enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Insider threat

ENISA Threat Landscape

Overview

An insider threat is an action that may result in an incident, performed by someone or a group of people affiliated with or working for the potential victim. There are several patterns associated with threats from the inside. A well-known insider threat pattern (also known as 'privilege misuse') occurs when outsiders collaborate with internal actors to gain unapproved access to assets. Insiders may cause harm unintentionally through carelessness or because of a lack of knowledge. Since these insiders often enjoy trust and privileges, as well as knowledge of the organisational policies, processes and procedures of the organisation, it is difficult to distinguish between legitimate, malicious and erroneous access to applications, data and systems.[1]

The five types of insider threat can be defined according to their rationales and objectives:

a) the careless workers who mishandle data, break use policies and install unauthorised applications;

b) the inside agents who steal information on behalf of outsiders;

c) the disgruntled employees who seek to harm their organisation;

d) the malicious insiders who use existing privileges to steal information for personal gain;

e) the feckless third-parties who compromise security through intelligence, misuse or malicious access to or use of an asset.

All five types of insider threats should be continuously studied, as acknowledging their existence and their modus operandi should define the organisation's strategy for security and data protection.

__Findings

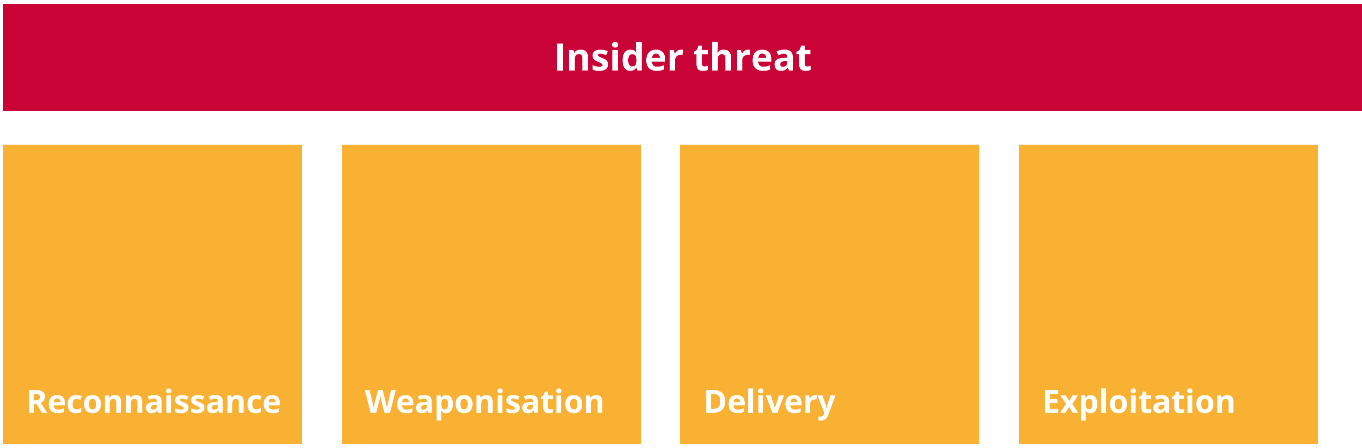
65%_ of the impact from insider threats includes damage to the organisation’s reputation and finances[12]

88%_ of the organisations surveyed recognise that insider threats are a cause for alarm[10]

€11,45_ million is the average annual cost of cybersecurity incidents caused by an insider to the organisation[8]

40%_ of the organisations surveyed feel vulnerable to having confidential business information exposed[11]

