enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Das Jahr im Rückblick

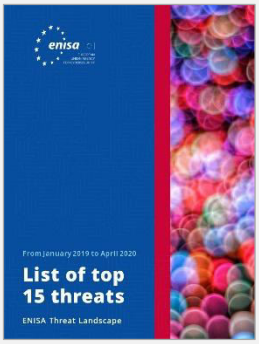
ENISA Threat Landscape

Vor dem Start

_ 8 Jahre Prüfung der Bedrohungslage

In diesem Jahr feiert die **Agentur der Europäischen Union für Cybersicherheit (ENISA)** ein Jahr des neuen Gesetzes über Cybersicherheit und die achte Ausgabe des Threat Landscape Report (ETL). Das Gesetz über die Cybersicherheit[1] überarbeitet und stärkt die Rolle der ENISA, indem es ihr ein dauerhaftes Mandat, mehr Ressourcen und neue Aufgaben erteilt. Darüber hinaus schlägt die Agentur mit einem neuen Geschäftsführer, einer neuen Strategie und einer neuen Organisationsstruktur ein neues Kapitel auf. Angesichts all dieser Änderungen ist es an der Zeit, dass sich auch der ETL ändert und eine neue Struktur und ein modernes Erscheinungsbild annimmt, weg von einem langen und statischen Berichtstyp. Mit seiner neuen visuellen Identität und seinem neuen Format ist der ETL-Bericht zu einem vielseitigen, dynamischen und benutzerfreundlichen digitalen Bericht geworden, der versucht, die Erwartungen eines wachsenden und anspruchsvollen Publikums zu erfüllen.

ETL 2012



ETL 2020

ENISA Threat Landscape Entwicklung von 2012 bis 2020

_ ETL-Format

Diese Ausgabe gibt einen Überblick über die Bedrohungslage im Zeitraum zwischen Januar 2019 und April 2020 und ist folgendermaßen strukturiert.

DAS JAHR IM RÜCKBLICK Dieser Bericht bietet einen allgemeinen Überblick über die Bedrohungslage und beschreibt die wichtigsten Themen, auf die in allen anderen Berichten verwiesen wird. Er enthält auch die ENISA-Liste der 15 wichtigsten Bedrohungen, Schlussfolgerungen und Empfehlungen.

ÜBERSICHT ÜBER CYBERTHREAT INTELLIGENCE. Dieser Bericht fasst die wichtigsten Themen zusammen, die für die Community der Cyber Threat Intelligence (CTI) relevant sind, sowie die Themen, die in verschiedenen Foren diskutiert werden.

SEKTORALE UND THEMATISCHE BEDROHUNGSANALYSE. Dieser Bericht fasst die neuesten Arbeiten von ENISA zusammen und beschreibt die Bedrohungslage für bestimmte Sektoren und Technologien. In diesem Jahr präsentieren wir die Ergebnisse der Arbeit für 5G, das Internet der Dinge (IoT) und Smart Cars.

HAUPTVORFÄLLE IN DER EU UND WELTWEIT. Dieser Bericht bietet einen Überblick über wichtige Cybersicherheitsvorfälle in der EU und weltweit und zeigt die Lehren auf, die wir daraus ziehen können.

FORSCHUNGSTHEMEN Dieser Bericht enthält wichtige Aspekte im Zusammenhang mit der Forschung und Innovation im Bereich der Cybersicherheit.

AUFKOMMENDE TRENDS Dieser Bericht identifiziert aufkommende Trends und konzentriert sich auf die Herausforderungen und Chancen für die Zukunft im Bereich Cybersicherheit.

LISTE DER 15 GRÖSSTEN BEDROHUNGEN. Ein Bericht für jede Bedrohung mit einem allgemeinen Überblick, den Ergebnissen, schwerwiegenden Vorfällen, Statistiken, Angriffsmethoden und entsprechenden Gegenmaßnahmen.

Vor dem Start

Methoden

Der für den ETL-Bericht erstellte Inhalt basiert auf Informationen aus Open Source, hauptsächlich strategischer Natur, und deckt mehr als einen Sektor, eine Technologie und einen Kontext ab. Der Bericht versucht, branchen- und herstellerunabhängig zu sein und verweist oder zitiert die Arbeit aus verschiedenen Sicherheitsforschungen, Sicherheitsblogs und Nachrichtenmedienartikeln, die im gesamten Text in mehreren Endnoten klar angegeben sind.

