enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Informations-lecks

ENISA Threat Landscape

Überblick

Eine Datenschutzverletzung liegt vor, wenn Daten, für die eine Organisation verantwortlich ist, einem Sicherheitsvorfall ausgesetzt sind, der zu einer Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität führt.[1] Eine Datenschutzverletzung verursacht häufig einen Informationsverlust, der eine der größten Bedrohungen für das Internet darstellt. Es deckt eine Vielzahl kompromittierter Informationen ab, von personenbezogenen Daten (PII) über in IT-Infrastrukturen gespeicherte Finanzdaten bis hin zu persönlichen Gesundheitsinformationen (PHI), die in den Medien von Gesundheitsdienstleistern gespeichert sind.

Wenn in den Schlagzeilen von Bulletins, Blogs, Zeitungen und technischen Berichten Sicherheitsverletzungen genannt werden, liegt der Schwerpunkt meist entweder auf Gegnern oder auf dem katastrophalen Versagen der Cyber-Defense-Prozesse und -Techniken. Die unbestreitbare Wahrheit ist jedoch, dass der Verstoß trotz der Auswirkungen oder des Umfangs eines solchen Ereignisses in der Regel durch die Handlung eines Einzelnen oder durch einen organisatorischen Prozessfehler verursacht wird.[2]

Erkenntnisse

2.013_bestätigte Datenoffenlegungen in 2019

Im ersten Halbjahr 2019 verzeichneten die Organisationen einen Anstieg der Offenlegungen um 11 % gegenüber 2018.[5,6]

14 %_aller Vorfällen im Finanzsektor waren Datenoffenlegungen

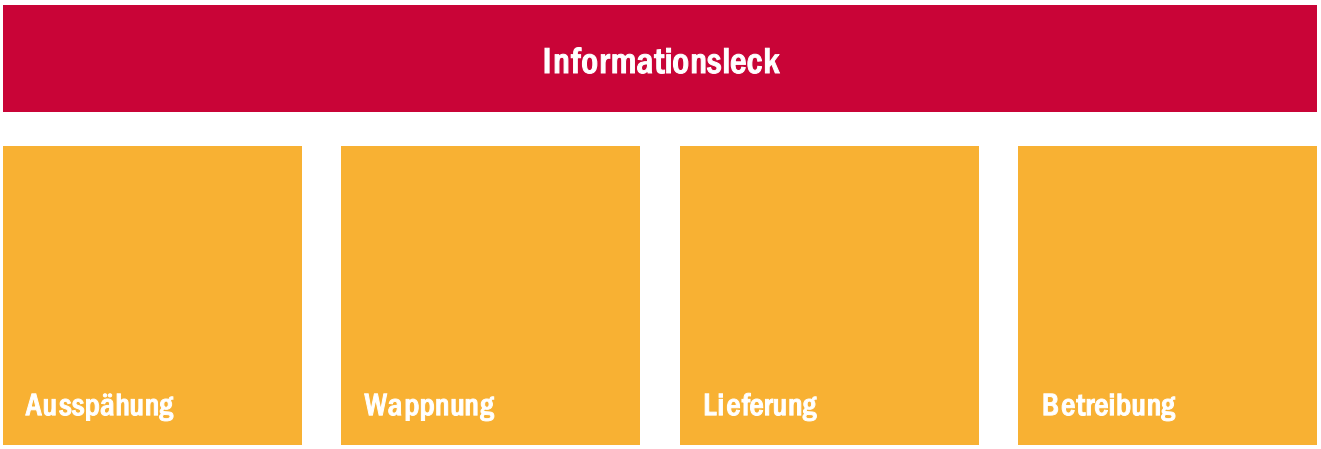
In 47 % dieser Fälle war das Opfer eine Bank.[9]

4,1_Milliarden Datensätze wurden im ersten Halbjahr 2019 offengelegt

E-Mail und Passwörter standen ganz oben auf der Liste.[10]

€5,46_Millionen sind die höchsten Kosten, die dem Gesundheitssektor angefallen sind[11]

Kill chain



Schritt des Angriffs-Workflows

Umfang des Zwecks

Installation

Command & Control

Zielführende Maßnahmen

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.

