secure soc

FORSCHUNGSBERICHT

DEUTSCH / SEPTEMBER 2026

Vergleichender Mapping-Bericht.

TEIL 01

WP2 – SECURESOC

02. September 2026

secure soc

Sozialpartner für Resilienz und Sicherheit
Kritische Infrastrukturen schützen, das Bewusstsein für Cybersicherheit stärken und Desinformation durch sozialen Dialog bekämpfen.

securesoc.oegb.at

Verfasst von **VÖWG und ÖGB**
Veröffentlichungsdatum: September 2026

ÖGB
Österreichischer Gewerkschaftsbund
Johann-Böhm-Platz 1
1020 Wien, Österreich
www.oegb.at

VÖWG
Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs
Stadiongasse 6–8
1010 Wien, Österreich
voewg.at

ÖGB VÖWG

Co-funded by the European Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen der Autorinnen und Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Generaldirektion Beschäftigung, Soziales und Integration wider. Weder die Europäische Union noch die Bewilligungsbehörde können dafür verantwortlich gemacht werden.

IN DIESEM BERICHT

Inhalt

01 EU-Cybersicherheitsstrategie 4

02 Desinformation am Arbeitsplatz 22

03 Operatives Glossar – Terminologie für Infoboxen 34

↳ Anmerkungen 41

01 / BERICHT

EU-Cybersicherheitsstrategie

DIE EU-CYBERSICHERHEITSSTRATEGIE

Cybersicherheit wird in dem *EU Rechtsakt zur Cybersicherheit* (EU-VO 2019/881) als „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen" definiert. Diese Definition wird von der *NIS-2-Richtlinie* (EU) 2022/2555) dahingehend präzisiert, dass die Sicherheit von Netz- und Informationssystemen die Fähigkeit ist, Ereignisse abzuwehren, welche die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der verarbeiteten Daten oder der über diese Systeme angebotenen Dienste beeinträchtigen könnten.

Um ebendiese Sicherheit gewährleisten zu können, schafft die *EU-Cybersicherheitsstrategie für die digitale Dekade* den strategisch-politischen Rahmen für „ein globales, offenes, freies und sicheres Internet" (Europäische Kommission, 2020). Die 2020 veröffentlichte, und seitdem kontinuierlich verbesserte, Strategie gliedert sich systematisch in drei wesentliche Handlungsbereiche:

- Resilienz, technologische Souveränität und Führungsrolle,
- Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion,
- Förderung eines globalen, offenen Cyberraums (Europäische Kommission, 2020).

Im Folgenden werden die drei Säulen der EU-Cybersicherheitsstrategie ausführlicher erläutert und Case Studies zu Cyberattacken in der EU aufgerollt, um die Entstehung der Cybersicherheitsstrategie besser nachvollziehen zu können.

Resilienz, technologische Souveränität und Führungsrolle

Diese Säule beschäftigt sich damit die Abwehrfähigkeit der Union durch den Schutz kritischer Infrastrukturen, die Sicherung der technologischen Lieferketten und die Förderung europäischer Eigenständigkeit bei Schlüsseltechnologien zu stärken (Europäische Kommission, 2020). Hier wird vor allem mit normativen Mitteln gearbeitet. Der EU kommt hier laut *WEF-Outlook 2026*[1] eine besondere Relevanz zu, da 78% der befragten CISOs[2] angeben, dass Unterschiede zwischen Rechtssystemen die Umsetzung von Sicherheitsmaßnahmen erschweren und eine harmonisierte Rechtsordnung zur Stabilität beitragen würde (World Economic Forum, 2026).

Um resiliente Infrastrukturen und kritische Dienste zu stärken, sieht die *EU-Cybersicherheitsstrategie* die Überarbeitung der ursprünglichen NIS-Richtlinie sowie die Schaffung eines neuen Rahmens für die physische Resilienz vor (Europäische Kommission, 2020). In weiterer Folge wurden im Rahmen der Strategie die Schwesterrichtlinien[3] *NIS-2-Richtlinie* und *CER-Richtlinie* am 14. Dezember 2022 verabschiedet. Die *NIS-2-Richtlinie*, die *CER-Richtlinie* und die *DORA-Verordnung* bilden gemeinsam das regulatorische Fundament für die Sicherheit lebenswichtiger Sektoren.

Die *NIS-2-Richtlinie* soll das gemeinsame Cybersicherheitsniveau in der gesamten EU regulieren und das Funktionieren des Binnenmarkts verbessern (Richtlinie (EU) 2022/2555, 2022). Die Richtlinie gilt für öffentliche und private Unternehmen, die mindestens 50 Mitarbeiter beschäftigen und/oder über 10 Mio. € Umsatz bzw. Jahresbilanz erwirtschaften und in einem Sektor von hoher Kritikalität[4] oder anderen kritischen Sektoren[5] tätig sind. Diese Einrichtungen werden verpflichtet, Risikomanagementmaßnahmen zu ergreifen, welche laut Artikel 21 u.a. ein Konzept zur Risikoanalyse, die Bewältigung von Sicherheitsvorfällen und die Lieferkettensicherheit vorsehen.

Mit der *NIS-2-Richtlinie* werden auch mehrstufige Berichtspflichten für erhebliche Sicherheitsvorfällen[6] eingeführt. Die frühe Warnung soll als Erstmeldung innerhalb von 24 Stunden dem zuständigen CSIRT[7] vorgelegt werden, worauf innerhalb von 72 Stunden die Incident-Meldung folgen muss, welche eine detailliertere Beschreibung enthält. Schlussendlich soll binnen eines Monats der Abschlussbericht mit Ursachenanalyse und ergriffenen Abhilfemaßnahmen präsentiert werden. Laut *NISG*[8], melden Betreiber an ihr sektorspezifisches *CERT*[9] oder an das nationale *CERT*[10], welche die Meldung an das Bundesministerium für Inneres weiterleiten (Republik Österreich, 2026).

Ein entscheidender Punkt der neuen Richtlinie ist die persönliche Haftung der Führungskräfte für Verstöße gegen Risikomanagement- oder Berichtspflichten sowie die Verpflichtung zu regelmäßigen Schulungen für Mitglieder der Leitungsorgane (Richtlinie (EU) 2022/2555, 2022). Diese Maßnahmen werden für wesentliche Einrichtungen im Rahmen einer Ex-ante- und Ex-post-Aufsicht überwacht, während wichtige Einrichtung lediglich einer reaktiven Ex-post-Aufsicht unterliegen. Dabei können Behörden bei Verstößen Geldbußen von bis zu 10 Mio. € oder 2% des weltweiten Vorjahresumsatzes verhängen sowie das vorübergehende Verbot der Ausübung von Leitungsaufgaben für Führungskräfte aussprechen.

Die *CER-Richtlinie* (Richtlinie (EU) 2022/2557, 2022) fokussiert sich auf die physische Widerstandsfähigkeit kritischer Einrichtungen und ergänzt dadurch die *NIS-2-Richlinie*. Die *CER-Richtlinie* soll die Resilienz stärken und dadurch sicherstellen, dass kritische Infrastruktur, also Dienste, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten im Binnenmarkt unerlässlich sind, ungehindert erbracht werden können. Diese Resilienz wird in der *CER-Richtlinie* als „die Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen“ definiert (Richtlinie (EU) 2022/2557, 2022). Die Mitgliedstaaten werden durch diesen Rechtsakt verpflichtet, einen nationalen Rahmen zu schaffen, um die Resilienz zu gewährleisten. Dazu gehört eine nationale Strategie, welche Verbesserungen der Resilienz kritischer Einrichtungen vorsieht. In Österreich ist dies die „Österreichische Strategie für die Resilienz kritischer Einrichtungen (ÖSRKE 2026)“, die durch das *Resilienz kritischer Einrichtungen-Gesetz* (RKEG) umgesetzt wurde. Zusätzlich muss eine regelmäßige Risikobewertung und Identifizierung kritischer Einrichtungen erfolgen, sodass Staaten diese Einrichtungen durch Leitfäden, Übungen, Schulungen und gegebenenfalls Finanzmittel unterstützen können (Richtlinie (EU) 2022/2557, 2022).

Die 2022 verabschiedete *DORA-Verordnung* ist ein Baustein der europäischen Cybersicherheitsstrategie, der speziell auf den Finanzsektor zugeschnitten ist (Verordnung (EU) 2022/2554, 2022). Diese Verordnung soll die digitale operationale Resilienz von Finanzunternehmen[11] und IKT (Informations- und Kommunikationstechnologie) -

Drittdienstleistern[12] stärken; dies bedeutet, dass sie Bedrohungen wie Cyberangriffen oder Systemausfällen widerstehen, darauf reagieren und sich davon erholen können. Dies soll durch IKT-Risikomanagement mittels Identifizierung, Bewertung und Behandlung von Risiken, die durch die Nutzung von Netz- und Informationssystemen entstehen können, erreicht werden. Dazu gehören die Meldung von IKT-Vorfällen an die Finanzaufsichtsbehörde, Tests der digitalen Resilienz (darunter alle drei Jahre fortgeschrittene, bedrohungsorientierte Penetrationstests), Mindestvorgaben und Überwachung kritischer IKT-Drittdienstleister durch europäische Aufsichtsbehörden sowie der freiwillige Informationsaustausch unter Finanzunternehmen.

Ein weiterer Bereich der europäischen Cybersicherheitsstrategie ist die Sicherheit des „Internets der Dinge“ (IoT[13]), bei der insbesondere die Prinzipien „Security-by-Design“ und „Security-by-Default“ etablieren werden sollen, um unsicheren Geräte als Einfallstor für Cyberangriffe vorzubeugen (Verordnung (EU) 2024/2847, 2024). Diese Prinzipien werden durch den *Cyber Security Act* und den *Cyber Resilience Act* rechtlich verankert.

Der *Cyber Security Act* (CSA; Rechtsakt zur Cybersicherheit) (Verordnung (EU) 2019/881, 2019) wurde 2019 verabschiedet und verleiht der Cybersicherheitsagentur ENISA ein dauerhaftes Mandat als zentrales Kompetenzzentrum und als Referenzpunkt für Beratung und Sachkenntnis in der Union. Der Rechtsakt etabliert den Europäischen Rahmen für Cybersicherheitszertifizierung (ECCF), welcher einen unionsweiten Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen schafft und so der Fragmentierung des Binnenmarkts entgegenwirkt. Dabei werden die Vertrauenswürdigkeitsstufen „basic“, „substantial“ und „high“ von der ENISA[14], beraten von der Europäischen Gruppe für die Cybersicherheitszertifizierung (bestehend aus nationalen Behörden), ausgestellt. Dies soll das Vertrauen in digitale Lösungen stärken und unionsweit einheitliche Standards schaffen.

Der *Cyber Resilience Act* (CRA; Rechtsakt zur Cyberresilienz) (Verordnung (EU) 2024/2847, 2024) wurde 2024 beschlossen und soll bis Dezember 2027 schrittweise in Kraft treten. Der Hersteller muss im Rahmen der Verordnung sicherstellen, dass Produkte bereits während der Planung und Entwicklung sicher konzipiert werden („Security-by-Design“), sie mit einer sicheren Standardkonfiguration ausstatten („Security-by-Default“) und über den gesamten Unterstützungszeitraum (orientiert an der voraussichtlichen Nutzungsdauer) Sicherheitsaktualisierungen bereitstellen. Bei Standalone-Software präzisiert der Leitfaden der Kommission, dass das Inverkehrbringen bereits dann erfolgt, wenn die Entwicklungsphase abgeschlossen ist und das Produkt erstmals zum Download oder zur Nutzung angeboten wird (Europäische Kommission, 2026). Ein entscheidender Zusatz ist hierbei die Einbeziehung von Datenfernverarbeitungslösungen (RDPS), das heißt, dass cloud-Backends rechtlich als Teil des Produkts gelten, wenn sie für dessen Funktionsfähigkeit notwendig sind und unter der Verantwortung des Herstellers entwickelt wurden.

Im *CRA* ist die Produktklassifizierung in „wichtige Produkte“ (Klasse I und II), welche strengeren Konformitätsprüfungen unterliegen, und „kritische Produkte“ (Anhang IV), die eine verpflichtende europäische Zertifizierung benötigen können, verankert. Ein Produkt, das nach einem geeignetem CSA-Schema zertifiziert wurde, erfüllt automatisch die entsprechenden Anforderungen des CRA („Konformitätsvermutung“) (Verordnung (EU) 2024/2847, 2024). Nachträgliche Änderungen gelten als „wesentlich“, wenn sie das Risikoprofil oder die

Zweckbestimmung des Produkts verändern, was eine neue Konformitätsbewertung erforderlich macht (Europäische Kommission, 2026). Reine Sicherheitsupdates zur Behebung von Schwachstellen werden hingegen im Regelfall nicht als wesentliche Änderung eingestuft.

Teil der ersten Säule ist ebenfalls der Aufbau technologischer Souveränität und Kapazität, und ein Beispiel hierfür ist das Projekt DNS4EU. Um die Abhängigkeit von wenigen großen Unternehmen außerhalb der EU zu verringern, versucht die Initiative DNS4EU, einen eigenen öffentlichen europäischen DNS-Auflösungsdienst[15] als Alternative zu schaffen (Europäische Kommission, 2020). Der Dienst wird so konzipiert, dass er höchste Sicherheits- und Datenschutznormen einhält und den Grundsätzen des konzeptionsbedingten Datenschutzes (Privacy by Design) entspricht.

Um den Status der Cybersicherheit einzelner Mitgliedstaaten sowie der gesamten EU zu beschreiben, wird gem. *Art 18 der NIS-2-Richtlinie* eine quantitative und qualitative Bewertung von der ENISA durchgeführt und in dem EU Cybersecurity Index (EU-CSI) veröffentlicht (ENISA, 2025). Der Index misst zahlreiche spezifische Indikatoren und Messgrößen (z.B. Vorfallsraten, Investitionen, Forschung, Nutzerverhalten) auf einer Skala von 0 bis 100, die in die Hauptbereichen („Policy“[16], „Capacity“[17], „Operations“[18] und „Market/Industry“[19]) zusammengefasst werden, um so multidimensionale Konzepte quantifizierbar zu machen.

Die Domäne „Policy“ bewertet quantitativ und qualitativ, wie weit die Mitgliedstaaten bei der Schaffung politischer und rechtlicher Grundlagen für die Cybersicherheit sind (ENISA, 2025). Im Jahr 2024 ist „Policy“ mit einem EU-Durchschnitt von 66,09 Punkten der am höchsten bewertete Bereich des gesamten Index. Es bestehen jedoch große Unterschiede zwischen den Mitgliedstaaten in diesem Bereich, was bedeutet, dass die normativen Werkzeuge existieren, aber die Umsetzungstiefe stark variiert.

2. Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion

Die zweite Säule fokussiert sich darauf, die Mitgliedstaaten dabei zu unterstützen, ihre Bürger und Bürgerinnen sowie wirtschaftliche und nationale Sicherheitsinteressen durch eine verstärkte operative Zusammenarbeit und die Mobilisierung technischer Instrumente zu verteidigen (Europäische Kommission, 2020). Im WEF-Report 2026 wird die Relevanz dieser Maßnahmen durch die Statistik bestätigt, die besagt, dass nur 45% der CEOs im Privatsektor zuversichtlich sind, dass ihr Land angemessen auf Cyberangriffe gegen kritische Infrastrukturen reagieren könnte (World Economic Forum, 2026).

Hierbei wird auf eine Kombination aus institutionellen Plattformen, wie der Joint Cyber Unit und der ENISA, spezialisierten Netzwerken, wie dem CSIRT-Netzwerk, EU-CyCLONe und der NIS-Koordinationsgruppe sowie operativen Werkzeugen des Cyber Solidarity Acts gesetzt („CSoA“) (Europäische Kommission, 2020; Richtlinie (EU) 2022/2555, 2022; Verordnung (EU) 2025/38, 2025).

Die Joint Cyber Unit („JCU“) wurde im Rahmen der EU-Cybersicherheitsstrategie als Plattform konzipiert, welche die bisher oft getrennt agierenden Fachkreise in einem gemeinsamen Raum zusammenführt (Europäische Kommission, 2020). Dazu gehören die NIS-Behörden (inklusive der spezialisierten Netzwerke) auf ziviler Ebene, Strafverfolgungsbehörden, wie Europol/EC3[20], die Diplomatie[21] und die Cyberabwehr. Durch die Zusammenarbeit dieser Gemeinschaften kann das Potenzial der gegenseitigen operativen Unterstützung besser ausgeschöpft, und somit ein

gemeinsames Lagebild sowie eine koordinierte Reaktion und Wiederherstellung effizienter gewährleistet werden. Die JCU ist jedoch keine neue, eigenständige Behörde, sondern fungiert als „Rückfallebene“, an der diese Akteure zusammenkommen, um sich gegenseitig mit Fachwissen zu unterstützen.

