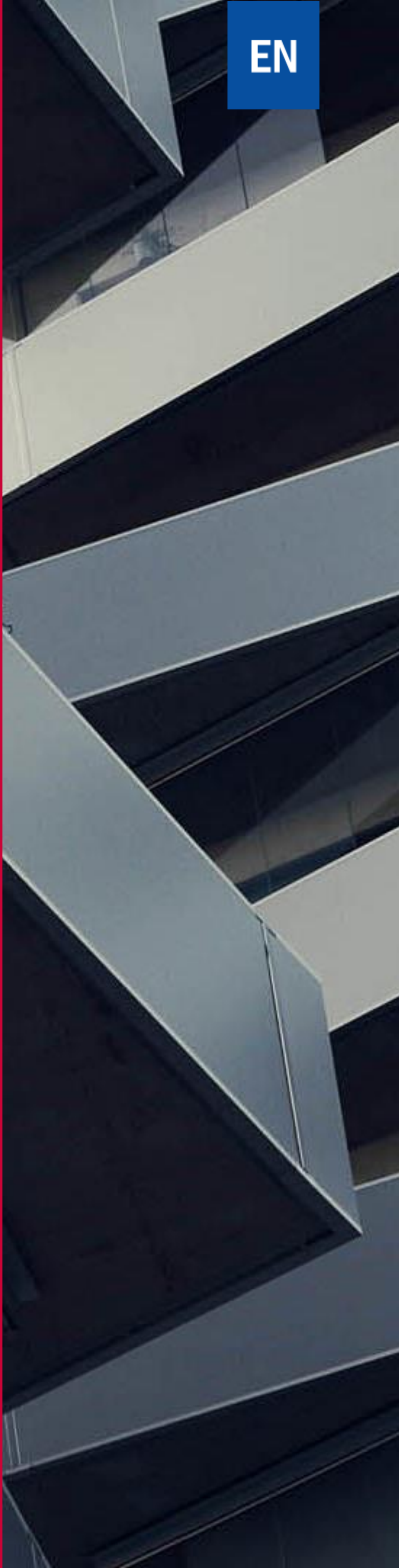
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

EN



From January 2019 to April 2020

Data breach

ENISA Threat Landscape

Overview

A data breach is a type of cybersecurity incident in which information (or part of an information system) is accessed without the right authorisation, typically with malicious intent, leading to the potential loss or misuse of that information. It also includes 'human error' that often happens during the configuration and deployment of certain services and systems, and may result in unintentional exposure of data.[1]

In many cases, companies or organisations are not aware of a data breach happening in their environment because of the sophistication of the attack and sometimes the lack of visibility and classification in their information system.[2] Based on research, it takes approximately 206 days to identify a data breach in an organisation.[3] Thus, the time to contain, remediate and recover the data means that it takes longer to return to normal.

Despite all the risks involved, organisations keep even more data[4] using cloud storage infrastructures and complex on-premises environments. These environments are gradually more exposed to new and different risks, proportional to the sensitiveness of the information stored. It comes as no surprise that, the number of data breaches increased in 2019 and 2020. New findings also suggest that the impact is not felt exclusively when a data breach is discovered - the financial impact can remain for more than 2 years after the initial incident.

_Findings

54%_ increase in the total number of breaches by midyear 2019 compared with 2018.

71%_ of the data breaches were financially motivated. Nearly 25% had long term strategic goals (nation state/ espionage).[5]

32%_ of the data breaches involve phishing activity according to IOCTA 2019.[6] A report suggests that phishing is at the top of the list of major contributors to data breaches. The report also mentions that e-mail is the prime delivery method of malware (94%) in a chain of events leading to a data breach.[3]

52%_ of data breaches involved hacking.[5] Other tactics utilised are social attacks (33%), malware (28%) and mistakes or errors (21%). Since 2016 hacking has been the main cause of data breaches in healthcare. During 2019 nearly 59% of the reported breaches were caused by hacking.[7]

70%_ of the data breaches expose e-mails. Although username/e-mail and passwords (i.e credentials) are easily changed in contrast with personal details (i.e. date of birth), the focus is mostly on these in data breaches.[8]

55%_ of the responders to a Eurobarometer survey responded that they are concern about their data being accessed by criminals and fraudsters.

