GEMEINSAM MACHEN **WIR** IHR **UNTERNEHMEN** SICHER**!**

LINK11

GLASFASER RUHR

GLASFASER RUHR Geschäftsfelder

BUSINESS-LÖSUNGEN FÜR INTERNET & TELEFON

CARRIER VERTRIEB

DATACENTER MIT SERVER-HOUSING UND COLOCATION

IMMOBILIEN-SERVICES FÜR STÄDTISCHE EINRICHTUNGEN UND WOHNUNGS-WIRTSCHAFTEN

SICHERE STANDORT-VERNETZUNG FÜR UNTERNEHMEN

ZUR SECURITY LAGE DER NATION
-
DEUTSCHLAND IM FOKUS

DDOS ANGRIFFE ERKLÄRT

Gezielte Überlastung eines Systems / einer Schnittstelle durch

- Zu viele Anfragen zur gleichen Zeit
- Zu große Anfragen
- Viele falsche Anfragen
- Ausnutzen von Schwachstellen

Quelle: dpa

LINK11

EIN LAGEBILD

AKTUELLE BEDROHUNGSLAGE

29.05.2024 / 13:32

HVV: Hackerangriff legte Online-Ticketkauf fast einen Tag lang lahm

Artikel vorlesen

00:00 / 01:21 1X BotTalk

Auf den Hamburger Verkehrsverbund ist ein Hackerangriff verübt worden. Von Dienstagnachmittag bis Mittwochmittag war der Ticketkauf über die App nicht oder nur eingeschränkt möglich.

Wer am Dienstag oder Mittwoch versuchte, über die HVV-App oder übers Internet ein Ticket zu kaufen, wurde mit folgender Mitteilung konfrontiert: „Wegen einer technischen Störung ist die Anmeldung in der hvv App derzeit nicht möglich. Bitte nutzt den anonymen Ticketkauf in der hvv App oder die hvv switch App."

Details zum Sicherheitsvorfall

DDoS Ausfall

Betr. (Organisation)	Bundesamt des Innern und für Heimat
Datum (Veröffent.)	12.06.2024
Land	Deutschland
Vorfall	Die prorussische Hackergruppe NoName057(16) hat das Bundesamt für Logistik und Mobilität und das Bundesministerium des Innern und für Heimat am 11. Juni 2024 in Form einer DDos-Attacke angegriffen. Sie nennen den Besuch des ukrainischen Präsidenten in Deutschland als Grund.
Täter	NoName057(16)
Quellen	11.06.2024:

30.01.2025	Metronom	DE	Webseite wegen DDoS-Angriff mehrere Tage nicht erreichbar. » Details
30.01.2025	enno	DE	Webseite nach DDoS-Angriff tagelang nicht erreichbar. » Details
30.01.2025	erixx	DE	Webseite nach DDoS-Attacke tagelang nicht erreichbar. » Details
30.01.2025	erixx Holstein	DE	DDoS-Angriff legt Webseite tagelang lahm. » Details
17.12.2024	Carl Walther GmbH	DE	Waffenhersteller fällt DDoS-Angriff zum Opfer. » Details
17.12.2024	Vattenfall	DE	Pressebereich von DDoS-Attacke betroffen. » Details
17.12.2024	Bundesinnenministerium (BMI)	DE	Massiver DDoS-Angriff legt Webseite des Innenministeriums lahm. » Details
22.11.2024	Bundesnachrichtendienst (BND)	DE	Webseite von deutscher Sicherheitsbehörde Ziel von DDoS-Angriff. » Details
22.11.2024	Bundeskriminalamt (BKA)	DE	Polizeibehörde des Bundes Ziel von DDoS-Attacke. » Details
22.11.2024	Bundesamt für Verfassungsschutz	DE	Webseite der deutschen Verfassungshüter von DDoS-Attacke heimgesucht. » Details