Kill chain



Insider threat

Reconnaissance

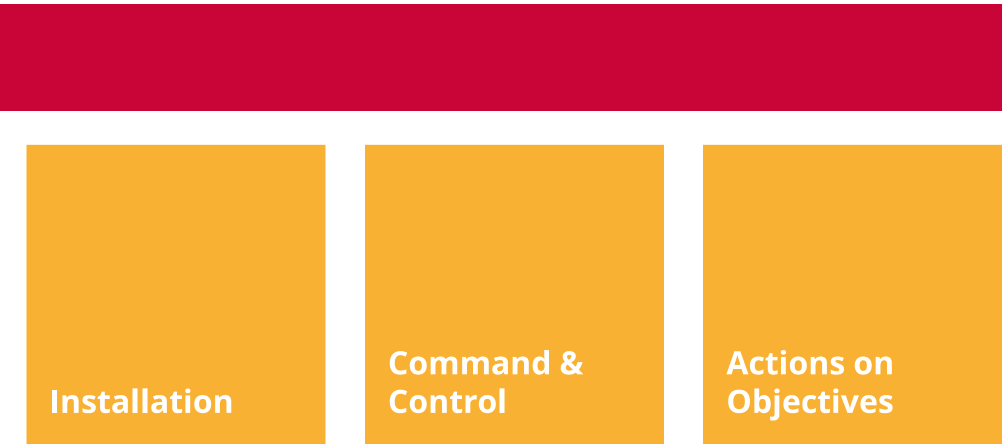
Weaponisation

Delivery

Exploitation

🟥 *Step of Attack Workflow*

🟧 *Width of Purpose*



Installation

Command & Control

Actions on Objectives

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

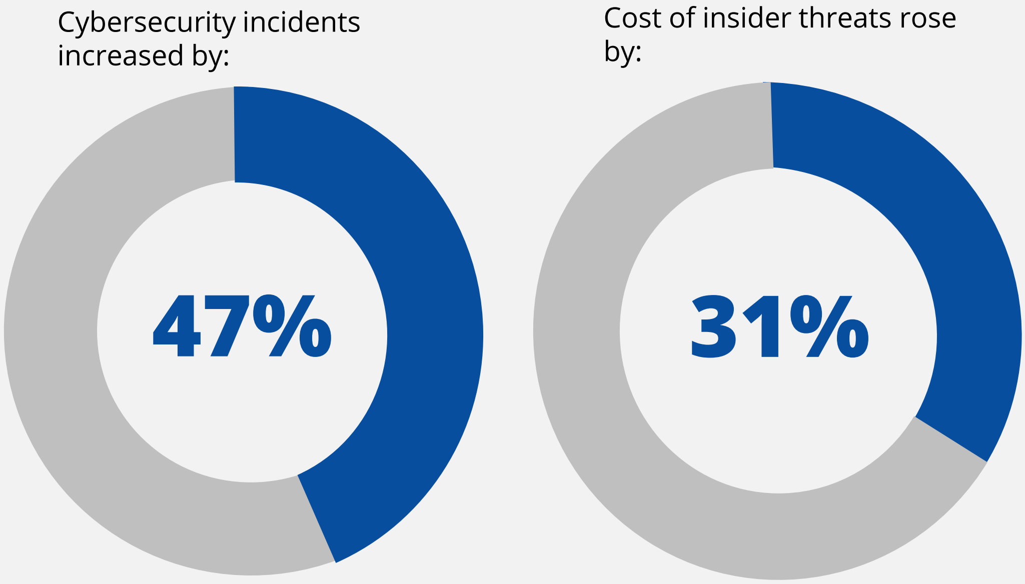
Description

_Money rules

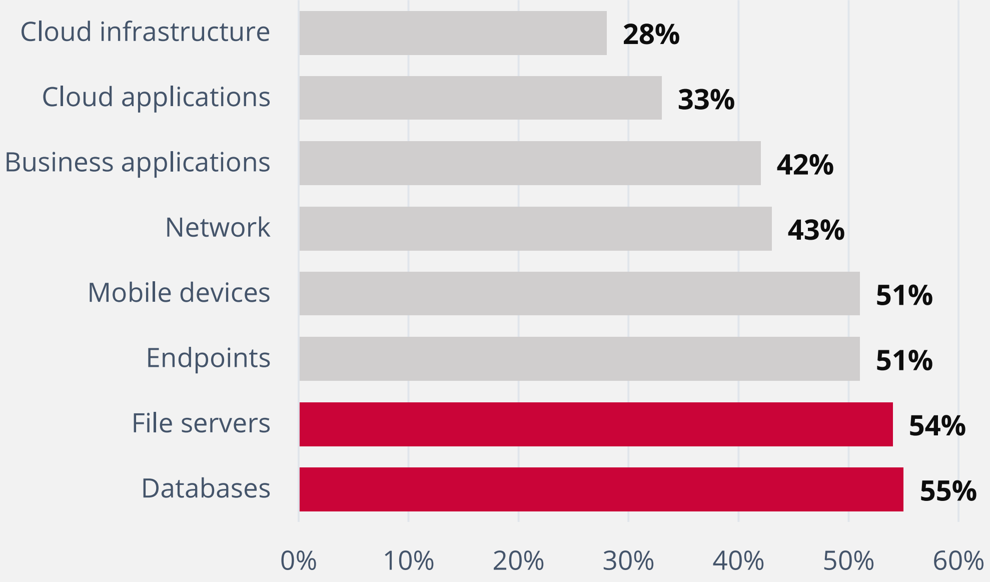
Due to the increasing cost of other attack vectors, attackers are willing to offer large amounts of money to insiders. The price of insiders varies, depending on the insider's position in the company, the company itself, the type and complexity of service that is requested, the type of data that are exfiltrated and the level of security at the company. Some of the ways attackers recruit insiders include: (1) simply posting an offer on forums and offering a reward for certain information; (2) disguising their actions so that employees don't realize they are acting illegally, disclosing personal information or engaging in insider activity; and (3) blackmailing.[4]

