Die Cybersecurity effektiv managen

Reto Zbinden,
Rechtsanwalt / CEO, Swiss Infosec AG

1. Einleitung

Die rasante Digitalisierung in nahezu allen Branchen – so auch in Anwaltskanzleien – steigert nicht nur die Effizienz, sie schafft auch neue Herausforderungen, gerade im Bereich der Cybersicherheit und stellt ein erhebliches Risiko für die Vertraulichkeit, Verfügbarkeit und die Integrität sensibler Mandantendaten dar. In einem zunehmend vernetzten Umfeld sehen sich alle Organisationen mit diversen Risiken konfrontiert, die von Cyberangriffen bis hin zu Datenschutzverletzungen, so genannten Data Breaches, reichen. Für kleine und mittlere Kanzleien, die nicht über die Ressourcen grosser Organisationen verfügen, ist es deshalb wichtig, effektive und praktikable Massnahmen gegen Cybersicherheitsrisiken zu ergreifen.

Unter Cybersicherheit verstehen wir sämtliche Risiken, Massnahmen, Prozesse und Aufgaben auf organisatorischer und technischer Ebene zur Identifikation, Analyse und Bewältigung von Cyberbedrohungen und -angriffen. Cybersicherheit ist also viel mehr als reine IT Security. Cybersicherheit ist ein wichtiger Teil der Informationssicherheit mit Schnittstellen einerseits zum Krisenmanagement/Business Continuity Management und andererseits zu IT Security, Datenschutz und Informationsschutz sowie IT-Prozessen an und für sich.

Dieser Artikel bietet einen Überblick über die wesentlichen Aspekte des Cyber Security Managements und gibt praxisnahe Empfehlungen, um diesen Herausforderungen proaktiv zu begegnen.

2. Risiken im Cyber Security Management

Ein zentraler Punkt im Cyber Security Management ist das Risikomanagement und somit die Identifikation und Bewertung von Risiken. Eine sorgfältige Analyse der bestehenden IT-Infrastruktur ist entscheidend, um potenzielle Sicherheitslücken zu identifizieren. Dies umfasst die Überprüfung von Software- und Hardwarekomponenten, Netzwerksicherheit, Lieferantenbeziehungen, Prozessen und potenziellen Risiken durch menschliche Fehler oder externe Bedrohungen.

Hierbei ist es wichtig, die effektiven Risiken für das eigene Unternehmen zu identifizieren und zu verstehen.

Von gezielten Phishing-Angriffen bis hin zu Ransomware-Attacken können die Bedrohungen vielfältig sein. Ein gutes Verständnis der verschiedenen Cybersicherheitsrisiken ist entscheidend, um wirksame Schutzmassnahmen zu entwickeln. Hier werfen wir einen Blick auf Beispiele von verschiedenen Bedrohungen, denen Unternehmen heute ausgesetzt sind.

Phishing-Angriffe:

Phishing ist eine der häufigsten Bedrohungen, bei der Angreifer versuchen, durch Täuschung an vertrauliche Informationen zu gelangen. Dies kann durch gefälschte E-Mails, gefälschte Anrufe, gefälschte Websites, Deepfakes (digitale Fälschungen von Gesichtern, Körpern, Szenen etc., die mit Künstlicher Intelligenz (KI) erstellt werden) oder andere manipulative Methoden geschehen. Mitarbeitende sollten regelmässig in der Erkennung von Phishing-Angriffen geschult werden, um die Gefahr zu minimieren.

Ransomware-Attacken:

Ransomware ist neben Phishing eine der ernsthaftesten Bedrohungen, bei der Angreifer die Systeme oder Daten eines Unternehmens verschlüsseln und Lösegeld für deren Freigabe verlangen. Ein robustes Backup- und Wiederherstellungssystem ist unerlässlich, um den möglichen Schaden einer solchen Attacke zu begrenzen.

