enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Sektorale und thematische Bedrohungsanalyse

Überblick

Abgesehen von der Angabe der Motive der Gegner liefert sie Hinweise auf die häufigsten Angriffstechniken und die Gefährdung durch Bedrohungen, die für einen bestimmten Sektor gelten, und gibt somit Schutzanforderungen und -prioritäten an. In Bezug auf Themen trägt die Analyse von Bedrohungen und Herausforderungen im Zusammenhang mit bestimmten neuen Technologien zur Beurteilung, Bewertung und Minderung künftiger Risiken bei.

Kontextualisierte Cyber Threat Intelligence (CTI) für Sektoren ist ein wichtiges vorbereitendes Instrument, um Schlussfolgerungen zu erwarteten Cyberangriffen innerhalb eines bestimmten Sektors zu ziehen.

Sektorvorfallstatistik im Vergleich zur bewerteten Exposition aufstrebender Sektoren

Die Kontextualisierung der sektoralen CTI basiert hauptsächlich auf Cybersicherheitsvorfällen in einem Sektor. Dies ist zwar eine Standardmethode für vorhandene und etablierte IT-Komponenten und digitale Dienste, deckt jedoch keine neuen Technologien ab. Dies liegt hauptsächlich daran, dass für Technologien, die sich nur in einer Pilot- oder Versuchsphase befinden, keine Informationen zu Vorfällen vorhanden sind. CTI für neue Technologien wird durch Bedrohungsanalysen von Asset-Kategorien kontextualisiert, die für einen bestimmten Sektor relevant sind. ENISA führt solche Bewertungen für aufstrebende Sektoren wie 5G, IoT[5] und Smart Cars durch[6]. Sektorale und thematische Threat Landscape-Berichte und Bewertungen des Basisschutzes sind die Methoden, mit denen ENISA CTI kontextualisiert.

In diesem Bericht präsentieren wir neben sektoralen CTI, die sich auf vorfallbasierte Statistiken stützen, eine Zusammenfassung der bewerteten CTI für aufstrebende Technologiesektoren auf der Grundlage von ENISA-Arbeiten.


" 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

Überblick

_Die dringende Notwendigkeit einer genauen und aktuellen Statistik über sektorale Vorfälle

Sektorale Ereignisstatistiken sind ein wesentliches Instrument, um die Dynamik der Bedrohungsentwicklung, die Motive der Gegner, die Offenlegung von Vermögenswerten und Maßnahmen zur Erreichung von Zielen zu verstehen. Aufgrund der Komplexität der Angriffe, der Abhängigkeiten zwischen den Zielobjekten und der sektorübergreifenden Natur der ausgenutzten Sicherheitslücken weisen die Vorfallstatistiken einige inhärente Unsicherheiten auf, die sich aus den folgenden Fakten ergeben.

- In verschiedenen Branchenstatistiken sehen wir eine Reihe von Vorfällen, die **als „unbekannt" eingestuft** wurden[1,2]. Dieser Prozentsatz variiert zwischen 1,5 % und 5 %. Wenn diese Vorfälle mit einigen der bekannten Sektoren in Verbindung gebracht werden könnten, könnte dieser Prozentsatz die Reihenfolge der Ziele beeinflussen. Darüber hinaus führt die erhebliche Anzahl unbekannter Angriffstechniken (ca. 15 %) zu einer gewissen Unsicherheit bei der Bewertung der Motive der Bedrohungsakteure.
- **Die meisten Angriffe dauern mehr als einen Schritt (durchschnittlich drei), um die Ziele des endgültigen Opfers zu erreichen.** In vielen Fällen werden mehrere Zielobjekte aus verschiedenen Sektoren in einen einzigen Angriff einbezogen. Daher kann ein in einem Sektor aufgezeichneter Vorfall aus mehreren Vorfällen in anderen Sektoren resultieren, die Zwischenschritte des Angriffs sind. Solche Abhängigkeiten zwischen Vorfällen können die Genauigkeit der Vorfallstatistik beeinträchtigen.
- Neben der Anzahl der Vorfälle pro Sektor ist die **Art der verwendeten Angriffstechniken** ein wichtiges Element für die statistische Analyse. Diese Informationen können nützliche Hinweise auf den am häufigsten verwendeten Angriffsvektor liefern und dazu beitragen, die für einen bestimmten Sektor erforderlichen Schutzmaßnahmen zu priorisieren.

