WIRTSCHAFTSKAMMER WIEN
Werbung · Marktkommunikation

Digital. Sicher.

Praxisleitfaden Cybersecurity

Version 1.0 | Jänner 2026

Dr. Cornelius Granig

Liebe Mitglieder, liebe Kolleg:innen,

wir sind die gewählte Interessenvertretung von rund 13.000 Unternehmen in der Wiener Kommunikations- und Werbebranche. Unser Ziel ist es, Rahmenbedingungen mitzugestalten, Orientierung bei komplexen Themen zu geben und Services bereitzustellen, die Ihren unternehmerischen Alltag spürbar erleichtern.

In einer zunehmend digitalisierten Wirtschaftswelt ist Cybersicherheit zu einer der zentralen Herausforderungen geworden, der wir uns proaktiv stellen müssen. Die Kommunikationsbranche gehört zu den am stärksten von Cyberangriffen bedrohten Wirtschaftszweigen. Das ist kein Zufall: Wir arbeiten tagtäglich mit sensiblen Kundendaten, entwickeln wertvolle kreative Konzepte und verantworten erhebliche Werbebudgets. Diese Werte machen uns zu einem attraktiven Ziel für Cyberkriminelle.

Der professionelle Umgang mit digitalen Risiken ist die Voraussetzung für wirtschaftliche Stabilität, verantwortungsbewusste Unternehmensführung und den langfristigen Erfolg jedes Unternehmens. Mit diesem Praxisleitfaden stellen wir Ihnen ein Werkzeug zur Verfügung, das Sie dabei unterstützt, Cyberrisiken strukturiert einzuordnen, Prioritäten zu setzen und passende Maßnahmen nachhaltig im Betrieb zu verankern – unabhängig von Unternehmensgröße oder technischem Vorwissen. Der Leitfaden ist auf die Bedürfnisse unserer Branche zugeschnitten, stärkt das Bewusstsein für aktuelle Bedrohungen und zeigt praxisnahe Maßnahmen zur Risikoreduktion auf.

Ergänzend können Sie auf konkrete Unterstützungsangebote der Wirtschaftskammer zurückgreifen – von der rund um die Uhr erreichbaren Cybersecurity-Hotline (0800 888 133) bis zu Checklisten und Informationsangeboten.

Ich lade Sie ein, den Leitfaden aktiv zu nutzen: als Grundlage für Entscheidungen, als Impuls für interne Gespräche und als Startpunkt, um die Sicherheitskultur im Team zu stärken. Jede konsequente Verbesserung erhöht nicht nur die Resilienz Ihres Unternehmens, sondern auch die Zukunftsfähigkeit unserer gesamten Branche.

Mit freundlichen Grüßen

Roland Grafl
Fachgruppenobmann-Stellvertreter
Fachgruppe Werbung und Marktkommunikation der Wirtschaftskammer Wien

Liebe Mitglieder, liebe Leser:innen,

unser Arbeitsalltag hat sich durch die Digitalisierung grundlegend verändert. Wir bewegen große Mengen sensibler Kundendaten, betreiben Datenbanken, managen Budgets und Social-Media-Profile. Moderne KI-Tools und Cloud-Plattformen helfen uns dabei – und öffnen dadurch gleichzeitig neue Angriffspunkte.

Cyberkriminelle haben das längst erkannt. Die Folge sind täuschend echte Phishing-E-Mails, Anrufe oder Chat-Nachrichten, die zu Passwörtern, Freigaben oder Zahlungsprozessen führen sollen. Ransomware kann Daten verschlüsseln, die Arbeitsfähigkeit innerhalb kurzer Zeit oft nachhaltig blockieren und existentiell bedrohliche Schäden anrichten. Kontoübernahmen in Social Media oder Ads können zu manipulativen Postings, unautorisierten Anzeigen oder Reputationsschäden führen. Zusätzlich entstehen Risiken über externe Tools, Dienstleister:innen und Lieferketten – bis hin zu falsch konfigurierten Cloud- oder Weboberflächen.

Künstliche Intelligenz macht die Lage ambivalent: Sie hilft, Auffälligkeiten früh zu erkennen und Schutzprozesse zu automatisieren. Gleichzeitig nutzen Angreifer:innen KI, um Täuschungen glaubwürdiger und skalierbarer zu machen – von perfekt formulierten Nachrichten bis zu Deepfakes und synthetischen Stimmen. Entscheidend ist daher nicht, ob wir KI einsetzen, sondern wie bewusst wir Chancen und Risiken steuern.

Dieser Praxisleitfaden übersetzt die wichtigsten Bedrohungen in konkrete, branchenrelevante Schritte: klare Verantwortlichkeiten und Prozesse, konsequente Mehrfaktor-Authentifizierung, sauberes Zugriffs- und Berechtigungsmanagement, regelmäßige Backups sowie kontinuierliche Sensibilisierung im Team – ergänzt um Hinweise zur sicheren Zusammenarbeit mit Partner:innen und Dienstleister:innen.

Nutzen Sie den Leitfaden als Fahrplan: Starten Sie mit den Basismaßnahmen, definieren Sie Prioritäten und bauen Sie Ihre Sicherheitsstrategie Schritt für Schritt aus. Jeder umgesetzte Schritt stärkt Ihre Resilienz – und schützt das, was unsere Arbeit ausmacht: Kreativität, Verlässlichkeit und Vertrauen.

Mit herzlichen Grüßen

Eva Mandl
Mitglied des Fachgruppenausschusses
Fachgruppe Werbung und Marktkommunikation der Wirtschaftskammer Wien

INHALTSVERZEICHNIS

1 Einleitung

Das Leben in der Informationsgesellschaft ist für uns alle zur Selbstverständlichkeit geworden. Digitale Technologien prägen unseren Alltag, unser Arbeitsumfeld und unsere Kommunikation. Besonders deutlich wurde dies während der Corona-Pandemie.

Die neuen Informations- und Kommunikationstechnologien haben dazu beigetragen, dass fast alle Bereiche des wirtschaftlichen und gesellschaftlichen Lebens trotz tiefgreifender Einschränkungen funktionsfähig blieben. Videokonferenzen ermöglichten neue Formen der Zusammenarbeit, digitale soziale Netzwerke sorgten für Austausch und Gemeinschaft, und Messenger-Dienste entwickelten sich spätestens in dieser Zeit zu einem unverzichtbaren Werkzeug für berufliche und private Kommunikation.

Die tiefgreifende und fast durchgängige Digitalisierung aller Bereiche unseres Lebens bringt jedoch nicht nur Vorteile mit sich, sondern stellt unsere Gesellschaft vor große Herausforderungen. Eine davon ist die wachsende Unsicherheit über die zukünftige Entwicklung des Arbeitsmarktes. Viele traditionelle Berufsbilder verändern sich grundlegend oder verschwinden, während neue, technologieorientierte Tätigkeitsfelder entstehen.

Der zunehmende Einsatz von „Künstlicher Intelligenz“ (nachfolgend: KI) führt dazu, dass Arbeitsprozesse automatisiert werden, was langfristig zu einer deutlichen Reduktion bestimmter Arbeitsplätze führen kann. Diese Umbrüche verlangen nicht nur nach technischen Kompetenzen, sondern auch nach einer Anpassung unserer Ausbildungssysteme und einer aktiven Auseinandersetzung mit den sozialen Folgen dieser Veränderungen.

Parallel dazu verschärft sich ein weiterer Trend, der unsere digitalisierte Gesellschaft stark belastet. Während die Nutzung digitaler Anwendungen in nahezu allen Lebensbereichen zunimmt, wächst auch die Zahl der Cyberangriffe in alarmierendem Ausmaß, was sich deutlich in der Kriminalitätsstatistik widerspiegelt. Bereits jede sechste in Österreich angezeigte Straftat wird im digitalen Raum begangen. Diese Entwicklung betrifft nicht nur große internationale Konzerne, sondern zunehmend auch kleine und mittlere Unternehmen, Selbstständige sowie Privatpersonen.

Gerade Unternehmerinnen und Unternehmer der Fachgruppe Werbung und Marktkommunikation stehen im Fokus dieser Bedrohungen. Ihre Tätigkeiten machen sie in vielfältiger Weise zu attraktiven Zielen für Cyberkriminelle. Sie arbeiten mit sensiblen Kunden- und Projektdaten, entwickeln wertvolle kreative Konzepte und verantworten oftmals erhebliche Budgets für Werbeschaltungen und Kampagnen. Viele betreiben umfangreiche Online-Profile, verwalten Social-Media-Plattformen oder organisieren digitale Marketingaktivitäten für ihre Kund:innen. Andere agieren als Influencer, arbeiten eng mit unterschiedlichen Plattformen zusammen und sind stark auf den sicheren Betrieb ihrer digitalen Kanäle angewiesen. Hinzu kommt die zunehmende Nutzung externer KI-Werkzeuge sowie Cloud-Dienste, die zwar weitere kreative und organisatorische Möglichkeiten eröffnen, zugleich aber auch neue Risiken mit sich bringen.

All diese Faktoren machen Unternehmen und Selbstständige im Bereich der Fachgruppe Werbung und Marktkommunikation zu besonders attraktiven Angriffszielen. Cyberangriffe zielen häufig darauf ab, Werbekonten zu manipulieren, Zugangsdaten abzugreifen oder kreative Inhalte zu stehlen. Die Folgen können gravierend sein. Sie reichen von der Beeinträchtigung laufender Kampagnen über den Diebstahl oder Verlust von Daten, damit einhergehende Reputationsschäden bis hin zu erheblichen finanziellen Belastungen durch Produktionsausfälle, Wiederherstellungsmaßnahmen oder Lösegeldforderungen professioneller Erpressungsnetzwerke.

In einer Branche, die sich durch Kreativität, Innovation, Geschwindigkeit und hohe digitale Präsenz auszeichnet, ist ein professioneller Umgang mit Cyberrisiken kein optionaler Zusatz mehr, sondern eine grundlegende Voraussetzung für wirtschaftliche Stabilität und langfristigen Erfolg.

Der vorliegende Praxisleitfaden soll dazu beitragen, das Bewusstsein für Cyberbedrohungen zu stärken, praxisnahe Orientierung zu bieten und konkrete Maßnahmen vorzustellen, mit denen Unternehmen ihre digitale Sicherheit erhöhen und Risiken wirksam reduzieren können.

Sie richtet sich an alle Mitglieder der Fachgruppe Werbung und Marktkommunikation, die sich aktiv mit den Herausforderungen des digitalen Zeitalters auseinandersetzen und ihre Organisationen verantwortungsvoll schützen wollen.

1.1 Verbesserung der Cyberhygiene

Der aus dem Griechischen stammende Begriff Hygiene bezeichnet traditionell die Gesamtheit wissenschaftlicher Erkenntnisse und praktischer Maßnahmen, die der Erhaltung und Förderung der Gesundheit dienen. Während sich dieser Begriff ursprünglich ausschließlich auf den menschlichen Körper und die physische Umwelt bezog, gewinnt er in Zeiten umfassender Digitalisierung eine erweiterte Bedeutung. Das Internet und die damit verbundenen Technologien haben sich in den vergangenen Jahrzehnten von einem spezialisierten Arbeitsinstrument zu einem allgegenwärtigen Bestandteil unseres gesellschaftlichen, wirtschaftlichen und privaten Lebens entwickelt. Digitale Systeme begleiten unseren Alltag in einer Intensität, die vergleichbar ist mit grundlegenden Infrastrukturen wie Energie oder Wasser.

Vor diesem Hintergrund gewinnen Fragen der digitalen Sicherheit zunehmend an Bedeutung. So wie mangelnde Hygiene im medizinischen Kontext zu Infektionen führt, kann eine unzureichende digitale Hygiene das Risiko für Datenverlust, Cyberangriffe und den Ausfall kritischer Systeme erheblich erhöhen. Um die Sicherheit und Funktionsfähigkeit unserer digitalen Umgebung zu gewährleisten, bedarf es daher eines systematischen und bewusst gestalteten Umgangs mit Risiken und Schutzmechanismen. Diese Gesamtheit an organisatorischen und technischen Maßnahmen wird heute unter dem Begriff „Cyberhygiene“ zusammengefasst.

Cyberhygiene beschreibt moderne Vorgehensweisen und Schutzvorkehrungen, mit denen digitale Systeme stabil, widerstandsfähig und sicher betrieben werden können. Ihr Ziel ist es, digitale Angriffsflächen zu minimieren und Schäden abzuwenden, die

durch unerlaubte Zugriffe, Schadsoftware oder technische Fehlkonfigurationen entstehen könnten. Ähnlich wie im Gesundheitswesen basiert das Konzept der Cyberhygiene auf einem Zusammenspiel aus geeigneten Werkzeugen, gelebten Routinen und kontinuierlicher Qualitätssicherung.

Im Analogievergleich zu Desinfektions- und Schutzmaßnahmen im Gesundheitswesen stehen im digitalen Bereich verschiedene technische Hilfsmittel zur Verfügung. Dazu zählen Firewalls, die unbefugte Zugriffe verhindern, Schadsoftwarescanner, die Angriffe erkennen und blockieren, sowie Werkzeuge zur Verschlüsselung sensibler Informationen. Ergänzt werden diese durch organisatorische Verfahren wie Mehrfaktor-Authentifizierung, sichere Passwortverwaltung oder die strukturierte Vergabe von Zugriffsrechten.

Wirksame Cyberhygiene verlangt mehr als punktuelle Interventionen. Unternehmen, Institutionen und auch Einzelpersonen müssen Strategien entwickeln, mit denen Sicherheitsmaßnahmen nahtlos in den täglichen Arbeitsablauf integriert werden. Automatisierte Prozesse übernehmen dabei eine zentrale Rolle. Dazu gehören regelmäßige Datensicherungen, die Aktualisierung von Softwarekomponenten, das Monitoring sicherheitsrelevanter Protokolle und die Kontrolle unüblicher Datenabflüsse. Entscheidend ist, dass diese Sicherheitsprozesse zuverlässig, wiederkehrend und möglichst ohne manuellen Aufwand ablaufen. Eine nachhaltige Sicherheitskultur kann nur entstehen, wenn diese Aufgaben selbstverständlich Teil der betrieblichen Routine werden.

Wie im Gesundheitsbereich Hygienevorschriften regelmäßig überprüft und angepasst werden müssen, so erfordert auch die Cyberhygiene eine fortlaufende Auseinandersetzung mit neuen Bedrohungen, technologischen Entwicklungen und veränderten organisatorischen Rahmenbedingungen. Werkzeuge und Verfahren verlieren mit der Zeit an Wirksamkeit, wenn sie nicht aktualisiert oder überprüft werden. Nutzerinnen und Nutzer müssen regelmäßig für sicherheitsrelevante Themen sensibilisiert werden, etwa durch verpflichtende Passwortänderungen, den Einsatz biometrischer Identifikationsmerkmale oder die automatische Löschung veralteter Daten. Kontinuierliche Schulungen und klare Verantwortlichkeiten tragen wesentlich dazu bei, dass Sicherheitsmaßnahmen langfristig greifen und nicht nur formal erfüllt, sondern tatsächlich gelebt werden.

Cyberhygiene ist daher nicht nur ein technisches Thema, sondern ein umfassendes Organisationsprinzip, das sowohl die technische Infrastruktur als auch das menschliche Verhalten berücksichtigt. Sie bildet die Grundlage für vertrauenswürdige digitale Prozesse, schützt Unternehmenswerte, fördert die Resilienz gegenüber Cyberangriffen und stärkt letztlich das Vertrauen in die digitale Transformation.

1.2 Cybersecurity und Künstliche Intelligenz

In der digitalen Welt besteht seit vielen Jahren ein grundlegendes Ungleichgewicht: Organisationen, Unternehmen und staatliche Einrichtungen müssen große und vielfältige Bereiche ihrer IT schützen, die aus komplexen Systemen, sensiblen Daten und zahlreichen Schnittstellen bestehen.

Angreifer:innen müssen dagegen lediglich einen einzigen Fehler in diesen Schutzvorkehrungen finden, eine kleine Sicherheitslücke oder eine unachtsame Handlung, um Schaden anzurichten. Diese strukturelle Asymmetrie prägt die Realität der Cybersicherheit seit ihren Anfängen und erklärt, warum Verteidigung im digitalen Raum stets anspruchsvoller und aufwendiger ist als der Angriff.

Künstliche Intelligenz hat lange Zeit als wichtige Unterstützung gedient, um diese Benachteiligung auszugleichen. Sie half dabei, große Mengen an Daten zu analysieren, verdächtige Muster frühzeitig zu erkennen und Routinearbeiten zu automatisieren, die für menschliche Teams schwer zu bewältigen wären. Dadurch konnten Sicherheitsabteilungen schneller reagieren, besser priorisieren und insgesamt effektiver arbeiten.

Doch die rasante Weiterentwicklung besonders leistungsstarker KI verändert dieses Gleichgewicht. Immer deutlicher zeichnet sich ab, dass Angreifer:innen von diesen neuen Möglichkeiten in einem überproportionalen Ausmaß profitieren könnten. Diese Entwicklung birgt enorme sicherheitspolitische, wirtschaftliche und gesellschaftliche Herausforderungen.

Ein zentrales Problem stellen die stark gestiegenen Kosten dar, die moderne KI-Systeme verursachen. Sie benötigen spezialisierte Hardware, große Datenmengen und erhebliche Rechenkapazitäten. Für Verteidiger:innen bedeutet dies, dass der flächendeckende Einsatz solcher KI entlang der gesamten digitalen Infrastruktur oft finanziell kaum zu bewältigen ist. Sie müssten überall gleichzeitig auf dem neuesten Stand sein, um jede potenzielle Angriffsfläche zu schützen.

Angreifer:innen hingegen können sich die teuerste und leistungsfähigste KI gezielt für einzelne Angriffe zunutze machen. Diese Ressourcenasymmetrie könnte dazu führen, dass die Verteidigung zunehmend unter Druck gerät, während Angreifer:innen ihre Mittel effizienter einsetzen.

Hinzu kommt ein zweiter Trend von großer Tragweite. KI kann in absehbarer Zeit in der Lage sein, die vollständige Angriffskette („Kill Chain“) selbstständig zu durchlaufen. Das bedeutet, dass ein solches automatisiertes Angriffssystem in der Lage wäre, ein Ziel auszuspähen, Schwachstellen zu identifizieren, geeignete Angriffsmethoden auszuwählen und in Systeme einzudringen, Daten zu stehlen oder Schäden anzurichten – ohne dass ein Mensch eingreifen müsste. Diese Automatisierung würde Angriffe nicht nur schneller, sondern auch skalierbarer machen. Sie könnten in Sekundenbruchteilen beginnen und abgeschlossen sein, weit bevor Menschen überhaupt eine Chance hätten zu reagieren. In geopolitisch angespannten Situationen könnten solche automatisierten Cyberoperationen sogar zu unkontrollierten Eskalationsdynamiken beitragen.

Ein drittes Risiko ergibt sich aus der nach wie vor bestehenden Unzuverlässigkeit von KI-Systemen, die zwar beeindruckende Leistungen erbringen aber auch große Fehler machen, Situationen falsch interpretieren oder unvorhersehbare Entscheidungen treffen.

In der Verteidigung können solche Fehlreaktionen gravierende Folgen haben, etwa wenn ein System falschen Alarm auslöst, kritische Abläufe unterbricht oder legitime Aktivitäten fälschlich blockiert. Angreifer:innen sind hier im Vorteil, da sie weniger Wert auf Stabilität legen müssen. Ein fehlerhafter Angriff ist für sie kein gravierendes Problem, solange die Wahrscheinlichkeit eines erfolgreichen Angriffs steigt.

Diese technologischen Herausforderungen entfalten sich vor dem Hintergrund einer veränderten politischen und gesellschaftlichen Landschaft. Staaten und Institutionen müssen darüber entscheiden, wie weit sie KI in sicherheitsrelevanten Bereichen nutzen und wie sie gleichzeitig sicherstellen, dass menschliche Expertise nicht verloren geht.

Es stellt sich auch die Frage, wie Verantwortlichkeiten geregelt werden, wenn Entscheidungen von KI-Systemen getroffen werden, die weitreichende Folgen haben können. Parallel dazu findet weltweit ein intensiver Wettbewerb um die technologische Vorherrschaft statt. Staaten und Unternehmen investieren enorme Summen in die Entwicklung leistungsfähiger KI, die nicht nur wirtschaftliche Vorteile verspricht, sondern auch als strategische Ressource betrachtet wird.

In dieser Situation ist es entscheidend zu verstehen, dass der Einfluss von KI auf Angreifer:innen und Verteidiger:innen nicht grundsätzlich festgelegt ist. Die Balance ist veränderbar.

Für nicht-technische Entscheidungsträger bedeutet dies vor allem: Die Frage der Cybersicherheit ist längst nicht mehr nur eine technische Aufgabe. Sie ist zu einem politischen, wirtschaftlichen und gesellschaftlichen Kernthema geworden. Künstliche Intelligenz kann enorme Vorteile bieten, aber ihre Risiken müssen sorgfältig gesteuert werden.

In dieser praktischen Leitlinie wird dargestellt, welche KI-basierten Funktionalitäten und Systeme für die Mitglieder der Fachgruppe Werbung und Marktkommunikation besonders relevant sein können, um ihre Cybersicherheit nachhaltig zu verbessern.

2 Bedrohungslage

Die Cybersicherheitslage ist weltweit weiterhin äußerst angespannt. Wesentliche Treiber dafür sind Konflikte wie der Krieg Russlands gegen die Ukraine, der auch seinen Niederschlag im Cyberspace findet.

Gleichzeitig sorgt die fortschreitende Digitalisierung in nahezu allen Branchen dafür, dass neue Schwachstellen entstehen und bestehende Angriffsflächen größer werden.