_Rogue actions Urbi et Orbi

A former software engineer from a cloud service provider took advantage of a misconfigured web application firewall and accessed more than 100 million customers' accounts and credit card records. The company has since fixed the vulnerability and stated that 'no credit card account numbers or log-in credentials were compromised'. This insider-threat case is particularly interesting because the former employee turned hacker wasn't worried about hiding the identity. The hacker shared the hacking method with colleagues from Capital One on a chat service. The hacker also posted the information on GitHub (using the full name) and bragged on social media about it too. This kind of behaviour is a phenomenon psychologist's call 'leakage' whereby insiders who plot to do damage reveal their plans. Capital One expects the breach to cost up to US $150 million (ca. €127 million).[5]



Incidents and cost trends. Source: ObserveIT[8]



IT assets vulnerable to insider threats. Source: Help Systems[9]

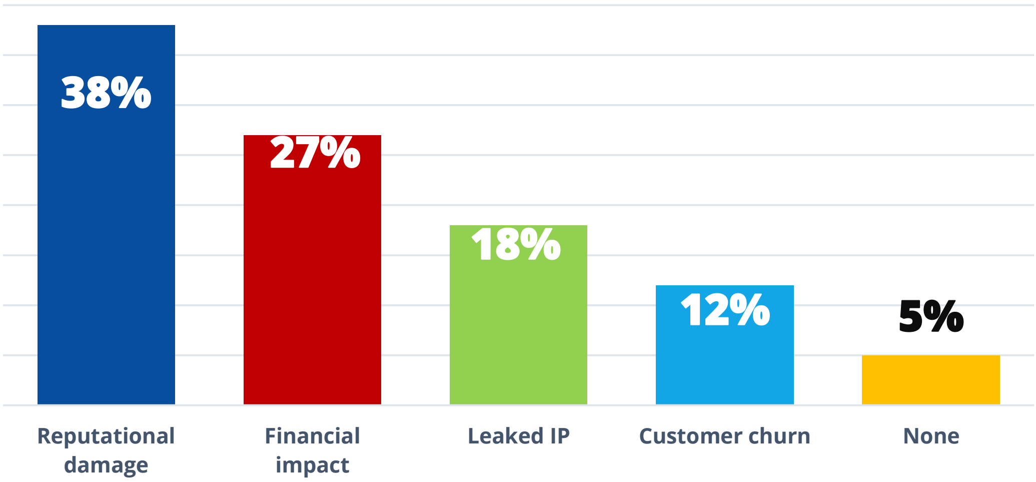
Attack vectors

_How

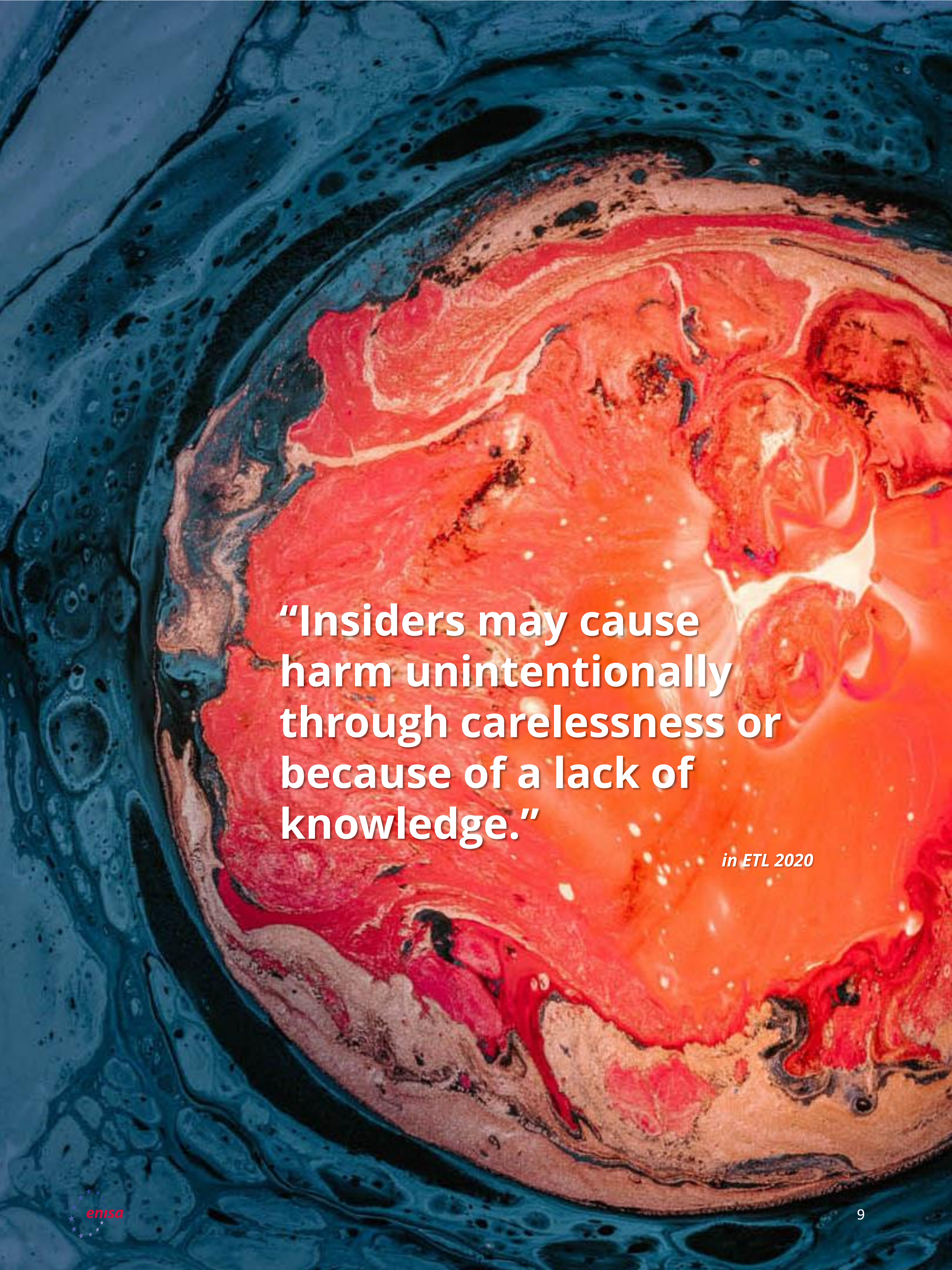
A recent survey[14] revealed that groups are the most dangerous insider threats within companies and other organisations.

According to cybersecurity experts[15], phishing (38%) is the biggest vulnerability in the case of unintentional insider threats. In a lower position of the list are spear phishing (21%), the weak or reused passwords (16%), orphaned accounts (10%) and browsing of suspicious sites (7%).

_ Impact area of insider threat incidents



Source: Egress[12]



> **“Insiders may cause harm unintentionally through carelessness or because of a lack of knowledge.”**
>
> ***in ETL 2020***

Mitigation

_Proposed actions

