berry buro

DOSSIER SPECIAL

TOUS CONCERNÉS

Sommaire

Les équipes commerciales et techniques se tiennent à votre disposition pour répondre à vos questions et vous accompagner dans la mise en place de stratégie efficientes de protection de vos systèmes informatiques et de vos données.

Bonne lecture

Contexte

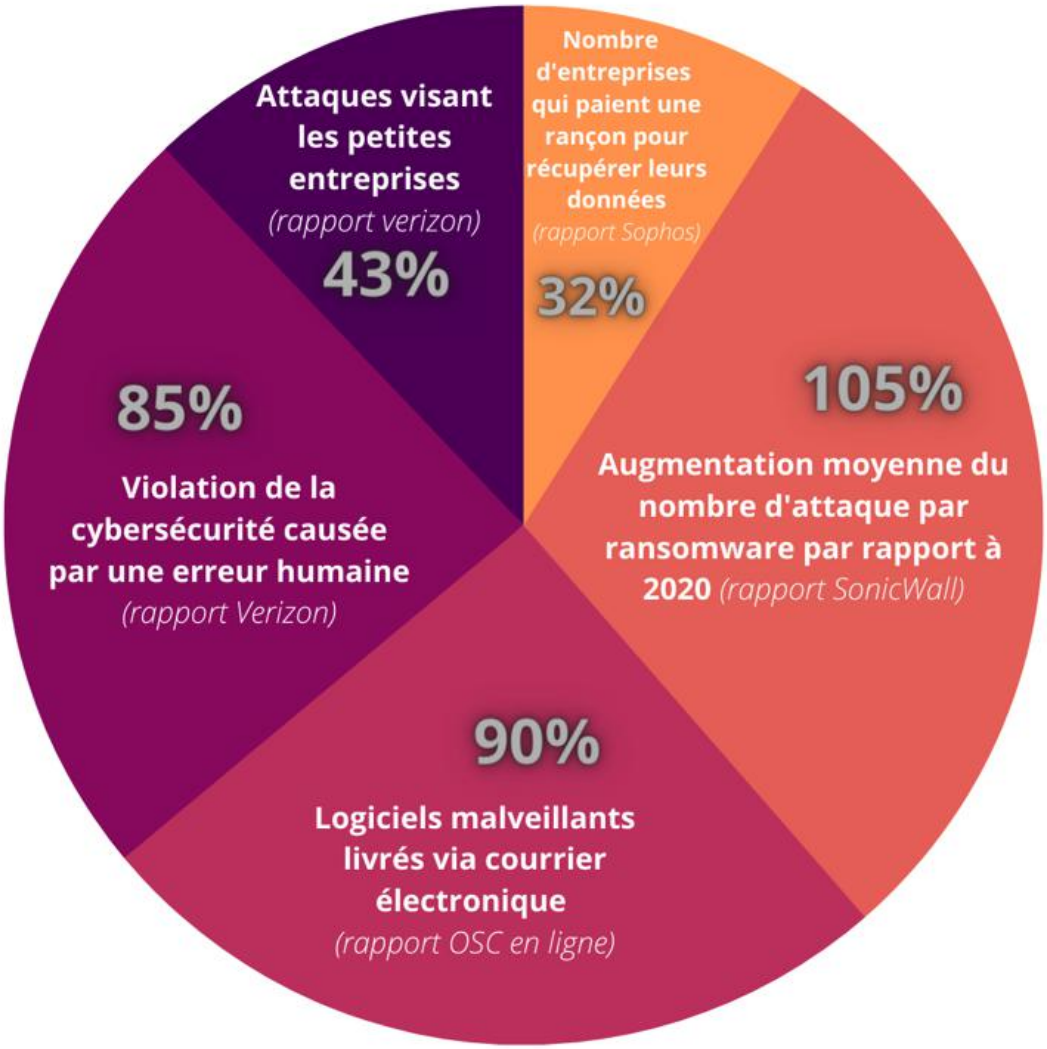
A partir du moment où une entreprise, une association ou une administration utilise un système d'information, elle est sous la menace de la **cybercriminalité** qui malheureusement augmente et se perfectionne d'année en année en ne faisant plus de distinctions entre TPE, PME ou grand groupe.

