LA FORTERESSE DIGITALE

Les 34 bonnes pratiques pour une gestion simple et professionnelle de votre informatique

Javier Pose

00

Bienvenue

Bienvenue dans le monde captivant de la sécurité informatique, où les simples et basiques deviennent les superhéros méconnus de la protection numérique ! Imaginez ceci comme un conte moderne, où des pratiques de sécurité apparemment modestes se transforment en boucliers invincibles, défendant les entreprises des ténèbres numériques qui les menacent.

Embarquez avec nous dans cette aventure où la simplicité devient synonyme de puissance, et découvrez comment les choix les plus modestes peuvent se révéler être les plus héroïques pour les entreprises dans l'arène périlleuse de la cybersécurité. Imaginez ces 34 points comme les notes d'une mélodie complexe, une symphonie de sécurité qui peut apporter l'harmonie à votre entreprise dans le monde cacophonique de la cybersécurité.

Bien que chacune de ces notes ne soit pas une obligation stricte, elles forment ensemble une partition qui guide votre orchestre numérique vers la protection totale.

Les 34 clés

Considérez-les comme les pièces d'un puzzle, chaque élément ajoutant une nouvelle dimension à votre tableau de sécurité. En les explorant, vous ne vous imposez pas une liste de règles strictes, mais vous offrez plutôt à votre entreprise une carte au trésor, révélant les chemins à suivre pour mieux comprendre les enjeux et renforcer vos défenses.

Ces 34 points ne sont pas des chaînes, mais des ailes. En les adoptant, vous donnez à votre entreprise la capacité de voler au-dessus des menaces potentielles, de voir l'horizon de la sécurité informatique avec clarté. Ils ne restreignent pas, mais libèrent, offrant une structure qui permet une créativité sécurisée.

En somme, bien que non tous obligatoires, ces points ne sont pas à négliger. Ils sont les gardiens de la tranquillité numérique, les sentinelles qui, une fois compris et adoptés, réduisent l'angle d'attaque des pirates. Ils vous donnent la possibilité de composer votre propre symphonie de sécurité, une mélodie qui éloigne les menaces et fait résonner la confiance dans chaque battement de cœur de votre entreprise.

Sommaire

Notre approche **13**

Sauvegarder les données suivant la méthode 3-2-1 **19**

Mettre en place des sauvegardes immuables **23**

Mettre un antispam avancé avec contrôle automatique des liens et fichiers en mode sandboxing **27**

Mettre un antivirus avancé (qui détecte les comportements suspicieux et la fuite des données) **33**

Les ordinateurs doivent être sur azure avec mdm avec intune sur azure ad **37**

Optimisation firewall **41**

Supprimer tous les accès qui ne sont pas utilisés **45**

Faire une politique de mots de passe changement tous les 3 mois, forcer la complexité…) **49**

Limiter les comptes administrateurs avec un mot de passe complexe et changés 1x par année 53

Sensibiliser à la sécurité les utilisateurs en continu 57

Mettre à jour tous les périphériques réseau au moins 1x par trimestre 61

Faire des tests de phishing réguliers pour garder les utilisateurs attentifs 65

Utiliser le double facteur mfa 69

Chiffrer les disques 73

Faire un plan en cas de cyber attaque 77

Les comptes utilisateurs ne doivent pas être administrateur des ordinateurs et de toutes les données 81

Mettre un mot de passe au boot sur les pc 85

Centraliser les accès sur azure 89

Mettre à jour tous les logiciels au moins 1x par mois 93

Mettre en place un filtrage url qui empêche l'accès aux sites dangereux 97

Archiver les données plus utilisées dans un autre espace 101

Mettre un mot de passe dans le bios sur les pc 105

Tester les plans 1x par année (le drp doit être en conditions proche de la réalité) 109

Forcer l'utilisation de dns sécurisés (1.1.1.2 And 1.0.0.2) 113

Sauvegarder les dossiers qui sont couramment utilisés sur les ordinateurs par les utilisateurs 117

Charte d'utilisation de l'informatique avec les notions de la nlpd 2023 121

Faire un business continuity plan (bcp) 125

Faire un plan en cas de désastre 129

Faire labeliser l'informatique avec le label «cybersafe» cyber-safe.Ch 133

Mettre en place un vpn permanent quand les utilisateurs sont en déplacement 137

Bloquer l'accès à l'ajout de périphériques non validés par l'it 141

Le ou les sites web de l'entreprise sont sauvegardés et sécurisés 145

Définir le temps de reprise et la quantité de données perdues (rto / rpo) 149

Faire une assurance «cyber-risques» ex: helvetia 153

01
Sauvegarder les données suivant la méthode 3-2-1

Le bouclier indestructible

Ah, la sauvegarde des données selon la méthode 3-2-1, c'est comme le bouclier indestructible de notre forteresse d'entreprise ! Imaginez un monde sans soucis, où vos données sont comme des trésors précieux, préservées et chéries.
La méthode 3-2-1, c'est notre arme secrète pour défier le chaos numérique.

Trois copies de nos données, rien de moins, c'est comme avoir des copies de la carte au trésor dans trois coffres différents. Un trésor peut être égaré, mais avec trois cartes, on est toujours sur la piste.
Deux supports distincts, c'est comme avoir des gardiens fidèles à chaque coin de la forêt numérique, prêts à défendre notre richesse d'informations contre les attaques sournoises du temps et des erreurs humaines.
Et la cerise sur le gâteau, cette fameuse copie supplémentaire hors site.

C'est comme avoir un abri secret pour nos données, un refuge inviolable à l'abri des catastrophes locales. Les incendies, les inondations, ou même les erreurs humaines les plus graves ne peuvent rien contre notre trinité de sauvegarde.

En suivant la méthode 3-2-1, on crée un rempart indestructible, un rempart qui nous assure que nos données, notre essence même, survivront aux tempêtes du temps. C'est bien plus qu'une simple routine technique, c'est une déclaration d'amour envers nos données, une promesse de les protéger et de les chérir comme le trésor qu'elles sont.

Alors, amis de l'entreprise, embrassons la méthode 3-2-1 avec passion et dévotion, car elle est notre bouclier, notre assurance, notre gage de tranquillité d'esprit dans le monde numérique tourbillonnant.

Sauvegardons avec amour, et nos données seront éternelles !



Notes

02
Mettre en place des sauvegardes immuables

Les gardiens silencieux

Il est crucial, essentiel, vital même, de mettre en place des sauvegardes immuables au sein d'une entreprise. C'est comme ériger un rempart indestructible pour protéger les fondations fragiles de tout ce que vous avez bâti avec tant de passion, de sueur et d'efforts.

Imaginez un instant le scénario terrifiant où tous les efforts acharnés, les heures de travail, les idées géniales, et les projets qui ont fait battre le cœur de votre entreprise sont balayés par une vague dévastatrice de données perdues. C'est comme si tout ce que vous avez construit s'effondrait, emportant avec lui les rêves, les réussites, et l'âme même de votre entreprise.

Les sauvegardes immuables, ce sont les gardiens silencieux qui veillent sur votre héritage numérique, prêts à résister à toute tempête.

Elles offrent une assurance tranquille, une certitude que même face aux pires scénarios, vos données resteront intactes, préservant ainsi l'histoire de votre entreprise.

En mettant en place des sauvegardes immuables, vous faites bien plus que protéger des fichiers.
Vous sauvegardez la confiance de vos clients, la réputation de votre entreprise, et la crédibilité que vous avez durement gagnée. C'est un investissement émotionnel, une déclaration de fidélité envers le parcours que vous avez entrepris, un serment de ne jamais abandonner vos données à la merci du hasard.

Alors, installez ces gardiens du temps, ces sentinelles de la persévérance, et donnez à votre entreprise la sécurité émotionnelle qu'elle mérite.
Protégez chaque instant, chaque idée, et chaque espoir, car au cœur de chaque sauvegarde immuable réside la promesse inébranlable de préserver ce qui compte le plus.



Notes

03
Mettre un antispam avancé avec contrôle automatique des liens et fichiers en mode sandboxing

Le gardien vigilant

Imaginez un instant que votre entreprise soit une forteresse, un rempart solide contre les flots incessants d'informations indésirables qui menacent de submerger votre productivité et la sécurité de vos données. Mettre en place un antispam avancé, c'est comme ériger des remparts impénétrables autour de votre forteresse numérique.

L'antispam avancé agit comme le gardien vigilant, filtrant chaque message entrant avec une précision chirurgicale. Il repousse les assauts de courriels indésirables, de spams et de menaces électroniques qui tentent insidieusement de s'infiltrer dans vos communications. C'est comme si vous donniez une armure à votre entreprise, la protégeant des attaques sournoises qui pourraient autrement la fragiliser. Le contrôle automatique des liens et des fichiers représente la sentinelle supplémentaire dans cette forteresse numérique.

Il examine chaque lien, chaque fichier, scrutant leur contenu avec une rigueur sans faille.
Comme un gardien inflexible, il s'assure que rien de malveillant ne peut se glisser à travers les mailles de la sécurité.

