III. QUARTAL, 2023

Allianz

CYBER-NEWSLETTER

Aktuelle Entwicklungen

Tools für Künstliche Intelligenz als potenzielles Cybersicherheitsrisiko

Die Fortschritte im Bereich der künstlichen Intelligenz und speziell im Bereich der LLM (Large Language Models) haben zu einer Vielzahl nützlicher Entwicklungen geführt, darunter auch Chatbots wie Chat GPT von OpenAI oder das kürzlich vorgestellte Bard von Google. Diese leistungsstarken KI-Tools können menschenähnliche Gespräche führen und bei einer Vielzahl von Aufgaben helfen, wie beispielsweise Verfassen von Artikeln, bei Recherchen oder der Generierung von Softwarecode.

Diese Fähigkeiten machen sich vermehrt auch Cyberkriminelle zunutze. Gepaart mit ihren Kenntnissen zu Schwachstellen und Angriffsvektoren nutzen sie die neuen Tools, um schädlichen Code (Malware) zu schreiben, der von ihnen gezielt eingesetzt werden kann. Darüber hinaus können sie mit den KI-Lösungen Phishing-Emails und gefälschte Webseiten in hoher Qualität sowie in mehreren Sprachen oder Deep Fakes erstellen. Durch den Einsatz von KI-Tools fallen somit weitere Barrieren, vor allem finanzieller Natur, die es immer mehr Akteuren erlauben, cyberkriminelle Aktivitäten zu durchführen. Auch deshalb ist in naher Zukunft mit einem weiteren Anstieg von Cyberangriffen zu rechnen.

IN DIESER AUSGABE

Weitere Hintergründe über die Nutzung von KI-Tools durch Cyberkrimelle

Über die Nutzung von KI-Tools seitens von Cyberkriminellen hat bereits die europäische Polizeibehörde Europol gewarnt und das Fachmagazin golem berichtet. Es treten vermehrt auch spezifische KI-Lösungen auf, die dediziert cyberkriminellen Zwecke dienen, wie z. B. Worm GPT.

Allianz

Wie Unternehmen von strukturierten Cyber-Risikomanagementprozessen profitieren

Beinahe jedes Unternehmen verfügt über Dokumente und Prozesse zur Etablierung eines internen Risikomanagements. Im Fokus der Risikomanagementprozesse stehen hierbei oft finanzielle Risiken, während IT-, Informationssicherheit oder Datenschutzrisiken häufig vernachlässigt werden. Dies gilt für kleine und mittlere, aber auch für große Unternehmen. Dabei liegen die Vorteile des Aufbaus von Cyber-Risikomanagementstrukturen auf der Hand. Sie verhelfen Unternehmen zu mehr Transparenz bezüglich des Sicherheitsstatus ihrer Informationswerte und der Identifikation von Maßnahmen, die ihrer Resilienz- und Widerstandsfähigkeit zu Gute kommen. Die Etablierung eines Risikomanagementsystems, das auch Cyber-Risiken berücksichtigt, kann Unternehmen zudem dabei helfen regulatorischen Anforderungen mehrerer Gesetze zu erfüllen. Doch wie lässt sich ein Cyber-Risikomanagementsystem initial etablieren?

Zuerst sollten Unternehmen für sich entscheiden, welchen Bedrohungen und Gefährdungen sie ausgesetzt sind bzw. für sie relevant sein könnten. Dazu können beispielsweise Szenarien wie Cyber-Angriffe oder Naturkatastrophen gehören, die zu unmittelbaren Schäden der IKT-Infrastrukturen führen. Diese und weitere Szenarien können auch sog. Bedrohungs- und Gefährdungskatalogen entnommen werden, die beispielsweise von Bundesamt für Sicherheit- in der Informationstechnik (BSI) veröffentlich werden. Des Weiteren sollten Unternehmen weitere Informationsquellen identifizieren, die ihnen als Hinweisgeber für IKT-Risiken fungieren. Dazu gehören Prozesse wie das Schwachstellen- und Patchmanagement, Meldungen von Herstellern und Dienstleistern und das Life-Cycle-Management. Gehen wir beispielsweise davon aus, dass eine bestimmte Schwachstelle nicht mithilfe eines Sicherheitspatches geschlossen werden kann (u. a. weil kein Patch verfügbar oder das zu patchende System veraltet ist), so muss dieser Umstand an das IKT-Risikomanagement weitergegeben werden. In einem nächsten Schritt wird dieser Umstand, also das Risiko, einer Bewertung unterzogen.