- Deploy a deep packet inspection (DPI) technology for anomaly detection which gives industrial users a trusted platform for monitoring the flow of process control command flow and telemetry data, and protect against outside threats. At the same time, it mitigates the risk of 'advanced' insider interference from engineers, SCADA operators or other internal staff with direct access to systems.[16]
- Introduce an insider threat countermeasures plan into the overall security strategy and policies. This plan typically includes a risk management framework, business continuity plan (BCP), disaster recovery program (DRP), a financial and accounting management policies and a legal and regulatory management.[1]
- Build a security programme that consists of: conducting threat hunting activities, performing vulnerability scanning and penetration testing, implementing personnel security measures, employing physical security measures, implement network security solutions, employing endpoint security solutions, applying data security measures, employing identity and accessing management measures, establishing incident management capabilities, retaining digital forensics services and utilisation of artificial Intelligence (AI) methods to prevent insider attacks.
- Draw up a security policy on insider threats, based on user awareness, wich is one of the most effective controls for this type of cyberthreat.
- Implement robust technical controls. Traditional security measures tend to focus on external threats, but these are usually not efficient at identifying internal risks emanating from inside the organisation. To protect assets, implement tools such as data loss prevention (DLP) to prevent data exfiltration.[1]

- Reduce the number of users with privileges and access to sensitive information. If an employee doesn’t need to have access to some information to do their work, it is better to restrict what they can see, thus avoid improper access.[17]
- Harden the digital environment, which includes tightening up the security of the network, systems, applications, data and accounts.[1]