Bei der Erstellung des ENISA-Berichts über die Bedrohungslage verfolgten wir einen zweigleisigen Ansatz. Zunächst führten wir eine eingehende Recherche der verfügbaren Literatur aus offenen Quellen wie Nachrichtenmedienartikeln, Expertenmeinungen, Geheimdienstberichten, Vorfallanalysen und Sicherheitsforschungsberichten durch. Zweitens führten wir Interviews mit Mitgliedern der ETL-Interessengruppe, die Experten auf diesem Gebiet sind, und Mitgliedern der EU Cyber Threat Intelligence Community. Letztere haben uns geholfen, die Liste der 15 wichtigsten Bedrohungen zu definieren und die Annahmen über die Trends und zukünftigen Herausforderungen in der Cybersicherheit zu validieren.

Wir danken auch den Mitgliedern der CTI Stakeholder Group für die Unterstützung bei der Erstellung der Berichte während dieser acht Ausgaben. Die Mitglieder dieser Gruppe überprüfen und validieren die für jeden ETL-Bericht erstellte Analyse und stimmen über die jährliche Liste der 15 wichtigsten Cyber-Bedrohungen ab.

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.

Wer sollte was lesen?

Der ETL-Bericht ist teils strategisch, teils technisch und enthält Informationen, die sowohl für technisch versierte als auch für nicht versierte Leser relevant sind. Der ETL richtet sich an unterschiedliche Zielgruppen und verwendet je nach Fachgebiet und Bedeutung des Themas für technisch nicht versierte Leser unterschiedliche Niveaus der Fachsprache. In der folgenden Tabelle wird die Art der Zielgruppe und der Inhalt für jeden ETL-Bericht beschrieben.

ETL-BERICHT	ART DES INHALTS	ZIELGRUPPE
DAS JAHR IM RÜCKBLICK	Allgemein	Alle
CTI ÜBERSICHT ↗	Speziell	Mitglieder der CTI-Community und Praktiker.
SEKTORALE UND THEMATISCHE BEDROHUNGSANALYSE ↗	Strategisch	Strategische Managementexperten, politische und allgemeine Entscheidungsträger, Risikoanalysten, Cybersicherheitsmanager und Führungskräfte.
HAUPTVORFÄLLE IN DER EU UND WELTWEIT. ↗	Strategisch	Strategische Managementexperten, politische und allgemeine Entscheidungsträger, Risikoanalysten, Cybersicherheitsmanager und Führungskräfte.
FORSCHUNGSTHEMEN ↗	Strategisch	Strategische Managementexperten, politische und allgemeine Entscheidungsträger, Risikoanalysten, Cybersicherheitsmanager und Führungskräfte.
AUFKOMMENDE TRENDS ↗	Strategisch	Strategische Managementexperten, politische und allgemeine Entscheidungsträger, Risikoanalysten, Cybersicherheitsmanager und Führungskräfte.
LISTE DER 15 GRÖSSTEN BEDROHUNGEN ↗	Technische Maßnahmen	Informationssicherheitsmanager (ISM), Chief Information Security Officers (CISO), Cybersicherheitsspezialisten und CTI-Analysten.

Die 15 größten Bedrohungen

Die größten Bedrohungen 2018		Beurteilte Trends
1	Schadsoftware (Malware)	---
2	Webbasierte Angriffe	↗
3	Angriffe auf Webanwendungen	---
4	Phishing	↗
5	Serviceverweigerung	↗
6	Spam	---
7	Botnetze	↗
8	Datenschutzverletzungen	↗
9	Insider-Bedrohung	↙
10	Physische Manipulation, Beschädigung, Diebstahl und Verlust	---
11	Informationsleck	↗
12	Identitätsdiebstahl	↗
13	Cryptojacking	↗
14	Ransomware	↙
15	Cyberspionage	↙

Die größten Bedrohungen 2019-2020		Beurteilte Trends	Änderung der Reihenfolge
1	Malware ↗	---	---
2	Webbasierte Angriffe ↗	---	↗
3	Phishing ↗	↗	↗
4	Angriffe auf Webanwendungen ↗	---	↙
5	Spam ↗	↙	↗
6	Serviceverweigerung ↗	↙	↙
7	Identitätsdiebstahl ↗	↗	↗
8	Datenschutzverletzungen ↗	---	---
9	Insider-Bedrohung ↗	↗	---
10	Botnetze ↗	↙	↙
11	Physische Manipulation, Beschädigung, Diebstahl und Verlust ↗	---	↙
12	Informationsleck ↗	↗	↙
13	Ransomware ↗	↗	↗
14	Cyberspionage ↗	↙	↗
15	Crytojacking ↗	↙	↙

Legende: Entwicklungen Abnehmend, --- Stabil, Steigend **Rang:** Ansteigend, --- Gleich, Absteigend

Überblick

Was hat sich an der Lage geändert?

