DE

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Von Januar 2019 bis April 2020

Hauptvorfälle in der EU und weltweit

ENISA Threat Landscape

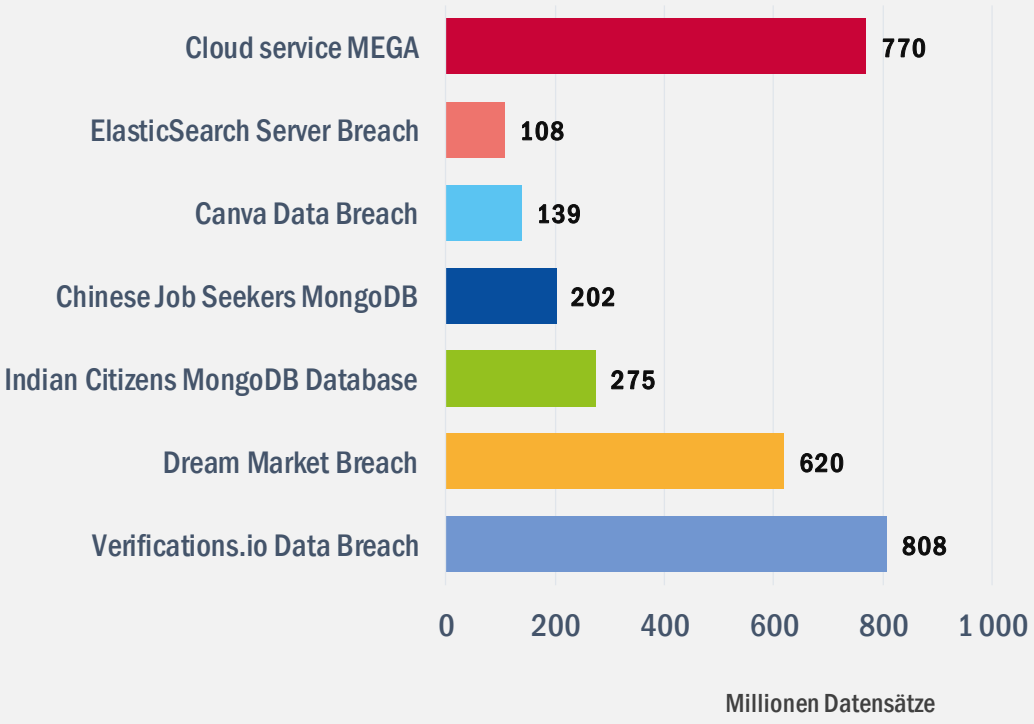
Überblick

Die Komplexität der Bedrohungsfähigkeiten nahm 2019 zu, und viele Gegner nutzten Exploits, Diebstahl von Anmeldedaten und mehrstufige Angriffe. Die Anzahl der Vorfälle mit Datenschutzverletzungen ist immer noch sehr hoch, und die Menge gestohlener Finanzinformationen und Benutzeranmeldeinformationen nimmt zu. In einigen Fällen kann das Nicht-Patchen einer bekannten Sicherheitsanfälligkeit in einem angemessenen Zeitraum, was sich möglicherweise auf verwendete Software oder Bibliotheken auswirkt, schwerwiegende Auswirkungen haben.

Während des letzten Jahrzehnts **hat Malware ENISAs Liste der 15 größten Bedrohungen angeführt, dennoch können viele Sicherheitssysteme diese Bedrohung nicht erkennen**. Über viele Jahre hinweg wurde Malware hauptsächlich durch böswilligen E-Mail-Spam und in jüngerer Zeit durch subtil gestaltete Phishing-Nachrichten verbreitet. Technologieunternehmen und E-Mail-Anbieter investierten gleichermaßen in Spam-Filter, um die Erkennung bösartiger Anhänge zu verbessern. **Gegner sind jetzt jedoch innovativ, um ihre Chancen zu erhöhen, potenzielle Opfer zu erreichen.** Viele dieser Innovationen haben sich in dieser Zeit für böswillige Akteure ausgezahlt.

Die COVID-19-Pandemie hat Gesundheitsorganisationen und Fachkräfte weltweit unter Druck gesetzt, und die Gesundheit ist zu einem der wichtigsten Sektoren beim Schutz vor Cyberangriffen geworden. Die Anzahl der Vorfälle mit Ransomware für den Gesundheitssektor war bereits hoch, stieg jedoch während der Pandemie noch weiter an.