Ein wichtiger Stakeholder in der JCU ist die ENISA (Europäische Kommission, 2020). Die Agentur fungiert als das zentrale Kompetenzzentrum für Cybersicherheit in der EU und ist der primäre Bezugspunkt für Beratung und Sachkenntnis für die Mitgliedstaaten und EU-Organe (ENISA, 2026). Die ENISA ist zwar im *Cybersecurity Act* verankert, jedoch wird im geplanten *Cybersecurity Act 2* weiter zum „Single Point of Expertise“ erklärt, der auch Aufgaben aus der *NIS-2-Richtlinie*, dem *Cyber Resilience Act* (CRA) und dem *Cyber Solidarity Act* (CSoA) bündelt (Europäische Kommission, 2026). Zurzeit unterstützt die ENISA aktiv die NIS-Koordinationsgruppe und koordiniert das CSIRTs-Netzwerk sowie EU-CyCLONe (Richtlinie (EU) 2022/2555, 2022).

Die NIS-Koordinationsgruppe besteht aus Vertretern der Mitgliedstaaten der EU, der Kommission und der ENISA[22] (Richtlinie (EU) 2022/2555, 2022). Zusammen wird ein zweijähriges Arbeitsprogramm und eine Orientierungshilfe zur Umsetzung der NIS-2-Richtlinie erstellt, zudem werden Unions-Risikobewertungen für kritische Lieferketten durchgeführt sowie ein Austausch über bewährte Verfahren zum Risikomanagement und zu Meldepflichten gepflegt.

Das CSIRTs-Netzwerk setzt sich aus den nationalen Computer-Notfallteams (CSIRTs) der Mitgliedstaaten und dem CERT-EU zusammen[23] (Richtlinie (EU) 2022/2555, 2022). Durch den technischen Informationsaustausch über Sicherheitsvorfälle, Cyberbedrohungen und Schwachstellen können koordinierte Reaktionen auf Vorfälle, die mehrere Mitgliedstaaten betreffen, effektiver umgesetzt werden. Dies geschieht insbesondere auch durch die Zusammenarbeit mit den Cyber-Hubs des europäischen Cybersicherheits-Warnsystems. Die ENISA führt hierbei die Sekretariatsgeschäfte, welche administrative, technische und finanzielle Unterstützung umfassen.

Das Netzwerk EU-CyCLONe ist speziell für das koordinierte Management von großflächigen Cybersicherheitsvorfällen und -krisen auf operativer Ebene zuständig und besteht aus Vertretern der Behörden der Mitgliedstaaten für das Cyberkrisenmanagement sowie der Kommission (Richtlinie (EU) 2022/2555, 2022). Es ist das Bindeglied zwischen der technischen Ebene (CSIRTs) und der politischen Ebene der EU, und entwickelt dementsprechend europäische Lagebilder, Folgenabschätzung und unterstützt die Entscheidungsfindung auf politischer Ebene. Die ENISA führt hierbei die Sekretariatsgeschäfte.

Die ENISA ist ebenfalls verantwortlich für „Cyber Europe“, eine seit dem Jahr 2010 bestehende Serie großangelegter, grenzüberschreitender Cyberübungen (Bundesministerium für Inneres, 2025). Im Zweijahresrhythmus werden komplexe Cybersicherheitsvorfälle, die sich im Verlauf zu großflächigen Cyberkrisen entwickeln können, simuliert, um die technische und operative Abwehrbereitschaft der Union zu testen sowie die Zusammenarbeit zwischen den Mitgliedstaaten und EU-Institutionen zu evaluieren. Zum Beispiel versuchten im Jahr 2024 der fiktive Staat „Voltaros“ und vermeintlich staatlich gelenkte APT-Akteure, durch Cyberangriffe auf kritische Infrastrukturen das politische Machtgleichgewicht zu verschieben. Mit diesen Übungen wird der EU-Blueprint für das Cyberkrisenmanagement, also das gemeinsame europäische Handbuch für Notfälle, unter Realbedingungen erprobt und Lücken in den Standard Operating

Procedures (SOP) geschlossen (Bundesministerium für Inneres, 2026). Bei den Übungen sind der öffentliche Sektor (CSIRTs), der Privatsektor (Unternehmen aus kritischen Sektoren) und die EU vertreten (Bundesministerium für Inneres, 2025).

Der *Cyber Solidarity Act* („CSoA"; Verordnung (EU) 2025/38, 2025) liefert konkrete operative Werkzeuge und finanzielle Ressourcen, um den von der *NIS-2-Richtlinie* etablierten Handlungsrahmen zur Cybersicherheit handlungsfähig zu machen. In diesem Rechtsakt werden drei Instrumente festgelegt. Erstens, das europäische Cybersicherheits-Warnsystem, welches aus nationalen und grenzüberschreitenden Cyber-Hubs besteht, die hochmoderne Technologie nutzen, um Cyberbedrohungen in Echtzeit zu erkennen. Diese stehen im Kontakt mit dem CSIRTs-Netzwerk und EU-CyCLONe. Zweitens, der Cybernotfallmechanismus, welcher die EU-Cybersicherheitsreserve bereitstellt, einem Pool aus vertrauenswürdigen privaten Sicherheitsdienstleistern, die auf Antrag eines Mitgliedstaats oder eines EU-Organs sofort technische Hilfe bei der Reaktion und der anfänglichen Wiederherstellung nach einem massiven Angriff leisten. Diese Information werden an die JCU vermittelt, und auch das CSIRT-Netzwerk kann hier im Krisenfall um Unterstützung anfragen. Drittens, der europäische Überprüfungsmechanismen für Cybersicherheitsvorfälle[24], welcher auf Ersuchen der Kommission oder des Netzwerks EU-CyCLONe die Hauptursachen und gewonnenen Erkenntnisse ermitteln und umsetzen soll.

Im EU-Cybersecurity-Index misst die Domäne „Operations", wie effektiv technische und operative Maßnahmen in der Praxis umgesetzt werden, um auf Bedrohungen zu reagieren und die Widerstandsfähigkeit kritischer Systeme aufrechtzuerhalten (ENISA, 2025). Der EU-Durchschnitt von 57,63 Punkten ist relativ zum Skalenmaximum von 100 Punkten niedrig, da vier der fünf Indikatoren für diese Kategorie sehr niedrig ausfallen. Dies zeigt sich beispielsweise in der geringen Nutzung von KI-Technologien für die IKT-Sicherheit (Score: 3,18), den unzureichenden Cybersicherheitsinvestitionen wesentlicher Einrichtungen (Score: 7,14), dem Mangel an formellen CSIRT-Zertifizierungen (Score: 10,31) sowie die geringe Quote an Unternehmen, die systematische Risikoanalysen durchführen (Score: 32,01). Daraus lässt sich ableiten, dass die funktionale Verteidigungsbereitschaft unionsweit noch erhebliches Steigerungspotenzial aufweist.

3. Förderung eines globalen, offenen Cyberraums

Die dritte Säule fokussiert sich darauf, die europäische Vision eines globalen, freien und sicheren Internets weltweit zu verankern und die EU als führende globale Akteurin in der Cyberpolitik zu etablieren (Europäische Kommission, 2020). In diesem Kontext werden ein starkes diplomatisches Reaktions- und Abschreckungssystem, technologische Souveränität und internationale Standards und Normen gefördert.

Der WEF Global Security Outlook 2026 unterstreicht die besondere Relevanz dieses Bereichs. Der Anteil der Befragten, die wenig Vertrauen in die Fähigkeit ihres Landes haben, auf größere Cybervorfälle zu reagieren, ist von 26% in 2025 auf 31% im Jahr 2026 angestiegen (World Economic Forum, 2026). Dies zeigt, dass operative Handlungsfähigkeit nicht nur technisch von Bedeutung ist, sondern auch eine Frage des Vertrauens in staatliche Resilienz darstellt.

Die *EU Cyber Diplomacy Toolbox* („Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities") bildet seit 2017 einen Rahmen innerhalb der Gemeinsamen Außen- und Sicherheitspolitik („GASP"), um koordinierte diplomatische Antworten auf Cyberbedrohungen zu

ermöglichen (Council of the European Union, 2023). Dabei wird die Reaktion der EU an den Schweregrad des Vorfalls angepasst (Council of the European Union, 2023). Dies bedeutet, dass z.B. präventive und kooperative Maßnahmen, wie öffentliche Bewusstseinsbildung, diplomatischer Dialog, vertrauliche Demarchen oder vertrauensbildende Maßnahmen zur Vermeidung von Missverständnissen eingesetzt werden können (Bundesministerium für Inneres, 2024). Es können aber auch restriktive Maßnahmen (Sanktionen), wie das Einfrieren von Vermögenswerten, oder Einreiseverbote, verhängt werden. Die Nutzung der Toolbox muss sechs Prinzipien folgen: den Schutz der EU, ihrer Bürger und Mitgliedstaaten gewährleisten, die allgemeinen Außenbeziehungen zum betroffenen Staat berücksichtigen, die strategischen Ziele der EU-Außenpolitik erreichen, dem Umfang, der Komplexität und den Auswirkungen des Angriffs entsprechen sowie internationalen Rechtsnormen und die Menschenrechte einhalten (Council of the European Union, 2023).

Wenn die Befolgung der Prinzipien gewährleistet ist, kann die Toolbox in einem mehrstufigen Verfahren umgesetzt werden (Council of the European Union, 2023). Sobald eine Bedrohung erkannt wird, werden Informationen (oft durch das EU-INTCERN[25]) ausgetauscht und in Ratsgremien wie der horizontalen Arbeitsgruppe für Cyber-Fragen („HWPCI“) beraten. Im Falle des Einsatzes von restriktiven Maßnahmen entscheidet der Rat der EU auf Vorschlag des Hoher Vertreter der Union für Außen- und Sicherheitspolitik. Eine Attribuierung (Zurechnung) des Angriffs ist eine souveräne politische Entscheidung der Mitgliedstaaten, kann aber auf EU-Ebene koordiniert werden. Die *EU Hybrid Toolbox* ist eine Erweiterung der *Cyber Diplomacy Toolbox*, und wird für Angriffe verwendet, die über reine Cyberattacken hinausgehen, wie etwa hybride Kampagnen, die Cyberangriffe mit Desinformation oder wirtschaftlichem Zwang verknüpfen (Bundesministerium für Inneres, 2025). Auch die *FIMI-Toolbox* („Foreign Information Manipulation and Interference Toolbox“) ist eine solche Erweiterung, welche auf die Bekämpfung von ausländischer Informationsmanipulation und Einmischung spezialisiert ist (Council of the European Union, 2023).

Die *NATO-Reaktionsmechanismen* sollen die drei Kernaufgaben der NATO, Abschreckung und Verteidigung, Krisenprävention und-management sowie kooperative Sicherheit, auch im digitalen Raum gewährleisten (Bundesministerium für Inneres, 2024). Am bedeutendsten ist hierbei, dass ein massiver Cyberangriff den Bündnisfall gemäß Artikel 5 des Nordatlantikvertrags auslösen kann (Lété, 2017). Dies bedeutet, dass die Alliierten einen schwerwiegenden digitalen Angriff auf einen Mitgliedstaat als Angriff gegen alle werten und kollektiv darauf reagieren können. Zusätzlich zu diesem Reaktionsmechanismus verfügt die NATO über ein etabliertes Krisenreaktionssystem, das auf eine schnelle und koordinierte Reaktion der Alliierten abzielt. Dies wird mit der EU synchronisiert, und auch auf der technischen Ebene werden mittels der NATO Communications and Information Agency („NCIA“) und dem CERT-EU Informationen ausgetauscht. Auch im Cyber Defence Pledge (2016 verabschiedet und 2023 aktualisiert) verpflichten sich die Alliierten auf höchster politischer Ebene, Cyberverteidigung zu priorisieren und Informationsaustausch über Bedrohungen zu verstärken sowie die Aus- und Weiterbildung auszuweiten (North Atlantic Treaty Organization, 2016). Diese mit der NATO koordinierten Maßnahmen sind Bestandteil der EU-Cybersicherheitsstrategie (Europäische Kommission, 2020).

Die EU verstärkt ihr Engagement in internationalen Normungsgremien, um sicherzustellen, dass technologische Standards weltweit sicher, ethisch und auf den Menschen ausgerichtet bleiben und verhindert wird, dass technologische Standards von Akteuren gesetzt werden, die autoritäre

Internetmodelle oder Massenüberwachung fördern (Europäische Kommission, 2020). Anvisierte Gremien sind unter anderem die ISO („International Organization for Standardization“)[26], die ITU („International Telecommunication Union“)[27], die IEC („International Electrotechnical Commission“)[28], das ETSI („European Telecommunications Standards Institute“)[29] und das IEEE („Institute of Electrical and Electronics Engineers“)[30].

Das EU-Konzept für verantwortungsvolles staatliches Verhalten ist essenzieller Teil der EU-Außen- und Sicherheitspolitik, da die EU ihr Instrumentarium für die Cyberdiplomatie ausdrücklich nutzt, um den UN-Rahmen für verantwortungsvolles staatliches Verhalten weltweit zu unterstützen und dessen Einhaltung durchzusetzen (Europäische Kommission, 2020). Das heißt, dass das bestehende Völkerrecht und die UN-Charta (insbesondere das Verbot der Gewaltanwendung und das Recht auf Selbstverteidigung) uneingeschränkt im Cyberraum gelten (Council of the European Union, 2023). Des Weiteren unterstützt die EU elf freiwillige, nicht bindende Normen, die festlegen, was Staaten im Cyberraum tun sollten (z. B. Unterstützung bei Vorfällen) und was sie unterlassen müssen (z. B. Angriffe auf kritische Infrastrukturen). Um die oft abstraktem UN-Normen in die praktische Anwendung zu überführen, treiben die EU und ihre Mitgliedstaaten das *UN-Programme of Action to Advance Responsible State Behaviour in Cyberspace* massiv voran (Europäische Kommission, 2020). Dabei soll ein Mechanismus etabliert werden, der die praktische Einhaltung der elf freiwilligen UN-Normen regelmäßig überprüft und fördert, um den Austausch bewährter Verfahren zwischen den Staaten zu ermöglichen und Entwicklungsländer technisch und rechtlich dabei zu unterstützen, ihre Cybersicherheit zu erhöhen und internationale Normen einzuhalten.

Die Stärkung des internationalen Kapazitätsaufbau ist nicht nur im Rahmen der UN relevant, die EU hat zudem die *EU-Agenda für den Cyberkapazitätsaufbau* entwickelt, um diese Bemühungen im Einklang mit der *Agenda 2030* der UN für nachhaltige Entwicklung zu steuern (Europäische Kommission, 2020). Dafür wurde das Gremium „EU Cyber Capacity Building Board“ geschaffen, das Fortschritte überwacht, Synergien ermittelt und Lücken in der Unterstützung von Drittstaaten schließt. Das EU CyberNet ist hierbei das EU-finanzierte operative Netzwerk der EU, welches Fachwissen für den weltweiten Kapazitätsaufbau bündelt. Ziel dieser Bemühungen ist es, Partnerländer (insbesondere im Westbalkan, in der Nachbarschaft der EU und in Ländern mit rascher digitaler Entwicklung) dabei zu unterstützen, ihre eigene Cyberresilienz zu erhöhen.

Die EU verknüpft den Aspekt der Abschreckung untrennbar mit der Fähigkeit, Cyberkriminelle weltweit zu identifizieren und strafrechtlich zu verfolgen (Europäische Kommission, 2020). Das *Global Programme on Cybercrime* unterstützt Staaten direkt beim Aufbau nationaler Kapazitäten zur Verbrechensbekämpfung und wird vom UN-Büro für Drogen- und Verbrechensbekämpfung (UNODC) mit Sitz in Wien geleitet (Bundesministerium für Inneres, 2024). Europol und ENISA arbeiten hier eng zusammen, um Synergien zwischen technischer Cybersicherheit und kriminalpolizeilicher Arbeit zu nutzen (Europäische Kommission, 2020).

CASE STUDIES ZUR VERSTÖßE GEGEN DIE CYBERSICHERHEIT IN DER EU

WannaCry (Mai 2017) - *Windows Schwachstelle führte zu Angriff auf NHS durch Ransomware*

Vorfall → Am 12. Mai 2017 begann der weltweite Ransomware-Angriff WannaCry, der innerhalb 24 Stunden über 200.000 Computer in mindestens 150 Ländern infizierte (House of Commons, 2018). Der Angriff nutzte die Windows-Schwachstelle MS17-010[31] unter Verwendung des „EternalBlue"-Exploits[32] aus (EuRepoC, 2026b). Diese Schwachstelle im SMBv1-Protokoll[33] war der US-Geheimdienstbehörde NSA bereits jahrelang bekannt, bevor sie durch die Gruppe „Shadow Brokers" öffentlich gemacht wurde (Steinberg et al., 2021). Obwohl Microsoft bereits im März 2017 einen kritischen Patch bereitgestellt hatte, war dieser auf vielen Systemen zum Zeitpunkt des Angriffs noch nicht installiert worden (EuRepoC, 2026b).

Methode → WannaCry verfügte über eine Wurm-Funktionalität, die es der Schadsoftware ermöglichte, sich nach der initialen Infektion eines Geräts automatisch lateral in Netzwerken über das SMBv1-Protokoll zu verbreiten (EuRepoC, 2026b). Sobald ein System kompromittiert war, setzte die Ransomware eine asymmetrische Verschlüsselung ein, um Nutzerdateien zu sperren und Lösegeldzahlungen zu fordern. Der Angriff wurde erst gestoppt, als ein Sicherheitsforscher zufällig einen im Code eingebetteten „Kill-Switch" in Form einer Domain[34] aktivierte (House of Commons, 2018).