2.1 Sicherheitslage in Österreich

Im „Cybercrimereport 2024“ hielt das österreichische Innenministerium fest, dass die Anzahl der angezeigten Cybercrime-Delikte im Jahresvergleich etwas zurückgegangen ist, diese sich allerdings weiterhin auf einem hohen Niveau befindet.

Internetkriminalität	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2015	10.010	4.157	41,5 %
Jahr 2016	13.103	5.072	38,7 %
Jahr 2017	16.804	6.470	38,5 %
Jahr 2018	19.627	7.332	37,4 %
Jahr 2019	28.434	10.187	35,8 %
Jahr 2020	35.915	12.012	33,4 %
Jahr 2021	46.179	17.020	36,9 %
Jahr 2022	60.195	20.378	33,9 %
Jahr 2023	65.864	20.818	31,6 %
Jahr 2024	62.328	19.785	31,7 %
Veränderung zum Vorjahr	-5,4 %	-5,0 %	0,1 %-Punkte

Tabelle: 10-Jahresvergleich Internet-Kriminalität in Österreich (2015-2024)[1]

Der Anteil der Computerkriminalität an der Gesamtkriminalität geht in Richtung 25 Prozent, während die Aufklärungsquote signifikant, nämlich fast 20 Prozent) geringer ist. Nicht einmal jeder dritte Fall von Computerkriminalität wird aufgeklärt.

[1]BMI (Österreich): Cybercrimereport 2024, S. 6

Gesamtkriminalität	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2015	517.869	227.854	44,0 %
Jahr 2016	537. 792	246.854	45,9 %
Jahr 2017	510.536	255.581	50,1 %
Jahr 2018	472.981	248.110	52,5 %
Jahr 2019	488.912	256.851	52,5 %
Jahr 2020	433.811	235.331	54,2 %
Jahr 2021	410.957	227.184	55,3 %
Jahr 2022	488.949	255.176	52,2 %
Jahr 2023	528.010	276.043	52,3 %
Jahr 2024	534.193	282.833	52,9 %
Veränderung	1,2%	2,5%	0,7%-Punkte

Tabelle: Entwicklung der Gesamtkriminalität in Österreich (2015-2024)[2]

2.2 Sicherheitslage in Deutschland

Bei der Vorstellung des Lageberichts zur IT-Sicherheit in Deutschland für das Jahr 2025 betonten die Präsidentin des Bundesamts für Sicherheit und der deutsche Innenminister wichtige Fortschritte bei der Bekämpfung der Cyberkriminalität sowie eine wachsende Widerstandsfähigkeit der kritischen Infrastrukturen. Dennoch zeigt sich, dass die Gefahrensituation im digitalen Raum in keiner Weise entschärft ist. Die Bedrohungsakteure agieren zunehmend professionell, international vernetzt und technisch hochgerüstet.

Die folgenden Risikofaktoren dominieren das aktuelle Bedrohungsbild:

- Nicht ausreichend geschützte oder fehlerhaft konfigurierte Systeme und Anwendungen ermöglichen es Angreifer:innen, sich unbemerkt Zugang zu Netzwerken zu verschaffen und Daten zu entwenden. Für Werbe- und Kommunikationsunternehmen betrifft dies insbesondere Content-Management-Systeme, Projektplattformen, Online-Kampagnensysteme und externe Dienstleisteranbindungen.

[2]BMI (Österreich): Polizeiliche Kriminalitätsstatistik, S. 13

- Bekannte Sicherheitslücken werden häufig erst verspätet geschlossen. Gleichzeitig steigt die Zahl neuer Schwachstellen rasant an. Zwischen Juli 2024 und Juni 2025 nahm die Zahl der täglich neu entdeckten Sicherheitslücken um 24 Prozent zu. Dies stellt IT-Abteilungen und Dienstleister vor enorme Herausforderungen und erfordert kontinuierliche Aufmerksamkeit und Aktualisierung.[3]

- Der Bericht zeigt zudem eine leichte Entspannung bei finanziell motivierten Cyberangriffen, die um neun Prozent zurückgingen. Dieser Rückgang ist vor allem auf erfolgreiche internationale Ermittlungsoperationen mit deutscher Beteiligung zurückzuführen.

- Dennoch stellen Angriffe mit Ransomware die größte Einzelbedrohung dar. Gerade in der Branche Werbung und Marktkommunikation kann ein Ransomware-Angriff besonders gravierende Folgen haben, da er Produktionsprozesse blockiert, Kundendaten kompromittiert und laufende Kampagnen abrupt zum Stillstand bringen kann.

- Parallel dazu nimmt die Aktivität staatlich gesteuerter Akteure zu. Diese verfolgen langfristige politische oder wirtschaftliche Ziele und orchestrieren hochkomplexe Angriffe, die häufig schwer zu erkennen sind. Während sich diese Angriffe primär gegen Bereiche der kritischen Infrastruktur richten, geraten zunehmend auch Unternehmen ins Visier, die Einfluss auf Meinungsbildung, öffentliche Kommunikation oder Zugang zu sensiblen Kundendaten haben. Damit rücken Agenturen, Medienunternehmen und Kommunikationsdienstleister stärker in den Fokus als bisher.

[3] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2025, S. 3 ff.

2.3 „Crime as a Service“ und Datendiebstahl

In der vernetzten Welt von heute ist der digitale Raum zu einem unverzichtbaren Bestandteil des gesellschaftlichen, wirtschaftlichen und privaten Alltags geworden. Kommunikation, Handel, Verwaltung und kritische Infrastrukturen sind in hohem Maße von digitalen Technologien abhängig.

Diese Entwicklung bringt jedoch nicht nur Effizienzgewinne und neue Möglichkeiten mit sich, sondern eröffnet zugleich weitreichende Missbrauchspotenziale. Die zunehmende digitale Durchdringung aller Lebensbereiche beschränkt sich längst nicht mehr auf legale und legitime Nutzungen, sondern wird in wachsendem Ausmaß auch von Akteuren der schweren und organisierten Kriminalität systematisch ausgenutzt.

Laut der europäischen Polizeibehörde EUROPOL weist jede Form schwerer und organisierter Kriminalität heute eine digitale Komponente auf. Kriminelle Aktivitäten hinterlassen digitale Spuren, nutzen Online-Dienste zur Planung und Koordination oder verlagern ganze Geschäftsmodelle in den virtuellen Raum. Von Cyberbetrug, Identitätsdiebstahl und Ransomware-Angriffen über den illegalen Handel mit Drogen und Waffen bis hin zu Geldwäsche und Terrorismusfinanzierung ist das Internet nicht mehr lediglich eine unterstützende Plattform. Es hat sich vielmehr zur zentralen Infrastruktur entwickelt, auf der kriminelle Wertschöpfungsketten aufbauen und skaliert werden.

Waren in den letzten Jahren Ausfälle von Computersystemen und die damit einhergehende Erpressung der Opfer Delikte, die den betroffenen Firmen und Organisationen schwer zu schaffen machen, so sind das heute vor allem Datendiebstähle.

Europol beschreibt in einem Bericht, die zunehmende Brisanz, die damit einhergeht, wenn Kriminelle Daten kopieren und gleich oder später gegen ihre Opfer ausspielen:[4]

„Daten sind die neue Währung der Macht. Sie werden von kriminellen Akteuren gestohlen, gehandelt und ausgebeutet. Gleichzeitig sind sie ein entscheidendes Instrument für Strafverfolgungsbehörden, um illegale Aktivitäten nachzuverfolgen, Täter zu identifizieren und kriminelle Netzwerke zu zerschlagen. Daten sind zu einem zentralen Handelsgut geworden und werden zunehmend von kriminellen Netzwerken oder hybriden Bedrohungsakteuren gestohlen, gehandelt und missbraucht. (...) Da Daten ein derart begehrtes und wertvolles Gut sind, ist zu erwarten, dass ihr illegaler Handel in Geschäftsmodellen nach dem Prinzip ‘Crime as a Service’ weiter an Bedeutung gewinnt. Der Verkauf gestohlener sensibler Informationen wird auf kriminellen Marktplätzen noch häufiger werden. Ein besonders kritischer Aspekt dieser Bedrohung besteht darin, dass gestohlene Daten nicht immer sofort oder nur einmal genutzt werden. In vielen Fällen werden sie über mehrere Jahre hinweg mehrfach eingesetzt, wobei Opfer wiederholt ins Visier der Täter geraten.“

[4]Europol (2025): The changing DNA of serious and Organized Crime, S. 16

3 Angriffe und Abwehr

Die angespannte Sicherheitslage im Internet hat unmittelbare Auswirkungen auf Unternehmen der Fachgruppe Werbung und Marktkommunikation, die in besonderem Maße von reibungslosen digitalen Prozessen abhängig sind.

Kreative Workflows, die Speicherung von Daten in Clouds, Kundendatenbanken, Marketing, Automatisierung und datengetriebene Analyseplattformen bilden ein komplexes Ökosystem, das bei einem Angriff innerhalb kürzester Zeit empfindlich gestört werden kann.

Vor diesem Hintergrund steht nachstehend eine Übersicht über die wichtigsten und bedrohlichsten Angriffsformen, die für die Fachgruppe Werbung und Marktkommunikation von besonderer Bedeutung sind.

Daneben werden Sicherheits- und Präventionsmaßnahmen beleuchtet bzw. die mögliche Unterstützung durch Werkzeuge aus dem Bereich der Künstlichen Intelligenz (KI).

3.1 Phishing-E-Mails und Social Engineering

Die E-Mail-Inbox stellt nach wie vor die größte Schwachstelle in der Abwehr von Cyberangriffen dar, die mittels Phishing-E-Mails oder Social-Engineering-Tricks begonnen werden.

Angriffe erfolgen häufig über gezielt konstruierte, scheinbar seriöse Angebote, vermeintlich echte Kundenanfragen oder professionell wirkende Profile angeblicher Influencer. Diese Kontaktaufnahmen sind in der Regel sorgfältig vorbereitet und darauf ausgelegt, Vertrauen aufzubauen und die Aufmerksamkeit der Betroffenen zu binden. Ziel der Vorgehensweisen ist es, Mitarbeitende oder Organisationen zur Preisgabe sensibler Informationen zu verleiten oder technische Zugriffsmöglichkeiten zu schaffen.

Im Fokus stehen dabei insbesondere der unbefugte Zugang zu IT-Systemen, die Kompromittierung von Passwörtern und Zugangsdaten sowie der Diebstahl interner Daten. In vielen Fällen dienen diese Angriffe als Einstiegspunkt für weiterführende kriminelle Aktivitäten, etwa den Diebstahl von Daten, Betrugshandlungen oder die Vorbereitung umfassender Cyberangriffe.

Sicherheitsmaßnahmen gegen solche Angriffe

Gegen solche Angriffe ist eine abgestimmte Kombination aus organisatorischen, technischen und personellen Maßnahmen erforderlich. Entscheidend ist dabei nicht die einzelne Maßnahme, sondern das Zusammenspiel aller Schutzebenen sowie deren regelmäßige Überprüfung und Anpassung an neue Bedrohungslagen. Gerade bei Phishing und Social-Engineering zeigt sich, dass Angreifer:innen gezielt Schwächen an der Schnittstelle zwischen Mensch, Prozess und Technik ausnutzen.
Auf organisatorischer Ebene sind klare und verbindliche Prozesse von zentraler Bedeutung. Externe Anfragen, etwa Angebote, Kooperationsvorschläge oder

Kontaktaufnahmen über soziale Medien, sollten nicht informell oder spontan bearbeitet werden, sondern einem definierten Prüf- und Freigabeprozess unterliegen.

Zuständigkeiten müssen eindeutig festgelegt sein, ebenso Eskalationswege für ungewöhnliche, zeitkritische oder emotional formulierte Anfragen. Ergänzend dazu sind klare Richtlinien für den Umgang mit Passwörtern, Zugangsdaten und sensiblen Informationen notwendig, um Unsicherheiten im Arbeitsalltag zu vermeiden und einheitliches Handeln sicherzustellen.

Eine tragende Rolle spielt die Sensibilisierung und kontinuierliche Schulung der Mitarbeiter:innen. Sie sind eine der wichtigsten Verteidigungslinien gegen Phishing und Social-Engineering, da viele Angriffe bewusst auf menschliche Aufmerksamkeit und Vertrauen abzielen. Regelmäßige Awareness-Maßnahmen helfen dabei, typische Betrugsmuster wie gefälschte E-Mails, manipulierte Nachrichten oder Fake-Influencer-Profile frühzeitig zu erkennen. Besonders wirksam sind praxisnahe Beispiele und kurze, wiederkehrende Auffrischungen, die das Thema präsent halten und die Aufmerksamkeit im Arbeitsalltag erhöhen, ohne den operativen Betrieb zu belasten.

Ergänzend dazu sind technische Schutzmaßnahmen unverzichtbar. Der konsequente Einsatz von Mehrfaktorauthentifizierung für E-Mail-Konten, Cloud-Dienste und interne Systeme reduziert das Risiko erheblich, dass kompromittierte Zugangsdaten zu einem erfolgreichen Angriff führen. Moderne E-Mail-Sicherheitslösungen und Spamfilter analysieren eingehende Nachrichten automatisiert und erkennen verdächtige Inhalte, Absender oder Links. Ebenso wichtig ist die Erkennung ungewöhnlicher Anmeldeversuche und verdächtigen Nutzerverhaltens. Zugriffsrechte sollten nach dem Prinzip der minimalen Rechtevergabe gestaltet und regelmäßig überprüft werden, um den möglichen Schaden bei einem Sicherheitsvorfall zu begrenzen.

Ein weiterer wichtiger Präventionsfaktor ist die konsequente Verifikation externer Kontakte. Neue Geschäftspartner, Influencer-Accounts oder Dienstleister sollten vor einer Zusammenarbeit überprüft werden, etwa durch Gegenprüfungen über offizielle Websites, bekannte Kontaktinformationen oder etablierte Kommunikationskanäle. Links, Dateianhänge und Login-Prompts sollten immer kritisch hinterfragt und niemals unreflektiert geöffnet werden, insbesondere wenn sie mit Zeitdruck oder ungewöhnlichen Aufforderungen verbunden sind.

Abgerundet wird die Prävention durch kontinuierliches Monitoring und vorbereitete Reaktionsprozesse. Die laufende Überwachung von Systemen und Nutzeraktivitäten ermöglicht es, verdächtige Vorgänge frühzeitig zu erkennen. Ebenso wichtig sind klar definierte Notfallpläne für den Fall eines Sicherheitsvorfalls. Sie stellen sicher, dass Zugänge rasch gesperrt, Schäden begrenzt und weitere Angriffe verhindert werden können, ohne wertvolle Zeit zu verlieren.

Unterstützung durch KI-Werkzeuge

Gerade in diesem Bereich gibt es viele elektronische Helferlein, die das Leben deutlich erleichtern.

Zuallererst seien Tools wie Mimecast angeführt, die eine KI-gestützte Echtzeit-Erkennung von Phishing-E-Mails mit Threat Intelligence anbieten.[5] Auch die Software „Microsoft Defender“ nutzt KI-Technologien zur Erkennung bösartiger URLs oder Anhänge in E-Mails.

KI-Plattformen für Social-Engineering-Prävention analysieren die Kommunikation, Profile und digitale Verhaltensdaten, um Identitätsfälschungen, Deepfakes oder manipulative Inhalte aufzudecken. Dazu zählt etwa „Doppel Vision“ – eine KI-Plattform, die vor Identitätsfälschungen und Social-Engineering schützt, indem sie die Angreifer-Infrastruktur erkennt und stört.[6]

Mit Hilfe von KI-Frameworks kann man die generelle Sicherheit verbessern, indem Musterabweichungen und unerwartete Aktivitäten sofort erkannt werden. Verhaltensanalytische Tools (z. B. Lepide Detect)[7] bauen normative Profile auf und erkennen ungewöhnliches Verhalten, das auf Social-Engineering oder Seitwärtsbewegungen im Netzwerk basiert („Lateral Movement“).

KI-unterstützte Threat-Detection-Systeme nutzen Techniken der natürlichen Sprachverarbeitung (NLP), um verdächtige Kommunikation frühzeitig zu identifizieren, noch bevor technische Schäden entstehen oder Konten kompromittiert werden. Sie ergänzen klassische Sicherheitsmechanismen um eine inhaltliche Bewertung und adressieren damit genau jene Angriffsmethoden, die zunehmend auf Glaubwürdigkeit und Überzeugungskraft setzen.

Österreichische Anbieter

Im Umfeld digitaler Identitäten und Vertrauensinfrastrukturen ist A-Trust[8] als österreichischer Vertrauensdiensteanbieter relevant. A-Trust bietet qualifizierte elektronische Signaturen, Identitätslösungen und Authentifizierungsdienste. Diese Technologien sind kein Phishing-Filter im engeren Sinn, reduzieren jedoch das Risiko von Social-Engineering erheblich, indem sensible Aktionen an starke Identitätsnachweise gekoppelt werden. In Kombination mit KI-basierter Risikoanalyse entsteht hier ein wirksamer Schutz gegen Identitätsmissbrauch.

3.2 Datendiebstahl, Verschlüsselung und Erpressung

Ransomware-Angriffe stellen für Agenturen und Unternehmen der Fachgruppe Werbung und Marktkommunikation eine der gravierendsten Cyberbedrohungen dar. Ziele solcher Angriffe sind insbesondere zentrale Serverstrukturen,

[5] vgl. Mimecast: Produkt „Advanced E-Mail Security” <https://www.mimecast.com/de/products/email-security/>

[6] vgl. Doppel-Vision von Doppel Inc. <https://www.doppel.com/platform>

[7] vgl. Lepide Detect <https://www.lepide.com/lepide-detect/>

[8] vgl. A-Trust <https://a-trust.at/>

Kreativdatenbanken, Asset-Libraries sowie sensible Kundendaten. Gerade Agenturen mit einem hohen Aufkommen an Dateien, Bild- und Videomaterial sind in besonderem Maße gefährdet, da diese Daten den Kern der operativen Wertschöpfung bilden.

Kommt es zu einer Verschlüsselung dieser Systeme durch Angreifer:innen, sind laufende Kampagnen, Produktionsprozesse und Kundenprojekte oft schlagartig blockiert. Neben unmittelbaren Betriebsunterbrechungen drohen erhebliche wirtschaftliche Schäden, der Reputationsverlust gegenüber Auftraggeber:innen sowie rechtliche Konsequenzen, etwa im Zusammenhang mit Fragen des Datenschutzes und sonstiger vertraglichen Verpflichtungen. Hinzu kommt, dass Angreifer:innen zunehmend mit der Veröffentlichung oder dem Weiterverkauf gestohlener Kreativ- und Kundendaten drohen, um den Erpressungsdruck weiter zu erhöhen.

Für Agenturen ist daher ein strukturierter und professioneller Umgang mit der Gefahr von Ransomware unerlässlich. Dazu zählen unter anderem eine konsequente Absicherung von Server- und Backup-Infrastrukturen, klar geregelte Zugriffs- und Berechtigungskonzepte, regelmäßige Datensicherungen sowie die Sensibilisierung der Mitarbeiter:innen für typische Angriffsszenarien. Nur durch eine Kombination aus technischen, organisatorischen und personellen Maßnahmen lässt sich das Risiko wirksam reduzieren und die digitale Handlungsfähigkeit auch im Krisenfall aufrechterhalten.

Sicherheitsmaßnahmen gegen solche Angriffe

Es empfiehlt sich ein mehrstufiges Sicherheitskonzept, das technische, organisatorische und personelle Maßnahmen systematisch kombiniert:

Technische Schutzmaßnahmen

Das Zugriffs- und Identitätsmanagement sollte durch den Einsatz von Mehrfaktor-Authentifizierung für Server, Cloud-Dienste, Kreativplattformen und E-Mail-Konten bzw. die Vergabe strikter Rollen und Rechte nach dem Prinzip der minimal notwendigen Berechtigungen gestaltet werden. Es bedeutet, dass Benutzer:innen, Systeme, Anwendungen und Prozesse ausschließlich jene Zugriffsrechte erhalten, die sie für ihre konkrete Aufgabe unbedingt benötigen, und nicht mehr.

Eine regelmäßige Überprüfung und die Bereinigung von Benutzerkonten müssen stattfinden, weiters die laufende Datensicherung, um die Wiederherstellbarkeit aller produktionsrelevanten Daten inklusive Kreativdatenbanken und Asset-Libraries sicherzustellen.

Durch die Trennung von Backup- und Produktivsystemen sowie die Nutzung von Offlinebackups bzw. unveränderlichen Backups hat man immer eine Version, die man benutzen kann, auch wenn Angreifer:innen ins System gelangt sind. Diese Backups sollten keine Verbindung nach außen haben und physisch vollständig von anderen Netzwerken und Zugriffsmöglichkeiten getrennt sein. Regelmäßige Tests der funktionierenden Datenwiederherstellung, um die Funktionsfähigkeit im Ernstfall sicherzustellen, sind unerlässlich.

Die konsequente Systemhärtung und ein professionelles Patch-Management bilden eine zentrale Grundlage moderner IT-Sicherheit. Die laufende Aktualisierung von

Servern, Betriebssystemen, Kreativsoftware und eingesetzten Plug-ins ist dabei von entscheidender Bedeutung. Sicherheitsupdates, Hotfixes und außerplanmäßige „Out of Band"-Updates müssen zeitnah eingespielt werden, da bekannte Schwachstellen oft innerhalb kürzester Zeit aktiv ausgenutzt werden.

In der Praxis kommen dafür unter anderem Patch-Management-Lösungen wie BigFix[9] vom Hersteller HCL zum Einsatz. Parallel dazu ist die gezielte Abschaltung nicht benötigter Dienste, Anwendungen und technischer Schnittstellen erforderlich, um die Angriffsfläche von Systemen systematisch zu reduzieren.

