EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Web application attacks

ENISA Threat Landscape

Overview

Web applications and technologies have become a core part of the internet by adopting different uses and functionalities. The increase in the complexity of web application and their widespread services creates challenges in securing them against threats with diverse motivations from financial or reputational damage to the theft of critical or personal information.[1] Web services and applications depend mostly on databases to store or deliver the required information. SQL Injection (SQLi) type of attacks are a well-known example and the most common threats against to such services. Cross-site scripting (XSS) attacks are another example. In this type of attack, the malicious actor misuses weaknesses in forms or other input functionalities of web applications that leads to other malicious features such as being redirected to a malicious website.[2]

While organisations are becoming proficient and developing more consistent automation in their web application lifecycle, they are demanding security as the most crucial part of their offering and prioritisation. This introduction of complex environments drives the adoption of new services such as Application Programming Interfaces (APIs). APIs, which create new challenges for web application security the organisations involved to consider more prevention and detection measures. For instance, roughly 80% of organisations adopting APIs deployed controls on their ingress traffic.[3] In this section, we review the threat landscape of web applications during 2019.

_Trends

20%_ of companies and organisations reported DDoS attacks on their application services on a daily basis[5]

Buffer overflow was the most common technique used (24%). HTTP flood (23%), resource reduction (23%), HTTPS flood (21%) and Low Slow 21% were other commonly used techniques.

63%_ of respondents to CyberEdge survey are using a web application firewall (WAF)

27,5% have plans to deploy this technology and 9,5% do not have any such plans.[15]

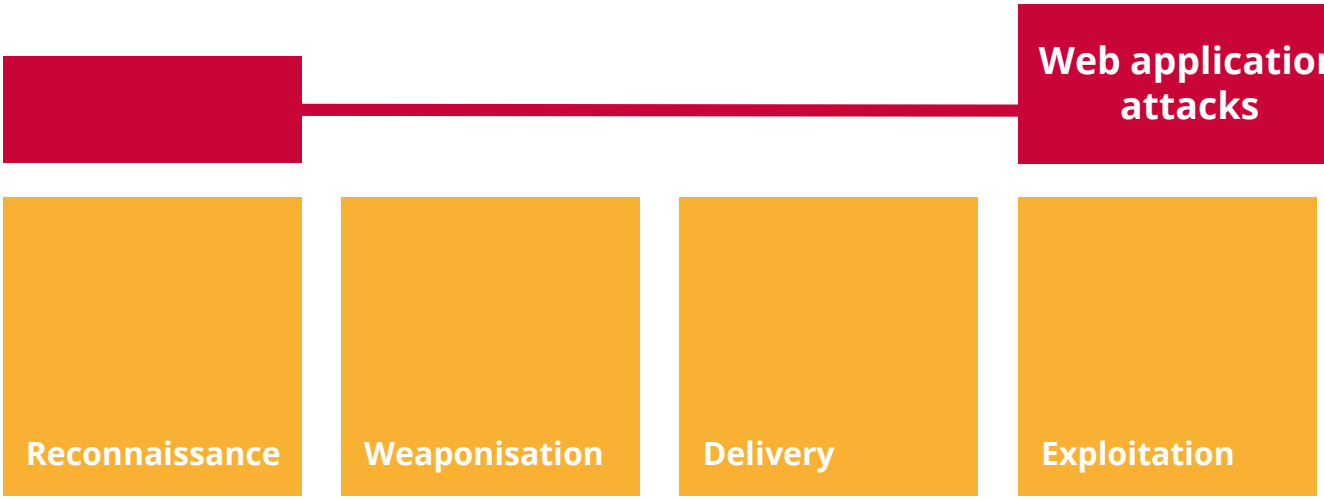
52%_ increase in the number of web application attacks in 2019 compared with 2018

According to a security researcher, the amount of web application attacks were almost flat compared with 2018 and rose sharply later in the year.[4]

84%_ of observed vulnerabilities in web applications were security misconfigurations