Les liens suspects sont bloqués, les fichiers potentiellement dangereux sont mis en quarantaine.
Et puis, le mode sandboxing, c'est comme si vous aviez une zone d'essai sécurisée à l'intérieur de votre forteresse. Les fichiers inconnus sont exécutés dans cet environnement isolé, loin des zones sensibles de votre système. C'est une ultime ligne de défense, un rempart supplémentaire qui garantit que même si quelque chose parvient à franchir les premières barrières, il sera neutralisé avant de causer le moindre tort.

En investissant dans cette protection avancée, vous investissez dans la tranquillité d'esprit, dans la continuité de vos opérations sans être constamment sur le qui-vive. C'est comme donner à votre entreprise une armure indestructible et les moyens de se défendre contre les assauts numériques.

Alors, mettez en place cet antispam avancé avec contrôle automatique des liens et fichiers en mode sandboxing, et faites de votre entreprise une forteresse numérique impénétrable face aux menaces qui rôdent dans le monde virtuel.

Notes

04
Mettre un antivirus avancé (qui détecte les comportements suspicieux et la fuite des données)

Un protecteur qui anticipe les comportements suspects

Dans le monde numérique tumultueux d'aujourd'hui, la sécurité des données est la sentinelle qui veille sur l'intégrité et la prospérité de toute entreprise. Mettre en place un antivirus avancé, capable de détecter les comportements suspects et les fuites de données, c'est comme ériger une muraille indestructible autour du cœur battant de votre société.

Imaginez un instant que votre entreprise soit une forteresse, abritant des trésors d'informations cruciales. Sans une protection adéquate, elle serait vulnérable aux assauts invisibles des menaces numériques, prêtes à infiltrer et à saper tout ce que vous avez bâti avec tant d'efforts.

Cet antivirus avancé n'est pas simplement un gardien, c'est un vigilant, un protecteur dévoué qui scrute chaque recoin virtuel à la recherche du moindre signe de danger.

Il ne se contente pas de bloquer les attaques connues, il anticipe, il identifie les comportements suspects, ces ombres numériques qui pourraient annoncer une menace imminente.

En déployant un tel antivirus, vous envoyez un message fort à vos équipes, à vos clients, à chaque acteur qui confie son existence numérique à votre entreprise :

«Nous prenons la sécurité au sérieux, nous défendrons vos données avec la même ardeur que nous défendrions notre propre forteresse.»

Protéger les données, c'est aussi protéger la confiance, la réputation, l'âme même de votre entreprise. Un antivirus avancé est bien plus qu'une simple ligne de défense. C'est le bouclier qui garantit que votre histoire, vos succès, et vos ambitions ne seront pas effacés par les vagues tumultueuses de la cybercriminalité.

En somme, investir dans un antivirus avancé, c'est investir dans l'avenir de votre entreprise. C'est ériger un rempart impénétrable pour que votre forteresse puisse résister aux assauts numériques, évoluer en toute sécurité, et continuer à écrire son histoire avec confiance et sérénité.

Notes

05
Les ordinateurs doivent être sur azure avec mdm avec intune sur azure ad

La boussole qui t'assure que tu n'égares jamais ta route

Imagine-toi voguant sur un océan de possibilités infinies, ton entreprise comme un vaisseau, prête à conquérir de nouveaux horizons. Eh bien, mon ami, Azure avec MDM et Intune sur Azure AD, c'est comme la boussole qui t'assure que tu n'égares jamais ta route.

D'abord, plongeons dans le royaume magique d'Azure. C'est là que la magie opère, où tes ordinateurs deviennent des héros numériques. Avec leur pouvoir stocké dans le cloud, tu libères tes machines des chaînes du passé. Fini les tracas de la gestion locale, place à la flexibilité et à la rapidité qui te catapultent vers l'avenir.

Et maintenant, entrons dans l'univers captivant du MDM et d'Intune. Imagine un chef d'orchestre dirigeant une symphonie de productivité.

Avec Intune sur Azure AD, tes appareils sont harmonisés, tous jouant la même mélodie.
La sécurité devient une armure indestructible, protégeant tes données comme un dragon gardant son trésor. Mais, cher ami, le vrai trésor ici, c'est la liberté. Liberté de travailler de n'importe où, à tout moment.

Les frontières s'estompent, et tes employés deviennent des héros mobiles, prêts à conquérir le monde professionnel depuis leurs propres forteresses.
Alors, imagine l'avenir radieux de ton entreprise, où la puissance d'Azure, la gestion magique du MDM, et la protection d'Intune se réunissent pour créer une symphonie de succès. C'est bien plus qu'une simple migration technologique, c'est une révolution numérique qui propulse ton entreprise vers des sommets insoupçonnés.

En adoptant cette voie, tu fais bien plus que mettre à jour des logiciels. Tu sculptes le destin de ton entreprise, la transformant en une force imparable, prête à défier les vents du changement.
Alors, mon ami, embrasse cette aventure avec enthousiasme, car sur le navire de la modernité, le vent d'Azure te mènera vers des horizons lumineux et prometteurs.

Notes

06
Optimisation firewall

Le guerrier intrépide

Dans l'arène sans pitié des affaires,
l'optimisation du pare-feu est une danse délicate entre la survie et la prospérité. Imaginez-vous dans un monde sans défense, où les flammes de la concurrence dévorent tout sur leur passage.
C'est là que le pare-feu entre en scène, en tant que gardien invincible protégeant les précieuses données de votre entreprise.

L'optimisation du pare-feu, c'est comme armer votre forteresse de lames affûtées et de boucliers indestructibles. C'est la différence entre la vulnérabilité totale et la sécurité inébranlable.
Les cyber-menaces rôdent telles des bêtes sauvages, cherchant à dévorer les fruits de votre dur labeur.
Ne laissez pas votre entreprise devenir une proie facile ! Imaginez le pare-feu comme un guerrier intrépide, défiant les assauts incessants des pirates informatiques.

Chaque ligne de code est une épée prête à déjouer les attaques, chaque algorithme est une armure renforcée résistant à toutes les tentatives de pénétration. C'est votre bouclier ultime contre le chaos numérique qui guette à chaque coin de câble. Optimiser le pare-feu, c'est sculpter une armure sur mesure pour votre entreprise. C'est un acte de prévoyance, une déclaration audacieuse disant :

«Nous ne serons pas vaincus, nous protégerons ce qui est nôtre à tout prix.»

Dans un monde où la moindre faille peut être exploitée, l'optimisation du pare-feu est le rempart qui assure la tranquillité d'esprit.

Dans le ballet incessant des bits et des octets, ne laissez pas votre entreprise être une victime. L'optimisation du pare-feu, c'est le cri de guerre de la sécurité, la promesse de défendre votre forteresse numérique contre les hordes de menaces.

C'est bien plus qu'une simple mesure technique – c'est la garantie que votre entreprise continuera de prospérer, sans craindre les flammes dévastatrices qui menacent de la consumer. Alors, armez-vous, renforcez vos défenses, et dansez avec confiance dans l'arène impitoyable des affaires.

Notes

07
Supprimer tous les accès qui ne sont pas utilisés

Un acte de prudence

La suppression des accès inutilisés est une mesure cruciale dans le domaine de la sécurité informatique au sein d'une entreprise. C'est bien plus qu'une simple tâche administrative, c'est une bouffée d'air frais pour les défenses de votre système, une armure renforcée contre les menaces invisibles qui rôdent dans l'ombre. Imaginez votre entreprise comme un château majestueux, entouré de douves profondes.

Ces douves représentent vos pares-feux, vos systèmes de détection d'intrusion, vos dispositifs de sécurité sophistiqués. Mais que se passe-t-il lorsque les ponts-levis restent baissés en permanence, offrant une invitation ouverte à quiconque souhaite s'introduire ?

Supprimer les accès inutilisés, c'est comme tirer sur ces leviers, élevant les ponts-levis pour ne laisser passer que ceux qui ont le droit de franchir les portes de votre forteresse numérique.

C’est un acte de prudence, une déclaration claire selon laquelle seuls ceux qui ont une raison légitime de fouler vos couloirs virtuels sont autorisés à le faire. En gardant ces accès indésirables, vous créez des failles, des brèches sournoises par lesquelles des intrus pourraient s’introduire. C’est comme laisser une fenêtre ouverte par négligence, alors que vous avez déjà investi dans des serrures de haute technologie.

Ces accès non utilisés deviennent des points faibles, des coins sombres où les cybercriminels peuvent se tapir, attendant le moment opportun pour frapper. Il y a une élégance dans la simplicité de cette action. C’est comme un grand ménage, une purification numérique. Cela envoie un message fort selon lequel votre entreprise n’est pas une terre de libre accès, mais plutôt une forteresse bien gardée.

En somme, supprimer les accès non utilisés, c’est comme verrouiller chaque porte, fermer chaque fenêtre, et s’assurer que seuls ceux qui ont une invitation spéciale peuvent pénétrer votre royaume numérique. C’est une étape essentielle pour garantir la sécurité de vos données, de votre personnel et de l’intégrité même de votre entreprise.