- Die Materialisierung von Bedrohungen hängt stark von bestehenden **Möglichkeiten ab, die von Gegnern erkundet werden.** Beispielsweise sind IT-Umgebungen aufgrund der COVID-19-Pandemie dezentralisiert worden. Dies schwächt die Sicherheitskontrollen des Unternehmens innerhalb des Unternehmensnetzwerks, was die Verlagerung von Angriffen von Unternehmenszielen auf einzelne Ziele erklärt.[1] Dieses Beispiel zeigt, dass beobachtete Änderungen in der Statistik angesichts der sich abzeichnenden Chancen „übersetzt" werden müssen.
- Aktuelle Statistiken werden unter Berücksichtigung verschiedener Kriterien erstellt. **Abweichungen in den Kriterien** der Statistik behindern Vergleiche zwischen Vorfallstatistiken. Ein Beispiel:
    - Abhängig von der Stakeholder/Contributors-Datenbank des Informationssammlers decken die Daten zur Statistik möglicherweise nicht alle Sektoren gleichmäßig ab;
    - Die Klassifizierung von Vorfällen kann auf der Grundlage ihrer Häufigkeit basieren, unabhängig von der Größe des Schadens (z. B. des Umfangs der verletzten Informationen) oder seiner Auswirkung.
- Ein wesentliches Element der Sektorstatistik ist die **Häufigkeit des Auftretens** einzelner Cyberbedrohungen. Dies gibt einen Eindruck von der in einem Sektor am häufigsten verwendeten Angriffsmethode. Solche Statistiken können Hinweise zum erforderlichen Grad an Bereitschaft oder Reife einzelner Sicherheitskontrollen geben, die die Gefährdung durch die relevanten Cyber-Bedrohungen verringern.
- In Anbetracht der oben genannten Fakten, die für die Ereignisstatistik relevant sind, enthält dieser Bericht eine ungefähre Rangfolge der Sektoren in Bezug auf beobachtete Vorfälle sowie einen Trend, der sich aus der sich abzeichnenden Dynamik der potenziellen Exposition jedes Sektors ergibt. Darüber hinaus werden einige Informationen zu den beliebtesten Angriffsmethoden pro Sektor gegeben. Zu diesem Zweck wurden Informationen aus verschiedenen Veröffentlichungen herangezogen.[1,2,3,4]

Trends in Bezug auf Vorfälle

SEKTOR	BELIEBTESTE BEDROHUNGEN/ANGRIFFE	VORFALL-TRENDS
Privatperson	• Phishing • Malware • Informationsleck • Datendiebstahl	Stabil
Mehrere Branchen	• Angriffe auf Webanwendungen • Phishing • Malware	Zunahme
Öffentliche Verwaltung, Verteidigung, soziale Dienste	• Malware • Phishing • Webbasierte Angriffek	Stabil leicht abnehmend
Finanz-/Bank-/Versicherungswesen	• Angriffe auf Webanwendungen • Insiderbedrohungen (unbeabsichtigter Missbrauch) • Malware • Datendiebstahl	Stabil
Gesundheit/ Medizin	• Malware • Insiderbedrohungen (unbeabsichtigter Missbrauch/Fehler) • Angriffe auf Webanwendungen	Zunahme
Bildung	• Malware • Ransomware • Webbasierte Angriffe	Stabil leicht abnehmend
Information und Kommunikation	• Angriffe auf Webanwendungen • Insiderbedrohungen (unbeabsichtigter Missbrauch/Fehler) • Malware	Stabil
Professionelle/ Digitale Dienste	• Angriffe auf Webanwendungen • Insiderbedrohungen (unbeabsichtigter Missbrauch/Fehler) • Malware	Stabil
Kunst, Unterhaltung und Spiele[8]	• Angriffe auf Webanwendungen • Malware • Phishing	Stabil
Produktion	• Malware • Angriffe auf Webanwendungen • Insiderbedrohungen (unbeabsichtigter Missbrauch/Fehler)	Stabil

