EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Physical manipulation/ damage/ theft/ loss

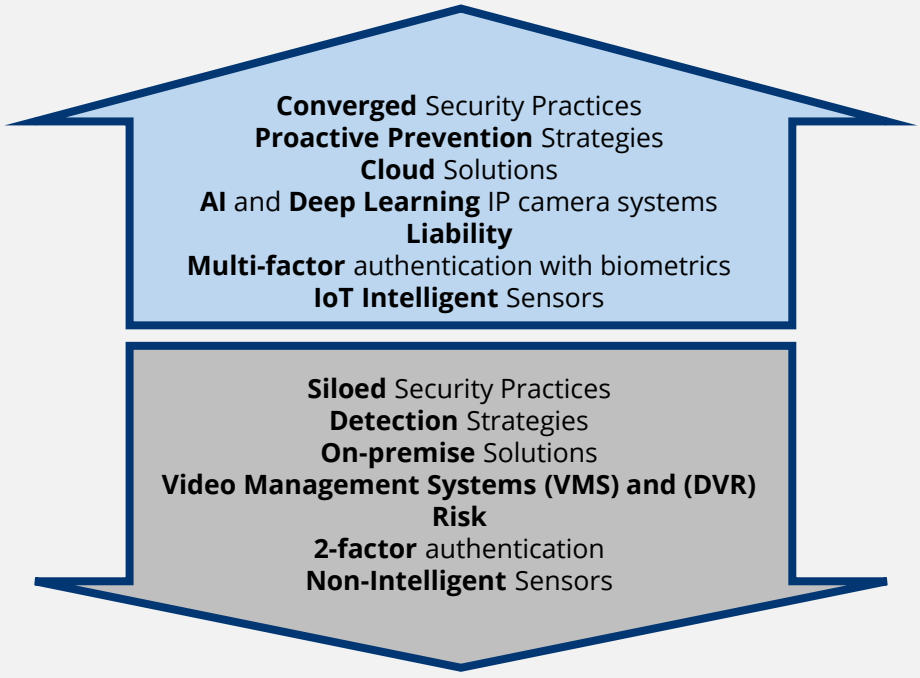
ENISA Threat Landscape

Overview

Physical tampering, damage, theft and loss has drastically changed in the past few years. The integrity of devices is vital for technology to become mobile and for most implementations of the Internet of Things (IoT). IoT can enhance physical security with more advanced and complex solutions.[1] This way, IP security-based systems with smart sensors, Wi-Fi cameras, smart security lighting, drones and electronic locks can provide surveillance data that are evaluated by Artificial Intelligence (AI) and Machine Learning (ML) mechanisms to identify threats and respond with minimum delay and maximum accuracy.[2] However, intelligent buildings, mobile devices and smart wearables can be exploited to bypass physical security measures.[3]

In 2019, ATM and POS related physical attacks continued in Europe and worldwide, but the resulting losses were lower than the average over the past decade. The good news is that the companies, IT managers and decision makers are leaning towards hybrid cyber and physical security plans, although in the past physical security was not a priority.