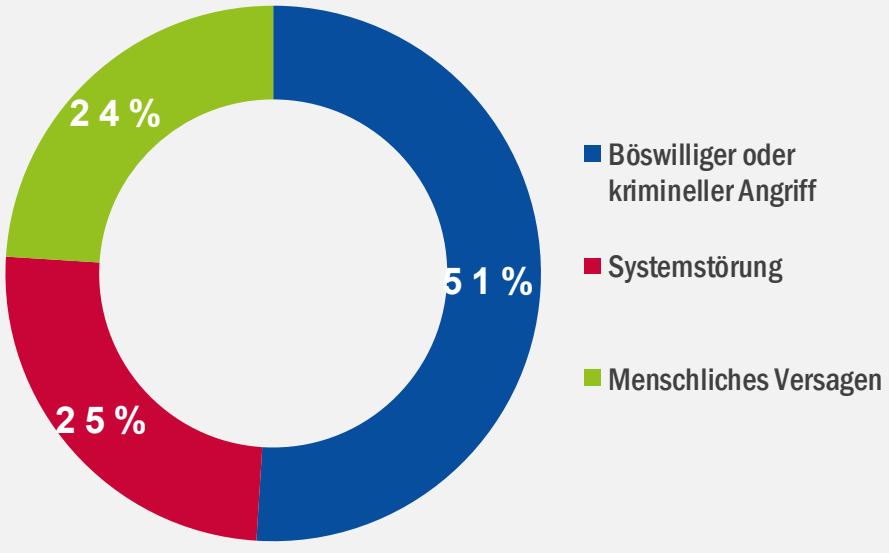
Weitere Informationen

Vorfälle

Hauptvorfälle Datenlecks

- Im Januar 2019 fand der unabhängige Forscher Troy Hunt im **Cloud-Speicherdienst MEGA** die E-Mail-Adressen und Passwörter von 773 Millionen Benutzern. Hunt nannte diesen verletzten Datensatz „Sammlung Nr. 1" und benachrichtigte den Dienst „Wurde ich Pwned?", damit die Kontoinhaber benachrichtigt werden konnten, ihre Anmeldepasswörter für den Zugriff auf die MEGA-Plattform zu ändern.[12] Im selben Monat gaben betrügerische Personen personenbezogene Daten, private Kommunikation und Finanzinformationen von Hunderten **deutscher Politiker** bekannt, mit Zielen, die jede politische Partei außer der rechtsextremen AfD vergegenwärtigen.[6]
- Im Februar 2019 wurden mehr als 61 Millionen Konten von 16 Websites gelöscht und im Dark Web zum Verkauf angeboten. Websitebesitzer von Whitepages, Dubsmash, Armor Games, 500px und ShareThis sahen, dass die gestohlenen Daten ihrer Benutzer für weniger als 20.000 USD (ca. 17.000 EUR) in Bitcoin verkauft wurden.[13]
- Im März 2019 stellten Hunderte Millionen **Facebook- und Instagram**-Nutzer fest, dass ihre Anmeldedaten durch das schlechte Passwortspeichermanagement des Social-Media-Unternehmens offengelegt wurden.[14]
- Im April 2019 wurden in Indien 12,5 Millionen Krankenakten schwangerer Frauen aufgrund eines undichten Regierungsservers einer Gesundheitsbehörde offengelegt. Die offengelegten medizinischen Informationen standen im Zusammenhang mit dem Gesetz über vorgeburtliche Diagnosetechniken, einem indischen Gesetz, das die vorgeburtliche Geschlechtsbestimmung verbot, um zu verhindern, dass indische Familien ungeborene Mädchen abtreiben und das Geschlechterverhältnis gegenüber Jungen verzerren.[15]

