Cyberrisiken

Sind Cyberversicherungen für Pensionskassen sinnvoll?

Pensionskassen, die ihre Cyberversicherungspolice zum Jahreswechsel erneuerten, mussten tief in die Tasche greifen. Deutliche Prämienerhöhungen, Verdopplung der Selbstbehalte und Reduzierung der Deckungsstrecken waren keine Ausnahmen. Obwohl sich die Situation etwas zu entspannen scheint, bleibt der Transfer von Cyberrisiken anspruchsvoll.

Rolf Th. Jufer
Partner,
Funk Gruppe Schweiz & Liechtenstein

Meist handelt es sich bei Angriffen auf Unternehmen und Pensionskassen um Ransomware-Attacken, die immer professioneller werden.

Kriminelle Erpresser sind professionell organisiert

Das Geschäftsmodell *Ransomware-as-a-Service*[1] entwickelt sich stetig weiter: Zum einen verschlüsseln die Angreifenden aktive Systeme und falls möglich Backups. Zum anderen stehlen sie vertrauliche Daten, um zusätzlich Druck ausüben zu können.

Diese als *Double-Extortion* (Doppelte Erpressung) bekannt gewordene Vorgehensweise entwickelt sich nun nach und nach zu einer Triple-Extortion weiter. Diese umfasst zusätzlich einen *DDoS-Angriff*[2] (auf Webseiten oder Kundenportale von Vorsorgewerken), um die angegriffene Kasse in die Knie zu zwingen und zur Zahlung des Lösegelds zu bewegen.

Die individuelle Lösegeldforderung wird dabei an die finanziellen Möglichkeiten des Angriffsziels angepasst. Pensionskassen scheinen aufgrund der gut sichtbaren Vermögensverhältnisse und der sensiblen sowie besonders schützenswerten Personendaten ein lohnendes Ziel für Cyberkriminelle zu sein.

Das schwächste Glied

«Einer klickt immer» – leider ein Running Gag in der Cybersecurity-Branche. Das schwächste Glied in jedem Cyber-Abwehrdispositiv ist der Mensch. Das einfachste Einfalltor für Cyberkriminelle ist und bleibt die Unwissenheit, Nachlässigkeit oder Neugier des Anwenders.

Der durch die Coronapandemie befeuerte Trend zum Homeoffice (auch bei Pensionskassenverwaltungen) bringt neue Schwachstellen in die IT-Systeme der Organisationen und erschwert die regelmässige Sensibilisierung der Mitarbeitenden hinsichtlich des ordnungsgemässen Umgangs mit Informationen und der modernen Gefahren des Internets.

Regelmässige Cyberfitness-Trainings sind unabdingbar

Die technischen Hürden für eine professionelle Cyberpolice sind das eine, die Cyberfitness der Mitarbeitenden das andere. Die Mitarbeitenden von Pensionskassen müssen mindestens jährlich spezifische Sensibilisierungstrainings durchlaufen, damit die Versicherbarkeit gewährleistet ist. Sinnvollerweise werden diese Trainings von regelmässigen, simulierten Phishing-Attacken begleitet. So

[1] Deutsch etwa: Erpressersoftware als Dienstleistung.

[2] Distributed Denial of Service (DDoS) nennt man einen Cyberangriff, der auf die Überlastung von Webservern, Online-Services oder ganzer Netzwerke zielt.

Leistungselemente qualitativer Cyberversicherungen

TAKE AWAYS

– Während die kriminellen Erpresserbanden mit professionellen Methoden vorgehen, bleibt das schwächste Glied in der Verteidigungskette in der Regel der einzelnde Mitarbeitende.
– Regelmässige Fitnesstrainings, um sich der Gefahren durch einen Angriff über die IT bewusst zu werden, sind deshalb ratsam.
– Der Markt für Cyberversicherungen ist anspruchsvoll; Prämien, Selbstbehalte und Deckungsbausteine sind detailliert zu verhandeln.
– Es ist deshalb auch für den Stiftungsrat empfehlenswert, sich intensiv mit der Problematik auseinanderzusetzen und externe Partner zuzuziehen, bevor ein Fall eintritt.

kann schnell und einfach überprüft werden, ob das Gelernte auch richtig angewendet wird und das Cyber-Abwehrdispositiv auch in Bezug auf das schwächste Glied funktioniert. Das Angebot an Trainings für Mitarbeitende ist vielfältig, ebenso die Palette an Lösungen bezüglich der Überprüfung des Konzepts. Viele Angebote sind anwenderfreundlich und nicht teuer.

IT-Outsourcing: Die Verantwortung lässt sich nicht delegieren

Viele Pensionskassen haben sinnvollerweise massgebliche Elemente der IT- und Cybersecurity einem Outsourcingpartner anvertraut oder nutzen die Infrastruktur des Kantons.

Die neuen Schweizer Datenschutzgesetze regeln die Risikotragung eindeutig, indem sie die juristische oder natürliche Person, die Daten erhebt und über ihren Verarbeitungszweck entscheidet, als Verantwortlicher definieren.[3] Dieser hat bei der Auslagerung von Datenverarbeitungsprozessen von Gesetzes wegen sicherzustellen, dass der Dienstleister bzw. Auftragsverarbeiter geeignete technische und organisatorische Massnahmen zum Datenschutz und zur Datensicherheit trifft.

Somit haftet stets der Verantwortliche gegenüber den betroffenen Personen für allfällige Datenschutzverletzungen und hat auch den vorgesehenen Meldepflichten nachzukommen. Ebenso entbindet die Auslagerung den Verantwortlichen nicht von der Pflicht, einen geeigneten Datenschutz zu organisieren und zu garantieren.

Unmittelbar verbunden mit der Auslagerung ist die Pflicht zur transparenten Information über den Verarbeitungszweck der Daten. In diesem Kontext müssen die betroffenen Personen vom Verantwortlichen nicht nur über den eindeutigen Zweck der Datenverarbeitung informiert werden, sondern auch über die Weitergabe ihrer Daten an den Auftragsverarbeiter (z. B. in Form einer Datenschutzrichtlinie). Zuletzt liegt es auch in der Verantwortung der Pensionskasse, die Zweckbindung auf Seiten ihrer Outsourcing-Partner sicherzustellen.

Pensionskassen, die IT-Outsourcing-Dienstleistungen beanspruchen, sind also gut beraten, die Datenschutz- und

[3] Zum Datenschutz siehe auch Akzent in der Schweizer Personalvorsorge 02/2023 und das Interview mit Ursula Uttinger in der Sonderausgabe «Externe Dienstleister» 2023, ab S. 12.

Sicherheitsstandards ihrer Outsourcingpartner abzuklären, umfassende Auftragsdatenbearbeitungsverträge abzuschliessen und vor allem auch alles vorzukehren, um als Unternehmen selbst den neuen gesetzlichen Vorhaben zu entsprechen.

Veränderte Strategie der Versicherer

Nach einer aggressiven Wachstumsstrategie mit tiefen «Marketingtarifen» und nachfolgend hohen Schäden, haben die Versicherungsgesellschaften einen radikalen Strategiewechsel vollzogen. Sie reduzieren den Deckungsumfang ihrer Policen insbesondere im Bereich Schäden durch oder im Zusammenhang mit Ransomware. Dies lässt sich auf die hohe Frequenz von Ransomware-Vorfällen zurückführen.

Schätzungsweise über 80 % der bekannten Schadenfälle stehen im Zusammenhang mit einer Ransomware. Folglich bieten einige Versicherer überhaupt keine Deckungen für Ransomware mehr an. Andere beschränken ihre Leistungen auf max. 50 % der Versicherungssumme oder beteiligen den Versicherungsnehmer zusätzlich an solchen Vorfällen. Generell haben sich die Kapazitäten der Rück- und Erstversicherer sowie der Deckungsumfang von Cyberversicherungen deutlich reduziert.

Pensionskassen sollten ihre finanziellen Cyberrestrisiken kennen

Es ist von Vorteil, sich als geschäftsführende Person der Kasse die Frage nach den Cyberrestrisiken frühzeitig zu stellen, um nicht vom Stiftungsrat mit derselben Fragestellung überrascht zu werden. Die wenig überzeugende Antwort wäre: «Mein Versicherungsberater hat mir die Zahl genannt, das sei der Durchschnittswert seiner Cyberversicherungsdeckungen.» Nur eine kassenspezifische Berechnung, basierend auf den individuellen Rahmenbedingungen, ist überzeugend.

Die Praxiserfahrung zeigt, dass die Quantifizierung der möglichen Kosten und Schäden, die aufgrund eines Cybervorfalls entstehen können, die Aufmerksamkeit der Führungspersonen hinsichtlich Cyberrisiken massiv erhöht. Einerseits kann daraus die notwendige Deckungssumme für eine Cyberversicherung abgeleitet werden, andererseits ein bewusster Entscheid hinsichtlich Eigentragung oder zusätzlichen Investitionen in Cybersecurity getroffen werden.

Auf Basis der finanziellen Cyberrestrisiken, die anhand der Kennzahlen der Kasse und verschiedener Daten und Erfahrungswerten berechnet werden, wird mit der Geschäftsführung und idealerweise Teilen des Stiftungsrats ein strukturiertes Gespräch durchgeführt.

Diese Diskussion schafft nicht nur Transparenz für die Kasse, sondern bildet auch eine sinnvolle Basis für den Grundsatzentscheid, ob ein Risikotransfer an eine Versicherungsgesellschaft stattfinden soll oder nicht. Zudem kann im Krisenfall bei Sammeleinrichtungen gegenüber den Destinatären oder den angeschlossenen Unternehmen nachvollziehbar dargelegt werden, dass der Risikomanagementprozess bezüglich Cyberrisiken bewusst, vollständig und sorgfältig abgearbeitet wurde. Schliesslich stehen bei einem Cybervorfall nicht nur die Reputation der Pensionskasse, sondern auch die Reputation der Geschäftsführung und des Stiftungsrats auf dem Spiel.

Risikotransfer bewusst abwägen

Der Stiftungsrat kann auf Basis der quantifizierten Cyberrestrisiken und der Angebote des Versicherungsmarkts eine bewusste Entscheidung treffen. Aufgrund unserer Erfahrungen entscheiden sich ca. 40 % der Organisationen für eine Versicherungslösung. Moderne Cyberversicherungen umfassen auch das Krisenmanagement und setzen erfahrene Cyber-Krisenmanager sowie weitere Incident-Response-Dienstleister zugunsten der Pensionskasse ein. Diese sind z. B. in der Lage, mit den Angreifern zu verhandeln und so Lösegeldforderungen durch Verhandlungserfolg zu reduzieren.

Die restlichen ca. 60 % investieren die entsprechenden Mittel in die Cybersecurity und in die Ausbildung ihrer Mitarbeitenden. Wir empfehlen in solchen Fällen, dass der *Incident Reponse* (Reaktionsfähigkeit bei erfolgreichem Angriff) besondere Beachtung geschenkt wird. Das heisst, dass sowohl der Krisenstab der Kasse als auch alle relevanten Partner die Massnahmen im Cyber-Krisenfall nicht nur organisatorisch vorbereiten, sondern auch regelmässig üben.