DE

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Von Januar 2019 bis April 2020

Forschungsthemen

Überblick

Im Bereich der Cybersicherheit entwickeln sich aufgrund von Forschungs- und Innovationsaktivitäten von Wissenschaftlern, Industrie und Fachleuten auf der ganzen Welt neue Konzepte und Ideen. Dies sind wichtige Schritte, da das Innovationstempo von Gegnern (z. B. böswilligen Akteuren) höher ist als das von Cybersicherheitsspezialisten beim Finden von Lösungen, um sie davon abzuhalten. Abgesehen von der grundlegenden Cybersicherheitshygiene und -schulung sind Investitionen in Forschung und Innovation die beste Option für Verteidiger, um näher an das heranzukommen, was zur Verbesserung der Sicherheit im Cyberspace erforderlich ist. In diesem Bericht stellen wir einige der wichtigsten Forschungs- und Innovationsthemen im Bereich Cybersicherheit vor, die in der EU und auf der ganzen Welt untersucht wurden.

Besseres Verständnis der menschlichen Dimension

Cybersicherheit wird immer noch als die Praxis des Schutzes von Netzwerken, Informationssystemen und Daten (NIS) angesehen. Diese Definition muss über technische Fragen hinaus weiter ausgebaut werden, um soziale, verhaltensbezogene und wirtschaftliche Belange sowie die unterschiedlichen Rollen der beteiligten Parteien einzubeziehen. Dies sollte eine Priorität in zukünftigen Cybersicherheitsforschungs- und Innovationsdiskussionen darstellen. Ein besseres Verständnis der menschlichen Dimension ist der Schlüssel für die Definition einer Cybersicherheitsstrategie, damit Sicherheitsentscheidungen getroffen werden, um ihre Bedürfnisse, Fähigkeiten und Erwartungen zu erfüllen.

Cybersicherheitsforschung und -innovation

Im Jahr 2019 haben wir einen Anstieg der Anzahl von Testlaboren und Cyber-Bereichen[1] beobachtet, die lokal und in Cloud-Angeboten verfügbar wurden. Dies sind wichtige Ressourcen für Forscher, um Angriffe zu simulieren, Betreiberszenarien zu entwickeln, Betriebsdaten zu erhalten und Verteidigungsstrategien in einer virtuellen Mehrzweckumgebung zu testen. In vorhandenen Testumgebungen fehlt es jedoch daran, viele Schwachstellen zu replizieren, die normalerweise die Sicherheit gefährden, z. B. menschliche und technische Faktoren. Um die Effizienz zu verbessern, ist es wichtig, den Umfang und die Genauigkeit dieser Testlabore zu erforschen, zu innovieren und neue technische Lösungen vorzuschlagen.

Überblick

5G-Sicherheit

Der Ausbau von 5G-Mobilfunknetzen in einigen Ländern begann 2019, es wird jedoch erwartet, dass die Anzahl der Installationen im Jahr 2021 zunimmt. Diese nächste Generation der Mobilkommunikation ist für den sozialen und wirtschaftlichen Fortschritt der Europäischen Union von größter Bedeutung. Daher ist die zukünftige Forschung und Entwicklung von 5G-Sicherheitslösungen entscheidend für die Nachhaltigkeit und Zuverlässigkeit dieser Technologie. Im Jahr 2019 veröffentlichte ENISA einen Threat Landscape-Bericht für 5G-Netze, in der einige kritische Sicherheitsaspekte im Zusammenhang mit dieser neuen Technologie untersucht wurden.[2] Schlüsselthemen in der Forschung und Innovation der 5G-Sicherheit sollten die folgenden Aspekte berücksichtigen.

- Die Forschung und Entwicklung von Sicherheitskontrollen zum Schutz des Netzwerks, der physischen Elemente und der Datenschichten bietet somit eine mehrschichtige Schutzlösung. Mit 5G Netzwerken werden Daten in zentralen Cloud-Servern, Zwischennebelknoten und Edge-Geräten gespeichert, was die Komplexität bei der Implementierung einer Sicherheitslösung erhöht.

