XPERTOS IT
Your IT Booster

NEWSLETTER

Technews Juillet 2022

Sommaire

CYBER ATTACK

Le cyber-monde évolue toujours vers un endroit plus dangereux mais aussi opportuniste pour les entreprises basées sur le Web. Il existe de nouvelles cyberattaques et tendances en matière de cybersécurité que vous devez suivre pour combattre ces attaques.

Les entreprises du monde entier ont besoin d'une mise à jour sur ces dernières menaces et mesures, car les deux dernières années ont eu l'un des impacts les plus importants sur la protection des données sensibles et l'anonymat en ligne. Nous avons ce qu'il vous faut et avons rassemblé toutes les nouvelles tendances et menaces

Types des Attaques

Adoption du travail à distance et des nouvelles menaces de sécurité

le modèle de travail à distance persistera même après la pandémie avec 25 % de la main-d'œuvre des pays développés travaillant à distance. C'est certainement une amélioration car la plupart des gens pensent qu'ils sont plus productifs en travaillant à distance et cela économise des ressources pour les entreprises.

Cependant, les cybermenaces associées en raison du risque accru d'escroqueries par hameçonnage et des failles de sécurité potentielles de l'accès à distance sont certainement préoccupantes. C'est pourquoi les entreprises ayant un modèle de travail à distance doivent évaluer la structure et les politiques de leur réseau pour se préparer aux nouvelles menaces de la vie professionnelle.

Les Vulnérabilités potentielles du cloud Computing

Comme nous l'avons mentionné ci-dessus, le modèle de travail à distance et l'avancement du cloud computing offraient un moyen plus pratique de stocker et de partager des informations. Aujourd'hui, les réseaux ne dépendent plus autant du matériel ; tout peut être fait dans le cloud.

Mais ce nouveau modèle de stockage des données est potentiellement vulnérable. Bien sûr, les années nous ont appris de précieuses expériences en matière de sécurité cloud, mais la prudence reste une bonne option.

Les parties les plus vulnérables du cloud proviennent de l'utilisateur final ; les entreprises doivent toujours surveiller le cloud pour empêcher les utilisateurs malveillants, les erreurs des employés et les accès non autorisés.

Les dernières menaces de rançongiciels

Les entreprises basées sur le Web dans le monde entier souffrent quotidiennement de ransomwares. Ils étaient déjà l'une des cyberattaques les plus importantes, mais les chiffres semblent encore grimper. Nous devons mettre davantage l'accent sur les ransomwares car les dernières statistiques de cybersécurité ont montré que 79 % de toutes les actions de réponse rapide ont été déclenchées par ces attaques.
Pour éviter d'être victime d'un ransomware, opter pour les dernières tendances en matière de cybersécurité est crucial. La transition vers un modèle Zero Trust serait un excellent choix car il s'avère efficace contre les ransomwares.

Appareils mobiles menacés

Les appareils mobiles tels que les ordinateurs portables et les smartphones sont devenus une partie importante de notre vie quotidienne. Que ce soit pour le travail ou pour un usage personnel, ils sont l'un des appareils technologiques les plus utilisés de notre époque.

Nombre croissant de menaces internes

Le Swiss Cyber Institute montre que 34% des entreprises subissent chaque année des menaces internes. Apparemment, la portée de la menace est beaucoup plus grande que nous ne pouvons l'imaginer. Qu'il soit causé par des erreurs humaines ou une mauvaise utilisation, le risque de violation de données d'initiés est toujours là pour les entreprises.

Les tendances avancées en matière de cybersécurité telles que la segmentation du réseau et l'authentification multi facteur sont d'excellents moyens de prévenir de tels risques. En plus de contrôler qui peut accéder à vos réseaux privés, il est également crucial de décider à quoi les initiés peuvent accéder.

Règles de protection des données

Les menaces et attaques croissantes que nous avons mentionnées ci-dessus ont provoqué une tendance significative ; la réglementation gouvernementale. Les gouvernements du monde entier cherchent des moyens de normaliser la sécurité des réseaux pour protéger les clients et les entreprises.

Les principales réglementations telles que HIPAA, FISMA et ISO montrent la voie à suivre pour sécuriser les réseaux d'entreprise. Mais ne vous méprenez pas, il

Existe différentes normes que vous devez suivre en fonction du pays et de l'industrie.

La meilleure chose à faire ici est de trouver votre réglementation contraignante et de vous y conformer du mieux que vous pouvez. Cela permettra à la fois d'éviter les problèmes juridiques et de protéger votre réseau mieux que jamais.

Automatisation de la cybersécurité et utilisation de l'IA

Grâce aux avancées technologiques, nous disposons d'outils d'automatisation et d'IA pour aider les professionnels de l'informatique dans leurs tâches. Parcourir d'énormes quantités de données peut être un problème pour ces employés et cela peut entraîner des failles de sécurité. Après tout, l'erreur est humaine.