_New and outdated security practices

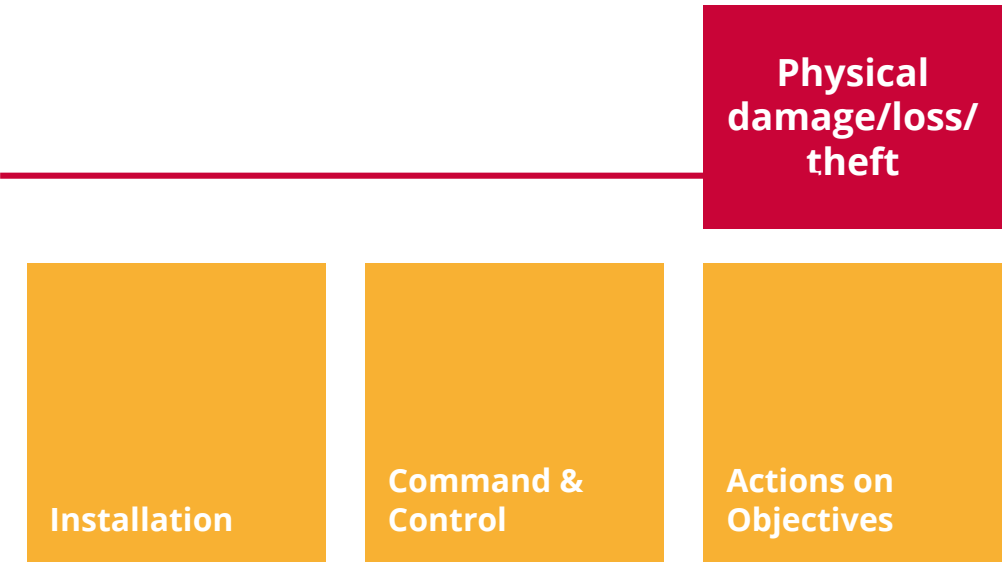


Source: Boonedam blog[4]

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

Trends

_Physical access is the biggest backdoor

In April 2019, Vishwanath Akuthota, pleaded guilty to vandalism, having destroyed equipment with an electric charge using a malicious USB device. The devices destroyed were owned by the College of Saint Rose in Albany, New York, the college Akuthota had graduated from. For the purpose of this attack, he accessed 66 workstations and numerous monitors and digital podiums. The 'USB killer' key he used was purchased online. The college spent more than US $50.000 (ca. €42.452) replacing the equipment and more than US $7.000 (ca. €5.943) in paying the employee who dealt with this incident. Akuthota faced 10 years imprisonment and a maximum fine of US $250.000 (ca. €212.257).[5]

_Physical security lacks corporate attention

During 2019, various surveys of physical security took place. Some of these surveys focused on CEOs, IT managers and decision-makers across several industries, and the results give a good idea on how physical security is handled within companies. CEOs across industry sectors appeared to lean towards a combined cyber and physical security plan to protect their assets against threats, considering factors such as insider threats, the importance of infrastructure and the integrity of the company's networks. In these combined security plans, the most emphasis, budget and personnel were given to investments in cybersecurity (i.e. 83-86% of the respective resources), while 14-17% of the company's resources were spent on physical security. In Europe, the majority of IT managers (77%) stated that the physical security of their company's assets was outdated.[7]

_Physical security as-a-service

A trend in 2019 was enhancing physical security by enabling hosted security solutions. The majority of IT managers' security plans had already shifted towards cloud-and IoT-enabled scheme or they were planning to make this shift in a 12-month period. The decision-makers reported that they were already evaluating video surveillance-as-a-service (VSaaS) and access control as-a-service (ACaaS) solutions to improve incident detection and minimum response times and reduce false positive rates. VSaaS and ACaaS improved both physical security and cybersecurity, although just a few of the IT managers identified physical security as their priority.[8]

_ATMs' physical security failed the test of time

Just as was observed in 2018, in this reporting period, ATMs were vulnerable to tampering and physical damage with the ultimate goal of stealing the cash within. In Ireland nine incidents were reported in Q1 2019 alone.[9] Some of the attackers were very dramatic using stolen diggers, breaking down walls, and scooping the ATMs into vans or cars. In other cases, the attacks were completed within minutes using explosives, chain lassoing, and ram-raiding.[10] In the Netherlands, 71 ATM bombing attacks (Plofkraken in Dutch) took place in one November's weekend alone, compared with 43 similar attacks during the whole of 2018. ABN AMRO bank was forced to remove 470 vulnerable ATMs, and the Dutch Banking Association (NVB) decided to shut down all cash machines nation-wide every night between 11 p.m. and 7 a.m. during December.[11] 2019 is the fourth consecutive year that physical attacks on ATMs haves increased.

