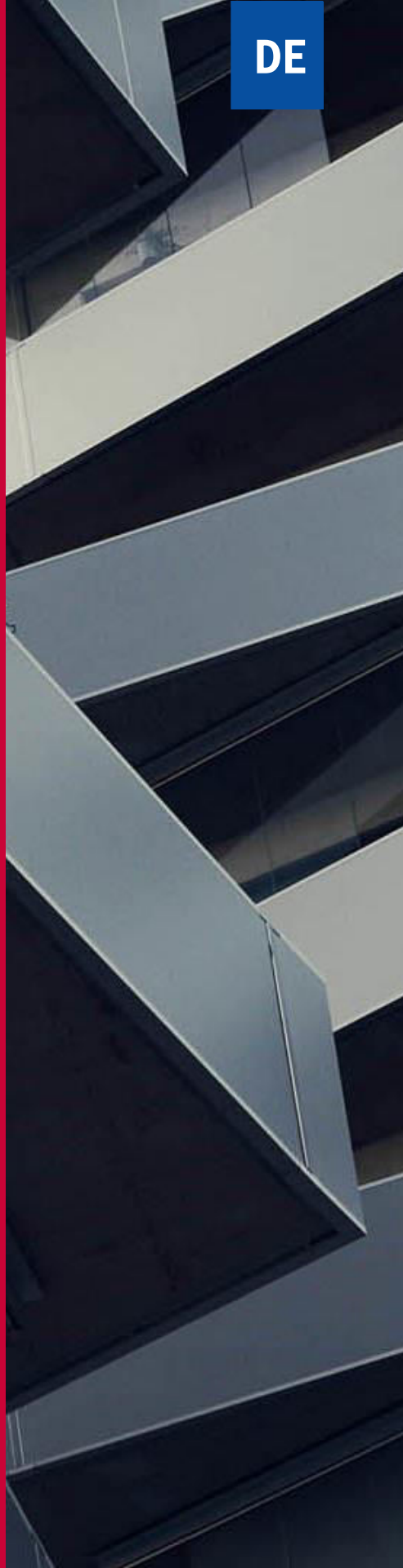
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE



Von Januar 2019 bis April 2020

Datenschutz verletzung

ENISA Threat Landscape

Überblick

Eine Datenschutzverletzung ist eine Art von Cybersicherheitsvorfall, bei dem auf Informationen (oder Teile eines Informationssystems) ohne die richtige Genehmigung zugegriffen wird, normalerweise mit böswilliger Absicht, was zum potenziellen Verlust oder Missbrauch dieser Informationen führt. Dazu gehört auch „menschliches Versagen", das häufig bei der Konfiguration und Bereitstellung bestimmter Dienste und Systeme auftritt und zu einer unbeabsichtigten Offenlegung von Daten führen kann.[1]

In vielen Fällen sind Unternehmen oder Organisationen aufgrund der Komplexität des Angriffs und manchmal der mangelnden Sichtbarkeit und Klassifizierung in ihrem Informationssystem nicht über eine Datenschutzverletzung in ihrer Umgebung informiert.[2] Basierend auf Untersuchungen dauert die Identifizierung in einer Organisation ungefähr 206 Tage.[3] Die Zeit zum Erhalten, Korrigieren und Wiederherstellen der Daten bedeutet daher, dass die Rückkehr zur Normalität länger dauert.

Trotz aller damit verbundenen Risiken speichern Unternehmen mithilfe von Cloud-Speicherinfrastrukturen und komplexen lokalen Umgebungen noch mehr Daten[4]. Diese Umgebungen sind nach und nach neuen und unterschiedlichen Risiken ausgesetzt, die proportional zur Empfindlichkeit der gespeicherten Informationen sind. Kein Wunder daher, dass die Anzahl der Datenschutzverletzungen in den Jahren 2019 und 2020 gestiegen ist. Neue Erkenntnisse deuten auch darauf hin, dass die Auswirkungen nicht ausschließlich zu spüren sind, wenn ein Datenverstoß festgestellt wird. Die finanziellen Auswirkungen können nach dem ersten Vorfall länger als zwei Jahre bestehen bleiben.

Erkenntnisse

54 %_Zunahme der Anzahl der Verstöße bis Mitte 2019 im Vergleich zu 2018.

71 %_ der Datenschutzverletzungen waren finanziell motiviert. Fast 25 % hatten langfristige strategische Ziele (Nationalstaat/Spionage).[5]

32 %_der Datenschutzverletzungen beinhalten Phishing-Aktivitäten gemäß IOCTA 2019.[6] Ein Bericht legt nahe, dass Phishing ganz oben auf der Liste der Hauptverursacher von Datenschutzverletzungen steht. In dem Bericht wird auch erwähnt, dass E-Mail die Hauptübermittlungsmethode für Malware (94 %) in einer Kette von Ereignissen ist, die zu einer Datenschutzverletzung führen.[3]

52 %_der Datenschutzverletzungen beinhalten Hacking.[5] Andere angewandte Taktiken sind soziale Angriffe (33 %), Malware (28 %) und Fehler oder Irrtümer (21 %). Seit 2016 ist Hacking die Hauptursache für Datenschutzverletzungen im Gesundheitswesen. Im Jahr 2019 wurden fast 59 % der gemeldeten Verstöße durch Hacking verursacht.[7]

70 %_ der Datenschutzverletzungen beziehen sich auf offen gelegte E-Mails. Obwohl Benutzername/E-Mail und Passwörter (also Anmeldedaten) im Gegensatz zu personenbezogenen Daten (z. B. Geburtsdatum) leicht geändert werden können, liegt der Schwerpunkt bei Datenschutzverletzungen hauptsächlich auf diesen.[8]

55 %_der Befragten einer Eurobarometer-Umfrage gaben an, dass sie besorgt seien, dass Kriminelle und Betrüger auf ihre Daten zugreifen.

Zeitplan

2019

_ Januar

MEGA Cloud (NZ) erlitt eine Datenschutzverletzung, die 770 Millionen E-Mails und 21 Millionen Passwörter enthüllte.[9]

_ Februar

Der Verkäufer rühmt sich, 620 Millionen Konten von 16 gehackten Websites gestohlen zu haben, die jetzt im Dark Web zum Verkauf stehen.[10]

_ März

12,5 Millionen Krankenakten von schwangeren Frauen des Gesundheitszentrums der indischen Regierung (IN) aus dem Jahr 2014 wurden der Öffentlichkeit zugänglich gemacht.[11]

_ August

Schwerwiegender Verstoß gegen das von Banken, (britischen) Polizei- und Verteidigungsunternehmen verwendete Biometrie-System.[16]

_ September

Mastercard (BE) wurde Opfer einer Datenschutzverletzung, von der ca. 90.000 Kunden in Europa betroffen waren.[17]

_ Oktober

Die Kontoinformationen von über 7,5 Millionen Benutzern aus Adobe (USA) wurden aufgrund einer ungeschützten Online-Datenbank offengelegt.[18]

_ November

UniCredit (IT) Opfer einer Datenschutzverletzung, bei der 3 Millionen Datensätze verloren gegangen sind.[19]

_ Dezember

Der Anbieter von Smart-Kameras, Wyze (USA), erlitt Ende Dezember zwei Sicherheitsverletzungen, als Datenbanken mehr als zwei Wochen lang freigelegt wurden.[20]

2020

_ Januar

250 Millionen Kundendienst- und Supportdatensätze von Microsoft (USA), die bis ins Jahr 2005 zurückreichen, wurden veruntreut.[21]

_ April

Facebook (USA) meldete eine Datenschutzverletzung, die 540 Millionen Benutzerdatensätze auf exponierten Servern enthüllte.[12]

_ Mai

Bei First American Financial Corp. (USA) sind Hunderte Millionen Rechtstitelversicherungsunterlagen durchgesickert.[13]

_ Juli

Personenbezogene Daten von Kreditkartenkunden von Capital One (USA) wurden verletzt.[15]

_ Juni

100 Millionen Datensätze wurden durch den unbefugten Zugriff von Evite-Kunden auf einen Datenspeicher verfügbar gemacht.[14]

_ Februar

Ein ungeschützter Google (USA) Cloud-Server mit den personenbezogenen Daten von 200 Millionen US-Einwohnern.[22]

_ März

Das Unternehmen für biometrische Lösungen Antheus Tecnologia (BR) litt unter einem Datenleck.[23]

_ April

Hackers erhielten die Anmeldedaten von zwei Mitarbeitern von Marriott (USA) und brachen im Januar 2020 in das System ein.[24]

Entwicklungen

_Die Kosten einer Datenschutzverletzung für Unternehmen erstrecken sich über viele Jahre

Sicherheitsforscher stellten fest, dass ein Drittel der Kosten im Zusammenhang mit einer Datenschutzverletzung mehr als ein Jahr nach dem Vorfall anfällt. Genauer gesagt fallen rund 22 % dieser Kosten im zweiten Jahr an, während 11 % der Kosten erst mehr als zwei Jahre nach dem ersten Vorfall anfallen. Diese Raten waren für stark regulierte Organisationen wie Finanzdienstleistungen und Gesundheitswesen im Vergleich zu anderen Sektoren höher.[3]
Die Akzeptanz von Cloud- oder Multi-Cloud-Umgebungen nimmt rapide zu, ähnlich wie die Datenmenge, die in diesen Umgebungen gespeichert und verarbeitet wird.

_Kleine Fehler können zu großen Verstößen führen

Das Sichern der Cloud-Umgebung ohne Verlust der Flexibilität für Infrastruktur und Ressourcen kann problematisch sein. Eine einzelne Fehlkonfiguration kann dazu führen, dass die gesamte vertrauliche Datenbank verfügbar gemacht wird. Ein Sicherheitsforscher ist der Ansicht, dass die meisten Datenschutzverletzungen in der Cloud auf Fehlkonfigurationen zurückzuführen sind und größtenteils unbeabsichtigt sind. Netflix, Ford und TD Bank sind nur einige Beispiele unter vielen anderen. Aus einer anderen Perspektive kosten Datenschutzverletzungen aufgrund böswilliger Versuche zwar immer noch mehr, aber Verstöße aufgrund von Systemfehlern oder menschlichen Fehlern verursachen im Durchschnitt immer noch erhebliche Kosten in Höhe von durchschnittlich 3,24 Millionen USD (ca. 2,74 Millionen EUR).[3]

Datenschutzverletzungen kosten Kleinunternehmen mehr

Die Kosten für Datenschutzverletzungen bei Unternehmen oder großen Organisationen mit mehr als 25.000 Mitarbeitern betragen 204 USD (ca. 173 EUR) pro Mitarbeiter. Der Gesamtbetrag wird auf rund 5,11 Millionen USD (ca. 4,33 Millionen EUR) geschätzt. Für kleine Unternehmen (500-1.000 Mitarbeiter) liegen die durchschnittlichen Kosten dagegen bei 3.533 USD (ca. 3.000 EUR) pro Mitarbeiter. Dies entspricht Gesamtkosten von 2,65 Millionen USD (ca. 2,24 Millionen EUR) für kleine Unternehmen.[3]

Finanzieller Gewinn ist das Hauptmotiv

Es ist bekannt, dass böswillige-/Bedrohungsakteure bei Datenschutzverletzungen die Fäden in der Hand haben (wobei zu berücksichtigen ist, dass sie manchmal das Ergebnis eines Fehlers sein können). In diesem Sinne sind externe Bedrohungsakteure die Hauptursache für Datenschutzverletzungen, und dies könnte Aktivitäten wie Botnetz umfassen[4]. In diesem Zusammenhang wurde der finanzielle Gewinn wiederholt als Hauptmotiv für Datenschutzverletzungen identifiziert, die durch diese Gruppen von Akteuren verursacht wurden. Spionage[4] war ebenfalls eines der Hauptmotive für Datenschutzverletzungen, stand jedoch nicht so weit oben auf der Liste wie der persönliche oder finanzielle Vorteil. Dieser Trend stimmte nahezu mit den Ergebnissen von 2010-2011 überein.[5]

Entwicklungen

Quantencomputer- und Datensicherheitsbedenken

Kryptografieanforderungen spielen im Zeitalter des Quantencomputers eine wichtige Rolle und heben kritische Sicherheitsprobleme hervor. 72 % der Unternehmen glauben, dass sich Quantencomputer (in den nächsten 5 Jahren) strategisch auf ihre kryptobezogenen Operationen auswirken werden. Laut den Ergebnissen der Umfrage sind 92 % der Befragten besorgt über die Offenlegung sensibler Daten durch den Einsatz dieser Technologie in der Computerbranche. Die wichtigsten Strategien, die die Befragten zur Behebung dieser Probleme vorschlugen, waren die Änderung der Sicherheitsarchitektur und die Bereitstellung der wichtigsten Verwaltungsinfrastrukturen.[26]

Gesundheitswesen - ein konsequenter Fokus für böswillige Akteure

Das Gesundheitswesen ist weiterhin eines der attraktivsten Ziele für Cyberkriminelle, die Ransomware und Phishing techniken einsetzten. Die Eindämmung und Wiederherstellung kostete solche Unternehmen Millionen von Euro. Im Jahr 2019 meldeten 400 Gesundheitsunternehmen eine Datenschutzverletzung in Patientenakten. Dies war für Gesundheitsunternehmen ein neuer Rekord.[7]

Multi-Cloud - die neue Herausforderung für die Datensicherheit

Eine von einem Sicherheitsforscher durchgeführte Umfrage ergab, dass 9 von 10 Unternehmen daran denken, Cloud-Umgebungen zu verwenden oder dass sie diese bereits verwenden. Ungefähr 44 % der Befragten glauben auch, dass diese Umgebungen eine Herausforderung für die Implementierung angemessener Datensicherheitsmaßnahmen darstellen.[25]

Art der exponierten Daten (%)

Art der Daten	2019	2018	2017
E-Mail	70	44	32
Passwort	64	39	27
Name	23	37	41
Verschiedenes	18	19	15
Sozialversicherungsnummer	11	22	27
Kreditkarte	11	16	19
Anschrift	11	22	30
Konto	10	7	4
Unbekannt	8	13	18
Geburtsdatum	8	13	12
Medizinisch	5	9	7
Finanziell	5	13	19

Tabelle 1 - Quelle: Cyber Risk Analytics[8]

Entwicklungen

_Kontinuierliche Abnahme der Verstöße gegen kartenbasierte Verstöße

Laut einem Sicherheitsbericht wurde im Jahr 2019 ein Rückgang der Verstöße gegen Verkaufsstellen durch Karten-Skimming (mit Vorlage einer Karte) festgestellt. Dies stellt eine Verlagerung vom traditionellen Geldautomaten-Skimming und Kartenzahlungen zu Webanwendungen im Einzelhandel dar. Obwohl die Anzahl der Vorfälle in diesem Bereich abgenommen hat, lässt sich daraus nicht genau schließen, ob die Anzahl der Datenschutzverletzungen abnimmt oder eher eine Verschiebung des Vektors stattfindet. Der Rückgang könnte jedoch mit einer umfassenderen Implementierung von Chip- und Pin-fähigen Karten/Terminals (auch als EMV bekannt) zusammenhängen.[6]

_Was ist in naher Zukunft zu erwarten?

Laut einem Sicherheitsforscher sollten Gesundheitsorganisationen auf einen Anstieg der Anzahl von Datenschutzverletzungen um 10 bis 15% vorbereitet sein, bei denen ihre Dienstleister das Hauptziel sein werden[7]. Basierend auf den Ergebnissen der ersten sechs Monate des Jahres 2019 wird allgemein erwartet, dass die Anzahl der Datenschutzverletzungen trotz des Bewusstseins der Führungskräfte und der Anstrengungen, die viele Unternehmen zur Sicherung ihrer Daten unternehmen, alarmierend zunehmen.[8]

_Datenschutzverletzungen nach Sektor und Organisationsgröße

Vorfälle	Verstöße	Klein	Groß	Unbekannt
Unterbringung	61	34	7	20
Verwaltung	17	6	6	5
Landwirtschaft	2	2	0	0
Bauwesen	11	7	3	1
Bildung	99	14	8	77
Unterhaltung	10	2	3	5
Finanzen	207	26	19	162
Gesundheitswesen	304	29	25	250
Informationswesen	155	20	18	117
Management	2	1	1	0
Produktion	87	10	22	55
Bergbau	15	2	5	8
Sonstige Dienstleistungen	54	6	5	43
Gewerblich	157	34	10	113
Öffentlich	**330**	**17**	**83**	**230**
Immobilien	14	6	3	5
Einzelhandel	139	46	19	74
Handel	16	4	8	4
Transport	36	3	9	24
Versorgungssektor	8	2	0	6
Unbekannt	289	0	109	180
Gesamt	2,013	271	363	1.379

Tabelle 2 - Quelle: Verizon DBIR, 2019[5]

Angriffsvektoren

- **E-MAIL/PHISHING.** Das Nachahmen eines Drittanbieters oder eines Partners per E-Mail ist für böswillige Akteure ein einfacher Gewinn. Es ist bekannt, dass dies der Vektor ist, der von Cyberkriminellen am häufigsten verwendet wird, um ihre Opfer anzugreifen, und die Ursache für die meisten Datenschutzverletzungen (fast 40 % der Verstöße im Gesundheitswesen).[7,]
- **CLOUD/WEB-ANWENDUNGEN.** Dies spiegelt Webanwendungen wider, die als Vektor für Versuche böswilliger Akteure verwendet werden, Daten oder kritische Vorgänge zu veruntreuen. Der Diebstahl von Anmeldedaten für den Zugriff auf webbasierte E-Mail-Portale ist ein hervorragendes Beispiel. Das Ausnutzen von Schwachstellen in Anwendungsservern, um informationsstehelende Malware oder Formjacking-Angriffe einzuschleusen, sind weitere Beispiele in diesem Vektor.[↗]
- **INSIDER-BEDROHUNG.** Dies bezieht sich hauptsächlich auf nicht autorisierte oder böswillige Versuche, Ressourcen zu verwenden. Es sollte beachtet werden, dass bei der Analyse und Meldung Fehlkonfigurationen oder Fehler (menschliches Versagen) durch interne Teams im Allgemeinen auch als „Insider“ bezeichnet werden können. Obwohl die meisten Datenschutzverletzungen durch externe böswillige Akteure durchgeführt werden, spielen Insider mit oder ohne privilegierten Zugriff immer noch eine Schlüsselrolle bei Datenschutzverletzungen.[5]

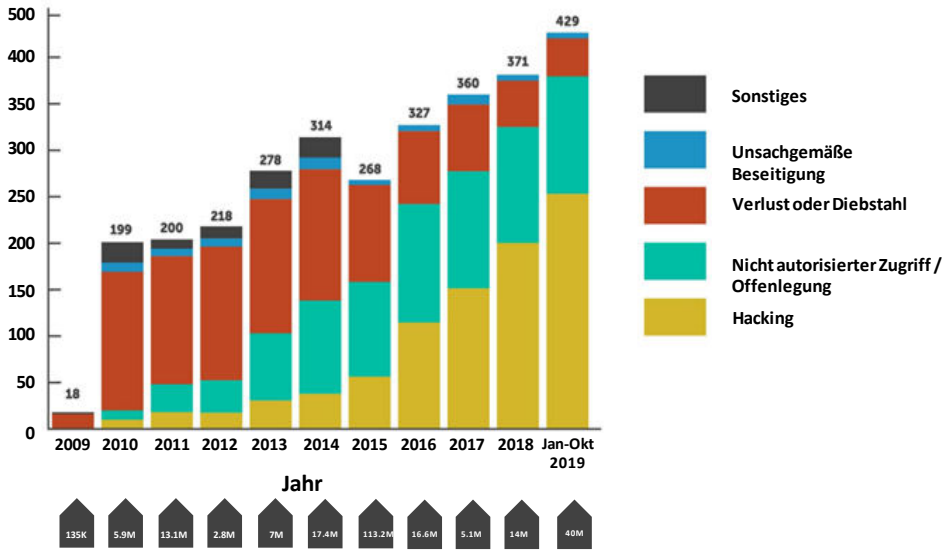
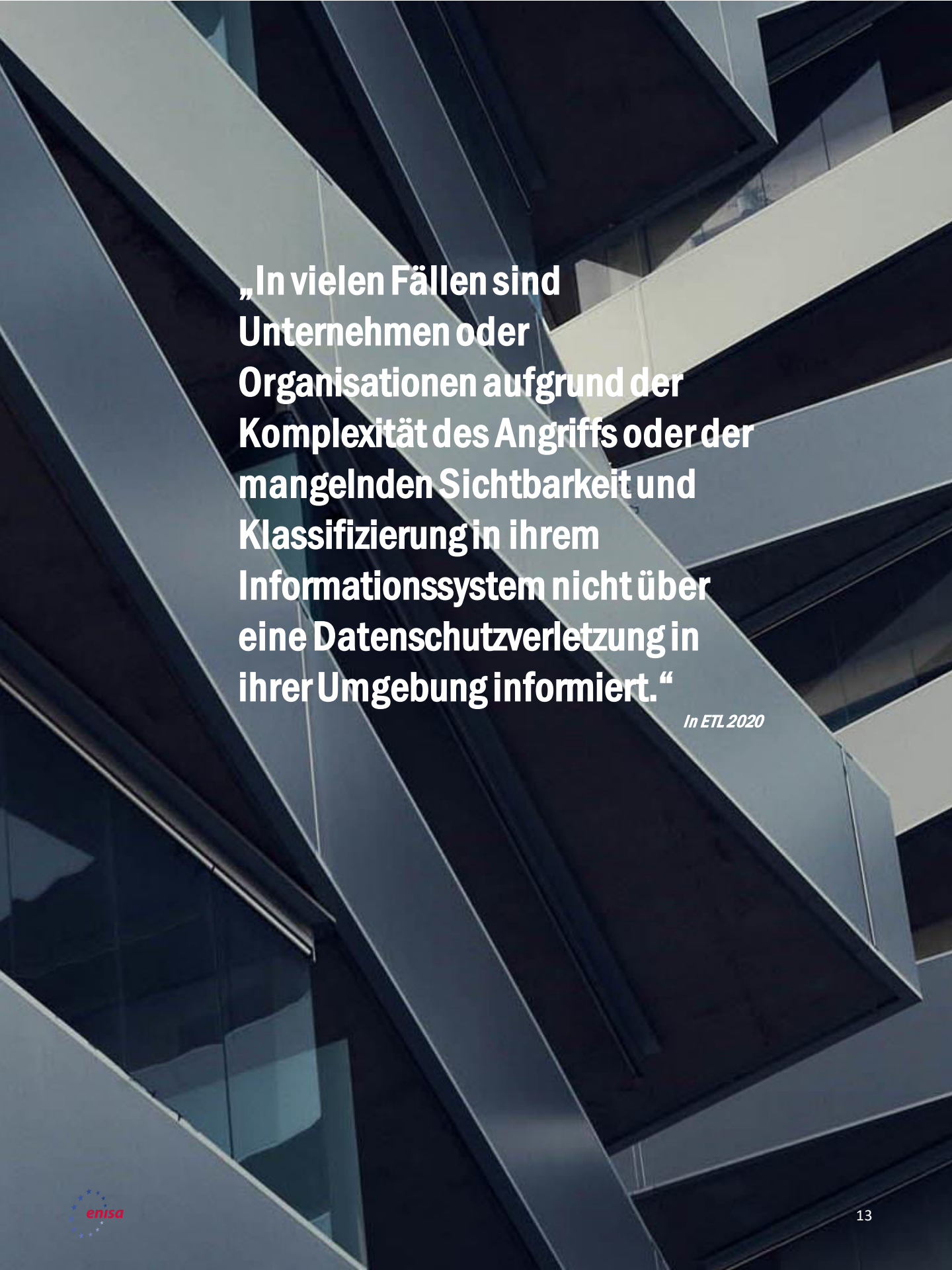


Abbildung 1: An einem Verstoß beteiligte Instanzen. Quelle: Horizon[7]



„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

Minderung

Vorgeschlagene Maßnahmen

- Datenschutzverletzungen sind im Allgemeinen das Ergebnis anderer Bedrohungen, und die Schadensbegrenzung überschneidet sich mit anderen in diesem Bericht erörterten.
- Gegebenenfalls Investition in hybride Datensicherheitsinstrumente, die sich darauf konzentrieren, in einem Modell mit gemeinsamer Verantwortung für Cloud-basierte Umgebungen zu arbeiten.[26]
- Entwicklung und Pflege eines Plans zur Sensibilisierung für Cybersicherheit. Bereitstellung von Schulungs- und Simulationsszenarien zur Identifizierung von Social Engineering- und Phishing-Kampagnen für Mitarbeiter.[7]
- Richten Sie ein Incident-Response-Team ein und pflegen Sie es. Bewerten Sie Incident-Response-Pläne regelmäßig.[3]
- Identifizieren und klassifizieren Sie vertrauliche/personenbezogene Daten und wenden Sie Maßnahmen zur Verschlüsselung derselben während der Übertragung und in der Ablage an.[3] Mit anderen Worten: Setzen Sie Funktionen zur Verhinderung von Datenverlust ein.
- Steigern Sie die Investitionen in Erkennungs- und Alarmierungswerkzeuge sowie in die Fähigkeit, Datenschutzverletzungen einzudämmen und darauf zu reagieren.
- Entwickeln und pflegen Sie strenge Richtlinien, die sichere Passwörter (Passwortverwaltung) und die Verwendung der Multi-Faktor-Authentifizierung erzwingen.
- Erwägen Sie die Verwendung von Modellen, die den Ansatz der „geringsten Berechtigung“ verwenden, um Sicherheit sowohl für lokale als auch für externe Ressourcen zu bieten (d. h. Zero-Trust-Modelle).
- Investieren und erstellen Sie Richtlinien und Pläne für die Zusammenarbeit mit Governance-, Risikomanagement- und Compliance-Teams.[26]


" Im nächsten Jahrzehnt werden Cybersicherheitsrisiken aufgrund der zunehmenden Komplexität der Bedrohungslandschaft, des kontroversen Ökosystems und der Erweiterung der Angriffsfläche schwieriger zu bewerten und zu interpretieren sein."
In ETL 2020

Literaturangaben

1. "What is data breach?" Norton. https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

2. "What is data breach?" Malwarebytes. https://www.malwarebytes.com/data-breach/

3. "Cost of Data Breach Report." 2019. IBM Security, Ponemon Institute. https://www.ibm.com/security/data-breach

4. Dhritimaan Shukla, Kush Wadhwa. "Data breach – threat landscape. Unauthorised exposure of an organisation's critical data." PWC India. https://www.pwc.in/consulting/forensic-services/data-breach-threat-landscape.html

5. "Verizon Data Breach Investigations Report." 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

6 Catherine De Bolle. "Internet Organised Crime Threat Assessment (IOCTA)." 2019. European Cyber Crime Centre (EC3), Europol. https://www.europol.europa.eu/iocta-report

7. "2020 Healthcare Cybersecurity Horizon Report." 2020. Fortified Health Security. https://fortifiedhealthsecurity.com/wp-content/uploads/2019/12/Fortified-Health-Security-2020-Horizon-Report.pdf

8. Inga Goddijn. "2019 Midyear QuickView Data Breach Report – Cyber Risk Analytics." August 2019 https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf

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

10. Chris Williams. "620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts." 11. Februar, 2019 The Register. https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/

11. 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/

12. "Losing Face: Two More Cases of Third-Party Facebook App Data Exposure." 3. April, 2019. UpGuard. https://www.upguard.com/breaches/facebook-user-data-leak

13. "First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records." 24. Mai 2019. KrebsonSecurity. https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

14. "Data Incident, Evite." 14. Mai, 2019. Evite. https://www.evite.com/security/update

15. "Information on the Capital One Cyber Incident." 23. September, 2019. CapitalOne. https://www.capitalone.com/facts2019/

16. 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

17. Neil Hodge. "Mastercard reveals data breaches in third-party loyalty program." 27. August, 2019 Compliance Week.

https://www.complianceweek.com/data-privacy/mastercard-reveals-data-breaches-in-third-party-loyalty-program/27614.article

18. Catalin Cimpanu. "Adobe left 7.5 million Creative Cloud user records exposed online." 26. Oktober, 2019. ZDNet. https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/

19. Charlie Osborne. "UniCredit reveals data breach exposing 3 million customer records." 28. Oktober, 2019. ZDNet. https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/

20. Chris Isidore. "Smart camera maker Wyze hit with customer data breach." 30. Dezember, 2019. CNN. https://edition.cnn.com/2019/12/30/tech/wyze-data-breach/index.html

21. Davey Winder. "Microsoft Security Shocker As 250 Million Customer Records Exposed Online." 22. Januar, 2020. Forbes. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#2d3f9dca4d1b

22. Paul Bischoff. "US property and demographic database of 200 million records leaked on the web." 5. März 2020. Comparitech. https://www.comparitech.com/blog/vpn-privacy/200-million-us-database-leaked/

23. Jim Wilson. "Brazil: Millions of Records Leaked, Including Biometric Data." 11. März, 2020. Safety Detectives. https://www.safetydetectives.com/blog/antheus-leak-report/

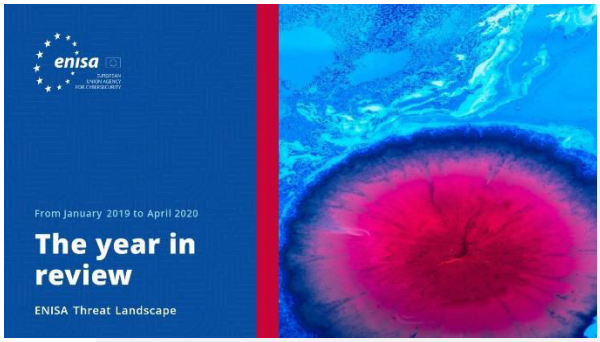
24. Zack Whittaker. "Marriot says 5.2 million guest records were stolen in another data breach." 1. April, 2020. Techrunch. https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/?renderMode=ie11

25. "2019 Thales Data Threat Report – Global Edition" Thales Security, 2019. https://cpl.thalesgroup.com/data-threat-report

26. "2020 Thales Data Threat Report – Global Edition" Thales Security, 2020. https://cpl.thalesgroup.com/data-threat-report

27. Laura Paine. "2019 Verizon DBIR Shows Web Applications and Human Error as Top Sources of Breach." 8. Mai, 2019. Veracode. https://www.veracode.com/blog/security-news/2019-verizon-dbir-shows-web-applications-and-human-error-top-sources-breach

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**

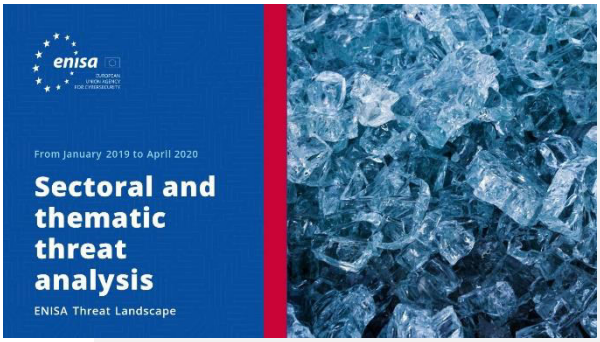
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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

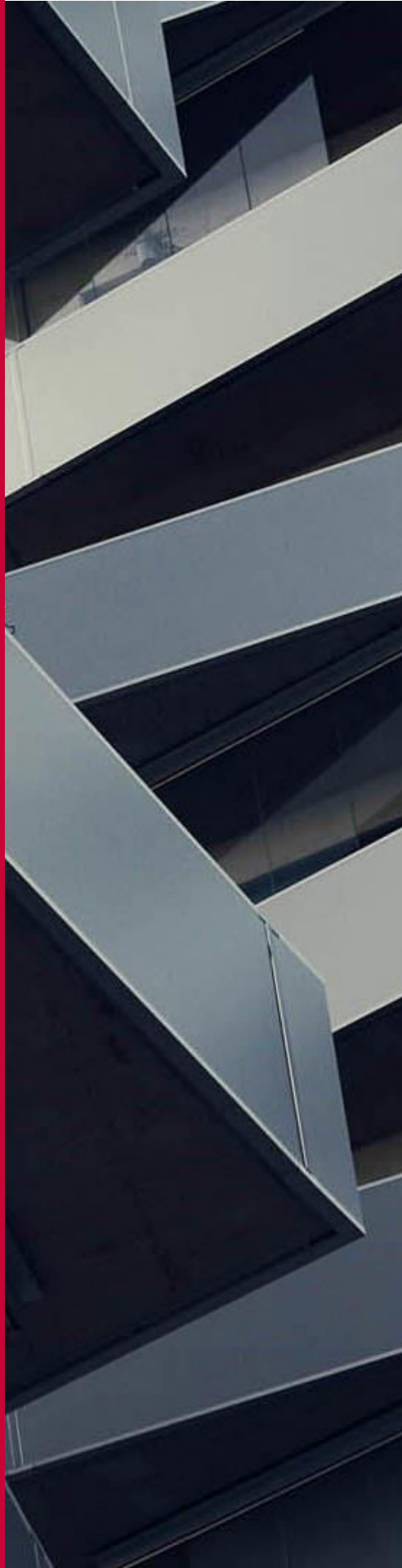
Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung 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