enisa

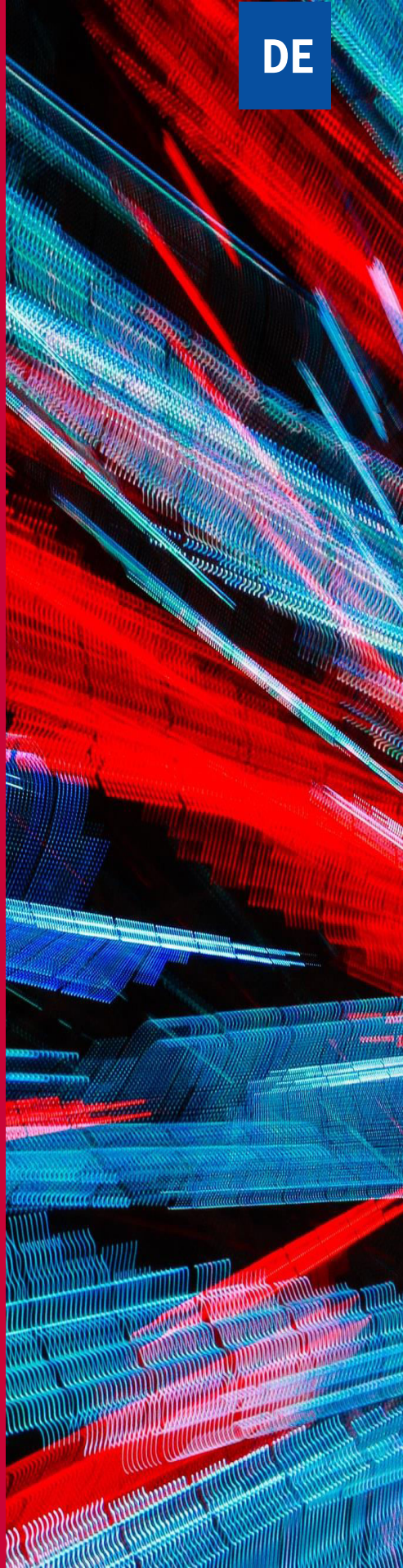
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Aufkommende Trends

ENISA Threat Landscape



Überblick

_Was ist zu erwarten?

Zu Beginn eines neuen Jahrzehnts können wir erhebliche Veränderungen in der Art und Weise erwarten, wie wir Cybersicherheit oder die Sicherheit des Cyberspace wahrnehmen und verstehen. Der Cyberspace im Sinne von **ISO/IEC 27032:2012**[1] **ist eine „komplexe Umgebung, die sich aus der Interaktion von Personen, Software und Diensten im Internet durch damit verbundene technologische Geräte und Netzwerke ergibt, die in keiner physischen Form existiert".** Der Schutz dieser komplexen Umgebung wird noch schwieriger, da wir mehr Menschen, Geräte, Systeme verbinden und mehr Prozesse und Dienste im Netzwerk ausführen. Wir sind auch mehr von seiner Zuverlässigkeit, Integrität, Verfügbarkeit und Vertrauenswürdigkeit abhängig, um zu arbeiten, in Beziehung zu treten und viele unserer täglichen Aktivitäten auszuführen. Mit dieser wachsenden Abhängigkeit ergeben sich für böswillige Akteure mehr Möglichkeiten, den Cyberspace zu nutzen, um Personen und Organisationen zu manipulieren, einzuschüchtern, zu täuschen, zu belästigen und zu betrügen. Der Schutz von Einzelpersonen, Unternehmen und Organisationen bei der Nutzung des Cyberspace wird sich im Laufe des nächsten Jahrzehnts tendenziell von der traditionellen Netzwerk- und Informationssicherheit (NIS) zu einem umfassenderen Konzept mit Inhalten und Diensten verlagern.

Während des letzten Jahrzehnts hat die „vierte industrielle Revolution" das Tempo des Wandels erheblich beschleunigt und das verändert, *was* Menschen tun, *wie* sie es tun, welche Fähigkeiten erforderlich sind, wo Arbeit geleistet wird, wie Arbeitsbeziehungen strukturiert sind und wie Arbeit organisiert ist, sowie verteilt und belohnt wird.

Aufgrund der aktuellen COVID-19-Pandemie beginnen wir das Jahrzehnt mit einer neuen Norm und tiefgreifenden Veränderungen in der physischen Welt und im Cyberspace. Mit sozialer Distanzierung oder Beschränkung neigen Menschen dazu, den virtuellen Raum zu nutzen, um zu kommunizieren, Beziehungen miteinander und Kontakte zu knüpfen. Diese neue Norm wird neue Herausforderungen in der digitalen Wertschöpfungskette und insbesondere in der Cybersicherheitsbranche mit sich bringen.