SEKTOR	EINFLUSSFAKTOREN
Privatperson	Die Selbstisolierung aufgrund von COVID-19-Lockdownmaßnahmen hat zu verteilten/dezentralen IT-Umgebungen und zur Isolierung von Benutzern geführt, die leichter zu täuschen sind und über weniger Sicherheitskontrollen verfügen, als dies in zentralisierten Umgebungen der Fall war.
Mehrere Branchen	Remote-Benutzer haben aufgrund von COVID-19-Lockdownmaßnahmen Angriffe durch Phishing und Verlust vertraulicher Informationen (z.B. Anmeldedaten) erlebt.
Öffentliche Verwaltung, Verteidigung, soziale Dienste	Die Nutzung von Cloud-Diensten kann die Sicherheit öffentlicher Angebote beeinflusst haben. Trotzdem haben die Sozialdienste aufgrund von Finanzhilfen, die den Bürgern während der COVID-19-Pandemie angeboten wurden, erhebliche Angriffe erhalten.
Finanz-/ Bank- /Versicherungswesen	Die Komplexität des Finanzsektors macht es schwierig, die Bedrohungslandschaft zu interpretieren, da verschiedene Bereiche innerhalb von Finanzdienstleistungen und Banken völlig unterschiedlichen Cyberrisiken und -bedrohungen ausgesetzt sein können.
Gesundheit/ Medizin	Die Aufmerksamkeit, die Cyberkriminelle den Gesundheitszielen widmen, hat aufgrund finanzieller Motive und der Bedeutung des Sektors während der COVID-19-Pandemie erheblich zugenommen.
Bildung	Obwohl dieser Sektor stabil ist, wurde er aufgrund des Interesses an COVID-19-Forschungsergebnissen im Jahr 2020 von Cyberspionage-Kampagnen ins Visier genommen.
Information und Kommunikation	Dieser Sektor steht aufgrund der Schwierigkeiten beim Schutz einer riesigen Angriffsfläche, die durch digitale Medienplattformen eingeführt wird, ständig unter Druck. Für Online-Medienunternehmen sind Angriffe, die Reputationsschäden verursachen, eine der größten Bedrohungen.
Professionelle/ Digitale Dienstleistungen	Obwohl dieser Sektor stabil ist, wurde er 2020 von verschiedenen Kampagnen ins Visier genommen, um Informationen von Nutzern digitaler Telearbeitsdienste während der COVID-19-Pandemie von zu Hause aus zu erhalten.
Kunst, Unterhaltung und Spiele	Der Wechsel von einem lizenzierten zu einem Abonnement-Geschäftsmodell, das von der Glücksspielbranche übernommen wurde, machte diesen Sektor für Cyberkriminelle attraktiver.[8]
Produktion	Angriffe auf die Lieferkette und Angriffe auf industrielle Steuerungssysteme stellen die Hauptbedrohung für produzierende Unternehmen dar, da diese eine komplette Produktionslinie stilllegen können. Der Diebstahl von Daten zum geistigen Eigentum ist eine weitere ernsthafte Bedrohung für diesen Sektor.

