enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Cyberspionage

ENISA Threat Landscape

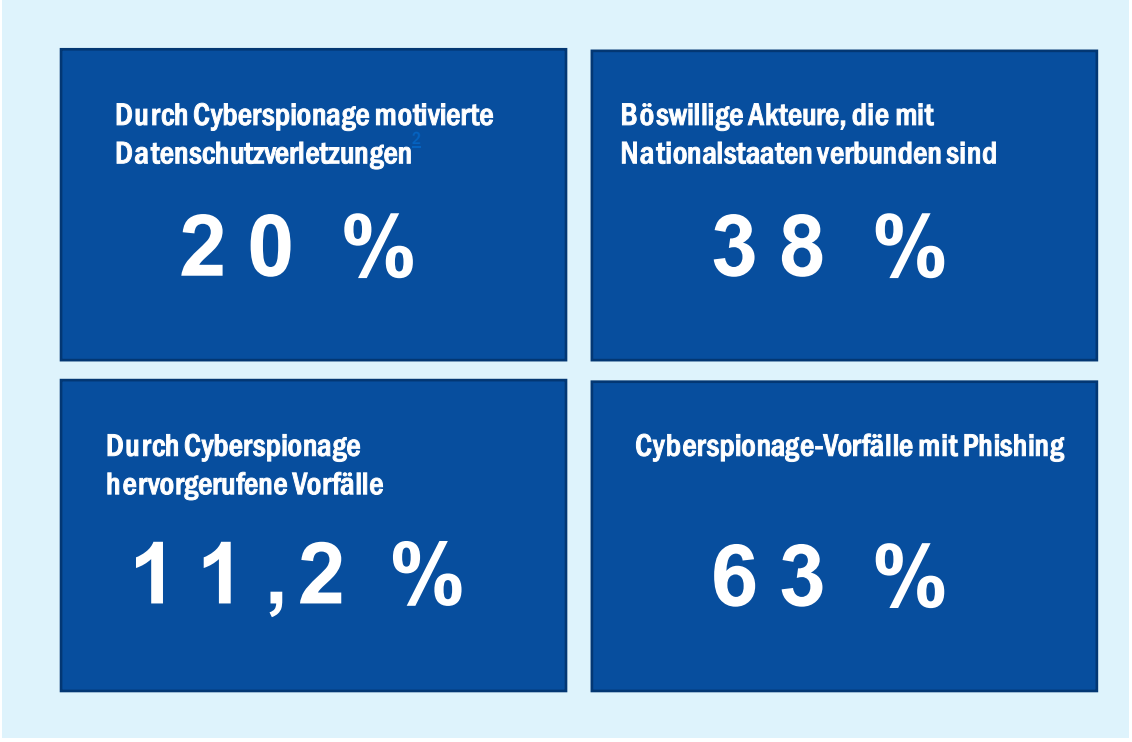
Überblick

Cyberspionage wird im Manuskript zur Cybersicherheit sowohl als Bedrohung als auch als Motiv angesehen. Es ist definiert als „die Verwendung von Computernetzwerken, um illegalen Zugang zu vertraulichen Informationen zu erhalten, die normalerweise von einer Regierung oder einer anderen Organisation gehalten werden“.[1]

Im Jahr 2019 enthüllten viele Berichte, dass globale Organisationen Cyberspionage (oder nationalstaatlich geförderte Spionage) als wachsende Bedrohung für den Industriesektor sowie für kritische und strategische Infrastrukturen auf der ganzen Welt betrachten, darunter Ministerien, Eisenbahngesellschaften, Telekommunikationsanbieter, Energieunternehmen, Krankenhäuser und Banken. Cyberspionage konzentriert sich darauf, die Geopolitik zu lenken und Staats- und Geschäftsgeheimnisse, Rechte an geistigem Eigentum und geschützte Informationen in strategischen Bereichen zu stehlen. Sie mobilisiert auch Akteure aus Wirtschaft, Industrie und ausländischen Geheimdiensten sowie Akteure, die in ihrem Namen arbeiten. In einem kürzlich veröffentlichten Bericht waren Analysten von Bedrohungsinformationen nicht überrascht zu erfahren, dass 71 % der Unternehmen Cyberspionage und andere Bedrohungen als „Black Box“ behandeln und immer noch mehr darüber erfahren.

Im Jahr 2019 nahm die Zahl der von Nationalstaaten gesponserten Cyberangriffe auf die Wirtschaft zu, und es ist wahrscheinlich, dass dies auch weiterhin so bleibt. Im Einzelnen nehmen nationalstaatlich geförderte und andere von Gegnern verursachte Angriffe auf das industrielle Internet der Dinge (IIoT) in den Sektoren Versorger, Öl und Erdgas (ONG) sowie im verarbeitenden Gewerbe zu. Darüber hinaus weisen Cyberangriffe von APT-Gruppen (Advanced Persistent Threat) darauf hin, dass finanzielle Angriffe häufig durch Spionage motiviert sind. Gruppen wie die Cobalt Group, Carbanak und FIN7 haben mit Taktiken, Techniken und Verfahren (TTPs), die denen ihrer Spionagekollegen ähneln, angeblich erfolgreich große Finanzinstitute und Restaurantketten ins Visier genommen.

- Der Ausschuss für auswärtige Angelegenheiten des Europäischen Parlaments forderte die Mitgliedstaaten auf, eine Cyber-Defense-Einheit einzurichten und gemeinsam an ihrer gemeinsamen Verteidigung zu arbeiten. Darin heißt es: „Das strategische Umfeld der Union hat sich verschlechtert, ...um den vielfältigen Herausforderungen zu begegnen, die sich direkt oder indirekt auf die Sicherheit ihrer Mitgliedstaaten und ihrer Bürger auswirken. Dabei umfassen Fragen, die die Sicherheit der EU-Bürger betreffen, Folgendes: Bewaffnete Konflikte unmittelbar im Osten und Süden des europäischen Kontinents und fragile Staaten; Terrorismus - und insbesondere Dschihadismus -, Cyberangriffe und Desinformationskampagnen; ausländische Einmischung in europäische politische und Wahl-Prozesse “.[42]
- Bedrohungsakteure, die durch finanzielle, politische oder ideologische Vorteile motiviert sind, konzentrieren sich zunehmend auf Angriffe auf Lieferantennetzwerke mit schwachen Cybersicherheitsprogrammen. Cyberspionage-Gegner haben ihre Angriffsmuster langsam auf die Ausbeutung von Lieferkettenpartnern von Dritt- und Viertanbietern verlagert.[1]



Störfälle

- Das südkoreanische Verteidigungsministerium gab bekannt, dass unbekannte Hacker Computersysteme im Beschaffungsbüro des Ministeriums kompromittiert hatten.[3]
- Das US-Justizministerium kündigte eine staatlich geförderte Operation mit einem Botnetz an, das durch die Ausrichtung auf Unternehmen aus den Bereichen Medien, Luft- und Raumfahrt, Finanzen und kritische Infrastruktursektoren gestört werden soll.[16]
- Das norwegische Softwareunternehmen Visma gab bekannt, dass es von Hackern angegriffen wurde, die versuchten, den Kunden des Unternehmens Geschäftsgeheimnisse zu stehlen.[4]
- Einzelpersonen wurden in einem frühen Stadium des Zugangs zu Computersystemen mehrerer politischer Parteien und des australischen Bundesparlamentstages ertappt.[17]
- Das europäische Luft- und Raumfahrtunternehmen Airbus gab bekannt, dass es von mutmaßlichen nationalstaatlich gesponserten Hackern angegriffen wurde, die personenbezogene und IT-Identifikationsdaten vieler Mitarbeiter gestohlen haben.[19]
- Nach einem Angriff auf indische Streitkräfte in Kaschmir zielten pakistanische Hacker auf fast 100 Websites und kritische Systeme der indischen Regierung.[5]
- Die indonesische nationale Wahlkommission berichtete, dass chinesische und russische Personen die Wählerdatenbank vor den Präsidentschafts- und Parlamentswahlen im Land überprüft hatten.[20]
- Ausländische Hacker haben vor den EU-Wahlen im Mai mehrere europäische Regierungsbehörden ins Visier genommen.[21]
- Die australische Signalverwaltung gab bekannt, dass sie Cyberangriffe gegen ISIS im Nahen Osten durchgeführt hatte.[22]
- Die finnische Polizei untersuchte einen DoS-Angriff gegen den Webdienst, mit dem die Stimmenzahlen der finnischen Wahlen veröffentlicht wurden.[6]
- Das Hongkonger Büro von Amnesty International gab bekannt, dass es Opfer eines Cyberangriffs geworden war.[23]
- Die israelischen Streitkräfte starteten einen Luftangriff auf die Hamas, nachdem sie erfolglos versucht hatten, israelische Ziele zu hacken.[7]

