



Von Januar 2019 bis April 2020

Angriffe auf Webanwendungen

ENISA Threat Landscape

Überblick

Webanwendungen und -technologien sind durch die Verwendung unterschiedlicher Verwendungszwecke und Funktionen zu einem zentralen Bestandteil des Internets geworden. Die zunehmende Komplexität von Webanwendungen und ihren weit verbreiteten Diensten schafft Herausforderungen bei der Sicherung derselben gegen Bedrohungen mit unterschiedlichen Motiven, von finanziellen oder Reputationsschäden bis hin zum Diebstahl kritischer oder personenbezogener Daten.¹ Webdienste und -anwendungen hängen hauptsächlich von Datenbanken ab, um die erforderlichen Informationen zu speichern oder bereitzustellen. SQLi-Angriffe (SQL Injection) sind ein bekanntes Beispiel und die häufigsten Bedrohungen für solche Dienste. Ein weiteres Beispiel sind Cross-Site-Scripting-Angriffe (XSS). Bei dieser Art von Angriff missbraucht der böswillige Akteur Schwachstellen in Formularen oder anderen Eingabefunktionen von Webanwendungen, die zu anderen schadhafte Funktionen führen, z. B. zur Weiterleitung auf eine betrügerische Website.²

Während Unternehmen in ihrem Webanwendungslebenszyklus immer kompetenter werden und eine konsistentere Automatisierung entwickeln, fordern sie Sicherheit als wichtigsten Teil ihres Angebots und ihrer Priorisierung. Diese Einführung komplexer Umgebungen führt zur Einführung neuer Dienste wie APIs (Application Programming Interfaces). APIs, die die beteiligten Unternehmen vor neue Herausforderungen für die Sicherheit von Webanwendungen stellen, um mehr Maßnahmen zur Prävention und Erkennung in Betracht zu ziehen. Beispielsweise haben rund 80 % der Unternehmen, die APIs einsetzen, Steuerelemente für ihren eingehenden Datenverkehr bereitgestellt.³ In diesem Abschnitt untersuchen wir die Bedrohungslandschaft von Webanwendungen im Jahr 2019.



Entwicklungen

20 % der Unternehmen und Organisationen meldeten täglich DDoS-Angriffe auf ihre Anwendungsdienste⁵

Buffer-Overflow war die am häufigsten verwendete Technik (24 %). HTTP-Flood (23 %), Ressourcenreduzierung (23 %), HTTPS-Flood (21 %) und Low Slow 21 % waren weitere häufig verwendete Techniken.

63 % der Befragten der CyberEdge-Umfrage verwenden eine Webanwendungs-Firewall (WAF).

27,5 % haben Pläne, diese Technologie einzusetzen, und 9,5 % haben diese nicht.¹⁵

52 % Zunahme der Anzahl der Angriffe auf Webanwendungen im Jahr 2019 im Vergleich zu 2018

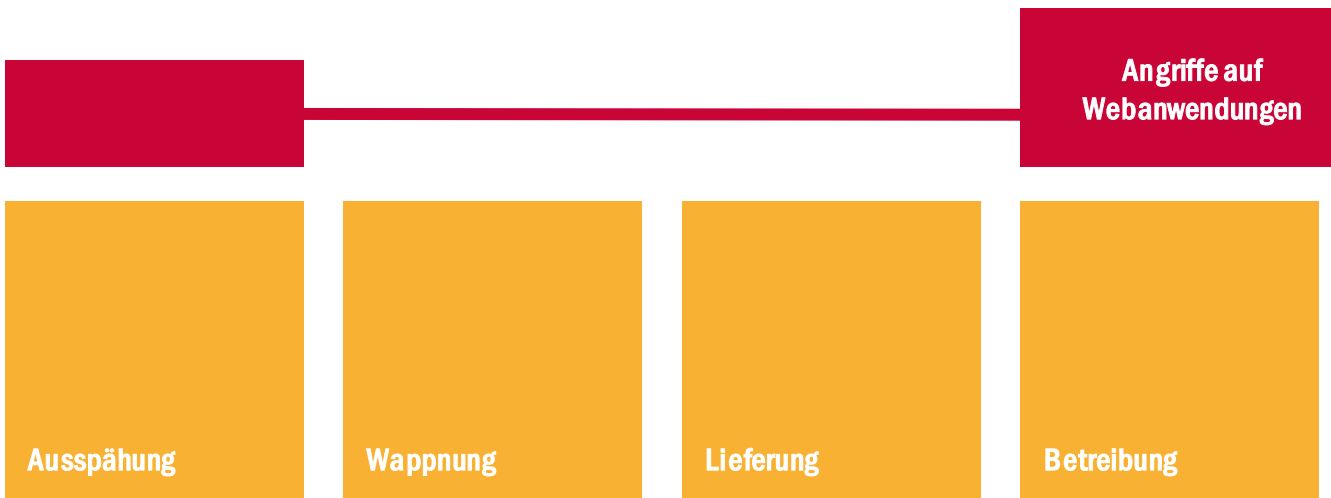
Laut einem Sicherheitsforscher war die Anzahl der Angriffe auf Webanwendungen im Vergleich zu 2018 nahezu unverändert und stieg später im Jahr stark an.⁴