Folgen → Im Vereinigten Königreich war insbesondere der National Health Service (NHS) massiv betroffen. Laut dem Bericht des National Audit Office (NAO) waren 80 von 236 NHS-Trusts (34%) in England beeinträchtigt. Infolgedessen mussten schätzungsweise 19.494 medizinische Termine und Operationen abgesagt werden. Zudem waren 595 Hausarztpraxen infiziert, und fünf Krankenhäuser sahen sich gezwungen, Rettungswagen zu anderen Standorten umzuleiten. Die finanziellen Schäden für den NHS wurden auf etwa £92 Mio. geschätzt, während die globalen Kosten des Angriffs in die Milliarden gingen (EuRepoC, 2026b).

Motiv/Täter → Sicherheitsbehörden des Vereinigten Königreichs (NCSC), der USA und Kanadas identifizierten die nordkoreanische Hackergruppe Lazarus (auch als APT38 bekannt) als die mutmaßlichen Täter (EuRepoC, 2026b). Da die Angreifer Lösegelder bis zu 600 USD in Bitcoin verlangten, wird von einem primär finanziellen Motiv ausgegangen. Experten vermuten aufgrund der technischen Ineffizienz bei der Entschlüsselung jedoch auch eine geopolitische Komponente zur Destabilisierung oder als Ablenkungsmanöver (Bendiek & Schulze, 2021).

EU-Reaktion → Der Vorfall erhöhte den Druck zur Umsetzung der *NIS-1-Richtlinie* innerhalb der EU erheblich (Bendiek & Schulze, 2021). Als Teil der „Cyber Diplomacy Toolbox" verhängte der Rat der EU im Juli 2020 gezielte Sanktionen gegen die nordkoreanische Firma Chosun Expo, die mit der Lazarus-Gruppe in Verbindung gebracht wurde (Council of the European Union, 2020). Diese Maßnahmen umfassten das Einfrieren von Vermögenswerten und Einreiseverbote, um von künftigen böswilligen Cyberaktivitäten abzuschrecken.

Ableitung → Die Untersuchungen des NAO und des House of Commons ergaben, dass grundlegende IT-Hygiene, wie ein konsequentes Patch-Management[35] und die Absicherung von Firewalls, den Angriff im NHS weitgehend hätte verhindern können (NAO, 2018). Es wurde deutlich, dass Incident-Response-Pläne existieren und vorab mit lokalen Organisationen getestet

werden müssen, da die Kommunikation im Ernstfall oft improvisiert war (House of Commons, 2018). Schließlich unterstrichen die Befunde die Notwendigkeit einer zentralisierten Aufsicht und klarer Verantwortlichkeiten, um die Cybersicherheit kritischer Sektoren nachhaltig zu erhöhen.

NotPetya (Juni 2017) - *Daten von Banken, Behörden, Energieversorger irreversibel zerstört*

Vorfall → Der Cyberangriff NotPetya begann am 27. Juni 2017, dem Vorabend des ukrainischen Verfassungstages (EuRepoC, 2026g). Obwohl die Schadsoftware oberflächlich wie eine Ransomware erschien, handelte es sich technisch um einen Wiper, der darauf ausgelegt war, Daten auf infizierten Systemen irreversibel zu zerstören (Steinberg et al., 2021). Der Angriff verbreitete sich von der Ukraine aus weltweit und wird von den USA als der destruktivste und kostspieligste Cyberangriff der Geschichte eingestuft (EuRepoC, 2026g).

Methode → Die initiale Infektion erfolgte durch eine Supply-Chain-Kompromittierung der ukrainischen Buchhaltungssoftware M.E.Doc, die von rund 80% der Unternehmen in der Ukraine zur Steuerabwicklung genutzt wurde (Steinberg et al., 2021). Die Angreifer nutzten Hintertüren in Software-Updates, um die Malware in die Netzwerke der Nutzer einzuschleusen. Einmal im System, verbreitete sich NotPetya automatisch lateral innerhalb lokaler Netzwerke durch den „EternalBlue"-Exploit (EuRepoC, 2026g). Zusätzlich kam das Tool „Mimikatz" zum Einsatz, um Anmeldedaten aus dem Arbeitsspeicher zu extrahieren und so auch auf bereits gepatchte Systeme überzugreifen. Die Malware verschlüsselte nicht nur Dateien, sondern überschrieb den „Master Boot Record" der Festplatten, was eine Wiederherstellung unmöglich machte. Die Lösegeldforderung von 300 USD in Bitcoin diente laut Experten lediglich als politischer Deckmantel für die Sabotage (Steinberg et al., 2021).

Folgen → Die weltweiten finanziellen Schäden werden auf insgesamt über 10 Milliarden USD geschätzt (EuRepoC, 2026g). In der EU und global waren zahlreiche Großkonzerne massiv betroffen, z.B. der dänische Schifffahrtsriese Maersk erlitt Schäden zwischen 250 und 300 Millionen USD und musste 17 seiner 76 internationalen Häfen vorübergehend schließen (EuRepoC, 2026g). Die FedEx-Tochter TNT Express verzeichnete Sanierungskosten von rund 400 Millionen USD (Steinberg et al., 2021). Der Pharmakonzern Merck meldete Verluste in Höhe von 870 Millionen USD. Weitere betroffene Unternehmen waren Saint-Gobain (Frankreich), Reckitt Benckiser (UK) und Beiersdorf (Deutschland) (EuRepoC, 2026g). In der Ukraine fielen die Strahlenüberwachungssysteme in Tschernobyl, das Metrosystem in Kiew, Flughäfen sowie zahlreiche Banken und Energieversorger aus.

Motiv/Täter → Sicherheitsbehörden der Five-Eyes-Staaten und der Ukraine attribuierten den Angriff der russischen Militärgeheimdienst-Einheit 74455 (GRU), die auch unter dem Namen Sandworm ist (EuRepoC, 2026g). Das Motiv lag in der strategischen Destabilisierung der Ukraine im Rahmen des seit 2014 andauernden politisch-militärischen Konflikts mit Russland. Der Angriff sollte laut EuRepoC als Warnsignal an Unternehmen dienen, die in der Ukraine investieren oder geschäftlich tätig sind.

EU-Reaktion → Der Vorfall führte zur ersten koordinierten diplomatischen Reaktion der EU auf eine Cyberoperation (EuRepoC, 2026g). Im Juli 2020 verhängte der Rat der EU gezielte Sanktionen gegen das Hauptzentrum für Spezialtechnologien des GRU (Sandworm), einschließlich des Einfrierens von Vermögenswerten. Zur Verbesserung der

grenzüberschreitenden Koordinierung bei kriminellen Cyber-Großereignissen wurde zudem das „EU Law Enforcement Emergency Response Protocol“ unter der Federführung von Europol etabliert.

Ableitung → Der Fall NotPetya verdeutlicht die extreme Verwundbarkeit durch Drittanbieter-Software und unzureichende Patch-Zyklen, denn Microsoft hatte den notwendigen Sicherheits-Patch (MS17-010) bereits drei Monate vor dem Angriff im März 2017 veröffentlicht hatte, viele Organisationen diesen jedoch nicht installiert hatten (EuRepoC, 2026g). Als zentrale präventive Maßnahmen wurden die Notwendigkeit einer strikten Netzwerksegmentierung, um die laterale Ausbreitung zu stoppen, sowie die Implementierung robuster Offline-Backups identifiziert (Steinberg et al., 2021). Politisch markierte der Angriff den Übergang zu einer aktiven EU-Cyber-Diplomatie, die staatliche Akteure durch koordinierte öffentliche Attribution und Sanktionen von künftigen Angriffen abschrecken soll (EuRepoC, 2026g).

Brno University Hospital (März 2020) - *Server von tschechischen Krankenhaus während Covid-19 gesperrt*

Vorfall → Der Ransomware-Angriff auf das Universitätsklinikum Brno („Fakultní nemocnice Brno“) fand im März 2020 statt, was mit dem Beginn der ersten COVID-19-Welle in Europa zusammenfiel (NÚKIB, 2021). Die NÚKIB („National Cyber and Information Secutiry Agency“) stufte diesen Vorfall als den schwersten IT-Sicherheitsvorfall des Jahres in Tschechien ein. Die Ransomware wurde am 13. März 2020 aktiviert und verschlüsselte weite Teile der Server-Infrastruktur.

Methode → Die Angreifer nutzten eine Kombination aus Phishing, Ransomware und der Ausnutzung technischer Schwachstellen in den Systemen (NÚKIB, 2021). Entsprechend einem beobachteten Trend bei modernen Cyberangriffen handelte es sich nicht um eine völlig wahllose Kampagne, sondern um einen gezielten Angriff, bei dem die Täter nach dem Eindringen Zeit im Netzwerk verbrachten, um die Daten zu bewerten, bevor sie die Verschlüsselung starteten. Die NÚKIB gab in der Folge spezifische Warnungen vor Kampagnen heraus, die den Kontext der Pandemie ausnutzten.

Folgen → Der Angriff führte zu massiven Betriebseinschränkungen an drei Standorten des Klinikums: der Hauptklinik in Bohunice, der Kinderklinik und der Frauenklinik (NÚKIB, 2021). Die IT-Systeme fielen vollständig aus, wodurch geplante Operationen abgesagt werden mussten und die Versorgung von Akutpatienten durch Umleitungen in andere Krankenhäuser beeinträchtigt wurde. Da das Klinikum eines der größten Zentren für COVID-19-Tests im Land war, wurde die tschechische Pandemie-Reaktion unmittelbar geschwächt. Der finanzielle Schaden wurde auf hunderte Millionen tschechische Kronen beziffert.

Motiv/Täter → Der Angriff wird kriminellen Gruppierungen zugeschrieben, deren Hauptmotiv finanzieller Gewinn war (NÚKIB, 2021). Solche Täter wählen ihre Opfer oft opportunistisch aus und konzentrieren sich während der Pandemie verstärkt auf den Gesundheitssektor, da sie davon ausgehen, dass Krankenhäuser aufgrund des lebenswichtigen Charakters ihrer Dienste unter hohem Druck eher bereit sind, Lösegelder zu zahlen.

EU-Reaktion → In Tschechien führte der Vorfall unmittelbar zu gesetzlichen Änderungen, denn die Regelungen für Anbieter wesentlicher Dienste wurde angepasst, um die Anzahl der regulierten Krankenhäuser von 16 auf etwa 46 zu erhöhen und deren Sicherheitsanforderungen massiv zu verschärfen (NÚKIB, 2021). Im November 2020 verabschiedete Tschechien zudem

eine neue nationale Cybersicherheitsstrategie (NÚKIB, 2021). Auf EU-Ebene diente der Fall Brno als mahnendes Beispiel für die Verwundbarkeit des Gesundheitssektors und trug zur politischen Beschleunigung der *NIS-2-Richtlinie* ((EU) 2022/2555) bei, die darauf abzielt, die Cybersicherheit kritischer Sektoren unionsweit zu harmonisieren und zu stärken.

Ableitung → Dieser Fall verdeutlicht, dass kritische Infrastrukturen in Krisenzeiten besonders vulnerabel sind. Als zentrale Präventionsmaßnahmen wurden die Notwendigkeit einer strikten Netzwerksegmentierung, konsequentes Patch-Management und insbesondere die Implementierung sowie regelmäßige Wiederherstellungsprüfung von Offline-Backups identifiziert (NÚKIB, 2021).

HAFNIUM-Kampagne (März 2021) - *Daten von EU-Finanzaufsichts-behörde gestohlen*

Vorfall → Am 2. März 2021 gab Microsoft bekannt, dass eine staatlich unterstützte Hackergruppe aus China, identifiziert als HAFNIUM, vor-Ort-Versionen der Microsoft Exchange Servers weltweit angegriffen hatte (Winder, 2021). Schätzungen zufolge wurden dabei weltweit über 250.000 Systeme kompromittiert, aber ein besonders prominentes Opfer in der EU war die Europäische Bankenaufsichtsbehörde (EBA), die am 7. März 2021 bestätigte, dass ihre Exchange-Server Ziel des Angriffs gewesen waren (Feldman et al., 2021).

Methode → Die Angreifer nutzten eine Kette von vier Zero-Day-Schwachstellen, um ohne gültige Zugangsdaten administrativen Zugriff auf die Server zu erhalten (EuRepoC, 2026c). Nach der initialen Kompromittierung installierten die Täter Webshells als Hintertüren, um die Server aus der Ferne zu steuern. Über diesen Zugriff wurden E-Mail-Postfächer exportiert, Daten des Offline-Adressbuchs heruntergeladen und Zugangsdaten aus dem Systemspeicher (LSASS-Prozess) gestohlen, um einen langfristigen Zugriff auf die Netzwerke der Opfer zu gewährleisten (Microsoft Threat Intelligence, 2021).

Folgen → Im Fall der EBA wurde zunächst befürchtet, dass vertrauliche E-Mail-Kommunikation und personenbezogene Daten abgeflossen sein könnten, aber eine abschließende Untersuchung durch die EBA in Zusammenarbeit mit CERT-EU ergab jedoch am 9. März 2021, dass der Vorfall begrenzt blieb und keine Datenextraktion stattgefunden hatte (Winder, 2021). Dennoch verursachte die Kampagne global massive Schäden, insbesondere bei kleinen Unternehmen und Behörden. Für den Finanzsektor wurde der Angriff als ernsthafte Bedrohung der Cyber-Resilienz eingestuft, da die Manipulation wichtiger Institutionen zu Marktinstabilitäten und einem Vertrauensverlust führen kann (Feldman et al., 2021).

Motiv/Täter → Die Kampagne wurde von Microsoft mit hoher Sicherheit der Gruppe HAFNIUM zugeschrieben, die als staatlich geförderte Gruppe aus China agiert (Winder, 2021). Im Juli 2021 erfolgte eine formelle Attribution durch die EU, die USA und die NATO, die den Angriff Akteuren zuordneten, welche mit dem chinesischen Ministerium für Staatssicherheit in Verbindung stehen (EuRepoC, 2026c). Die Gruppe verfolgt primär Cyber-Spionage und hat in der Vergangenheit gezielt US-Forschungseinrichtungen für Infektionskrankheiten, Anwaltskanzleien, NGOs und politische Thinktanks angegriffen (Microsoft Threat Intelligence, 2021).

EU-Reaktion → Die EU forderte im Rahmen einer koordinierten Reaktion die sofortige Installation der von Microsoft bereitgestellten Notfall-Patches (EuRepoC, 2026c). Am 19. Juli 2021 verurteilte die EU die böswilligen Cyberaktivitäten im Rahmen der Cyber Diplomacy Toolbox offiziell. Der Vorfall verstärkte den Fokus auf die regulatorische Umsetzung der NIS-Richtlinien und führte zu

einer Intensivierung der Zusammenarbeit zwischen nationalen Behörden und EU-Institutionen wie der Joint Cyber Unit, um die operative Koordinierung bei grenzüberschreitenden Vorfällen zu verbessern (Feldman et al., 2021).

Ableitung → Der Fall HAFNIUM unterstreicht, dass reines Patch-Management bei bereits kompromittierten Systemen nicht ausreicht, da installierte Webshells auch nach dem Schließen der Schwachstelle aktiv bleiben (Feldman et al., 2021). Als zentrale Lehren wurden die Notwendigkeit einer strikten Netzwerksegmentierung zur Verhinderung von Seitwärtsbewegung sowie die kritische Prüfung von vor-Ort-Lösungen gegenüber Cloud-Lösungen identifiziert, da Exchange Online nicht betroffen war (Microsoft Threat Intelligence, 2021).

Viasat KA-SAT / AcidRain (Februar 2022) - *Lieferkette parallel zu Invasion der Ukraine kompromittiert*

Vorfall → Der Cyberangriff auf das Satellitennetzwerk Viasat KA-SAT-Netzwerk begann am 24. Februar 2022, zeitgleich mit dem Beginn der russischen Militärinvasion in die Ukraine (Guerrero-Saade & Amerongen, 2022). Ziel des Angriffs war die Satelliten-Bodeninfrastruktur (Modems und Router) des KA-SAT-9A-Netzwerks, was zu weitreichenden Ausfällen der Breitbanddienste in der Ukraine und mehreren EU-Mitgliedstaaten führte (EuRepoC, 2026f).

Methode → Die Angreifer verschafften sich vermutlich über eine Supply-Chain-Attacke und eine falsch konfigurierte VPN-Anwendung Zugang zum vertrauenswürdigen Verwaltungssegment des Netzwerks (EuRepoC, 2026f). Von dort aus bewegten sie sich lateral und nutzten ihren Zugriff, um mittels legitimer Management-Befehle massenhaft die Wiper-Malware AcidRain auf die Modems übertragen. AcidRain überschrieb gezielt Daten im Flash-Speicher der Geräte, wodurch diese inoperabel wurden und entweder eine Neuinstallation der Firmware oder ein kompletter Austausch der Hardware notwendig war.

