KPMG

Verlagstrends Special

Cybersecurity

Wie sich Verlage auf veränderte Bedrohungslagen einstellen

In Kooperation mit dem

MVFP
Medienverband
der freien Presse

Inhalt

Vorwort

In jüngster Zeit vermehren sich Angriffe auf Websites und Nachrichtenportale bekannter Medienhäuser und verdeutlichen damit die digitale Verletzbarkeit des Sektors. Für Cyberkriminelle ist er ein sehr attraktives Ziel, denn Medienunternehmen haben einen großen Bestand umfangreicher Userdaten, der es ihnen erlaubt, personalisierten Content anzubieten. Hoch ist das Erpressungspotenzial auch beim Diebstahl der Identitätsdaten aus Bereichen wie Politik und Prominenz. Nicht zuletzt eignet sich die Glaubwürdigkeit von Medienmarken außerdem für den Missbrauch durch Fake News und politischer Propaganda.

„Aufgrund einer technischen Störung ist unser Portal derzeit nicht erreichbar", war Mitte Juni 2023 auf einer der 50 meistbesuchten Nachrichten-Websites Deutschlands zu lesen. Grund war ein Cyberangriff auf den hauseigenen IT-Dienstleister. Ein solcher System-ausfall ist für die Branche das Worst-Case-Szenario, weil es ein unverzichtbarer Teil des Geschäftsmodells ist, rund um die Uhr mit allen Services online zu sein.

In den vergangenen Jahren hat sich die Sensitivität der Verlagsbranche gegenüber Cyberrisiken erheblich verstärkt. In unserer Studie „Verlagstrends 2023" war für 75 Prozent der befragten Verlage die Bedrohung der Unternehmenssicherheit ein wichtiger Megatrend.

Gerade in jüngster Zeit hat sich die Bedrohungslage durch die geopolitischen Spannungen weiter verschärft. Es geht mittlerweile nicht nur um Erpressung und Sabotage, sondern auch um den Missbrauch von Medienmarken für Fake News und politische Propaganda. Bei vielen Verlagen steht Cybersicherheit daher weit oben auf der Management-Agenda.

Das Risiko, ein Opfer von Cyberattacken zu werden, beschränkt sich nicht auf große Unternehmen und Verlagsgruppen, sondern betrifft Verlage jeder Größe und Ausrichtung. Häufig werden Angriffe über Bots ausgeführt, die flächendeckend und massenhaft agieren. Der potenzielle Schaden kann auch und gerade für kleine Verlage verheerend sein – etwa wenn durch den Ausfall von IT-Systemen Rechnungen nicht gestellt, Dienstleister nicht bezahlt oder Inhalte nicht produziert werden können.

Cybersecurity ist zudem eine Daueraufgabe. Die Täter entwickeln sich weiter und nutzen modernste Technologien für ihre Angriffe. Entsprechend müssen die Schutzmaßnahmen beständig aktualisiert und erweitert werden. Mit der zunehmenden Verbreitung von künstlicher Intelligenz (KI) bekommt Cybersecurity nochmals eine neue Bedeutung.

Die vorliegende Studie bietet einen Einblick in die gegenwärtige Bedeutung und den Status quo von Cybersecurity im Verlagswesen. Die Umfragedaten unserer Studie bieten wertvolle Erkenntnisse darüber, wie Verlagshäuser ihre digitale Infrastruktur schützen und die Wirksamkeit ihrer Sicherheitsvorkehrungen überwachen. Die Ergebnisse verdeutlichen die aktuelle Bedrohungslage und unterstreichen die Dringlichkeit effektiver Sicherheitsmaßnahmen.

Die Studienergebnisse basieren auf einer Online-Befragung von 118 Verlagen aus Deutschland, die im Herbst 2023 durchgeführt wurde. Unser Dank gilt allen Mitwirkenden und insbesondere den Umfrageteilnehmenden.

Wir wünschen Ihnen eine interessante Lektüre.

Dr. Michael Falk

Partner, Consulting, Cybersecurity
KPMG AG Wirtschaftsprüfungs-gesellschaft

Lutz Drüge

Geschäftsführer Fachvertretung Die Publikumsmedien im Medi-enverband der freien Presse

Prof. Dr. Thomas Hess

Direktor des Instituts für Digi-tales Management und Neue Medien,Ludwig-Maximilians-Universität München

Executive Summary

Cybersecurity hat eine hohe Priorität.
Die Verlage in Deutschland sind sich der neuen Gefahrenlage und ihrer digitalen Verletzlichkeit bewusst. Cybersecurity hat für die Mehrheit der Verlage eine sehr hohe Priorität, was auf die zunehmende Sensibilisierung für digitale Bedrohungen hinweist. Mit der fortschreitenden Digitalisierung und Technologiedurchdringung steigt das Sicherheitsrisiko in der Verlagsbranche. Vor allem große Presseverlage sehen sich erhöhten Risiken ausgesetzt.

Die Verlage sehen sich gut geschützt – trotzdem gibt es Schadensfälle.
Die meisten Verlage sehen sich bei den drei Sicherheitskategorien Prävention, Erkennung und Reaktion gut aufgestellt, aber Angreifer haben häufig einen Technologie- und Know-how-Vorsprung. Tatsächlich sind mehrere Verlage Opfer von Angriffen geworden. Die Hälfte der Verlage hat in den letzten zwölf Monaten mindestens einen Angriff registriert, bei fast 40 Prozent der Angegriffenen war mindestens ein Angriff erfolgreich.

Cyberangriffe haben häufig gravierende Konsequenzen.
Die Auswirkungen erfolgreicher Cyberangriffe sind vielfältig und gravierend. Von den Verlagen, die Opfer krimineller Hacker wurden, berichten 50 Prozent von einer spürbaren Beeinträchtigung ihrer Geschäftstätigkeit. Datenverluste, finanzielle Einbußen und Imageschäden sind die häufigsten Folgen.

Es gibt Handlungsbedarf bei Sicherheitskonzepten und Überwachungssystemen.
Sicherheitskonzepte, Überwachungssysteme und Präventionsmaßnahmen sind zentrale Elemente zur Minimierung der Angriffsrisiken. Immerhin 28 Prozent der befragten Verlage verfügen über ein ausführliches Sicherheitskonzept, weitere 47 Prozent besitzen zumindest ein allgemeines Sicherheitskonzept und 56 Prozent sind mit einem Monitoringsystem ausgestattet, das rund um die Uhr aktiv ist.

Wirksamkeitsprüfungen sind häufig unzureichend.
Die meisten Verlagshäuser setzen auf Partnerschaften und externe Unterstützung, wenn es um Sicherheitschecks und Wirksamkeitsprüfung eingeleiteter Schutzmaßnahmen geht. Allerdings führen nur wenige Verlage GAP-Audits durch, messen den Securitystatus anhand von KPIs oder führen szenariobasierte Tests durch.

Ressourcen und Reifegrad

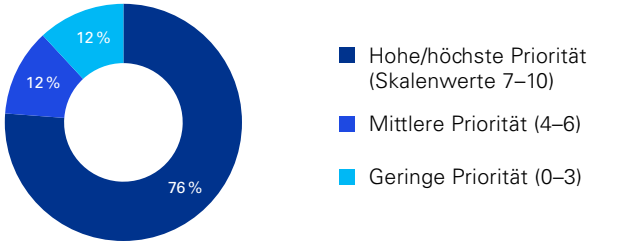
Cybersecurity hat in der Verlagsbranche stark an Bedeutung gewonnen. Für 76 Prozent der Verlage hat das Thema eine hohe Priorität. Etwa 40 Prozent der befragten Verlage haben formale Security-Zuständigkeiten in ihrer Organisation verankert. Der Großteil der Verlage sieht sich gut aufgestellt gegenüber Cyberattacken.

Die zunehmende Bedrohungslage und prominente Schadensfälle in der Medienbranche haben das Thema Cybersicherheit auf die Management-Agenda rücken lassen. Für 76 Prozent der befragten Verlage hat Cybersecurity hohe oder höchste Priorität (vgl. Abb. 1). Entsprechend hoch sind die Investitionen in die IT-Sicherheit: Bei 45 Prozent der Verlage belaufen sich die Ausgaben auf circa einem Prozent des Jahresumsatzes, bei acht Prozent sind es sogar mehr als drei Prozent (vgl. Abb. 2).

43 Prozent der befragten Verlage haben formale Security-Zuständigkeiten in ihrer Organisation verankert. Die Mehrheit der Verlage hat diese Aufgabe informell besetzt, lediglich sechs Prozent verfügen über keine Besetzung (vgl. Abb. 3).