Nous faisons en effet face ces dernières années à une recrudescence de ces **cyberattaques**, à la fois au niveau mondial, national mais également au niveau régional. Les grands groupes ne sont plus les seules **victimes** comme vous pourrez le constater dans la suite de ce dossier spécial cybersécurité.

En tant qu'acteur local et régional engagé dans l'accompagnement des entreprises, associations et administrations publiques, il est de notre responsabilité de communiquer et vous donner le plus de visibilité possible sur ces menaces afin que vous puissiez agir et prendre les bonnes décisions.

Chiffres et statistiques : Comprendre la situation actuelle

Afin de pouvoir bien appréhender la situation actuelle et la menace que représente la **cybercriminalité**, il est pertinent d'isoler certains **chiffres** et certaines statistiques clés décrivant la situation actuelle.



Le Saviez-Vous ?

Aujourd'hui, les avions de chasse nouvelle génération sont plus menacés par les cyberattaques que par les missiles ennemis.

A la lecture de ces différentes statistiques, on comprend qu'il y a une **accélération** de la **cybercriminalité** depuis plusieurs années.

La crise sanitaire, en partie avec le déploiement rapide du télétravail sans stratégie de protection, a accélérée ce phénomène. Il faut également avoir à l'esprit que la cybercriminalité est malheureusement lucrative. Elle est jusqu'à **5 fois** plus rentable que les autres formes de criminalité et escroquerie.

Si les grands groupes étaient, il est vrai, les premières cibles des cyberattaques, la tendance s'inverse clairement et il raisonnablement envisageable que ce soient désormais les TPE et les PME qui soient majoritairement visées.

Pourquoi ?

Si les grandes sociétés ont mis du temps, elles ont dans l'ensemble plutôt bien réagi à ces menaces en consentant des **investissements nécessaires** pour limiter leurs failles de sécurité et se **protéger** contre ces menaces.

A l'inverse, les TPE/PME sont moins sensibilisées à ces risques et considèrent majoritairement que la protection de leur système informatique est un enjeu moindre… à tort.

Le coût d'une attaque *(création du virus, temps nécessaire, surveillance, …)* est relativement faible et les hackers ont la possibilité de démultiplier la portée de leurs attaques auprès d'un grand nombre d'entreprises en même temps ce qui rend tout à fait intéressant et potentiellement rentable l'attaque de TPE / PME.

A date, la question n'est plus vraiment de savoir si vous allez être ciblé par une cyberattaque mais plutôt quand.

Les principales menaces : Quelles sont-elles ?

Les pirates font preuve d'une créativité sans fin pour atteindre leur but. A défaut de pouvoir dresser une liste exhaustive des techniques mises en place, voici les principales menaces auxquelles vous pourriez être confrontés :

Phishing / Hameçonnage

Technique consistant à envoyer des mails frauduleux qui ressemblent à des mails provenant de sources fiables. L'objectif est de soutirer des données personnelles telles que des mots de passe, numéros de carte bancaire, carte d'identité...
C'est l'attaque la plus courante.

Ransomwares / Rançongiciel

Logiciel malveillant qui prend en otage des données personnelles ou professionnelles. Pour ce faire, un rançongiciel chiffre ces données puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.
Le paiement ne garantit pas que les fichiers seront récupérés ou le système restauré.

Malware / Malveillant

Programme développé dans le but de nuire un système informatique, de nos jours, appelé virus, en infectant les fichiers à l'aide d'un code malveillant.

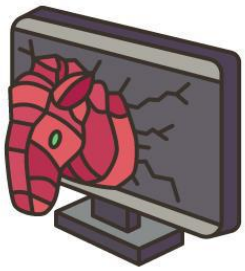
Usurpation d'identité

L'une des principales motivations des personnes qui collectent frauduleusement vos données personnelles est de les utiliser afin de se faire passer pour vous et pouvoir soutirer par la suite différents éléments *(document, numéro de compte, argent, ...)* auprès d'autres personnes.