Hauptvorfälle Datenschutzverletzungen



Zeitplan

2019

_ Januar

MEGA Cloud (NZ) erlitt eine Datenschutzverletzung, die 770 Millionen E-Mails und 21 Millionen Passwörter enthüllte.[1]

_ Februar

Verification.io (US) legte ca. 800 Millionen Datensätze bloß.[2]

_ März

Norsk Hydro (NO) war Opfer eines Ransomware-Angriffs.[3]

_ August

Das bulgarische Finanzamt (BG) erlitt eine Datenschutzverletzung, bei der personenbezogene Daten von allen erwachsenen Bürgern offengelegt wurden.[8]

_ September

Mastercard (BE) wurde Opfer einer Datenschutzverletzung, von der ca. 90.000 Kunden in Europa betroffen waren.[9]

_ Oktober

Websites und der nationale Fernsehsender in Georgia (GE) erlitten einen koordinierten Cyberangriff.[30]

_ November

UniCredit (IT) wurde Opfer einer Datenschutzverletzung, bei der 3 Millionen Datensätze verloren gegangen sind.[10]

_ Dezember

Prosegur (SP) erlitt einen Ransomware-Angriff, der den Betrieb störte.[11]

2020

_ Januar

Der österreichische Außenminister (AT) wurde Ziel eines Cyberangriffs.[12]

_ April

Facebook (USA) meldete eine Datenschutzverletzung, die 540 Millionen Benutzerdatensätze auf exponierten Servern enthüllte.[4]

_ Mai

Thyssen-Krupp und Bayer (DE) waren Ziel einer Spionage-Malware.[5]

_ Juli

City Power (ZA) wurde Opfer eines Ransomware-Angriffs, der die Energieversorgung in Johannesburg unterbrach.[7]

_ Juni

Fünf Krankenhäuser in Rumänien (RO) wurden durch eine Badrabbit Ransomware getroffen.[6]

_ Februar

Die INA Group (HR) wurde Opfer eines Ransomware-Angriffs.[13]

_ März

Das ENTSO-E (BE) -Netzwerk wurde kompromittiert und Opfer eines Eindringens.[14]

_ April

Über 500.000 Zoom-Konten (USA) wurden im Dark Web zum Verkauf angeboten.[31]

Die häufigsten Zielbranchen

In der Schusslinie

Die Sektoren, die in diesem Zeitraum am meisten angesprochen wurden, waren digitale Dienste, die Regierungsverwaltung und die Technologiebranche. Angriffe auf digitale Dienstleister werden häufig stellvertretend vorgenommen, um andere, attraktivere Ziele zu erreichen. Im Gegensatz dazu ermöglichten Angriffe auf die Technologiebranche böswilligen Akteuren, die Lieferkette zu gefährden oder nach Schwachstellen zu suchen, die ausgenutzt werden konnten.

Die E-Mail-Plattform **verifications.io**[18], erlitt aufgrund einer ungeschützten MongoDB-Datenbank eine schwerwiegende Datenschutzverletzung. Daten von über 800 Millionen E-Mails wurden offengelegt und enthielten vertrauliche Informationen, einschließlich personenbezogener Daten (PII).

In einem beliebten Hacking-Forum des Cloud-Dienstes **MEGA** wurden über 770 Millionen E-Mail-Adressen und 21 Millionen eindeutige Passwörter offengelegt[1]. Dies wurde die bedeutendste Sammlung von verletzten persönlichen Anmeldeinformationen in der Geschichte mit dem Namen „Sammlung Nr. 1“.

Der Cloud- und Virtualisierungsanbieter **Citrix** wurde Opfer eines gezielten Cyberangriffs. Um Zugriff auf die Citrix-Systeme zu erhalten, nutzten die Angreifer mehrere kritische Software-Schwachstellen wie CVE-2019-19781 und verwendeten eine Technik namens Passwort-Spaying.

Der Cloud-Hosting-Anbieter **iNSYNQ**[19] erlebte einen Ransomware-Angriff, bei dem Kunden länger als eine Woche nicht auf ihre Daten zugreifen konnten, sodass sie sich auf lokale Backups verlassen mussten.

Die häufigsten Zielbranchen

Digitale Dienste_ Dienste wie E-Mail, soziale und kollaborative Plattformen sowie Cloud-Anbieter wurden 2019 angegriffen. Diese wurden auch als Proxies für weitere Angriffe verwendet.