In der Bewertungsphase wird zum einem eruiert, welche Negativfolgen für das Unternehmen aus einem Risiko resultieren könnten und zum anderen, wie wahrscheinlich ein Eintritt des Schadensereignisses sein könnte. Dabei sollten Kriterien vorab definiert werden, die eine Einschätzung des Schadens erlauben und finanzielle, prozessuale sowie dem Unternehmensruf schädigende Aspekte berücksichtigen. Solche Kriterien sollten auch für die Eintrittswahrscheinlichkeit eruiert werden (z. B. wie oft ein Schadensereignis innerhalb einer gewissen Zeitspanne eintreten könnte oder in der Vergangenheit bereits eingetreten ist). Aus der Kombination zwischen Schaden und Eintrittswahrscheinlichkeit ergibt sich die Höhe des Risikos, die mithilfe einer sog. Risikomatrix abgebildet werden kann.

Nach der Bewertung des potenziellen Schadens und der Eintrittswahrscheinlichkeit erfolgt die Identifikation von Maßnahmen, mit denen das Risiko mitigiert werden kann. Anhand dieser Maßnahmen kann das Risiko dann einer erneuten Bewertung bezüglich des Schadens und der Eintrittswahrscheinlichkeit unterzogen werden, um zu prüfen, ob die identifizierten Maßnahmen tatsächlich geeignet sind, das Risiko zu reduzieren. Idealerweise folgt dann auch bereits eine Planung zur Implementierung der identifizierten Maßnahmen.

Cyber-Risikomanagement in der Praxis

Der Artikel beschreibt einen Risikomanagementprozess, der an den Standard ISO / IEC 27005 angelehnt ist.

Allianz

Best Practices für den Umgang mit schweren Datenschutzverletzungen und Cyber-Krisen

Verletzungen des Schutzes personenbezogener Daten und der Verlust der Vertraulichkeit dieser gehören zu den größten Bedrohungen für Unternehmen. Doch viele von ihnen reagieren bei einem solchen Vorfall nicht in einer Art und Weise, die den Bedürfnissen ihrer Kunden oder den Meldepflichten gegenüber den Behörden gerecht wird. Sofort nach Bekanntwerden eines schweren Vorfalls folgt eine kritische Phase, in der ein Unternehmen wenig Zeit hat, um die geeigneten Entscheidungen zu treffen, die zu dem Erfolg oder Misserfolg im Umgang mit dem Vorfall oder der Krise führen. Selbst wenn dies nicht einfach erscheint, sollten die in dieser Phase getroffenen Verfügungen immer faktenbasiert erfolgen und Panik vermieden werden.

Der Schlüssel zum erfolgreichen Umgang mit schwerwiegenden Datenschutzverletzungen und Cyber-Krisen liegt in der Prävention. Unternehmen sind gut damit beraten, sich proaktiv auf Datenschutzverletzungen und andere Cyber-Krisenszenarien vorzubereiten. Hierzu gehört die Auseinandersetzung mit diesen Szenarien und der möglichen Konsequenzen für das Unternehmen. Unternehmen sollten sich daher die Frage stellen, wie sie auf solche Fälle reagieren würden. Wie würden sie beispielsweise handeln, wenn ihre sensibelsten Informationen, personenbezogene Daten oder Gesundheitsdaten ihrer Mitarbeiter an die Öffentlichkeit geraten? Was würden sie tun, wenn diese durch Kriminelle verschlüsselt werden und ein Erpressungsschreiben vorliegt? Wären sie in der Lage, die Daten aus ihren Backups wiederherzustellen? Wüssten sie, mithilfe welcher IT-Systeme die betroffenen Daten verarbeitet wurden und wie sie mit anderen Systemen verbunden sind oder welche Experten innerhalb des Unternehmens sowie außerhalb bei der Behandlung des Vorfalls involviert werden sollten? Oder wüssten sie, an welche Behörden sie den Vorfall melden sollten und innerhalb welcher Frist dies zu erfolgen hat?

Ein weiterer Aspekt, der in Krisenfällen oft unterschätzt wird, ist die Krisenkommunikation und der Umgang mit Informationen, die an Mitarbeiter, Geschäftspartner, Behörden oder die Medien zu geben sind. Neben den gesetzlichen Meldepflichten ist eine zeitnahe und transparente Kommunikation mit relevanten Stakeholdern oft das entscheidende Element, wenn es darum geht, langfristige Reputationsschäden zu vermeiden. Krisenmanagementpläne sollten deshalb auch diese Aspekte beachten und idealerweise Kern- und Haltebotschaften sowie Kontakte von Krisenkommunikationsexperten beinhalten.

Die Pläne sollten in Workshops und Übungen getestet und anschließend weiter verbessert werden. Bei einer Übung können sich Unternehmen mit den o. g. Cyber-Krisenszenarien auseinandersetzen und ihre Reaktion in einem kontrollierten Umfeld testen.

Von der Erstellung von Notfallbüchern, Reaktions- und Krisenmanagementplänen sowie der Durchführung von Übungen profitieren Unternehmen auch hinsichtlich der immer strenger werdenden regulatorischen Anforderungen in Bezug auf die IT- und Informationssicherheit und den Datenschutz, die u. a. von der EU-Datenschutz-Grundverordnung (EU-DSGVO), dem IT-Sicherheitsgesetz oder dem Digital Operational Resilience Act (DORA) in diesem Kontext verlangt werden.

Best Practices in Bezug auf das Management von Cyber-Krisenszenarien
Als Quelle für den oberen Artikel diente die Veröffentlichung von Allianz Commercial *„Cyber: dealing with a data breach“*, in dem mehrere Experten wertvolle Ratschläge für den Umgang mit Cyber-Krisen geben.

Allianz

Krankenhaus nach Ransomware-Vorfall insolvent

Medienberichten zufolge musste ein Krankenhaus im US-Bundesstaat Illinois im Juni 2023 wegen der Folgen eines Ransomware-Angriffs Insolvenz anmelden.

Durch die Attacke wurden die Computersysteme des Krankenhauses „St. Margaret's Health" lahmgelegt, sodass über mehrere Monate hinweg keine finanziellen Ansprüche an Versicherungen und staatliche Einrichtungen gestellt werden konnten. Dies führte wiederum zu drastischen finanziellen Folgen, die zur Schließung des Krankenhauses geführt haben mit weitreichenden Folgen für die lokale Krankenversorgung. Als weitere Gründe für die Insolvenzanmeldung gab das Krankenhaus zudem Personalmangel an.

In den letzten Jahren kam es zu einer Häufung von Meldungen zu Cyberattacken auf Krankenhäuser. Unter anderem musste eines der größten Hospitäler in Barcelona nach einem Ransomware-Angriff hunderte Operationen absagen. Auch in Deutschland fielen bereits mehrere Krankenhäuser und Kliniken Cyberkriminellen zum Opfer. Über die finanziellen Folgen für die Krankenhäuser hinaus hatten Patienten in der Folge mit Verzögerungen in der Abwicklung von Gesundheitsleistungen zu kämpfen.

Das Beispiel zeigt, welch verheerende Folgen Ransomware-Angriffe haben können. Im vergangenen Jahr meldete auch ein deutsches Traditionsunternehmen in der Fahrradbranche nach einem solchen Angriff Insolvenz an.

DORA setzt Finanzunternehmen stärker unter Druck

Die Anforderungen der Richtlinie und der Verordnung über die digitale operationale Resilienz (DORA) setzen Unternehmen in der Finanz- und Versicherungsbranche und deren Dienstleister unter Druck. Die Regularien zielen darauf ab, die Widerstandsfähigkeit ihrer digitalen Systeme zu stärken und die Maßnahmen hierzu innerhalb der EU-Mitgliedsstaaten zu vereinheitlichen.

Um diese Ziele zu erreichen, sieht die DORA die Umsetzung mehrerer Maßnahmen vor. Dazu gehören die Etablierung eines IKT-Risikomanagements, das Risiken, die auf Dritte zurückzuführen sind (u. a. durch Dienstleister) berücksichtigt sowie ein Meldewesens für IKT-Vorfälle. Auch die Implementierung von Cybersicherheitstests wird gefördert. Die Verordnung gibt vor, dass diese Anforderungen bis Januar 2025 umgesetzt werden müssen.

Neben Kredit- und Zahlungsinstituten gehören zum Adressatenkreis der Gesetze auch Versicherungs- und Rückversicherungsunternehmen, Anbieter von Kryptowährungen, Einrichtungen der betrieblichen Altersvorsorge und IKT-Dienstleister.

Hintergründe zum Ransomware-Vorfällen, die zu Insolvenzen geführt haben

Als Quelle für den oberen Artikel diente u. a. eine Veröffentlichung des Fachmagazins heise. Dort finden Sie auch Informationen zu weiteren betroffenen Unternehmen.

Mehr Informationen zur DORA

Unter den folgenden Links finden sie weitere Informationen und die Gesetzestexte zur DORA-Richtlinie und DORA-Verordnung.