Auf allen Arbeitsplätzen sollte eine professionelle Endpoint-Schutzlösung implementiert sein, die neben klassischem Virenschutz auch verhaltensbasierte Erkennung, Schutz vor Ransomware und der Ausnützung von Sicherheitslücken (Exploits) bietet. Typische Herstellerlösungen in diesem Bereich sind etwa Microsoft Defender for Endpoint[10]. Derartige Systeme ermöglichen eine zentrale Verwaltung und eine schnelle Reaktion auf sicherheitsrelevante Vorfälle auf Endgeräten.

Auf Ebene von Netzwerk und Infrastruktur ist eine klare Segmentierung des Netzwerks essenziell, um im Fall eines Sicherheitsvorfalls die Ausbreitung von Schadsoftware zu begrenzen und besonders schützenswerte Systeme zu isolieren. Technisch wird dies häufig durch moderne Firewall- und Netzwerkarchitekturen umgesetzt, etwa mit Lösungen von Fortinet, Palo Alto Networks, Cisco oder Sophos. Ergänzend dazu kommen spezialisierte E-Mail-Sicherheitslösungen zum Einsatz, um Phishing-Angriffe, betrügerische Nachrichten und Schadanhänge frühzeitig zu erkennen und abzuwehren. Beispiele hierfür sind Mimecast, Microsoft Defender for Office 365 oder Hornetsecurity.

[9]vgl. die Endpunktmanagement-Software Bigfix von HCL <https://www.hcl-software.com/de/products/bigfix>

[10]vgl. Microsoft Defender for Endpoint < https://www.microsoft.com/de-de/security/business/endpoint-security/microsoft-defender-endpoint>

Abgerundet wird dieses Sicherheitskonzept durch die kontinuierliche Überwachung verdächtiger Aktivitäten mittels zentraler Logging- und Monitoring-Systeme. Plattformen wie „Splunk SIEM“[11] (Security Information and Event Management) sammeln und korrelieren sicherheitsrelevante Ereignisse aus unterschiedlichen Systemen. Dadurch können Angriffe frühzeitig erkannt, analysiert und gezielt Gegenmaßnahmen eingeleitet werden, bevor größerer Schaden entsteht.

Die Rolle der verschlüsselten Speicherung

An dieser Stelle ist besonders hervorzuheben, wie wichtig die konsequente Verschlüsselung sensibler, personenbezogener oder vertraulicher Daten für die digitale Sicherheit von Agenturen, Studios und Kommunikationsdienstleistern ist. Gerade in der Werbe- und Medienbranche werden regelmäßig vertrauliche Informationen verarbeitet, etwa Kundendaten, Kampagnenunterlagen, kreative Entwürfe oder Vertragsdokumente. Eine wirksame Verschlüsselung stellt sicher, dass diese Inhalte auch dann geschützt bleiben, wenn es Angreifer:innen gelingt, in IT-Systeme einzudringen oder Daten von Speichermedien zu kopieren. Ohne entsprechende Schutzmaßnahmen können abgeflossene Dateien unmittelbar ausgewertet, weiterverkauft oder für Erpressungsversuche genutzt werden. Durch Verschlüsselung wird dieses Risiko deutlich reduziert, da die Daten ohne das zugehörige Passwort oder den entsprechenden Schlüssel nicht lesbar sind und damit ihren unmittelbaren Nutzen für Angreifer:innen verlieren.

In der praktischen Umsetzung wird häufig übersehen, dass viele der im Arbeitsalltag eingesetzten Programme bereits integrierte und kostenfreie Verschlüsselungsfunktionen bereitstellen. Anwendungen wie Adobe Acrobat (Pro) oder Microsoft Office ermöglichen es, Dokumente direkt mit Passwort und Verschlüsselung abzusichern, ohne dass zusätzliche Lizenzkosten oder spezielles technisches Know-how erforderlich sind. Auch größere Datenmengen können einfach geschützt werden, indem ganze Ordnerstrukturen als verschlüsselte und passwortgeschützte ZIP-Archive nach dem AES-256 Industriestandard (z. B. mit Hilfe von 7-Zip) gespeichert oder weitergegeben werden.

Besonders relevant ist dieser Schutz bei der Zusammenarbeit mit externen Dienstleister:innen, Freelancer:innen und Kund:innen sowie beim Austausch sensibler Unterlagen über E-Mail oder Cloud-Plattformen. Verschlüsselung schafft hier eine zusätzliche Sicherheitsebene und sorgt dafür, dass selbst bei Fehlkonfigurationen, versehentlichen Freigaben oder kompromittierten Benutzerkonten kein unmittelbarer Zugriff auf vertrauliche Inhalte möglich ist. Sie trägt damit wesentlich dazu bei, das Risiko von Datenmissbrauch, Reputationsschäden und rechtlichen Konsequenzen zu reduzieren und den verantwortungsvollen Umgang mit Informationen im Arbeitsalltag zu unterstützen.

[11] vgl. Splunk SIEM:
< https://www.splunk.com/de_de/blog/learn/siem-security-information-event-management.html>

Organisatorische Maßnahmen und Notfallpläne

Die organisatorische Abwehr von Ransomware-Angriffen beginnt mit klar definierten Zuständigkeiten und Verantwortlichkeiten innerhalb der Organisation. Es muss eindeutig festgelegt sein, wer für IT, Sicherheit, Informationssicherheit und die Koordination bei Cybervorfällen verantwortlich ist. Für den Ernstfall sollten sowohl interne als auch externe Ansprechpersonen benannt sein, etwa IT-Dienstleister:innen, Incident-Response-Spezialist:innen oder rechtliche Berater:innen. Diese Klarheit verhindert Verzögerungen und Unsicherheiten in einer Krisensituation, in der schnelle und koordinierte Entscheidungen entscheidend sind.

Ein zentrales Element ist ein strukturierter Cybersecurity-Notfallplan, der konkrete Abläufe bei einem Ransomware-Angriff beschreibt. Dieser Plan sollte regeln, wie technische, organisatorische und kommunikative Maßnahmen ineinandergreifen, welche Systeme priorisiert behandelt werden und wie Eskalationsstufen aussehen. Ebenso wichtig ist die Festlegung klarer Kommunikationswege gegenüber Kundinnen und Kund:innen, Geschäftspartner:innen und gegebenenfalls der Öffentlichkeit. Transparente und abgestimmte Kommunikation trägt wesentlich dazu bei, Reputationsschäden zu begrenzen und Vertrauen zu erhalten. Parallel dazu muss die Organisation auf rechtliche und datenschutzrechtliche Meldepflichten vorbereitet sein, insbesondere im Hinblick auf die DSGVO und branchenspezifische Vorgaben.

Da Ransomware-Angriffe häufig über externe Schnittstellen erfolgen, spielt das Management von Lieferketten und Dienstleistern eine zentrale Rolle. Externe IT-Dienstleister, Cloud-Anbieter oder Kreativplattformen sollten verbindlichen Sicherheitsanforderungen unterliegen, die vertraglich festgelegt und regelmäßig überprüft werden. Dazu gehören auch die konsequente Kontrolle und Aktualisierung von Zugriffsrechten externer Partner:innen, um unnötige oder veraltete Zugänge zu vermeiden.
Der menschliche Faktor bleibt einer der häufigsten Auslöser erfolgreicher Angriffe und muss daher organisatorisch adressiert werden.

Eine kontinuierliche Sensibilisierung der Mitarbeitenden ist unerlässlich. Regelmäßige Schulungen zu den Themen Phishing-E-Mails, Social-Engineering und dem sicheren Umgang mit Daten stärken das Risikobewusstsein im Arbeitsalltag. Ergänzend dazu sollten klare Regeln für den Umgang mit externen Speichermedien sowie mit mobilen Endgeräten definiert und kommuniziert werden.

Auch die Arbeitsorganisation selbst trägt wesentlich zur Prävention bei. Die konsequente Trennung von privaten und beruflichen Geräten sowie Konten reduziert das Risiko, dass Schadsoftware aus dem privaten Umfeld in Unternehmenssysteme eingeschleppt wird. Für Remotezugriffe und Homeoffice sind klare Richtlinien erforderlich, die Sicherheitsanforderungen, Zugriffsrechte und technische Mindeststandards verbindlich regeln. Auf diese Weise wird sichergestellt, dass flexible Arbeitsmodelle nicht zu zusätzlichen Einfallstoren für Ransomware werden.

Unterstützung durch KI-Werkzeuge

Künstliche Intelligenz kann eine wichtige Hilfe zum Schutz vor Ransomware Angriffen und der unbefugten Verschlüsselung von Daten spielen.

Im Bereich des Schutzes von Arbeitsplätzen und Servern kommen sogenannte Endpoint-Detection- und Response-Lösungen zum Einsatz. Tools wie CrowdStrike Falcon[12] nutzen maschinelles Lernen, um verdächtige Prozesse, ungewöhnliche Dateiaktivitäten und typische Verschlüsselungsmuster frühzeitig zu erkennen. Falcon ist eine cloudnative Cybersicherheitsplattform für Endpunktschutz, die mit einem KI-gestützten Sensor Bedrohungen in Echtzeit erkennt und abwehrt, indem sie Endpunkte, Identitäten und Cloud-Workloads absichert. Diese Systeme können automatisch eingreifen, betroffene Geräte isolieren und Ransomware stoppen, bevor ganze Projektverzeichnisse oder Asset-Libraries verschlüsselt werden. Gerade für Agenturen mit vielen Kreativarbeitsplätzen ist dieser Schutz besonders relevant.

Ein zweites zentrales Einsatzfeld ist die E-Mail-Sicherheit, da Ransomware-Angriffe häufig mit Phishing-Nachrichten beginnen. KI-gestützte Lösungen wie Mimecast oder Microsoft Defender for Office 365 analysieren das Absenderverhalten, Inhalte und Kommunikationsmuster deutlich tiefer als klassische Spamfilter. Sie erkennen manipulierte Anhänge, gefälschte Login-Seiten und SocialEngineering-Versuche und blockieren diese, bevor sie Mitarbeitende erreichen.

Auch im Bereich der Netzwerküberwachung und Angriffserkennung spielen KI-Werkzeuge eine wichtige Rolle. Lösungen wie Darktrace[13] lernen das normale Verhalten eines Netzwerks und identifizieren Abweichungen in Echtzeit. Dazu zählen etwa ungewöhnliche Datenbewegungen, unerwartete Zugriffe auf Server oder automatisierte Prozesse, die auf eine beginnende Verschlüsselung hindeuten. Solche Systeme sind besonders hilfreich, um Angriffe zu erkennen, die sich bereits innerhalb der Infrastruktur ausbreiten.

Für den Schutz von Cloud-Diensten, Kollaborationstools und Identitäten kommen KI-gestützte Sicherheitsfunktionen von Plattformanbietern zum Einsatz. Ein Beispiel ist Microsoft Entra ID Protection[14]. Diese Lösung erkennt auffällige Anmeldeversuche, kompromittierte Konten und riskante Konfigurationen und unterstützt Unternehmen dabei, unbefugte Zugriffe frühzeitig zu unterbinden.

Ergänzend dazu gibt es KI-basierte Tools im Bereich des „Security Information and Event Management“ sowie der automatisierten Reaktion auf Vorfälle. Plattformen wie Splunk sammeln sicherheitsrelevante Ereignisse aus unterschiedlichen Systemen, bewerten diese mithilfe von KI und priorisieren echte Bedrohungen. Für

[12]vgl. Falcon vom Hersteller Crowdstrike:
https://www.crowdstrike.com/de-de/platform/

[13]vgl. Darktrace – beispielsweise für E-Mail-Sicherheit:
<https://www.darktrace.com/de/products/email>

[14]vgl. Microsoft Entra ID Protection unterstützt Organisationen dabei, identitätsbasierte Risiken zu erkennen, zu untersuchen und zu beseitigen.
<https://learn.microsoft.com/de-de/entra/id-protection/overview-identity-protection>

Agenturleitungen entsteht dadurch mehr Transparenz über die eigene Sicherheitslage, ohne sich in technischen Details zu verlieren.

Nicht zuletzt gewinnen auch Awareness und Trainingslösungen an Bedeutung. Anbieter wie KnowBe4[15] nutzen KI, um realistische Phishing-Simulationen durchzuführen und Schulungsinhalte gezielt an das Risikoprofil der Mitarbeitenden anzupassen. Damit wird der menschliche Faktor systematisch in das Sicherheitskonzept eingebunden.

Tools aus Österreich

Eine wirksame Abwehr von Ransomware-Angriffen erfordert heute eine ganzheitliche Sicherheitsarchitektur, die technologische Leistungsfähigkeit mit lokaler operativer Kompetenz verbindet. In der Praxis hat sich eine Kombination aus mehreren ineinandergreifenden Maßnahmen als besonders effektiv erwiesen.

Grundlage bildet der Einsatz einer internationalen KI-gestützten Endpoint-Detection-and-Response--Plattform (EDR), die in der Lage ist, auch unbekannte Angriffsvarianten anhand von Verhaltensmustern frühzeitig zu erkennen und automatisiert zu unterbinden. Solche Plattformen ermöglichen eine kontinuierliche Überwachung aller Endpunkte und bieten insbesondere bei schnell eskalierenden Ransomware-Angriffen einen entscheidenden Zeitvorteil.

Ergänzend dazu ist der Betrieb dieser Sicherheitslösungen durch im Land tätige Anbieter von großer Bedeutung. Lokale Betreiber bringen nicht nur ein tiefes Verständnis für regulatorische Anforderungen und branchenspezifische Risiken mit, sondern stellen auch eine schnelle Reaktionsfähigkeit im Ernstfall sicher.

Für die Umsetzung einer integrierten Sicherheitsarchitektur empfiehlt sich die Zusammenarbeit mit einem erfahrenen Systemintegrator und Managed-Security-Anbieter wie dem Cancom-Konzern[16], der über umfassende Erfahrungen in der Integration internationaler KI-gestützter Sicherheitsplattformen verfügt, kombiniert mit lokalem Betrieb, Managed-Detection und Response sowie kontinuierlichem Threat-Hunting. Durch die Bündelung von Technologie, Betrieb und Beratung aus einer Hand kann dieses deutsch-österreichische Unternehmen die Widerstandsfähigkeit gegenüber Ransomware-Angriffen nachhaltig stärken und gleichzeitig den organisatorischen Aufwand reduzieren.

3.3 Missbrauch von Werbe- und Social-Media-Konten

Die unbefugte Übernahme von Werbekonten auf Plattformen wie Meta, Google Ads oder TikTok stellt für Unternehmen der Werbung und Marktkommunikation ein erhebliches wirtschaftliches und reputationsbezogenes Risiko dar. Beim sogenannten „Account Hijacking“ verschaffen sich Angreifer:innen Zugriff auf zentrale Werbe- und

[15] vgl. Knowbe4 – Security Awareness Trainings <https://www.knowbe4.com/>

[16] vgl. Cancom Active Cyber Defence Center < https://www.cancom.at/it-security/cyber-defense-center>

Kampagnenkonten und nutzen diese für eigene Zwecke und das häufig, ohne dass die betroffenen Agenturen oder Auftraggeber:innen dies zunächst bemerken.

Die Folgen solcher Vorfälle sind vielschichtig. Neben dem unmittelbaren finanziellen Schaden durch missbräuchlich eingesetzte Werbebudgets können unautorisierte Kampagneninhalte auftauchen, die nicht den vereinbarten Kommunikationszielen entsprechen oder gegen rechtliche und ethische Standards verstoßen. Dies kann zu erheblichen Imageverlusten für Kund:innen führen und zugleich das Vertrauensverhältnis zwischen Agentur und Auftraggeber:in nachhaltig beeinträchtigen. In besonders sensiblen Fällen drohen darüber hinaus Sperren der betroffenen Werbekonten durch die Plattformbetreiber, was laufende Kampagnen verzögert oder vollständig zum Erliegen bringen kann.

Für Agenturen ist diese Form des Cyberrisikos besonders kritisch, da Werbekonten häufig mit hohen Budgets, mehreren Nutzerzugängen und engen zeitlichen Abläufen verbunden sind. Kompromittierte Zugangsdaten, unzureichend abgesicherte Benutzerrechte oder Phishing-Angriffe auf Mitarbeitende zählen zu den häufigsten Ursachen solcher Übernahmen. Umso wichtiger ist ein professioneller und präventiver Umgang mit der Absicherung von Werbeplattformen und zugehörigen Konten.

Social-Media-Konten

Die Manipulation bereits veröffentlichter Social-Media-Posts stellt ein erhebliches Risiko für die Glaubwürdigkeit von Marken und Auftraggeber:innen dar. Angreifer:innen verändern Texte, Bilder oder Verlinkungen bestehender Beiträge oder ersetzen diese vollständig durch fremde Inhalte. Da solche Änderungen oft unbemerkt erfolgen und zeitlich verzögert entdeckt werden, können manipulierte Posts über Stunden oder Tage hinweg falsche Botschaften, betrügerische Links oder politisch extreme Inhalte verbreiten. Für Agenturen bedeutet dies nicht nur einen unmittelbaren Reputationsschaden, sondern auch den Verlust der redaktionellen Hoheit über die Markenkommunikation ihrer Kund:innen.

Ein weiteres kritisches Szenario stellen unautorisierte Live-Streams dar. Über kompromittierte Konten können Angreifer:innen Live-Übertragungen starten, ohne dass Agenturen oder Unternehmen dies unmittelbar kontrollieren oder stoppen können. Solche Streams werden häufig genutzt, um irreführende Inhalte, Scam-Angebote oder rufschädigende Aussagen zu verbreiten.

Besonders problematisch ist dabei die hohe Reichweite von Liveformaten sowie deren algorithmische Bevorzugung auf vielen Plattformen. Selbst kurze Sequenzen können nachhaltig negative Auswirkungen auf das Markenimage haben und lassen sich im Nachhinein kaum vollständig aus dem digitalen Raum entfernen.

Die Weitergabe privater Nachrichten an Dritte betrifft einen besonders heiklen Bereich der Marktkommunikation. In Direktnachrichten befinden sich oft vertrauliche Informationen wie Kampagnenabsprachen, Preisdetails, Vertragsanbahnungen oder personenbezogene Daten. Bei einer Kompromittierung können diese Inhalte gezielt weitergeleitet, veröffentlicht oder zur Erpressung genutzt werden. Darüber hinaus besteht die Gefahr, dass private Nachrichten manipuliert oder aus dem Kontext gerissen werden, um Kund:innen, Influencer:innen oder Geschäftspartner:innen gegeneinander auszuspielen. Gemeinsam ist diesen Bedrohungen, dass sie nicht nur technische Sicherheitslücken ausnutzen, sondern gezielt auf Vertrauen, Öffentlichkeit und Geschwindigkeit abzielen. Gerade im Bereich Werbung und Marktkommunikation, wo Inhalte oft in Echtzeit entstehen und verbreitet werden, wirken sich solche Vorfälle besonders schnell und intensiv aus. Sie unterstreichen die Notwendigkeit klarer Zugriffsregelungen, kontinuierlicher Überwachung von Accounts sowie definierter Notfallprozesse für den Fall einer Kontenübernahme.

Ein strukturierter Schutz vor „Account Hijacking“ umfasst daher nicht nur technische Sicherheitsmaßnahmen, sondern auch klare organisatorische Regeln und ein hohes Maß an Sensibilisierung. Der Schutz von Werbe- und Social-Media-Konten ist damit ein wesentlicher Bestandteil verantwortungsvoller Agenturarbeit und professioneller Marktkommunikation. Er dient nicht nur der Absicherung von Budgets und Kampagnen, sondern auch dem nachhaltigen Schutz von Marken, Reputation und Kundenbeziehungen.

Sicherheitsmaßnahmen gegen solche Angriffe

Eine zentrale Präventionsmaßnahme stellt die konsequente Absicherung aller Werbekonten durch starke Authentifizierungsmechanismen dar. Die verpflichtende Nutzung von Mehrfaktor-Authentifizierung für alle Nutzerkonten reduziert das Risiko erheblich, dass gestohlene oder „abgephishte“ Zugangsdaten missbraucht werden können. Gerade bei Konten mit hohen Budgets oder administrativen Rechten sollte der Zugriff zusätzlich auf vertrauenswürdige Geräte und definierte Nutzerkreise beschränkt werden. Ebenso wichtig ist eine regelmäßige Überprüfung der hinterlegten E-Mail- Adressen und Wiederherstellungsoptionen, da diese häufig als Einfallstor für Kontoübernahmen dienen.

Darüber hinaus spielt ein strukturiertes Berechtigungsmanagement eine entscheidende Rolle. Agenturen sollten sicherstellen, dass Mitarbeitende und externe Partner:innen nur jene Zugriffsrechte erhalten, die sie für ihre aktuelle Aufgabe benötigen. Administratorrechte sollten restriktiv vergeben und zeitlich begrenzt sein. Ehemalige Mitarbeiter:innen sowie nicht mehr benötigte Agentur- oder Kundenkonten müssen konsequent und zeitnah entfernt werden, um unkontrollierte Zugänge zu vermeiden.

Einen weiteren wichtigen Präventionsfaktor stellt die Absicherung der internen Arbeitsumgebung dar. Da viele Kontoübernahmen ihren Ursprung in Phishing-Angriffen haben, ist der Schutz von E-Mail-Konten und Endgeräten unmittelbar mit

dem Schutz von Werbeplattformen verknüpft. Professionelle E-Mail-Sicherheitslösungen, aktuelle Endgerätesicherheit und regelmäßige Systemaktualisierungen tragen dazu bei, Schadsoftware und betrügerische Nachrichten frühzeitig zu blockieren. Ergänzend dazu sollten Login-Benachrichtigungen und sicherheitsrelevante Warnmeldungen der Plattformen aktiv genutzt und nicht ignoriert werden.