Die Jahre 2019 und 2020 brachten erhebliche Veränderungen der in diesen Berichten beschriebenen Cyber-Bedrohungslage mit sich. Zwei unterschiedliche Tatsachen haben wesentlich zu diesen Veränderungen beigetragen: Die historisch einzigartigen, abrupten Transformationskräfte, die durch die Pandemie des **Coronavirus 2019 (COVID-19)** freigesetzt wurden, und der stetig zunehmende Trend bei den **fortgeschrittenen Gegnerfähigkeiten von Bedrohungsakteuren.** Bemerkenswerterweise hat letzterer die Auswirkungen der COVID-19-Pandemie im Cyberraum verstärkt.

Die COVID-19-Pandemie erzwang die groß angelegte Einführung von Technologie, um eine Vielzahl kritischer Aspekte der Krise zu bewältigen, wie z. B. die Koordinierung der Gesundheitsdienste, die internationale Reaktion auf die Verbreitung von COVID-19, die Einführung von Telearbeitssystemen, Fernunterricht und zwischenmenschlicher Kommunikation, Kontrolle von Lockdown-Maßnahmen, Telefonkonferenzen und vieles mehr. Angesichts dieser Situation haben die Unternehmensführer die sich abzeichnenden Risiken einer abrupten (technologischen) Übernahme bewertet, die sich aus der durch die COVID-19-Pandemie erzwungenen Transformation ergeben[2]. **Und die Cybersicherheit war mit einem Paradoxon konfrontiert: Sie war sowohl die Herausforderung als auch die Chance bei dieser Transformation.** Die Änderungen in der IT-Landschaft haben die bestehenden Cybersicherheitsmaßnahmen geschwächt und ihre rasche Anpassung zu einer Herausforderung gemacht. Gleichzeitig **ermöglicht die Cybersicherheit das Vertrauen in neu auftretende Anwendungsfälle für digitale Dienste und bietet somit die Möglichkeit, die Transformation zu erleichtern.**

Während der Arbeit von zu Hause aus **mussten Cybersicherheitsspezialisten vorhandene Abwehrmechanismen an ein neues Infrastrukturparadigma anpassen** und versuchen, das Risiko einer Vielzahl neuartiger Angriffe zu minimieren, bei denen die Einstiegspunkte das mit dem Internet verbundene Heim der Mitarbeiter und andere intelligente Geräte sind. Gleichzeitig und unter hohem Druck mussten sie Lösungen implementieren, die auf zuvor weniger vertrauenswürdigen Komponenten basierten, wie z. B. Fernzugriff über das öffentliche Internet, Cloud-Dienste, ungesicherte Video-Streaming-Dienste sowie mobile Geräte und Apps. Die notwendige Reaktion auf die COVID-19-Pandemie, um die Sicherheit zu gewährleisten und gleichzeitig die Auswirkungen auf Unternehmen zu verringern, hat Unternehmen an die Grenzen ihrer Fähigkeit gebracht, auf Änderungen zu reagieren. Darüber hinaus befanden sich die Cybersicherheitsfachkräfte, die sich schnell an zahlreiche sich ändernde Arbeitsmuster anpassen mussten, an den Grenzen ihrer Kapazitäten.

In kurzer Zeit mussten IT-Sicherheitsexperten schnell auf die Herausforderungen reagieren, die sich aus der Arbeit von zu Hause aus ergaben, z. B. Datenbewegungen von Unternehmen, wenn Mitarbeiter über ihr Heim-Internet auf Cloud-basierte Apps, Unternehmenssoftware, Videokonferenzen und geteilte Datenbanken zugriffen.

Da die COVID-19-Pandemie noch nicht vollständig unter Kontrolle ist und aufgrund der Unsicherheit über ihre künftige Ausbreitung, geht man davon aus, dass sie weiterhin Cybersicherheitsfachleute herausfordern wird. Darüber hinaus wird sie angesichts der verstrichenen Zeit, bevor Vorfälle entdeckt und analysiert werden, noch lange Zeit die Cyber-Bedrohungslage beeinflussen. Die COVID-19-Pandemie zeigte, dass böswillige Akteure über Fähigkeiten verfügten, die es ihnen ermöglichten, sich schnell auf diese Transformation einzustellen. In den Jahren 2019-2020 konzentrierte sich die feindliche Vorgehensweise auf die Personalisierung von Angriffsvektoren. Fortgeschrittene Methoden zum Stehlen von Anmeldedaten, Credential-Stuffing, gezielte Phishing-Angriffe, fortschrittliche Social-Engineering-Angriffe, fortschrittliche Techniken zur Verschleierung von Malware und eine umfassendere Durchdringung mobiler Plattformen sind die bedeutendsten Leistungen der Cyberkriminellen im Berichtszeitraum. Wenn diese beginnen, diese Fortschritte mit künstlicher Intelligenz und maschinellem Lernen zu kombinieren, werden wir in Zukunft mehr erfolgreiche Angriffe und nicht nachweisbare Kampagnen erleben.