Regierungsverwaltung_ Die finanziellen Erträge aus Lösegeldzahlungen machen den öffentlichen Sektor zu einem der attraktivsten Ziele für Ransomware-Angriffe.

Technologiebranche_ Die Technologiebranche wurde 2019 hauptsächlich durch Angriffe in der Lieferkette getroffen, die versuchten, die Entwicklung von Software durch Zero-Day-Exploits und Backdoors-Angriffe zu gefährden.

Finanziell_ Die Anzahl der Vorfälle mit Finanzorganisationen und nicht unbedingt mit Banken hat im Berichtszeitraum erheblich zugenommen.

Gesundheitswesen_ Die Zahl der Angriffe auf den Gesundheitssektor nimmt weiter zu.

Entwicklungen

_Über die Grenze

- Im Jahr 2019 wurde weltweit eine intensive **Trojaner-Aktivität** beobachtet. Emotet und Agent Tesla waren die häufigsten und gefährlichsten Arten von Malware.
- **Phishing** blieb eine der erfolgreichsten Techniken zur Bereitstellung bösartiger Instrumente. Zu den leistungsstarken Phishing-Ködern gehören Telefonbetrug, gefälschte Rechnungen, Zahlungen, Angebote sowie Kauf- und Kundenaufträge.
- **Ransomware** generiert weiterhin erhebliche finanzielle Belohnungen für böswillige Akteure. In einer kürzlich durchgeführten Studie wurden von Menschen betriebene Ransomware-Kampagnen[17], identifiziert, in denen Gegner Diebstahl von Anmeldedaten und „lateral Movement"-Pfade anwenden, die traditionell mit gezielten Angriffen wie denen von nationalstaatlichen Akteuren verbunden sind.
- **Karten-Skimming**-Programme sind in den Jahren 2019 und 2020 aufgrund der zunehmenden Anzahl von Online-Käufern zu einer erheblichen Bedrohung geworden.
- **Die Kompromittierung geschäftlicher E-Mails (Business E-Mail Compromise, BEC)** ist aufgrund der großen Menge an Anmeldedaten und personenbezogenen Daten, die im letzten Jahrzehnt gestohlen wurden, eine wachsende Bedrohung.
- Unternehmen erleiden jeden Monat durchschnittlich 12 Angriffe in Bezug auf den **Diebstahl von Anmeldedaten**, bei denen der Angreifer gültige Anmeldedaten identifizieren kann.

Erkenntnisse

84 % der Cyberangriffe beruhen auf Social Engineering

67 % der Malware wurden über verschlüsselte HTTPS-Verbindungen bereitgestellt[34]

230.000 täglich neue Belastungen durch Malware

6 Monate dauert es im Durchschnitt, bis eine Datenschutzverletzung entdeckt wird

71 % der Unternehmen erkannten Malware-Aktivitäten, die sich von einem Mitarbeiter auf einen anderen ausbreiteten[35]

Akteure

_Wer

Zu wissen, wer für einen Cybersicherheitsvorfall verantwortlich ist oder welcher Person oder Gruppe dieser zugeordnet werden kann, ist immer noch eine sehr entmutigende Aufgabe und oft sinnlos. Aus Sicht der Bedrohungsinformationen ist es jedoch wichtig, Verhaltensweisen zu klassifizieren und die Dynamik und *Vorgehensweise* bestimmter Gegner zu verstehen. Diese Analyse hilft Datenschützern oft, nach bestimmten Spuren zu suchen und zu versuchen, die nächste gegnerische Aktion zu antizipieren.

Die **Lazarus-Gruppe** zum Beispiel, eine angeblich staatlich geförderte Gruppe für fortgeschrittene persistente Bedrohungen (Advanced Persistent Threat, APT), war im Berichtszeitraum Berichten zufolge sowohl bei finanziell als auch bei spionagemotivierten Angriffen aktiver. Die Gruppe wurde mit mehreren Vorfällen in Verbindung gebracht, einschließlich der **AppleJeus-Kampagne**, die sich an Benutzer der Kryptowährungs-Handelsplattform und deren Systeme richtet.[22] Zu den wichtigsten Vorfällen, die dieser Gruppe zugeordnet werden, gehören:

- Hacking eines indischen Kernkraftwerks und einer Weltraumforschungsorganisation im November 2019;
- Kompromittierung einer Kryptowährungs-Handels-App für Börsenadministratoren im Oktober 2019;
- Angriff auf Geldautomaten (ATMs) und Banken in Indien, identifiziert im September 2019;
- Zielgruppe sind Android-Nutzer in Südkorea über trojanisierte Apps im Google Play Store, die im August 2019 identifiziert wurden.

