La réponse d'incident

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : La réponse d'incident : analyser et réagir face à une cyberattaque / Adrien Voisin, Guillerme Duvillié

Auteur(s) : Voisin, Adrien (19..-....)

Autre(s) auteur(s) : Duvillié, Guillerme (1989-....)

Publication : Louvain-la-Neuve : De Boeck Supérieur, DL 2026

Description matérielle : 1 volume (357 pages) : schémas, graphiques, couverture illustrée en couleurs ; 24 cm

Collection : Informatique

ISBN : 978-2-8073-6979-5

EAN : 9782807369795

Appartient à la collection : Informatique (Louvain-la-Neuve) 2684-2475

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Bibliographie pages 341-342

Résumé ou extrait : Sécuriser son infrastructure face aux cyberattaques n'est plus suffisant. Il faut se préparer au pire. A la suite d'une cyberattaque, les entreprises ou les institutions publiques doivent se redresser. Pour cela, il est avant tout nécessaire de comprendre ce qui s'est passé. Qui les a attaquées et pourquoi ? Quelles failles techniques ou humaines ont été exploitées pour prendre le contrôle de leur infrastructure ? Quelles données ont été exfiltrées ? L'objectif de ce livre est de montrer comment il est possible, à partir d'une masse d'informations, de trouver les éléments importants qui permettront de comprendre une attaque et de potentiellement récupérer des données compromises. Pour rencontrer ces objectifs, l'ouvrage s'articule autour de trois parties qui répondent respectivement aux questions : "Quelles preuves récolter ? Comment les récolter ? Comment les analyser ?" Ce livre propose une approche innovante dans laquelle le lecteur suivra une enquête à travers un scénario réaliste de cyberattaque. Le lecteur sera également invité à mener lui-même cette analyse grâce aux différents exercices et ressources mis à disposition par les auteurs. De plus, ce livre est accompagné de recommandations de lectures

supplémentaires afin d'approfondir certaines thématiques.

Sujet - Nom commun : Cyberterrorisme
Cybercriminalité
Systèmes informatiques -- Mesures de sûreté
Cyberdéfense