CYBERSÉCURITÉ

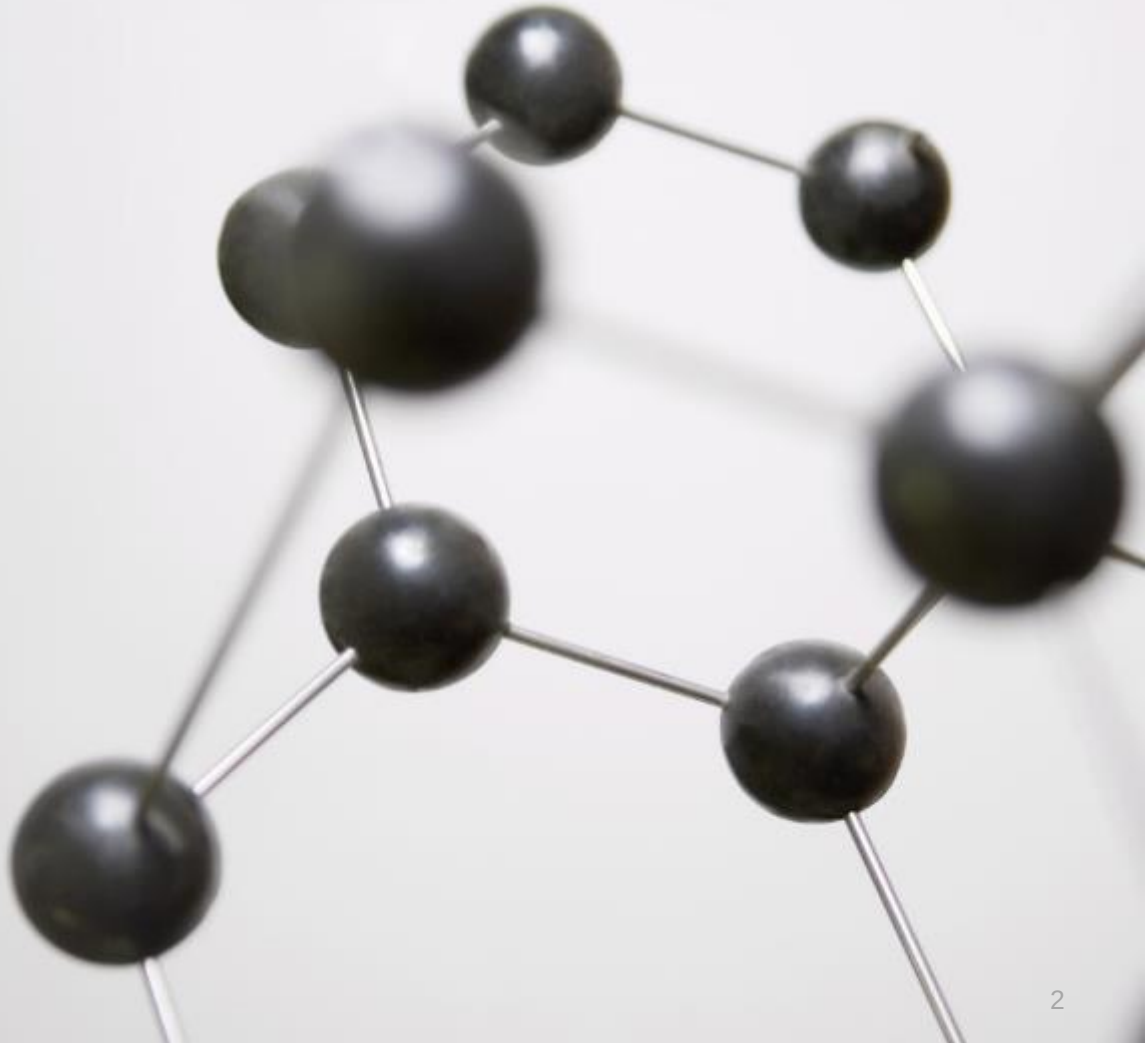
PARTENARIAT FRANCE CHIMIE / ACCENTURE - TRANSFORMATION DIGITALE DE LA CHIMIE

accenture

FRANCE CHIMIE

« Dans le monde de la cybersécurité, la dernière chose que vous voulez est d'avoir une cible dessinée sur vous. »

Tim Cook, 17 mars 2017



SOMMAIRE

PANORAMA SUR LA CYBERSÉCURITÉ

QU'EST-CE QUE C'EST ?

Il s'agit de la pratique consistant à protéger toutes les ressources, dispositifs et structures interconnectés, principalement pour garder en sécurité les informations qu'ils stockent, traitent ou auxquelles ils ont accès.

QUELLE VALEUR APPORTÉE ?

- **PROTÉGER LES RÉSEAUX ET LES DONNÉES** CONTRE LES ACCÈS NON AUTORISÉS
- **AMÉLIORER LA SÉCURITÉ DE L'INFORMATION** ET DE LA GESTION DE LA CONTINUITÉ DES ACTIVITÉS
- **AMÉLIORER LA CONFIANCE DES PARTIES PRENANTES** DANS LES DISPOSITIFS DE SÉCURITÉ DES INFORMATIONS
- **RÉDUIRE LES DÉLAIS DE RECOUVREMENT** EN CAS DE VIOLATION

LE RISQUE AUGMENTE AU FUR ET À MESURE DE L'ÉVOLUTION DES SYSTÈMES, SANS QUE LES CAPACITÉS DE SÉCURITÉ NE SOIENT PRISES EN COMPTE

LE NUMÉRIQUE ÉLARGIT LA SURFACE D'ATTAQUE

L'automatisation, les appareils connectés, les nouvelles capacités IT/OT et les technologies basées sur le cloud sont adoptées - souvent avec peu ou pas de sécurité intégrée.

+

LES ACTEURS DE LA MENACE VISENT NOTAMMENT LA PRODUCTION

Les acteurs de la menace bien financés utilisent des outils et des tactiques sophistiqués pour cibler les entreprises manufacturières à des fins politiques et financières.