- Die Erforschung und Entwicklung von Standards und Anforderungen für Sicherheitskontrollen zur Implementierung in miteinander verbundenen Netzwerken mit mehreren Eigentümern, Topologien, Betreibern und einer diversifizierten Vielzahl von Geräten und Netzwerkschichten.

- Die Forschung und Entwicklung von Schlüsselverwaltungsfunktionen, die eine sichere Interoperabilität zwischen Knoten ermöglichen, die ressourcenbeschränkte Edge- und IoT-Geräte verbinden. Diese Funktion sollte eine effektive Zugriffskontrolle, Authentifizierung, Kryptografie und Schlüsselverwaltungstechniken für Knoten mit begrenzten Ressourcen umfassen.

EU-Forschungs- und Innovationsprojekte zur Cybersicherheit

- Die EU arbeitet daran, ein Pilotprojekt für ein Kompetenznetzwerk für Cybersicherheit einzurichten. CONCORDIA[3], ECHO[4], SPARTA[5] und CyberSec4Europe[6] sind die vier Gewinner-Pilotprojekte des Cybersecurity-Aufrufs „Horizont 2020" für 2018: „Einrichtung und Betrieb eines Pilotprojekts für ein europäisches Kompetenznetzwerk für Cybersicherheit und Entwicklung einer gemeinsamen europäischen Roadmap für Cybersicherheitsforschung und -innovation". Die EU erwartet, mit diesen vier Pilotprojekten ihre Cybersicherheitskapazitäten zu stärken und künftigen Herausforderungen im Bereich der Cybersicherheit zu begegnen, um einen sichereren digitalen Binnenmarkt der EU zu schaffen.
- Die EU gewährt 38 Millionen EUR für den Schutz kritischer Infrastrukturen vor Cyber-Bedrohungen. Die Europäische Kommission hat angekündigt, über Horizont 2020 mehr als 38 Millionen EUR für das Forschungs- und Innovationsprogramm der EU bereitzustellen. Das Programm soll mehrere innovative Projekte im Bereich des Schutzes kritischer Infrastrukturen vor Cyber- und physischen Bedrohungen unterstützen und Städte intelligenter und sicherer machen.[7]
- Die EU hat eine Einladung zur Einreichung von Vorschlägen für Cybersicherheit in Höhe von 10,5 Millionen EUR veröffentlicht. Die Kommission hat im Rahmen des Programms „Connecting Europe Facility" (CEF) eine neue Einladung im Wert von 10,5 Millionen EUR für Projekte herausgegeben, mit denen die Cybersicherheitsfähigkeiten und die Zusammenarbeit Europas zwischen den Mitgliedstaaten verbessert werden sollen.[8]

CTI-Forschung und -Innovation

Schnelle Verbreitung von CTI-Methoden und -Inhalten

Im Berichtszeitraum wurden verschiedene Forschungsbedürfnisse ermittelt, und hier werden Maßnahmen zur Bewältigung dieses Bedarfs vorgeschlagen. Diese wurden in einige Kategorien eingeteilt, um den Umfang besser widerzuspiegeln. Obwohl diese Kategorien nicht überlappungsfrei sind, weisen sie auf Bereiche mit potenziellen CTI-Verbesserungen hin.

