enisa

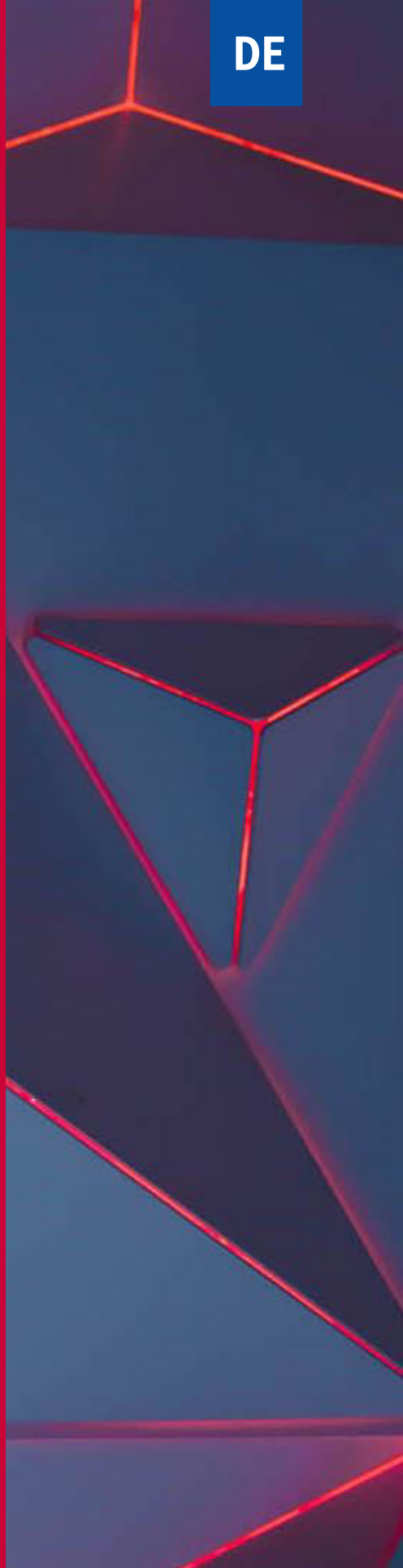
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Physische Manipulation / Schäden / Diebstahl / Verlust

ENISA Threat Landscape



Überblick

Physische Manipulationen, Schäden, Diebstahl und Verluste haben sich in den letzten Jahren drastisch verändert. Die Integrität von Geräten ist entscheidend für die Mobilität der Technologie und für die meisten Implementierungen des Internet der Dinge (IoT). IoT kann die physische Sicherheit mit fortschrittlicheren und komplexeren Lösungen verbessern.[1] Auf diese Weise können IP-sicherheitsbasierte Systeme mit intelligenten Sensoren, Wi-Fi-Kameras, intelligenter Sicherheitsbeleuchtung, Drohnen und elektronischen Schlössern Überwachungsdaten bereitstellen, die von Künstlicher Intelligenz (KI) und Mechanismen des maschinellen Lernens (ML) ausgewertet werden, um Bedrohungen zu identifizieren und mit minimaler Verzögerung und maximaler Genauigkeit zu reagieren.[2] Intelligente Gebäude, mobile Geräte und intelligente Wearables können jedoch auch genutzt werden, um physische Sicherheitsmaßnahmen zu umgehen.[3]

Im Jahr 2019 wurden in Europa und weltweit weiterhin physische Angriffe im Zusammenhang mit Geldautomaten und POS durchgeführt. Die daraus resultierenden Verluste lagen jedoch unter dem Durchschnitt des letzten Jahrzehnts. Die gute Nachricht ist, dass sich Unternehmen, IT-Manager und Entscheidungsträger auf hybride Pläne für Cyber- und physische Sicherheit konzentrieren, obwohl physische Sicherheit in der Vergangenheit keine Priorität hatte.