Ingénierie sociale

Technique que les hackers utilisent pour vous manipuler et ainsi obtenir vos informations personnelles et/ou à vous solliciter un paiement.
Elle peut être combinée avec l'une des menaces répertoriées ici pour vous rendre plus susceptible de cliquer sur des liens, de télécharger des malwares ou de faire confiance à une source malveillante.

Cheval de Troie



Type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Son but est de faire entrer cette fonctionnalité malveillante sur l'ordinateur et de l'installer à l'insu de l'utilisateur.

Cryptojacking

Le domaine des cryptomonnaies est assez récent. C'est l'acte de détourner un ordinateur pour extraire des crypto-monnaies contre la volonté des utilisateurs, via des sites Web ou des virus informatiques.

Rootkit

Le rootkit désigne un ensemble de logiciels destinés à prendre le contrôle de votre ordinateur, tout en restant le plus discret possible. Cette discrétion les rend extrêmement difficiles à identifier, d'autant que leurs opérations sont souvent invisibles pour l'utilisateur.

Spywares

Un spyware, ou logiciel-espion, est un logiciel indésirable qui enregistre votre activité sur votre ordinateur, dans le but de collecter vos informations personnelles et vos habitudes de navigation, à l'abri des regards et surtout du vôtre.

S'il ne fallait en retenir qu'une ???

Le ransomware, probablement.

C'est en ce moment la menace qui se développe le plus dans la cybercriminalité et qui peut entraîner des conséquences très graves pour une entreprise, association ou administration.

Quelques exemples contemporains de victimes de cyberattaque :

L'actualité récente est malheureusement riche d'exemples de sociétés qui ont été victimes de cyberattaques.

Au niveau mondial :

- *COLONIAL PIPELINE, USA – Mai 2021 :*
  La société américaine, transportant des hydrocarbures, est victime d'une attaque au ransomware. 100 giga-octets de données ont été dérobés et cryptés par les pirates qui menacent de rendre publique ces informations. Durant l'arrêt des activités, aéroports et stations-services n'ont plus été approvisionnés en carburant.
  La société a finalement payé la rançon.

- *AXA PARTNERS, ASIE – Mai 2021 :*
  La société est victime d'une attaque de type ransomware sur son marché asiatique avec la perte de données sensibles de type passeport et carte d'identité.
  La société aurait finalement payé la rançon.

Au niveau national :

- *LISE CHARMEL, LYON – Novembre 2019 :*
  1150 salariés du groupe sont touchés.
  En février 2020, la société est placée en redressement judiciaire.

- *MMA, PARIS – Juillet 2020 :*
  La société est victime d'une cyberattaque. Les services de gestion et le site WEB sont paralysés pendant plusieurs jours. Malgré tout, le pire a été évité et MMA a annoncé ne pas avoir payé de rançon.

Au niveau régional :

- *CONSEIL DEPARTEMENTAL DE LA VIENNE, 21 janvier 2021 :*
  Le Conseil Départemental est victime d'une cyberattaque. Il aura fallu plusieurs semaines avant de pouvoir retrouver l'ensemble des moyens informatiques et téléphonique. Le département a estimé les conséquences financières à au moins 400 000 €.

- *POLE SANTE LEONARD DE VINCI, CHAMBRAY LES TOURS, 10 janvier 2022 :*
  Le pôle de santé est victime d'une attaque par ransomware avec une rançon estimée à plusieurs centaines de milliers d'euros. Une centaine d'opérations ont été déprogrammées quotidiennement avant que le fonctionnement puisse reprendre correctement.

- *FAIENCERIE DE GIEN, GIEN, 17 février 2022 :*
  La Faïencerie de GIEN est victime d'une attaque au ransomware. Une demande de rançon a été émise pour que l'entreprise récupère ses données. L'entreprise tourne au ralenti et ne peut plus traiter les commandes.

- *MAIRIE DE SAUMUR, 23 mars 2022 :*
  La mairie est victime d'une cyberattaque. Les services de la ville se retrouvent perturbés mais le pire semble évité.

Ces informations sont publiques et disponibles dans la presse régionale ou nationale. Elles traduisent bien la **recrudescence d'attaques et la grande diversité des cibles touchées.**
Les conséquences sont plus ou moins grave à la fois au regard de l'ampleur de l'attaque et au regard du niveau de protection mis en place.