Überblick

_ Zusammenfassung

Die folgende Liste fasst die wichtigsten Trends zusammen, die im Berichtszeitraum in Bezug auf die Cyber-Bedrohungslage beobachtet wurden. Diese werden auch in den verschiedenen Berichten, die die Bedrohungslage 2020 beschreiben, ausführlich besprochen.

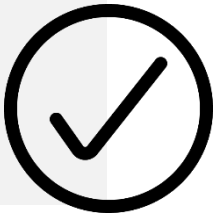
01_ Die Angriffsfläche in der Cybersicherheit nimmt weiter zu, während wir in eine neue Phase der digitalen Transformation eintreten.

02_ Nach der COVID-19-Pandemie wird es eine neue soziale und wirtschaftliche Norm geben, die noch stärker von einem sicheren und zuverlässigen Cyberspace abhängt.

03_ Der Einsatz von Social-Media-Plattformen bei gezielten Angriffen ist ein schwerwiegender Trend und erreicht verschiedene Bereiche und Arten von Bedrohungen.

04_ Fein gezielte und anhaltende Angriffe auf hochwertige Daten (z. B. geistiges Eigentum und Staatsgeheimnisse) werden von staatlich geförderten Akteuren sorgfältig geplant und ausgeführt.

05_ Massiv verteilte Angriffe mit kurzer Dauer und großer Wirkung werden mit mehreren Zielsetzungen
wie dem Diebstahl von Anmeldedaten verwendet.



_ Zusammenfassung

06_ Das Motiv für die meisten Cyberangriffe ist nach wie vor finanzieller Natur.

07_ Ransomware ist nach wie vor weit verbreitet und hat für viele Unternehmen kostspielige Konsequenzen.

08_ Dennoch bleiben viele Cybersicherheitsvorfälle unbemerkt oder es dauert lange, bis sie erkannt werden.

09_ Mit mehr Sicherheitsautomatisierung werden Unternehmen mehr in eine Vorbereitung/Bereitschaft investieren, wobei Cyberthreat Intelligence als Hauptkompetenz verwendet wird.

10_ Die Zahl der Phishing-Opfer wächst weiter, da die menschliche Dimension als schwächstes Glied ausgenutzt wird.

Bei all den Veränderungen in Bezug auf die Cyber-Bedrohungslage und den Herausforderungen, die durch die COVID-19-Pandemie entstanden sind, ist es noch ein langer Weg, bis der Cyberspace zu einer vertrauenswürdigen und sicheren Umgebung für alle wird.

Überblick

_ Sind sich die EU-Bürger der Risiken und Herausforderungen des Cyberspace bewusster?