84 % der beobachteten Schwachstellen in Webanwendungen waren Sicherheitsfehlfunktionen

Es folgten Cross-Site-Scripting (53 %) und interessanterweise eine fehlerhafte Authentifizierung (45 %).³



Kill chain



-  *Schritt des Angriffs-Workflows*
-  *Umfang des Zwecks*





Das Cyber Kill Chain® Framework wurde von Lockheed Martin entwickelt und basiert auf einem militärischen Konzept, das mit der Struktur eines Angriffs zusammenhängt. Um einen bestimmten Angriffsvektor zu untersuchen, verwenden Sie dieses Kill-Chain-Diagramm, um jeden Schritt des Prozesses sowie die vom Angreifer verwendeten Hilfsmittel, Techniken und Verfahren festzuhalten.

[WEITERE INFORMATIONEN](#)

— Verbesserte Zusammenarbeit zwischen Anwendungssicherheit und Anwendungsentwicklung

Laut der von einem Sicherheitsforscher durchgeführten Umfrage⁵, könnte einer der Faktoren, die zu einer solchen ineffektiven Sicherheit beitragen, die Entscheidung über den Besitz von Sicherheitstools sein. Die Umfrage präsentierte die Ansichten der Top-Influencer in diesem Bereich, in denen die IT-Führung und die Geschäftsinhaber und nicht der Chief Information Security Officer (CISO) genannt wurden.

— Wachsende Bedeutung von Application Programming Interfaces (APIs)

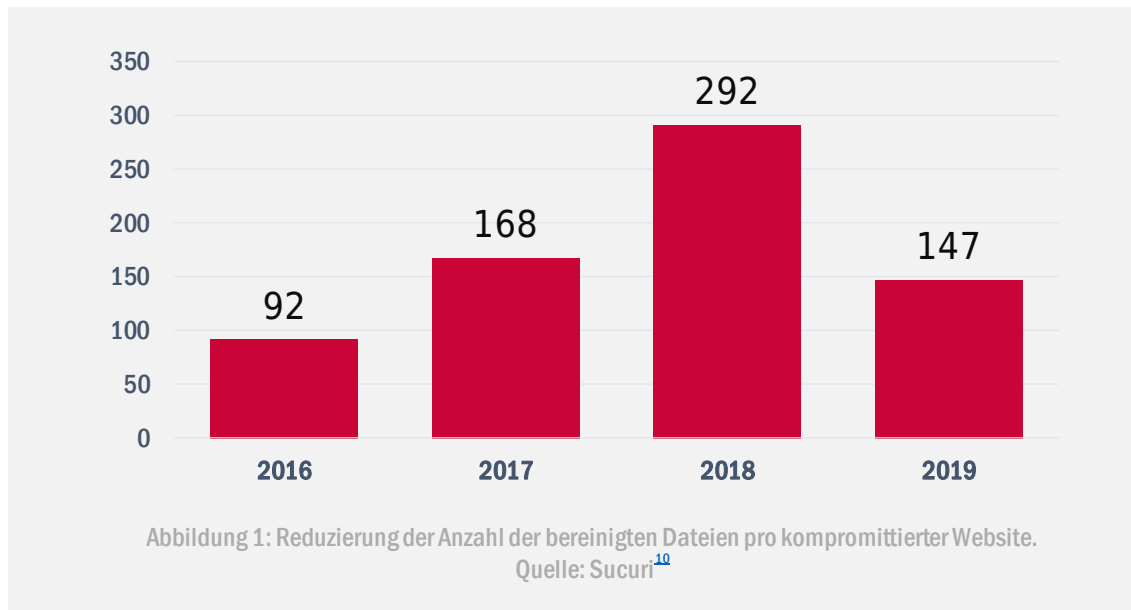
APIs sind in der Webanwendungsarchitektur nicht neu, und ihre allgemein akzeptierte Verwendung führt zu bestehenden Risiken und ihrer Wahrscheinlichkeit der Ausnutzung aufgrund der Erweiterung der Bedrohungslandschaft. Dementsprechend veröffentlichte das Open Web Application Security Project (OWASP) eine Top-10-Liste von API-Sicherheitsmaßnahmen (6), die eine priorisierte Möglichkeit bieten, diese Fähigkeit in der Webanwendungsarchitektur zu sichern. Ein Beispiel für eine solche Bedrohung sind die PHP-API-Angriffe: Laut einem anderen Sicherheitsforscher suchten 87 % der Scans des API-Verkehrs nach verfügbaren PHP-APIs.⁷

