LA CYBERSECURITE A L'USAGE DES DIRIGEANTS

LIVRE BLANC

Edition 2020

CLUSIF

OSSIR

AVANT-PROPOS

Le CLUSIF et l'OSSIR, les deux plus anciennes associations de sécurité informatique françaises, parlent en général à des passionnés de cybersécurité. Dans ce guide, nous souhaitons sortir de notre zone de confort et nous adresser à vous, dirigeants d'entreprise et cadres exécutifs.

Nous voulons vous convaincre que la sécurité informatique n'est ni un sujet réservé aux seuls initiés ni un puits financier sans fond. Notre objectif est de démystifier au maximum le jargon technique pour éclairer les enjeux de l'entreprise et les risques associés.

Dans son rapport 2019 sur les risques globaux, le World Economic Forum positionne le risque cybersécurité dans le top 4, devant la perte de la biodiversité, une crise fiscale ou encore une pandémie.

Qu'on le veuille ou non, la cybersécurité est devenue un enjeu sociétal, la presse se faisant quotidiennement l'écho de catastrophes numériques survenues dans le monde. Les comités exécutifs et conseils de surveillance n'échappent pas à cette question.

En tant que dirigeant, votre responsabilité n'est pas de devenir expert, mais d'avoir un avis éclairé pour garantir la pérennité de votre entreprise.

Nous espérons que ce guide vous aidera dans cette mission.

Jean-Philippe GAULIER
Président de l'OSSIR

Pierre RAUFAST
Administrateur du CLUSIF

TABLE DES MATIÈRES

LES CONTRIBUTEURS

Nous tenons à remercier chaleureusement toutes les personnes qui ont pu contribuer à la création de ce livre blanc. C'est le résultat d'un mélange de cultures, de travail, d'échange et de soutien.

Par ordre alphabétique

- William BOURGEOIS
- Grégory FABRE, Cyberzen
- Cédric GASPARD
- Jean-Philippe GAULIER, Cyberzen
- Nicolas HANTEVILLE
- Mojdeh HOJDAT-PANAH-DAURELLE, Pôle emploi
- Jean-Philippe ISCKIA, digital.security
- Vladimir KOLLA, PatrOwl
- Christophe LABOURDETTE, CNRS/ENS-Paris-Saclay
- Christophe LAYEN, Cultures et Mutation
- Julien LITTLER
- Luc MENSAH
- Pierre RAUFAST, Michelin
- Quoc Hiep TRAN, Orange

Merci à nos nombreux relecteurs et relectrices :

Stéphane ADAMIAK, Grégory ADROT, Luména DULUC, Hervé MAFILLE, Lionel MOURER, Stéphanie PHILIPPE, Hervé SCHAUER, Eric VAUTIER, Franck VEYSSET.

Les illustrations de ce document ont été réalisées par Carlo BRUZZESI. (instagram : @carloartwork)

INTRODUCTION

POURQUOI LIRE CE GUIDE ?

L'informatique s'est enracinée dans l'entreprise[1]. Plus personne ne s'imagine passer des commandes à la main, faire sa comptabilité sur papier ni envoyer un télégramme. Tout passe par un ordinateur, un smartphone et Internet. Cette transition inévitable engendre des gains de rapidité, de flexibilité et d'ouverture à l'international.

Cela a transformé nos vies et notre société. Sans informatique, nous nous retrouvons démunis, sans pouvoir faire fonctionner l'entreprise ou l'administration. La mécanique s'enraye sans réel moyen de repartir. Mais quand ça marche, l'ensemble semble fonctionner par magie.

De ce constat, nous avons souhaité aborder des thèmes qui nous semblent essentiels pour comprendre les fondements de votre système d'information*, les enjeux qui y sont liés et les risques auxquels vous devez faire face.

Si les risques sont communs, les réponses, elles, sont propres à chacun, car elles dépendent de votre stratégie, de votre engagement, de votre appétence aux risques, de votre fonctionnement et de votre budget.

Nous avons divisé ce guide en trois grandes parties : Mon entreprise ; L'entreprise interconnectée ; Gouvernance et confiance numérique.

Il est bien sûr impossible en quelques pages de traiter un sujet aussi important et complexe de manière exhaustive, mais nous espérons que cette lecture vous apportera un premier éclairage suffisant.

1. Dans ce guide, le terme « entreprise » regroupe différents types d'organisations : aussi bien une administration, une association qu'une entreprise privée.

LA SÉCURITÉ INFORMATIQUE

On imagine souvent la sécurité informatique, ou la « cybersécurité », selon son appellation marketing, comme un domaine extrêmement complexe où seuls les spécialistes ont le droit de cité. Heureusement, il est possible de résumer cette complexité en quelques concepts facilement manipulables par tout un chacun ; c'est l'ambition de ce guide. Chaque thème est présenté simplement par sa définition, les enjeux pour l'entreprise et les risques afférents.

De plus, voici les critères de sécurité de haut niveau que vous pourrez questionner à chaque chapitre :

- **disponibilité** : l'accès aux ressources* du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues ;
- **intégrité** : garantie que le système et l'information traitée ne peuvent être modifiés que par une action volontaire et légitime ;
- **confidentialité** : propriété d'une information qui n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés.

Ces critères vous aideront à lister les risques auxquels vous êtes exposés ainsi que la stratégie à appliquer dans ce domaine.

LE CYBERRISQUE

Pour comprendre les risques auxquels nous sommes exposés, il faut avant tout comprendre ce qui est concerné : les collaborateurs, les données à protéger ou les infrastructures sous-jacentes tout au long de leur transfert, leur traitement ou leur stockage.

Pourquoi mon entreprise est-elle une cible ?

On dénombre cinq causes possibles :

- **La cybercriminalité** : les nouvelles "mafias" en ligne dont le but est de gagner de l'argent au travers d'arnaques, de chantages ou de vols. Ce sont de vrais professionnels, qui attaquent tous azimuts.
- **La malveillance par négligence** : résulte de la désinvolture des collaborateurs ou partenaires quant aux politiques de sécurité internes et mettent l'entreprise en situation de risque.
- **L'atteinte à l'image** : ciblée, elle contribue à la campagne de déstabilisation d'une personne ou d'une entité dont les effets sont amplifiés par l'importance actuelle des réseaux sociaux.
- **L'espionnage** : ciblé. Sous couvert d'intelligence économique, certains concurrents ou États utilisent les vulnérabilités informatiques pour espionner les secrets d'une entreprise.
- **Le sabotage** : ciblé, il est réalisé à des fins de déstabilisation (économique ou politique) ou pour des raisons idéologiques (activisme).

Quelles sont les conséquences pour mon entreprise ?

Elles sont de natures diverses. Les plus fréquentes sont financières ; de réputation ou d'image ; de productivité ; juridiques, pouvant entraîner des

conséquences légales ou financières ; humaines (vitales ou handicapantes) dans le cas, par exemple, d'un sabotage.

Comment traiter ces cyberrisques ?

Il y a aujourd'hui quatre grandes familles de solutions pour traiter les risques :

- **l'évitement**, en supprimant l'activité ou la condition qui mène au risque ;
- **le transfert ou partage** avec un tiers (ex. : assureur) ;
- **le renforcement** des mesures techniques ou organisationnelles pour diminuer l'impact ou la potentialité ;
- **l'acceptation** du risque accompagné d'une provision financière.

Une cartographie des risques et des plans de mitigation est essentielle. Tous les acteurs, métiers et techniques doivent contribuer à la définition de ces documents et à leur mise à jour.

MON ENTREPRISE

1
COURRIER ÉLECTRONIQUE : LA FACE CACHÉE

<< WOW! J'AI GAGNÉ À LA GRANDE LOTERIE D'INTERNET! >>
<< MOI AUSSI! >>
<< ...ET MOI AUSSI! >>
LE JOUR OÙ LE FILTRE ANTI-SPAM TOMBA EN PANNE...

Définition

La plus simple comparaison que l'on puisse faire avec le courrier électronique est son équivalent postal : la carte postale.

Le courrier électronique est l'un des premiers services disponibles sur Internet ; c'est également l'un des plus employés aujourd'hui dans le monde de l'entreprise.

Il permet à plusieurs utilisateurs de s'échanger des messages de manière asynchrone. Ce système ne garantit généralement en rien la disponibilité, la confidentialité ou l'intégrité des messages échangés. Il ne garantit pas non plus le fait que le destinataire reçoive bien le message qui lui a été envoyé. Pour résumer, la seule garantie de l'utilisateur réside dans la certitude de l'envoi du message.

Par ailleurs, en matière d'obligations légales, un message numérique a la même valeur légale qu'un écrit. Il est reconnu comme preuve de conclusion d'un contrat et il est soumis au secret des correspondances.