=

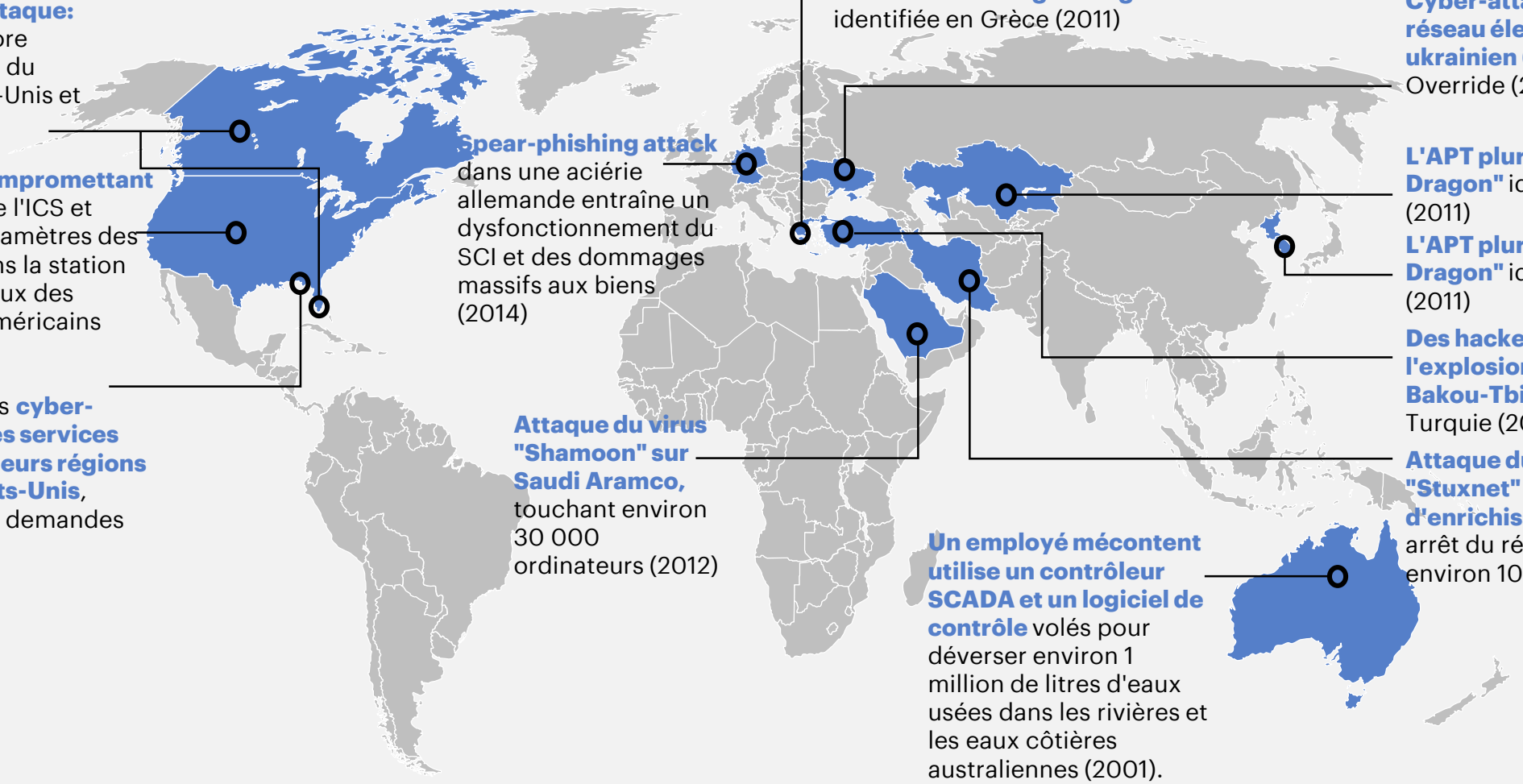
LE RISQUE COMMERCIAL AUGMENTE

Les risques comprennent le vol ou l'altération de la propriété intellectuelle (PI), les problèmes de qualité des produits, les préoccupations relatives à la sécurité des travailleurs ou des consommateurs, les violations de la réglementation et les perturbations opérationnelles.

PANORAMA SUR LA CYBERSÉCURITÉ

LES RÉCENTES CYBER-ATTAQUES CONTRE DES ORGANISATIONS INDUSTRIELLES

LE VOLUME CROISSANT DE CYBERATTAQUES CONTRE LES SCI ET LES INFRASTRUCTURES CRITIQUES CONSTITUE UN **RISQUE RÉEL POUR LES ENTREPRISES CLIENTES ET LES ÉCONOMIES NATIONALES.**



"Ransomware" attaque: installations offshore dans dans le Golfe du Mexique aux Etats-Unis et au Canada (2015)

Cyber-attaque compromettant les composants de l'ICS et manipulant les paramètres des flux chimiques dans la station d'épuration des eaux des services publics américains (2016)

La CIA confirme les **cyber-attaques contre les services publics dans plusieurs régions en dehors des États-Unis**, accompagnées de demandes d'extorsion (2008)

Spear-phishing attack dans une aciérie allemande entraîne un dysfonctionnement du SCI et des dommages massifs aux biens (2014)

Multi-années "Night Dragon" APT identifiée en Grèce (2011)

Attaque du virus "Shamoon" sur Saudi Aramco, touchant environ 30 000 ordinateurs (2012)

Un employé mécontent utilise un contrôleur SCADA et un logiciel de contrôle volés pour déverser environ 1 million de litres d'eaux usées dans les rivières et les eaux côtières australiennes (2001).