_Neue und veraltete Sicherheitspraktiken

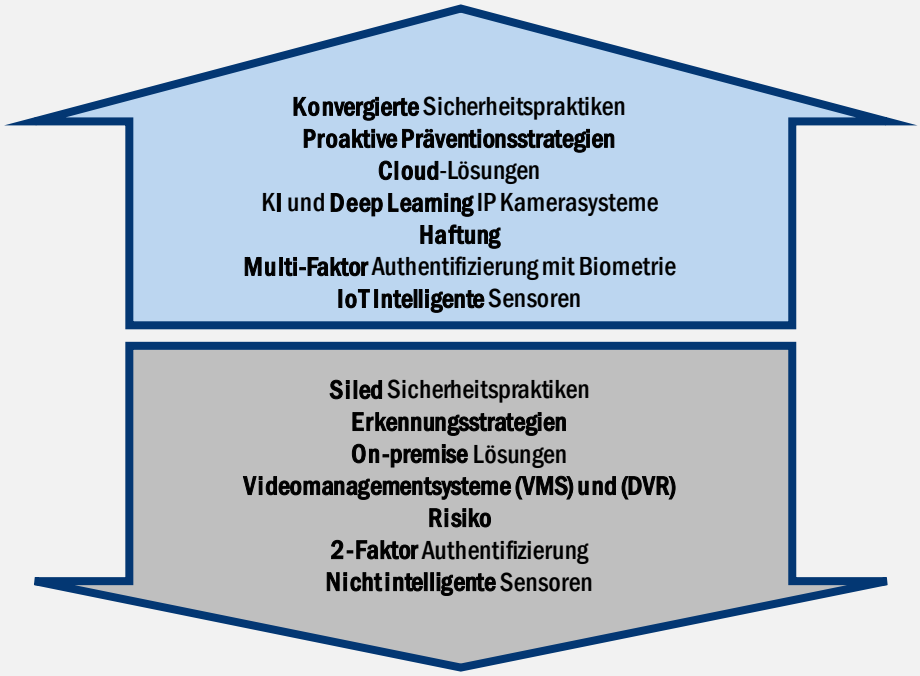
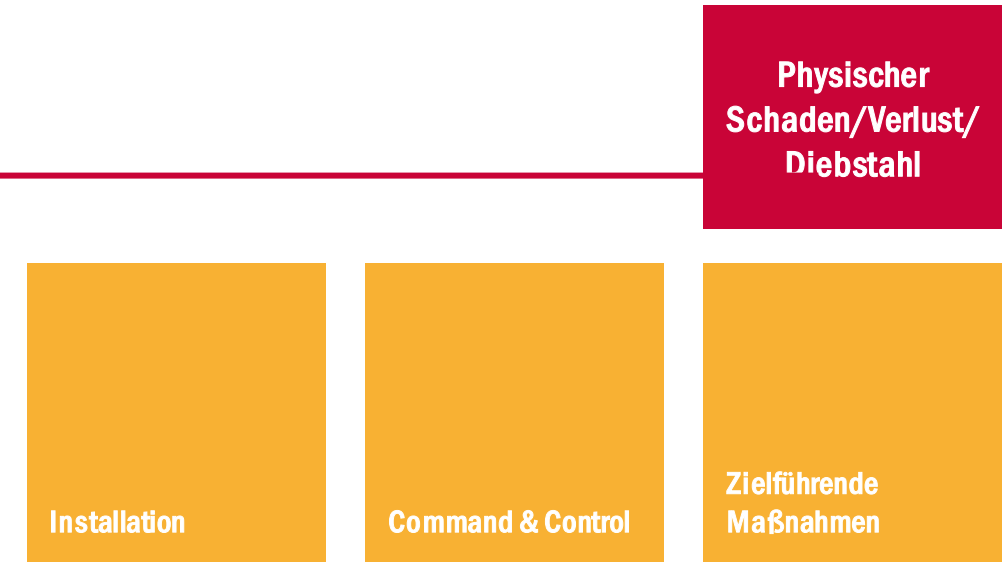


Abbildung 1 - Quelle: Boonedam blog[4]

Kill chain

Schritt des Angriffs-Workflows

Umfang des Zwecks



Das Cyber Kill Chain® Framework wurde von Lockheed Martin entwickelt und basiert auf einem militärischen Konzept, das mit der Struktur eines Angriffs zusammenhängt. Um einen bestimmten Angriffsvektor zu untersuchen, verwenden Sie dieses Kill-Chain-Diagramm, um jeden Schritt des Prozesses sowie die vom Angreifer verwendeten Hilfsmittel, Techniken und Verfahren festzuhalten.