Le passage des échanges commerciaux au numérique a également placé l'adresse de courrier électronique comme l'identifiant unique, la boîte aux lettres électronique comme centralisateur de tous les contrats, que ce soit pour les professionnels ou pour les particuliers.

Loin de son usage initial, la messagerie est aujourd'hui un melting-pot utilisé pour le transfert de fichiers, l'archivage, la messagerie instantanée et, accessoirement, le courrier.

Les enjeux métier

Le courrier électronique est aujourd'hui au cœur des échanges ; d'abord en interne, entre les collaborateurs. Il permet l'échange d'idées, d'informations, de documents. Il permet également d'établir une communication souple et permanente avec ses prospects, clients et partenaires. Lorsque la messagerie ne répond plus, l'entreprise est lourdement impactée.

La messagerie d'entreprise est également un lieu important de stockage du patrimoine informationnel, regroupant les carnets d'adresses forgés au cours des échanges, les décisions et arbitrages, mais également les appels d'offres, les réponses, les grilles tarifaires, les plans stratégiques...

Les risques pour l'entreprise

Confidentialité et intégrité des messages : sans signature électronique, l'émetteur peut être usurpé ; sans chiffrement*, un courriel peut aisément être modifié ou divulgué.

Phishing* ou hameçonnage* : c'est l'un des outils de l'ingénierie sociale*. À travers une imposture envoyée par courriel, l'attaquant cherche à récupérer des informations sur la victime (comme ses identifiants), à déployer un virus, un rançongiciel* ou tout simplement à persuader la cible de réaliser un transfert financier, comme c'est le cas dans l'arnaque (ou fraude) au président*. C'est une menace omniprésente.

Les messageries professionnelles disponibles sur Internet sont la cible privilégiée pour s'introduire dans le système d'information* via le vol de mot de passe. Une authentification forte (MFA*) est nécessaire pour limiter ce risque.

Patrimoine : Il ne faut pas négliger non plus la perte du patrimoine informationnel en cas de perte des données de la messagerie électronique.

Pour aller plus loin :

Niveau standard

Quels sont les impacts pour votre entreprise si la messagerie électronique est interrompue pendant une semaine ?

Niveau avancé

Comment votre entreprise se prémunit-elle contre l'arnaque au président* ?

2

BYOD*/ATAWAD* : JAMAIS SANS MON PORTABLE

« COMMENT VEUX-TU QUE J'INSTALLE EXCEL SUR TA CONSOLE DE JEUX ?!? »

Définition

Que ce soit sous l'impulsion des clients, des partenaires ou des collaborateurs, les nouvelles façons de consommer l'informatique conduisent à une mutation des solutions d'accès au système d'information* de l'entreprise. Elles nécessitent l'assouplissement des contraintes liées aux horaires, aux terminaux ou aux moyens de connexion.

Ce phénomène appelé ATAWAD* (Any Time, Any Where, Any Device), que certains appellent « mobiquité », offre une plus grande souplesse aux collaborateurs dans l'accès et le partage de contenus. Par exemple en permettant d'utiliser un smartphone personnel depuis chez soi pour se connecter à sa messagerie professionnelle.

Le BYOD* (Bring Your Own Device) répond à une attente forte des utilisateurs, celle de disposer d'outils et de technologies personnels quel que soit le contexte d'utilisation.

Les enjeux métier

Ces concepts débrident les limites concernant l'accès au système d'information*.

Ils permettent le lissage de la frontière entre les mondes "professionnel" et "personnel", laissant aux collaborateurs plus d'autonomie dans l'organisation de leur travail.

Utilisé en mobilité depuis n'importe quel terminal, cela peut améliorer l'efficacité des processus métier en aidant à leur numérisation.

Enfin, c'est un facteur d'attractivité, notamment chez les nouvelles générations qui préfèrent choisir leurs équipements et les conditions d'utilisation.

Les risques pour l'entreprise

Ouvrir son système d'information* à n'importe quel terminal depuis n'importe quel lieu augmente forcément la surface d'attaque*.

Il convient d'encadrer ces nouvelles pratiques par des référentiels décrivant les bonnes pratiques et les mesures techniques mises en place. Une charte opposable liste les droits et devoirs des salariés vis-à-vis du respect des règles d'usage.

Pour être efficaces, ces documents doivent être accompagnés d'une sensibilisation récurrente des collaborateurs.

Dans cette configuration, la perte d'information est le plus souvent liée à un vol de terminal. C'est une obligation de l'entreprise de s'en protéger (cf. CNIL, Commission Nationale Informatique et Liberté et RGPD*, Règlement Général sur la Protection des Données), notamment au moyen d'inventaires à jour et par le chiffrement* des périphériques.

L'installation d'applications d'origine douteuse induit un risque de piégeage de matériel (*cheval de Troie**).

Il existe des solutions pour gérer ces flottes de terminaux et répondre à ces risques (MDM*, Mobile Device Management). Ces solutions permettent de forcer les exigences de sécurité souhaitées (par exemple déverrouillage par code PIN), de limiter les installations d'application ou d'effacer à distance toutes les données sensibles.

Pour aller plus loin :

Niveau standard

Comment vous assurez-vous qu'aucun document confidentiel de l'entreprise n'est présent sur les mobiles personnels de vos collaborateurs ?

Niveau avancé

Comment contrôlez-vous que les matériels personnels sont sains avant de les autoriser à se connecter à votre système d'information ?

3
ACCÈS DISTANT : ACCÉDER AU SI DEPUIS SON VOILIER

<< C'EST QUOI CE DISTRIBUTEUR AUTOMATIQUE DANS NOTRE SALON? >>
<< JE N'ARRIVE PAS À TRAVAILLER SANS PAUSE CAFÉ! >>

Définition

L'accès distant, c'est la connexion aux systèmes d'information de l'entreprise depuis l'extérieur.

Elle concerne majoritairement les collaborateurs et les partenaires pour satisfaire les besoins de télétravail, d'astreinte ou de solutions de mobilité sur le terrain, mais aussi des besoins de collaboration de l'entreprise étendue.

Par exemple, un commercial pourra faire une proposition, récupérer des documents marketing ou passer des commandes en présence de son client. Un assistant pourra gérer les agendas de ses patrons depuis son domicile. Un partenaire pourra, depuis son entreprise, faire du codesign sur un projet commun.

Pour cela, il est indispensable de sécuriser ces canaux de communication.

Les enjeux métier

La mise en place d'accès distant sur votre système d'information* ouvre de nombreuses perspectives métier, humaines et organisationnelles.

Les principales sont les suivantes :

- faciliter la consolidation d'information ;
- flexibiliser l'accès au système d'information* et renforcer son efficacité (nomadisme) ;
- satisfaire les attentes des salariés (télétravail) ;
- ouvrir le système d'information* de l'entreprise à ses partenaires (travail collaboratif, codesign, entreprise étendue, sous-traitance) ;
- interconnecter des filiales ou des sites géographiques distants ;
- diminuer les astreintes sur site, les déplacements ;
- renforcer l'application des politiques de sécurité.

Les risques pour l'entreprise

L'accès à distance au système d'information* de l'entreprise augmente sa surface d'attaque* en ouvrant de "nouvelles portes". Les attaques dites supply-chain utilisent un maillon faible de votre organisation (le réseau interne d'un fournisseur ou d'un sous-traitant par exemple) pour s'introduire dans votre système d'information* (risque de vol, fuite de données, sabotage, propagation de malware...).

C'est cette interconnexion mal sécurisée entre sites qui peut favoriser la propagation de malware et produire un effet domino sur l'ensemble du système d'information* (cas de NotPetya entre les filiales ukrainiennes et européennes).

Pour aller plus loin :

Niveau standard

Êtes-vous sûr que tous les accès à votre système d'information* sont connus ? Sont-ils chiffrés ?

Niveau avancé

Est-il nécessaire que votre système d'information* soit intégralement accessible à distance ? N'y a-t-il pas trop de "portes" ouvertes ? Pour combien d'utilisateurs ?

4

L'ANNUAIRE D'ENTREPRISE : UN SERVICE POUR LES GOUVERNER TOUS

« ON VEUT ÊTRE ADMINISTRATEURS DE NOS ORDINATEURS! »
« ON VEUT NOS DROITS! »

Définition

Les organisations sont désormais structurées autour de leurs systèmes d'information. Afin de faciliter et contrôler les accès des utilisateurs, ces systèmes proposent l'utilisation d'annuaires. Ces solutions contiennent des informations relatives à des **ressources informatiques*** ou à des personnes : des identités, des comptes et des rôles appelés « privilèges ».