Cyber-attaque sur le réseau électrique ukrainien (2015) et Crash Override (2016)

L'APT pluriannuelle "Night Dragon" identifiée au Kazakhstan (2011)

L'APT pluriannuelle "Night Dragon" identifiée à Taiwan (2011)

Des hackers ont provoqué l'explosion d'un pipeline BP Bakou-Tbilissi-Ceyhan en Turquie (2014)

Attaque du logiciel malveillant "Stuxnet" sur l'installation d'enrichissement de l'uranium, arrêt du réseau et touchant environ 10 000 machines (2010)

PANORAMA SUR LA CYBERSÉCURITÉ

LE RISQUE EST RÉEL : LES INFRACTIONS ONT UN IMPACT SUR LES BÉNÉFICES ET LA CHAÎNE D'APPROVISIONNEMENT

À LA SUITE DES RÉCENTES ATTAQUES, **LA SÉCURITÉ EST DÉSORMAIS UNE PRÉOCCUPATION AU NIVEAU DU CONSEIL.**

Hydro

"La cyber-attaque contre Norsk Hydro a coûté près de 52 millions de dollars"

Insurance Journey, 2019

MAERSK

"Selon M. Moller-Maersk, le coût des cyberattaques pourrait atteindre 300 millions de dollars."

Financial Times, Reuters, 2017

SIEMENS

56% des personnes interrogées dans le secteur des services publics s'attendent à une attaque des infrastructures critiques dans les 12 prochains mois

Siemens and Ponemon Institute, 2019

IBM

"Les cyberattaques contre des cibles industrielles ont doublé au cours des 6 derniers mois."

IBM's X-Force IRIS, 2019

Mondelēz International

"La cyber-attaque va réduire de 3% la croissance des revenus du deuxième trimestre."

CNBC, 2017

MERCK

" 30 000 ordinateurs et 7 500 serveurs touchés, soit des pertes totales de 1,3 milliard de dollars "

NotPetya attack, 2017

PANORAMA SUR LA CYBERSÉCURITÉ

QUELLES SONT LES DIFFÉRENTES MENACES?

SCRIPT KIDDIES
Terme dérogatoire désignant les personnes qui utilisent des techniques de piratage mais possédants des compétences limitées, s'appuyant principalement sur des outils automatisés téléchargés sur Internet.

CRIMINALITÉ ORGANISÉE
Le point commun entre ces groupes est le motif (profits illégaux) et l'intention. Leur niveau de compétences est varié et leurs ressources sont plus abondantes que chez les script kiddies ou les hacktivistes.

INSIDERS
Ils peuvent être de n'importe quel niveau de compétences, mais ils ont probablement des connaissances et des autorisations d'accès plus larges que les étrangers. Leurs motivations peuvent varier et leurs ressources ont tendance à être limitées.

HACKTIVISTES
Ils utilisent des techniques de piratage pour atteindre certains objectifs activistes, comme le désaccord éthique. Leurs motivations sont personnelles ou idéologiques et leurs ressources peuvent varier considérablement d'un groupe à l'autre.

ETATS-NATIONS/APT
Les menaces persistantes avancées (APT) utilisent des techniques avancées pendant une longue période. Leurs motivations sont politiques ou économiques, et elles sont exécutées par des attaquants hautement qualifiés disposant de ressources importantes.

CONCURRENTS
L'espionnage d'entreprise est motivé par des raisons financières. Leur niveau de compétence peut varier, mais il est généralement élevé, et les ressources sont généralement importantes (elles peuvent être soutenues par des initiés).

QUELLES VULNÉRABILITÉS?

Une vulnérabilité est la faiblesse causée par une caractéristique/un élément, ou un groupe de caractéristiques, qui peut être utilisé pour accéder à un système ou lui nuire.

Il existe un large éventail de vulnérabilités. Elles sont également connues sous le nom de surface d'attaque.

- Vulnérabilités des réseaux
- Supply Chain
- Fournitures (Services publics)
- Cloud Computing
- Big Data
- Applications et services orientés web
- Systèmes
- Accès physique
- Processus

PANORAMA SUR LA CYBERSÉCURITÉ

L'IMPORTANCE DE LA CYBERSÉCURITÉ

LA CYBERSÉCURITÉ N'EST PAS SEULEMENT UNE QUESTION DE **TECHNOLOGIE**, C'EST AUSSI UNE QUESTION DE **PERSONNES.** LA PRATIQUE DE LA CYBERSÉCURITÉ VISE À PROTÉGER NON SEULEMENT LES INFORMATIONS ET LES BIENS, MAIS AUSSI LES PERSONNES QUI LEUR SONT LIÉES.

CONSÉQUENCES D'UNE CYBERATTAQUE POUR L'ENTREPRISE CONCERNÉE :

- L'arrêt d'une chaîne d'approvisionnement, entraînant des pertes de plusieurs millions de dollars pour une entreprise.
- L'accès et la révélation d'informations stratégiques sur une entreprise, qui la conduit à la faillite.

IMPACT DIRECT SUR LA VIE DES GENS :

- La divulgation d'informations personnelles privées, telles que l'état de santé, les préférences sexuelles, les opinions politiques, etc.
- L'accès à des informations bancaires et le vol d'argent.
- L'accès à des appareils personnels qui peuvent compromettre l'intégrité des personnes, voire leur vie.

QUELS IMPACTS LIÉS AU MANQUE DE SÉCURITÉ?

C — CONFIDENTIALITY

Perte économique :

- Divulgation d'informations commerciales confidentielles, comme une fusion

Perte de réputation :

- Divulgation d'informations personnelles ou privées, comme une affection de santé.

I — INTEGRITY

Perte d'intégrité physique :

- Modification des coordonnées de vol, affectant l'atterrissage

Impact social :

- Modification d'informations politiques, telles que les résultats d'élections.

A — AVAILABILITY

Perte de vies humaines :

- Indisponibilité des dispositifs dans un environnement médical

Qualité de vie :

- Indisponibilité de services d'usage quotidien, tels que les services de transport.