WEITERE INFORMATIONEN

Entwicklung

_ Der physische Zugang ist die größte Hintertür

Im April 2019 bekannte sich Vishwanath Akuthota des Vandalismus schuldig, nachdem er Geräte mit einer elektrischen Ladung unter Verwendung eines böswilligen USB-Geräts zerstört hatte. Die zerstörten Geräte gehörten dem College of Saint Rose in Albany, New York, an dem Akuthota seinen Abschluss gemacht hatte. Für diesen Angriff griff er auf 66 Arbeitsplatzspeicher und zahlreiche Monitore und digitale Podien zu. Der von ihm verwendete „USB-Killer"-Schlüssel wurde online gekauft. Das College gab mehr als 50.000 USD (ca. 42.452 EUR) für den Austausch der Ausrüstung und mehr als 7.000 USD (ca. 5.943 EUR) für die Bezahlung des Mitarbeiters aus, der sich mit diesem Vorfall befasst hatte. Akuthota wurde mit einer Freiheitsstrafe von 10 Jahren und einer Höchststrafe von 250.000 USD (ca. 212.257 EUR) bestraft.[5]

_ Die physische Sicherheit wird von Unternehmen vernachlässigt

Im Jahr 2019 fanden verschiedene Erhebungen zur physischen Sicherheit statt. Einige dieser Umfragen konzentrierten sich auf CEOs, IT-Manager und Entscheidungsträger in verschiedenen Branchen. Die Ergebnisse geben einen guten Überblick über den Umgang mit physischer Sicherheit in Unternehmen. CEOs tendieren branchenübergreifend offenbar zu einem kombinierten Plan für Cyber- und physische Sicherheit, um ihre Vermögenswerte vor Bedrohungen zu schützen. Dabei wurden Faktoren wie Insider-Bedrohungen, die Bedeutung der Infrastruktur und die Integrität der Unternehmensnetzwerke berücksichtigt. In diesen kombinierten Sicherheitsplänen wurde der Schwerpunkt, das Budget und das Personal auf Investitionen in die Cybersicherheit gelegt (d. h. 83-86 % der jeweiligen Ressourcen), während 14-17 % der Ressourcen des Unternehmens für physische Sicherheit ausgegeben wurden. In Europa gab die Mehrheit der IT-Manager (77 %) an, dass die physische Sicherheit der Vermögenswerte ihres Unternehmens veraltet sei.[7]

_Physische Sicherheit als Dienstleistung

Ein Trend im Jahr 2019 war die Verbesserung der physischen Sicherheit durch die Aktivierung gehosteter Sicherheitslösungen. Die meisten Sicherheitspläne von IT-Managern hatten sich bereits auf Cloud- und IoT-fähige Systeme verlagert, oder sie planten, diese Verschiebung in einem Zeitraum von 12 Monaten vorzunehmen. Die Entscheidungsträger gaben an, dass sie bereits VSaaS- (Video Surveillance-as-a-Service) und ACaaS-Lösungen (Access Control as-a-Service) evaluierten, um die Erkennung von Vorfällen und minimale Reaktionszeiten zu verbessern und die Anzahl falsch positiver Ergebnisse zu verringern. VSaaS und ACaaS verbesserten sowohl die physische Sicherheit als auch die Cybersicherheit, obwohl nur einige der IT-Manager die physische Sicherheit als ihre Priorität identifizierten.[8]

_Die physische Sicherheit von Geldautomaten hat den Test der Zeit nicht bestanden

Wie bereits im Jahr 2018 festgestellt wurde, waren Geldautomaten in diesem Berichtszeitraum anfällig für Manipulationen und physische Schäden mit dem Ziel, das darin enthaltene Geld zu stehlen. In Irland wurden allein im ersten Quartal 2019 neun Vorfälle gemeldet.[9] Einige der Angreifer gingen auf drastische Art vor, als sie gestohlene Bagger verwendeten, Mauern einrissen und die Geldautomaten in Lieferwagen oder Autos schaufelten. In anderen Fällen wurden die Angriffe innerhalb von Minuten mit Sprengstoff, Ketten-Lasso und Rammangriffen durchgeführt.[10] In den Niederlanden fanden allein an einem Novemberwochenende 71 Bombenangriffe auf Geldautomaten („Plofkraken“ auf Niederländisch) statt, verglichen mit 43 ähnlichen Angriffen in ganz 2018. Die ABN AMRO Bank musste 470 gefährdete Geldautomaten entfernen, und der niederländische Bankenverband (NVB) beschloss, im Dezember jeden Abend zwischen 23.00 Uhr und 7.00 Uhr morgens landesweit alle Geldautomaten abzuschalten.[11] 2019 ist das vierte Jahr in Folge, dass physische Angriffe auf Geldautomaten zugenommen haben.