Timeline

2019

_ January

MEGA cloud (NZ) suffered a data breach exposing 770 million emails and 21 million passwords.[9]

_ February

620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts.[10]

_ March

12,5M medical records of pregnant woman of Indian government (IN) healthcare center, going back to 2014 were exposed to public.[11]

_ August

Major breach found in biometrics system used by banks, (UK) police and defence firms.[16]

_ September

Mastercard (BE) suffered a data breach affecting ca. 90K customers in Europe.[17]

_ October

The account information of over 7.5 million users from Adobe (US) was exposed due to an unprotected online database.[18]

_ November

UniCredit (IT) victim of a data breach leaking 3 million records.[19]

_ December

The smart camera provider Wyze (US) suffered two breaches at the end of December when databases were left exposed for over two weeks.[20]

2020

_ January

250 million customer service and support records from Microsoft (US), going all the way back to 2005, were breached.[21]

_ April

Facebook (US) reported a data breach exposing 540 million user records on exposed servers.[12]

_ May

First American Financial Corp. (US) leaked hundreds of millions of title insurance records.[13]

_ June

100 million records exposed by unauthorised access to a data storage from Evite customers.[14]

_ July

Personal information from Capital One (US) credit card customers breached.[15]

_ February

An unprotected Google (US) cloud server containing the personal data of 200 million US residents.[22]

_ March

Biometric solutions company Antheus Tecnologia (BR) suffered from a data leak.[23]

_ April

Hackers obtained the login details from two Marriott (US) employees and broke into the system in January 2020.[24]

Trends

_The cost of a data breach for organisations spreads over many years

Security researchers found that one third of the costs related to a data breach are incurred more than 1 year after the incident. In more detail, around 22% of these costs are incurred in the second year, while 11% of the costs are accounted for more than 2 years after the initial incident. These rates were higher for highly regulated organisations, such as those in financial services and healthcare, in comparison with other sectors.[3] The adoption of cloud or multi-cloud environments is increasing rapidly similar to the amount of data stored and processed in these environments.

_Small mistakes could lead to big breaches

Securing the cloud environment without losing all the flexibility it brings to the infrastructure and resources can be problematic. A single misconfiguration can result in exposing the entire sensitive database. A security researcher believes that majority of data breaches in the cloud are a result of misconfiguration and they are mostly unintentional. Netflix, Ford and TD Bank are only few examples among many others. From a different perspective, although data breaches resulting from malicious attempts still cost more, breaches caused by system glitches or human errors still represent a considerable cost on average US $3,24 million (ca. €2,74 million).[3]

_Data breaches cost more to small business

The cost of data breaches to enterprises or large organisation with more than 25.000 employees is US $204 (ca. €173) per employee. The total amount estimation at around US $5,11 million (ca. €4,33 million). In contrast, for small companies (500-1.000 employees) the average cost is around US $3.533 (ca. €3.000) per employee. This represents a total cost of US $2,65 million (ca. €2,24 million) for small businesses.[3]

_ Financial gain is the prime motivation

Malicious/threat actors are known to be the ones pulling the string in data breaches (bearing in mind that sometimes they may be the result of a mistake). In that sense, external threat actors are the main cause of data breaches, and this could include activities such as botnets↗. In this regard, financial gain has been repeatedly identified as the main motivation behind data breaches facilitated by these groups of actors. Espionage↗ also was one of the key motives behind data breaches but not as high up the list as personal or financial gain. This trend was almost consistent with the results observed in 2010-2011.[5]

Trends

_ Quantum-computing and data security concerns

Cryptography requirements play a vital role in the quantum-computing era and highlight critical security issues. 72% of organisations believe that quantum computing will affect their crypto related operations strategically (in the next 5 years). According to the results of the survey, 92% of respondents are concerned about the exposure of sensitive data by using this technology in the computing industry. The main strategies respondents suggested for tackling such concerns were changing the security architecture and deploying key managements infrastructures.[26]

_Healthcare - a consistent focus for malicious actors

Healthcare continued to be one of the most attractive targets for cybercriminals using ransomware↗ and phishing↗ techniques costing such organisations millions of euros to contain and recover from the impact. In 2019, 400 healthcare companies reported a data breach in patient records. This was a record for healthcare organisations.[7]