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.

Es sind zu viele Variablen zu berücksichtigen, um das Cyber-Risikomanagement effektiv zu gestalten. Ein wichtiger Faktor ist die technologische Vielfalt, die die meisten Unternehmen heute erleben. Ein weiterer Aspekt ist die Weiterentwicklung von Programmen, Taktiken, Techniken und -verfahren (TTPs), mit denen Gegner Angriffe ausführen. Böswillige Akteure passen die TTPs nach Bedarf an die Umgebung ihres Opfers an und arbeiten mit anderen zusammen, um ihre Ziele zu erreichen.

Das Definieren einer Risikostellung, das Verwalten von Daten, das Anwenden relevanter Metriken und das Reagieren auf Änderungen sind Hindernisse für die Entwicklung einer effektiven Strategie zur Steuerung des Cyber-Risikos. **Während des nächsten Jahrzehnts werden neue Ansätze erforderlich sein, um sich von der Siloanalyse fernzuhalten und sich einer Matrix von miteinander verbundenen Faktoren, Variablen und Bedingungen zu nähern.** Dies ist eine große Herausforderung für viele Unternehmen, die versuchen, ihre Infrastruktur, ihren Betrieb und ihre Daten vor stärkeren, besser ausgestatteten und ausgerüsteten Gegnern zu schützen.

Aufkommende Trends

Zehn Cybersicherheitsherausforderungen

01_Umgang mit systemischen und komplexen Risiken

Das Cyber-Risiko ist durch die Geschwindigkeit und das Ausmaß seiner Verbreitung sowie die potenzielle Absicht von Bedrohungsakteuren gekennzeichnet. Die Vernetzung verschiedener Systeme und Netzwerke ermöglicht eine schnelle und weite Verbreitung von Cyber-Vorfällen, wodurch es schwieriger wird, Cyber-Risiken zu bewerten und zu mindern.

02_Weite Verbreitung der Erkennung kontroverser KI.

Die Erkennung von Bedrohungen, die KI ausnutzen, um einen Angriff zu starten oder eine Erkennung zu vermeiden, wird eine große Herausforderung für die Zukunft der Cyber-Abwehrsysteme darstellen.[14]

03_Reduzierung unbeabsichtigter Fehler.

Mit der wachsenden Anzahl von Systemen und Geräten, die mit dem Netzwerk verbunden sind, sind unbeabsichtigte Fehler weiterhin eine der am häufigsten ausgenutzten Sicherheitslücken bei Cybersicherheitsvorfällen. Neue Lösungen zur Reduzierung dieser Fehler werden einen wichtigen Beitrag zur Reduzierung der Anzahl von Vorfällen leisten.

04_Bedrohungen der Lieferkette und Dritter.

Die diversifizierte Lieferkette, die die heutige Technologiebranche kennzeichnet, bietet Bedrohungsakteuren neue Möglichkeiten, diese komplexen Systeme zu nutzen und die vielfältigen Schwachstellen auszunutzen, die durch ein heterogenes Ökosystem von Drittanbietern verursacht werden.[16]

05_Sicherheits-Orchestrierung und Automatisierung.

Cyber Threat Intelligence und Verhaltensanalysen werden mit der Automatisierung von Prozessen und Analysen an Bedeutung gewinnen. Durch Investitionen in Automatisierung und Orchestrierung können
Cybersicherheitsfachleute in die Entwicklung robusterer Cybersicherheitsstrategien investieren.

06_Reduzierung von Fehlalarmen.

Dieses lange erwartete Versprechen ist der Schlüssel für die Zukunft der Cybersicherheitsbranche und für den Kampf gegen die Alarmmüdigkeit.

07_Zero-Trust Sicherheitsstrategien.

Angesichts des zunehmenden Drucks auf IT-Systeme aufgrund neuer Geschäftsanforderungen wie ortsungebundenes Arbeiten, Digitalisierung des Geschäftsmodells und Datenausbreitung wird von vielen Entscheidungsträgern Zero-Trust als die Lösung de facto zur Sicherung von Unternehmensressourcen angesehen.

08_Migrationsfehler in der Enterprise Cloud.

Da viele Unternehmen ihre Daten auf Cloud-basierte Lösungen migrieren, erhöht sich die Anzahl der Konfigurationsfehler, wodurch Daten einem potenziellen Missbrauch ausgesetzt werden. Cloud-Dienstanbieter werden das Problem beheben, indem sie Systeme implementieren, die diese Art von Fehlern automatisch identifizieren.

09_Hybride Bedrohungen.

