des entreprises ont été visées par une cyberattaque et 61% des entreprises estiment avoir subi un impact financier et 38% en terme d'image

Le coût moyen d'une cyberattaque est de 800 000€ pour les entreprises



Sources : https://www.chubb.com/fr-fr/_assets/documents/20190129_chubb_-risques-emergents_vfinale.pdf

L'impact de la cybercriminalité pour les entreprises est difficile à mesurer car les victimes gardent le silence. Il est fortement croissant et probablement sous-estimé dans ce schéma.

LES PERTES

Le montant moyen des pertes financières annoncées par les entreprises sur la base de l'auto déclaration est de **1,5 M€/an.**

Le document « anticipation, stratégie contre la cybercriminalité » du ministère de l'intérieur annonce que le coût moyen d'une cyberattaque est de 300 000€ pour une entreprise de moins de 1000 salariés et de 1 300 000€ si plus de 5000 salariés. Il annonce aussi qu'il faut en moyenne 9 semaines pour réparer les dommages. Ces résultats intéressants sont collectés grâce à une plateforme pluri partenaires qui permet la plainte en ligne et le signalement à la police judicaire.

On constate aisément que la transparence n'est pas de mise actuellement. On comprend aussi les raisons qui poussent les entreprises à ne pas dévoiler la situation réelle compte tenu de l'impact négatif que cela pourrait occasionner chez leurs clients.

LES INVESTISSEMENTS

Il est intéressant de noter que 5 à 10 % du budget global de l'entreprise devrait être alloué à la cybersécurité. C'est en tout cas l'estimation de Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui précise : « oui, la sécurité a un coût, mais ce n'est pas grand-chose comparé au prix à payer lorsqu'on est victime d'une attaque informatique. »

70% des RSSI pensent que les solutions techniques sont en fait assez peu efficaces.

Le niveau des investissements confirme la réalité de la menace et des pertes et il constitue un signal positif pour le marché de la cybersécurité et de la confiance dans la numérisation des entreprises.

LES PRINCIPAUX FAITS REDOUTÉS PAR LES ENTREPRISES

Selon une étude réalisée par InfoPro, les attaques les plus redoutées des entreprises françaises sont les ransomware (53%), l'infection par un logiciel espion (47%), ou la destruction d'information (43%).

LES OBJETS CONNECTES

Le terme d'objets connectés ou d'Internet des Objets (IdO) (en anglais Internet Of Things, IOT) ne fait pas encore consensus sur sa définition, ce qui s'explique par la jeunesse de ce concept en pleine mutation. L'IEEE définit l'IOT comme un « réseau d'éléments chacun muni de capteurs qui sont connectés à Internet ».

Les objets connectés à l'Internet (IOT) envahissent chaque jour un peu plus nos espaces de vie (santé, voiture, chaine alimentaire, sport, habitat …) et ceux de nos entreprises. D'après une étude de Strategy Analytics on estime qu'il y a 22 milliards d'objets connectés à Internet (Internet of Things- IoT) dans le monde.