Mais heureusement, il existe d'excellents services qui automatisent la détection et la réponse aux menaces à l'aide de l'IA et de protocoles de sécurité contextuels. Votre équipe informatique peut grandement bénéficier de ces services en allégeant sa

Charge de travail et en éliminant les failles d'origine humaine.

Investir dans l'IA et l'automatisation pour la cybersécurité est également excellent pour réduire les coûts à long terme. Ne doutez donc pas du prix de son déploiement dans un premier temps, il vous reviendra avec un réseau plus sécurisé et moins de travail manuel.

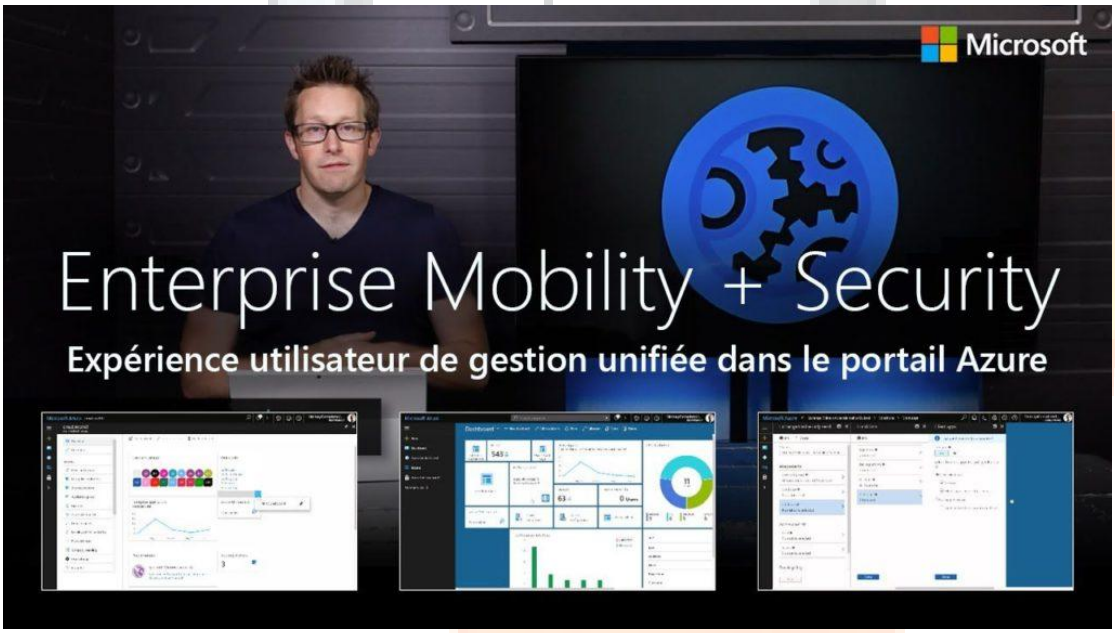
Conclusion

Assurer la cybersécurité est un processus sans fin. Il y a toujours de meilleurs services de sécurité et de plus grandes menaces. Le pire, c'est que ces menaces évoluent chaque année. Au fur et à mesure que nous

devenons plus dépendants d'Internet avec nos données personnelles, ils continueront à le faire.

C'est pourquoi les utilisateurs d'Internet, en particulier les organisations professionnelles, doivent garder un œil sur les dernières menaces et tendances. Ils peuvent mettre à jour leurs réseaux et leurs structures de sécurité en conséquence pour mieux atténuer ces risques.

CE QUI COMPOSE LA SOLUTION Microsoft EMS & SES CAPACITÉS



Microsoft EMS et ses produits renforcent les fonctionnalités de sécurité de Windows 10 et d'Office 365

Et les étendent à l'ensemble de votre environnement, y compris aux applications tierces.

Les produits Enterprise Mobility Security se déclinent comme suit :

Vous pouvez utiliser vos fichiers synchronisés directement dans l'Explorateur de fichiers et y accéder même en mode hors connexion. Dès que vous repasserez en ligne, les modifications que vous ou d'autres personnes avez apportées seront synchronisées automatiquement.

- Azure Active Directory – La solution de gestion des identités et des accès la plus fiable du marché
- Microsoft Intune – Gestion unifiée des points de terminaison mobiles, gestion des accès et protection des données dans le cloud
- Azure Information Protection – Classification, suivi, protection et chiffrement des données dans le cloud.
- Microsoft Cloud App Sécurité – Agent de sécurité d'accès au cloud assurant la détection des menaces et des risques.
- Microsoft Advanced Threat Analytics – Plateforme locale qui protège contre les cyberattaques ciblées et les menaces internes avancées.
- Azure Advanced Threat Protection – Solution hébergée dans le cloud qui permet d'identifier, de détecter et d'analyser les menaces, les compromissions et les actions malveillantes.

