Cybersécurité des infrastructures critiques

Appliquer et mettre en œuvre la directive NIS2

Étienne de Séréville
Officier central de sécurité,
officier de réserve Expert Cyber,
enseignant à l'Institut Polytechnique de Paris

DUNOD

Édition : Matthieu Daniel et Aleksandra Czarnecka
Direction et conception graphiques de la couverture :
Nicolas Wiel – Elizabeth Riba (graphiste)
Mise en page : Kepler SI

© Dunod, 2025
11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-089047-7

TABLE DES MATIÈRES

AVANT-PROPOS

Mon intention en écrivant cet ouvrage est de partager des pratiques de cybersécurité issues d'expériences en réponse à des problématiques régulièrement rencontrées au sein d'entités. Elle s'inscrit dans la perspective de l'application en 2024 de la directive européenne Network Information Security dite NIS2. Celle-ci va concerner un nombre important d'entités essentielles et surtout importantes, françaises et européennes. Le but est d'assurer dans le temps un niveau de cybersécurité élevé et commun dans l'Union européenne.

Chaque chapitre aborde un aspect spécifique de la cybersécurité des systèmes d'information supportant les infrastructures critiques. Ils traitent de leur périmètre et de leur écosystème, de leurs vulnérabilités, des menaces potentielles et de leurs risques. Puis, ils abordent les mesures de cybersécurité à mettre en œuvre pour assurer une gouvernance efficace, une protection robuste, une détection précoce des incidents et une résilience face aux crises de cybersécurité.

Cet ouvrage propose également d'explorer des tendances futures en matière de cybersécurité. Cela permet d'anticiper les risques engendrés par les évolutions technologiques et les nouvelles menaces, afin de permettre aux acteurs concernés de se préparer aux défis à venir.

À travers cette initiative, je souhaite fournir aux dirigeants d'entités, aux professionnels de la cybersécurité, aux décideurs et aux parties prenantes, des connaissances et des outils pour renforcer la cybersécurité de leurs systèmes d'information. Les étudiants trouveront aussi comment parfaire leurs connaissances pour faire face aux cybermenaces.

Cet ouvrage est une contribution pour renforcer la résilience de notre société numérisée.

« Je ne saurai prévoir mais je saurai fonder. Car l'avenir on le bâtit »,

Antoine de Saint-Exupéry, *Citadelle*, XX.

ÉDITORIAUX

1. ÉDITORIAL DE NUMEUM

« La cybersécurité est un enjeu stratégique majeur pour l'ensemble des acteurs économiques et ne peut plus, aujourd'hui, être ignorée par les dirigeants d'entreprises. En 2024, une entreprise sur deux déclarait avoir été victime d'une cyberattaque (baromètre du CESIN 2024). Dans ce contexte de massification et de sophistication des attaques, il devient essentiel de renforcer la maturité de nos entreprises en matière de cybersécurité. Des réglementations européennes ambitieuses mais nécessaires comme NIS2 vont en ce sens. Elles posent un cadre de confiance commun, indispensable au développement économique et à l'innovation.

Chez Numeum, nous sommes convaincus que ces réglementations ne doivent pas être perçues comme des contraintes mais comme des opportunités. Pour que le numérique soit un moteur d'innovation et de compétitivité à l'échelle européenne, il est impératif que ce numérique soit de confiance. La cybersécurité joue donc ici un rôle clé.

Nous croyons que NIS2 va faire de la cybersécurité un réflexe collectif et va instaurer une véritable culture de la cybersécurité partagée par l'ensemble des acteurs économiques.

Pour ce faire, il est indispensable que NIS2 soit un succès opérationnel. C'est en jouant collectif, avec les entreprises, les institutions et les territoires, que nous relèverons ce défi commun. L'ouvrage que vous tenez entre les mains contribue pleinement à cet objectif en vous accompagnant dans la mise en place de mesures de cybersécurité sur vos SI et donc dans votre mise en conformité avec NIS2.

Je vous souhaite bonne lecture. »

Véronique Torner, présidente de Numeum

numeum

2. ÉDITORIAL DE L'INSTITUT POLYTECHNIQUE DE PARIS

« Nos vies sont tellement entrelacées avec le numérique que nous avons tous une conscience plus ou moins aigüe de l'importance de la cybersécurité.

Les exemples récents d'hôpitaux rançonnés ont frappé les imaginations. Mais, si nous ne sommes pas des spécialistes du sujet, nous ignorons la variété et la sophistication des menaces, et encore plus la nécessaire complexité des contre-mesures à construire. L'enseignement supérieur et la recherche sont doublement concernés. D'abord parce que leurs établissements sont des organisations qui non seulement communiquent largement en interne et avec l'extérieur par des moyens électroniques, mais aussi manipulent et échangent un grand nombre de données, de celles touchant à la pédagogie et aux étudiants à celles, massives, issues de la recherche. En tant que telles, elles sont des cibles faciles, on l'a vu récemment à l'université Paris-Saclay. Ensuite parce qu'elles ont la capacité et le devoir d'élaborer et de transmettre le savoir le plus avancé sur la question.

Ce livre, basé sur des enseignements dispensés à l'Institut Polytechnique de Paris et nourri de très nombreux exemples d'attaques réelles, éclaire un paysage touffu et en pleine évolution.

L'utilité et la pertinence de cette démarche ne font pas de doute. »

Thierry Coulhon, professeur et président
du directoire de l'Institut Polytechnique de Paris

INSTITUT POLYTECHNIQUE DE PARIS

ÉTAT D'URGENCE NATIONAL !