Folgen → In der Ukraine fielen zu Beginn der Invasion tausende Modems aus, was die Kommunikation der ukrainischen Polizei und des Militärs sowie intelligenter Waffensysteme störte (Guerrero-Saade & Amerongen, 2022). Der Vorfall hatte auch massive Spillover-Effekte in der EU, z.B. in Deutschland konnten 5.800 Windkraftanlagen des Herstellers Enercon nicht mehr ferngesteuert oder überwacht werden (EuRepoC, 2026f). Insgesamt waren zehntausende Nutzer und Organisationen betroffen; allein für das Enercon-System mussten rund 30.000 Ersatzmodems verschickt werden und der finanzielle Gesamtschaden wird auf Millionenbeträge geschätzt.

Motiv/Täter → Der Angriff wird offiziell der Russischen Föderation (speziell dem Militärgeheimdienst GRU) zugeschrieben (EuRepoC, 2026f). Laut Eurpoean Repository of Cyber Incidents liegt es nahe, dass das Motiv die strategische Sabotage der ukrainischen Führung und Verteidigungsfähigkeit am ersten Tag des Krieges war.

EU-Reaktion → Am 10. Mai 2022 verurteilte die EU den Angriff in einer Erklärung des Hohen Vertreters offiziell und forderte im Rahmen der Cyber Diplomacy Toolbox Konsequenzen für die Täter (EuRepoC, 2026f). Der Vorfall verstärkte den politischen Fokus auf die Sicherheit von Lieferketten und trug zur Finalisierung der *NIS-2-Richtlinie* bei, die nun strengere Anforderungen an das Risikomanagement in Lieferketten für kritische Infrastrukturen stellt.

Ableitung → Der Fall verdeutlicht, dass Cyberangriffe heute ein integraler Bestandteil hybrider Kriegsführung sind und gezielt zur operativen Lähmung eingesetzt werden können (EuRepoC, 2026f). Kommerzielle Satellitensysteme erweisen sich aufgrund abweichender Sicherheitsstandards als besonders verwundbar. Eine nachhaltige Cyber-Resilienz erfordert daher eine enge Verzahnung von IT-Sicherheit mit der physischen Widerstandsfähigkeit (gemäß CER-Richtlinie) und den Ausbau effektiver Frühwarnsysteme.

DDoS-Angriff auf EU-Parlament (November 2022) - *Überflutung von Servern des Parlaments*

Vorfall → Am 23. November 2022 verabschiedete das Europäische Parlament eine Resolution, in der Russland als staatlicher "Unterstützer des Terrorismus" eingestuft wurde (EuRepoC, 2026d). Nur wenige Stunden nach dieser Abstimmung wurde die offizielle Website des Parlaments durch einen massiven Cyberangriff lahmgelegt. Die Präsidentin des Parlaments, Roberta Metsola, bestätigte den Vorfall auf Twitter und sprach von einem „raffinierten Cyberangriff“, zu dem sich eine kremlnahe Gruppe bekannt habe (Der Spiegel, 2022).

Methode → Bei dem Angriff handelte es sich um eine DDoS-Attacke (Distributed Denial of Service). Dabei überfluteten die Angreifer die Webserver mit Millionen von Anfragen, um die Systemressourcen zu überlasten und die Website für legitime Nutzer unerreichbar zu machen (Carter, 2022).

Folgen → Die Website war für mindestens eine Stunde (EuRepoC, 2026d) bzw. laut Medienberichten der Brussels Times für mehrere Stunden in Europa und den USA nicht oder nur sehr eingeschränkt erreichbar (Carter, 2022). Es kam jedoch zu keinem Abfluss sensibler Daten, da DDoS-Angriffe technisch nicht darauf ausgelegt sind, in Netzwerke einzudringen, sondern lediglich deren Kapazitäten erschöpfen (Der Spiegel, 2022). Der Angriff wird als eine gezielte politische Provokation gewertet, die unmittelbar auf die vorangegangene Resolution reagierte (EuRepoC, 2026d).

Motiv/Täter → Die pro-russische Hacktivistengruppe KillNet übernahm auf ihrem Telegram-Kanal die Verantwortung für den Angriff (EuRepoC, 2026d). Sie begründete die Aktion explizit als Reaktion auf die Einstufung Russlands durch das Parlament. KillNet ist für ähnliche Kampagnen gegen staatliche und private Institutionen in westlichen Ländern (z. B. Norwegen, Tschechien, Litauen) bekannt, die sich kritisch gegenüber dem russischen Vorgehen in der Ukraine äußern (Der Spiegel, 2022).

EU-Reaktion → Die EU-Institutionen reagierten mit scharfer Verurteilung; Roberta Metsola antwortete auf den Vorfall demonstrativ mit dem Hashtag „#SlavaUkraini“ (Der Spiegel, 2022). Laut dem NIS-Jahresbericht 2024 sind DDoS-Attacken inzwischen die führende Ursache für IT-Ausfälle im öffentlichen Sektor der EU, was die Notwendigkeit von Mindestsicherheitsstandards und einer beschleunigten Umsetzung von Richtlinien wie NIS-2 weiter verdeutlicht hat (NIS Cooperation Group, 2025).

Ableitung → Der Fall demonstriert die hohe politische Relevanz von Cybersecurity, da technische Angriffe zunehmend als Werkzeug zur symbolischen Machtdemonstration und Propaganda eingesetzt werden (EuRepoC, 2026d). Auch wenn kein physischer oder tiefer IT-Schaden entstand, diente die zeitweilige Nichterreichbarkeit der Website dazu, politisches Kapital aus der Störung einer demokratischen Institution zu schlagen und die Resilienz der EU-Kommunikation öffentlich infrage zu stellen.

BIBLIOGRAFIE

Bendiek, A., & Schulze, M. (2021, Dezember). Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag hack and the attack on the OPCW (SWP Research Paper 11). Stiftung Wissenschaft und Politik (SWP).

Dokument/Quelle direkt öffnen

Bundeskanzleramt. (2024, Dezember). Bericht Cybersicherheit für das Jahr 2023. Wien.

Dokument/Quelle direkt öffnen

Bundesministerium für Inneres. (2025). Bericht Cybersicherheit für das Jahr 2024. Wien.

Dokument/Quelle direkt öffnen

Bundesministerium für Inneres. (2026). Bericht Cybersicherheit für das Jahr 2025. Wien.

Dokument/Quelle direkt öffnen

Bundesministerium für Inneres. (2026, 16. Januar). Nationale Risikoanalyse gem. RKEG 2026. Wien.

Dokument/Quelle direkt öffnen

Bundesministerium für Inneres. (2026, 16. Januar). Österreichische Strategie für die Resilienz kritischer Einrichtungen (ÖSRKE 2026). Wien.

Dokument/Quelle direkt öffnen

Carter, D. (2022, 23. November). European Parliament website hit by DDoS attack. The Brussels Times.

Dokument/Quelle direkt öffnen

Council of the European Union. (2020, 30. Juli). Council Decision (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

Dokument/Quelle direkt öffnen

Der Spiegel. (2022, 24. November). Hacker legen Website des EU-Parlaments lahm.

Dokument/Quelle direkt öffnen

Europäische Kommission. (2026, 27. Juli). Anhang der Mitteilung an die Kommission: Billigung des Inhalts des Entwurfs einer Mitteilung der Kommission – Leitfaden der Kommission für die Anwendung der Verordnung (EU) 2024/2847 (Gesetz über Cyberresilienz) (C(2026) 5252 final)

Dokument/Quelle direkt öffnen

Europäische Kommission. (2025). Proposal for a Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act 2).

Dokument/Quelle direkt öffnen

Europäische Kommission & Hoher Vertreter der Union für Außen- und Sicherheitspolitik. (2020, 16. Dezember). Gemeinsame Mitteilung an das Europäische Parlament und den Rat: Die Cybersicherheitsstrategie der EU für die digitale Dekade (JOIN(2020) 18 final).

Dokument/Quelle direkt öffnen

Europäische Union. (2019, 17. April). Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit). Amtsblatt der Europäischen Union, L 151/15.

Dokument/Quelle direkt öffnen

Europäische Union. (2022, 14. Dezember). Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie). Amtsblatt der Europäischen Union, L 333/80.

Dokument/Quelle direkt öffnen

Europäische Union. (2022, 14. Dezember). Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen (CER-Richtlinie). Amtsblatt der Europäischen Union, L 333/164.

Dokument/Quelle direkt öffnen

Europäische Union. (2022, 14. Dezember). Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates über die digitale operationale Resilienz im Finanzsektor (DORA-Verordnung). Amtsblatt der Europäischen Union, L 333/1.

Dokument/Quelle direkt öffnen

Europäische Union. (2024, 23. Oktober). Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung). Amtsblatt der Europäischen Union, L 2024/2847.

Dokument/Quelle direkt öffnen

Europäische Union. (2024, 19. Dezember). Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union (Cybersolidaritätsverordnung). Amtsblatt der Europäischen Union, L 2025/38.

Dokument/Quelle direkt öffnen

Europäische Union. (2026, 13. Juli). Beschluss (GASP) 2026/1713 des Rates zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen. Amtsblatt der Europäischen Union, L 2026/1713.

Dokument/Quelle direkt öffnen

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2020, December 16). Joint communication to the European Parliament and the Council: The EU's cybersecurity strategy for the digital decade (JOIN(2020) 18 final).

Dokument/Quelle direkt öffnen

European Repository of Cyber Incidents (EuRepoC). (2026a, 23. Februar). Incident details: The pro-Russian group Killnet disrupted both state and private targets in Czech Republic in April 2022 (Last updated).

Dokument/Quelle direkt öffnen

European Repository of Cyber Incidents (EuRepoC). (2026b, 20. Mai). Incident details: North Korean state-sponsored hacking group Lazarus launched WannaCry ransomware attack infecting over 200,000 computers in 150 countries… in May 2017 (Last updated).

Dokument/Quelle direkt öffnen

European Repository of Cyber Incidents (EuRepoC). (2026c, 26. Mai). Incident details: China-Nexus group Hafnium exploited ProxyLogon zero-day vulnerabilities in Microsoft Exchange Server globally starting January 2021 (Last updated).

Dokument/Quelle direkt öffnen

European Repository of Cyber Incidents (EuRepoC). (2026d, 26. Mai). Incident details: Pro-Russian group Killnet took down the European Parliament website with a DDoS attack on 23 November 2022 (Last updated).

Dokument/Quelle direkt öffnen

European Repository of Cyber Incidents (EuRepoC). (2026e, 10. Juni). Incident details: Sub-cluster of Russian APT Sandworm allegedly deployed AcidPour wiper against Ukrainian telecommunication providers since 13 March 2024 (Last updated).

Dokument/Quelle direkt öffnen

European Repository of Cyber Incidents (EuRepoC). (2026f, 10. Juni). Incident details: Viasat hack: Russian military intelligence disrupted Ukrainian satellite broadband services in February 2022 (Last updated).

Dokument/Quelle direkt öffnen

European Repository of Cyber Incidents (EuRepoC). (2026g, 16. Juni). Incident details: The Russian state-sponsored APT Sandworm initially targeted Ukrainian infrastructures with wiper-campaign called "NotPetya" since June 2017, affecting targets worldwide (Last updated).

Dokument/Quelle direkt öffnen

European Union. (2026, January 21). Vertrag über die Arbeitsweise der Europäischen Union (AEUV), Art. 18 [Consolidated version]. Rechtsinformationssystem des Bundes. https://ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008048&FassungVom=2026-01-21&Artikel=18&Paragraf=&Anlage=&Uebergangsrecht=

Dokument/Quelle direkt öffnen

European Union Agency for Cybersecurity. (2025). The EU-cybersecurity index 2024: EU-level insights and next steps.

Dokument/Quelle direkt öffnen

European Union Agency for Cybersecurity. (2026). Consolidated annual activity report 2025. Luxemburg: Amt für Veröffentlichungen der Europäischen Union.

Dokument/Quelle direkt öffnen

Feldman, L., Thomas, R., Jaffe, P., & Barton, R. (2021, 10. März). The Hafnium attack: Evolving risk of cyber-attacks for the finance sector. Freshfields Bruckhaus Deringer.

Dokument/Quelle direkt öffnen

Guerrero-Saade, J. A., & Amerongen, M. van. (2022, 31. März). AcidRain | A modem wiper rains down on Europe. SentinelLabs.

Dokument/Quelle direkt öffnen

Hogeveen, B. (2022, März). The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN. Australian Strategic Policy Institute.

Dokument/Quelle direkt öffnen

House of Commons Committee of Public Accounts. (2018, 18. April). Cyber-attack on the NHS: Thirty-second report of session 2017–19 (HC 787).

Dokument/Quelle direkt öffnen

Kerttunen, M., & Hemmelskamp, J. (2023a, März). Case study: NotPetya. European Repository of Cyber Incidents (EuRepoC).

Dokument/Quelle direkt öffnen

Kerttunen, M., & Hemmelskamp, J. (2023b, 4. Oktober). Case study: Viasat. European Repository of Cyber Incidents (EuRepoC).

Dokument/Quelle direkt öffnen

Lété, B., & Pernik, P. (2017). EU–NATO cybersecurity and defense cooperation: From common threats to common solutions (Policy Brief No. 38). German Marshall Fund of the United States.

Dokument/Quelle direkt öffnen

Microsoft Threat Intelligence. (2021, 2. März). HAFNIUM targeting Exchange Servers with 0-day exploits. Microsoft Security Blog.

Dokument/Quelle direkt öffnen

National Audit Office (NAO). (2018, 24. April). Investigation: WannaCry cyber attack and the NHS (HC 414).

Dokument/Quelle direkt öffnen

National Cyber and Information Security Agency (NÚKIB). (2021). 2020 report on cyber security in the Czech Republic.

Dokument/Quelle direkt öffnen

NIS Cooperation Group. (2025, August). Annual report NIS Directive incidents 2024.

Dokument/Quelle direkt öffnen

North Atlantic Treaty Organization. (2016, 8. Juli). Cyber defence pledge.

Dokument/Quelle direkt öffnen

Rat der Europäischen Union. (2017, 19. Juni). Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf bösartige Cyberaktivitäten („Instrumentarium für die Cyberdiplomatie“) (Dokumenten-Nr. 10474/17).

Dokument/Quelle direkt öffnen

Rat der Europäischen Union. (2023, 8. Juni). Revised implementing guidelines of the cyber diplomacy toolbox (Dokumenten-Nr. 10289/23).

Dokument/Quelle direkt öffnen

Republik Österreich. (2026, 13. Juli). Netz- und Informationssystemsicherheitsgesetz – NISG (Fassung vom 13.07.2026). Rechtsinformationssystem des Bundes (RIS).

Dokument/Quelle direkt öffnen

Steinberg, S., Stepan, A., & Neary, K. (2021). NotPetya: A Columbia University case study (SIPA-21-022.1). Columbia University School of International and Public Affairs (SIPA).

Dokument/Quelle direkt öffnen

Winder, D. (2021, März). Microsoft Exchange attacks are declared an emergency by Homeland security. Forbes.

Dokument/Quelle direkt öffnen

World Economic Forum. (2026, Januar). Global cybersecurity outlook 2026. In Zusammenarbeit mit Accenture.

Dokument/Quelle direkt öffnen

Desinformation am Arbeitsplatz

Risiken der digitalen Transformation am Arbeitsplatz

Die technologischen Innovationen der vergangenen Jahre bieten ein enormes Potenzial für die Arbeitswelt, sind jedoch untrennbar mit neuen, tiefgreifenden Belastungen verknüpft (EPRS, 2025). Dieses Spannungsfeld am digitalen Arbeitsplatz ergibt sich aus dem Ziel, durch Innovationen massive Effizienzsteigerungen zu erreichen, während Beschäftigte zunehmend mit einer systematischen Arbeitsintensivierung und invasiven Überwachung konfrontiert sind (Garben, 2017). Digitale Technologien werden bereits von 89% der europäischen Beschäftigten regelmäßig an ihrem Arbeitsplatz genutzt (Dragano, 2024). Beobachtete Konsequenzen dieses Wandels für viele Arbeitnehmer sind ein Gefühl der permanenten Überwachung, ein verschlechtertes Arbeitsklima sowie eine wachsende Bedrohung durch Desinformation. Diese Symptome zeigen, dass das wirtschaftliche Risiko zunehmend auf den Arbeitnehmer verlagert wird und diese dadurch ein neues Arbeitsverhältnis entwickeln.

Technostress durch Nutzung des Algorithmischen Managements

Als algorithmisches Management (AM) wird der Einsatz von Systemen bezeichnet, die traditionelle Managementfunktionen wie die Erteilung von Anweisungen, die Überwachung oder die Bewertung von Mitarbeitenden teilweise oder vollständig automatisieren (EPRS, 2025). Dabei werden verschiedene Grade der technologischen Autonomie unterschieden: Beim KI-gestützten Management liefert die KI Daten und Analysen, während die menschliche Führungskraft die volle Entscheidungsgewalt behält. Beim KI-erweiterten Management erstellt das System Vorschläge oder Empfehlungen, die von Menschen überprüft werden müssen. Die höchste Stufe bildet das KI-automatisierte Management, das eigenständig Entscheidungen mit minimalem menschlichem Eingriff trifft.