Capacités de Microsoft Enterprise Mobility Security

✓ GESTION DES IDENTITÉS ET DES ACCÈS DES COLLABORATEURS

L'identité permet de sécuriser les connexions entre les personnes, les appareils, les applications et les données. Renforcez votre sécurité et gagnez en productivité avec une solution d'identification unique et globale qui vous offre à la fois la flexibilité et le contrôle.

✓ PROTECTION DES INFORMATIONS SENSIBLES

Protégez vos données sensibles partout, même quand elles sont en transit ou partagées. Gagnez en visibilité et en contrôle sur l'utilisation des fichiers avec une solution de protection des informations complète et intégrée.

✓ PROTECTION CONTRE LES MENACES INTÉRIEURES ET EXTÉRIEURES

Détectez et analysez les menaces avancées, les identités compromises et les actions malveillantes au sein de vos environnements locaux et dans le cloud. Protégez votre organisation avec une intelligence intégrée adaptative.

✓ GESTION UNIFIÉE DES POINTS DE TERMINAISON

Aidez les utilisateurs à être productifs en tout lieu, tout en sécurisant les informations de l'entreprise. Les solutions de gestion flexibles et sécurisées de Microsoft EMS vous permettent d'offrir des expériences mobiles protégées sur tous vos appareils (PC, smartphones, tablettes).

✓ SÉCURITÉ D'ACCÈS AU CLOUD

Gagnez en visibilité sur vos applications et services cloud. Tirez des enseignements d'analyses sophistiqués et contrôlez le déplacement de vos données afin de pouvoir réagir aux cyber-menaces et les combattre.

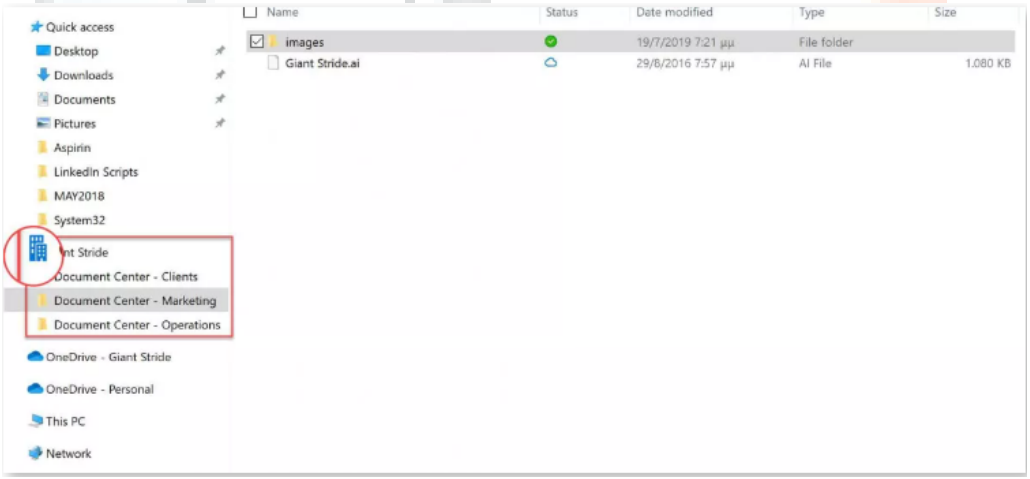
HOW TO SYNC A DOCUMENT LIBRARY WITH YOUR COMPUTER

Synchroniser votre ordinateur avec SharePoint pour Office 365

Malgré le fait que SharePoint pour Office 365 est - entre autres - un outil de gestion de documents basé sur le Web, vous avez la possibilité de synchroniser vos documents avec votre ordinateur.

Suivez ces étapes :

1- Accédez au site SharePoint.
2- Sélectionnez la bibliothèque de documents que vous souhaitez synchroniser.
3- Cliquez sur le bouton de synchronisation.
4- Si vous y êtes invité, cliquez sur "Ouvrir Microsoft OneDrive"



Travailler avec la synchronisation

Lorsque vous synchronisez vos bibliothèques de documents, vous remarquerez peut-être des icônes à côté de vos fichiers/dossiers synchronisés.

Ces icônes vous indiquent en fait l'état du fichier/dossier :

XPERTOS IT

Icon	Description
	If you see that icon, it means that the file/folder is shared with other people.
	If you see that icon, it means that the file/folder is available only online.
	If you see that icon, it means that you have tried to open that file and it became locally available.
	If you see that icon, it means that you have set the file/folder to always be available offline.
	If you see that icon, it means that the file/folder has settings that prevent it from syncing.
	If you see that icon, it means that an error occurred and the file/folder cannot be synced.