L'idée n'est bien entendu pas de céder à la panique mais il faut désormais appréhender que la cybercriminalité soit une réalité et un danger pour les professionnels mais également les particuliers. Libre à chacun ensuite de se positionner sur ce sujet au regard des enjeux économiques de sa propre structure.

Quels sont les risques et les enjeux ?

Face à ces attaques, les risques sont **multiples** et les enjeux sont souvent proportionnels à l'usage et la dépendance que vous avez vis-à-vis de votre système d'information.

Cela peut aller de **la perte financière** directe si des informations de paiement ont été compromises en passant par **la perte de données** confidentielles et cruciales à votre activité jusqu'à **l'arrêt et la paralysie** complète de votre organisation en cas d'attaque d'envergure avec des **difficultés** à redémarrer votre activité.

Il y a donc de forts enjeux financiers bien sûr, mais également des enjeux en termes d'image et de réputation.

Idées reçues : On fait le tour, on fait le tri.

1) « Un anti-virus et un pare-feu protègent contre toutes les cyberattaques »

⇨ **FAUX – En partie**

Un des premiers réflexes pour se protéger est souvent de prendre un antivirus voire un pare-feu. S'il est indispensable, l'antivirus est loin d'être suffisant pour contrer une cyberattaque.

En effet, une étude menée par la CPME révèle que 90% des petites entreprises touchées par une cyberattaque se pensaient protégées par un antivirus. En effet, les hackers développent des virus et techniques capables de contourner les défenses techniques que vous aurez mise en place.

Gardez à l'esprit que 80% des intrusions font suite à une erreur humaine !

2) « Nous avons déjà une sauvegarde, nous sommes immunisés »

⇨ FAUX – En partie

Avoir une stratégie de sauvegarde de ses données est indispensable ; encore faut-il que cette stratégie soit complète.

Avoir une seule sauvegarde ne permet pas de se protéger totalement contre les cyberattaques. Si cette dernière est connectée au réseau, elle peut être chiffrée lors d'une attaque.

Alors quelle stratégie appliquer ? On vous explique tout dans les pages suivantes.

3) « Payer la rançon permettra de récupérer ses données »

⇨ FAUX

Selon une enquête SOPHOS 2019, une entreprise qui paie une rançon récupère en moyenne 2/3 de ses données. Payer la rançon, même si ça semble l'option la plus simple (et peut être la plus couteuse) n'est que rarement une bonne idée.

D'autant plus qu'il faudra par la suite reconstruire votre système informatique précédemment infecté.

4) « Nos collaborateurs sont au courant des techniques de cyberattaques, nous sommes en sécurité »

⇨ FAUX – En partie

En êtes-vous certains ?

Les techniques de phishing et d'ingénierie sociale sont de plus en plus élaborées. Précédemment, elles étaient facilement reconnaissables *(fautes d'orthographes grossières, erreurs de syntaxe, …),* les messages sont de plus en plus élaborés manuellement et avec beaucoup de soin rendant leurs identifications plus difficiles.

Les principales failles de sécurité :

De manière synthétique, il est possible d'identifier quatre grands domaines générateurs de failles de sécurité :

1) Les défauts de mise à jour
   - ⇨ Un défaut de mise à jour, ce sont des potentielles failles de sécurité identifiées qui ne sont pas comblées par l'apport du correctif de la mise à jour.

2) Les mots de passe dits faibles
   - ⇨ Eviter les mots de passe trop simple du type « prenom1234 » qui sont simples à découvrir pour les hackers.

3) Les erreurs humaines (phishing, …)
   - ⇨ Cliquer sur un email malveillant peut permettre au pirate de rentrer dans vos systèmes informatiques.

4) Les mauvaises pratiques (fichier Excel avec tous les mots de passe, connexion à un wifi public en tapant ses mots de passe, …)
   - ⇨ Le travail du pirate se voit facilité par ce type de pratiques.

Identifier les principales failles de sécurité, c'est bien. Les traiter, c'est mieux.

L'approche et les conseils de BERRY BURO

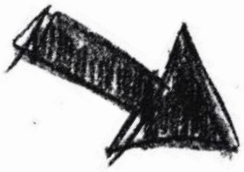
BERRY BURO est référencé professionnel cyber malveillance. Nous vous accompagnons dans la mise en place de stratégie de protection et de sécurisation de votre écosystème informatique et de vos données. Nous suivons avec attention l'évolution du marché et des solutions de protections proposées par nos partenaires.

PROFESSIONNEL RÉFÉRENCÉ

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

En matière de cybersécurité, soyons malgré tout humbles et lucides : il n'existe pas une solution miracle permettant une protection absolue. En revanche, la combinaison de plusieurs bonnes pratiques et la mise en place de solutions performantes permet de grandement minimiser les risques de faille en cas de cyberattaque tout en décourageant les hackers … et vous permettre surtout d'être plus serein chaque jour dans vos activités.

Nous avons donc défini sept piliers en matière de sécurité informatique afin de proposer une stratégie la plus complète possible.



1) Sensibilisation et formation des utilisateurs

Il s'agit là du tout premier rempart aux cyberattaques. L'utilisateur est en effet en première ligne derrière son ordinateur ou smartphone face aux risques de cyberattaque.

Rappelons que 80% des intrusions proviennent d'une erreur ou d'un manque de vigilance humain. L'utilisateur est souvent vu, parfois à juste titre, comme le maillon faible dans les organisations mais il peut devenir à contrario une majeure partie de la solution. Pour cela, il faut mener des actions de sensibilisation et de communiquer autour des risques engendrés par la cybercriminalité pour impliquer les utilisateurs dans cette démarche.

Nous tenons à votre disposition une fiche regroupant les « 10 mesures essentielles pour la sécurité numérique » à destination des utilisateurs.

Nous avons également la capacité de vous accompagner sur la prévention et la formation de vos utilisateurs de manière via la mise en place d'actions et dispositifs récurrents.

Vous avez un doute sur un email ou une question ? Nous sommes à votre disposition pour y répondre.

La sécurité des mots de passe est une clé, sans mauvais jeu de mot, dans la stratégie globale de sécurité d'un système informatique.

Il faut bannir les fichiers Excel rassemblant ses différents mots de passe ou pire encore les mots de passe de ses collaborateurs ou du service.

Il faut également créer des mots de passe fort, difficile à deviner pour les hackers. Des gestionnaires/créateurs de mots de passe existent afin de créer des mots de passe complexe pour vos différents accès.

Il convient également d'aller vers la double ou la multi authentification.

Concrètement, cela consiste lors d'une connexion à avoir deux sources distinctes d'identifiants, par exemple un courriel et un mot de passe puis un sms reçu avec un code d'authentification.

Vous souhaitez mettre en place **la double authentification** ? Contactez-nous !

Allô BERRY BURO ?

3) Contrôler les accès au système informatique

Il est important de maitriser et de savoir quelles sont les personnes qui peuvent avoir accès à votre système informatique.

Une politique de droit d'accès est dans ce sens importante à mettre en place pour définir les rôles au sein de votre structure.

Un compte et des accès administrateur est par nature réservé à … un administrateur et non pas à l'ensemble des collaborateurs.

Cela rentre d'ailleurs parfaitement dans la conformité à la RGPD.

Dans ce sens, il est également impératif d'avoir un inventaire précis de l'ensemble des appareils informatiques permettant d'être connectés au réseau *(pc, tablettes, smartphones, …).* Cela permet de réaliser une matrice utilisateurs / appareils et ainsi cartographier précisément votre structure.

Nous pouvons vous accompagner aussi bien sur votre conformité RGPD que sur la mise en place d'une politique de gestion des accès.

4) Mise en place d'un antivirus et d'un pare-feu

Un antivirus, déployé sur l'ensemble des postes et serveurs de votre organisation, est indispensable. Il va permettre de prévenir les menaces et protéger votre organisation contre les programmes malveillants.

Nous déployons régulièrement la solution Endpoint Protection de notre partenaire Symantec.

C'est une solution approuvée et particulièrement performante, mondialement reconnue. A contrario, historiquement, nous ne travaillons pas avec Kaspersky et, aux égards du contexte actuel, nous ne recommandons pas son utilisation.

Quant à lui, le pare-feu va permettre d'inspecter le flux de données circulant entre le réseau externe *(internet)* et votre réseau interne afin de filtrer ce trafic et de bloquer le trafic malveillant. Les pares-feux peuvent être logiciel ou matériel mais nous conseillons d'avoir les deux. La mise en place d'un pare-feu physique, de nos partenaires ALLIED ou SONICWALL, couplée une couche logicielle permet de créer des politiques de sécurité personnalisées en fonction de vos besoins.

Nous vous accompagnons, non seulement dans la définition des bons équipements *(logiciels et matériels)* et nous prenons en charge les paramétrages nécessaires à la sécurité souhaitée.

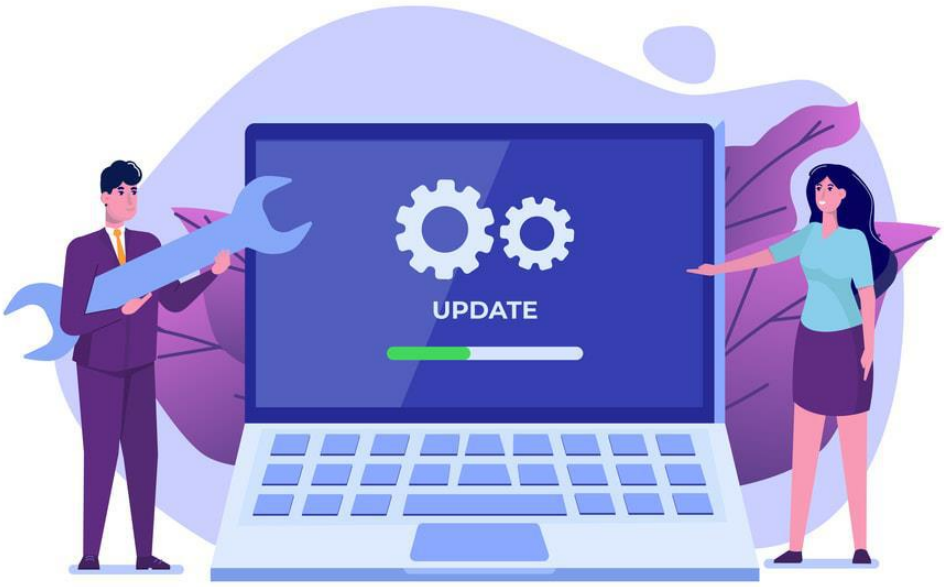
N'hésitez pas à nous contacter pour découvrir NOS OFFRES

5) Des mises à jour … à jour

Les mises à jour ne sont pas superflues. Très souvent, outre le fait d'apporter une évolution aux logiciels ou systèmes concernées, elles intègrent la mise en place de nouveaux protocoles de sécurité. Il est donc essentiel de procéder à ces mises à jour **régulièrement** pour permettre à son système de ne pas avoir de faille de sécurité connue. C'est d'autant plus dommage lorsqu'un correctif est disponible.

Certaines mises à jour sont en principe gratuites *(Windows, Microsoft, système, …),* d'autres peuvent être payantes dans le cadre d'abonnements annuels *(pare feu, …).*

Nous vous recommandons malgré tout de souscrire à ces abonnements annuels car ils permettent de maintenir à jour votre niveau de sécurité.



6) Sauvegarde

Soyons clair : la mise en place de sauvegardes est **STRATEGIQUE** au sein de votre entreprise, association ou administration.

Imaginez-vous seulement quelques instants perdre les fichiers sur lesquels vous travaillez tous les jours, perdre vos emails et vos contacts, votre base client, vos programmes, …

En matière de sauvegarde, le meilleur conseil est de tendre vers la stratégie 3-2-1.

- 3 sauvegardes distinctes

Une copie originale n'est que rarement suffisante. La règle est d'avoir trois sauvegardes ; dans ce cas la probabilité de défaillance est évaluée à 1/1000 000. Une de ces copies peut avoir une défaillance, il vous restera au moins un autre exemplaire de votre sauvegarde.