Laut der EWCS-Umfrage[36] 2024 sind bereits 42,3% der Beschäftigten in der EU von AM betroffen, wobei dieser Wert mittelfristig auf 55,5% steigen soll. Die Verbreitung variiert regional stark, etwa von 70,1% in Dänemark bis hin zu 27,2% in Griechenland. Auch sektoral zeigen sich deutliche Unterschiede, da AM im Finanz- und Transportwesen besonders präsent ist, während es in der Landwirtschaft seltener eingesetzt wird. Zudem nutzen Großunternehmen[37] die Technologie häufiger als Kleinbetriebe (53% zu 31%).

Diese Technologie kann zwar Entscheidungsprozesse erleichtern, bringt jedoch auch erhebliche Belastungen für Arbeitnehmer:innen mit sich, insbesondere den sogenannten „Technostress“ (EPRS, 2025). Dieses Phänomen bezeichnet die psychische Belastung, die durch die Arbeit mit digitalen Technologien entsteht (Dragano, 2024). Es wird durch verschiedene Stressoren charakterisiert: ständige Unsicherheit aufgrund chronischer digitaler Transformationsprozesse („Techno-Uncertainty“), Belastung durch steigende Komplexität („Techno-Complexity“), Stress durch technische Unzuverlässigkeit („Techno-Unreliability“) sowie die Angst vor einer Ersetzung

durch Technik oder qualifizierteres Personal („Techno-Insecurity“). Der European Parliamentary Research Service hat herausgefunden, dass die Exposition gegenüber AM statistisch mit einem Anstieg der Stressrate um 6,2% verknüpft ist (EPRS, 2025).

Vorangetrieben wird dieser Stress maßgeblich durch Faktoren wie den Techno-Overload, welcher durch ein digital diktiertes hohes Arbeitstempo, ständige Unterbrechungen sowie belastende Multitasking-Anforderungen charakterisiert ist (Dragano, 2024). Laut Joint Research Centre der Europäischen Kommission wird die Arbeitsgeschwindigkeit bereits bei 52,3% der EU-Beschäftigten unmittelbar von digitalen Technologien bestimmt (González Vázquez et al., 2024). Von ebenso großer Bedeutung ist die Techno-Invasion, die durch permanente mobile Erreichbarkeit die Trennung von Arbeit und Privatleben auflöst, eine durchgängige Always-on-Kultur schafft und damit die für die Erholung der Beschäftigten essenziellen Phasen erheblich stört (Dragano, 2024). Das European Law Institute und die Europäische Kommission betonen hierbei, dass dies eine regulatorische Antwort erfordert, weshalb das Recht auf Nichterreichbarkeit zunehmend als integraler Bestandteil des Arbeitsschutzes („EU Occupation Safety and Health“) begriffen wird.

AM-Systeme sind primär auf maximale Effizienz programmiert, wobei menschliche Faktoren wie Müdigkeit oder soziale Bedürfnisse oft ignoriert werden (EPRS, 2025). Dies zwingt Mitarbeiter:innen zu anhaltend hoher Geschwindigkeit und schränkt ihr individuelles Urteilsvermögen sowie ihre fachliche Kreativität massiv ein. Besonders bemängelt wird hierbei der „Black-Box“-Effekt, also die mangelnde Transparenz bei algorithmischer Entscheidungsprozessen (European Commission, 2021). Laut der EWCS-Umfrage 2024 geben von den 26% der Beschäftigten, deren Arbeit durch Computerprogramme beeinflusst wird, nur etwas mehr als die Hälfte (insgesamt 15% aller Befragten) an, dass es in ihrem Unternehmen ein klares Verfahren gibt, um gegen automatisierte Entscheidungen vorzugehen. Dies erschwert es erheblich, unfaire Bewertungen oder Sanktionen wirksam anzufechten (European Commission, 2021).

Angesichts dieser Herausforderungen fordern die Abgeordneten des Europäischen Parlaments eine horizontale „Richtlinie zum algorithmischen Management“ um einen kohärenten, arbeitsplatzspezifischen Rahmen zu schaffen, der sicherstellt, dass die gesamte Belegschaft vor den Risiken digitaler Steuerung geschützt wird (Europäisches Parlament, 2025). Ein Kernpunkt dieser Forderung ist auch der „Human-in-Command“-Ansatz, der fordert, dass bedeutende Beschäftigungsentscheidungen wie Kündigungen oder Gehaltsänderungen niemals ausschließlich durch einen Algorithmus getroffen werden dürfen, sondern zwingend einer menschlichen Überprüfung unterliegen müssen.

Beispiel Box: KI-basierte Triage und Personalplanung im französischen Gesundheitswesen

Nach der Covid-19 Pandemie wurde AM wie Kronos [38] verstärkt, um für Personalmängeln und hohen Patient:innendurchlauf zu kompensieren (EPRS, 2025). Hauptsächlich dient es der Einsatzplanung, also Algorithmen entscheiden über Schichtrotationen, Aufgabenzuweisungen und Urlaubsanträge. In Notaufnahmen erfolgt die Echtzeit-Zuweisung von medizinischem Personal zu Patienten durch KI-basierte Triage-Systeme. Diese Technologie schränkt jedoch die Fähigkeit des Personals ein, Aufgaben eigenständig zu priorisieren oder ganzheitlich auf Patienten einzugehen, was zu einem Gefühl des Mikromanagements führt. Die ständigen digitalen Benachrichtigungen verursachen zudem eine „Alarm-Müdigkeit" und erhöhen das Burnout-Risiko, insbesondere bei Pflegekräften und Nachwuchspersonal.

Beispiel Box: Effizienzmaximierung im italienischen Logistiksektor

Der hohe Zeitdruck und das dynamische Umfeld im Logistiksektor war Hauptmotivation für die Einführung von AM (EPRS, 2025). Unternehmen setzen Plattformen wie Kronos oder Hubstaff [39] ein, um Lieferpläne und Routen in Echtzeit zu automatisieren. Echtzeit-Dashboards visualisieren den Standort der Fahrer, überwachen Leistungsmetriken und optimieren Routen rein auf Effizienz und ignorieren dabei oft menschliche Faktoren wie notwendige Pausen, Verkehrsstress oder die Herausforderungen der städtischen Navigation. Dies führt zu einer massiven Arbeitsintensivierung und einem ständigen Überwachungsdruck, da niedrige Leistungswerte automatisch Disziplinarmaßnahmen auslösen können. Zudem fördert AM in diesem Sektor prekäre Arbeitsmodelle, die einer „Gig-Economy" [40] ähneln.

Beispiel Box: Rekordstrafe für invasive Überwachung durch Amazon France

Amazon setzte ein extrem präzises System ein, das die Unterbrechungen beim Scannen von Paketen bis auf die Sekunde genau maß und die Arbeitsgeschwindigkeit kontinuierlich überwachte (EPRS, 2025). Die französische Datenschutzbehörde (CNIL) verhängte im Dezember 2023 dafür eine Strafe von 32 Millionen Euro, weil das System gegen den Grundsatz der Datenminimierung (DSGVO) verstieß, da die Überwachung der Pausenzeiten als übermäßig eingestuft wurde. Zudem wurde die mangelnde Transparenz gerügt, da die Mitarbeiter nicht angemessen über das intrusive Bewertungssystem informiert worden waren.

Digitale Überwachung am Arbeitsplatz

Die technischen Fortschritte des digitalen Zeitalters haben die systematische Überwachung am Arbeitsplatz von der reinen Erfassung von Arbeitsergebnissen zu einer ganzheitlichen Erfassung der Person weiterentwickelt, was häufig im Konflikt mit dem Grundrecht auf Privatsphäre steht (EPRS, 2025). Moderne Überwachungstechnologien können mittels GPS, Smartphones und Wearables den Standort und Bewegung der Mitarbeiter erfassen, was insbesondere in der Logistik- und Plattformarbeit zum Einsatz kommt (Ball, 2021). Durch Tastenanschläge und Klickverhalten kann via Software ermittelt werden wie und wann gearbeitet wird (EPRS, 2025). Es existieren mittlerweile sogar Systeme, die Gesichtsausdrücke, Tonfall, Herzfrequenz oder Gehirnströme analysieren, um Aufmerksamkeit oder Stress zu messen (Global Workplace Law & Policy, 2024).

Die so erzeugten Datenanalysen können Grundlage eines „Social Sorting" sein, bei dem elektronische Profile erstellt und genutzt werden, um automatisiert über die künftige Arbeitszuweisung, die Entlohnung oder sogar die Wahrscheinlichkeit einer Kündigung zu entscheiden (Ball, 2021) Wie drastisch dieser Trend ist, zeigt die Tatsache, dass während der Pandemie die Suchanfragen nach Software zur Überwachung von Mitarbeitern im Homeoffice zeitweise um das 17-fache anstiegen (Ball, 2021). Der Österreichische Gewerkschaftsbund warnt in diesem Zusammenhang vor dem geplanten „Digitalen EU-Omnibus", der Schutzrechte und die Mitbestimmung von Betriebsräten bei der Einführung solcher Überwachungssysteme schwächen könnte (ÖGB, 2025).

Die durch digitale Technologien ermöglichte permanente Sichtbarkeit am Arbeitsplatz erzeugt eine psychologische Dynamik, die als Panopticon-Effekt bezeichnet wird (Ball, 2021). Dies bedeutet, dass sich Mitarbeiter permanent beobachtet fühlen und dadurch unter ständiger Anspannung stehen. Da die Überwachung oft undurchsichtig ist, versuchen Arbeitnehmer, ihr Verhalten präventiv so zu steuern, dass sie vom Algorithmus positiv bewertet werden. Diese Form der unbezahlten Arbeit zur aktiven Gestaltung der eigenen digitalen Wahrnehmung wird als „Scopic Labour" definiert. Die daraus resultierende Überwachungsangst („Surveillance Anxiety") führt dazu, dass notwendige Pausen häufig übersprungen werden, was wiederum das Risiko für Stress, Erschöpfung und Burnout signifikant erhöht (EPRS, 2025).

Laut EPRS verspürten 37% der Beschäftigten eine verstärkte Überwachung durch diese Technologien an ihrem Arbeitsplatz. Prof. Dr. Kurt Pärli von der Universität Basel weist jedoch darauf hin, dass Arbeitnehmer eine berechtige Erwartung auf Privatsphäre haben dürfen und die Eingriffe in die Privatsphäre auf einer klaren gesetzlichen Grundlage beruhen, einen legitimen Zweck verfolgen und verhältnismäßig sein müssen (Pärli, 2020). Ein entscheidender Meilenstein in der EU-Gesetzgebung ist der „EU AI Act", der den Schutz der Privatsphäre stärken soll, indem Emotionserkennungstechnologie verboten wird. Zusätzlich räumt er Betroffenen ein Recht auf eine verständliche Erklärung der Logik hinter algorithmischen Entscheidungen ein (European Union, 2024).

Beispiel Box: Standort- und Bewegungsdaten

Deliveroo ist ein online-Lieferdient, der Kunden per App mit Gerichten aus lokalen Restaurants und Supermärkten verbindet (Ball, 2021). Laut Berichten aus dem Jahr 2016/2017 werden Fahrer während des Lieferprozesses lückenlos überwacht. Es werden Daten zur durchschnittliche Zeit für die Annahme von Aufträgen, die Fahrzeit zum Restaurant, die Wartezeit auf Kunden sowie die Anzahl verspäteter oder nicht zugewiesener Aufträge gemessen.

Uber ist ein Vermittlungsdienst für Fahrdienste, der Fahrgäste per App mit lizenzierten Mietwagen- und Taxiunternehmen verbindet (Garben, 2017). Das Unternehmen sammelt laut Studien seit 2015 GPS-, Beschleunigungsdaten von den Smartphones der Fahrer, wobei riskantes Fahrverhalten wie starkes Beschleunigen oder abruptes Bremsen zur automatisierten Deaktivierung des Kontos führen kann.

Beispiel Box: Tastenanschläge und Verhaltensüberwachung

Der globale Callcenter-Anbieter Teleperformance nutzte während der Pandemie (2021) Webcams, um in regelmäßigen Abständen Fotos von Mitarbeitern an ihren heimischen Schreibtischen zu machen, was als unverhältnismäßiger Eingriff in den privaten Raum kritisiert wurde (Ball, 2021).

Die Bank Barclays pilotierte in den Jahren 2017 -2019 in dem Vereinigten Königreich ein System, welches die Computernutzung der Mitarbeiter trackte, nachdem sie zuvor bereits „Black Boxes“ unter Schreibtischen installiert hatte, um die physische Anwesenheit zu überwachen (Ball, 2021).

Beispiel Box: Biometrie und Emotionserkennung

Unternehmen wie HireVue[41] oder Cognisess[42] nutzen Algorithmen, um Gesichtsausdrücke, Tonfall und Körpersprache in Videointerviews zu analysieren, was die Basis für Einstellungsentscheidungen bilden kann (Ball, 2021). Sie sind seit 2017 verstärkt im Einsatz.

Das britische Konsumunternehmen Unilever produziert und vertreibt alltägliche Produkte in den Bereichen Ernährung, Körperpflege, Beauty und Haushalt (Global Workplace Law & Policy, 2024). Es nutzte ab 2018 massiv KI-gestützte Videointerviews, um Tausende von Bewerbern effizient vorzusortieren. Solche Systeme werden unter dem neuen EU AI Act als Hochrisiko-KI eingestuft (European Union, 2024).

Bedrohung durch Desinformation

Durch die Nutzung von generativer KI hat die Bedrohung durch Desinformation am Arbeitsplatz nie dagewesene Ausmaße erreicht. Unter Desinformation versteht man nachweislich falsche oder irreführende Informationen, die mit der Absicht erstellt, präsentiert und verbreitet werden,

die Öffentlichkeit zu täuschen oder einen wirtschaftlichen Gewinn zu erzielen (EDMO, 2024). Aktuell ist eine drastische Skalierung und Professionalisierung von Angriffen zu beobachten, welche sowohl die gesellschaftliche Stabilität als auch die Integrität von Unternehmen gefährden (European Commission, 2021).

Die Nutzung von Large Language Models hat beispielsweise die Effektivität von Social-Engineering-Angriffen[43] massiv gesteigert (ENISA, 2025). KI ermöglicht es Angreifern, täuschend echte E-Mails, ohne die früher typischen Grammatik- oder Rechtschreibfehler zu verfassen, was deren Erkennung erheblich erschwert. Bis Anfang 2025 machten KI-gestützte Phishing-Kampagnen bereits mehr als 80% aller weltweit beobachteten Social-Engineering-Aktivitäten aus. Das Konzept des Phishing-as-a-Service (PhaaS) wird dabei durch Plattformen wie „Darcula [44] oder „Lucid“[45] vorangetrieben, welche die Erstellung von Phishing-Kits automatisieren und es somit auch technisch weniger versierten Akteuren ermöglichen, komplexe Angriffe gegen hunderte Organisationen gleichzeitig zu starten (European Commission, 2021).

Durch die gesteigerte Menge an KI-erzeugtem Content verändert sich auch das Informationsökosystem grundlegend. Bereits im November 2024 übertraf die Menge an KI-Inhalten erstmals die von Menschen erstellten Inhalt und im Mai 2025 erreichte KI-generierter Content einen Anteil von 52% des gesamten digitalen Inhalts (Bentzen, 2024). Diese Flut an synthetischen Daten führt dazu, dass es immer schwieriger wird, Fakten von Fiktion zu unterscheiden und begünstigt das sogenannte „Liar's Dividend“, bei dem Akteure die Existenz von Deepfakes nutzen, um echte Beweise gegen sich als Fälschung abzutun.

Desinformationskampagnen sind koordinierte Operationen die manipulative Narrative massenhaft zu verbreiten (EDMO, 2024). Generative KI erlaubt es, manipulative Narrative kostengünstig zu skalieren, was das Vertrauen in Institutionen und interne Entscheidungsprozesse systematisch untergraben kann (European Union, 2024). Täuschend echte Deepfakes von Führungskräften können beispielsweise genutzt werden, um Marktmanipulationen zu betreiben oder die Reputation eines Unternehmens durch gefälschte Skandale zu beschädigen (Abendroth Dias et al., 2025). Diese manipulierten Informationen können zu fehlerhaften Entscheidungsprozessen und erheblichen finanziellen Verlusten führen (Hoxtell, 2024).

Am Arbeitsplatz fungieren solche Desinformationskanäle häufig als Einfallstore für Cyberattacken. In der Praxis weichen Mitarbeiter oft auf informelle Messenger-Strukturen aus, um Arbeitsabläufe zu koordinieren (EPRS, 2025). Dies entzieht sich der offiziellen Kontrolle der IT-Sicherheit und schafft neue Sicherheitslücken für Desinformation und gezielte Angriffe innerhalb des Unternehmens.

Besonders Frauen sind von der verstärkten Nutzung von generativer KI häufiger negativ betroffen, denn 99% der Opfer von nicht-konsensualen Deepfake-Inhalten, wie pornografischen Bildmanipulationen, sind Frauen (Bentzen, 2024). Laut EPRS dienen diese Angriffe oft der Einschüchterung und Vertreibung von Frauen aus dem öffentlichen Raum, verursachen schweres psychisches Trauma und schädigen die Reputation nachhaltig.

Um diesen Bedrohungen entgegenzuwirken, sieht der EU AI Act bereits Transparenzpflichten für Deepfakes sowie Verbote für manipulative KI-Praktiken vor (European Union, 2024). Zudem verpflichtet der Digital Services Act (DSA) große Plattformen, systemische Risiken durch Desinformation aktiv zu mindern (Bentzen, 2024).

Beispiel Box: Spionage und Desinformation auf LinkedIn

Eine Form der Desinformation ist durch den Rekrutierungsprozess, in dem zunehmend gefälschte IT-Arbeitskräfte und Profile zur Infiltration genutzt werden (ENISA, 2025). Verantwortlich ist der staatlich verbundene nordkoreanische Akteur Famous Chollima, der verstärkt beobachtet wurde, wie er versuchte, als IT-Mitarbeiter in EU-Unternehmen, insbesondere in sensiblen Regierungs- und Verteidigungsbereiche, angestellt zu werden. Die Gruppe setzt dabei generative KI ein, um täuschend echte LinkedIn-Personas zu generieren, die einerseits der Kommunikation mit Zielorganisationen dienen und andererseits dazu genutzt werden, Malware über manipulierte Jobangebote oder Bewerbungen zu verbreiten. Neben der Cyber-Spionage durch strategische Datensammlung wurden diese Akteure auch dabei beobachtet, wie sie nach Vertragsende Erpressungsmethoden einsetzten, um Einnahmen zu generieren.

Beispiel Box: Desinformation in KI durch manipulierte Information auf Wikipedia

Desinformation wird häufig über vermeintlich vertrauenswürdige Wissensquellen in den Arbeitsalltag eingeschleust, um deren Glaubwürdigkeit für manipulative Zwecke auszunutzen (Bentzen, 2024). Die Fallstudie zum russischen Pravda-Netzwerk „Portal Kombat“, wobei Analysen von DFRLab und CheckFirst zeigten, dass Akteure seit Beginn des Angriffskriegs gegen die Ukraine verstärkt Hyperlinks zu Portal-Kombat-Domänen in Wikipedia-Quellen platzierten, um manipulative Narrative zu „waschen“ und Sanktionen gegen staatlich kontrollierte russische Medien zu umgehen. Da Wikipedia aufgrund seiner Mehrsprachigkeit und seines enormen Umfangs eine der zentralen Ressourcen für das Training von Large Language Models darstellt, führt diese Praxis zu einer systematischen Daten-Vergiftung. Dies heißt, dass manipulierten Informationen direkt in die KI-Chatbots, welche von Beschäftigten zunehmend als Werkzeuge für die tägliche Recherche oder Entscheidungsfindung am Arbeitsplatz genutzt werden, was langfristig die Integrität interner Unternehmensprozesse und die Qualität der digitalen Gemeingüter gefährdet.

Beispiel Box: Deepfakes der italienischen Ministerpräsidentin

Italiens Ministerpräsidentin Giorgia Meloni reagierte im Mai 2026 auf eine Welle von KIgenerierten Bildern, die sie in Unterwäsche zeigen und als echt ausgegeben wurden (Tagesschau, 2026). Viele Nutzer:innen hielten das Deepfake für authentisch, griffen sie öffentlich an und warfen ihr unwürdiges Verhalten vor. Der Vorfall zeigt, wie schnell Deepfakes erheblichen Reputationsschaden verursachen können.

Verschlechtertes Arbeitsklima

Die fortschreitende Digitalisierung führt auch zu einer grundlegenden Veränderung des sozialen Gefüges am Arbeitsplatz, welche spezifische Belastungen mit sich bringt, die das Arbeitsklima verschlechtern und die Gesundheit der Beschäftigten gefährden kann.

Seit der Covid-19-Pandemie lässt sich eine tiefgreifende Veränderung der Arbeitskultur feststellen, die durch einen massiven Anstieg von Homeoffice und Fernarbeit geprägt ist (ELI, 2023). Um den Arbeitsanforderungen gerecht zu werden, neigen insbesondere Hochqualifizierte in entgrenzten Verhältnissen zur „interessierten Selbstausbeutung“, wobei 27% der im Homeoffice Beschäftigten angeben, regelmäßig in ihrer Freizeit zu arbeiten (Klammer et al., 2017). Laut aktuellen Daten berichten 43,5% der EU-Beschäftigten von isolierter Arbeit, was den Teamzusammenhalt schwächt und das Risiko für Depressionen und Burnout signifikant erhöht (EU-OSHA, 2025). Ein Teil dieser Entwicklung ist die „Disintermediation“, also wenn menschliche Vorgesetzte zunehmend durch algorithmische Plattformen ersetzt werden, was die soziale Unterstützung im Krisenfall untergräbt und zu einem Verlust an Wertschätzung führt (Ball, 2021; Heider & Streithofer, 2022).

Durch den starken Fokus auf Effizienzsteigerung steigt der Wettbewerbsdruck auf die Belegschaft erheblich. Digitalisierung zielt dabei häufig darauf ab, Leerläufe zu vermeiden, was zu einer deutlichen Arbeitsverdichtung und einer Beschleunigung des Arbeitstempos führt (Heider & Streithofer, 2022). Laut der OSH-Pulse-Umfrage geben 52% der Beschäftigten an, dass digitale Technologien das Tempo ihrer Arbeit unmittelbar bestimmen (EU-OSHA, 2025). Gleichzeitig werden Gamifizierungstechniken und Bestenlisten eingesetzt, um Beschäftigte psychologisch zu steuern und durch „Nudges“ zu höherer Geschwindigkeit anzuhalten, wodurch Kolleginnen und Kollegen eher als Konkurrenten denn als Teammitglieder wahrgenommen werden (EPRS, 2025). Auch Kundenbewertungen werden teilweise direkt zur Bestrafung oder Aufgabenzuweisung genutzt, wodurch Vorurteile der Kundschaft ungefiltert auf die Beschäftigten übertragen werden.

Der digitale Arbeitsplatz hat zudem messbare Auswirkungen auf die physische Gesundheit. In Österreich sind laut Statistik Austria 86,4% der Erwerbstätigen mindestens einem körperlichen oder psychischen Gesundheitsrisiko ausgesetzt (Heider & Streithofer, 2022). Etwa 37% der EU-Beschäftigten klagen über allgemeine Erschöpfung infolge chronischen Stresses (EU-OSHA, 2025). In Österreich nennen 37,3% der Beschäftigten eine starke Beanspruchung der Sehkraft als Hauptrisiko des digitalen Arbeitsplatzes (Dragano, 2024). Das lange Sitzen, ein Merkmal der digitalen Arbeitswelt, kann muskuloskelettale Probleme (Rückenschmerzen) verschärfen, besonders wenn keine professionelle Ausstattung (Stühle, Beleuchtung) zur Verfügung gestellt werden. Daten zeigen, dass 42% der Frauen und 39% der Männer mindestens drei Viertel ihrer Arbeitszeit im Sitzen verbringen (EU-OSHA, 2025).

Beispiel Box: Kommunikation im Bankbetreib

Im österreichischen Bankbetrieb illustriert die Digitalisierung den Verlust zwischenmenschlicher Kommunikation und die Schwächung des Teamgefüges (Madner, 2019). Früher kommunizierten Teammitglieder persönlich, um Probleme zu lösen oder sich abzustimmen, aber durch die Einführung digitaler Steuerungssysteme wird heute jede Aufgabe einzeln über das System zugewiesen, wobei Mitarbeiter oft nicht einmal mehr wissen, wer außer ihnen noch an dem Gesamtprojekt arbeitet. Fragen zur Arbeit werden ebenfalls nur noch systemintern erfasst und können kaum noch persönlich geklärt werden. Die soziale Unterstützung im Team schwindet massiv, da informelle Gespräche und der persönliche Austausch durch anonyme, standardisierte Systemabläufe ersetzt werden.

Beispiel Box: Dienstplanung im Modeeinzelhandel

Im stationären Modehandel erfolgt die Personalplanung computergestützt auf Basis von Wetterdaten oder Vorjahresumsätzen so knapp, dass oft bewusst eine „Notbesetzung“ eingeplant wird (Madner, 2019). Die Digitalisierung dient hier als Argument für eine weitere Verdichtung, sodass beispielsweise die Zeitvorgabe für einen Bezahlvorgang von früher 27 Sekunden auf nur noch 22 Sekunden reduziert wurde, um Personaleinsparungen gegenzurechnen. Das heißt, wenn das Kundenaufkommen steigt, müssen die Mitarbeiter faktisch „schneller rennen“, um die Vorgaben zu erfüllen. Dies führt zu enormem Stress und dadurch zu drastischer Verschlechterung der Arbeitsbedingungen.

Durch die zunehmende Nutzung von digitalen Plattformen und AM-Strukturen entsteht ein Modell der „atomisierten Arbeitszeit“, bei dem Arbeitskraft in kleinsten Einheiten eingekauft wird und nur noch „aktive“ Sekunden vergütet werden (EPRS, 2025). Die Bedrohung wird durch Desinformationskampagnen und KI-gestütztes Phishing verschärft und die Arbeitnehmer tragen in Form von gesundheitlichen und psychosozialen Konsequenzen die Folgen. Deshalb erfordert die Gestaltung der digitalen Zukunft einen kohärenten regulatorischen Rahmen, um Effizienz nicht auf Kosten der Gesundheit und Privatsphäre zu maximieren. Zukünftige digitale Resilienz am Arbeitsplatz soll durch einen "Human-in-Command" Ansatz, der Förderung der KI-Kompetenz und die frühzeitige Einbindung der Belegschaft verbessert werden. Die zentrale Herausforderung bleibt, digitale Innovationen so zu steuern, dass sie das Potenzial zur Arbeitserleichterung voll ausschöpfen, ohne das Fundament des sozialen Schutzes und des menschlichen Wohlbefindens zu erodieren (EPRS, 2025).

Bibliografie

Abendroth Dias, K., Arias Cabarcos, P., Bacco, F. M., Bassani, E., Bertoletti, A., et al. (2025). Generative AI Outlook Report: Exploring the Intersection of Technology, Society and Policy. European Commission, Joint Research Centre.

Dokument/Quelle direkt öffnen

AnySecura. (2026, June 7). Hubstaff review: Core features, pros, and cons. https://www.anysecura.com/blogs/hubstaff.html

Dokument/Quelle direkt öffnen

Ball, K. (2021). Electronic monitoring and surveillance in the workplace: Literature review and policy recommendations. European Commission, Joint Research Centre.

Dokument/Quelle direkt öffnen

Bentzen, N. (2024). Information manipulation in the age of generative artificial intelligence (Briefing PE 757.647). European Parliamentary Research Service (EPRS).

Dokument/Quelle direkt öffnen

Dragano, N. (2024, 29. August). Gesundheitsrisiken und Prävention in der digitalen Arbeitswelt: Technostress, Ergonomie und Unfallsicherheit. Aus Politik und Zeitgeschichte (APuZ)/bpb.de.

Dokument/Quelle direkt öffnen

Dragano, N., Riedel-Heller, S. G., & Lunau, T. (2021). Haben digitale Technologien bei der Arbeit Einfluss auf die psychische Gesundheit? Der Nervenarzt, 92(11), 1111–1120.

Dokument/Quelle direkt öffnen

European Agency for Safety and Health at Work [EU-OSHA]. (2025). OSH Pulse: Occupational safety and health in the era of climate and digital change (Flash Eurobarometer).

Dokument/Quelle direkt öffnen

European Commission. (2021). First phase consultation of social partners under Article 154 TFEU on improving the working conditions in platform work (C(2021) 2611).

Dokument/Quelle direkt öffnen

European Commission. (2026). Verhaltenskodex zur Bekämpfung von Desinformation. Gestaltung der digitalen Zukunft Europas.

Dokument/Quelle direkt öffnen

European Digital Media Observatory [EDMO]. (2024). How is disinformation addressed in the member states of the European Union? 27 country cases.

Dokument/Quelle direkt öffnen

European Law Institute [ELI]. (2023). Guiding Principles on Workers' Right to Disconnect.

Dokument/Quelle direkt öffnen

European Parliament. (2021). Bericht über gerechte Arbeitsbedingungen, Rechte und sozialen Schutz für Plattformbeschäftigte – neue Beschäftigungsformen im Zusammenhang mit der digitalen Entwicklung (2019/2186(INI)).

Dokument/Quelle direkt öffnen

European Parliamentary Research Service [EPRS]. (2025). Digitalisation, artificial intelligence and algorithmic management in the workplace: Shaping the future of work (PE 774.670).

Dokument/Quelle direkt öffnen

European Union. (2016). Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets).

Dokument/Quelle direkt öffnen

European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Dokument/Quelle direkt öffnen

European Union Agency for Cybersecurity [ENISA]. (2025). ENISA threat landscape 2025.

Dokument/Quelle direkt öffnen

Eurofound. (2025). European Working Conditions Survey 2024: First findings (A. Parent-Thirion, B. Gerstenberger, J. Cabrita, F. Eiffe, S. Riso, K. Fric, J. Hurley, & C. White). Publications Office of the European Union.

Dokument/Quelle direkt öffnen

Garben, S. (2017). Protecting workers in the online platform economy: An overview of regulatory and policy developments in the EU. European Agency for Safety and Health at Work.

Dokument/Quelle direkt öffnen

Global Workplace Law & Policy. (2024). The Prohibition of AI Emotion Recognition Technologies in the Workplace under the AI Act.

Dokument/Quelle direkt öffnen

González Vázquez, I., Curtarelli, M., Anyfantis, I., Brun, E., & Starren, A. (2024). Digitalisation and workers wellbeing: The impact of digital technologies on work-related psychosocial risks (JRC138992). European Commission, Joint Research Centre.

Dokument/Quelle direkt öffnen

Heider, A., & Streithofer, P. (2022). Arbeitnehmer:innenschutz I: Überbetrieblicher Arbeitnehmer:innenschutz (Skriptum Arbeitsrecht 08A). Wien: Verlag des ÖGB GmbH.

Dokument/Quelle direkt öffnen

Hoxtell, W. (2024). Umgang mit Desinformation in Europa: Herausforderungen und Gelegenheiten für zivilgesellschaftliche Organisationen und Privatsektor. Bertelsmann Stiftung.

Dokument/Quelle direkt öffnen

Klammer, U., Steffes, S., Maier, M., Arnold, D., Stettes, O., Bellmann, L., & Hirsch-Kreinsen, H. (2017). Arbeiten 4.0 – Folgen der Digitalisierung für die Arbeitswelt. Wirtschaftsdienst, 97(7), 459–476.

Dokument/Quelle direkt öffnen

Netcraft. (2025). Inside the Lighthouse and Lucid PhaaS campaigns targeting 316 global brands. https://www.netcraft.com/blog/inside-the-lighthouse-and-lucid-phaas-campaigns-targeting-316-global-brands

Dokument/Quelle direkt öffnen

Österreichischer Gewerkschaftsbund (ÖGB). (2025, Dezember). Digitaler EU-Omnibus: Gefahr für Beschäftigtenrechte (Factsheet). https://www.oegb.at

Dokument/Quelle direkt öffnen

Pärli, K. (2020). Die EGMR-Rechtsprechung zum Schutz der Privatsphäre und vor Überwachung am Arbeitsplatz. Europäische Zeitschrift für Arbeitsrecht (EuZA), 224–235.

Dokument/Quelle direkt öffnen

Reifinger, I. (2021, 7. Oktober). Arbeit der Zukunft: Immer schneller, immer mehr, immer digitaler [Interview geführt von P. Leinfellner]. oegb.at. https://www.oegb.at

Dokument/Quelle direkt öffnen

Riso, S., & Litardi, C. (2024). Employee monitoring: A moving target for regulation. Eurofound.

Dokument/Quelle direkt öffnen

Swiss Cybersecurity. (2024, 28. März). Phishing-as-a-Service-Plattform verschickt iMessages im Namen hunderter Marken. https://www.swisscybersecurity.net/news/2024-03-28/phishing-as-a-service-plattform-verschickt-imessages-im-namen-hunderter

Dokument/Quelle direkt öffnen

Tagesschau. (2026, 5. Mai). Kampf gegen Deepfakes: Meloni verurteilt KI-Bild als „gefährliches Instrument“. https://www.tagesschau.de/ausland/europa/meloni-ki-deepfakes-100.html

Dokument/Quelle direkt öffnen

Yun Chee, F. (2025, 4. Februar). EU lays out guidelines on misuse of AI by employers, websites and police. Reuters.

Dokument/Quelle direkt öffnen

03 / TERMINOLOGIE

Operatives Glossar – Terminologie für Infoboxen

Um ein einheitliches Verständnis über alle Partnerländer hinweg zu gewährleisten, werden die Schlüsselbegriffe des Projekts für diese Erhebung wie folgt definiert. Ziel in diesem Abschnitt ist die Festlegung der Terminologiefür das Forschungsdesign.