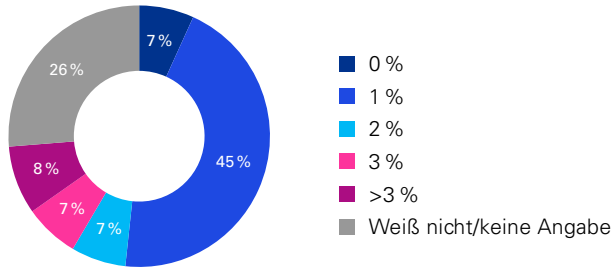
Die häufig fehlende formale Zuständigkeit erklärt sich zum Teil damit, dass der Schutz der Daten und Systeme oftmals an externe IT-Dienstleister übertragen wird. Insbesondere kleine und mittelständische Verlage haben ihre IT-Systeme meist an externe Dienstleister ausgelagert, die zugleich für die Sicherheit der Daten und Systeme zuständig sind. Diese Verlage halten keine eigenen Ressourcen dafür bereit.

Abb. 1: Bedeutung von Cybersecurity
Wie wichtig ist Cybersecurity für Ihr Unternehmen? (n = 118)
Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



Quelle: KPMG in Deutschland, 2024

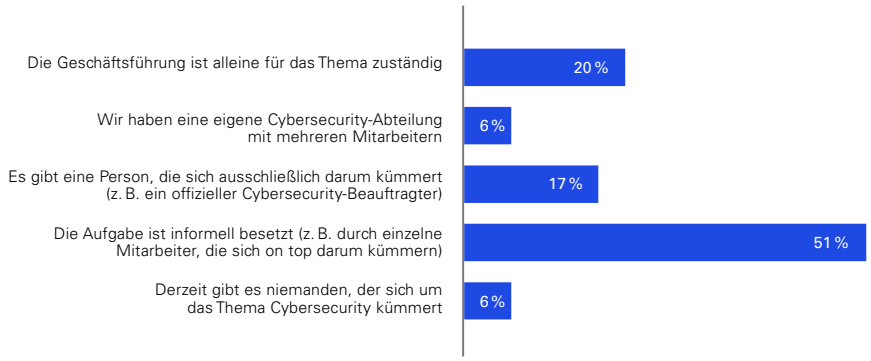
Abb. 2: Cybersecurity-Ausgaben
Wie hoch sind Ihre jährlichen Ausgaben für Cybersicherheit im Verhältnis zum Umsatz (in %)? (n = 118)
Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



Quelle: KPMG in Deutschland, 2024

Allerdings müssen auch die externen IT-Dienstleister kontrolliert und deren Schutzleistungen regelmäßig aktualisiert werden. Auch wenn der Verlag das Thema IT-Sicherheit auslagert, entzieht er sich damit nicht der Verantwortung.

Abb. 3: Cybersecurity-Verantwortlichkeiten
Inwieweit haben Sie dedizierte Cybersecurity-Ressourcen bei sich im Unternehmen? Inwieweit ist in Ihrem Verlagshaus eine Person oder Abteilung für Cybersecurity zuständig? (n = 118)
Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



Quelle: KPMG in Deutschland, 2024

Cybersecurity-Maßnahmen lassen sich in drei Kategorien unterteilen:

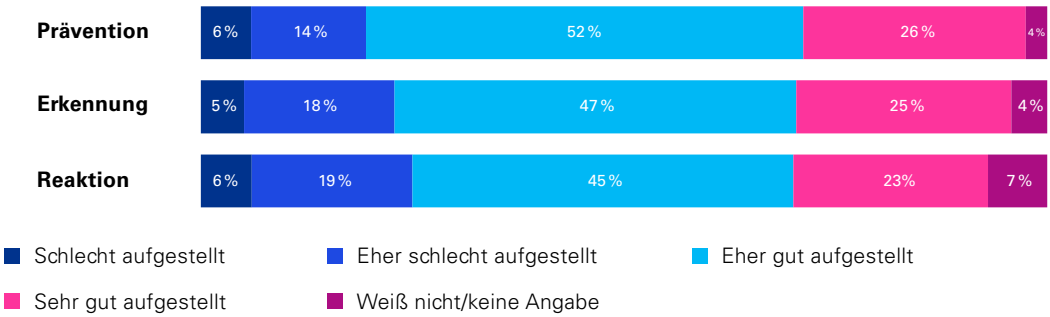
- **Prävention:** Früherkennung von Bedrohungen und Verhinderung von Cyberangriffen sowie von Kompromittierungen der IT-Infrastruktur und der Geschäftsprozesse
- **Erkennung:** Erkennung von Angriffen und von Unregelmäßigkeiten bzw. Anomalien
- **Reaktion:** Abwehr erkannter Cyberangriffe auf die IT-Infrastruktur und Geschäftsprozesse

Viele der befragten Verlage sehen sich also gut geschützt vor externen Angriffen. Im nächsten Kapitel zeigt sich allerdings, dass die Realität oft komplexer ist als angenommen. Tatsächlich wurden im letzten Jahr einige Verlage Opfer krimineller Hackerattacken. Mögliche Ursachen für diese Fehleinschätzung könnten sein, dass Verlage sich auf vorhandene Sicherheitsmaßnahmen verlassen, ohne diese regelmäßig zu aktualisieren oder dass sie mit dem Tempo neu aufkommender Bedrohungen nicht mithalten können.

Abb. 4: Cybersecurity-Reifegrad

Wie gut aufgestellt sehen Sie Ihr Verlagshaus in den folgenden drei Security-Kategorien? (n = 118)

Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



Quelle: KPMG in Deutschland, 2024

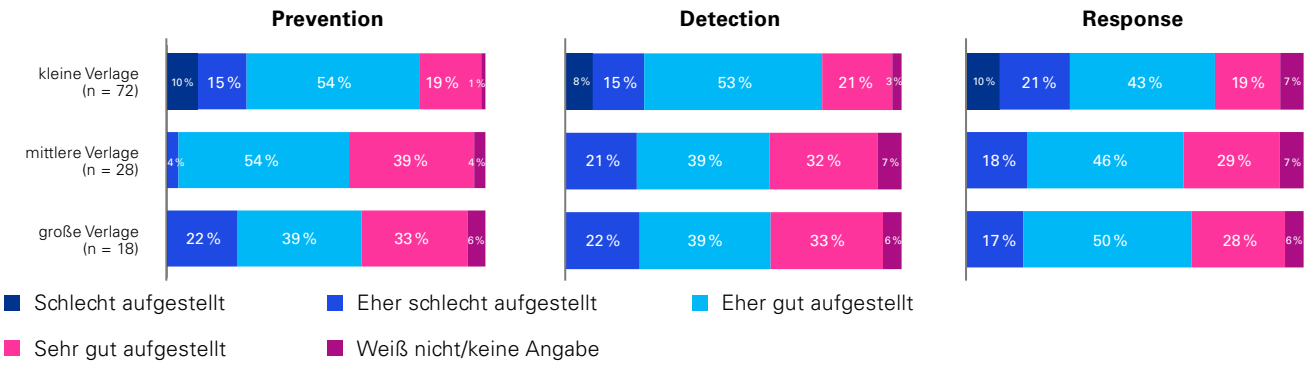
Die große Mehrheit der Verlage (78 Prozent) sieht sich im Bereich der Prävention gut bis sehr gut aufgestellt, lediglich 20 Prozent haben hier nach eigener Einschätzung Handlungsbedarf (vgl. Abb. 4). Ein ähnliches Bild zeigt sich in Bezug auf Erkennung und Reaktion. Auch für diese beiden Kategorien geben die meisten Verlage einen hohen Reifegrad ihrer IT-Sicherheitssysteme an. Die positive Selbsteinschätzung gilt weitestgehend für Verlage aller Größenklassen (vgl. Abb. 5). Selbst kleine Verlage bezeichnen sich mehrheitlich als gut gewappnet vor Cyberattacken.

Zusammenfassend lässt sich sagen, dass die häufig angenommene Sicherheit durch verschiedene Faktoren relativiert wird. Das kann an der fehlenden Aktualisierung von Sicherheitsmaßnahmen, mangelnder Sensibilisierung der Mitarbeitenden und fehlenden Schulungen mit Bezug auf aktuelle Bedrohungen und unentdeckten Schwachstellen liegen. Es ist daher entscheidend, dass Unternehmen ihre Sicherheitsstrategie regelmäßig überprüfen und aktualisieren, um sich effektiv vor den sich ständig verändernden Cyberbedrohungslagen zu schützen.

Abb. 5: Cybersecurity-Reifegrad – Auswertung nach Verlagsgröße*

Wie gut aufgestellt sehen Sie Ihr Verlagshaus in den folgenden drei Security-Kategorien? (n = 118)

Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



Quelle: KPMG in Deutschland, 2024

**Kleine Verlage = bis 49 Mitarbeitende/mittlere Verlage = 50 bis 299 Mitarbeitende/große Verlage = 300 und mehr Mitarbeitende*

Schadensfälle & Konsequenzen

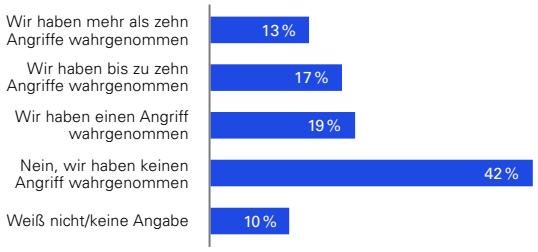
Cyberangriffe sind kein theoretisches Risiko, sondern Teil des Verlagsalltags. Die Hälfte der Verlage hat in den letzten zwölf Monaten mindestens einen Angriff registriert, bei fast 40 Prozent der Angegriffenen war mindestens eine Attacke erfolgreich. Ransomware, Phishing und Datenlecks sind die gängigsten Arten der Cyberangriffe.

