Medienunternehmen im Visier von Cyber-kriminellen

VORBEUGUNG VON UND UMGANG MIT CYBERANGRIFFEN

AUTOREN

Dr. Clemens Birkert
Rechtsanwalt, Assoziierter Partner, OPPENLÄNDER Rechtsanwälte und

David Pfau
Head of Data & Privacy, conreri digital development GmbH

Die Zahl der durchschlagenden Cyberangriffe nimmt kontinuierlich zu. Allein im Jahr 2022 entstand bei deutschen Unternehmen ein geschätzter Schaden in Höhe von 200 Milliarden Euro. Auch der Kreis der Betroffenen vergrößert sich stetig. Cyberkriminelle greifen mittlerweile nicht nur große Weltkonzerne und staatliche Einrichtungen an, sondern zunehmend auch kleine und mittelständische Unternehmen. Auch Medienunternehmen geraten verstärkt ins Visier.

Aufgrund ihrer Vernetzung in verschiedenen Unternehmensbranchen stellen sie ein vielversprechendes Ziel dar. Bei einem Ausfall der technischen Infrastruktur drohen hohe wirtschaftliche Schäden. Aus Sicht der Cyberkriminellen erhöht dies die Chance auf Lösegeldzahlungen, was den Sektor für die Hackerszene besonders attraktiv macht.

Proaktives Tätigwerden erforderlich

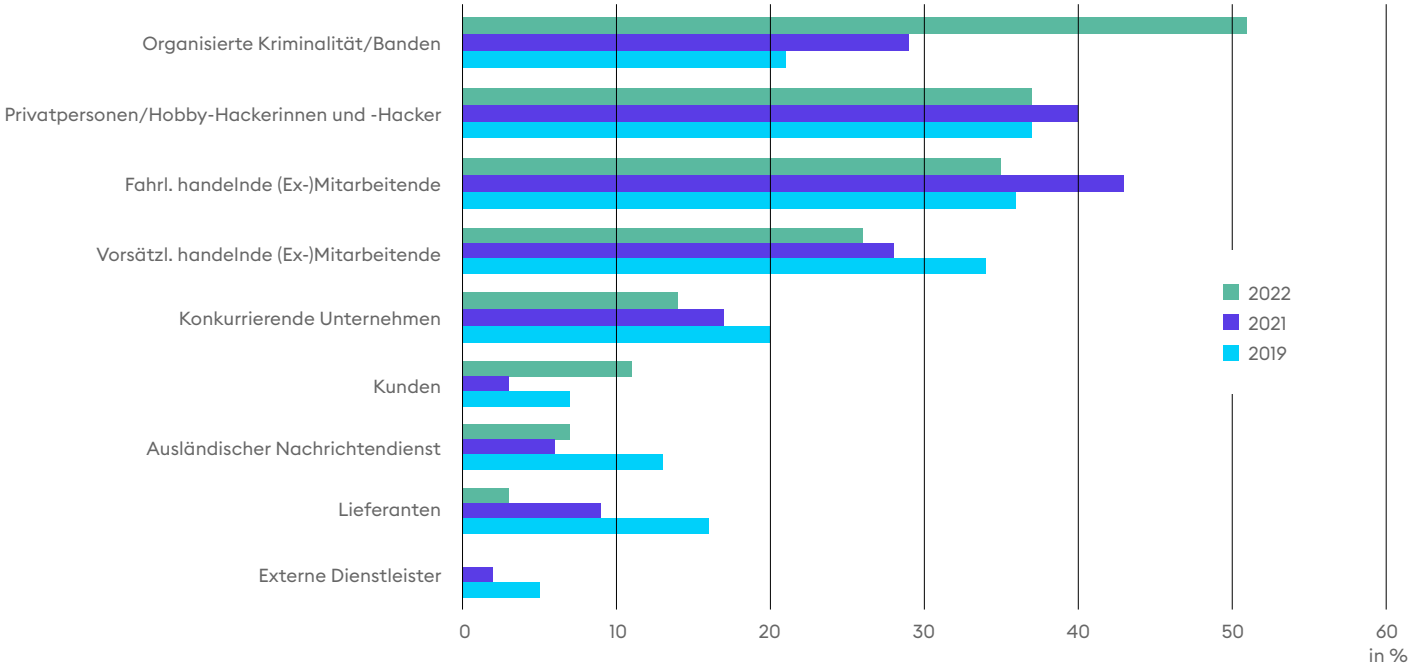
Trotz gesteigerter Sensibilität und – in weiten Teil – deutlich verbesserter Sicherheitsstandards besteht bei nahezu allen Unternehmen Handlungsbedarf. Die Medienbranche ist in besonderem Maße darauf angewiesen, sich proaktiv um die Absicherung ihrer IT-Infrastruktur zu kümmern. Das liegt zum einen an der zunehmenden Konfrontation mit Cyberangriffen. Zum anderen ist der Sektor „Medien und Kultur“ bislang von wichtigen gesetzlichen Cybersicherheits-Regularien unberührt geblieben. Der Sektor unterliegt nicht den gesetzlichen Sicherheitsanforderungen für kritische Infrastruktureinrichtungen, die im **Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)** reguliert sind (vgl. § 2 Abs.10 BSIG). Auch die neue >