- Im Mai 2019 erlitt **DoorDash**, ein Lebensmittel-Lieferservice, eine Datenschutzverletzung, von der fast 5 Millionen Benutzer betroffen waren. Die anschließende Untersuchung ergab, dass auf Informationen wie Namen, E-Mail-Adressen, Lieferadressen, Bestellverlauf, Telefonnummern und Passwörter zugegriffen wurde. Das Unternehmen gab an, dass auch auf die letzten vier Ziffern der Kreditkarten und Bankkontonummern einiger Verbraucher zugegriffen wurde.[16]
- Im Juni 2019 begann die **American Medical Collection Agency (AMCA)**, Kunden über einen Systemhack zu informieren, der gegen die Abrechnungs- und medizinischen Daten einiger ihrer Kunden verstieß, darunter 11,9 Millionen Datensätze über **Quest Diagnostics**, eine der größten Blutuntersuchungsunternehmen in den Vereinigten Staaten.
- Laut einer kürzlich eingereichten 8K-Meldung der Securities and Exchange Commission hatte ein Hacker zwischen dem 1. August 2018 und dem 30. März 2019 fast acht Monate lang Zugang zum AMCA-System erhalten.[17]



Ursachen für die Offenlegung von Informationen. Quelle: Ponemon, IBM Security[22]

Vorfälle

Hauptvorfälle Datenlecks

- Im Juli 2019 erlitt das Finanzunternehmen **Capital One** einen Informationsverlust, der 100 Millionen Kreditkartenanträge, 140.000 Sozialversicherungsnummern und 80.000 Bankkontonummern betraf. Capital One berichtete, dass keine Kreditkartenkontonummern oder Anmeldedaten offengelegt wurden. Der Verstoß enthüllte jedoch Namen, Adressen, Postleitzahlen, Telefonnummern, E-Mail-Adressen und Geburtsdaten.[18]
- Im August 2019 wurden 160 Millionen Datensätze von **MoviePass** unverschlüsselt gelassen. Da die Datenbank des Unternehmens nicht durch ein Passwort geschützt war, wurden die Kreditkartennummern und andere Details der Kunden offengelegt. Die Datenbank blieb mehrere Tage online.[19] In der Zwischenzeit wurden durch ein massives Leck 27,8 Millionen biometrische Personalakten der **British Metropolitan Police, von Banken und Verteidigungsunternehmen** freigelegt. Die Datenbank wurde von Suprema verwaltet, einem Unternehmen, das mit der britischen Polizei zusammenarbeitet.[20,21]
- Im September 2019 wurden mehr als 218 Millionen **„Words with Friends"** -Spielerkonten gehackt. Die Benutzerdatenbank enthielt Daten von Android- und iOS-Spielern, die das Spiel vor dem 2. September installiert hatten. Das Hacker-Team „Gnostic Players" hat auf Informationen wie Spielernamen, E-Mail-Adressen, Login-Identitäten und mehr zugegriffen.[23]
- Im Oktober 2019 hinterließ Adobe 7,5 Millionen Creative Cloud-Kundendatensätze in einer unsicheren Datenbank. Der Informationsverlust umfasste die E-Mail-Adressen und den Zahlungsstatus der Benutzer.[24]
- Im November 2019 gewährte Facebook etwa 100 App-Entwicklern unberechtigten Zugriff auf die Profildaten seiner 70.000 Kunden. Einer von ihnen hat die personenbezogenen Daten gestohlen und sie später betrügerisch verwendet.[25]