État d'urgence national au Costa Rica à la suite de cyberattaques massives avec rebond, 2022

Le 17 avril 2022, une cyberattaque par un ransomware de la famille du malware TrickBot a commencé contre une trentaine d'institutions du gouvernement du Costa Rica. Il utilisait des techniques d'obscurcissement du code et du chiffrement AES-256 et RSA-2048. Il exploitait les vulnérabilités CVE-2022-22947 et CVE-2022-22954 (exécution de code à distance dans VMware Workspace ONE Access and Identity Manager). L'attaque a conduit aussi à des défacements de sites Internet, d'installation de portes dérobées et des vols de fichiers. L'accès illicite a été réalisé à l'aide d'informations d'identification compromises suite à un mail piégé. Puis, l'attaque s'est poursuivie par des actions de latéralisation conduisant à une large diffusion sur les systèmes des institutions interconnectées. Des actions de contrôle-commande à distance (C2) ont permis d'installer le malware sur de nombreux équipements et de faire fuiter les données. Un message sur le forum du groupe Conti a fait état du piratage d'un téraoctet de données.

Le groupe cybercriminel Conti a revendiqué cette attaque et a exigé une rançon de 10 millions de dollars contre la non-divulgation d'informations sur les citoyens et les entreprises. En guise de preuve, le groupe a publié, le 20 avril, 5 Go d'informations volées au ministère des Finances.

L'attaque s'est ensuite prolongée par des dénis de services numériques, du hameçonnage (*phishing*) et des tentatives d'intrusion sur les ports d'accès distants, pour d'autres administrations, des municipalités et des entreprises privés du pays.

Une nouvelle attaque par ransomware a été menée le 31 mai par le groupe Hive Ransomware, demandant 5 millions de dollars en bitcoins, contre la Caisse de sécurité sociale. Il a obligé l'institution à désactiver tous ses systèmes critiques contenant les informations médicales des patients et les frais d'assurance de la population. Plus de 100 établissements hospitaliers et laboratoires ont aussi été touchés, conduisant à l'arrêt immédiat de nombreux systèmes critiques, impactant plus de 800 serveurs et 9 000 ordinateurs d'utilisateurs finaux. Le dossier de santé numérique, connecté avec le système de collecte centralisé, a été touché. Le travail hospitalier s'est poursuivi en mode dégradé suivant un plan d'urgence avec papier et crayons.

Le président Rodrigo Chaves Robles a décrété l'état d'urgence nationale le 8 mai 2022. Considérant cette attaque comme un acte de terrorisme, il a catégoriquement refusé le paiement de rançons. Des dizaines de travailleurs sont descendus dans la rue pour protester contre le paiement inférieur à ce qui leur était dû, à cause de l'impossibilité d'actualiser les salaires. Pour gérer cette crise, le Costa Rica a dû faire appel à l'assistance technique de fournisseur comme Microsoft et de services étatiques spécialisés. À partir du 11 juin, les systèmes ont commencé à être restaurés et remis en service. Les systèmes informatiques arrêtés ont été nettoyés et restaurés, causant des pertes estimées à 30 millions de dollars par jour.

Avec le développement d'Internet, des smartphones, de l'informatique en nuage (*cloud computing*) et de l'intelligence artificielle entre autres, les technologies numériques ou de l'information et de la communication (TIC, ou ICT, Information and Communication Technologies) n'ont cessé d'être adoptées dans de nombreuses activités. Du fait de capacités de collecte massive, de calcul rapide, de stockage et d'échange de données toujours croissants, les technologies numériques ont été intégrées dans la gestion et le pilotage de la plupart des infrastructures industrielles et de services de nos sociétés contemporaines.

Des secteurs tels que la santé, l'énergie, les transports, la finance, les télécommunications, les services publics et autres industries critiques dépendent de technologies numériques pour assurer des services continus et fiables. Les systèmes d'information de services essentiels peuvent inclure des bases de données sensibles, comme personnelles, des réseaux de communication cruciaux (terrestres, sous-marins et satellitaires), des infrastructures de paiement, des systèmes de contrôle industriel, et d'autres composants importants pour le fonctionnement nominal d'une entité.

Cependant, cette révolution numérique a également engendré de nouveaux défis techniques : dépendance, fiabilité, sécurité. Ainsi, les menaces liées à la cybersécurité sont devenues une préoccupation majeure. Les acteurs malveillants cherchent à saboter les systèmes, voler les données ou manipuler les informations. Ils agissent par idéologie, malveillance ou appât du gain par exemple.

Annulation d'élection en Roumanie, 2024

En décembre 2024, la Roumanie a annulé le premier tour de son élection présidentielle en raison d'une manipulation de l'information via TikTok. La Cour constitutionnelle roumaine a invalidé le scrutin après avoir constaté des ingérences étrangères, notamment russes, visant à promouvoir un candidat nationaliste. Les services de renseignement ont identifié des comptes suspects et des influenceurs rémunérés diffusant massivement des contenus en faveur du candidat, exploitant les algorithmes de TikTok pour amplifier leur lectorat. Cette situation a mis en lumière la vulnérabilité des processus électoraux face aux manipulations sur les réseaux sociaux. L'Union européenne a réagi en invoquant le Digital Services Act (DSA), exigeant de TikTok la conservation des données liées aux élections pour une analyse approfondie.

Dans ce contexte de dépendance et de risques de cybersécurité, le législateur impose des obligations de gouvernance, de protection, de défense et de résilience des systèmes d'information critiques. D'importance vitale ou essentiels, les systèmes d'information essentiels et importants sont essentiels pour le fonctionnement normal des infrastructures critiques d'une entité, entreprise, administration ou association. Et ce, pour leur pilotage et la gestion de leur maintien en condition opérationnelle au niveau de fonctionnement attendu.