Entwicklungen

_ Geldautomatenmanipulation

Im Jahr 2019 waren die häufigsten Ausprägungen von Geldautomatenmanipulationen das Einfangen von Karten, das Einfangen von Bargeld und der Betrug bei der Umkehrung von Transaktionen. Das große Bild für das Jahr ist, dass die Manipulationen an Geldautomaten und Tankstellen dank der gestiegenen EMV-Zahlungen zurückgegangen sind. Der EMV-Standard, benannt nach den drei Unternehmen, die ihn eingeführt haben (Europay, Mastercard und Visa), beschreibt die Spezifikationen für Smartcards, Zahlungsterminals und Geldautomaten. EMV-Karten (auch bekannt als Chip und PIN- oder Chipkarten) mit Mikrochips. Die Einführung von EMV-Karten hat den Betrug durch den Einsatz von Karten zumindest teilweise gestört.[12] Leider wurden EMV-Karten außerhalb Europas noch nicht umfassend eingeführt, und selbst innerhalb Europas haben nur wenige Länder die Geokontrolle eingeführt, das Betrugsbekämpfungsprogramm für EMV-Karten.[13]

_Vorfälle

- Killer USB-Verstöße unterstreichen die Notwendigkeit physischer Sicherheit. Vishwanath Akuthota, ein Absolvent des College of Saint Rose in Albany, New York, bekannte sich schuldig, Geräte mit einem böswilligen USB-Gerät zerstört zu haben.[5]
- Gauner benutzen Bagger, um Geldautomaten in Nordirland zu stehlen. Die Zahl der physischen Angriffe auf Geldautomaten steigt in der EU.[9]
- Das niederländische „Plofkraken“. Explosive Angriffe (bekannt als „Plofkraken") auf niederländische Geldautomaten. Aufgrund einer Sicherheitslücke hauptsächlich auf die Maschinen der ABN AMRO Bank ausgerichtet. Es veranlasste die Bank, etwa 470 ihrer Geldautomaten in den Niederlanden zu entfernen.[11]

Erkenntnisse

4 % der Verstöße wurden durch physische Aktionen verursacht[12]

20 % der Cybersicherheitsvorfälle starteten oder endeten mit einer physischen Aktion[12]

5. häufigste implementierte böswillige Aktion auf Ressourcen waren physische Angriffe auf Geldautomaten[12]

54 % der Datenschutzverletzungen über alle Sektoren hinweg beinhaltete einen physischen Angriff als Hauptmethode

48 % der IT-Manager verwenden Cloud-basierte Videoüberwachung oder Zugangskontrolle[8]

72 % der Mitarbeiter halten vertrauliche Informationen in öffentlich zugänglichen Bereichen für die größte Bedrohung für die Datensicherheit[14]

65 % der über 1.000 befragten Mitarbeiter gaben an, Verhaltensweisen und Praktiken anzuwenden, die als riskant für die physische Sicherheit eingestuft wurden[15]

Minderung

Vorgeschlagene Maßnahmen

- Verwenden Sie die Verschlüsselung in allen Informationsspeichern und -flüssen außerhalb des Sicherheitsbereichs (Geräte, Netzwerke, Cloud-Dienste usw.).
- Verwenden Sie Inventare über Ihre Ressourcen, um die Geräte der Benutzer zu verfolgen und die Eigentümer daran zu erinnern, die Verfügbarkeit zu überprüfen.
- Sorgen Sie für einen eingeschränkten Zugang zu Bereichen, die vertrauliche Informationen oder Geräte enthalten.
- Implementieren Sie gut dokumentierte Richtlinien für die physische Sicherheit und integrieren Sie physische Sicherheitsmaßnahmen in digitale, um einen ganzheitlichen Ansatz zu erzielen.
- Verwenden Sie Versicherungspolicen, um Verluste sowohl bei physischen als auch bei Cyber-Risiken abzudecken.
- Entwickeln Sie Benutzerhandbücher für mobile Geräte (Smartphones, Tablets, Laptops usw.) und befolgen Sie die beste Praxis.
- Richten Sie gut kommunizierte Verfahren zum physischen Schutz von Vermögenswerten ein, einschließlich Verlust, Beschädigung und Diebstahl.
- Stellen Sie sicher, dass Geräte erst entsorgt werden, nachdem persönliche oder vertrauliche Informationen sicher gelöscht wurden.[6]
- Reduzieren Sie die Reaktionszeit bei Diebstahl, Beschädigung und Verlust.
- Implementieren Sie eine Multi-Faktor-Authentifizierung, bei der Benutzeranmeldedaten mit biometrischen Daten, Smartcards oder anderen physischen Token kombiniert werden.[16]
- Überprüfen Sie die Geräte regelmäßig auf Änderungen oder Austausch.[6]
- Implementieren Sie Prozesse, um autorisierte Besucher oder Mitarbeiter zu erkennen und ordnungsgemäße Zugriffsrechte zuzuweisen.[6]
- Implementieren Sie Zugriffsüberwachungssysteme, Zugriffskontrollsysteme, sichere Zugriffsdaten und intelligente Zugriffsgeräte (z. B. intelligente Schlösser, intelligente Schlüssel) für Bereiche, in denen sensible Geräte untergebracht sind.[6]