- Im Dezember 2019 wurde ein **niederländischer Politiker** mit drei Jahren Gefängnis konfrontiert, weil er 100 iCloud-Konten von Frauen gehackt und Nacktbilder offengelegt hatte. Es wurde festgestellt, dass der Politiker die persönlichen iCloud-Konten der Frauen mit Anmeldedaten gehackt hat, die bei früheren Verstößen gegen die öffentliche Datenbank festgestellt wurden.[26] Im selben Monat wurden die Details von über 10,7 Millionen Resortgästen von **Metro-Goldwyn-Mayer (MGM)** bei einem Hacking-Forum bekannt gegeben. Zu den durchgesickerten Informationen gehörten der vollständige Name des Kunden, Privatadressen, Telefonnummern, E-Mail-Adressen und Geburtsdaten.[27]

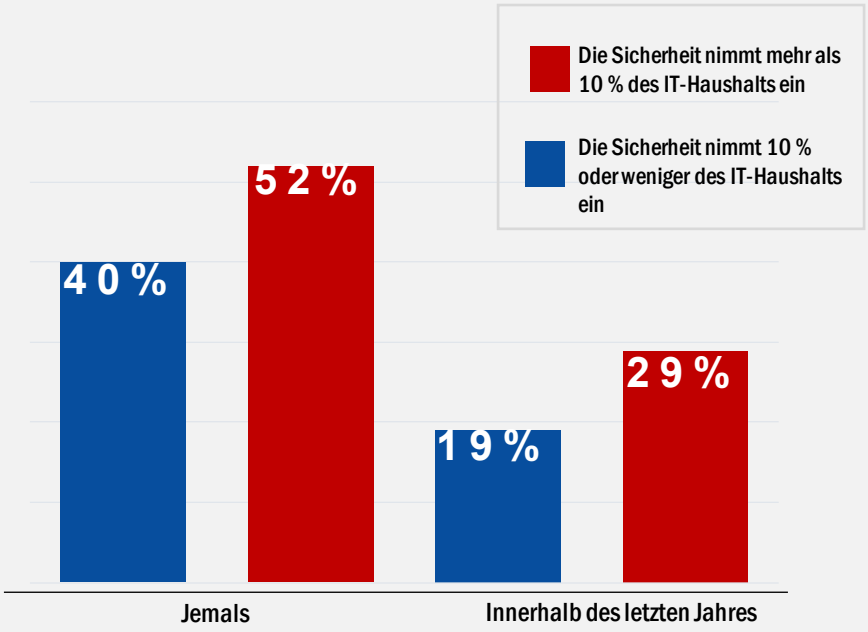


Abbildung 1: Häufigkeit von Vorfällen nach ausgegebenem Sicherheitsaufwand. Quelle: CNET[14]

Angriffsvektoren

_Wie

Der primäre Angriffsvektor bei Informationslecks sind Insider. Dieser Begriff wird verwendet, um eine Person zu beschreiben, die daran interessiert ist, wichtige Insiderinformationen im Auftrag eines Dritten zu „filtern“. Andere häufige Angriffsmethoden, die von dieser Bedrohung verwendet werden, sind Fehlkonfigurationen, Schwachstellen und menschliche Fehler.