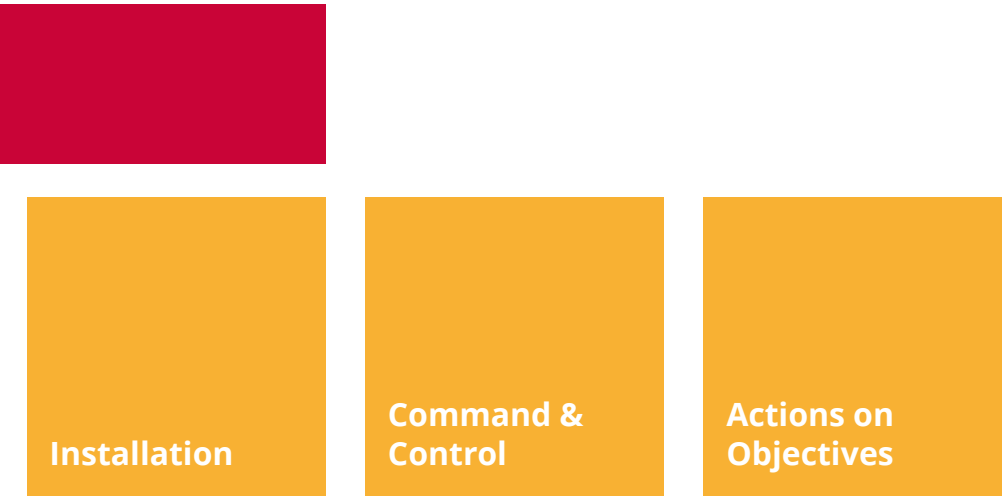
This was followed by cross-site scripting (53%) and broken authentication interestingly (45%).[9]

Kill chain



Step of Attack Workflow

Width of Purpose



The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

MORE INFORMATION

Description

_Improved collaboration between application security and application development

According to the survey conducted by a security researcher[5], one of the factors contributing to such ineffective security could be the decision-making about ownership of security tools. The survey presented the views of top influencers in this area naming IT leadership and business owners and not the chief information security officer (CISO).

_Growing importance of Application Programming Interfaces (APIs)

APIs are not new in web application architecture, and their widely accepted usage reintroduces existing risks and their likelihood of exploitation as a result of the widening of the threat landscape. Accordingly, the Open Web Application Security Project (OWASP) published a top 10 list of API security measures 6 providing a prioritised way to secure such capability in web application architecture. One instance of such a threat is the PHP API attacks: according to another security researcher, 87% of the scanning of API traffic was searching for available PHP APIs.[7]

_Authorisation and authentication failures

These are usually the leading cause of malicious actors gaining access to critical information (i.e. fast retailing breach[8]). According to a security researcher, the breaches of critical data are the second most pressing threat to web application security.[9]

Growing trend with SQL injection (SQLi)

A recent security research identified that, two-thirds of web application attacks include SQLi attacks. While other web application attack vectors either remained steady or are growing, SQLi attacks continued to grow sharply, and particularly specially escalated during the holiday season of 2019.[11] The findings from this research also identified that the finance industry faces more local file inclusion (LFi) attacks compared with other sectors.[12]

