MANZ – QUALITÄT SEIT 1849

11 | 2025 | 773–860 | ecolex

ecolex

FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT

Schwerpunkt

Cybercrime

> NIS-2
> Hacking
> Prävention

Recht hören. Der ecolex-Podcast!

Besitzstörung durch Kfz

Kartellschadenersatz

Geschäftsführerhaftung

Kündigungsschutz im Ausland

Stabilitätsabgabe

Geheimhaltung im IFG

ECOLEX.MANZ.AT

ISSN 1022-9418

MANZ

Checkliste: Aktuelle Cybercrime-Phänomene und Präventionsmaßnahmen für Unternehmen

CHECKLISTE. Cybercrime entwickelt sich zu einer immer größeren Gefahr für Unternehmen: Täter agieren vermehrt in professionalisierten Strukturen und unter Einsatz künstlicher Intelligenz. Schwachstellen im Sicherheitssystem oder unzureichende Ressourcen werden gezielt ausgenutzt. Ransomware, Phishing-Angriffe und Online-Betrugsfälle führen nicht nur zu finanziellen Schäden, sondern bergen auch rechtliche und reputative Risiken. Präventionsmaßnahmen zur Sensibilisierung von Mitarbeitern und strukturierte Reaktionspläne sind essenziell, um Cybercrime-Angriffe frühzeitig zu erkennen und wirksam abzuwehren.
ecolex 2025/429

Mag.[a] **Claudia Brewi** ist Rechtsanwältin in Wien und Vorstandsmitglied der Austrian White Collar Crime Association (AWCCA) – Vereinigung für Wirtschaftsstrafrecht.

A. Aktuelle Cybercrime-Phänomene und Bedrohungen für Unternehmen

Cybercrime stellt Unternehmen in Österreich und Deutschland zunehmend vor komplexe Herausforderungen.[1)] Während klassische Delikte wie Betrug digital erweitert werden, gewinnen spezifische Phänomene wie Ransomware und Phishing-Angriffe massiv an Bedeutung.[2)] Täter bedienen sich zunehmend KI, um Angriffe zu personalisieren und schwerer erkennbar zu machen. Zudem hat sich ein regelrechter *„Marktplatz"* für Cybercrime entwickelt: Über *„Crime as a Service"* können Täter im Darknet Expertise und Dienstleistungen zukaufen.[3)] Die Tätergruppen im Bereich Cybercrime agieren professionalisiert und sind hochgradig international vernetzt sowie mit erheblichen finanziellen Mitteln ausgestattet.[4)] Ländergrenzen oder Sprachbarrieren verlieren zunehmend an Bedeutung. Damit wächst die Zahl potenzieller Opfer ebenso wie die Reichweite der Angriffe.[5)]

Die daraus resultierenden Schäden stellen Unternehmen vermehrt vor große finanzielle und reputative Herausforderungen. Daneben sehen sich Unternehmen oder ihre Führungskräfte auch mit zivil- und strafrechtlichen Haftungsansprüchen konfrontiert.[6)] Fehlende oder unzureichende Compliance- und Sicherheitsmaßnahmen können zu Organhaftungen führen; Datenschutzverletzungen[7)] können Verwaltungsstrafen und Schadenersatzforderungen nach sich ziehen. Zudem verschärft die NIS-2-RL die Anforderungen an IT-Sicherheit und Incident-Response erheblich.[8)] Effektive Präventionsmaßnahmen sind daher nicht nur wirtschaftlich geboten, sondern können auch exkulpierend wirken.

B. Präventionsmaßnahmen zur Schadens- und Haftungsminimierung

1. Cybercrime

Cybercrime-Angriffe können Unternehmen in unterschiedlicher Art und Weise treffen.[9)] Durch Phishing-Angriffe können sensible Daten wie Betriebsgeheimnisse, Zahlungsdaten und digitale Zugriffe in die Hände von Tätern gelangen. Durch Ransomware blockierte Kommunikationswege oder Datenverluste können binnen Stunden den Betrieb und die Handlungsfähigkeit von Unternehmen massiv einschränken. Darüber hinaus sind Unternehmen aufgrund der Digitalisierung vermehrt Betrugsfällen ausgesetzt. Wirksame Präventionsmaßnahmen sind daher essenziell, um Cybercrime-Angriffe oder zumindest den damit verbundenen Schaden möglichst gering zu halten. Unternehmen müssen sicherstellen, dass sie im Ernstfall reagieren und va die Geschäftskontinuität sichern können. Sie müssen die notwendigen technischen, organisatorischen und rechtlichen Maßnahmen zur Angriffsabwehr und Stärkung ihrer Resilienz setzen.