Desinformation

Definition: Desinformation ist die absichtliche Verbreitung falscher oder irreführender Inhalte über digitale Kommunikationskanäle mit dem Ziel, Empfänger:innen bewusst zu täuschen (link). Abzugrenzen ist Desinformation von „Misinformation“ (unabsichtlich falsche Informationen) und „Malinformation“ (echte Informationen, die mit schädlicher Absicht verwendet werden, z. B. durch Leaks oder gezielte Kontextverschiebung). (link)

Formen der Desinformation:

Fake News: Der politisch aufgeladene Begriff Fake News ist ein Synonym für Desinformation. Hier liegt der Fokus auf viraler Verbreitung, um ein breites Publikum zu erreichen ("Clickbaiting"). Charakteristisch sind stark emotionalisierte Überschriften, einfache Schuldzuweisungen und das Ausnutzen bestehender Vorurteile oder Unsicherheiten. (link)

Beispiel Russischer Angriffskrieg: Das Correctiv-Faktencheck-Team hat im ersten Kriegsjahr über 150 Behauptungen von russischen Staatsmedien und kremlnahen Accounts überprüft. Beispielsweise wird Selenskyj unterstellt, er habe ein Kasino in Zypern gekauft, und die Liveaufnahmen aus der Ukraine seien gestellt oder stammten aus dem Videospiel „Call of Duty“. (source) Solche Narrative zielen darauf ab, das Vertrauen in demokratische Institutionen und Medien systematisch zu untergraben, was auch Auswirkungen auf die europäische Sicherheits- und Außenpolitik hat.

Beispiel 5G und Corona: Der Ausbau des Mobilfunkstandards 5G in Wuhan soll mit der Entstehung des Coronavirus in Verbindung stehen. Unabhängige Recherchen ergeben, dass 5G weder Zellabbau noch grippeähnliche Symptome verursacht. (link)

Deepfakes: Bei Deepfakes handelt es sich um mithilfe von KI erstellte, manipulierte Bilder und Videos, die biometrische Merkmale von Personen wie Aussehen, Mimik oder Stimme täuschend echt imitieren. (link) Durch die zunehmende Verfügbarkeit generativer KI sinkt die Eintrittsbarriere für solche Manipulationen erheblich, was deren Erkennung erschwert.

Beispiel Parlamentswahlkampf in der Slowakei 2023: In einem KI-manipulierten Audio ist zu hören, wie der Spitzenpolitiker Šimečka angeblich erklärt, wie er die Wahl beeinflussen wolle. Diese Aufnahme wurde von politischen Gegnern in Umlauf gebracht, um Šimečka vor der Wahl zu diskreditieren. (Guardian)

Beispiel Wahlbeeinflussung US: Die 73-jährige Gail Huntley erhielt vor der US-Präsidentschaftswahl einen Anruf, in dem die Stimme des demokratischen Kandidaten Joe Biden ihr riet, ihre Stimme zunächst „aufzubewahren“. Dieser KI-generierte Anruf sorgte für Aufsehen, da er zeigt, wie weit diese Technologie bereits fortgeschritten ist und eingesetzt wird. (Guardian) (siehe hier Vishing)

Auch bei der irischen Präsidentschaftswahl 2025 und in den Niederlanden werden KI-generierte Deepfakes als politische Propaganda eingesetzt. (link) Die EU reagiert darauf unter anderem mit Regulierungen wie dem Digital Services Act (DSA), der Plattformen stärker in die Pflicht nimmt, gegen Desinformation vorzugehen.

Dekontextualisierung und selektive Statistiken: Wenn Inhalte aus ihrem ursprünglichen Kontext herausgerissen werden, verlieren sie oft ihre ursprüngliche Bedeutung und werden als Instrument der Manipulation eingesetzt. (link) Korrekte Daten werden selektiv ausgewählt, verfälscht oder falsch interpretiert, um eine unzutreffende Schlussfolgerung zu belegen. Gerade im wirtschaftlichen Umfeld können solche verzerrten Darstellungen z. B. bei Arbeitsmarktdaten oder Unternehmenskennzahlen falsche Entscheidungen begünstigen. Siehe hierzu Section 3.

Motive: Der Kommunikationswissenschaftler Schulz-Tomančok identifiziert dabei zwei zentrale Motive: Zum einen gibt es ökonomische Interessen, bei denen durch emotionalisierende Falschmeldungen Werbeeinnahmen generiert werden, und zum anderen gibt es politische Ziele, die darauf abzielen, den öffentlichen Diskurs zu beeinflussen. (link)

Relevanz im Arbeitsalltag: Verschwörungstheorien und populistische Narrative verbreiten sich oft über den Kollegenkreis und können so ein Arbeitsklima erheblich verschlechtern, da eine gemeinsame Faktenbasis für Entscheidungen fehlt (link). Wenn ein ganzes Unternehmen Ziel einer Desinformationskampagne wird, kann dies zu Vertrauensverlust führen und somit zu rechtlichen und finanziellen Folgen führen. (link) Wenn systemrelevante Berufe Berufe in der kritischen Infrastruktur betroffen sind, kann dies die Versorgungssicherheit und Resilienz negativ beeinflussen bwz. bedrohen.

Reputationsangriffe: Eine häufige Ausformung von Desinformation sind gezielte Kampagnen, die sich gegen bestimmte Unternehmen, Personen oder Gruppen richten, um deren Ansehen zu schädigen. Durch Diffamierung, gefälschte Bewertungen und künstlich produzierte Shitstorms soll die öffentliche Meinung beeinflusst werden. (link)

Gerüchte

Definition: Gerüchte sind Behauptungen, die ohne überprüfbaren Nachweis ihrer Richtigkeit weitergegeben werden, dabei aber oft als objektive Informationen erscheinen (link). Dies fällt in die Kategorie der Misinformation, also Informationen, die falsch oder irreführend sind, jedoch ohne bewusste Täuschungsabsicht verbreitet werden (link) Gerüchte entstehen häufig in Situationen von Unsicherheit oder Informationsmangel. Sie erfüllen eine soziale Funktion, indem sie versuchen, „Wissenslücken” zu schließen – auch wenn die Inhalte nicht verifiziert sind. In digitalen Arbeitsumgebungen (z. B. interne Chats, soziale Netzwerke) verbreiten sie sich deutlich schneller und erreichen in kurzer Zeit große Teile der Mitarbeitenden.

Beispiele im Arbeitsalltag: Zurzeit kursieren beispielsweise bei VW Gerüchte über Standortschließungen. Der Konzern hat sich nach eingebrochenen Gewinnen die Beraterfirma McKinsey ins Haus geholt, um einen "tiefgreifenden Umbau" voranzutreiben. (link)

Arbeitnehmervertreterinnen und -vertreter kritisieren die möglichen Standortschließungen als „unverantwortliche Drohungen“. Solche Drohungen erhöhen im Regelfall das Gefühl von Jobunsicherheit, die laut diversen Studien einen negativen Einfluss auf psychische und körperliche Gesundheit. (link)

In Deutschland müssen Arbeitgeber dem Betriebsrat gem. §111 BetrVG frühzeitig und umfassend über geplante Betriebsänderungen zu informieren, und darauffolgend muss ein Sozialplan erstellt werden, um negative Auswirkungen auf Arbeitnehmer zu reduzieren. Der Betriebsrat dient daher als eine gute Informationsquelle.

Auch auf EU-Ebene existieren Informations- und Konsultationsrechte für Arbeitnehmer:innen (z. B. durch die EU-Richtlinie 2002/14/EG), die Transparenz fördern und die Entstehung von Gerüchten reduzieren sollen. (link)

Beispiele auf politischer Ebene: Gerüchte sind auch im politischen Kontext ein relevantes Instrument, um öffentliche Meinung zu beeinflussen. Das Gerücht, Annalena Baerbock wolle Haustiere verbieten oder die Witwenrente abschaffen, war eine gezielte Falschmeldung aus rechten und verschwörungsaffinen Communities in sozialen Netzwerken und Messengern, die über Sharepics und Posts in den Mainstream gelangte. Laut Studien zielten 71% aller falschen Behauptungen im Wahlkampf auf Baerbock, wobei traditionelle Medien die Fake News unbeabsichtigt weiterverbreiteten, indem sie sie als Fragen oder „Diskussionen" aufgriffen, obwohl Faktenchecker sie längst als Fake entlarvt hatten. Experten werten dies als Teil einer koordinierten Desinformationskampagne, die über soziale Medien ausgelöst und durch mediale Berichterstattung verstärkt wurde. (link)

Generative KI, Social-Media-Algorithmen und Filterblasen

Soziale Medien, KI und die damit einhergehenden Algorithmen nutzen personalisierte Empfehlungssysteme, um das Engagement von Nutzer:innen zu maximieren („Filterblasen“) und schaffen so ein stark verzerrtes Realitätsbild. Diese Systeme basieren auf der Auswertung großer Datenmengen (z. B. Klickverhalten, Verweildauer, Interaktionen) und optimieren Inhalte nicht nach ihrem Wahrheitsgehalt, sondern nach der Aufmerksamkeit, die sie generieren (link)

Generative KI: Durch KI ist es exponentiell einfacher und billiger, massenhaft plausible Texte, Kommentare und „News“ zu produzieren sowie Deepfakes und synthetische Avatare (virtuelles Abbild oder Stellvertreter einer Person in der digitalen Welt, z. B. Profilbild) zu erstellen und Inhalte in vielen Sprachen und auf viele Zielgruppen zugeschnitten zu generieren. (link)

Filterblasen: Social-Media-Plattformen nutzen Empfehlungsalgorithmen, die Inhalte danach ranken, um die Wahrscheinlichkeit zu erhöhen, dass Nutzer:innen möglichst viel Zeit auf ihren Plattformen verbringen. Das führt dazu, dass, wenn man einmal politisch polarisierendere Inhalte konsumiert hat, einem oft mehr davon angezeigt werden. Dieses System favorisiert oft polarisierende und emotionalisierende Inhalte, die dementsprechend systematisch bevorteilt werden. Dadurch entstehen falsche Informationsgrundlagen. (link)

Suchmaschinen und KI: Durch Algorithmen im Hintergrund kann die Sichtbarkeit verschiedener Inhalte manipuliert werden. Dabei spielen Ranking-Kriterien, Personalisierung und kommerzielle Interessen eine zentrale Rolle. Auch KI-gestützte Suchsysteme (z. B. Antwortsysteme statt Linklisten) können die Informationsauswahl weiter verengen.

Studie Politische Kandidaten: Laut einer Studie von Epstein und Robertson korreliert die Sichtbarkeit eines politischen Kandidaten mit der Wahlabsicht. Durch Manipulation des Rankings einer Suchmaschine können potenzielle Wähler dazu gebracht werden, einen bestimmten Kandidaten zu wählen, ohne dass ihnen diese Beeinflussung bewusst wird. Diese Manipulation funktioniert im Durchschnitt bei 20 Prozent der unentschlossenen Wähler („Search Engine Manipulation Effect"). (link)

Beispiel DeepSeek AI: Laut einem vom Nationalen Ausschuss für Cybersicherheitsstandards veröffentlichten technischen Dokument darf chinesische generative KI, wie der Chatbot DeepSeek, keine Inhalte enthalten, die gegen die „sozialistischen Kernwerte" des Landes verstoßen. Dazu gehören Inhalte, die „zum Umsturz der Staatsmacht und zum Sturz des sozialistischen Systems aufrufen" oder die „die nationale Sicherheit und die nationalen Interessen gefährden und dem Ansehen des Landes schaden". (link)

Relevanz International: Politische Gruppen oder auch staatliche Akteure nutzen die Algorithmen sozialer Medien aus, um bestimmte Themen (siehe selektive Information) oder eben Desinformationen künstlich nach oben zu spielen. (link) Vom Weltwirtschaftsforum wird die KI-gesteuerte Fehl- und Desinformation in seinem globalen Risikobericht als derzeit größtes Risiko für eine globale Krise in den kommenden zwei Jahren genannt. (link)

Beispiel Wahlbeeinflussung Indonesien: Im Rahmen der Wahl 2024 hat OpenAI bekannt gegeben, dass dessen Produkte weitläufig verwendet wurde, um Wahlkampfmaterial zu erstellen, die Stimmung in den sozialen Medien verfolgen, interaktive Chatbots entwickeln und Wähler gezielt anzusprechen. (Guardian)

Beispiel Wahlkampagnen Trump: US-Medien berichteten 2026 von hunderten KI-generierten „Influencern", die als junge Männer/Frauen (teils als Beamt:innen dargestellt, teils spärlich bekleidet) zu Themen wie Abtreibung oder dem Irakkrieg Stellung nahmen und so hyperzielgerichtete, personalisierte Werbung für Politiker machten. (Standard)

Relevanz am Arbeitsplatz OECD Studie: Obwohl wegen des KI-Booms Arbeitsplatzverluste befürchtet wurden, führte die Technologie eher zu einer Umschichtung der Arbeit, welche die Arbeitsbedingungen, -möglichkeiten und die Anforderungen an Arbeitskräfte angeht. Laut der OECD Studie gibt es vier dominierende Trends, einerseits werden vor allem die repetitiven, regelbasierten oder gefährlichen Aufgaben von KI übernommen andererseits wird eine erhöhte KI-Kompetenz erwartet. Daraus lässt sich ableiten, dass der KI-Trend den Arbeitsmarkt ungleich betrifft, da bestimmte Grppen stärker von Automatisierung betroffen sind oder weniger Zugang zu Weiterbildung haben und so mehr gefährdet sind. Außerdem wird eine höhere Arbeitsintensität erwartet, diese wiederum steht in der Kritik weil Beschäftigte berichten von höherem Tempo, stärkerer Überwachung (siehe Sektion X) oder dem Gefühl, „immer verbunden" zu sein. (link)

Social Engineering – Betrugsmasche, Scamming

Definition: Beim Social Engineering handelt es sich um eine Strategie, die dazu dient, Menschen dazu zu bringen, sensible Informationen (Passwörter, Finanzinformationen, sensible Daten usw.) preiszugeben. Beim Scamming wird der Fokus darauf gelegt, die menschliche Psychologie auszunutzen, statt technische Schwachstellen auszunutzen. (link)

Identitätsbetrug: Identitätsbetrug liegt vor, wenn Angreifer personenbezogene Daten einer Person ohne deren Zustimmung oder Wissen nutzen, um damit Verträge abzuschließen, Waren zu bestellen oder Ähnliches. Oft geschieht Identitätsbetrug durch Hacking oder Social Engineering. (link)

Überzeugungsversuche und Täuschung: Bei Überzeugungsversuchen gibt sich der Täter oft als vertrauenswürdige Person aus, um die Schwäche des Opfers auszunutzen. Typische Rollen sind z. B. IT-Support, Vorgesetzte oder externe Dienstleister. (link)

Methoden:

Phishing: Beim Phishing werden über E-Mails, Nachrichten oder Websites Links verbreitet, über die der Angreifer an sensible Daten (Zugangsdaten, Bankinformationen etc.) gelangt. Der Trick dabei ist, dass die Websites oft legitim wirken. (link)

Spear Phishing: Beim Spear-Phishing handelt es sich um eine hochgradig personalisierte Form des Phishings. Dabei werden personenspezifische Daten, die man über soziale Medien finden kann, verwendet (z. B. Arbeitsplatz, derzeitige Projekte, Hobbys, Urlaubsdestinationen). (link)

Vishing: Beim Vishing, einer Form des Phishings, wird die Sprachkommunikation (Telefonanrufe) genutzt. (link)

Angler-Phishing: Beim Angler-Phishing wird vor allem versucht, Nutzer:innen von sozialen Netzwerken zu täuschen. (link)

Quishing: Quishing ist eine Form des Phishings, bei der QR-Codes gescannt werden. (link)

Clone-Fishing: Beim Clone-Fishing wird eine echte, von einer vertrauenswürdigen Institution ausgesandte E-Mail verwendet, bei der der echte Link durch einen manipulierten Link ersetzt wird. (link)

Whaling: Whaling beschreibt das gezielte Phishing von Menschen in Führungspositionen. (link)

Baiting: Beim „Baiting“ wird mithilfe eines Köders versucht, Menschen dazu zu bringen, sensible Daten preiszugeben bzw. Schadsoftware auf ihren Laptop zu laden, um an diese Daten zu gelangen. Beispiele für Köder sind versprochene Geschenke, kostenlose Software, starke Rabatte usw. (link)

Erpressung: Erpressung geschieht durch die Androhung, sensible Informationen offenzulegen oder Systeme zu stören, wenn kein Lösegeld gezahlt wird. Angreifer schüren Angst, um ihre Opfer unter Druck zu setzen. (link)

Malware: Malware ist der Überbegriff für jegliche Art von schädlicher Software.

Ransomware: Ransomware ist eine Schadsoftware, die Daten auf dem Gerät verschlüsselt oder den Zugriff auf Speichersysteme sperrt. Um wieder an die Daten zu gelangen, fordern die Angreifer ein Lösegeld. (link)

Virus: Viren sind Programme, die sich selbst vervielfältigen und möglichst viele Netzwerke und Datensysteme infizieren.

Trojaner: Trojaner sind Softwareprogramme, die sich als nützliche Programme tarnen und im Hintergrund heimlich Türen für Angreifer öffnen.