Trends

ATM tampering

During 2019, the main expressions of ATM tampering were card trapping, cash trapping and transaction reversal fraud. The big picture for the year is that ATM and petrol pump tampering decreased, thanks to the increase in EMV payments. The EMV standard, named after the three companies that introduced it (i.e. Europay, Mastercard, and Visa), describes the specifications for smart cards, payment terminals and ATMs. EMV cards (aka Chip and PIN or chip cards) integrated circuit chips. The adoption of EMV cards disrupted card-present fraud, at least partially.[12] Unfortunately, EMV cards have not yet been widely implemented outside Europe and even within Europe, only a few countries have adopted geo control, an EMV card's anti-fraud utility.[13]

Incidents

- Killer USB breach highlights need for physical security. Vishwanath Akuthota, an alumnus of the College of Saint Rose in Albany, New York, pleaded guilty for vandalising equipment using a malicious USB device.[5]
- Crooks use digger to steal ATMs in Northern Ireland. The number of physical attacks on ATMs is rising across the EU.[9]
- Dutch Plofkraken. Explosive attacks (known as 'Plofkraken') Dutch ATMs. Mostly focused on ABN AMRO bank's machines because of a vulnerability. It led the bank to remove about 470 of its cash machines across the Netherlands.[11]

Findings

4%_ of breaches were caused by physical actions[12]

20%_ of cybersecurity incidents started or ended with a physical action[12]

5th_ most implemented malicious action on assets was physical attacks on ATMs[12]

54%_ of data breaches across all sectors included a physical attack as the main method

48%_ of IT managers use cloud-based video surveillance or access control[8]

72%_ of employees consider leaving sensitive information in publicly accessible areas the most serious threat to data security[14]

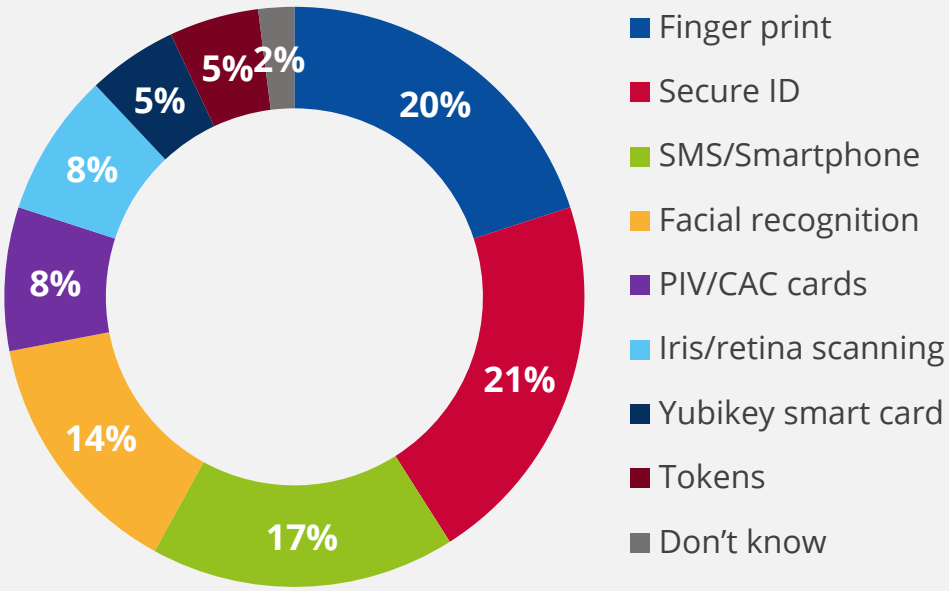
65%_ of over 1.000 employees surveyed reported behaving in ways and adopting practices identified as risky for physical security[15]

Mitigation

Proposed actions

- Use encryption in all information storage and flow that is outside the security perimeter (devices, networks, cloud services, etc.).
- Use asset inventories to keep track of users' devices and remind owners to check availability.
- Ensure limited access to areas containing sensitive information or equipment.
- Implement well-documented physical security policies and integrate physical security measures with digital ones to achieve a holistic approach.
- Use insurance policies to cover losses to both physical and cyber-related risks.
- Develop user guides for mobile devices (smartphones, tablets, laptops, etc.) and follow best practices.
- Establish well-communicated procedures for the physical protection of assets, including loss, damage and theft.
- Ensure that devices are disposed after personal or sensitive information had been securely deleted.[6]
- Reduce the response time for theft, damage and loss incidents.
- Implement multi-factor authentication combining user credentials with biometrics, smart cards or other physical tokens.[16]
- Inspect devices periodically for alterations or replacements.[6]
- Implement processes to detect authorized visitors or employees and assign proper access rights.[6]
- Implement access monitoring systems, access control systems, strong access credentials, and smart access devices (e.g. smart locks, smart keys) for areas housing sensitive equipment.[6]