Checkliste allgemeiner Präventionsmaßnahmen[10)]:

- ✓ **Mitarbeitersensibilisierung:** Laufende Information und Schulungen zu aktuellen Cybercrime-Fällen sowie sicherem Umgang mit E-Mails, Passwörtern und verdächtigen Anfragen.
- ✓ **IT-Infrastruktur stärken:** Einsatz moderner Sicherheitslösungen (Firewalls, Virenschutz, Spamfilter, Multi-Faktor-Authentifizierung, KI-gestützte Tools). Regelmäßige Updates, um Sicherheitslücken zu schließen.
- ✓ **Datensicherung und Backups:** Regelmäßige, verschlüsselte Sicherungen mit geprüften Wiederherstellungstests, um Datenverluste zu vermeiden und Betriebsfähigkeit sicherzustellen.

---

1) *Deloitte*, Cyber Security Report 2024 (2025) 5 ff; *KPMG*, Cybersecurity in Österreich (2025) 11 ff, 37 ff; *EY*, Datenklaustudie 2025 (2025) 24 ff.
2) *BMI*, Polizeiliche Kriminalstatistik 2024 (2025) 57.
3) *Brewi/Royer*, Praxishandbuch Cybercrime (2025) 8.
4) *EY*, Datenklaustudie 2025 (2025) 30.
5) *BMI*, Polizeiliche Kriminalstatistik 2024 (2025) 17; *KPMG*, Cybersecurity in Österreich (2025) 41.
6) *Krepil* in *Brewi/Royer* (Hrsg), Praxishandbuch Cybercrime (2025) 347 ff.
7) *EY*, Datenklaustudie 2025 (2025) 28; *Sekanina/Wrabetz* in *Brewi/Royer* (Hrsg), Praxishandbuch Cybercrime (2025) 395 ff.
8) *EY*, Datenklaustudie 2025 (2025) 57; *Blümel* in *Brewi/Royer* (Hrsg), Praxishandbuch Cybercrime (2025) 311 ff.
9) *Haunschmid* in *Brewi/Royer* (Hrsg), Praxishandbuch Cybercrime (2025) 28 ff; *Deloitte*, Cyber Security Report 2024 (2025) 8, 12; *KPMG*, Cybersecurity in Österreich (2025) 59 ff, 150; *EY*, Datenklaustudie 2025 (2025) 27.
10) *BMI*, Polizeiliche Kriminalstatistik 2024 (2025) 21 ff; *Deloitte*, Cyber Security Report 2024 (2025) 13, 19 f; *EY*, Datenklaustudie 2025 (2025) 35 ff, 67 ff; *CrowdStrike*, Global Threat Report 2025 (2025) 11 f.

- ✓ **Incident-Response-Plan:** Festgelegte Notfallmaßnahmen mit klaren Zuständigkeiten, Kommunikationswegen und Einbindung externer Berater.
- ✓ **Business Continuity Management:** Strategien zur Aufrechterhaltung wesentlicher Geschäftsprozesse während und nach einem Angriff.
- ✓ **Krisenkommunikation:** Ausarbeitung interner und externer Kommunikationslinien sowie Festlegung von Freigabemechanismen im Ernstfall.
- ✓ **Risikoanalysen:** Kontinuierliche Bewertung und Kategorisierung von Risiken sowie technischer Schwachstellen zur Früherkennung.
- ✓ **Compliance-System:** Implementierung und laufende Anpassung interner Richtlinien (Betrugsprävention, NIS-2, DSGVO, Passwort- und Gerätemanagement, Meldepflichten).
- ✓ **Penetration-Tests:** Regelmäßige Simulationen von Angriffsszenarien zur Prüfung der Reaktionsfähigkeit und Beseitigung identifizierter Schwachstellen.

