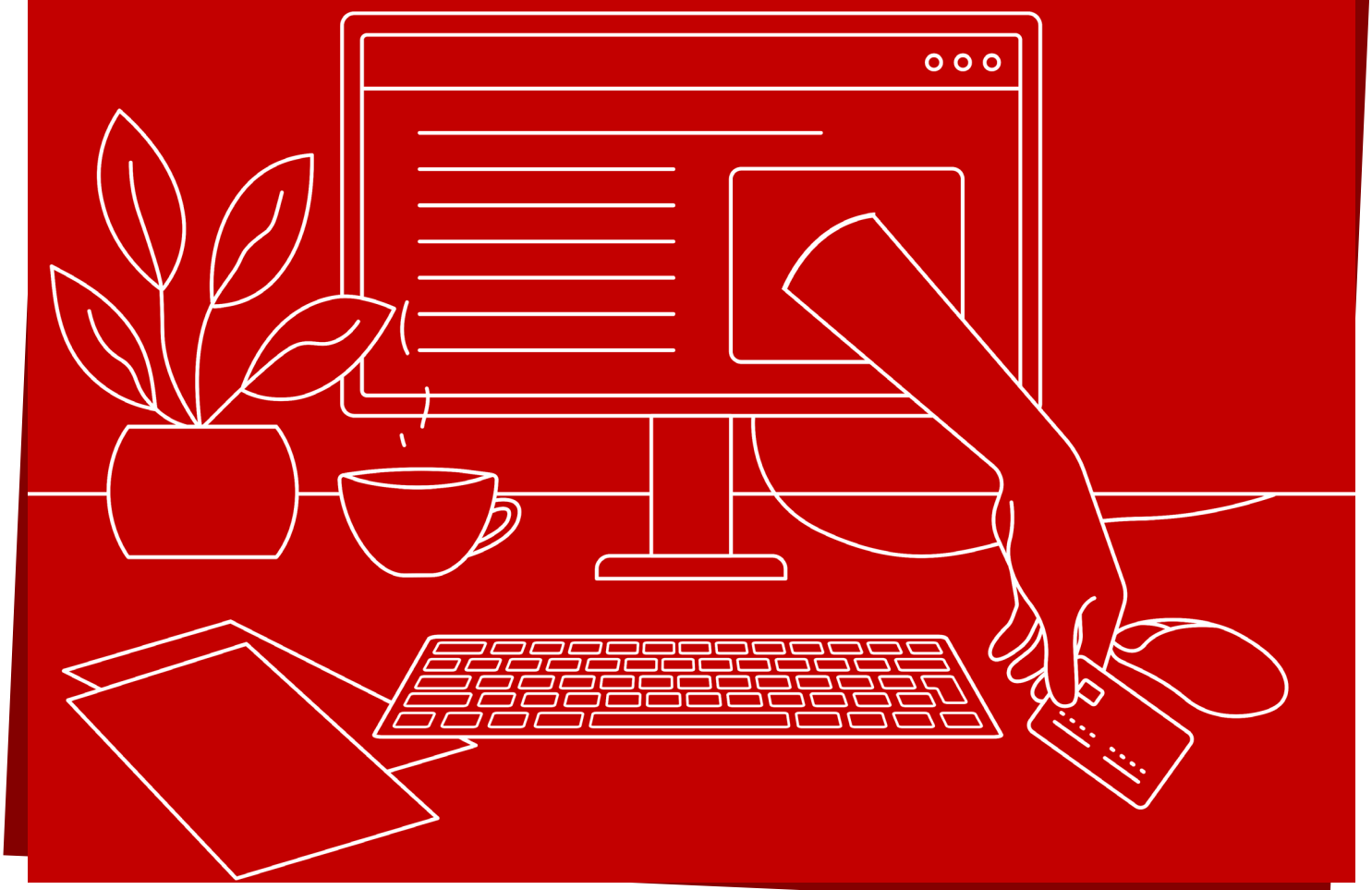
FIDSUD

EXPERTISE COMPTABLE | CONSEIL | AUDIT

N° 5

AVRIL. / JUIN. 2024

La cybersécurité : un enjeu pour votre entreprise ?