Details zum Sicherheitsvorfall ×

DDoS Ausfall

Betr. (Unternehmen)	enno
Datum (Veröffent.)	31.01.2025
Land	Deutschland
Vorfall	Aufgrund eines DDoS-Antrags war die Webseite der norddeutschen Eisenbahngesellschaft enno vom 27. bis 30. Januar 2025 teilweise nicht erreichbar. Zugreisende mussten auf Informations-Apps anderer Anbieter ausweichen. Auch erixx, erixx Holstein und Metronom waren Opfer des Angriffs, da diese Unternehmen denselben Server nutzen. Am 31. Januar 2025 meldete enno, dass die Webseite wieder normal erreichbar sei.
Quellen	30.01.2025: Heise Online 30.01.2025: Hamburger Abendblatt 31.01.2025: Seevetal Aktuell

Home > Cyberangriffe

DDOS-ATTACKE

Netzwerkangriff auf IT-Dienstleister der Energieversorgung Filstal

Die Energieversorgung Filstal (EVF) ist von einer DDoS-Attacke auf deren IT-Dienstleister imos betroffen.

Home > Cyberangriffe

TECHNISCHE AUSFÄLLE

Hackerangriff auf Trinkwasserverband Stade

Hacker haben die IT-Systeme des Trinkwasserverbands Stader Land (TWV) lahmgelegt. Die

Städtisches Portal dortmund.de derzeit nicht erreichbar - Server sind Ziel eines Überlastungsversuchs

Do 12. Oktober 2023
18:00 Uhr

Seit Donnerstag, 12. Oktober, 8:30 Uhr, läuft ein Überlastungsversuch auf das städtische Internetportal dortmund.de. Die wichtigsten Services und Dienstleistungen der Stadt Dortmund sind derzeit unter rathaus.dortmund.de verfügbar.

Es handelt sich um einen sogenannten dDOS-Angriff: Durch massenhafte Anfragen wurden die Server vollkommen überlastet. Seitdem ist dortmund.de für die Bürger*innen weitestgehend nicht mehr erreichbar. Der Hosting-Anbieter der Stadt Dortmund arbeitet mit externen Experten an Gegenmaßnahmen. Städtische Daten und die IT der Stadtverwaltung sind nicht betroffen.

KEINE GEFAHR FÜR DEN MITTELSTAND?

Weit gefehlt!

- Cyber Incidents größtes Risiko für KMUs
- Lücke beim Sicherheitsniveau wächst
- Attacken werden schnell größer UND komplexer
- Es wird gezielt nach niedrigeren Schutzniveaus gesucht.

Die durchschnittlichen **Kosten** für **KMUs** bei einer DDoS Attacke liegen bei **~120T€**!

Laut Allianz Risk Barometer sind Cyber Incidents das #1 Risiko für KMUs (33%)

Die Lücke bei der Resilienz gegenüber Cyberangriffen zwischen großen Unternehmen und KMUs wächst weiter.

Zuverlässigen Schutz gewähren nur noch Lösungen, die mit dem Grad der Bedrohung wachsen

Zunehmende Nutzung von KI und Bots ermöglichen es, Schwachstellen vor dem Angriff zu finden und gezielt anzugreifen

Umso niedriger das Schutzniveau, umso wahrscheinlicher ist ein Angriff und umso häufiger sind die Angriffe.

Quellen: VEKO Online – DDoS-Angriff kann Unternehmen Millionen kosten (veko-online.de)
ALLIANZ RISK BAROMETER 2024

LINK11 EUROPEAN CYBER REPORT 2025

Das DDoS Risiko ist realer denn je

+137% Gesamtanzahl Attacken im Link11 Netzwerk 2024 vs. 2023

Multi-Vektor-Angriffe

Kombination aus Layer 3/4 und Layer 7 über 4 Tage, 145 Mio. Requests **wechselnde Angriffsmuster**

Von Gigabit zu Terabit

Der größte im Link11-Netzwerk gemessene Angriff erreichte mit **1,4 Tbit/s** in Europa eine neue Dimension.