Un système d'information* comprend généralement un service d'annuaire, organisé en arborescence et géré par des normes standard. La plus courante est le protocole Lightweight Directory Access Protocol (**LDAP***) qui régit l'interrogation et la modification des services d'annuaire, ainsi que leurs interactions.

Les fournisseurs de systèmes d'exploitation ont nommé leurs annuaires en utilisant la norme LDAP* de façon spécifique. Par exemple : Active Directory pour Microsoft/Windows, Apple Open Directory chez Apple/Mac OS...

Les enjeux métier

Les annuaires sont des éléments capitaux du système d'information*. Ils permettent aux personnes autorisées d'accéder uniquement aux informations qu'elles ont le droit de connaître. Ils permettent également la centralisation de la gestion des identités, des ressources* et des droits d'accès, simplifiant ainsi les tâches d'administration (création, suppression, modification, revues périodiques).

Les risques pour l'entreprise

Les annuaires qui sont des éléments critiques du système d'information* contiennent, la plupart du temps, des données à caractère personnel.

Une organisation défectueuse et/ou une mauvaise gestion des annuaires peuvent amener des collaborateurs ou des personnes malveillantes à accéder à des informations qu'ils ne sont pas en droit de connaître,

mettant ainsi l'organisation en défaut par rapport au Règlement Général de Protection des Données (RGPD*).

La sécurisation insuffisante des annuaires peut permettre à une personne malveillante d'en prendre la maîtrise, d'usurper les droits des utilisateurs privilégiés* et de prendre le contrôle de tout ou partie du système d'information*. Il pourra ensuite voler des données, bloquer le système d'information* pour obtenir une rançon avec des identifiants légitimes difficiles à détecter.

Les annuaires sont critiques et doivent être protégés pour éviter de mettre en péril l'entreprise.

Pour aller plus loin :

Niveau standard

À quand remonte votre dernier audit de sécurité de l'annuaire ?

Niveau avancé

Combien de personnes ont un compte administrateur sur votre annuaire ? Est-ce justifié ?

5
CYCLE DE VIE : POURQUOI REMPLACER SES MINITELS

CHAQUE ANNÉE, L'OBSOLESCENCE INFORMATIQUE CONTINUE À FAIRE DES VICTIMES

Définition

Chaque composant (matériel ou logiciel) a un cycle de vie propre intégrant plusieurs étapes : sa conception, ses phases de développement, d'utilisation et de maintenance, sa fin d'utilisation (ou décommissionnement*).

Ce cycle de vie dépend essentiellement de la stratégie du fournisseur.

Les enjeux

Un composant informatique critique pour l'entreprise doit être pleinement fonctionnel et disponible.

Pour garantir cela, des équipes informatiques internes ou externes doivent veiller à maintenir ce composant en "bonne santé numérique" ; c'est-à-dire appliquer les correctifs nécessaires, surveiller sa consommation de ressources informatiques*, anticiper les pannes, etc.

Quand un composant (matériel ou logiciel) est obsolète et n'est donc plus maintenu par son fabricant, cette mission devient plus difficile à réaliser.

Le composant peut très bien rester fonctionnel chez le client ; en revanche, la prise de risques augmente, car le fabricant n'apportera aucun support en cas de problème ou de vulnérabilité.

Les risques

- **Risque d'instabilité ou de failles de sécurité :**

Pendant sa durée de vie utile, si le produit n'est pas régulièrement mis à jour, il pourra devenir instable et générer une rupture de service ou être victime d'un piratage.

Le processus périodique de mise à jour (patching*) permet de limiter ce risque. Par exemple, les attaques Wannacry de 2017 ciblaient des systèmes vulnérables, non mis à jour.

- **Risque d'obsolescence :**

Lorsqu'un composant n'est plus maintenu, il devient obsolète.

Son propriétaire peut continuer à l'utiliser ; cependant, il n'aura plus de support ni de correctifs et encourt les risques décrits dans le point précédent.

Du point de vue sécurité, une vulnérabilité découverte sur un composant obsolète ne pourra pas être corrigée à un coût économique acceptable. Cela crée une faille de sécurité dans le système d'information* et augmente la surface d'attaque* de l'entreprise.

D'un point de vue business, cela fige la capacité du système d'information* à évoluer fonctionnellement et techniquement. Cela peut pénaliser la compétitivité de l'entreprise par des difficultés d'évolution ultérieure.

En conclusion, la décision de remplacer un composant résulte d'une pondération entre les risques à éviter, le coût et la valeur métier apportée par ce changement.

Pour aller plus loin :

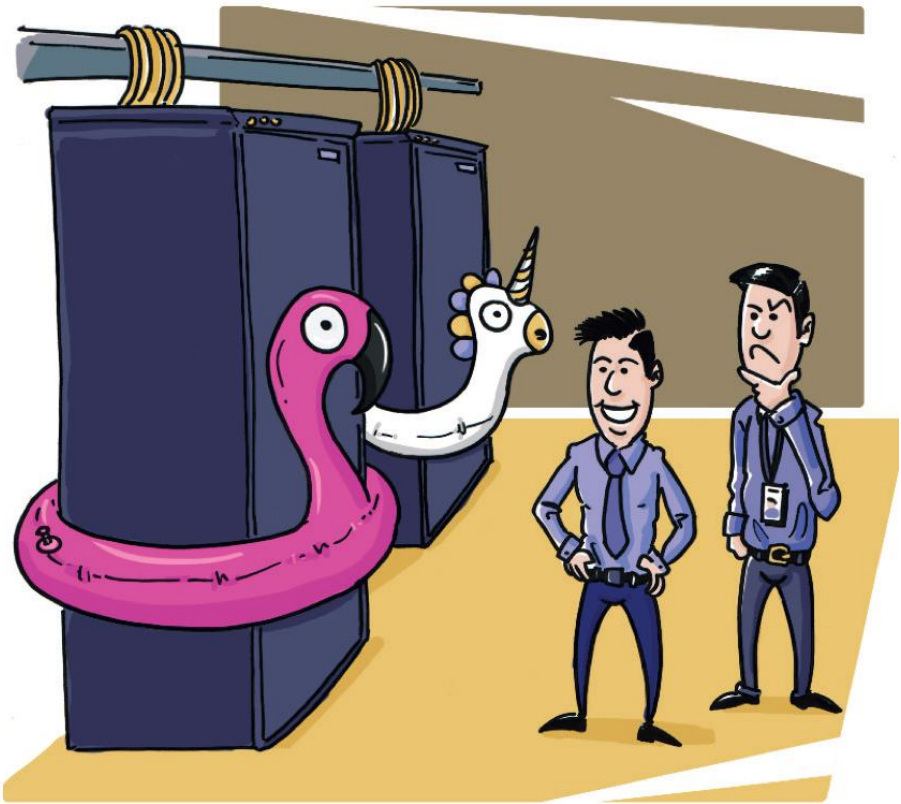
Niveau standard

Quel est l'âge de votre application la plus ancienne et quel est son coût de maintien en condition opérationnel ?

Niveau avancé

Au vu du compromis risque/valeur, à quel moment est-il plus raisonnable de remplacer une application obsolète ?

6
PRA*/PCA* : SURVIVRE À UN ARMAGEDDON



« EST-CE QUE VOUS ÊTES SÛR QU'IL S'AGIT DU MEILLEUR MOYEN POUR PROTEGER NOS SERVEURS EN CAS D'INONDATION? »

Définition

Le Plan de Continuité d'Activité (PCA*) permet le fonctionnement de l'ensemble des activités critiques de l'entreprise en cas de sinistre. C'est un dispositif préventif qui n'a pas vocation à être exhaustif, mais qui interroge sur la criticité des ressources informatiques* et leur continuité de service. Par exemple, dans le cas de la perte d'un accès à Internet (coupure de fibre), une liaison satellite est disponible immédiatement.

Le Plan de Reprise d'Activité (PRA*) représente l'ensemble des procédures et moyens (organisationnels, humains et techniques) permettant d'assurer graduellement la reprise d'activité vers le fonctionnement nominal. Par exemple, le déport progressif d'un datacenter vers un autre après une inondation.

Les enjeux

Le premier enjeu est de continuer à fournir aux clients et aux usagers un service, même dégradé, pendant un sinistre.

Le deuxième enjeu vise à rétablir le retour au fonctionnement nominal afin d'assurer pleinement la mission de l'organisation.

Le troisième enjeu est de sensibiliser et former ses personnels afin que le retour à la normale s'effectue dans le calme et soit efficace, tout en limitant les impacts pour les usagers.

Enfin, il est primordial d'avoir une cartographie des risques mise à jour conjointement entre la direction, le métier et le service informatique.