Neben technischen Maßnahmen ist die Sensibilisierung der Mitarbeiter:innen von zentraler Bedeutung. Viele Angriffe setzen auf Zeitdruck, angebliche Konto-Warnungen oder fingierte Supportnachrichten. Regelmäßige Schulungen und klare interne Richtlinien helfen dabei, solche Täuschungsversuche zu erkennen und richtig darauf zu reagieren. Mitarbeitende sollten wissen, dass Plattformbetreiber niemals per E-Mail oder Messengerdiensten zur Eingabe von Passwörtern oder Einmalcodes auffordern und dass verdächtige Nachrichten konsequent gemeldet werden müssen.

Organisatorische Maßnahmen

Klare interne Zuständigkeiten für Werbekonten und definierte Abläufe für den Ernstfall erleichtern eine rasche Reaktion. Dazu gehört insbesondere, zu wissen, wie Plattform-Support-Stellen kontaktiert werden können, welche Schritte bei einer vermuteten Kontoübernahme sofort zu setzen sind und wie Kund:innen transparent informiert werden können. Eine dokumentierte Vorgehensweise reduziert Unsicherheit und Zeitverluste in einer akuten Krisensituation.

Wer sich bei verschiedenen Diensten mit einem einzigen Google-, Apple- oder Facebook-Konto anmeldet, macht sich stark abhängig. Wird dieser zentrale Zugang gesperrt oder gehackt, können im schlimmsten Fall entweder mehrere Konten gleichzeitig verloren gehen oder von Kriminellen gekapert werden. Daher sollten je nach Plattform unterschiedliche Logins verwendet werden.

Unterstützung durch KI-Werkzeuge

Zur Absicherung von Werbekonten, Kreativsystemen und digitalen Zugängen kommen in der Praxis verschiedene Kategorien von KI-gestützten Sicherheitslösungen zum Einsatz. Zum Schutz von Arbeitsplätzen und Servern werden unter anderem Endpoint-Schutzlösungen wie CrowdStrike Falcon genutzt. Diese erkennen verdächtige Prozesse, automatisierte Verschlüsselungsversuche und ungewöhnliche Aktivitäten auf Endgeräten und können Angriffe frühzeitig stoppen.

Im Bereich der E-Mail-Sicherheit kommen KI-basierte Lösungen wie Mimecast, Barracuda oder Microsoft Defender zum Einsatz. Sie analysieren Inhalte, Absenderverhalten und Kommunikationsmuster und blockieren Phishing-Nachrichten, die häufig der Ausgangspunkt für Kontoübernahmen sind.
Zur Absicherung von Benutzerkonten und Identitäten werden KI-gestützte Identitätsschutzfunktionen genutzt, etwa Microsoft Entra ID Protection oder vergleichbare Cloud-Sicherheitsdienste. Diese erkennen auffällige Anmeldeversuche, ungewöhnliche Zugriffe oder kompromittierte Konten und können zusätzliche Sicherheitsmaßnahmen auslösen.

Für die Erkennung von Angriffen innerhalb der IT-Infrastruktur werden KI-basierte Netzwerküberwachungslösungen wie Darktrace eingesetzt. Sie identifizieren

Abweichungen vom normalen Netzwerkverhalten und ermöglichen ein frühzeitiges Eingreifen.

Ergänzend dazu sorgen zentrale SIEM-Analyseplattformen wie Splunk für einen gesamthaften Überblick über sicherheitsrelevante Ereignisse. Sie bündeln Informationen aus verschiedenen Systemen und priorisieren relevante Vorfälle mithilfe von KI.

Zur Stärkung des menschlichen Faktors werden KI-gestützte Awareness-Lösungen wie KnowBe4 eingesetzt, die realistische Phishing-Simulationen durchführen und Schulungsmaßnahmen gezielt anpassen.

Anbieter aus Österreich

Ein wichtiger österreichisch-deutscher Anbieter ist die Firma Cancom mit ihrem Security-Operation-Center (SOC) im Bereich IT-Monitoring, Automatisierung und Incident-Erkennung.

Dieser Anbieter setzt KI-gestützte Analysewerkzeuge ein, um ungewöhnliche Prozessketten, verdächtige Speicherzugriffe oder atypische Systemlast zu erkennen. Gerade bei Ransomware ist Geschwindigkeit entscheidend, da die frühe Erkennung von Angriffen entscheidend zur Eindämmung des möglichen Schadens von Cyberangriffen beiträgt.

3.4 Angriffe über die „Lieferkette“

Die Unternehmen der Fachgruppe Werbung und Marktkommunikation haben erhebliche Sicherheitsrisiken durch ihre Abhängigkeiten von externen Partner:innen, die teilweise tief in operative, kreative und technische Prozesse eingebunden sind.

Agenturen und Auftraggeber:innen arbeiten heute in komplexen Ökosystemen aus Freelancer:innen, spezialisierten Softwarelösungen, Hosting- und Cloud-Providern sowie Produktionspartnern für Video, Audio und Content. Jede zusätzliche Schnittstelle erhöht dabei die Angriffsfläche und erschwert die vollständige Kontrolle über sicherheitsrelevante Abläufe.

Ein großes Risiko liegt in der Auslagerung von Zugriffen und Verantwortlichkeiten. Externe Partner:innen benötigen häufig Zugänge zu Social-Media-Konten, Werbeplattformen, Content-Management-Systemen, Analyse-Tools oder internen Ablagestrukturen. Diese Zugriffe werden in der Praxis oft pragmatisch vergeben, ohne klare zeitliche Begrenzung, ohne abgestufte Rollenmodelle und ohne regelmäßige Überprüfung. Sobald ein externer Account kompromittiert wird, sei es durch Phishing, Schadsoftware oder unsichere Endgeräte, kann dies unmittelbare Auswirkungen auf die Kommunikationskanäle von betroffenen Kund:innen haben.

Besonders anspruchsvoll ist die Situation bei Freelancer:innen, die projektbezogen eingebunden sind und meist mit eigener Infrastruktur arbeiten. Unterschiedliche Sicherheitsstandards, private Geräte, wechselnde Netzwerke und parallele Tätigkeiten für mehrere Auftraggeber:innen erhöhen das Risiko, dass Sicherheitsvorfälle nicht sofort erkannt werden. Das gilt auch für den Datenaustausch mit diesen über unsichere Wechselmedien wie USB-Sticks oder externe Speichermedien. Für Agenturen entsteht dadurch ein blinder Fleck, da sich Sicherheitsmaßnahmen nur eingeschränkt auf externe Arbeitsumgebungen ausdehnen lassen.

Auch der zunehmende Einsatz externer Softwaretools für Social-Media-Management, Kampagnensteuerung, Analyse oder Automatisierung bringt neue Abhängigkeiten mit sich. Diese Tools greifen häufig über Schnittstellen direkt auf Social-Media-Konten und Werbebudgets zu. Sicherheitslücken beim Anbieter, fehlerhafte Updates oder kompromittierte API-Schlüssel können dazu führen, dass Angreifer:innen gleichzeitig auf zahlreiche Accounts zugreifen. In solchen Fällen sind nicht nur einzelne Unternehmen betroffen, sondern ganze Kundensegmente oder Branchen.

Hinzu kommen Risiken im Bereich Hosting, Cloud-Services und technischer Infrastruktur. Websites, Kampagnenplattformen oder Asset Libraries werden oft von externen Providern betrieben. Kommt es dort zu Sicherheitsproblemen, können Inhalte manipuliert, Schadcodes eingebunden oder Weiterleitungen auf betrügerische Seiten gesetzt werden. Über Social-Media-Kanäle verbreiten sich solche Manipulationen besonders schnell und können das Vertrauen in eine Marke nachhaltig untergraben.

Auch Produktionspartner wie Videoproduktionsfirmen, Postproduktion oder Grafikstudios sind sicherheitsrelevant, da sie Zugriff auf unveröffentlichte Kampagnen, Rohmaterial und sensible Abstimmungen erhalten. Der Austausch großer

Datenmengen über Cloud-Speicher, File-Transfer-Dienste oder mobile Datenträger erfolgt häufig unter Zeitdruck und ohne durchgängige Sicherheitsrichtlinien. Dadurch steigt das Risiko eines Datenabflusses, vorzeitiger Veröffentlichungen oder der gezielten Manipulation von Inhalten.

Insgesamt zeigt sich, dass Schwachstellen bei externen Partner:innen weniger auf einzelne technische Fehler zurückzuführen sind, sondern auf strukturelle Herausforderungen in der Zusammenarbeit. Fehlende einheitliche Sicherheitsanforderungen, unklare Zuständigkeiten und mangelnde Transparenz über Zugriffsrechte machen es Angreifer:innen leichter, die schwächste Stelle in der Kette auszunutzen.

Für die Fachgruppe Werbung und Marktkommunikation bedeutet dies, dass Cybersicherheit nicht isoliert betrachtet werden darf, sondern als integraler Bestandteil des gesamten Partner- und Lieferantennetzwerks verstanden werden muss.

Sicherheitsmaßnahmen gegen solche Angriffe

Ein zentraler Ansatzpunkt ist ein strukturiertes und diszipliniertes Zugriffsmanagement. Externe Partner:innen sollten ausschließlich jene Zugriffsrechte erhalten, die sie für ihre konkrete Aufgabe benötigen. Administrative Vollzugriffe sind auf ein Minimum zu beschränken. Zugänge müssen zeitlich begrenzt und projektbezogen vergeben und nach Abschluss der Zusammenarbeit konsequent entzogen werden. Regelmäßige Überprüfungen bestehender Berechtigungen helfen, veraltete oder vergessene Zugänge zu identifizieren.

Ein weiterer wesentlicher Präventionsfaktor ist die konsequente Absicherung von Konten durch Mehrfaktor-Authentifizierung. Social-Media-Konten, Werbeplattformen, Cloud-Dienste und Management-Tools sollten ausschließlich mit zusätzlicher Authentifizierung betrieben werden. Dadurch wird das Risiko deutlich reduziert, dass kompromittierte Passwörter allein zu einer Kontoübernahme führen.

Ergänzend dazu ist eine saubere Trennung von persönlichen und geschäftlichen Zugängen wichtig. Externe Partner:innen sollten nach Möglichkeit nicht mit privaten Accounts arbeiten, sondern mit eindeutig zuordenbaren, geschäftlichen Benutzerkonten. So bleibt nachvollziehbar, wer wann auf welche Systeme zugegriffen hat und verdächtige Aktivitäten können schneller erkannt werden.

Im Umgang mit externen Softwaretools und Plattformen empfiehlt sich eine bewusste Auswahl und regelmäßige Neubewertung. Tools sollten nur jene Berechtigungen erhalten, die zwingend erforderlich sind. Nicht mehr genutzte Integrationen sind aktiv zu entfernen. Zusätzlich ist es sinnvoll, sich über Sicherheitskonzepte, Zertifizierungen und Update-Prozesse der Anbieter zu informieren, um Abhängigkeiten besser einschätzen zu können.

Ein weiterer Präventionsbaustein ist die Sensibilisierung und klare Kommunikation von Sicherheitsanforderungen. Externe Partner:innen sollten vor Projektstart über grundlegende Sicherheitsregeln informiert werden, etwa zur Nutzung sicherer Endgeräte, zum Umgang mit Zugangsdaten oder zur Erkennung von Phishing-

Versuchen. Klare Erwartungen reduzieren Fehlverhalten, das oft nicht aus böser Absicht, sondern aus Unwissen entsteht.

Auch vertragliche Regelungen spielen eine wichtige Rolle. Sicherheitsanforderungen, Vertraulichkeitspflichten, Meldewege bei Sicherheitsvorfällen sowie Verantwortlichkeiten sollten explizit festgehalten – und überprüft! – werden. Dies schafft nicht nur rechtliche Klarheit, sondern erhöht auch das Bewusstsein für die Bedeutung von Cybersicherheit auf allen Seiten.

Schließlich ist die Vorbereitung auf den Ernstfall Teil wirksamer Prävention. Definierte Notfallprozesse für kompromittierte Konten, klare Zuständigkeiten und schnelle Kommunikationswege ermöglichen es, im Fall eines Vorfalls rasch zu reagieren und Schäden zu begrenzen. Gerade in der Marktkommunikation, wo Zeit und öffentliche Wahrnehmung eine große Rolle spielen, ist Reaktionsfähigkeit ein entscheidender Schutzfaktor.

Unterstützung durch KI-Werkzeuge

Moderne Tools können mit KI-Unterstützung einen wirksamen Beitrag leisten, um Risiken durch externe Partner:innen frühzeitig zu erkennen und Sicherheitsvorfälle rund um Social-Media-Konten, Kampagnenplattformen und sensible Inhalte zu verhindern. Sie wirken dabei vor allem unterstützend, indem sie Auffälligkeiten automatisiert analysieren, menschliche Fehler reduzieren und Reaktionszeiten verkürzen.

Ein wichtiger Einsatzbereich ist die Überwachung von Kontozugriffen und Identitäten. KI-basierte Sicherheitslösungen können kontinuierlich Login-Verhaltensmuster wie Uhrzeiten, Standorte, genutzte Geräte oder Arbeitsabläufe analysieren. Weichen diese Muster deutlich vom Normalverhalten ab, etwa durch einen Login aus einem ungewöhnlichen Land oder durch automatisierte Aktionen, wird ein Alarm ausgelöst oder der Zugriff blockiert. Solche Funktionen bietet beispielsweise die Software Microsoft Defender for Identity[17]. Diese Software überwacht kontinuierlich Identitäten in lokalen und hybriden IT-Umgebungen und erkennt automatisch verdächtige Aktivitäten. Auf dieser Basis kann gezielt reagiert werden, etwa durch automatisierte Maßnahmen bei kompromittierten Identitäten, wie das Sperren von Konten, das Erzwingen von Passwortänderungen oder das Einschränken von Zugriffsrechten. Dadurch lassen sich Schäden wirksam begrenzen und die Sicherheit von sensiblen Daten und Systemen nachhaltig stärken.

Im Bereich der Phishing- und Social-Engineering-Abwehr spielen KI-Tools ebenfalls eine wichtige Rolle. Externe Partner:innen sind häufig Ziel gefälschter E-Mails oder Nachrichten, die auf den Diebstahl von Zugangsdaten abzielen. KI-gestützte E-Mail-Sicherheitslösungen wie Mimecast oder Microsoft Defender analysieren Sprache, Absenderverhalten und Kontext und erkennen auch neue, bisher unbekannte Angriffsmuster und können verdächtige Nachrichten automatisch isolieren oder kennzeichnen.

[17] vgl. Microsoft Defender for Identity <https://learn.microsoft.com/de-de/defender-for-identity/what-is>

Zur Absicherung von Social-Media-Konten und veröffentlichten Inhalten können KI-Funktionen in professionellen Managementplattformen zum Einsatz kommen. Diese überwachen laufend Profiländerungen, Post-Bearbeitungen, unautorisierte Veröffentlichungen oder Live-Streams. Auffällige Aktivitäten werden sofort gemeldet, sodass Agenturen rasch reagieren können. Entsprechende Funktionen finden sich etwa bei Brandwatch einer führenden Social-Media-Monitoring- und Consumer-Intelligence-Plattform, die dabei hilft, Online-Daten aus sozialen Medien, Blogs, Foren und Nachrichten zu sammeln und zu analysieren, um Einblicke in die Zielgruppe, Trends und Markenwahrnehmung zu gewinnen, sowie Social-Media-Aktivitäten zu verwalten und Krisen frühzeitig zu erkennen.[18]

Ein weiterer relevanter Bereich ist die Analyse von Berechtigungen externer Softwaretools. Viele Social-Media- und Kampagnen-Tools greifen über Schnittstellen direkt auf Konten und Werbebudgets zu. KI-gestützte Cloud-Security und SaaS-Monitoring-Lösungen erkennen überprivilegierte Zugriffe, veraltete Integrationen oder riskante Konfigurationen. Beispiele hierfür sind Microsoft Defender, oder Palo Alto Prisma SaaS, die Transparenz über angebundene Tools und deren Rechte schaffen.

Beim Austausch sensibler Inhalte mit Videoproduktionsfirmen, Grafikstudios oder Hosting-Partnern unterstützen KI-basierte Data-Loss-Prevention (DLP)-Lösungen. Diese erkennen automatisch, wenn vertrauliche Informationen wie Kundendaten, interne Abstimmungen oder unveröffentlichte Kampagnen unkontrolliert weitergegeben werden. Lösungen wie Symantec DLP[19] helfen dabei, einen Datenabfluss frühzeitig zu verhindern oder zumindest sichtbar zu machen.

[18] vgl. Brandwatch <https://www.brandwatch.com>

[19] vgl. Symantec DLP von Broadcom <https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention>

Österreichische Anbieter

Für die Reputations-, Medien- und Stimmungsanalyse gibt es ebenfalls starke österreichische Anbieter. Observer Brand Intelligence mit Sitz in Innsbruck ist international etabliert und bietet KI-gestützte Medienbeobachtung, Social-Media-Monitoring und Reputationsanalyse.

Die Plattform wird häufig von Kommunikationsabteilungen, Agenturen und Konzernen genutzt, um ungewöhnliche Ausschläge, Shitstorms oder missbräuchliche Kommunikation frühzeitig zu erkennen.

Ein weiterer interessanter Anbieter ist Talkwalker. Die Firma wurde ursprünglich in Österreich gegründet und ist seither nach Luxemburg übersiedelt. Sie nutzt KI-Funktionen für Social-Listening, Image-Erkennung und Trendanalyse und ist besonders relevant zur Früherkennung von Reputationsrisiken, etwa nach einer Kontoübernahme oder bei manipulierten Kampagnen.

3.5 Angriffe gegen Software-Schwachstellen

Wenn Anbieter:innen oder Angreifer:innen gezielt nach Softwareschwachstellen suchen, konzentrieren sie sich häufig auf Datenbanksysteme, die über Webinterfaces erreichbar sind. Solche Schnittstellen bilden das Rückgrat vieler moderner Anwendungen, etwa für Kundenportale, Kampagnenplattformen, Content-Management-Systeme oder Analyse-Tools. Über diese Interfaces werden Daten abgefragt, gespeichert oder verändert und genau hier setzen viele Angriffe an.

Ein klassisches Angriffsszenario besteht darin, manipulierte Datenbankabfragen, sogenannte „SQL-Abfragen“, einzuschleusen mit dem Ziel, die vorgesehenen Sicherheitsmechanismen zu umgehen und einen unerlaubten Zugriff auf Daten zu erlangen. Gelingt dies, können Angreifer:innen sensible Informationen auslesen, bestehende Datensätze verändern oder sogar komplette Datenbanken löschen. Besonders kritisch ist dies, wenn es sich um Kundeninformationen, Zugangsdaten, Kampagnendaten oder interne Steuerungsinformationen handelt. Solche Angriffe sind technisch oft unscheinbar, ihre Auswirkungen jedoch gravierend, da sie im Hintergrund stattfinden und lange unentdeckt bleiben können.

Mit dem Einsatz von KI-Agenten hat diese Form von Angriffen eine neue Dimension erreicht. Während klassische Angriffe meist manuell vorbereitet und schrittweise durchgeführt wurden, sind KI-gestützte Systeme in der Lage, Angriffe automatisiert, skalierbar und adaptiv umzusetzen. Agenten können Webinterfaces kontinuierlich analysieren, unterschiedliche Eingabevarianten testen und in kürzester Zeit tausende potenzielle Angriffspfade ausprobieren. Dabei lernen sie aus jeder Reaktion des Systems und passen ihre Abfragen dynamisch an, um Sicherheitsfilter gezielt zu umgehen.

Besonders problematisch ist, dass solche KI-Agenten nicht nur bekannte Schwachstellen ausnutzen, sondern auch unbekannte oder falsch konfigurierte Systeme identifizieren können. Sie erkennen Muster in Fehlermeldungen, Antwortzeiten oder Systemreaktionen und leiten daraus Rückschlüsse auf die zugrunde liegende Datenbankstruktur und Sicherheitsarchitektur ab. Dadurch steigt die Erfolgswahrscheinlichkeit solcher Angriffe erheblich – und das selbst bei Systemen, die als grundsätzlich gut abgesichert gelten.

Für Organisationen der Fachgruppe Werbung und Marktkommunikation bedeutet diese Entwicklung ein deutlich erhöhtes Risiko. Viele der eingesetzten Tools und Plattformen basieren auf webbasierten Datenbankanwendungen, die oft von externen Anbietern betrieben oder gemeinsam mit Partner:innen genutzt werden. Eine erfolgreiche Kompromittierung kann nicht nur zum Verlust sensibler Daten führen, sondern auch zur Manipulation von Inhalten, Kampagnen oder Auswertungen und damit zu unmittelbaren wirtschaftlichen und Reputationsschäden.

Sicherheitsmaßnahmen gegen solche Angriffe

Angriffe, die mit KI-Unterstützung betrieben werden, können die klassische Logik von punktuellen Sicherheitsüberprüfungen zunehmend unterlaufen. Die Geschwindigkeit, Lernfähigkeit und Automatisierung dieser Systeme erfordert einen grundlegenden Perspektivwechsel in der Sicherheitsstrategie. Der Schutz von Webinterfaces und angebundenen Datenbanksystemen wird damit zu einer zentralen Herausforderung moderner Cybersicherheit, insbesondere in datengetriebenen und kommunikations-intensiven Branchen.