Bedrohungen für neue Technologien

_ Nächste Generation der Mobilkommunikation oder 5G

VERWANDTE KOMPONENTEN - VERMÖGENSGRUPPEN	BEDROHUNG
Kernnetzwerk	Missbrauch durch Fernzugriff, Spitzen des Authentifizierungsverkehrs, Missbrauch von Benutzerauthentifizierungs-/Autorisierungsdaten, Missbrauch von gehosteten Netzwerkfunktionen von Drittanbietern, Missbrauch der rechtmäßigen Abhörfunktion, Ausnutzung der API (Application Programming Interface), Ausnutzung schlecht gestalteter Architektur und Planung, Ausnutzung falsch oder schlecht konfigurierter Systeme/Netzwerke, fehlerhafte Verwendung oder Verwaltung des Netzwerks, der Systeme und Geräte, Betrugsszenarien im Zusammenhang mit Roaming-Verbindungen, seitliches Eindringen, Speicherabbau, Manipulation des Netzwerkverkehrs, Netzwerkausspähung und Informationserfassung, Manipulation von Netzwerkkonfigurationsdaten, böswillige Überflutung der Kernnetzwerkkomponenten, böswillige Umleitung des Datenverkehrs, Manipulation des Netzwerkressourcen-Orchestrators, Missbrauch von Audit-Tools, opportunistische und betrügerische Nutzung gemeinsam genutzter Ressourcen, Registrierung böswilliger Netzwerkfunktionen, Traffic-Sniffing, Seitenkanalangriffe
Zugriff auf das Netzwerk	Missbrauch von Frequenzressourcen, ARP-Vergiftung (Address Resolution Protocol), Fake Access-Netzwerkknoten, Flooding-Angriff, IMSI-Fangangriffe, Störung der Funkfrequenz, MAC-Spoofing, Manipulation von Konfigurationsdaten des Zugangsnetzwerks, Funkstörungen, Manipulation des Funkverkehrs, Sitzungsentführung, Signalbetrug, Signalstürme

VERWANDTE KOMPONENTEN - VERMÖGENSGRUPPEN	BEDROHUNG
Multi Edge Computing	Falsches oder betrügerisches MEC-Gateway, Überlastung des Edge-Knotens, Missbrauch von Edge-Open-Application-Programmierschnittstellen (APIs)
Virtualisierung von Netzwerkfunktionen und softwaredefinierten Netzwerken	Missbrauch des DCI-Protokolls (Data Centers Interconnect), Missbrauch von Cloud-Rechenressourcen, Umgehung der Netzwerkvirtualisierung, Missbrauch des virtualisierten Hosts
Physische Infrastruktur	Manipulation von Hardwaregeräten, Naturkatastrophen, die sich auf die Netzwerkinfrastruktur auswirken, physische Sabotage/Vandalismus der Netzwerkinfrastruktur, Bedrohung durch Mitarbeiter Dritter, die auf die Einrichtungen von MNO zugreifen, Nutzung des UICC-Formats (Universal Integrated Circuit Card), Kompromittierung der Benutzergeräte
Alle oben genannten 5G-Asset-Gruppen	Denial of Service (DoS), Datenschutzverletzung, Leckage, Diebstahlzerstörung und Manipulation von Informationen, Abhören, Ausnutzung von Software- und Hardwareschwachstellen, schädliche Codes oder Software, gefährdete Lieferkette, Anbieter und Dienstleister, gezielte Bedrohungen/Angriffe, Ausnutzen von Fehlern in Sicherheits-, Verwaltungs- und Betriebsverfahren, Missbrauch der Authentifizierung, Identitätsdiebstahl oder Spoofing

Bedrohungen für neue Technologien

_ Internet der Dinge (IoT)

VERWANDTE KOMPONENTEN – VERMÖGENSGRUPPEN	BEDROHUNG
Menschlicher Faktor	Insider-Bedrohung, Teamwork-Probleme, interne Einschränkungen, Hacktivismus, Verlust von Support-Diensten, Ausfall von Versorgungsunternehmen, Netzwerkausfall, unbeabsichtigte Änderungen, Sabotage, Verstoß gegen Regeln und Vorschriften, Verstoß gegen Gesetze, Vertragsanforderungen, Nichteinhaltung vertraglicher Anforderungen (z. B. Softwarewartung) , Software-Nutzung, Social Engineering, Identitätsdiebstahl.
Software-Design	Insider-Bedrohung, Hacktivismus, unbeabsichtigte Änderungen, fehlerhafte Verwendung oder Verwaltung von Geräten und Systemen, Sabotage, SDLC-Prozessfehler, Fehler Dritter, Nichteinhaltung vertraglicher Anforderungen (z. B. Softwarewartung), Software-Ausnutzung, Verlust/Leckage von Informationen.
Softwareentwicklung	Insider-Bedrohung, Hacktivismus, Verlust von Support-Diensten, unbeabsichtigte Änderungen, fehlerhafte Verwendung oder Verwaltung von Geräten und Systemen, Sabotage, Vandalismus und Diebstahl, Software-Schwachstellen, SDLC-Prozessfehler, Wartungsfehler, Autorisierungsmissbrauch, Software-Nutzung, Manipulation der SDLC-Infrastruktur, Verlust/Leckage von Informationen.
Software-Bereitstellung	Insider-Bedrohung, Hacktivismus, Verlust von Support-Diensten, unbeabsichtigte Änderungen, fehlerhafte Verwendung oder Verwaltung von Geräten und Systemen, Sabotage, Vandalismus und Diebstahl, Software-Schwachstellen, SDLC-Prozessfehler, Fehler Dritter, Autorisierungsmissbrauch, Software-Nutzung, Manipulation der SDLC-Infrastruktur, Serviceverweigerung, Manipulation von Informationen, Offenlegung, Verlust/Leckage von Informationen.

VERWANDTE KOMPONENTEN - VERMÖGENSGRUPPEN	BEDROHUNG
Daten	Insider-Bedrohung, Hacktivismus, Verlust von Support-Diensten, unbeabsichtigte Änderungen, fehlerhafte Verwendung oder Verwaltung von Geräten und Systemen, Sabotage, Vandalismus und Diebstahl, Software-Schwachstellen, SDLC-Prozessfehler, Fehler Dritter, Autorisierungsmissbrauch, Software-Nutzung, Manipulation der SDLC-Infrastruktur, Serviceverweigerung, Manipulation von Informationen, Offenlegung, Verlust/Leckage von Informationen.
Wartung	Insider-Bedrohung, Hacktivismus, Ausfall von Versorgungsunternehmen, Netzwerkausfall, unbeabsichtigte Änderungen, fehlerhafte Verwendung oder Verwaltung von Geräten und Systemen, Schäden durch Dritte, Sabotage, Vandalismus und Diebstahl, Angriffe mit physischem Zugriff, erzwungener Zugriff, Vertragsanforderungen, Software-Schwachstellen, SDLC-Prozessfehler, Fehler Dritter, Nichterfüllung vertraglicher Anforderungen (z. B. Softwarewartung), Wartungsfehler, Missbrauch der Autorisierung, Software-Nutzung, Manipulation der SDLC-Infrastruktur, Serviceverweigerung, Manipulation von Informationen, Offenlegung, Verlust/Leckage von Informationen
Softwarebestandteile	Insider-Bedrohung, Hacktivismus, Verlust von Support-Diensten, unbeabsichtigte Änderungen, fehlerhafte Verwendung oder Verwaltung von Geräten und Systemen, Schäden durch Dritte, Informationslecks, Sabotage, Vandalismus und Diebstahl, Angriffe mit physischem Zugriff, erzwungener Zugriff, Vertragsanforderungen, Software-Schwachstellen, SDLC-Prozessfehler, Fehler Dritter, Nichterfüllung vertraglicher Anforderungen (z. B. Softwarewartung), Wartungsfehler, Missbrauch der Autorisierung, Software-Nutzung, Manipulation der SDLC-Infrastruktur, Serviceverweigerung, Manipulation von Informationen, Offenlegung, Verlust/Leckage von Informationen