Neue Vorgehensweisen sind anfällig für Bedrohungen der virtuellen und physischen Welt. Die Verbreitung von Desinformation oder gefälschten Nachrichten ist beispielsweise ein wesentlicher Bestandteil der hybriden Bedrohungslandschaft. Das EUvsDisinfo[15] ist ein Vorzeigeprojekt der East StratCom Task Force des Europäischen Auswärtigen Dienstes, die eingerichtet wurde, um der Desinformationsgefahr zu begegnen.

10_Die Attraktivität der Cloud-Infrastruktur als Ziel wird zunehmen.

Die zunehmende Abhängigkeit von der öffentlichen Cloud-Infrastruktur erhöht das Risiko von Ausfällen. Fehlkonfigurationen von Cloud-Ressourcen sind nach wie vor die Hauptursache für Cloud-Angriffe, aber Angriffe, die direkt auf die Cloud-Dienstanbieter abzielen, werden bei Hackern immer beliebter.

Aufkommende Trends

Ausgaben für Cybersicherheit

Laut Gartner[17], werden viele Vorstände nach Jahren intensiver Investitionen in die Cybersicherheit bessere Daten und ein besseres Verständnis der Renditen verlangen. Dies ist hauptsächlich auf wachsende Ausgaben für Cybersicherheit zurückzuführen, die proportional zu den Investitionen in neue Technologien sind. Laut einem Bericht von IDC[22], beliefen sich die Ausgaben für Cybersicherheit im Jahr 2019 auf 103 Milliarden USD (ca. 87,5 Milliarden EUR), also 9,4 % mehr als im Vorjahr. Sicherheitsmanager werden in Kürze auf die Ergebnisse jahrelanger Investitionen überprüft und sind unerlässlich, um verbesserte Daten über die erzielten Ergebnisse zu erhalten.

Cyber Threat Intelligence hilft bei der Definition von Cybersicherheitsstrategien

Cyber Threat Intelligence (CTI)[7] soll Organisationen dabei unterstützen, besser vorbereitet zu sein, indem sie ihr Wissen über die Bedrohungslandschaft verbessern. Anstatt sich ausschließlich auf Informationen zu stützen, die von internen Systemen oder Feeds generiert werden (was über das Bekannte bekannt ist), wird die Wirksamkeit von CTI durch das Wissen über das *Warum*, das *Wie* und das, was dem Cybersicherheitsteam unbekannt ist, bestimmt. Das Wertversprechen einer CTI-Funktion oder eines CTI-Programms besteht darin, die Bereitschaft des Unternehmens zu verbessern, seine kritischen Vermögenswerte vor unbekannten Bedrohungen zu schützen.

Die Bedrohungslandschaft kennen

Da mehr Automatisierung und Orchestrierung der Cybersicherheit als wachsender Trend angesehen werden, werden **Cybersicherheitsteams weniger Zeit für die Überwachung von Aktivitäten und mehr für Bereitschafts- und Vorbereitungsaufgaben aufwenden.** Eine gut konzipierte CTI-Funktion kann kontextbezogenes und umsetzbares Wissen über Bedrohungen bereitstellen, um strategische, operative und taktische Stakeholder im gesamten Unternehmen zu informieren. In der Praxis sollte eine CTI-Fähigkeit darauf abzielen, die folgenden Fragen unter Berücksichtigung der Anforderungen der Interessenvertreter sowie des Kontextes und der Umgebung der Organisation zu beantworten:

- Was ist die Angriffsfläche?
- Was sind die wertvollsten Vermögenswerte und das Cyber-Terrain?
- Was sind die kritischsten Schwachstellen?
- Was sind die am häufigsten verwendeten Angriffsmethoden?
- Wie verhalten sich Gegner normalerweise und wie gehen sie vor?
- Wie sieht die Bedrohungslandschaft aus für:
    - den Sektor und die Art von Geschäften, die die Organisation betreibt?
    - das technologische Umfeld, in dem die Organisation aktivist?
- Was muss getan werden, um die Risiken dieser Bedrohungen zu mindern, und wer tut dies?

Mangel an Cybersicherheitskompetenzen

Der Mangel an hochqualifizierten Technologiefachleuten ist bereits ein Problem für Europas Digitalisierungsambitionen. Laut einer Studie[23] geben über 70 % der europäischen Unternehmen an, dass mangelnde Qualifikation ihre Anlagestrategien behindert, während 46 % der Unternehmen Schwierigkeiten bei der Besetzung von Stellen aufgrund von Fachkräftemangel in Schlüsselbereichen wie der Cybersicherheit melden.

Aufkommende Trends

Fünf Trends in Bezug auf Cyberbedrohungen

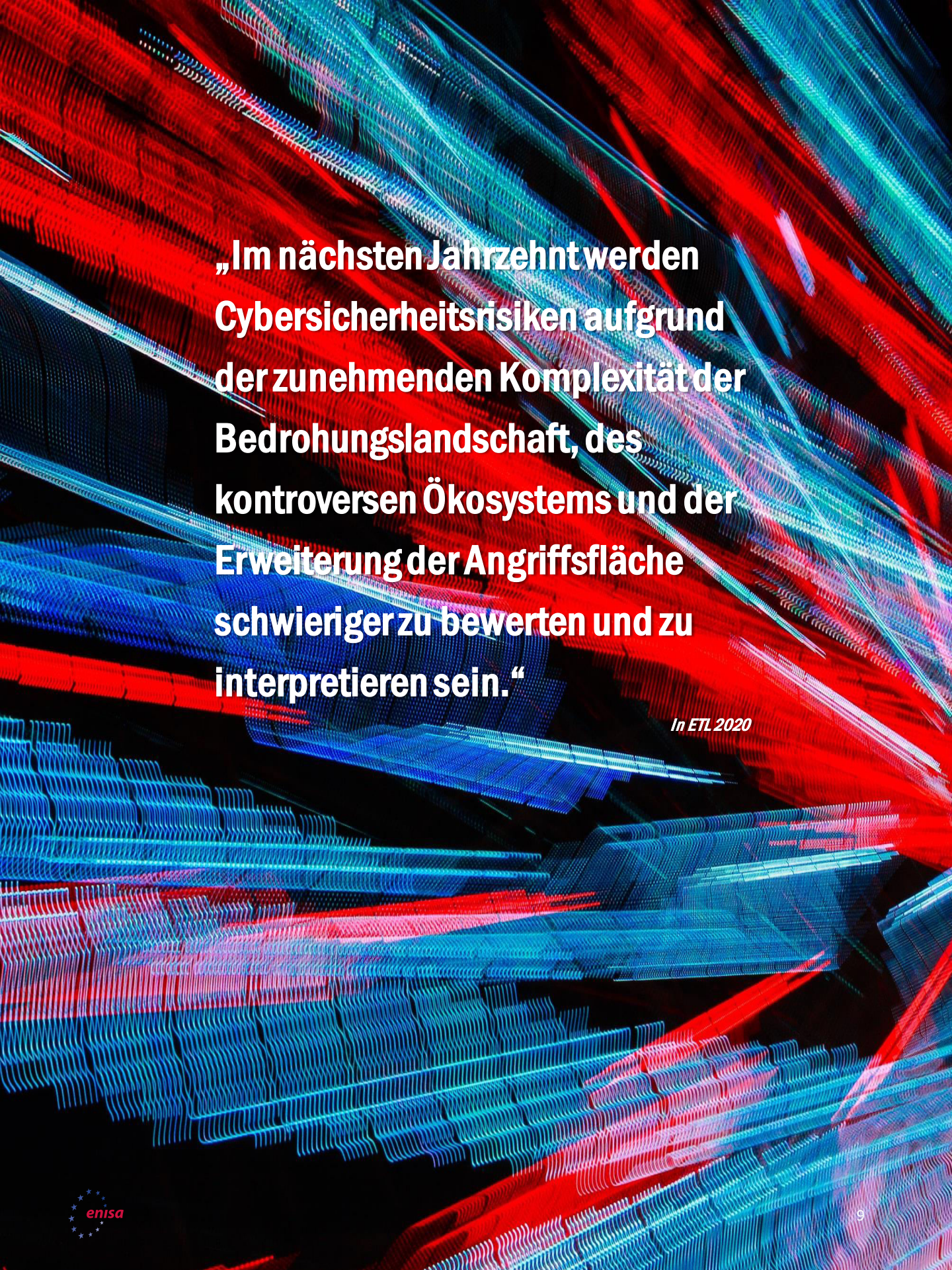
01_Malware erhält ein Upgrade. Stämme der Malware Familie werden auf neue Versionen mit zusätzlichen Funktionen, Verteilungs- und Weitergabemechanismen aktualisiert. Emotet zum Beispiel, eine Malware, die ursprünglich 2014 als Banking-Trojaner entwickelt wurde, hat sich zu einem der effektivsten Malware-Distributoren von 2019 entwickelt.[2]

02_Bedrohungen werden vollständig mobil. Benutzer sind zunehmend auf mobile Geräte angewiesen, um ihre sensibelsten Konten zu sichern. Die Verwendung von 2fa, das an einen App-Authentifikator oder über eine Textnachricht gebunden ist, ist eines der Beispiele. Da immer mehr Malware vollständig mobil ist, machen betrügerische Apps, SIMJacking und Betriebssystem-Exploits diese Geräte zum schwächsten Glied und sind daher äußerst anfällig für Angriffe.