Ein zentraler Präventionsfaktor ist die sichere Entwicklung und Konfiguration von Anwendungen. Webinterfaces müssen so gestaltet sein, dass Benutzereingaben grundsätzlich nicht direkt in Datenbankabfragen übernommen werden. Der Einsatz vorbereiteter Abfragen und moderner Frameworks reduziert die Angriffsfläche erheblich. Ebenso wichtig ist eine restriktive Rechtevergabe auf Datenbankebene, sodass selbst bei einer erfolgreichen Manipulation nur begrenzte Datenbereiche betroffen wären.

Ergänzend dazu spielt die Absicherung der Schnittstellen eine wesentliche Rolle. Web-Application-Firewalls können verdächtige Abfragen erkennen und blockieren, bevor sie die Anwendung erreichen. Moderne Systeme nutzen dabei Verhaltensanalysen und maschinelles Lernen, um auch neuartige Angriffsmuster zu identifizieren, die von klassischen Signaturen nicht erfasst werden. Gerade bei KI-Agenten, die tausende Varianten testen, sind solche Schutzmechanismen besonders wichtig und wirksam.

Ein weiterer wichtiger Präventionsbaustein ist die kontinuierliche Überwachung des Systemverhaltens. KI-gestützte Monitoringsysteme analysieren Zugriffsfrequenzen, Antwortzeiten und Fehlermeldungen in Echtzeit. Ungewöhnliche Muster, etwa eine hohe Anzahl leicht variierter Abfragen oder systematisches Ausloten von Fehlermeldungen, können frühzeitig erkannt und automatisch eingeschränkt werden. So lässt sich verhindern, dass Angreifer:innen über längere Zeit unbemerkt Informationen sammeln.

Auch die „Härtung“ der Infrastruktur ist entscheidend. Dazu gehören regelmäßige Updates von Datenbanksystemen, Webservern und Frameworks sowie das rasche Schließen bekannter Schwachstellen. Viele erfolgreiche Angriffe nutzen nicht neue, sondern bereits bekannte Sicherheitslücken, die aus Zeit- oder Ressourcenmangel offengeblieben sind. Automatisierte Prozesse für das Patch- und Schwachstellenmanagement helfen, dieses Risiko deutlich zu reduzieren.

Nicht zu unterschätzen ist die Bedeutung der Segmentierung von Systemen und Daten. Kritische Datenbanken sollten nicht direkt aus dem Internet erreichbar sein, sondern über zusätzliche Sicherheitsstufen geschützt werden. Eine klare Trennung von Entwicklungs-, Test- und Produktionssystemen verhindert zudem, dass Schwachstellen aus weniger geschützten Umgebungen in den produktiven Betrieb durchschlagen.

Schließlich ist auch die organisatorische Prävention ein wesentlicher Faktor. Klare Zuständigkeiten, dokumentierte Sicherheitsanforderungen an externe Softwareanbieter und regelmäßige Sicherheitsüberprüfungen erhöhen die Resilienz

deutlich. Gerade bei cloudbasierten Tools und Plattformen sollte vorab geklärt werden, wie diese mit Schwachstellen umgehen, wie schnell sie reagieren und welche Schutzmechanismen implementiert sind.

Unterstützung durch KI-Werkzeuge

Zur Prävention von KI-gestützten Angriffen auf Webinterfaces und angebundene Datenbanksysteme kommen heute zunehmend KI-basierte Sicherheitslösungen zum Einsatz, die Angriffe nicht nur blockieren, sondern ihr Verhalten analysieren, einordnen und frühzeitig erkennbar machen. Diese Tools sind besonders relevant, weil moderne Angriffe automatisiert, adaptiv und in hoher Geschwindigkeit ablaufen und damit klassische regelbasierte Schutzmechanismen oft überfordern.

Eine zentrale Rolle spielen KI-gestützte Web-Application-Firewalls. Sie überwachen den gesamten Datenverkehr zwischen Nutzern und Webanwendungen und analysieren eingehende Abfragen in Echtzeit. Mithilfe von Verhaltensanalysen erkennen sie auch stark variierte oder neuartige SQL-Injection-Versuche, wie sie von KI-Agenten automatisiert erzeugt werden. Lösungen wie Cloudflare WAF[20] nutzen maschinelles Lernen, um zwischen legitimen Zugriffen und gezielten Manipulationsversuchen zu unterscheiden und Angriffe bereits vor Erreichen der Anwendung zu blockieren.

Ergänzend dazu kommen KI-basierte Systeme zur Anomalie und Angriffserkennung zum Einsatz. Diese Tools lernen das normale Verhalten von Webanwendungen, APIs und Datenbanken und erkennen Abweichungen, etwa ungewöhnlich hohe Abfragefrequenzen, systematisches Ausloten von Fehlermeldungen oder automatisierte Testläufe unterschiedlicher Query-Varianten. Plattformen wie Darktrace, Vectra AI oder ExtraHop analysieren den laufenden Datenverkehr und machen verdächtige Muster sichtbar, die auf vorbereitende oder laufende Angriffe hindeuten.

Weitere wichtige Bausteine sind das KI-unterstützte Schwachstellen-Scanning und Sicherheitstests. Solche Tools prüfen Webanwendungen und Schnittstellen kontinuierlich auf bekannte und unbekannte Schwachstellen. Durch KI werden Tests dynamisch angepasst und an das konkrete Verhalten der Anwendung angeglichen, wodurch auch komplexe Angriffsszenarien erkannt werden können. Ein mächtiges Tool stellt die cloudbasierte Lösung HCL AppScan[21] dar, mit der Anwendungen, APIs, Container und Infrastruktur gesamthaft und robust getestet werden können.

Zur übergreifenden Auswertung sicherheitsrelevanter Ereignisse werden KI-basierte SIEM-Plattformen eingesetzt. Sie korrelieren Logdaten aus Webservern, Datenbanken, Anwendungen und Sicherheitskomponenten und nutzen KI, um relevante Vorfälle zu priorisieren und Angriffsmuster über mehrere Systeme hinweg zu erkennen. Lösungen wie Splunk Enterprise Security helfen dabei, auch komplexe Angriffsketten frühzeitig zu identifizieren.

[20] vgl. Cloudflare Web Application Firewall (WAF)
<https://www.cloudflare.com/de-de/application-services/products/waf/>

[21] vgl. HCL AppScan:
< https://www.hcl-software.com/de/products/appscan >

Für Organisationen im Bereich Marktkommunikation sind insbesondere jene KI-Werkzeuge relevant, die Webanwendungen, Plattformen und Schnittstellen schützen, da ein Großteil der eingesetzten Systeme webbasiert ist und sensible Daten verarbeitet. KI unterstützt hier vor allem die Früherkennung automatisierter, lernfähiger Angriffsmuster, die mit herkömmlichen Methoden nur schwer zu erfassen sind. Entscheidend bleibt jedoch, dass diese Technologien in klare Sicherheitsprozesse eingebettet sind und nicht als isolierte Einzellösungen verstanden werden.

Anbieter aus Österreich

Dynatrace mit Sitz in Linz setzt künstliche Intelligenz und maschinelles Lernen ein, um Anwendungen, Webservices, APIs und Datenbankzugriffe in Echtzeit zu analysieren und zu überwachen. Die Plattform erfasst dabei kontinuierlich eine Vielzahl technischer und funktionaler Parameter und baut auf dieser Basis ein detailliertes Modell des normalen System- und Nutzerverhaltens auf. Dieses Verständnis des Regelbetriebs ermöglicht es, selbst geringfügige Abweichungen frühzeitig zu identifizieren und sichtbar zu machen.

Besonderes Augenmerk liegt auf der Analyse von Webinterfaces und Schnittstellen, da diese in modernen digitalen Geschäftsmodellen häufig die wichtigste Angriffsfläche darstellen. Dynatrace erkennt unter anderem ungewöhnliche Abfragefrequenzen, fehlerhafte oder manipulierte Requests, auffällige Zugriffsmuster sowie atypische Antwortzeiten oder Rückgabewerte von Anwendungen und Datenbanken. Solche Anomalien können auf automatisierte Angriffe, missbräuchliche Nutzung von Schnittstellen oder gezielte Versuche hinweisen, Schwachstellen in datenbankbasierten Systemen auszunutzen.

Auch wenn Dynatrace nicht primär als klassisches IT-Sicherheitsprodukt positioniert ist, trägt die kontinuierliche Verhaltensanalyse wesentlich zur Früherkennung sicherheitsrelevanter Vorfälle bei. Angriffe können so bereits in einem sehr frühen Stadium erkannt werden, noch bevor es zu Datenabflüssen, Systemausfällen oder spürbaren Beeinträchtigungen für Kund:innen kommt. Durch die enge Verzahnung von Performance-Monitoring, Datenanalyse und KI-gestützter Anomalie-Erkennung unterstützt Dynatrace Organisationen dabei, technische Störungen und potenzielle Sicherheitsvorfälle ganzheitlich zu betrachten. Dies erleichtert nicht nur die rasche Ursachenanalyse, sondern ermöglicht auch ein koordiniertes Vorgehen zwischen IT-Betrieb, Softwareentwicklung und Sicherheitsverantwortlichen. Auf diese Weise leistet die Plattform einen wichtigen Beitrag zur Erhöhung der Resilienz digitaler Anwendungen und zur Reduktion von Risiken im laufenden Betrieb.

4 Sicherheitsmaßnahmen aus der Praxis

Die nachfolgenden Sicherheitstipps wurden für die Praxis der Fachgruppe Werbung und Marktkommunikation entwickelt.

Diese Anregungen sollen dabei helfen, möglichst viele Präventionsmaßnahmen umzusetzen, um Cyberangriffe einzudämmen und ihnen effektiv zu begegnen.

4.1 Für Unternehmen

Tipp 1: Notwendige Analyse der Schatten-IT

Als Schatten-IT in Unternehmen bezeichnet man Programme und Dienste, die von Benutzer:innen verwendet werden, obwohl das Unternehmen diese nicht dafür vorgesehen hat.

Beispielsweise bieten Firmen ihren Mitarbeiter:innen häufig nur geringen Komfort im EDV-Bereich und fast gar keine Möglichkeiten für den Austausch von sensiblen Dokumenten mit eigenen IT-Lösungen, weil ihre wichtigen Systeme schon sehr alt sind und nicht mehr zeitgemäß funktionieren.

Viele User verwenden in solchen Unternehmen deshalb moderne Chat-Clients wie WhatsApp und Signal und schicken einander über diese privat installierten Apps Fotos von Verträgen, Sujets oder wichtigen Dokumenten. Die Fotos haben sie häufig mit privaten Smartphones, die ebenfalls nicht vom Unternehmen zugelassen sind, gemacht. In der Realität entwickelt sich so eine große, nicht vom Unternehmen selbst betriebene Schatten-IT, die für die Benutzer:innen dieser Organisation fast genauso wichtig ist wie die zertifizierten und zugelassenen Systeme des Arbeitgebers.

Es ist deshalb hoch an der Zeit, neben der dokumentierten IT- und IT-Security-Architektur auch die Schatten-IT zu durchforsten. Hier spielt auch die sogenannte Shadow-Cloud eine besondere Rolle – zum Beispiel die Verwendung von Dropbox und ähnlichen Anbietern für den Dateiaustausch.

Was hier hilft, ist die Entwicklung von zeitgemäßen Angeboten für den Dateiaustausch und die Dateiübertragung an die eigenen Mitarbeitenden. In den meisten Fällen stellt sich nämlich heraus, dass Benutzer:innen gerne auf unternehmenseigene Systeme umsteigen und die Shadow-Cloud verlassen, wenn die bereitgestellten Alternativen die notwendigen Funktionen bieten.

Tipp 2: Auswahl der richtigen Sicherheitsberater

Für Firmen und Organisationen ist es wichtig, wirklich fachkundige Berater:innen im Bereich der Computersicherheit oder zur Aufarbeitung von Cyberangriffen einzusetzen.

Vorsicht vor kleinen Anbietern geboten, die eine Unmenge an verschiedenen Dienstleistungen anbieten, in denen auch Cybersecurity enthalten ist, ohne einen wirklichen Schwerpunkt darzustellen. Das Ziel solcher Unternehmen ist häufig nicht nur die singuläre Beratung in kleinem Rahmen oder die Behebung eines akuten Problems – sondern der Abschluss möglichst umfangreicher Aufträge, um die Einbindung von Subauftragnehmern zu ermöglichen und damit ihre allfällige Inkompetenz im Bereich Computersicherheit zu verbergen.

Daher ist es sehr wichtig, beim Abschluss von Verträgen immer darauf zu bestehen, dass zu jedem Zeitpunkt zumindest ein:e erfahrene:r Mitarbeiter:in des Beratungsunternehmens aus diesem Bereich anwesend und greifbar ist. Dieser sollte auch außerhalb des Beratungsunternehmens – auf Kundenseite – IT- und IT-Security-Erfahrungen gesammelt haben, zum Beispiel als Chief Information Security Officer (CISO), als Netzwerktechniker oder als Forensiker.

Eine weitere Gefahr stellen Unternehmen dar, deren Ziel es hauptsächlich ist, bestimmte Software- oder Hardwareprodukte an den Kunden zu bringen – seien es eigene oder von ihnen vertriebene. Diese Produkte sind zumeist sehr gewinnträchtig und können durch geschickte Maintenance-Verträge auch über lange Zeit Lizenzeinnahmen bringen. Um dieses Ziel zu erreichen, werden in manchen Fällen von derartigen Firmen sehr günstige oder sogar unentgeltliche Beratungen angeboten, die Probleme der Kund:innen aber nicht oder nur schlecht lösen, dafür aber häufig neue herbeireden – und das so lange, bis ein Produkt der Firma angekauft oder gemietet wird.

Auf diese beschriebene Art und Weise sind viele Projekte im Bereich der Computersicherheit gescheitert, da zu wenig Fachwissen und Erfahrung vorhanden waren. Der Bereich Cybersecurity ist besonders anfällig für schlechte Beratung, da es oft keine Möglichkeit gibt, den Erfolg der Berater:innen eindeutig zu messen. Diese können sich nämlich leicht auf unklare, unzugängliche, kriminelle Vorgänge berufen (z. B. Angriffe aus dem Darknet), die nicht vorhersehbar waren. Kund:innen können infolge nicht nachvollziehen, ob neu auftretende Probleme das Resultat mangelhafter Beratung sind oder aufgrund externer Faktoren tatsächlich nicht gelöst oder verhindert werden konnten. Die besten Berater:innen für diesen Themenbereich sind Personen, die bereits operativ im Bereich Cybersecurity tätig waren und auch über Beratungs-Know-how verfügen. Sie können die anstehenden Probleme schneller und mit weit weniger finanziellem Aufwand behandeln, lösen oder zumindest verbessern.

Vorsicht vor Berater:innen, die behördliche Strafverfolgung anbieten

Besonders kritisch muss auch die Rolle von Berater:innen gesehen werden, die versuchen, die Aufgaben von Strafverfolgungsbehörden zu übernehmen oder sich in diese einzumischen. Das ist äußerst fragwürdig und Unternehmen sollten von vornherein Abstand davon nehmen, auch wenn Mitarbeitende von Cybersecurity-Firmen früher für Behörden tätig waren.

Denn auf eigene Faust zu ermitteln, kann schwere und kontraproduktive Entwicklungen nach sich ziehen, die dem Unternehmen noch mehr Schaden zufügen als die Vorfälle, die eigentlich untersucht wurden.

Überdies kann es sein, dass solcherart ermittelte Ergebnisse vor Gericht ein Verwertungsverbot nach sich ziehen. Im Extremfall kann es sogar passieren, dass Organe von Unternehmen, die solche „Beratungsleistungen" in Auftrag gegeben haben, damit Straftaten oder deren Anstiftung begünstigen und daher selbst angeklagt werden.

Behördliche Ermittlungen und Cybersecurity-Beratung müssen voneinander getrennt sein und dürfen nicht vermischt werden!

Leider sind in den letzten Jahren immer wieder Fälle aufgetreten, in denen Mitarbeiter:innen von Cybersecurity-Firmen, die als „Gelegenheitsinformanten" für Behörden tätig waren, oder eine Behördennähe zumindest vorgaben, die Ermittlungen gegen Cyberkriminalität nachhaltig beeinflusst haben.

Medienberichte über derartige Fälle, in denen Informanten oder privatwirtschaftliche Hilfskräfte von Behörden Daten an Cyberkriminelle weitergegeben haben, sollten Anlass genug sein, eine klare Trennung zwischen behördlicher Arbeit und privatwirtschaftlicher Beratung sicherzustellen.[22]

[22]vgl. Laufer, Daniel in: Der Standard: „Staatsschutz-Informant leakte Beweismaterial über Bombendrohungen", am 26. Juni 2025
< https://www.derstandard.at/story/3000000275380/staatsschutz-informant-leakte-beweismaterial-ueber-bombendrohungen>

Tipp 3: Benutzer- und Zugriffsverwaltung / Konfigurationsmanagement

In größeren Organisationen sollte ein Identitäts- und Zugriffsmanagement-System (IAM) eingerichtet werden, das intelligent mit dem Verzeichnis der Benutzer:innen in der Organisation verbunden ist (z. B. über die Schnittstellen LDAP oder Active Directory). Jede Benutzerinteraktion sollte aufgezeichnet werden und für spätere Auswertungen zur Verfügung stehen.

Wenn in der Organisation eine Single-Sign-On-Lösung implementiert ist, die Benutzer:innen rollenspezifisch gleichzeitig an mehrere Systeme anmeldet, sollte unbedingt der Einsatz von Mehr-Faktor-Authentifizierung überlegt werden (z. B. durch Sicherheits-Token oder Smartcards).

Im Zuge der Einrichtung eines solchen Systems ist es auch ratsam, ein Inventar der gesamten Hard- und Software im Unternehmen anzulegen und sicherzustellen, dass diese im Sinne der Benutzer- und Zugriffsverwaltung richtig konfiguriert ist und beispielsweise keine Standard-Passwörter verwendet werden oder bekannte „Hintertüren“ geschlossen wurden.

Tipp 4: Verschlüsselung verwenden

Neue Programme sollten verschlüsselt kommunizieren und Daten speichern können.

Das gilt auch für extern zugekaufte Software (z. B. Instant-Messaging-Dienste), die man maßgeschneidert für viele Unternehmen konfigurieren kann, auch um die Benutzer:innen von den in der Schatten-IT benutzten Services wegzubringen.

Tipp 5: Sichere Software entwickeln und einsetzen

Viele Unternehmen leben mit einem Moloch aus alter, schlecht gewarteter Software. In manchen Fällen sind die Entwickler:innen schon im Ruhestand oder verstorben, die Software wird aber trotzdem nicht ausgetauscht, weil damit verbundene unwägbare Kosten oder mögliche Systemausfälle befürchtet werden. Die Risiken, die man damit eingeht, sind meist viel größer als die Folgen einer kontrollierten Ablöse.

Sollte eine solche stattfinden, müssen aber neben funktionalen Aspekten – wie der leichteren Handhabbarkeit durch Benutzer:innen und der guten Administrierbarkeit neuer Software – unbedingt auch Verbesserungen im Sicherheitsbereich stattfinden.

Eine Bestandsaufnahme und Erneuerung der IT-Architektur ist immer eine große Chance für die Verbesserung der IT-Security-Architektur!

Tipp 6: Netzwerksegmentierung

Netzwerksegmentierung bezeichnet die strukturierte Aufteilung eines IT-Netzwerks in mehrere logisch oder physisch getrennte Teilbereiche, sogenannte Segmente. Ziel ist es, den Datenverkehr zu kontrollieren, Sicherheitsrisiken zu begrenzen und die Ausbreitung von Angriffen zu verhindern.

Im Falle des Eindringens eines Angreifers kann so ein Flächenbrand verhindert werden. Der Kärntner Landeshauptmann Peter Kaiser hat von „digitalen Brandabschnitten“ gesprochen, die nach dem Angriff der Gruppe „BlackCat“ auf die Kärntner Landesregierung im gesamten Netzwerk konsequent implementiert wurden.[23]

Statt eines großen, durchgehend verbundenen Netzwerks werden Systeme nach Funktion, Schutzbedarf oder Nutzung getrennt. So befinden sich etwa Büroarbeitsplätze, Server, Produktionssysteme, Gastnetzwerke oder Cloud-Anbindungen in unterschiedlichen Segmenten, zwischen denen der Datenverkehr gezielt geregelt wird.

Der sicherheitstechnische Kern der Netzwerksegmentierung liegt darin, dass nicht jedes System mit jedem anderen System frei kommunizieren darf. Zugriffe zwischen Segmenten sind nur erlaubt, wenn sie fachlich notwendig sind und werden über Firewalls, Zugriffskontrollen oder Sicherheitsregeln überwacht. Dadurch wird das Prinzip der minimalen Verbindung konsequent umgesetzt.

Wenn ein Arbeitsplatzrechner durch Phishing oder Schadsoftware kompromittiert wird, kann sich die Angreifer:in ohne Segmentierung oft frei im gesamten Netzwerk bewegen. Mit Netzwerksegmentierung bleibt der Angriff zunächst auf ein einzelnes Segment beschränkt. Der Zugriff auf sensible Server, Datenbanken oder Backups ist blockiert oder stark eingeschränkt. So lassen sich Schäden deutlich begrenzen.

Besonders wichtig ist Netzwerksegmentierung als Schutzmaßnahme gegen Ransomware. Moderne Ransomware versucht nach der Erstinfektion weitere Systeme zu erreichen, Administratorrechte zu erlangen und möglichst viele Daten zu verschlüsseln. Durch Segmentierung wird diese seitliche Bewegung erschwert oder unterbunden. Selbst bei einem erfolgreichen Angriff bleibt die Wirkung räumlich begrenzt.