- **Die Ergebnisse von Forschungsprojekten im Bereich CTI müssen bewertet und einem breiteren CTI-Kontext** zugeordnet werden, um Überschneidungen und Lücken zu identifizieren und sie mit bestehenden kommerziellen CTI-Produkten, -Dienstleistungen und -Praktiken vergleichbar zu machen. Dies wird dazu beitragen, die Ergebnisse an die Benutzergemeinschaft weiterzugeben. Gleichzeitig werden bestehende Lücken durch zusätzliche Funktionen, Inhalte und Prozesse geschlossen. EU-Projekte (Horizon H2020) mit CTI-Relevanz sind hervorragende Kandidaten für diese Aufgabe und tragen zur Verbesserung der CTI-Praktiken bei.
- **Die Bereitstellung und Verwendung von Open-Source-CTI-Material sollte gefördert werden.** Dies erleichtert den Wissenstransfer, senkt aber auch den Schwellenwert für CTI-Kenntnisse. Open-CTI ist der perfekte Kandidat für diesen Zweck, da es die Aufnahme von CTI aus mehreren Quellen in eine einzige Basis unterstützt, die von verschiedenen Benutzern gemeinsam genutzt werden kann, und gleichzeitig eine Reihe von Funktionen zur Verwaltung dieser Informationen bietet. Durch die Einführung von Open-CTI können Benutzer wertvolle Informationen bei einer relativ niedrigen Qualifikationsschwelle erhalten.

_Forschung, die zu neuen Entwicklungen führt

Die Notwendigkeit, **CTI** mit anderen etablierten Cybersicherheitsinstrumenten **zu stärken**, erfordert die strukturelle und kontextbezogene Entwicklung dieses Bereichs. Gleichzeitig werfen die technologischen Fortschritte aufkommender Technologien die Frage auf, wie CTI von diesen Entwicklungen profitieren kann. Der **voraussichtliche Forschungsbedarf** im Bereich CTI wird daher zur Verbesserung von Prozessen, Funktionen, Automatisierung, Inhaltsstruktur und -validierung, Servicebereitstellung, Geschwindigkeit zum Benutzer/zur Verbreitung, CTI-Bereitstellung und Zuordnungen beitragen.

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

CTI-Forschung und -innovation

Funktionalität, Automatisierungsgrad und Einhaltung der Reifeanforderungen

- **Die Prozessautomatisierung wird in CTI eine Schlüsselrolle spielen.** Während moderne Cyberangriffe stark automatisiert sind, versuchen Unternehmen, sich manuell oder teilweise durch Automatisierung gegen sie zu verteidigen. Dies ist ein ungleicher Wettbewerb, der die Geschwindigkeit und Reaktionsfähigkeit verlangsamt. Die Untersuchung der möglichen Automatisierung von CTI-Prozessen ist von entscheidender Bedeutung, um ein Gleichgewicht zwischen Angreifern und Verteidigern herzustellen. Um dies zu erreichen, ist eine gründliche Analyse der CTI-Prozessschritte und Optionen zur Automatisierung dieser Schritte über verfügbare und aufkommende Technologien erforderlich.
- **Die Anforderungen an die CTI-Reife müssen genauer festgelegt werden.** Obwohl einige Kriterien und Anforderungen für die Auswahl von CTI-Funktionen für verschiedene CTI-Benutzerprofile entwickelt wurden (z. B. Threat Intelligence Plattformen oder TIPs), sind ähnliche Anforderungen für weitere CTI-Produkte, -Dienstleistungen und -Programme erforderlich. Solche Anforderungen sind mit mehreren Reifegraden und Ausgaben der Benutzer sowie mit Arten von CTI verbunden. Ähnliche Kriterien/Anforderungen sind für verschiedene andere Elemente einer CTI-Infrastruktur erforderlich, z. B. Instrumente, bewährte Verfahren, gemeinsame Nutzung von Plattformen usw. Abgesehen von der Entwicklung von CTI-Fähigkeitsreifemodellen sind daher Forschungsarbeiten erforderlich, um zu zeigen, wie CTI-Funktionen den verschiedenen CTI-Reifegraden entsprechen. Diese Arbeit wird dazu beitragen, die Akzeptanz von CTI-Praktiken zu beschleunigen.
- **Die Verwendung von KI/ML in CTI sollte weiter untersucht werden.** Dies reduziert die Anzahl der manuellen Schritte bei der CTI-Analyse und erhöht den Wert von ML-Funktionen im Rahmen von CTI-Aktivitäten.

