Cyber-résilience en entreprise

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Cyber-résilience en entreprise : enjeux, référentiels et bonnes pratiques / [Sébastien Déon]

A pour autre édition sur un support différent : Cyber-résilience en entreprise enjeux, référentiels et bonnes pratiques Sébastien Deon 2e édition 2023 St-Herblain Editions ENI Epsilon 978-2-409-04145-7

Auteur(s) : Déon, Sébastien (19..-....)

Mention d'édition : 2e édition

Publication : St-Herblain : Éditions ENI

Date de copyright : C 2023

Description matérielle : 1 volume (576 pages) : illustrations, couverture illustrée en couleur ; 22 cm

Collection : Epsilon 1960-3444

ISBN : 978-2-409-04144-0

EAN : 9782409041440

Appartient à la collection : Epsilon (Saint-Herblain) 1960-3444

Classification décimale Dewey : 658.478

Note sur la publication, la production, etc. : La graphie correcte du lieu d'édition est : Saint-Herblain

Note sur les bibliographies et les index : Index

Résumé ou extrait : "Cette seconde édition du livre sur la cyber-résilience en entreprise est destinée aux personnes en charge de mettre en oeuvre la sécurité numérique au sein des entreprises (DSI, RSSI, Directeur Cybersécurité, experts et consultants...) qui souhaitent comprendre les enjeux et contraintes de la cybersécurité et qui souhaitent s'impliquer dans l'amélioration continue de la sécurité des Systèmes d'information. Il est un véritable guide pour la mise en oeuvre de la cyber-résilience des systèmes d'information reposant sur quatre dimensions : cyber-prévention, cyber-détection, cyber-protection et cyber-remédiation. Avec une approche pragmatique et progressive, l'auteur expose les enjeux et présente

les principaux référentiels et les différentes réglementations en vigueur (NIST CSF, RGPD, ITIL, SecNumCloud, ISO27k, ISO 22031, ISO 20000, HDS, NIS/2, DSA, DMA, DGA, EUCS). Il fournit ensuite une explication détaillée d'une analyse de risques réalisée avec la méthode EBIOS avant de transmettre au lecteur des bonnes pratiques sur la sécurisation des SI et des workloads dans le cloud public Azure. La souveraineté numérique et le nouveau paysage IT sont largement abordés afin d'ancrer la réflexion cyber dans un contexte de protectionnisme européen, ainsi que la sécurité de données qui nécessite gouvernance et outillage sans failles. Le recours à la sauvegarde externalisée et aux PRA/PCA avec une nouvelle approche de Resilience as a Service est explicité ainsi que la proposition de référentiel sur la sécurité applicative, le fonctionnement et le contenu du SOC (Security Operations Center) idéal ou encore la présentation du contexte cyber dans le secteur de la santé. Deux nouveaux chapitres viennent compléter le dispositif de cyber-résilience à 360° avec l'implémentation d'un système de management de la sécurité de l'information (SMSI) et la cyber-assurance. Pour finir, un chapitre complet est dédié à la présentation d'un exemple permettant de faire valoir au lecteur les bons réflexes à adopter pour l'hébergement de données de santé. Des exemples d'implémentation technique de logiciels open source sont également détaillés en annexe, notamment avec la solution de détection d'intrusions Wazuh et le scanner de vulnérabilités OpenVAS."

Sujet - Nom commun : Systèmes informatiques -- Mesures de sûreté
Protection de l'information (informatique)
Entreprises -- Systèmes d'information