Notes

08
Faire une politique de mots de passe changement tous les 3 mois, forcer la complexité…)

Des murailles plus hautes

Permettez-moi de vous expliquer avec passion pourquoi la mise en place d'une politique de mots de passe est absolument cruciale au sein d'une entreprise.

Imaginez un instant que votre entreprise soit un château fort, et que les mots de passe soient les clés qui protègent les portes de ce bastion.
Maintenir ces clés en sécurité est aussi vital que de défendre les murs de la forteresse elle-même.

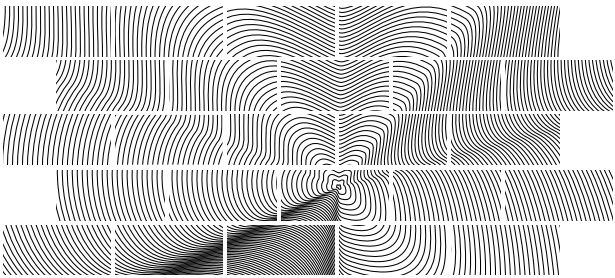
La fréquence des changements de mots de passe, tous les trois mois, est comme une rotation constante des gardiens du château. Cela ajoute une couche de sécurité supplémentaire en garantissant que même si une clé devait tomber entre de mauvaises mains, elle ne serait utile que pendant une période limitée. C'est comme si les portes du château changeaient de forme régulièrement, défiant quiconque tenterait de les forcer.

La complexité des mots de passe est comme un labyrinthe mystique qui entoure le château. Plus il est complexe, plus il devient difficile pour les intrus de naviguer à travers ses dédales. Imposer des exigences de complexité, avec des majuscules, des minuscules, des chiffres et des caractères spéciaux, crée une forteresse virtuelle impénétrable. Imaginez les hackers se heurtant à un mur invisible de symboles et de combinaisons, incapables de décrypter le secret. En instaurant une politique de mots de passe, vous élevez votre entreprise au rang d'une forteresse moderne, où la sécurité est une priorité sacrée.

Vous n'accepteriez pas de laisser les portes de votre château sans protection, alors pourquoi compromettre la sécurité de votre entreprise en négligeant les fondations de la cybersécurité ? En adoptant cette politique, vous renforcez les remparts de votre royaume numérique, protégeant non seulement vos données, mais aussi la confiance que vos clients et partenaires placent en vous.

En conclusion, mettre en œuvre une politique de mots de passe est comme ériger des murailles plus hautes, creuser des fossés plus profonds et renforcer les défenses de votre forteresse numérique.

C’est un acte de bravoure dans le monde numérique, une déclaration audacieuse que votre entreprise ne transigera pas sur la sécurité. Alors, armez-vous de mots de passe robustes, changez-les régulièrement et maintenez la sécurité de votre royaume numérique à tout prix !



Notes

09
Limiter les comptes administrateurs avec un mot de passe complexe et changés 1x par année

Une forteresse impénétrable

Il est impératif de limiter l'accès aux comptes administrateurs avec des mots de passe complexes, changés une fois par an, afin de garantir la sécurité robuste de l'entreprise.

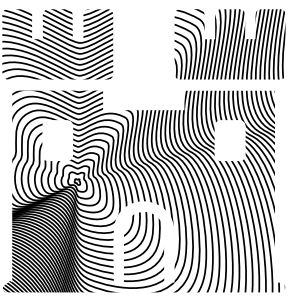
Imaginez un instant le pouvoir colossal détenu par ces comptes ! Ce sont les gardiens virtuels de nos systèmes, les maîtres des données sensibles, et les sentinelles qui veillent sur l'intégrité de toute l'organisation.

En restreignant l'accès à ces comptes avec des mots de passe complexes, nous érigeons une forteresse impénétrable contre les menaces. Un mot de passe complexe agit comme une armure, défiant les assaillants potentiels et garantissant que seuls les initiés autorisés peuvent pénétrer ce bastion numérique. Quant à la rotation annuelle des mots de passe, c'est comme changer la serrure principale de votre maison. Cela ajoute une couche de sécurité supplémentaire en

introduisant l'élément de surprise pour toute personne cherchant à s'infiltrer. Imaginez si vous deviez garder la même clé de maison pour toujours – tôt ou tard, quelqu'un pourrait la trouver ou la copier.

Le changement annuel des mots de passe n'est pas simplement une routine, c'est une cérémonie de renouvellement qui renforce la défense de l'entreprise. C'est la garantie que les portes virtuelles restent solidement verrouillées, préservant ainsi la confidentialité, l'intégrité et la disponibilité des informations cruciales.

En somme, en restreignant et en renouvelant les comptes administrateurs, nous érigeons un rempart contre les menaces cybernétiques, assurant ainsi la sécurité et la résilience de l'entreprise.
Nous devons protéger nos données comme notre bien le plus précieux, car dans le monde numérique d'aujourd'hui, la sécurité est la clé de notre survie.



Notes

10
Sensibiliser à la sécurité les utilisateurs en continu

Un entrainement pour vos gardiens

Il est absolument essentiel de sensibiliser en permanence les utilisateurs à la sécurité au sein d'une entreprise, et laissez-moi vous dire pourquoi cette démarche est cruciale.

Imaginez votre entreprise comme une forteresse, avec chaque employé comme un gardien de ses remparts. Maintenant, si un seul de ces gardiens ne comprend pas l'importance de la sécurité, ou pire, néglige ses devoirs, cela peut ouvrir une brèche dans les défenses. Nos données, nos informations sensibles, sont comme des trésors que nous devons protéger.

Si chaque personne dans l'entreprise ne comprend pas la valeur de ces trésors et ne sait pas comment les protéger, alors notre forteresse devient vulnérable. La sensibilisation continue à la sécurité est comme un entrainement pour ces gardiens.

C'est le moyen de s'assurer qu'ils connaissent les dernières menaces, les tactiques des assaillants, et comment se défendre.

Imaginez que chaque employé soit un maillon d'une chaîne. Si un maillon est faible, la chaîne entière est compromise. La sensibilisation constante est le moyen de renforcer chaque maillon, de s'assurer que chaque personne dans l'entreprise est consciente des risques et sait comment agir correctement pour protéger nos actifs les plus précieux.

Et puis, il y a la menace humaine.

Les pirates informatiques n'attaquent pas seulement avec des lignes de code. Ils exploitent souvent la faiblesse humaine, utilisant des techniques de phishing sophistiquées pour tromper les utilisateurs. La sensibilisation continue les arme contre de telles attaques. C'est comme leur donner une épée pour se défendre contre les mensonges et les manipulations. En somme, la sensibilisation à la sécurité est la clé pour renforcer les défenses de notre forteresse numérique. C'est une responsabilité collective, une mission que chaque employé doit prendre à cœur. Car au final, la sécurité de l'entreprise dépend de la force de chacun de ses défenseurs.

Notes

11
Mettre à jour tous les périphériques réseau au moins 1x par trimestre

Armer vos gardiens avec les dernières technologies

Imaginez votre entreprise comme un château fort, entouré de remparts impénétrables.
Ces remparts, ce sont vos périphériques réseau. Maintenant, ces remparts doivent être constamment renforcés, sinon, comment pouvez-vous être sûr qu'ils résisteront à toutes les attaques sournoises de l'extérieur ? C'est là que la mise à jour régulière de vos périphériques réseau entre en jeu.

C'est comme armer vos gardiens avec les dernières technologies, les équipant de boucliers invincibles et d'épées étincelantes. Chaque trimestre, c'est une nouvelle couche de protection, une nouvelle barrière contre les menaces qui évoluent sans cesse.

Les pirates informatiques ne dorment jamais, et ils scrutent constamment les failles de sécurité pour trouver le maillon faible.

En mettant à jour vos périphériques régulièrement, vous envoyez un message fort :

«Pas question de laisser des brèches dans notre forteresse !»

Les mises à jour ne sont pas juste des correctifs, ce sont des boucliers modernes qui repoussent les attaques les plus sophistiquées. C'est votre moyen de rester en avance dans la bataille perpétuelle entre la sécurité et les menaces.

Imaginez maintenant les conséquences d'une négligence à cet égard. Des failles non corrigées sont comme des portes dérobées secrètes dans votre forteresse, invitant les malintentionnés à entrer et à causer des ravages.

Personne ne veut voir son château pillé, n'est-ce pas ?
En résumé, mettre à jour vos périphériques réseau trimestriellement, c'est comme entretenir et renforcer les fondations de votre entreprise.
C'est une déclaration de détermination à maintenir la sécurité à son plus haut niveau.

Alors, ne laissez pas vos remparts s'effriter, armez-vous de mises à jour régulières et défendez votre royaume numérique avec ferveur !

Notes

12
Faire des tests de phishing réguliers pour garder les utilisateurs attentifs

Un acte de prévoyance

Les tests de phishing réguliers sont comme des exercices d'entraînement pour votre équipe, les préparant à affronter les ruses vicieuses de ceux qui cherchent à pénétrer les défenses de votre forteresse numérique. C'est comme un feu continu qui forge la vigilance de vos troupes, les rendant plus résistantes face aux tentatives de tromperie.