[23] Steinkogler, Stefan in: Kronenzeitung: „Auftrag im Wahlkampf? Kärnten will nach Attacke gegen Hacker vorgehen“, 24.11.2025 <https://www.krone.at/396337>

Tipp 7: Sicherheit in Drahtlosnetzwerken und Überwachungssysteme

Aus Medienberichten ging nach der Verhaftung von angeblichen russischen Agenten in den Niederlanden, die neben der Organisation für das Verbot chemischer Waffen (OPCW) mit einem Wi-Fi-Einbruchswerkzeug aufgefahren waren, hervor, dass drahtlose Netzwerke von Kriminellen als Einfallstore in unsere Systeme genutzt werden.[24]

Wichtig für die Sicherheit im WLAN ist die Verwendung von qualifizierten Passwörtern für Router und Clients und auch die regelmäßige Information, welche Geräte darüber angeschlossen sind. Die von Apple mitgeliefert Routine „Wireless Diagnostics" generiert einen Bericht über das Netzwerk, von dem man umgeben ist. Diesen sollte man aufmerksam analysieren, auf Schwachstellen überprüfen und gegebenenfalls korrigierend eingreifen.

Organisationen sollten analysieren, wie weit ihre drahtlosen Netze reichen, um Hacking-Versuche von Eindringlingen von der Straße oder naheliegenden Gebäuden zu unterbinden. Für hochsichere Unternehmensteile sollte grundsätzlich der aktuelle Verschlüsselungsstandard WPA3 eingesetzt werden, da er ein deutlich höheres Sicherheitsniveau als ältere Versionen bietet. Ist der flächendeckende Einsatz von WPA3 aufgrund älterer Endgeräte noch nicht möglich, sollte zumindest WPA2 mit AES-Verschlüsselung verwendet werden. Veraltete oder unsichere Verfahren wie WPA oder WPA2 mit TKIP sind konsequent zu deaktivieren, da sie keinen ausreichenden Schutz mehr bieten.

Moderne Echtzeit-Sicherheitsüberwachungssysteme

Unternehmen sollten den Einsatz von übergreifenden SIEM-Lösungen[25] überprüfen, die Netzwerke und Systeme rund um die Uhr überwachen und bei Angriffen Alarm schlagen.

Überdies ist der Einsatz spezieller Software zur Entdeckung von Eindringlingen (Intrusion-Detection) und von Datenabflüssen (Data-Leak-Prevention) anzuraten – vor allem in Organisationen, in denen Kriminelle laufend versuchen, über technische Mittel einzudringen oder über Social-Engineering Mitarbeitende dazu anzustiften, ihnen sensible Informationen zu senden.

[24] Deutsche Welle: Niederlande vereiteln Russen-Attacke auf OPCW, 4. Oktober 2018 <https://www.dw.com/de/niederlande-vereiteln-cyber-attacke-russischer-spione-auf-opcw/a-45751523 >

[25] SIEM ist die Abkürzung für „Security Information and Event Management"

Tipp 8: Hardware-Strategie auch für privat genutzte Geräte überprüfen

Unternehmen sollten laufend die von ihnen im Rechenzentrum und von ihren Benutzer:innen verwendete Hardware im Hinblick auf Sicherheitsfragen evaluieren. Manche Organisationen tauschen alte Desktop-Computer und Smartphones nicht aus, sondern stellen den Usern frei, stattdessen eigene Geräte zu verwenden.

Was am Anfang wie eine Einsparung, gepaart mit einem gewissen zusätzlichen Komfort für die Anwender aussieht (sie können ja ihre privaten und beruflichen Programme im gleichen System verwenden), rächt sich im Falle eines Schadsoftwarebefalls, der durch den privaten Nutzungsteil verursacht wird.

Noch viel mehr gilt das für USB-Sticks, bei denen Unternehmen ausschließlich die Nutzung von verschlüsselten, vom Unternehmen ausgegebenen Devices zulassen sollten.

Auch zufällig in Büros am Boden oder sonst wo aufgelesene USB-Sticks sollten nicht in Computer gesteckt, sondern sofort der Sicherheitsabteilung übergeben werden, die sie auswerten kann.

Tipp 9: Schwachstellen prüfen / Cyberhygiene-Checkups

„Ethische Hacker“ oder „White Hats“ überprüfen die Sicherheitsvorkehrungen im Auftrag von Unternehmen oder Organisationen.

Um einen Eindruck von diesen Tests zu bekommen, kann man auch im Internet frei verfügbare Scanner verwenden. Eine Übersicht findet man auf der Website des OWASP (Open Web Application Security Project). Der dort aufgeführte „Zed Attack Proxy“ (ZAP) ist ein unentgeltlicher Scanner, der viele Schwachstellen findet.[26] Ein weiterer sehr einfach verwendbarer Scanner, der aber nicht so tiefe Analysen vornimmt, ist Sucuri, der Webseiten auf Malware checkt.[27]

Mittels Penetrationstests werden Angriffe auf ein Rechnersystem oder eine Website simuliert, um mögliche Schwachstellen, Verwundbarkeiten oder Konfigurationsfehler zu finden. Dabei können Tools zum Einsatz kommen, die denen von Hacker:innen ähneln. Werden solche Tests im Rahmen eines größeren Audits durch externe Spezialist:innen durchgeführt, sollten vorher die für IT-Security-Verantwortlichen informiert werden, da ihre Warnsysteme anschlagen sollten. Vertraut man diesen nicht, empfiehlt es sich, vorab jeden Schritt so zu dokumentieren, dass keine langwierige Diskussion über etwaige Hacking-Versuche entsteht, die dann zumeist weit über die Maßnahme selbst hinausgeht.
Achtung: Werden bei solchen Tests wichtige, geschäftskritische Systeme eines Unternehmens überprüft, muss unbedingt sichergestellt sein, dass Backup- oder Ausfallssicherungsmöglichkeiten bestehen, falls ein solches System durch den

[26] OWASP: Zed Attack Proxy by Checkmarx
<https://www.zaproxy.org>

[27] Sucuri: Free website malware and security checker
<https://sitecheck.sucuri.net>

Penetrationstest zum Stillstand kommt (beispielsweise das Internet-Banking-Portal einer Bank).

Cyberhygiene-Checkup

Jede Organisation sollte mindestens alle zwei Jahre einen umfassenden Cyberhygiene-Checkup durchführen lassen. Besonders empfehlenswert ist dabei die Einbindung externer Spezialist:innen, da diese nicht nur technische Schwachstellen identifizieren, sondern auch mit Branchenstandards und Best-Practices vertraut sind. In der Werbe- und Marktkommunikationsbranche betrifft dies vor allem Systeme zur Datenverwaltung, Kollaborationstools, cloudbasierte Kreativplattformen und kundennahe Produktionsprozesse. Die im Checkup entdeckten Schwachstellen sollten stets im Zusammenhang mit den wichtigsten Prozessen bewertet werden. Aus dieser Analyse entsteht eine priorisierte Liste von Verbesserungsmaßnahmen, die Teil der strategischen Risikobewertung der Organisation wird.

Tipp 10: Abschluss einer gewerblichen Cyberversicherung

Durch die Nutzung der neuen Informations- und Kommunikationstechnologien sind vielfältige Gefahrenquellen entstanden, die es in der Agrar- und Industriegesellschaft in dieser Form nicht gab. Versicherungen entwickeln immer wieder neue Produkte und haben für den Bereich der Cyberversicherung eine große Produktbandbreite definiert, die verdeutlicht, wie komplex diese Themenstellung ist.

Eine Gruppe von Chief Risk Officers von Versicherungsunternehmen (CRO Forum) hat eine lange Liste von Cyberrisiken entwickelt, die vielfältige versicherbare Bereiche aufführt:

- Betriebsunterbrechung durch IT-Systeme
- Betriebsunterbrechung durch den Ausfall von IT-Drittleistern
- Daten- und Softwareverlust
- Betrug oder Finanzvergehen
- Cyberlösegeld oder Erpressung
- Verlust oder Diebstahl von geistigem Eigentum
- Kosten für die Aufarbeitung von Cyberattacken
- Verletzung des Datenschutzes
- Reputationsverlust
- Versagen der Netzwerksicherheit oder Netzwerkausfall
- Rechtliche Beratungs- und Verteidigungskosten
- Ersatz von Strafzahlungen an Behörden (soweit rechtlich zulässig)
- Psychologische Betreuungskosten
- Haftungskosten für beschädigte Produkte
- Haftungskosten für die Geschäftsführung
- Umweltschäden
- Körperverletzung und sogar in manchen Fällen der Tod von Menschen

Jedem Unternehmen wird daher geraten, den Abschluss von Versicherungen gegen solche Risiken anzudenken. Schon die Diskussion über die Versicherbarkeit mit dem potenziellen Versicherer kann den Ausschlag für den Start einer unternehmensweiten Sicherheitsoffensive geben, da Versicherer häufig vor dem Abschluss bestimmte Maßnahmen anregen, um Risiken einzudämmen.

4.2 Für den persönlichen Bereich

Tipp 1: Überprüfung bestehender Datenlecks

Jeder kann mit unentgeltlich am Internet verfügbaren Tools herausfinden, ob eine bestimmte E-Mail-Adresse schon einmal Teil eines Datenlecks war. Über den „HPI Identity Leak Checker“[28] kann ermittelt werden, ob zu einem E-Mail-Konto gehörige Informationen und Passwörter bereits in einem bekannten Hack enthalten sind. Dieser Identitäts-Checker verfügt derzeit über Daten von fast 15 Milliarden gehackten Konten aus 2.000 Datenlecks.

Täglich kommen fast eineinhalb Millionen neue Konten dazu, die in Datenlecks enthalten sind. Gibt man auf der Website des HPI Identity Leak Checker seine E-Mail-Adresse an, wird dem Absender auf diese Adresse ein Bericht zugestellt, aus dem hervorgeht, ob diese Adresse – oder zugehörige Informationen – Teil eines Datenlecks waren.

Für größere Unternehmen und Organisationen gibt es dieses Überprüfungswerkzeug auch als kostenpflichtiges Service. Sie können dort ihre E-Mail-Domäne registrieren lassen und erhalten danach regelmäßig Listen mit allen E-Mail-Adressen, die in der Domäne von einem Datenleck betroffen sind.

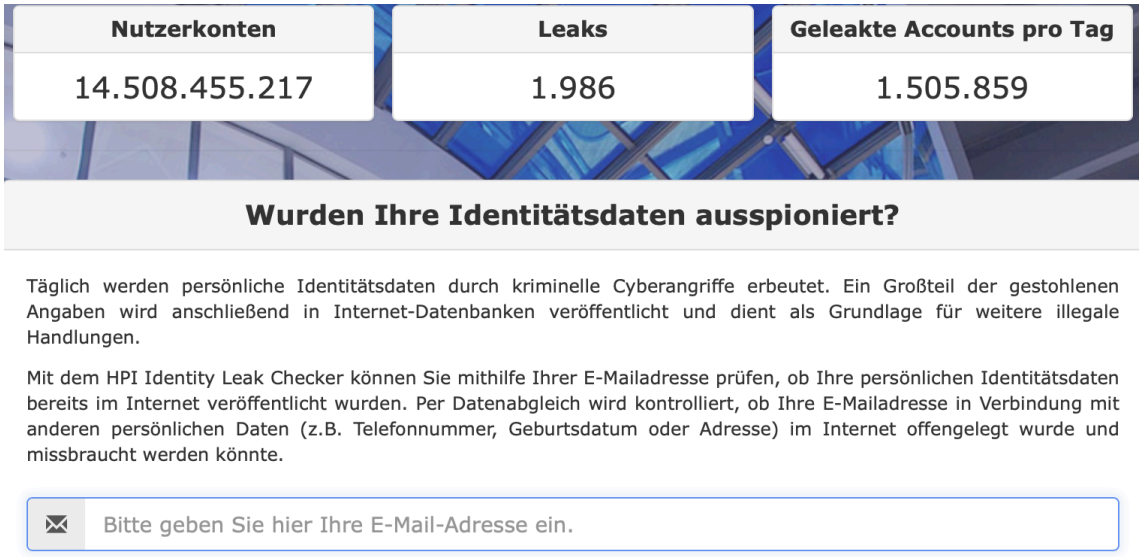


Abbildung: HPI Identity Leak Checker, im Dezember 2026

[28] Hasso-Plattner-Institut: HPI Identity Leak Checker <https://sec.hpi.de/ilc/search?lang=de>

Tipp 2: Sichere Passwörter und Passwort-Manager

Ein wichtiges Einfalltor für Cyberkriminalität sind einfache und leicht ausspähbare oder errechenbare Passwörter. Das Hasso-Plattner-Institut veröffentlicht jedes Jahr eine Liste der beliebtesten Passwörter im deutschen Sprachraum.

Die häufigsten Passwörter sind:

Passworthäufigkeiten

#	Passwort	Häufigkeit
1	123456	8,06 ‰
2	123456789	3,87 ‰
3	password	1,89 ‰
4	qwerty	1,83 ‰
5	12345	1,37 ‰
6	12345678	1,16 ‰
7	111111	1,15 ‰
8	qwerty123	1,01 ‰
9	1q2w3e	0,96 ‰
10	123123	0,84 ‰

Abbildung: Häufigste Passwörter laut Hasso-Plattner-Institut[29]

Die fünf beliebtesten Passwörter in Österreich – laut einem Bericht in der österreichischen IT-Welt:[30]

- admin
- qqqq1111
- 123456
- password
- 12345678

[29]vgl. Hasso Plattner Institut: IT-Security für Unternehmen, vom 10. Dezember 2025 <https://sec.hpi.de/ilc/HPI_ILC_Client_Unternehmen_Angebot.pdf>

[30]vgl. IT-WELT.AT: „admin“ ist 2025 das beliebteste Passwort in Österreich, 20. November 2023 <https://itwelt.at/news/admin-ist-2025-das-beliebteste-passwort-in-oesterreich/>

Über die Website „How secure is my password“[31] kann man die Sicherheit von Passwörtern überprüfen. Sie errechnet die Zeit, die benötigt wird, um das angegebene Passwort mit modernen Programmen zu cracken.

Folgt man den folgenden fünf Regeln und ändert die Passwörter laufend, lebt man sicherer:

- Länge von mehr als 15 Zeichen
- Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen verwenden
- Möglichst keine Wörter aus dem Wörterbuch
- Keine Wiederverwendung von gleichen oder ähnlichen Passwörtern bei unterschiedlichen Anwendungen und Diensten
- Passwortwechsel bei Sicherheitsvorfällen und für Passwörter, welche die obigen Regeln nicht erfüllen

Passwort-Manager sind eine große Hilfe

Für viele Benutzer:innen ist es schwierig, den Überblick über viele verschiedene und lange Passwörter zu behalten. Dabei kann man inzwischen aus einer großen Anzahl von Passwort-Managern auswählen, die neben Passwörtern und Benutzer-IDs auch sensible Informationen wie PIN-Codes und andere geheime Informationen verschlüsselt speichern. Ein gutes Programm in diesem Bereich ist der Passwort-Manager mSecure des Herstellers mSeven Software, der sowohl als mobile App (für iOS und Android) als auch am Desktop für macOS und Windows verfügbar ist. Im sogenannten „Security Center“ macht mSecure auf schwache, doppelte und alte Passwörter aufmerksam, die dann direkt geändert werden können. Die Daten werden in einer speziell geschützten Cloud des Betreibers verschlüsselt gespeichert.[32]

Da man niemals sicher sein kann, dass nicht auch dieses System trotz inhärenter Verschlüsselung einmal gehackt wird, sollte man aber auch hier nicht die vollen Passwörter und Details speichern, sondern einen Teil davon in einem anderen System oder sogar auf Papier an einem sicheren Ort verfügbar halten.

Wichtig: Wenn man sich von einem unsicheren Rechner aus angemeldet hat (z. B. von einem fremden Smartphone oder Computer), sollten man danach unbedingt die betroffenen Passwörter ändern, da man nicht weiß, ob Keylogger installiert waren, die die verwendeten Passwörter aufgezeichnet haben!

[31] vgl. How secure is my password?
<https://www.security.org/how-secure-is-my-password/>

[32] vgl. Secure Your Digital Life with mSecure
<https://www.msecure.com>

Tipp 3: Mehr-Faktor-Authentifizierung

Neben dem verbesserten Passwort-Management ist der Einsatz von Mehr-Faktor-Authentifizierung auf jeden Fall zu empfehlen.

Die verschiedenen Faktoren, die dabei verwendet werden, kommen aus unterschiedlichen Bereichen: einerseits aus dem Bereich „Wissen“ (darunter fällt ein Passwort oder ein selbst gewählter PIN-Code), andererseits aus dem physischen Besitz (beispielsweise eine Smartcard oder ein Token, der einen Code anzeigt) oder aus einer „Eigenschaft“ (beispielsweise ein biometrisches Merkmal wie ein Fingerabdruck).

Zwei- oder Mehr-Faktor-Authentifizierungen sind viel sicherer als einfache Passwörter, da es dann nicht mehr ausreicht, ein solches abzufangen (z. B. durch Phishing oder über den Einsatz von Keyloggern), um illegal in ein System einzudringen. Es steht auch für die meisten Kreditkarten zur Verfügung (z. B. bei Mastercard „Secure Pay“ oder „Verified by Visa“) und verhindert deren Missbrauch.

Tipp 4: Sorgfältiger Umgang mit persönlichen Daten

Persönliche Daten sind ein wahrer Schatz, dessen viele Kriminelle habhaft werden wollen. Die Motive können vielfältig sein – hier nur einige davon:

- Jemand möchte Sie erpressen.
- Jemand möchte Ihre Identität fälschen.
- Jemand möchte bei Ihnen zu Hause einbrechen und benötigt die Adresse.
- Jemand möchte Daten über Sie weiterverkaufen.
- Jemand möchte Sie stalken.

Diese Liste kann beliebig fortgesetzt werden und zeigt auf, dass jede:r wachsam sein sollte, wem diese wertvollen Daten gegeben werden. Die Eingabe der Sozialversicherungsnummer, von Kontoverbindungen oder gar das Versenden von Reisepasskopien per E-Mail können im Falle von Datenlecks zu großen Problemen für Betroffene führen.

Missbrauch persönlicher Fotos

Eine interessante Möglichkeit, um herauszufinden, ob etwa das eigene Profilbild oder Fotos widerrechtlich von anderen verwendet werden, bietet die Google-Bildersuche. Dazu muss man ein Bild in die Google-Suche hochladen. Diese liefert dann als Ergebnis, ob sie eine Person erkannt hat bzw. ob das Bild in einem Profil verwendet wird. Häufig werden im Internet Bilder von Models, Schauspielern und anderen in der Öffentlichkeit stehenden Persönlichkeiten für Fake-Profile in sozialen Netzwerken missbraucht. Für Bilder sollte man auch immer die Speicherung von Informationen über den Aufnahmeort abschalten (das so genannte Geo-Tagging), weil sonst Kriminelle über den Aufnahmeort des Fotos wertvolle Hinweise über den Aufenthaltsort, das Bewegungsprofil oder die Wohnsituation erhalten können.

Tipp 5: Einsatz von Schadsoftware-Scannern und regelmäßige Updates

Jeder Computer und jedes Smartphone benötigen einen guten Virenscanner und eine Firewall, damit laufend die Gefahr der Infektion mit Schadsoftware überprüft und abgewendet werden kann. Auf Webbrowsern sollten Funktionen zur Ausführung aktiver Inhalte sowie zum Auslesen von Informationen gezielt eingeschränkt werden, ohne die grundsätzliche Nutzbarkeit moderner Webanwendungen zu beeinträchtigen. Dazu zählen insbesondere das Blockieren von Third-Party-Cookies, die Aktivierung integrierter Tracking-Schutzmechanismen und Safe-Browsing-Funktionen sowie der Einsatz restriktiver und geprüfter Browser-Erweiterungen. Ergänzend empfiehlt sich die Nutzung getrennter Browserprofile für unterschiedliche Zwecke sowie die Beschränkung auf ausschließlich notwendige Erweiterungen, um die Angriffsfläche möglichst gering zu halten.

Überdies muss regelmäßig das Einspielen von Updates und Patches für alle verwendeten Systeme geprüft und durchgeführt werden. Dazu gehören vor allem Betriebssystem-Updates und ab und zu auch der Wechsel der Hardware, um ein neues, besseres Betriebssystem mit neuen Sicherheitsmerkmalen zu installieren.

Wichtig sind auch die vielen Geräte, die inzwischen das „Internet der Dinge" ausmachen. Auch diese müssen regelmäßig einem Update unterzogen werden.

Tipp 6: Backups von allen wichtigen Systemen

Gerade die Angriffe mit Ransomware zeigen, wie wichtig es ist, laufend Backups der Systeme zu erstellen und diese über lange Zeit sicher zu speichern.

Die Aufbewahrung der Backups sollte auf keinen Fall am Ort der Systeme erfolgen, da etwa bei einem Brand die völlige Zerstörung aller Daten droht, falls nicht noch ein zusätzliches Cloud-Backup existiert.

Wichtig ist auch, Backups über mehrere Monate oder Jahre aufzubewahren. In vielen Unternehmen bestehen regulatorische Regelungen für die Aufbewahrungspflicht. Oft ist es nämlich schwierig, den Zeitpunkt des Befalls durch Schadsoftware zu ermitteln, die sich über Monate im System einnistet.

Gleiches gilt für die kriminelle Veränderung von Daten und Programmen. Einerseits helfen regelmäßige Backups Computerforensiker:innen bei der Suche nach digitalen Spuren, andererseits lassen sich gegebenenfalls wesentliche Daten rekonstruieren, die durch Schadsoftware oder sonstige Sabotage zerstört wurden.

Wichtig: Backups sollten immer verschlüsselt abgespeichert werden. Das gilt besonders auch für Cloud-Backups!