Les risques

La perte partielle ou totale des ressources informatiques* clés entraînant une rupture de service a pour conséquences possibles :

- une perte financière à la suite de ventes non réalisées pendant l'absence de service ou des pénalités pour non-respect contractuel ;
- une atteinte à l'image auprès des investisseurs, clients et opinion publique ;
- un risque légal lié à une rupture contractuelle des engagements de la société ;
- un risque de perte de propriété intellectuelle ou de données.

Pour aller plus loin :

Niveau standard

Combien de jours votre entreprise peut-elle fonctionner sans informatique ? Combien cela vous coûte-t-il ?

Niveau avancé

Qui est en charge d'anticiper les crises et de les gérer ?

L'ENTREPRISE INTERCONNECTEE

7

DNS* : L'ANNUAIRE MONDIAL QUE VOUS UTILISEZ SANS MÊME LE SAVOIR

« JE VOUDRAIS REJOINDRE MES AMIS AU 104.28.1.196 »
« AH OUI, LE SITE DE L'OSSIR. CABINE 1 »

Définition

Internet représente l'interconnexion entre des ordinateurs à travers le monde. Inventé par des ingénieurs et des universitaires, c'est le produit d'un ensemble de concepts et de technologies dont les plus anciennes datent des années soixante.

Il existe plusieurs services reposant sur Internet : le web, le courriel, le peer-to-peer, la téléphonie, mais aussi des services invisibles à l'utilisateur comme le DNS*. C'est une technologie primordiale qui permet de convertir une information technique dans un nom de domaine humainement compréhensible.

Cette technologie vitale pour le bon fonctionnement d'Internet repose sur un maillage complexe d'intermédiaires. Aucune entreprise ne peut aujourd'hui s'en passer.

Les enjeux métier

Le DNS* est essentiel pour toute entreprise proposant du contenu ou des services en ligne (sur Internet ou sur intranet, y compris la messagerie, la téléphonie IP ou des sites web)

Les enjeux pour **l'image** de l'entreprise sont majeurs : celle-ci doit essayer de disposer de noms de domaine permettant de protéger ses marques, et d'être identifiée facilement sur Internet.

De la même manière, la **disponibilité** du service DNS* est un enjeu essentiel pour le bon fonctionnement de ses activités numériques.

Les risques pour l'entreprise

Le service DNS* peut être touché par des soucis de **disponibilité** entraînant l'incapacité d'accéder à des sites web. Cela peut être dû à un bug logiciel, une erreur humaine ou une attaque par déni de service*.

Le nom d'une entreprise peut être subtilement travesti pour être utilisé dans des campagnes de phishing* ou de fraudes. C'est le typosquatting*.

Par exemple : monentreprlse.com vs monentreprise.com

Enfin, le nom DNS* de votre entreprise peut être "**squatté**" si vous ne l'avez pas renouvelé à temps (cybersquatting*) ou utilisé dans un nom de domaine similaire.

Par exemple : monentreprise-support.com sera utilisé dans une arnaque pour usurper le service support d'une société.

Pour aller plus loin :

Niveau standard

Savez-vous combien vous coûte annuellement la protection de vos noms de domaine ? Faites-vous de la veille ?

Niveau avancé

Êtes-vous armé pour traiter un éventuel conflit juridique sur ce sujet ? Usurpation de noms, oubli de renouvellement, etc.

8

WWW : LA RUÉE VERS LE WEB

LES RISQUES DE LA NAVIGATION SUR INTERNET...

Définition

Le web ne doit pas être confondu avec Internet (fiche précédente). Le web est la partie d'Internet la plus connue du grand public grâce au « surf sur les sites web » mais aussi pour les blogs, les forums de discussion, le streaming, les réseaux sociaux, etc.

Les enjeux métier

Une entreprise doit avoir une présence numérique sur la Toile pour maîtriser son image et mieux servir ses clients et partenaires.

Un site web **vitrine** (corporate) lui permet d'informer en temps réel les différents acteurs de la vie de l'entreprise (clients, actionnaires, journalistes, etc.).

Un site **marchand** lui ouvre les portes du commerce en ligne et la dématérialisation de son catalogue.

Sa présence active sur les **réseaux sociaux** permet de communiquer plus largement, d'atteindre plus efficacement ses clients et favorise son attractivité, son image ou sa capacité à recruter.

Pour les **salariés**, l'accès au web est devenu un réflexe quotidien dans leurs vies personnelle et professionnelle. Leur donner accès aux sites déontologiquement validés leur permettra de participer à la vie de l'entreprise sur les réseaux sociaux et d'être plus efficaces.

Les risques pour l'entreprise

- **Risques éthiques et légaux**

Il existe des catégories de sites web qui ne sont pas professionnelles ou contraires aux lois ou à l'éthique de l'entreprise (drogue, terrorisme, pornographie, etc.). Afin de protéger le salarié et son employeur, il convient de filtrer le surf en entreprise par l'utilisation de catégories thématiques.

- **Risques d'infection via le surf**

Un salarié peut infecter une entreprise via un fichier malveillant téléchargé sur Internet ou à partir d'un site web, lui-même infecté. Des solutions qui filtrent le trafic web existent pour limiter ces risques.

- **Risques de piratage de site web**

Les sites web peuvent être piratés et induire des pertes financières (perte de disponibilité), des impacts sur la réputation ou des infractions légales (fuite de données). Il faut garantir la protection de ces sites qui, bien souvent, sont hébergés par des sociétés externes.

- **Risques de perte de contrôle de son image**

Une entreprise peut rapidement perdre le contrôle de son image sur le web par :

- l'inexistence sur les réseaux sociaux et l'impossibilité de réagir rapidement à un événement ;
- l'usurpation d'identité dans les réseaux sociaux et l'envoi de messages non approuvés ;
- la non-maîtrise d'un événement générant un emballement médiatique (mauvais buzz) et des milliers de commentaires négatifs sur la Toile.

La communication sur les réseaux sociaux doit être gérée.

Pour aller plus loin :

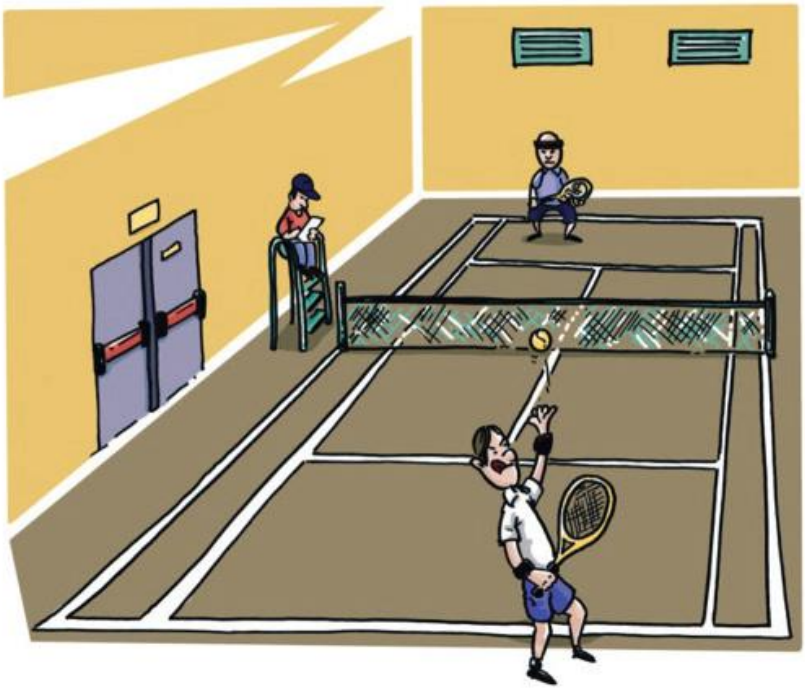
Niveau standard

Savez-vous le nombre exact de vos sites web exposés sur Internet ? Quelqu'un le sait-il vraiment ?

Niveau avancé

Avez-vous fait auditer techniquement la sécurité de vos sites web ?

9
CLOUD : LA TÊTE DANS LE NUAGE, LES PIEDS SUR TERRE



UNE FOIS TOUT MIGRÉ DANS LE CLOUD, LE COMEX TROUVA TOUT DE SUITE UNE IDÉE POUR TRANSFORMER L'ANCIENNE SALLE SERVEURS

Définition

Le cloud désigne l'hébergement chez un prestataire de solutions informatiques accessibles à distance. Les composants techniques utilisés sont opérés par le prestataire qui en assure la disponibilité et la mise à jour.

On distingue habituellement trois types de solutions cloud représentant 3 offres de services "clé en main" : de la location d'une seule infrastructure (IaaS*), d'une plateforme système administrée (PaaS*) jusqu'à l'offre de service logicielle (SaaS*).