Komplexität und Geschwindigkeit

Die Angriffe sind **schneller und kürzer**, 65% der Angriffe erreichen ihr Maximum innerhalb von 10 bis 60s.

https://www.link11.com/de/download/european-cyber-report-2025/

DIE HOLY LEAGUE – EINE NEUE BEDROHUNG

- Neue Hacker Allianz aus >70 einzelnen Gruppen
- Koordinierte Angriffe gegen „den Westen“
- religiöse Rhetorik und politische Propaganda zur Rekrutierung
- Extrem organisiertes und koordiniertes Vorgehen

Ziel:

Destabilisierung westlicher Länder

Konkretes dazu:

- „Cyberwar“ Kriegserklärung gegen Frankreich am 06.12.2024
- Vendetta gegen Spanien nach Verhaftung von Hacktivisten
- Koordination einzelner Gruppen und Aufteilung der Ziele:
  - *NoName057* und *People’s Cyber Army* greifen größte Städte und die größten KRITIS Unternehmen Frankreichs an(z.B. AXA)
  - *Mr Hamza* greift Regierungsstellen an (Außenministerium, Cybersecurity Agency, Nuklear Energie Behörde)
  - *Z-Pentest* attackiert den Mittelstand, Energie-, Automobil- und Hotellerie Unternehmen

Fazit: >50 DDoS Attacken, 50 teilweise sensible Dokumente und >100GB an Daten der französischen Regierung erbeutet. In nur 4 Tagen konzentrierter Aktivität!

https://www.link11.com/de/download/european-cyber-report-2025/
Russian And Palestinian Hacktivists Uniting Against France

„…so ernst die Lage ist, sie ist nicht verzweifelt, sie ist nicht hoffnungslos.“

FALLBEISPIEL

STADT DORTMUND

Das Projekt

- Relaunch der Online Services und der Dortmund App am 19.Oktober 2023
- 500 Dienstleistungen & 200 Anträ oder Services online verfügbar
- Rund 45.000 Unterseiten
- Über 3 Millionen monatliche Aufrufe
- aktive Arbeit zur Umsetzung dauerte 14 Monate.

DIE LÖSUNG

Ein Anruf bei Link11 / Ihrem Dienstleister

- Notfall-Onboarding, durch den Dienstleister begleitet
  - Kurzfristiges Meeting und Einrichtung der Proxy Umleitung
    - Schutz der Systeme, Abwehr der Angriffe
      - Systeme online

✓

      - Go Live

Welche Systeme sind zum Einsatz gekommen?

Zum Schutz der Web Applikation (Website) vor DDoS Angriffen

Zum Schutz der Web Applikation (Website) vor Zero Day und anderen Attacken (nach OWASP-10)

- **Einfaches Onboarding und Flexibilität**
- **Automatisierte & zuverlässige Angriffsabwehr**
- **Multi TB Kapazität, niedrige Latenzen, Triple SLAs**
- **Persönlicher Kundenservice DE+EN 24/7**
- **100% DSGVO-konform**