— Autorisierungs- und Authentifizierungsfehler

Dies ist normalerweise die Hauptursache dafür, dass böswillige Akteure Zugang zu kritischen Informationen erhalten (z. B. der Fast Retailing Verstoß⁸). Laut einem Sicherheitsforscher sind Verstöße gegen kritische Daten die zweithäufigste Bedrohung für die Sicherheit von Webanwendungen.⁹

Wachsender Trend mit SQL Injection (SQLi)

Eine kürzlich durchgeführte Sicherheitsuntersuchung ergab, dass zwei Drittel der Angriffe auf Webanwendungen SQLi-Angriffe umfassen. Während andere Angriffsmethoden für Webanwendungen entweder stabil blieben oder zunahmen, nahmen die SQLi-Angriffe weiterhin stark zu und eskalierten insbesondere während der Ferienzeit 2019.¹¹ Die Ergebnisse dieser Untersuchung ergaben auch, dass die Finanzbranche mehr lokalen „File inclusions“ (LFi) ausgesetzt ist im Vergleich zu anderen Sektoren.¹²

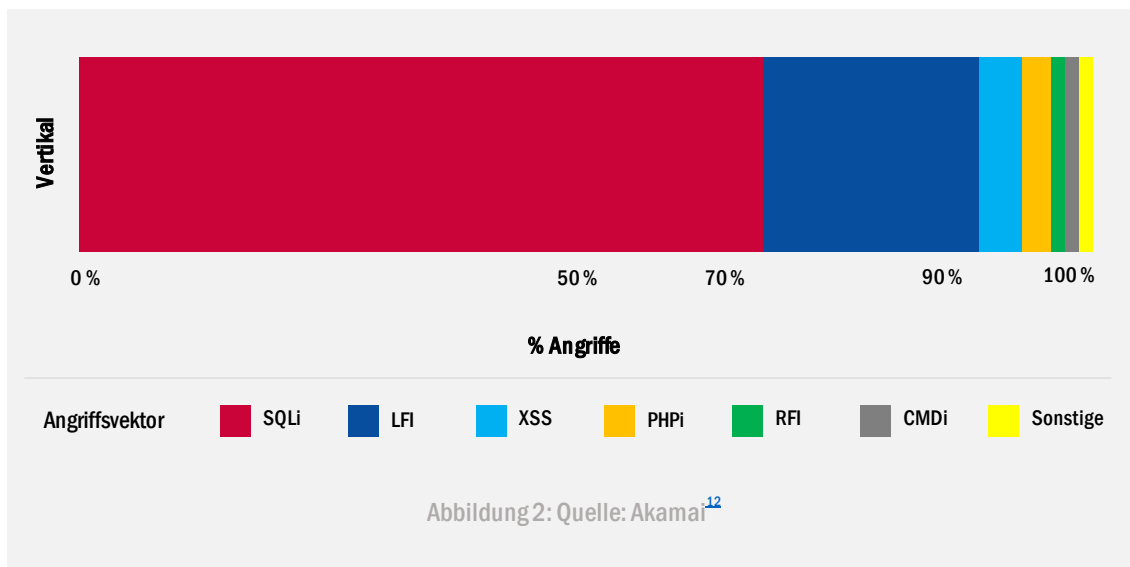


Angriffsvektoren

— Angriffsvektoren für Webanwendungen

Es besteht die allgemeine Auffassung, dass Angriffe auf Webanwendungen sehr unterschiedlich sind. Daten aus Sicherheitsuntersuchungen deuten jedoch darauf hin, dass die meisten Angriffe auf Webanwendungen auf SQLi oder LFI beschränkt sind.^{11,13,14} Ein anderer Bericht legt nahe, dass SQLi, Directory Traversal, XSS, fehlerhafte Authentifizierung und Sitzungsverwaltung ganz oben auf den Angriffsmethoden stehen, die bei dieser Art von Angriffen verwendet werden.⁴

SONICWALL meldete auch einen ähnlichen Trend für die Top-Webanwendungsangriffe für 2019. In der Liste SQLi standen Directory Traversal, XSS, fehlerhafte Authentifizierung und Sitzungsverwaltung ganz oben.⁴