Zero-Day-Exploits:

So genannte Zero-Day-Exploits nutzen Sicherheitslücken aus, die den Entwicklern noch nicht bekannt sind. Organisationen sollten ihre Systeme regelmässig aktualisieren und Schwachstellen proaktiv identifizieren, um das Risiko von Zero-Day-Angriffen zu minimieren.

Insider-Bedrohungen:

Insider-Bedrohungen können von aktuellen oder ehemaligen Mitarbeitenden ausgehen, die unberechtigten Zugriff auf sensible Informationen haben. Eine umfassende Zugriffskontrolle und Überwachung können helfen, solche Risiken zu minimieren.

Diese Beispiele verdeutlichen, wie vielschichtig und dynamisch die Bedrohungen im Bereich der Cybersicherheit sein können. Unternehmen müssen auf technischer und organisatorischer Ebene gegen Cyberrisiken vorgehen, bzw. deren Auswirkungen reduzieren.

3. Massnahmen für ein effektives Cyber Security Management

Folgende Massnahmen sollte eine Anwaltskanzlei zu ihrem Schutz schrittweise umsetzen:

1. Wiederherstellbarkeit der geschäftskritischen Prozesse festlegen

Die Wiederherstellbarkeit der geschäftskritischen Prozesse muss innert nützlicher Frist sichergestellt sein. Fragen, wie lange ein Prozess (oder gar das ganze Unternehmen) stillstehen darf, bevor es existenziell wird, oder wie lange die IT für die Wiederherstellung der Prozesse inklusive dazugehöriger Applikationen und Daten benötigt, müssen klar beantwortet sein. Die Antworten darauf zeigen den Risikoappetit und daraus abgeleitet die Breite und Tiefe der festzulegenden Massnahmen.

2. Solide und regelmässig geprüfte Backup-Infrastruktur

Die Backup-Infrastruktur soll nach dem 3-2-1-0-Prinzip aufgestellt sein: Also drei Kopien aller wichtigen Daten, zwei verschiedene Speichertypen, mindestens ein Backup offline/unveränderlich und Null Fehler bei der Konsistenzprüfung jedes Backup-Vorgangs.

3. Vorbereitung für den Ernstfall

Jede Vorbereitung ist besser als keine. Eine Organisationsstruktur und eine Vorgehensweise für den Ernstfall müssen definiert und geübt werden. Nicht zu vergessen ist, die IT mit entsprechenden Kompetenzen für den Notfall auszustatten, um erforderliche Sofortmassnahmen durchsetzen zu können. Die gleiche Organisationsstruktur kann für jede Art von Krise genutzt werden, nicht nur im Fall einer Cyberattacke.

4. Durchgängige Sicherheit bei Schnittstellen

Fernzugriffsmöglichkeiten in das eigene Unternehmen aus dem Internet sind auf das erforderliche Minimum zu beschränken und durchgängig mit Mehrfaktorauthentifizierung abzusichern.

5. Sichere Konfiguration von Endgeräten und Absicherung administrativer Zugriffe

Viele Standardkonfigurationen von Endgeräten sind tendenziell unsicher konfiguriert. Ein genauer Blick lohnt sich. Auch administrative Zugriffe sind über Mehrfaktorauthentifizierung abzusichern und administrative Privilegien sollten nach dem so genannten «Least-Privilege-Prinzip» (Prinzip der minimalen Rechte) eingeschränkt werden.

6. Eingeschränkte Zugriffsberechtigung

Mit einem Rollen- und Berechtigungskonzept sorgt man dafür, dass die Zugriffsberechtigungen angemessen verteilt werden. In KMU haben oftmals alle auf alles Zugriff, womit ein Angreifer nur einen einzigen Benutzer kompromittieren muss, um Zugriff auf sämtliche Daten zu erhalten.

7. Regelmässige Sicherheitsaudits

Regelmässig durchgeführte Sicherheitsaudits sind entscheidend, um die Wirksamkeit der implementierten Sicherheitsmassnahmen zu bewerten und anzupassen. Diese Audits sollten sowohl interne als auch externe Sicherheitsüberprüfungen (z. B. beim IT-Provider oder anderen Lieferanten) umfassen, um eine Bewertung der Sicherheitslage der Kanzlei zu gewährleisten.

8. Anpassung an neue Bedrohungen

Da sich Cyberbedrohungen ständig weiterentwickeln, müssen auch Anwaltskanzleien ihre Sicherheitsstrategien kontinuierlich überdenken und anpassen. Dies beinhaltet das Verständnis neuer Bedrohungsmuster und das Implementieren fortschrittlicher Sicherheitslösungen, um diesen entgegenzuwirken.

9. Regelmässige Sensibilisierung und Ausbildung

Insgesamt trägt die regelmässige Sensibilisierung und Schulung (z. B. mit eLearning, Präsenzveranstaltungen, Workshops etc.) dazu bei, die Sicherheitsresilienz eines Unternehmens zu stärken und die Wahrscheinlichkeit von Cyberangriffen zu minimieren. Menschen bleiben eine potenzielle Schwachstelle im Cybersicherheitskontext. Eine kontinuierliche Sensibilisierung vermindert das Fehlverhalten, schärft das Bewusstsein für aktuelle Bedrohungen und stärkt die Sicherheitskultur zum Schutz von Unternehmensinformationen.

10. Unterstützung durch externe Partner

Sorgen Sie dafür, dass im Ernstfall innert nützlicher Frist eine kompetente Unterstützung da ist. Gemeinsam mit den Partnern sind Reaktionszeiten, Zugriffsmöglichkeiten und Allgemeines zur Zusammenarbeit festzulegen.

4. Bewährte Frameworks

Um eine strukturierte Herangehensweise an das Cyber Security Management zu gewährleisten, sind Frameworks wie ISO 27001 (Internationale Norm für Informationssicherheitsmanagement) und das Cybersecurity Framework des NIST (Umfassender Leitfaden für Cybersecurity des National Institute of Standards and Technology) heute unverzichtbar. Die Verwendung dieser etablierten Frameworks – auch ohne Zertifizierung – bildet das Rückgrat eines effektiven Cyber Security Managements.

Die konsequente Anwendung dieser Frameworks bietet nicht nur einen soliden Schutz vor Cyberbedrohungen, sondern signalisiert auch Klienten, Partnern, Mitarbeitenden und Behörden, dass das Unternehmen die höchsten Standards in Bezug auf Informationssicherheit einhält. Darüber hinaus erleichtert es die Einhaltung gesetzlicher Vorgaben und schafft eine Grundlage für kontinuierliche Verbesserung im Bereich der Cybersecurity.

5. Fazit

In einem sich ständig weiterentwickelnden digitalen Umfeld ist ein proaktives Cyber Security Management von entscheidender Bedeutung. Dieser Artikel hat die wichtigsten Aspekte beleuchtet, von der Risikobewertung bis zur Umsetzung bewährter Praktiken unter Verwendung international anerkannter Frameworks. Unternehmen, insbesondere in der Rechtsbranche, stehen vor der Herausforderung, ihre sensiblen Daten zu schützen und die Integrität ihrer digitalen Infrastruktur zu gewährleisten. Die Einhaltung bewährter Praktiken und die Anwendung internationaler Standards sind Schlüsselkomponenten, um diesen Herausforderungen erfolgreich zu begegnen.

Résumé en français:

L'article donne un aperçu des défis de la cybersécurité et propose des recommandations pratiques pour y faire face de manière proactive. Un point central de la gestion de la cybersécurité est la gestion des risques et donc l'identification et l'évaluation des risques. Il est important d'identifier et de comprendre les risques effectifs pour sa propre entreprise afin de mettre en œuvre des mesures techniques et organisationnelles – notamment la mise en place d'une infrastructure de sauvegarde solide, une préparation proactive aux situations d'urgence ou une sensibilisation régulière – contre les menaces telles que les attaques de phishing ou les attaques de ransomware et de renforcer ainsi la résilience de l'entreprise en matière de sécurité.