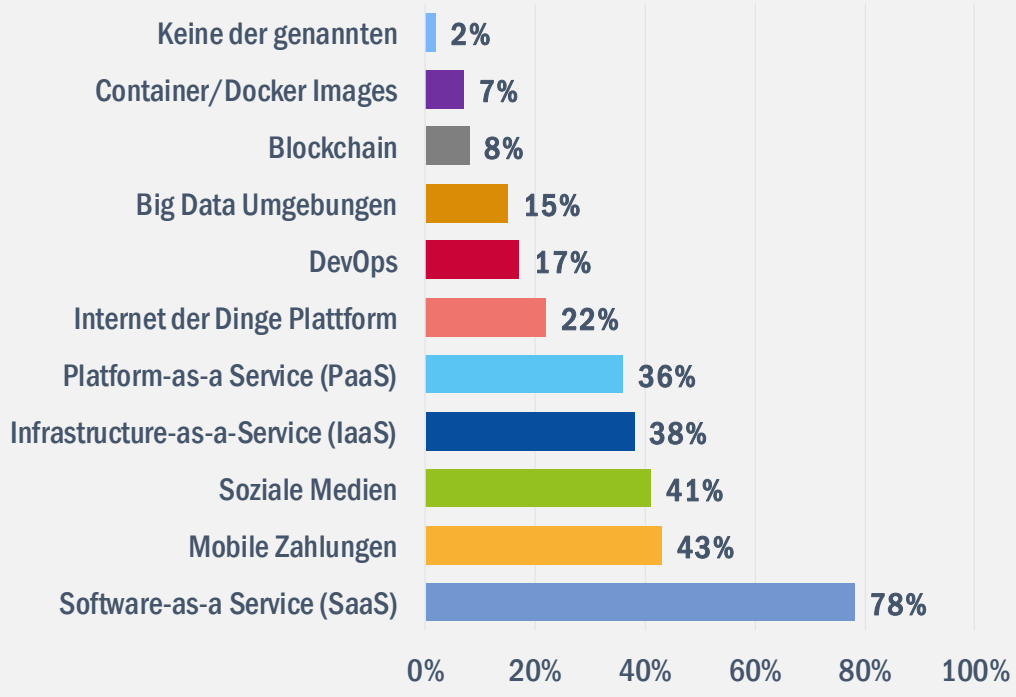


Abbildung 2: Arten von gespeicherten sensiblen oder regulierten Daten. Quelle: Thales[40]

„Eine Datenschutzverletzung führt häufig zu einem Informationsverlust, der eine der größten Cyber-Bedrohungen darstellt und eine Vielzahl kompromittierter Informationen abdeckt. “

In ETL 2020

Minderung

Vorgeschlagene Maßnahmen

- Anonymisieren, pseudonymisieren, minimieren und verschlüsseln Sie Daten gemäß den Bestimmungen der EU-DSGVO, des California Consumer Privacy Act (CCPA) und des mehrstufigen chinesischen Schutzes der Informationssicherheit (MLPS 2.0).[28,29,30,31] Überprüfen Sie immer die Regulierungsverpflichtungen für Gegenunternehmen, die nicht unter bilaterale oder multilaterale Initiativen fallen.[32,33,34]
- Speichern Sie Daten nur auf sicheren IT-Ressourcen.[35]
- Beschränken Sie die Benutzerzugriffsrechte nach dem Need-to-know-Prinzip.[35,36] Widerrufen Sie die Zugriffsrechte aller Personen, die keine Mitarbeiter sind.[35]
- Informieren und schulen Sie das Personal Ihrer Organisation regelmäßig.[35,37]
- Verwenden Sie Technologie-Tools, um mögliche Datenlecks zu vermeiden, z. B. Schwachstellen-Scans, Malware-Scans und DLP-Tools (Data Loss Prevention). Stellen Sie Daten und tragbare System- und Geräteverschlüsselung bereit und sichern Sie Gateways.[36,38]
- Ein Business Continuity Plan (BCP) ist für die Behandlung von Datenverletzungen von entscheidender Bedeutung. In diesem Plan werden die Art der gespeicherten Daten und ihr Speicherort sowie die potenziellen Verbindlichkeiten bei der Implementierung von Datensicherheits- und Wiederherstellungsmaßnahmen beschrieben. Ein BCP beinhaltet eine effektive Reaktion auf Vorfälle, die darauf abzielt, die durch einen solchen Vorfall verursachten Schäden zu beheben, zu verwalten und zu beheben.[39]


„In vielen Fällen sind Unternehmen oder Organisationen aufgrund der Komplexität des Angriffs oder der mangelnden Sichtbarkeit und Klassifizierung in ihrem Informationssystem nicht über eine Datenschutzverletzung in ihrer Umgebung informiert.“
In ETL 2020

Literaturangaben

1. "What is a data breach and what do we have to do in case of a data breach?" Europäische Kommission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_de

2. "The humn factor of cyber security." CSO https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html

