enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

Attaques d'applications web

Paysage des menaces de l'ENISA

Aperçu

Les applications et technologies web sont devenues un élément central de l'internet en adoptant différents usages et fonctionnalités. L'augmentation de la complexité des applications web et la généralisation de leurs services créent des difficultés pour les protéger contre des menaces aux motivations diverses, allant du préjudice financier à l'atteinte à la réputation, en passant par le vol d'informations critiques ou personnelles.[1] Les services et applications web dépendent principalement de bases de données servant à stocker ou à fournir les informations requises. Parmi les exemples bien connus, citons les attaques de type «SQL injection» (SQLi) qui constituent les menaces les plus courantes contre ces services. Les attaques de type «cross-site scripting» (XSS) en sont un autre exemple. Dans ce type d'attaque, l'acteur malveillant utilise abusivement les faiblesses des formulaires ou d'autres fonctionnalités de saisie des applications web pour mener à d'autres dispositifs malveillants, comme le fait d'être redirigé vers un site web malveillant.[2]

Alors que les organisations deviennent de plus en plus compétentes pour développer une automatisation plus cohérente du cycle de vie de leurs applications web, elles exigent désormais que la sécurité soit l'élément primordial de leur offre et au centre de leurs priorités. Cette introduction d'environnements complexes favorise l'adoption de nouveaux services, comme les interfaces de programmation d'applications (API - *Application Programming Interfaces*). Les API, qui créent de nouvelles problématiques pour la sécurité des applications web, peuvent nécessiter d'autres de mesures de prévention et de détection. Ainsi, environ 80 % des organisations utilisant des API ont déployé des contrôles sur leur trafic entrant.[3] Dans cette section, nous passerons en revue le paysage des menaces des applications web en 2019.

_Tendances

20 %_ des entreprises et organisations ont signalé quotidiennement des attaques par déni de service distribué sur leurs services d'application[5]
La technique la plus utilisée a été le dépassement de la mémoire tampon (24 %). Parmi les autres techniques fréquemment utilisées, on trouve celles de type HTTP Flood (23 %), de réduction des ressources (23 %), HTTPS Flood (21 %) et Low Slow (21 %).

63 %_ des personnes interrogées dans le cadre de l'enquête CyberEdge utilisent un pare-feu applicatif web (WAF - *Web Application Firewall*)
27,5 % prévoient de déployer cette technologie et 9,5 % n'ont pas de tels projets.[15]

52 %_ d'augmentation du nombre d'attaques d'applications web en 2019 par rapport à 2018
Selon un chercheur en sécurité, le nombre d'attaques d'applications web est d'abord resté quasiment similaire à celui de 2018 avant de subir une forte hausse plus tard dans l'année.[4]

84 %_ des vulnérabilités observées dans les applications web étaient dues à des erreurs de configuration de la sécurité
Viennent ensuite les vulnérabilités de type «cross-site scripting» (53 %) et, curieusement, de type «broken authentication» (45 %).[9]

Chaîne de frappe

Étape du processus d'attaque

Ampleur de l'objectif

Installation

Commande et contrôle

Actions vis-à-vis des objectifs

Mis au point par Lockheed Martin, le modèle de Cyber Kill Chain® s'inspire d'un concept militaire lié à la structure d'une attaque. Pour étudier un vecteur d'attaque en particulier, utilisez cette chaîne de frappe schématisée pour représenter chaque étape du processus puis référencer les outils, les techniques et les procédures utilisés par l'attaquant.

EN SAVOIR PLUS

Description

_Une meilleure collaboration entre la sécurité des applications et le développement des applications

Selon l'enquête menée par un chercheur en sécurité[5], l'un des facteurs contribuant à l'inefficacité de cette sécurité pourrait s'expliquer par le processus décisionnel relatif à la propriété des outils de sécurité. Cette enquête a exposé les points de vue des principaux influenceurs dans ce domaine, à savoir les dirigeants et les propriétaires d'entreprises informatiques, mais pas ceux des responsables de la sécurité des systèmes d'information (RSSI).