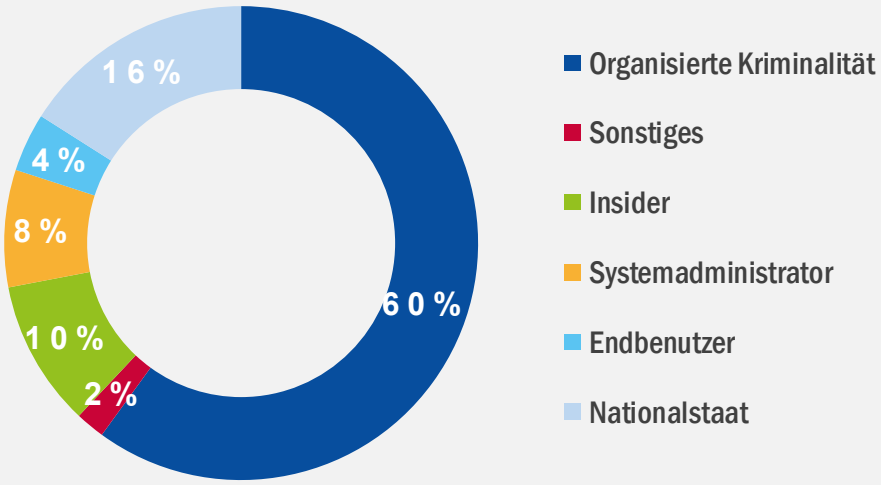
Die aktivsten Akteure

TURLA_ Es wurde berichtet, dass die Gruppe 2019 in mehr als 40 Ländern auf Microsoft Exchange-E-Mail-Server in den Bereichen Bildung, Regierung, Militär, Forschung und Pharmazie ausgerichtet war.[23]

APT27_ Es wurde berichtet, dass die Gruppe die SharePoint-Server von Regierungsorganisationen in zwei verschiedenen Ländern im Nahen Osten kompromittiert hat.

VICIOUS PANDA_ Im April 2020 wurde die mongolische öffentliche Verwaltung angeblich von der Gruppe ins Visier genommen.[24]

GAMAREDON_ Die Gruppe hat Berichten zufolge das Verteidigungsministerium der Ukraine in einer Spear-Phishing-Kampagne ab Dezember 2019 angegriffen.[25]



Motive

_Warum

Obwohl es schwierig ist, die Hauptmotive für einen Cyberangriff zu bestimmen, können wir sie dennoch anhand des Ergebnisses des Vorfalls kategorisieren.

Finanziell: Die Anzahl der beobachteten Vorfälle, die zum Diebstahl von Informationen, Daten und Benutzeranmeldedaten geführt haben, ist im Berichtszeitraum am höchsten. In den meisten Fällen besteht die Absicht darin, Daten/Informationen zu stehlen und im Dark Web zu verkaufen. Andere Verwendungen dieser Informationen/Daten, um andere Arten von Angriffen mit einem völlig anderen Ergebnis wie Spionage oder Finanzbetrug zu ermöglichen, können ebenfalls identifiziert werden. Mehr als 620 Millionen Kontodaten wurden von 16 gehackten Websites gestohlen und auf dem beliebten Dark-Web-Marktplatz Dream Market zum Verkauf angeboten.

Spionage: Dies ist ein Motiv für eine zunehmende Anzahl gemeldeter Angriffe, hauptsächlich aufgrund anhaltender geopolitischer und wirtschaftlicher Spannungen. Die Anzahl der Vorfälle ist nicht wesentlich, aber aufgrund Größe und Umfang steht sie an zweiter Stelle in der Liste der fünf wichtigsten Motive von ENISA. Einige bemerkenswerte Vorfälle sind die im April 2019 gemeldeten, bei denen ein Mitarbeiter von General Electric und ein chinesischer Geschäftsmann vom US-Justizministerium wegen Wirtschaftsspionage und Diebstahls der Geschäftsgeheimnisse von General Electric angeklagt wurden.[20] AgenceFrance Presse (AFP) berichtete, dass Airbus Opfer einer ausgeklügelten Cyberspionagekampagne geworden ist. Berichten zufolge haben Angreifer die IT-Systeme mehrerer Airbus-Zulieferer verletzt und sind von dort aus in die IT-Systeme des Unternehmens eingedrungen.[21]

Die fünf wichtigsten Motive: Finanzen, Spionage, Störung, Politik und Vergeltung.