VERFÜGBARKEIT SICHERSTELLEN

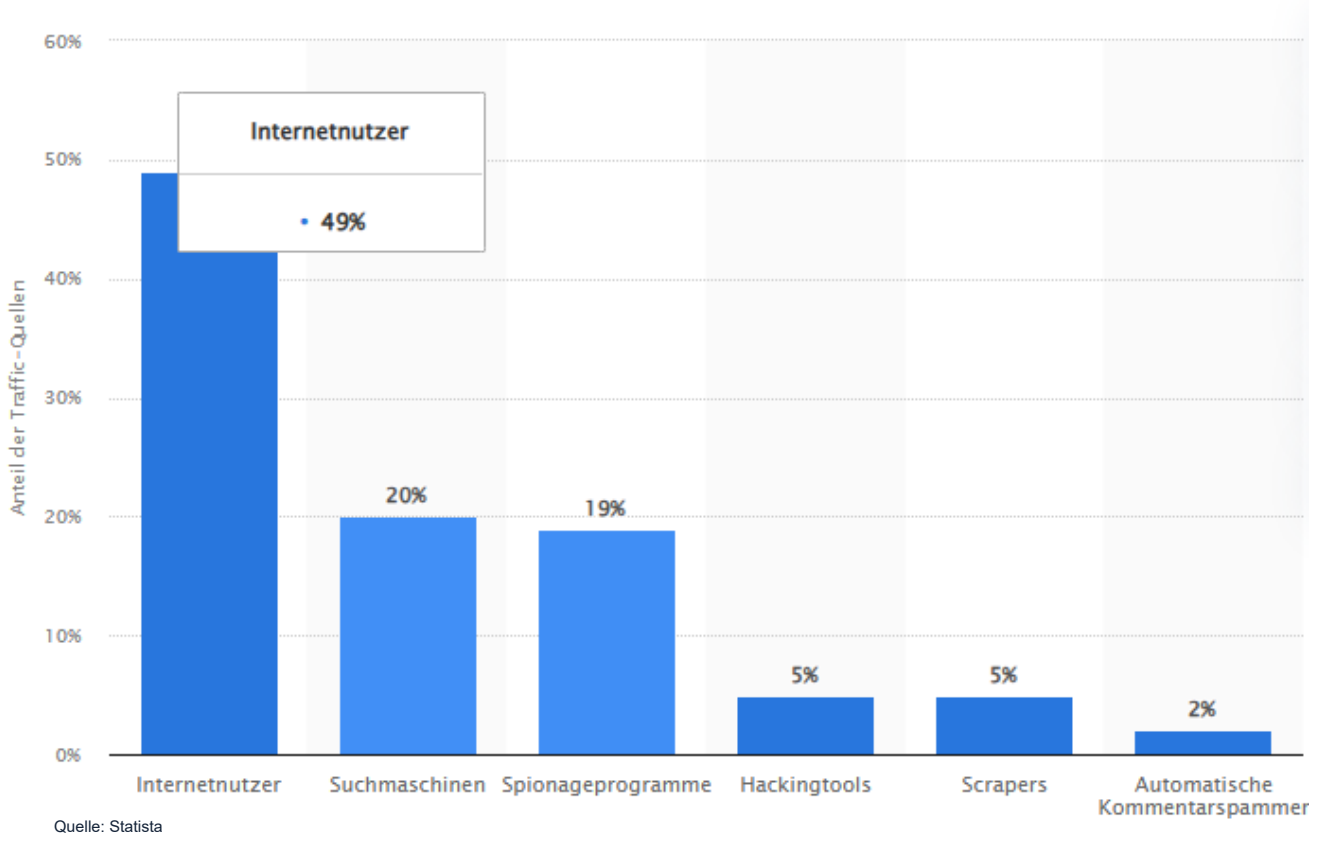
Was muss geschützt werden?

- Ihre digitalen Assets (Homepage, Onlineshop, API´s, VPN, etc.)

Sind es wirklich „nur“ DDoS Angriffe?

- BOTs und Scraper erzeugen heute mehr als 50% des Traffics!
- Zero-Day-Lücken
- Account Takeover
- SQL-Injections
- …

Unsere Aufgabe ist es, die Verfügbarkeit von Unternehmen im Netz sicherzustellen,
um dadurch Ihre Investitionen in die Digitalisierung zu schützen.



Quelle: Statista

DATENSCHUTZ UND COMPLIANCE

- EU-US Datenschutzrahmen wackelt: Nach *Safe Harbor* und *Privacy Shield* steht nun auch das *DPF* auf der Kippe.
- „zunehmende Kontrolle von Regierungsdatenbanken durch das neue Department of Government Efficiency (DOGE) unter Leitung von Elon Musk…“
- Compliance Richtlinien der EU müssen umgesetzt werden (DORA, NIS-2, CRA, KI-Verordnung, KRITIS, Ad-hoc Meldepflichten…)

Wissen Sie, was mit Ihren Daten und denen Ihrer Kunden passiert?

Und: Wissen Ihre Kunden das auch?