_Am meisten bevorzugte Alternativen für Benutzer-Anmeldedaten in MFA

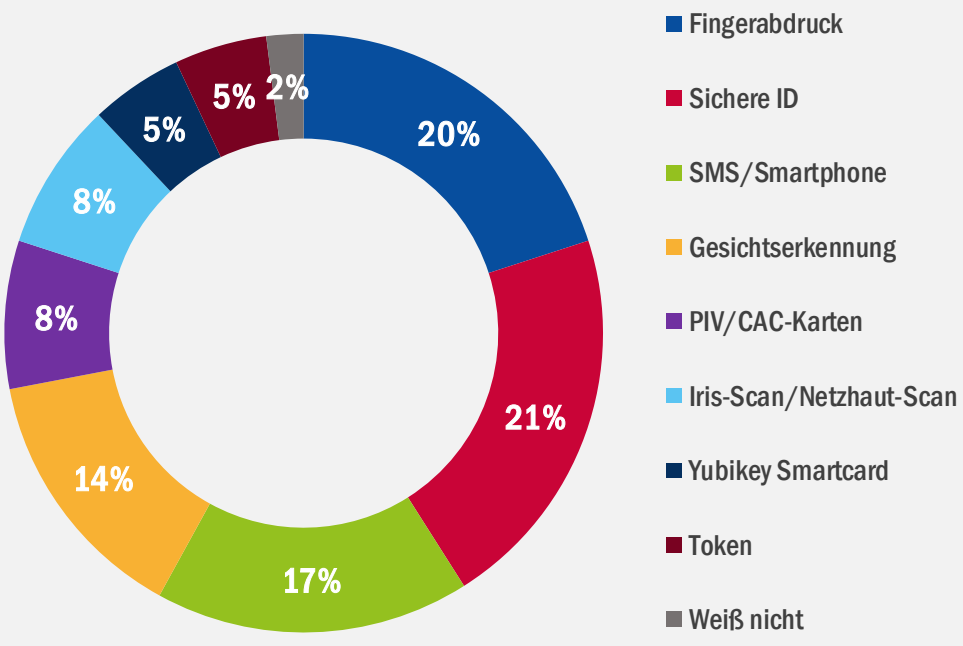


Abbildung 2 - Quelle: ORACLE & KPMG[16]

Literaturangaben

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]". 27. August, 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". 23. April, 2019. Infosec Magazine. https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1/

6 "PCI DSS Quick Reference." Juli 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." 7. Mai, 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." 16. April, 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." 29. Mai, 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.' 19. Dezember, 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." 9. Dezember, 2019. European Payments Council. https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report

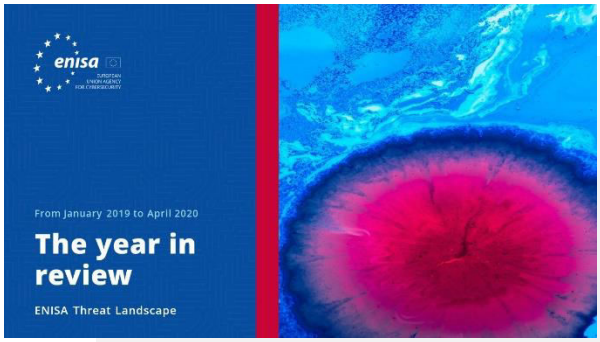
14. "2019 Eye on Privacy Report." 2019. MediaPRO. https://pages.mediapro.com/Eye-on-Privacy-Report-2019-LP.html

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


"Im nächsten Jahrzehnt werden Cybersicherheitsrisiken aufgrund der zunehmenden Komplexität der Bedrohungslandschaft, des kontroversen Ökosystems und der Erweiterung der Angriffsfläche schwieriger zu bewerten und zu interpretieren sein."
In ETL 2020