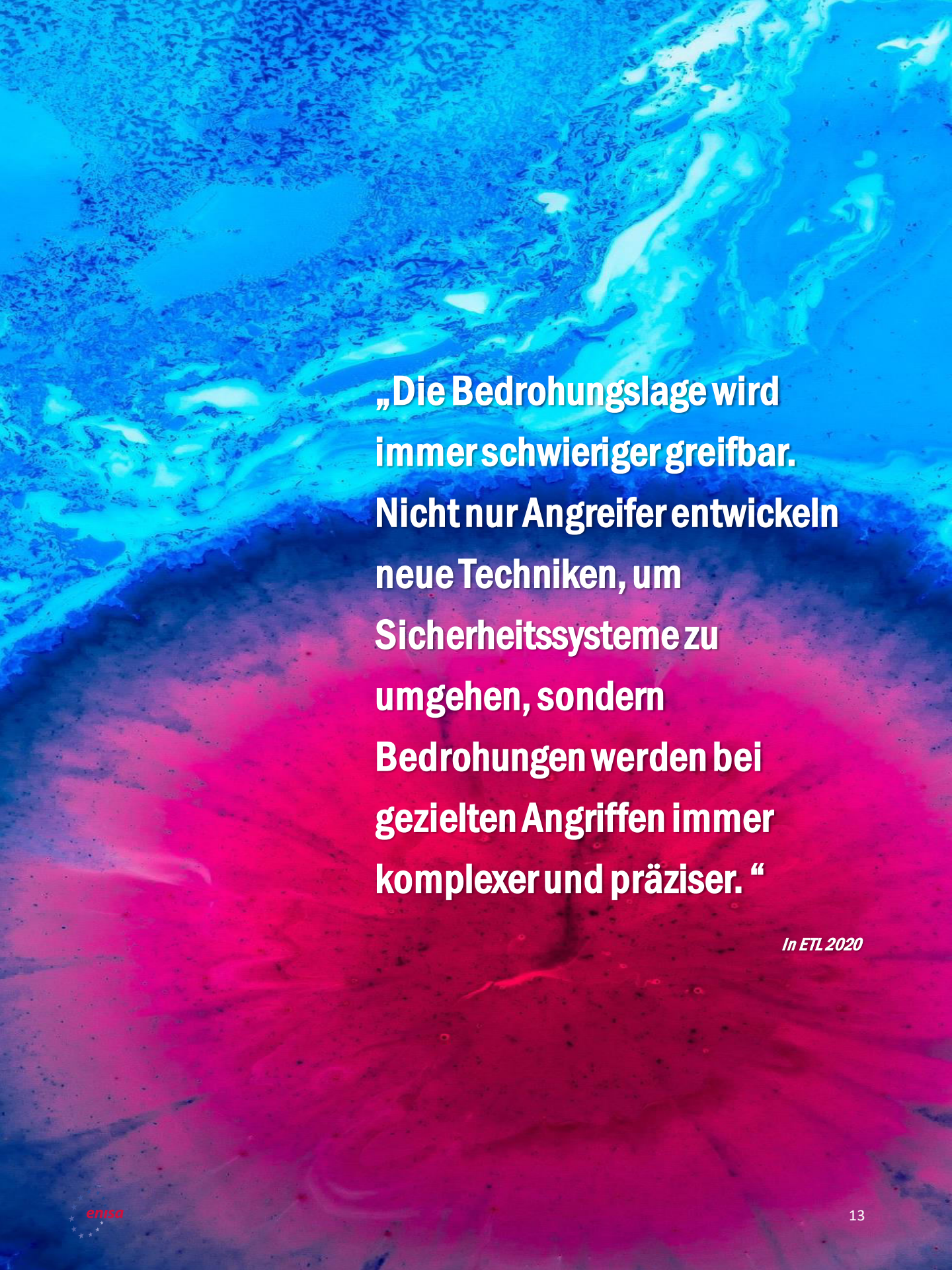
Die Europäische Kommission hat 2019 eine spezielle Eurobarometer-Umfrage[4] vorbereitet, um das Bewusstsein, die Erfahrungen und die Wahrnehmung der EU-Bürger für Cybersicherheit zu verstehen.

EUROBAROMETER

Die Ergebnisse dieser Umfrage zeigen, dass die Internetnutzung in Europa weiter zunimmt, insbesondere über Smartphones, und dass sich die Bürger der potenziellen Online-Gefahren bewusster sind.

Laut den Ergebnissen der Umfrage haben Bedenken hinsichtlich des Datenschutzes und der Sicherheit im Internet bereits dazu geführt, dass mehr als 9 von 10 Internetnutzern ihr Online-Verhalten geändert haben - meistens, indem sie keine E-Mails von unbekannten Personen geöffnet, Antivirensoftware installiert, nur bekannte und vertraute Websites besucht und nur ihre eigenen Computer benutzt haben.

Obwohl diese Ergebnisse sehr ermutigend sind, fallen viele Benutzer immer noch auf Online-Betrug und E-Mail-Phishing-Köder herein. Dies zeigt, dass böswillige Akteure ausgefeilte Angriffe verwenden, die schwerer zu erkennen und zu vermeiden sind. Daher müssen die Strategien zur Schadensbegrenzung regelmäßig aktualisiert werden, um den neuesten verfügbaren Informationen (CTI) zu Angriffstechniken Rechnung zu tragen.


„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

Was ist zu erwarten?