03_Angreifer verwenden neue Dateitypen wie Disc-Image-Dateien (ISO und IMG) zur Verbreitung von Malware. DOC-, PDF-, ZIP- und XLS-Dateien sind nach wie vor der am häufigsten verwendete Anhangstyp für die Verbreitung von Malware, andere Typen werden jedoch immer beliebter. Einige Kampagnen zur Verbreitung von AgentTesla InfoStealer und NanoCore RAT wurden 2019 unter Verwendung des Bilddateityps gefunden.

04_Zunahme gezielter und koordinierter Ransomware-Angriffe. Im Jahr 2019 kam es zu einer Eskalation hochentwickelter und gezielter Ransomware -Exploits, wobei der öffentliche Sektor, Gesundheitsorganisationen und bestimmte Branchen ganz oben auf der Liste standen. Angreifer verbringen mehr Zeit damit, Informationen über ihre Opfer zu sammeln, genau zu wissen, was zu verschlüsseln ist, um maximale Störungen und höhere Lösegeldbeträge zu erzielen.

05_Angriffe mit Ausfüllen von Anmeldedaten sind weit verbreitet. Das Ausfüllen von Anmeldedaten - das automatische Einfügen gestohlener Kombinationen aus Benutzernamen und Passwort durch umfangreiche automatisierte Anmeldeanfragen, die gegen eine Webanwendung gerichtet sind - wird sich aufgrund eines Jahrzehnts mit einer abnormalen Anzahl von Datenschutzverletzungen und Billionen gestohlener personenbezogener Daten vermehren.


„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

Aufkommende Trends

Zehn aufkommende Trends in Bezug auf Angriffsvektoren

01_ Angriffe werden mit kurzer Dauer und größerer Wirkung massiv verteilt

Diese Angriffe sollen die höchstmögliche Anzahl von Geräten betreffen, die personenbezogene Daten stehlen oder den Zugriff auf Daten durch Verschlüsselung der Dateien blockieren können.

02_ Fein gezielte und anhaltende Angriffe werden sorgfältig mit klar definierten und langfristigen Zielen geplant

Böswillige Akteure planen diese Art von Angriffen, um hochwertige Daten wie Finanzinformationen, geistiges und industrielles Eigentum, Geschäftsgeheimnisse, klassifizierte Informationen usw. zu erhalten.

03_ Böswillige Akteure verwenden digitale Plattformen für gezielte Angriffe

Böswillige Akteure untersuchen das Potenzial digitaler Plattformen zur Unterstützung gezielter Angriffe (z. B. soziale Medien, Spiele, Messaging, Streaming usw.). Von Diebstahl personenbezogener Daten für Spear-Phishing-Angriffe bis hin zur breiten Verbreitung von Malware sind digitale Plattformen mit einer hohen Anzahl von Abonnenten effiziente Angriffsvektoren, die bei böswilligen Akteuren immer beliebter werden.

04_ Die Nutzung von Geschäftsprozessen wird zunehmen

Mit mehr Automatisierung und weniger menschlichem Eingreifen können Geschäftsprozesse böswillig geändert werden, um Gewinn für einen Angreifer zu generieren. Diese allgemein als Business Process Compromise (BPC) bekannte Technik wird von verfahrenstechnischen Spezialisten häufig unterbewertet, da keine ordnungsgemäße Risikobewertung vorliegt.

05_ Die Angriffsfläche wird immer größer

E-Mail ist nicht mehr das wichtigste und einzige Werkzeug und der Hauptangriffsvektor für Phishing. Böswillige Akteure nutzen jetzt andere Plattformen, um zu kommunizieren und um Opfer zum Öffnen gefährdeter Webseiten zu bewegen. Ein neuer Trend zeichnet sich durch die Verwendung von SMS, WhatsApp, SnapChat und Social Media Messenger ab.

06_Telearbeit wird über Heimgeräte genutzt

Mit vermehrtem Arbeiten im Home-Office und dem Verbinden ihrer Geräte mit Unternehmensnetzwerken steigt das Risiko, neue Einstiegspunkte für Angreifer zu eröffnen. Mit der COVID-19-Pandemie wird dieser Trend IT-Manager dazu drängen, die Sicherheitsrichtlinien zu verschärfen und dringende Änderungen an der IT-Infrastruktur vorzunehmen.

07_Angreifer sind besser vorbereitet

Angreifer wählen ihre Ziele sorgfältig aus, führen Ausspähungen bestimmter Mitarbeiter durch und zielen auf diese mit Spear-Phishing-Angriffen ab, um verwendbare Anmeldedaten für das Unternehmen zu erhalten. Sobald die Angreifer Zugriff auf einen einzelnen Computer erhalten, können sie Penetrationstest-Tools wie Mimikatz verwenden, um Anmeldedaten mit erhöhten Berechtigungen zu sammeln und auszunutzen.