_Importance croissante des interfaces de programmation d'applications (API)

Les API ne sont pas une nouveauté dans l'architecture des applications web; en outre, leur utilisation largement acceptée réintroduit les risques existants et leur probabilité d'exploitation en raison de l'élargissement du paysage des menaces. En conséquence, l'*Open Web Application Security Project* (OWASP) a publié la liste des dix principales mesures de sécurité dédiées aux API[6], permettant d'établir des priorités afin de garantir cette capacité dans l'architecture des applications web. Les attaques des API PHP illustrent cette menace; selon un autre chercheur en sécurité, 87 % de l'analyse du trafic des API consistait à rechercher des API PHP disponibles.[7]

_Échecs d'autorisation et d'authentification

Ils sont généralement la principale cause permettant aux acteurs malveillants d'accéder à des informations critiques (par ex., la violation de données de Fast Retailing[8]). Selon un chercheur en sécurité, les violations de données critiques représentent la deuxième menace la plus importante pour la sécurité des applications web.[9]

L’injection SQL (SQLi): une tendance à la hausse

Une étude récente sur la sécurité a révélé que deux tiers des attaques d’applications web impliquaient des injections SQL (SQLi). Si les autres vecteurs d’attaque des applications web sont restés stables ou se développent, les attaques par injection SQL ont continué à croître fortement et se sont particulièrement intensifiées pendant la période des fêtes de fin d’année 2019.[11] Les résultats de cette étude ont également montré que le secteur financier était confronté à davantage d’attaques par inclusion de fichier local (LFI - *Local File Inclusion*) par rapport aux autres secteurs.[12]

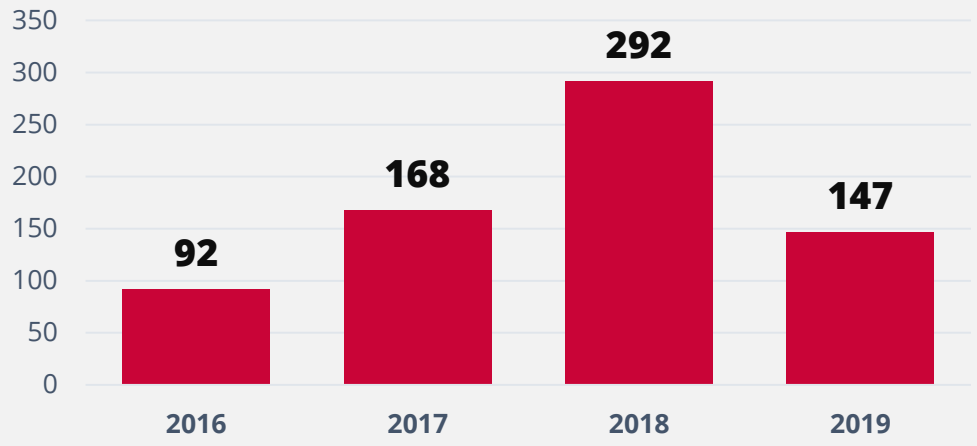


Figure 1: Réduction du nombre de fichiers nettoyés par site compromis. Source: Sucuri[10]

Vecteurs d’attaque

Vecteurs d’attaque d’applications web

On s’accorde généralement à penser que les attaques d’applications web sont assez diverses. Or, les données issues des recherches en matière de sécurité suggèrent que la majorité des attaques des applications web se limitent au type SQLi ou LFi.[11,13,14] Un autre rapport suggère que les vecteurs d’attaque de type SQLi, traversée de répertoire (*directory traversal*), XSS, violation d’authentification et de gestion de session (*broken authentication and session management*) sont ceux les plus utilisés dans ce type d’attaques.[4]

SONICWALL a également signalé une tendance similaire pour les principales attaques d’applications web survenues en 2019. En haut de la liste figuraient les attaques de type SQLi, *directory traversal*, XSS, *broken authentication and session management*.[4]

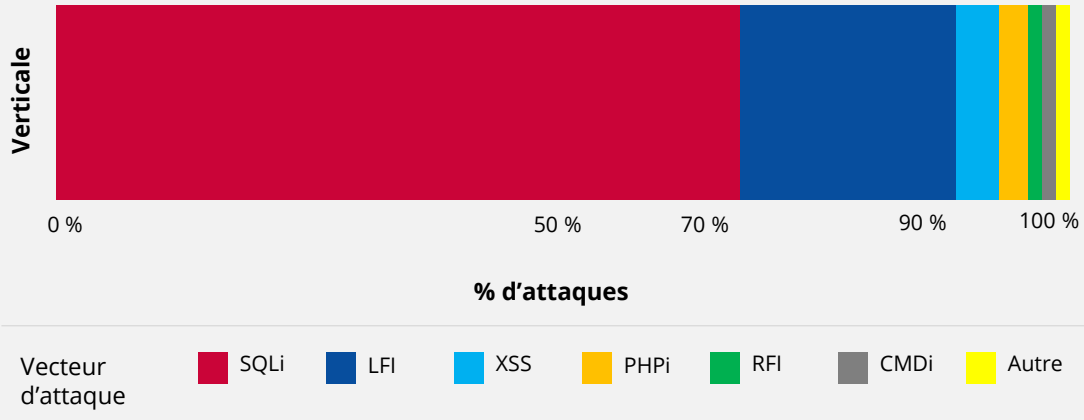


Figure 2: Source: Akamai[12]