Onedrive est l'application utilisée pour synchroniser votre ordinateur avec SharePoint. Vous pouvez facilement localiser son icône de nuage bleu, carrément dans la barre des fenêtres.

L'état général de la synchronisation peut être facilement repéré si vous faites attention à l'icône elle-même, comme décrit ci-dessous :

Icon	Description
	If you see that icon, it means that the application is currently syncing.
	If you see that icon, it means that the application is in pause state. You can right click on the icon and select **resume syncing**.
	If you see that icon, it means that the application encountered an error. You can click on the icon to learn more about the problem.
	If you see that icon, it means that your account needs attention.

XPERTOS IT

Bulletin de sécurité- Juin 2022

Date de publication	Gravité	Article	Produit
14 Juin 2022	important	5014355	Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)
14 Juin 2022	important	5014553	Microsoft SQL Server 2017 for x64-based Systems (CU 29)
14 Juin 2022	important	5014353	Microsoft SQL Server 2019 for x64-based Systems (CU 16)
14 Juin 2022	important	5014164	Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)
14 Juin 2022	important	5014356	Microsoft SQL Server 2019 for x64-based Systems (GDR)

Focus Métier RSSI

RESPONSABLE DE LA SECURITE DES SYSTEMES D'INFORMATION

RSSI est l'abréviation de Responsable de la Sécurité des Systèmes d'Information. Face aux risques de plus en plus élevés auxquels est exposé le système informatique d'une entreprise, la mise en place d'une politique de sécurité de l'information devient plus que nécessaire. C'est le RSSI, responsable sécurité de l'entreprise, qui s'en charge. Le RSSI tient un rôle important au sein de la structure, car il (ou elle) possède les compétences nécessaires pour créer, gérer et pérenniser la stratégie de sécurité qui correspond le mieux aux besoins de l'entreprise. Par ailleurs, le RSSI travaille en étroite collaboration avec la direction des systèmes informatiques ou DSI.

Les qualités d'un bon RSSI

Un responsable dédié, compétent et efficace est requis pour diriger la branche sécurité et lutter contre les différentes menaces informatiques. Ces dernières sont en effet en augmentation et se diversifient de plus en plus. Cet expert doit posséder des qualités spécifiques, notamment en culture sécurité. Il s'assure également de la veille technologique appliquée au domaine informatique.

Les compétences du RSSI

Le responsable RSSI doit posséder des compétences spécifiques pour mener à bien sa mission :

- Maîtrise de la charte d'utilisation des systèmes informatiques de l'entreprise ;
- Maîtrise des différents systèmes de sécurité informatique adoptés par l'entreprise ;
- Compétences juridiques en lien avec le domaine de la sécurité informatique, notamment en ce qui concerne le RGPD.

Quel est le rôle du RSSI ?

Le responsable de la sécurité des systèmes informatiques est chargé de :

- Définir la stratégie de sécurité à adopter ;
- Mettre en œuvre la stratégie ;
- Prévention des risques, notamment à travers une bonne communication avec les collaborateurs ;
- Sensibiliser, former et responsabiliser les collaborateurs face aux menaces qui pèsent sur la sécurité informatique ;
- Identifier et protéger les données sensibles ;
- Veiller sur la sécurité des systèmes informatiques, du réseau interne et externe de l'entreprise, ainsi que des applications ;
- Veiller sur la sécurité et l'intégrité des matériels ;
- Mettre en place une stratégie de prévention contre les fuites de données ;
- Adopter un plan de reprise d'activité informatique ;
- Se former en continu.

Quelles sont les autres missions du RSSI ?

Le RSSI doit pouvoir identifier tous les aspects des risques informatiques afin de sensibiliser les collaborateurs et adopter les politiques de sécurité les plus appropriées. Il lui revient d'appliquer une stratégie qui permet de :

- Sécuriser les accès distants aux applications et données de l'entreprise, y compris au niveau des collaborateurs ;

- Sécuriser les appareils mobiles qui peuvent être des sources potentielles de pertes de données sensibles ;

- Renforcer la sécurité cloud de l'entreprise face aux cybermenaces ;

- Améliorer l'expérience des collaborateurs en mettant en place des outils spécifiques pour de meilleures performances et une meilleure productivité au travail.

Source Fiche pratiques Silicone.fr

Vous voulez interagir avec notre équipe technique ?

Rejoignez-nous à notre page Linkedin

https://www.linkedin.com/company/xpertos-group/mycompany/?viewAsMember=true

Contactez-nous

Rue de la bourse, Immeuble Zarrad Appt B21 Lac II – 1053

contact@xpertos-group.com