_ Nationalstaatlich gesponserte Akteure werden wohl:

TREND	BESCHREIBUNG	BEDROHUNG
→	**Weiterhin** den Cyberspace dazu verwenden, um Angriffe gegen Wahlprozesse im Ausland zu starten, um damit die demokratischen Systeme und Menschenrechte zu bedrohen.[5]	**Angriffe gegen Menschenrechte und demokratische Systeme**
→	**Weiterhin** die Opposition belästigen und ihre Bürger durch Manipulation von Informationen in sozialen Netzwerken in Verbindung mit Spyware-Kampagnen überwachen.	**Angriffe gegen Menschenrechte und demokratische Systeme**
↗	**Ausgefeilte Desinformationskampagnen** starten[6], um Wahrnehmungen zu beeinflussen oder Meinungen zugunsten einer bestimmten politischen Agenda oder finanzieller Spekulationsziele zu manipulieren.	**Desinformations kampagnen**
↗	Den Wettlauf um Cyber-Waffen[7] **erhöhen**, um Cyber-Fähigkeiten zu entwickeln. Da der Cyberspace als Kriegsgebiet betrachtet wird, werden Nationalstaaten wahrscheinlich durch gesponserte Agenten nach Cyberwaffen suchen, um einen Cyberkonflikt vorzubereiten.	**Unkontrolliertes Cyber-Wettrüsten**
↗	Strategische Ziele **verfolgen**: Z.B. Erlangung von Geschäftsgeheimnissen durch Spionage, Druckmittel bei politischen Entscheidungen, Finanzierung des Regimes durch Finanzbetrug, Durchführung von Cyber-fähigen Informationsoperationen und schließlich Schwächung oder Demoralisierung des Gegners durch störende oder destruktive Aktivitäten.	**Datendiebstahl**

Cyber-Täter werden wohl:

TREND	BESCHREIBUNG	BEDROHUNG
→	Sich **weiterhin** an Jugendliche und junge Erwachsene wenden mit Sextortion-Angriffen (Webcam-Erpressung), die die Opfer psychisch und letztendlich physisch treffen.[8]	**Sextortion (Webcam-Erpressung)**
↗	Die Anzahl der Cybermobbing-Angriffe während und nach der COVID-19-Pandemie bei Jugendlichen **erhöhen**, die vermehrt digitale Plattformen für persönliche oder Bildungszwecke nutzen.[9]	**Cyber-Belästigung**

Cyber-Kriminelle werden wohl:

TREND	BESCHREIBUNG	BEDROHUNG
↗	Den Einsatz von KI-basierten Tools **erhöhen**, um glaubwürdige Fälschungen (Bild-, Audio- und Videoformat) zu erstellen, die allgemein als Deep-Fakes bezeichnet werden, um Unternehmen zu betrügen.	**Deep Fake**
→	Die Taktik **verbessern**, die die Geschäftsprozesse gefährdet, um finanzielle Vorteile zu erzielen.	**Gefährdung von Geschäftsprozessen (BPC)**
→	Eine Ebene in der Organisation **absenken** - unterhalb der Geschäftsleitung -, um geschäftliche E-Mails zu kompromittieren.	**Gefährdung von geschäftlichen E-Mails**
→	Die Verwendung von Managed Service Providern (MSPs) zur Verbreitung von Malware **erhöhen**.	**Malware**

Schlussfolgerungen und Empfehlungen

Konkrete Schlussfolgerungen/Empfehlungen

- In den letzten Jahrzehnten lebten politische Entscheidungsträger und Technologen in zwei getrennten Welten und sprachen verschiedene Sprachen. Um den Herausforderungen der Digitalisierung zu begegnen, sollten diese von Grund auf **zusammenarbeiten** und einen gemeinsamen Ansatz entwickeln. Da der größte Teil der heutigen Technologie mit dem Cyberspace verbunden ist, ist der Beitrag von Cybersicherheitsexperten in vielen dieser Diskussionen von größter Bedeutung.
- Angesichts der wachsenden technologischen Innovation und der raschen Ausweitung des Cyberspace ist eine wirksame und umfassende EU-Cybersicherheitspolitik von entscheidender Bedeutung. **Ausgereifte Cybersicherheitsrichtlinien** werden die erforderlichen Sicherheitskapazitäten auf allen Ebenen der Gesellschaft bereitstellen: Regierungen, kritische Infrastrukturen, Unternehmen, tertiärer Sektor und Einzelpersonen. Die Sicherheitskapazität muss effektiv und flexibel sein, um neuen sich ergebenden Herausforderungen zu begegnen, um mit der sich ständig ändernden Natur des Cyberspace fertig zu werden.
- Angesichts der zunehmenden Zahl von Interessengruppen der EU und der Mitgliedstaaten, die an CTI-Aktivitäten beteiligt sind, ist die **Zusammenarbeit und Koordinierung** der EU-weiten CTI-Aktivitäten von zentraler Bedeutung. ENISA wird die Zusammenarbeit mit verschiedenen Interessengruppen fördern und einen ersten Versuch unternehmen, die CTI-Anforderungen verschiedener Interessengruppen zu ermitteln, insbesondere innerhalb der EU (d. h. der Kommission, EU-Gremien, Agenturen und Mitgliedstaaten).
- CTI sollte als Hauptinstrument für die **Vorbereitung auf Cybersicherheit** und die Ermöglichung risikobasierter Ansätze angesehen werden. Die Integration von CTI in Sicherheitsmanagementprozesse wird CTI dabei helfen, die Verbreitung in verwandten Bereichen zu fördern, und die Agilität von normalerweise langwierigen Prozessen wie Zertifizierung und Risikobewertung erhöhen. Darüber hinaus wird CTI als Vermittler von Notfallentscheidungen angesehen, die im Krisenmanagement erforderlich sind.
- Die Relevanz von CTI für strategische und politische Entscheidungen wird allgemein akzeptiert und als wesentlich angesehen, um die **Verbindung zu geopolitischen Informationen** und cyber-physischen Systemen zu erleichtern. Auf diese Weise kann CTI in EU-weite Entscheidungsprozesse einbezogen werden, der Kontext kann jedoch erweitert werden, um hybride Bedrohungen zu identifizieren.