« ÉDITO »

Aujourd'hui, une majorité écrasante des entreprises est présente d'une manière ou d'une autre sur les **espaces numériques** et il devient impensable de pouvoir envisager le développement de son activité de façon totalement déconnectée.

Là où le progrès et les évolutions technologiques peuvent apporter **des opportunités** pour l'entreprise, ils sont également **une source de risques.** La **cybercriminalité** ne cesse en effet de se développer et les escrocs du numérique ont trouvé dans les entreprises de toutes tailles une cible de choix pour arriver à leurs fins.

Sachant que le coût moyen des conséquences d'une cyberattaque s'élève à près de **100 000 €** pour une entreprise, la cybersécurité doit être une préoccupation de premier ordre pour toutes les structures, quelle que soit leur taille ou leur activité.

Les menaces et enjeux de la cybersécurité

Les conséquences d'une cyberattaque peuvent s'avérer désastreuses pour toute entreprise touchée. Il est donc essentiel de savoir **identifier les signes et indices,** afin de reconnaitre les différents types d'attaques et ce qu'elles visent à obtenir.

En partant des attaques les plus fréquentes pour aller vers les plus rares, il est possible de citer :

L'hameçonnage

L'hameçonnage ou **phishing** : avec ce type d'escroquerie, les cybercriminels n'en ont pas qu'après l'argent de leurs cibles. Les **données** qu'ils peuvent obtenir ont également une très grande valeur pour eux. Ils peuvent soit les revendre au plus offrant, soit s'en servir eux-mêmes pour ensuite chercher un profit monétaire auprès de leurs cibles.

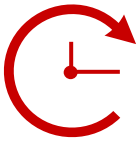
Très souvent, la tentative d'hameçonnage se fera à l'occasion d'une prise de contact, par **email ou SMS**, dans laquelle une personne se fait passer pour un interlocuteur de confiance afin de soutirer des informations critiques au destinataire.

Si des filtres techniques existent pour bloquer au maximum ces tentatives, ils ne sont pas efficaces à 100 %. La vigilance est alors le dernier rempart.

Certains indices permettent d'identifier les tentatives frauduleuses d'hameçonnage :

l'adresse email ne semble **pas cohérente** avec le sujet ou les fonctions prétendues de l'expéditeur

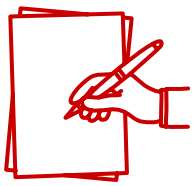
l'expéditeur se montre **pressant** dans sa demande



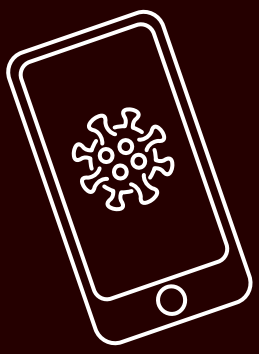
l'expéditeur n'est **pas préalablement connu**

le destinataire est invité à cliquer sur un lien renvoyant vers un **site non identifiable**

la syntaxe est de **mauvaise qualité**



le message n'est pas ou **peu personnalisé**



Les virus

Les infections par **virus** ou **malware** sont l'atteinte directe la plus commune. On entend par là, l'installation, à l'insu d'un utilisateur, d'un logiciel sur un ordinateur ou un téléphone. Les virus peuvent avoir des effets très variés et permettre de soutirer des informations professionnelles confidentielles, des données bancaires, des données personnelles ou alors, porter atteinte directement aux systèmes d'informations de l'entreprise pour les mettre hors de fonctionnement.

→ De **bons pare-feu et antivirus**, régulièrement mis à jour et, comme toujours, la vigilance des utilisateurs, sont les meilleurs moyens de réduire les risques.

La messagerie

Les **piratages de messageries** sont simples à mettre en place et extrêmement rémunérateurs pour les cybercriminels. En entrant dans la messagerie d'un dirigeant ou d'un salarié, un escroc peut causer énormément de dommages, notamment en demandant des transferts de fonds ou en interceptant la facture d'un prestataire pour y modifier les informations de paiement.