Die wichtigsten Motive

Die folgende Abbildung zeigt, dass **Finanzen** nach wie vor das Hauptmotiv für die meisten Cyberangriffe ist. In einigen Fällen können mehrere Motive innerhalb eines einzelnen Angriffs identifiziert werden. Zum Beispiel sind Spionage, Politik, Finanzen und Störung oft kombinierte Motive. Viele Vorfälle stammen von automatisierten Systemen und werden als Service geliefert und in Kryptowährung bezahlt. Diese Dienste umfassen die Verteilung von Ransomware, Command and Control (C2), Distributed Denial of Service (DDoS), Spam und andere illegale Aktivitäten.

Angriffsvektoren

_ Wie

Cyberangriffe erfolgen durchschnittlich in drei Schritten, um an die wertvollen Vermögenswerte eines Opfers zu gelangen. Bei der Überprüfung der am häufigsten verwendeten Angriffsvektoren müssen der Einstiegspunkt, die Vorgehensweise und die Asset-Aktion priorisiert werden. Dies sind die kritischsten Phasen, die unterschiedliche Ansätze in einer Verteidigungsstrategie erfordern.

Einstiegspunkt: Im Jahr 2019 gehören zu den Techniken, die am häufigsten zum Starten eines Cyberangriffs verwendet werden, Brute Force mit gestohlenen Anmeldedaten, Social Engineering, Konfigurationsfehler und der Betrieb von Webanwendungen. Die Nutzung von Webanwendungen wurde beispielsweise häufig als Einstiegspunkt verwendet, da diese Art von Anwendung zunehmend zur Übertragung von Daten in die Cloud eingesetzt wurde. Fehler in der Cloud-Konfiguration und der Missbrauch von Systemen waren bei einer Vielzahl von Vorfällen ein wesentlicher Einstiegspunkt. Der Einsatz von Social Engineering zur Planung eines Angriffs basiert auf Instrumenten wie Phishing und Business E-Mail-Kompromittierung (BEC)[16]. Andere Techniken, die seltener, aber ebenso wichtig sind, sind die Ausnutzung von Schwachstellen (von nicht gepatchten Systemen und Zero-Days) und Software-Backdoors, die häufig bei komplexeren und ausgeklügelteren Angriffen verwendet werden.

Vorgehensweise: Die Installation von Malware ist die am häufigsten verwendete Technik in der Phase „Vorgehensweise". Einmal installiert, hilft sie dem Gegner, auszuspähen, sich in den Systemen und Netzwerken des Opfers zu bewegen, zusätzliche Instrumente wie Ransomware zu installieren, Daten zu stehlen und mit einem C2-Server zu kommunizieren.

_Fünf begehrteste Vermögenswerte durch Cyberkriminelle

01_Gewerbliches Eigentum und Geschäftsgeheimnisse

Gewerbliches Eigentum und Geschäftsgeheimnisse sind aufgrund ihres hohen Werts für ihre Eigentümer, den Markt und in einigen Fällen die kriminelle Welt die begehrtesten Vermögenswerte.

02_Staatliche/militärische Informationen

Dieser Vermögenswert beinhaltet alle Informationen, die ein Staat als vertraulich erachtet. Im Jahr 2019 machten der Handel und die diplomatischen Spannungen zwischen den Ländern diese Art von Informationen noch attraktiver.

03_Serverinfrastruktur

Die Serverinfrastruktur ist das erste vertrauliche Asset, bei dem es sich nicht um Daten handelt. Bei vielen Angriffen ist die Übernahme der Serverinfrastruktur des Opfers das Hauptziel.

04_Authentifizierungsdaten

Authentifizierungsdaten sind wertvolle Ressourcen zur Erzielung von Gewinnen, aber auch als Ziel zur Unterstützung eines Angriffs.

05_Finanzielle Daten

Finanzielle Daten wie Kreditkarten-, Bank- und Zahlungsinformationen sind für Cyberkriminelle immer wertvoll.

Strategische Intelligenz

_Was hat sich in der Landschaft mit der Covid-19-Pandemie verändert?