Fast 50 Prozent der befragten Verlage haben in den letzten zwölf Monaten mindestens einen Cyberangriff wahrgenommen (vgl. Abb.6). Tatsächlich dürfte die Zahl noch größer sein, denn viele Attacken bleiben unbemerkt. Cyberangriffe sind kein theoretisches Risiko, sondern eine reale Bedrohung.

Angesichts der zunehmenden Komplexität der Bedrohungslandschaft ist es von entscheidender Bedeutung, dass Verlage ihre Cybersicherheitsmaßnahmen kontinuierlich überprüfen, aktualisieren und verbessern, um ihr Geschäft und ihre digitalen Vermögenswerte zu schützen.

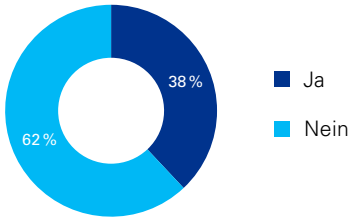
Abb. 6: Anzahl und Erfolgsquote der Cyberangriffe

Wie viele Cyberangriffe gab es in Ihrem Verlagshaus in den letzten zwölf Monaten? (n = 118)
Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



Quelle: KPMG in Deutschland, 2024

War mindestens ein Angriff auf Ihr Unternehmen erfolgreich? (n = 67)
Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



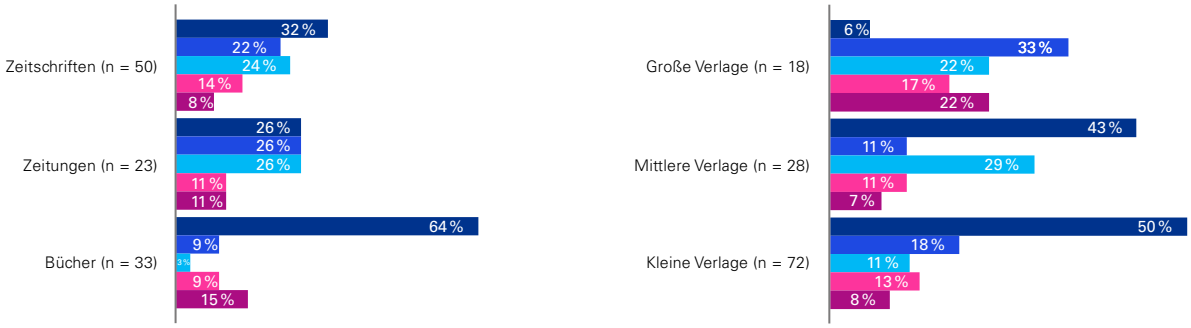
Quelle: KPMG in Deutschland, 2024

Bei nahezu 40 Prozent war mindestens einer der Angriffe erfolgreich – das heißt schadhaft für die Verlage (vgl. Abb. 6). Hier zeigt sich, dass im Bereich der IT-Sicherheit häufig noch Handlungsbedarf besteht. Bei relativ vielen Verlagen sind die Präventionsmaßnahmen ausbaufähig.

Die Ergebnisse nach Verlagsausrichtung und Verlagsgröße zeigen zum einen, dass Zeitungs- und Zeitschriftenverlage deutlich öfter ein Ziel von Cyberangriffen sind als Buchverlage. Zum anderen werden große Unternehmen häufiger attackiert als mittelgroße und kleine Verlage (vgl. Abb. 7). Allerdings sollte auch hier eine Dunkelziffer einkalkuliert werden. Bisweilen werden Angriffe gar nicht bemerkt.

Abb. 7: Anzahl der Cyberangriffe nach Verlagsgröße und -ausrichtung

Wie viele Cyberangriffe gab es in Ihrem Verlagshaus in den letzten zwölf Monaten? (n = 118)
Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



- Nein, wir haben keinen Angriff wahrgenommen
- Ja, wir haben einen Angriff wahrgenommen
- Ja, wir haben bis zu zehn Angriffe wahrgenommen
- Ja, wir haben mehr als zehn Angriffe wahrgenommen
- Weiß nicht/keine Angabe

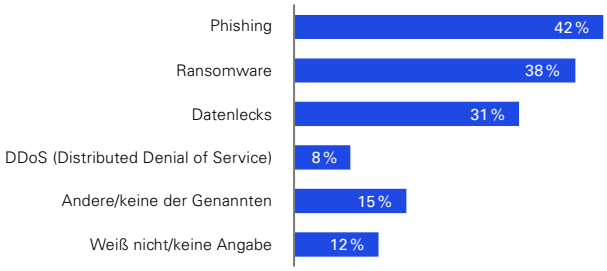
Quelle: KPMG in Deutschland, 2024

Die befragten Verlage, die Opfer von Cyberangriffen wurden, berichten über verschiedene Angriffsarten: Phishing ist die häufigste Form der Hackerattacke (42 Prozent), gefolgt von Ransomware (38 Prozent) und Datenlecks (31 Prozent). Eine vergleichsweise seltene Angriffsform ist Distributed Denial of Service (DDoS).

Die drei Hauptangriffsarten stellen ernste Bedrohungen dar. Dennoch gibt es bewährte Maßnahmen, die das Risiko minimieren: (1) Sensibilisierung der Mitarbeitenden (z. B. Schulungen, interne Awareness-Kampagnen), (2) regelmäßige Back-ups, (3) Aktualisierung von Software, Betriebssystemen und anderen Anwendungen sowie (4) Schutz der IT-Architektur und -Infrastruktur.

Die Auswirkungen erfolgreicher Cyberangriffe sind vielfältig und gravierend. Von den Verlagen, die Opfer von Cyberkriminellen wurden, berichten 50 Prozent von einer spürbaren Beeinträchtigung ihrer Geschäftstätigkeit (vgl. Abb. 9). Bei 23 Prozent kam es zu Datenverlusten und finanziellen Einbußen. Zwölf Prozent erlitten Imageschäden etwa durch Bekanntwerden der Angriffe in der Öffentlichkeit. Außerdem gaben etwa 19 Prozent der Verlage an, dass sie die langanhaltenden Folgen in ihrer Gesamtheit nur schwer abschätzen können. Ursachen für diese Unwissenheit könnten sein: Mangelnde Überwachung und Schadenserkennung oder fehlende Transparenz innerhalb des Verlags.

Abb. 8: Angriffsarten
Welche Arten von Cyberangriffen haben in Ihrem Unternehmen stattgefunden? (n = 26, Verlage, die Opfer von Angriffen wurden)
Mehrfachnennungen möglich

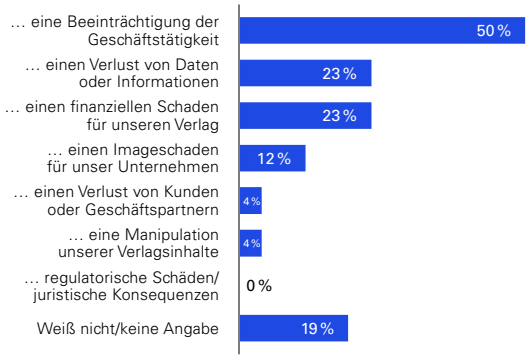


Quelle: KPMG in Deutschland, 2024

Unwissenheit ist gefährlich, denn so können sich die Verlage nicht vor einem möglichen weiteren Angriff schützen. Um vorzubeugen, sollten die Verlage Cybersicherheit zügig zum integralen Bestandteil ihrer Unternehmensstrategie machen. Dabei helfen Fragen, die die potenzielle Fallhöhe durch Attacken eruieren und dem Thema intern Nachdruck verleihen: Wie gehe ich mit einer Ransomware-Attacke inklusive Lösegeldforderung um? Kann ich meine Daten wiederherstellen, ohne dafür bezahlen zu müssen? Wie groß ist der Schaden durch eine Betriebsunterbrechung?

Abb. 9: Auswirkungen der Cyberangriffe
Wie haben sich diese Angriffe auf Ihren Verlag ausgewirkt? (n = 26, Verlage, die Opfer von Angriffen wurden).
Mehrfachnennungen möglich

Durch die Angriffe gab es…



Quelle: KPMG in Deutschland, 2024

Um all diese Herausforderungen zu bewältigen, ist es entscheidend, proaktive Maßnahmen zu ergreifen, wie zum Beispiel regelmäßige Sicherheitsaudits, Penetrationstests, Schulungen für Mitarbeitende, Implementierung von fortschrittlichen und zugleich aktuellen Sicherheitslösungen und eine transparente Kommunikation innerhalb des Verlags sowie mit externen Stakeholdern im Falle eines Cyberangriffs.

Michael Falk
Partner, Consulting,
Cybersecurity bei KPMG
KPMG AG Wirtschaftsprüfungsgesellschaft

Welche Maßnahmen sollten nach einem Cyberangriff umgesetzt werden? Wie kann der Schaden möglichst schnell begrenzt werden?

Die große Mehrheit der befragten Verlage (81 Prozent) hat umgehend eine umfassende Überprüfung ihrer Sicherheitsmaßnahmen durchgeführt und zusätzliche Schutzmechanismen implementiert (vgl. Abb. 10). Hier zeigt sich eine schnelle Reaktionsfähigkeit und ein proaktiver Ansatz, um künftige Angriffe abwehren zu können.

50 Prozent der Verlage haben zusätzliche Schulungsprogramme für ihre Mitarbeitenden eingeführt, um das Bewusstsein für IT-Sicherheit zu stärken. Knapp 40 Prozent der Verlage sind Partnerschaften mit externen Spezialisten eingegangen, um Sicherheitsbewertungen und Empfehlungen zur Verbesserung ihrer IT-Sicherheit zu erhalten. Acht Prozent haben ein spezialisiertes Incident-Response-Team etabliert, um schnell auf künftige Angriffe reagieren zu können.

Es überrascht wenig, dass mittelständische und große Verlage umfangreicher auf Cyberangriffe reagieren können als kleinere Verlage. Cybersicherheit ist ressourcenintensiv und erfordert Fachkompetenz, um geeignete Maßnahmen einleiten zu können.

Etwas überraschend ist dagegen, dass selbst viele Großverlage keine speziellen Sicherheits- bzw. Response-Teams eingerichtet haben, um zukünftigen Angriffen frühzeitig und umfangreich begegnen zu können (vgl. Abb. 10). Ein möglicher Grund dafür könnte sein, dass externe Sicherheitsfirmen auch diese Aufgabe übernehmen.

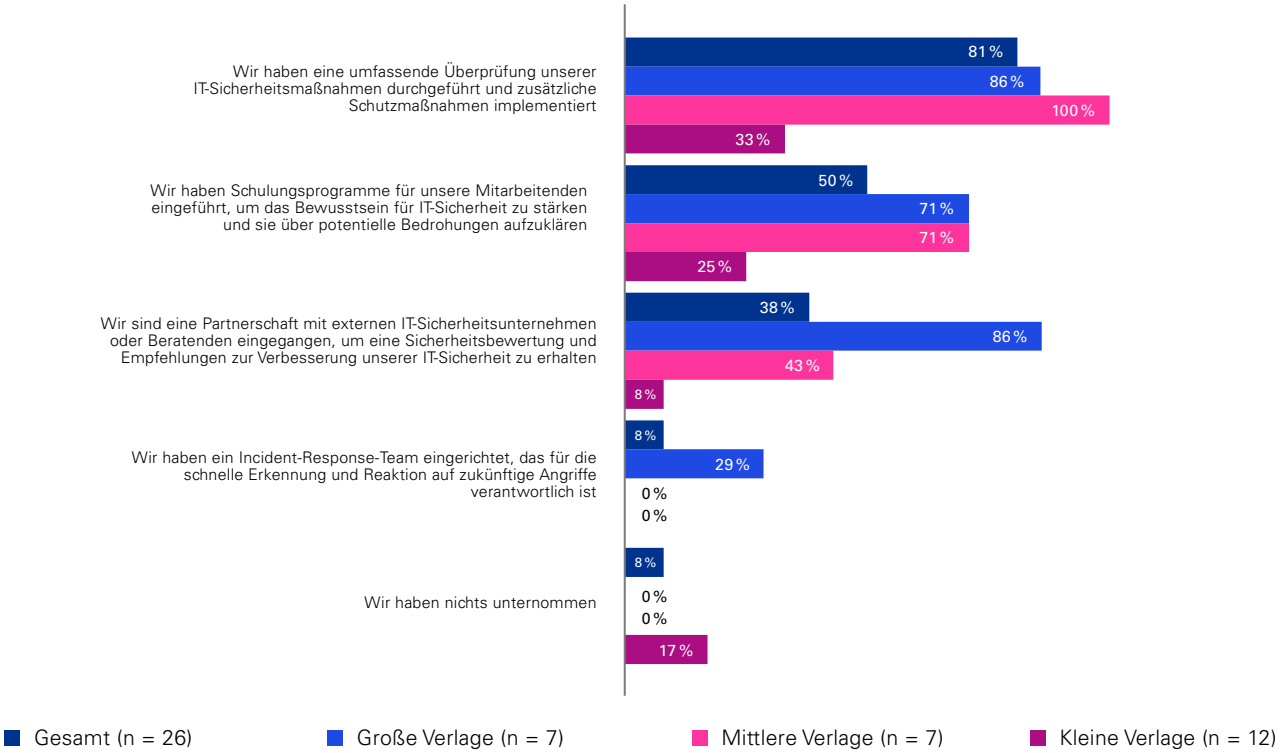
Insgesamt 17 Prozent der kleineren Verlage haben nach einem Cyberangriff nichts unternommen. Das kann fatal sein und schwerwiegende Konsequenzen haben. In solchen Fällen sollten umgehend Schulungsprogramme für Mitarbeitende eingeführt werden, um das Bewusstsein für IT-Sicherheit und für potenzielle Bedrohungen zu schaffen. Diese Maßnahme ist kostengünstig und bedarf wenig Vorbereitung und geringen Aufwand. Sie ist für kleine und große Verlage umsetzbar.

Zusammenfassend lässt sich sagen, dass jede kleine Aktivität besser ist, als gar nichts zu unternehmen. Cybersecurity sollte Management-Priorität haben und bedarf stetiger Maßnahmen.

Abb. 10: Maßnahmen nach einem Angriff

Welche Maßnahmen hat Ihr Unternehmen ergriffen, um die IT-Sicherheit zu verbessern, nachdem ein Cyberangriff stattgefunden hat? (n = 26, Verlage, die Opfer von Angriffen wurden). Mehrfachnennungen möglich.

Mehrfachnennungen möglich



Quelle: KPMG in Deutschland, 2024

Cybersecurity bei der SDZ

Interview mit Jochem Kranz, Chief Digital Officer & Chief Technology Officer, SDZ Mediengruppe

Sehr geehrter Herr Kranz, lassen Sie uns direkt einsteigen. Können Sie uns mehr über die Struktur Ihrer IT erzählen, insbesondere wie die Sicherheitsverantwortlichkeiten organisiert sind?
In der SDZ Mediengruppe ist die IT zentral in einer Tochtergesellschaft organisiert. Im Gegensatz zu anderen Unternehmen, bei denen es eine IT-Abteilung gibt, handelt es sich hier um ein eigenständiges Unternehmen, das für alle Gesellschaften der Gruppe als eigenes Profitcenter agiert. Innerhalb dieser Unit ist das Thema Cybersecurity, und Security allgemein, fest verankert. Cybersecurity ist zwar noch nicht so lange ein großer Begriff, aber Sicherheit im Allgemeinen, vor allem im Zusammenhang mit IT und allen damit verbundenen Komponenten hat schon seit den Anfängen des Internets einen hohen Stellenwert. Das Thema „Netzwerksicherheit“, sowohl intern als auch extern, und der Fokus auf die Absicherung der Clients hat angesichts der zahlreichen Cyberattacken in den letzten Jahren aber sehr stark zugenommen.

> **Der Schutz vor Cyberangriffen ist nicht nur eine technische Angelegenheit, sondern auch eine Frage der Verteidigung unserer demokratischen Prinzipien und der Sicherung unserer kritischen Informationsinfrastruktur.**

Wie wichtig ist Cybersecurity für Ihr Unternehmen, insbesondere in Anbetracht der jüngsten Entwicklungen?
Nun, die Bedeutung von Cybersecurity ist schon lange bekannt. Ich erinnere mich daran, die erste Firewall 1996 in Betrieb genommen zu haben. Damals war bereits klar, dass man das Unternehmensnetzwerk nach außen hin absichern muss. Mit der zunehmenden Vernetzung, insbesondere der Auslagerung von Systemen in die Cloud, dem massiven Change in Richtung des „mobilen Arbeitens“ durch die Coronakrise und die Zunahme der globalen Bedrohungen ist das Thema Cybersecurity in den letzten Jahren aber deutlich stärker in den Fokus gerückt.

Wir hatten vor etwa zehn bis fünfzehn Jahren bereits Angriffe mit Verschlüsselungssoftware, aber damals waren die Angriffe weniger professionell und die Auswirkungen nicht so weitreichend wie heute. Heute kann ein Angriff das gesamte IT-Netzwerk und damit das gesamte Unternehmen lahmlegen.