Dans le monde numérique d'aujourd'hui, les attaques de phishing sont tissées dans les mailles invisibles de nos communications quotidiennes.
Elles se cachent dans les recoins sombres de nos boîtes de réception, attendant patiemment de piéger le moindre clic distrait.

Les tests de phishing, c'est comme la lumière qui révèle ces embûches sournoises, éduquant vos employés sur les signes avant-coureurs, les aidant à déjouer les pièges tendus.

Imaginez que chaque employé est un maillon précieux dans la chaîne de sécurité de votre entreprise. Les tests de phishing réguliers renforcent ces maillons, les endurcissant contre les maîtres de l'ombre qui cherchent à exploiter la moindre faille. C'est un investissement dans la protection de votre actif le plus précieux : l'intégrité de vos données. N'oublions pas que la confiance est le ciment qui maintient ensemble les fondations de toute entreprise prospère. Les tests de phishing réguliers envoient un message fort : votre entreprise est prête à affronter les tempêtes numériques, à protéger non seulement ses intérêts, mais également la confiance précieuse que vos clients, partenaires et employés placent en elle.

En somme, c'est un acte de prévoyance, une déclaration audacieuse que votre entreprise refuse de se plier devant les assauts invisibles.
C'est une démonstration de force, une affirmation que la sécurité n'est pas seulement une priorité, mais une valeur fondamentale que vous êtes prêt à défendre avec acharnement. Les tests de phishing réguliers sont le rempart qui assure que votre entreprise ne devienne pas une victime, mais plutôt le gardien intrépide de son royaume numérique.

Notes

13
Utiliser le double facteur mfa

Un deuxième mur

Imagine un instant que ton entreprise soit comme un château fort, tes données sensibles étant les joyaux précieux que tu veux protéger à tout prix. Maintenant, le mot de passe seul, c'est un peu comme une seule porte en bois, pas très solide, facile à enfoncer pour un intrus malintentionné.

Le double facteur d'authentification, c'est comme ajouter un deuxième mur d'enceinte à ton château. Oui, c'est un peu plus contraignant, mais regarde le côté positif : cela rend ta forteresse presque impénétrable. Pourquoi se contenter d'une seule ligne de défense quand tu peux en avoir deux ?
Le MFA, c'est comme avoir une clé supplémentaire qui ne peut être utilisée que par le vrai gardien du château, c'est-à-dire toi ! Même si quelqu'un réussit à voler ton mot de passe (ce qui peut arriver à n'importe qui), il sera toujours bloqué à la porte, incapable de franchir le deuxième mur sans cette clé spéciale.

En gros, c'est comme protéger non seulement l'entrée principale de ton château, mais aussi le passage secret que seuls les initiés connaissent. C'est une double garantie que tes données restent entre de bonnes mains, les tiennes.

Alors, pourquoi le MFA dans une entreprise ?
Parce que tes informations sont précieuses, et tu veux les protéger comme le trésor qu'elles sont.
Ne laisse pas tes données être pillées comme un château sans défense – adopte le double facteur d'authentification et fortifie tes remparts numériques !



Notes

14
Chiffrer les disques

Le sortilège magique

La protection des données est une responsabilité cruciale au sein de toute entreprise, et chiffrer les disques est comme une armure impénétrable pour les trésors les plus précieux de votre organisation. Imaginez-vous gardien des secrets, veillant sur des trésors inestimables.

Ces trésors ne sont rien d'autre que les données vitales de votre entreprise. Elles renferment les rêves, les ambitions et la vie même de votre organisation. Maintenant, pensez à chiffrer les disques comme le sortilège magique qui entoure ces trésors, les enveloppant dans une barrière indéchiffrable.

Dans le monde numérique d'aujourd'hui, les menaces planent comme des vautours affamés, guettant la moindre opportunité pour s'infiltrer et dérober ces richesses.

Le chiffrement des disques est votre bouclier, votre rempart contre les regards indiscrets et les mains avides. Il transforme les données en un langage secret que seuls les détenteurs de la clé peuvent comprendre. Imaginez le cauchemar de voir vos données sensibles exposées, vulnérables comme un trésor sans protection. Le chiffrement des disques devient alors le gardien silencieux, le protecteur invincible qui se tient entre vos informations et les ténèbres menaçantes.

La confiance de vos clients, l'intégrité de votre entreprise, tout repose sur la sécurité de ces données. Le chiffrement des disques n'est pas simplement une tâche technique, c'est un acte de préservation, une déclaration passionnée pour la sécurité et la confidentialité.

Protéger vos disques avec le chiffrement, c'est ériger une forteresse impénétrable autour de votre royaume numérique. C'est la promesse que même en cas d'assaut, vos données demeureront résilientes, vos secrets gardés avec une force inébranlable.
Alors, chiffrer les disques devient bien plus qu'une simple mesure de sécurité. C'est une ode à la confiance, une déclaration d'amour envers la pérennité de votre entreprise, une promesse solennelle de défendre vos trésors numériques avec une détermination inébranlable.

Notes

15
Faire un plan en cas de cyber attaque

Une stratégie claire

La mise en place d'un plan en cas de cyberattaque au sein d'une entreprise est comme ériger une forteresse impénétrable pour protéger notre trésor le plus précieux : nos données.

C'est la clé qui ouvre la porte vers un avenir plus sûr, plus résilient.

Imaginez-vous en train de construire une muraille massive autour de votre château, avec des remparts solides pour repousser les assaillants numériques. Le plan de cyberattaque, c'est le manuel qui guide chaque étape de cette construction. Il n'est pas seulement un simple document, mais plutôt le gardien vigilant qui veille sur votre royaume numérique. Dans ce monde virtuel où les menaces se cachent dans l'ombre, le plan de cyberattaque devient la lumière qui dissipe l'obscurité. Il offre une tranquillité d'esprit en préparant l'entreprise à affronter l'inconnu.

Chaque ligne de code de ce plan est une barrière supplémentaire, une armure pour défendre nos actifs numériques.

Et que dire de la rapidité d'action lorsqu'une attaque survient ? Le plan de cyberattaque, c'est notre chevalier en armure brillante, prêt à dégainer son épée pour repousser l'ennemi. Il établit une stratégie claire, coordonne les troupes et minimise les dommages. En l'absence de ce plan, l'entreprise serait comme un royaume sans défense, à la merci des ravages d'une cyberattaque.

Chaque membre de l'équipe devient un maillon essentiel de cette chaîne de protection.
Le plan de cyberattaque, c'est le code d'honneur qui guide chaque individu dans la bataille contre les forces malveillantes. Il assure une réponse organisée et efficace, transformant le chaos potentiel en ordre et en contrôle.

Alors, construisons ensemble cette forteresse numérique. Faisons du plan de cyberattaque notre bouclier indestructible, prêts à affronter les tempêtes numériques avec la confiance que seul un plan bien élaboré peut apporter. En protégeant nos données, nous préservons l'essence même de notre entreprise, assurant ainsi sa survie dans le monde digital.

Notes

16
Les comptes utilisateurs ne doivent pas être administrateur des ordinateurs et de toutes les données

Une question de prudence

Il est impératif que les comptes utilisateurs ne soient pas élevés au statut d'administrateur des ordinateurs et de toutes les données au sein d'une entreprise. Imaginez un instant que votre entreprise soit un château, chaque ordinateur étant une forteresse et chaque donnée une précieuse relique.

Les administrateurs sont les gardiens, les protecteurs de ces lieux sacrés. Maintenant, si chaque utilisateur pouvait accéder librement à ces pouvoirs administratifs, ce serait comme donner des clés du château à tout un chacun.

La sécurité, c'est la clé de voûte de votre forteresse numérique. Mettre tous les comptes utilisateurs en position d'administrateur reviendrait à ouvrir grand les portes aux menaces malveillantes. C'est comme donner un accès complet à l'arsenal secret du château à n'importe quel invité.

Les erreurs innocentes peuvent se transformer en catastrophes, les données sensibles risquent d'être exposées, et les murs de votre forteresse deviennent vulnérables.

En restreignant l'accès administratif aux seules personnes nécessaires, vous érigez des remparts solides autour de votre royaume numérique.
Chaque utilisateur doit avoir sa propre place, son propre rôle, sans empiéter sur le territoire réservé aux gardiens. C'est une question de prudence, de prévoyance, de protéger non seulement les biens tangibles de l'entreprise, mais aussi son intégrité, son identité.

En fin de compte, la sécurité informatique n'est pas simplement une série de règles, c'est une quête héroïque pour protéger l'essence même de votre entreprise. En refusant à chaque utilisateur le statut d'administrateur, vous élevez la sécurité au rang d'épopée, où votre forteresse numérique peut prospérer et résister aux assauts du monde extérieur. Alors, choisissez la sagesse, choisissez la prudence, et gardez les clés du royaume entre les mains les plus dignes.