Les rançongiciels

Les **rançongiciels** ou **ransomware** sont des virus qui présentent la particularité de ne pas se cacher. Une fois l'ordinateur infecté, le ransomware va en limiter le fonctionnement en **chiffrant ses données** pour les rendre inexploitables. Il se fera alors connaitre de l'utilisateur pour demander le paiement d'une rançon en échange du rétablissement du système.

> Ces virus sont **particulièrement dangereux** lorsque l'on sait qu'ils entraînent un dépôt de bilan chez les 2/3 des PME qui sont touchées.

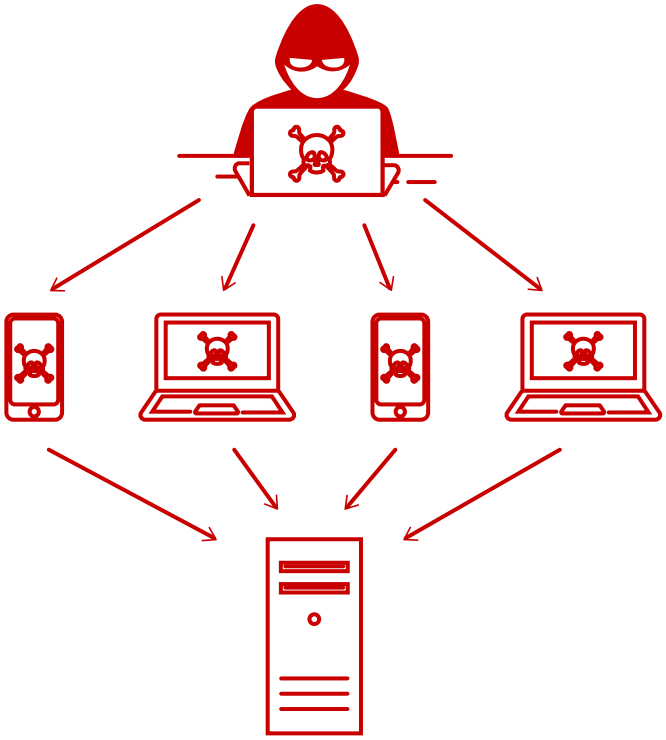
→ Pour s'en prémunir, la meilleure solution reste de **sauvegarder très régulièrement ses données** pour pouvoir rétablir son système à partir d'une version antérieure.

Le paiement de la rançon est globalement déconseillé. En effet, il n'existe aucune garantie que les cybercriminels tiendront parole et débloqueront les données une fois le paiement reçu.

Les attaques DDoS

L'attaque par **déni de service distribué (DDoS)** est une méthode qui vise à rendre un site, un service ou une application indisponible pour ses utilisateurs en surchargeant les capacités d'un serveur. L'attaquant va se servir de nombreux ordinateurs (souvent eux-mêmes infectés par un virus) pour lancer **un nombre de connexions très important et simultanées** vers la cible.

Une fois la limite des capacités des serveurs atteinte la cible « tombe » et les utilisateurs et clients potentiels n'y ont plus accès. Ce n'est pas le type d'attaque qui cause le plus de dommages, mais il est compliqué de s'en protéger.



Les pertes de matériels

Les **pertes de matériels** sont également une source non négligeable d'insécurité. Toutes les faiblesses de la cybersécurité ne sont pas numériques. La perte ou le vol d'un équipement appartenant à l'entreprise offrent aux cybercriminels une porte d'entrée de choix dans le réseau interne, ce qui leur permet d'accéder facilement à l'ensemble des données et fichiers auxquels l'appareil a accès.

Les exemples d'attaques cités ici sont les plus fréquents. Pour autant, cette liste n'est pas exhaustive. Il faut donc absolument rester en alerte et effectuer une veille permanente pour s'informer des méthodes « préférées » des cybercriminels.

Organiser sa protection technique

Savoir reconnaître les cyberattaques est une première étape, mais elle restera sans effet si l'entreprise ne se prépare pas pour se prémunir et répondre aux risques numériques.

Plusieurs précautions simples doivent donc être observées pour assurer une base solide à sa cybersécurité.