3. Howard Poston. "Common causes of large breaches (Q1 2019)." 1. Mai, 2019. INFOSEC Institute. https://resources.infosecinstitute.com/common-causes-of-large-breaches/#gref

4. J. Clement. "Average cost of data breaches worldwide from 2014 to 2019." 13. August, 2019. Statista. https://www.statista.com/statistics/987474/global-average-cost-data-breach/

5. "2019 Data Breach Investigations Report." 2019 Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

6 "Cyber Threatscape Report." 2019. iDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

7. "Cybercrime will cost businesses over $2 trillion by 2019." 12. Mai, 2015. Juniper Research https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

8. "How much would a data breach cost your business?." 2019 IBM https://www.ibm.com/security/data-breach

9. G. Dautovic. "Top 25 Financial Data Breach Statistics for 2020." 11. März, 2020. Fortunly. https://fortunly.com/statistics/data-breach-statistics#gref

10. Davey Winder."Data Breaches Expose 4.1 BIllion Records In First Six Months of 2019." 20. August, 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#40479be4bd54

11. "Cost of a Data Breach Report." 2019 Ponemon Institute – IBM. https://databreachcalculator.mybluemix.net/executive-summary/

12. Troy Hunt. "The 773 Million Record "Collection #1." Data Breach" 17. Januar, 2019. Troy Hunt. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

13. Lewis Morgan. "List of data breaches and cyber attacks in February 2019 – 873,919, 635 records leaked." 26. Februar, 2019 IT Governance. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2019-692853046-records-leaked

14. Rae Hodge. "2019 Data Breach Hall of Shame: These were the biggest data breaches of the year." 27. Dezember, 2019. CNET. https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

15. Catalin Cimpanu. "Indian govt agency left details of millions of pregnant women exposed online." 1. April, 2019. ZDNet. https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

16. Shelby Brown. "DoorDash data breach affected 4.9M customers, drivers, merchants." 26. September, 2019. CNET. https://www.cnet.com/news/doordash-data-breach-affected-4-9-million-customers-workers-and-merchants/

17. Jessica Davis. "11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach." 3. Juni, 2019. HealthITSecurity https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach

18. Alfred Ng, Mark Serrels. "Capital One data breach involves 100 million credit card applications." 30. Juli, 2019. CNET. https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/

19. Shelby Brown. "Data breaches timeline: EasyJet cyberattack exposes over 9M people, and more." 19. Mai, 2020 CNET. https://www.cnet.com/how-to/equifax-mgm-resorts-beyond-every-major-security-breach-and-data-hack-update/

20. Josh Taylor. "Major breach found in biometrics system used by banks, UK police and defence firms." 14. August, 2019 The Guardian https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

21. Guy Fawkes. "Report: Data Breach in Biometric Security Platform Affecting Millions of Users." 16. Juni, 2020. vpnMentor. ttps://www.vpnmentor.com/blog/report-biostar2-leak/

22. "Cost of a Data Breach Report." 2019 Ponemon - IBM Security. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

23. Oscar Gonzalez. "Zynga data breach exposed 200 million Words with Friends players." 1. Oktober, 2019. CNET. https://www.cnet.com/news/people-rarely-change-their-passwords-after-a-data-breach-study-says/

24. John E Dunn. "Adobe database exposes 7.5 million Creative Cloud users." 28. Oktober, 2019. Naked Security. https://nakedsecurity.sophos.com/2019/10/28/adobe-database-exposes-7-5-million-creative-cloud-users/

25. "Insider Sold 68K Customer Records to Scammers: Trend Micro." 8. November, 2019. CISOMAG. https://www.cisomag.com/insider-sold-68k-customer-records-to-scammers-trend-micro/

26. Catalin Cimpanu. "Dutch politician faces three years in prison for hacking iCloud accounts and leaking nudes." 3. Dezember, 2019. ZDNet. https://www.zdnet.com/article/dutch-politician-faces-three-years-in-prison-for-hacking-icloud-accounts-and-leaking-nudes/

27. Corinne Reichert. "MGM Resorts confirms data breach of 10.7 million guests." 19. Februar, 2020 https://www.cnet.com/news/mgm-resorts-confirms-data-breach-of-10-million-guest-accounts/

28. „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)." 27. April, 2016. Europäisches Parlament, Rat der Europäischen Union. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

29. "AB-375 Privacy: personal information: businesses, Assembly Bill No. 375, Chapter 55." 29. Juni, 2018. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

30. Shrub Chandrasekaran, Justin Fishman. "China's Cybersecurity Future and its Impact on U.S. Business." 31. Oktober, 2019. Jolt Digest. https://jolt.law.harvard.edu/digest/chinas-cybersecurity-future-and-its-impact-on-u-s-business

31. Reed Smith LLP. "MLPS 2.0: China's enhanced data security multi-level protection scheme and related enforcement updates." 9. Oktober, 2019. Lexology. https://www.lexology.com/library/detail.aspx?g=36c6932b-bf41-4e08-b430-e3bc839a2328

32. "Data protection if there's no Brexit deal." 13. September, 2018. GOV. UK, Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

33. Eduardo Ustaran, "Brexit and data protection: Laying the odds." 21. September, 2018. Privacy Perspectives, iapp. https://iapp.org/news/a/brexit-and-data-protection-laying-the-odds/

34. Ibrahim Hasan. "Data protection and Brexit." 5. September, 2016. Gazette. https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article

35. Eric Dosal. "5 Tips to Prevent Data Leakage at Your Company." 15. März, 2018. Compuquip Cybersecurity.https://www.compuquip.com/blog/5-tips-to-prevent-data-leakage-at-your-company

36. "10 ways to protect sensitive business data." 28. Oktober, 2019. QuoStar. https://www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/

37. "Annual Cybersecurity Report." 2018. Cisco https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

38. "Cybercrime tactics and techniques: Q2 2018." 2018. Malwarebytes Labs

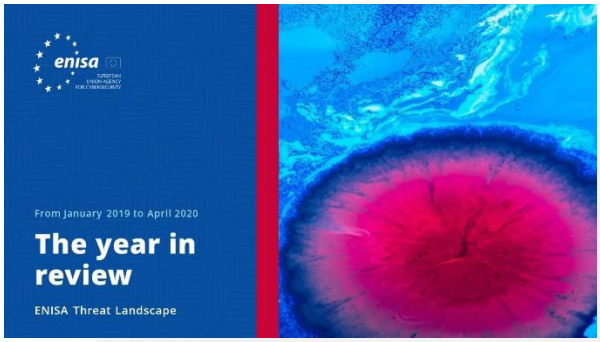
https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf

39. Mona Mangat. "81 Eye-Opening Data Breach Statistics for 2020." 27. Januar, 2020. phoenixNAP. https://phoenixnap.com/blog/data-breach-statistics

40. "2020 Data Threat Report – Global Edition." 2020 Thales Group. https://www.thalesesecurity.com/2020/data-threat-report

41. Oscar Gonzalez. "Zynga data breach exposed 200 million Words with Friends players." 1. Oktober, 2019. C|net.https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/

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**

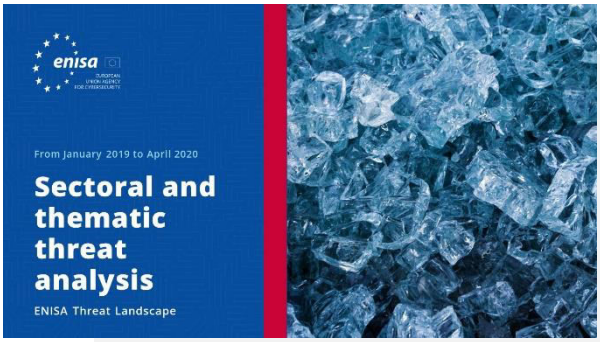
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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