References

1. “Insider Threat Report”, 2019. Verizon. https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

2. “Insider Threat Statistics Facts and Figures“. Ekran System. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

3. “CyberEdge 2019 CDR Report” 2019. CyberEdge. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

4. “Corporate Security Predictions 2020”. 2019. December 3, 2019. Kapersky.

https://securelist.com/corporate-security-predictions-2020/95387/

5. “Famous Insider Threat Cases” September 2019. Security Boulevard. https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/

6. “The rise of insider threats: Key trends to watch” 2019. Tech Beacon.

https://techbeacon.com/security/rise-insider-threats-key-trends-watch

7. “Cost of Cybercrime study” 2019. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

8. “Cost of Insider Threats”, 2020. Observer IT. https://www.observeit.com/cost-of-insider-threats/

9. “Cybersecurity Insiders 2019 Insider Threat Report”, 2019. Help Systems.https://www.helpsystems.com/cta/2019-cybersecurity-insiders-insider-threat-report

10. “Forcepoint Insider threat Data Protection” 2017. Force Point.

https://www.forcepoint.com/sites/default/files/resources/files/brochure_insider_threat_data_protection_en.pdf

11. “State of Insider Threats in the Digital Workplace” 2019. Better Cloud. https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

12. “Insider Data Breach Survey 2019”. 2019. Egress. https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

13. “Insider Threat Report”. 2019. Nucleos Cyber. https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf

14. “Insider Threat Report”. 2019. Haystax. https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

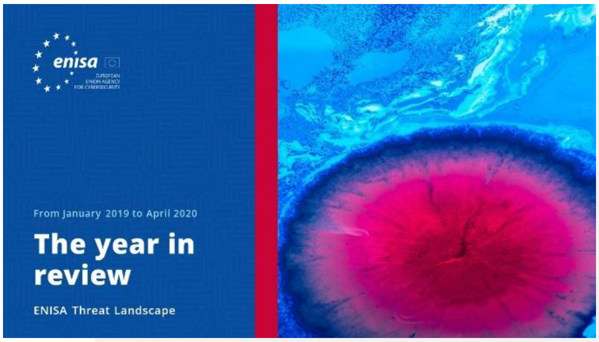
15. “Insider Threat Report”. 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

16. “Kaspersky Industrial CyberSecurity: solution overview 2019”. 2019. Kaspersky. https://ics.kaspersky.com/media/KICS-Solution-overview-2019-EN.pdf

17. “Post-vacation cybersecurity tuneup: Get your company ready!”. September 1, 2017. Panda. https://www.pandasecurity.com/mediacenter/adaptive-defense/cyber-security-get-company-ready/

> **“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



From January 2019 to April 2020

The year in review

ENISA Threat Landscape

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

From January 2019 to April 2020

ENISAs' list of top 15 threats

ENISA Threat Landscape

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

From January 2019 to April 2020

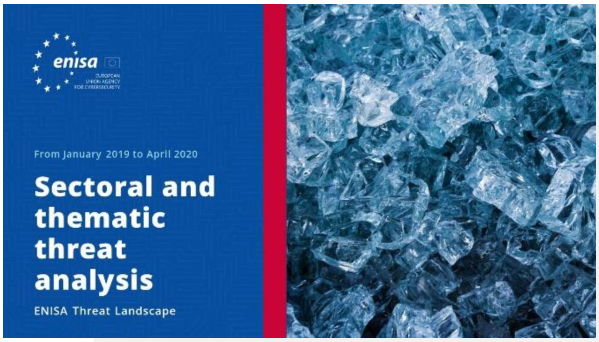
Research topics

ENISA Threat Landscape

ENISA Threat Landscape Report **Research topics**

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

READ THE REPORT



From January 2019 to April 2020

Sectoral and thematic threat analysis

ENISA Threat Landscape

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

Contextualised threat analysis between January 2019 and April 2020.

READ THE REPORT

From January 2019 to April 2020

Emerging trends

ENISA Threat Landscape

ENISA Threat Landscape Report **Emerging trends**

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

READ THE REPORT

From January 2019 to April 2020

Cyberthreat intelligence overview

ENISA Threat Landscape

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

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

READ THE REPORT

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.

Copyright Notice

© European Union Agency for Cybersecurity (ENISA), 2020
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover: © Wedia. For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

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

All rights reserved. Copyright ENISA 2020.

https://www.enisa.europa.eu