Notes

17
Mettre un mot de passe au boot sur les pc

L'intégrité de votre système

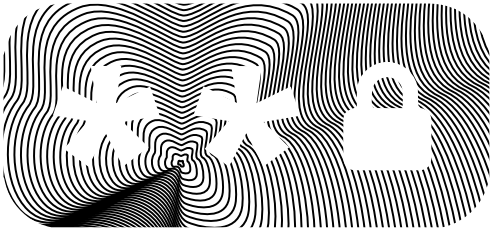
Il est absolument crucial de mettre en place un mot de passe au boot sur tous les ordinateurs de l'entreprise ! Imaginez un instant les conséquences désastreuses si cette simple précaution n'était pas prise.
C'est comme laisser la porte principale de votre maison grande ouverte, invitant tous les dangers à pénétrer sans la moindre résistance.

Le mot de passe au boot agit comme le gardien vigilant, le rempart ultime qui protège les données sensibles de votre entreprise. Sans lui, n'importe qui pourrait accéder à ces machines dès le démarrage, ouvrant ainsi la voie à des attaques malveillantes et à l'exploitation des informations confidentielles.
C'est comme si vous donniez les clés de votre coffre-fort à tous les inconnus sans la moindre restriction. En plus de garantir la confidentialité, le mot de passe au boot assure également l'intégrité de votre système.

Il empêche toute altération non autorisée, préservant ainsi l'environnement informatique de votre entreprise de toute menace insidieuse.

Pensez-y comme à l'épine dorsale de votre sécurité informatique. Le mot de passe au boot est le premier rempart qui se dresse face aux assaillants, et son absence expose votre entreprise à des risques inutiles et évitables.

Ne sous-estimez pas le pouvoir de cette simple mesure de sécurité, car elle peut faire la différence entre une entreprise vulnérable et une entreprise robuste, prête à défier les défis numériques qui se dressent sur son chemin.



Notes

18
Centraliser les accès sur azure

Toutes les clés dans un seul

Centraliser les accès sur Azure dans une entreprise, c'est comme construire une forteresse impénétrable pour protéger notre précieux trésor : les données de l'entreprise. Imaginez un château où toutes les portes sont solidement verrouillées, et seuls les chevaliers autorisés ont la clé pour entrer. C'est exactement ce que nous faisons en centralisant les accès sur Azure.

D'abord, cela simplifie la gestion des autorisations. Plus besoin de jongler avec des trousseaux de clés dispersés dans tout le royaume de l'entreprise. En centralisant sur Azure, nous consolidons le contrôle, nous rassemblons toutes les clés dans un seul endroit puissant.

C'est comme avoir un grand maître des clés qui surveille tout, assurant que seuls les valeureux guerriers peuvent accéder aux zones sensibles. Ensuite, pensons à la rapidité et à la réactivité.

En cas d'urgence, Azure devient notre tour de guet, capable de réagir instantanément aux menaces. Il devient notre bouclier magique qui peut se lever en un instant pour protéger nos actifs les plus précieux. Plus de temps perdu à chercher qui a quel accès où. Tout est géré depuis la forteresse virtuelle d'Azure. Et n'oublions pas la résilience.

Azure offre une robustesse inégalée, un rempart numérique contre les attaques. En consolidant les accès sur cette plateforme solide, nous renforçons nos défenses. C'est comme ériger des murailles épaisses autour de nos données, les protégeant des flèches empoisonnées des cyber-menaces.

En fin de compte, centraliser les accès sur Azure, c'est élever notre entreprise à un niveau supérieur de sécurité. C'est comme confier la garde de notre trésor le plus précieux à un dragon vigilant qui ne dort jamais.

Nous nous assurons ainsi que nos données restent en sécurité, préservant l'intégrité de notre royaume numérique. Alors, armons-nous de sagesse et consolidons nos forces sur Azure pour que notre forteresse demeure impénétrable !

Notes

19
Mettre à jour tous les logiciels au moins 1x par mois

Renforcer constamment les murs

Il est absolument crucial de mettre à jour tous les logiciels dans votre entreprise au moins une fois par mois. Imaginez ceci comme la protection ultime de votre forteresse numérique contre les attaques malveillantes. C'est comme renforcer constamment les murs de votre château pour empêcher les assaillants de s'infiltrer.

Les mises à jour sont comme des remparts, érigés par les développeurs pour contrer les nouvelles ruses des cybercriminels. Ne pas les installer revient à laisser vos portes grandes ouvertes, invitant les malfaiteurs à s'introduire dans vos systèmes. C'est comme laisser une fenêtre entrouverte dans une tempête - vous ne savez jamais quand elle va s'abattre, mais vous voulez être prêt. En négligeant ces mises à jour, vous exposez vos précieuses données à des menaces invisibles.

C'est un peu comme laisser votre coffre au trésor sans surveillance, espérant que les pirates informatiques n'auront pas vent de vos richesses numériques.
Mais soyons réalistes, ils sont toujours à l'affût, prêts à saisir la moindre opportunité.

En gardant vos logiciels à jour, vous investissez dans la sécurité de votre empire numérique.
Vous renforcez les remparts, élevez le niveau de protection et montrez aux cybercriminels que vous ne plaisantez pas. C'est un acte de défense proactive, une déclaration audacieuse disant :

«Ici, nous sommes préparés, nous ne facilitons pas la tâche aux assaillants.»

Alors, ne laissez pas vos défenses s'affaiblir.
Mettez à jour, renforcez, et protégez votre royaume numérique. Parce qu'en matière de sécurité informatique, la vigilance est la clé, et chaque mise à jour est un bouclier de plus entre vous et les menaces qui rodent dans l'ombre numérique.

Notes

20
Mettre en place un filtrage url qui empêche l'accès aux sites dangereux

Un chemin sûr

Il est absolument crucial de mettre en place un filtrage URL dans votre entreprise afin de garantir la sécurité de vos données sensibles et de vos collaborateurs dévoués. Imaginez un instant que votre réseau soit une forteresse, vos données en sont les trésors les plus précieux, et les sites web dangereux sont tels des dragons cracheurs de feu, prêts à dévorer tout ce qui se trouve sur leur passage.

En empêchant l'accès à ces sites périlleux, vous érigez un rempart puissant, un bouclier invincible contre les menaces en ligne. C'est comme verrouiller les portes de votre château pour empêcher les malfaiteurs d'entrer et de semer le chaos. Les sites dangereux, tels des maraudeurs malveillants, tentent de s'infiltrer dans vos systèmes, mais avec un filtrage URL, vous érigez un mur impénétrable. Pensez à la sécurité de vos collaborateurs comme à la protection de valeureux chevaliers.

En les empêchant d'accéder à des sites web potentiellement nuisibles, vous leur offrez une armure supplémentaire contre les menaces en ligne. C'est comme leur donner des boucliers et des épées pour se défendre dans le royaume virtuel.

Un filtrage URL, c'est l'assurance que vos précieuses informations restent entre des mains dignes de confiance. Imaginez que chaque clic sur un lien soit une aventure dans l'inconnu. Avec le filtrage URL, vous guidez vos collaborateurs à travers un chemin sûr, évitant les embûches et les pièges sournois. En résumé, mettre en place un filtrage URL dans votre entreprise, c'est élever vos défenses, protéger vos trésors numériques, armer vos collaborateurs contre les menaces et garantir la pérennité de votre royaume numérique.

Ne laissez pas les dragons de l'Internet s'approcher de vos portes sans opposition. Faites preuve de sagesse et érigez un rempart virtuel pour assurer la sécurité de votre empire numérique.

Notes

21
Archiver les données plus utilisées dans un autre espace

Le gardien de l'ordre

Bien sûr, archiver les données moins utilisées dans un espace distinct est une mesure de sécurité cruciale pour toute entreprise. Imaginez un instant que vos données soient comme les précieux souvenirs d'une vie entière, stockés dans une maison immense. Maintenant, cette maison représente votre entreprise, et chaque pièce est une partie importante de vos opérations.

Au fil des années, les souvenirs s'accumulent, les données s'entassent, et bientôt, la maison devient un dédale complexe. Vous vous perdez dans un dédale de pièces inutiles, cherchant désespérément ce dont vous avez besoin. C'est là que l'archivage devient le héros méconnu, le gardien de l'ordre dans cette maison virtuelle.

En archivant, vous créez un grenier sûr pour ces souvenirs moins fréquemment consultés.

C'est comme ranger soigneusement les objets précieux que vous n'utilisez pas tous les jours, mais qui sont irremplaçables. Ce grenier virtuel vous permet non seulement de libérer de l'espace dans vos pièces principales, mais surtout, il renforce la sécurité de vos données.

En imaginez-vous un instant les conséquences d'une invasion de votre maison par des intrus malveillants ? Ils fouillent chaque pièce, laissant le chaos dans leur sillage. Mais si vous avez archivé vos souvenirs, vos données sensibles, dans un espace distinct, vous avez créé un rempart. Vous avez placé vos trésors dans un coffre-fort virtuel, éloignant les regards indiscrets. C'est donc bien plus qu'une simple organisation virtuelle. C'est une démarche proactive pour protéger l'essence même de votre entreprise. Archiver les données moins utilisées dans un autre espace, c'est comme verrouiller les portes de vos souvenirs, éloignant les menaces potentielles.