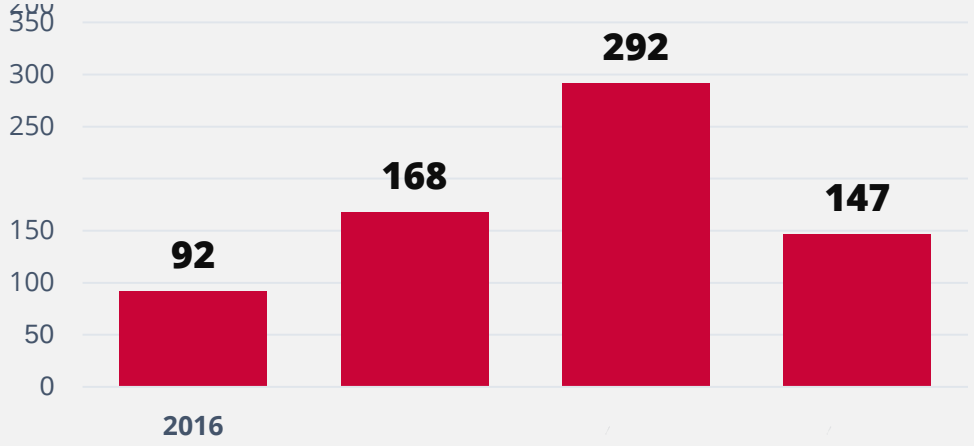


Figure 1: Reduction on the number of files cleaned per compromised site. Source: Sucuri[10]

Attack vectors

Web application attack vectors

There is general perception that web application attacks are quite diverse. However, data from security research suggests that the majority of web application attacks are limited to SQLi or LFi.[11,13,14] Another report suggests that SQLi, directory traversal, XSS, broken authentication and session management are on the top of the attack vectors used in this type of attacks.[4]

SONICWALL also reported a similar trend for the top web application attacks for 2019. On the list SQLi, directory traversal, XSS, broken authentication and session management were on the top.[4]

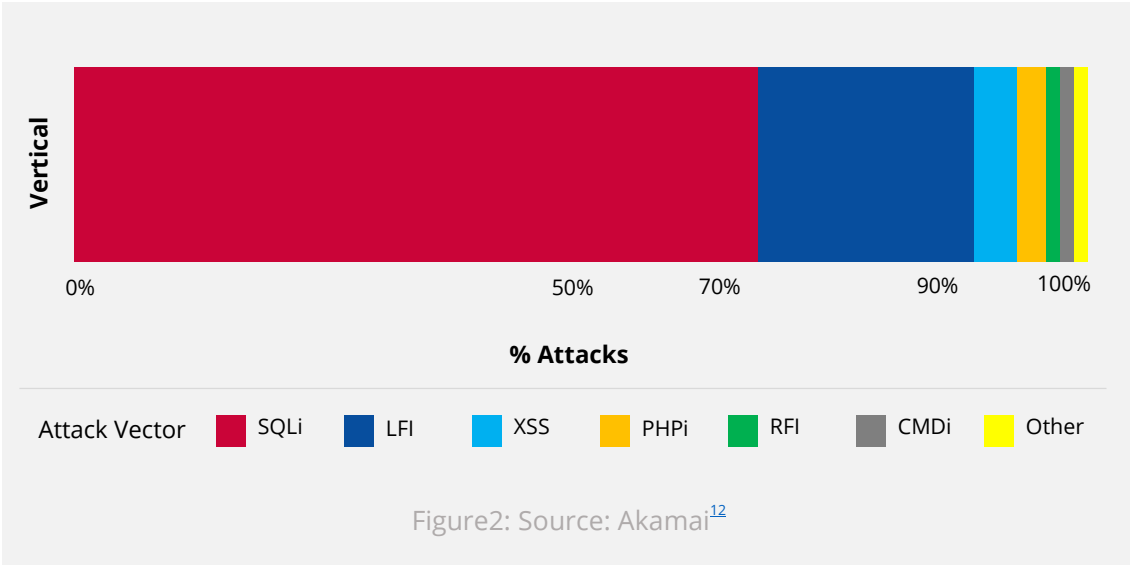
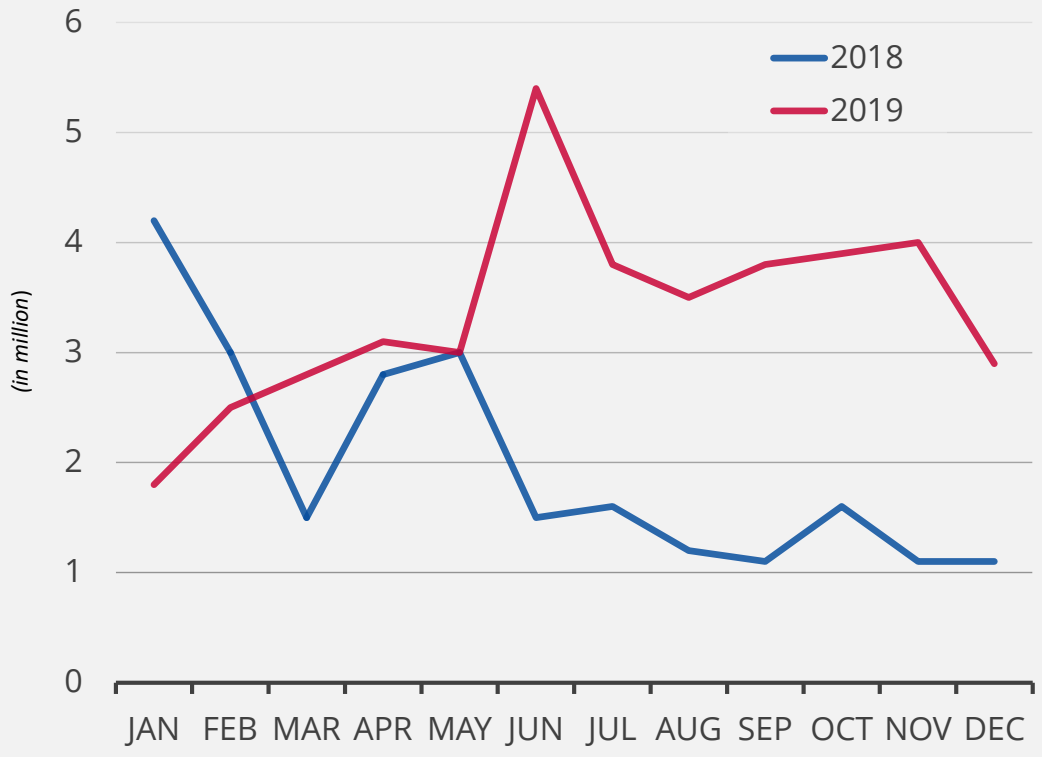