Brücken in verwandte Gebiete

- **Es müssen neuartige Ansätze für die Aufnahme von CTI-Wissen durch Domänen** entwickelt werden, die davon profitieren können. Beispiele sind Cyber-Bereiche, hybride Bedrohungen, Lieferketten und geopolitische Bewertungen sowie Krisen. In dieser Hinsicht sollte man sich die folgenden Fragen stellen. An welchen Punkten kann CTI berücksichtigt werden? Welche CTI-Inhalte sind relevant? Was sind die Validierungskriterien für die Angemessenheit von CTI-Informationen? Wie kann CTI in Informationen über die betreffende Domain eingebunden werden? Welche Informationen aus diesen Domains können zu CTI hinzugefügt werden? Die erzielten Synergien, die sich in diesen Fragen widerspiegeln, können Anwendungsfälle und Inhaltsqualität auf omnidirektionale Weise verbessern.

- **CTI ist für eine Reihe von Disziplinen von wesentlicher Bedeutung.** Beispiele hierfür sind die Risikobewertung, das Risikomanagement sowie die Definition von Schutzanforderungen und die Zertifizierung. Für diese Disziplinen ist es von Vorteil, CTI richtig einzusetzen. Der Beitrag der CTI zu diesen Disziplinen kann anhand von Informationen wie Bedrohungsmodellen, Informationen zu Bedrohungsakteuren (Fähigkeiten, Motive), Angriffsmethoden und Exploits ermittelt werden. Obwohl relevantes Material vorhanden ist (z. B. ATT&CK Angriffsrahmen[9]), sind erhebliche Arbeiten erforderlich, um solche Informationsschnittstellen zu identifizieren und zu standardisieren.

CTI-Forschung und -innovation

Wirksamkeit von CTI-Operationen

- **Methoden zur effektiven Nutzung von CTI werden ein Instrument zur Entscheidungsfindung sein.** Solche Methoden zur effizienten Bereitstellung von CTI werden Entscheidungsträgern helfen, den Wert von CTI zu verstehen, und Praktikern helfen, die Kapitalrendite in CTI zu bewerten. Solche Methoden/KPIs müssen Faktoren berücksichtigen, die über den CTI-Inhalt hinausgehen, und dabei Verbesserungen berücksichtigen, die während des gesamten Lebenszyklus des Sicherheitsmanagements und der Risikominderung erzielt wurden. Optimalerweise wird die Messung der Effektivität von Investitionen in CTI Teil einer viel umfassenderen Betrachtung der Wirtschaftlichkeit der Cybersicherheit in verschiedenen Arten von Organisationen sein (z. B. gemäß Sicherheitsanforderungen, Reifegraden usw.).

- Obwohl kostengünstige Tools zum Aggregieren, Analysieren und Verbreiten von CTI vorherrschen, sind möglicherweise **einige Untersuchungen erforderlich, um automatisierte Instrumente zum Verwalten der verbrauchten und produzierten CTI** zu finden. Anders als standardisierte Datenformate (z. B. CSV-Dateien, STIX, TAXII) können Standard-CTI-Funktionen Gegenstand solcher Untersuchungen sein, gefolgt von der Entwicklung kostengünstiger Open-Source-Instrumente, die solche Funktionen unterstützen.

Entwicklung der CTI-Struktur und des Inhalts

- Da CTI zusätzliche Bereiche durchdringt, **müssen Informationen aus diesen Kontexten an die ursprüngliche CTI-Wissensbasis zurückgegeben werden.** Beispielsweise müssen CTI-Strukturen definiert werden, um geopolitische und hybride Bedrohungsinformationen zu erfassen. Gleiches gilt für die Relevanz von CTI für Risiken, Vorfälle, forensische Analysen, Sicherheitsstufen usw. Die vorhandenen CTI-Formate müssen weiterentwickelt werden, um Informationen zu erfassen, die aus diesen Abhängigkeiten in CTI stammen.