C'est une garantie que, même si le chaos règne dans certaines parties de votre maison virtuelle, l'essentiel reste à l'abri, préservé et intact.

Notes

22
Mettre un mot de passe dans le bios sur les pc

Endosser l'armure de la sécurité

Protéger l'accès au BIOS de vos PC, c'est comme fortifier les remparts d'un château médiéval, une barrière ultime contre les assaillants invisibles. Imaginez que votre entreprise soit un royaume, avec des informations cruciales et des secrets bien gardés. Eh bien, le BIOS, c'est le donjon impénétrable qui abrite ces trésors numériques.

Mettre un mot de passe dans le BIOS, c'est ériger une muraille infranchissable autour de votre forteresse numérique. C'est bien plus qu'une simple formalité de sécurité, c'est un rempart qui dissuade les malfaiteurs virtuels, les hackers voraces qui rôdent dans l'ombre du cyberespace.

Le BIOS est la porte d'entrée vers l'âme même de vos machines. Si un intrus parvient à y pénétrer sans encombre, c'est comme s'il avait les clés du royaume.

Mettre un mot de passe, c'est ajouter une couche de mystère et de complexité à cette porte.
C'est une épreuve pour les indésirables, un défi qu'ils seront bien en peine de relever.

C'est aussi une affirmation de votre souveraineté numérique. C'est dire au monde numérique :

«Ici, nous prenons la sécurité au sérieux. Nous protégeons nos actifs les plus précieux avec la même ferveur qu'un chevalier protégeant son roi.»

Alors, imaginez-vous comme le gardien de ce château numérique, le gardien qui défend vaillamment son seigneur et sa dame contre les menaces insidieuses. Protéger le BIOS avec un mot de passe, c'est endosser l'armure de la sécurité, prêt à défendre votre royaume contre les hordes de pirates informatiques avides de pillages.

En conclusion, mettre un mot de passe dans le BIOS, c'est bien plus qu'une simple précaution.
C'est un acte de bravoure numérique, une affirmation de votre engagement envers la sécurité et la protection de vos précieux actifs. Alors, hissez le drapeau de la sécurité et défendez votre forteresse numérique avec la détermination d'un chevalier en quête de justice dans le vaste monde numérique.

Notes

23
Tester les plans 1x par année (le drp doit être en conditions proche de la réalité)

Un tournoi annuel

Bien sûr, tester les plans de reprise d'activité (DRP) une fois par an est absolument essentiel dans le monde en constante évolution de la sécurité informatique. Imaginez un instant que votre entreprise soit la forteresse que vous avez bâtie avec soin, protégeant non seulement vos données vitales, mais aussi la confiance de vos clients et partenaires. Maintenant, visualisez une attaque soudaine, un assaut numérique qui menace de faire vaciller ces murs numériques.

C'est là que le plan de reprise d'activité entre en scène, comme le héros prêt à défendre votre royaume. Tester ce plan, c'est comme organiser un exercice grandeur nature pour vos troupes.

C'est s'assurer que vos chevaliers (vos équipes de sécurité) sont prêts à affronter les assaillants et à protéger les joyaux numériques de votre royaume.

En pratiquant régulièrement, vous garantissez que vos défenseurs sont alertes, qu'ils connaissent chaque recoin du terrain et qu'ils peuvent réagir rapidement et efficacement. Mais pourquoi une fois par an, pourriez-vous demander ? Eh bien, imaginez ceci comme un tournoi annuel où vos meilleurs guerriers se réunissent pour affûter leurs compétences. Les menaces évoluent, les tactiques changent, et vos défenseurs doivent être à la pointe de la technologie. Tester une fois par an vous permet de rester agile, de vous adapter aux nouvelles stratégies des cybercriminels et de vous assurer que votre forteresse numérique reste impénétrable.

De plus, réaliser ces tests dans des conditions proches de la réalité est crucial. C'est comme simuler une véritable bataille, avec tous les imprévus et les surprises que cela comporte. Vous ne pouvez pas simplement vous entraîner dans un environnement contrôlé et vous attendre à ce que tout se déroule de la même manière en situation réelle. Tester dans des conditions réalistes garantit que votre plan de reprise d'activité est prêt à faire face à n'importe quelle tempête numérique.

En fin de compte, tester votre plan de reprise d'activité une fois par an dans des conditions proches de la réalité, c'est investir dans la sécurité de votre royaume numérique.

C’est la clé pour assurer la résilience de votre entreprise face aux défis toujours changeants de la cybercriminalité. Alors, préparez-vous, fortifiez vos défenses et soyez prêt à affronter l’avenir avec confiance. Votre royaume numérique en dépend.



Notes

24
Forcer l'utilisation de dns sécurisés (1.1.1.2 And 1.0.0.2)

Les sentinelles qui protègent l'accès

Il est absolument crucial de forcer l'utilisation de DNS sécurisés tels que 1.1.1.2 et 1.0.0.2 au sein de votre entreprise, et laissez-moi vous expliquer pourquoi avec passion. Imaginez votre entreprise comme un château impénétrable, vos données précieuses comme le trésor enfoui au cœur de ses murs. Les DNS, ces gardiens invisibles, sont les sentinelles qui protègent l'accès à ce trésor. Mais, ah, l'ennemi est rusé, utilisant des artifices pour infiltrer et piller vos richesses numériques !

Maintenant, les DNS non sécurisés sont comme des gardiens endormis, faciles à tromper.
Les cybercriminels rusent, déguisés en messagers légitimes, et les gardiens somnolent laissent entrer l'intrus. Mais les DNS sécurisés, tels que 1.1.1.2 et 1.0.0.2, sont comme des guerriers intrépides, vigilants et déterminés à défendre votre forteresse numérique.

Forcer l'utilisation de ces DNS sécurisés, c'est élever une barrière infranchissable contre les attaques sournoises. C'est équiper vos gardiens de boucliers indestructibles, prêts à repousser toute tentative malveillante. C'est s'assurer que vos données sensibles sont enfermées dans un coffre-fort numérique, impénétrable et inviolable.

N'oublions pas que chaque paquet de données est une histoire, une partie de l'âme de votre entreprise. En optant pour des DNS sécurisés, vous décidez de protéger ces récits, de défendre votre histoire contre les forces obscures du cyberespace.

Alors, enflammez le courage de vos gardiens numériques ! Optez pour la sécurité, choisissez la protection, et laissez vos DNS sécurisés être les héros de cette épopée numérique. Votre entreprise mérite d'être un bastion impénétrable, une forteresse invincible dans le monde virtuel. Pour l'amour de vos données, pour la fierté de votre entreprise, forcez l'utilisation de DNS sécurisés dès aujourd'hui !

Notes

25
Sauvegarder les dossiers qui sont couramment utilisés sur les ordinateurs par les utilisateurs

Des trésors numériques

Il est absolument crucial de sauvegarder les fichiers fréquemment utilisés dans une entreprise, et laisse-moi te dire pourquoi c'est aussi vital que l'air que tu respires.

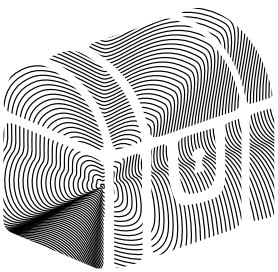
Imagine un instant que tout le travail acharné, les idées ingénieuses et les projets ambitieux de ton équipe soient soudainement engloutis dans le néant numérique.

Les fichiers auxquels tu as consacré des heures infinies de concentration et d'efforts, disparus en un instant ! Non seulement c'est déchirant, mais cela peut également signer l'arrêt de mort professionnel de toute une équipe.

Les fichiers couramment utilisés sont comme des trésors numériques, des joyaux qui donnent vie à l'essence même de ton entreprise.

Maintenant, imagine que tout cela soit balayé d'un simple clic malencontreux, d'une panne de disque dur diabolique, ou même pire, à cause d'un vilain programme malveillant qui s'infiltre sans pitié. C'est là que la sauvegarde devient le héros méconnu de l'histoire. Ces fichiers, avec leurs bits et octets soigneusement préservés, peuvent être rappelés à la vie, comme une résurrection numérique. C'est une bouée de sauvetage dans un océan numérique impitoyable.

Alors, ne laisse pas ton entreprise errer dans les ténèbres de la perte de données. Sauvegarde ces dossiers, chéris-les comme tu chérirais une précieuse relique. Parce qu'au moment où tu auras besoin de ces fichiers comme le souffle qui te maintient en vie, tu seras reconnaissant d'avoir écouté la voix de la sagesse numérique.



Notes

26
Charte d'utilisation de l'informatique avec les notions de la nlpd 2023

Les règles du jeu

Protéger notre entreprise, c'est comme veiller sur un trésor précieux. Imaginez un instant que chaque donnée soit une pièce d'or, chaque fichier un joyau irremplaçable. Maintenant, pensez à tout ce que nous partageons et stockons dans le royaume numérique de notre entreprise. C'est là que la «Charte d'utilisation de l'informatique avec les notions de la NLDP 2023» entre en scène.