08_Verschleierungstechniken werden verfeinert

Bedrohungsakteure arbeiten kontinuierlich an Innovationen, um Bedrohungen effektiver und weniger anfällig für Erkennungen zu machen. Der Anubis, ein Android-Banking-Trojaner und -Bot, wurde verbreitet, indem er sich als harmlose App tarnte, hauptsächlich über den Google Play Store.[1]

09_Die automatisierte Nutzung nicht gepatchter Systeme und nicht mehr verfügbarer Anwendungen wird zunehmen

Der im Jahr 2019 beobachtete ungewöhnliche Anstieg des Telnet-Verkehrs zu Port 445 enthüllte die Ausweitung von Würmern und Exploits wie Eternal Blue. Telnet, das nur noch im Bereich der IoT-Geräte verwendet wird, verzeichnete in dem Zeitraum die größten Volumina.

10_Cyber-Bedrohungen rücken an den Rand

Edge-Geräte werden an den Grenzen zwischen miteinander verbundenen Netzwerken bereitgestellt. Wir haben einen wachsenden Trend mit Angriffen auf diese Geräte - wie Router, Switches und Firewalls - festgestellt, die erhebliche Auswirkungen auf ein Unternehmen und das verbundene digitale Ökosystem haben.

Literaturangaben

1. "ISO/IEC 27032:2012". ISO https://www.iso.org/standard/44375.html

2. "Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk." 2. April, 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

3. "Understanding the relationship between Emotet, Ryuk and TrickBot." 14. April, 2019. Intel471. https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

4. "Investigating WMI Attacks" 9. Februar, 2019. SANS. https://www.sans.org/blog/investigating-wmi-attacks/

5. "RDP Abuse and Swiss Army Knife Tool Used to Pillage, Encrypt and Manipulate Data" 18. Dezember, 2019. Bitdefender. https://labs.bitdefender.com/2019/12/rdp-abuse-and-swiss-army-knife-tool-used-to-pillage-encrypt-and-manipulate-data/

6 "Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook" 10. Juli, 2019. CNBC. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html

7. "This is how we might finally replace passwords" 27. Mai, 2019. C | Net. https://www.cnet.com/news/this-is-how-we-might-finally-replace-passwords/

9. "Authentication standards to help reduce the world's over-reliance on passwords." FIDO. https://fidoalliance.org/overview/

10. "How Much Cyber Sovereignty is Too Much Cyber Sovereignty?" 3. Oktober, 2019. Council on Foreign Relations. https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

11. "Conceptualising Cyber Arms Races". 2016. NATO. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

12. "Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training" 2018. UNESCO. https://en.unesco.org/fightfakenews

13. "The Big Connect: How Data Science is Helping Cybersecurity". 12. Juni, 2019. Info Security Group. https://www.infosecurity-magazine.com/blogs/data-science-helping-cybersecurity-1/

14. "Are You Ready For The Age Of Adversarial AI? Attackers Can Leverage Artificial Intelligence Too". 9. Januar, 2020. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/are-you-ready-for-the-age-of-adversarial-ai-attackers-can-leverage-artificial-intelligence-too/#2a76dee14703

15. https://euvsdisinfo.eu/

16. "FBI Alerts Companies of Cyber Attacks Aimed at Supply Chains". 21. Februar, 2020. Bitsight. https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains

17. "Gartner Identifies the Top Seven Security and Risk Management Trends for 2019". 5. März, 2019. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma

18. "Android banking trojan." 3. Oktober, 2019. Cyare. https://cyware.com/news/exploring-the-nature-and-capabilities-of-anubis-android-banking-trojan-6ea7dec4

19. "5 Top Trends for Mobile Cyber Security in 2020". 9. Januar, 2020. Corrata. https://corrata.com/5-top-trends-for-mobile-cyber-security-in-2020/

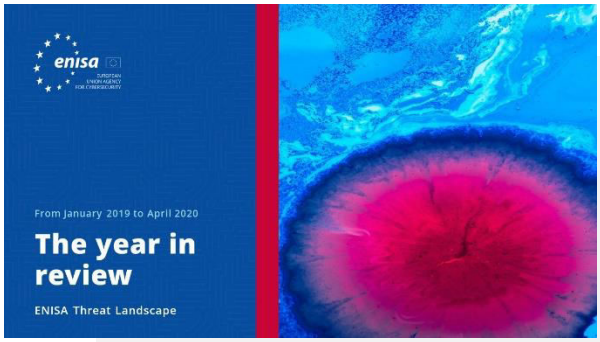
20. "Malicious Attachments Remain a Cybercriminal Threat Vector Favorite". 27. August, 2020 Threat Post. https://threatpost.com/malicious-attachments-remain-a-cybercriminal-threat-vector-favorite/158631/