2. Phishing

Phishing-Angriffe stellen für Unternehmer noch immer eines der größten Risiken im Bereich Cybercrime dar. Beim Phishing versuchen Täter, betroffene Personen zur Preisgabe sensibler Personen-, Zugangs- oder Zahlungsdaten zu bewegen. Dazu geben sie sich mittels betrügerischer E-Mails, SMS-Nachrichten, Briefen, Telefonanrufen oder Anzeigen/Webseiten als vertrauenswürdiges Gegenüber aus (zB als Bankinstitut, Behörde, Zustelldienst) und versuchen, die Daten mittels Eingabelinks oder mündlicher Auskünfte herauszulocken. Es werden täuschend echte Logos oder Designs eingesetzt, oft in Kombination mit Spoofing (Fälschung von Absender- oder Rufnummerndaten).[11)]

Mit Hilfe von KI und Social Engineering werden Angriffe zunehmend perfektioniert. KI ermöglicht es, Erkennungsmerkmale und Kommunikationsmuster bekannter Institutionen oder Personen professionell nachzubilden.[12)] Bei Social Engineering wird gezielt die innere Struktur eines Unternehmens bzw das Umfeld eines Mitarbeiters analysiert und Vertrauens- oder Autoritätsverhältnisse ausgenutzt, um diese zur Bekanntgabe von Daten zu verlocken.[13)] Bereits ein unbedachter Klick oder ein kurzes Telefonat kann den Zugang zu Zahlungsdaten und Systemen eines Unternehmens eröffnen und neben widerrechtlichen Auszahlungen insb auch Folgeangriffe wie Ransomware begünstigen.

- ✓ **Einschränkung von Zugriffsrechten:** Zugriff auf sensible Daten und Systeme auf *„Need-to-know"*-Basis.
- ✓ **Klare Verhaltensrichtlinien:** Überprüfung von E-Mails, Telefonnummern und Links auf Übereinstimmung mit dem bekannten Aufbau. Gegenprüfung mit bekannten Kontaktdaten.
- ✓ **Phishing-Tests:** Sensibilisierung für verdächtige Nachrichten und typische Angriffsmuster.
- ✓ **Open-Source-Recherche:** Abfrage von (Unternehmens-) Webseiten im Hinblick auf Phishing-Warnungen.

3. Ransomware

Nach aktuellen Analysen hat sich die Zahl der von Ransomware-Angriffen betroffenen Unternehmen zw 2022 und 2025 nahezu verdoppelt.[14)] Dabei verschaffen sich Täter Zugang zu IT-Systemen, verschlüsseln Daten und fordern anschließend Lösegeld für deren Freigabe.[15)] Besonders KMU sind gefährdet. Fehlende Ressourcen für IT-Sicherheit, veraltete Systeme und unzureichende Backup-Strategien machen sie zu bevorzugten Angriffszielen. Doch auch große Unternehmen sind aufgrund der vermehrten Digitalisierung von Geschäftsprozessen exponiert.[16)] Selbst partielle Ausfälle der IT-Infrastruktur können weitreichende Folgen haben – von der Unterbrechung der Kommunikation oder Produktion bis hin zum Stillstand ganzer Geschäftsabläufe. Bei der Bestimmung der Höhe des geforderten Lösegelds orientieren sich Täter einerseits an der Finanzkraft des Unternehmens sowie andererseits an den Sicherheitsvorkehrungen und Backup-Strategien.[17)] Daneben sind Unternehmen aufgrund des Datenabflusses Reputations- und Haftungsfolgen ausgesetzt.

Auch in diesem Bereich machen sich Täter vermehrt KI zunutze, um Sicherheitslücken zu erkennen und zu umgehen. Der infolge eines Ransomware-Angriffs stattfindende Austausch mit Tätern ist hochgradig professionalisiert. Die Gewährleistung der Rückgabe bzw Entschlüsselung der Daten nach Lösegeldzahlung ist essenziell für das *„Geschäftsmodell"* der Täter.

- ✓ **Zero Trust Prinzip:** Jeder Zugriff muss authentifiziert und autorisiert werden.
- ✓ **Netzwerksicherheit:** Überwachung, Erkennen und Blockieren verdächtiger Aktivitäten, um unautorisierte Zugriffe oder Datenabflüsse hintanzuhalten.
- ✓ **Meldesysteme:** Etablierung eines Mechanismus, auf dessen Basis Cyberangriffe sofort gemeldet werden können, um die notwendigen Maßnahmen zu ergreifen.
- ✓ **Segmentierung:** Aufteilung der Netzwerke zur Einschränkung der Ausbreitung von Schadsoftware.