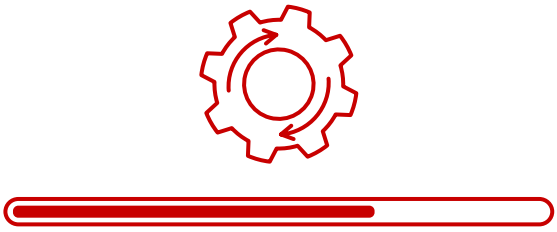
L'aspect le plus évident est **d'optimiser sa protection sur le plan technique.** La cybersécurité n'est pas qu'une question d'informatique, mais il est impossible d'envisager être en sécurité sans se concentrer sur cet aspect.

Les logiciels de sécurité

L'utilisation de logiciels dédiés à la sécurité des systèmes est donc primordiale.

Parmi eux, **l'antivirus** représente l'évidence. Il s'agit d'un logiciel qui va opérer une surveillance constante des fichiers de l'appareil sur lequel il est installé. À l'aide des connaissances accumulées au fil des années sur les différents malwares, l'antivirus vérifie le fonctionnement du système pour y détecter des signes potentiels d'une infection et limiter sa propagation.

Le **pare-feu** de son côté opère de façon assez similaire à l'antivirus, à la différence qu'il porte sa surveillance sur les flux de données transitant sur l'appareil par internet.



Les mises à jour

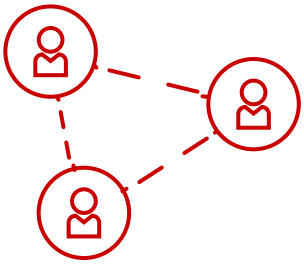
Pour l'ensemble des logiciels de sécurité, mais aussi pour toutes les applications et systèmes d'exploitation utilisés, il faut veiller à effectuer très régulièrement des **mises à jour.** Les éditeurs de ces produits améliorent sans cesse leurs logiciels en tenant compte des évolutions technologiques et des failles qui ont déjà pu être identifiées.

Ne pas effectuer les mises à jour revient donc à volontairement ne pas profiter de la version la plus sécurisée d'un logiciel tout en s'exposant à des cyberattaques profitant de faiblesses connues.

Les sauvegardes

En effectuant des **sauvegardes régulières** de l'ensemble des données du système, il est possible de se relever plus facilement en cas d'incident majeur portant atteinte au réseau ou en cas d'attaque par ransomware.

Les données ainsi sauvegardées doivent être stockées de façon sécurisée et de préférence à part du réseau principal.



La gestion des accès

Il n'est pas nécessaire que chaque salarié d'une entreprise puisse avoir accès à l'ensemble des données de l'entité. Il convient alors de mettre en place une **politique de contrôle des accès** se basant sur le métier et les responsabilités de chacun.

En cloisonnant ainsi les données, les risques que des informations ou données sensibles puissent fuiter se trouvent fortement limités.

Les bonnes pratiques à adopter

Si l'aspect technique sert de fondation à la cybersécurité, il faut comprendre que la faille préférée des cybercriminels est la **composante humaine.**

Plutôt que de multiplier les efforts pour faire tomber les barrières de systèmes, applications et logiciels imaginés par des professionnels, il apparaît plus simple pour une personne mal intentionnée de s'attaquer à la **faiblesse de l'utilisateur.**

Il est alors nécessaire d'éduquer et de former l'ensemble de ses effectifs, quel que soit leur métier, afin d'assurer une prise de **conscience globale** des risques et enjeux attachés à la cybersécurité.

D'autant que l'entreprise n'est pas la seule mise en danger par une cyberattaque. Celle-ci ayant à sa disposition des données personnelles relatives à ses salariés, ils peuvent également se trouver directement exposés en cas d'atteinte au système.

Plusieurs bonnes pratiques doivent donc être transmises pour rappeler que la cybersécurité est l'affaire de tous.

Le mot de passe

Le mot de passe joue le rôle de première barrière dans la sécurité d'un système. Il doit donc répondre à plusieurs exigences pour pouvoir assurer pleinement son rôle.

https://www.commentquonfaitunmotdepasse.com

Nom d'utilisateur :

Jean-Marc Boudalu

Mot de passe :

******

Force :

Il doit :

être unique pour chaque personne : les mots de passe partagés entre plusieurs personnes sont à proscrire

être original : il faut éviter les mots de passe communs (12345, azerty, 00000, password, etc.)