Les enjeux métier

L'utilisation de service cloud permet de :

- accélérer la mise en service de solutions informatiques à l'international et sa réponse au marché ;
- rationaliser son budget en payant uniquement à l'usage et au consommé réel. Accroître sa flexibilité d'usage en fonction du besoin ;
- changer la nature des investissements matériels vers l'immatériel et optimiser son ratio CAPEX / OPEX ;
- s'affranchir dans une certaine mesure des problématiques d'obsolescence du système d'information* ;
- assurer la maîtrise de l'accès à ses données dans le respect des lois (ex. RGPD*).

Les risques pour l'entreprise

La centralisation : elle augmente la surface d'exposition aux attaques. Il s'ensuit des menaces plus fréquentes. De façon générale, toute faille d'un système exposé sur Internet a des répercussions immédiates. Par exemple, des robots cherchent en permanence des vulnérabilités exposées.

La connaissance : le système d'information* est administré techniquement par un tiers, ce qui engendre la perte de savoirs et de maîtrise interne du système d'information*.

La confidentialité : les fuites de données sont souvent dues à une mauvaise configuration des accès par les clients ou par des dispositifs de protection défaillants de l'hébergeur.

La réversibilité et portabilité : lors de la clôture ou de la résiliation d'un contrat, il est primordial de pouvoir récupérer ses données dans un format intelligible et réutilisable chez un autre fournisseur. Attention aux risques de trop forte **dépendance**.

Un surcoût lié à une utilisation abusive : mauvaise configuration, prévisions sous-estimées ou piratage de ressources*.

La non-maîtrise de la **disponibilité** induit une dépendance au fournisseur de service et peut entraîner une perte de service.

Shadow-IT* : le métier s'affranchit de la DSI et met en péril la continuité, la sécurité des données et l'image de l'entreprise.

Pour aller plus loin :

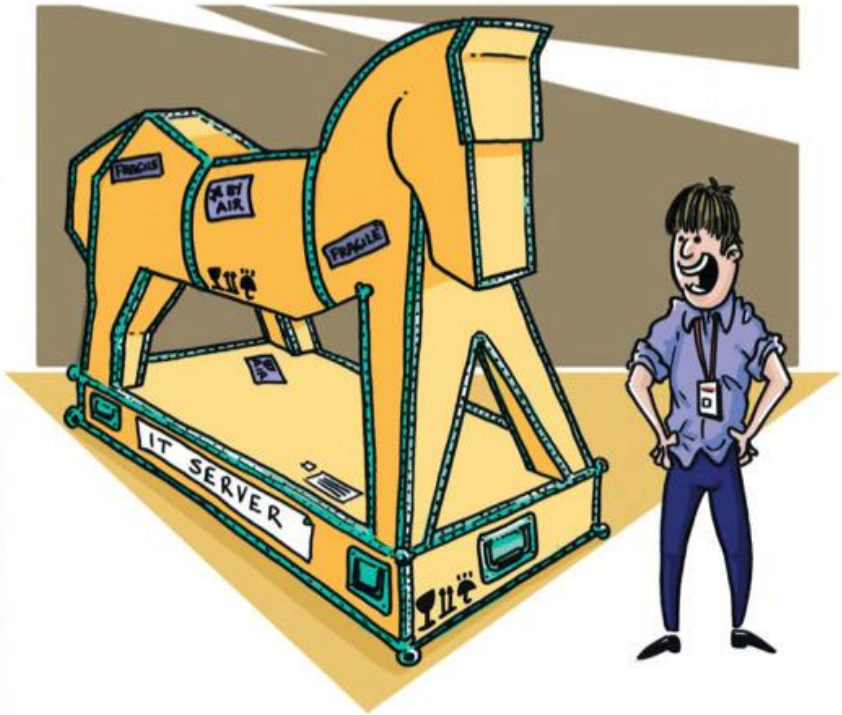
Niveau standard

Connaissez-vous le nombre exact de services cloud utilisés par votre entreprise ? Quelqu'un le sait-il vraiment ?

Niveau avancé

Avez-vous vérifié la présence et le fonctionnement d'une clause de réversibilité des données ?

10
PARTENAIRES : LES LIAISONS DANGEREUSES



<< J'AI HÂTE D'INTÉGRER LE NOUVEAU SERVEUR DANS NOTRE RÉSEAU! >>

Définition

L'entreprise se consacre avant tout à son cœur de métier. Pour tout le reste, en fonction de sa stratégie, de sa maturité et de sa taille, la délégation de service est une pratique commune. Elle est réalisée par des prestataires ou des partenaires.

Nous considérons ici la chaîne d'approvisionnement (Supply Chain) comme l'ensemble des partenaires et des fournisseurs impliqués dans les processus et activités permettant la création des biens et/ou services fournis par l'entreprise.

Les enjeux métier

Les enjeux de la sous-traitance résident dans la flexibilité et la fluidité de la ressource. C'est le partenaire qui adapte son dispositif aux surcharges ou sous-charges éventuelles, permettant à l'entreprise de se concentrer sur son cœur de métier et aux développements des compétences critiques.

C'est souvent le cas en informatique, où les développements de logiciels sont sous-traités à des entreprises spécialisées. Dans ce cas, on s'appuie sur leur expertise pour obtenir un logiciel de qualité et exempt de vulnérabilité.

En contrepartie, une sous-traitance s'accompagne d'une perte de compétences internes sur le fonctionnement de l'entreprise (processus, outils, marchés, etc.).

C'est tout l'enjeu d'une vision d'externalisation que de mesurer les gains au regard de cette perte de connaissances.

Afin de maximiser les bénéfices d'une sous-traitance, l'interconnexion du système d'information* de l'entreprise avec celui de son partenaire permettra un meilleur travail collaboratif.

Les risques pour l'entreprise

En cas de prêt de ressources*, l'entreprise doit non seulement s'assurer de la compétence de la ressource avant sa prise de fonction, mais également de son intégrité afin d'éviter toute fuite d'information, négligence ou malveillance.

En cas d'interconnexion de réseau, il faut garder à l'esprit que vos prestataires n'ont pas forcément la même hygiène informatique ou la même exigence en matière de sécurité. Plusieurs risques sont à envisager, entre autres celui d'infections virales par propagation ou de rebonds d'un pirate par l'intermédiaire des liens de partage.

En cas de développement ou d'installation de logiciel, il faut s'assurer qu'aucune vulnérabilité de sécurité n'est présente dans le produit, afin de ne pas permettre à un pirate de l'exploiter. Cela peut être un acte volontaire (on parle alors de porte dérobée*) ou d'un code mal sécurisé qui introduit des vulnérabilités supplémentaires dans votre système d'information. Dans tous les cas, un contrôle du code et/ou un audit doit faire partie de la procédure de réception.

Le **RGPD*** indique en cas de délégation que les obligations fixées restent identiques en matière de protection de données personnelles. Une entité qui sous-traite reste responsable des traitements. On parle de coresponsabilité.

Pour aller plus loin :

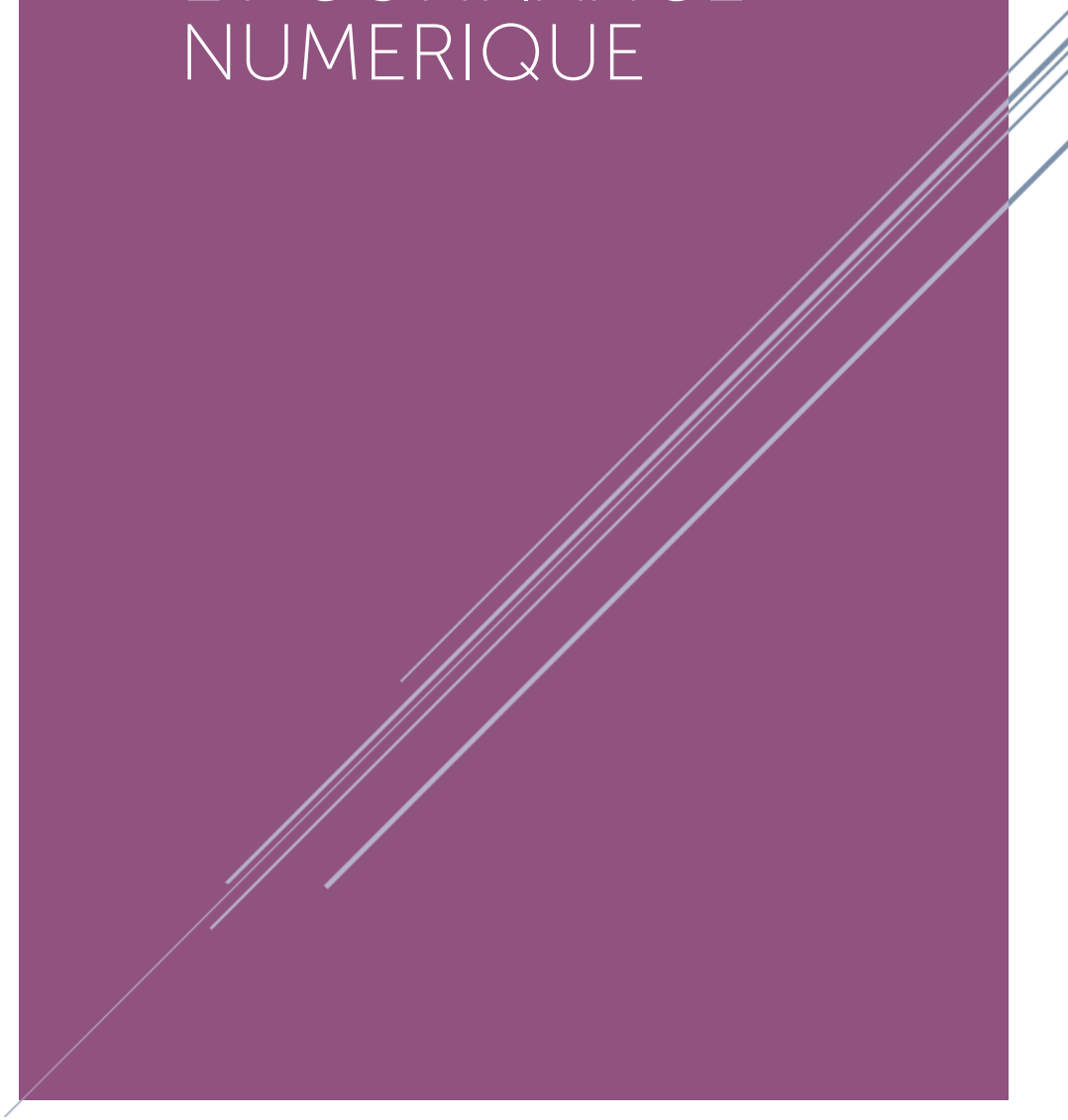
Niveau standard

Un de vos partenaires subit une cyberattaque, êtes-vous en sécurité ?

Niveau avancé

Comment savez-vous qu'aucun produit fourni par votre partenaire ne vous expose à une faille de sécurité ? Comment le qualifier ?

GOUVERNANCE ET CONFIANCE NUMERIQUE



11
JURIDIQUE : DURA LEX, SED LEX

<< AU VOLEUR! >>
<< NON! JE FAIS VALOIR MON DROIT À L'ANONYMAT >>

Définition

Devant l'apathie relative des entreprises en matière de cybersécurité et face aux enjeux sociétaux croissants du numérique, les États ont réagi avec de nouvelles réglementations pour protéger les clients et les citoyens.

La France, pionnière dans le domaine, a adopté dès 1978 les premières lois sur la protection des données personnelles. Plus récemment, en 2013, c'est la **Loi de Programmation Militaire** (LPM) qui impose aux 200 entreprises les plus stratégiques du pays, qualifiées d'Opérateurs d'Importance Vitale (OIV), de renforcer la sécurité de leurs systèmes informatiques critiques. Dans le même esprit, les instances européennes ont adopté en juillet 2016 la directive **Network and Information Security** (NIS). Elle a pour objectif d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne jugés essentiels pour l'activité économique et sociétale des pays.

Sur le sujet de la protection des données à caractère personnel, le **Règlement Général sur la Protection des Données (RGPD*)** applicable en mai 2018 renforce et unifie la protection des données pour les citoyens de l'Union européenne. Cette tendance se poursuit en 2020 avec l'**ePrivacy**, qui renforce la protection des communications électroniques personnelles et de leurs métadonnées*.

Les enjeux métier

Associée jusqu'ici à l'idée de contraintes et de dépenses, la cybersécurité doit être considérée aujourd'hui comme un atout compétitif et un investissement productif. La conformité (RGPD*, LPM...) devient un critère de sélection pour les clients soucieux à l'idée de confier des données personnelles, voire sensibles.

En interne, la « pression » légale des décrets d'application joue le rôle de catalyseur pour les projets de mise en conformité, ce qui in fine augmente le niveau global de sécurité de l'entreprise. Par exemple, le RGPD* apporte

une plus grande transparence des acteurs grâce à la notification obligatoire en cas de fuite de données.

Les risques pour l'entreprise

Les risques principaux de non-respect de la législation sont de deux natures.

- Un **risque juridique** accompagné de pénalités financières ou pénales : jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise pour une violation grave du RGPD* et jusqu'à 5 ans d'emprisonnement.

  Les instances nationales de surveillance ont vu leur pouvoir se renforcer et de nombreux audits sont actuellement en cours, amenant à des sanctions jusque-là jamais atteintes (ex. : amende de 50 millions d'euros pour Google par la CNIL).

- Un **risque d'image et une perte de confiance** des clients, investisseurs ou collaborateurs internes en cas de fuite de données personnelles massive. Cette perte de confiance, dans un contexte de mutation numérique, peut être très préjudiciable pour le futur de l'entreprise.

  Toutes ces nouvelles lois numériques contribuent à une meilleure hygiène informatique et à une montée globale de la maturité des entreprises dans ce domaine. Cette contrainte légale est donc une opportunité.

Pour aller plus loin :

Niveau standard

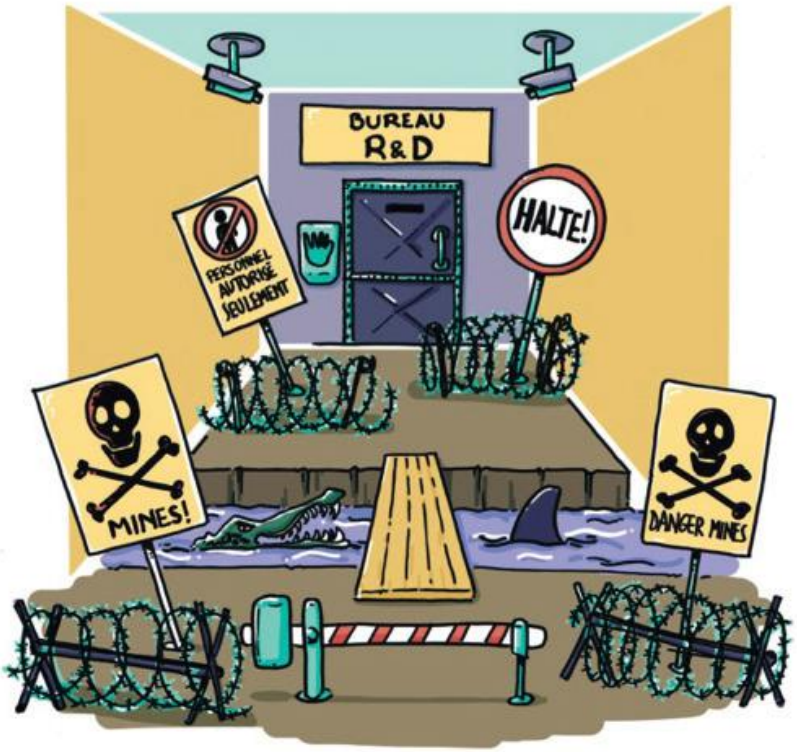
Savez-vous combien vous a coûté l'intégration du RGPD* dans votre système d'information ?

Niveau avancé

Qui anticipe chez vous les prochaines lois numériques et leurs impacts sur votre entreprise ?

12

PROPRIÉTÉ INTELLECTUELLE : PROTÉGER L'IMMATÉRIEL DANS UN MONDE IMMATÉRIEL



<< RIEN NE RENTRE! >>
<< OUI...MAIS RIEN NE SORT NON PLUS... >>

Définition

Est-il encore nécessaire d'expliquer ce qu'est la propriété intellectuelle ? Sûrement pas. Cependant, les récentes mutations technologiques liées à Internet en bouleversent l'approche et la maîtrise.

Là où, auparavant, l'entreprise avait une logique de "coffre-fort", le patrimoine informationnel est aujourd'hui disséminé entre les logiciels internes, les cloud ou les solutions non déclarées, dites Shadow IT*. Cela modifie considérablement les enjeux et les risques sur ce sujet.

Les enjeux métier

L'avance technologique n'est pas qu'une simple question de protection de la propriété intellectuelle. À l'ère numérique, une possibilité consiste à privilégier l'agilité et la rapidité d'exécution à la protection. Cette approche est pertinente pour certains domaines où la durée de vie du produit est courte mais n'est pas universelle.

L'essor du big data et des nouveaux métiers associés promettent, entre autres, un gain en marketing et R&D, ce qui place la donnée dans son ensemble comme un nouvel Eldorado, induisant de nouveaux challenges en propriété intellectuelle.