Figure2: Source: Akamai[12]

_Web application attacks



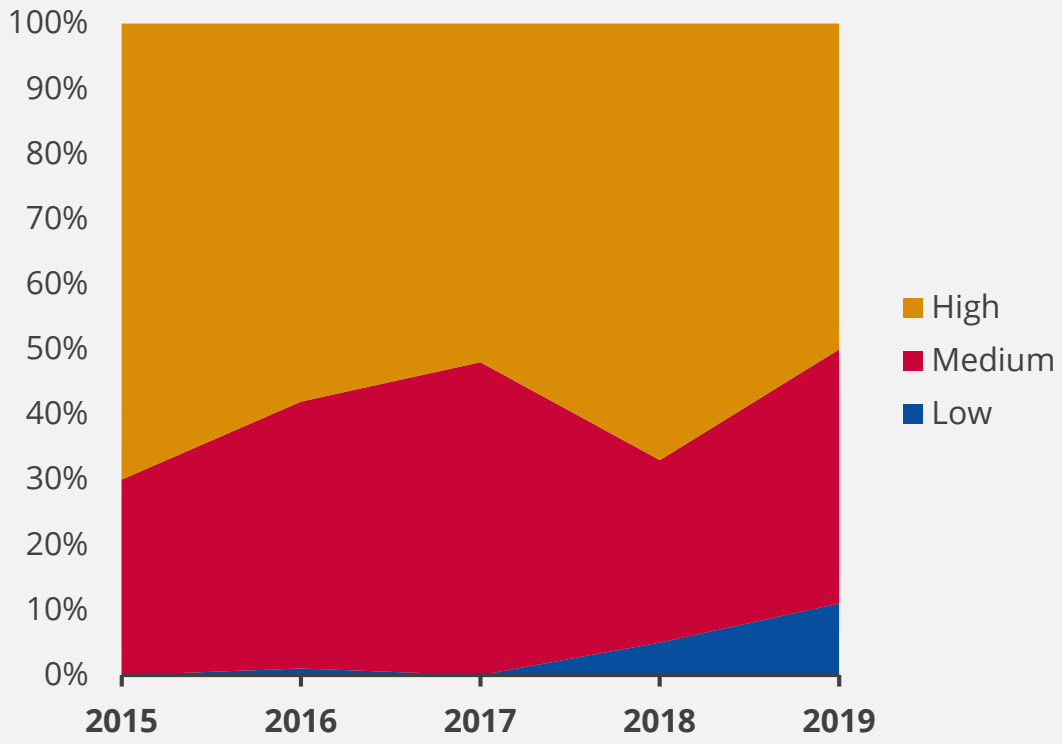
Source: Sonicwall[4]