être composé de plusieurs types de caractère différents (lettres majuscules ET minuscules, caractères spéciaux, chiffres)

Il ne doit pas :

contenir d'informations personnelles relatives à l'utilisateur (date de naissance, lieu de naissance ou de résidence, nom des enfants ou d'un animal de compagnie, etc.)

contenir des phrases toutes faites : une fois les premiers mots identifiés la totalité du mot de passe est facilement complétée

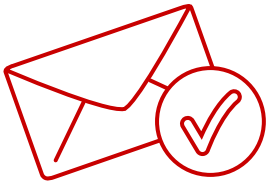
Des études existent permettant d'estimer la résistance d'un mot de passe face aux outils dont disposent les cybercriminels. Il est donc aisé de voir qu'en ajoutant un petit peu de complexité, un mot de passe gagne rapidement en efficacité !

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE EN 2023 ?

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
5	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
7	Immédiat	Immédiat	1 seconde	2 secondes	4 secondes
8	Immédiat	Immédiat	28 secondes	2 minutes	5 minutes
9	Immédiat	3 secondes	24 minutes	2 heures	6 heures
10	Immédiat	1 minute	21 heures	5 jours	2 semaines
11	Immédiat	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 années	3 000 années	15 000 ans
14	52 secondes	1 an	17 000 ans	202 000 ans	1 million d'années
15	9 minutes	27 ans	898 000 ans	12 millions d'années	77 millions d'années
16	1 heure	713 ans	46 millions d'années	779 millions d'années	5 milliards d'années
17	14 heures	18 000 ans	2 milliards d'années	48 milliards d'années	380 milliards d'années
18	6 jours	481 000 ans	126 milliards d'années	1 trillion d'années	26 trillions d'années

Source : Hive Systems

Il est à noter toutefois que dans les années à venir, le développement des ordinateurs quantiques viendra changer en profondeur ces estimations de durées. C'est pourquoi des **sécurités supplémentaires** doivent être imaginées et développées.



La double authentification

L'une des méthodes, de plus en plus populaire et présente, est celle de la **double authentification.**

Il ne s'agit pas ici de changer directement les modalités d'accès à un service ou un matériel par mot de passe. Mais plutôt de les **compléter.**

Une fois la double authentification mise en place, l'utilisateur se connectera comme à son habitude avec son mot de passe. Mais après cela, une **seconde étape d'authentification** sera déclenchée.

Il pourra par exemple recevoir un **SMS** ou un **email** l'invitant à **confirmer son identité** en cliquant sur un nouveau lien ou en renseignant un code à usage unique.

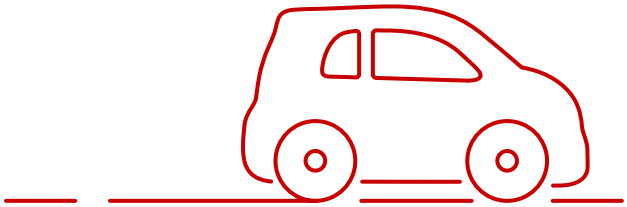
Les méthodes de double authentification sont nombreuses et apportent un renfort de sécurité non négligeable, même dans l'hypothèse où un mot de passe serait compromis.

La sensibilisation des effectifs

Tout comme le dirigeant avisé doit s'entraîner à reconnaitre les risques de cyberattaque, il faut que l'ensemble des effectifs soit sensibilisé.

Il est donc recommandé d'organiser des **formations** pour transmettre les bases à ses équipes et d'organiser des communications régulières afin d'effectuer des rappels et de communiquer sur l'actualité.

Il est également possible d'organiser des tests en conditions réelles en émettant, par exemple, des faux mails de phishing qui permettront de mesurer le niveau de vigilance des équipes.



Les déplacements professionnels

Les déplacements professionnels peuvent être une source importante d'insécurité. Plusieurs précautions simples sont recommandées pour éviter toute déconvenue.

Premièrement, un conseil qui vaut pour toutes situations, mais dont l'importance se trouve accrue lors des déplacements : **éviter les réseaux Wi-Fi publics !**

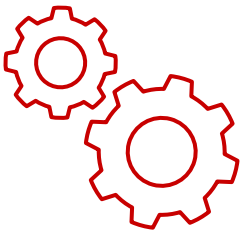
Il faut bien comprendre que s'il est facile et pratique de se connecter à ces réseaux, cela l'est tout autant pour un cybercriminel qui aura alors l'opportunité de partager un réseau non sécurisé avec de nombreux utilisateurs.

Il pourra alors avoir accès à **l'ensemble des données qui transitent par ce réseau,** qui servira de catalyseur pour l'ensemble des risques évoqués au préalable.

En parallèle, pour les déplacements plus importants, et tout particulièrement pour les déplacements à l'étranger, il est recommandé d'utiliser du matériel dédié spécialement à ces occasions.

En effet, emporter en déplacement un ordinateur ou un smartphone qui est utilisé quotidiennement, c'est emmener avec soi un nombre important de données sur la vie et l'activité de l'entreprise et qui sont, pour la plupart, sans objet avec le but poursuivi par ce déplacement.

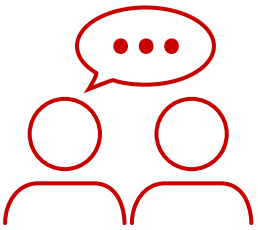
Ainsi, avoir du matériel dédié et contenant le minimum de données permet d'éviter trop de déconvenues en cas de perte ou de vol du matériel.



Mettre en place une stratégie de réponse

S'il est opportun de se préparer pour prévenir une attaque, il l'est tout autant de se préparer à réagir afin de ne pas se trouver démuni face à une situation de crise.

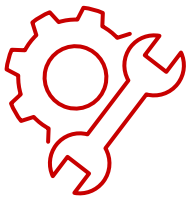
Il est, par exemple, préférable d'avoir des process définis pour :



faire remonter l'information d'une menace une fois celle-ci identifiée

circonscrire l'attaque et **endiguer la menace**

en référer aux autorités compétentes (comme la CNIL dans l'hypothèse d'une fuite de données personnelles)



mettre en place les **démarches de restauration des systèmes**

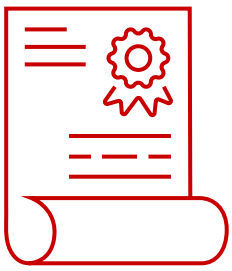
Les mots de passe les plus utilisés...

...et à éviter !

123456 - admin - 12345678 - 123456789 - 1234 - 12345 - password - 123 - abcdef - 0000
Aa123456 - 1234567890 - 1234567 - 123123 - 111111 - Password - 12345678910
000000 - admin123 - user123 - 1111 - P@ssw0rd - 654321 - azerty - Pass@123
toutou - 112233 - 102030 - abc123 - Aa@123456 - 1a2z3e4r - 123321 - azertyuiop
87654321 - 987654321 - 123123123 - 11223344 - 0987654321 - demo - 12341234
Azerty1 - azerty123 - Admin@123 - netflix - 1a2z3e4r5t - loulou - 11111111 - Demo@123
Admin - 666666 - 0123456789 - football1 - 121212 - 1234azer - admin@123
123456789a - Aa112233 - qsdfghjklm - Password1 - 888888 - admin1 - test - Aa123456@
qsd123 - User1 - marseille - azer1234 - fortnite - 123aze - 202020 - chouchou - qsdf1234
Abcd@1234 - user123456789 - 12344321 - aa123456 - 1122334455 - pokemon
Abcd1234 - guest - 88888888 - Admin123 - secret - 1122 - admin1234 - Password@123
a1z2e3r4 - [illegible] - Welcome - Abcd@123
Welcome@123 - minecraft - 101010 - Pass@1234 - [illegible] - 123456a - aze123 - code
zidane - [illegible] - a123456
1111111111 - motdepasse1 - 999999 - adminHW - 10203 - 12121212 - 12345678901
222222 - 7777777 - 12345678900 - [illegible] - azerty12345 - cheval - abc12345
1111111 - a123456789 - iloveyou - Passw0rd - 123123123 - hello - aaaaaa - Welcome1
password123 - 123456aA@ - 1234554321 - a1z2e3r4t5 - 1234512345 - 1a2z3e
a1b2c3d4 - admin123456 - Azerty123 - test123 - Password123 - 1234567899
Aa159753 - Test@123 - admin12345 - soleil - adminadmin - 1234abcd - azerty1234
123abc - 123456a@ - Aa102030 - Abc@1234 - 1a2b3c4d - 12345azerty - Bienvenue1
azerty123 - aaaaaaaa - a1234567 - azerty123456 - 55555 - lol12345 - Aa123456789
999999999 - test1234 - Motdepasse123 - Netflix1 - 147258369 - bonjour - 741852963
user - guest123 - ordinateur - 951951 - 753951 - Hello123 - mdp123456 - xxx123
bonjour123 - 12345678@ - jetaime - doudou123 - Demo123456 - meilleurmotdepasse
789654123 - 000000a - 122333 - AzErTy - foot123 - 123aze - 222222 - superman
qsdfgh - apple - myspace1 - 987654 - nbvcxw - xoxo - MoTdEpAsSe - Test123456
123azerty - AzErTy112233 - 10203040 - hell0 - @zerty1 - b0nj0ur - 4444Aa

