Le guide de cybersécurité Devolutions

Devolutions

LA CYBERSÉCURITÉ EST UN DOMAINE TRÈS LARGE, EN CONSTANTE CROISSANCE.

La cybersécurité est un domaine très large, en constante croissance. C'est pour vous aider à demeurer au fait des bonnes pratiques et vous offrir des conseils et des astuces que nous vous offrons ce guide de cybersécurité. C'est en quelque sorte une « sélection organisée » de plusieurs de nos billets de blogue. Vous n'avez qu'à cliquer sur les liens qui vous intéressent pour en savoir plus.

Nous mettrons ce guide à jour sur une base régulière. On vous suggère donc d'ajouter cette page à vos favoris et d'y revenir souvent. Si vous souhaitez qu'on couvre des sujets en particulier ou si vous souhaitez devenir un rédacteur invité qui partagera sa sagesse et son expérience avec notre communauté, n'hésitez pas à m'écrire à dsthilaire@devolutions.net.

Catégories

- **Gestion des menaces**
- **Gestion des accès**
- **Gestion des mots de passe**
- **Gestion des utilisateurs finaux**
- **Travail à distance**
- **Optimisation de la sécurité**
- **Outils**
- **Développement de carrière**
- **Statistiques**
- **Formation**

GESTION DES MENACES

Logiciel malveillant

Avant de pouvoir protéger vos appareils et votre organisation contre les attaques de logiciels malveillants, vous devez connaître votre ennemi. Découvrez six types de logiciels malveillants, ainsi que les bonnes pratiques pour rester en sécurité. Cliquez ici.

Abus de privilèges

Les utilisateurs qui disposent d'un accès privilégié à un compte reçoivent « les clés du royaume » –ou du moins les clés des étages et des pièces maîtresses du royaume – afin d'être plus productifs et efficaces dans leurs tâches quotidiennes. Malheureusement, les utilisateurs privilégiés sont également des cibles pour les pirates informatiques qui souhaitent pirater les appareils et les réseaux pour voler des données. Une enquête de Centrify a révélé que 74 % des violations de données proviennent d'une utilisation frauduleuse de comptes privilégiés. Pour découvrir quels types d'utilisateurs commettent des abus de privilèges et comment les arrêter, cliquez ici.

Logiciel espion

Les logiciels espions – également connus sous le nom de ***stalkerware*** en anglais – existent depuis un certain temps. Ils se présentent sous de nombreuses formes, du simple cookie au logiciel de surveillance complet. Quelle que soit sa forme, le logiciel espion est conçu dans un seul but : permettre au pirate informatique qui l'a installé d'apprendre quelque chose sur sa victime sans se soucier de son consentement ou de sa vie privée. Pour apprendre à vous protéger et à protéger votre entreprise contre les logiciels espions, cliquez ici.

Initié malveillant

Le monde des affaires regorge de possibilités et d'innovations. Malheureusement, il est également plein de risques et de menaces. Empêcher les initiés, qu'ils soient compromis, mécontents ou agents doubles, de violer intentionnellement vos données aidera votre entreprise à rester en sécurité. Pour en savoir plus, cliquez ici.

Initié négligent

Selon l'enquête 2019 d'Insider Data Breach commandée par Egress et menée par Opinion Matters, 79 % des responsables informatiques estiment qu'au cours des 12 derniers mois, leurs propres employés ont accidentellement mis en danger les données de l'entreprise. Ce qui est encore plus révélateur, c'est que 55 % des employés qui ont délibérément – mais pas malicieusement – partagé des données contre les règles l'ont fait parce que leur entreprise ne leur a pas fourni les outils nécessaires. Pour découvrir comment prévenir les violations de données causées par des employés négligents, cliquez ici.

Fraude en ligne

Vous êtes peut-être très familier avec les fraudes en ligne, mais qu'en est-il de vos collègues qui le sont moins? Ce qu'ils ne savent pas pourrait coûter très cher, à eux comme à l'entreprise. Pour découvrir sept fraudes en ligne célèbres que vos utilisateurs finaux doivent absolument connaître, cliquez ici.

Droits administratifs

Dans le monde hors ligne, nous ne laissons pas n'importe qui se promener dans nos bureaux à la recherche de dossiers et ouvrir les tiroirs des armoires. Nous avons un système d'accès basé sur les rôles pour garder les choses en sécurité. Par contre, dans le monde en ligne, les entreprises qui donnent à chacun des droits administratifs – généralement parce que c'est plus pratique de le faire – violent ce principe de sécurité

fondamental et mettent leurs données et leur réputation en danger. Pour découvrir quatre raisons pour lesquelles donner à tous vos employés des droits administratifs est une mauvaise idée, cliquez ici.

RDP

Le piratage de LabCorp, un des plus grands laboratoires d'analyses sanguines aux États-Unis, a soulevé des questions légitimes sur les stratégies de défense des entreprises à une époque où les cyberattaques peuvent se produire à tout moment. Bien qu'il y ait probablement de nombreux facteurs qui ont conduit à l'attaque, ça vaut la peine de comprendre pourquoi les pirates informatiques ciblent le protocole RDP (*Windows Remote Desktop Protocol*). Cliquez ici.

Sécurité des logiciels

ZipCrypto vient avec Windows, mais il ne doit jamais être utilisé, parce qu'il est complètement défectueux et relativement facile à craquer. Tout ce qu'un bon pirate doit connaitre, ce sont les 12 octets de texte brut et où ils se trouvent dans le zip (qui peuvent être facilement trouvés) afin de décrypter tout le contenu de l'archive en moins d'une minute. Pour en savoir plus sur cette vulnérabilité critique et comment y remédier, cliquez ici.

Les **téléversement de fichiers** effectués par l'utilisateur sont essentiels pour de nombreuses applications et services d'entreprise. Par exemple, le téléversement de fichiers est une fonction fondamentale des portails de soins de santé, des systèmes de gestion de contenu (CMS) et des applications de messagerie. Cependant, permettre aux utilisateurs de téléverser des fichiers comporte son lot de risques. Les pirates essaient constamment de violer les systèmes et de voler des informations en intégrant du contenu malveillant. Pour découvrir comment éviter ce type de crise avec des techniques préventives appropriées, cliquez ici.

GESTION DES ACCÈS

Gestion des accès privilégiés

La meilleure – et honnêtement la seule – solution à la menace croissante de cybersécurité consiste à passer de la réactivité à la proactivité. On ne doit plus se demander : « que devons-nous faire lorsque nous sommes piratés? », mais plutôt « puisque quelqu'un va certainement essayer de nous pirater, comment pouvons-nous renforcer nos défenses et garder une longueur d'avance sur les méchants? » La réponse : mettre en application les six éléments d'une stratégie complète de gestion des accès privilégiés (PAM) nouvelle génération. Pour découvrir comment vous y prendre, cliquez ici.

Séparation des tâches

La séparation des tâches (de l'anglais ***Segregation of Duties*** ou SoD) est une politique qui interdit à une seule personne d'être responsable de l'exécution de tâches conflictuelles. L'objectif, comme indiqué dans la norme ISO/CEI 27001, est de réduire les possibilités de manipulation ou d'utilisation abusive ou non autorisée des actifs organisationnels. Autrement dit, lorsque plusieurs personnes sont impliquées dans des tâches à caractère sensible, il y a moins de chances qu'une personne essaie d'enfreindre les règles ou que les erreurs ne soient pas détectées. Pour en savoir plus sur la mise en œuvre d'une SoD, cliquez ici.

Injection des identifiants

La réinitialisation de mots de passe est plus sûre que d'avoir le même mot de passe disponible en permanence pour plusieurs connexions. Cependant, il existe des problèmes de sécurité liés à cette façon de faire. Par exemple, les pirates pourraient potentiellement voler des mots de passe et accéder aux comptes avant qu'ils ne soient réinitialisés. Et malheureusement, les acteurs malveillants n'ont pas besoin de beaucoup de temps pour infliger de gros dégâts, y compris la création de portes dérobées pour ressaisir les comptes une fois que les mots de passe ont été réinitialisés. Pour découvrir comment l'injection des identifiants contribue à réduire cette menace, cliquez ici.

Surveillance de comptes privilégiés

Les organisations misent sur des comptes privilégiés pour accroître leur productivité et leur efficacité. Malheureusement, les pirates informatiques s'appuient également sur des comptes privilégiés vulnérables pour briser des réseaux, accéder aux systèmes critiques et voler des données confidentielles – souvent en restant incognito pendant des mois, voire des années. Un sondage mené à l'échelle mondiale par le Ponemon Institute pour IBM a révélé que le délai moyen pour détecter une violation est de 197 jours. De plus, il faut en moyenne 69 jours supplémentaires pour contenir les dommages. Pour découvrir sept types de comptes privilégiés que votre entreprise doit sécuriser et comment les surveiller afin de protéger vos données, votre réputation et vos clients, cliquez ici.

Sécurité *Zero Trust*

Introduite il y a environ dix ans par l'analyste de Forrester John Kindervag, le concept de sécurité ***Zero Trust*** est basé sur l'idée qu'on ne doit faire confiance à personne, même si elle utilise un réseau de confiance. À la place, avant d'accéder à des parties du réseau, les utilisateurs, les appareils et les applications doivent être authentifiés via des technologies comme l'authentification multifacteur, une bonne gestion des identités

et des accès, le chiffrement, l'analyse, etc. Pour découvrir les bases de la sécurité *Zero Trust* ainsi que huit bonnes pratiques, cliquez ici.

Principe du moindre privilège

Le principe du moindre privilège (POLP) est une politique selon laquelle les utilisateurs finaux n'ont que l'accès dont ils ont besoin pour effectuer leur travail – ni plus ni moins. L'objectif est de minimiser la taille de la surface d'attaque et, au bout du compte, de réduire la probabilité et la gravité d'une cyberattaque. Pour en savoir plus sur POLP et les bonnes pratiques, cliquez ici.

Gestion des identités privilégiées

Le cœur d'un système de gestion des identités privilégiées (PIM) robuste et fonctionnel consiste à déterminer qui devrait – et, tout aussi important, qui ne devrait pas – avoir un accès administratif aux systèmes critiques. Les utilisateurs ont souvent la possibilité d'accéder à des données sécurisées, de modifier les configurations, d'installer des logiciels, de modifier les comptes, etc. Pour en savoir plus sur cette approche ainsi que sur les bonnes pratiques, cliquez ici.

GESTION DE MOTS DE PASSE

Bonnes pratiques de gestion de mots de passe

Une bonne gestion des mots de passe est essentielle, mais également difficile. Pour découvrir une liste mise à jour des 10 bonnes pratiques de gestion des mots de passe qui peuvent empêcher une violation de données coûteuse et potentiellement catastrophique, cliquez ici.

Erreurs fréquentes en matière de sécurité de mots de passe

Malheureusement, les pirates identifient facilement ces erreurs et en profitent pour lancer des attaques contre les terminaux et les réseaux. Des recherches ont montré que 81 % des violations de données sont causées par des mots de passe compromis, faibles et réutilisés, tandis que 29 % de toutes les violations (quel que soit le type d'attaque) impliquent l'utilisation d'informations d'identification volées. Pour découvrir cinq erreurs courantes de sécurité des mots de passe et comment les corriger, cliquez ici.

Enregistrement des mots de passe dans les navigateurs

Comme nous le savons tous, la cybersécurité est une priorité absolue ces jours-ci, d'autant plus que les violations de données deviennent plus courantes, complexes et coûteuses. Et si vous êtes administrateur système ou que vous travaillez en SecOps ou InfoSec, vous savez également que les utilisateurs finaux sont généralement le maillon le plus faible de la chaîne de sécurité. Malheureusement, les fonctionnalités d'enregistrement de mots de passe basées sur le navigateur font généralement partie du problème. Pour découvrir pourquoi l'enregistrement des mots de passe dans les navigateurs est une mauvaise idée, cliquez ici.

Bonnes politiques de gestion de mots de passe

Les violations de données se produisent tout le temps, tant dans les grandes entreprises que dans les PME. Les experts considèrent d'ailleurs ces dernières comme un ground zero pour la cybercriminalité. C'est pourquoi l'élaboration de bonnes politiques de gestion des mots de passe est essentielle pour les entreprises de toutes tailles. Toutefois, l'élaboration de telles politiques n'est pas une finalité. Elles doivent être adoptées et appliquées. Pour découvrir cinq conseils pour informer vos utilisateurs sur les bonnes pratiques de gestion de mots de passe, cliquez ici.

GESTION DES UTILISATEURS FINAUX

Gestion de la fatigue liée à la sécurité

Les utilisateurs finaux ont toujours été (et seront toujours) le maillon le plus faible de la chaîne de sécurité informatique. Cette vulnérabilité est aggravée par une condition appelée « fatigue sécuritaire », que le *National Institute of Standards and Technology* (NIST) décrit comme « une lassitude ou une réticence à faire face à la sécurité informatique ». Pour découvrir comment faire face à cette menace particulièrement dangereuse, cliquez ici.

Achats en ligne sécurisés

Nous aimons tous les achats en ligne. Cependant, nous ne sommes pas les seuls. Les pirates les aiment aussi, parce que ça leur donne une excellente occasion de pirater des comptes, de déployer des logiciels malveillants et de voler des données confidentielles, notamment des informations de carte de paiement et de compte bancaire. Pour découvrir six conseils pour des achats en ligne plus sécuritaires, cliquez ici.

Utilisation sécuritaire des médias sociaux

Ironiquement, ce qui rend les médias sociaux si populaires est aussi ce qui les rend si dangereux : la croyance que les gens communiquent avec des personnes qu'ils connaissent – ou du moins, avec des gens qui n'essaieront pas de pirater leur appareil et de voler leur identité. Comme le souligne le *New York Times*, « l'erreur humaine qui pousse les gens à cliquer sur un lien qui leur est envoyé dans un courriel est exponentiellement plus importante sur les médias sociaux, parce que les gens se considèrent entre amis ». Pour découvrir les bonnes pratiques pour assurer la sécurité sur les médias sociaux, cliquez ici.

Gestion des mots de passe par les employés

Les employés qui peuvent « se gérer eux-mêmes » sont très appréciés. Après tout, personne ne veut (ou ne devrait vouloir) microgérer tout ce qu'un employé fait. La microgestion est non seulement lassante pour toutes les personnes impliquées, mais elle est inefficace et coûteuse. Cependant, certaines tâches ne devraient pas être attribuées aux employés, quel que soit leur niveau de compétence et de fiabilité. Sur le haut de la liste se trouve la gestion des mots de passe. Pour découvrir pourquoi c'est une si grosse erreur de laisser les employés gérer les mots de passe, cliquez ici.

Intégration des employés

L'ajout d'un nouveau membre à l'équipe est excitant et il est toujours agréable de dire « bienvenue à bord » en organisant un déjeuner d'équipe ou en regardant une vidéo d'orientation. Cependant, certaines choses doivent être faites avant l'arrivée d'un nouvel employé. Pour découvrir trois tâches clés de cybersécurité à garder à l'esprit, cliquez ici.

Départ des employés

Pour toutes sortes de raisons, le roulement d'employés fait partie de la vie. Même les entreprises qui se retrouvent sur les listes des « meilleurs employeurs » comme Google et Costco doivent être préparées au départ d'employés. Pour découvrir cinq tâches clés de cybersécurité, cliquez ici.

TRAVAIL À DISTANCE

Protection des données à la maison

Nous savons tous que la protection des données au travail est une priorité, parce qu'une violation peut entraîner une perte de clients, une atteinte à la réputation, des coûts d'enquête et de réparation, et peut-

être même des poursuites, des amendes et des sanctions. Aussi effrayant que tout ça puisse paraître, il existe des moyens de réduire les risques de piratage, comme l'utilisation d'un outil de gestion de mots de passe solide et fiable plutôt qu'un chiffrier Excel et des ***Post-it***. Pour découvrir comment protéger vos données à la maison, cliquez ici.

Sécurité des travailleurs à distance

Auparavant, les travailleurs à distance – qu'on appelait généralement des télétravailleurs – étaient des exceptions qui suscitaient l'envie chez ceux qui devaient faire chaque jour un trajet interminable vers le bureau où ils s'enfermaient de 9h à 17h dans un cubicule sans fenêtres. La situation est radicalement différente aujourd'hui. Les travailleurs à distance ne sont plus seulement une pièce du casse-tête de la main-d'œuvre, ils sont devenus la pièce maîtresse. Pour découvrir 10 conseils pour aider les travailleurs à distance à rester en sécurité, cliquez ici.

Renforcement du réseau sans fil domestique

Si vous pensez que votre réseau sans fil à domicile est de facto sécuritaire, détrompez-vous! Au contraire, il contient plusieurs vulnérabilités par défaut qui pourraient conduire à une violation de données coûteuse et stressante. De plus, les pirates pourraient utiliser des informations volées pour tenter de pénétrer dans le réseau de votre entreprise. Pour découvrir neuf conseils pour rendre votre réseau sans fil à domicile plus sécuritaire, cliquez ici.

OPTIMISATION DE LA SÉCURITÉ

Optimisation de la sécurité des données dans AWS

Bien qu'Amazon dispose d'une expertise et d'une infrastructure en matière de sécurité, vous êtes ultimement responsable de la sécurité de vos données. Diverses mesures sont nécessaires pour protéger vos données contre les cybercriminels, pour se conformer aux exigences réglementaires et pour garder vos informations hors de danger. Pour découvrir le modèle AWS de responsabilité partagée en matière de sécurité des données, ainsi que les bonnes pratiques pour vous aider à maximiser la sécurité de vos données sur AWS, cliquez ici.

Optimisation de la sécurité du nuage

Les outils infonuagiques permettent de connecter des systèmes et de générer des informations interfonctionnelles. Cependant, comme les applications génèrent des données sensibles, les protocoles de

sécurité sont hyper importants. Pour découvrir les bonnes pratiques pour sécuriser les données dans le nuage, cliquez ici.

Optimisation de la sécurité des fichiers

De nos jours, il ne suffit pas de sécuriser le périmètre de votre organisation. Vous devez penser au-delà des murs de votre entreprise en tenant compte de la manière dont les travailleurs à distance, les partenaires et les fournisseurs accèdent à vos systèmes et données. Cela implique de s'assurer que les fichiers sensibles sont toujours sous votre contrôle. Pour découvrir par où commencer en ce qui a trait à la sécurité des fichiers, cliquez ici.

Élaboration d'une politique de cybersécurité

Le meilleur moyen de garantir la protection des informations importantes est d'avoir une politique de cybersécurité exhaustive. C'est la première étape pour vous s'assurer que votre entreprise respecte les lois nationales et internationales et stocke les données correctement. Pour découvrir des conseils fondamentaux qui vous aideront à développer une politique de cybersécurité, cliquez ici.

OUTILS

Détection et réponse sur les terminaux (EDR)

La sécurité EDR (de l'anglais ***Endpoint Detection and Response***) fournit aux entreprises les moyens de surveiller, détecter et répondre aux menaces des terminaux. Grâce à l'application de solutions et de bonnes pratiques EDR, les entreprises peuvent observer plus facilement ce qui se passe sur les terminaux. EDR fournit également aux organisations les outils nécessaires pour protéger le réseau contre les menaces entrantes. Pour en savoir plus sur les menaces des terminaux et comment la technologie EDR peut assurer la sécurité de votre personnel et de votre entreprise, cliquez ici.

Outils de sécurité essentiels

Nous savons tous que les fuites de données sont en augmentation. Ça signifie que le QI des utilisateurs en matière de cybersécurité augmente, non? Pourtant, ce n'est pas le cas! Selon une enquête du Pew Research Center, la majorité des utilisateurs ne connaissent pas certains sujets, termes et concepts d'importance majeure en matière de cybersécurité. Pour combler ce manque de connaissances, découvrez quatre outils de sécurité que tous les utilisateurs doivent connaître. Cliquez ici.

DÉVELOPPEMENT DE CARRIÈRE

Postes en demande

Selon une enquête de Trend Micro, près de la moitié de toutes les organisations ne disposent actuellement pas des spécialistes en cybersécurité dont elles ont besoin. Et selon une étude de Gartner, le nombre de postes de sécurité informatique non pourvus devrait atteindre 1,5 million d'ici la fin de 2020. Pour découvrir six postes que les entreprises ont du mal à remplir, cliquez ici.

Meilleures certifications

Si vous envisagez de faire progresser votre carrière dans le domaine de la cybersécurité, faites preuve de patience, parce que vos compétences continueront d'être en demande. Le ***Bureau of Labor Statistics*** des États-Unis a estimé un taux de croissance de 37 % pour les emplois en cybersécurité (et autres services de sécurité de l'information) entre 2012 et 2022. Pour découvrir sept certifications populaires et respectées qui pourraient lancer ou améliorer votre carrière dans le domaine de la cybersécurité, cliquez ici.

Pénurie de main-d'oeuvre qualifiée en cybersécurité

Un récent sondage de SANS confirme ce que les experts en cybersécurité savent depuis des lustres : il y a une pénurie de main-d'oeuvre qualifiée en cybersécurité, qui s'aggrave de jour en jour. Pour en savoir plus sur les lacunes en ce qui concerne les connaissances en cybersécurité, cliquez ici.

STATISTIQUES

Statistiques de cybersécurité

Oubliez les ***script kiddies*** du passé qui tentent de détruire des machines et de faire des ravages. Les cybercriminels d'aujourd'hui sont sophistiqués, implacables et bien financés. Pour découvrir 20 statistiques sur la cybercriminalité qui illustrent à quel point la situation est catastrophique et pourquoi la sécurité doit être la priorité numéro un, cliquez ici.

FORMATION

Plateforme de formation en cybersécurité

Une plateforme de formation en cybersécurité est un portail en ligne qui fournit aux employés une formation

à leur rythme, pratique et basée sur leurs compétences en matière de détection et d'atténuation des menaces, dans un environnement simulé en direct et dynamique. Pour en savoir plus sur ces plateformes et pourquoi elles sont des investissements judicieux (et certains diraient essentiels) pour toutes les entreprises, y compris les PME, cliquez ici.

Formation sur la sensibilisation à la sécurité

Bien que de nombreux métiers soient pris en charge par l'automatisation et la technologie, les entreprises ont encore besoin d'humains pour s'occuper de la plupart des tâches et des interactions avec les clients. Les tâches simples et répétitives sont automatisées, mais les décisions clés nécessitent toujours des personnes. Ces tâches effectuées par des personnes sont constamment ciblées par les pirates. Pour se défendre contre une grande variété de cyberattaques, une formation de sensibilisation à la sécurité est essentielle. Pour en savoir plus, cliquez ici.