> **NIS-2-Richtlinie** der EU ändert daran nichts. Die **Datenschutz-Grundverordnung** sieht zwar gesetzliche Pflichten vor, personenbezogene Daten vor dem Zugriff unberechtigter Dritter zu schützen sowie eine sichere Datenverarbeitung zu gewährleisten (vgl. Art. 32 DSGVO). Die gesetzlichen Pflichten sind jedoch recht abstrakt gehalten; konkrete technische Vorgaben zur Abwehr von Cyberangriffe werden nicht gemacht.

Entwicklungen im Täterkreis

Medienunternehmen sollten sich aber mit konkreten Maßnahmen auf Cyberangriffe vorbereiten. Dabei müssen sie sich auf eine vielschichtige Tätergruppe einstellen. Während in der Vergangenheit häufig **Kleinkriminelle** und **Hobbyhackerinnen und -hacker** aktiv waren, nimmt der Anteil der **organisierten Kriminalität** in den letzten Jahren stark zu, während die Aufklärungsquoten sinken. Das Augenmerk richtet sich dabei verstärkt nach Osten, insbesondere zu Ländern wie Russland und China. Neben dieser Drohkulisse sind auch **unabsichtlich handelnde (Ex-)Mitarbeiterinnen und Mitarbeiter** ein häufiges Einfallstor für Cyberkriminelle. Sie stellten einen erheblichen Risikofaktor für die Cybersicherheit eines Unternehmens dar, welchem insbesondere durch Aufklärung und Schulung der Mitarbeitenden entgegengewirkt werden kann.

VON WELCHEM TÄTIGKEITENKREIS GING HANDLUNG AUS (IN PROZENT)

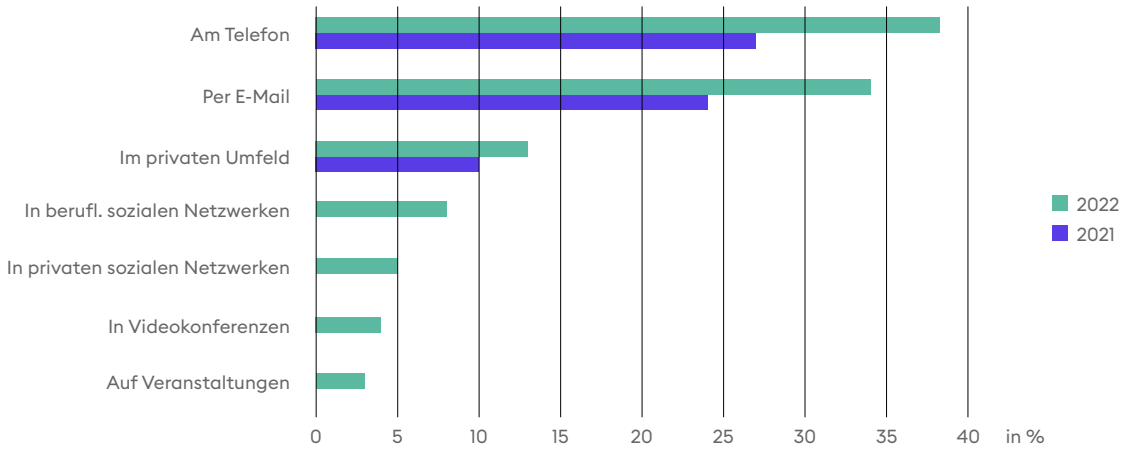


Quelle: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

Phishing und Ransomware

Auch bei den Angriffsmethoden gibt es Trends in der Hackerszene. Eine Vielzahl der Angriffe zielt auf Beschäftigte ab und versucht über diese Zugriff auf geschützte Daten zu erlangen. In den letzten Jahren sind dabei vermehrt Angriffe via Phishing und Ransomware aufgetreten. Beim Phishing versuchen die Angreiferinnen und Angreifer mithilfe gefälschter Kommunikation Zugangsdaten, Passwörter, Bankverbindungen etc. zu erlangen. Meist ist die Kommunikation so gestaltet, dass sie die Neugier der Empfängerinnen und Empfänger wecken, etwaige >

GENUTZE KANÄLE (IN PROZENT)



Quelle: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

> Unachtsamkeit bei Routineanliegen ausnutzen oder durch den Anschein von Dringlichkeit oder Autorität eine Stresssituation auslösen. Dabei werden verschiedene Kontaktmöglichkeiten genutzt, insbesondere E-Mail und Telefon, aber auch SMS und Social Media-Kanäle wie LinkedIn oder Xing.

Häufige Ransomware-E-Mail Betreffe lauten etwa „Agenda morgen", „Passwortüberprüfung sofort", „Gehaltsabrechnung" oder „Bewerbung". Auf den ersten Blick scheinen die E-Mails von einer vertrauten Quelle zu stammen, etwa von Geschäftspartnerinnen und Geschäftspartner. Die Empfängerinnen und Empfänger werden dann meist über einen Link auf eine Webseite weitergeleitet oder in der E-Mail aufgefordert, Informationen einzugeben oder Dokumente herunterzuladen. Hierdurch wird den Cyberkriminellen der Zugriff auf geschützte Daten ermöglicht, um diese einzusehen, zu kopieren, zu löschen, zu veröffentlichen oder zu verschlüsseln. Letzteres geschieht regelmäßig durch den Einsatz sog. Ransomware („Lösegeld-Software"). Hierbei entziehen Angreiferinnen und Angreifer den Betroffenen den Zugriff auf Daten oder ganze Systeme und machen die Zugänglichmachung von der Zahlung eines Geldbetrags abhängig.

Identifikation von Cyberangriffen

Cyberangriffe via Phising und Ransomware können leicht vermieden werden – jedenfalls in der Theorie. Im stressigen Arbeitsalltag sieht dies aber häufig anders aus. Entscheidend ist hier die Sensibilität der Angestellten für das Thema Cyberangriffe. Mitarbeitende sollten es sich zur Gewohnheit machen, verdächtige Nachrichten zu prüfen, bevor sie mit ihnen interagieren. Eingehende Nachrichten sollten einer kritischen Gesamtschau unterzogen werden, wobei Anzeichen wie vage Sachverhaltsdarstellungen, eine fehlende direkte Anrede, Grammatik- und Orthografie-Fehler, Hinweise auf einen dringenden Handlungsbedarf und die Aufforderung zur Eingabe von Daten, Öffnung von Dateien oder Aufruf eines Hyperlinks beachtet werden sollten.

Das BSI empfiehlt folgenden 3-Sekunden-Check bei jeder E-Mail:

- → Ist der Absender bekannt und mit dem wahren Absender identisch?
- → Ist der Betreff und der Text sinnvoll?
- → Wird ein Anhang von diesem Absender erwartet?
- → Bei Auffälligkeiten sollte eine Detailprüfung, ggf. mit Unterstützung der IT-Abteilung, erfolgen. >

> Vorbereitung auf den Ernstfall

Für die Cybersicherheit ist eine umfassende Vorbereitung auf Cyberangriffe von entscheidender Bedeutung. Dabei sind insbesondere folgende Faktoren zu berücksichtigen:

1 Die **Sensibilisierung** der Mitarbeiterinnen und Mitarbeiter für Datenschutz und IT-Sicherheit durch regelmäßige Schulungen ist ein wesentlicher Baustein, um sich vor Angriffen zu schützen. Cloudbasierte Learning-Management-Systeme und Phishing-Simulationen können Teil der Sensibilisierungsstrategie sein.

2 IT-Abteilungen müssen die **notwendigen Ressourcen und Kompetenzen** erhalten, um mit den Entwicklungen der Cyberkriminalität mithalten zu können und im Ernstfall handlungsfähig zu sein. Soweit die entsprechende Kompetenz im Unternehmen nicht vorhanden ist, sollte auf externe Unterstützung zurückgegriffen werden.

3 Die **technische Umgebung** sollte stets auf dem aktuellsten Stand der Technik gehalten werden. Neben aktuellen Virenscannern und Firewalls sollte Software eingesetzt werden, die Anomalien im IT-System erkennt. Zudem sollte eine belastbare Back-up-Strategie vorhanden sein.

4 Zuletzt ist die Etablierung eines **Notfallmanagements** wichtig. Die unternehmensinterne Verantwortung und Rollenverteilung muss in einem >

EXKURS: CYBERANGRIFFE BEI GESCHÄFTSPARTNERN UND -PARTNERINNEN

Auch eingesetzte Dienstleister und verbundene Unternehmen können Opfer von Cyberangriffen werden. Von einem solchen Vorfall kann auch Ihr Unternehmen mittelbar betroffen sein, etwa wenn der Dienstleister in Ihrem Auftrag personenbezogene Daten Ihrer Kundinnen und Kunden oder Beschäftigten verarbeitet. Falls Sie von Geschäftspartnerinnen oder -partnern über einen Cyberangriff informiert werden, sollten Sie daher insbesondere die folgenden Punkte prüfen:

- → Handelt es sich um eine aktive Geschäftsbeziehung?
- → Hat Ihr Unternehmen einen digitalen Zugang zur Firmenumgebung Ihrer Geschäftspartnerinnen und -partner?
- → Haben die Geschäftspartnerinnen und -partner Zugriff auf Ihre Systemumgebung?
- → Sind personenbezogene Daten eigenen Angestellten und/oder Kundinnen und Kunden betroffen?
- → Liegen in Ihrem Unternehmen ungewöhnliche IT-Vorgänge, wie beispielsweise eine Verlangsamung der technischen Prozesse oder hohe Prozessorleistungen vor?

Sollten Sie eine oder mehrere der zuvor genannten Fragen bejaht haben, sollten Sie folgende Maßnahmen im Einzelfall prüfen:

- → Sperrung der Zugänge der Geschäftspartnerinnen oder -partnern auf die eigene Systemwelt;
- → Sperrung Ihres Kontos bei den Geschäftspartnerinnen und -partner;
- → Prüfung der eigenen Betroffenheit in Bezug auf personenbezogene Daten;
- → Prüfung, ob und inwieweit Daten in Ihren internen Systemen gelöscht oder verändert wurden;
- → Prüfung, ob ein ungewöhnlich hoher Datenabfluss in der IT-Infrastruktur stattgefunden hat;
- → Veranlassen Sie einen Scan Ihrer Systeme auf Schadsoftware.

Bitte nehmen Sie bei der Klärung der zuvor genannten Fragestellungen nur per Telefon Kontakt zu Ihren Geschäftspartnerinnen und -partner auf.

> Notfallplan klar geregelt werden. Sollte der Ernstfall eintreten, müssen die verantwortlichen Entscheidungsträgerinnen und Entscheidungsträger wissen, was zu tun ist. Regelungen zum Einsetzen einer Task-Force (mit Geschäftsleitung, IT-Verantwortliche, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, externer Unterstützung), zu alternativen Kommunikationskanälen und zur Kommunikation mit Mitarbeiterinnen und Mitarbeitern, Behörden und Betroffenen sind essentiell, um im Ernstfall richtig und schnell reagieren zu können.

Sofortmaßnahmen bei einem erfolgreichen Cyberangriff

Bei einem Cyberangriff muss schnell reagiert werden. Die betroffene Hard- und Software muss identifiziert, isoliert und soweit möglich die Endgeräte ausgeschaltet werden. Zudem sollte das bereits etablierte Notfallmanagement in die Praxis umgesetzt werden. Dies umfasst insbesondere die Einbindung aller Entscheidungsträgerinnen und Entescheidungstäger. Im Regelfall werden betroffene Unternehmen auch externe Unterstützung durch Forensikerinnen und Forensiker, Versicherungen und sonstige IT-Expertinnen und -Experten angewiesen sein. Da es bei einem Cyberangriff regelmäßig zu einer Verletzung personenbezogener Daten kommt, sollten auch die datenschutzrechtlichen Pflichten nach der Datenschutz-Grundverordnung im Blick behalten werden.

Über eine mögliche Meldung des Vorfalls an die Datenschutzbehörden und ggf. die betroffenen Personen sollte frühzeitig beraten werden. Sämtliche Prozesse und Entscheidungen sind im eigenen Interesse zu dokumentieren – das gilt auch für etwaige Kontrollmaßnahmen. ■

» Unabsichtlich handelnde Mitarbeiterinnen und Mitarbeiter sind ein häufiges Einfallstor für Cyberkriminelle. Diesem Risikofaktor muss insbesondere durch Aufklärung und Schulung der Mitarbeiterinnen und Mitarbeiter entgegengewirkt werden. «