_Multi-cloud - the new challenge for data security

A survey conducted by a security researcher reported that 9 out of 10 companies are thinking of using or already using cloud environments. Approximately 44% of their responders also believe that these environments are challenging for implementing proper data security measures.[25]

__Types of data exposed (%)

Type of data	2019	2018	2017
E-mail	70	44	32
Password	64	39	27
Name	23	37	41
Miscellaneous	18	19	15
Social security number	11	22	27
Credit card	11	16	19
Address	11	22	30
Account	10	7	4
Unknown	8	13	18
Date of birth	8	13	12
Medical	5	9	7
Financial	5	13	19

Source: Cyber Risk Analytics[8]

Trends

_Continuous decrease in 'card-present' breaches

According to a security report, a decrease in point of sale and card-skimming breaches (where card is presented) was identified during 2019. This represents a shift from traditional ATM skimming↗ and card payments to web application in retail industry. Although the number of incidents decreased in this area, is not an accurate to conclude that the number of data breaches decrease rather but a shift in the vector. The decrease though might be related to a wider implementation of chip and pin enabled cards/terminals (also known as EMV).[6]

_What to expect in the near future?

According to a security researcher, healthcare organisations should be prepared for a 10%-15% increase in the number of data breaches, in which their service providers will be the main target[7]. More generally, based on the results from the first 6 months of 2019, it is expected that the number of data breaches will increase at an alarming rate, despite the awareness of senior leaders and the effort that many organisations are putting into to secure their data.[8]

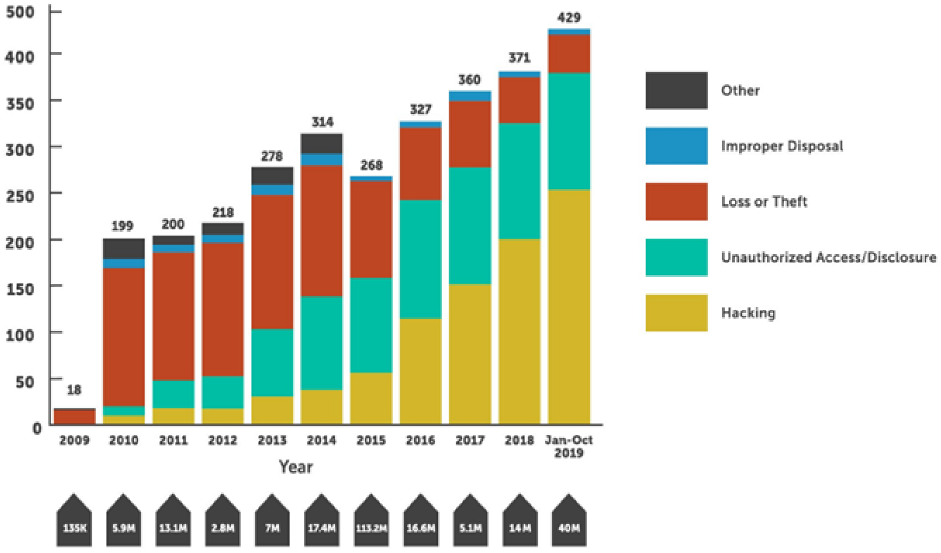
_Data breaches by sector and organization size

Incidents	Breaches	Small	Large	Unknown
Accommodation	61	34	7	20
Administrative	17	6	6	5
Agriculture	2	2	0	0
Construction	11	7	3	1
Education	99	14	8	77
Entertainment	10	2	3	5
Finance	207	26	19	162
Healthcare	304	29	25	250
Information	155	20	18	117
Management	2	1	1	0
Manufacturing	87	10	22	55
Mining	15	2	5	8
Other services	54	6	5	43
Professional	157	34	10	113
Public	**330**	**17**	**83**	**230**
Real Estate	14	6	3	5
Retail	139	46	19	74
Trade	16	4	8	4
Transportation	36	3	9	24
Utilities	8	2	0	6
Unknown	289	0	109	180
Total	2.013	271	363	1,379

Source: Verizon DBIR, 2019[5]