LES PRINCIPAUX ENJEUX MÉTIER ADRESSÉS

SUPPLY CHAIN & LOGISTIQUE
- Suivi de la Supply Chain
- Développement de l'écosystème des partenaires

★★★★

EXCELLENCE INDUSTRIELLE
- Suivi commande temps réel
- Cout et reduction du temps des cycles

★★★★

MAINTENANCE
- Aide à la prise de décision à travers l'advanced Analytics
- Sécurité des employés et équipements industriels

★★★★

VALORISATION DES COMPÉTENCES ET NOUVELLES MÉTHODES DE TRAVAIL
- Optimisation gestion de la main d'œuvre
- Efficacité et gestion du stress des employés

★☆☆☆

R&D
- Développement des compétences
- Optimisation gestion de la main d'œuvre

★★★☆

NOUVEAU BUSINESS MODEL
- Augmentation valeur perçue client
- Amélioration expérience utilisateur

★☆☆☆

LES LACUNES TECHNIQUES TYPIQUES

La visibilité sur l'inventaire et l'utilisation des équipements est souvent limitée

La plupart des réseaux ne sont pas correctement segmentés et sécurisés

Les vulnérabilités sont rarement corrigées de manière cohérente

Les dispositifs/applications ne sont pas toujours conçus de manière sûre

Les environnements ne sont pas efficacement surveillés pour détecter les menaces

Les vulnérabilités du réseau OT ne sont pas atténuées

LES LACUNES LIÉES À DES PROCESSUS

L'obligation de rendre compte, les rôles et les responsabilités sont souvent peu clairs

La gouvernance est rarement bien établie, en particulier dans le domaine de l'AIM et de la gestion du changement

Les questions de succession générationnelle sont associées à un manque d'expertise en matière de sécurité

Souvent, les processus de gestion des mutations industrielles n'intègrent pas - ou ne peuvent pas intégrer - la sécurité

Les plans d'intervention portent sur la maintenance, la réparation et l'exploitation (MRO), mais rarement sur la cybersécurité

Les pratiques ne sont souvent pas normalisées dans les domaines de l'informatique

QUELLES COMPÉTENCES REQUISES?

LA CYBERSECURITE EST UN SUJET QUI DOIT ETRE PORTE PAR LE COMEX

CEO | Chief Executive Officer
Responsable final de la stratégie et des actions entreprises au sein de l'entreprise.

CSO | Chief Security Officer
Responsable de la sécurité de l'organisation, en alignant les intérêts commerciaux sur la conformité des politiques de sécurité interne et externe.

CIO | Chief Information Officer
Responsable des technologies de l'information de l'entreprise, en alignant les stratégies générales sur l'informatique, pour atteindre les objectifs fixés.

CISO | Chief Information Security Officer
Responsable de l'alignement de l'infosec sur les objectifs commerciaux, de l'élaboration et de la supervision de la conformité aux politiques en matière d'infosec.

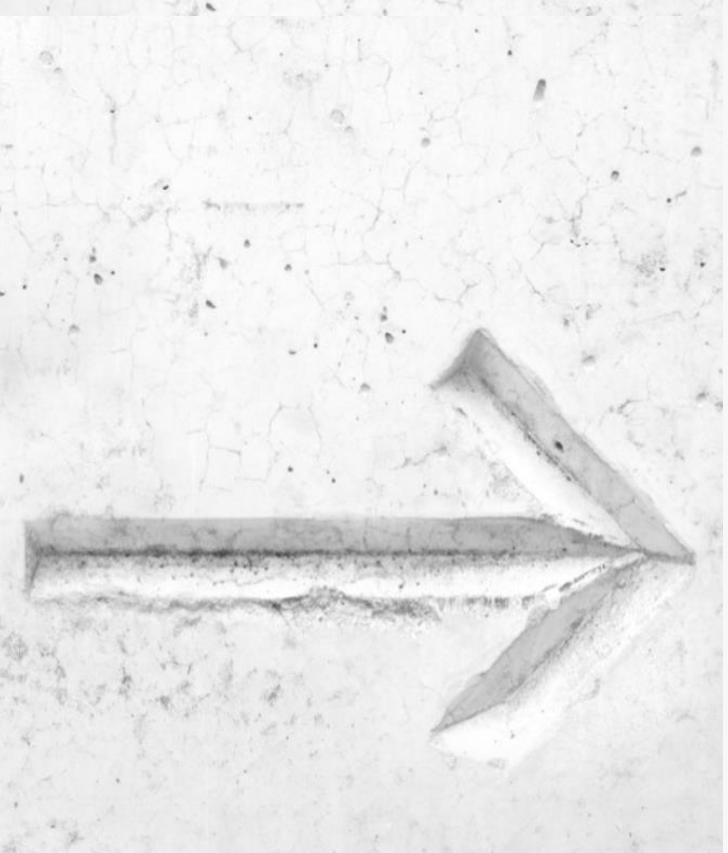
CTO | Chief Technology Officer
Directeur technique chargé de la gestion quotidienne de l'informatique.

SPÉCIALISTES

CONSULTANT EN CYBERSÉCURITÉ
Spécialiste externe qui est engagé pour fournir des conseils ou un soutien dans le cadre d'une activité ou d'un processus de cybersécurité (évaluation des risques, mise en œuvre de mesures de sécurité, équipe SOC, etc.)

ÉQUIPES ROUGE/BLEU
Des spécialistes qui simulent respectivement l'expérience d'une équipe d'attaque/défense.

COMMENT IMPLÉMENTER LA CYBERSÉCURITÉ DANS MON ENTREPRISE?



LES PHASES D'UNE ÉVALUATION DES RISQUES

Une évaluation des risques (RA) est le processus qui consiste à identifier les risques qui peuvent affecter nos processus ou nos infrastructures et à prendre des décisions pour les gérer.

Il existe plusieurs cadres ou lignes directrices qui peuvent être suivis pour la réaliser, mais les étapes les plus courantes sont les suivantes :

1. **Définir le champ d'application** (domaines concernés, processus, systèmes, etc.)
2. **Identifier les outils** (outils physiques et logiques)
3. **Identifier les menaces** affectant le champ d'application sélectionné
4. **Identifier les vulnérabilités** et les **garanties existantes**
5. **Évaluer le risque** (quantifier les pertes possibles et leur probabilité de survenance)
6. **Gérer le risque** (accepter, atténuer, éviter ou transférer)

COMMENT IMPLÉMENTER LA CYBERSÉCURITÉ DANS MON ENTREPRISE?