_ Geschäftliche Schlussfolgerungen/ Empfehlungen

- Im Jahr 2019 wurde eine zunehmende Anzahl von **Testlaboren und Cyber-Bereichen**[10] vor Ort mit Cloud-Angeboten verfügbar. Dies sind wichtige Ressourcen für die Schulung des Personals, die Simulation von Angriffen und das Testen verschiedener Verteidigungsstrategien. Alles in einer virtuellen Mehrzweckumgebung.
- Obwohl einige CTI-Kriterien und -Anforderungen für verschiedene CTI-Benutzerprofile entwickelt wurden, sind **ähnliche Anforderungen** für weitere CTI-Produkte, -Dienstleistungen und -Instrumente erforderlich. CTI-Anbieter müssen die Anforderungen der Benutzer stärker berücksichtigen, um die Einführung von CTI-Produkten und -Diensten zu erleichtern.
- Investitionen in einige grundlegende CTI-Konzepte, insbesondere in **CTI-Reifegrade und Bedrohungshierarchien**, sind für die Einführung von CTI sehr nützlich. Anbieter müssen ihre Angebote an verschiedenen CTI-Reifegraden ausrichten, um eine effiziente Nutzung von CTI in Organisationen unterschiedlicher Größe und Budgets zu ermöglichen.
- Auf lange Sicht sieht es so aus, als ob **OpenCTI**[11] eine gute Lösung für die Fragmentierung von CTI-Angeboten sein könnte, da CTI-Quellen verschiedener Typen in eine einzige Tooling-Umgebung integriert werden können. CTI-Anbieter müssen die erforderlichen „Brücken" für ihre Produkte bereitstellen, um die Integration mit OpenCTI zu ermöglichen. Das Cyber Range-Konzept wurde ursprünglich 2013 von der Europäischen Verteidigungsagentur (EDA) im Bericht „Gemeinsames Personalziel für die militärische Zusammenarbeit in Cyber-Bereichen in der Europäischen Union" als Mehrzweckumgebung zur Unterstützung von drei Hauptprozessen definiert: Wissensentwicklung, Sicherstellung und Verbreitung.