Most preferable alternatives for user's credentials in MFA



Source: ORACLE & KPMG[16]

References

1. "Physical Security Guide". Kisi. https://pages.getkisi.com/physical-security-guide

2. Jonathan Wackrow. "Security Convergence: Addressing Evolving Cyber and Physical Security Threats". 2019. Teneo. https://www.teneo.com/vision-book/2019/security-convergence-addressing-evolving-cyber-and-physical-security-threats/

3. Pierluigi Paganini. "Modern Physical Security Awareness Is More Than Dumpster Diving [Updated 2019]". August 27, 2019. Infosec Institute. https://resources.infosecinstitute.com/modern-physical-security-awareness-is-more-than-dumpster-diving/#gref

4. Pierre Bourgeix. "2019: What's In & Out in Physical Security". 2019. Boon Edam. https://blog.boonedam.us/2019-whats-in-out-in-physical-security

5. Danny Bradbury. "Killer USB Breach Highlights Need For Physical Security". April 23, 2019. Infosec Magazine. https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1/

6. "PCI DSS Quick Reference." July 2018. PCI Security Standards Council. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

7. "76% Security Professionals Face Cybersecurity Skills Shortage: Report." May 7.2020. CISOMAG. https://cisomag.eccouncil.org/security-leaders-lack-cybersecurity-skills/

8. '2019 Landscape Report: Hosted Security Adoption In Europe.' 2019. Morphean. https://morphean.com/whitepaper/

9. Catalin Cimpanu. "Crooks use digger to steal ATMs in Northern Ireland as ATM physical attacks rise across the EU." April 16, 2019. ZDNet. https://www.zdnet.com/article/crooks-use-digger-to-steal-atms-in-northern-ireland-as-atm-physical-attacks-rise-across-the-eu/

10. Jovi Umawing. "Everything you need to know about ATM attacks and fraud: Part 1." May 29, 2019. Malwarebytes Labs. https://blog.malwarebytes.com/101/2019/05/everything-you-need-to-know-about-atm-attacks-and-fraud-part-1/

11. 'ATM Explosive Attacks - Dutch ATMs to be shut down overnight to counter ATM explosive attacks.' December 19, 2019. European Association for Secure Transactions (EAST). https://www.association-secure-transactions.eu/dutch-atms-to-be-shut-down-overnight-to-counter-atm-explosive-attacks/

12. '2019 Payment Security Report', 2019 Data Breach Investigations Report. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

13. "2019 Payment Threats and Fraud Trends Report." December 9, 2019. European Payments Council. https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report

14. "2019 Eye on Privacy Report." 2019. MediaPRO. https://pages.mediapro.com/Eye-on-Privacy-Report-2019-LP.html

15. 'Report: 2020 State of Privacy and Security Awareness." 2020. MediaPRO. https://www.mediapro.com/report-2020-state-of-privacy-security-awareness/

16. "Oracle and KPMG Cloud Threat Report." 2019. ORACLE & KPMG. https://www.oracle.com/fr/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf


“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

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

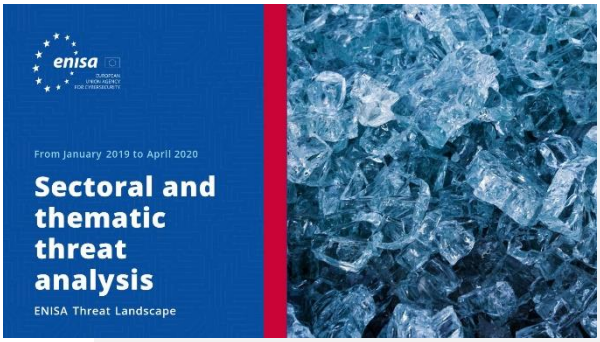
ENISA Threat Landscape Report
List of Top 15 Threats

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