Cyberbedrohungen

Cybersicherheit: Bei der Cybersicherheit geht es darum, digitale Infrastrukturen (inklusive Software, Server, Daten, Geräte etc.) vor böswilligen Angriffen zu schützen und unbefugten Zugriff sowie Schäden zu vermeiden. Dabei stehen laut EU die Vertraulichkeit (Datenzugriff nur für Berechtigte), Integrität (transparente Veränderung von Daten) und Verfügbarkeit (Funktionsfähigkeit von Systemen) im Vordergrund. Dieses sogenannte „CIA-Triade"-Modell (Confidentiality, Integrity, Availability) bildet die Grundlage moderner Sicherheitskonzepte. (link Cybersicherheit ist keinesfalls ein rein technisches Problem, sondern hat massive strategische, politische und wirtschaftliche Konsequenzen.

Cyberattacken: Bei Cyberattacken werden technische Schwachstellen und menschliche Fehler ausgenutzt, um Schäden an digitalen Infrastrukturen anzurichten, Daten zu stehlen, Systeme lahmzulegen oder Lösegeld zu erpressen. (link) Kritische Infrastrukturen (Energie, Gesundheit, Verkehr, Finanzen), öffentliche Verwaltungen, KMUs und Privatpersonen sind alle von einem reibungslosen Funktionieren dieser Systeme abhängig.

Bedrohung der Verfügbarkeit: Die Bedrohung der Verfügbarkeit besteht darin, dass Systeme und Dienste unbrauchbar gemacht werden, beispielsweise durch Denial-of-Service-Angriffe (DoS/DDoS), bei denen Server durch massenhafte Anfragen überlastet werden (link)

Malware: Das Ziel der Malware besteht darin, Kontrolle über Systeme zu erlangen und die Opfer der Cyberattacke (Privatpersonen, öffentliche Institutionen, Unternehmen, etc, ...) dann zu erpressen. Dies kann beispielsweise durch die Verschlüsselung von Daten erfolgen. Es werden auch Drohungen mit der Veröffentlichung oder dem endgültigen Verlust der Daten ausgesprochen. (link)

Gefährdung von Daten: Der unbefugte Zugriff auf sensible oder geschützte Daten wie zum Beispiel beim Hacking, Phishing, Insider-Missbrauch oder mangelhafte Zugangskontrollen stellt eine Gefährdung der Daten dar. (link)

Beispiel EU:

Angriff aufs Europäische Parlament: Im Jahr 2022 wurde die Website des Europäischen Parlaments Ziel eines hochentwickelten Cyberangriffs einer dem Kreml nahestehenden Hackergruppe, kurz nachdem europäische Abgeordnete Russland als Staatssponsor des Terrorismus eingestuft hatten. Die IT-Dienste des Parlaments konnten den Angriff zwar abwehren, doch der Vorfall unterstreicht die wachsende Bedrohung durch staatlich geförderte Cyberattacken in der EU. (link)

Angriff auf nationale Grundversorger: Französische Krankenhäuser (das Centre Hospitalier Sud Francilien in Corbeil-Essonnes nahe Paris, das Krankenhaus in Cannes sowie das Centre Hospitalier de Versailles) waren wiederholt Ziel von Ransomware-Angriffen. Dabei verschlüsseln Hacker Systeme, fordern Lösegeld und drohen damit, sensible Patientendaten zu veröffentlichen. Dies führte unter anderem dazu, dass Krankenhäuser Notfallpatienten abweisen mussten. (eca.europa)

Angriff auf IT Infrastruktur: Im Juli 2021 wurde der Landkreis Anhalt-Bitterfeld Ziel eines Ransomware-Angriffs, der zur Verschlüsselung zentraler Server und zur Lahmlegung der gesamten Verwaltung führte. Der Landkreis musste Sozialleistungen vorübergehend stoppen

und konnte über 200 Tage lang zahlreiche bürgernahe Dienstleistungen nicht regulär anbieten. Die Gesamtkosten beliefen sich auf rund 2,5 Millionen Euro, und einige Daten konnten bis heute nicht vollständig wiederhergestellt werden. (link) (link)

EU Cybersicherheitsstrategie: Aufgrund der EU-Cybersicherheitsstrategie und der NIS-Richtlinie wurden nationale Regelungen verabschiedet. Dabei sind die Einrichtung nationaler CERTs/CSIRTs (Computer Emergency Response Teams), Meldepflichten für Cybervorfälle, Anforderungen an Betreiber kritischer Infrastrukturen sowie die Förderung von Forschung, Innovation und Bewusstseinsbildung von großer Bedeutung. (link)

Cyberbedrohung am Arbeitsplatz: Cyberbedrohung am Arbeitsplatz: Beschäftigte sind oft das „Einfallstor" für Angriffe und gleichzeitig die ersten Betroffenen bei Ausfällen, Datenlecks oder Erpressungen. Typische Risiken im Arbeitsalltag sind beispielsweise unsichere Passwörter, fehlende Software-Updates oder das Öffnen verdächtiger Anhänge. (link)

Wahlmanipulation Slovenien: Der israelisches Privatgeheimdienst- und Überwachungsunternehmen, BlackCube, wird im Vorfeld der slowenischen Parlamentswahl 2026 verdächtigt gemeinsam mit lokalen Akteur:innen verdeckte Aufnahmen und kompromittierendes Material genutzt zu haben, um die Regierung Golob mit Korruptionsvorwürfen zu belasten und so die Wahl zu beeinflussen. (link)

QUELLENHINWEISE

Anmerkungen

1. Das Weltwirtschaftsforum (WEF) ist eine internationale Organisation für öffentlich-private Zusammenarbeit, die führende Akteure aus Politik und Wirtschaft zusammenbringt, um globale Agenden zu gestalten (World Economic Forum, 2026). Ihr jährlicher Bericht „Global Cybersecurity Outlook" misst die weltweite Cyber-Bedrohungslage sowie die Wahrnehmung und Bereitschaft globaler Entscheidungsträger (World Economic Forum, 2026).

2. CISO (Chief Information Security Officer): Das für die Informationssicherheit verantwortliche Leitungsorgan einer Organisation, das die strategische und operative Steuerung von Cyberrisiken (wie Ransomware oder Lieferketten-Resilienz) verantwortet und die Schnittstelle zwischen der technischen Abwehrebene und der Geschäftsführung bildet (World Economic Forum, 2026).

3. Die NIS-2- und die CER-Richtlinie werden in Cybersecurity Act 2 (2026) als „Schwesterrichtlinien" bezeichnet (Europäische Kommission, 2026). Physische und digitale Sicherheit sind untrennbar miteinander verwoben (Richtlinie (EU) 2022/2557, 2022). Es gibt gegenseitige Anerkennung, bei der unter CER als „kritisch" identifizierte Einrichtungen im Rahmen der NIS-2 automatisch als „wesentliche Einrichtungen" eingestuft werden, was ein einheitlich hohes Schutzniveau sicherstellt (Richtlinie (EU) 2022/2557, 2022). Um Doppelarbeit zu vermeiden und den Verwaltungsaufwand für Unternehmen zu minimieren, schreiben die Richtlinien zudem eine enge Zusammenarbeit der Behörden sowie den Austausch von Informationen über Vorfälle vor, wodurch Redundanzen bei Aufsichts- und Meldeprozessen effizient verhindert werden (Richtlinie (EU) 2022/2557, 2022).

4. Energie (Strom, Gas, Öl, Wasserstoff), Verkehr (Luft, Schiene, Straße, See), Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen (Krankenhäuser, Labore, Apotheken), Trinkwasserversorgung, Abwasserbewirtschaftung, Digitale Infrastruktur (Rechenzentren, Cloud, DNS, IXPs), Verwaltung (zentrale und regionale Ebene) und Raumfahrt (Richtlinie (EU) 2022/2555, 2022).

5. Post und Kurierdienste, Abfallbewirtschaftung, Herstellung, Verarbeitung und Vertrieb chemischer Stoffe, Herstellung, Verarbeitung und Vertrieb von Arzneimitteln, Herstellung, Verarbeitung und Vertrieb von Medizinprodukten, Verarbeitung und Vertrieb von Lebensmitteln, Öffentliche elektronische Kommunikationsnetze und dienste und Anbieter bestimmter digitaler Dienste (z. B. soziale Plattformen, Suchmaschinen, OnlineMarktplätze) (Richtlinie (EU) 2022/2555, 2022).

6. Vorfälle mit schwerwiegenden Betriebsstörungen oder hohen finanziellen Verlusten (Richtlinie (EU) 2022/2555, 2022).

7. CSIRT (Computer Security Incident Response Team): Eine spezialisierte Einheit, die für die Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen zuständig ist, technische Unterstützung bei der Reaktion auf Angriffe leistet und als zentrale Informationsdrehscheibe für die operative Zusammenarbeit fungiert (Europäische Kommission, 2026a).

8. NISG ist die österreichische Umsetzung der NIS-2-Richtlinie.

9. Ein CERT (Computer Emergency Response Team) ist eine spezialisierte Expertengruppe zur Gewährleistung der Sicherheit von Netz- und Informationssystemen, die Organisationen bei der Vermeidung, Erkennung und operativen Bewältigung von Cyber-Risiken und Sicherheitsvorfällen unterstützt (Richtlinie (EU) 2022/2555, 2022)

10. In Österreich CERT.at und/oder GovCERT (Bundesministerium für Inneres, 2024)

11. Dazu zählen Kreditinstitute (Banken), Zahlungsinstitute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen, Versicherungsunternehmen und Zentralverwahrer (Verordnung (EU) 2022/2554, 2022).

12. Auch Unternehmen, die kritische IT-Dienste für den Finanzsektor bereitstellen (z. B. Cloud-Anbieter wie Amazon Web Services oder Microsoft Azure), fallen unter den Überwachungsrahmen (Verordnung (EU) 2022/2554, 2022).

13. IoT (Internet of Things / Internet der Dinge): Elektronische Geräte (wie smarte Haushaltsgeräte, Wearables oder industrielle Sensoren), die mit dem Internet vernetzt sind, um Automatisierung, Datenerhebung sowie Fernsteuerung zu ermöglichen, wobei sie aufgrund ihrer Vernetzung häufig neue Angriffsflächen für Cyberaktivitäten bieten (Bundesministerium für Inneres, 2026)

14. Die ENISA arbeitet für die Kommission die „möglichen Schemata" aus die von der Kommission durch Durchführungsrechtsakte dann offiziell angenommen werden (Bundesministerium für Inneres, 2024).

15. Ein DNS-Diensteanbieter ist eine Einrichtung, die öffentlich verfügbare rekursive Dienste zur Auflösung von Domänennamen für Internet-Endnutzer oder autoritative Dienste zur Auflösung für Dritte erbringt (Richtlinie (EU) 2022/2555, 2022).

16. Entwicklung und Umsetzung von Cybersicherheitsrichtlinien und -strategien (ENISA, 2025)

17. Dieser Bereich bewertet die Fähigkeit der Gesellschaft, Cyberbedrohungen zu erkennen und Vorfälle zu verhindern (ENISA, 2025)

18. Dieser Bereich bewertet die Fähigkeit eines Mitgliedstaats, Cybersicherheitsoperationen durchzuführen und die Resilienz (Widerstandsfähigkeit) sicherzustellen (ENISA, 2025)

19. Gemessen wird die Fähigkeit des Privatsektors, Cyberbedrohungen und -vorfälle zu verhindern, zu erkennen und zu analysieren (ENISA, 2025)

20. Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität unterstützt nationale Behörden. In Österreich ist das Cyber Crime Competence Center (C4) im Bundeskriminalamt die relevante Behörde für IT-Ermittlungen und digitale Forensik (Bundesministerium für Inneres, 2024).

21. Hierunter fällt der Europäische Auswertige Dienst unter Leitung des Hohen Vertreters der Europäischen Union für Außen- und Sicherheitspolitik. In Säule drei finden Sie mehr zur Cyber Diplomacy Toolbox.

22. Der Europäische Auswärtige Dienst ist als Beobachter dabei.

23. Die Kommission nimmt als Beobachter teil.

24. Durch die ENISA

25. Das EU-INTCEN ist das zivile nachrichtendienstliche Analysezentrum der Union und bildet das Rückgrat für die Lageerfassung im Cyberraum (Europäische Kommission, 2020)

26. Sie entwickelt weltweit gültige Standards in fast allen technischen und nicht-technischen Bereichen (Europäische Kommission, 2020).

27. Die Internationale Fernmeldeunion ist eine Sonderorganisation der Vereinten Nationen für Informations- und Kommunikationstechnologien (Europäische Kommission, 2020).

28. Die Internationale Elektrotechnische Kommission ist für die weltweite Normung im Bereich der Elektrotechnik und Elektronik zuständig (Europäische Kommission, 2020).

29. Das Europäische Institut für Telekommunikationsnormen ist eine offiziell anerkannte europäische Normungsorganisation mit Sitz in Frankreich (ENISA, 2026)

30. Das IEEE ist ein weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informationstechnik (Europäische Kommission, 2020).

31. Ein sicherheitsrelevanter Fehler im Windows-Betriebssystem, der durch Design, Implementierung oder Konfiguration entstehen kann (Bendiek & Schulze, 2021).

32. Ein Exploit ist eine Methode oder ein spezifischer Programmcode, der dazu dient, eine Sicherheitslücke (Schwachstelle) in Hardware- oder Softwarekomponenten auszunutzen. Dadurch können Angreifer unbeabsichtigte Befehle ausführen, wie etwa ein Programm zum Absturz bringen, Benutzerrechte erweitern oder beliebigen Schadcode ausführen (Bendiek & Schulze, 2021).

33. Ein Netzwerkprotokoll ist ein standardisierter Satz von Regeln für den Datenaustausch zwischen Geräten in einem Netzwerk. Es ermöglicht beispielsweise den gemeinsamen Zugriff auf Dateien oder Drucker (Steinberg et al., 2021).

34. Ein im WannaCry-Code eingebetteter Mechanismus; durch die Registrierung einer spezifischen Internetadresse stoppte ein Sicherheitsforscher die weitere Ausbreitung und Verschlüsselung der Malware (House of Commons, 2018)

35. Prozesse zur systematischen Installation von Software-Updates, um Sicherheitslücken wie MS17-010 zu schließen (EuRepoC, 2026b).

36. Die EWCS (European Working Conditions Survey; Europäische Erhebung über die Arbeitsbedingungen) ist eine umfassende Umfrage zur Überwachung der Arbeitsqualität in Europa, die von Eurofound durchgeführt wird (EPRS, 2025).

37. Großunternehmen sind Unternehmen mit mehr als 250 Mitarbeitern und Kleinbetriebe sind Unternehmen mit weniger als 50 Mitarbeitern.

38. Kronos ist eine spezialisierte Softwareplattform für das algorithmische Management (AM), die zunehmend in Sektoren wie der Logistik und dem Gesundheitswesen eingesetzt wird, um menschliche Managementfunktionen zu automatisieren (EPRS, 2025).

39. Hubstaff ist eine Softwareplattform zur Zeiterfassung und Produktivitätsüberwachung für Teams, mit der Arbeitszeiten erfasst, Aktivitäten anhand von Screenshots nachverfolgt und damit verbundene Arbeitsabläufe wie die Berichterstellung oder Zahlungen automatisiert werden können (AnySecura, 2026).

40. Die Gig-Economy beschreibt einen Teil des Arbeitsmarktes, in dem kleine Aufträge kurzfristig über digitale Plattformen an unabhängige Auftragnehmer, Freiberufler oder geringfügig Beschäftigte vermittelt werden (Dragano et al., 2021). Ein Kernproblem ist die häufige Einstufung der Arbeiter als Selbstständige, obwohl sie durch Algorithmen ähnlich stark kontrolliert werden wie Angestellte (European Commission, 2021).

41. HireVue ist eine KI-gestützte Video-Interview- und Recruiting-Plattform, mit der Unternehmen Bewerber:innen per On-Demand- oder Live-Video vorsortieren und bewerten (Guardian, 2018).

42. Cognissess ist ein Anbieter für kognitive Tests und psychometrische Assessments, der im Recruiting zur Einschätzung von Fähigkeiten, Eignung und Potenzial eingesetzt wird (Guardian, 2018).

43. Social Engineering-Angriffe bezeichnen psychologische Manipulationstaktiken, mit denen Angreifer Personen dazu verleiten, unbewusst oder unfreiwillig Zugriff auf Systeme, Daten oder finanzielle Ressourcen zu gewähren (Abendroth Dias et al., 2025).

44. Darcula ist eine chinesischsprachige Phishing-as-a-Service-Plattform für weltweite Betrugskampagnen per SMS, iMessage und RCS, die gefälschte Webseiten bekannter Marken erstellt (Swiss Cybersecurity, 2024). Sie imitiert mehr als 200 Organisationen weltweit und nutzt automatisierte Phishing-Kits, um Mitarbeiter täuschend echt wirkende Login-Seiten anzuzeigen (ENISA, 2025).

45. Lucid ist eine Phishing-as-a-Service-Plattform, die von der chinesischen Cyberkriminalitätsgruppe XinXin betrieben wird (Netcraft, 2025). Diese fokussiert sich auf mobile Messaging-Dienste (iMessage und RCS) und erreichte damit Ziele in über 88 Ländern (ENISA, 2025).