Attaques d'applications web

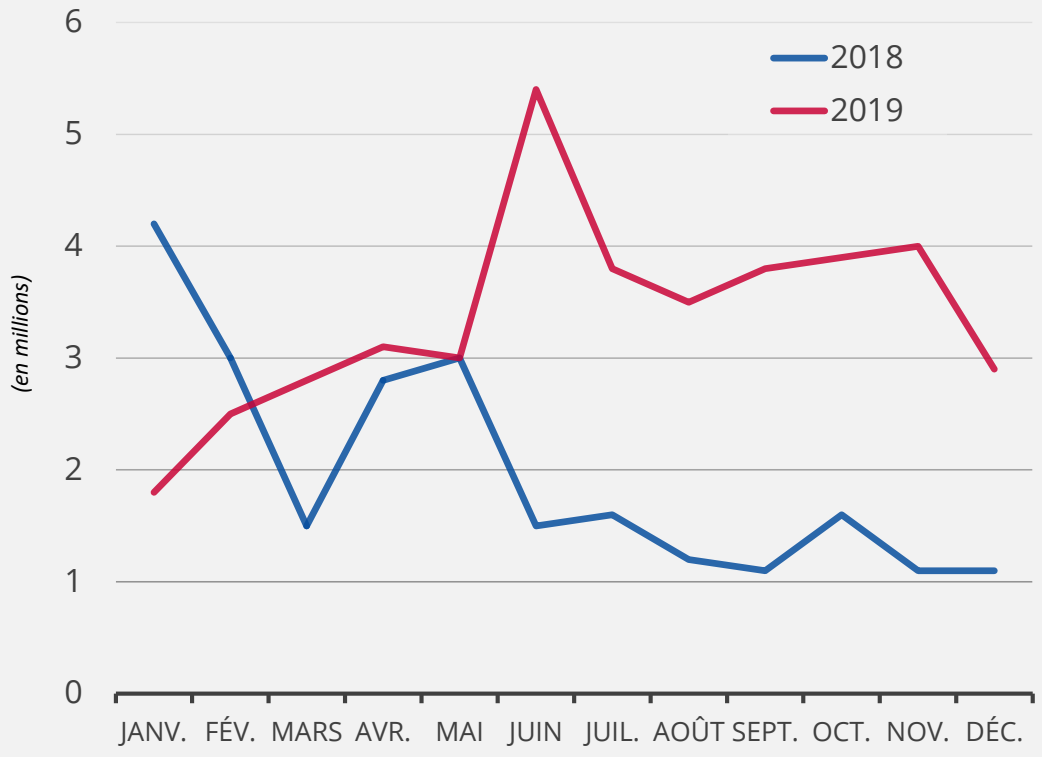


Figure 3 - Source: Sonicwall[4]

Atténuation

Actions proposées

- Utiliser des techniques de validation et d'isolement des données d'entrée pour les attaques par injection (c.-à-d. instructions paramétrées, échappement de la saisie utilisateur, validation en entrée, etc.)[16].
- Implémenter des pare-feu applicatifs web afin de garantir des mesures préventives et défensives[17] (également connus sous le nom de patch virtuel).[18]
- Pour les API d'applications web[19]:
  - mettre en œuvre et maintenir un inventaire des API et les valider par rapport aux balayages du périmètre et à la découverte interne par l'intermédiaire des équipes de développement et d'exploitation;
  - chiffrer la communication et la connexion des API;
  - fournir les bons mécanismes d'authentification et les niveaux d'autorisation appropriés.
- Intégrer les processus de sécurité des applications dans le cycle de vie du développement et de la maintenance des applications.[20]
- Restreindre l'accès au trafic entrant pour les services requis uniquement.[20]
- Déployer des capacités de gestion du trafic et de la bande passante.
- Imposer le durcissement des serveurs d'applications web et maintenir une bonne gestion des correctifs et des processus de test.[21]
- Effectuer des évaluations sur les vulnérabilités et les risques avant et pendant le développement de l'application web.
- Réaliser régulièrement des tests d'intrusion pendant l'implémentation et après le déploiement.