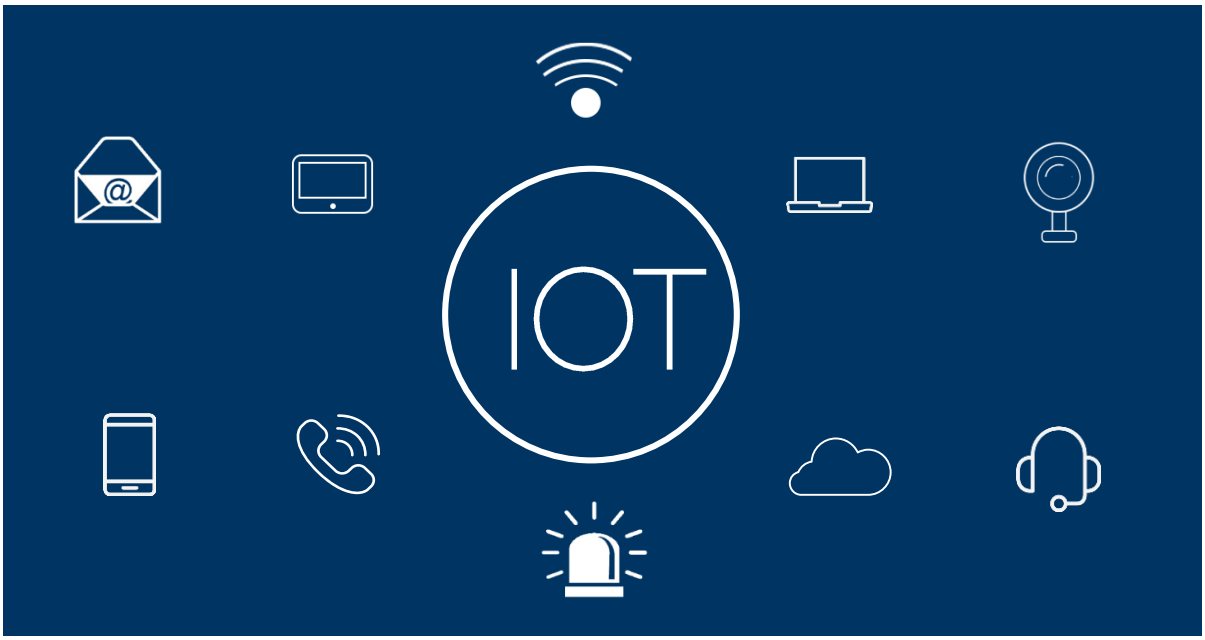
Quant à l'avenir, elle prévoit 38,6 milliards d'appareils connectés d'ici 2025 et 50 milliards d'ici 2030.

Sources : https://www.lesechos.fr/idees-debats/cercle/cyber-securite-tous-mobilises-face-aux-intrusions-malveillantes-992393
https://www.mac4ever.com/actu/143604_il-y-aurait-22-milliards-d-objets-connectes-dans-le-monde-strategy-analytics

LES OBJETS CONNECTES (suite)

La baisse continue des coûts de l'électronique embarqué permet dès aujourd'hui de numériser une partie de votre vie professionnelle et personnelle.

Leur grand nombre constituera une vraie difficulté en terme de recensement et de maitrise technologique. Par exemple, il y aura plus de code informatique dans les IOT des futures voitures que dans un A380.



Les IOT partagent avec les ordinateurs les mêmes vulnérabilités. Ils présentent donc les mêmes risques et les mêmes cyberattaques vis-à-vis des systèmes technologiques avec lesquels ils échangent. De plus, il est difficile actuellement de bien protéger un IOT car il y a peu de place et d'énergie dans ce type d'objet pour y intégrer le code de sécurité.

L'objectif principal d'un IOT est **d'offrir un service limité et fiable à très faible coût.** Les IOT ont des interfaces de communication multi protocoles donc complexes à maitriser (les protocoles de communication des IOT ne sont pas tous de type IP, donc Internet). Il n'y a donc pas vraiment d'approche de type « secure by design » pour les IOT à ce jour. Enfin, la détection des attaques via les IOT est à ce stade difficile à opérer compte tenu de la simplicité de l'architecture même de ces objets.

LES OBJETS CONNECTES (suite)

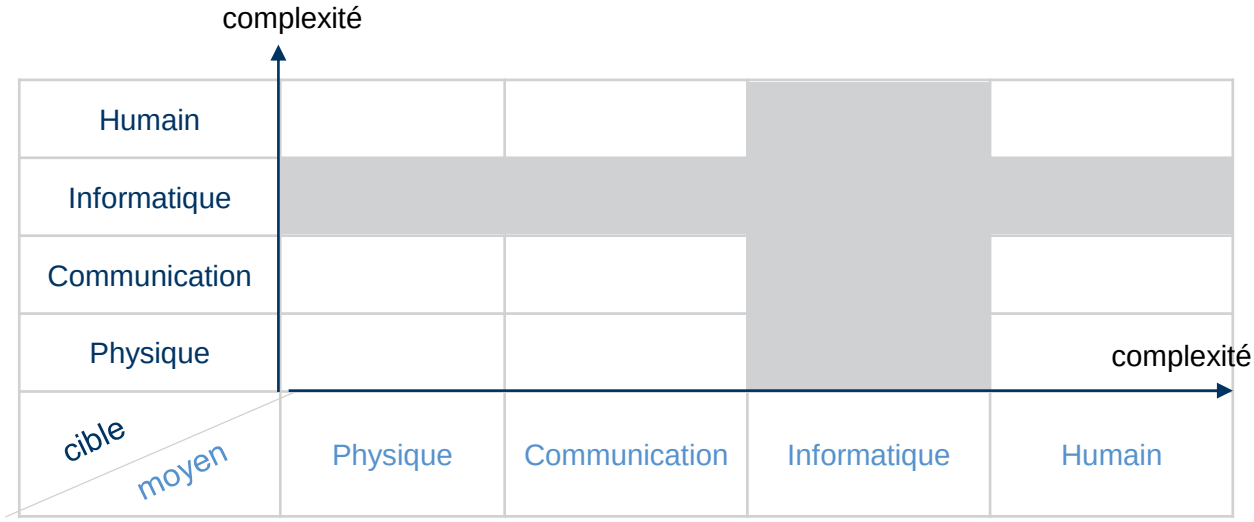
Ces derniers mois, de nombreuses initiatives ont vu le jour. Elles proposent des modèles, des guides et des politiques de sécurité pour l'Internet des Objets (IoT) livres blancs de la GSMA5, de l'ENISA6, de l'ARCEP7, guides IoT de l'OWASP8, etc.

Comme dans tout domaine naissant, émergera avec le temps une bonne pratique couramment acceptée et permettant de définir un socle commun de sécurité pour les objets connectés et leurs infrastructures, comme cela est le cas avec la sécurité des Systèmes d'Information traditionnels, dont l'IoT est devenue une extension. A l'évidence la sécurité des IOT est un défi non résolu à ce jour. Elle reste un enjeu majeur pour les années à venir.

L'ÉVOLUTION DE LA MENACE

La menace s'exprime comme un **danger potentiel** qui existe dans l'environnement du système indépendamment de celui-ci.

En fait, on peut approfondir le concept de menace comme l'application de quatre moyens d'action (humain, informatique, communication et physique) sur quatre cibles (humain, informatique, communication et physique) selon le schéma suivant :



On peut ainsi comprendre que le concept de menace n'est pas réduit au seul moyen informatique sur une cible informatique (comme les virus, les malwares, les rootkit, …) mais qu'il est vaste car il permet de combiner des moyens et des cibles pour obtenir de effets de grande complexité.

Par exemple un moyen informatique peut menacer les quatre cibles : une cible physique par un engin explosif piloté numériquement à distance, une cible de communication comme un réseau IP ou un réseau industriel voir un IOT, une cible informatique comme une APT et une cible humaine par compromission ou social ingénierie.

On comprend ainsi qu'il est difficile de conduire des analyses de la menace et surtout de contrer les cyberattaques. On est passé d'une approche mono moyen-mono cible à une approche multi moyens –multi cibles. Les scénarios opérationnels offensifs qui mettent en œuvre ces approches sont devenus d'une complexité proportionnelle à l'explosion combinatoire des moyens-cibles.

Chapitre 3 : identifier les enjeux majeurs de la cyberdéfense pour les ETI

Les enjeux de la cyberdéfense peuvent s'apprécier à deux niveaux :

LE NIVEAU GLOBAL

Les principaux enjeux globaux sont :

- **Les enjeux de souveraineté nationale et d'intérêt supérieur de la nation**
- **Les enjeux de gouvernance mondiale du cyberespace**
- **Les enjeux de maitrise technologique du cyberespace :**

→ Maitrise de l'industrie des équipements du réseau Internet
→ Maitrise de l'infrastructure du réseau Internet
→ Maitrise de l'industrie des processeurs et des ordinateurs
→ Maitrise de l'industrie des systèmes d'exploitation de nos ordinateurs
→ Maitrise de l'industrie du logiciel
→ Maitrise de l'industrie des bases de données et annuaires
→ Maitrise des technologies des moteurs de recherche
→ …

- **Les enjeux de confiance dans le cyberespace et dans l'économie numérique**
- **Les enjeux relatifs à la place et la dignité de l'Homme face au cyberespace**

→ L'homme restera-il au centre de ce nouvel espace mondial virtuel ?
→ Le cyberespace restera-t-il au service de l'homme en agissant pour le bien de l'humanité ?
→ L'homme maitrisera-il son invention dans le court moyen terme ?
→ Transhumanisme : évolution de la relation entre l'homme et la machine

Les enjeux de la cyberdéfense peuvent s'apprécier à deux niveaux :

LE NIVEAU ETI

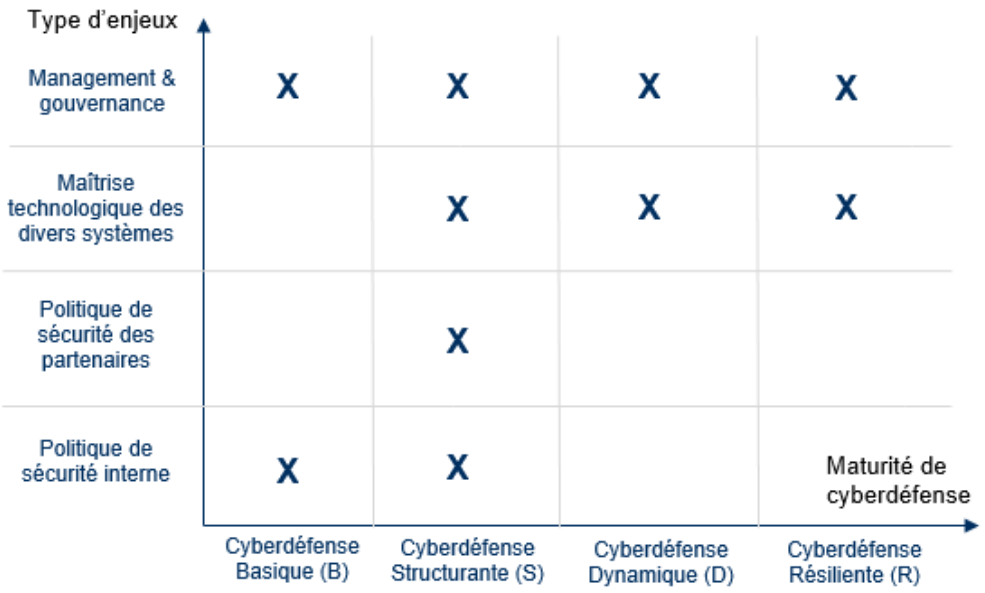
On a vu, dans le chapitre 1, qu'il est possible de structurer la maturité de la cyberdéfense en quatre niveaux :

1. *Cyberdéfense basique (B) (mesures basiques de première nécessité)*
2. *Cyberdéfense structurante (S) (mesures structurantes de protection)*
3. *Cyberdéfense dynamique (D) (mesures de sécurité gérées dynamiquement)*
4. *Cyberdéfense résiliente (R) (mesures de continuité d'activité et d'amélioration continue)*

Les enjeux des ETI peuvent être classés en quatre types

01	02	03	04
Politique de sécurité interne à l'entreprise	Politique de sécurité relative aux partenaires	Maitrise technologique des divers systèmes	Management et gouvernance

On obtient la matrice suivante :



Chapitre 4 : réaliser un auto diagnostic « cyber »

Avant toute chose, il est important de pouvoir se situer dans la prise en compte de la maturité de la sécurité numérique et de la cyberdéfense de son entreprise.

L'objectif de ce quatrième chapitre est de proposer une démarche méthodologique pragmatique, très simple à mettre en œuvre sous la forme d'un auto diagnostic « cyber » **à réaliser par le dirigeant lui-même**.

Cet auto diagnostic prend peu de temps (environ 15-30 mn) et doit être fait par le dirigeant lui-même, avec son équipe de direction, pour montrer son implication et pour qu'il découvre, par lui-même, le niveau réel de protection numérique et de cyberdéfense de son entreprise.

La grille ci-dessous présente un exemple d'auto diagnostic qui propose **2 à 4 questions relatives** aux **10 domaines clés** suivants :

1. Stratégie- Finalité
2. Maitrise des biens essentiels
3. Maitrise Politique, organisationnelle, gouvernance
4. Maitrise juridique
5. Maitrise des ressources humaines
6. Maitrise de la sécurité technique
7. Maitrise Assurance
8. Maitrise du traitement des incidents
9. Maitrise de la continuité d'activité
10. Conformité et audit

Cette grille permet aussi d'apprécier le niveau de maturité cyberdéfense d'une entreprise :

1. Cyberdéfense basique (B) (mesures basiques de première nécessité)
2. Cyberdéfense structurante (S) (mesures structurantes de protection)
3. Cyberdéfense dynamique (D) (mesures de sécurité gérées dynamiquement)
4. Cyberdéfense résiliente (R) (mesures de continuité d'activité et d'amélioration continue)

Pour ces 4 niveaux de cyberdéfense, la grille établit **un bilan par maturité cyberdéfense, une note de maturité et un graphique.**

Avec ce guide, il est livré un **outil logiciel d'auto diagnostic** pour automatiser le travail :

Sur l'onglet n°1 (auto diagnostic)

se trouve les questions classées par domaine. Pour chaque question il y a quatre types de réponses possibles : « oui », « plutôt oui », « non », « plutôt non ».

L'outil calcule automatiquement la note sur une échelle de 0 à 4 pour chaque question et calcule la synthèse des réponses pour chacun des 10 domaines sur une échelle de 0 à 4.

Sur l'onglet n°2 (bilan domaine)

se trouve un bilan par domaine, une note moyenne par domaine et un graphique « radar ».

Sur l'onglet n°3 (bilan maturité cyberdéfense)

se trouve un bilan par maturité cyberdéfense, une note de maturité et un graphique. Ainsi l'auto diagnostic « cyber » permet à l'entreprise d'établir un double bilan par domaine et par maturité de la cyberdéfense.

Questionnaire d'autodiagnostic du dirigeant de l'entreprise

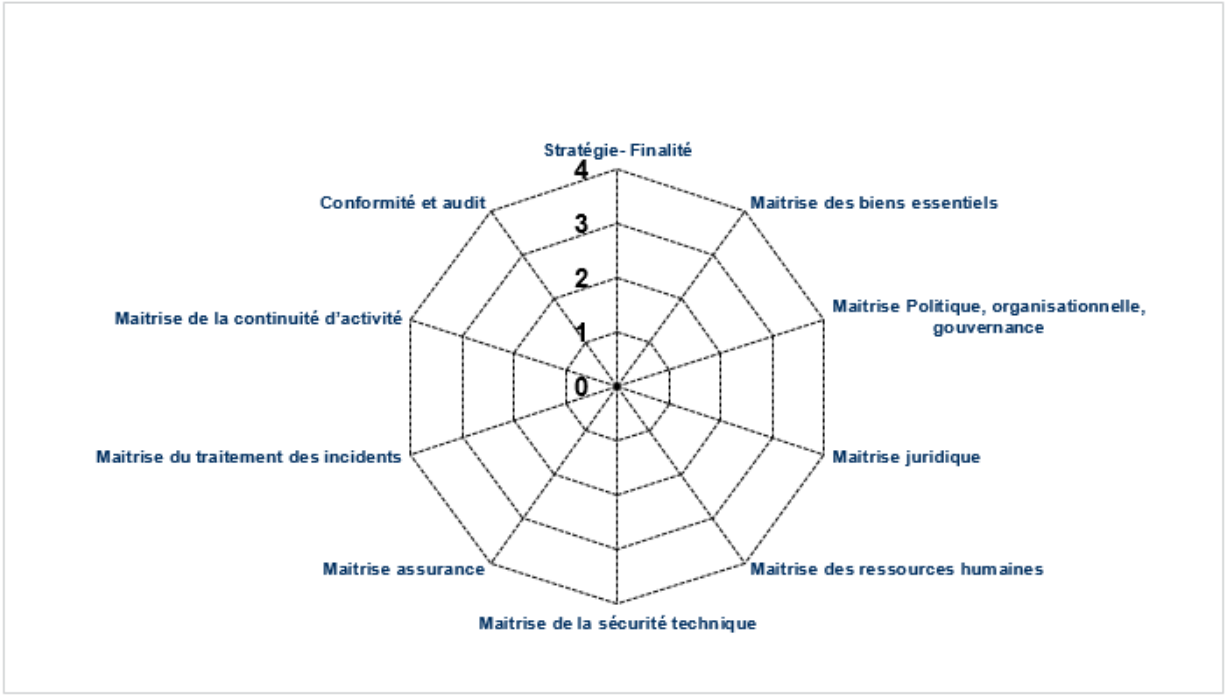
Domaine	Question pour le dirigeant	Réponse	Note	Synthèse par domaine
Stratégie- Finalité	La prise en compte de la cybersécurité est-elle une valeur ajoutée qui va contribuer au développement de mon entreprise?		N/A	0.00
	Ai-je connaissance des risques et des impacts qui concernent mon entreprise en terme de perte de client, d'image, d'informatique, risque juridique...?		N/A	
	Ai-je défini et formalisé les évenements redoutés qui concernent mon entreprise?		N/A	
	Ai-je connaissace d'une démarche qui permet de protéger numériquement de mon entreprise?		N/A	
Maitrise des biens essentiels	Ai-je une connaissance du systeme d'information et/ou de production de mon entreprise (fonction metiers, localisation)?		N/A	0.00
	Ai-je formalisé une cartographie du systeme d'information et/ou de production de mon entreprise?		N/A	
	Ai-je identifié les biens essentiels à proteger dans mon entreprise?		N/A	
	Ai-je formaliser et mis en œuvre une politique des droits d'accès pour protéger les biens essentiels de mon entreprise?		N/A	
Maitrise Politique, organisationnelle, gouvernance	Ai-je défini et formalisé une organisation dédiée à la sécurité avec des procédures d'applications écrites ?		N/A	0.00
	Ai-je défini et formalisé les acteurs en charge de la sécurité clairement identifiés (RSSI, responsable de la gestion des incidents et de crise)?		N/A	
	Ai-je défini et formalisé les responsabilités en terme de sécurité?		N/A	
	Suis-je impliqué pour définir et piloter le changement en terme de prise en compte de la sécurité?		N/A	
Maitrise juridique	Ai-je défini et formalisé des clauses de sécurité dans les contrats des salariés?		N/A	0.00
	Ai-je défini et formalisé des clauses de sécurité dans le reglement intérieur?		N/A	
	Ai-je défini et formalisé une charte de sécurité?		N/A	
	Ai-je défini et formalisé des clauses de sécurité pour les sous-traitants?		N/A	
Maitrise des ressources humaines	Ai-je défini et mise en œuvre une sensibilisation des personnes tenant les postes clés (équipe de direction, cadres)?		N/A	0.00
	Ai-je défini et mise en œuvre une sensibilisation des personnes gérant des informations sensibles du système d'information et/ou de production?		N/A	
	Ai-je défini et mise en œuvre une gestion des arrivées, mutations et des départs des personnes détenteurs d'informations sensibles?		N/A	
	Ai-je défini et mise en œuvre une gestion du personnel non permanent (stagiaires, intérimaires, prestataires...)		N/A	
Maitrise de la sécurité technique	Ai-je défini et mise en œuvre des moyens de sécurité physique pour protéger mon entreprise (GTB, locaux sécurisé, ZRR, contrôle d'accès ...)?		N/A	0.00
	Ai-je défini et mise en œuvre des moyens de protection du parc informatique de mon entreprise (sauvegarde, authentification, gestion des comptes, sécurité des ordinateurs ...)?		N/A	
	Ai-je défini et mise en œuvre des moyens de protection des services du niveau middleware (messagerie, annuaire d'entreprise, bases de données)?		N/A	
	Ai-je défini et mise en œuvre des moyens de sécurité des réseaux pour protéger mon entreprise (firewall, cloisonnement des réseaux, filtrage des flux, WIFI ...)?		N/A	
	Ai-je défini et mise en œuvre des moyens de sécurité réseaux pour protéger les communications extérieures avec les partenaires et les salariés nomades ?		N/A	
	Ai-je défini et mise en œuvre des moyens de protection du système automatisé de production de mon entreprise		N/A	
	Ai-je défini et mise en œuvre des moyens de sécurité téléphonique pour protéger mon entreprise (sécurité des smartphones, codes d'accès téléphoniques, autocomutateur ...)?		N/A	

Il est recommandé de faire cet auto diagnostic tous les ans pour mesurer la progression de l'entreprise

Bilan de l'autodiagnostic par domaine de la cyberdéfense de l'entreprise

Domaine de cyberdéfense	Synthèse/4
Stratégie- Finalité	0.0
Maitrise des biens essentiels	0.0
Maitrise Politique, organisationnelle, gouvernance	0.0
Maitrise juridique	0.0
Maitrise des ressources humaines	0.0
Maitrise de la sécurité technique	0.0
Maitrise assurance	0.0
Maitrise du traitement des incidents	0.0
Maitrise de la continuité d'activité	0.0
Conformité et audit	0.0

Note moyenne des domaines	0.0 / 4



Conclusion : le rôle du dirigeant dans la cyberdéfense

Face à une cyberattaque, certains dirigeants témoignent de leur désir, dans un premier temps, de vouloir contre attaquer pour se venger des dommages causés par l'attaque. Puis ils se ressaisissent. En effet, le droit français encadre le volet offensif en le réservant à certains domaines réservés de l'Etat. Il n'est donc pas possible aux entreprises d'utiliser, elles-mêmes, un arsenal offensif pour régler ses comptes.

Afin de se prémunir des attaques, les entreprises doivent d'abord sécuriser leurs biens essentiels et ensuite évaluer cycliquement la résistance de ses systèmes aux attaques par des audits techniques et organisationnels et des opérations de « pentest ». L'entreprise doit organiser une surveillance permanente de ses systèmes en assurant le maintien en condition de sécurité et en permettant de détecter au plus vite les incidents. Elle doit conduire une analyse détaillée des évènements intervenant dans le système afin de réagir rapidement en cas d'attaque.

Afin de limiter les conséquences des attaques, les entreprises peuvent superviser dynamiquement la sécurité de leurs systèmes dans le cadre d'un SOC (« Security Operation Center ») interne ou sous-traité. Après une attaque, elles peuvent établir les preuves numériques par des opérations de « Forensic » pour porter plainte ou apporter les preuves à sa compagnie d'assurance. Ces diverses opérations entrent dans le champ de la cyberdéfense des entreprises. Elles doivent être managées comme n'importe quel autre processus de l'entreprise. Le rôle du dirigeant est essentiel pour obtenir l'adhésion de son personnel.

A ce stade, se pose la question de la vision, du leadership et de la gouvernance du dirigeant en matière de cyberdéfense. En effet, un dirigeant qui a une vision dans ce domaine est capable de transformer un frein en un atout pour son entreprise et ses clients. Il permet de donner du sens à l'activité car il sait où il va. Il sait fixer des objectifs et convaincre en interne et en externe.

La prise de décision, l'allocation budgétaire, la mesure, le reporting, la transparence et la responsabilisation sont des attributs clés d'une démarche efficace qui concilie la nécessité de protéger et celle de gérer l'entreprise. La vision du dirigeant inspire la force de l'accomplir par les collaborateurs. Le dirigeant doit donner la vision en permanence pour encourager sa réalisation par ses collaborateurs. C'est lui le pilote pour créer une dynamique de la transformation et d'entretenir la confiance.

Améliorer le leadership et la gouvernance est sans doute plus important que le développement d'outils et de compétences technologiques. Le dirigeant doit initier et conduire le changement de culture. En effet, avec l'accélération provoquée par le numérique et le pouvoir que la technologie donne aux individus, il faut changer le comportement et l'engagement des employés et des clients.

La cyberdéfense doit répondre aux besoins des personnes à travers les changements de culture.

A propos de NXO

Leader indépendant de l'intégration et de la gestion des flux digitaux pour les entreprises et les administrations, NXO conçoit, déploie et exploite des solutions de Communication & Collaboration, Infrastructures digitales et Sécurité. Avec un chiffre d'affaires de 240 m€ et 40 implantations en métropole et dans les DOM-TOM, NXO compte aujourd'hui 1 250 collaborateurs dont l'expertise reconnue permet d'attirer les meilleurs talents.

Pour en savoir plus,

Site web
www.nxo.eu

Contactez-nous
contact@nxo.eu

Retrouvez-nous également sur les réseaux sociaux

NXO France – NextiraOne

NextiraOne (NXO France)

NextiraOne (NXO France)

NXO France – Nextiraone