Im Jahr 2019 setzte ENISA die Kartierung der Bedrohungslandschaft fort und half Entscheidungsträgern und Politikern dabei, Strategien zur Verteidigung von Bürgern, Organisationen und des Cyberspace zu definieren. Diese Arbeit ist Teil der Strategie von ENISA, ihren Interessenvetretern strategische Informationen zur Verfügung zu stellen. Das zentrale Thema im Jahr 2019 war die nächste Generation der Mobilfunktelekommunikation (5G) auf Ersuchen der Europäischen Kommission und der Mitgliedstaaten. **Die Agenturwird diese thematischen Bedrohungslandschaftsberichte weiterhin produzieren**, und im Jahr 2020 liegt der Schwerpunkt auf künstlicher Intelligenz.

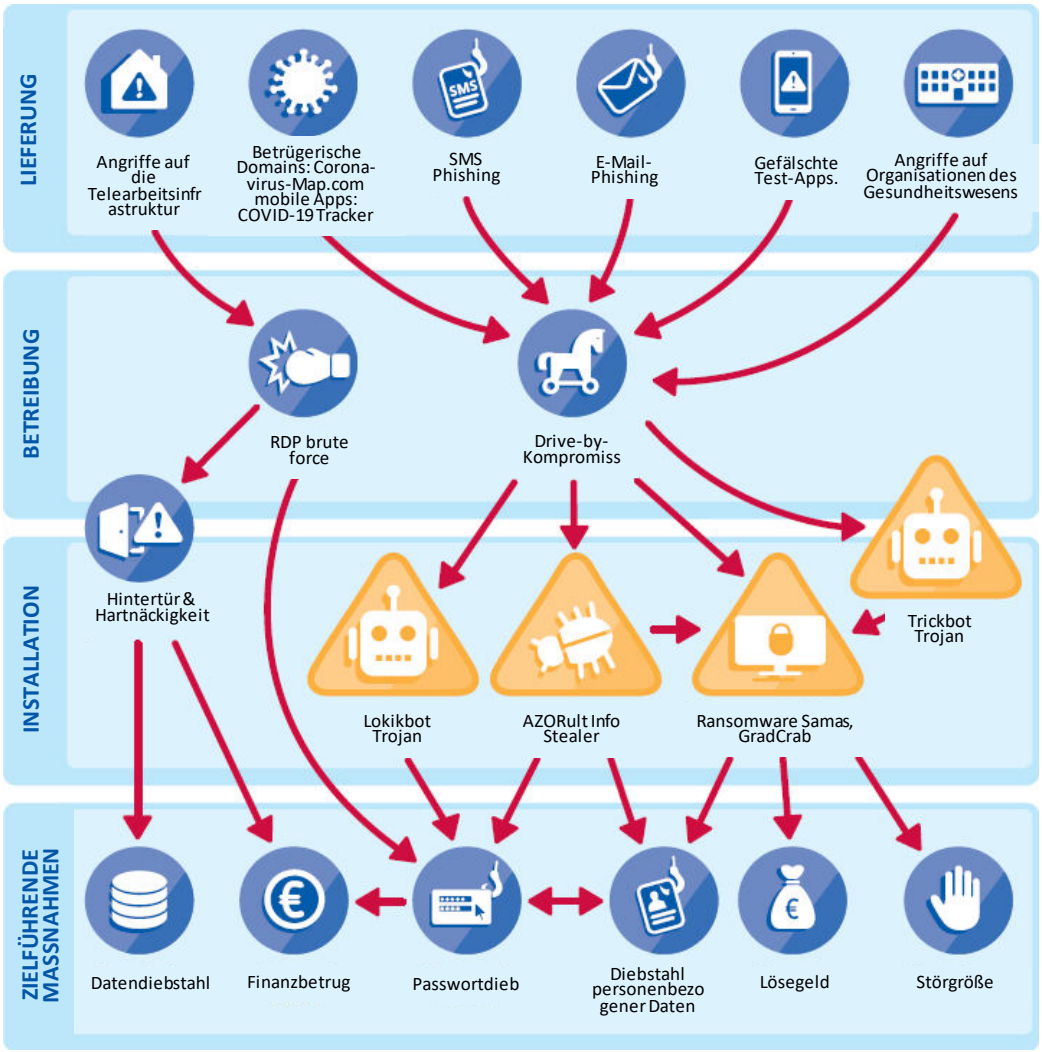
Die COVID-19-Pandemie war eine produktive Zeit für böswillige Akteure, die Angriffe auf sensible Bereiche wie Gesundheitsdienstleister und von zu Hause aus arbeitende Personen durchführen. ENISA kartiert die während der Pandemie erlebte Bedrohungslandschaft und berät zu Minderungsmaßnahmen, mit denen versucht werden soll, die Gefährdung zu verringern.