- Ein iranisches Netzwerk von Websites und Konten wurde angeblich verwendet, um falsche Informationen über die Vereinigten Staaten, Israel und Saudi-Arabien zu verbreiten.[24]
- Kroatische Regierungsbehörden wurden in einer Reihe von Angriffen von nicht identifizierten staatlich geförderten Hackern angegriffen. Die Malware-Nutzdaten waren Empire Backdoor und SilentTrinity, von denen keines zuvor gesehen worden war.[26]
- Libyen verhaftete zwei Männer, denen vorgeworfen wurde, mit einer russischen „Trollfarm" zusammengearbeitet zu haben, um die Wahlen in mehreren afrikanischen Ländern zu beeinflussen.[27]
- Mehrere große deutsche Industrieunternehmen, darunter BASF, Siemens und Henkel, gaben bekannt, Opfer einer staatlich geförderten Hacking-Kampagne geworden zu sein.[28]
- Eine staatlich geförderte Gruppe führte angeblich eine Reihe von Cyberangriffen gegen ägyptische Journalisten, Wissenschaftler, Anwälte, Menschenrechtsaktivisten und Politiker durch.[8]
- Eine staatlich geförderte Hacking-Gruppe zielte auf Diplomaten und hochkarätige russischsprachige Benutzer in Osteuropa ab, unter Verwendung von Malware namens Attor.[29]
- Es wurde festgestellt, dass eine israelische Cybersicherheitsfirma Spyware verkauft hat, mit der hochrangige Regierungs- und Militärbeamte in mindestens 20 Ländern angegriffen wurden, indem eine Sicherheitslücke in WhatsApp ausgenutzt wurde.[32]
- Eine 7-jährige Kampagne einer nicht identifizierten spanischsprachigen Spionagegruppe hatte offenbar den Diebstahl sensibler Kartendateien von hochrangigen Beamten der venezolanischen Armee zur Folge.[10]
- Eine staatlich geförderte Cyberspionage-Gruppe führte angeblich eine Phishing-Kampagne gegen chinesische Regierungsbehörden und staatliche Unternehmen durch, um Informationen zu wirtschaftlichem Handel, Verteidigungsfragen und Außenbeziehungen zu erhalten.[33]
- Das tschechische Außenministerium wurde Opfer eines Cyberangriffs eines nicht näher bezeichneten ausländischen Staates.[34]
- Ein nichtstaatlicher Akteur zielte mit einem großen DDoS-Angriff auf die britische Labour-Partei ab, bei dem die Computersysteme der Partei vor den nationalen Wahlen vorübergehend offline geschaltet wurden.[36]