IMPLEMENTATION D'UNE STRATEGIE DE DEFENSE, LA DEFENSE EN PROFONDEUR

Une cyberdéfense efficace ne consiste pas seulement à tenir les "méchants" à l'écart ! Il faut adopter une stratégie de sécurité de défense en profondeur.

Une stratégie de défense en profondeur garantit que les cyber attaquants doivent pénétrer plusieurs niveaux de cyberdéfense et de mécanismes de surveillance pour accélérer une attaque.

Chaque niveau de défense entravera et ralentira l'attaquant et augmentera la probabilité de détection en surveillant et en corrélant les petits changements qu'ils effectuent afin de faire progresser l'attaque.

Gouvernance de la sécurité

- Rôles, responsabilités, processus et procédures nécessaires à une gouvernance efficace de la sécurité.

Intégrité du système

- Durcissement du système
- Authentification et autorisation du système
- Gestion des correctifs
- Détection d'intrusion
- Protection contre les logiciels malveillants
- Enregistrement des événements de sécurité

Sécurité physique

- Accès physique restreint aux panneaux de contrôle et aux salles
- Surveillance, gardiens, clôtures de périmètre
- Cabinets et salles de données fermés à clé
- Gestion des visiteurs, registres de sécurité physique

Sécurité des réseaux

- Architecture sécurisée
- Segmentation du réseau
- Pare-feu, passerelles bidirectionnelles
- Listes de contrôle d'accès sur les dispositifs de réseau
- Communications cryptées, SSL/TLS, VPN

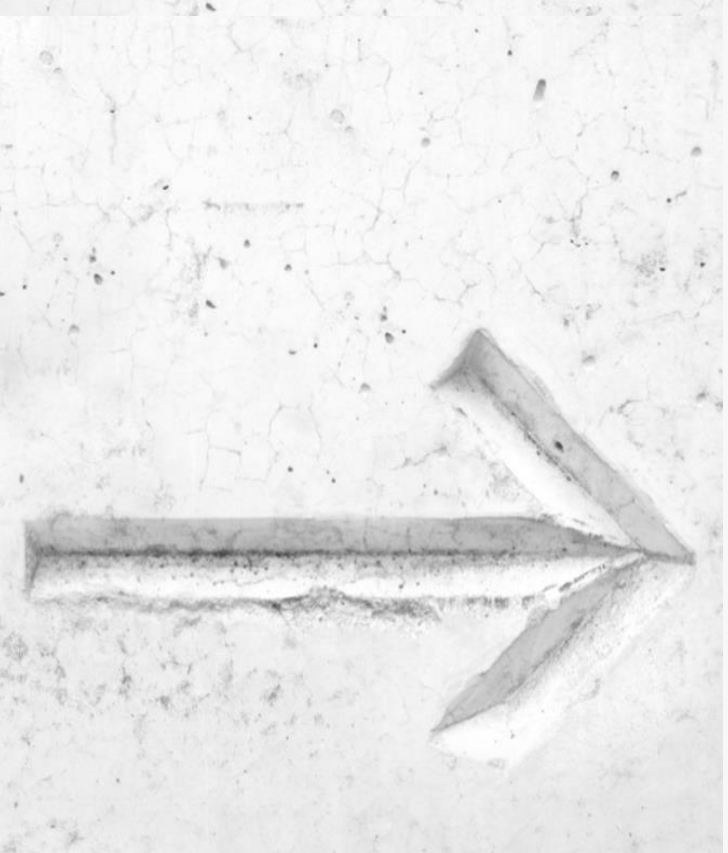
Sécurité du système de contrôle industrie

- Contrôle d'accès
- Audit automatisé des dispositifs
- Détection des anomalies

Application sécurité

- Liste blanche des candidatures
- Contrôle de la configuration
- Authentification et autorisation
- Gestion des correctifs
- Audit

COMMENT IMPLÉMENTER LA CYBERSÉCURITÉ DANS MON ENTREPRISE?



EXEMPLE DE MODÈLE OPÉRATIONNEL OT

Modèle de fonctionnement des Principales catégories

Modèle opérationnel de contrôle des sous-catégories pour une meilleure vue d'ensemble et la conformité avec les directives de la NIST

Alignement des entreprises

Gouvernance de la sécurité

Sécurité architecture

Cybersecurité Business & Governance

Management Cybersécurité

Operations Cybersécurité

Ressources securité

Management de la sécurité

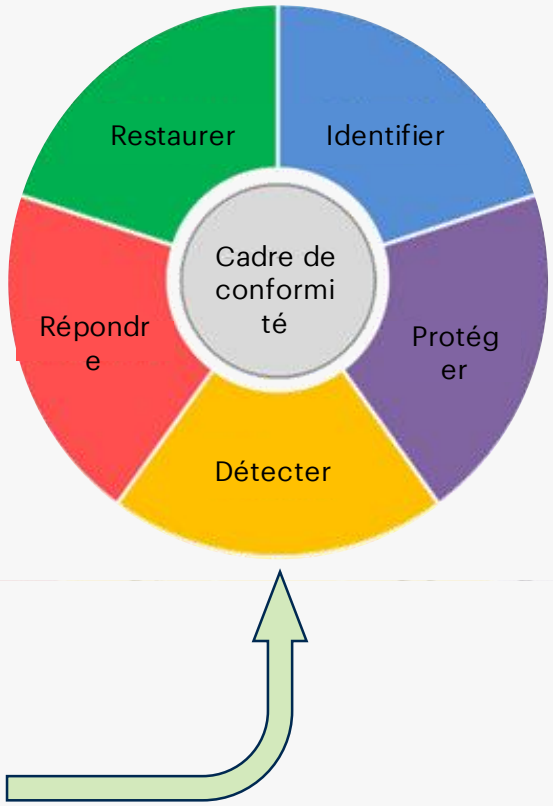
- Programme de sécurité, feuille de route et amélioration continue
- Information sécurité gestion des risques
- Gestion de la conformité en matière de sécurité
- Formation et sensibilisation à la sécurité

Sécurité des opérations

- Gestion des menaces et des vulnérabilités
- Sécurité des infrastructures & applications
- Gestion et réponse aux incidents de sécurité
- Surveillance de la sécurité, analyses, mesures et rapports
- Gestion des identités et des accès

Ressources sécurité

- IT/OT & HR Ressource Management
- Sécurité Supply Chain
- Sécurité physique



QUELQUES CAS D'USAGE POUR ILLUSTRER

ÉVALUATION DES RISQUES DE CYBERSÉCURITÉ POUR UNE SOCIÉTÉ BIOPHARMACEUTIQUE

QUEL BESOIN?