ENISA teilt ihre Cybersicherheitsempfehlungen zur COVID-19-Pandemie zu einer Vielzahl von Themen, einschließlich Telearbeit, Online-Shopping und E-Health, und bietet den betroffenen Sektoren wertvolle aktuelle Sicherheitsratschläge.[32]

Das **Brno University Hospital** in der Tschechischen Republik erlitt mitten in der COVID-19-Pandemie einen Cyberangriff[33], der es zwang, Patienten umzuleiten und Operationen zu verschieben. Der Vorfall wird als kritisch angesehen, da dieses Krankenhaus eines der größten COVID-19-Testlabors der Tschechischen Republik ist.

_COVID-19 Bedrohungslandschaft

ENISA bereitete viele Ressourcen für eine Aufklärungskampagne vor und teilte andere interne und externe Ressourcen für Cybersicherheitsexperten, die Sicherheitsfragen im Zusammenhang mit den Herausforderungen während der COVID-19-Pandemie abdeckten. Eine dieser Ressourcen war eine Analyse der kritischsten Bedrohungen in diesem Zeitraum.



Literaturangaben

1. "MEGA Data Breach Exposed 773 Million Email Addresses and Passwords." 19. Januar, 2019. Latest Hacking News. https://latesthackingnews.com/2019/01/19/mega-data-breach-exposed-773-million-email-addresses-and-passwords/

2. "Largest Leak in History: Email Data Breach Exposes Over Two Billion Personal Records." 8. April, 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/largest-leak-in-history-email-data-breach-exposes-over-two-billion-personal-records/

3. "LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company." 20. März, 2019. Recorded Future. https://www.recordedfuture.com/lockergoga-ransomware-insight/

4. "Researchers find 540 million Facebook user records on exposed servers." 3. April, 2019. Tech Crunch. https://techcrunch.com/2019/04/03/facebook-records-exposed-server/

5. "Winnti: Attacking the Heart of the German Industry" 24. Juli, 2019. Web.br. https://web.br.de/interaktiv/winnti/english/

6 "Cyber-attacks against 5 hospitals in Romania. CCR's website, also hacked" 20. Juni, 2019. Romanian Journal. https://www.romaniajournal.ro/society-people/cyber-attacks-five-hospitals-romania-ccr-website-hacked/

7. "Here's how ransomware attacks like the one on CityPower work – and why some victims end up paying criminals millions" 25. Juli, 2019. Business Insider South Africa. https://www.businessinsider.co.za/ransomware-attack-on-citypower-johannesburg-why-victims-pay-criminals-2019-7

8. "Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged." 30. August, 2019. Bank Info Security. https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000

9. "Breach Of Mastercard Loyalty Program Affected 90K Germans' Data" 23. August, 2019. PYMNTS.com. https://www.pymnts.com/news/security-and-risk/2019/mastercard-loyalty-program-data-breach-germany/

10. "UniCredit confirms data breach" 28. Oktober, 2019. PrivSec Report. https://gdpr.report/news/2019/10/28/privacy-unicredit-confirms-data-breach/

11. "Prosegur Hacked: Spanish SOC Provider Hit by Ryuk Ransomware" 28. November, 2019. Computer Business Review. https://www.cbronline.com/news/prosegur-hacked-ransomware

12. "Serious cyber-attack' on Austria's foreign ministry" 5. Januar, 2020. BBC. https://www.bbc.com/news/world-europe-50997773

13. "Croatia's largest petrol station chain impacted by cyber-attack" 20. Februar, 2020. ZDNet. https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/

14. "European power grid organization says its IT network was hacked" 9. März, 2020. Cyberscoop. https://www.cyberscoop.com/european-entso-breach-fingrid/

15. "Fullz House hackers pivot from phishing to Magecart card skimming attacks" 26. November, 2019. ZDNet. https://www.zdnet.com/article/fullz-house-threat-group-pivots-from-phishing-to-magecart-card-skimming-attacks/

16. "FBI warns of cloud based BEC attacks." 8. April, 2020. Info Security. https://www.infosecurity-magazine.com/news/fbi-warns-of-cloudbased-bec-attacks/

17 "Microsoft Alerts Healthcare to Human-Operated Ransomware" 1. April, 2020. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/microsoft-alerts-healthcare-to-human-operated-ransomware/d/d-id/1337463