21. "10 trends shaping the future of work". Oktober 2019. EPSC. https://op.europa.eu/en/publication-detail/-/publication/e77a1580-0cf5-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-121729338

22. "Global security spending to top $103 billion in 2019, says IDC", 20. März, 2019. ZDNet. https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

23. "Insights into skills shortages and skills mismatch. learning from Cedefop's European skills and jobs survey". 2018. CEDEFOP. https://www.cedefop.europa.eu/files/3075_en.pdf

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**

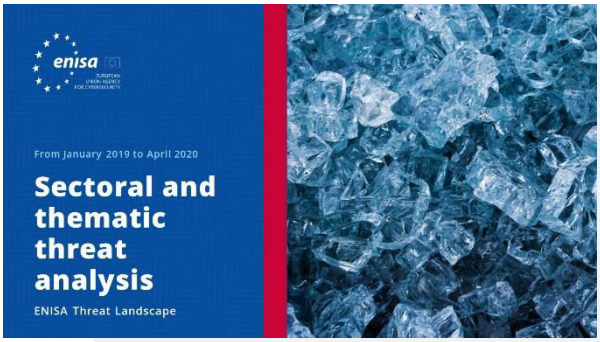
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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.

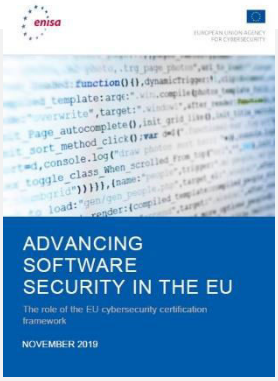
LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Übersicht über Cyber Threat Intelligence

Der aktuelle Stand der Cyber Threat Intelligence in der EU.

LESEN SIE DEN BERICHT

Sonstige Publikationen



Verbesserung der Software-Sicherheit in der EU

Präsentiert Schlüsselelemente der Software-Sicherheit und bietet einen kurzen Überblick über die wichtigsten vorhandenen Ansätze und Standards in der sicheren Software-Entwicklungslandschaft.

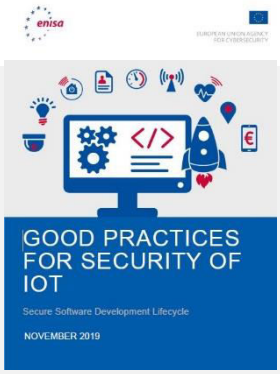
LESEN SIE DEN BERICHT

Beste Praxis der ENISA für die Sicherheit von Smart Cars

Gute Praktiken für die Sicherheit intelligenter Fahrzeuge, nämlich vernetzte und (halb-) autonome Fahrzeuge, um die Erfahrung der Fahrzeugbenutzer zu verbessern und die Fahrzeugsicherheit zu verbessern

.