Applications web par gravité maximale des vulnérabilités détectées

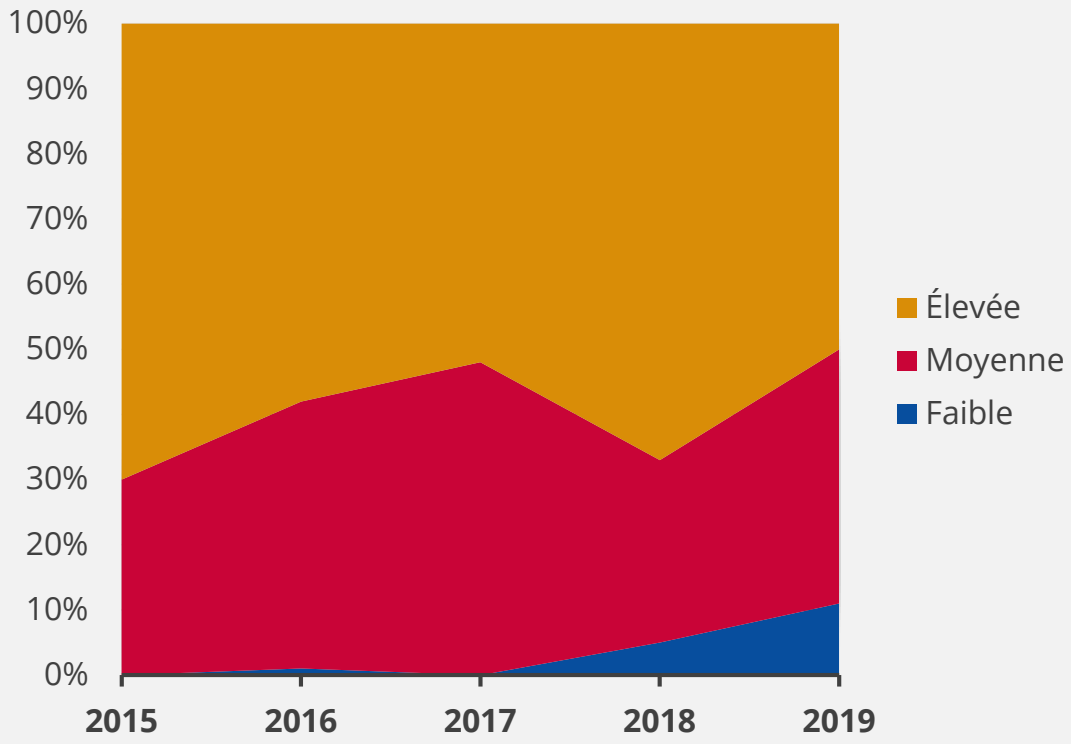


Figure 4 - Source: Positive Technologies[9]

Références

1. «The Future Is the Web! How to Keep It Secure?» Octobre 2019. Acunetix. https://www.acunetix.com/whitepaper-the-future-is-the-web/

2. «What Is a Web Application Attack and how to Defend Against It». 2019. Acunetix. https://www.acunetix.com/websitesecurity/web-application-attack/

3. «2020 State of Application Services Report» F5 Networks, 2020. https://www.f5.com/state-of-application-services-report

4. «Sonicwall Cyber Threat Report». 2020. SonicWall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. «The State of Web Application Security, Protecting Application in the Microservice Era.» 2019. Radware. https://www.radware.com/resources/was-report-2019/

6. «API Security Top 10 2019.» OWASP. https://owasp.org/www-project-api-security/

7. Raymond Pompon, Sander Vinberg. «Aplication Protection Report 2019, Episode 5: API Breaches and the Visibility Problem.» 13 août 2019. F5 Labs https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

8. «Unauthorized Logins on Fast Retailing Online Store Websites due to List Type Account Hacking and Request to Change Password.» 13 mai 2019. Fast Retailing. https://www.fastretailing.com/eng/group/news/1905132000.html

9. «Web Applications vulnerabilities and threats: statistics for 2019.» 13 février 2020. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/#id9

10. Esrtevao Avillez. «2019 Website Threat Research Report.» 2019. Sucuri. https://sucuri.net/wp-content/uploads/2020/01/20-sucuri-2019-hacked-report-1.pdf

11. «State of the Internet / Security | Web Attacks and Gaming Abuse (Volume 5, Issue 3).» 2017-2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-executive-summary-2019.pdf