Comment se faire accompagner ?

Les simples précautions, même avec la meilleure des volontés, peuvent s'avérer insuffisantes et il est alors essentiel de savoir s'entourer d'experts et de professionnels qualifiés pour construire sa cybersécurité.



Labels et certifications

Il faut donc savoir identifier les repères de confiance pour se tourner vers ceux dont les services ont prouvé leurs qualités.

→ **Expert Cyber :** créé en 2021, ce label permet d'identifier des professionnels dont les performances ont été testées concernant les problématiques de systèmes d'information professionnels, de téléphonie et de sites internet ;

→ **SecNumCloud :** ce label est décerné pour les solutions de cloud conformes à un référentiel édité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour assurer un niveau de sécurité maximal pour les données hébergées chez ces prestataires ;

→ **CSPN :** ce certificat, également délivré par l'ANSSI, permet d'identifier les services dont la sécurité a été éprouvé par des tests ;

→ **HDS :** ce certificat désigne les services de cloud adaptés au stockage de données de santé et conformes aux règles particulièrement strictes qui les accompagnent.

Outils recommandés

Plusieurs **outils** et **services** peuvent s'avérer d'une grande aide pour **s'informer, se préparer et réagir** aux cyberattaques. Il n'est, bien sûr, pas possible d'en dresser une liste exhaustive, mais certaines références sont particulièrement utiles à noter :

→ **le CERT-FR** relaie les alertes de cybersécurité en cours ;

→ **le guide de l'ANSSI** pour faire son propre audit de cybersécurité ;

→ **les plateformes de dépôt de plainte** en cas d'attaque ;

→ **le formulaire à adresser à la CNIL** en cas de fuites de données personnelles ;

→ **le site cybermalveillance.gouv.fr** pour s'informer et approfondir le sujet de la cybersécurité.

Conclusion

En conclusion, il est nécessaire que **l'ensemble des collaborateurs** de l'entreprise prenne conscience des enjeux de la cybersécurité. Des risques pouvant paraître minimes peuvent s'accompagner de conséquences extrêmement graves pour l'entreprise. La **formation** et la **vigilance continues** des équipes constituent un atout inestimable pour se protéger.

Mais l'aspect technique de la cybersécurité revêt une importance tout aussi grande et doit faire l'objet d'autant d'attention. Les cybercriminels n'ont de cesse de repousser les limites pour arriver à leurs fins et il faut savoir bien s'entourer et se doter des meilleurs outils pour assurer la pérennité de ses systèmes d'information.

FIDSUD

EXPERTISE COMPTABLE | CONSEIL | AUDIT

Nous sommes là pour vous accompagner, n'hésitez pas à nous contacter !

https://fidsudcdba.fr/