18. "Verification.io suffers major data breach." 15. März, 2019. PrivSec Report. https://gdpr.report/news/2019/03/15/verification-io-suffers-major-data-breach/

19. "Inside the Insynq attack: 'We had to assume they were listening'" 8. August, 2019. Accounting Today. https://www.accountingtoday.com/news/inside-the-insynq-ransomware-attack-we-had-to-assume-they-were-listening

20. "Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets". 23. April, 2019. USA DoJ. https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

21. "Airbus supply chain hacked in a cyberespionage campaign" 27. September, 2019. CERT-EU. https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf

22. "Lazarus group's 'AppleJeus' sequel targets cryptocurrency traders" 10. Januar, 2020. The Cyber-Security Source. https://www.scmagazineuk.com/lazarus-groups-applejeus-sequel-targets-cryptocurrency-traders/article/1670446

23 "Russian Nation-State Group Employs Custom Backdoor for Microsoft Exchange Server" 7. Juli, 2019. Dark Reading. https://www.darkreading.com/application-security/russian-nation-state-group-employs-custom-backdoor-for-microsoft-exchange-server/d/d-id/1334628

24. "Vicious Panda: The COVID Campaign" 12. März, 2020. Check Point Research. https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

25. "Gamaredon APT Improves Toolset to Target Ukraine Government, Military" 5. Februar, 2020. Threat Post. https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/

26. "Virus attacks Spain's defense intranet, foreign state suspected: paper" 26. März, 2019. Reuters. https://www.reuters.com/article/us-spain-security-cyberattack/virus-attacks-spains-defense-intranet-foreign-state-suspected-paper-idUSKCN1R7115

27 "115 Million Pakistani Mobile Users Data Go on Sale on Dark Web" 10. April, 2020. Rewterz. https://www.rewterz.com/articles/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web

28. "Your business hit by a data breach? Expect a bill of $3.92 million" 23. Juli, 2019. ZDNet. https://www.zdnet.com/article/your-business-hit-by-a-data-breach-expect-a-bill-of-3-92-million/

29. "Cyber Security Statistics for 2019" 21. März, 2019. Cyber Defense. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

30. "Georgia 'I'll Be Back' Cyber Attack Terminates TV, Takes Down 15,000 Websites." 29. Oktober, 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites/#1a5746347a48

31. "Half a million Zoom accounts for sale on the dark web." 16. April, 2020. We Live Security by ESET. https://www.welivesecurity.com/2020/04/16/half-million-zoom-accounts-sale-dark-web/

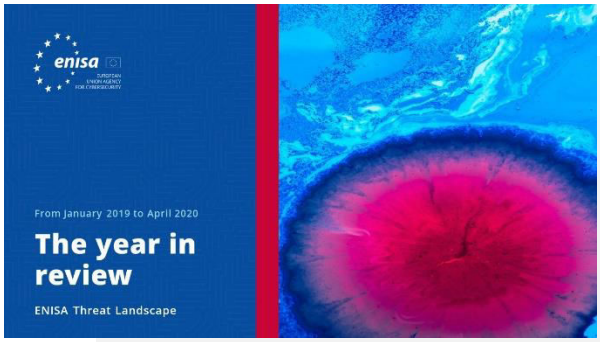
32. "ENISA COVID-19 Resources". ENISA https://www.enisa.europa.eu/topics/wfh-covid19

33. "Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak" 17. März, 2020. Security Magazine. https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak

34. "Most malware in Q1 2020 was delivered via encrypted HTTPS connections". 25. Juni, 2020 Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

35. "Malware statistics and facts for 2020" 29. Juli, 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/

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**

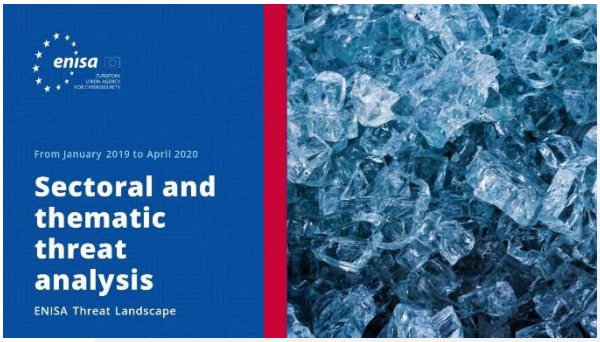
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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

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 Anmeldedaten 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