- **Neue Technologien wie KI** können zur Validierung analysierter CTI verwendet werden. Solche Instrumente können die manuelle CTI-Analyse ergänzen oder sogar ersetzen, bieten aber auch Unterstützung während des gesamten Lebenszyklus von CTI (z. B. Überprüfung der Relevanz von CTI anhand vorhandener Vorfallinformationen). Solche neuartigen Ansätze für CTI werden die Qualität und Relevanz der Informationen verbessern.

Literaturangaben

1. 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.

2. "ENISA threat landscape for 5G Networks". 21. November, 2019 ENISA https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

3. https://www.concordia-h2020.eu/

4. https://echonetwork.eu/

5. https://www.sparta.eu/news/

6 https://cybersec4europe.eu/

7. https://ec.europa.eu/programmes/horizon2020/en/news/eu-grants-%E2%82%AC38-million-protection-critical-infrastructure-against-cyber-threats

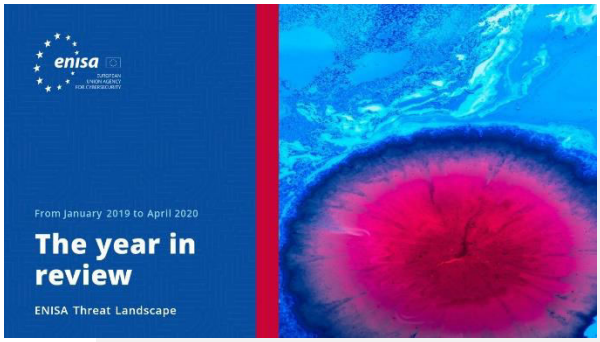
8. https://ec.europa.eu/digital-single-market/en/news/eu105-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and

9. https://attack.mitre.org/

„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



ENISA Threat Landscape Bericht **Das Berichtsjahr**

Eine Zusammenfassung der bedeutendsten Cybersicherheitstrends des Jahres.

LESEN SIE DEN BERICHT

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

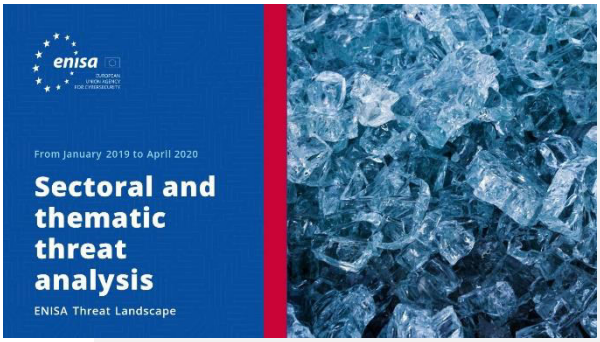
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape-Bericht **Hauptvorfälle in der EU und weltweit**

Die bedeutendsten Cybersicherheitsvorfälle zwischen Januar 2019 und April 2020.

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

Fahrplan für die Zusammenarbeit zwischen CSIRTS und LE

Ein Fahrplan für die Zusammenarbeit zwischen CSIRTs, insbesondere mit nationalen und staatlichen Strafverfolgungsbehörden (LE) und der Justiz.

LESEN SIE DEN BERICHT

EU-Statusbericht zur Entwicklung von MS-Vorfällen

Eine Studie, die auf die Analyse des aktuellen operativen Incident Response-Aufbaus in NISD-Sektoren abzielt und die jüngsten Änderungen identifiziert.

LESEN SIE DEN BERICHT

ENSIA CSIRT Modell für die Reifebeurteilung

Eine aktualisierte Version der „Herausforderungen für nationale CSIRTs in Europa im Jahr 2016: Studie über „CSIRIT Reife“, die von der ENISA in 2017 veröffentlicht wurde

LESEN SIE DEN BERICHT

„Die Komplexität der Bedrohungsfähigkeiten nahm 2019 zu, und viele Gegner nutzten Exploits, Diebstahl von Anmeldeinformationen und mehrstufige Angriffe.“

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