„Europäische Unternehmen, die auf US-Cloud-Dienste setzen, müssen sich auf massive Rechtsunsicherheiten einstellen.“

Quellen: https://www.ferner-alsdorf.de/eu-us-data-privacy-framework-wankt-wie-trumps-politik-europaeische-unternehmen-bedroht/

Transparenz bei Datenspeicherung & -verarbeitung Ihrer Partner, Geoblocking, Geofencing und Captcha Kontrolle können helfen Compliance Vorgaben zu erfüllen.

FALLBEISPIEL

MITTELSTAND & COMPLIANCE

Mittelständischer Batteriehersteller aus Süddeutschland erleidet Cyber-Angriff.

Folgen:

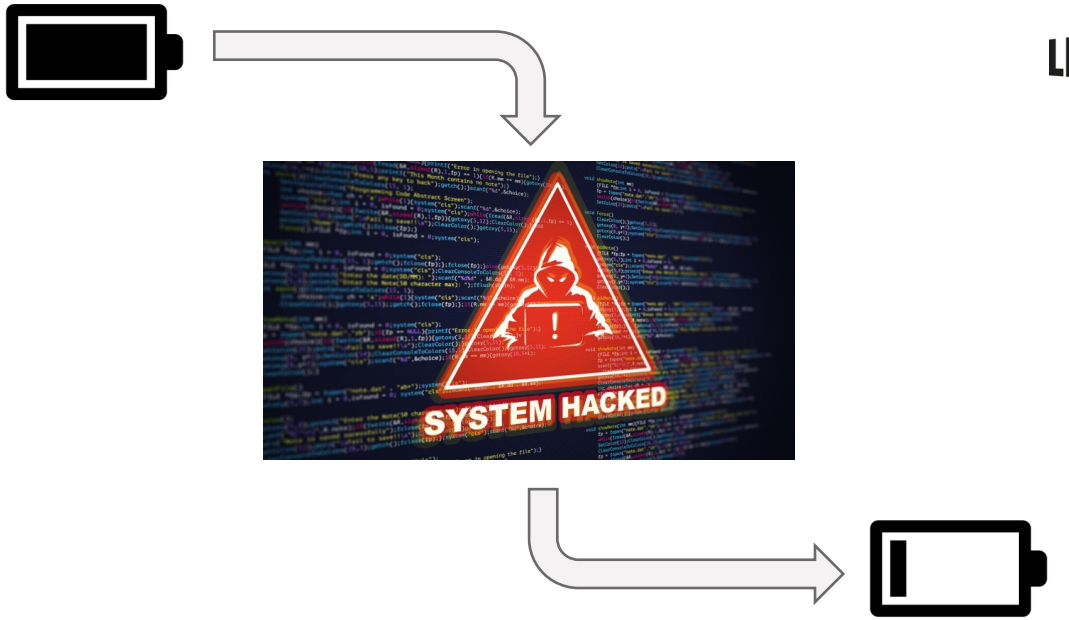
- Produktion (5 Standorte) wochenlang gestoppt
- Aktienkurs um 90% gefallen
- Finanzielle Lage verschlechtert → Restrukturierungs-Verfahren
- Rettung nur durch neue Kapitalbeteiligungen

Folgeangriffe verhindern Ad-hoc Meldungen & Veröffentlichungen über die Websites

→ Unternehmen riskiert zusätzliche BaFin Bußgelder.

Link11 stellt Verfügbarkeit der Websites sicher!

Compliance Anforderungen werden erfüllt.



Ellwangen, ISIN:

Publication of inside information pursuant to Article 17 of Regulation (EU) No 596/2014

affected by cyber attack

Ellwangen, February 13th 2024

Last night, February 12th 2024, the was the target of a cyber attack on parts of its IT systems. This affects the five production plants and the administration. The IT systems and thus also production were proactively shut down temporarily for security reasons and disconnected from the internet. The IT systems and the extent of the impact are currently being reviewed. The utmost care is being taken to ensure data integrity.

The extent of the actual damage cannot be determined at this time.