Themenbezogen



ENISA Threat Landscape Bericht **Das Berichtsjahr**

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Liste der 15 größten Bedrohungen**

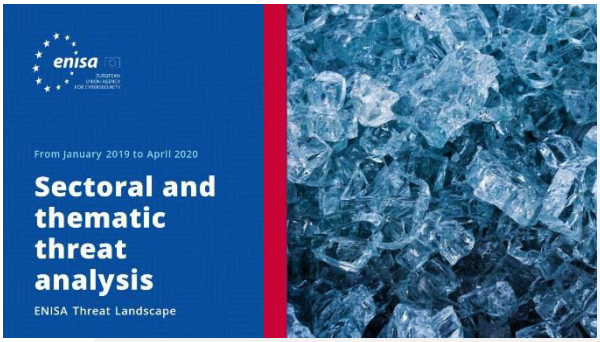
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Forschungsthemen**

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

LESEN SIE DEN BERICHT



ENISA Threat Landscape-Bericht
Sektorale und thematische Bedrohungsanalyse

Kontextualisierte Bedrohungsanalyse zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Aufkommende Trends

Die bedeutendsten Cybersicherheitstrends, die zwischen Januar 2019 und April 2020 beobachtet wurden.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Übersicht über Cyber Threat Intelligence

Der aktuelle Stand der Cyber Threat Intelligence in der EU.

LESEN SIE DEN BERICHT

Über

_ Die Agentur

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur der Europäischen Union für Cybersicherheit wurde 2004 gegründet und durch das EU-Gesetz zur Cybersicherheit gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von ICT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, sie kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Information über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Mitwirkende

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) und *alle Mitglieder der ENISA CTI Interessenvertreter:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) und Thomas Hemker.

Herausgeber

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

Kontaktangaben

Für Fragen über dieses Dokument, verwenden Sie bitte enisa.threat.information@enisa.europa.eu.
Für Medienanfragen zu dieser Stellungnahme verwenden Sie bitte die folgenden Kontaktangaben: press@enisa.europa.eu.

Wir würden gerne Ihr Feedback zu diesem Bericht erhalten!
Bitte nehmen Sie sich einen Moment Zeit, um den Fragebogen auszufüllen. Um das Formular zu öffnen, können Sie hier klicken.

Impressum/Rechtshinweise

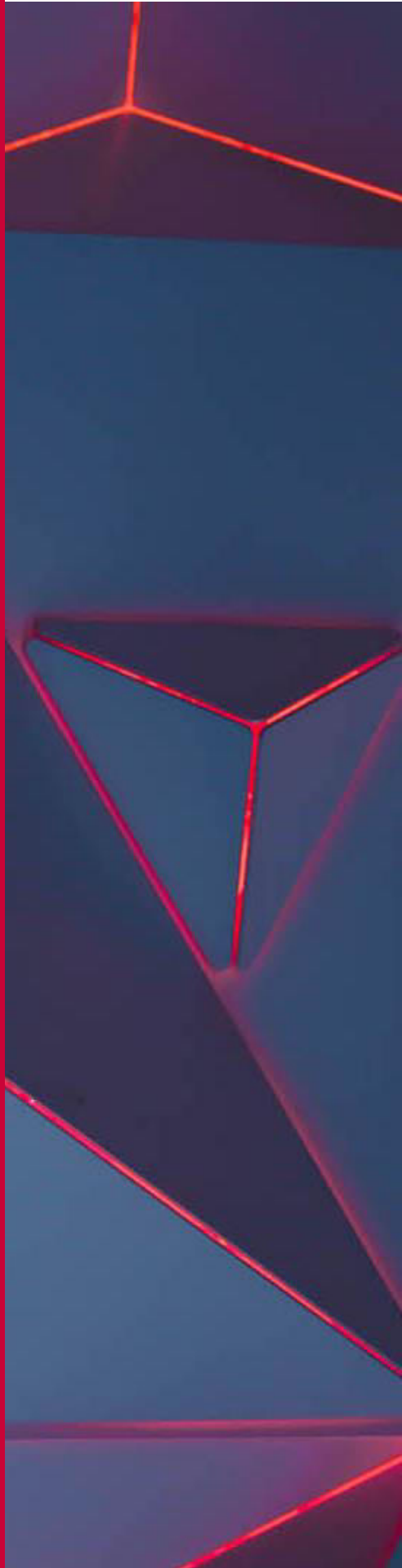
Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann in angemessenen Abständen aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Informationszwecke gedacht. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

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

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Griechenland
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