Attack vectors

- **E-MAIL/PHISHING**. Impersonating a third-party supplier or a partner using e-mail is an easy win for the malicious actors. This is known to be the vector most often used by cybercriminals to target their victims and the cause of most of data breaches (almost 40% of breaches in healthcare).[7]
- **CLOUD/WEB APPLICATIONS.** This reflects web applications being used as a vector for attempts by malicious actors to breach data or critical operations. Stealing credentials to access web-based e-mail portals is a prime example. Exploiting weaknesses in application servers to inject/deliver information-stealing malware or formjacking attacks are other examples in this vector.[7]
- **INSIDER THREAT.** This mainly refers to unauthorised or malicious attempts to use resources. It should be noted that generally in analysis and reporting misconfiguration or mistakes (human error) by internal teams may also be referred to as 'insiders'. Although most data breaches are facilitated by external malicious actors, it is still the case that insiders with or without privileged access are playing a key role in data breaches.[5]



Entities involved in a breach. Source: Horizon[7]

“In many cases, companies or organisations are not aware of a data breach happening in their environment because of the sophistication of the attack and sometimes the lack of visibility and classification in their information system.”

in ETL 2020

Mitigation

_Proposed actions

- Data breach is generally the outcome of other threats and the mitigation overlaps with others discussed in this report.
- Consider investing in hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.[26]
- Develop and maintain a cybersecurity awareness plan. Provide training and simulation scenarios for identifying social engineering and phishing campaigns for staff.[7]
- Establish and maintain an incident response team and evaluate incident response plans frequently.[3]
- Identify and classify sensitive/personal data and apply measures for encrypting such data in transit and at rest.[3] In other words deploy data loss prevention capabilities.
- Increase investment in detection and alerting tools and in the ability to contain and respond to a data breach.
- Develop and maintain strong policies enforcing strong passwords (password management) and the use of multi-factor authentication.
- Consider using models that take the 'least privilege' approach to provide security for both on- and off-premises resources (i.e. zero-trust models).
- Invest and create policies and plans for engaging with governance, risk management and compliance teams.[26]

“During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface.”

in ETL 2020

References

1. “What is data breach?” Norton. https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

2. “What is data breach?” Malwarebytes. https://www.malwarebytes.com/data-breach/

3. “Cost of Data Breach Report.” 2019. IBM Security, Ponemon Institute. https://www.ibm.com/security/data-breach

4. Dhritimaan Shukla, Kush Wadhwa. “Data breach – threat landscape. Unauthorised exposure of an organisation’s critical data.” PWC India. https://www.pwc.in/consulting/forensic-services/data-breach-threat-landscape.html

5. “Verizon Data Breach Investigations Report.” 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

6. Catherine De Bolle. “Internet Organised Crime Threat Assessment (IOCTA).” 2019. European Cyber Crime Centre (EC3), Europol. https://www.europol.europa.eu/iocta-report

7. “2020 Healthcare Cybersecurity Horizon Report.” 2020. Fortified Health Security. https://www.fortifiedhealthsecurity.com/resources/2020-healthcare-cybersecurity-horizon-report/

8. Inga Goddijn. “2019 Midyear QuickView Data Breach Report – Cyber Risk Analytics.” August 2019. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf

9. Troy Hunt. “The 773 Million Record "Collection #1" Data Breach.” January 17, 2019. TroyHunt. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

10. Chris Williams. “620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts.” February 11, 2019. The Register. https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/

11. Catalin Cimpanu. “Indian govt agency left details of millions of pregnant women exposed online.” April 1, 2019. ZDNet. https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

12. “Losing Face: Two More Cases of Third-Party Facebook App Data Exposure.” April 3, 2019. UpGuard. https://www.upguard.com/breaches/facebook-user-data-leak

13. “First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records.” 24 May, 2019. KrebsonSecurity. https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

14. “Data Incident, Evite.” May 14, 2019. Evite. https://www.evite.com/security/update

15. “Information on the Capital One Cyber Incident.” September 23, 2019. CapitalOne. https://www.capitalone.com/facts2019/

16. Josh Taylor. “Major breach found in biometrics system used by banks, UK police and defence firms.” 14 August, 2019. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