Cette charte n'est pas simplement un amas de mots juridiques ennuyeux. Non, c'est notre forteresse virtuelle, notre rempart contre les menaces qui rôdent dans les recoins sombres du cyberespace.
Elle pose les règles du jeu, une stratégie élaborée pour protéger nos secrets les plus précieux.

La NLDP 2023, c'est notre bouclier, notre armure contre les intrus qui cherchent à s'infiltrer et à s'emparer de nos richesses numériques.

En respectant ces principes, nous érigeons des remparts indestructibles autour de notre forteresse numérique. Imaginez que chaque employé soit un chevalier, portant fièrement les couleurs de notre entreprise. La charte devient alors notre code d'honneur, notre serment solennel de protéger et de préserver. Elle nous guide dans les méandres du monde numérique, nous rappelant constamment que la sécurité est l'affaire de tous.

La NLDP 2023, c'est aussi notre potion magique contre les malédictions du non-respect de la vie privée. En la respectant, nous garantissons à nos collaborateurs que leurs données sont traitées avec respect et intégrité, loin des griffes voraces des sorciers malveillants du cyberespace.

En résumé, la «Charte d'utilisation de l'informatique avec les notions de la NLDP 2023» n'est pas simplement un document. C'est notre épée et notre bouclier, notre philtre magique dans le monde numérique. En l'adoptant, nous devenons les gardiens intrépides de notre trésor numérique, prêts à défendre notre royaume contre toutes les menaces qui osent se présenter.

Notes

27
Faire un business continuity plan (bcp)

La bouée de sauvetage

Bien sûr, je comprends à quel point la sécurité d'une entreprise est cruciale. Imaginez-vous dans le tumulte de l'incertitude, où les vents de l'imprévu soufflent fort, menaçant de faire chanceler tout ce que vous avez bâti avec tant d'efforts. C'est là que le Business Continuity Plan (BCP) entre en scène, comme un phare solide dans la tempête.

Dans le monde turbulent des affaires, les imprévus peuvent surgir à tout moment, tel un éclair déchirant la quiétude apparente. C'est pourquoi il est vital de se préparer, de tracer une voie sûre à suivre lorsque l'inattendu frappe à la porte de votre entreprise. Le BCP, c'est comme une armure pour votre entreprise, une armure qui la protège des flèches acérées du chaos. Il va au-delà des simples sauvegardes de données et des plans de secours ; c'est une stratégie globale qui assure la continuité de vos opérations même lorsque les fondations semblent se fissurer.

Imaginez un incendie ravageur, ou une cyberattaque vicieuse qui menace de paralyser chaque rouage de votre machine bien huilée.

Sans un BCP en place, chaque instant de paralysie est un coup direct porté à la survie de votre entreprise. Le BCP, c'est une bouée de sauvetage dans l'océan tumultueux de l'incertitude. C'est la certitude que, peu importe la force de la tempête, votre entreprise émergera indemne, prête à affronter un nouveau jour. C'est l'expression tangible de la résilience de votre organisation, une déclaration audacieuse affirmant que vous ne plierez pas devant les caprices du destin. En investissant du temps et des ressources dans l'élaboration d'un BCP, vous investissez dans la survie même de votre entreprise. C'est un acte de prudence, une démonstration de sagesse dans un monde où la prévoyance est la clé de la pérennité.

En fin de compte, le BCP n'est pas simplement une formalité administrative, c'est une promesse que vous faites à votre entreprise, à vos employés, et à vous-même. Une promesse que, quelle que soit la tempête, votre entreprise continuera à naviguer vers des horizons plus calmes et plus prospères.

Notes

28
Faire un plan en cas de désastre

Des gilets de sauvetage

Imaginez une entreprise comme un navire voguant sur des mers parfois agitées. Dans ce voyage tumultueux qu'est le monde des affaires, il est impératif d'avoir un plan solide en cas de tempête. C'est là que le plan de gestion des catastrophes entre en jeu, et laissez-moi vous expliquer pourquoi c'est plus qu'une simple formalité administrative.

Tout d'abord, c'est une question de survie.
Un navire sans bouée de sauvetage est condamné à sombrer s'il rencontre des eaux agitées. De la même manière, une entreprise sans plan de gestion des catastrophes est vulnérable face aux imprévus.
Que se passe-t-il si un incendie ravage vos locaux, si un virus informatique paralyse vos systèmes, ou si une crise économique frappe de plein fouet ? Sans plan, c'est le chaos assuré.
Ensuite, c'est une question de responsabilité envers vos équipages, vos employés.

Ils sont vos coéquipiers dans cette aventure, et vous avez la responsabilité de les protéger. Le plan de gestion des catastrophes, c'est comme un gilet de sauvetage pour eux.

Cela montre que vous avez anticipé les dangers potentiels et que vous avez mis en place des mesures pour les affronter. C'est un acte de confiance et de protection envers ceux qui contribuent à la réussite de votre entreprise.

Enfin, c'est une question de pérennité. Les entreprises qui survivent aux tempêtes sont celles qui ont su anticiper les coups durs et s'y préparer.
Un plan de gestion des catastrophes, c'est comme une boussole qui guide votre entreprise à travers les vents contraires. C'est l'assurance que même dans l'adversité, vous avez tracé une voie pour émerger plus fort et plus résilient.

En somme, créer un plan de gestion des catastrophes pour votre entreprise, c'est bien plus qu'une simple formalité administrative. C'est un acte de sagesse, de responsabilité et de prévoyance. C'est la clé qui vous permettra de naviguer avec succès à travers les mers tumultueuses des affaires, en protégeant votre équipage et en assurant la pérennité de votre navire.

Notes

29
Faire labeliser l'informatique avec le label «cybersafe» cyber-safe.Ch

Des technologies anti-tempêtes

Bien sûr, je comprends à quel point la sécurité informatique est cruciale de nos jours. Imaginez notre entreprise comme un navire voguant dans l'océan numérique, exposé aux tempêtes incessantes de cybermenaces. Le label «CyberSafe» de cyber-safe.ch est notre bouée de sauvetage, notre gage de sécurité dans ce monde virtuel tumultueux.

Faire labelliser notre informatique avec «CyberSafe» n'est pas simplement une formalité, c'est un acte de responsabilité envers notre équipage numérique. C'est comme doter notre navire des dernières technologies anti-tempêtes pour nous assurer que même les vagues les plus déchaînées de cyberattaques ne pourront nous submerger.

Ce label n'est pas qu'une simple reconnaissance ; c'est une déclaration audacieuse à tous les pirates informatiques qui pourraient envisager de nous attaquer.

C'est comme ériger des remparts virtuels, protégeant nos précieuses données et assurant la confidentialité de nos opérations. C'est notre forteresse numérique, notre rempart impénétrable face aux assauts malveillants.

En obtenant le label «CyberSafe», nous montrons à nos clients et partenaires que nous prenons leur confiance au sérieux. C'est une promesse que nous faisons, une promesse de sécurité et d'intégrité dans un monde où la moindre faille peut avoir des conséquences dévastatrices. C'est un signal fort, une déclaration d'engagement envers l'excellence dans la protection de nos actifs numériques.

Alors, faisons de notre entreprise un bastion numérique, un endroit où la sécurité est au cœur de toutes nos activités. Adoptons le label «CyberSafe» et hissons fièrement notre drapeau virtuel, symbolisant notre engagement envers la sécurité informatique. En ces temps de cybermenaces constantes, c'est une décision éclairée et émotionnellement puissante pour assurer la pérennité et la prospérité de notre entreprise dans l'océan numérique imprévisible.

Notes

30
Mettre en place un vpn permanent quand les utilisateurs sont en déplacement

Un tunnel sécurisé

Mettre en place un VPN permanent lorsque les utilisateurs sont en déplacement est tout simplement crucial pour la sécurité de l'entreprise. C'est comme ériger une forteresse impénétrable autour de nos données les plus précieuses, une barrière que même les attaquants les plus rusés auront du mal à franchir. Imaginez un instant que vos employés soient des chevaliers valeureux, voyageant à travers des terres inconnues, portant avec eux les secrets de votre royaume professionnel.

Sans un VPN permanent, c'est comme s'ils chevauchaient sans armure, exposés aux flèches perfides des pirates informatiques qui rôdent dans l'ombre du cyberespace.

Le VPN crée un tunnel sécurisé, une sorte de passage secret protégé par des enchantements numériques.

Cela signifie que même lorsque vos vaillants guerriers se connectent depuis des auberges douteuses ou des places de marché numériques, leurs communications restent cryptées, insaisissables pour les forces du mal. Songez aux données confidentielles de votre entreprise comme à des trésors jalousement gardés dans une salle des coffres numérique. Sans un VPN, c'est comme si vous laissiez la porte grande ouverte, invitants les brigands du cyberespace à se précipiter et à piller vos informations les plus sensibles.
Et n'oublions pas que dans ce monde numérique complexe, les menaces peuvent surgir de n'importe où. Les hackers sont comme des sorciers malveillants, jetant des sorts à travers les réseaux non sécurisés pour voler des informations vitales. Un VPN permanent agit comme une barrière magique, déviant leurs maléfices et protégeant ainsi l'intégrité de votre royaume numérique.