Vorfälle

Der Fall General Electric

Xiaoqing Zheng, ein amerikanischer Staatsbürger chinesischer Abstammung, wurde beschuldigt, gegen General Electric (GE) ausspioniert zu haben. Herr Zheng hat angeblich die Geheimnisse der Turbinentechnologie von GE gestohlen und sie einem chinesischen Geschäftsmann übergeben, der sie angeblich einem chinesischen Beamten übergeben hat. Herr Zheng hat von 2008 bis 2018 bei GE gearbeitet[15]

Das Justizministerium der Vereinigten Staaten beschuldigte die beiden Männer, Informationen gestohlen zu haben, um ihre eigenen Geschäftsinteressen an zwei Forschungs- und Entwicklungsunternehmen für Turbinen - Liaoning Tianyi Aviation Technology Co. Ltd. und Nanjing Tianyi Avi Tech Co. Ltd. - voranzutreiben.[47]

Die *Vorgehensweise* dieses Insider-Bedrohungsakteurs umfasste:

- Kopieren von Geheimnissen auf ein USB-Laufwerk, bis GE die Verwendung dieser Geräte blockiert hat;
- Verschlüsseln der Geheimnisse und Verwenden der Steganographie, um Datendateien im Binärcode digitaler Fotodateien zu verbergen;
- Anschließen eines iPhones an den Desktop-Computer, um das Bild zu kopieren;
- Senden der Dateien an seine persönliche E-Mail-Adresse.

Minderungsmaßnahmen

Aufgrund des umfassenden Charakters dieser Bedrohung könnten mehrere der in diesem Bericht für andere Bedrohungen empfohlenen Minderungsmaßnahmen als Teil der folgenden grundlegenden Minderungskontrollen eingesetzt werden[2]:

- Identifizierung geschäftskritischer Rollen in der Organisation und Einschätzung deren Exposition gegenüber Spionagerisiken. Bewertung solcher Risiken anhand von Geschäftsinformationen (d. h. Business Intelligence).
- Erstellung von Sicherheitsrichtlinien, die Personal-, Geschäfts- und Betriebssicherheitskontrollen berücksichtigen, um die Risikominderung zu gewährleisten. Dazu sollten Regeln und Praktiken für die Sensibilisierung, Unternehmensführung und Sicherheitsmaßnahmen gehören.
- Etablierung von Unternehmenspraktiken, um zu kommunizieren und die Mitarbeiter in den entwickelten Regeln zu schulen.
- Entwicklung von Bewertungskriterien (KPIs), um den Vorgang zu bewerten und an bevorstehende Änderungen anzupassen.
- Erstellung einer Whitelist für kritische Anwendungsdienste, abhängig von der bewerteten Risikostufe.
- Bewertung von Schwachstellen und regelmäßiges Patchen der Software, insbesondere für Systeme, die sich am Rand befinden.
- Implementierung des Need-to-Know-Prinzips zum Definieren von Zugriffsrechten und Einrichtung von Kontrollen, um den Missbrauch privilegierter Profile zu überwachen.
- Einrichtung einer Inhaltsfilterung für alle eingehenden und ausgehenden Kanäle (z. B. E-Mail, Web, Netzwerkverkehr).

Literaturangaben

1. "Cyber Threatscape Report. 2019." IDefense - Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

2. "Data Breach Investigations Report 2020" DBR & Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

3. Catalin Cimpanu."Hackers breach and steal data from South Korea's Defense Ministry" 16. Januar, 2019. ZDNet. https://www.zdnet.com/article/hackers-breach-and-steal-data-from-south-koreas-defense-ministry/

4. Jack Stubbs."China hacked Norway's Visma to steal client secrets: investigators" 6. Februar, 2019. Reuters. https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141

5. Kate Fazzini. "In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides". 28. Februar, 2019 CNBC. https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html

6 Kati Pohjanpalo. "Finland Detects Cyber Attack on Online Election-Results Service". 10. April, 2019. Bloomberg.

https://www.bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service

7. Lily Hay Newman "What Israel's Strike on Hamas Hackers Means For Cyberwar" 5. Juni, 2019. Wired. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

8."Egypt Is Using Apps to Track and Target Its Citizens, Report Says" 3. Oktober, 2019. The New York Times https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html