Bedrohungen für neue Technologien

_ Intelligente Fahrzeuge

VERWANDTE KOMPONENTEN - VERMÖGENSGRUPPEN	BEDROHUNG
Fahrzeugsensoren und -aktoren	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Bedrohungen für autonome Sensoren, Bedrohungen gegen KI und ML, Sabotage, Vandalismus, Diebstahl, Seitenkanalangriffe, Fehlerinjektion, Ausfall oder Fehlfunktion eines Sensors/Aktuators, Ausnutzung von Software-Schwachstellen, Entführung von Kommunikationsprotokollen, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, fehlerhafte Verwendung der Konfiguration von Fahrzeugkomponenten, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.
Entscheidungsalgorithmen **Auto-Steuergeräte, Verarbeitungs- und Entscheidungskomponenten** **Intelligente Autos Infrastruktur- und Backend-Systeme**	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Bedrohungen für autonome Sensoren, Bedrohungen gegen KI und ML, Sabotage, Vandalismus, Diebstahl, Ausfall oder Fehlfunktion eines Sensors/Aktuators, Ausnutzung von Software-Schwachstellen, Versagen oder Störung eines Services, Entführung von Kommunikationsprotokollen, Datenwiedergabe, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, fehlerhafte Verwendung der Konfiguration von Fahrzeugkomponenten, Verlust des GNSS-Signals, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.

VERWANDTE KOMPONENTEN - VERMÖGENSGRUPPEN	BEDROHUNG
Fahrzeugfunktionen Fahrzeugsensoren und -aktoren Auto-Steuergeräte, Verarbeitungs- und Entscheidungskomponenten	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Bedrohungen für autonome Sensoren, Bedrohungen gegen KI und ML, Sabotage, Seitenkanalangriffe, Fehlerinjektion, Diebstahl, Ausfall oder Fehlfunktion eines Sensors/Aktuators, Ausnutzung von Software-Schwachstellen, Versagen oder Störung eines Services, Entführung von Kommunikationsprotokollen, Datenwiedergabe, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, fehlerhafte Verwendung der Konfiguration von Fahrzeugkomponenten, verbrauchte Fahrzeugbatterie, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.
Software-Management Auto-Steuergeräte, Verarbeitungs- und Entscheidungskomponenten Kommunikationskomponenten im Fahrzeug	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Sabotage, Seitenkanalangriffe, Fehlerinjektion, Diebstahl, Ausfall oder Fehlfunktion eines Sensors/Aktuators, Ausnutzung von Software-Schwachstellen, Versagen oder Störung eines Services, Entführung von Kommunikationsprotokollen, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.
Kommunikationskomponenten im Fahrzeug	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Sabotage, Seitenkanalangriffe, Fehlerinjektion, Diebstahl, Ausfall oder Fehlfunktion eines Sensors/Aktuators, Ausnutzung von Software-Schwachstellen, Entführung von Kommunikationsprotokollen, Datenwiedergabe, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, fehlerhafte Verwendung der Konfiguration von Fahrzeugkomponenten, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.

Bedrohungen für neue Technologien

Intelligente Fahrzeuge

VERWANDTE KOMPONENTEN - VERMÖGENSGRUPPEN	BEDROHUNG
Kommunikationsnetzwerke und -protokolle **Auto-Steuergeräte, Verarbeitungs- und Entscheidungskomponenten** **Kommunikationskomponenten im Fahrzeug**	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Sabotage, Diebstahl, Ausfall oder Fehlfunktion eines Sensors/Aktuators, Ausnutzung von Software-Schwachstellen, Entführung von Kommunikationsprotokollen, Datenwiedergabe, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, fehlerhafte Verwendung der Konfiguration von Fahrzeugkomponenten, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.
Externe Komponenten in der näheren Umgebung **Intelligente Autos Infrastruktur- und Backend-Systeme**	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Sabotage, Vandalismus, Diebstahl, Ausnutzung von Software-Schwachstellen, Versagen oder Störung eines Services, Entführung von Kommunikationsprotokollen, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, Verlust des GNSS-Signals, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.