12. «Sate of the Internet Security | Financial Services – Hostile Takeover Attempts (Volume 6, Issue 1).» 2020. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf

13. «Q4 2016 State of The Internet Security Report» 2016.Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf

14. «Q4 2017 State of the Internet Security Report» 2017. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf

15. «2019 Cyberthreat Defense Report.» 2019. CyberEdge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

16. «AppSec Advisor: Injection Attacks.» Octobre 2019. CIS Center for Internet Security. https://www.cisecurity.org/newsletter/injection-attacks/

17. «Cybersecurity threatscape: Q3 2019.» 2 décembre 2019. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q3/#id5

18. «Virtual Patching Best Practices.» OWASP. https://owasp.org/www-community/Virtual_Patching_Best_Practices

19. Raymond Pompon, Sander Vinberg. «Aplication Protection Report 2019, Episode 5: API Breaches and the Visibility Problem.» 13 août 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

20. «2020 Cyber Threats, Business Email Compromise.» 22 octobre 2019. https://www.uscloud.com/blog/top-cyber-threats-in-2020/

21. Sara Boddy, Remi Cohen. «Regional Threat Perspectives, Fall 2019: Asia.» 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/regional-threat-perspectives--fall-2019--asia

«L’augmentation de la complexité des applications web et la généralisation de leurs services créent des difficultés pour les protéger contre des menaces aux motivations diverses, allant du préjudice financier à l’atteinte à la réputation, en passant par le vol d’informations critiques ou personnelles.»

ETL 2020

Documents connexes

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Bilan de l'année**

Résumé des tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

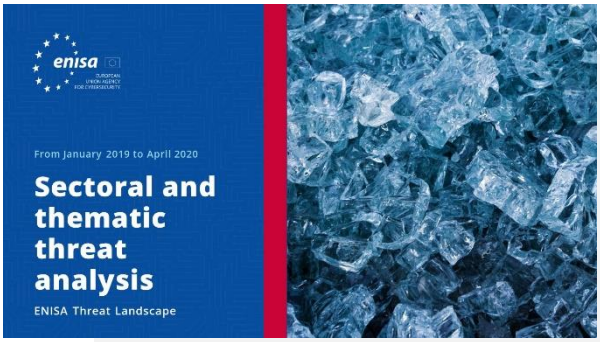
Rapport sur le Paysage des menaces de l'ENISA
Liste des 15 principales menaces

Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Thèmes de recherche

Recommandations concernant les thèmes de recherche provenant de divers secteurs de la cybersécurité et du renseignement sur la cybermenace.



LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Analyse sectorielle et thématique de la menace**

Analyse contextualisée de la menace entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Tendances émergentes**

Principales tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Aperçu du renseignement sur la cybermenace**

L'état actuel du renseignement sur la cybermenace dans l'UE.

À propos

_ L'Agence

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union dont la mission consiste à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis cybernétiques de demain. En partageant les connaissances, en renforçant les capacités et en organisant des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et, au bout du compte, maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations sur l'ENISA et ses travaux, consultez le site https://www.enisa.europa.eu/media/enisa-en-francais/.

Contributeurs

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) et *tous les membres du groupe des parties prenantes CTI de l'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT-UE) et Thomas Hemker.

Éditeurs

Marco Barros Lourenço (ENISA) et Louis Marinos (ENISA).

Contact

Pour toute question sur ce document, veuillez utiliser l'adresse enisa.threat.information@enisa.europa.eu.

Pour les demandes de renseignements des médias concernant le présent document, veuillez utiliser l'adresse press@enisa.europa.eu.

Nous aimerions avoir votre avis sur ce rapport!
Merci de prendre un moment pour remplir le questionnaire.
Pour accéder au formulaire, veuillez cliquer ici.

Avis juridique

Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA à moins d'être adoptée conformément au règlement (UE) nº 526/2013. Elle ne représente pas nécessairement l'état des connaissances et l'ENISA peut l'actualiser périodiquement.

Les sources de tiers sont citées de façon adéquate. L'ENISA n'est pas responsable du contenu des sources externes, notamment des sites web externes, mentionnées dans la présente publication.

La présente publication est uniquement destinée à des fins d'informations. Elle doit être accessible gratuitement. Ni l'ENISA ni aucune personne agissant en son nom n'est responsable de l'utilisation qui pourrait être faite des informations contenues dans la présente publication.

ISBN: 978-92-9204-354-4

DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grèce
Tél.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu