Praxisstudien kompakt

Gut gemachte Studien zu aktuellen Themen der Wirtschaft sind für Praktiker und Wissenschaftler gleichermaßen interessant. Die Rubrik „Praxisstudien kompakt“ gibt Einblicke in relevante und informative Studien rund um die Thematik Medienwirtschaft.

In dieser Ausgabe präsentieren wir Ihnen die Studie „Cybersecurity – Wie sich Verlage auf veränderte Bedrohungslagen einstellen“. Der Fokus der Studie von KPMG liegt auf der aktuellen Bedeutung und dem Status quo der Cybersicherheit im Verlagswesen. Es werden die Bedrohungslage, Schadensfälle sowie die Wirksamkeit von Sicherheitsmaßnahmen in deutschen Verlagen präsentiert. Abschließend werden basierend auf den Umfrageergebnissen und der Analyse der Bedrohungslandschaft konkrete Handlungsempfehlungen für Verlage abgeleitet. Die Ergebnisse verdeutlichen, dass Cybersicherheit eine zentrale Rolle spielt und dass es weiterhin signifikanten Handlungsbedarf gibt, um die digitalen Infrastrukturen und Geschäftsprozesse effektiv zu schützen.

Falls Sie uns auf weitere Praxisstudien aufmerksam machen möchten, welche aus Ihrer Sicht in dieser Rubrik Platz finden sollten, wenden Sie sich gerne an Nina Zwingmann unter nina.zwingmann@lmu.de.

Cybersecurity: Wie sich Verlage auf veränderte Bedrohungen einstellen

Die Studie wurde von KPMG in Zusammenarbeit mit dem Medienverband der freien Presse (MVFP) erstellt und basiert auf einer Online-Umfrage, die im Herbst 2023 unter 118 deutschen Verlagen durchgeführt wurde. KPMG ist eine global agierende Wirtschaftsprüfungs- und Beratungsfirma, die regelmäßig Studien in verschiedenen Branchen durchführt, um Trends und Entwicklungen zu analysieren. Die Kooperation mit dem MVFP und die Einbindung externer Experten gewährleisten eine fundierte und praxisnahe Analyse der aktuellen Cybersicherheitslage. Ziel der Studie ist es, die Bedrohungslage für Verlage zu bewerten, bestehende Sicherheitsmaßnahmen zu untersuchen und konkrete Handlungsempfehlungen zur Verbesserung der Cybersicherheit abzuleiten.

Verschärfte Bedrohungslage durch Cyberattacken. Laut der Studie hat sich die Bedrohungslage für Verlage in den letzten Jahren signifikant verschärft. Ein markantes Beispiel dafür ereignete sich im Juni 2023, als eine der beliebtesten Nachrichten-Websites Deutschlands nach einem Cyberangriff auf ihren IT-Dienstleister offline war. Solche Vorfälle sind besonders kritisch, da die Verlagsbranche darauf angewiesen ist, ihre Dienste rund um die Uhr online verfügbar zu halten. Die zunehmende Sensibilität der Branche für Cyberrisiken zeigt sich darin, dass 75 % der

befragten Verlage die Sicherheit ihres Unternehmens als vorrangigen Megatrend betrachten. Zusätzlich werden die geopolitischen Spannungen haben als weitere Verschärfung der Situation angeführt, da neben finanziellen Erpressungen und Sabotageakten auch die gezielte Verbreitung von Falschinformationen und politischer Propaganda in den Fokus der Angreifer gerät. Cyberangriffe treffen Verlage jeder Größe, und insbesondere kleinere Verlage können durch Systemausfälle erheblich geschädigt werden. Die Angreifer nutzen zunehmend fortschrittliche Technologien und entwickeln ihre Methoden ständig weiter, was von den Verlagen kontinuierliche Anpassungen und Verbesserungen ihrer Sicherheitsstrategien verlangt.

Prävention, Erkennung und Reaktion als Maßnahmen. Cybersicherheitsmaßnahmen lassen sich in drei Hauptkategorien einteilen: Prävention, Erkennung und Reaktion. Obwohl 78 % der Verlage sich in der Prävention gut bis sehr gut aufgestellt sehen und ähnliche Einschätzungen für Erkennung und Reaktion bestehen, offenbart die Studie eine Diskrepanz zwischen Wahrnehmung und Realität. Tatsächlich wurden im vergangenen Jahr mehrere Verlage Opfer von Cyberangriffen, obwohl sie ihre Sicherheitsmaßnahmen als ausreichend betrachteten. Diese Fehleinschätzung wird darauf zurückgeführt, dass Sicherheitsmaßnahmen nicht regelmäßig aktualisiert werden und es an Sensibilisierung und Schulungen der Mitarbeitenden mangelt. Nur 43 % der befragten Verlage haben formale Security-Zuständigkeiten in ihrer Organisation verankert, während viele andere diese Aufgabe informell besetzen oder an externe IT-Dienstleister auslagern. Insbesondere kleinere Verlage können durch Systemausfälle erheblich geschädigt werden, wenn IT-Systeme ausfallen und betriebliche Abläufe gestört werden.

Cyberattacken als reale Bedrohung. Dass Cyberangriffe der bittere Alltag für Verlage sind, wird klar herausgestellt: Fast die Hälfte der befragten Verlage hat in den letzten zwölf Monaten mindestens einen Cyberangriff registriert, wobei etwa 40 % dieser Angriffe erfolgreich waren. Die häufigsten Angriffsarten sind Phishing, Ransomware und Datenlecks. Die Konsequenzen dieser Angriffe sind erheblich: 23 % der betroffenen Verlage berichten von Datenverlusten und finanziellen Einbußen, während 12 % Imageschäden erlitten haben. Diese gravierenden Auswirkungen verdeutlichen den dringenden Handlungsbedarf zur Verbesserung der Cybersicherheitsmaßnahmen, um solche Schäden in Zukunft zu minimieren. Es wird überraschenderweise festgestellt, dass selbst viele Großverlage keine speziellen Sicherheits- oder Response-Teams eingerichtet haben, um zukünftigen Angriffen frühzeitig und effektiv begegnen zu können. Als kostengünstige Maßnahme werden Schulungsprogramme für Mitarbeitende vorgeschlagen, um das Bewusstsein für IT-Sicherheit und potenzielle Bedrohungen zu erhöhen.

Maßnahmen für mehr Unternehmenssicherheit. Sicherheitskonzepte, Überwachungssysteme und Präventionsmaßnahmen werden als zentrale Elemente zur Minimierung von Angriffsrisiken und Schadensfällen herausgestellt. Während 56 % über ein rund um die Uhr arbeitendes Monitoringsystem verfügen, haben nur 28 % der Verlage umfassende Cybersicherheitskonzepte. Besonders kleine Verlage und das Buchsegment weisen hier Defizite auf. Obwohl Maßnahmen wie Datensicherung (86 %), Zugriffskontrollen (74 %) und Mitarbeiterschulungen (69 %) verbreitet sind, besteht laut Studie erheblicher Handlungsbedarf. Nur 25 % der Verlage führen regelmäßig Pentests durch, 15 % nutzen GAP-Audits, und 11 % messen ihren Sicherheitsstatus mit KPIs. Es fehlt insbesondere an regelmäßigen Schulungen und systematischem Monitoring.

Die Studie empfiehlt sieben grundlegende Maßnahmen zur Verbesserung der Unternehmenssicherheit. Erstens sollten Unternehmen stets die neuesten Systemupdates installieren und grundlegende Schutzmaßnahmen umsetzen, da mehr als 75 % der erfolgreichen Angriffe auf unzureichende Kontrollen zurückzuführen sind. Zweitens ist es essenziell, die wichtigsten Assets zu identifizieren und besonders zu schützen, da begrenzte Ressourcen oft priorisiert werden müssen. Drittens sollten Unternehmen mögliche Angriffsszenarien analysieren, um die wahrscheinlichsten Bedrohungen vorherzusehen und entsprechende Schutzmaßnahmen zu ergreifen. Viertens ist die Sicherheit der Lieferkette entscheidend, da das schwächste Glied oft das Einfallstor für Angriffe ist. Fünftens sollten Sicherheitsverantwortliche eng mit anderen Unternehmensbereichen sowie mit Kunden und Lieferanten zusammenarbeiten, um Vertrauen und Unterstützung bei potenziellen Vorfällen zu gewährleisten. Sechstens sollte eine starke Sicherheitskultur im Unternehmen gefördert werden, damit alle Mitarbeitenden an einem Strang ziehen. Schließlich bietet Cybersicherheit die Chance, finanzielle Schäden und Reputationsverluste zu vermeiden und gleichzeitig die Wettbewerbsfähigkeit und Unternehmensziele zu sichern.

Fallstudie: Cybersecurity bei der SDZ Mediengruppe. Die IT der SDZ Mediengruppe ist zentral in einer Tochtergesellschaft organisiert, die als eigenständiges Profitcenter für alle Gesellschaften der Gruppe agiert. Cybersicherheit ist fest in dieser Einheit verankert und hat seit den Anfängen des Internets einen hohen Stellenwert. Angesichts der zunehmenden Cyberattacken hat der Fokus auf Netzwerksicherheit und die Absicherung der Clients stark zugenommen. Mit der zunehmenden Vernetzung und dem mobilen Arbeiten ist die Bedeutung der Cybersicherheit weiter gestiegen. Früher waren Angriffe weniger professionell und hatten geringere Auswirkungen, heute jedoch können solche Angriffe das gesamte IT-Netzwerk lahmlegen, was umfassendere Sicherheitsmaßnahmen erfordert. Daher investiert die SDZ Mediengruppe nun in eine 24/7-Überwa-

chung und schnelle Reaktionszeiten. Ein konkreter Vorfall zeigte die Effektivität dieser Maßnahmen: Ein Mitarbeiter klickte auf einen gefälschten Chrome-Aktualisierungsbanner, woraufhin der betroffene Client innerhalb von 15 Minuten isoliert wurde. Die größten Sicherheitsrisiken gehen von unbeabsichtigten Handlungen der Mitarbeitenden aus, weshalb deren Sensibilisierung und Schulung entscheidend sind. Ein erfolgreicher Ransomware-Angriff führte zur Verschlüsselung vieler virtueller Server und zum Datenabzug. Dank einer guten Backup-Policy konnten gravierende Produktionsstopps vermieden werden.

Handlungsempfehlungen und Ausblick. Mit der zunehmenden Digitalisierung steigt das Sicherheitsrisiko in der Verlagsbranche, und Cyberangriffe werden in den nächsten Jahren häufiger und intensiver. Es wird angenommen, dass 65 % der Verlage in den nächsten zwei bis drei Jahren verstärkte Cyberangriffe erwarten können. Daher empfiehlt die Studie, dass Verlage proaktiv und frühzeitig handeln, um umfassende Schutzmechanismen zu etablieren. Dazu gehören ausreichende Investitionen in Cybersicherheit und klare organisatorische Zuständigkeiten, wie Sicherheitsbeauftragte oder Incident-Response-Teams. Automatisierte Frühwarnsysteme und klare Alarmierungsprozesse sollten eingeführt werden, um Netzwerke und Systeme in Echtzeit zu überwachen. Sicherheitskonzepte sollten spezifische Anforderungen berücksichtigen und regelmäßig auf ihre Wirksamkeit geprüft werden, um Schwachstellen frühzeitig zu erkennen und zu beheben. Der Schutz von Identitäten und Accounts ist essenziell, etwa durch Multifaktorauthentifizierung, und entdeckte Datenlecks müssen sofort geschlossen werden. Schließlich sollten Sicherheitsstrategien kontinuierlich an neue Bedrohungen angepasst werden, durch regelmäßige Schulungen und enge Zusammenarbeit mit IT-Fachleuten.

Zusammenfassend lässt sich sagen, dass Cybersicherheit für die deutsche Verlagsbranche von höchster Priorität ist, da die Bedrohungslage durch digitale Angriffe stetig zunimmt. Die Mehrheit der Verlage erkennt die Notwendigkeit, sich gegen digitale Bedrohungen zu wappnen, dennoch sind viele Verlage trotz vorhandener Schutzmaßnahmen Opfer von Cyberangriffen geworden. Diese Angriffe haben oft schwerwiegende Konsequenzen, wie Datenverluste, finanzielle Einbußen und Imageschäden, und beeinträchtigen die Geschäftstätigkeit erheblich. Es besteht ein erheblicher Handlungsbedarf, umfassende Sicherheitskonzepte zu entwickeln und effektive Überwachungssysteme zu implementieren, um den Schutz der digitalen Infrastrukturen zu gewährleisten. Der Bericht zeigt, dass nur ein kleiner Teil der Verlage über detaillierte Sicherheitskonzepte verfügt und dass viele Verlage ihre Schutzmaßnahmen nicht regelmäßig auf Wirksamkeit prüfen. Die Studie verdeutlicht, dass die Verlagsbranche zwar zunehmend sensibilisiert ist, jedoch weiterhin erhebliche Maßnahmen ergreifen muss, um den ständig neuen Herausforderungen der Cybersicherheit gerecht zu werden. Nur durch kontinuierliche Anpassung und Verbesserung der Sicherheitsstrategien können Verlage ihre digitalen Vermögenswerte und Geschäftsprozesse effektiv schützen und die Resilienz gegen Cyberangriffe stärken.

Die volle Studie steht auf der Webseite von KPMG kostenlos zum Download zur Verfügung.

Nina Zwingmann, MSc., LMU München
Prof. Dr. Martin Gläser,
Hochschule der Medien Stuttgart