Les entreprises sont aujourd'hui plus ouvertes aux collaborations externes (partenariats industriels, universitaires, etc.). L'équilibre entre cette ouverture et la protection intellectuelle est à définir.

Les nouvelles technologies permettent parfois des usages violant la propriété intellectuelle (par exemple le téléchargement illicite, échange peer-to-peer). Il faut veiller à ne pas faire d'amalgame et à ne pas diaboliser la technologie.

Dans un contexte international et du fait de la dispersion de l'information liée au cloud, il faut conserver la maîtrise de son patrimoine informationnel.

Les risques pour l'entreprise

Face à la multiplication incontrôlée des cloud, le risque est de ne plus savoir où sont ses informations et quels sont les niveaux de protection associés (exemple : manque d'inventaire, de clauses contractuelles...).

Par ailleurs, le vol se mue en copie numérique, ce qui est difficile à détecter.

Enfin, il y a une difficulté technique et juridique à protéger parfaitement ses données dans le monde numérique : cela est dû à l'absence de législation homogène sur les brevets logiciels et la possibilité de rétroconception des produits.

Pour aller plus loin :

Niveau standard

Est-ce un problème si votre patrimoine informationnel, c'est-à-dire le savoir métier et client de votre entreprise, est aujourd'hui éparpillé dans différents cloud à travers le monde ?

Niveau avancé

Quel est le juste coût de la protection intellectuelle traitée par votre système d'information ?

13
CERTIFICATION : PROVIDENCE, PARATONNERRE OU PARAPLUIE ?

<< ENCORE UNE OU DEUX CERTIFICATIONS ET ON POURRA ENFIN LANCER NOS PRODUITS SUR LE MARCHÉ >>

Définition

Être certifié, c'est répondre à un cahier des charges donné par une norme établie par des organisations externes.

Le processus est tripartite :

- l'organisme audité (qui implémente la norme) ;
- l'organisme de certification indépendant accrédité par une autorité d'accréditation (COFRAC en France) ;
- un référentiel normatif qui contient les exigences à respecter.

Les normes les plus connues sont :

- ISO9001 : définit les critères d'un système de management en prônant une approche processus et l'amélioration continue ;
- ISO27001 : mise en œuvre d'un système de management de la sécurité de l'information ;
- ISO27005 : gestion des risques dans le contexte de la sécurisation des systèmes d'information.

Hors obligation sectorielle ou légale (par exemple le référentiel PCI-DSS pour les acteurs de la chaîne monétique des cartes de paiement), une certification n'est pas obligatoire. Une organisation peut mettre en place un Système de Management de la Sécurité de l'Information répondant partiellement aux exigences exprimées.

Les enjeux métier

Les enjeux d'une certification :

- **Reconnaissance/Crédibilité** : être reconnu par un organisme accrédité et indépendant.
- **Financier** : un effort anticipé sur la durée coûte moins cher qu'un effort « one shot » à la suite d'une crise.

- **Marketing** : parfois, les certifications font partie des exigences d'appel d'offres.
- **Optimisation** : une certification engendre une plus grande maturité des processus, favorise l'amélioration continue et développe une culture commune au sein de l'entreprise.

Les risques pour l'entreprise

Ne pas être certifié, c'est prendre le risque :

- **D'un point de vue business** : de rater les appels d'offres, de ne pas respecter les exigences légales et réglementaires.
- **D'un point de vue managérial** : la certification peut modifier profondément la structure de l'entreprise et nécessite l'appui inconditionnel de la direction. L'engagement budgétaire et humain est important : il ne faut pas le sous-estimer.
- **D'un point de vue technique** : obtenir une certification de complaisance ou par un organisme non accrédité qui couvre les aspects procéduraux sans en avoir les moyens techniques. Cela induit un faux sentiment de sécurité : la certification ne protège pas contre les cyberattaques.

La technique seule ne saurait pallier l'ensemble des menaces sans prendre en compte les aspects fonctionnels et de gouvernance.

Pour aller plus loin :

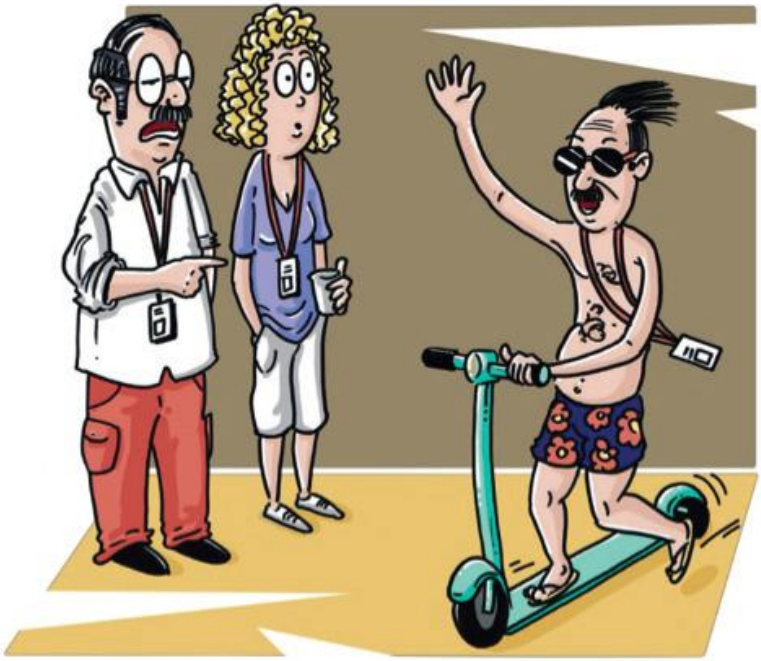
Niveau standard

Dans quelle mesure une certification ISO 27001 protège-t-elle d'une cyberattaque ?

Niveau avancé

Comment calculez-vous l'efficience de votre certification ISO 27001 ?

14
ATTRACTIVITÉ : EMBAUCHE-MOI SI TU PEUX



ESPRIT START-UP: ROGER POUSSE LE BOUCHON UN PEU TROP LOIN...

Définition

Une entreprise est attractive lorsqu'elle attire spontanément les meilleurs candidats et sait conserver ses talents, mais également lorsqu'elle séduit de nouveaux clients. Sa marque joue un rôle important dans l'atteinte de cet objectif et repose, en partie, sur son identité numérique. Celle-ci se définit par :

- l'image qu'elle donne à travers ses **sites web** ;
- sa présence et son dynamisme sur les **réseaux sociaux** grand public et professionnels (qualité, quantité & réactivité) ;
- l'image de l'entreprise renvoyée par les **publications** la concernant ;
- des **témoignages** et notations de ses salariés, de ses dirigeants ou de ses clients ;
- ses **valeurs** et sa **culture**.

Les enjeux métier

- Renvoyer une **image** de son entreprise conforme à ses valeurs, inciter les meilleurs à la rejoindre et renforcer la motivation et l'engagement des autres parties prenantes.
- Assurer la **confiance** de ses clients vis-à-vis de l'intégrité du système d'information* et du patrimoine informationnel confié.

La cybersécurité est un domaine en tension. Le **recrutement** de profils compétents est clé pour assurer la protection de votre entreprise. Cette capacité à recruter est directement liée à sa réputation.

Les risques pour l'entreprise

L'e-réputation peut-être facilement entachée par de la manipulation d'informations : des "fake-news", un changement de contenu d'un site

web, l'association de contenu non-éthique avec votre société, l'usurpation d'identité ou de nom de domaine, l'implication involontaire dans des actes répréhensibles.

Le risque est de perdre le contrôle de votre image, et donc de nuire à votre attractivité.

Pour aller plus loin :

Niveau standard

Savez-vous ce que l'on dit de votre entreprise sur les réseaux sociaux ?

Niveau avancé

Vos ressources informatiques* sont-elles formées à la cybersécurité ?

15

SOUVERAINETÉ NUMÉRIQUE : L'ESPIONNAGE ÉCONOMIQUE VOUS REMERCIE

« JE VOUS ASSURE QUE SUR NOTRE CLOUD, VOS DONNÉES NE SERONT PAS PARTAGÉES AVEC UN ÉTAT ÉTRANGER »

Définition

La **souveraineté** est la capacité pour une entité à définir ses propres règles. Elle s'oppose à l'ingérence.

La **souveraineté numérique** consiste à **maîtriser** les impacts du numérique sur nos vies et nos activités, par une **alliance** entre l'État et les entreprises. Le concept a été développé afin de répondre à la domination états-unienne actuelle de l'Internet illustrée par la centralisation des institutions, des acteurs et des données sur son territoire et le pouvoir de ses agences de renseignement.