— Angriffe auf Webanwendungen

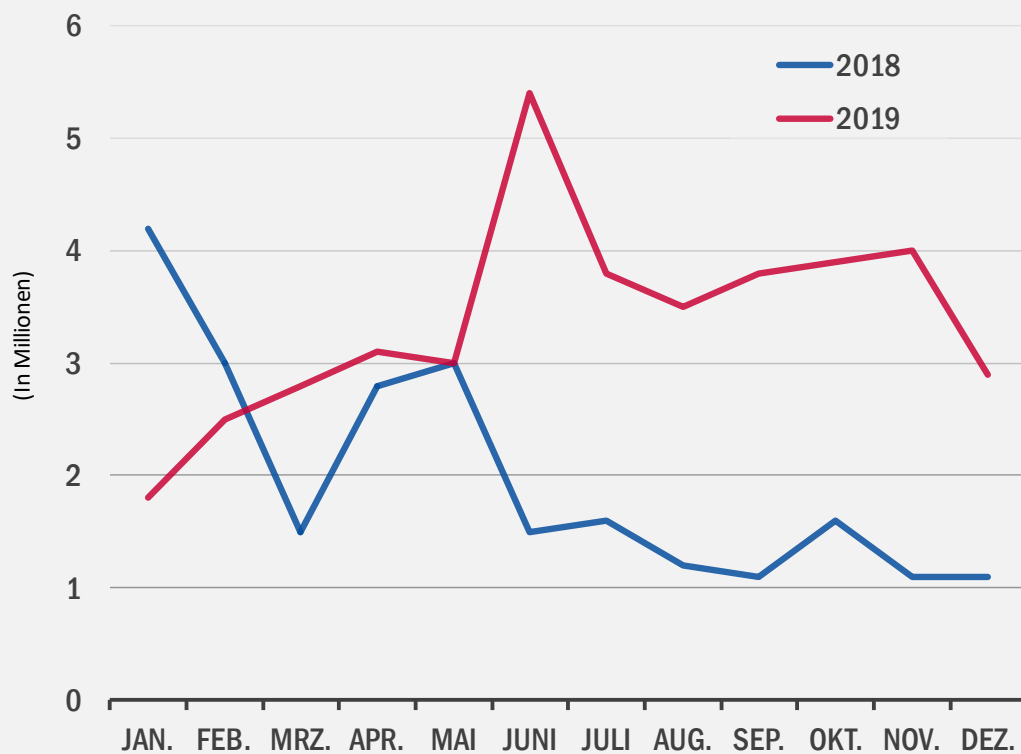


Abbildung 3 - Quelle: Sonicwall⁴

— Vorgeschlagene Maßnahmen

- Verwenden Sie Eingabevalidierungs- und Isolationstechniken für Angriffe mit Einschleusungen (also parametrisierte Anweisungen, Escape-Benutzereingaben, Eingabevalidierung usw.)¹⁶.
- Implementieren Sie Webanwendungs-Firewalls für vorbeugende und defensive Maßnahmen (17) (auch als virtuelles Patching bezeichnet).¹⁸
- Für Webanwendungs-APIs¹⁹:
 - Implementierung und Pflege eines Inventars von APIs und Validierung dieser anhand von Perimeter-Scans und interner Erkennung durch Entwicklungs- und Betriebsteams;
 - Verschlüsselung der API-Kommunikation und -Verbindung;
 - Bereitstellung der richtigen Authentifizierungsmechanismen und Berechtigungsstufen.
- Integration der Anwendungssicherheitsprozesse in den Zyklus der Anwendungsentwicklung und -wartung.²⁰
- Beschränkung des Zugriffs auf eingehenden Datenverkehr nur für die erforderlichen Dienste.²⁰
- Bereitstellung von Funktionen zur Verwaltung von Datenverkehr und Bandbreite.
- Erzwingen des Härtens von Webanwendungsservern und Bereitstellung von guten Patch-Management- und Testprozessen.²¹
- Durchführung von Schwachstellen- und Risikobewertungen vor und während der Entwicklung von Webanwendungen.
- Durchführung regelmäßiger Penetrationstests während der Implementierung und nach der Bereitstellung.