4. Online-Betrugsfälle

Betrugsdelikte sind kein neues Phänomen, erreichen durch die fortschreitende Digitalisierung jedoch eine neue Dimension.[18)] Täter nutzen gezielt organisatorische Schwachstellen, digitale Kommunikationswege und die Automatisierung geschäftlicher Abläufe, um Unternehmen erheblich zu schädigen. Dabei treten Onlinebetrugsfälle in unterschiedlichen Erscheinungsformen auf, die jeweils auf Täuschung und Missbrauch von Vertrauen beruhen.[19)] Besonders relevant sind:

a) CEO-Fraud (Fake President Fraud)

Beim sog CEO-Fraud geben sich Täter als Gf oder leitende Angestellte aus und veranlassen Mitarbeiter zur Durchführung vermeintlich dringender Zahlungen oder zur Herausgabe sensibler Daten. Typisch sind hoher Zeitdruck, die Aufforderung zu Geheimhaltung und die Verwendung gefälschter Absenderadressen oder Telefonnummern.[20)] Zunehmend werden wiederum Social Engineering und Deepfakes eingesetzt. Durch im Internet veröffentlichte Bilder und Videos können das Erscheinungsbild und sogar die Stimme von Personen täuschend echt nachgebildet werden. Dadurch wirken Angriffe noch glaubwürdiger und können selbst geschulte Mitarbeiter leicht

11) *BMI/BK*, Cybercrime Report 2023 (2024) 27 f.
12) *CrowdStrike*, Global Threat Report 2025 (2025) 6.
13) *CrowdStrike*, Global Threat Report 2025 (2025) 6.
14) *Deloitte*, Cyber Security Report 2024 (2025) 4.
15) *BMI/BK*, Cybercrime Report 2023 (2024) 215 f.
16) *Deloitte*, Cyber Security Report 2024 (2025) 3.
17) *BMI*, Polizeiliche Kriminalstatistik 2024 (2025) 23.
18) *KPMG*, Cybersecurity in Österreich (2025) 89.
19) *BMI*, Polizeiliche Kriminalstatistik 2024 (2025) 20.
20) *Brewi* in *Brewi/Royer* (Hrsg), Praxishandbuch Cybercrime (2025) 73 f.

getäuscht werden.[21] In Österreich kam es bereits zu Millionenschäden durch CEO-Fraud.[22]

- ✓ **Sensibilisierung auf Deep Fakes:** Achtsamkeit auf verwaschene Konturen, unnatürliche Mimik, unlogische Schatten oder Hintergründe, fehlendes Blinzeln oder metallischen, monotonen Klang der Stimme oder falsche Aussprache.
- ✓ **Multi-Faktor-Authentifizierung:** Einrichtung und Funktionalität einer zumindest Zwei-Faktor-Authentifizierung bei Zahlungen.
- ✓ **Verfizierungsprozesse:** Zwingende Freigabe von Transaktionen besonderer Höhe zB durch Rückruf oder schriftliche Bestätigung.
- ✓ **Sicherheitsfragen:** Prüfung der Identität und Legitimität des Gegenübers durch persönliche Rückfragen bzw zu Unternehmensinterna.

b) Bestellbetrug

Beim Bestellbetrug können Täter sowohl auf Dienstleister- oder Kundenseite auftreten.[23] Im ersten Fall bieten Täter auf Webseiten tatsächlich nicht existierende oder minderwertige Waren oder Dienstleistungen an. Dabei kommt es häufig auch zu Identitätsdiebstählen, indem sich die Täter zur Täuschung über ihre Seriosität bspw fremder Unternehmensdaten im Impressum bedienen. Im zweiten Fall geben sich Täter als vermeintlich seriöse Geschäftspartner aus, bestellen Waren oder Dienstleistungen und leisten keine Zahlung.

Unternehmen sind daher einerseits wirtschaftlichen Schäden bei Fake-Bestellungen ausgesetzt und andererseits einer potenziellen Rufschädigung bei Identitätsmissbrauch.

- ✓ **Bonitäts- und Identitätsprüfung:** Datenabgleich mit bekannten und öffentlichen Daten bei aufrechten und neuen Geschäftsbeziehungen.
- ✓ **Monitoring:** Regelmäßige Prüfung der eigenen Unternehmensdaten im Internet, um Identitätsmissbrauch frühzeitig zu erkennen.
- ✓ **Sensibilisierung:** Schulungen im Einkauf und in der Buchhaltung zur Erkennung verdächtiger Bestellungen und Rechnungen.
- ✓ **Datensammlung:** Verdachtsfälle umgehend melden und dokumentieren.

c) Investmentbetrug (Cyber-Trading-Fraud)

Auch wenn Investmentbetrugsfälle im Vergleich zu anderen Online-Betrugsformen nach der Polizeilichen Kriminalstatistik weniger weit verbreitet sind, waren sie dennoch 2024 für den größten finanziellen Schaden verantwortlich.[24] Beim Cyber-Trading-Fraud werden gefälschte Handels- oder Investmentplattformen betrieben, die vermeintlich seriöse Finanzprodukte oder Kryptowährungen anbieten. Nach ersten Einzahlungen verweigern die Täter Rückzahlungen, Plattformen verschwinden oftmals abrupt.[25] Betroffen sind sowohl Unternehmen als auch Mitarbeiter, die im geschäftlichen Kontext getäuscht werden.