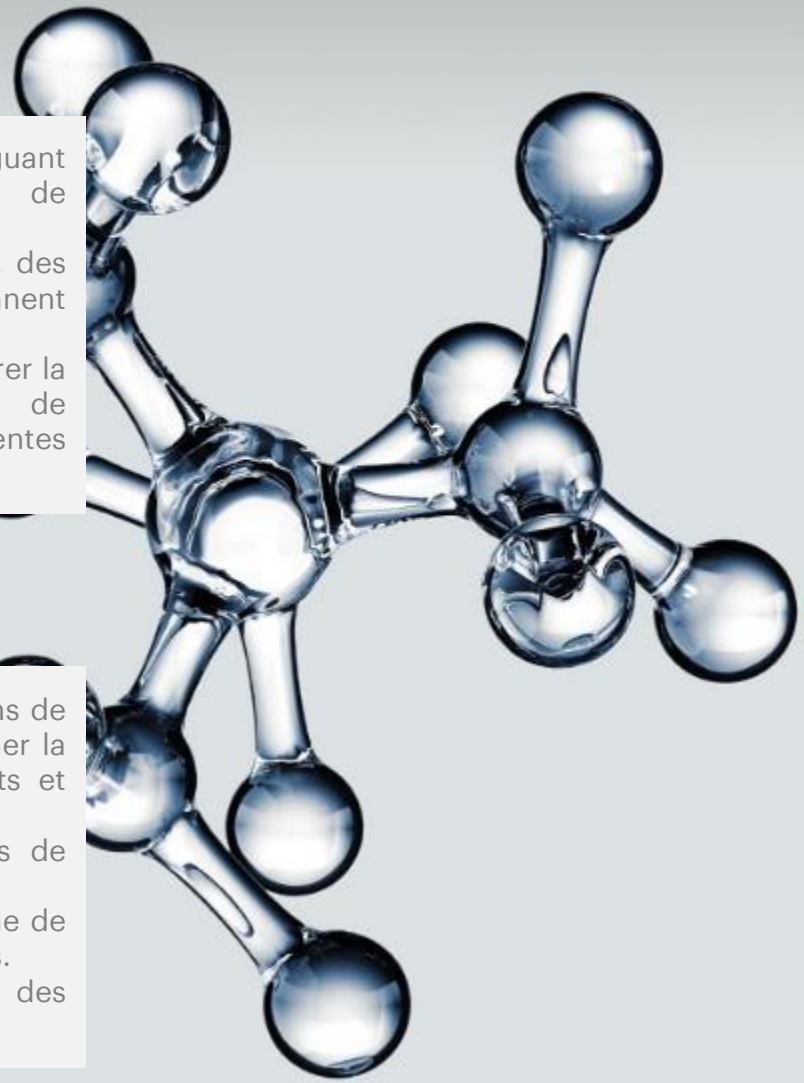
En raison d'une série d'acquisitions, cette organisation avait un écosystème informatique largement décentralisé, avec une visibilité limitée des risques et des expositions à la cybersécurité dans toute l'entreprise.

COMMENT?

- Effectuer un diagnostic à 360 degrés en cataloguant les risques et les expositions en matière de cybersécurité des TI, des TI étendues et des tiers.
- Inventorier l'écosystème étendu des applications, des systèmes et des fournisseurs externes qui soutiennent l'organisation.
- Élaborer une feuille de route détaillée pour améliorer la couverture des programmes de sécurité de l'information, en fonction des objectifs et des attentes des unités opérationnelles.

QUELLE VALEUR?

- Accroître la visibilité des risques et des expositions de l'entreprise en matière de sécurité, et mieux aligner la mission de sécurité de l'information sur les buts et objectifs fixés par le chef d'entreprise.
- Comprendre les tierces parties, les fournisseurs de services et les relations en aval.
- Améliorer l'alignement des objectifs du programme de sécurité avec les objectifs des unités commerciales.
- Améliorer la compréhension des risques et des expositions en matière de sécurité des entreprises.



QUELLES SOLUTIONS SUR LE MARCHÉ?