VERWANDTE KOMPONENTEN - VERMÖGENSGRUPPEN	BEDROHUNG
Server, Systeme und Cloud Computing Intelligente Autos Infrastruktur- und Backend-Systeme	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Sabotage, Ausnutzung von Software-Schwachstellen, Versagen oder Störung eines Services, Entführung von Kommunikationsprotokollen, Datenwiedergabe, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, Verlust des GNSS-Signals, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.
Informationen	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Bedrohungen für autonome Sensoren, Bedrohungen gegen KI und ML, Sabotage, Vandalismus, Diebstahl, Seitenkanalangriffe, Fehlerinjektion, Ausfall oder Fehlfunktion eines Sensors/Aktuators, Ausnutzung von Software-Schwachstellen, Versagen oder Störung eines Services, Entführung von Kommunikationsprotokollen, Datenwiedergabe, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Informationslecks, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, fehlerhafte Verwendung der Konfiguration von Fahrzeugkomponenten, Verlust des GNSS-Signals, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.
Menschen	Serviceverweigerung, Malware, Manipulation von Informationen, gezielte OEM-Angriffe, nicht autorisierte Aktivitäten, Identitätsdiebstahl, Missbrauch von Berechtigungen, Sabotage, Vandalismus, Diebstahl, Ausfall oder Fehlfunktion eines Sensors/Aktuators, Ausnutzung von Software-Schwachstellen, Versagen oder Störung eines Services, Entführung von Kommunikationsprotokollen, Datenwiedergabe, Man-in-the-Middle-Angriff / Sitzungsentführung, unbeabsichtigte Änderung der Daten- oder Fahrzeugkomponentenkonfiguration, Verwendung von Informationen und/oder Geräten aus einer unzuverlässigen Quelle, fehlerhafte Verwendung der Konfiguration von Fahrzeugkomponenten, Verlust des GNSS-Signals, Verbrauchte Fahrzeugbatterie, Netzwerkausfall, Nichteinhaltung vertraglicher Anforderungen, Verstoß gegen Regeln, Vorschriften oder Gesetze / Missbrauch personenbezogener Daten.

Literaturangaben

1. "April 2020 Cyber Attacks Statistics". 3. Juni, 2019. HACKMAGEDDON. https://www.hackmageddon.com/2020/06/03/april-2020-cyber-attacks-statistics/

2. "Data Breach Investigation Report" 2019. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

3. "CIRCL - Operational Statistics" 2019. CIRCL. https://www.circl.lu/opendata/statistics/

4. "Survey: The Third Annual Study on the State of Endpoint Security Risk". 2020. https://engage.morphisec.com/2020-endpoint-security-risk-study

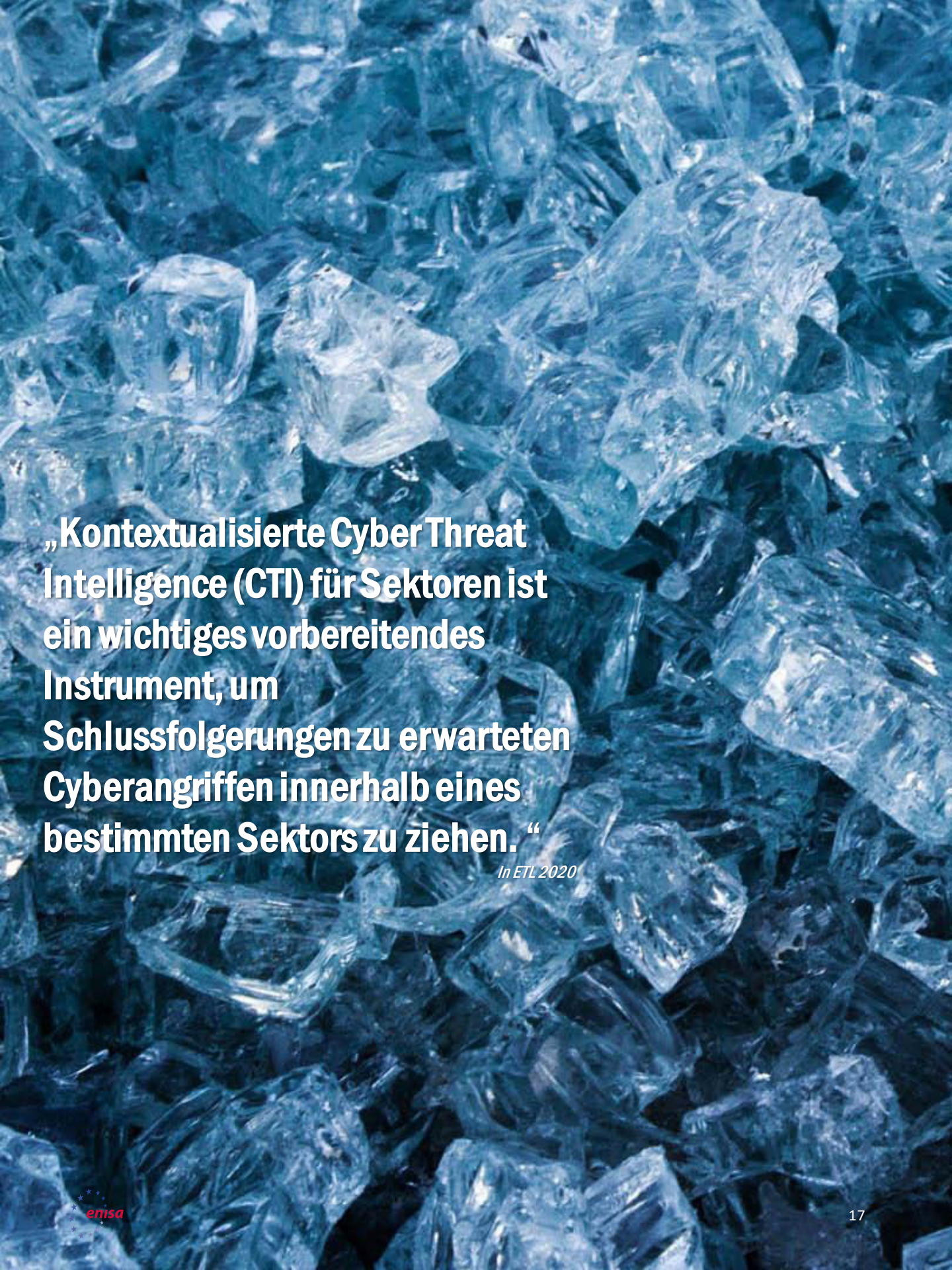
5. "Good Practices for Security of IoT - Secure Software Development Lifecycle". 19. November, 2019. ENISA https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