Tipp 7: Verschlüsselung verwenden / VPN und sichere Clouds

Die meisten Websites setzen das HTTPS-Protokoll ein, das eine sichere und verschlüsselte Kommunikation mit ihnen ermöglicht. Dazu muss lediglich ein Zertifikat angemeldet und jährlich erneuert werden und auf der Website im WWW-Verzeichnis eingespielt sein. Wie gut eine Website dahingehend abgesichert ist, kann man einfach über die Services SSL-Scanner oder Web Inspector prüfen.

Während Privatanwender die kostenlose PGP-Verschlüsselung nützen können, empfiehlt sich für größere Organisationen der Einsatz von Chipkarten, die auch zugleich als Mitarbeitendenausweise verwendet werden können.

Eine weitere wichtige Lösung sind moderne elektronische Identitäts- und Signaturdienste, wie sie in Österreich unter anderem von A-Trust bereitgestellt werden. Diese Lösungen ermöglichen eine rechtskonforme, hochsichere digitale Identifikation sowie qualifizierte elektronische Signaturen über Cloud und Mobilgeräte hinweg. Sie stellen eine zeitgemäße Weiterentwicklung der klassischen Bürgerkarte dar und bieten mit mobilen Signaturen und cloudbasierten Vertrauensdiensten eine praxistaugliche Alternative ohne zusätzliche Hardware, bei gleichzeitig hohem Sicherheitsniveau.

Nachrichten und Speicherplatz

Nicht zu vergessen ist auch die Verschlüsselung von Festplatten und USB-Sticks, die meist sehr einfach mit den vom jeweiligen Betriebssystem zur Verfügung stehenden Mitteln möglich ist. Wichtig ist bei vertraulichen Nachrichten auch, dass E-Mails oder E-Mail-Anhänge verschlüsselt versendet werden.

Verschlüsselung im Netzwerk

Private und Firmen können inzwischen sehr einfach ihre Kommunikation verschlüsseln, indem sie VPNs (sogenannte „Virtuelle private Netzwerke“) verwenden. Diese ermöglichen es, zwar das öffentliche Netzwerk zu verwenden, dort aber einen sogenannten „IP-Tunnel“ zwischen sich und den Heimsystemen aufzubauen, durch den sicher kommuniziert werden kann. Über das Verwenden von VPNs hinaus empfiehlt sich auch die Verwendung von sicheren Cloud-Lösungen. Diese stehen keineswegs nur großen Unternehmen zur Verfügung, sondern können auch von privaten Anwenderinnen und Anwendern etwa von Hornetdrive[33], einem verschlüsselten Cloud-Speicher, bezogen werden.

Chat-Systeme

In Zeiten zunehmender Bedrohungen durch Datenlecks in Chat-Systemen empfiehlt es sich, sich die Sicherheitsmerkmale der Anbieter anzuschauen. Hier sind das Schweizer Threema (vom Hersteller Threema GmbH) oder Signal (vom Hersteller Open Whisper Systems) gute Beispiele für sichere, fortgeschrittene Applikationen.

[33] vgl. Hornetdrive – verschlüsselter Cloud-Speicher aus Deutschland < https://hornetdrive.com/de/>

Tipp 8: Sichere E-Mails und mehr E-Mail-Disziplin

Der alte Spruch „Jedes Schrifterl ist ein Gifterl“ gilt besonders bei der Verwendung von nicht verschlüsselten E-Mails, die relativ einfach von Unbefugten mitgelesen werden können. Sehr vertrauliche Inhalte sollten immer verschlüsselt ausgetauscht oder überhaupt nicht elektronisch übermittelt werden.

Es empfiehlt sich auch die Verwendung eines E-Mail-Anbieters, der verschlüsselt operiert, wie beispielsweise ProtonMail vom Schweizer Anbieter Proton Technologies AG in Genf. Je nach Sicherheitsstandard sollte die Möglichkeit, über Webmail ins E-Mail-System einzusteigen, überlegt werden. Hier kann es beispielsweise vorkommen, dass man unter Nutzung eines öffentlichen Rechners (etwa in einer Flughafenlounge) in sein E-Mail-System einsteigt, ohne zu bemerken, dass ein Krimineller vorher einen Keylogger auf diesem Rechner installiert hat. Wird in diesem Fall keine Mehr-Faktor-Authentifizierung verwendet, könnte ein:e Cyberkriminelle:r nun ausreichende Anmeldeinformationen ausgespäht haben, um sich im Namen eines anderen Users anzumelden.

Tipp 9: Vorsicht vor unbekannten USB-Sticks

USB-Sticks oder das, was dafür gehalten wird, können großen Schaden anrichten und durch Anstecken den betroffenen Computer mit Malware infizieren.

Ein gutes Beispiel ist der „Rubber Ducky“, ein USB-Stick, der, an einen Computer angesteckt, ein Backdoor („Hintertür“) installiert, Dokumente und Passwort stiehlt und einen Angriffsvektor für spätere Penetrationstests aufbaut.

Man sollte nur USB-Sticks verwenden, deren Herkunft man kennt und die vor der Verwendung geprüft wurden!

Tipp 10: Abschluss einer Cyberversicherung für Privatpersonen und Haushalte

Viele Versicherungsunternehmen bieten inzwischen im Rahmen von Hausratsversicherungen oder als separat gekennzeichnete Cyberprodukte die Absicherung gegen finanzielle Schäden durch Cyberangriffen an.

Ein österreichischer Versicherer hat im Rahmen der Erweiterung einer Haushaltsschutz-Versicherung eine umfangreiche „IT-Assistance“ für Probleme mit Computern oder Unterhaltungselektronik im Angebot. Der Versicherer wirbt u. a. mit folgenden Leistungsmerkmalen:

- Soforthilfe durch ein:e IT-Spezialist:in per Chat oder Telefon bei Fragen zu Computer, Smartphone und Co.
- Hilfe bei Hard- und Software-, Netzwerk- oder Internetproblemen
- Beratung bei Identitätsdiebstahl und Cybermobbing

5 Krisenmanagement

Aktuelle Cyberattacken zeigen häufig, wie rasch und unvorhersehbar digitale Krisen entstehen können. Auch die Mitglieder der Fachgruppe Werbung und Marktkommunikation sind davon zunehmend betroffen. Die Branche arbeitet hochgradig vernetzt, setzt eine Vielzahl digitaler Tools ein, verwaltet wertvolle Kundendaten und steht unter kontinuierlichem Zeitdruck. All diese Faktoren machen Agenturen, Kreativstudios, Medienhäuser und Kommunikationsabteilungen zu attraktiven Zielen für Angreifer:innen.

Der zuverlässige und störungsfreie Betrieb digitaler Systeme ist daher ein zentraler Erfolgsfaktor für die gesamte Branche. Auch bei größter Sorgfalt kann es jedoch zu schweren Vorfällen kommen. In einer Branche, in der Inhalte oft zeitkritisch produziert und veröffentlicht werden, ist die schnelle Erkennung und Eindämmung eines Angriffs besonders wichtig.

Moderne Software zur Prävention von Datenlecks kann auffällige Datenbewegungen frühzeitig erkennen, etwa wenn große Datenmengen untypisch exportiert oder externe Verbindungen hergestellt werden. Dies ist besonders relevant für Agenturen, die täglich mit sensiblen Daten ihrer Kund:innen arbeiten und oft einen hohen Anteil an externen Zugriffen verwalten. Auch die Nutzung eines Security-Operation-Centers (SOC) kann die Früherkennung oder Abwehr einer Cyberattacke erleichtern.

Trotz aller Vorsorge braucht jede Organisation einen belastbaren Notfallplan für den Ernstfall, der folgende Maßnahmen enthält:

- Die sofortige Abschottung betroffener Systeme, um Kampagnenmaterialien, Kundeninformationen und Kommunikationsdaten zu schützen.

- Die Möglichkeit, ein elektronisches Notsystem zu aktivieren, um den laufenden Betrieb zumindest eingeschränkt fortzuführen.

- Die Fähigkeit, kurzfristig auch ohne digitale Werkzeuge arbeitsfähig zu bleiben, etwa indem wichtige Tätigkeiten vorübergehend analog durchgeführt werden.

- Die klare und schnelle Kommunikation mit Mitarbeitenden, Kund:innen und Partner:innen, im Bedarfsfall auch über papierbasierte Informationswege.

Gerade in kreativen und kommunikationsintensiven Branchen ist Transparenz entscheidend. Unternehmen, die offen informieren und professionell handeln, behalten das Vertrauen ihrer Kund:innen und festigen ihre Position als verlässliche Partner.

Organisationen, die einen Cybervorfall strukturiert bewältigen, zeigen zugleich, dass sie nicht nur kreative Exzellenz bieten, sondern auch verantwortungsbewusst mit digitalen Risiken umgehen.

Cyberkrisen lassen sich nicht vollständig vermeiden, sie können aber zu einem wichtigen Entwicklungsschritt werden. Wer gut vorbereitet ist, stärkt nicht nur die

eigene Resilienz, sondern erhöht auch die Glaubwürdigkeit gegenüber bestehenden und potenziellen Auftraggeber:innen.

Die Mitglieder der Fachgruppe Werbung und Marktkommunikation können dadurch zeigen, dass professionelle Kreativarbeit und verantwortungsvolle digitale Sicherheitskultur untrennbar zusammengehören.

Vorbereitung auf Krisen

Die Vorbereitung auf Krisensituationen ist eine grundlegende Voraussetzung dafür, dass Unternehmen auch unter außergewöhnlichen Umständen handlungsfähig bleiben. Dabei betrifft Krisenvorsorge nicht nur Organisationen als Ganzes, sondern auch Führungskräfte und Mitarbeitende auf individueller Ebene. Insbesondere Krisen, die mit dem Ausfall von IT oder Kommunikationssystemen einhergehen, können den Geschäftsbetrieb massiv beeinträchtigen und erfordern daher eine gezielte und realistische Vorbereitung.

Solche Situationen entstehen nicht nur durch gezielte Angriffe krimineller Akteure. Auch ein großflächiger Stromausfall, technische Defekte in Rechenzentren, Ausfälle von Cloudanbietern oder Störungen bei Telekommunikationsanbietern können dazu führen, dass digitale Systeme kurzfristig oder über längere Zeit nicht verfügbar sind. Gerade diese Szenarien werden in der Praxis häufig unterschätzt, obwohl ihre Auswirkungen vergleichbar gravierend sein können.

Vor diesem Hintergrund ist es notwendig, frühzeitig festzulegen, wie im Ernstfall zumindest für einen begrenzten Zeitraum analog weitergearbeitet werden kann. Das Ziel ist, den vollständigen Stillstand zu vermeiden und die wichtigsten Funktionen der Organisation aufrechtzuerhalten, bis digitale Systeme wieder stabil zur Verfügung stehen. Analoge Notfallprozesse sind dabei kein Ersatz für moderne IT, sondern eine bewusste Überbrückungslösung zur Sicherung der Handlungsfähigkeit.

Die kritischen Kernprozesse einer Organisation sollten so definiert sein, dass sie auch ohne IT-Unterstützung zumindest eingeschränkt weitergeführt werden können. Dazu zählen etwa Entscheidungsfindung, interne und externe Kommunikation, Kundenkontakt, Freigaben oder grundlegende Verwaltungsabläufe. Diese Prozesse müssen bekannt, dokumentiert und regelmäßig überprüft werden, damit sie im Krisenfall nicht improvisiert durchgeführt werden müssen.

Business-Continuity-Plan

Ein zentraler Bestandteil der Vorbereitung auf Krisen ist ein Business-Continuity-Plan. Darin wird beschrieben, welche Systeme besonders kritisch sind, welche Alternativen oder Ersatzlösungen bei einem Ausfall greifen und wie ein Notbetrieb ohne IT-Systeme konkret organisiert ist. Der Plan legt fest, welche Aufgaben priorisiert werden, wer Entscheidungen trifft und wie der Übergang vom Krisenbetrieb zurück in den Normalbetrieb erfolgt.

Die schriftliche Auseinandersetzung mit diesen Fragestellungen führt in der Praxis oft zu wichtigen Erkenntnissen, da sehr genau analysiert wird, an welchen Stellen IT-Systeme tatsächlich unverzichtbar sind, wo Abhängigkeiten bestehen und wo Risiken bislang unterschätzt wurden.

Eine strukturierte Krisenvorbereitung ist auch für den Abschluss und die Aufrechterhaltung einer Cyberversicherung von wesentlicher Bedeutung. Versicherer erwarten nachvollziehbare Konzepte zur Aufrechterhaltung des Geschäftsbetriebs, klar definierte Zuständigkeiten und dokumentierte Notfallprozesse. Unternehmen, die hier gut vorbereitet sind, verbessern nicht nur ihre Resilienz, sondern auch ihre Versicherbarkeit und ihre Position im Schadensfall, da Nachweise für das sorgfältige und ordentliche Handeln gefordert werden.

Zusammenstellung des Krisenstabs

Sowohl die Definition der Krisenorganisation als auch die Einrichtung eines Krisenstabs sind zentrale Elemente des professionellen Umgangs mit Cyberangriffen und anderen schwerwiegenden IT- Sicherheitsvorfällen.

Bereits in den ersten Stunden entscheidet sich, ob ein Unternehmen oder eine Organisation strukturiert und handlungsfähig bleibt oder in operative und kommunikative Unordnung gerät. Entsprechend wichtig ist es, rasch klare Zuständigkeiten und Entscheidungswege festzulegen.

Zu den unmittelbaren Sofortmaßnahmen zählt die Zusammenstellung jener Personen, die an den unterschiedlichen Stellen des Unternehmens an der Bewältigung der Krise zusammenwirken müssen. Vorteilhaft ist, wenn der Krisenstab eines Unternehmens schon vor dem Auftreten einer großen Krise definiert wurde, weil man dann viel schneller handlungsfähig ist.

Der Krisenstab sollte interdisziplinär besetzt sein und sowohl Management, IT und Informationssicherheit als auch Kommunikation, Recht, Datenschutz und gegebenenfalls Personalwesen umfassen. Je nach Größe und Struktur des Unternehmens sollten auch externe Expert:innen eingebunden werden, etwa aus den Bereichen IT-Forensik, Rechtsberatung und Krisenkommunikation.

Ein:e externe:r Krisenmanager:in hilft in der Praxis oft, den Überblick zu bewahren und aufgrund der Erfahrung dieser Person, schnell und professionell Entscheidungsalternativen zu präsentieren.

In der Krise sind eindeutige Entscheidungsbefugnisse unerlässlich. Lange Abstimmungsprozesse oder unklare Verantwortlichkeiten führen zu Verzögerungen

und erhöhen das Schadenspotenzial. Insbesondere dann, wenn digitale Freigabe- und Genehmigungssysteme nicht verfügbar sind, müssen analoge Ersatzregelungen greifen. Dazu zählen klar definierte Unterschriftenregelungen, mündlich mögliche Freigaben durch autorisierte Personen sowie eine strukturierte Dokumentation aller solcherart getroffenen Entscheidungen.

Der Krisenstab übernimmt dabei nicht nur die operative Steuerung der technischen Maßnahmen, sondern auch die Priorisierung von Aufgaben, die Koordination interner und externer Beteiligter sowie die laufende Lagebewertung. Eine analoge Begleitdokumentation durch Protokolle, Whiteboards oder Listen von Maßnahmen, unterstützt die Übersicht und Nachvollziehbarkeit, insbesondere bei längeren Krisen oder wechselnden Beteiligten.

Von besonderer Bedeutung ist die frühzeitige Kontaktaufnahme mit wichtigen externen Dienstleistern. Dazu zählen insbesondere Banken und Zahlungsdienstleister, aber auch Versicherungen, zentrale Lieferanten oder Betreiber kritischer Infrastrukturen. So kann die finanzielle Handlungsfähigkeit des Unternehmens auch beim Ausfall interner Systeme sichergestellt werden, etwa durch alternative Zahlungswege, manuelle Freigaben oder temporäre Anpassungen von Limits und Prozessen.

Eine klar strukturierte Krisenorganisation stellt sicher, dass Maßnahmen koordiniert erfolgen, Informationen gebündelt werden und Entscheidungen auch unter Zeitdruck tragfähig bleiben. Sie bildet damit die Grundlage für eine wirksame technische, organisatorische und kommunikative Bewältigung der Krise und erleichtert zugleich die spätere Aufarbeitung und vergleichsweise sanfte Rückkehr in den Normalbetrieb.

Krisenkommunikation

Eine professionelle Krisenkommunikation sollte bereits im Vorfeld klar definiert und organisatorisch verankert sein. In einer akuten Krisen- oder Notsituation können dadurch vorab ausgewählte und spezialisierte Berater:innen (deren Zeit schon vorab reserviert wurde) unverzüglich eingebunden werden. Aufwendige Abstimmungen oder zeitkritische Verhandlungen über finanzielle Konditionen von Beratungsverträgen verzögern im Ernstfall die Reaktionsfähigkeit und führen dazu, dass wertvolle Zeit verloren geht, die für Schadensbegrenzung und Steuerung der Situation entscheidend sein kann.

Die Unterstützung bei der Krisen-PR und Öffentlichkeitsarbeit ist ein zentraler Bestandteil des gesamten Krisenmanagements und dient dazu, auch in sehr dynamischen und belastenden Situationen handlungsfähig zu bleiben.

Damit soll vor allem sichergestellt werden, dass die Deutungshoheit über das Geschehen nicht an Medien oder sonstige Dritte verloren geht. Das Vertrauen muss bei allen relevanten Anspruchsgruppen gesichert sein oder wiederhergestellt werden, um rechtliche und wirtschaftliche Folgeschäden sowie Imageprobleme so gering wie möglich zu halten.

Am Beginn steht die klare Festlegung eines Krisenkommunikators, der personenident mit dem Leiter des Krisenmanagements sein kann. Diese Rolle ist von entscheidender Bedeutung, da sie als einzige offiziell autorisierte Stimme der Organisation nach

außen auftreten sollte. Der Krisenkommunikator koordiniert sämtliche Aussagen, stimmt Inhalte intern ab und sorgt dafür, dass Informationen zeitgerecht, konsistent und nachvollziehbar kommuniziert werden. Dadurch wird verhindert, dass unterschiedliche oder widersprüchliche Botschaften von verschiedenen Stellen nach außen gelangen. Auch für die Kommunikation innerhalb der Organisation ist es wünschenswert, wenn diese von der gleichen Stelle durchgeführt wird.

Parallel dazu erfolgt die Definition der internen und externen Kommunikationsinhalte. Mitarbeitende benötigen rasch Orientierung und Sicherheit, um Gerüchten, Unsicherheit oder Fehlverhalten vorzubeugen. Extern müssen Kund:innen, Geschäftspartner:innen, Medien sowie weitere Stakeholder sachlich, transparent und zielgruppengerecht informiert werden. Dabei ist klar festzulegen, welche Informationen zu welchem Zeitpunkt und über welche Kanäle kommuniziert werden.

Ein wesentlicher Schwerpunkt liegt auf der Erstellung eines belastbaren Erststatements sowie eines einheitlichen Wordings. Dieses dient als Grundlage für Presseanfragen, Interviews und schriftliche Stellungnahmen. Gleichzeitig werden Fach- und Führungskräfte auf mögliche Rückfragen vorbereitet, damit auch in spontanen Gesprächssituationen konsistente Aussagen erfolgen. Einheitliche Sprachregelungen schaffen Sicherheit nach innen und außen und tragen wesentlich zur Glaubwürdigkeit der Organisation bei.

Nach Möglichkeit sollte die Krisenkommunikation in Zusammenarbeit mit einer professionellen PR-Agentur durchgeführt werden. Insbesondere bei größerer medialer Aufmerksamkeit, internationaler Berichterstattung oder sensiblen Reputationslagen kann externe Unterstützung helfen, die Kommunikation professionell zu steuern und zusätzliche Ressourcen bereitzustellen. Die Kommunikationsstrategie sollte dabei dem Prinzip einer offenen und transparenten Kommunikation im Sinne einer kontrollierten Offensive folgen. Das bedeutet, aktiv zu informieren und Verantwortung zu zeigen, ohne operative Details oder rechtlich sensible Inhalte unkontrolliert preiszugeben.

Im Umgang mit Öffentlichkeit und Medien sollte situationsabhängig entschieden werden, ob eine Pressemitteilung ausreichend ist oder ob zusätzlich eine Pressekonferenz einberufen werden muss. Maßgeblich dafür sind Art, Umfang und gesellschaftliche Relevanz der Krise sowie das öffentliche Interesse. Unabhängig vom gewählten Format ist eine gute inhaltliche Vorbereitung entscheidend, um auch kritischen Nachfragen souverän begegnen zu können.

Begleitend dazu sollte ein laufendes Monitoring des öffentlichen Meinungsbildes gemacht werden. Klassische Medien, Onlinemedien, soziale Netzwerke und Fachforen sollten dabei beobachtet werden, um Stimmungen, Narrative, Fehlinformationen oder Eskalationstendenzen frühzeitig zu erkennen. Auf dieser Basis kann die Kommunikationsstrategie laufend angepasst werden, etwa durch Klarstellungen, ergänzende Informationen oder gezielte Hintergrundgespräche.

Kommunikation und Meldung an Behörden

Ein zentraler Bereich im Krisenmanagement ist die professionelle Kommunikation mit Behörden, insbesondere mit der Polizei und Justiz. Dazu gehört die vollständige und

sachlich korrekte Formulierung einer Anzeige unter Darstellung der relevanten Sachverhalte und möglicher Straftatbestände. Die Erst- und Folgekommunikation mit den Ermittlungsbehörden und der laufende Kontakt während der Ermittlungen sollte zu jedem Zeitpunkt durch professionelle Berater:innen durchgeführt werden.