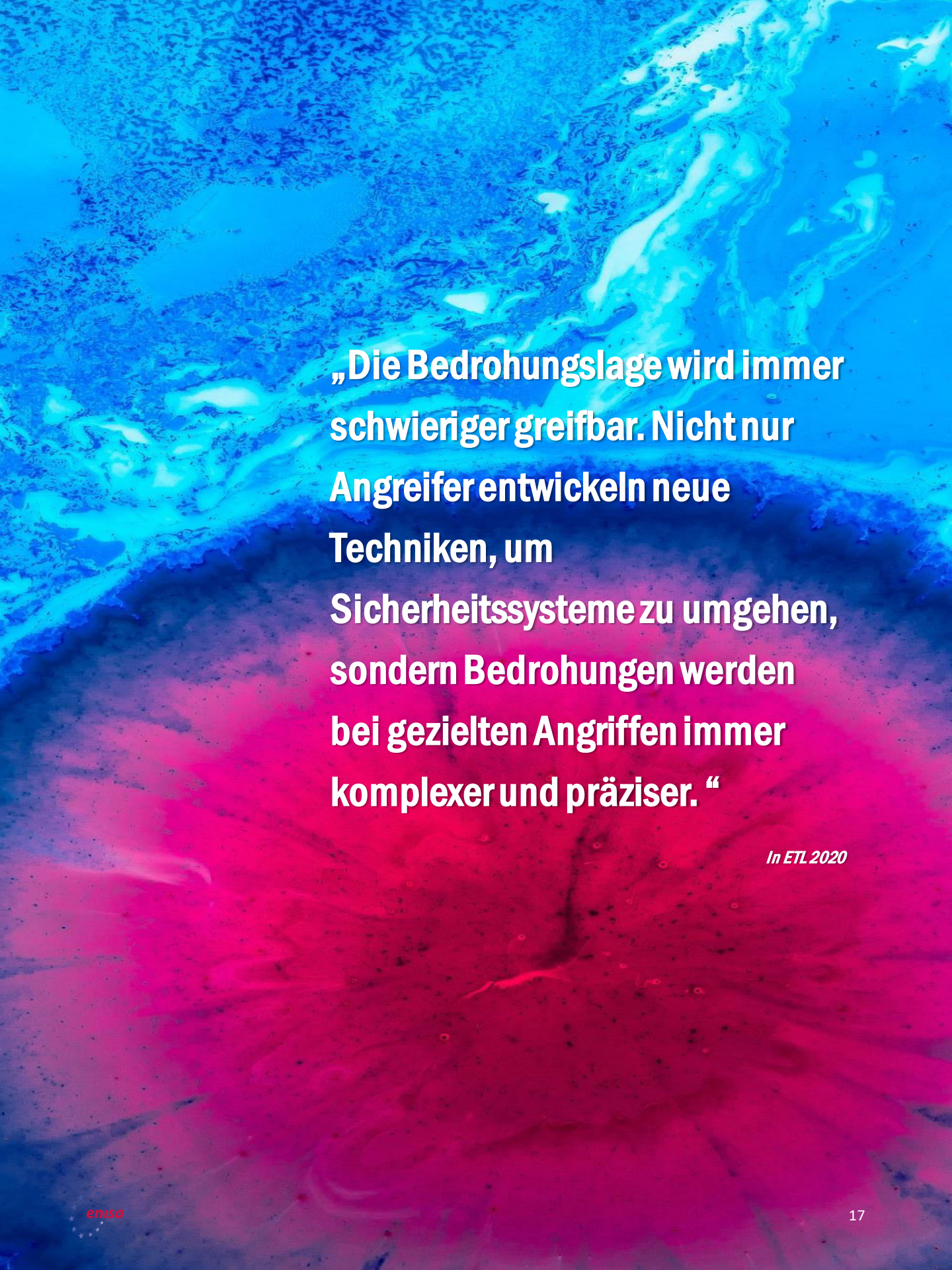
LESEN SIE DEN BERICHT



Gute Praktiken für die Sicherheit von IoT - Sicherer Softwareentwicklungszyklus

ioT-Sicherheit mit besonderem Schwerpunkt auf Richtlinien für die Softwareentwicklung.

LESEN SIE DEN BERICHT


„Die Bedrohungslage wird immer schwieriger greifbar. Nicht nur Angreifer entwickeln neue Techniken, um Sicherheitssysteme zu umgehen, sondern Bedrohungen werden bei gezielten Angriffen immer komplexer und präziser. “
In ETL 2020

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

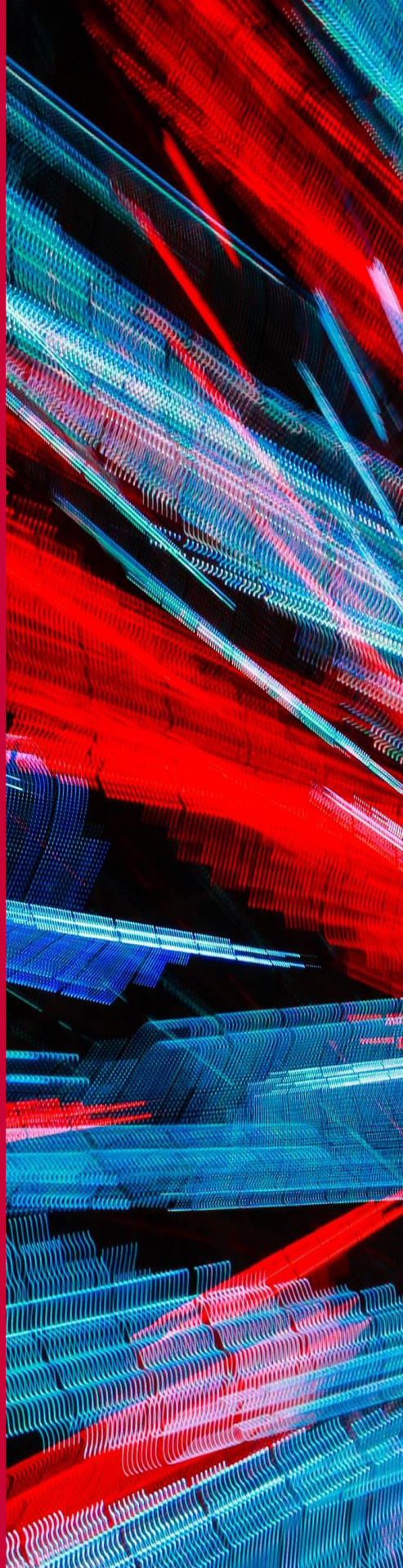
Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung 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