17. Neil Hodge. “Mastercard reveals data breaches in third-party loyalty program.” August 27, 2019. Compliance Week.

https://www.complianceweek.com/data-privacy/mastercard-reveals-data-breaches-in-third-party-loyalty-program/27614.article

18. Catalin Cimpanu. “Adobe left 7.5 million Creative Cloud user records exposed online.” October, 26.2019. ZDNet. https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/

19. Charlie Osborne. “UniCredit reveals data breach exposing 3 million customer records.” October 28, 2019. ZDNet. https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/

20. Chris Isidore. “Smart camera maker Wyze hit with customer data breach.” December 30.2019. CNN. https://edition.cnn.com/2019/12/30/tech/wyze-data-breach/index.html

21. Davey Winder. “Microsoft Security Shocker As 250 Million Customer Records Exposed Online.” January 22, 2020. Forbes. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#2d3f9dca4d1b

22. Paul Bischoff. “US property and demographic database of 200 million records leaked on the web.” March 5, 2020. comparitech. https://www.comparitech.com/blog/vpn-privacy/200-million-us-database-leaked/

23. Jim Wilson.“Brazil: Millions of Records Leaked, Including Biometric Data.” March 11, 2020. Safety Detectives. https://www.safetydetectives.com/blog/antheus-leak-report/

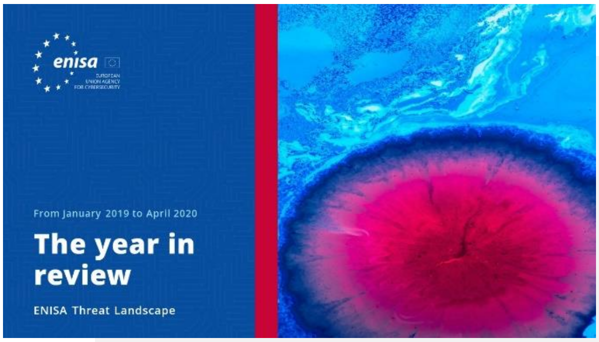
24. Zack Whittaker.“Marriot says 5.2 million guest records were stolen in another data breach.” April 1, 2020. Techrunch. https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/?renderMode=ie11

25. “2019 Thales Data Threat Report – Global Edition” Thales Security, 2019. https://cpl.thalesgroup.com/data-threat-report

26. “2020 Thales Data Threat Report – Global Edition” Thales Security, 2020. https://cpl.thalesgroup.com/data-threat-report

27. Laura Paine. “2019 Verizon DBIR Shows Web Applications and Human Error as Top Sources of Breach.” May 8, 2019. Veracode. https://www.veracode.com/blog/security-news/2019-verizon-dbir-shows-web-applications-and-human-error-top-sources-breach

Related



From January 2019 to April 2020

The year in review

ENISA Threat Landscape

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.

From January 2019 to April 2020

ENISAs' list of top 15 threats

ENISA Threat Landscape

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.

From January 2019 to April 2020

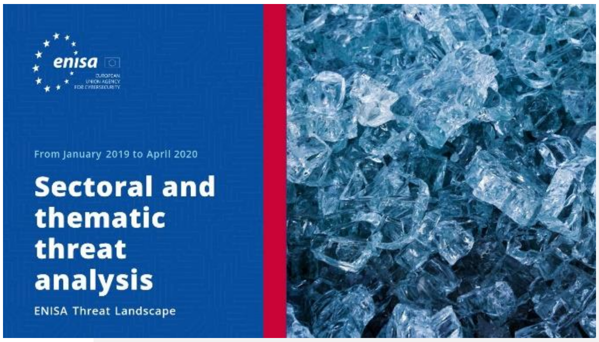
Research topics

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report
Research topics

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



From January 2019 to April 2020

Sectoral and thematic threat analysis

ENISA Threat Landscape

READ THE REPORT

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

Contextualised threat analysis between January 2019 and April 2020.

From January 2019 to April 2020

Emerging trends

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Emerging trends**

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

From January 2019 to April 2020

Cyberthreat intelligence overview

ENISA Threat Landscape

READ THE REPORT

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

The current state of play of cyber threat 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

Copyright Notice

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