QUELQUES EXEMPLES DE TECHNOLOGIES D'EXPLOITATION

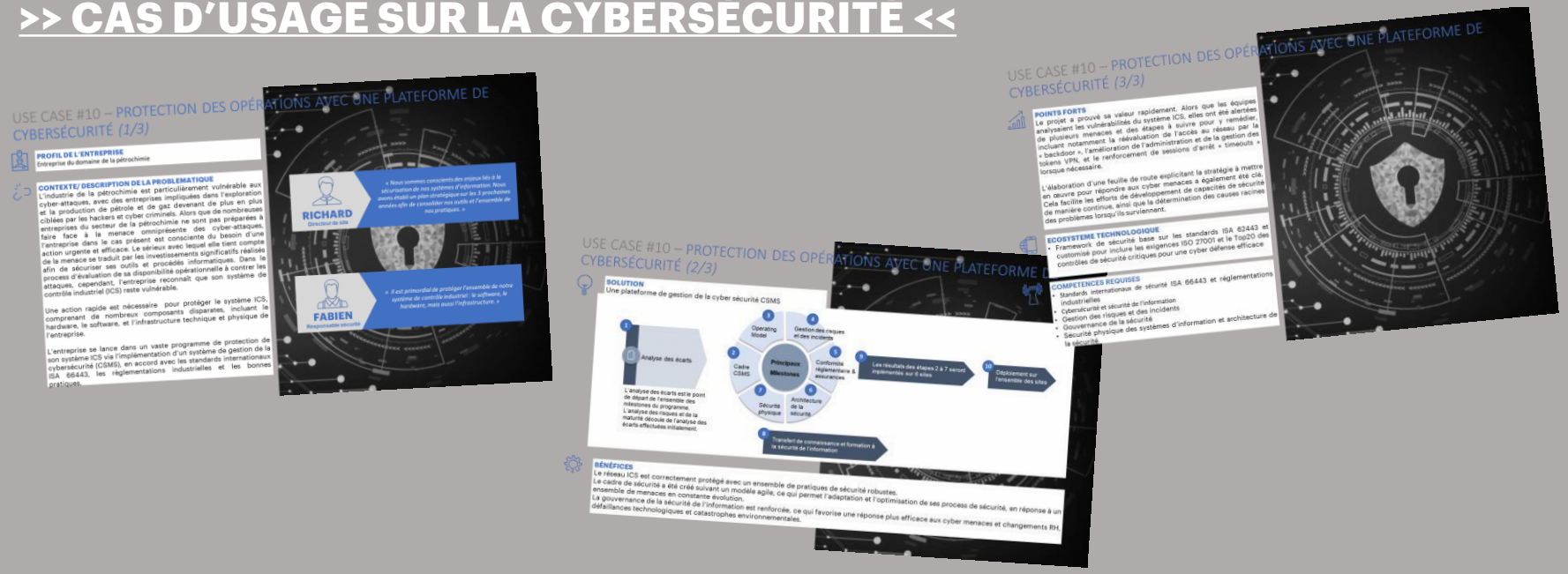
Plusieurs solutions existent en fonction des différents types de couches

OFFICE	COUCHE 4
DMZ	COUCHE 3.5
SCADA	COUCHE 3
SUBSTATION WINDMILL BUILDING AUTOMATION	COUCHE 2 COUCHE 1

paloalto NETWORKS
CISCO
splunk>
CISCO
FORTINET
Barracuda
CYBERARK
SIEMENS
CISCO
NOZOMI NETWORKS
FORTINET
paloalto NETWORKS
JUNIPER NETWORKS
FORESCOUT
SECURITY MATTERS
sprecher automation
ABB
SIEMENS
RUGGEDCOM
HIRSCHMANN

LIENS VERS LES CAS D'USAGE SUR LA CYBERSECURITE

>> CAS D'USAGE SUR LA CYBERSÉCURITÉ <<



POUR ALLER PLUS LOIN

LIENS ACCENTURE

- https://www.accenture.com/fr-fr/insights/cyber-security-index?c=fr_fr_cyberresilience_10369697&n=psgs_brand_1018&gclid=Cj0KCQjw0Mb3BRCaARIsAPSNGpW6AqtZ8XFh9NogAzSt2c77W8n0uADQJKBXnH2zw7YHYbG7ydqeZCUaApRtEALw_wcB
- https://www.accenture.com/fr-fr/insights/security/communication-comme-reponse-aux-cybermenaces-en-periode-de-crise
- https://www.accenture.com/fr-fr/insights/security/invest-cyber-resilience

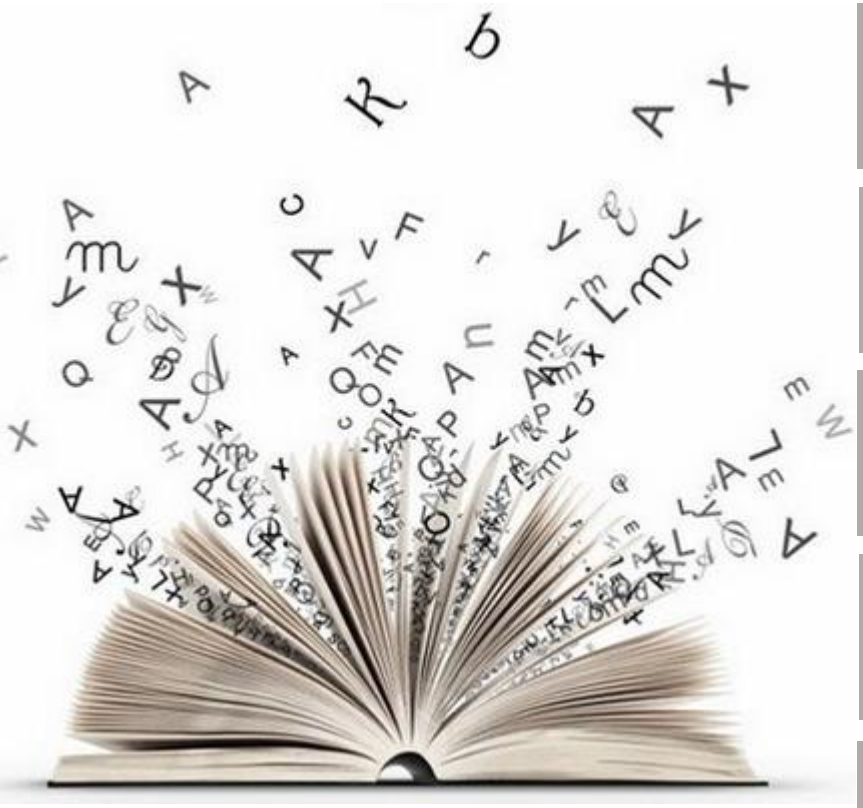
AUTRES ARTICLES

- https://www.latribune.fr/supplement/ceux-qui-transforment-la-france/la-cybersecurite-enjeu-majeur-des-temps-modernes-837235.html

VIDÉOS

- https://youtu.be/r5OEIY7oz6I
- https://youtu.be/yI-UKjeY9j4

LEXIQUE AUTOUR DE LA CYBERSÉCURITÉ



OT	Les systèmes de technologie opérationnelle (OT) pilotent et contrôlent tous les processus physiques des opérations de fabrication
INFOSEC	Terme utilisé pour désigner la "sécurité de l'information" et désigne l'activité consistant à protéger l'information en gérant les risques qui peuvent l'affecter
AUTHENTIFICATION	Processus consistant à identifier l'identité d'un utilisateur, en s'assurant qu'il peut avoir accès au système et/ou aux fichiers. Cela peut se faire soit par un mot de passe, soit par un balayage de la rétine, soit par un balayage des empreintes digitales, parfois même par une combinaison des éléments ci-dessus.
VIOLATION DES DONNÉES	Le résultat d'un pirate informatique qui réussit à pénétrer dans un système, à prendre le contrôle de son réseau et à exposer ses données, généralement des données personnelles couvrant des éléments tels que les numéros de carte de crédit, les numéros de compte bancaire, les numéros de sécurité sociale...
DOMAINE	Une série d'ordinateurs et de périphériques associés (routeurs, imprimantes, scanners), qui sont tous connectés comme une seule entité.
PARE-FEU	Toute technologie, qu'elle soit logicielle ou matérielle, utilisée pour empêcher les intrus d'entrer
CRYPTAGE	Codage utilisé pour protéger vos informations contre les pirates informatiques. Pensez-y comme le code utilisé pour envoyer un message codé top secret d'espion
MALWARE	Ensemble "malveillants" et de "logiciels", décrivant une grande variété de mauvais logiciels utilisés pour infecter et/ou endommager un système. Les rançons, les vers, les virus et les chevaux de Troie sont tous considérés comme des logiciels malveillants. Il est le plus souvent transmis par des courriers électroniques non sollicités (spam)

CYBERSÉCURITÉ

FOCUS SUR DIFFERENTS SUJETS LIES A LA CYBERSECURITE :

- *Durcissement des systèmes*
- *Cryptographie*
- *Sécurité physique*

PANORAMA SUR LE DURCISSEMENT DES SYSTÈMES

QU'EST-CE QUE LE DURCISSEMENT DES SYSTEMES ?

Le *durcissement des systèmes* est le processus qui consiste à sécuriser un système en identifiant et en réduisant ses vulnérabilités (surface d'attaque).

- DURCISSEMENT DES OS
- DURCISSEMENT DES APPLICATIONS
- DURCISSEMENT DES SERVERS
- DURCISSEMENT DES BASES DE DONNEES

À cette fin, on utilise différents outils, techniques et meilleures pratiques :

- DURCISSEMENT DES SYSTÈMES
- DURCISSEMENT DES EQUIPMENTS
- DURCISSEMENT NETWORK

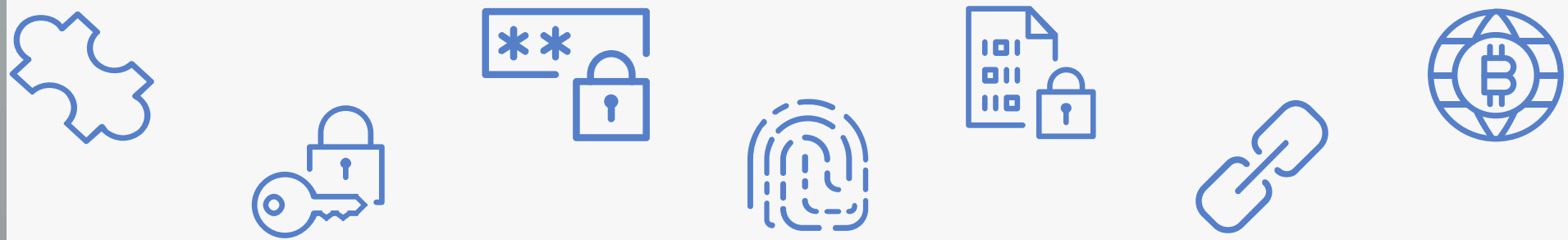
PANORAMA SUR LA CRYPTOGRAPHIE

QU'EST-CE QUE LA CRYPTOGRAPHIE?

LA CRYPTOGRAPHIE COMPREND UN ENSEMBLE DE TECHNIQUES QUI VISENT À FOURNIR DES COMMUNICATIONS SÉCURISÉES AFIN QUE DES PARTICIPANTS NON AUTORISÉS NE PUISSENT PAS OBTENIR LES INFORMATIONS QUI SONT TRANSFÉRÉES PAR LE RÉSEAU.

Afin de garantir la sécurité des communications, ces techniques visent à transformer les données lisibles transférées (que tout le monde peut comprendre) en informations qui ne peuvent être lues que par des participants légitimes.

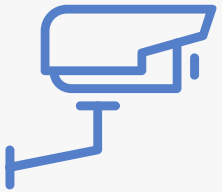
Ces techniques ont gagné en complexité depuis des d'années jusqu'à aujourd'hui.



PANORAMA SUR LA SÉCURITÉ PHYSIQUE

QU'EST-CE QUE LA SECURITE PHYSIQUE?

Un aspect essentiel du contrôle physique implique des **barrières physiques pour empêcher l'accès aux systèmes informatiques et aux réseaux.**



Les mises en œuvre les plus efficaces exigent que **plus d'une barrière physique soit franchie pour y accéder**.

Ce type d'approche est la défense en profondeur déjà mentionnée ou le **système de barrières multiples**.

Idéalement, un système sécurisé devrait compter au moins trois barrières physiques :

PÉRIMÈTRE
Entrée sécurisée du bâtiment où les systèmes sont hébergés avec une liste de contrôle et des éléments de sécurité physique.

CENTRE INFORMATIQUE
Il doit comporter une porte verrouillée qui nécessite une identification pour y accéder.

SALLE D'ORDINATEURS
Elle doit également avoir une porte verrouillée et soigneusement surveillée.