6 "ENISA good practices for security of Smart Cars". 25. November, 2019. https://www.enisa.europa.eu/publications/smart-cars

7. Die ausgewählte Reihenfolge der Sektoren wurde durch Konsolidierung von Statistiken aus verschiedenen vorfallbasierten Berichten durchgeführt. Es liefert mediale Werte für den Berichtszeitraum (2019-Q1 2020) und kann geringfügig von den in monatlichen oder vierteljährlichen Berichten angegebenen Werten abweichen.

8. "Player vs. Hacker: Cyberthreats to Gaming Companies and Gamers'. 16. März, 2020. GSMA Intelligence. https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/

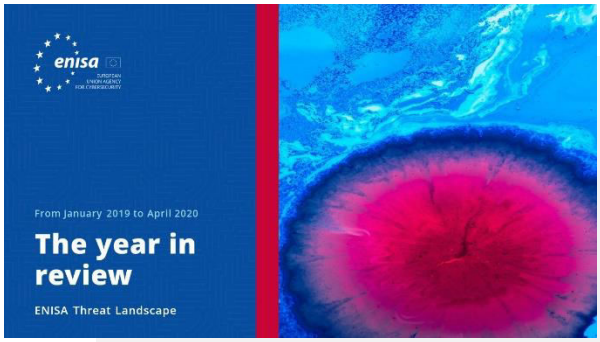
9. Erwähnenswert ist, dass die Gefährdung anhand detaillierter Bedrohungskategorien bewertet wurde, die von ENISA entwickelt wurden (siehe https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view) und dass sie für verschiedene Sektorbeurteilungen verwendet wurde. Aufgrund des Fehlens von Ereignisdaten für aufstrebende Sektoren wird die Bedrohungsbewertung detaillierter durchgeführt, um einen umfassenderen Ansatz zu erhalten.



„Kontextualisierte Cyber Threat Intelligence (CTI) für Sektoren ist ein wichtiges vorbereitendes Instrument, um Schlussfolgerungen zu erwarteten Cyberangriffen innerhalb eines bestimmten Sektors zu ziehen. “

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
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 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