Cela demande une **prise de conscience** collective et politique sur toute la chaîne du numérique, autant matérielle que logicielle.

Les enjeux métier

- Protéger le patrimoine informationnel de son entreprise.
- Renforcer la souveraineté de l'État dans le domaine du numérique pour garantir les services régaliens et la protection de ses citoyens.

Cela est uniquement possible à condition d'avoir des acteurs économiques locaux en mesure de proposer des solutions matérielles et logicielles compétitives.

Ces enjeux sont **économiques, éthiques et géopolitiques** : les individus ont le droit à la confidentialité de **leurs données** et de leur **vie privée**. Ceci est exacerbé dans un contexte où certains États utilisent leur capacité d'écoute pour faire de l'intelligence économique.

Il est donc important d'évaluer ce risque stratégique.

Le **RGPD*** illustre parfaitement le rapport de forces difficile entre la protection des données personnelles des citoyens européens et son application mondiale. La souveraineté numérique croise les autres types de souveraineté, ce qui induit des **conflits**.

Les risques pour l'entreprise

- L'ingérence facilitée par une porte dérobée* dans des systèmes d'information mise en place par des acteurs étatiques étrangers. Cela peut se traduire par la perte de données confidentielles ou par le sabotage destiné à déstabiliser une entité (ex. : la crise des centrales électriques au Venezuela en 2019).
- Une politique extraterritoriale d'un pays en sa faveur s'appliquant mondialement en opposition à la souveraineté des autres pays. Par exemple, en utilisant le Patriot Act (ou Cloud Act* ou e-Discovery*), la justice américaine peut trouver des indices* dans les données d'une société prouvant un commerce avec un pays sous embargo.

Pour aller plus loin :

Niveau standard

Connaissez-vous l'ANSSI ?

Niveau avancé

Avez-vous été sensibilisé personnellement aux risques cyber ?

NOTEZ VOTRE CONNAISSANCE DE LA CYBERSÉCURITÉ

À travers ce guide, nous vous invitons à découvrir les sujets importants qui affectent votre entreprise. Pour chaque question en fin de chapitre, notez de 0 à 5 votre niveau de connaissance. 0 représentant une absence totale d'information, 5 étant une maîtrise parfaite de l'implémentation et du suivi.

		Standard	Avancé
Mon entreprise	Courrier électronique : La face cachée		
	BYOD/ATAWAD : Jamais sans mon portable		
	Accès distant : Accéder au SI depuis un voilier		
	L'annuaire d'entreprise : Un service pour les gouverner tous		
	Cycle de vie : Pourquoi remplacer ses minitels ?		
	PRA*/PCA* : Survivre à un Armageddon		

		Standard	Avancé
L'entreprise interconnectée	DNS* : L'annuaire mondial que vous utilisez sans même le savoir		
	WWW : La ruée vers le Web		
	Cloud : La tête dans le nuage, les pieds sur terre		
	Partenaires : Les liaisons dangereuses		

		Standard	Avancé
Gouvernance & confiance numérique	Juridique : Dura lex, sed lex		
	Propriété intellectuelle : Protéger l'immatériel dans un monde immatériel		
	Certification : Providence, paratonnerre ou parapluie ?		
	Attractivité : Embauche-moi si tu peux		
	Souveraineté numérique : L'espionnage économique vous remercie		

GLOSSAIRE

A

Arnaque (ou fraude) au président : Pratique consistant pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers.

ATAWAD (Any Time, Any Where, Any Device) : Capacité d'un usager en situation de mobilité à se connecter à un réseau sans contrainte de temps, de localisation ou de terminal.

AVEC : « Apportez Votre Équipement personnel de Communication ». Voir BYOD.

B

BYOD (Bring Your Own Device) : Pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel.

C

Cheval de Troie : Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante.

Chiffrement des données : Technique rendant les données illisibles, sauf si une action spécifique (déchiffrement) est exercée pour en autoriser l'accès.

Cloud Act : Loi fédérale des États-Unis adoptée en 2018 sur la surveillance des données personnelles, notamment dans le cloud. Cette loi permet aux forces de l'ordre US de contraindre les fournisseurs de services américains à fournir les données demandées stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers.

Cybersquatting : Action malveillante qui consiste à faire enregistrer un nom de domaine dans le seul but de bloquer toute attribution ultérieure de ce nom au profit de titulaires plus naturels ou légitimes.

D

Décommissionnement : Fin de vie d'une application ou d'un équipement informatique.

Déni de service : Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

DNS : Système de bases de données et de serveurs assurant la correspondance entre les noms de domaine ou de site utilisés par les internautes et les adresses numériques utilisables par les ordinateurs.

E

E-discovery : Loi américaine permettant l'investigation et l'instruction préalable au procès civil et commercial qui est essentielle pour toute action en justice aux États-Unis. Les demandes de communication qui sont faites à cette occasion auprès des entreprises peuvent concerner des milliers de courriers électroniques des salariés. Le refus d'obtempérer peut déboucher sur un jugement défavorable.

H

Hameçonnage : Voir Phishing.

I

IaaS (Infrastructure as a Service) : Infrastructures de datacenters où le client déploie son système d'information. Par exemple : Amazon Web Service, Google Cloud Platform, Microsoft Azure, etc.

Ingénierie sociale : Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.

L

LDAP (Lightweight Directory Access Protocol) : Terme pouvant désigner le protocole, la structure de données ou l'implémentations des services d'annuaires.

MDM (Mobile Device Management) : Application permettant la gestion d'une flotte d'appareils mobiles, qu'il s'agisse de tablettes ou de smartphones.

Métadonnée : Donnée servant à définir ou à décrire une autre donnée, quel que soit son support. Un exemple type est d'associer à une donnée la date à laquelle elle a été produite ou enregistrée, ou à une photo les coordonnées GPS du lieu où elle a été prise.

MFA : *Multiple Factor Authentification,* ou vérification en deux étapes, est une méthode par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification.

Mobiquité : Fusion des termes « mobilité » et « ubiquité ». Voir ATAWAD.

P

PaaS (Platform as a Service) : Plateforme intégrant les services techniques essentiels (envoi de courriel, stockage de données, puissance de calcul, etc.) où le client installe ses couches métier. Par exemple, stockage de données en ligne, hébergeur d'environnement web, etc.

Patching : Mise à jour permettant de corriger une vulnérabilité, apporter une fonctionnalité ou améliorer le fonctionnement d'un logiciel.

PCA (Plan de Continuité d'Activité) : Il permet à un système d'information de fonctionner même en cas de désastre ou de crise majeure, quitte à ce que ce soit en « mode dégradé ».

Phishing : Vol d'identités ou d'informations confidentielles par subterfuge. Un système d'authentification est simulé par un utilisateur malveillant qui essaie de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

Porte dérobée : Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive.

PRA (Plan de Reprise d'Activité) : C'est un ensemble de procédures (techniques, organisationnelles, sécurité) qui permet à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d'information en cas de sinistre important ou d'incident critique.

R

Rançongiciel : Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Le terme « rançongiciel » (ou *ransomware* en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon.

Ressources : Ensemble des composants, matériels ou logiciels, connectés à un ordinateur. Tout composant de système interne est une ressource. Les ressources d'un système virtuel incluent les fichiers, les connexions au réseau, et les zones de mémoire.

RGPD (Règlement Général sur la Protection des Données) : Règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.

S

SaaS (Software as a Service) : Logiciel où le client assure la personnalisation de ses processus métier et de son identité visuelle. Par exemple, Microsoft Office 365, Salesforce, etc.

Shadow IT : Solutions informatiques non connues des équipes informatiques et donc hors du périmètre de suivi, de protection et de contrôle.

Surface d'attaque : Somme des différents points faibles (les « vecteurs d'attaque ») par lesquels un utilisateur non autorisé (un « pirate ») pourrait potentiellement s'introduire dans un environnement logiciel et en soutirer des données.

Système d'information : ensemble des matériels contenant les informations nécessaires pour accomplir la mission de l'entreprise et des réseaux permettant leurs échanges.

T

Typosquatting : Action malveillante qui consiste à déposer un nom de domaine très proche d'un autre nom de domaine, dont seuls un ou deux caractères diffèrent.

U

Utilisateurs privilégiés : Dans un système, il existe en général des utilisateurs disposant de droits spéciaux leur permettant d'administrer le système.

V

VPN (Virtual Private Network) : Système permettant de créer un lien direct entre des ordinateurs distants, via un réseau qui sécurise l'échange.

NOTE

CLUSIF
Web : https://clusif.fr/
Twitter : @clusif
Mail : clusif@clusif.fr

OSSIR
Web : https://ossir.org
Twitter : @OSSIRFrance
Mail : secretariat@ossir.org