Bei Bedarf gibt es auch die Notwendigkeit einer erweiterten Zusammenarbeit mit der Justiz, etwa im Rahmen von Akteneinsicht oder der Abstimmung weiterer rechtlicher Schritte. Ergänzend müssen „Take-Down-Notices" vorbereitet und koordiniert zu Stande kommen, wenn gestohlene Daten veröffentlicht oder im Internet verbreitet werden. Zudem müssen Informationen anderer Behörden oder Stellen eingeholt werden, die bei der technischen, organisatorischen oder operativen Abwehr des Angriffs unterstützen können.

Wenn eine Verletzung des Schutzes personenbezogener Daten vorliegt, muss die Datenschutzbehörde informiert werden. Dabei sind die Meldefristen gemäß der nationalen Umsetzung der Datenschutzgrundverordnung und des österreichischen Datenschutzgesetzes relativ kurz bemessen:

- Bei Verletzungen des Schutzes personenbezogener Daten muss innerhalb von 72 Stunden eine Meldung an die Datenschutzbehörde gemacht werden, sobald ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht.
  (Art. 33 DSGVO)

- Die betroffenen Personen müssen ohne unangemessene Verzögerung informiert werden, wenn ein hohes Risiko für ihre Rechte und Freiheiten vorliegt.
  (Art. 34 DSGVO)

Bei Bedarf sollte auch in Fragen der Behördenkommunikation eine externe Rechtsberatung eingebunden werden, um datenschutzrechtliche und anders gelagerte gesetzliche Pflichten korrekt zu erfüllen und Risiken zu minimieren. Ebenso sollte die Kommunikation an betroffene Personen gemäß den Vorgaben des Datenschutzrechts professionell vorbereitet und begleitet werden.

Bei börsennotierten Unternehmen kann eine Ad-hoc-Meldung notwendig sein, ebenso die Information der Finanzmarktaufsicht oder anderer zuständiger Aufsichtsorgane. Sind Geschäftsgeheimnisse, sensible Unternehmensinformationen oder Erfindungen betroffen, müssen gegebenenfalls weitere Stellen oder Rechteinhaber informiert werden.

In besonderen Situationen sollte auch eine strukturierte und kontrollierte Kommunikation mit kriminellen Angreifer:innen diskutiert werden, stets mit klarer Zielsetzung und in enger Abstimmung mit Rechtsberatung und Behörden.

Neues Cybersicherheitsgesetz in Österreich (NISG 2026)

Am 12. Dezember 2025 wurde im Nationalrat nach langem Tauziehen zwischen den politischen Parteien das neue Cybersicherheitsgesetz beschlossen, das anschließend erfolgreich im Bundesrat bestätigt wurde. Das Gesetz dient der Umsetzung der europäischen NIS2-Richtlinie und wird neun Monate nach Kundmachung im

Bundesgesetzblatt, am 1. Oktober 2026 in Kraft treten. Bis zu diesem Zeitpunkt gilt das NISG 2018.

Mit dem NISG 2026 wird der Anwendungsbereich der Cybersicherheitsregulierung deutlich ausgeweitet und zugleich konkretisiert. Erfasst sind nun nicht mehr nur klassische Betreiber kritischer Infrastruktur, sondern auch sogenannte wesentliche und wichtige Einrichtungen aus zahlreichen Sektoren wie Energie, Verkehr, Gesundheit, digitale Dienste, öffentliche Verwaltung sowie ausgewählte Industrie und Dienstleistungsbereiche. Wesentliche Einrichtungen unterliegen dabei strengeren Aufsichts- und Sanktionsmechanismen, während wichtige Einrichtungen ebenfalls umfassende Sicherheits- und Meldepflichten erfüllen müssen.

Für ca. 4.000 Unternehmen und Einrichtungen ab mittlerer Größe aus 18 festgelegten gesellschaftlich relevanten Sektoren werden künftig verbindliche Sicherheitsanforderungen sowie Meldepflichten bei Sicherheitsvorfällen gelten. Diese Regelungen betreffen nicht nur die unmittelbar erfassten Organisationen selbst, sondern erstrecken sich ausdrücklich auch auf die Sicherheit der Lieferkette. Unternehmen sind damit verpflichtet, nicht nur die eigenen IT-Systeme angemessen abzusichern, sondern auch die Cybersicherheitsrisiken ihrer IT-Dienstleister, Cloud-Anbieter, Softwarelieferanten sowie weiterer kritischer Zulieferer systematisch zu bewerten. Um gesetzeskonform zu handeln, müssen betroffene Einrichtungen ihre Dienstleister und Lieferanten vertraglich dazu verpflichten, angemessene Risikomanagement- und Sicherheitsmaßnahmen umzusetzen und deren Einhaltung nachzuweisen. Damit entfaltet die Regulierung eine weitreichende Wirkung über die direkt betroffenen Unternehmen hinaus.

Auch Organisationen, die formell nicht unter die Richtlinie fallen, geraten mittelbar in den Anwendungsbereich des NISG 2026, sobald sie Leistungen für regulierte Unternehmen erbringen. Sicherheitsanforderungen, Nachweispflichten und vertragliche Absicherungen werden dadurch zu einem festen Bestandteil von Geschäftsbeziehungen.
Für Unternehmen der Fachgruppe Werbung und Marktkommunikation ergeben sich daraus nicht nur neue Anforderungen, sondern vor allem zusätzliche geschäftliche Möglichkeiten.

Viele Kund:innen aus regulierten Branchen werden Unterstützung bei der Umsetzung der neuen Vorgaben benötigen, insbesondere in den Bereichen Krisenkommunikation, strukturierte Informationsprozesse, Stakeholder-Kommunikation sowie bei der Vorbereitung für die korrekte Reaktion auf meldepflichtige Vorfälle. Agenturen und Kommunikationsdienstleister können hier mit spezifischem Know-how, standardisierten Prozessen und branchenspezifischer Erfahrung einen klaren Mehrwert bieten.

Von besonderer Relevanz sind die speziellen Rahmenbedingungen für das Krisenmanagement, die durch die Regulierung vorgegeben werden. Sicherheitsvorfälle unterliegen klar definierten Zeitfenstern für Erstmeldungen, Zwischenberichte und Abschlussmeldungen. Diese engen Fristen erfordern eine sehr gute organisatorische Vorbereitung, klare Zuständigkeiten und eingespielte Abläufe zwischen Technik, Management, Recht und Kommunikation. Improvisation ist in diesen Situationen kaum möglich.

Gerade im Krisenfall zeigt sich, wie wichtig vorab definierte Prozesse, vorbereitete Kommunikationsbausteine und ein funktionierender Krisenstab sind. Unternehmen, die ihre Krisenorganisation und ihre externe Kommunikation bereits im Vorfeld an die regulatorischen Anforderungen anpassen, können Meldepflichten fristgerecht erfüllen, Reputationsschäden begrenzen und zugleich gegenüber Kund:innen, Behörden und Öffentlichkeit professionell auftreten. Je nach Vorfall sind Meldungen an ab dem 1. Oktober 2026 an das Bundesamt für Computersicherheit und ein sektorspezifisches CSIRT erforderlich. Das NISG 2026 sieht dazu einen mehrstufigen Meldeprozess vor:

- Frühwarnung innerhalb von 24 Stunden
- Erstmeldung innerhalb von 72 Stunden
- Abschlussbericht nach spätestens einem Monat

Die gesetzlichen Neuregelungen führen zu einer deutlich engeren Verzahnung von IT-Sicherheit, unternehmensweitem Risikomanagement und strategischer Kommunikation. Cybervorfälle sind nicht mehr ausschließlich ein technisches Thema, sondern haben unmittelbare Auswirkungen auf Reputation, Vertrauen, Geschäftskontinuität und regulatorische Haftung.

Für die Mitglieder der Fachgruppe Werbung und Marktkommunikation ergibt sich die große Chance der Positionierung als qualifizierte und verlässliche Partner:innen für betroffene Kund:innen. Sie können ihre Kompetenzen gezielt einbringen, um Organisationen bei der Entwicklung krisenfester Kommunikationsstrategien, bei der Vorbereitung auf Cybervorfälle sowie bei der professionellen internen und externen Krisenkommunikation zu unterstützen. Damit leisten sie einen aktiven Beitrag zur Stärkung der organisatorischen Resilienz und zur nachhaltigen Krisenfestigkeit ihrer Kund:innen.

6 Wirtschaftskammer Cybersecurity-Ressourcen

6.1 Cybersecurity-Hotline und die UBIT

Die Cybersecurity-Hotline der Wirtschaftskammer steht Mitgliedsbetrieben als verlässliche Anlaufstelle bei akuten Sicherheitsvorfällen im digitalen Raum zur Verfügung. Unter der kostenlosen Telefonnummer 0800 888 133 erhalten Unternehmen rund um die Uhr Unterstützung, wenn es zu Cyberangriffen, konkreten Verdachtsfällen oder anderen sicherheitsrelevanten Zwischenfällen kommt. Das Serviceangebot richtet sich besonders an kleine und mittlere Betriebe, die im Ernstfall rasch Orientierung benötigen und nicht über eigene IT-Sicherheitsabteilungen verfügen.

Im ersten Schritt bietet die Hotline eine strukturierte und niederschwellige Ersthilfe. Gemeinsam mit den betroffenen Unternehmen wird die jeweilige Situation eingeschätzt und eingeordnet. Dabei werden Art und mögliche Tragweite des Vorfalls analysiert, etwa ob es sich um einen laufenden Angriff, einen bereits erfolgten Sicherheitsvorfall oder einen begründeten Verdacht handelt. Auf dieser Basis erhalten Betriebe konkrete Sofortempfehlungen zur Schadensbegrenzung und zur Stabilisierung des laufenden Betriebs. Ergänzend werden Hinweise gegeben, wie sich weitere Risiken kurzfristig reduzieren lassen und welche nächsten Schritte sinnvoll sind.

Eine wichtige Rolle kommt der Fachgruppe Unternehmensberatung, Buchhaltung und Informationstechnologie, kurz UBIT, zu. Über das Netzwerk der UBIT stehen qualifizierte Berater:innen sowie IT-Sicherheitsdienstleister zur Verfügung, die im Bedarfsfall rasch und gezielt eingebunden werden können.

Die Hotline fungiert dabei als Schnittstelle, um betroffene Unternehmen an geeignete Expert:innen zu vermitteln, die bei der technischen Analyse, der Bereinigung kompromittierter Systeme, der Wiederherstellung des IT-Betriebs sowie bei organisatorischen und rechtlichen Fragestellungen unterstützen.

Über die enge Einbindung der UBIT wird sichergestellt, dass Mitgliedsbetriebe auf geprüfte und erfahrene Ansprechpartner zurückgreifen können, die mit den Anforderungen von kleinen und mittleren Unternehmen vertraut sind. Dies betrifft sowohl akute Notfallsituationen als auch weiterführende Maßnahmen zur nachhaltigen Verbesserung der IT-Sicherheit, etwa durch Risikoanalysen, Sicherheitskonzepte oder begleitende Beratungsleistungen.

Durch die ständige Erreichbarkeit stellt die Cybersecurity-Hotline sicher, dass betroffene Betriebe auch außerhalb üblicher Geschäftszeiten nicht alleine gelassen werden. Gerade bei Angriffen wie Ransomware, Phishing oder beim Verdacht auf Datenabflüsse ist eine rasche Reaktion entscheidend, um wirtschaftliche Schäden, Betriebsunterbrechungen und Reputationsverluste möglichst gering zu halten.

6.2 IT-SAFE.AT

Die Wirtschaftskammer Österreich bietet mit der Plattform www.it-safe.at[34] eine verlässliche und praxisnahe Unterstützung für Unternehmen im Bereich der IT-Sicherheit und Cybersicherheit.

Das Angebot richtet sich insbesondere an kleine und mittlere Unternehmen und verfolgt das Ziel, Betriebe für digitale Risiken zu sensibilisieren und ihnen konkrete Hilfestellung bei der Absicherung ihrer IT-Systeme zu geben. In einer zunehmend digitalisierten Wirtschaft, in der nahezu alle Geschäftsprozesse auf IT-gestützten Anwendungen basieren, stellt diese Unterstützung einen wichtigen Beitrag zur Stärkung der digitalen Widerstandsfähigkeit dar.

Ein wichtiges Anliegen von it-safe.at ist es, das Verständnis dafür zu fördern, dass IT-Sicherheit keine einmalige Maßnahme ist, sondern als kontinuierlicher und ganzheitlicher Prozess verstanden werden muss.

Technische Schutzlösungen, organisatorische Regelungen und das Sicherheitsbewusstsein der Mitarbeiter:innen greifen dabei ineinander und müssen regelmäßig überprüft und angepasst werden. Gleichzeitig zeigt die Initiative auf, dass bereits mit grundlegenden und gut umsetzbaren Maßnahmen ein hohes Maß an Schutz erreicht werden kann und viele gängige Angriffsformen dadurch deutlich an Wirkung verlieren.

Die Plattform stellt Unternehmen eine Vielzahl kostenloser Ressourcen zur Verfügung, darunter praxisorientierte Handbücher, Checklisten und einen umfassenden Onlineratgeber. Diese Inhalte unterstützen Betriebe dabei, typische Cyberrisiken zu erkennen, Sicherheitslücken zu identifizieren und geeignete Schutzmaßnahmen Schritt für Schritt umzusetzen. Der Fokus liegt dabei auf verständlichen, alltagstauglichen Empfehlungen, die auch ohne tiefgehendes technisches Spezialwissen angewendet werden können.

[34] vgl. IT-SAFE.AT <https://www.wko.at/it-sicherheit/it-sicherheit?shorturl=it-safeat>

6.3 IT-Security Experts Group

Die „IT-Security Experts Group“[35] ist ein österreichweiter Zusammenschluss qualifizierter IT-Dienstleister sowie Berater:innen mit ausgewiesener Expertise im Bereich der IT-Sicherheit.

Ziel dieses Netzwerks ist es, Unternehmen in ganz Österreich einen verlässlichen Zugang zu fachkundiger Unterstützung bei sicherheitsrelevanten Fragestellungen zu ermöglichen und gleichzeitig hohe Qualitätsstandards in der Beratung und Umsetzung von Sicherheitsmaßnahmen sicherzustellen.

Die Mitglieder der „IT Security Experts Group“ erbringen ihre Leistungen auf Grundlage klar definierter Qualitätskriterien und standardisierter Vorgehensweisen. Diese gemeinsamen Rahmenbedingungen sorgen dafür, dass Beratungsleistungen, technische Analysen und Umsetzungsprojekte nachvollziehbar, strukturiert und an bewährten Best-Practices ausgerichtet sind. Unternehmen profitieren dadurch von einem einheitlichen Qualitätsniveau, unabhängig davon, welcher konkrete Dienstleister oder welch:e Berater:in beauftragt wird.

Das Leistungsspektrum der „IT Security Experts Group“ umfasst eine breite Palette an Dienstleistungen im Bereich der IT-Sicherheit. Dazu zählen unter anderem Risikoanalysen, Sicherheitsüberprüfungen, die Entwicklung von Sicherheitskonzepten, die Unterstützung bei der Einführung technischer Schutzmaßnahmen sowie die Begleitung von Unternehmen im Umgang mit Sicherheitsvorfällen.

Auch präventive Maßnahmen wie Schulungen, Sensibilisierungsprogramme und die laufende Weiterentwicklung bestehender Sicherheitsstrukturen sind Teil des Angebots.
Durch die Bündelung von Fachwissen und Erfahrung stellt die „IT Security Experts Group“ insbesondere für kleine und mittlere Unternehmen eine wertvolle Orientierungshilfe dar. Betriebe erhalten Zugang zu qualifizierten Ansprechpartnerinnen und Ansprechpartnern, die mit den spezifischen Anforderungen unterschiedlicher Branchen vertraut sind und praxisnahe, umsetzbare Lösungen anbieten.

Kontakt: +43 1 51450 3600

[35] vgl. https://www.wko.at/itsecurity

6.4 TV-Sendung „Cyber & More“

In Zusammenarbeit mit der Wirtschaftskammer Wien wurde von Dr. Cornelius Granig der Branchentalk „Cyber & More“ entwickelt, der auf W24 und im R9-Senderverbund ausgestrahlt wird.

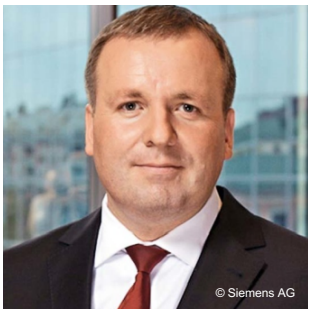
Diese Fernsehsendung beschäftigt sich mit aktuellen Entwicklungen, Risiken und Lösungsansätzen rund um Cybersecurity, Digitalisierung und technologische Innovationen. Im Mittelpunkt stehen dabei praxisnahe Fragestellungen, die Unternehmen, Organisationen und die Gesellschaft insgesamt betreffen.

Thematisch geht es unter anderem um Cyberangriffe, Datenschutz, IT-Sicherheit im Unternehmensalltag, digitale Resilienz sowie um neue Bedrohungen durch Phishing, Ransomware oder Social-Engineering. Gleichzeitig beleuchtet die Sendung auch Chancen der Digitalisierung, etwa den Einsatz von künstlicher Intelligenz, Automatisierung oder moderner IT-Infrastrukturen, und ordnet diese aus sicherheitstechnischer und wirtschaftlicher Perspektive ein.

Ein wesentliches Merkmal von „Cyber & More“ ist der starke Praxisbezug. Expert:innen aus Wirtschaft, IT-Sicherheit, Beratung und Forschung erklären komplexe technische Zusammenhänge verständlich, zeigen reale Fallbeispiele und geben konkrete Handlungsempfehlungen. Dadurch richtet sich die Sendung nicht nur an IT-Fachleute, sondern auch an Entscheidungsträgerinnen und Entscheidungsträger, Unternehmerinnen und Unternehmer sowie an ein breiteres interessiertes Publikum.

„Cyber & More“ versteht sich damit als Informations- und Orientierungsformat, das Bewusstsein für digitale Risiken schafft, Hintergrundwissen vermittelt und aufzeigt, wie Betriebe ihre IT-Sicherheit strukturiert verbessern können, ohne den Blick auf wirtschaftliche und organisatorische Aspekte zu verlieren.

7 Über den Autor



Dr. Cornelius Granig ist ein österreichischer Sicherheitsexperte, Unternehmensberater, Autor und Journalist mit Sitz in Wien.

Er promovierte an der Universität Wien im Fach Politikwissenschaften mit einer interdisziplinären Dissertation über die Entwicklung der Informationsgesellschaft und gilt als einer der profiliertesten Experten im deutschsprachigen Raum für Cybersecurity, Computerkriminalität, strategisches Risiko und Krisenmanagement sowie für Fragen der Compliance, Corporate-Governance und Korruptionsprävention. Seine Arbeit bewegt sich an der Schnittstelle von Technologie, Wirtschaft, Sicherheitspolitik und Gesellschaft.

Dr. Granig ist bei der europäischen Polizeibehörde Europol akkreditiert, beim TÜV als Auditor für ISO 27001 und beim internationalen Branchenverband ISACA im Bereich Cybersecurity zertifiziert (CISM). Seit dem Jahr 2022 leitet er das Universitätsinstitut für Sicherheitsforschung und Krisenmanagement an der SFU in Wien.

Seine berufliche Laufbahn ist geprägt von langjähriger Erfahrung in Vorstandsfunktionen in internationalen Konzernen wie Raiffeisen, Siemens, IBM und der Vienna Insurance Group. Er verfügt dadurch über ein tiefes Verständnis für komplexe Organisationsstrukturen, regulatorische Anforderungen und strategische Entscheidungsprozesse auf Vorstandsebene. Diese internationale Managementerfahrung bildet die Grundlage für seinen analytischen und zugleich praxisorientierten Zugang zu sicherheitsrelevanten Fragestellungen.

Granig betrachtet Cybersecurity nicht nur als technische Disziplin, sondern als Führungsaufgabe, die Organisation, Prozesse, Unternehmenskultur und rechtliche Rahmenbedingungen gleichermaßen umfasst. In seiner Beratungstätigkeit unterstützt er Unternehmen, öffentliche Institutionen und Entscheidungsträger:innen dabei, ihre digitale Resilienz zu stärken, Risiken frühzeitig zu erkennen und wirksame Präventions- und Krisenmanagement-Mechanismen aufzubauen.

Als Autor hat Cornelius Granig in den letzten Jahren mehrere Bücher veröffentlicht, in denen er komplexe und oft schwer zugängliche Themen wie das Darknet, digitale Finanzkriminalität, organisierte Kriminalität im Internet und Machtstrukturen im digitalen Raum für eine breitere Öffentlichkeit verständlich aufbereitet.

Darüber hinaus ist er journalistisch tätig und kommentiert regelmäßig aktuelle Entwicklungen in den Bereichen Sicherheit, Technologie und Politik in nationalen und internationalen Medien und als Cybersecurity-Experte der Kronen Zeitung.

Impressum und Kontakt

Offenlegung nach § 25 Mediengesetz

Fachgruppe Werbung und Marktkommunikation,
Fachgruppe Wien Wirtschaftskammer Wien

Straße der Wiener Wirtschaft 1
1020 Wien | Österreich

Telefon: +43 1 514 50 3512
Telefax: +43 1 514 50 3796

E-Mail: werbungwien@wkw.at
Web: https://www.werbungwien.at/

Tätigkeitsbereich: Interessenvertretung sowie Information, Beratung und Unterstützung der jeweiligen Mitglieder als gesetzliche Interessenvertretung.

Dieser Leitfaden dient lediglich der Erstinformation und kann vor allem eine individuelle rechtliche Beratung nicht ersetzen. Kostenlose Auskünfte erhalten Mitglieder auch bei ihren Wirtschaftskammern in den Bundesländern.

Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr.
Eine Haftung ist ausgeschlossen.