Schlussfolgerungen und Empfehlungen

Schlussfolgerungen und Empfehlungen aus Forschung und Lehre

- Die EU sollte weiterhin in **F&E im Bereich Cybersicherheit** investieren, wobei der Schwerpunkt auf langfristigen und risikoreichen Forschungsinitiativen liegt. Langfristige Forschung und Innovation sind für die meisten Organisationen des Privatsektors eine kostspielige und unerreichbare Aufgabe.
- Die Erweiterung des Wissens und der Fachkenntnisse im Bereich Cybersicherheit ist entscheidend, um die Bereitschaft und Widerstandsfähigkeit zu verbessern. Die EU sollte weiterhin **Kapazitäten aufbauen**, indem sie in Schulungsprogramme für Cybersicherheit, professionelle Zertifizierungen, Übungen und Sensibilisierungskampagnen investiert.
- Die Cybersicherheitsforschung sollte Fachwissen aus sozialen, Verhaltens- und Wirtschaftsdisziplinen umfassen. **Multidisziplinäre Forschung** im Bereich Cybersicherheit sollte EU-weit gefördert und angeregt werden.
- Die Ergebnisse von Forschungsprojekten im Bereich Cybersicherheit und insbesondere im Bereich CTI müssen bewertet und einem breiteren Kontext zugeordnet werden, um Überschneidungen und Lücken zu identifizieren und sie mit bestehenden kommerziellen Produkten, Dienstleistungen und Praktiken vergleichbar zu machen. Dies wird dazu beitragen, diese Ergebnisse an die Benutzergemeinschaft weiterzugeben.
- Es müssen neuartige Ansätze für die Aufnahme von CTI-Wissen durch Domänen entwickelt werden, die davon profitieren können. **Beispiele sind Cyber-Bereiche, hybride Bedrohungen und geopolitische Bewertungen.** Die erzielten Synergien können Anwendungsfälle und Inhaltsqualität auf multidirektionale Weise verbessern.
- Der Einsatz von **künstlicher Intelligenz (KI)** und maschinellem Lernen (ML) im Rahmen von CTI sollte weiter untersucht werden. Dies reduziert die Anzahl der manuellen Schritte bei der Analyse von CTI und erhöht den Wert von Funktionen für maschinelles Lernen im Rahmen von CTI-Aktivitäten.
- Die Bereitstellung und Verwendung von Open-Source-CTI-Material sollte gefördert werden. Dies erleichtert den **Wissenstransfer**, senkt aber auch den Schwellenwert für die erforderlichen CTI-Kenntnisse.

"Die Komplexität der Bedrohungsfähigkeiten nahm 2019 zu, und viele Gegner nutzten Exploits, Diebstahl von Anmeldedaten und mehrstufige Angriffe."

In ETL 2020

Literaturangaben

1. "EU Cybersecurity Act". April, 2019. EU Parliament and Council https://eur-lex.europa.eu/eli/reg/2019/881/oj

2. "COVID-19 Risks Outlook: A Preliminary Mapping and its Implications". 19. Mai 2020 WEF. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications

3. "Joint communication to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions. Tackling COVID-19 disinformation - Getting the facts right". Juni 2020 Europäische Kommission https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008

4. "Special Eurobarometer 499: Europeans' attitudes towards cyber security". 29. Januar 2020. https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

5. "EUvsDosinfo" https://euvsdisinfo.eu/european-elections-2019/

6 "Manipulating Social Media to Undermine Democracy". 2017. Freedom House, https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy

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

8. "How online 'sextortion' drove one young man to suicide". 8. Februar 2018. Today. https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735

9. "Cyberbullying may increase during COVID-19 pandemic, expert says". 30. März 2020. Healio. https://www.healio.com/news/pediatrics/20200330/cyberbullying-may-increase-during-covid19-pandemic-expert-says

10. Das Cyber Range-Konzept wurde ursprünglich 2013 von der Europäischen Verteidigungsagentur (EDA) im Bericht „Gemeinsames Personalziel für die militärische Zusammenarbeit in Cyber-Bereichen in der Europäischen Union" als Mehrzweckumgebung zur Unterstützung von drei Hauptprozessen definiert: Wissensentwicklung, Sicherstellung und Verbreitung.

11. Open CTI. https://www.opencti.io/en/

„CTI hat sich im Bereich Cybersicherheit als wesentliches Instrument zur Verbesserung der Agilität und Effizienz bei der Verteidigung von Cyberangriffen fest etabliert.“

In ETL 2020

Themenbezogen

LESEN SIE DEN BERICHT

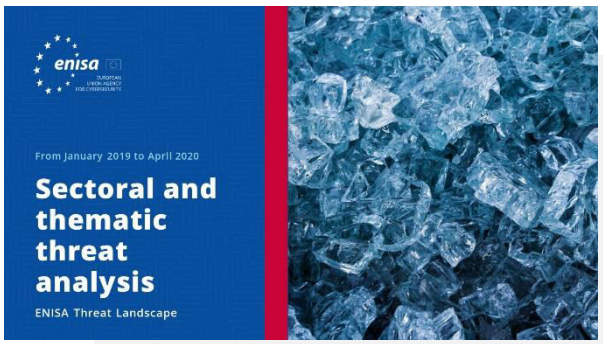
ENISA Threat Landscape Bericht
Liste der 15 größten Bedrohungen

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.

ENISA Threat Landscape-Bericht
Hauptvorfälle in der EU und weltweit

Die bedeutendsten Cybersicherheitsvorfälle 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 diesem Bericht verwenden Sie bitte die folgenden Kontaktangaben:
press@enisa.europa.eu.

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