Webanwendungen nach maximalem Schweregrad der gefundenen Schwachstellen

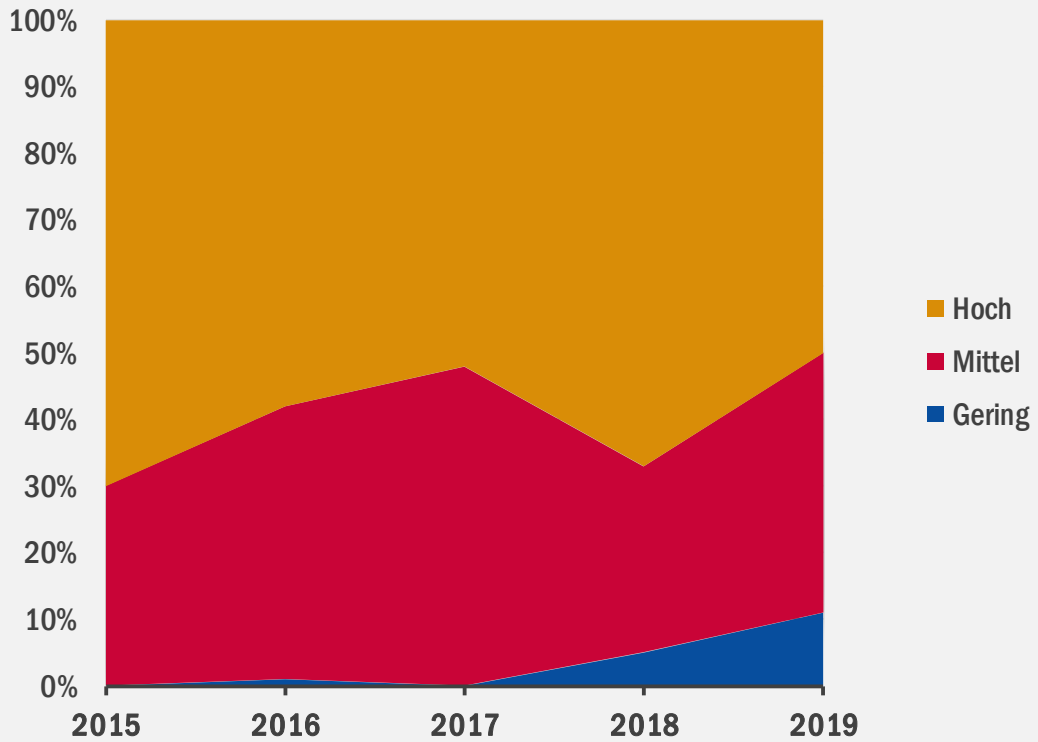


Abbildung 4 - Quelle: Positive Technologies²

Literaturangaben

1. "The Future Is the Web! How to Keep It Secure?" Oktober 2019. Acunetix. <https://www.acunetix.com/whitepaper-the-future-is-the-web/>
2. "What Is a Web Application Attack and how to Defend Against It". 2019. Acunetix. <https://www.acunetix.com/websitesecurity/web-application-attack/>
3. "2020 State of Application Services Report" F5 Networks, 2020. <https://www.f5.com/state-of-application-services-report>
4. "Sonicwall Cyber Threat Report". 2020. Sonicwall. <https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/>
5. "The State of Web Application Security, Protecting Application in the Microservice Era." 2019. Radware. <https://www.radware.com/resources/was-report-2019/>
6. "API Security Top 10 2019." OWASP. <https://owasp.org/www-project-api-security/>
7. Raymond Pompon, Sander Vinberg. "Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem." 13. August, 2019. F5 Labs <https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem>
8. "Unauthorized Logins on Fast Retailing Online Store Websites due to List Type Account Hacking and Request to Change Password." 13. Mai, 2019. Fast Retailing. <https://www.fastretailing.com/eng/group/news/1905132000.html>
9. "Web Applications vulnerabilities and threats: statistics for 2019." 13. Februar, 2020. Positive Technologies. <https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/#id9>
10. Esrtevaio Avillez. "2019 Website Threat Research Report." 2019. Sucuri. <https://sucuri.net/wp-content/uploads/2020/01/20-sucuri-2019-hacked-report-1.pdf>
11. "State of the Internet / Security | Web Attacks and Gaming Abuse (Volume 5, Issue 3)." 2017-2019. Akamai. <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-executive-summary-2019.pdf>
12. "State of the Internet Security | Financial Services – Hostile Takeover Attempts (Volume 6, Issue 1)." 2020. Akamai. <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf>
13. "Q4 2016 State of The Internet Security Report" 2016. Akamai. <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf>
14. "Q4 2017 State of the Internet Security Report" 2017. Akamai. <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf>
