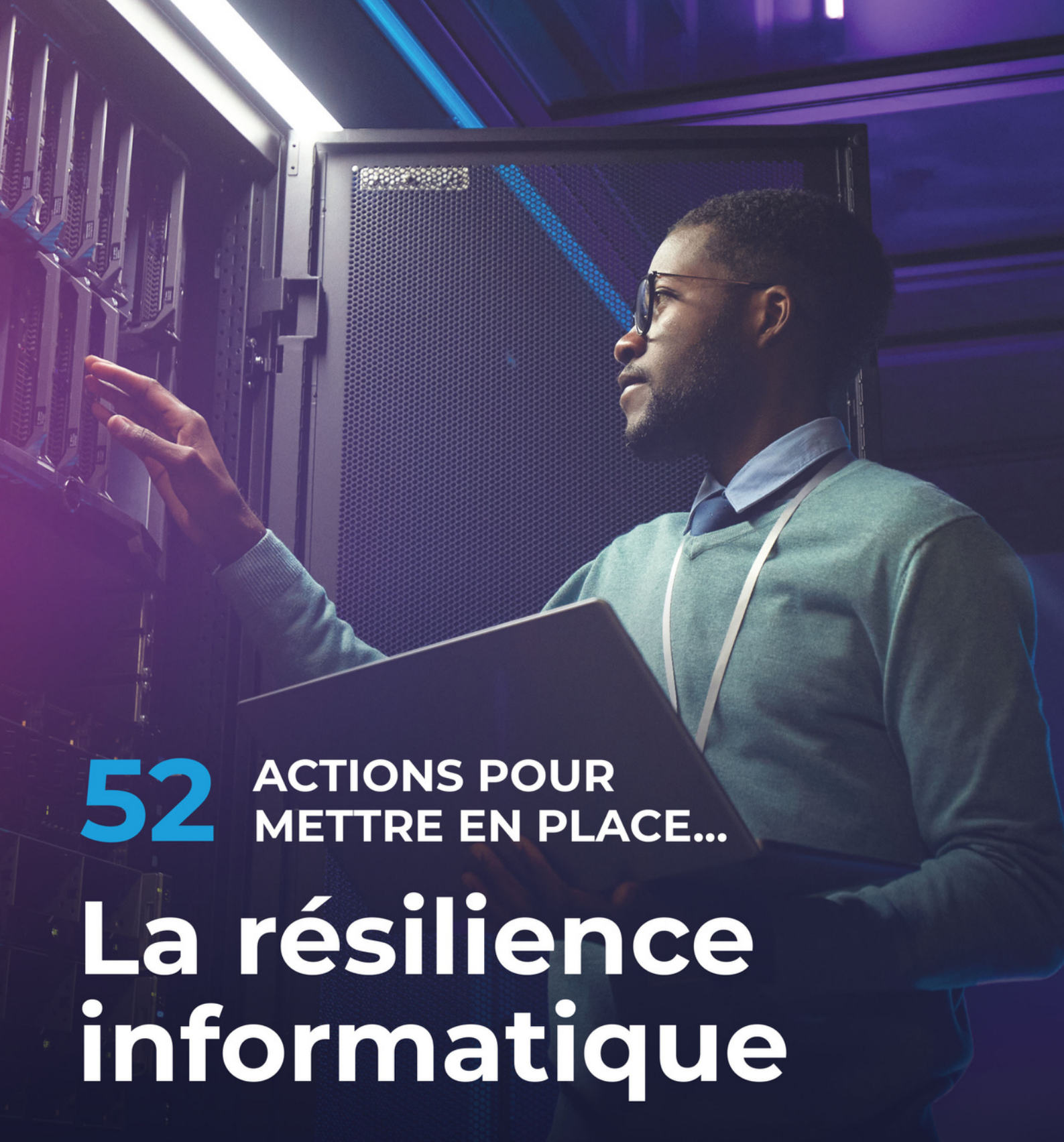


52 ACTIONS POUR METTRE EN PLACE...

La résilience informatique

LE LIVRE BLANC

Édition 2024

www.deessi.si

déessi

Au cœur de votre système d'information

Sommaire

52 ACTIONS POUR METTRE EN PLACE
LA RESILIENCE INFORMATIQUE

01
EDITO

Découvrez **Déessi** et les objectifs de ce livre blanc.

02
MODE D'EMPLOI

Nos conseils pour parcourir ce livre blanc et en tirer le meilleur parti.

03
INFRASTRUCTURE LOCALE

Action n°1 : Sécuriser et protéger son local informatique 4
Action n°2 : Disposer d'un pare-feu nouvelle génération 5
Action n°3 : Disposer d'onduleurs 6
Action n°4 : Virtualiser ses serveurs 7
Action n°5 : Redonder sa connexion Internet locale 8

10
POSTES DE TRAVAIL

Action n°6 : Assurer une mise à jour constante des postes de travail 11
Action n°7 : Disposer d'un anti-virus professionnel, centralisé et de dernière génération 12
Action n°8 : Avoir une politique de contrôle des accès 13
Action n°9 : Chiffrer ses disques dur, notamment les portables 14
Action n°10 : Centraliser la gestion des postes de travail et appareils mobiles 15

17
MESSAGERIE

Action n°11 : Héberger la messagerie sur un serveur dédié 18
Action n°12 : S'assurer de la sécurisation de sa messagerie électronique 19
Action n°13 : Externaliser la messagerie . 20

Sommaire

52 ACTIONS POUR METTRE EN PLACE LA RESILIENCE INFORMATIQUE

22

MESURES ORGANISATIONNELLES

Action n°14 : Formaliser sa politique de sécurité informatique 23
Action n°15 : Disposer d'une procédure d'arrivée et de départ pour collaborateurs .. 24
Action n°16 : Sensibiliser et former ses collaborateurs à la sécurité informatique ... 25
Action n°17 : Disposer d'un PCA / PRA 26
Action n°18 : Définir un RTO / RPO 27
Action n°19 : Nommer un DPO 28
Action n°20 : Disposer d'un RSSI 29
Action n°21 : Auditer son système d'information régulièrement 30
Action n°22 : Recourir à un prestataire externe pour auditer le SI 31
Action n°23 : Définir la charte informatique 32
Action n°24 : Être conforme au RGPD 33
Action n°25 : Avoir un registre de traitement des données 34
Action n°26 : Mettre en place des clauses de réversibilité avec ses prestataires 35
Action n°27 : Définir des SLA/garanties de services avec vos prestataires 36
Action n°28 : Vérifier la responsabilité civile de vos prestataires pour les risques informatiques 37
Action n°29 : Formaliser la politique de sécurité fournisseurs dans un PAS (Plan d'Assurance Sécurité) 38

46

SAUVEGARDE

Action n°36 : Réaliser une sauvegarde ... 49
Action n°37 : Externaliser la sauvegarde .50
Action n°38 : Réaliser des tests de sauvegarde 51
Action n°39 : Chiffrer sa sauvegarde 52
Action n°40 : Définir une fréquence de sauvegarde adaptée aux besoins de la structure 53

38

INFRASTRUCTURE EXTERNALISÉE

Action n°30 : Avoir une connexion Internet redondée avec bascule 41
Action n°31: Choisir un hébergement dédié 42
Action n°32 : Héberger son informatique externalisée en France 43
Action n°33 : Disposer d'un monitoring et d'une surveillance humaine du SI 44
Action n°34 : Contrôler et assurer la disponibilité du SI 45
Action n°35 : Mettre en place des remontées d'alertes automatiques 46

53

TRAVAIL A DISTANCE

Action n°41 : Sécuriser les accès au SI avec un VPN 56
Action n°42 : S'équiper d'une téléphonie Full IP 57
Action n°43 : Posséder une charte de télétravail 58
Action n°44 : Utiliser une solution de partage de documents professionnelle 59
Action n°45 : Fournir un matériel dédié uniquement aux usages professionnels 60
Action n°46 : Disposer d'un outil de visioconférence sécurisé 61

Sommaire

52 ACTIONS POUR METTRE EN PLACE LA RESILIENCE INFORMATIQUE

62

SITE WEB

Action n°47 : Établir un cloisonnement entre son site web et son réseau local 65
Action n°48 : Protéger son site web avec un antivirus / firewall / antispam 66
Action n°49 : Disposer d'un site web monitoré et infogéré 67
Action n°50 : Mettre à jour son site web en continu 68
Action n°51 : Activer le protocole HTTPS pour son site web 69
Action n°52 : Héberger son site web sur un serveur dédié 70

70

A PROPOS D'IVISION

Qui sommes-nous 71
Ligne éditoriale 73
Contactez-nous: 74

EDITO

Selon l'étude Global Data Protection Index (GDPI) de 2020 pour la France, 37 % des entreprises ont subi des temps d'inactivité non planifiés de leur système informatique, avec un coût moyen de 382 000 dollars.

L'objectif de ce livre blanc intitulé **"52 actions pour mettre en place la résilience informatique"** est de présenter un éventail des pratiques permettant aux entreprises d'assurer la résilience de leur système d'information.

Résilience informatique : la capacité d'assurer la **continuité du fonctionnement** de son système d'information, en cas de **panne**, de **pic d'activité**, de **piratage informatique**, d'**erreur humaine** et plus généralement pour toute situation inopinée"

Découvrez à travers cet ouvrage **52 actions concrètes** pour protéger votre système d'information, réduire les risques de piratage ou d'indisponibilité, ou encore, disposer des procédures adéquates pour assurer la continuité **en cas de sinistre** informatique**.**

Ce livre blanc vous offrira des **réponses à des questions** telles que :

- Quelles sont les meilleures pratiques en matière de **sauvegarde informatique** ?
- Faut-il obligatoirement **nommer un DPO** pour la gestion des données personnelles ?
- Dans **quel pays** vaut-il mieux choisir son **hébergement informatique** ?
- Quels sont les avantages d'un prestataire externe pour un **audit de SI** ?
- Quels sont les usages d'une **charte informatique** et d'une **charte de télétravail** ?
- Qu'est-ce qu'une **clause de réversibilité** et comment l'établir avec ses prestataires ?
- etc.

Outre **le concept** en lui-même, chacune des actions présentées est accompagnée de **ses enjeux**, utiles à la prise de décision, et de **ses avantages**, pour y voir clair sur les bénéfices pour votre structure.

Nous vous souhaitons une excellente lecture !

Déessi, au cœur de votre système d'information
Certifiée ISO27001 pour ses services d'hébergement informatique et de sauvegarde de données.

Mode d'emploi

Comment utiliser ce livre blanc ?

PRINCIPE

Ce livre blanc est organisé en **8 chapitres** et **52 actions**. Certaines de ces actions sont liées et amènent parfois à des répétitions. C'est parce que nous avons voulu construire cet ouvrage **comme un outil**, et que **chaque action** et **chaque chapitre** peut être **parcouru de façon individuelle** et **dans n'importe quel ordre**.

DÉCOUPAGE D'UN CHAPITRE

Un chapitre est découpé en **3 parties distinctes** :

- **L'introduction**, qui présente et contextualise le sujet,
- **Les actions** (entre 4 à 15 actions par chapitre),
- Une section "**Pour aller plus loin**" pointant vers des ressources supplémentaires pour approfondir l'une des notions abordées. De plus, vous y retrouverez un lexique contenant certaines notions abordées dans le chapitre, et qui sont indiquées dans le corps du texte par un astérisque.

DÉCOUPAGE D'UNE ACTION

Ce livre blanc comporte 52 actions. Chaque action se découpe en **3 parties** :

- La partie "**Principe**" qui introduit le point abordé dans cette action,
- La partie "**Enjeux**" qui explicite plus précisément ce point et mentionne les enjeux de cette action, notamment vis-à-vis de la cyber-résilience,
- La partie "**Avantages**" qui résume les avantages apportés par cette action.

VOS QUESTIONS ET REMARQUES

Nous espérons que cet ouvrage vous apporte un éclairage concret sur la thématique de la cyber résilience et ses problématiques associées à la gestion et au développement de votre entreprise. Nous avons souhaité aborder un large éventail de notions, tout en restant **simple** et **pédagogique**. Bien évidemment, ce livre blanc ne peut prétendre à l'exhaustivité. Nous vous remercions par avance de votre compréhension si vous constatez qu'une problématique est manquante.
Pour toute remarque ou commentaire, merci de nous contacter à l'aide du lien présent ci-dessous.

Des remarques ? Des questions ?
N'hésitez pas à nous contacter via notre site Internet.
Rendez-vous sur https://www.deessi.si/contact/

INFRASTRUCTURE LOCALE

L'infrastructure informatique d'une entreprise correspond à tous les éléments matériels (notamment serveurs), logiciels, réseaux et câblages qui permettent le **fonctionnement de l'environnement informatique** de l'entreprise.

On parle **d'infrastructure locale** lorsque ces éléments sont hébergés **au sein des locaux de l'entreprise**, par opposition à une infrastructure hébergée sur une plateforme externe, dans le Cloud et / ou chez un hébergeur professionnel.

Action n°1 : Sécuriser et protéger son local informatique

PRINCIPE

Au-delà des dangers immatériels liés aux menaces informatiques, le système d'information repose sur des structures physiques, notamment des serveurs, qui abritent les données et les applications de l'entreprise. Il ne faut pas sous-estimer la **fragilité des équipements**, ni la possibilité qu'ils soient soumis à des **incidents dans le monde physique**. C'est là toute l'utilité de la **sécurisation**, de **l'entretien** et de la **protection** des locaux abritant les équipements.

ENJEUX

Différents éléments sont à prendre en compte pour **assurer l'intégrité physique** des **machines** et des **serveurs** de l'entreprise.

- **Restrictions** et **contrôles d'accès** permettant de limiter des malfaisances ou des erreurs humaines
- **Climatisation de la salle**, car un arrêt de la climatisation signifie souvent une surchauffe ou un arrêt de fonctionnement des appareils
- Lutte et prévention des **catastrophes naturelles** (incendies, inondations, etc.)
- Lutte et prévention des **autres incidents**, comme les surtensions électriques par exemple.

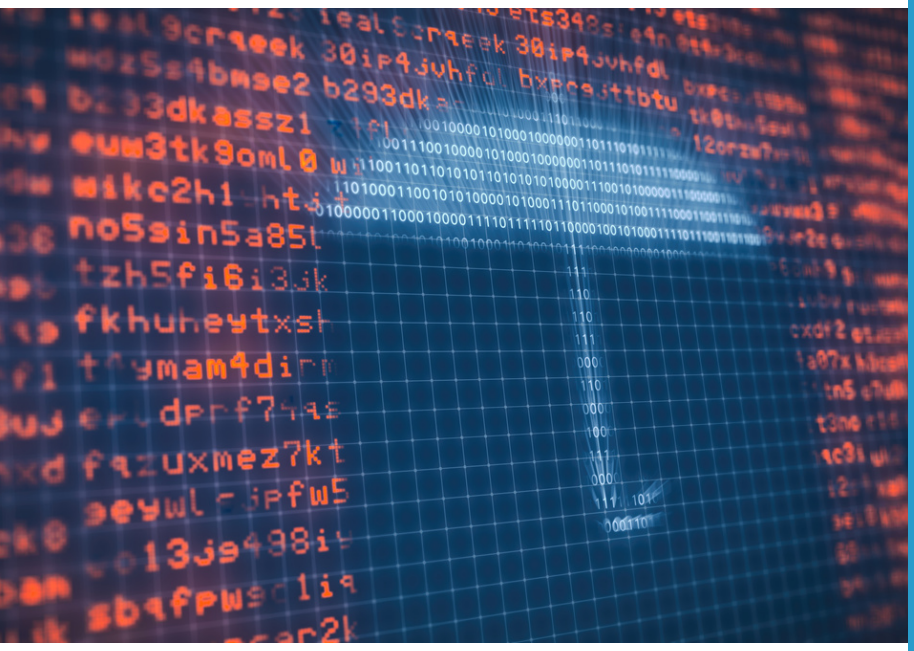
Outre les **mesures de protection**, qui permettent de prévenir les incidents, **l'entretien** du matériel de ses **bonnes conditions de fonctionnement** est essentiel pour diminuer les risques. De plus, en cas d'incident avéré, des **mesures correctrices** doivent être également prévues afin de protéger le matériel malgré le sinistre et d'en assurer la continuité de fonctionnement.

Dans le cadre d'un **hébergement local**, confier l'étude des risques et leur prévention à un prestataire expert permettra de **diminuer la probabilité d'incidents.** Cependant, pour une prise en charge maximale, il sera plus efficace de choisir un hébergement externalisé sécurisé, assuré au sein d'un datacenter professionnel. En effet, ces hébergements professionnels sont actuellement à la pointe en matière de sécurisation physique et toutes leurs garanties et services associés sont précisés au sein de contrats d'hébergement.

AVANTAGES

- Alimentation redondante
- Refroidissement
- Lecteurs de badge
- Système biométrique
- Vidéosurveillance 24/24
- Sécurité incendies

Action n°2 : Disposer d'un pare-feu nouvelle génération



PRINCIPE

De plus en plus soumises aux attaques informatiques, les entreprises doivent disposer de solutions permettant de **limiter les intrusions sur leur réseau**.

Un pare-feu est un système logiciel et/ou matériel de **protection informatique** qui a pour but de **filtrer** l'accès de certains flux entrant et sortant dans le système, ce qui permet notamment de stopper les attaques ou les intrusions **avant leur entrée dans le système**. Les pare-feux nouvelle génération disposent de fonctionnalités avancées. On distingue le pare-feu de l'antivirus, dont l'action se déroule au sein même du système.

AVANTAGES

- Gestion à distance
- Automatisation de scénarios
- Personnalisation de protocoles

ENJEUX

Le pare-feu permet de **surveiller le trafic réseau entrant,** et de **gérer le trafic inconnu** avec des règles spécifiques.

En particulier, les **pare-feux de nouvelle génération** comprennent mieux les détails du trafic mesuré et ont des fonctionnalités supplémentaires. Au-delà des **réglages traditionnels** (filtrage de paquets, inspection dynamique, proxy* *(voir lexique)*, blocage d'IP, blocage de noms de domaine, blocage de ports etc.) les pare-feux nouvelle génération disposent de **systèmes de prévention des intrusions** et **d'inspection des paquets** avancés.

De plus, ils **identifient mieux** la provenance du trafic et offrent une **gestion des droits basée** sur les annuaires d'utilisateurs.

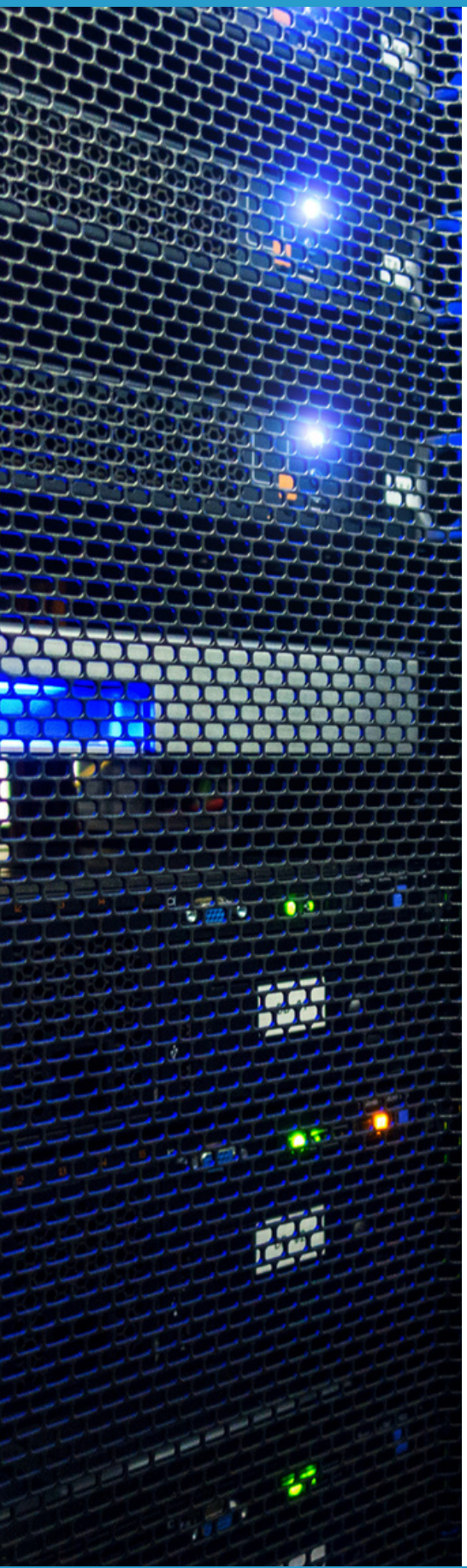
Enfin, entre autres fonctionnalités, certains permettant également de **déchiffrer** et **analyser le trafic chiffré** avec SSL/TLS* *(voir lexique)*.

À noter que ces pare-feux nécessitent des licences qui doivent être mises à jour régulièrement.

Quel que soit le pare-feu sélectionné, le défi reste pour les organisations d'obtenir cette sécurité optimale **tout en conservant de hautes performances**.

Dans une optique de résilience, il est également opportun de redonder son pare-feux afin de permettre la continuité d'activité en cas de panne.

Action n°3 : Disposer d'onduleurs



PRINCIPE

Utilisé dans le cadre d'installations informatiques, un **onduleur** est un matériel qui **détecte une panne d'électricité** ou **une surtension** et permet de **continuer à alimenter** en électricité votre système informatique, grâce à des batteries.

Ainsi, l'objectif est de permettre la **protection du système d'information**, même en cas de **panne électrique**.

ENJEUX

Parce que dans certains cas, les incidents et panne de courant peuvent être fréquents, l'onduleur est un élément essentiel de **la résilience** de votre système d'information.

En effet, l'onduleur apporte une protection à votre système contre les **incidents électriques** de type microcoupures, pics de tension, surtensions, creux de tensions, parasites ou encore variations de fréquence.

Pour bien dimensionner le choix votre onduleur, vous devrez vous assurer de sa capacité à fournir la **puissance nécessaire** à votre système et à vos équipements en cas de panne.

Vous devez également vous assurer que la **durée d'autonomie** de l'onduleur s'intègre dans le **PCA**/**PRA*** *(voir lexique)* que vous avez idéalement établi.

De plus, la **taille** de l'onduleur ou la **vitesse de rechargement** des batteries pourront être des critères de choix supplémentaires.

À noter par ailleurs que les batteries des onduleurs ont une **durée de vie limitée** (entre 3 et 5 ans). Il faut donc les tester régulièrement et les remplacer si nécessaire.

Dans une optique de résilience informatique, il est également important de redonder votre onduleur.

AVANTAGES

- Protection contre les incidents électriques
- Assure la continuité d'activité en cas de panne d'électricité et permet un arrêt conforme des serveurs

Action n°4 : Virtualiser ses serveurs

PRINCIPE

La **virtualisation de serveurs** consiste à **diviser un serveur physique** en **plusieurs instances virtualisées** indépendantes.

Chaque **serveur virtuel** ainsi créé fonctionne comme **une machine indépendante** et peut disposer d'un système d'exploitation et de ses propres paramètres et applications. Les ressources du serveur initial sont **divisées et réparties entre les différentes instances** de façon à leur permettre un fonctionnement approprié et efficient.

AVANTAGES

- Réduction du nombre des serveurs physiques
- Flexibilité d'attribution des ressources
- Optimisation des coûts
- Optimisation énergétique
- Optimisation des performances
- Simplification de gestion, PCA/PRA, sauvegardes

ENJEUX

La **virtualisation de serveurs** possède de nombreux intérêts :

- Le plus important réside dans **la flexibilité** apportée par cette nouvelle organisation des systèmes, puisqu'il est possible d'allouer les éventuelles **ressources non utilisées à d'autres instances**, tout en conservant la possibilité de les réattribuer en fonction des priorités. En effet, un serveur informatique est **généralement sous-utilisé**, du fait de la nécessité de conserver des ressources en réserve en cas de montée en charge.
- De plus, la virtualisation apporte une **simplification** sur le plan de l'installation, du paramétrage et de la gestion de l'ensemble des serveurs.
- Les machines virtualisées / mutualisées offrent ainsi une **rationalisation** et une **réduction** des **coûts de fonctionnement** et des **coûts énergétiques**, ceci apportant également une dimension écologique à la démarche.
- La compartimentation des instances présente par ailleurs des **avantages sur le plan de la sécurité**, l'instance hôte n'étant pas visible des éventuels pirates.
- Un serveur virtualisé offre une **flexibilité** au niveau de la gestion des ressources, ainsi que de meilleures possibilités en termes de création d'**environnements de tests** et d'**environnements de développement**.
- Enfin, combinée avec le Cloud, la virtualisation offre les meilleures possibilités de flexibilité informatiques, tout en permettant un **business modèle** à la **consommation** et à la **demande**.

Action n°5 : Redonder sa connexion Internet locale

PRINCIPE

Une **connexion internet redondée** consiste à fournir **plusieurs connexions Internet** au système d'informations afin d'assurer une **continuité de service**. Si la première connexion est en dysfonctionnement, alors **la seconde connexion prend le relais**.

ENJEUX

Une **connexion internet redondée** est un élément indispensable pour assurer la **continuité de l'activité** de l'entreprise **en cas de panne** de sa connexion internet principale.

Cette redondance peut être prévue pour s'effectuer **sans aucune intervention humaine**, **automatiquement** et **sans aucune coupure**, permettant aux collaborateurs de continuer leur travail sereinement.

La redondance de l'accès internet fonctionne tant pour le **transfert des données** que pour le **transfert de la voix**, assurant ainsi également la continuité de la technologie VOIP.

À noter qu'il est possible de bénéficier d'une **redondance d'accès** avec des **supports technologiques différents**, par exemple, ADSL/SDSL, Fibre ou 4G. Il est également bon de miser sur une **diversité des opérateurs** en ayant un opérateur nominal et un 2ème opérateur en secours. En effet, lorsqu'un opérateur tombe en panne, c'est généralement l'ensemble du secteur de cet opérateur qui est concerné.

Dans le cadre de la résilience et de connexions Internet profesionnelles, on portera une attention particulière aux GTI (conditions contractuelles d'intervention) et aux GTR (conditions contratcuelles de retour en activité).

Enfin il est possible de **sous-traiter** la redondance de ces connexions internet et de leur gestion à un **prestataire externe**, afin de simplifier et de limiter les échanges avec les différents fournisseurs d'accès.

AVANTAGES

- Assure la continuité d'activité en cas de panne Internet
- Bascule possible automatique et sans intervention humaine
- Redondance entre différentes technologies et opérateurs
- Sous-traitance pour simplifier la gestion

Pour aller plus loin

LEXIQUE

Proxy
La notion de proxy est utilisée dans différents domaines. En informatique, notamment dans le cadre d'un environnement réseaux, un proxy est un serveur qui fait l'intermédiaire entre des services informatiques, des équipements (ordinateurs, smartphones, tablettes etc.) et Internet, afin d'apporter une accélération de la navigation, un anonymat et une couche de sécurité supplémentaire.

SSL/TLS
La technologie SSL (Secure Sockets Layer) est un protocole de chiffrement des données permettant de garantir la sécurité et l'intégrité de données échangées entre des serveurs, des machines et des applications en réseau, ou encore lors de la connexion d'un navigateur web à un serveur. La technologie TLS (Transport Layer Security) est une nouvelle version, encore plus sûre, de la technologie SSL.

PCA/PRA
Mesures mises en place pour garantir la continuité de fonctionnement du système d'information (dans le cadre d'un PCA) ou la reprise de l'activité (dans le cadre d'un PRA).

RESSOURCES

Sécurité : Protéger les locaux (CNIL)
Fiche pratique abordant rapidement quelques bonnes pratiques liées à la sécurité des locaux abritant le système d'information. "*L'accès aux locaux doit être contrôlé pour éviter ou ralentir un accès direct, non autorisé, que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs.*"
https://www.cnil.fr/fr/securite-proteger-les-locaux

POSTES DE TRAVAIL

Les **postes de travail**, fixes ou mobiles, sont les outils de travail des collaborateurs au quotidien.

Outre la nécessité de les **mettre à jour** en permanence, de contrôler leur **obsolescence** et maintenir leur **bon fonctionnement**, les postes de travail sont sous la **menace de risques** : risques physiques, risques liés à une mauvaise utilisation, et bien entendu risques liés à la sécurité informatique.

L'enjeu de la gestion des postes de travail passe par une **rationalisation des méthodes de gestion** (centralisation, facilité de déploiement, facilité de mise à jour...) et par leur **sécurisation en toute situation**.

Action n°6 : Assurer une mise à jour constante des postes de travail

PRINCIPE

Le poste de travail d'un collaborateur est composé d'un **système d'exploitation** et de nombreux outils et applications. Ces éléments sont susceptibles de disposer, à tout moment, d'une **mise à jour**, qu'il s'agisse d'une nouvelle fonctionnalité, d'une mise en conformité, ou encore d'un correctif de sécurité. Les **mises à jour constantes** permettent d'assurer à tout moment la sécurité et le bon fonctionnement de l'ensemble du système d'information.

ENJEUX

Qu'il s'agisse du système d'exploitation du poste utilisateur, ou de l'un de ses composants, logiciels, outils... les outils informatiques sont généralement et idéalement **évolutifs** et **sujets à des mises à jour** régulières. L'entreprise doit s'assurer que **ces mises à jour sont réalisées**, quel que soit le nombre de collaborateurs, le type de matériel ou qu'il s'agisse d'un matériel sur site ou distant.

À l'heure où il existe une véritable course contre la montre en matière de **sécurité informatique**, disposer de postes informatiques **mis à jour en temps réel** permet de s'assurer d'une **fiabilité** plus importante de son système d'information. À condition cependant de s'assurer de **tester les mises à jour** et de disposer des sauvegardes adéquates avant leur déploiement sur **l'ensemble du parc**, car il est également possible qu'une mise à jour entraîne un bug ou une incompatibilité sur l'équipement concerné.

Pour effectuer ces mises à jour, les entreprises font généralement appel à des **solutions de gestion de parc informatique**, permettant de manager l'ensemble de la flotte de l'entreprise de façon centralisée. Avec ce type d'outil, les mises à jour des postes de travail peuvent ainsi être **réalisées à distance** et **gérées de façon centralisée**.

Avec ces outils, il est également possible de mettre en place ou d'automatiser des procédures spécifiques, qui vont faciliter le travail de gestion et de maintenance du parc de l'entreprise sur le long terme.

AVANTAGES

- Réduction de la surface d'attaque informatique
- Maintient en bon fonctionnement de l'ensemble des outils IT utilisés par les collaborateurs

Action n°7 : Disposer d'un anti-virus professionnel, centralisé et de dernière génération

PRINCIPE

Un antivirus est un **logiciel** dont l'objectif est de **détecter des menaces informatiques de type virus** (mais également vers informatiques, chevaux de Troie* *(voir lexique)* etc) et de **les stopper** ou **les mettre en quarantaine**, de façon à protéger la machine ou le système informatique concerné.

Si ce type de logiciel peut être géré individuellement sur chaque poste ou serveur, il est également possible de disposer **d'antivirus professionnels centralisés**, spécifiquement conçus pour la protection de l'ensemble d'un système d'information d'une structure et répondants aux critères de protection les plus évolués, pour s'adapter à l'évolution des menaces.

AVANTAGES

- Protection et détection en temps réel contre tous les types d'attaques malveillantes
- Contrôle centralisé de l'ensemble de la politique de sécurité du parc informatique
- Analyses incluant l'intelligence artificielle (EDR)
- Sans impact sur les performances et la bande passante

ENJEUX

Un **antivirus professionnel** et de **dernière génération** est nécessaire pour protéger au mieux son système des failles et des piratages. Ce type d'antivirus permet d'assurer une **protection en temps réel** face à tous types de menaces et de disposer d'une solution **mise à jour de façon régulière**.

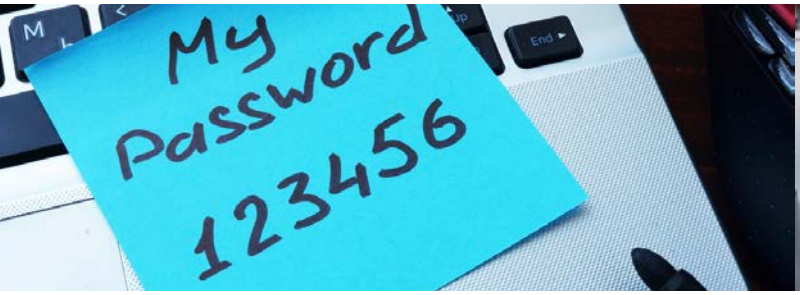
Pour répondre aux besoins des structures les plus exigeantes en matière de fonctionnement du SI, l'antivirus devra **ne pas affecter la bande passante** et **les ressources** des appareils concernés.

Au-delà du téléchargement de bases de données anti-virales, un antivirus moderne se doit d'utiliser le principe de **l'EDR (Endpoint Detection and Response)**. Grâce à son intelligence artificielle et en analysant les comportements des utilisateurs, l'antivirus va détecter les modifications inhabituelles ou de grosse ampleur.

Grâce à sa gestion centralisée, un antivirus professionnel permet une **meilleure efficience** et **facilité de gestion**.

Capable d'assurer **la protection de l'ensemble de la flotte**, qu'il s'agisse de postes fixes, d'ordinateurs portables, de smartphones ou de matériels annexes, l'antivirus permet de créer une **politique générale** de protection et d'édicter des **règles pour l'ensemble du parc**. Il donne également accès au statut de l'ensemble des appareils **dans un même tableau de bord**. Enfin, l'activation ou la désactivation de l'antivirus **est contrôlée à distance**, et **ne peut être modifiée par l'utilisateur** lui-même.

Action n°8 : Avoir une politique de contrôle des accès



PRINCIPE

Une **politique de contrôle des accès permet de s'assurer** que l'accès à une donnée, et à fortiori l'accès à une donnée critique, est limitée aux seuls utilisateurs définis et autorisés.

Le contrôle des accès peut être effectué par **différents moyens** (mots de passe, double authentification, empruntes digitales...) et par la mise en place de **procédures spécifiques** (complexité des mots de passe, périodicité de renouvellement etc.)

ENJEUX

Tout d'abord, il est important d'identifier les **niveaux de criticité** des informations de l'entreprise afin **d'adapter le contrôle des accès** à ces différents niveaux.

En matière de contrôle des accès, il est recommandé de se baser sur les **consignes de l'ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information), c'est-à-dire, de disposer de mots de passe avec une **complexité forte,** des mots de passe **renouvelés régulièrement** et complétés par une **double authentification** lorsque nécessaire.

Lorsqu'une **périodicité de changement** de mot de passe est fixée, le service informatique doit idéalement mettre à disposition des collaborateurs **des outils**, comme des **gestionnaires de mots de passe,** pour que le renouvellement se fasse sans encombre.

Il est également utile de définir des **règles de renouvellement des mots de passe** à appliquer lorsqu'il y a **suspicion de faille**, de **fragilité du système** ou **d'intrusion**.

Enfin, en cas de besoins de sécurité accrus, il est possible de mettre en place des systèmes de **mots de passe à usage unique**, en ayant notamment recours à des tokens.

À noter qu'il est également important de mettre en place une procédure de **contrôle des connexions de périphériques**, tels que les clés USB et les appareils mobiles.

AVANTAGES

Réduction des risques informatiques liés aux accès frauduleux et aux fuites de données

Action n°9 : Chiffrer ses disques dur, notamment les portables

PRINCIPE

Le **chiffrement du disque dur** d'un **ordinateur portabl**e est une méthodologie de protection informatique permettant de contraindre l'accès aux données du matériel à **l'utilisation d'une clé de déchiffrement**.

Sans cette clé, les données sont **inaccessibles** et **inintelligibles** pour quiconque mettrait la main sur l'appareil ou accèderait à son contenu. Ce type de procédure permet ainsi de protéger l'appareil et est d'autant plus recommandé en **situation de mobilité**, **déplacement professionnel**, dans les **lieux publics**, ou si les données sont particulièrement **sensibles**.

ENJEUX

Si les ordinateurs fixes ne sont généralement accessibles qu'aux employés et bénéficient de la protection des locaux et de la politique de sécurité du SI de l'entreprise, il n'en est pas de même pour les **ordinateurs portables**, que les employés sont amenés à **emporter chez eux**, pour **le télétravail**, dans les **déplacements professionnels** ou autre s**ituation de mobilité**.

Il n'est pas rare qu'un ordinateur portable professionnel soit **perdu** ou **volé** dans un lieu public ou une chambre d'hôtel par exemple, ou encore, qu'un portable soit **compromis**, lors de l'accès à **un réseau Internet public**.

Le chiffrement des disques dur des ordinateurs portables de votre entreprise permet de **rendre impossible l'accès aux données** de ce matériel si l'on ne dispose pas d'une **clé de déchiffrement**.

Malgré ses avantages évidents, cette procédure peut être **contraignante**, notamment dans le cas où l'utilisateur **perd la clé de chiffrement** et ne peut plus légitimement accéder à ses propres données. Afin de permettre la récupération des données en toutes circonstances, il est important que la procédure soit **managée par le service informatique** de l'entreprise, de façon à disposer de **solutions alternatives** de récupération de la clé.

AVANTAGES

S'assurer que les données ne sont pas exploitables en cas d'accès frauduleux ou de perte de matériel

Action n°10: Centraliser la gestion des postes de travail et appareils mobiles

PRINCIPE

Tandis que les **flottes d'appareils des entreprises** sont de plus en plus hétérogènes, que les usages sont de plus en plus diversifiés, et que dans le même temps, les enjeux de protection de ces appareils sont toujours plus forts, il est possible de **réduire les efforts et les risques** en recourant à une **solution de management centralisé** de sa flotte informatique.

Ces solutions sont généralement des **outils logiciels**, permettant de **monitorer** et de **gérer à distance l'ensemble des postes fixes, mobiles, smartphones** et **autres appareils**, le tout, dans une seule et même interface.

AVANTAGES

- Réduire le temps, les coûts et les efforts de gestion de toute la flotte d'appareils de l'entreprise
- Renforcer la sécurité des appareils
- Automatiser et suivre l'ensemble des actions

ENJEUX

Le recours à un **outil de gestion centralisé** des **postes de travail** et **appareils mobiles** offre de nombreux avantages et une **réduction des efforts de gestion**, notamment lorsque la flotte de l'entreprise est **importante** (nombre d'appareils), **diversifiée** (différents appareils, fixes, portables, smartphones), possède **différents systèmes d'exploitation** et également que les appareils correspondent à **différents usages** au sein de la structure (poste fixe en entreprise, ordinateur portable en déplacement, tablette mobile chez les clients etc.)

Une solution de gestion centralisée offre notamment les avantages suivants :

- **Protection des accès** aux appareils par différentes méthodes ou codes de verrouillage,
- **Gestion à distance** de toute la flotte des appareils de l'entreprise, fixes comme mobiles,
- Permet de disposer d'un **état des lieux / état de santé** du parc,
- Gestion des sites web et application **accessibles en liste blanche** pour l'utilisateur, par exemple, en vue de mieux gérer les usages personnels/professionnels
- **Géolocalisation** et **geo-fencing*** *(voir lexique)* des appareils, permettant de s'assurer que ceux-ci sont utilisés dans le respect des conditions définies par l'entreprise ou sa charte informatique
- Etc.

Certaines de ces applications de centralisation de gestion des postes disposent idéalement de **fonctionnalités avancée**s, de type, automatisation des tâches, reporting, suivi des sauvegardes etc.

Pour aller plus loin

LEXIQUE

***Cheval de Troie**
En informatique, un cheval de Troie est un type de virus caché à l'intérieur d'un autre programme. Il permet à un attaquant ou à un programme de s'introduire dans le système. Le Cheval de Troie se déclenche généralement à retardement, rendant plus difficile son repérage et son éradication.

***Geo fencing**
Le geo-fencing est une technologie de géolocalisation qui permet de surveiller les déplacements d'objets ou de personnes dans un périmètre prédéfini. En informatique, il est possible de l'utiliser pour surveiller la géolocalisation de la flotte d'appareils de l'entreprise.

RESSOURCES

Sécurité informatique : la méthode ultime pour créer vos mots de passe
Dans cet article, nous vous proposons une méthode pour créer des mots de passe complexes et faciles à retenir, tout en respectant les recommandations de l'Anssi. *"En effet, tandis que les services en ligne, les applications et logiciels se sont multipliés, c'est un véritable casse-tête pour les utilisateurs que de disposer de mots de passe complexes et le plus possible, uniques..."*
https://www.deessi.si/securite-informatique-methode-ultime-creer-vos-mots-de-passe/

Comment chiffrer ses documents et ses répertoires ?
La CNIL propose dans cette page des conseils pour le chiffrage de document. *"Dans le cadre de votre travail ou chez vous, vous conservez des documents qui peuvent contenir des informations confidentielles qui ne devraient pas être accessibles à tous. Le chiffrement répond à cette problématique..."*
https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

MESSAGERIE

Principal outil de communication, la messagerie électronique est l'application la plus courante dans le domaine professionnel, au sein de l'entreprise, mais aussi pour la communication avec les partenaires et les clients.

Sur le plan de la sécurité informatique, elle est cependant l'une des premières portes d'entrée des piratages. Les données stratégiques et confidentielles qu'elle contient nécessitent donc des procédures spécifiques de gestion, de paramétrage et de résilience.

Action n°11 : Héberger la messagerie sur un serveur dédié

PRINCIPE

Une **messagerie sur serveur dédié** consiste à héberger sa messagerie sur un serveur dont l'usage est **uniquement réservé à sa propre structure**, par opposition à l'hébergement sur un serveur mutualisé, dont les ressources sont partagées avec d'autres structures ou utilisateurs.

ENJEUX

Lorsqu'une messagerie est hébergée sur un serveur mutualisé, elle est davantage soumise aux failles de sécurité et aux infections.

L'hébergement de sa messagerie Internet **sur un serveur dédié** permet de **réduire les risques informatiques**, mais aussi, de disposer d'un hébergement **aux ressources mieux maîtrisées**, tant sur le plan de la **disponibilité** et de la **qualité de service**, que des **options de paramétrage** et de **gestion avancée**.

Le tout permettant de garantir à la structure la bonne continuité de fonctionnement de sa messagerie et la **réduction des failles de sécurité** éventuelles pour l'ensemble de son système.

AVANTAGES

- Garanties de disponibilité,
- Fonctionnalités de gestion et de paramétrage avancées,
- Sécurité accrue

Action n°12 : S'assurer de la sécurisation de sa messagerie électronique

PRINCIPE

La messagerie électronique, outil de gestion des emails de l'entreprise, est un **élément de vigilance** important des équipes de sécurité informatique. Elle possède une **surface d'exposition très large** étant donné que n'importe qui peut interagir par ce biais avec une personne interne à l'entreprise.

Une **messagerie électronique sécurisée** est généralement équipée de fonctionnalités additionnelles, tels que de solutions **antispam** et **antivirus**. De plus, ce type de messagerie, habituellement réservée à un **usage professionnel**, est soumis à des protocoles de **fonctionnement** spécifiques.

ENJEUX

Assurer la **sécurité d'un service de messagerie** consiste à vérifier que la donnée est émise par la bonne personne, que cette donnée est complète, qu'elle n'est ni altérée ni corrompue et qu'elle ne présente pas de risques pour la personne qui la reçoit.

Un **outil de messagerie électronique professionnel** offre des **règles de paramétrages** qui vont permettre à la structure ou à l'entreprise de mieux contrôler l'usage de la messagerie et les risques informatiques associés. Il est en effet important de s'assurer que l'email provient de la bonne personne / service, et qu'il ne contient pas d'élément pouvant corrompre le SI et la sécurité de l'entreprise.

Ainsi, c'est le recours à des compétences expertes, capables de définir la **politique de sécurité de la messagerie** et d'effectuer les **paramétrages correspondants**, qui permettent de s'assurer de la viabilité et de la pérennité de sa messagerie.

AVANTAGES

- Antivirus,
- Antispam,
- Protocole SPF* *(voir lexique),*
- DKIM* et DMARC* *(voir lexique),*
- Paramétrages avancés

Action n°13 : Externaliser la messagerie

PRINCIPE

Une messagerie est externalisée lorsque sa gestion et son hébergement ont été **confiés à un prestataire externe**.
Le prestataire devient le **garant du bon fonctionnement** de la plateforme, de **sa maintenance** et de **son administration**.

Sur le plan de la résilience informatique, il est important de s'assurer des **engagements contractuels de la plateforme** et des **engagements de services du prestataire** en matière de garanties de continuité d'activité ou de reprise d'activité.

AVANTAGES

- Garanties de disponibilité,
- Accès nomade,
- Capacités de stockage étendues,
- Sauvegardes,
- Antispam,
- Antivirus,
- Protocoles de sécurité

ENJEUX

La messagerie électronique constitue l'un des premiers éléments de vigilance en matière de sécurité informatique.

Elle est souvent la cible d'attaques, ou un **point d'entrée pour les pirates** (phishing* *(voir lexique)*, rançongiciels* (voir lexique)...) et les **données stockées** dans la messagerie sont généralement **confidentielles** et indispensables au bon fonctionnement de la structure.

S'assurer de disposer d'une messagerie **disponible**, **protégée** et **récupérable en cas d'incident** en la confiant à un prestataire externe spécialisé est donc un élément vital de la mise en place de la résilience informatique.

Lorsque la messagerie est confiée à un prestataire, il est important d'étudier avec soin le contrat stipulant les engagements de celui-ci en matière de **disponibilité**, de **sauvegarde** et de **réversibilité** des données.

Pour aller plus loin

LEXIQUE

***Phishing :** Tentative d'usurper une identité pour récupérer des informations personnelles à des fins malintentionnées malveillantes. Exemple : Mail de votre président demandant un virement discret de trésorerie, relance sur un non-paiement ou sur une date de garantie qui arrive à échéance, menace de fermeture d'un compte, message d'un ami en détresse, suivi de colis, renouvellement d'identifiants de fournisseur Internet etc...

***Protocole SPF (Sender Policy Framework) :** Protocole de validation de courrier électronique permettant de détecter et de bloquer une éventuelle usurpation de courrier électronique. Consiste dans une autorisation des serveurs sources d'émettre des emails pour un nom de domaine.

***DMARC :** Protocole d'authentification de courrier électronique assurant une protection du canal de courrier électronique au niveau du nom de domaine. Applique une vérification d'usurpation de l'identité de l'émetteur.

***DKIM (DomainKeys Identified Mail**) : Méthode d'authentification du courrier électronique qui détecte l'usurpation d'identité.

***Rançongiciel** (En anglais, ransomware) **:** Logiciel malveillant ayant pour action de bloquer l'accès à des données en les chiffrant, avec pour objectif de demander à la victime une rançon en échange de la récupération de l'accès.

RESSOURCES

La messagerie électronique : première porte d'entrée du piratage informatique
Un article IVISION présentant les enjeux de sécurité informatique concernant la messagerie électronique. "*Outre les dommages liés aux éventuelles pertes de données ou indisponibilité du système d'information, la réception de nombreux spams à aussi pour conséquence de monopoliser la bande passante, faire perdre du temps aux employés, ou encore, de surcharger la boîte mail...*"
https://www.ivision.fr/messagerie-electronique-premiere-porte-dentree-piratage-informatique/

Infographie : les 10 avantages de la messagerie hébergée
À télécharger : une infographie reprenant 10 avantages de la messagerie hébergée pour les entreprises.
https://www.deessi.si/infographie-10-avantages-de-messagerie-hebergee/

Le contrôle de l'utilisation d'internet et de la messagerie électronique
Un article de la CNIL qui aborde les dispositifs de contrôle d'Internet et de la messagerie pouvant être mis en place par les entreprises.
"Des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau peuvent conduire les entreprises ou les administrations à mettre en place des outils de contrôle de la messagerie..."
https://www.cnil.fr/fr/le-controle-de-lutilisation-dinternet-et-de-la-messagerie-electronique

MESURES ORGANISATIONNELLES

Qu'il s'agisse de protéger le système d'information avec des outils ou par la prévention de risque, ou de prendre en charge les incidents et rétablir la disponibilité du système, les **mesures organisationnelles** sont le cœur de la mise en place de la **cyber-résilience**.

Il s'agit de prévoir à l'avance les **procédures et politiques adaptées** à chaque situation, mais aussi, les **moyens**, tant **matériels** que de r**essources humaines**, de mettre en œuvre ces procédures dans le respect des besoins de la structure concernée.

Action n°14 : Formaliser sa politique de sécurité informatique

PRINCIPE

La **politique de sécurité informatique** est **une stratégie** visant à maximiser la sécurité informatique d'une entreprise.
Elle est **matérialisée** dans un ou plusieurs **documents** qui reprennent l'ensemble des **enjeux, objectifs, analyses, actions** et **procédures** faisant partie de cette stratégie.

Elle couvre de **nombreux domaines**, tels que la maintenance du parc informatique, les formations et la sensibilisation des employés, les droits d'accès, les procédures d'accès et d'utilisation des outils informatiques, ou encore la protection des données sensibles.

AVANTAGES

- Démarche globale d'amélioration continue
- Identification, analyse et arbitrage des risques
- Donne un cadre aux bonnes pratique de la structure en matière de SSI
- Facilite l'application de procédures de PCA/PRA* *(voir lexique)* et gestion de crise

ENJEUX

La **politique de sécurité informatique** est généralement élaborée et mise à jour par **le responsable informatique** de la structure ou par une personne **sensibilisée aux risques**.

Elle repose sur une **connaissance** précise de tous **les éléments qui composent le système d'information** et sur la mise en place d'une stratégie de **gestion** et de **réduction des risques** informatiques.

Après une **analyse de l'existant**, des procédures de **prise en charge des risques informatiques** seront déterminés, en leur attribuant les **moyens nécessaires** à cette prise en charge, qu'il s'agisse de moyens **humains**, **matériels ou logiciels**.

La mise en place de la politique de sécurité informatique peut être effectuée en interne, mais il existe des avantages à **sous-traiter** tout ou partie de cette tâche a un **prestataire externe**, notamment, la **neutralité de l'analyse** de l'existant, des **risques** et de l'attribution des différents **moyens** visant à résoudre les incidents.

Un contrat permettra de déterminer le **périmètre d'intervention** du prestataire, ainsi que la **charge de travail**, les différentes **responsabilités** et les **engagements** de chaque acteur du projet.

Action n°15 : Disposer d'une procédure d'arrivée et de départ pour les collaborateurs

PRINCIPE

Lors de **l'intégration** d'un collaborateur, des **droits d'accès** lui sont déterminés, au regard du niveau de ses responsabilités et du niveau de criticité de l'information dont il doit disposer. Tout au long de sa carrière, ses droits d'accès évoluent en fonction de ses responsabilités. Enfin, de la même façon, au départ d'un collaborateur, il est nécessaire de s'assurer que ses droits d'accès lui sont désormais **restreints**, voire que les comptes en question **sont détruits**, de façon à **minimiser les risques** de sécurité informatique.

ENJEUX

Dans un premier temps, les accès et droits obtenus par le nouveau collaborateur doivent entrer dans le cadre de **processus** et de **règles édictées** suite à des décisions réfléchies et éclairées, de manière à **exposer le moins possible** le système d'information de l'entreprise tout en permettant au collaborateur de **travailler sereinement**.

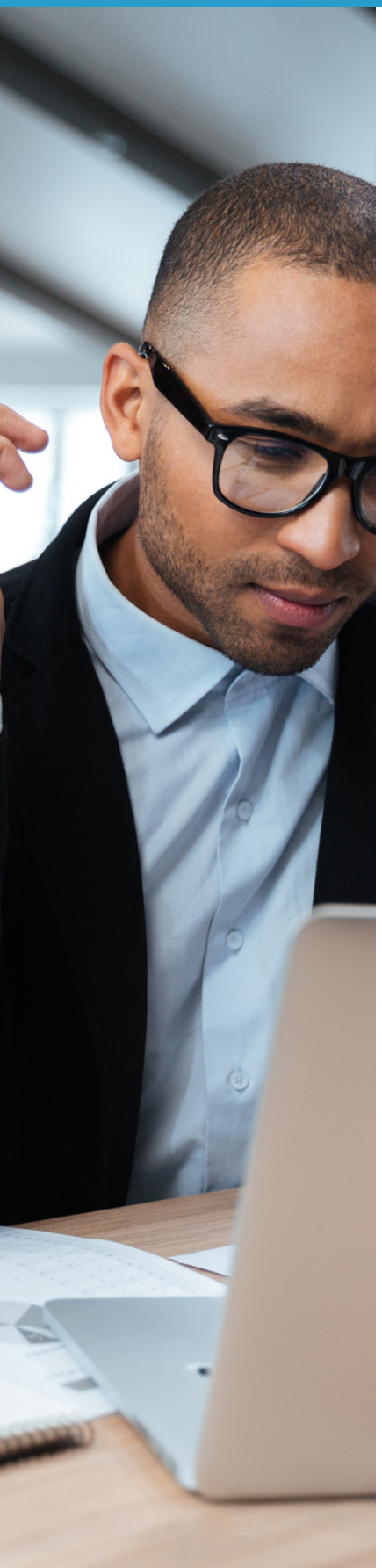
La question est également critique au moment du **départ de l'employé**, car cette étape est souvent **moins contrôlée**. Il est primordial de disposer de procédure visant à s'assurer que le collaborateur ne peut **plus accéder aux éléments du système d'information** de l'entreprise et que les comptes ne restent pas **ouverts** ou **dormants**. Ceci permet de **minimiser le risque de piratage** de ces comptes ou **leur accès** par des personnes malintentionnées.

Toutes ces procédures de départ et d'arrivées des collaborateurs peuvent être mises en place suivant la **politique de sécurité informatique** de l'entreprise, en collaboration bien entendu avec les autres services, et notamment RH, de la structure.

AVANTAGES

- Réduction des risques juridiques
- Réduction des risques informatiques

Action n°16 : Sensibiliser et former ses collaborateurs à la sécurité informatique



PRINCIPE

Quels que soient les moyens mis en œuvre pour réduire les risques informatiques, le maillon faible de la sécurité reste **les erreurs humaines**. C'est pourquoi **former**, **sensibiliser** et **responsabiliser** ses collaborateurs aux **bonnes pratiques de sécurité** est l'un des moyens les plus efficients pour **diminuer les risque d'incidents** et de **malveillances** éventuelles.

ENJEUX

Le **phishing** (technique visant à tromper le collaborateur en vue d'obtenir des identifiants, droits d'accès, informations bancaires etc.), les **vols d'identifiants** ou encore la **compromission d'adresses mail professionnelles** sont parmi les formes les plus courantes **d'ingénieries sociales**, autrement dit, de malfaisances informatiques se produisant suite à une tromperie ou à un leurre des collaborateurs.
C'est pourquoi, **sensibiliser ses collaborateurs** permet de **réduire les risques** d'erreurs, de piratages, de pertes de données et d'indisponibilité du système d'information.

Les enjeux de cette sensibilisation sont d'autant plus importants dans le cadre du **travail à distance**, car l'employé est **n'est plus tout à fait protégé** par le cadre du **système d'information de l'entreprise.** Il est donc plus à même de subir des expositions à des piratages ou à des fraudes.
La sensibilisation peut passer par la mise en place d'une **charte de sécurité informatique**, par **des formations**, **des communications** adressées aux employés ou encore par la mise en place de simulations d'intrusion.

À noter que les collaborateurs sont généralement **volontaires** pour se former et mieux maitriser les risques, ce qui est un atout de taille pour la mise en place de ces procédures. La sensibilisation est donc une étape primordiale de la **politique de sécurité informatique** de l'entreprise et doit être reconnue comme telle par la DSI ou la direction de l'entité.

AVANTAGES

- Réduction des risques informatiques
- Respect de procédures de conformité (ex. RGPD*)
- Implication de tous dans la sécurité du système d'information

Action n°17 : Disposer d'un PCA / PRA

PRINCIPE

Le **PCA (Plan de Continuité d'Activité)** désigne un ensemble de mesures permettant de garantir une **continuité de fonctionnement** de tout ou partie de son système d'information en cas de panne ou d'incident.

Le **PRA (Plan de Reprise d'Activité)** permet quant à lui de garantir, **dans un délai donné**, une **reprise d'activité** de tout ou partie du système d'information.

Tous deux sont des éléments vitaux de la mise en place d'une stratégie de résilience informatique.

AVANTAGES

- Limitation des conséquences de l'indisponibilité du SI
- Analyse des risques
- Mise en place de stratégies de secours
- Procédures RH et management du personnel
- Documentation
- Procédures de tests

ENJEUX

Mettre en place un **PCA (Plan de continuité d'activité)** ou **PRA (Plan de reprise d'activité)** permet de **limiter** les **impacts liés à une interruption d'activité**, qu'il s'agisse de conséquences financières, internes, juridiques ou encore liées à la satisfaction des clients et à la réputation de l'entreprise.

PCA et PRA consistent à mettre en place, au préalable, une **cellule de crise**, des **moyens** et des **procédures** permettant de gérer tout type d'incident informatique et d'assurer soit la continuité, soit la reprise immédiate de l'activité.

Sont impliqués dans l'élaboration d'un PCA ou d'un PRA **la documentation** et **les procédures organisationnelles** de l'entreprise, tout ou partie des **collaborateurs**, la gestion des **ressources informatiques** et **telecom**, ainsi que les **partenaires** de l'entreprise, fournisseurs, sous traitants ou autre.

Afin d'évaluer ses besoins en continuité ou reprise d'activité, il est nécessaire d'être capable de prévoir le coût d'une éventuelle indisponibilité.
Pour chaque service de votre structure, combien couterait une indisponibilité de service de 2H ? De 4H? D'une journée ou plus ?

Un audit peut vous aider à établir ces éléments. Il est possible d'être **accompagné** par **des spécialistes** dans la mise en place de ces procédures, que ce soit sur le plan **purement technique** comme sur le plan de **l'organisation**.

Action n°18 : Définir un RTO / RPO

PRINCIPE

Le **RTO (Recovery Time Objective)** et le **RPO (Recovery Point Objective)** sont des indicateurs référents et d'objectifs qui interviennent notamment dans le cadre de la mise en place d'un plan de reprise d'activité (PRA).

Il s'agit de définir, de façon hypothétique, une **durée** pendant laquelle le **système d'information sera non fonctionnel** ou pendant laquelle les données de l'entreprise ne seront **plus enregistrées**. Ces deux paramètres correspondent donc à des durées que la structure détermine elle-même en fonction de ses enjeux de gestion et de stratégie.

ENJEUX

Le **RTO (Recovery Time Objective)** désigne un **objectif de temps de remise en fonction** pour un **service déterminé** au sein du système d'information. Lorsque la structure ne dépend pas du service concerné de façon critique, un RTO de plusieurs heures, voire de plusieurs jours, peut être envisagé. À l'inverse, lorsque l'arrêt du service implique de graves dysfonctionnements ou un arrêt total de l'activité, le RTO peut être limité à un temps défini.

Le RTO d'un service correspond ainsi au **temps d'incapacité maximale** du service accepté par l'entreprise. C'est donc un indicateur décisif dans le PRA (Plan de reprise d'activité) de l'entreprise. Dans certains cas, le RTO peut être intégré au PRA de façon contractuelle.

Le **RPO (Recovery Point Objective ou Point antérieur de Restauration)** désigne de son côté la **durée maximale écoulée depuis le dernier point de restauration des données**. Le RPO détermine ainsi le **temps acceptable de perte de données** entre le dernier enregistrement et l'instant de perte d'un service. Ce paramètre est un élément important de la stratégie de sauvegarde, déterminant notamment la fréquence (toutes les 5 minutes, plusieurs fois par jour, une fois par jour...) ainsi que la volumétrie de ces sauvegardes.

AVANTAGES

- Définition des objectifs PRA de l'entreprise
- Élaboration de la stratégie de sauvegarde

Action n°19 : Nommer un DPO

PRINCIPE

Un **DPO (Délégué à la Protection des Données)** désigne un rôle chargé au sein d'une structure de toutes les actions entourant la **protection des données personnelles**. Cette fonction peut être exercée par une personne ou une équipe au sein de la structure, mais également par un prestataire externe ou une personne morale.
Ce rôle a été introduit par **la loi RGPD*** *(voir lexique)*, qui s'applique au traitement des données personnelles des citoyens de l'Union européenne. Selon le type de structure et de données traitées, il peut être obligatoire ou non de disposer d'un DPO au sein de son entreprise.

ENJEUX

À la fois juriste et technicien, il peut être notamment demandé au **DPO** de **cartographier le traitement des données personnelles** avec l'élaboration d'un **registre des traitements** et de travailler à la **protection des données** sous tous ses aspects (accès, stockage, sécurité informatique en général...) Une **documentation spécifique** doit également être assurée.

Un poste dédié de DPO doit être obligatoirement attribué dans les **organismes publics**, ainsi que dans les entreprises dont le traitement des données est **suffisamment spécifique** (par ex. données sensibles, données de santé, données de mineurs etc.). Pour tous **les autres cas**, il est recommandé de faire assurer la gestion des données personnelles soit par **un collaborateur**, soit par une équipe, soit encore par un **organisme externe**, par exemple, un prestataire en sécurité informatique et/ou un cabinet d'avocats.

Sur le plan des avantages, un DPO apporte généralement une **plus grande rigueur** en matière de **sécurité informatique** et représente un élément valorisant et rassurant dans les relations avec les partenaires et prestataires externes (partenaires commerciaux, appels d'offres, investisseurs etc.)

La démarche du DPO pourra être éclairée ou appuyée par la mise en place **d'audit de conformité RGPD**, qui peut être effectué notamment par des prestataires techniques et / ou juridiques spécialisés.

AVANTAGES

- Respect de la conformité RGPD* *(voir lexique)*
- Amélioration de la sécurité informatique
- Amélioration de la protection des données
- Création de valeur /différentiation concurrentielle

Action n°20 : Disposer d'un RSSI

PRINCIPE

Au sein d'une entreprise, le **RSSI** est le **Responsable de la Sécurité du Système d'Information**. Parmi ses attributions, on retrouve la gestion des **incidents de sécurité** informatique, l'établissement de la **politique de sécurité** du système d'information ou encore la mise en place de la sensibilisation des collaborateurs.

ENJEUX

Responsable de la sécurité du patrimoine informationnel de l'entreprise, le RSSI assure un rôle **d'alerte**, de **conseil** et **d'assistance**. Outre la mise en œuvre de la **politique de sécurité informatique** de la structure, il est également généralement chargé de la **veille** liée à toutes les problématiques de sécurité du SI, des problématiques qui évoluent en permanence.

Profil pointu sur le plan technique, il dispose parfois de **connaissances juridiques** et **règlementaires** liées à la gestion du système d'information, avec notamment des connaissances sur le **RGPD*** *(voir lexique)*. Multi-compétences, ce profil a tendance également à se diversifier et à être de plus en plus **stratégique**, du fait de la complexification des systèmes d'information et des menaces auxquelles peuvent être soumises les entreprises.

Toutes les entreprises ne disposent pas d'un RSSI. On rencontre plus fréquemment cette fonction au sein des **grands groupes**, bien plus rarement au sein des PME. Dans les entreprises sans RSSI, ce poste peut être par exemple assurée par le **responsable informatique** de l'entreprise. À savoir qu'il est également possible **d'externaliser cette fonction**, à temps complet ou non, à un prestataire spécialisé.

AVANTAGES

- Réalisation de la veille technologique
- Élaboration et application de la politique de sécurité informatique
- Veille au respect de la conformité légale du SI de l'entreprise
- Mise en place la sensibilisation et la formation des collaborateurs à la sécurité informatique

Action n°21 : Auditer son système d'information régulièrement

PRINCIPE

L'audit de système d'information est une **procédure** permettant d'avoir, à un instant T, une vue d'ensemble des **éléments qui composent** le système d'information d'une entreprise ou d'une organisation. Outre un inventaire, l'audit permet idéalement de déterminer les **interactions** entre ces éléments, de faire un état des lieux des **performances** et de **l'obsolescence**, mais aussi, de déterminer les besoins et les pratiques des utilisateurs, et à un niveau **stratégique**, de déterminer les enjeux et les risques du SI pour l'entreprise.

ENJEUX

L'**audit de système d'information** est la première brique de **rationalisation** de la gestion du système d'information. Effectuer un audit de SI, ce n'est pas juste faire un inventaire du système d'information. En effet, l'audit est souvent commandité pour évaluer la bonne adéquation des besoins de l'entreprise avec ce qui est proposé par le service IT de la structure. Il s'agit également de vérifier si le système d'information répond aux facteurs de **performance** et aux **objectifs stratégiques** de l'organisation.

Ainsi, l'audit permet d'évaluer la **conformité du SI** avec les obligations légales, les **optimisations budgétaires** possibles, **l'efficience** et la **pérennité** du système d'information. Il permet par ailleurs de travailler à l'optimisation du **traitement des processus métiers** de l'entreprise par le système d'information et de s'assurer de **l'interopérabilité** et de **l'accessibilité du système.** L'audit permet par ailleurs de mesurer si les services proposés par le fournisseur, qu'ils soient internes ou externes à la structure, sont en adéquation avec les besoins des utilisateurs métier. Enfin, l'audit peut également évaluer la **sécurité du SI**, même si cette partie fait souvent l'objet d'un **audit de sécurité** à part entière.

Nombre d'entreprises entreprennent la réalisation d'un audit de système d'information après des incidents de gestion ou de sécurité, en cas de changement de dimension, d'une reprise ou d'une revente de l'activité. Pourtant, la réalisation d'audits récurrents reste le meilleur moyen de conserver la maîtrise des décisions prises autour de la gestion et du développement de son SI au quotidien.

AVANTAGES

- Connaître le niveau de sécurité global de son SI
- Définir une politique d'accès
- Définir une feuille de route et un plan d'actions
- Évaluer la sûreté de la politique de sauvegardes
- Évaluer les configurations réseau
- Constitue la base de la mise en place d'un PCA* ou d'un PRA* *(voir lexique)*

Action n°22 : Recourir à un prestataire externe pour auditer le SI

PRINCIPE

L'audit de système d'information permet d'établir les éléments qui composent le SI d'une entreprise ou d'une organisation, ainsi que les enjeux d'usages, de performances, de sécurité et de stratégie liés à l'utilisation de ce système. Tandis qu'il est possible de mettre en œuvre cette démarche en interne au sein de son entreprise en la **confiant à son responsable informatique** ou à **sa DSI**, le recours à un **prestataire externe spécialisé** permet de bénéficier de certains avantages, notamment sur le plan de la **neutralité** et de **multiplicité des domaines** et des **compétences** concernées.

ENJEUX

Lors d'un **audit de système d'information**, l'ensemble des logiciels et des matériels, informatiques, électroniques ou de télécommunication de la structure sont évalués, qu'il s'agisse de **ressources physiques** (fibres optiques, surface d'hébergement, alimentation électrique, climatisation...) ou de **plates-formes logicielles** ou **matérielles** (serveurs, systèmes d'exploitation, bases de données…) qui participent au stockage, à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'entreprise. On inclut parfois également dans l'audit **les personnels** qui conçoivent, déploient, maintiennent et rendent opérationnel ces ressources, ou encore les procédures liées à ces ressources.

Pour un audit de SI qui n'oublie aucun détail, certains aspects seront à **maîtriser par l'auditeur**, qui devra réaliser une **cartographie des données, informations** et **ressources informatiques** de l'organisation, mais aussi, prendre connaissance des différentes **politiques** et **procédures** liées au système d'information de l'entreprise (politique de sécurité du système d'information, chartes utilisateurs etc.**)**

Le recours à un **prestataire externe** permet de s'assurer de bénéficier de **recommandations neutres** et de **compétences pointues** et **multidisciplinaires**. Un prestataire permet par ailleurs d'apporter des réponses dans le cadre de **problématiques précises**, par exemple concernant la **conformité à la législation** d'un domaine en particulier, ou encore dans l'optique d'évaluer la **sécurité du système d'information**.

Enfin, avantage qui a son importance, contrairement à l'interne, un prestataire est évalué par rapport à une **obligation de résultats.**

AVANTAGES

- Neutralité de l'audit et obligation de résultat
- Multi-compétences pointues
- Évaluation de problématiques précises (conformité, performances, sécurité etc.)

Action n°23: Définir une charte informatique

PRINCIPE

La **charte informatique** est un **document de référence** précisant les contextes d'utilisation des **outils informatiques** et des **informations sensibles** ou **personnelles** liées au cadre de l'entreprise.
Elle s'adresse généralement **aux collaborateurs**, pour qui elle définit les usages et les cadres d'utilisation des outils et équipements informatique au sein de l'entreprise en question.

ENJEUX

La **charte informatique** est un élément indispensable de la **stratégie de sécurité informatique** et de **prévention des risques**, mais pas seulement. Elle possède également des **enjeux de communication** et surtout, des enjeux de **responsabilité** vis-à-vis de **l'utilisation par les collaborateurs** de tous les matériels, données et outils informatique de l'entreprise.

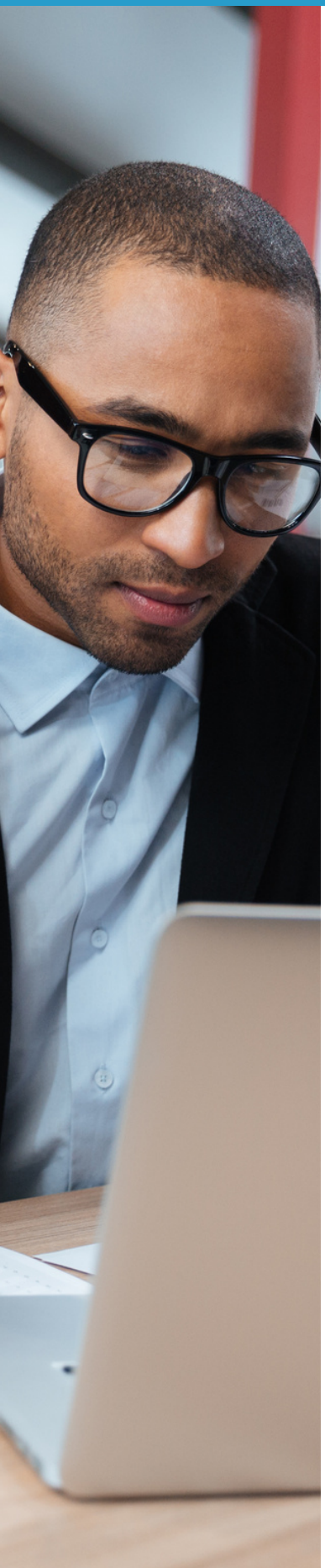
De plus, elle fait partie du **règlement intérieur** en cas de **litige entre l'employeur** et les **salariés**, et doit respecter le **code du travail**. Ainsi, la charte informatique peut avoir un rôle dans le cadre de **décisions judiciaires**.

Généralement, parmi les grandes thématiques traitées à l'intérieur de la charte informatique, on retrouve : **règles d'utilisation** de tous les éléments composants le système d'information de l'entreprise et ses données, le **cadre** et le **contrôle** de ces éléments sur le plan de l'utilisation professionnelle et personnelle, la **confidentialité** et la **protection des données** de l'entreprise ou encore le **respect des règles d'utilisation** des **droits d'accès** mis à disposition de l'employé. À noter que sur le plan de la **sécurité informatique**, elle permet **d'informer**, se **sensibiliser** et surtout de **responsabiliser** les collaborateurs. Elle a donc un rôle direct sur la **réduction des risques** provenant d'erreurs humaines.

AVANTAGES

- Définition des droits et des devoirs des collaborateurs vis-à-vis du SI
- Fixe un cadre légal à l'utilisation du SI en complément du contrat de travail
- Sensibilisation et responsabilisation des collaborateurs à la sécurité informatique

Action n°24 : Etre conforme au RGPD



PRINCIPE

En français, **“Règlement Général sur la Protection des Données”**, le **RGPD** est une directive européenne établissant les règles à respecter concernant le traitement effectué par les entreprises et les administrations des données à caractère personnel. Applicable depuis le 25 mai 2018, il s’adresse à **toutes les structures**, publiques comme privées, quelle que soit leur taille.

ENJEUX

Les principaux enjeux de la **conformité RGPD** sont bien évidemment en premier lieu, **juridiques**.

En France, à l'issue de contrôle ou de plaintes, en cas de non-application de la loi, la CNIL se réserve le droit de prononcer des **rappels à l'ordre**, des **astreintes à la conformité**, des **limitations** ou une **suspension** du traitement des données personnelles par l'entreprise. Elle peut également prononcer des **amendes**, dont le montant peut s’élever jusqu’à **20 millions d’euros** ou jusqu’à **4 % du chiffre d’affaires annuel mondial**. Enfin, ces sanctions peuvent être rendues publiques par la CNIL.

Au-delà des enjeux juridiques, on note également le risque de **mise en pause de l'activité**, **risque financier** et **risque sur l'image de marque** de l'entreprise. L'autre volet de la conformité RGPD concerne la **sécurité informatique**. Parce que le RGPD cherche à protéger l'intégrité des données personnelles des citoyens, il dispose de nombreuses mesures incitatives à une **amélioration de la sécurité informatique** de la structure, notamment sur le plan préventif. Ainsi, une mise en conformité RGPD aura des impacts positifs sur la sécurité des données de l'entreprise.

Enfin, la mise en conformité RGPD peut également avoir un impact positif sur **l'image de l'entreprise**, en montrant sa volonté aux utilisateurs de **respecter leurs droits** en matière de gestion des données personnelles.

AVANTAGES

- Audit de gouvernance et audit technique
- Respect de la réglementation
- Réduction des risques en sécurité informatique, compromission des données, risques financiers, risques sur l'image de marque
- Connaissance des vulnérabilités & amélioration de la protection du SI

Action n°25 : Avoir un registre de traitement des données

PRINCIPE

Le registre de traitement des données est un document lié à la mise en place du RGPD* *(voir lexique)* et permettant le recensement et l'analyse de l'ensemble des données personnelles traitées par une structure.

AVANTAGES

- Respect de réglementation
- Capacité à fournir aux organismes compétents les éléments de preuve du respect de cette conformité

ENJEUX

L'obligation de tenir un **registre des traitements** dans le cadre de la loi RGPD peut concerner n'importe quel type d'organisme, **public comme privé et** quelle que soit sa taille, dès lors qu'il traite des données personnelles de citoyens de l'Union Européenne.

Cependant, pour les structures de **moins de 250 employés,** seules les **données suivantes** doivent obligatoirement faire l'objet d'un traitement **:**

- Les **traitements non occasionnels** (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.),
- Les traitements susceptibles de comporter un **risque pour les droits et libertés des personnes** (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.)
- Les traitements qui portent sur des **données sensibles** (exemple : données de santé, infractions, etc.).

À noter qu'il existe un registre spécifique pour les **activités de sous-traitanc**e des données personnelles, et qui concerne donc les entreprises ou organismes sous-traitants.

Sur le site de la **CNIL**, **organisme de référence** pour la mise en œuvre de ce registre de données, on peut retrouver des informations sur le **contenu du registre**, ainsi que des **modèles de registres à télécharger**.

Les enjeux de la tenue du registre sont ainsi du domaine de la **conformité juridique**. Ce registre relève également de la **responsabilité du DPO (délégué à la protection des données)** de votre structure ou entreprise, si vous disposez d'un DPO, ou encore, ou à défaut par **l'employé ou l'organisme** chargé par votre structure **d'appliquer le RGPD.**

Action n°26 : Mettre en place des clauses de réversibilité avec ses prestataires

PRINCIPE

Une **clause de réversibilité** est une **clause contractuelle** permettant au client une **reprise en main** de la **fonction** ou du **service externalisé** sans aucune limitation.

Une clause de réversibilité est indispensable dans le cadre de **prestations informatiques externalisées**, afin de s'assurer de la possibilité de **récupérer en interne** ou de pouvoir **librement confier à un nouveau prestataire** le service ou la fonction externalisée, ainsi que l'ensemble des données concernées.

ENJEUX

Disposer d'une **clause de réversibilité** dans le cadre de la **sous-traitance** de prestations ou de services IT est indispensable pour sa **stratégie de résilience informatique**.

En effet, l'entreprise cliente doit s'assurer que les **conditions de ses contrats** avec ses différents prestataires lui permettent de **reprendre la main en toutes circonstances** sur les services ou fonctions concernés par la sous-traitance.

Il est recommandé d'énoncer la clause de réversibilité comme une **clause essentielle du contra**t avec le prestataire. Parmi les éléments à prendre en compte lors de la rédaction de la clause, il faudra s'assurer des éléments suivants :

- de pouvoir récupérer les éléments **dans l'état dans lequel ils seront** au moment de la sortie du contrat,
- que les données seront dans un **format lisible** par l'entreprise,
- que le prestataire **offre son assistance** pour permettre la récupération de ces éléments, quelle que soit la situation,
- que les éléments seront **restaurés dans une durée raisonnable,**
- etc.

Outre les serveurs externalisés, cette clause est cruciale pour d'autres éléments du système d'information tels que le stockage de données en cloud, les applications hébergées, la gestion de la sécurité informatique et les infrastructures réseau. Ces composantes sont essentielles à la **continuité** et à la **souveraineté opérationnelle** de l'entreprise.

Parfois, la mise en place d'un **"plan de réversibilité"** peut être nécessaire entre le prestataire et son client, afin de définir certaines procédures d'utilisation ou de documentation permettant de garantir la réversibilité en fin de contrat.

AVANTAGES

- Liberté de changer de prestataire ou de récupérer en interne un service ou une fonction externalisée à tout moment

Action n°27 : Définir des SLA / garanties de services avec vos prestataires

PRINCIPE

Dans le cadre d'une prestation de service informatique, il est important de détailler les attentes et les responsabilités de chacun afin de **fiabiliser la prestation** et de **réduire les risques de mésentente**.
Au sein du contrat informatique, les **SLA (Service Level Agreement)** définissent un **accord de services** entre un fournisseur et son client, en formalisant les garanties d'engagement du prestataire, tant sur les résultats et les performances attendues que sur les délais d'intervention et de résolution des incidents.

ENJEUX

Qu'il s'agisse d'un contrat d'infogérance, d'hébergement, de support informatique / helpdesk, ou de toute autre prestation de service informatique, il est important de disposer d'une partie **SLA (Service Level Agreement).**

- En premier lieu, les SLA couvrent le **périmètre de la prestation**, notamment, le service concerné, les infrastructures et la plage horaire.
- Également, les SLA se doivent d'indiquer les garanties en termes **de performance** et de **disponibilité**, en veillant à définir des objectifs qui soient concrets, mesurables et atteignables.

Généralement, les SLA feront une distinction entre les i**ncidents non bloquants** et les **incidents critiques**, ceci faisant l'objet d'une caractérisation propre aux besoins de chaque entreprise. De plus, les SLA détermineront précisément les engagements du prestataire :

- en matière de **garantie de temps d'intervention (GTI)**, c'est-à-dire, le délai dans lequel les prestataires s'engagent à prendre en charge l'incident,
- en matière de **garantie de temps de rétablissement (GTR)**, c'est-à-dire le délai dans lequel il s'engage à ce que le problème ait été effectivement résolu.

Dans certains cas, il sera utile d'ajouter aux SLA une description des **pénalités dues** par le prestataire en cas de non-respect de ses engagements.
Il est également possible de mentionner la **PSG (Plage de Service Garantie)**, qui représente la durée pendant laquelle l'hébergeur assure la disponibilité du service proposé. L'hébergeur s'engage ainsi à rétablir ce service dans un délai minimum prévu appelé **GTR, ou Garantie Temps rétablissement**.

AVANTAGES

- Facilite l'évaluation du niveau de service
- Oblige le fournisseur et son client à être attentif et précis concernant le service attendu
- Protège les clients des attentes non respectées et le fournisseur des critères ambigus

Action n°28 : Vérifier la Responsabilité Civile de vos Prestataires pour les Risques Informatiques

PRINCIPE

Tout prestataire, quelle que soit sa taille ou son domaine d'activité, peut être la cible d'une attaque informatique qui pourrait impacter les données ou les informations appartenant à l'entreprise cliente. Il est important de contrôler que **vos prestataires** sont équipés d'une **assurance de responsabilité civile** couvrant les risques informatiques.

ENJEUX

Contrôler la **couverture en responsabilité civile** de **vos fournisseurs informatiques** est primordial pour la gestion des risques de votre entreprise. En effet, cette démarche vous prémunit contre d'éventuels **dommages collatéraux** : si le prestataire est attaqué, en tant qu'entreprise cliente, vous êtes moins susceptible de subir des pertes importantes, car l'assurance peut couvrir les frais de réparation et de récupération.

De plus, un prestataire bien assuré est souvent **mieux préparé** à gérer les conséquences d'une attaque informatique, réduisant ainsi l'impact sur l'entreprise cliente. Cette vérification témoigne de **l'engagement du prestataire en matière de sécurité informatique** et démontre qu'il met en place des mesures pour sécuriser ses partenariats et ses opérations.

Enfin, en contrôlant la responsabilité civile de vos prestataires, vous répondez aux **exigences réglementaires en matière de RGPD**, renforçant la conformité de votre entreprise.

AVANTAGES

- **Gestion des Risques** : Réduit le risque de pertes financières et de dommages à la réputation pour l'entreprise en cas de faille de sécurité chez le prestataire.
- **Conformité Réglementaire** : Contribue à la conformité avec les réglementations en vigueur concernant la protection des données et la sécurité informatique.

Action n°29 : Formaliser la politique de sécurité fournisseurs dans un PAS (Plan d'Assurance Sécurité)

PRINCIPE

Élaborer une politique de sécurité **fournisseurs** dans un **Plan d'Assurance Sécurité (PAS)** permet de préciser les attentes, les normes et les obligations en matière de sécurité informatique entre une entreprise et ses fournisseurs.

Mettre en place ce type de démarche pour vos propres fournisseurs vous permet d'établir des normes et des protocoles de sécurité communs aux différentes entreprises, dans le but de **minimiser les menaces** pesant sur la sécurité de votre système d'information.

ENJEUX

La formalisation de la politique de sécurité avec les fournisseurs dans un **Plan d'Assurance Sécurité (PAS)** permet de créer un cadre de travail sécurisé, en s'assurant que les partenaires suivent les mêmes standards.

Un PAS peut couvrir des aspects tels que la **gestion des accès**, la **protection des données**, la **réponse aux incidents** et la **conformité aux réglementations**. Il permet de prévenir certaines failles de sécurité et de minimiser les impacts de potentiels incidents de sécurité.

Enfin, il permet également d'identifier et de gérer les risques liés à la sous-traitance, d'améliorer la transparence et la traçabilité des actions de sécurité et de renforcer la confiance entre l'entreprise et ses fournisseurs.

AVANTAGES

- **Réduction des Risques de Sécurité** : Minimise les risques de sécurité liés à la collaboration avec les fournisseurs
- **Uniformisation des Pratiques de Sécurité** : Assure que tous les fournisseurs mettent en œuvre un niveau de sécurité adapté
- **Conformité Réglementaire** : Aide à satisfaire aux exigences réglementaires en matière de protection des données et de sécurité des systèmes d'information.

Pour aller plus loin

LEXIQUE

***RGPD**
En français “Règlement Général sur la Protection des Données”, le RGPD est une directive européenne établissant les règles à respecter concernant le traitement effectué par les entreprises et les administrations des données à caractère personnel. Applicable depuis le 25 mai 2018, il s’adresse à toutes les structures, publiques comme privées, quelle que soit leur taille.

***PCA/PRA**
Procédures mises en place pour garantir la continuité de fonctionnement du système d’information (dans le cadre d’un PCA) ou la reprise de l’activité (dans le cadre d’un PRA).

RESSOURCES

Mettre en place une politique de sécurité informatique : les bonnes pratiques (+ infographie)
Un article Déessi dédié à l'élaboration de la politique de sécurité d'une entreprise et comprenant une infographie à télécharger. *"Une politique de sécurité informatique est une stratégie visant à maximiser la sécurité informatique d’une entreprise. Elle est matérialisée dans un document qui reprend l’ensemble des enjeux, objectifs, analyses, actions et procédures faisant partie de cette stratégie..."*
https://www.deessi.si/mettre-en-place-une-politique-de-securite-informatique-les-bonnes-pratiques/

RGPD : le DPO est-il obligatoire pour votre entreprise ?
La loi RGPD impose-t-elle à votre structure de nommer un DPO ? La réponse dans cet article. *"Pour mettre en œuvre cette nouvelle réglementation, il a été pensé une fonction spéciale : le « Data Protection Officer », appelé en français « Délégué à la protection des données ». À la fois juriste et technicien, il est en charge de toutes les actions entourant la protection des données personnelles..."*
https://www.deessi.si/rgpd-le-dpo-est-il-obligatoire-pour-votre-entreprise/

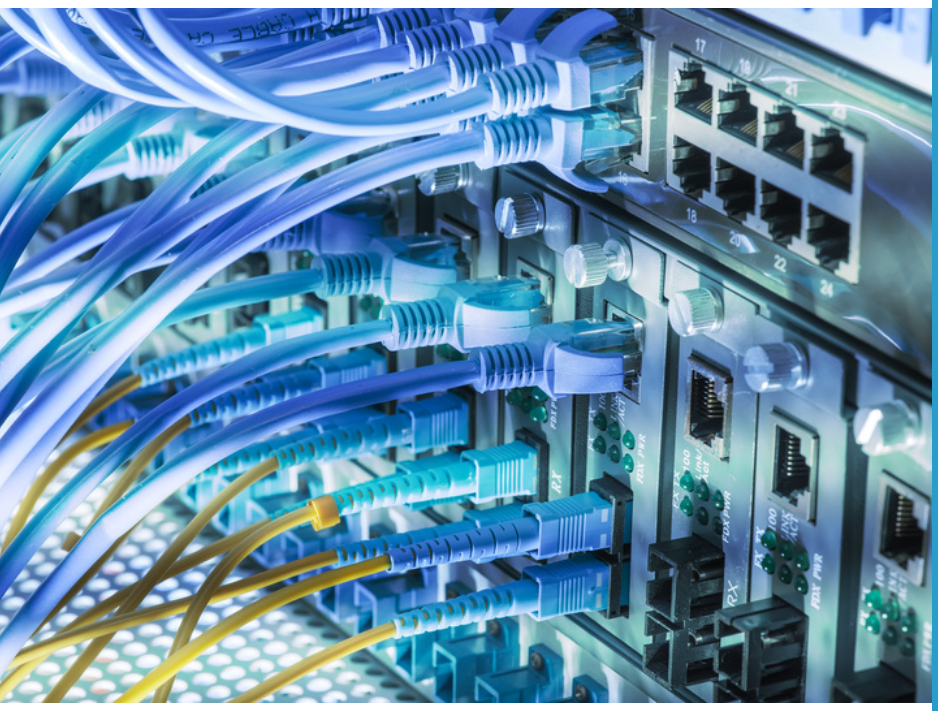
INFRASTRUCTURE EXTERNALISÉE

Parce que les systèmes d'information sont **de plus en plus complexes** à gérer, beaucoup d'entreprises se lancent dans **l'externalisation de leur SI**. L'objectif : s'affranchir de contraintes de gestion, bénéficier d'une meilleure expertise, et limiter les ressources à déployer.

Qu'il s'agisse d'hébergement de données, de bases de données, de sites web, d'applications, de messageries, ou encore, de toute l'infrastructure informatique de l'entreprise, un **service externalisé** est un service qui est **administré** par un **prestataire externe, et souvent même, hébergé par ce dernier** dans ses propres installations.

Entre autres atouts, recourir à des services externalisés et/ou hébergés, permet aux TPE et PME de disposer d'une **qualité de service pointue** et d'une **sécurité maîtrisée**, sans avoir à disposer des ressources et de l'expertise humaines et matérielles en interne

Action n°30 : Avoir une connexion Internet redondée avec bascule



PRINCIPE

Une **connexion Internet redondée** est une connexion Internet pour laquelle on dispose d'une connexion de secours, en plus de la connexion principale.

La seconde connexion **prend le relai**, automatiquement ou suite à une intervention humaine, en cas d'indisponibilité de la première connexion.

AVANTAGES

- Maintien du fonctionnement du SI ou reprise de l'activité en cas d'incident,
- Garantie de disponibilité,
- Garantie de niveau de service
- Maintien de la connexion Internet sans interruption et sans intervention humaine
- Bascule sur la connexion de secours sans délai et à tout moment

ENJEUX

Élément vital du système d'information de l'entreprise, la **connexion Internet** est souvent indispensable au **maintien de l'activité**. Cependant, toutes les structures ne mettent pas forcément en place **une solution de secours**.

Disposer d'une **seconde connexion Internet** répondant aux besoins de l'entreprise permet de s'assurer de la reprise ou de la continuité de l'activité **en cas de panne**.

Également, la seconde connexion peut permettre d'optimiser les performances et la bande passante des différents flux du système d'information, par exemple, on peut décider d'utiliser cette seconde connexion pour l'usage exclusif de la téléphonie.

À noter qu'il est important de définir les **modalités de déclenchement** ou de **mise en action** de cette connexion redondée, soit que le processus soit **automatique**, soit qu'il **nécessite une intervention** de la part des équipes informatiques ou du prestataire concerné.

La mise en place d'une **bascule automatique des liens Internet** est utile dans le cas où la structure ou l'entreprise **ne peut supporter une éventuelle interruption** de l'activité. La bascule s'effectue **sans délai** et à **tout moment**, même si **aucune équipe informatique n'est d'astreinte**.

Suite à la bascule des liens Internet, la structure dispose d'un **maintien continu de sa connexion** même en cas de panne ou d'incident.

À noter qu'il est utile que ce basculement automatique **soit régulièrement testé** pour s'assurer de son bon fonctionnement en toutes circonstances.

Action n°31: Choisir un hébergement dédié

PRINCIPE

Un **hébergement dédié** offre à la structure le recours à un ou plusieurs **serveurs uniquement réservé(s) à son propre usage**. Ce type d'hébergement s'accompagne de **possibilités plus étendues de gestion** et **de paramétrage** et nécessite des **compétences spécifiques** en administration de serveurs.

ENJEUX

Les données d'une entreprise ou d'une organisation constituant des **ressources vitales, sensibles** et parfois même **critiques**, il est désormais standard de les héberger sur un **serveur dédié à la structure**, plutôt que de les stocker sur des machines partagées avec d'autres utilisateurs. Ceci est indispensable pour **limiter les incidents**, mais aussi, pour **en garder la parfaite maîtrise**.

L'administration d'un serveur dédié étant **plus pointue**, des **compétences en administration serveur** ou le recours à un prestataire infogérant seront généralement nécessaires.

Outre les données hébergées par l'entreprise elle-même, il est important de tenir compte des **applications ou services** en mode SAAS* (voir lexique), qui sont hébergés par des éditeurs tiers. En effet, ceux-ci utilisent rarement des machines dédiées pour chacun de leurs clients.

AVANTAGES

- Garantie de disponibilité
- Réseau électrique stable
- Protection des accès physiques
- Fonctionnalités de gestion et de paramétrage sur mesure

Action n°32 : Héberger son informatique externalisée en France

PRINCIPE

Dans le cadre de **l'externalisation** de tout ou partie d'un système d'information, il est important de **connaître** et de **choisir la localisation du centre de données*** *(voir lexique)* du prestataire hébergeur. En effet, cette localisation peut avoir des impacts importants sur la **qualité du service**, mais aussi, sur l'intégrité des données et sur les **droits** et les **devoirs** du prestataire et du client vis-a-vis de la gestion et de la **sécurité de ces données**.

ENJEUX

Héberger ses données à l'étranger n'est pas sans **conséquences :**

- En effet, d'une part, la loi prévoit des clauses de contrat et une autorisation spéciale à obtenir auprès de **la CNIL** lors de transfert de données personnelles hors de l'Union Européenne.
- D'autre part, la **localisation de l'hébergement** implique que l'hébergeur **soit soumis à des lois étrangères** en matière de protection et de respect des données. Par exemple, aux États-Unis, le Cloud Act est une loi fédérale de 2018 et qui autorise les instances de justice américaine à contraindre les fournisseurs de services américains à fournir les données relatives aux communications électroniques d'un particulier ou d'une entreprise, et ce, quel que soit leur lieu de stockage.
- De plus, sur le plan de **l'efficacité du service** et de **sa pérennité**, la localisation des centres de données a aussi un impact sur **la rapidité** et **la sécurité** des communications.

L'idéal pour une entreprise française est donc d'héberger ses données **à proximité des nœuds de transit, c'est-à-dire entre l'entreprise, ses propres serveurs** et **ses clients**.
Sur le plan légal et de la règlementation, il est préférable de choisir des centres de données situés en France (ou du moins en Europe) afin de bénéficier des lois européennes en matière de protection et de confidentialité des données, ainsi que du RGPD.

Pour finir, il est important de s'assurer que le datacenter est implanté dans un environnement technologique et concurrentiel qui pousse le prestataire à s'améliorer sans cesse pour proposer des prestations de qualité toujours supérieure.

AVANTAGES

- Rapidité et efficacité des communications
- Conformité avec la législation
- Protection et confidentialité des données

Action n°33 : Disposer d'une supervision du SI

PRINCIPE

La **supervision** du système d'information consiste à mettre en place une **surveillance ou monitoring** afin de s'assurer à un instant T du bon fonctionnement des services informatiques, réseaux, applications, logiciels et matériels. Cette surveillance est idéalement complétée par de la **métrologie**, qui consiste dans l'étude de la charge supportée par ces éléments du système d'information dans le temps ou sur certaines périodes données.

La supervision s'effectue **à l'aide d'outils** chargés de remonter des alertes, mais aussi et surtout, avec la mise en place **d'une équipe dédiée à la supervision** de ces alertes et à **leur prise en charge.**

AVANTAGES

- Gestion du matériel des services et des logiciels,
- Gestion et supervision des sauvegardes
- Maintien en conditions opérationnelles de l'ensemble du système d'information
- Evolutions du système d'information en mode projet

ENJEUX

Les dispositifs logiciels de **surveillance des systèmes d'information** permettent de détecter les incidents et anomalies en direct et d'obtenir des alertes sur les dysfonctionnements du système.

Ils sont utiles aux DSI et permettent de gagner en temps et en efficacité, mais **ne remplacent pas totalement la surveillance humaine**, qui reste indispensable pour mettre en place des **mesures pro-actives**.

En effet, les équipes chargées de cette surveillance s'assurent du **bon fonctionnement des réseaux**, **machines et terminaux**, mais aussi, vérifient les **pare-feux** et **antivirus**, effectuent le suivi des **applications** et **logiciels**, leur **disponibilité** et leurs **mises à jour**.

Également, ces équipes effectuent la **surveillance réseau**, les **redémarrages serveurs**, la mise à jour des **systèmes d'exploitation** et la **vérification des sauvegardes de données**.

Ainsi, au-delà de la simple **résolution des problèmes** qui se présentent, la surveillance humaine permet de garantir un **niveau de qualité continu**, **prévenir les pannes** et les **intrusions** et de mettre en place les **plans d'actions** les mieux adaptées pour réagir aux situations de crise ou d'imprévus.

Action n°34 : Contrôler et assurer la disponibilité du SI

PRINCIPE

Un système d'information dispose de services qui ne possèdent pas tous la même criticité et qui ne tombent pas forcément en panne en même temps. La **disponibilité**, c'est la capacité pour un service du système d'information de continuer de fournir l'information demandée. Selon les besoins des entreprises, une **indisponibilité** de tout ou partie du système d'information peut être tolérée sur une durée plus ou moins longue. Dans d'autres cas, lorsque certaines indisponibilités ne sont pas tolérables, il est possible de mettre en place des contrôles et des mesures visant à **assurer une continuité permanente** du système ou du service concerné.

ENJEUX

Définir son besoin est le premier enjeu de la **mesure** et du contrôle de la **disponibilité du système d'information**. C'est en amont, avec sa DSI, son hébergeur et/ou son prestataire infogérant que ce besoin doit être correctement défini, si nécessaire, au moyen **d'audits** et de **mises en situations**.

Le **niveau de criticité** d'un système d'information pour une PME devrait être choisi en fonction de la nature de l'entreprise et de son **besoin en continuité des opérations**. Différents **niveaux de disponibilité** sont couramment utilisés dans les accords de niveau de service (SLA) avec des infogérants. Le minimum standard pour une majorité des entreprises est de 99%, mais le niveau de disponibilité peut être élevé jusqu'à 99,999% dans des environnements où chaque minute de panne peut avoir des conséquences significatives, comme dans les services de télécommunications ou les services financiers en ligne.

Une fois ce besoin identifié, il s'agit de mettre en œuvre **les moyens** de **surveiller le bon fonctionnement** du système et du réseau, à l'aide d'une **surveillance automatique** et / ou d'une **surveillance humaine**, mais aussi, de mettre en place des moyens de **redondances** (infrastructures, matériels, services) permettant d'assurer une **reprise rapide** ou une **continuité de fonctionnement** en cas de panne ou d'incident.

Ces processus devront prévoir également les **procédures de sauvegarde, de restauration des données et pourront se poursuivre par** la mise en place d'un PCA (Plan de Continuité d'Activité) ou d'un PRA (Plan de Reprise d'Activité).
Sur le plan stratégique, la connaissance de la disponibilité du système est un atout pour la DSI, qui permet de mieux dimensionner ses moyens, mais également, de s'assurer du service rendu auprès des services métiers et de mettre en valeur et valoriser les performances du SI.

AVANTAGES

- Valorisation l'état du système d'information
- Définition d'actions et de processus complémentaires (sauvegardes, PCA, PRA...)
- Mesure du service rendu auprès des services métiers
- Ajustement des besoins en disponibilité de services

Action n°35 : Mettre en place des remontées d'alertes automatiques

PRINCIPE

Virtualisés, hétérogènes et composés de multiples services externes additionnels, les systèmes d'informations sont de plus en plus complexes à gérer. Pour une **supervision** la plus efficace possible, le recours à des **logiciels de monitoring** disposant **d'alertes automatiques** offre aux équipes informatiques **la centralisation** de toutes les informations importantes et utiles à la prise de décision.

ENJEUX

Les remontées d'alertes automatiques, assurées par des solutions logicielles de monitoring, effectuent des analyses et des diagnostics constants de diverses parties du système d'information, telles que les sauvegardes, les serveurs, les réseaux, les applications, les bases de données, et les systèmes de sécurité comme les pare-feu et les systèmes de détection d'intrusion.
Ces outils peuvent également surveiller les performances du matériel, la consommation des ressources, et les processus système critiques pour assurer une gestion efficace et proactive du système d'information.

Ces solutions centralisent dans une même interface les **informations de santé** et de **bon fonctionnement du système d'information,** mais aussi, des **alertes en temps réel** sur les dysfonctionnements détectés.

Selon les cas, certains outils d'alertes disposent même de **fonctionnalités avancées**, les transformant en véritables **solutions de gestion de parc informatiques**. Dans ce cas, ces outils permettent également de disposer d'un **inventaire complet** des éléments matériels ou logiciel du système, mais également, de déployer, à distance, des agents sur vos équipements, ou encore, d'instaurer d'éventuelles procédures de surveillance et de suivi des équipements.

I est important d'ajouter que ces alertes doivent faire l'objet d'une analyse par une personne qualifiée, afin de garantir une interprétation correcte et une réaction appropriée aux potentiels problèmes identifiés.

AVANTAGES

- Suivi du fonctionnement du SI
- Centralisation des données dans une même interface
- Alertes en temps réel
- Fonctionnalités avancées possibles

Pour aller plus loin

LEXIQUE

SaaS
Le SaaS est une forme d'exploitation des logiciels qui se traduit à la fois par la disponibilité en ligne de l'application, mais aussi, par un business modèle associé avec un paiement de la licence sous forme d'abonnement. Les logiciels ou applications en mode SaaS sont directement hébergées, maintenues et mises à jour par leur éditeur, ce qui implique une facilité de gestion pour les entreprises. Pour le client, il est important de s'assurer des garanties de sécurité des données mises en place par l'éditeur, et parfois même, d'assurer elle-même des sauvegardes supplémentaires.

Datacenter
En français, "centres de données", un datacenter est un site physique regroupant des installations informatiques permettant de gérer ou de stocker les données informatiques d'une ou de multiples entités. Un datacenter peut ainsi correspondre à une structure privée ou à une entreprise dont le métier est de fournir hébergement de ces données à d'autres structures.

RESSOURCES

Hébergeur professionnel : faut-il le choisir en France ?
Découvrez dans cet article IVISION comment la localisation physique des données a de nombreux impacts, notamment en matière de sécurité des données et de droit applicable. *"Il importe à toute entreprise souhaitant faire héberger ses données, ou souhaitant les faire migrer, de se renseigner sur la politique de son prestataire hébergeur, et notamment sur la localisation de son ou de ses datacenters ainsi que sur les précautions mises en place pour se conformer à la législation."*
https://www.deessi.si/hebergeur-professionnel-faut-il-le-choisir-en-france/

Indisponibilité de service informatique, combien ça coûte aux entreprises ?
Un article didactique sur le sujet des coûts de l'indisponibilité du SI pour les entreprises. *"Selon la durée (de quelques heures à plusieurs semaines), l'indisponibilité des services entraîne une perte de revenus qui peut mener, dans le pire des cas, à la faillite. Évaluer le coût réel de l'indisponibilité informatique est un exercice difficile. Certains frais directs sont évidents, mais d'autres coûts sont indirects et de par là même, plus difficiles à identifier."*
https://www.deessi.si/indisponibilite-de-service-informatique-combien-ca-coute-aux-entreprises/

Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques (ANSSI)
Guide réalisé par l'ANSSI et utile pour le choix d'un prestataire d'hébergeur informatique. *Parce qu'il est indispensable, dans toute opération d'externalisation, de faire appel à des prestataires qui s'engagent sur la sécurité, l'ANSSI propose un guide de l'externalisation qui vous aidera à maîtriser les aspects de sécurité dans les marchés d'infogérance. On identifie trois grands domaines de risques (plus d'informations à l'intérieur) : la perte de maîtrise du système d'information ; les interventions à distance ; l'hébergement mutualisé.*
https://www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/

SAUVEGARDE

Qu'il s'agisse d'hébergement de données, de bases de données, de sites web, d'applications ou encore de messageries, un **service hébergé** est un service qui est **géré** et **administré** par un **prestataire externe** à la structure ou à l'entreprise.

Recourir à des services hébergés permet à des TPE ou à des PME de disposer d'une **qualité de service pointue** et d'une **sécurité maîtrisée**, sans avoir à disposer des ressources et de l'expertise humaines et matérielles en interne

SAUVEGARDE

Action n°36 : Réaliser une sauvegarde

PRINCIPE

Les données informatiques sont critiques pour l'entreprise. Véritable patrimoine dont la valeur est inestimable, il est crucial de veiller à les sécuriser et à en garantir l'intégrité.

Une **sauvegarde informatique** consiste à effectuer une copie de ses données sur un support différent du support initial. L'objectif est généralement de permettre la **récupération des données** en cas d'incidents de tous types, qu'il s'agisse de panne, de perte ou de destruction de la donnée, ou encore de vol, de piratage ou de perte d'intégrité de la donnée.

AVANTAGES

- Permettre la récupération des données en toute circonstance
- Respecter la législation en matière de protection des données

ENJEUX

Pour une entreprise, s'assurer de la capacité de récupérer ses données en cas d'incident est vital pour la pérennité de l'activité.

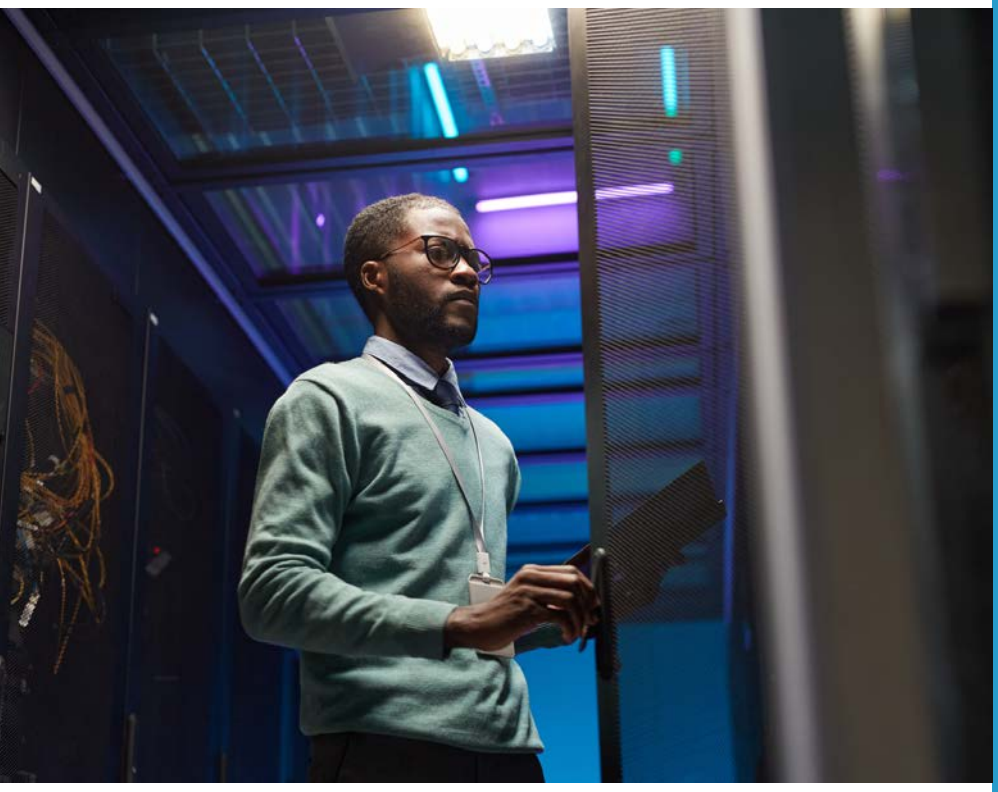
Les **sauvegardes professionnelles** répondent généralement au minimum au **schéma 3-2-1**, qui consiste à disposer de **3 copies différentes**, stockées sur **2 supports différents**, dont l'un des supports au moins est **externe au système**.

Cependant, dans le cas de données critiques ou de besoin spécifiques à l'entreprise, il est possible d'envisager des stratégies plus complexes incluant davantage de précautions ou d'éléments de redondance.

Les données des entreprises étant de plus en plus volumineuses, disparates, et à augmentation exponentielle, il est également nécessaire de mettre en place des **stratégies sélectives de sauvegarde**, c'est-à-dire, ne pas nécessairement sauvegarde l'ensemble du système mais déterminer quelles sont les données à sauvegarder, définir également le besoin est associé à cette sauvegarde (en termes de fréquence, de volumes et de redondance), ou encore, définir s'il faut réaliser une sauvegarde complète*, différentielle* ou incrémentielle* *(voir lexique)*.

En autres critères de performance de la sauvegarde professionnelle, il est également important de s'assurer que celle-ci ne gène pas le fonctionnement habituel du système d'information au quotidien.

Action n°37 : Externaliser la sauvegarde



PRINCIPE

Une **sauvegarde externalisée**, c'est une sauvegarde **confiée aux soins d'un prestataire et** inclue dans le cadre d'une **stratégie globale de gestion des données**.

L'objectif de confier sa sauvegarde un prestataire externe est de **bénéficier des services** et **des garanties** de ce prestataire concernant le fonctionnement de cette sauvegarde et sa restauration en cas de sinistre.

AVANTAGES

- Accès nomade
- Faible consommation de ressources matérielles
- Centre de données sécurisé
- Selon les garanties des prestataires : garantie de disponibilité, de tests de sauvegardes ou de restaurations, engagements de résultats

ENJEUX

En cas d'incident informatique avec perte de données, **la sauvegarde** est le dernier rempart permettant à l'entreprise de **limiter les dégâts**.

Malheureusement, les sauvegardes sont **peu testées** et leur fiabilité n'est généralement éprouvée **qu'en situation critique**.

Confier sa sauvegarde à un spécialiste permet de s'assurer de sa **sécurité**, de son **bon fonctionnement** et de sa **disponibilité**. Des éléments indispensables à maîtriser en cas d'incident.

En faisant appel à des **prestataires spécialisés** et qui disposent **d'infrastructures fiables et sécurisées**, les entreprises bénéficient de la supervision de leurs sauvegardes, sur des espaces **managés 24h/24,** et avec des systèmes de **sécurité supplémentaires**, comme la redondance des données sur un ou plusieurs autres serveurs.

Ils s'assurent également de bénéficier d'une **expertise à la pointe** des **bonnes pratiques**, afin de mettre en œuvre les **dernières recommandations** adaptées aux évolutions de pratiques en matière de sécurité informatique.

Ceci bien entendu sous couvert de s'assurer des conditions et des garanties auxquelles le prestataire s'engage, et que celles-ci correspondent précisément au besoin de sauvegarde de l'entreprise.

Action n°38 : Réaliser des tests de sauvegarde

PRINCIPE

Un **test de sauvegarde** consiste à effectuer une **restauration de sauvegarde** à la seule fin de vérifier que cette restauration s'effectue **sans problème** et que les données sont bien **récupérables**.

Ceci est particulièrement utile pour **détecter à l'avance** toute erreur ou dysfonctionnement qui pourraient rendre la sauvegarde **inopérante en situation de restauration**.

ENJEUX

Parce que les sauvegardes sont généralement des **procédures automatiques**, et qu'elles ne sont utiles qu'en situation d'urgence, il est très fréquent de **passer à côté des éventuels dysfonctionnements**, qui peuvent se manifester sous la forme d'un **échec de système** ou d'une **erreur** par exemple. Ceci peut avoir des **conséquences très importantes en situation d'urgence**, dans les cas où la sauvegarde est devenue le **seul moyen** de récupérer les données perdues ou corrompues par exemple.

La mise en place de tests réguliers de **sauvegardes complètes** assure que ces sauvegardes se déroulent sans encombres et garantit que l'intégralité des données sera accessible et exempte d'erreurs en toutes circonstances.

Il est important de définir la **procédure** et la **périodicité** à laquelle ces tests de sauvegarde sont réalisés et de déterminer les **équipes** ou **le prestataire** en charge de ces opérations. Ceci peut notamment être consigné dans un **plan de sauvegarde**, permettant à différents interlocuteurs, en situation d'urgence, de restaurer les données en suivant la documentation.

Bien évidemment, les tests de sauvegarde ne dispensent pas des **autres procédures indispensables**, comme par exemple de s'assurer que les sauvegardes sont bien redondées sur 2 ou 3 supports différents, situés à des localisations distinctes.

AVANTAGES

- Réduire le risque de sauvegarde inutilisable ou inopérante

Action n°39 : Chiffrer sa sauvegarde

PRINCIPE

Une sauvegarde de données consiste à disposer d'une copie des données utilisables en cas d'incident. Un **chiffrement de sauvegarde** consiste à **crypter les données de la sauvegarde** à l'aide d'un **algorithme** et d'un jeu de **clefs de chiffrement,** dans le but d'en garantir la **confidentialité** et l'**intégrité**.

ENJEUX

Généralement, une sauvegarde de données est effectuée de la façon suivante : les données sont **compressées**, ce qui permet de les déplacer plus facilement, puis elles sont **chiffrées,** ce qui permet de **garantir leur intégrité pendant et après leur déplacement**. Les enjeux pour l'entreprise sont importants, tant sur le plan des **menaces informatiques externes** que des éventuels **accès indiscrets** de collaborateurs.

Le chiffrement consiste à **rendre les données** de la sauvegarde **illisibles**, que ce soit **pendant le transport** ou **une fois stockées**, pour toute personne qui ne disposerait pas de la **clé de déchiffrement correspondante**.

Il existe différentes **normes et standards de chiffrements**, chiffrement symétrique, asymétrique, avec des longueurs de clé pouvant aller de 128 à 256 bits. La norme AES 256 Bits est actuellement la norme de chiffrement la plus évoluée sur le marché.

Face à l'augmentation du nombre et de la dangerosité des **crypto-virus**, il est essentiel de protéger spécifiquement les sauvegardes informatiques des accès non autorisés et des dommages potentiels causés par les **ransomwares**. En effet, ces sauvegardes représentent le dernier rempart contre ces menaces et leur intégrité est cruciale pour assurer la récupération des données après une attaque.

AVANTAGES

- Réduire le risque d'accès frauduleux aux données des sauvegardes de l'entreprise, qu'il s'agisse de menaces internes ou externes

Action n°40 : Définir une fréquence de sauvegarde adaptée aux besoins de la structure

PRINCIPE

Définir une **fréquence de sauvegarde** ne devrait idéalement pas être un choix arbitraire.

Outre la rationalisation des efforts de sauvegarde et des capacités techniques mises en œuvre, la mise en place d'un **calendrier de sauvegardes** est avant tout déterminée par la **stratégie de résilience informatique** de l'entreprise.

ENJEUX

Pour une entreprise, la définition des **fréquences de sauvegarde** sous forme d'un **calendrier** est souvent arbitraire ou liée à la nécessité de **contrôler les coûts de gestion** de la sauvegarde et d'être **cohérent avec les moyens techniques et humains** dont dispose l'entreprise pour cette tâche.

Cependant, même si ces critères de faisabilité et de ressources entrent en jeu, la fréquence de sauvegarde devrait idéalement être déterminée avant tout par **le RPO (Recovery Point Objective)**, c'est-à-dire la **durée maximale** autorisée pendant laquelle la structure est dans l'incapacité de continuer à enregistrer ses données. Par exemple, si l'entreprise détermine qu'en cas d'indisponibilité du système, une perte de données ne devrait pas excéder 10mn, dans ce cas, elle doit idéalement définir la fréquence de ses sauvegardes à 10mn.

RPO et calendrier de sauvegarde sont ainsi des éléments vitaux de la mise en œuvre de la stratégie de continuité de service, de sauvegarde des données et de résilience informatique de l'entreprise.

AVANTAGES

- S'assurer de ne subir aucune perte de données en cas d'incident informatique nécessitant la restauration d'une sauvegarde

Pour aller plus loin

LEXIQUE

Sauvegarde complète : Sauvegarder l'ensemble des données stockées sur la partition ou tout le disque concerné.

Sauvegarde incrémentielle : Sauvegarder uniquement les données modifiées ou ajoutées depuis la dernière sauvegarde, qu'il s'agisse d'une sauvegarde complète ou incrémentielle.

Sauvegarde différentielle : Sauvegarde des données modifiées ou ajoutées depuis la dernière sauvegarde complète.

RESSOURCES

Zoom sur : la sauvegarde managée
Découvrez les points de réflexion à considérer lorsque l'on confie sa sauvegarde à un prestataire. *"Pour l'entreprise, il s'agit de mettre au point une stratégie de sauvegarde en adéquation avec ses besoins et avec la criticité de son information. De leur côté, les prestataires, qui se voient confier le patrimoine stratégique de l'entreprise, sont au cœur de la stratégie de pilotage du système d'information. Pour les uns comme pour les autres, il est important de définir les contours de la prestation afin de s'assurer que chacun respecte ses droits et ses obligations et que la pérennité des données sera assurée. Dans cet article, nous allons donc nous pencher sur cette notion de sauvegarde managée et sur ce qu'elle recouvre."*
https://www.deessi.si/zoom-sur-la-sauvegarde-managee/

De la sauvegarde physique à la sauvegarde professionnelle dans le Cloud : mode d'emploi
Un article complet pour identifier les enjeux et les atouts de la sauvegarde de données dans le Cloud, à lire chez IVISION.
"Durant plusieurs décennies, la sauvegarde sur support physique était privilégiée. Et pourtant, ce type de sauvegarde n'est pas le plus adapté, notamment pour les TPE et les PME, et comporte un certain nombre de risques et de contraintes."
https://www.deessi.si/de-la-sauvegarde-physique-a-la-sauvegarde-professionnelle-dans-le-cloud-mode-demploi/

TRAVAIL À DISTANCE

La mise en place du **travail à distance**, qu'il s'agisse de télétravail régulier ou de salariés ayant des activités nomades ponctuelles, nécessite une **organisation** et des **moyens techniques** particuliers, avec notamment un **système d'information flexible**, offrant la possibilité de travailler et de collaborer depuis n'importe quel lieu.

De plus, le travail à distance entraîne des **risques spécifiques** en matière de **sécurité informatique**. En effet, lorsque le salarié travaille à domicile, il n'est plus protégé par les règles de sécurité mises en place au sein du système d'information de l'entreprise.

La sécurité des données manipulées par l'employé ou des fichiers accédés deviennent alors dépendants du lieu de connexion, des pratiques du salarié et du matériel utilisé.

Action n°41 : Sécuriser les accès au SI avec un VPN

PRINCIPE

Un **VPN (Virtual Private Network ou Réseau Privé Virtuel)** est une technologie garantissant une **navigation Internet sécurisée** et **anonyme.**
Plus précisément, il s'agit d'un **tunnel de connexion** virtuel qui permet des **échanges sécurisés** et **cryptés** entre un point A et un point B, A pouvant être, par exemple, un collaborateur en mobilité et B, le siège de l'entreprise.

AVANTAGES

- Sécurisation des données de l'entreprise
- Protection des équipements informatiques de l'entreprise
- Sécurisation des échanges sur site ou à distance

ENJEUX

Au sein de l'entreprise, le **VPN (Virtual Private Network)** est un réseau privé virtuel permettant notamment de **sécuriser les échanges de données de type "extranet"** et de mettre en place des **liaisons internet sécurisées** entre des sites distants.

Le but est de permettre d'assurer une **sécurité des échanges** beaucoup plus importante.

Un VPN procure **un accès sécurisé à toutes les ressources de l'entreprise**, qu'elles soient **internes** ou présentes dans **le Cloud**. Le VPN protège ainsi les **environnements Cloud**, les **serveurs de transfert** et les **bases de données** de l'entreprise.

Les **appareils des employés** bénéficient également de cette protection, même en **déplacement** ou en **télétravail**, et la protection VPN s'active lorsqu'ils se connectent à des réseaux inconnus ou non sécurisés.

Action n°42 : S'équiper d'une téléphonie Full IP

PRINCIPE

Parce que 2019 a sonné la fin du réseau téléphonique RTC* *(voir lexique)* en France, les entreprises utilisent désormais les **technologies VoIP** et **ToIP**, pour des **communications téléphoniques** qui transitent via le **protocole Internet**. La téléphonie IP permet de conserver les fonctionnalités de téléphonie traditionnelles, tout en ajoutant des briques fonctionnelles permettant d'améliorer les services de téléphonie et d'informatique.

On parle de **téléphonie « full IP »** lorsque les communications sont transportées en IP de bout en bout, depuis **l'opérateur jusqu'au poste téléphonique**.

ENJEUX

Par rapport à la **téléphonie IP simple**, la **téléphonie Full IP** offre toutes les options de services IP utiles aux entreprises, tout en réduisant les **risques de latences** ou de **dégradation de la qualité audio**.

La VOIP a pour avantage de permettre de **disposer de sa ligne fixe partout, sans contrainte** et sur **des appareils différents** indépendamment du reste de l'infrastructure en place (électrique, coupure internet, mauvaise connexion…). Autre avantage : les fonctionnalités avancées de la VOIP offrent la possibilité de réagir en cas de crise ou encore renvoyer un nombre d'appels importants vers une boîte vocale.

Ainsi, avec le Full IP, l'entreprise dispose d'une **qualité d'appels haute définition**, mais aussi, des autres **fonctionnalités** de la VOIP (**convergence** des services, mise en place de **numéros uniques** pour les lignes fixes et mobiles, **répondeur** téléphonique **unifié, options de standard téléphonique, etc.**)

Elle permet également de garantir que la **confidentialité du trafic entrant et sortant** de l'entreprise est **assurée**.

AVANTAGES

- Avantage budgétaire
- Souplesse d'exécution en mobilité
- Haute qualité des appels
- Unification des lignes fixes et mobiles
- Unification des messageries
- Interopérabilité avec services de type CRM
- Fonctionnalités additionnelles et de standard téléphonique

Action n°44 : Utiliser une solution de partage de documents professionnelle

PRINCIPE

Le **partage de document** est un processus incontournable de la collaboration en entreprise.

Au fur et à mesure des évolutions technologiques, les entreprises deviennent de plus en plus exigeantes en matière d'outils et de solutions de partages de documents, tant sur les **aspects pratiques** et **fonctionnels**, que sur la **sécurité informatique** et les **fonctionnalités avancées**.

AVANTAGES

- Accès nomade
- Travail collaboratif
- Centralisation de la documentation
- "Versioning" et historique du document
- Enregistrement automatique du document en temps réel

ENJEUX

Les fonctionnalités courantes de **partage de documents en entreprise** sont de **télécharger**, **consulter, modifier** et **renvoyer** les différents documents avec lesquels les collaborateurs interagissent dans le cadre de leurs fonctions. Ceci pose la problématique des **versions de fichiers**, qui nuit bien souvent à **l'efficacité** des échanges.

Les **solutions de partage de document modernes** ont réduit ce problème avec la possibilité de **travailler en commun sur des documents** disposant d'une **version unique**. Le document est **mis à jour en temps réel**, par les différents intervenants qui accèdent tous à cette **même version évolutive**. De plus, tous les collaborateurs sont capables d'accéder aux fichiers **de façon distante**, qu'ils travaillent dans les **locaux de l'entreprise** ou en **télétravail**, du moment qu'ils disposent d'un accès Internet.

La solution de partage de documents peut également fournir **d'autres avantages**, par exemple, disposer d'un **historique** et d'un **suivi des modifications**, ajouter de façon collaborative **des commentaires**, avec des **procédures de validation**, ou encore, protéger le partage du fichier avec des **liens temporaires** ou des **mots de passe**.

Ce type de solution constitue un outil indispensable pour **fiabiliser la collaboration** en entreprise tout en respectant les **bonnes pratiques de sécurité**.

Action n°43: Posséder une charte de télétravail

PRINCIPE

Une **charte de télétravail** est un document qui permet de formaliser **les conditions dans lesquelles le télétravail est réalisé** au sein de l'entreprise ou de la structure, pour l'ensemble des collaborateurs. La charte de télétravail reprend les **règles de travail** (durée, horaires) mais aussi les **moyens mis à disposition** (matériel informatique, outils et logiciels, ergonomie du poste de travail) ou encore, les **usages et pratiques** du collaborateur, comme le respect des pratiques de **sécurité informatique** ou la **confidentialité** des données. La charte de télétravail est souvent associée à la **charte informatique**.

ENJEUX

La **charte de télétravail** est un **document de référence** qui fixe les **droits** et les **devoirs** respectifs entre l'employeur et les employés **dans le cadre du télétravail**.

Sur le plan RH, elle concerne par exemple des éléments tels que la **durée de la période de télétravail**, les **horaires** ou encore **l'ergonomie du poste de travail**. Sur le **plan juridique,** c'est un document interne qui ajoute **des dispositions au contrat de travail**, sans toutefois s'y substituer. Ce document dispose d'une valeur en cas de litige. Il n'est cependant pas nécessaire de faire appel à un avocat pour le rédiger.

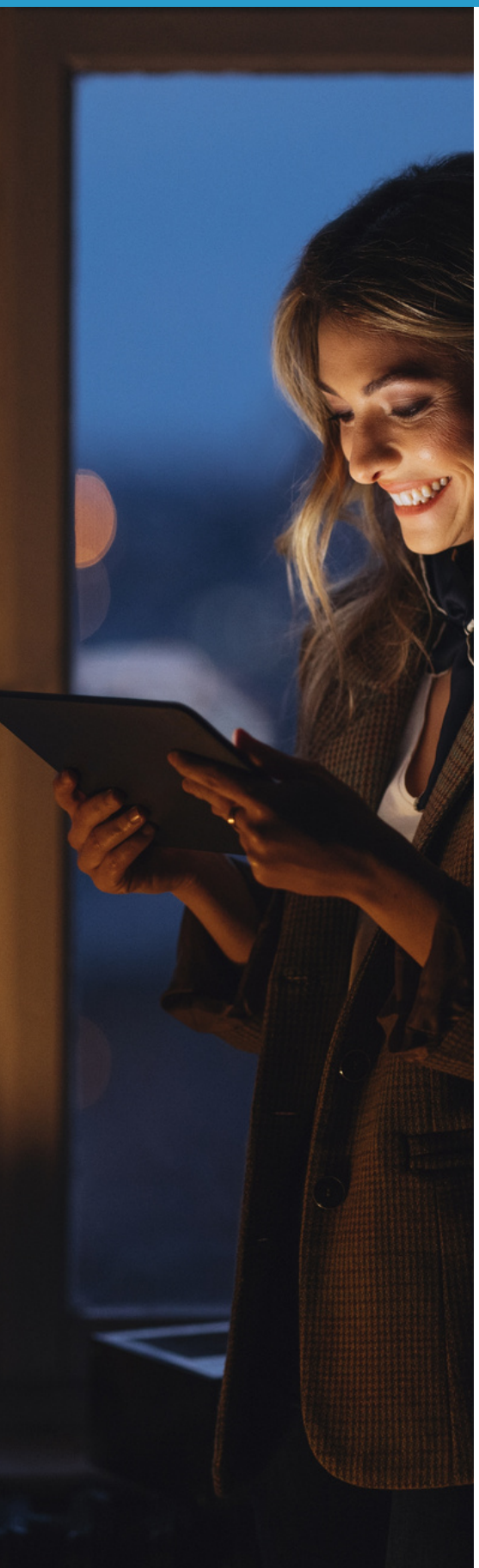
Sur le plan de la **résilience informatique**, la charte de télétravail jour un rôle lorsqu'il s'agit de définir le **matériel** qui sera **utilisé ou mis à disposition** des collaborateurs, les **règles d'utilisation** et de **protection informatique** de ce matériel, ou encore toutes les **règles de sécurité informatique** liées à l'exercice de l'activité et à **l'accès aux données et documents** de l'entreprise (usages personnels / professionnels, outils et logiciels, connexion internet etc.) dans le cadre du télétravail.

Cette charte est donc indispensable pour **sécuriser les pratiques des collaborateurs** contre des éventuelles failles ou piratages, dans des situations où **ils ne sont plus protégés par le système d'information** de l'entreprise.

AVANTAGES

- Définition des règles d'usages numériques et de sécurité informatique dans le cadre du télétravail
- Meilleur encadrement de l'organisation du télétravail
- Meilleure maîtrise des aspects légaux liés au télétravail

Action n°45 : Fournir un matériel dédié uniquement aux usages professionnels



PRINCIPE

Dans le cadre du **télétravail**, le **matériel utilisé** par les employés à une très grande incidence sur le r**espect des règles** et des **procédures** de l'entreprise, et en particulier sur le respect de la **politique de sécurité informatique** de l'entreprise.

Mettre à disposition des salariés un matériel **dédié uniquement aux usages professionnels** est un prérequis indispensable pour la **résilience informatique**.

ENJEUX

Pendant le télétravail, les employés peuvent être amenés à **relâcher leurs efforts** en matière de **respect des règles de sécurité informatique**. Ceci est d'autant plus vrai si le télétravail est une démarche nouvelle ou s'il est mis en place dans des conditions d'urgence, comme lors de la crise sanitaire de 2020.

L'utilisation d'**appareils personnels** pour des usages professionnels incite fortement à adopter de mauvaises habitudes, d'autant que ce matériel n'est pas intégré au système d'information de l'entreprise et ne possède pas d'outils de sécurité informatique efficaces.

Mettre à disposition des employés un **matériel dédié aux usages professionnels** permet de s'assurer que ce matériel est **protégé par les outils de l'entreprise** et **respecte les procédures** édictées par la politique de sécurité de la structure, qu'il s'agisse d'accéder au réseau de l'entreprise, de se connecter à un réseau externe ou de la politique de gestion des accès.

AVANTAGES

- Limitation du recours aux appareils personnels ***(BYOD)**** *(voir lexique)*
- Meilleur respect de la politique de sécurité informatique de l'entreprise
- Centralisation et simplification de l'administration des appareils

Action n°46 : Disposer d'un outil de visioconférence sécurisé

PRINCIPE

La **visioconférence** s'est récemment démocratisée en entreprise. La plupart des solutions de visioconférence permettent de répondre aux besoins standards de **réunions à distance**. Mais les problématiques de **sécurité informatique** et de **résilience** font qu'il existe désormais des enjeux autour de la sécurité et du respect de la confidentialité apportée par ce type d'outils.

ENJEUX

En entreprise, une **solution de vidéoconférence** peut être utilisée pour **dialoguer avec un interlocuteur**, le **voir,** mais aussi, **partager son écran** ou **échanger des documents**.

Outre la protection contre le piratage et la cybersécurité, les enjeux de stratégie et de confidentialité liés à la plateforme de visioconférence ne sont pas toujours bien anticipés par les entreprises, notamment sur le plan de la **propriété intellectuelle** ou du **piratage industriel**.

En matière de **sécurisation des données**, on privilégiera une solution **chiffrée de bout en bout**, et idéalement, répondant à des **normes de sécurité exigeantes** telles que la norme ISO/IEC 27001.

En matière de législation, il faut savoir que le **lieu d'hébergement des données** de la plateforme **détermine le droit applicable aux échanges**. Pour des entreprises françaises, il est donc préférable de privilégier un prestataire **situé en Europe**, d'une part pour s'assurer du droit concerné en cas de nécessité, mais aussi, afin que les données échangées soient bien **protégées par le RGPD**, et ne tombent pas sous le coup d'une législation étrangère, comme avec le Patriot Act ou le Cloud Act américain par exemple.

AVANTAGES

- Fonctionnalités collaboratives avancées
- Sécurité et confidentialité améliorée
- Contrôle du lieu d'hébergement des données
- Ganrantie du taux de disponibilité
- Respect des normes et certifications
- Respect du RGPD* *(voir lexique)*

Pour aller plus loin

LEXIQUE

***Réseau téléphonique RTC**
Le réseau téléphonique commuté ou réseau téléphonique commuté public est le réseau historique des téléphones fixes. Technologie obsolescente vouée à être remplacée par des technologies plus modernes, elle est en France en cours d'arrêt par Orange, avec un arrêt technique des lignes téléphoniques prévu en 2023.

***Ligne Numéris**
Désigne une ligne téléphonique utilisant un signal numérique (qui convertit la voix en une suite de 0 et 1) afin de transmettre une communication entre deux utilisateurs. Il s'agit de l'évolution technique des lignes analogiques.

***Ligne analogique :**
Ligne utilisant un signal analogique (qui convertit la voix, en signal électrique) afin de transmettre une communication entre deux utilisateurs. Il s'agit de la technologie historiquement utilisée depuis les années 70.

***BYOD (Bring Your Own Device – apporte ton propre appareil)**
Tendance qui consiste, pour les collaborateurs, à utiliser leurs terminaux personnels à des fins professionnelles. Ceci pose des problématiques en matière de sécurité puisque ces appareils ne sont pas répertorié dans le système d'infirmation de l'entreprise.

***Datacenter**
En français, "centres de données", un datacenter est un site physique regroupant des installations informatiques permettant de gérer ou de stocker les données informatiques d'une ou de multiples entités. Un datacenter peut ainsi correspondre à une structure privée ou à une entreprise dont le métier est de fournir hébergement de ces données à d'autres structures.

***RGPD**
En français “Règlement Général sur la Protection des Données”, le RGPD est une directive européenne établissant les règles à respecter concernant le traitement effectué par les entreprises et les administrations des données à caractère personnel. Applicable depuis le 25 mai 2018, il s'adresse à toutes les structures, publiques comme privées, quelle que soit leur taille.

Pour aller plus loin

RESSOURCES

TÉLÉTRAVAIL : CRISE SANITAIRE ET MISE EN ŒUVRE INFORMATIQUE

Un article Déessi répondant à la problématique de mettre en place le télétravail dans son entreprise de façon urgente, comme lors de la crise sanitaire. "*Pour répondre aux impératifs du contexte sanitaire, il a été recommandé aux entreprises de mettre en place le télétravail chaque fois que possible. Même si nous sommes régulièrement informés à ce sujet, il n'est pas toujours facile pour des structures de type TPE ou PME de mettre en place le télétravail, notamment en termes d'outils informatiques ou de procédures.*"

https://www.deessi.si/teletravail-crise-sanitaire-et-mise-en-oeuvre-informatique/

L'IMPORTANCE CROISSANTE DE LA MOBILITÉ ET DU TÉLÉTRAVAIL DANS LE MONDE PROFESSIONNEL CRÉE DE NOUVEAUX RISQUES SUR LES SYSTÈMES D'INFORMATION.

Un guide de l'ANSSI portant sur les aspects sécurité des systèmes d'information liés au travail à distance. *Le développement du nomadisme et du télétravail ne cesse de prendre de l'ampleur ces dernières années, et est aujourd'hui au centre des réflexions des directions informatiques. Cela amène à réfléchir sur la manière de sécuriser ces accès distants au système d'information (SI) de l'entité, afin de gérer les besoins de confidentialité et d'intégrité des données, ainsi que l'authentification des utilisateurs...*"

https://www.ssi.gouv.fr/administration/guide/recommandations-sur-le-nomadisme-numerique/

ARCHITECTURE AGILE POUR LE TÉLÉTRAVAIL : MISE EN ŒUVRE EN 4 ÉTAPES (+ INFOGRAPHIE)

Un article et une infographie pour aborder la mise en place d'un système d'information agile, permettant le travail à distance de façon efficace. "*Pour basculer d'un système d'information traditionnel à un système d'information agile, 4 aspects principaux sont à prendre en compte : le recours à une IT dématérialisée dans le Cloud, l'équipement des utilisateurs avec du matériel dédié et un poste de travail virtualisé, le renforcement de la sécurité informatique, que ce soit pour l'accès aux données, les échanges, les sauvegardes… et la mise en place d'une solution unifiée de communication.*"

https://www.deessi.si/architecture-agile-pour-le-teletravail-une-mise-en-oeuvre-en-4-etapes/

TÉLÉTRAVAIL À DOMICILE : LES BONNES PRATIQUES DE SÉCURITÉ INFORMATIQUE

Un article IVISION qui aborde le télétravail sous l'angle de la sécurité informatique. *"Le télétravail en général apporte aux entreprises son lot de risques informatiques. En effet lorsque le salarié travaille à domicile, il n'est plus protégé par les règles de sécurité mises en place par l'entreprise. Qu'il s'agisse des logiciels de protection (antivirus, firewall…), des règles d'accès aux informations ou des règles de partage, ou encore de la sécurité de la connexion internet, tous ces paramètres deviennent dépendants du lieu de connexion du salarié, des pratiques que lui-même va appliquer ou encore du matériel qu'il va utiliser."*

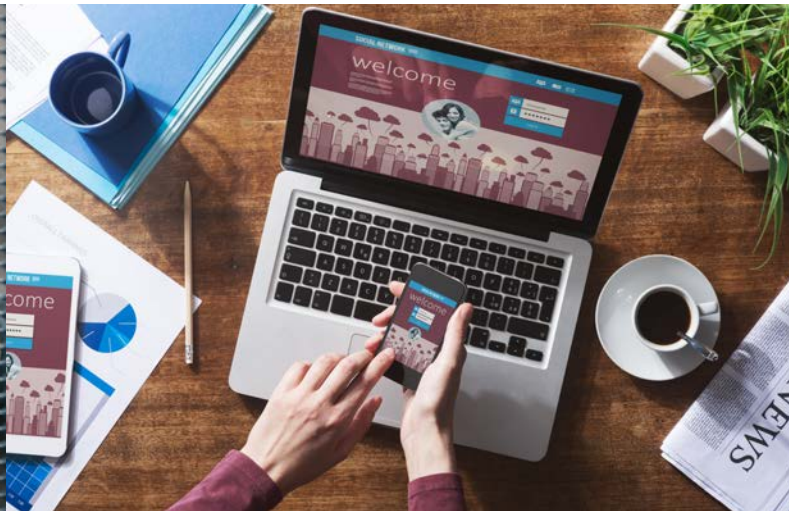
https://www.deessi.si/teletravail-a-domicile-les-bonnes-pratique-de-securite-informatique/

SITE WEB

Qu'il s'agisse d'une carte de visite, d'une vitrine commerciale, d'une boutique en ligne ou d'une plateforme offrant des services plus évolués, un site Internet représente souvent des **enjeux importants** pour la **bonne marche de l'activité** de l'entreprise.

Sont abordés dans ce chapitre des éléments concernant le maintien en **conditions opérationnelles** de son site Internet, mais également, son **hébergement**, sa **sécurité informatique** ou encore la nécessité de cloisonnement avec le reste du système d'information de la structure.

Action n°47 : Établir un cloisonnement entre son site web et son réseau local



PRINCIPE

Cloisonner son site web par rapport à son **réseau local** consiste à héberger le site dans une **instance indépendante du reste des données** de son entreprise.

Cette pratique permet de **réduire les risques de piratage de toutes les données** de l'entreprise en cas de compromission du site Internet lui-même. Elle est aujourd'hui couramment répandue, très peu d'éditeur ou d'hébergeur se risquant désormais à héberger un site internet en local.

ENJEUX

- Parce que le **site Internet d'une entreprise** est directement accessible sur le web, il s'agit d'une **porte d'entrée très fréquente** pour les **pirates informatiques**.
- Ceci est d'autant plus vrai que la plupart des sites Internet sont des **outils évolutifs**, soumis à des **changements fréquents** (mises à jour de modules*, de thèmes graphiques* *(voir lexique)*). De plus, **plusieurs intervenants** internes ou externes peuvent avoir la main sur le site, ce qui implique donc de multiples possibilités de **failles** ou **d'erreurs humaines**.
- C'est pourquoi il est nécessaire de mettre en place un **cloisonnement technique** avec le reste des **données de l'entreprise.** Ce cloisonnement doit être pensé de façon à s'assurer que le site **ne peut pas être utilisé pour infecter une autre partie du système d'information** de l'entreprise.

AVANTAGES

- Supression des risques de piratage du système d'information à travers un piratage éventuel du site Internet de l'entreprise

Action n°48 : Protéger son site web avec un antivirus / firewall / antispam

PRINCIPE

Comme toute machine composant le système d'information, un **site web** peut bénéficier **d'outils de protection** et de **sécurité informatique**, comme un antivirus ou un antispam par exemple.

ENJEUX

Les **piratages de sites Internet** sont fréquents, quotidiens, et touchent tous les types d'organismes ou de structures, quel que soit leur niveau de sécurité.

C'est pourquoi, un site Internet doit idéalement être **protégé avec des outils** de type **antivirus** ou **firewall professionnels**, qui apportent une couche de protection supplémentaire, au-delà de toutes les autres mesures pouvant être mises en œuvre par l'hébergeur informatique.

De plus, afin de réduire les **spams** et les techniques d'extorsions de donnés ou d'accès comme le **phishing*** *(voir lexique)* **reçus via vos formulaires de contacts**, il existe également des **antispams** spécifiquement pensés pour les sites Internet.

Pour un site Internet développé maison, on ajoutera en bonne pratique la réalisation régulières de scans de vulnérabilités et de revue de code. Qu'il s'agisse d'un CMS ou d'un site développé, l'utilisation du protocole HTTPS, des sauvegardes régulières et l'utilisation de mots de passes forts sont également des prérequis de sécurité indispensables. Il est également utile de protéger son site Internet contre les **attaques *DDoS**.

Lorsque l'entreprise **ne dispose pas des compétences** pour choisir et paramétrer ces outils, le **recours à un prestataire externe** peut s'avérer nécessaire. À noter toutefois que malgré toutes les mesures de protection possibles, le **risque zéro de piratage n'existe pas** et que les outils utilisés permettent seulement de **réduire le risque** de piratage.

AVANTAGES

- Réduction du risque de piratage du site Internet
- Réduction du nombre de spams reçus,
- Réduction des risques de phishing

Action n°49 : Disposer d'un site web monitoré et infogéré

PRINCIPE

Comme n'importe quelle ressource informatique, un site web peut disposer d'une **surveillance (monitoring)** et d'une **maintenance**, assurée par une équipe ou par un technicien dédié, l'objectif étant de réduire les indisponibilités, d'assurer la pérennité de l'outil et de fiabiliser la sécurité informatique.

AVANTAGES

- Suivi du bon fonctionnement du site web
- Réduction des risques d'indisponibilité
- Prévention de l'obsolescence
- Réduction des risques de sécurité informatique

ENJEUX

De **nombreux incidents** peuvent **impacter un site web**, qu'il s'agisse d'un problème de fonctionnement, d'une faille de sécurité, de l'obsolescence de l'un de ses composants ou de mises à jour à réaliser.

Un site web est très fréquemment créé avec **un logiciel de type Content Management System ou CMS** *(voir lexique)* et composé de **différents éléments,** comme des thèmes graphiques et des modules (*voir lexique*). Ces différents composants sont gérés indépendamment par **différents éditeurs** et ils disposent d'une **durée de vie**, de problématiques de **maintenances** et de **mises à jour,** tous différents les uns des autres.

Tout ceci fait du site Internet une ressource dont il faut prendre soin, et dont le **développement** et la **maintenance** doivent être **assurés en continu dans le temps**.

Lorsque des enjeux spécifiques de performance ou de rentabilité sont liés au site web, il est d'autant plus important de le **surveiller en permanence**, pour prévenir les incidents, améliorer le fonctionnement et accompagner l'évolutivité. Le **monitoring des performances** et du **fonctionnement** de votre site, ses **mises à jour** et sa **maintenance** doivent donc idéalement être assurés par une personne disposant des compétences requises, qu'il s'agisse de votre équipe informatique ou d'un **prestataire spécialisé**.

Ceci est indispensable pour **garantir la sécurité du site** sur le long terme et vous assurer de la pérennité de votre outil.

Action n°50 : Mettre à jour son site web en continu

PRINCIPE

De nos jours, les sites web sont très fréquemment construits avec un **socle technique appelé CMS** *(voir lexique)*, composé d'un logiciel et de différentes sous-couches techniques et graphiques de type thèmes graphiques* et modules* *(voir lexique...)*. Pour des raisons de fonctionnement et de sécurité, c'est l'ensemble de ce socle technique qui doit être maintenu avec la réalisation de mises à jour logicielles régulières.

ENJEUX

Contrairement aux apparences, un site Internet de dernière génération, réalisé avec un CMS (comme Wordpress, Prestashop, Drupal...), requiert un nombre important et fréquent de **mises à jour**. En effet, chaque élément du site peut être soumis à des **évolutions techniques** ou à des **mises à jour de sécurité** à tout moment, qu'il s'agisse du coeur du CMS, de son thème graphique ou de ses divers plugins. Il est recommandé de **réaliser ces mises à jour fréquemment** afin de diminuer les risques de piratages, mais aussi les risques d'obsolescence et les problèmes de fonctionnement.

Sur le plan technique, une mise à jour peut parfois causer des problèmes d'affichage ou de fonctionnement plus ou moins importants et pouvant aller jusqu'à l'indisponibilité du site en question.

Selon les enjeux de l'entreprise (enjeux économiques, poursuite de l'activité, image de marque etc), il est recommandé de déterminer une **stratégie de mises à jour** adaptée de façon à réduire les éventuels impacts de la réalisation de ces mises à jour, ce qui peut signifier par exemple de confier la réalisation de ces mises à jour à un professionnel.

De plus, le serveur du site web lui-même repose sur des éléments techniques de type PHP ou MysQL par exemple *(voir lexique)* et qui doivent également être mis à jour.

AVANTAGES

- Maintien du site en conditions opérationnelles de bon fonctionnement
- Réduction des risques d'indisponibilité
- Réduction de l'obsolescence
- Réduction des risques de sécurité informatique

Action n°51 : Activer le protocole HTTPS pour son site web

PRINCIPE

Le **protocole HTTPS** est un **protocole informatique** permettant de **sécuriser les échanges de données** entre des internautes qui visitent un site et le site web qui utilise ce protocole.

ENJEUX

Le **protocole HTTPS** fait partie d'une **stratégie de sécurisation** de son site Internet, mais aussi, d'une **standardisation de son site** par rapport aux **dernières normes technologiques** et de **référencement** des sites web.

En effet, lorsqu'un visiteur consulte un site Internet, **une interaction se crée** entre le serveur qui héberge le site en question et l'ordinateur du visiteur et des données sont échangées. Il peut s'agir d'échange de données comme un **nom d'utilisateur**, un **email**, un **numéro de téléphone**, ou encore, un **mot de passe** ou un **numéro de carte bancaire**.

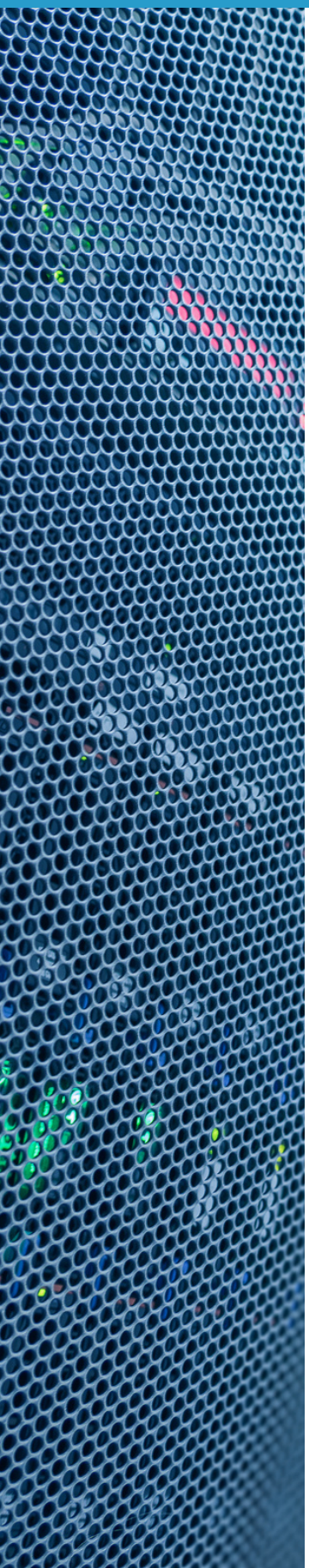
Le **protocole HTTPS** garantit la **confidentialité des données échangées** entre le visiteur et le serveur du site web. Élevé au rang de **règle par le moteur de recherche Google**, notamment dans le cadre de son algorithme de référencement naturel, le protocole HTTPS **améliore la sécurité du site Internet**, mais aussi, aide dans une certaine mesure à une **meilleure capacité de positionnement** dans les **premiers résultats des moteurs de recherche**.

Enfin, le protocole HTTPS étant une bonne pratique de sécurité informatique, **il est rassurant pour les visiteurs** de naviguer sur un site dont l'adresse commence par les fameuses lettres "https".

AVANTAGES

- Amélioration de la sécurité informatique du site
- Respect des critères de sécurité édictés par les moteurs de recherche
- Amélioration de la confiance des visiteurs dans la sécurité du site

Action n°52 : Héberger son site web sur un serveur dédié



PRINCIPE

Un site Internet est une instance logicielle qui doit être hébergée à l'intérieur d'une machine physique, un serveur. Généralement, cet **hébergement** est réalisé **de façon distante** auprès d'une entreprise spécialisée, **dans un centre d'hébergement de données**. Parmi les **offres courantes des hébergeurs**, il est possible de souscrire à un **hébergement mutualisé** : le site Internet sera hébergé sur une machine utilisée également pour d'autres clients, ou de souscrire à un **hébergement dédié**, permettant de disposer d'une machine entière uniquement réservée à son site web.

ENJEUX

Le choix entre un **hébergement dédié** et un **hébergement mutualisé** repose sur la **qualité de service attendue**.

En effet, lorsque plusieurs sites internet sont hébergés sur une même machine physique, d'une part, **les ressources sont divisées** entre ces différents sites, et d'autre part, **la frontière** qui sépare ces sites **en cas de piratage est plus réduite**.
Au contraire, un site internet **hébergé sur une seule machine** bénéficie de toutes les capacités et performances de cette machine, et voit ses risques de sécurité réduits, de par son isolement.

L'hébergement mutualisé présente ainsi l'avantage de **coûts réduits**, et dans une certaine mesure, de facilités d'administrations. Les ressources informatiques disponibles sont généralement **limitées et dépendantes** des autres sites hébergés sur la même machine. **L'hébergement dédié** présente quant à lui généralement **de meilleures performances** et **capacités technologiques**, ainsi qu'une **sécurité** et **des garanties accrues**.

De ce fait, on réservera l'hébergement mutualisé pour des sites internet ne disposant pas d'exigences spécifiques sur le plan des performances ou de la sécurité, et on recommandera **l'hébergement sur un serveur dédié** pour les sites web ayant **des enjeux financiers**, **professionnels** ou de **performance**.

AVANTAGES

- Capacité de sur-mesure
- Maximisation des capacités de performance
- Réduction des risques informatiques
- Administration du serveur d'hébergement plus poussée

Pour aller plus loin

LEXIQUE

***Phishing :** Tentative d'usurper une identité pour récupérer des informations personnelles à des fins malintentionnées malveillantes. Exemple : Mail de votre président demandant un virement discret de trésorerie, relance sur un non-paiement ou sur une date de garantie qui arrive à échéance, menace de fermeture d'un compte, message d'un ami en détresse, suivi de colis, renouvellement d'identifiants de fournisseur Internet etc...

***CMS :** CMS en anglais content management system - système de gestion de contenu est un logiciel qui permet de concevoir, gérer et mettre à jour des sites Web ou des applications mobiles de manière dynamique.
Ce type de logiciel est généralement constitué de différentes sous-couches graphiques (thème graphique) et/ou techniques et fonctionnelles (plugins ou modules) permettant, par l'ajout de ces éléments additionnels, d'aller au-delà des possibilités initiales du logiciel en question.

***Module (pour un CMS) :** Dans le cadre précis des CMS, un module ou plugin est un programme qui vient s'ajouter ou s'installer dans le CMS pour lui conférer des possibilités ou des fonctionnalités supplémentaires. Par exemple : module avancé de formulaire de contact, module antispam, module de sauvegarde etc.

***Thème :** Dans le cadre des CMS, un thème est un programme que l'on ajoute ou installe dans le CMS pour personnaliser l'affichage graphique de tout ou partie de ces éléments (pages, menus, boutons), mais aussi, dans une certaine mesure, personnaliser ou ajouter des fonctionnalités supplémentaires.

***PHP / MysQL :** PHP est un langage de programmation et MySQL est un système de gestion de base de données relationnelle. De nombreux CMS Open Source sont basés sur ce couple de technologies, comme les CMS WordPress, Joomla ou Drupal par exemple.

***DDos** : Une attaque DDoS (Distributed Denial of Service attack) est une attaque ayant pour but de rendre un service indisponible. L'attaque par déni de service peut bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web, empêcher la distribution de courriel dans une entreprise, ainsi que d'autres impacts informatiques.

RESSOURCES

SÉCURISER UN SITE WEB

Guide de sécurisation de site web édité par l'ANSSI. *"Les sites web sont par nature des éléments très exposés du système d'information. Leur sécurisation revêt une grande importance, et ce, à plusieurs titres. Les sujets abordés se concentrent autour des standards du Web, dont les implémentations côté navigateur requièrent des paramètres à spécifier lors du développement et de l'intégration d'un site ou d'une application web, de façon à en garantir la sécurité..."*
https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-des-sites-web/

À propos de Déessi

QUI SOMMES-NOUS

Créé en 1999, nous couvrons depuis 2004 l'ensemble des problématiques IT des PME et nous nous positionnons comme une véritable **DSI externalisée**. En nous appuyant sur l'expertise pointue de nos pôles de compétences (Help Desk, AMOA & Sécurité, Hébergement, Développement…), nous avons à cœur d'améliorer en continu la **qualité de service** et la **sécurité** des **systèmes d'information** de nos clients.

Avec **23** années d'expérience, **8M€** de chiffres d'affaires et plus de **60 collaborateurs en 2023**, notre société, agile et performante, infogère plus de 1500 serveurs et offre une disponibilité de ses infrastructures jusqu'à 99,95% en mode PCA.

Nous œuvrons pour des systèmes d'information **plus fiables** et **plus performants** en nous appuyant sur notre maîtrise des métiers de l'infogérance.

Nous sommes l'équipe informatique des TPE, des PME et petites collectivités locales. En mutualisant les investissements et les expertises techniques, nous proposons toutes les prestations d'une DSI, depuis le conseil stratégique jusqu'à la gestion quotidienne du système d'information.

Nos prestations :

- Audits (de sécurité, de performance, d'organisation etc.)
- Support aux utilisateurs,
- Maintien en Conditions Opérationnelles de vos outils : mise à jour des postes de travail, des serveurs, des différents équipements réseaux…
- Gestion au quotidien des serveurs, des sauvegardes, des antivirus,
- Hébergement « dédié » et complet (intégrant sauvegardes, sécurité, supervision …), avec des engagements de disponibilité.

Nous gérons tout ce qui vous permet de disposer d'un outil informatique efficace et évolutif. Vos besoins deviennent nos engagements

A propos de Déessi

LIGNE EDITORIALE

Engagée dans le développement et la compétitivité des PME, **Déessi** produit **des ressources** en continu afin d'apporter aux dirigeants et responsables IT des clés de décision sur la gestion, la sécurité et la pérennité de leur système d'information.

Nous communiquons à travers **de nombreux supports** : notre site internet, nos livres blancs, les réseaux sociaux, d'autres médias où nous sommes invités (blogs, publi rédactionnel...). Nous **couvrons l'actualité** et produisons régulièrement des **articles de fonds** et des **analyses.**

La ligne éditoriale de Déessi en 6 points :

- **Justesse des informations,** pour délivrer à nos lecteurs et abonnés les informations les plus exactes et les plus utiles possibles, au plus proche des tendances du secteur et de l'actualité.
- **Centré sur les usages,** avec un processus de production de contenus orienté utilisateurs, qui tient compte de leurs besoins, leurs centres d'intérêts et leurs interrogations.
- **Un style pédagogique : Déessi** donne la priorité à une rédaction claire, accessible et compréhensible, tout en utilisant à bon escient les concepts clés des thématiques abordées et en les vulgarisant le cas échéant.
- **Une démarche positive :** Les contenus de **Déessi** s'inscrivent dans une démarche positive de conseils et d'apports de solution, sans dramatiser.
- **Une valeur ajoutée :** Chaque contenu est rédigé dans un objectif de pertinence et de délivrer une véritable valeur ajoutée au lecteur, qu'il s'agisse d'expliquer un concept, de décrypter une tendance ou de partager une expertise.
- **Sans parti pris : Déessi** communique de façon factuelle, sans dénigrer les autres acteurs du marché.

NOS AUTEURS

Nos contenus sont systématiquement revus et validés par notre comité éditorial. De plus, pour les sujets les plus techniques et pointus, nous mettons à contribution tout ou partie des membres de notre comité de relecture, de façon à vous apporter une information juste, fiable et d'actualité.

COMITE EDITORIAL

Jean-Yves Zaoui, dirigeant de Déessi
Jérôme Chapeau, directeur de la communication
Marine Benhamou, chargée du marketing et du service client
Nathalie Gonzalves, chargée de communication digitale

COMITE DE RELECTURE

Maxime ARNAUDET
Ayyoub BACHI
David BÉNARD
Pierre GELGON
Edwin LECLERC
Eric MACHAULT
Gilbert NG KON TIA

CONTACTEZ-NOUS

Nous vous remercions pour votre attention et vous invitons à poursuivre la lecture sur notre site internet et sur nos réseaux sociaux.

Une remarque ? Une question ?

Rendez-vous sur https://www.deessi.si/ pour nous contacter.

Coordonnées

2, rue Mozart
92110 Clichy
Standard : +33 1 40 07 13 33
https://www.deessi.si/