Mitigation

Proposed actions

- Use input validation and isolation techniques for injection type attacks (i.e. parameterised statements, escape user input, input validation, etc.)[16].
- Implement web application firewalls for preventive and defensive measures17 (also known as virtual patching).[18]
- For web application APIs[19]:
  - implementing and maintaining an inventory of APIs and validating them against perimeter scans and internal discovery through development and operational teams;
  - encrypting API communication and connection;
  - providing the right authentication mechanisms and authorisation levels.
- Incorporate application security processes into the application development and maintenance life-cycle.[20]
- Restrict access to inbound traffic for required services only.[20]
- Deploy traffic and bandwidth management capabilities.
- Enforce web application server hardening and maintain a good patch management and testing processes.[21]
- Perform vulnerability and risk assessments before and during the web application development.
- Conduct regular penetration testing during implementation and after deployment.

Web applications by maximum severity of vulnerabilities found



Source: Positive Technologies[9]

References

1. "The Future Is the Web! How to Keep It Secure? " October 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. "Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem." August 13, 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." May 13, 2019. Fast Retailing. https://www.fastretailing.com/eng/group/news/1905132000.html

9. "Web Applications vulnerabilities and threats: statistics for 2019." February 13, 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. "State 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." October 2019. CIS Center for Internet Security. https://www.cisecurity.org/newsletter/injection-attacks/

17. "Cybersecurity threatscape: Q3 2019. " December 2, 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. "Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem." August 13, 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." October 22, 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

“The increase in the complexity of web application and their widespread services creates challenges in securing them against threats with diverse motivations from financial or reputational damage to the theft of critical or personal information.”

in ETL 2020

Related

READ THE REPORT

ENISA Threat Landscape Report
The year in review

A summary on the cybersecurity trends for the period between January 2019 and April 2020.

READ THE REPORT

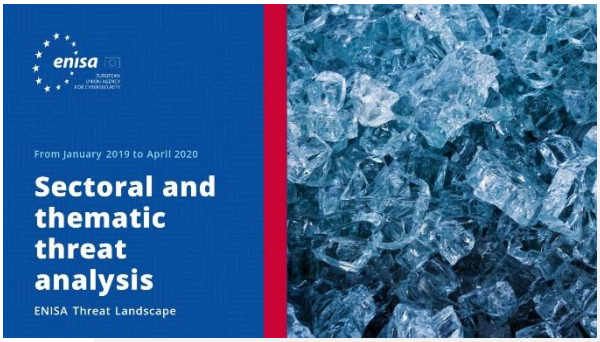
ENISA Threat Landscape Report
List of Top 15 Threats

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report
Research topics

Recommendations on research topics from various quadrants in cybersecurity and cyberthreat intelligence.



READ THE REPORT

ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report **Cyber Threat Intelligence overview**

The current state of play of cyberthreat intelligence in the EU.

About

_ The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors
Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

Editors
Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

Contact
For queries on this paper, please use enisa.threat.information@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

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

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu