E-BOOK

Cyber-threats.

Die 15 häufigsten Cyberangriffe und wie Sie sich dagegen schützen können.

InterNetX

Inhaltsverzeichnis.

“ Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders.”

– Ronald Reagan, 40. President der USA

Executive Summary.

Prognosen zufolge werden Cyberattacken in 2021 Schäden in Höhe von insgesamt 6 Billionen USD[1] verursachen. Würden wir diese Zahl dem weltweiten BIP gegenüberstellen, dann wäre das die drittgrößte Volkswirtschaft der Welt nach den USA und China.

Alle sollten sich darüber im Klaren sein: **zum Ziel eines Cyberangriffs zu werden, ist nicht mehr eine Frage des "ob", sondern des "wann".** Denn die Zahl der Cyberangriffe nimmt Jahr für Jahr zu. Das FBI vermeldet einen täglichen Anstieg der Cyberkriminalität um 300% seit Ausbruch der Pandemie.[2]
Aktuelle Trends, wie Cloud-Technologie und Homeoffice, verursachen mehr Schäden als je zuvor; die kommende 5G-Technologie wird die Verbindung Tausender IoT-Geräte ermöglichen und damit eine neue Schwachstelle bieten, die in großem Umfang angegriffen werden kann. Bis 2025 wird die Schadenshöhe durch Cyberkriminalität auf 10,5 Billionen USD jährlich[3] prognostiziert.

Schadenshöhe durch Cyberkriminalität weltweit

$6 BILLIONEN pro Jahr.

$500 MILLIARDEN pro Monat.

$115,4 MILLIARDEN pro Woche.

$16,4 MILLIARDEN pro Tag.

$684,9 MILLIONEN pro Stunde.

$11,4 MILLIONEN pro Minute.

$190,000 pro Sekunde.

Alle Zahlen (in USD) sind Voraussagen für 2021.

cybersecurityventures.com, vgl. Fn. 1.

1. Morgen, S. Cybercrime to Cost the World $10.5 Trillion Annually by 2020, Cybersecurity Ventures, 12. November 2020.
2. Walter, J. COVID-19 news: FBI Reports 300% Increase in Reported Cybercrimes, IMC Grupo, 2. Mai 2020.
3. Vgl. Fn. 1.

Cyberangriffe: Warum Sie in Ihrem Unternehmen das Bewusstsein dafür schärfen sollten.

In den letzten Jahren hat sich die Cyberkriminalität auf neue Ziele verlagert. Die Opfer sind nicht mehr nur große multinationale Unternehmen. Nun werden Cyberangriffe auch genutzt, um Einzelpersonen, öffentlichen und privaten Organisationen auf allen Ebenen zu schaden.

Jeder Angriff hat seine eigene Struktur mit unterschiedlichen Folgen, die ihn mehr oder weniger beängstigend machen. Die Intention bleibt jedoch immer die gleiche: **Cyberkriminelle wollen auf Kosten des Opfers hohe Gewinne aus ihren Angriffen erzielen.** Geht es um Identitäts- oder Datendiebstahl, kann das Opfer sowohl auf persönlicher als auch auf wirtschaftlicher Ebene betroffen sein. Obwohl es immer noch Lücken bei den Cybersecurity-Skills gibt und Unternehmen i. d. R. mangelhafte Sicherheitsmaßnahmen anwenden (z. B. beim Datenschutz), entwickelt sich die Verteidigung gegen Cyberbedrohungen weiter und wird ein wichtiges Thema, das Firmen zunehmend in den IT-Schutz investieren lässt.

Prognosen für 2022 zeigen, dass der **globale Markt für Informationssicherheit 170,4 Milliarden USD erreichen wird.**[4]

But let’s face it: Auch wenn alle technisch notwendigen Maßnahmen ergriffen werden, vollkommene Sicherheit wird es nie geben. Von einer sicheren digitalen Umgebung sind wir weit entfernt. Sicherheitsrichtlinien, Equipment und Technologie sind unerlässlich, aber das Bewusstsein für Risiken in Bezug auf die Cybersicherheit muss über die Grenzen der IT-Abteilungen hinausgeführt werden: **Jede Person im Unternehmen sollte genau verstehen, welche Bedrohungen es gibt und wie sie aussehen.** Verantwortungslose und uninformierte Mitarbeiter:innen sind vermutlich die größte Schwachstelle in Ihrem Unternehmen. Die wahre Gefahr kommt oft von innen. **Die erfolgreichste Waffe gegen Cyberbedrohungen ist Wissen,** d. h. die Schulung des Personals hilft, Risiken zu mindern und die Integrität Ihres Unternehmens, Ihrer Kommunikation und Ihrer Daten zu schützen.

4. Contu, R. et al. Forecast Analysis: Information Security, Worldwide, Gartner, 14. September 2018.

Die Top 15 Cyberangriffe: So können Sie sich schützen.

Hat man keine Kenntnisse über Cyberangriffe und ihre Methoden, ist es nicht möglich sich und das eigene Unternehmen davor schützen. Während Begriffe wie Malware oder Spam vertraut klingen, sind die Mechanismen dahinter meistens weniger geläufig. Die Frage, der wir hier nachgehen wollen, lautet: Was sind die 15 häufigsten Cyberattacken, auf die Sie 2021 achten sollten? Und wie können Sie sich davor schützen?

Was wir Ihnen hier vorstellen, sind nicht Cyberterrorismus-Angriffe, die auf die Destabilisierung der gesellschaftlichen Ordnung abzielen – mit weitreichenden Folgen und damit verbundenen ernsthaften Schäden in der realen Welt. Wenn auch einige Cyberangriffe dem „Hacktivismus“ zugerechnet werden können, d. h. Aktionen, die aus Gründen des Aktivismus und Protests auf Unternehmen und Organisationen abzielen, so werden wir uns hier auf Cyberangriffe konzentrieren, die aus persönlichen oder Profitgründen auf ein bestimmtes Opfer ausgerichtet sind.

Kurz gesagt: Es geht um Cyberbedrohungen, die üblicherweise auf Unternehmen abzielen. Wenn wir verstehen, woher sie stammen, wie sie zustande kommen und welche Risiken damit verbundenen sind, können wir uns besser schützen.

Was ist ein Cyberangriff?
Der Versuch durch einen unberechtigten Zugriff auf Netzwerke, Ressourcen, Systeminformationen oder Dienste zu erlangen. Sehr oft ist es auch das Ziel, die Integrität der Systeme zu beeinträchtigen und die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Daten zu beeinflussen.

01. Malware

Malware steht für „malicious software“. Im Allgemeinen bezeichnet man mit **Malware jede von Hackern entwickelte, intrusive Software.** Gängige Beispiele sind Viren, Würmer, Trojaner, Spyware, Adware und Ransomware. **Malware ist eindeutig die Nummer eins unter den Cyberbedrohungen in der Europäischen Union[5].**

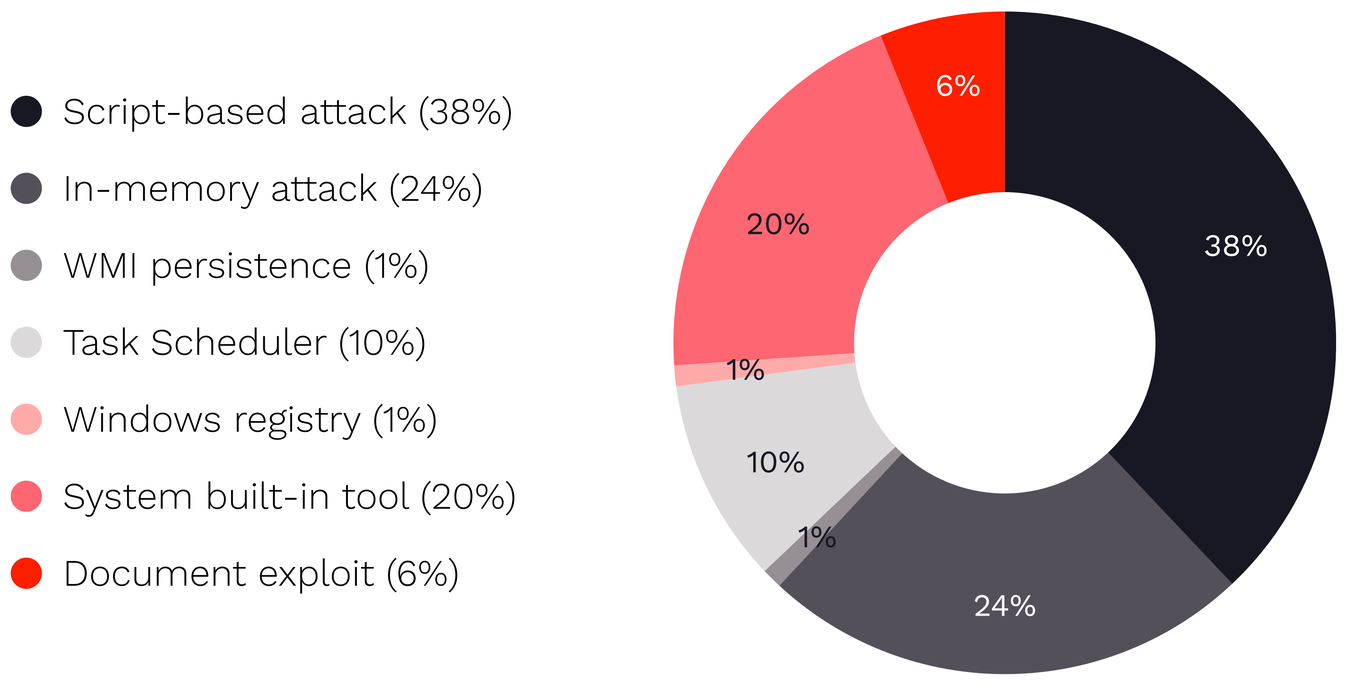
Diese Schadsoftware ist so konzipiert, dass sie heruntergeladen und installiert werden kann, ohne dass User davon wissen oder es überhaupt bemerken. Ist die Installation abgeschlossen, kann die Software schwerwiegende Schäden verursachen.

Malware wird auf Firmen- oder Privatgeräten angewendet, kommt aber auch als „Spion“ auf internationaler Regierungsebene zum Einsatz.

2020 gab es eine deutliche Verschiebung von Verbraucher- zu Unternehmenszielen (+13%) mit den folgenden fünf häufigsten Malware-Arten: Trojan.Emotet, Adware.InstallCore, HackTool, WinActivator, RiskWare.BitCoinMiner, Virus.Renamer.[6]

94% aller Malware-Formen in 2019 wurden per E-Mail zugestellt[7], 46,5% aller Malware in E-Mails hatten ein .docx-Dateiformat.

Dateilose Zwischenfälle in Prozent, aufgedeckt in Q1/2 2019



Johansen, A. G. What is fileless malware and how does it work?, Norton, abgerufen am 15. Juni 2021.

5. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Malware, 20. Oktober 2020.
6. Ibid.
7. Verizon. 2019 Data Breach Investigations Report (PDF), abgerufen am 15. Juni 2021.

2018 führte **1 von 13 Webanfragen zu Malware**[8]. Cyberkriminelle haben auch ihr Geschäftsmodell angepasst. Im Darknet handeln und verkaufen sie **MaaS (Malware as a Service)**: ein "Malware-Kit" mit einem Loader, Command- und Control-Server (C2) plus einer Backdoor zur Steuerung des infizierten Computers.

So schützen Sie sich vor Malware

- Zuallererst: Halten Sie Ihren Computer und Ihre Geräte immer auf dem neuesten Stand.
- Zudem sollte ein gutes aktives **Antivirenprogramm** möglichst all Ihre Systeme und Netzwerke abdecken.
- Verwenden Sie einen **E-Mail-Spamfilter,** um Ihr Postfach zu schützen und ausführbare Anhänge (z. B. .exe-Dateien) zu entfernen.
- Seien Sie beim Öffnen von E-Mail-Anhängen sehr vorsichtig, bevor Sie auf Links klicken oder etwas aus dem Internet herunterladen.
- Erlauben Sie Ihrer Firewall, den **TLS/SSL**-Datenverkehr, E-Mails und mobile Anwendungen zu entschlüsseln.
- Mit dem **DigiCert Smart Sea**l können Sie Ihren Websitebesuchern den Status Ihres Malwarescans zeigen.

MEHR ZUM EFFEKTIVEN MALWARE-SCHUTZ VON INTERNETX

8. Symantec, Internet Security Threat Report, March 2018.

02. Webbasierte Angriffe

Cyberkriminalität kann **Websysteme und -services einsetzen,** um Zielpersonen in die Irre zu führen. In diese Kategorie fallen böswillige URLs oder Skripte, die User auf maliziöse Inhalte lenken.

2020 wurden **39%** aller Datenlecks von Webapplikationen verursacht[9].

Genau das passiert zum Beispiel bei **Watering-Hole-Angriffen**: Diese beschreiben eine Strategie, bei der Cyberkriminelle durch Beobachtung oder durch Erraten der Websites, die das Ziel häufiger ansteuert, eine oder mehrere Websites mit Malware infizieren.

Formjacking ist eine weitere Technik, mit der böswilliger Code in die Online-Zahlungsformulare legitimer Websites eingeschleust wird.

Die Angriffsfläche ist größer als je zuvor. Im Internet (Stand Juni 2021) gibt es über 64,3 Millionen Live-Websites, die Content Management Systeme (CMS) verwenden[10]. Sie sind zu einem wichtigen Vektor webbasierter Angriffe geworden.

Aufgrund einer Vielzahl von Schwachstellen im Zusammenhang mit oft veralteten Plug-ins von Drittanbietern eröffnen sie Hackern ein breites Spektrum an Angriffsmöglichkeiten. Webbasierte Angriffe können auch auf die Verfügbarkeit einer Website, ihre Anwendungen und APIs abzielen oder **Brute-Force-Angriffe** verursachen, bei denen die Website mit vielen Anmeldeversuchen überflutet wird.[11]

9. Verizon, 2021 Data Breach Investigations Report, abgerufen am 15. Juni 2021.
10. BuiltWith, CMS Usage Distribution on the Entire Internet, abgerufen am 15. Juni 2021.
11. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 - Web-Based Attacks, 20 October 2020.

So schützen Sie sich gegen webbasierte Angriffe

- Achten Sie darauf, immer die **aktuellste Browser-Version** mit den dazugehörigen Plug-ins zu verwenden. Sie können potenzielle Sicherheitslücken oder Bedrohungen in Websites erkennen.
- Im Zweifelsfall haben Sie die Möglichkeit, Anwendungen zu isolieren und in Ihrem Browser eine Sandbox zu erstellen.
- Tools wie **Adblocker** oder **JavaScript Blocker** können die Ausführung von böswilligem Code in kompromittierten Websites verhindern.
- Halten Sie den Quellcode stets aktuell, wenn Sie Ihre Website in einem CMS betreiben. Neu herausgegebene Updates enthalten oft **Sicherheitspatches**.
- Verwenden Sie ein **TLS/SSL-Zertifikat,** um die Kommunikation zu verschlüsseln und Datendiebstahl zu verhindern.

03. Phishing

Das ist einer der beliebtesten Angriffe, von dem Sie sicher schon gehört haben: **80% der gemeldeten Sicherheitsangriffe in 2020 basierten auf Phishing[12].**

Während der COVID-19 Pandemie stiegen Phishing-Betrügereien innerhalb eines Monats um bis zu **667%**.[13]

Phishing-Angriffe erfolgen zwar über verschiedene Plattformen wie E-Mail, Messaging-Apps oder soziale Medien, aber der grundlegende Mechanismus bleibt gleich[14]: **Hacker nötigen die Zielperson zur Ausführung einer bestimmten Aktion.** Dies kann z. B. die Angabe von Login- oder E-Banking-Informationen sein, das Anklicken eines Links, der zu einer böswilligen Website führt, oder die Installation von Malware. Hat der User getan, was vom Kriminellen gefordert wurde, kann der Bedroher auf Konten zugreifen oder sich in Computersysteme einloggen.

Die weltweit bekannteste Phishing-Variante ist vermutlich der **Nigerian Prince Scam**, auch **419-Betrug** genannt.

Der Kriminelle kontaktiert User mit einer Geschichte über einen riesigen Geldbetrag, der in einer Bank feststeckt, oder über eine große Erbschaft, auf die wegen Regierungsbeschränkungen oder landesüblichen Steuern nur schwer zugegriffen werden kann. Der Betrüger bittet dann um Konto-daten, um ihm bei der Überweisung des Geldes zu helfen, und bietet im Gegenzug einen hohen Geldbetrag an.

12. Fruhlinger, J. Top Cybersecurity Facts, Figures and Statistics, CSO, 9. März 2020.
13. Symanovich, S. Coronavirus Phishing Emails: How To Protect against COVID-19 scams, Norton, 5. März 2020.
14. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 - Phishing, 20. Oktober 2020.

Mittlerweile sind Phishing-Angriffe viel präziser geworden und können Sie persönlich betreffen: Diese Art des gezielten Betrugs wird **Spear-Phishing** genannt und ist zu einem bedeutenden Teil der Cyberkriminalität geworden. 2019 haben 88% aller Unternehmen weltweit Erfahrungen mit Spear-Phishing gemacht[15].

So schützen Sie sich vor Phishing

- Hier gilt vor allem eine goldene Regel: Seien Sie vorsichtig, wem Sie Ihre Daten anvertrauen. Es gibt keine Technologie, die einen 100%igen Schutz gegen Scam-E-Mails bietet.
- **Prüfen Sie sorgfältig die Kontaktdaten des Absenders** und analysieren Sie einen Link vor dem Klick, indem Sie darüber hovern oder ihn per Copy-and-Paste in Ihren Browser eingeben.
- Verwenden Sie nur sichere Verbindungen über **HTTPS** und überprüfen Sie immer den Domain-Namen.

15. Egan, G. State of the Phish 2020, (PDF), Proofpoint, 23. Januar 2020.

04. Angriffe auf Webapplikationen

In den letzten Jahren haben sich im Web immer mehr Applikationen etabliert, deren Software auf Webservern und nicht mehr lokal auf dem Betriebssystem eines Geräts läuft.

Aus diesem Grund ist **die Sicherheit von Webanwendungen zu einem der wichtigsten Themen in der digitalen Umgebung geworden.** Im Vergleich zum Vorjahr wurde in 2019 ein Anstieg dieser Bedrohung um 52% registriert[16].

20% der Unternehmen und Organisationen berichteten 2020 von täglichen DDoS-Angriffen auf ihre Webanwendungen.
Die am häufigsten angewendete Technik war Buffer Overflow (24%), gefolgt von HTTP-Flood (23%), Ressourcenreduzierung (23%), HTTPS-Flood (21%) und Low Slow (21%)[17].

Das liegt vor allem an der Komplexität des Quellcodes, wodurch die Wahrscheinlichkeit von unvorhergesehenen Schwachstellen und böswilligen Code-Manipulationen stark erhöht wird.

Außerdem enthalten Web-Apps oft sehr sensible Daten, die ziemlich lukrativ sein können; die Angriffe können leicht ausgeführt und automatisiert gegen Tausende von Zielen gleichzeitig gestartet werden[18].

Die **Ziele der Cyberangriffe sind recht häufig Datenbanken und Web-anwendungen**, die zur Speicherung oder Lieferung von Informationen verwendet werden.

So auch im Fall eines **SQL-Injection-Angriffs** – vermutlich die gefährlichste Schwachstelle, die am häufigsten zur Manipulation einer Backend-Datenbank genutzt wird.

16. SonicWall. 2020 SonicWall Cyber Threat Report, 4. Februar 2020.
17. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Web Application Attacks, 20. Oktober 2020.
18. Imperva. Web Application Security, abgerufen am 15. Juni 2021.

So schützen Sie sich vor Angriffen auf Webanwendungen

- Als User können Sie nicht viel tun, um sich vor einer kompromittierten Webanwendung zu schützen. Achten Sie darauf, eine verschlüsselte Verbindung und einen aktuellen Browser zu verwenden. Es liegt in der Verantwortung des Anbieters, mögliche Schwachstellen zu erkennen und eine fehlerfreie Web-App auszuliefern. Dies kann auch mit einem professionellen **Software-Scanner** geschehen.
- Auch **Web-App-Firewall**s funktionieren bis zu einem gewissen Grad. Sie können zwar auf die Schwachstelle hinweisen, aber das Problem nicht beseitigen. Leider werden sie von Cyberkriminellen umgangen.
- Ein starkes Eingabe- und Injektionsvalidierungsverfahren trägt dazu bei, nur korrekt kodierte Daten durchzulassen.
- Implementieren Sie eine verschlüsselte Verbindung.
- Und nicht zuletzt: Suchen Sie sich auf einen professionellen **Internet Service Provider**, der Ihre Webanwendung mit maximaler Sicherheit, Verfügbarkeit und Leistung hosten kann.

05. Spam

Spam ist nicht nur lästig, sondern zählt im weiten Sinne auch zur Cyberkriminalität. Spam-Nachrichten stehen häufig in Verbindung mit Betrug oder Scam.

Im März 2020, auf dem Höhepunkt der Pandemiewelle, nahmen Scams um 400% zu[19]. Gegenwärtig werden 85% des weltweiten Spam-Aufkommens von Botnets versendet, einem Netzwerk aus kompromittierten Computern[21].

Fast **85%** aller weltweit verschickten E-Mails sind Spam[20]!

Im Gegensatz zu Phishing-Angriffen, bei denen es sich um gezielte Aktionen handelt, die in der Regel auf Social-Engineering-Techniken basieren, **wird Spam an eine Massenliste gesendet.**

Benutzer werden aufgefordert, eine kompromittierte Website zu besuchen – und die dort platzierte Malware erledigt dann den Rest um Einfallstore auf Systeme zu schaffen.

Die Nachrichten können z. B. eine gefälschte Meldung über den Ablauf einer Domain enthalten und User dazu auffordern, Kontodaten anzugeben.

Fallen Sie nicht auf solche böswilligen Aktionen herein und prüfen Sie ihre Mails nachsichtig.

19. O'Donoghue, C. et al. Coronavirus is Now Possibly The Largest-ever Security Threat - Here's How We may Be Able To Tackle It, Reed Smith, 24. März 2020.
20. Cvetićanin, N. What's On The Other Side Of Inbox - 20 Statistics For 2021, DataProt, 11. Februar 2021.
21. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Spam, 20. Oktober 2020.

So schützen Sie sich vor Spam

- Spammer greifen im Internet ständig neue E-Mail-Adressen ab, daher die wichtigste Empfehlung: Vermeiden Sie es, Ihre **E-Mail-Adresse öffentlich zu posten**.
- Ihr E-Mail-Client sollte die erste Spam-Filterrunde übernehmen und die meisten Nachrichten als potenziellen Spam markieren.
- Halten Sie eine Nachricht für verdächtig, **öffnen Sie keine Anhänge**, und vor allem antworten Sie nicht! Tun Sie dies doch, senden Sie eine klare Botschaft an die Hacker: diese E-Mail-Adresse ist aktiv. In der Folge werden Sie wahrscheinlich noch mehr Spam erhalten.
- Es gibt viele **Antiviren- und Spam-Filter-Tools**, die Ihnen helfen, E-Mails mit Malware zu erkennen und böswillige Nachrichten zu entschlüsseln.
- Verwenden Sie nicht Ihre geschäftliche E-Mail-Adresse, wenn Sie sich für Dienste, Rabatt-Newsletter oder Ähnliches anmelden.
- Spam wird zwar nicht verhindert, aber mit einem **S/MIME-Zertifikat** werden andere durch Spam beförderte E-Mail-Bedrohungen blockiert.

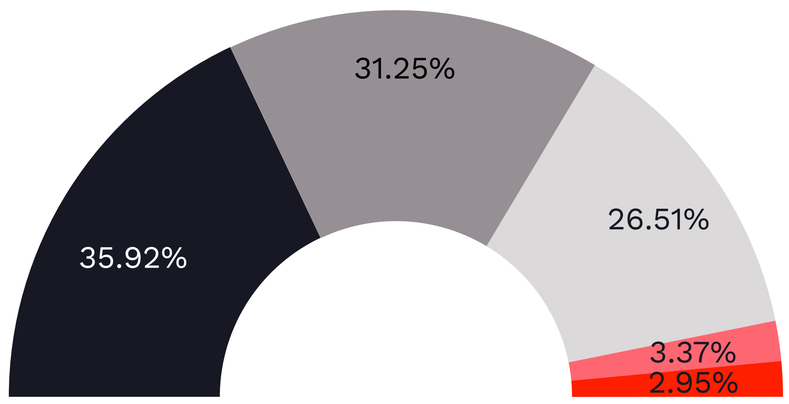
ENTDECKEN SIE S/MIME-LÖSUNGEN VON INTERNETX

06. Distributed Denial of Service (DDoS)

Hacker können einen oder mehrere webbasierte Dienste beeinträchtigen oder gezielt Elemente der Netzwerk-infrastruktursysteme überlasten. Die Auswirkungen reichen von nicht verfügbaren Diensten bis hin zu ganzen Websites, Anwendungen oder Unternehmen, die offline gestellt werden. In solchen Fällen spricht man von einem **Distributed Denial of Service (DDoS)-Angriff.**

Top 5 der am häufigsten attackierten Branchen[22]

in 2019 nach Zahl der Angriffe



Die **Top-Länder,** von denen aus DDoS-Angriffe geführt werden, sind China (26%), die Vereinigten Staaten (15%) und die Philippinen (7%)[23]. Die am häufigsten angegriffenen Länder sind Indien (22,57%), Taiwan (14,79%), Hongkong (12,23%), die Philippinen (11,36%) und die USA (8,73%)[24].

Das Ziel: Ressourcen völlig auslasten, um die Netzwerkkommunikation zu blockieren. Daher sind Server und Rechenzentren die bevorzugten Ziele. Bis 2023 rechnen Experten mit jährlich 15,4 Millionen DDoS-Angriffen.[25]

Im Vergleich zu **DOS (Denial of Service)** sind DDoS-Angriffe wesentlich gefährlicher, da sie Botnetze nutzen und so eine größere Reichweite erzielen.

22. Avishay, N., Kim, J. 2019 Global DDoS Threat Landscape Report, Imperva, 4. Februar 2020.
23. Help Net Security. Duration of Application DDoS Attacks Increasing, Some Go On For Days, 25. Juni 2020.
24. Vgl. Fn. 23.
25. Cisco. Cisco Annual Internet Report (2018–2023), 9. März 2020.

52% aller Angriffe dauerten weniger als 15 Minuten, 21% erreichten eine Dauer von einer Stunde. Längere DDoS-Angriffe zielen eher darauf ab, bleibende Schäden in der attackieren Infrastruktur zu verursachen.

Diese Angriffsart wird in Zukunft noch schlimmere Szenarien hervorrufen: Durch IoT und 5G werden mehr und mehr Geräte mit dem Internet verbunden und die DDoS-Angriffe werden immer ausgefeilter.

So schützen Sie sich gegen DDoS-Angriffe

- Sich vor DDoS-Angriffen zu schützen bedeutet vor allem: Seien Sie darauf vorbereitet, dieser Art von Angriff jederzeit standhalten zu können. Dazu benötigen Sie eine **skalierbare Infrastruktur** und Sie sollten einen **Abwehrplan** für den Fall eines Angriffs erstellen.
- Haben Sie schon einen **Disaster Recovery Plan** für ein DDoS-Angriffsszenario?
- Wenn Sie einen kritischen Dienst betreiben, der rund um die Uhr online sein muss, investieren Sie in **DDoS-Protection**. Fragen Sie Ihren ISP, wie auf diese Cyber-Bedrohung reagiert und welche Schutzlevels angeboten werden.
- Testen Sie Ihre Verteidigungsstrategie, passen Sie diese bei Bedarf an.

Der InterNetX DDoS Mitigation Service hilft, DDoS-Attacken zu entschärfen und so im Idealfall den Fortbetrieb betroffener Dienste oder Websites aufrechtzuerhalten, in jedem Fall aber Störungen auf ein Minimum zu reduzieren.

MEHR ZUR INTERNETX DDOS PROTECTION

07. Identitätsdiebstahl

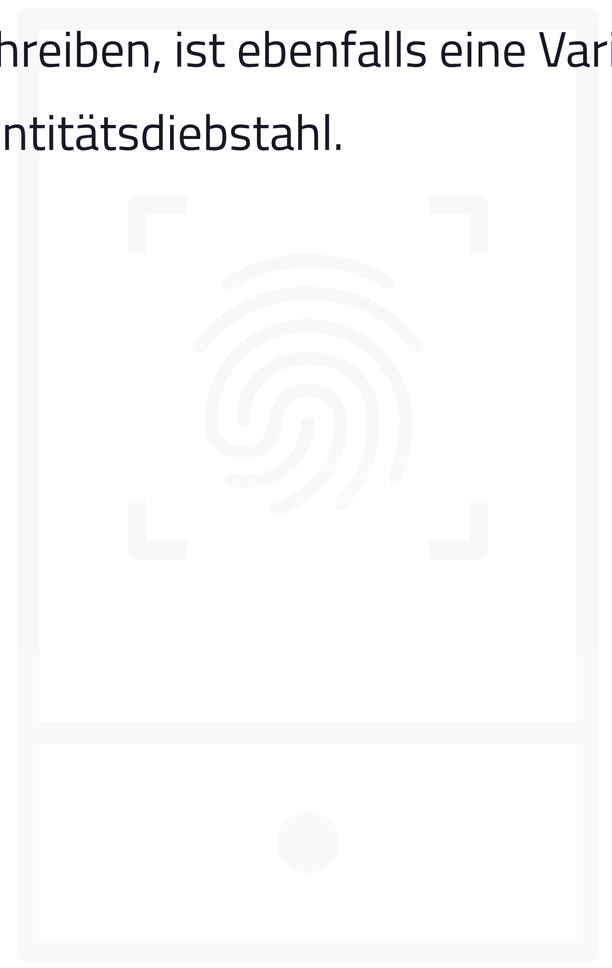
Daten werden häufiger gestohlen, als sich Internetnutzer vorstellen können.
Sie werden genutzt, um anstelle einer Person zu agieren, die nie erfahren wird, dass ihre Identität für böswillige Zwecke verwendet wurde.

Identitätsdiebstahl in den USA kostete die Amerikaner im Jahr 2020 insgesamt etwa **$43 MILLIARDEN**.[26]

Wir geben regelmäßig unsere persönlichen Identifizierungsdaten (Personal Identifiable Information, kurz: PII) im Internet ein. Hacker sammeln diese von internationalen Webservern ab. Sie können diese PII nutzen, um **im Namen einer Person handelnd**, finanzielle Gewinne zu erzielen – doch damit noch nicht genug.

Online-Impersonation (Nachahmung einer Person im Web) kann zum Beispiel dazu genutzt werden, eine SIM-Karte zu aktivieren und sich dann mit dieser Nummer bei bestimmten Diensten anzumelden. Der Kauf einer Geschenkkarte scheint eine sehr häufige Aktion nach einem Identitätsdiebstahl zu sein[27]. Diese Daten landen möglicherweise im Darkweb, wo sie organisiert und von Hackern abgerufen werden, um einen Angriff besser zu planen.

Und nicht zu vergessen:
Im Namen einer anderen Person in sozialen Netzwerken aufzutreten und ihr Aussagen zuzuschreiben, ist ebenfalls eine Variante von Identitätsdiebstahl.



26. Buzzard, J., Kitten, T. 2021 Identity Fraud Study: Shifting Angles, Javelin, 23. März 2021.
27. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 - Identity Theft, 20. Oktober 2020.

So schützen Sie sich gegen Indentitätsdiebstahl

- Damit Ihre sensiblen Daten nicht in die falschen Hände geraten, sollten Sie sich mit allen gängigen Vorkehrungen der Cybersicherheit schützen. Halten Sie Ihre Augen offen und fallen Sie nicht auf Phishing-E-Mails oder Malware herein.
- Verwenden Sie **sichere Passwörter** und seien Sie vorsichtig, wenn Sie in öffentlichen WiFi-Netzwerken surfen.
- Entscheiden Sie sich eher für Offline-Passwort-Manager, also solche zu nutzen, die von Ihrem Browser angeboten werden.
- Um Ihre Konten sicherer zu machen, sollten Sie, wann immer möglich, eine **Zwei-Faktor-Authentifizierung (2FA)** einsetzen.
- Geben Sie Ihre persönlichen Daten nicht bei unaufgeforderten und ungeprüften Anfragen weiter.

08. Datenlecks

Unternehmen speichern große Mengen an Daten, darunter viele persönliche und sensible Informationen, die entsprechend geschützt werden müssen. Das ist allerdings leichter gesagt als getan. **Bereits eine einzige „unbedeutende“ Fehlkonfiguration kann zur Offenlegung der Datenbank führen.**

Bis 2024 werden Geschäftsverluste, die durch von Cyberkriminalität verursachte Datenlecks entstehen, die Summe von **$5 MILLIARDEN** übersteigen[28]. Davon am meisten betroffene Daten sind E-Mails (70%) und Passwörter (64%).[29]

28. Jupiter Research. Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024, 27. August 2019.
29. Risk Based Security, Inc. 2019 MidYear QuickView Data Breach Report (PDF), August 2019.

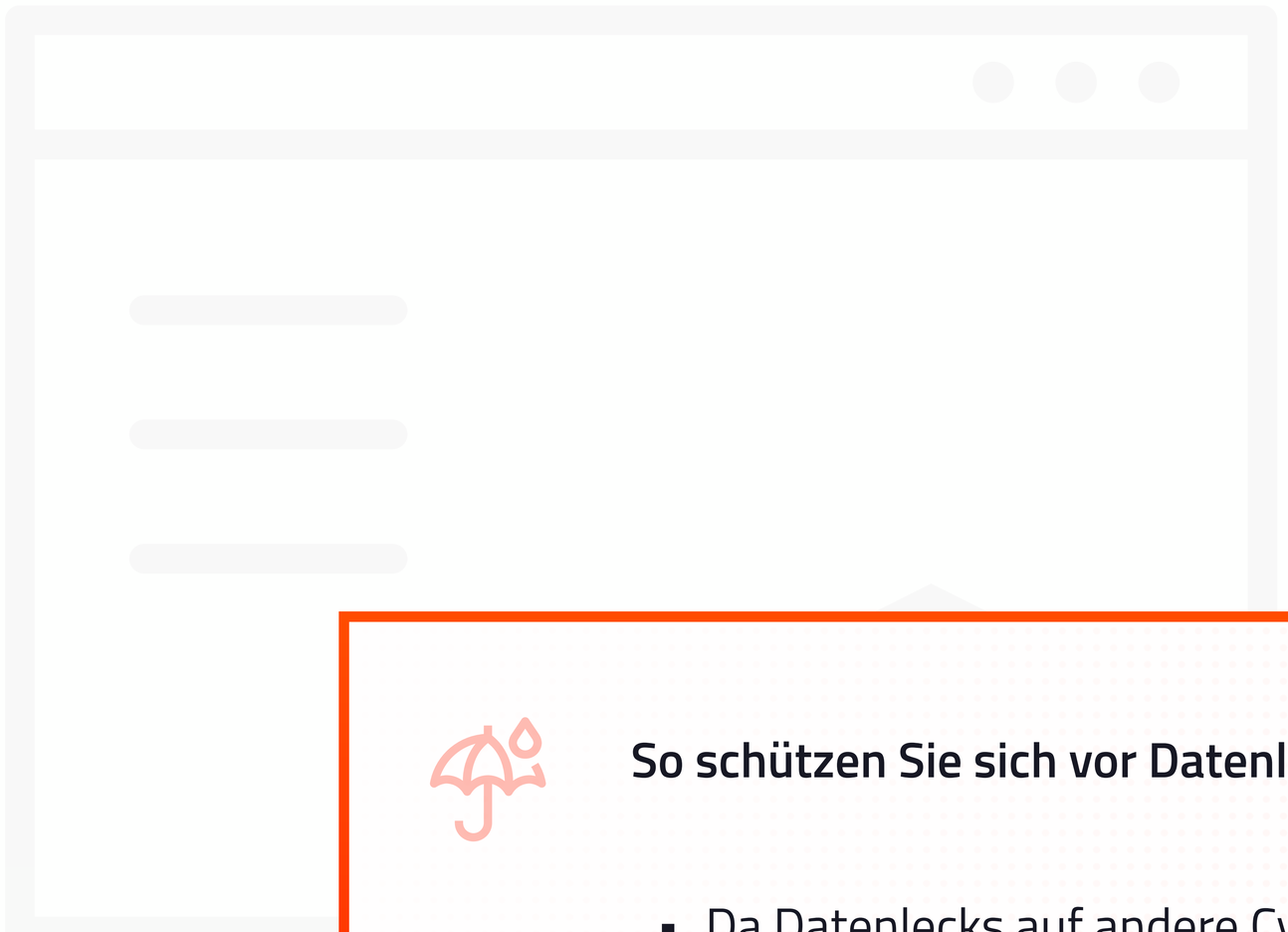
Ein Datenleck liegt vor, wenn Informationen ohne die erforderliche Berechtigung des Eigentümers abgerufen und unbefugt kopiert, offengelegt, verändert oder gelöscht werden, oder wenn der Zugriff auf diese Informationen nicht mehr möglich ist. Solche Aktionen können unbeabsichtigt geschehen – wenn sie jedoch vorsätzlich begangen werden, werden sie als Spionage, Datenverbreitung, Kompromittierung, Diebstahl, gewollte Verschlüsselung oder Zerstörung eingestuft.

Gewöhnlich werden derlei Daten für missbräuchliche Zwecke genutzt. In 71% der Fälle werden damit finanzielle Absichten verfolgt[30]. Besonders besorgniserregend dabei ist, dass sich **Unternehmen und Organisationen eines Datenlecks oft nicht bewusst sind** und sensible Informationen Hackern über einen längeren Zeitraum offenstehen.

Gemäß der DSGVO sollte ein Datenleck immer protokolliert und Betroffene innerhalb von 72 Stunden nach Feststellung des Datenlecks darüber informiert werden.[31]

2020 erkannten Unternehmen Datenlecks im Durchschnitt erst nach **228** Tagen und benötigten **80** Tage, um sie zu schließen.[32]

30. Verizon. 2019 Data Breach Investigations Report, vgl. Fn. 7.
31. European Commission. What is a Data Breach And What Do We Have To Do in Case of a Data Breach?, abgerufen am 15. Juni 2021.
32. IBM. Cost of a Data Breach Report 2020, abgerufen am 15. Juni 2021.



So schützen Sie sich vor Datenlecks

- Da Datenlecks auf andere Cyberbedrohungen zurückzuführen sind, sollten Sie einen allgemeinen **Cybersecurity-Schutzschild** verwenden.
- Schulen Sie alle Beteiligten, von den Endusern bis zu den IT-Mitarbeitern, und vergewissern Sie sich, dass sie sichere Passwörter und Verfahren zur **Passwortverwaltung** verwenden.
- Verschlüsseln Sie die gesamte Kommunikation und achten Sie dabei auf die Sicherheit von sensiblen und persönlichen Daten.
- Eine Investition in **Überwachungs- und Warntools** schützt Sie vor Datenlecks.

09. Insider Threats

Cyberbedrohungen lauern nicht nur außerhalb eines Unternehmens.

Alle internetfähigen Geräte bieten eine große Angriffsfläche für andere Unternehmen oder für die Konkurrenz, die Daten oder wichtige Ressourcen stehlen wollen.

Nach Einschätzung von Analysten wird der Datenmissbrauch in 2021 um **8%** zunehmen; ein Drittel (33%) dieser Datenverletzungen kommt aus den Reihen des eigenen Unternehmens[33].

Bei einem Insider Threat handelt es sich um eine Bedrohung, die von (oftmals ehemaligen) Mitarbeitern, Auftragnehmern, Geschäftspartnern und anderen Personen ausgeht. Sie sind daran interessiert, Ihre sensiblen Daten zu stehlen, Ihre Computersysteme anzugreifen oder Betrug zu begehen[35].

Die Wahrscheinlichkeit, dass Mitarbeiter Daten offenlegen, liegt bei 85%, da fast die Hälfte der Unternehmen nicht einschätzen kann, wie effektiv ihre Technologien Insider-Bedrohungen abwehren[34], und Unternehmen oftmals keine klaren und strengen Richtlinien haben. Durch die zunehmende Anzahl von Menschen, die aufgrund von COVID-19 von zu Hause aus arbeitet, wurde diese Bedrohung verstärkt.

Hierbei gibt es verschiedene Szenarien: Mitarbeiter:innen, werden, bewusst oder unbewusst, zu Spielfiguren in den Schachzügen eines Hackers.
Teammitglieder kommen einzig mit der Absicht zu einem Unternehmen, um sensible Daten zu stehlen, die sie an andere Unternehmen weitergeben.
Hacker können aus diversen Gründen eigenverantwortlich agieren, zumeist geht es jedoch um finanzielle Gewinne.

33. Shey, H. Predictions 2021: The Path To A New Normal Demands Increased Cybersecurity Resilience, Forrester, 26. Oktober 2020.
34. Code42. 2021 Data Exposure Report, abgerufen am 15. Juni 2021.
35. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Insider Threat, 20. Oktober 2020.

So schützen Sie sich vor Insider Threats

- Unmittelbare Maßnahmen zum Schutz Ihres Unternehmens gegen Insider Threats sind schwer umzusetzen und eventuell auch nicht durchführbar. Die Überwachung des Mitarbeiterverhaltens ist nicht zielführend. Sie müssen Ihre **Mitarbeiter:innen dahingehend schulen**, ein Bewusstsein für Datensicherheit zu entwickeln. Davon ausgehend können Sie bestimmte Bereiche überwachen, um mögliche Bedrohungen von innen abzuwehren.
- Nur einer bestimmten Anzahl an Nutzer:innen sollte Zugang zu sensiblen Daten erhalten.
- Generell ist es wichtig, ein **starkes und sicheres digitales Umfeld aufzubauen**, um böswilligen und schädlichen Aktionen vorzubeugen.
- Betriebsvorgänge, Dateien und E-Mails sollten zudem mit einem Warnsystem bei ungewöhnliche Aktionen ausgestattet sein.

10. Botnets

Ein Botnet setzt sich aus **mehreren über das Internet verbundene Geräte zusammen, die i. d. R. mit Malware infiziert sind.** Unter der Kontrolle von Cyberkriminellen, die über Peer-to-Peer (P2P) oder über ein Command & Control Center (C2) agieren, werden **Systeme und Infrastrukturen infiltriert. Dabei wird jede Sicherheitslücke ausgenutzt,** um Warntools mithilfe von Malware und Trojanern zu umgehen.

Anfang 2021 war die gTLD .com die Domain-Endung, die am häufigsten mit **Command & Control (C&C)** Botnets in Verbindung gebracht wurde. Auch die new gTLDs .top und .xyz werden seit Langem missbräuchlich attackiert und stehen an der Spitze der am häufigsten angegriffenen Top-Level-Domains.[36]

Diese Missbrauchstechnik wird dazu eingesetzt, unterschiedliche Betrugsmaschen und Cyberangriffe durchzuführen – meistens geschieht dies in großem Umfang über DDoS-Angriffe. Durch Künstliche Intelligenz und Automatisierung hat diese Technik einen großen Aufschwung erfahren, wodurch Cyberangreifer effizienter arbeiten können. **Das Hauptziel eines Botnets ist es nämlich, so viele Geräte wie möglich zu infizieren.**

Als Ressourcen und Rechenkapazitäten werden automatisierte Prozesse genutzt, von denen die Benutzer nichts wissen, **wodurch sie ein integraler Bestandteil eines Netzwerks mit ferngesteuerten Bots werden.** Das Zombie-Gerät erhält dann die Anweisungen vom Botmaster, Downloads anderer Malware-Typen zu übertragen, weitere Bots zu finden oder noch mehr schädliche Aktionen durchzuführen.

36. Spamhaus Malware. Spamhaus Botnet Threat Update: Q1 2021, 15. April 2021.

Mit Botnets können bestimmte Aktionen auf Hunderttausenden Geräten gleichzeitig durchgeführt werden, um DDoS-Angriffe auf Webserver auszuführen, eine Webseite mit übermäßigem Datenverkehr zu beeinträchtigen, gewisse Dienste zu blockieren, schädliche Software (Adware, Spyware, Ransomware usw.) für illegale Aktionen und Datenschutzverletzungen zu verbreiten, aber auch Bitcoins unter Verwendung der Leistung von Zombie-Computern herzustellen. Spamming scheint jedoch die Hauptmethode für diesen Zweck zu sein.[37]

So schützen Sie sich vor Botnets

- Die beste Verteidigungsstrategie gegen diese Bedrohung besteht darin, die **Schutzmaßnahmen in Ihrem Netzwerk** und an allen potenziellen Zugriffspunkte zu erhöhen, z. B. durch ein starkes Konfigurationsnetzwerk und Firewalls.
- Auch User fallen in diese Kategorie; deshalb ist es besonders wichtig, sie in Sachen Cybersicherheit zu schulen.
- Verwenden Sie **Tools,** die Verbindungen zu IP-Adressen blockieren, die mit Botnet-Aktivitäten in Verbindung stehen, oder prüfen Sie die Herkunft des Datenverkehrs z. B. mit reCAPTCHA.
- Die **Zwei-Faktor-Authentifizierung** kann eine zweifache Schutzebene gewährleisten und Botnet-Angriffe verhindern.

37. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Botnets, 20. Oktober 2020.

11. Physische Angriffe

Die IT-Infrastruktur Ihres Unternehmens stützt sich auf physische Systeme. Diese sind empfindlicher als Sie vielleicht denken. Sie müssen lediglich ein Glasfaserkabel durchtrennen, um den Betrieb zu unterbrechen. Geräte mit einer starken Integrität sind in unserer heutigen Welt besonders wichtig, da wir unsere Daten auf den Geräten speichern und uns auf sie verlassen. Angefangen von IoT über Smart Homes bis hin zu intelligenter Gebäude-technik oder Smart Wearables – wir müssen dafür sorgen, dass die Sicherheit der Daten gewährleistet wird und zusätzlich **eine Reihe neuer physischer Sicherheitsmaßnahmen ergreifen.** Anhand der folgenden Zahl wird deutlich warum:

In **54%** der Datenmissbrauchsfälle in allen Branchen waren physische Angriffe am häufigsten.[38]

Im Zusammenhang mit dem sogenannten **Internet of Everything (IoE)**, der nächsten Internet-Generation, beschäftigen sich Experten mit der Verschmelzung von physischem Schutz und Cybersecurity. Bei einem physischen Angriff verschaffen sich Kriminelle durch Gewalteinwirkung, Täuschung, Umgehung oder Deaktivierung von Zugangskontrollen Zugang zum physischen Objekt und zur Infrastruktur und können so das System und seine Daten manipulieren oder beschädigen.

38. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Physical manipulation/damage/theft/ loss, 20. Oktober 2020.

So schützen Sie sich vor physischen Angriffen

- Physische Angriffe können äußerst problematisch sein, vor allem für kleine und mittlere Unternehmen, die sich kein Sicherheitspersonal oder keine technische Infrastruktur leisten können. Neben den üblichen Cybersecurity-Maßnahmen ist es wichtig, dass Sie Ihr Team darin schulen, die Unternehmensumgebung durch Einsatz von Tools wie **Smart Locks** oder **Smart Keys** zu schützen.
- Stellen Sie sicher, dass Sie einen **Sicherheitsplan** und **Zugangskontrollen** für Eingangspunkte wie Türen und Fenster haben.
- **Alarmanlagen** und **Überwachungskameras** sind nach wie vor unverzichtbar und können auch ggf. auch wichtige Beweismittel für die Polizei liefern.
- Um auf der sicheren Seite zu sein, sollten Sie eine **Versicherung** abschließen, die sowohl bei physischen als auch bei Cyberangriffen Schäden, Diebstahl und Verluste abdeckt.
- Darüber hinaus sollten **Zugriffsrechte** nur an relevantes Personal in Ihrem Unternehmen vergeben werden.
- Verlassen Sie sich auf professionelle **Colocation**-Lösungen.

12. Informationslecks

Informationslecks bestehen dann, wenn **sensible Daten für Unbefugte offengelegt werden.** Dies ist oft auf ein Datenleck zurückzuführen, das in der Regel von jemandem innerhalb des Unternehmens oder durch eine Schwachstelle in einem Unternehmensprozess verursacht wurde. Informationen werden meist auf sehr banale Art veröffentlicht, z. B. durch falsche Anwendungs- oder Serverkonfigurationen, durch sensible Informationen in HTML-Kommentaren, im Quellcode oder einfach einsehbar für alle.

2019 waren **14%** aller Vorfälle im Finanzsektor auf die Offenlegung von Daten zurückzuführen.[39]

Das bisher größte Datenleck ist der **CAM4-Fall** mit der Offenlegung von 10,88 Milliarden Datensätzen – mit vollständigen Namen und E-Mail-Adressen.[40]

So schützen Sie sich gegen Informationslecks

- Der wichtigste Tipp: Speichern Sie Daten nur auf **sicheren Anlagen**.
- Erfassen Sie sensible Daten und nutzen Sie Kontrollen und/oder **Verschlüsselung** sowie sichere **Gateways**.
- Verwenden Sie **starke Sicherheitsprotokolle** und testen Sie sämtliche Konfigurationen und Einstellungen. Dazu können Sie Tools einsetzen, die gezielt nach Schwachstellen und Datenlecks suchen.

39. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Information Leakage, 20. Oktober 2020.
40. Tunggal A. T. The 56 Biggest Data Breaches, UpGuard, 14. Mai 2021.

13. Ransomware

Ransomware hat sich in den letzten Jahren zu einer der Hauptbedrohungen für die Cybersecurity entwickelt, und die Zahl dieser Angriffe nimmt weiter zu.

Alle **11 SEKUNDEN** wird ein Unternehmen Opfer eines Ransomware-Angriffs.[41]

Die Zahl der Angriffe ist hoch, denn Ransomware ist für Cyberkriminelle eine **relativ leicht zu startende Anwendung, die zudem hohe Gewinne abwirft[42].**

Schätzungen zufolge werden in 2021 die **globalen Kosten für Ransomware-Schäden 20 Milliarden USD erreichen[43].**
2020 waren die am stärksten betroffenen Bereiche die Dienstleistungsbranche, das Bildungswesen und Regierungen[44].

Ransomware kann sowohl Computer als auch mobile Geräte blockieren, aber auch einzelne elektronische Dateien verschlüsseln, wodurch User keinen Zugriff mehr auf ihre Daten haben. Zur Freigabe wird die Zahlung eines Lösegeldes eingefordert. Aber: Die Zahlung des Lösegelds ist keine Garantie dafür, dass Daten auch wirklich zurückgegeben werden!

So gaben Unternehmen, die Lösegeld zahlten, am Ende bis zu doppelt so viel aus, um ihre Daten wiederherzustellen. Hinzu kommt der Imageschaden für das Unternehmen, sollten diese Informationen an die Öffentlichkeit gelangen[45]. Wir empfehlen nachdrücklich nicht zu zahlen, sollten Sie Opfer von Ransomware werden.

2020 erhielten nur **26%** der Opfer nach einer Lösegeldzahlung ihre Daten zurück.[46]

41. Morgan S. Global Ransomware Damage Costs Predicted To Reach $20 Billion By 2021, Cybercrime Magazine, 21. Oktober 2019.
42. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 - Ransomware, 20. Oktober 2020.
43. Morgan, S. Global Ransomware Damage Costs Predicted To Reach $20 Billion By 2021, vgl. Fn. 41.
44. Blackfrog. The State of Ransomware in 2021, 1. Mai 2021.
45. Sophos. The State of Ransomware 2020 (PDF), Mai 2020.
46. Ibid.

So schützen Sie sich gegen Ransomware

- Um Ransomware effektiv entgegenzuwirken, sollten Unternehmen schnellstmöglich folgenden Doppelansatz verfolgen: **Mitarbeiterschulungen** und **innovative Tools**.
- Eine Ransomware-Verseuchung geschieht in der Regel per E-Mail. Daher ist es wichtig, Nachrichten zu erkennen, die böswillige Anhänge oder Links enthalten. Klicken Sie niemals auf E-Mails, die wie Spam aussehen oder auf unbekannte Websites verlinken, und öffnen Sie keine Anhänge, die nicht vertrauenswürdig erscheinen.
- Hacker versuchen auch, durch Anrufe, SMS oder E-Mails an persönliche Daten zu gelangen. Geben Sie keine Daten heraus, ohne die **Identität des Anfragestellers zu überprüfen**.
- Sofern Sie keine Backups erstellt oder geeignete Sicherheitsmaßnahmen installiert haben, können Sie in den meisten Fällen leider nur wenig unternehmen, sollten Sie Opfer von Ransomware werden. Aus technischer Sicht ist es wichtig, **Sicherheitssoftware-Tools** zu installieren, die darauf abzielen, die Folgen des Angriffs zu erkennen und abzuschwächen.
- Außerdem sollten Sie eine Lösung bereithalten, um Ihre Daten im Ernstfall speichern zu können.
- Sie könnten auch versuchen, die infizierten Computer mit Entschlüsselungssoftware zu entsperren. So bietet No More Ransom 59 Entschlüsselungs-Tools für 91 Ransomware-Familien an.

Die 10 gefährlichsten Ransomware-Programme der letzten Jahre!

14. Cyberspionage

Cyberspionage ist eine Form der Cyberkriminalität, die sich, unter anderem bedingt durch die digitale Transformation, auf die Gesellschaft und die gesamte Produktionskette auswirkt. Unter Cyberspionage versteht man **unterschiedliche Handlungen** mit dem Ziel, **auf einem bestimmten System nach vertraulichen Informationen zu suchen.** Sie wird eingesetzt, um Passwörter, E-Mails, Projekte, Pläne oder jede Art von Geheimnissen zu stehlen, in der Regel von Geschäftskonkurrenten oder **Rivalen, um militärische, politische oder wirtschaftliche Vorteile zu erlangen.** Spionageangriffe werden manuell von Menschen oder durch Malware durchgeführt. Letzteres betrifft meist große Unternehmen und wird als „Wirtschaftsspionage“ eingestuft. Diebstahl von personenbezogenen Daten „im klassischen Sinn“ führt zu noch mehr **Veruntreuung von geistigem Eigentum.** Der Diebstahl von Geschäfts- und Staatsgeheimnissen ist ein hoch profitables Business. Immer noch stehen 38% der Spionageaktionen im Zusammenhang mit Nationalstaaten[47].

In den beiden Weltkriegen wurde Spionage als Kriegsmittel eingesetzt. Doch erst während des Kalten Krieges führten die Sowjets besonders weitreichende Spionageverfahren ein, durch die sie an Unterlagen von amerikanischen Atomlaboren gelangten[48]. Mit dem Aufkommen des Internets in den 90er Jahren gewann Cyberspionage jedoch eine viel größere Reichweite.

47. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Cyber Espionage, 20. Oktober 2020.
48. U.S. Department of Energy. Espionage and The Manhattan Project, abgerufen am 15. Juni 2021.

Bei Cyberspionage-Einsätzen wird als Infektionsmedium das sogenannte Spear-Phishing genutzt. Unfassbare **63% der Fälle sind auf Phishing zurückzuführen**[49]. Im Vergleich zu anderen Cyberangriffen ist Cyberspionage zwar nicht die größte Bedrohung und hat nur einen Anteil von 10-26% an den Cyberangriffen, **aber sie ist eindringlicher und aggressiver als andere Methoden**[50].

So schützen Sie sich vor Cyberspionage

- Unternehmen steht eine Reihe von bewährten Verfahren zur Verfügung, um sich vor solchen Angriffen zu schützen und sie abzuwehren. Wie immer bildet das Personal die erste Verteidigungslinie. Daher sollten sich alle Mitarbeiter regelmäßig in Sachen **Cybersecurity schulen lassen**.
- Social Engineering und Phishing sind gängige Verfahren, mit denen sich Cyberspione Zugang zu sensiblen Systemen verschaffen. Die **Verschärfung der Sicherheitsmaßnahmen** kann die Bedrohung reduzieren.
- Eine gezielte **Managed Detection and Response (MDR)-Strategie**, zu der beispielsweise Security Information and Event Management (SIEM)-Technologien, Threat Intelligence, User and Entity Behavior Analysis (UEBA), Threat Search-Funktionen sowie die Integration in Technologien zur Endpoint Detection and Response (EDR) und Anti-Fraud-Systeme gehören, kann Hinweise zu möglichen Sicherheitslücken im Netzwerk und an den Endpunkten liefern.

49. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Cyber Espionage, siehe Fußnote 48.
50. Verizon. Cyber-Espionage Report 2020, 2020.

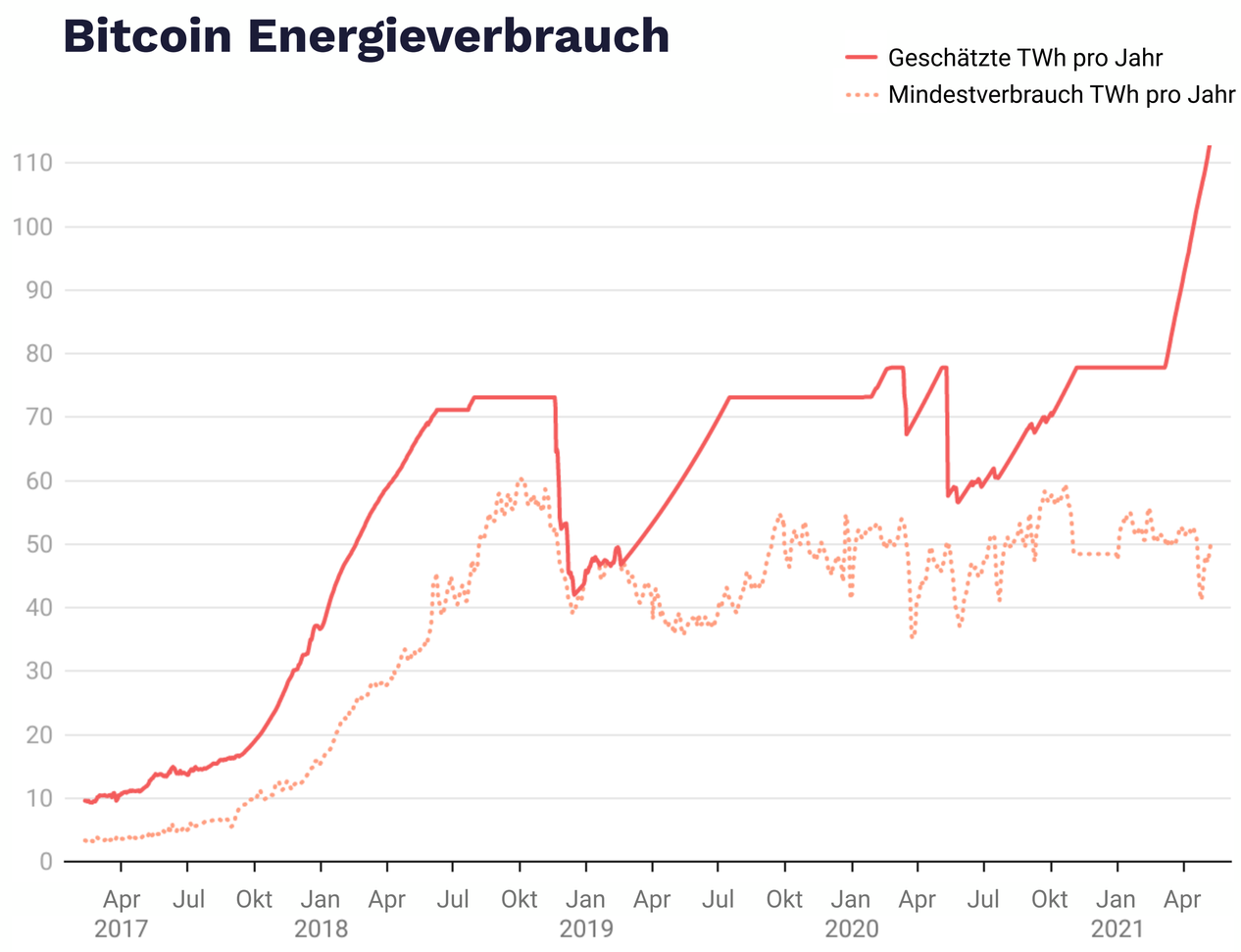
15. Cryptojacking

Kryptowährungsanleger haben ein neues Eldorado gefunden. Die Funktionsweise dieser digitalen Wertschöpfungsform basiert auf dem Prinzip der Kryptografie. **Kryptowährungen werden durch das sogenannte Mining erzeugt.** Bei diesem Prozess werden die Rechenressourcen eines Computers in Kryptowährungen umgewandelt. Die steigende Anzahl der auf dem Markt angebotenen Kryptowährungen verlangt nach immer mehr Rechenleistung, mehr als je zuvor. Und selbstverständlich wird für diesen Vorgang Strom benötigt.

Im Mai 2021 wurde der Bitcoin-Energieverbrauch auf fast

110 TWH PRO JAHR

geschätzt – das entspricht etwa dem Stromverbrauch der Niederlande innerhalb eines Jahres.[51]



BitcoinEnergyConsumption.com

51. Digiconomist. Bitcoin Energy Consumption Index, abgerufen am 15. Juni 2021.

Unter den Minern gibt es auch kriminelle Hacker, die böswillige Cryptomining-Techniken anwenden, um die Rechenleistung von Computern oder mobilen Geräten ahnungsloser User auszunutzen. Tatsächlich kann **jeder, der einen Computer besitzt, Kryptowährungen erzeugen.** Diese Bedrohung kann Webseiten und Geräte aller Art kompromittieren und vor allem Unternehmen enormen wirtschaftlichen Schaden zufügen.

Cryptojacking-Angriffe können auf unterschiedliche Weise durchgeführt werden. Es überrascht nicht, dass hauptsächlich Phishing dafür verwendet wird. Das Opfer wird dazu verleitet, auf den Link in einer schädlichen E-Mail zu klicken. Dieser führt zu einer Website, auf der ein Kryptomining-Code installiert wurde.

Ferner gibt es auch die Variante **„Drive-by-Cryptomining“**, bei der bösartiger JavaScript-Code in einer Webseite versteckt wird. Jeder, der diese Seite besucht, wird sofort infiziert und beginnt unverzüglich mit der Generierung von Krypowährungen.

Auch Mobilgeräte, die auf einem Android-Betriebssystem laufen, bleiben von Cryptojacking nicht verschont. Die meisten Angriffe auf Android sind auf Trojaner in böswilliger Apps zurückzuführen.

Die meisten Cryptojacking-Angriffe auf Android sind auf die Nutzung von böswilligen Apps zurückzuführen, die als Trojaner getarnt sind. In vielen Fällen werden die Smartphone-Ressourcen derart ausgenutzt, dass es zu einem Overload des Prozessors und folglich zur Überhitzung kommt. Sowohl der Akku als auch das Smartphone selbst wird beschädigt.

Desktop-Computer und Server verfügen über mehr Rechenleistung als Mobilgeräte. Da diese für Hacker nicht so ergiebig sind, besteht für mobile Geräte weniger Risiko.

So schützen Sie sich gegen Cryptojacking

Cryptojacking wurde so konzipiert, dass das Programm zu 100% verborgen bleibt, ohne den infizierten Rechner zu beschädigen. Zur Durchführung eines Kryptojacking-Angriffs stehen den Angreifern verschiedene Techniken zur Verfügung. Eine der beliebtesten weist große Ähnlichkeiten zu der Methode auf, die zur Verbreitung herkömmlicher Malware eingesetzt wird.

- Um Phishing-Aktionen abzuwehren, können **Ad-Blocking- und Anti-Cryptomining-Erweiterungen** auf den Browsern wirksame Schutzmaßnahmen sein.
- **Endpoint Protection oder Antiviren-Software** bieten in ihren Paketen oft integrierte Kryptomining-Erkennungstools. Microsoft Defender for Endpoint greift beispielsweise auf maschinelles Lernen mit Telemetrie zurück, um solche Bedrohungen zu erkennen[52].

Cybersecurity: Warum Sie Ihre Abwehrsysteme verstärken sollten.

Die meisten Menschen glauben, dass Cyberattacken nur durch ausgeklügeltes Netzwerk-Hacking entstehen. Diese Annahme kann viel Schaden anrichten, da den notwendigen Schutzmaßnahmen bei den täglichen Aufgaben im Internet zu wenig Beachtung geschenkt wird.

Die am meisten unterschätzten Cyberangriffe fallen unter die Kategorie **Social Engineering-Techniken**: CEO-Betrug, Spoofing (Fälschung von Absenderdaten zur Täuschung des Empfängers), Angriffe aus dem Bereich Business Email Compromise sowie verschiedene Techniken des Account-Hijacking mit schädlichen Anhängen. Seien Sie auch auf sozialen Plattformen, Messaging-Apps und E-Mail-Postfächern wachsam. Nur allzu häufig werden solche Anwendungen ohne hinreichende Aufmerksamkeit und ohne jede Art von Prävention genutzt.

So schützen Sie Ihr Unternehmen

Cyberattacken werden immer anspruchsvoller, gezielter, umfangreicher und bleiben immer öfter unentdeckt. Trotz wachsender Bemühungen, schützen sich viele KMUs nicht ausreichend.

- Der erste Schritt zur digitalen Sicherheit ist die Stärkung des **Bewusstseins für Cybersecurity** beim gesamten Personal. Schulungen sind zur Prävention unerlässlich.
- Sie können auch **KI-basierte Systeme** einsetzen, die in der Lage sind, Bedrohungen nach einer entsprechenden Lernphase zu filtern.
- Unternehmen müssen flexibel bleiben und ihr Augenmerk auf die Abwehr aller möglichen Cyberbedrohungen legen.
  Erhöhen Sie die Sicherheit und schützen Sie Ihr Unternehmen!

Quellenangaben.

- Avishay, Nadav, Kim, Johnathan. 2019 Global DDoS Threat Landscape Report, 4. Februar 2020.
- Blackfrog, The State of Ransomware in 2021, 1. Mai 2021.
- BuiltWith. CMS Usage Distribution on the Entire Internet, abgerufen am 15. Juni 2021.
- Buzzard, John, Kitten, Tracy. 2021 Identity Fraud Study: Shifting Angles, Javelin, 23. März 2021.
- Cisco. Cisco Annual Internet Report (2018–2023), 9. März 2020.
- Code42. 2021 Data Exposure Report, abgerufen am: 15. Juni 2021.
- Contu, Ruggero et al. Forecast Analysis: Information Security, Worldwide, Gartner, 14. September 2018.
- Cvetićanin, Nikolina. What's On The Other Side Of Inbox - 20 Statistics For 2021, DataProt, 11. Februar 2021.
- Digiconomist. Bitcoin Energy Consumption Index, abgerufen am:15. Juni 2021.
- Egan, Gretel. State of the Phish 2020, (PDF), Proofpoint, 23. Januar 2020.
- European Commission. What is a Data Breach And What Do We Have To Do in Case of a Data Breach?, abgerufen am: 15. Juni 2021.
- European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020, 20. Oktober 2020.
- Fruhlinger, Josh. Top Cybersecurity Facts, Figures and Statistics, CSO, 9. März 2020.
- Help Net Security. Duration of Application DDoS Attacks Increasing, Some Go On For Days, 25. Juni 2020.
- IBM, Cost of a Data Breach Report 2020, abgerufen am: 15. Juni 2021.
- Imperva. Web Application Security, abgerufen am 15. Juni 2021.
- Jupiter Research. Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024, 27. August 2019.
- Morgen, Steve. Cybercrime to Cost the World $10.5 Trillion Annually by 2020, Cybersecurity Ventures, 12. November 2020.
- Morgan Steve. Global Ransomware Damage Costs Predicted To Reach $20 Billion By 2021, Cybercrime Magazine, 21. Oktober 2019.

- O'Donoghue, Cynthia, et al. Coronavirus is Now Possibly The Largest-ever Security Threat - Here's How We may Be Able To Tackle It, Reed Smith, 24. März 2020.
- Risk Based Security, Inc. 2019 MidYear QuickView Data Breach Report (PDF), August 2019.
- Shey, Heide. Predictions 2021: The Path To A New Normal Demands Increased Cybersecurity Resilience, Forrester, 26. Oktober 2020.
- Spamhaus Malware, Spamhaus Botnet Threat Update: Q1 2021, 15. April 2021.
- Selvaraj, Karthik. Defending against cryptojacking with Microsoft Defender for Endpoint and Intel TDT, 26. April 2021.
- SonicWall. 2020 SonicWall Cyber Threat Report, 4. Februar 2020
- Sophos, The State of Ransomware 2020 (PDF), Mai 2020.
- Symanovich, Steve. Coronavirus Phishing Emails: How To Protect against COVID-19 scams, Norton, 5. März 2020.
- Symantec. Internet Security Threat Report, März 2018.
- Tunggal Abi Tyas. The 56 Biggest Data Breaches, UpGuard, 14. Mai 2021.
- U.S. Department of Energy. Espionage and The Manhattan Project, abgerufen am: 15. Juni 2021.
- Verizon. 2019 Data Breach Investigations Report (PDF), abgerufen am 15. Juni 2021.
- Verizon. Cyber-Espionage Report 2020, 2020.
- Walter, Jenna. COVID-19 news: FBI Reports 300% Increase in Reported Cybercrimes, IMC Grupo, 2. Mai 2020.

Bildnachweis.

- Coverbild: Rawpixel auf envato elements

Ohne Gewähr.

Dieses E-Book wurde von InterNetX GmbH mit größter Sorgfalt mit den zum Zeitpunkt der Herausgabe verfügbaren und aktuellsten Informationen erstellt. Alle Informationen entsprechen dem Stand der Technik und werden ohne Gewähr für ihre Richtigkeit und Vollständigkeit zur Verfügung gestellt. Die hier enthaltenen Informationen können ohne vorherige Ankündigung geändert werden und sind allgemeiner Art; daher sollten sie nicht für spezifische Zwecke verwendet werden. InterNetX übernimmt keine Haftung für Fehler oder Auslassungen in den hier bereitgestellten Informationen.

About.

InterNetX

With more than 4 million domains under management, InterNetX is one of the leading providers of white-label hosting and domain products. InterNetX provides Internet Service Providers, telecommunications companies and agencies with domains, shared and dedicated hosting products, security solutions and network connections. InterNetX also directly offers TLS/SSL and S/MIME products from leading certificate authorities.

Simone Catania specializes in B2B Tech Content Marketing. As Global Content & Communications Manager, Simone is the main author of InterNetX blog where we published our interview series “It’s all about domains”. Together with our creative team, he empowers and educates users about IT and internet-related topics.

InterNetX GmbH
Johanna-Dachs-Str. 55
93055 Regensburg
Germany
Phone +49 941 59559-0
Fax +49 941 59559-55
email: info@internetx.com
www.internetx.com

Follow us:

Subscribe to our newsletter:
www.internetx.com/internetxpress

InterNetX