- 2 sauvegardes stockées sur différents supports

Avoir ses différentes sauvegardes stockées sur un unique support présente un risque : le support en question peut présenter une défaillance ; dans ce cas, l'ensemble des sauvegardes risquent d'être perdues. L'idée est donc de stocker les sauvegardes sur deux supports différents afin de se prémunir de ce risque : serveur de stockage, NAS, disque dur, cloud

- 1 sauvegarde conservée hors site

Conserver ses différentes sauvegardes au même endroit présente également un risque en cas d'incendie ou de dégât des eaux par exemple (même s'il existe des solutions de sauvegarde résistantes au feu). Dans l'incendie du datacenter d'OVH par exemple, les serveurs de sauvegarde étaient situés à coté des serveurs de production : l'incendie a donc détruit l'original et les copies.

Différentes solutions peuvent s'offrir alors : un stockage dans le cloud, un stock sur un NAS dans un site distinct, un stockage sur un disque externe.

Le 

L'importance d'avoir une sauvegarde hors réseau est également prioritaire car elle se retrouvera complètement séparée de votre système informatique en cas d'attaque. Malgré toutes les stratégies de défense, les hackers peuvent réussir à chiffrer une sauvegarde lorsqu'elle est connectée au réseau. Le stockage sur un disque externe, amovible, à l'avantage de pouvoir répondre au besoin d'une sauvegarde hors site & hors réseau.

En cumulant cela à une sauvegarde dans le cloud, vous bénéficiez d'une stratégie efficace. 

Contactez-nous et découvrez nos différentes solutions de sauvegarde !

7) PCA et PRA

Vous avez scrupuleusement mis en place les 6 points précédents ?

Il en reste malgré tout un dernier : la mise en place soit d'un plan de reprise d'activité (PRA) soit d'un plan de continuité d'activité (PCA).

En effet, même si vous bénéficiez de sauvegardes saines, une cyberattaque peut paralyser votre activité mais grâce à nos conseils, vous aller pouvoir reprendre votre activité sans perte de données et dans un délai raisonnable *(selon la configuration de votre infrastructure informatique).*

Vous rentrez donc dans un **plan de reprise d'activité** après sinistre ; sinistre qui peut d'ailleurs être un incendie, une coupure électrique prolongée, …

La clé du succès résidera dans la possibilité de redémarrer vos systèmes informatiques et d'y restaurer vos données et logiciels.
La mise en place d'un PRA permet de savoir précisément quoi faire en cas de sinistre et de minimiser le temps d'indisponibilité.

Nous définissons ensemble vos enjeux : quel temps d'arrêt est acceptable pour vous, quels sont les postes critiques à devoir redémarrer en priorité, … C'est le meilleur moyen d'être rassuré et connaitre la capacité de votre entreprise, association ou administration à relancer son activité, sa production. C'est un gage de sécurité permettant également d'identifier les différentes failles complémentaires et de s'améliorer continuellement.

Nous recommandons ainsi, une fois la mise en place de ce PRA, de le tester chaque année afin d'identifier les potentielles anomalies *(matériel vieillissant et moins performant, sauvegarde externe non réalisée, …).*

En parallèle, votre activité peut également vous conduire à ne pas pouvoir envisager une coupure de votre activité.

Dans ce cas, nous basculons dans un plan de continuité d'activité (PCA) et nous définissons ensemble l'activité minimum que vous devez pouvoir conserver en cas de sinistre.

A ce moment, la notion de sinistre dépasse même la thématique de la cybersécurité et nous évaluons les différents évènements possibles : panne de courant, panne matériel, incendie, …

Au regard de vos réponses, nous définissons ensemble l'architecture de votre système informatique en allant bien au-delà de la notion de sauvegarde mais en abordant par exemple des notions de réplication, de redémarrage instantané dans le cloud, …

Si vous être confronté à ces problématiques, n'hésitez pas à nous consultez et nous vous accompagnerons à la fois dans la définition de vos indicateurs clés, dans la définition de votre infrastructure informatique et bien entendu dans son installation et sa maintenance.

Contactez-nous

contact@berry-buro.fr
mgueguen@berry-buro.fr

www.berry-buro.fr

0254033232