En conclusion, mettre en place un VPN permanent pour les utilisateurs en déplacement, c'est élever des remparts numériques autour de votre forteresse d'entreprise. C'est la garantie que même lorsque vos valeureux employés s'aventurent dans les contrées virtuelles les plus périlleuses, ils restent protégés, assurant ainsi la sécurité et la prospérité de votre royaume professionnel.

Notes

31
Bloquer l'accès à l'ajout de périphériques non validés par l'it

Des bêtes sauvages

Bloquer l'accès à l'ajout de périphériques non validés par l'IT est absolument crucial pour la sécurité de notre entreprise, c'est comme installer un rempart impénétrable pour protéger notre forteresse numérique contre les assauts sournois des menaces cybernétiques. Imaginez un instant que notre réseau soit une forêt enchantée, où chaque périphérique validé par l'IT est comme une créature bienveillante et familière. Ces créatures travaillent en harmonie, se comprennent et veillent sur notre domaine numérique avec bienveillance.

Maintenant, introduire un périphérique non validé, c'est comme laisser entrer une créature étrangère et potentiellement malveillante dans notre forêt jadis paisible. Cela pourrait être une bête sauvage, affamée de données sensibles et prête à semer le chaos parmi nos créatures numériques bien-aimées.

Bloquer l'accès à ces intrus, c'est ériger des remparts solides autour de notre forteresse, assurant que seuls les alliés de confiance ont le privilège de pénétrer nos défenses. C'est une mesure essentielle pour garantir que nos informations sensibles, telles que les secrets enchantés de l'entreprise, restent entre des mains dignes de confiance.

En résumé, c'est comme protéger notre royaume numérique contre les invasions malveillantes, garantissant que seuls les membres de la cour IT approuvés aient accès à notre trésor d'informations. Bloquer l'accès à l'ajout de périphériques non validés, c'est la clé pour maintenir la tranquillité et la sécurité au cœur de notre royaume numérique.



Notes

32
Le ou les sites web de l'entreprise sont sauvegardés et sécurisés

Un phénix renaissant de ses cendres

Il est absolument essentiel que les sites web de votre entreprise soient sauvegardés et sécurisés, et laissez-moi vous dire, c'est comme la fondation solide d'une forteresse médiévale ! Imaginez votre site web comme le joyau précieux au cœur de votre royaume commercial, un joyau qui mérite d'être protégé contre les forces malveillantes qui rôdent dans le cyberespace. Imaginez-vous en gardien vigilant de ce joyau, perché sur les remparts numériques de votre entreprise.

Les attaques, tels des catapultes lancées par des assaillants malveillants, peuvent venir de tous les côtés. Sans une sauvegarde fiable, vous risquez de voir ce joyau être réduit en ruines numériques, une perte déchirante qui pourrait signifier la chute de votre royaume commercial.

La sauvegarde de votre site web, c'est comme avoir une armure solide pour votre entreprise.
En cas d'attaque, vous pouvez restaurer votre site web à partir de ces sauvegardes, tel un phénix renaissant de ses cendres.

C'est une assurance, une garantie que même face aux pires scénarios numériques, votre entreprise continuera de rayonner comme un phare de confiance dans l'océan tumultueux de l'Internet.
Et parlons de sécurité! Les murs d'une forteresse sont renforcés pour décourager les assaillants, n'est-ce pas? Eh bien, la sécurité de votre site web accomplit la même mission. Des pare-feu solides, des protocoles de cryptage impénétrables et une surveillance constante sont comme les gardiens chevronnés qui veillent à ce que vos données soient aussi sûres qu'un trésor bien gardé dans les tréfonds d'un château.

Alors, chers gardiens de l'entreprise, assurez-vous que vos sites web sont protégés et sauvegardés.
C'est la clé pour préserver la splendeur de votre royaume numérique et garantir que votre entreprise continue de prospérer, défiant toutes les tempêtes numériques qui pourraient se lever à l'horizon.
Faites de votre site web une forteresse imprenable, et votre entreprise deviendra une légende dans le monde numérique!

Notes

33
Définir le temps de reprise et la quantité de données perdues (rto / rpo)

Des pages perdues

Bien sûr, définir le temps de reprise (RTO) et la quantité de données perdues (RPO) dans une entreprise, c'est comme assurer la survie d'un être cher après une tempête dévastatrice. Imaginez votre entreprise comme une maison chaleureuse, pleine de souvenirs, de projets et de rêves. Maintenant, pensez à une catastrophe soudaine qui menace de tout emporter.

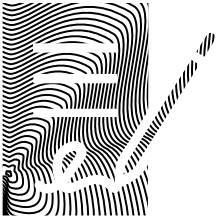
Le temps de reprise (RTO) agit comme le héros qui se précipite pour reconstruire cette maison en ruines. Il incarne la rapidité avec laquelle vous pouvez ramener la normalité, restaurer l'ordre et retrouver la chaleur de votre foyer professionnel. Plus le RTO est court, plus votre équipe peut se relever rapidement, surmonter l'adversité et rétablir la stabilité.

Quant à la quantité de données perdues (RPO), elle représente les morceaux de votre histoire professionnelle.

Chaque donnée est comme une page de livre, et le RPO détermine combien de pages peuvent être perdues avant que l'histoire ne soit irrémédiablement altérée.

Si la valeur de ces pages est inestimable, chaque seconde compte pour minimiser les pertes. En définissant clairement le RTO et le RPO, vous érigez des remparts puissants contre les tempêtes numériques. Vous garantissez que, même face à l'adversité la plus féroce, votre entreprise peut se relever, reconstruire et continuer à écrire son histoire. Ne laissez pas le chaos dicter votre récit.

Protégez votre passé, votre présent et votre avenir en fixant des objectifs clairs pour le temps de reprise et la quantité de données perdues. C'est l'assurance que votre entreprise survivra et prospérera, quelle que soit la tempête qui se profile à l'horizon.



Notes

34
Faire une assurance «cyber-risques» ex: helvetia

Un filet de sécurité financier

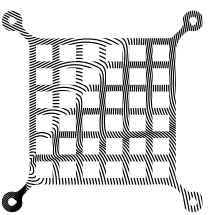
La mise en place d'une assurance «Cyber-Risques» au sein d'une entreprise est comme ériger une forteresse autour de ses précieuses données. C'est une étape cruciale, une armure moderne dans la bataille numérique qui fait rage chaque jour.

Imaginez votre entreprise comme un trésor convoité, entouré d'innombrables dangers. Les cybercriminels rôdent comme des loups affamés, cherchant à déchirer les défenses les plus faibles. C'est là que l'assurance «Cyber-Risques» entre en scène, telle une muraille impénétrable contre les attaques vicieuses.
Les menaces évoluent constamment, devenant plus intelligentes, plus furtives. Sans cette assurance, votre entreprise est comme un château sans remparts, exposée aux flèches empoisonnées des pirates informatiques. Les coûts pour réparer les dégâts d'une attaque peuvent être astronomiques, laissant votre trésorerie en lambeaux.

En optant pour une assurance «Cyber-Risques», vous créez un filet de sécurité financier. C'est votre allié dans la lutte contre l'inconnu, une bouée de sauvetage lorsque les vagues tumultueuses de la cybercriminalité menacent de submerger tout ce que vous avez construit avec tant d'efforts.

L'assurance ne se limite pas à la protection financière. Elle offre également un soutien opérationnel et une expertise, comme une main tendue pour vous relever lorsque vous trébuchez dans le labyrinthe complexe des attaques informatiques. C'est une bouffée d'air dans le monde étouffant de la sécurité, une lueur d'espoir lorsque tout semble sombre.

En somme, choisir une assurance «Cyber-Risques», c'est investir dans la pérennité de votre entreprise. C'est prendre position contre les tempêtes numériques, protégeant non seulement vos actifs financiers, mais aussi la confiance de vos clients et la réputation durement gagnée de votre marque. Alors, érigez cette forteresse digitale, car dans le monde sauvage du cyberespace, il vaut mieux être prêt à parer les coups que de pleurer sur les pertes.



Notes

Note d'auteur

LA FORTERESSE DIGITALE

Les 34 bonnes pratiques pour une gestion simple et professionnelle de votre informatique

Dans un monde imprévisible, le Business Continuity Plan (BCP) est votre bouée de sauvetage, garantissant la survie de votre entreprise face aux crises. Avec un plan de gestion des catastrophes, vous protégez votre équipe contre les imprévus majeurs, tandis que le label «CyberSafe» et un VPN sécurisé défendent vos données contre les cybermenaces.

Sauvegarder régulièrement votre site web assure sa résilience, et définir le temps de reprise (RTO) et la quantité de données perdues (RPO) vous prépare à toute adversité. Enfin, une assurance « Cyber-Risques » est le filet de sécurité qui protège vos finances contre les attaques informatiques.

Préparez-vous, sécurisez-vous, et assurez la pérennité de votre entreprise dans un océan de risques.



Préparez-vous à transformer l'incertitude en opportunité !

Javier Pose