15. "2019 Cyberthreat Defense Report." 2019. CyberEdge Group. <https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf>
16. "AppSec Advisor: Injection Attacks." Oktober 2019. CIS Center for Internet Security. <https://www.cisecurity.org/newsletter/injection-attacks/>
17. "Cybersecurity threatscape: Q3 2019." 2. Dezember, 2019. Positive Technologies. <https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q3/#id5>
18. "Virtual Patching Best Practices." OWASP. https://owasp.org/www-community/Virtual_Patching_Best_Practices
19. Raymond Pompon, Sander Vinberg. "Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem." 13. August, 2019. F5 Labs. <https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem>
20. "2020 Cyber Threats, Business Email Compromise." 22. Oktober, 2019. <https://www.uscloud.com/blog/top-cyber-threats-in-2020/>
21. Sara Boddy, Remi Cohen. "Regional Threat Perspectives, Fall 2019: Asia." 2019. F5 Labs. <https://www.f5.com/labs/articles/threat-intelligence/regional-threat-perspectives--fall-2019--asia>

Die zunehmende Komplexität von Webanwendungen und ihren weit verbreiteten Diensten schafft Herausforderungen bei der Sicherung derselben gegen Bedrohungen mit unterschiedlichen Motiven, von finanziellen oder Reputationsschäden bis hin zum Diebstahl kritischer oder personenbezogener Daten. “

In ETL 2020

Themenbezogen



ENISA Threat Landscape Bericht Das Berichtsjahr

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

[LESEN SIEDEN 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 SIEDEN BERICHT](#)

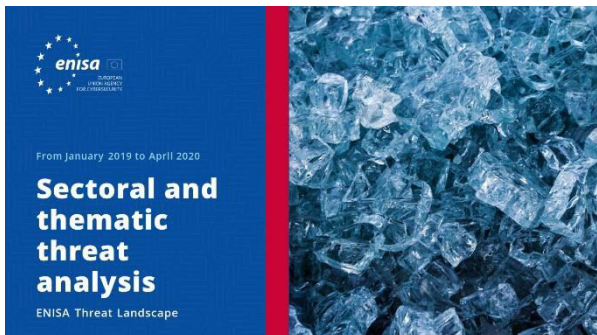


ENISA Threat Landscape Bericht Forschungsthemen

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

[LESEN SIEDEN BERICHT](#)





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.

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.

Hinweis zum Copyright

© European Union Agency for Cybersecurity (ENISA), 2020 Die Vervielfältigung ist gestattet, sofern die Quelle angegeben ist.

Copyright für das Bild auf dem Cover: © Wedia. Bei Verwendung oder Wiedergabe von Fotos oder sonstigem Material, das nicht dem Urheberrecht der ENISA unterliegt, muss die Zustimmung direkt bei den Urheberrechtseinhabern eingeholt 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



Alle Rechte vorbehalten. Copyright ENISA 2020.

<https://www.enisa.europa.eu>