In accordance with the emergency plan for such situations, the necessary precautionary measures were implemented immediately. Additionally, a task force was set up instantly to restore normal operations as quickly as possible and deal with the incident with the support of cyber security experts and data forensics specialists.

* * *

Aufgabe der Unternehmen ist es nicht, den Schutz aufzubauen, sondern den/die richtigen Anbieter auszuwählen!

VERTRAUEN SIE DEN EXPERTEN

Das **BSI** zur Prävention/Abwehr von DDoS Angriffen:

- **Einsatz** gezielter **DDoS-Abwehrsysteme**.
- **Verlagerung** besonders bedrohter Systeme **zu Drittanbietern**
- **Frühzeitige Einbindung** Internet-Service-Provider (ISP) bzw. **Hosting-Provider**
- **DDoS-Mitigation-Services bei Providern nutzen**

Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/DDoS/ddos_node.html

Laut **DSGVO** ist der Cloud-Anbieter der Auftragsverarbeiter (Art. 4. Nr. 8 DSGVO) und der **Cloud-Anwender der Verantwortliche.**

Quelle: https://www.datenschutzexperte.de/blog/datenschutz-im-unternehmen/datenschutz-und-sicherheit-bei-cloud-anbietern/

Ohne Angemessenheitsbeschluss (für USA das DPF) gilt:

Die **Ausnahmen** des Art. 49 DSGVO sind eng auszulegen und dürfen nach den Leitlinien des Europäischen Datenschutzausschusses **nicht für regelmäßige Datentransfers** verwendet werden, die eine Vielzahl von Personen betreffen.

Quelle: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Internationaler_Datentransfer.html

Der **BfDI:**

Bei allen Gegenmaßnahmen **muss** der Schutz der Vertraulichkeit der übermittelten Informationen und **der Datenschutz** der Nutzerinnen und (…) **gewährleistet bleiben**.

Quelle:https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/21TB_05_06.pdf?__blob=publicationFile&v=6

Jetzt Sie!
Fragen?

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

GLASFASER RUHR

LINK 11

WE PROTECT BETTER

KI GESTÜTZTE ANGRIFFE STEIGERN DAS RISIKO

Einfach verfügbar für jedermann DDoS-as-a-Service

Schon ab 10$ online verfügbar
Einfach und teilweise voll automatisiert
Geschäftsmodell stärkt den Angriffsmarkt

Erhöhte Angriffsgeschwindigkeit und Komplexität

Multi-Vektor-Attacken und Kombination der Angriffe
Angriffstechniken werden in Echtzeit angepasst
Geschwindigkeit wächst rasant weiter

Schrumpfende Budgets und Fachkräftemangel

Fachkräftemangel bei Cyber-Security Experten
Neue Richtlinien erschweren schnelle Reaktionen
IT-Budgets schrumpfen, Cyber-Security ist kein IT-Thema

Schwerwiegende Folgen und hohe Anforderungen

Erhöhte Anforderungen an Abwehrmaßnahmen
Gezielte Schwachstellen-Erkennung
Deepfakes und Social-Engineering

CLOUD, KI & ML IN DER ABWEHR

First-Line-of-Defense in der Cloud

Vorgelagerter Schutz verringert Risiken
Skalierbarkeit und Flexibilität in der Cloud
On-Demand Ressourcen und Wegfall eigener Hardware

AAA – Automatisiert, Always-on, Aktuell

Präzise und schnelle Erkennung durch ML (TTM!)
Reduktion menschlicher Fehler und Entlastung
Erkennung und Analyse neuer Angriffsmuster

Kostenreduktion und Effizienzsteigerung

Pay-per-Use-Modelle der Cloud bieten Flexibilität und Kosteneffizienz
KI in der Erkennung spart Zeit und senkt Kosten

Incident Response und verbesserte Compliance

Hoher Datenschutz durch Wahl passender Partner
Daten in der Cloud sicher und schnell verfügbar
Schnelle und präzise Reaktion auf Vorfälle