Wie haben sich diese Entwicklungen auf Ihre Sicherheitsstrategie ausgewirkt?
Die steigende Qualität der Angriffe erfordert eine bessere Vorbereitung. Die alten Low-Budget-Ansätze in der IT sind nicht mehr umsetzbar, wie es früher der Fall war. Wir müssen uns jetzt besser aufstellen, und das betrifft nicht nur die Technologie, sondern auch die Ressourcen und Investitionen, die in die Sicherheit fließen.

Wie haben sich Ihre Ressourcen und Sicherheitsmaßnahmen in den letzten Jahren entwickelt?
Es gab immer ein gewisses Sicherheitsniveau, aber in den letzten zwei Jahren haben wir definitiv in den Bereich der 24/7-Überwachung investiert. Früher war das nicht so stark im Fokus, aber wir haben erkannt, dass Cyberangriffe primär außerhalb der üblichen Arbeitszeiten stattfinden. Daher haben wir unsere Reaktionszeit verbessert und sind nun zu jeder Tages- und Nachtzeit einsatzbereit. Die schnelle Reaktionszeit „rund um die Uhr“ ist die notwendige Voraussetzung zur erfolgreichen Bekämpfung von Cyberangriffen. Wir setzen jetzt in erster Linie auf eine ausgereifte Endpoint-Überwachung unserer Clients. Wenn auf einem Endgerät eine Anomalie festgestellt wird, kann unser Security-Operation-Dienstleister den Client direkt nach der Angriffserkennung isolieren, das heißt „vom Netz nehmen“. Sind Server betroffen, können diese nach Rücksprache und Bewertung der Dringlichkeit ebenfalls temporär isoliert werden.

Können Sie uns von einem konkreten Vorfall berichten, der zu einer verstärkten Überwachung geführt hat?
Bei einem früheren Vorfall haben wir erst morgens um 6 Uhr etwas bemerkt, als es bereits zu spät war. Die Früherkennung ist entscheidend, um proaktiv auf Bedrohungen zu reagieren und Schäden verhindern zu können.

Lassen Sie uns einen Blick auf die letzten zwölf Monate werfen. Wie viele Cyberangriffe gab es in diesem Zeitraum auf Ihr Unternehmen?
Ja, gerne. Tatsächlich hatten wir in den letzten zwölf Monaten keine nennenswerten Angriffe. Allerdings gab es immer wieder auch interne Vorfälle. So haben unsere Entwicklerinnen und Entwickler weiterhin lokale Adminrechte und laden gelegentlich Software herunter, die unseren Überwachungssystemen auffällt. Auch das Arbeiten mit Tools wie Portscannern ist Teil ihrer Entwicklungsarbeit und löst ab und an noch einen falsch-positiven Alarm aus. In den letzten zwölf Monaten gab es ca. zwei Dutzend Fehlalarme, aber es ist immer besser, auf Nummer sicher zu gehen.

Können Sie uns von einem konkreten Vorfall berichten?
Wir hatten einen Fall, bei dem ein Mitarbeiter auf einen gefälschten Chrome-Aktualisierungsbanner klickte, obwohl wir Updates ausschließlich über unsere automatische Softwareverteilung durchführen. Innerhalb von 15 Minuten haben wir reagiert und den betroffenen Client isoliert. Der Mitarbeiter erhielt dann sofort ein neues Endgerät.

Könnten Sie uns mehr über die Arten von Angriffen berichten, die Sie beobachtet haben?
Über die Jahre hinweg haben wir festgestellt, die größten Sicherheitsrisikofaktoren die Mitarbeitenden selbst sind. Die Netzwerke selbst sind recht gut geschützt, aber unbeabsichtigte Handlungen wie das Öffnen von Links oder Anlagen in E-Mails sind ein großes Sicherheitsrisiko. Das Bewusstsein der Mitarbeitenden und Maßnahmen zur Sensibilisierung sind daher von hoher Bedeutung. Natürlich gibt es auch klassische Denial-of-Service-Angriffe, aber diese führen nicht direkt zu einem Eindringen in die Systeme.

> **Der Kampf findet ja längst nicht mehr nur mit schweren Waffen statt, sondern in Zeiten von Fake News findet er natürlich auch indirekt und sehr subtil statt.**

Lassen Sie uns genauer auf die Auswirkungen der Cyberangriffe auf Ihren Verlag eingehen. Sie erwähnten einen erfolgreichen Vorfall. Wie hat sich dieser spezielle Angriff ausgewirkt?
Ja, dieser Angriff hatte definitiv Auswirkungen. Zu der Zeit hatten wir noch keine Früherkennungssysteme implementiert. Die Auswirkungen waren erheblich – eine Vielzahl unserer virtuellen Server war verschlüsselt und Daten wurden abgezogen – eine klassische Ransomeware-Attacke. Glücklicherweise hatten wir eine sehr gute Back-up-Policy, die uns half, den Angriff ohne gravierende Produktionsstopps zu überstehen.

Welche Maßnahmen haben Sie nach dem Vorfall umgesetzt?
Wir haben verschiedene Maßnahmen ergriffen, darunter die Auslagerung zentraler Produktionssysteme im Sinne einer Risikoverteilung in die Hersteller-Cloud, den Aufbau einer dedizierten Netzwerksegmentierung, die Anschaffung einer neuen, leistungsfähigeren Firewall, die Minimierung von Adminrechten und die konsequente Implementierung von Multifaktorauthentifizierungen (MFA) für externe Zugriffe auf unser Netzwerk. Der Zugriff auf unsere Cloudsysteme wurde auf unser Netzwerk beschränkt. Zudem haben wir alle Desktop-PCs zugunsten von Laptops ausgetauscht und Software wird nun ausschließlich zentral über unsere Softwareverteilung organisiert. Außerdem haben wir Gästezugriffbeschränkungen mit einer zeitlichen Begrenzung eingeführt. Glücklicherweise konnten wir die Auslagerung der „On-Premises"- Systeme in die Cloud relativ reibungslos gestalten.

Welche generellen Erkenntnisse haben Sie aus diesem Vorfall gewonnen, die Sie anderen Medienhäusern empfehlen würden?
Die Früherkennung durch eine 24/7-Überwachung ist von größter Bedeutung und die Nutzung von Cloudressourcen zur Risikoverteilung ist ratsam. Außerdem sollten Sicherheitsvorkehrungen wie MFA für Netzwerkzugriffe konsequent implementiert oder sogar verpflichtend werden.

Abschließend würden wir gerne erfahren, warum Cybersecurity speziell für Medienunternehmen von grundlegender Bedeutung ist.
Wir gehören zur kritischen Infrastruktur, da wir eine wichtige Rolle im Pluralismus und der Informationsvermittlung inne haben. Medienhäuser, vor allem kleinere, stehen hier im Fokus von Cyberangriffen, da sie als potenzielle Schwachstellen gelten. Der präventive Schutz vor Angriffen – systemisch und verhaltenstechnisch, sowie eine robuste Back-up-Policy sind die entscheidenden „Waffen" für eine erfolgreiche Abwehr von Cyberangriffen.

Jochem Kranz
CDO & CTO,
SDZ Mediengruppe

Die 7 Basics für mehr Unternehmenssicherheit

01

Hausaufgaben erledigen
Mehr als 75% aller erfolgreichen Angriffe sind auf die Nichterfüllung grundlegender Kontrollen zurückzuführen. Daher sollten Unternehmen stets die neusten Systemupdates installieren und ihre Systeme entsprechend vor Angriffen schützen.

02

Kronjuwelen priorisieren
Für jedes Unternehmen ist es essenziell, seine Assets zu kennen, da sich Unbekanntes schwer schützen lasst. Da Ausgaben oftmals priorisiert werden müssen, ist es unabdingbar, die wirklich kritischen Assets zu kennen, um diesen ein besonderes Schutzniveau zu gewährleisten.

03

Angriffsvektoren kennen
Eine zentrale Überlegung, die Unternehmen anstellen sollten, ist die Frage nach den Angriffsszenarien: wer, warum und wie könnte sie angreifen. So können die wahrscheinlichsten Angriffsvektoren vorhergesehen und die Assets, die am ehesten angegriffen werden, geschützt werden.

04

Lieferkette schützen
Trotz der Herausforderungen konkurrierender Prioritäten sollte die Sicherheit von Lieferanten und Geschäftspartnern kein Hemmnis sein, sondern das Geschäft voranbringen. Angreifer wissen, dass das schwächste Glied in der Kette oftmals das Einfallstor für einen erfolgreichen Cyberangriff ist.

05

Vertrauen stärken
Angesichts zunehmender Cyberbedrohungen sollten Sicherheitsverantwortliche eng mit anderen Bereichen im gesamten Unternehmen sowie mit Kunden und Lieferanten zusammenarbeiten, um das Vertrauen und die Unterstützung bei (potenziellen) Vorfällen zu gewährleisten.

06

Kultur schaffen
Unternehmen sollten Cybersicherheit eine entsprechend hohe Bedeutung zuteilen, für Awareness sorgen und eine entsprechende Kultur im gesamten Unternehmen schaffen, um sicherzustellen, dass alle Mitarbeitenden an einem Strang ziehen.

07

Chance nutzen
Erfolgreiche Cyberangriffe können hohe finanzielle Schäden verursachen und die Reputation gefährden. Unternehmen sollten daher Cybersicherheit als eine Chance wahrnehmen, um nachhaltig wettbewerbsfähig zu sein und die Unternehmensziele zu erreichen.

Monitoring & Maßnahmen

Sicherheitskonzepte, Überwachungssysteme und Präventionsmaßnahmen sind zentrale Elemente zur Minimierung von Angriffsrisiken und Schadensfällen. Insgesamt 28 Prozent der Verlage können ein ausführliches Konzept für Cybersicherheit vorweisen. Mehr als die Hälfte der Befragten verfügen über ein Monitoringsystem, das im Falle eines Angriffs Alarm schlägt.

Hinsichtlich der Überwachsungssysteme zeigt sich ein geteiltes Bild. Mehr als die Hälfte der befragten Verlage (56 Prozent) verfügt über ein rund um die Uhr arbeitendes Monitoringsystem für kritische IT-Infrastrukturen und Daten. Lediglich ein Drittel der befragten Verlage verfügt über kein Monitoringsystem (vgl. Abb. 11). Besonders groß ist das Defizit bei den kleinen Verlagen und im Buchsegment.

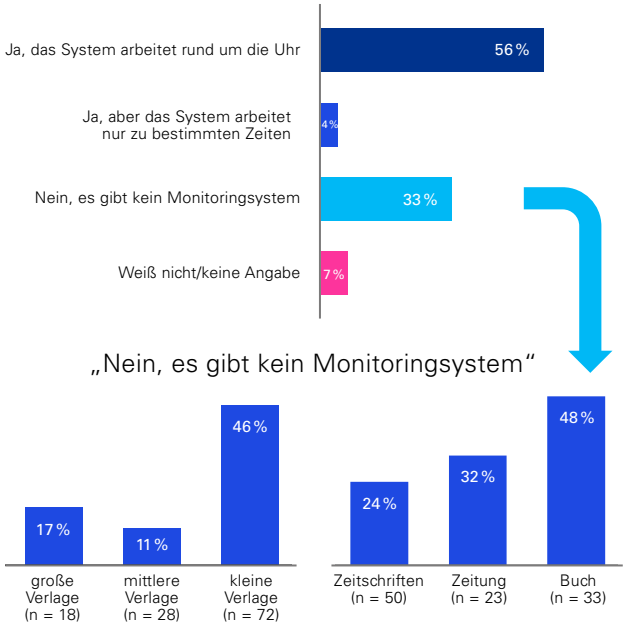
Ein ähnliches Bild ergibt sich im Hinblick auf spezifische Sicherheitskonzepte. Insgesamt 28 Prozent der Verlagshäuser haben ausführliche Schutzkonzepte mit spezifischen Cybersecurity-Anforderungen für verschiedene Anwendungsfälle entwickelt. 47 Prozent verfügen noch nicht über ein solches Sicherheitskonzept, erarbeiten aber gegenwärtig maßgeschneiderte Sicherheitslösungen. (vgl. Abb. 12).

Auch bei dem Reifegrad der Sicherheitskonzepte zeigen sich Unterschiede nach Verlagsgröße: 85 Prozent der mittelständischen und großen Verlage und lediglich 18 Prozent der kleineren Verlage verfügen über ausführliche Sicherheitskonzepte (vgl. Abb. 12).

Abb. 11: Monitoringsystem

Verfügt Ihr Verlagshaus über ein Monitoringsystem für kritische Systeme und Daten, das im Falle eines Angriffs Alarm schlägt? (n = 118)

Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.

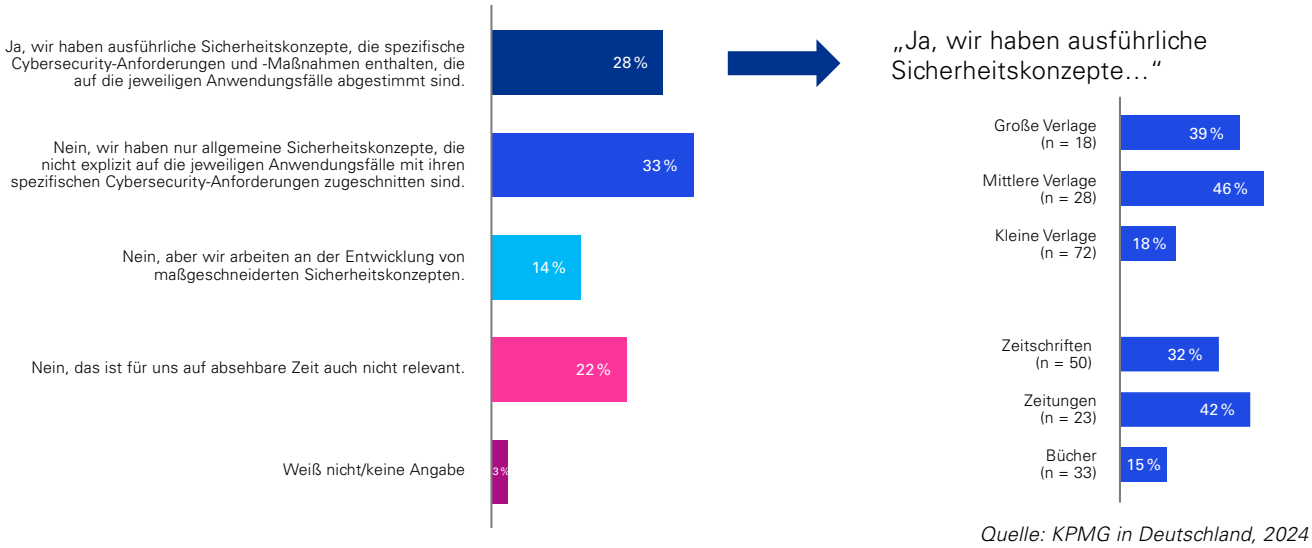


Quelle: KPMG in Deutschland, 2024

Abb. 12: Spezifische Sicherheitskonzepte

Verfügt Ihr Verlagshaus über spezifische Sicherheitskonzepte mit definierten Cybersecurity-Anforderungen für verschiedene Anwendungsfälle bzw. Angriffsszenarien? (n = 118)

Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



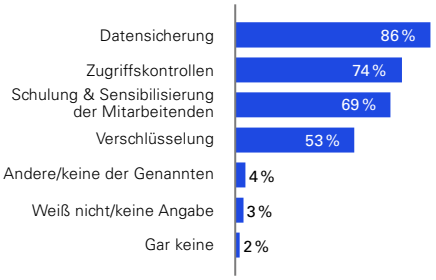
Quelle: KPMG in Deutschland, 2024

Zum Schutz sensibler Daten haben bereits viele Verlage verschiedene Sicherheitsmaßnahmen getroffen (vgl. Abb. 13a). Datensicherung (86 Prozent), Zugriffskontrollen (74 Prozent) und Schulungen zur Sensibilisierung der Mitarbeitenden (69 Prozent) sind dabei besonders weit verbreitet. Dies unterstreicht das Bewusstsein für den Schutz sensibler und vertraulicher Informationen in der Branche.

Hinsichtlich der Sicherheitsvorkehrungen gibt es kaum signifikante Unterschiede nach Verlagsgröße. Allerdings haben nur 57 Prozent der kleinen Verlage Schulungen implementiert, bei den mittleren und großen sind es jeweils fast 90 Prozent. Ein Blick auf die Verlagsausrichtung zeigt deutlichere Abweichungen: Zeitungsverlage sind grundsätzlich aktiver bei den Sicherheitsvorkehrungen als Zeitschriftenverlage, die wiederum wesentlich mehr Schutzmaßnahmen umsetzen als Buchverlage. (vgl. Abb. 11 und 12). Für die Wirksamkeitsprüfungen eingeleiteter Schutzvorkehrungen ziehen 62 Prozent der Verlage externe Dienstleister zur Unterstützung heran (vgl. Abb. 14). Handlungsbedarf besteht weiterhin: 25 Prozent der befragten Verlage führen regelmäßig ein Pentesting durch, 15 Prozent lassen ein GAP-Audit vornehmen und elf Prozent messen den Security-Status anhand von KPIs. Lediglich neun Prozent führen szenariobasierte Tests durch.

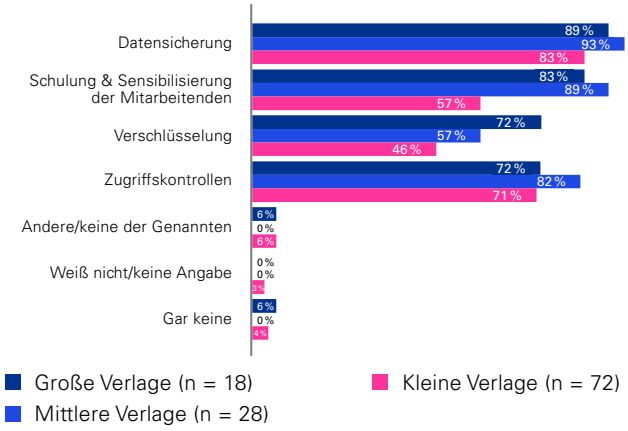
Basierend auf den Ergebnissen wird schnell ersichtlich, wo die Defizite liegen und welche Lücken die Verlage kurzfristig schließen sollten. Handlungsbedarf herrscht in den Bereichen Sensibilisierung und Schulungen der Mitarbeitenden, aber auch im systematischen Monitoring. Nur elf Prozent der befragten Verlage messen ihren Cybersecurity-Status regelmäßig anhand von KPIs. Obwohl Datensicherung und Zugriffskontrollen weit verbreitet sind, gibt es noch andere Sicherheitsmaßnahmen, die von Verlagen nicht ausreichend berücksichtigt werden, wie die Verschlüsselung von Daten oder die regelmäßige Überprüfung von Zugriffsrechten.

Abb. 13a: Sicherheitsvorkehrungen für sensible Daten
Welche Sicherheitsvorkehrungen hat Ihr Verlag getroffen, um sensible Daten (z. B. personenbezogene Daten, journalistische Quellen) zu schützen? (n = 118)
Mehrfachnennungen möglich



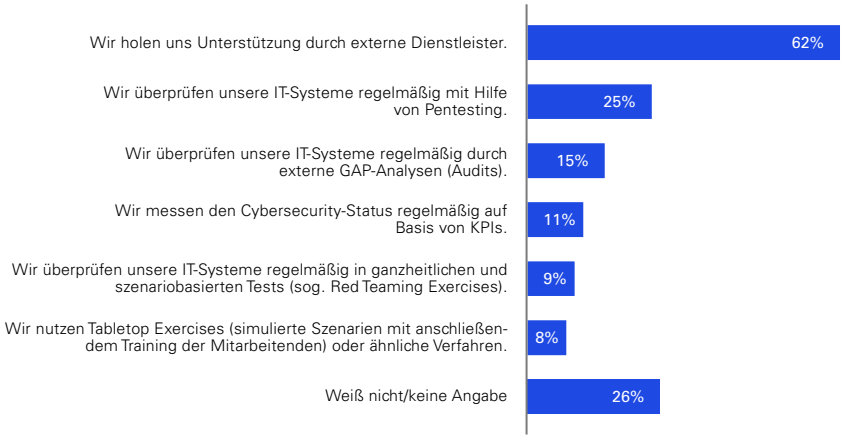
Quelle: KPMG in Deutschland, 2024

Abb. 13b: Sicherheitsvorkehrungen für sensible Daten nach Verlagsgröße
Mehrfachnennungen möglich



Quelle: KPMG in Deutschland, 2024

Abb. 14: Prüfung der Wirksamkeit von IT-Sicherheitsmaßnahmen
Wie überprüfen Sie in Ihrem Verlag die Wirksamkeit Ihrer IT-Sicherheitsmaßnahmen? (n = 118)
Mehrfachnennungen möglich



Quelle: KPMG in Deutschland, 2024

Ausblick

Mit der zunehmenden Digitalisierung und Technologiedurchdringung steigt das Sicherheitsrisiko in der Verlagsbranche. In den nächsten Jahren werden Häufigkeit und Intensität von Cyberangriffen zunehmen. Verlage sollten sich auf die steigende Gefahrenlage frühzeitig einstellen und proaktiv ein weitreichendes Sicherheitskonzept zum Schutz ihrer Systeme, Prozesse, Daten und Contentangebote entwickeln.

Die Umfrageergebnisse dieser Studie verdeutlichen die Dringlichkeit, sich auf eine sich verändernde Bedrohungslandschaft vorzubereiten und entsprechende Sicherheitslösungen zu implementieren, um die Funktionsfähigkeit der digitalen Infrastrukturen und Geschäftsprozesse zu gewährleisten. Die Gründe für den Risikoanstieg sind vielfältig. Polarisierung und geopolitische Spannungen sind dabei ein wichtiger Faktor: Gelingt es kriminellen Hackern, über Fakeprofile auf zentralen Informationsinstanzen Falschinformationen zu verbreiten, werden Newsportale zu Multiplikatoren von Desinformation und Fake News.

Der Großteil der Verlage hat die Gefahrenlage erkannt und prognostiziert für die nächsten zwei bis drei Jahre eine zunehmende Intensität von Cyberattacken: 65 Prozent der Befragten sehen ihr Verlagshaus verstärkt als Ziel von Cyberangriffen. Die zunehmende Bedrohung gilt für Verlage jeder Größe und Ausrichtung (vgl. Abb. 15).

Diese Einschätzung zeigt die steigende Sensibilität der Verlage für die Notwendigkeit vielschichtiger und robuster Sicherheitsmaßnahmen. Mit steigender Digitalisierung, Technologiedurchdringung und Datennutzung nehmen auch die vielschichtigen Sicherheitsrisiken in der Verlagsbranche zu.

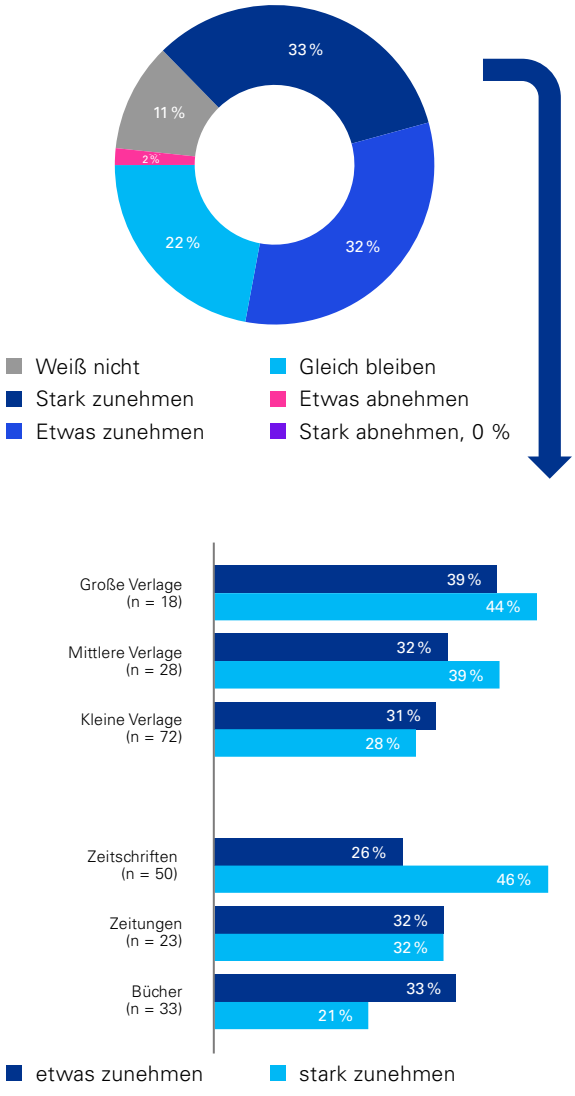
> „Digitalisierung, künstliche Intelligenz, geopolitische Spannungen – Cybersicherheit ist ein zentrales Thema, wenn es um den Schutz von sensiblen Daten, Geschäftsmodellen und Dienstleistungen geht. Nicht zuletzt wird das ‚Superwahljahr 2024' die Dringlichkeit eines umfassenden Schutzes vor Bedrohungen aus dem digitalen Raum einmal mehr unterstreichen. Gerade Presseverlage sind einer erhöhten Gefahr ausgesetzt, da sie als wichtige Informationsvermittler und Vertrauensanker eine besondere Verantwortung in unserer Gesellschaft tragen. Dabei geht es oft nicht nur um Erpressung oder Sabotage, sondern auch um den Missbrauch von Medienmarken zur Verbreitung von Desinformation und politischer Propaganda.
> Um dieser Herausforderung wirkungsvoll begegnen zu können, sind intensive und stets weiterentwickelte Maßnahmen in den drei Bereichen Prävention, Erkennung und Reaktion sowie die kontinuierliche Aus- und Weiterbildung der Mitarbeiterinnen und Mitarbeiter im Bereich der Cybersicherheit für die Pressebranche in Zukunft unerlässlich."
>
> **Lutz Drüge**
> Geschäftsführer Fachvertretung
> Die Publikumsmedien im MVFP

Verlage sollten daher verstärkt Schulungen zur Sensibilisierung der Mitarbeitenden implementieren, um das Bewusstsein für den Schutz sensibler und vertraulicher Informationen weiter zu erhöhen. Zudem sollten Verlage ihre Wirksamkeitsprüfungen verbessern, indem sie GAP-Audits vornehmen, den Security-Status anhand von KPIs messen oder szenariobasierte Tests durchführen, um sicherzustellen, dass ihre Schutzvorkehrungen effektiv sind.

Abb. 15: Einschätzung der Entwicklung von Cyberangriffen in den nächsten zwei bis drei Jahren

Wie schätzen Sie die Entwicklung von Cyberangriffen in den nächsten zwei bis drei Jahren auf Ihr Verlagshaus insgesamt ein? (n = 118)

Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



Quelle: KPMG in Deutschland, 2024

Handlungsempfehlungen

Proaktiv und frühzeitig agieren, ganzheitliche Schutzmechanismen schaffen
Mit der zunehmenden Digitalisierung steigt das Sicherheitsrisiko. Verlage sollten sich auf die steigende Gefahrenlage frühzeitig einstellen und proaktiv ein weitreichendes Sicherheitskonzept zum Schutz ihrer Systeme, Prozesse, Daten und Contentangebote entwickeln. Ein proaktiver Ansatz, der Präventions-, Erkennungs- und Reaktionsmechanismen integriert, wird immer wichtiger, um den ständig neuen Herausforderungen der Cybersicherheit erfolgreich zu begegnen.

Ressourcen bereitstellen, Sicherheit organisatorisch verankern
Schadensfälle können teuer werden. Investitionen in die Cybersicherheit sind notwendig und im Falle eines Angriffs zahlen sich diese aus. Verlage sollten ausreichend Ressourcen für den Schutz der Daten und Systeme bereitstellen und klare Zuständigkeiten in der Organisationsstruktur schaffen (z. B. einen Sicherheitsbeauftragten oder ein Incident-Response-Team). Die Auslagerung der IT-Sicherheit an externe Fachkräfte kann eine gute Lösung sein, wenn eigene Ressourcen und Kompetenzen fehlen.

Frühwarnsysteme implementieren
Die Überwachung von Netzwerken und Systemen sollte automatisiert werden, um Echtzeitdaten zu sammeln und verdächtige Aktivitäten zu identifizieren. Klare und eindeutige Alarmierungsprozesse sollten im Unternehmen implementiert werden.

Cyberspezifische Sicherheitskonzepte einrichten, Wirksamkeit prüfen
Die neuen Gefahrenlagen erfordern Sicherheitskonzepte, die spezifische Anforderungen für die verschiedenen Angriffsfälle berücksichtigen. Die Schutzmaßnahmen müssen mit verschiedenen Maßnahmen auf ihre Wirksamkeit überprüft werden. Durch regelmäßige Tests können Schwachstellen frühzeitig erkannt und behoben werden.

Identitäten und Accounts schützen, Datenabfluss verhindern
Eine der größten Gefahren für die Kompromittierung von IT-Systemen geht von falschen digitalen Identitäten aus. Funktionierendes Zugangsmanagement ist deshalb von großer Bedeutung – zum Beispiel durch Multifaktorauthentifizierung. Verlage sollten zudem in der Lage sein, sich effektiv vor Datendiebstahl zu schützen. Entdeckte Leaks müssen schnellstmöglich geschlossen werden.

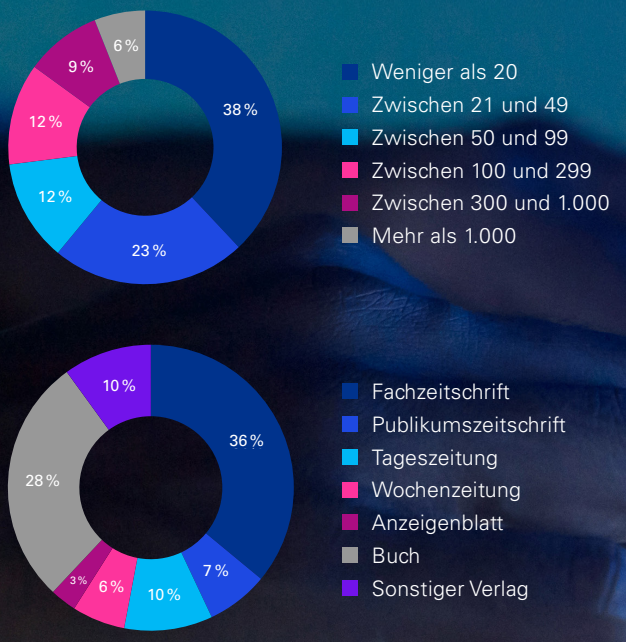
Fortlaufende Anpassung an aktuelle Bedrohungen
Cyberbedrohungen entwickeln sich ständig weiter. Daher sollten Verlagshäuser ihre Sicherheitsstrategien kontinuierlich an neue Bedrohungsszenarien anpassen. Dies erfordert regelmäßige Schulungen, enge Zusammenarbeit mit IT-Fachleuten und die Teilnahme an Fachveranstaltungen, um aktuelle Entwicklungen zu verfolgen.

Methodik

Unterstützt durch den Medienverband der freien Presse (MVFP) wurden im Herbst 2023 insgesamt 118 deutsche Verlage unterschiedlicher Größe und Ausrichtung befragt. Knapp die Hälfte der befragten Verlage (43 Prozent) hat ihren Schwerpunkt in den Segmenten der Fach- und Publikumszeitschriften (Abb. 16). Insgesamt 38 Prozent der befragten Unternehmen haben weniger als 20 Beschäftigte.

Die Befragten haben größtenteils Managementverantwortung: Insgesamt 51 Prozent haben die Geschäftsführung inne, 30 Prozent sind in einer leitenden Funktion im Bereich IT tätig oder arbeiten als Cybersecurity-Beauftragte. Weitere 15 Prozent sind in einer anderen Leitungsfunktion beschäftigt. Die Konzeption der Onlinebefragung und die statistische Auswertung wurden in Zusammenarbeit mit **Prof. Dr. Thomas Hess** und **Dr. Antonia Meythaler** durchgeführt.

Abb. 16: Stichprobenstruktur
Nach Größe und Ausrichtung (n = 118)
Abweichungen von 100 Prozent sind aufgrund von Rundungsdifferenzen möglich.



Quelle: KPMG in Deutschland, 2024

Über KPMG
KPMG ist eine Organisation unabhängiger Mitgliedsfirmen mit mehr als 273.000 Mitarbeitenden in 143 Ländern und Territorien. Auch in Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen und ist mit über 14.000 Mitarbeitenden an 27 Standorten präsent.

Für wesentliche Branchen unserer Wirtschaft hat KPMG eine geschäftsbereichsübergreifende Spezialisierung vorgenommen. Hier laufen die Erfahrungen der Expertinnen und Experten weltweit zusammen und tragen zusätzlich zur Beratungsqualität bei.

Über den MVFP
Der MVFP Medienverband der freien Presse vertritt die publizistischen, kulturellen, politischen und wirtschaftlichen Interessen von rund 350 Mitgliedsverlagen und von etwa 7.000 Zeitschriften- und Medienangeboten in der Branche. Die Gemeinschaft der Zeitschriftenverlage im Medienverband der freien Presse vereint große, mittlere und kleine Medienhäuser.

Der MVFP setzt sich für den Fortbestand der freien Presse, die Freiheit und Vielfalt der Meinungen und die Zukunft des marktwirtschaftlich finanzierten Journalismus als Garant für die freiheitlich demokratische Grundordnung ein.

Seine Mitglieder unterstützt der Verband mit Service-, Beratungs- und Bildungsangeboten in den drängenden Fragen der Veränderung der Märkte und der Digitalisierung. Gegenüber der Politik setzt sich der Medienverband der freien Presse für ordnungspolitische Rahmenbedingungen sowie für faire und transparente Wettbewerbungsbedingungen ein.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Dr. Markus Kreher
Partner, Head of TMT (Technology, Media & Telecommunications)
T +49 89 9282-4310
markuskreher@kpmg.com

Dr. Michael Falk
Partner, Consulting, Cybersecurity
T +49 40 32015-5879
mfalk@kpmg.com

An dieser Studie haben mitgewirkt:

Andre Braun
Senior Manager, Consulting, Cybersecurity
KPMG AG Wirtschaftsprüfungsgesellschaft

Lara Blankenhagen
Consulting, Cybersecurity
KPMG AG Wirtschaftsprüfungsgesellschaft

Lutz Drüge
Geschäftsführer Fachvertretung Die Publikumsmedien
Medienverband der freien Presse (MVFP)

Luisa Becker
Projektmanagerin Print & Digitale Medien (MVFP)

Kerstin Vogel
Director Business Development, Events & Training
MVFP Akademie

Prof. Dr. Thomas Hess
Direktor des Instituts für Digitales Management und Neue Medien
Ludwig-Maximilians-Universität München

Dr. Antonia Meythaler
Institut für für Digitales Management und Neue Medien
Ludwig-Maximilians-Universität München
Universität Potsdam

www.kpmg.de

www.kpmg.de/socialmedia