- ✓ **KYC und Due Diligence:** Sorgfältige Prüfung von neuen Geschäftspartnern und Investitionsmöglichkeiten.
- ✓ **Zulassung der FMA:** Kontrolle, ob Anbieter über eine Zulassung der FMA oder einer anderen europäischen Finanzaufsicht verfügen.
- ✓ **Interne Richtlinien:** Festgelegte Prozesse und Genehmigungen für Investitionsentscheidungen.
- ✓ **Risikobegrenzung:** Einsatz von Limits für Investitionsbeträge und verpflichtendes Vier-Augen-Prinzip.

C. Exkurs: Reaktion auf Cybercrime-Angriffe

Auch bei bestmöglicher Prävention ist ein Restrisiko nie auszuschließen. Um den Schaden dennoch gering zu halten, ist insb der Faktor Zeit entscheidend sowie ein strukturiertes Vorgehen, das insb folgende Schritte in Absprache mit dem Management und IT-Experten umfassen sollte:[26]

- ✓ **Systemsicherung:** Betroffene Systeme sofort vom Netzwerk trennen, um eine Ausbreitung zu verhindern. Passwörter sämtlicher Plattformen und Anwendungen ändern.
- ✓ **Interne und externe Inkenntnissetzung:** Unverzügliche Information des Managements, insb der internen Finanz- und IT-Abteilung. Finanzdienstleister sollten sofort kontaktiert werden, um Transaktionen ggf noch zu stoppen.
- ✓ **Kunden- und Mitarbeiterinformation:** Transparente Kommunikation im Fall von Datenabflüssen; Bereitstellung konkreter Handlungsempfehlungen an Betroffene.
- ✓ **Beweissicherung:** Alle verfügbaren Daten und Unterlagen sichern, ua E-Mail-Korrespondenz, Chat-Verläufe, Kontaktdaten, Webseitenadressen, Zahlungsbelege. Erstellung eines chronologischen Protokolls des Vorfalls.
- ✓ **Spezialisten und Behörden:** Kontaktaufnahme mit externen Rechts-, IT- und PR-Beratern; ggf Einschaltung der Strafverfolgungs- und Datenschutzbehörde.
- ✓ **Versicherung:** Den Vorfall umgehend der Cyber- oder Haftpflichtversicherung melden, um Deckungsansprüche zu wahren.

Schlussstrich

Cybercrime verlangt von Unternehmen mehr als punktuelle Sicherheitsmaßnahmen: Erforderlich ist ein umfassendes Risikomanagement, das technische Vorkehrungen mit rechtlicher Compliance und organisatorischen Strukturen verbindet. Zentrale Bedeutung kommt dabei der Unternehmensleitung zu, die im Rahmen ihrer Sorgfaltspflichten für adäquate Schutzmechanismen zu sorgen hat. Eine klare Strategie, laufende Evaluierung und gelebte Sicherheitskultur sind entscheidend. Nur so können die Geschäftskontinuität gesichert, Haftungsrisiken minimiert und das Vertrauen der Kunden sowie Geschäftspartner gewahrt werden.

Nützliche Links

https://www.watchlist-internet.at

Watchlist Internet ist eine unabhängige Informationsplattform zu aktuellen Betrugsfällen im Internet und mit Tipps, um sich vor Internetbetrug zu schützen.

https://www.fma.gv.at/category/news/?cat=42

Auf der Webseite der FMA erfolgen regelmäßig Warnungen zu betrügerischen Geschäftspartnern.

[21] *CrowdStrike*, Global Threat Report 2025 (2025) 7 f.
[22] *Kurier*, Betrugsprozess zu FACC: Wenn der Chef nicht echt ist, https://kurier.at/wirtschaft/betrugsprozess-zu-facc-wenn-der-chef-nicht-echt-ist/400465165 (abgefragt am 22. 9. 2025).
[23] *BMI*, Polizeiliche Kriminalstatistik 2024 (2025) 20 f.
[24] *BMI*, Polizeiliche Kriminalstatistik 2024 (2025) 21 f.
[25] *BMI*, Öffentliche Sicherheit 3–4/24.
[26] *EY*, Datenklaustudie 2025 (2025) 79.