9. Colin Lencher."Huawei accuses the US of 'launching cyber attacks' against the company" 4. September, 2019.The Verge. https://www.theverge.com/2019/9/4/20849092/huawei-cyberattacks-us-government-netowrks-employee-harassment

10. Catalin Cimpanu "A cyber-espionage group has been stealing files from the Venezuelan military" 5. August, 2019. ZDNet. https://www.zdnet.com/article/a-cyber-espionage-group-has-been-stealing-files-from-the-venezuelan-military/

11. Catalin Cimpanu. "Croatian government targeted by mysterious hackers" 5. Juli, 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

12. Michael McGowan. "China behind massive Australian National University hack, intelligence officials say" 6. Juni, 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

13. "General election 2019: Labour Party hit by second cyber-attack" 12. November, 2019. BBC https://www.bbc.com/news/election-2019-50388879

14. Nicole Perlroth, Matthew Rosenberg. "Russians Hacked Ukrainian Gas Company at Center of Impeachment" 13. Januar, 2020. The New York Times https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html

15. Danny Bradbury . "GE Engineer Charged for Novel Data Theft" 24. April, 2019. Info Security. https://www.infosecurity-magazine.com/infosec/ge-engineer-charged-data-theft-1/

16. "U.S. announces disruption of 'Joanap' botnet linked with North Korea". 30. Januar, 2019. CyberScoop. https://www.cyberscoop.com/joanap-botnet-north-korea-department-of-justice/

17. "The cyber attack on Parliament was done by a 'state actor' — here's how experts figure that out". 20. Februar, 2019. ABC News. https://www.abc.net.au/news/2019-02-20/cyber-activists-or-state-actor-attack-how-experts-tell/10825466

18. "While Trump was meeting with Kim Jong Un in Vietnam, North Korean hackers reportedly attacked targets in the US". 5. März 2019. Business Insider. https://www.businessinsider.com/north-korean-hackers-trump-kim-meeting-mcafee-2019-3

19. "Airbus hit by series of cyber attacks on suppliers". 26. September, 2019. France 24. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

20. "Indonesia Says Election Under Attack From Chinese, Russian Hackers". 12. März 2019. Bloomberg. https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers

21. "Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections". 21. März 2019. ZDNet. https://www.zdnet.com/article/cyber-espionage-warning-russian-hacking-groups-step-up-attacks-ahead-of-european-elections/

22. "Australian cyber soldiers hacked Islamic State and crippled its propaganda unit – here's what we know". 18. Dezember 2019. ABC News. https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426

23. "State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack". 25. April, 2019. Amnesty International https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

24. "New Report Shows How a Pro-Iran Group Spread Fake News Online". 14. März 2019. The New York Times https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html

25. "China behind massive Australian National University hack, intelligence officials say". 6. Juni, 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

26. "Croatian government targeted by mysterious hackers". 5. Juli, 2019. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

27. "Two Russians accused of election interference arrested in Libya". 8. Juli, 2019. Cyber Scout. https://cyberscout.com/en/blog/two-russians-accused-of-election-interference-arrested-in-libya

28. "BASF, Siemens, Henkel, Roche target of cyber attacks". 24. Juli, 2019. Reuters. https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

29. "New espionage malware found targeting Russian-speaking users in Eastern Europe" 10. Oktober, 2019. ZDNet. https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

30. "Advanced Israeli spyware is targeting Moroccan human rights activists". November 2019. The NextWeb. https://thenextweb.com/security/2019/10/14/advanced-israeli-spyware-is-targeting-moroccan-human-rights-activists/

31. "Hacking the hackers: Russian group hijacked Iranian spying operation, officials say". 21. Oktober, 2019. Reuters. https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

32. "Israeli spyware allegedly used to target Pakistani officials' phones". 19. Dezember, 2019. The Guardian. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones

33. "A phishing campaign with nation-state hallmarks is targeting Chinese government agencies". 8. August, 2019. https://www.cyberscoop.com/china-phishing-anomali-nation-state-apt/

34. "Foreign power was behind cyber attack on Czech ministry: Senate". 13. August, 2019. Reuters. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

35. "Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications.". 15. August, 2019. The Wall Street Journal. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

36. "Labour suffers second cyber-attack in two days" 12. November, 2019. The Guardian. https://www.theguardian.com/politics/2019/nov/12/labour-reveals-large-scale-cyber-attack-on-digital-platforms

37. "Extensive hacking operation discovered in Kazakhstan". 23. November, 2019 ZDNet. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

Literaturangaben

38. "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems". 20. November, 2019 Wired. https://www.wired.com/story/iran-apt33-industrial-control-systems/

39. "Russian 'Gamaredon' Hackers Back at Targeting Ukraine Officials". 6. Dezember, 2019. Security Week. https://www.securityweek.com/russian-gamaredon-hackers-back-targeting-ukraine-officials

40. "Iran announced it foiled 'really massive' foreign cyber attack". 11. Dezember, 2019. Security Affairs. https://securityaffairs.co/wordpress/94981/cyber-warfare-2/iran-foreign-cyber-attack.html

41. "Croatian government targeted by mysterious hackers". 5. Juli, 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

42. "Report on the implementation of the common foreign and security policy – annual report" 18. Dezember, 2019. EU Parliament. https://www.europarl.europa.eu/doceo/document/A-9-2019-0054_EN.html

43. "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent". 26. September, 2012. Krebs on Security. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information

44. "Energy Manufacturer Also Victimized by IE Zero Day in Watering Hole Attack". 2. Januar, 2013. The Washington Post https://threatpost.com/energy-manufacturer-also-victimized-ie-zero-day-watering-hole-attack-010213/77359/

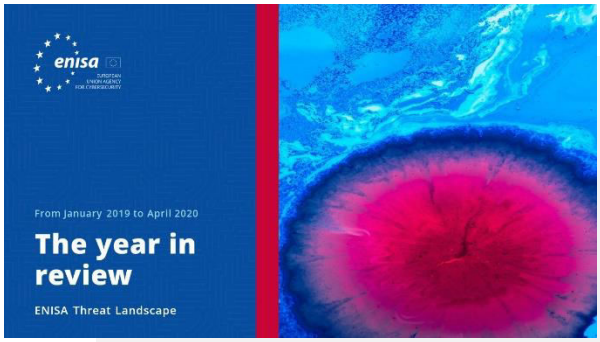
45. "The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity". 25. Februar, 2014. CrowdStrike Blog. https://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/

46. "Advanced Persistent Threat Groups". Fireeye. https://www.fireeye.com/current-threats/apt-groups.html

47. "U.S. accuses pair of stealing secrets, spying on GE to aid China". 23. April, 2019. Reuters. https://www.reuters.com/article/us-usa-justice-ge/us-accuses-pair-of-stealing-secrets-spying-on-ge-to-aid-china-idUSKCN1RZ24O


„Die Zahl der nationalstaatlich geförderten Cyberangriffe auf die Wirtschaft hat im Jahr 2019 zugenommen.“
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**

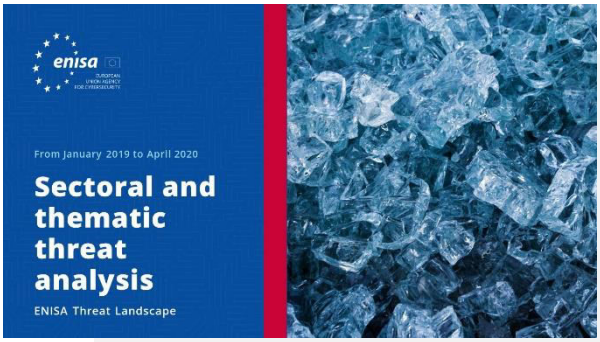
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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
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

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