Cyber Security

Wo die Gefahren der Digitalisierung lauern

Die Pensionskassen beschäftigen sich seit einigen Jahren mit der Digitalisierung ihrer Businessmodelle. Die technologischen Möglichkeiten bringen viele Annehmlichkeiten mit sich, stellen aber in puncto Sicherheit auch neue Herausforderungen an Stiftungsräte und Geschäftsführung.

IN KÜRZE

Laufend aktualisierte Hard- und Software sind zentrale Faktoren beim Schutz vor Cyber-Angriffen. Ebenso wichtig sind die Schulung und Sensibilisierung der Mitarbeitenden sowie Notfallkonzepte.

Fabio Poloni
Security Analyst, Compass Security Schweiz AG

Pensionskassen und Sozialversicherungen verfügen über eine hohe Anzahl an Personendaten und verwalten eine grosse Summe an finanziellen Mitteln – für Cyberkriminelle äusserst lohnende Gründe, gezielte Angriffe zu planen und durchzuführen. Als oberstes Organ der Stiftung ist der Stiftungsrat für die Überwachung von Geschäftsrisiken und somit auch für das Schüsselthema Cyber-Sicherheit verantwortlich. In diesem Artikel werden die gängigsten Problemfelder und aktuelle Gefahren beleuchtet.

Sichere Basis

In der IT-Organisation von Schweizer Pensionskassen werden meist Lösungen betrieben, die entweder inhouse verwaltet oder von einem externen Dienstleistern zur Verfügung gestellt werden.[1] Dabei steht die Funktionalität der Anwendungen an erster Stelle, die Sicherheit spielt oft eine untergeordnete Rolle.

In der Praxis zeigt sich zwar, dass die Angriffsfläche gegenüber dem Internet durch Firewalls gewöhnlich auf ein Minimum reduziert wird, Sicherheitsprobleme tauchen aber oft innerhalb des eigenen Netzwerks auf.

Beispiele:
- veraltete Server mit bekannten Sicherheitslücken,
- fehlende oder unzureichende Sicherheitseinstellungen,
- fehlende Abtrennung von Netzwerken,
- Benutzer mit zu vielen Berechtigungen.

Sicherheit muss als Prozess und nicht als Zustand verstanden werden. Was vor wenigen Jahren noch als sicher galt, kann heute kritische Sicherheitslücken aufweisen. Sicherheit soll nicht nur bei neuen Projekten ein Thema sein, auch bestehende Lösungen müssen regelmässig gewartet, hinterfragt und bei Bedarf abgelöst werden. Regelmässiges Überprüfen der Netzwerke, Anwendungen und Dienste deckt allfällige Schwachstellen auf. Während der Konzeptions- und Implementationsphase können Security Reviews kritische Sachverhalte identifizieren.

Risikofaktor Mensch

Technische Vorkehrungen sind unerlässlich, aber nicht ausreichend. Als Risikofaktor Nummer eins für Cyber-Kriminalität zählt heute der Mensch. Die meisten Angriffe auf Organisationen erfolgen initial via E-Mail. Mit vertrauenswürdigen, aber gefälschten E-Mails (Phishing-Mails) bewegen Angreifer Mitarbeitende dazu, eine schädliche Aktion auszuführen.

[1] Siehe auch Artikel «Pensionskassen-Ökosystem als Digitalisierungsplattform» von Philipp Sutter, Sondernummer Symposium 2018 der «Schweizer Personalvorsorge».

«Als Risikofaktor Nummer eins für Cyber-Kriminalität zählt heute der Mensch.»

Durch Klicken auf einen Link oder ein angehängtes Dokument kann Schadsoftware installiert werden, die den Angreifern Zugriff auf das Postfach oder das System verschafft. Damit ist die grösste Hürde bereits überwunden. Ab diesem Moment werden Daten gestohlen und weitere Schwachstellen gesucht und ausgenutzt. Lukrativ sind Ransomware-Angriffe, bei denen sensible Daten der Organisation entwendet oder verschlüsselt werden, um dann deren Freigabe durch Zahlung von Lösegeld zu versprechen.

Auch Angriffe, die aufs Abfangen persönlicher Daten (Passwörter) oder auf das Manipulieren von Transaktionsnummern (Online-Banking) zielen, werden meist über eine E-Mail ausgelöst.

Starke Sicherheitskultur

Mitarbeitende, die oft mit externen Partnern kommunizieren (Sekretariat, Kundenberatung, Kommunikation), sind solchen Angriffen besonders ausgesetzt. Gezieltes Awareness-Training schult sie im Bezug auf Risiken und Gefahren und sensibilisiert für das Thema (Informations-)Sicherheit. Die Mitarbeitenden entwickeln so ein Bauchgefühl für heikle Situationen. Für schwierige Situationen sollten auch Ansprechpersonen bestimmt werden, die jegliche Meldungen und Fragen ernst nehmen. Und sollte doch einmal ein Fehler passieren, soll lösungsorientiert und keinesfalls anklagend gehandelt werden.

Es ist auch unerlässlich, dass die Mitarbeitenden der IT-Abteilungen zu den für sie relevanten IT-Security-Themen geschult werden. Ein umfassendes Verständnis für die eingesetzten Technologien und ein geschärftes Bewusstsein für aktuelle Angriffe sind Voraussetzung für die Implementierung von IT-Sicherheit.

Wird die Sicherheitskultur auf oberster Ebene initiiert, durch die Geschäftsführung ermöglicht, in den Fachabteilungen umgesetzt und von allen Mitarbeitenden gelebt, bietet sie effektiven Schutz für die ganze Organisation.

Prävention, Detektion, Reaktion

Es ist eine Herausforderung, die Sicherheit immer auf dem aktuellen Stand zu halten. Alle künftigen, möglicherweise auftretenden Schwachstellen zu verhindern, ist unmöglich. Deshalb sollen nicht nur präventive Massnahmen getroffen werden, sondern die Sicherheit der IT-Infrastruktur auch regelmässig überprüft und eine funktionierende Überwachung eingesetzt werden.

Mit der IT-Administration und Fachleuten ist zu klären, wie Anomalien und Angriffe frühzeitig detektiert werden und was in solchen Fällen getan wird. Dann ist schnelles und überlegtes Handeln gefragt, denn Fehler und Verzögerungen können viel Geld kosten.

Der Vorfall soll am Schluss auch aufgearbeitet werden: Ursachenfindung, Schadensermittlung, Wiederherstellung, Verbesserungen, neue Erkenntnisse.

Die Frage ist nicht ob, sondern wann

Früher oder später werden vermutlich alle Organisationen mit einem Vorfall in der IT-Sicherheit konfrontiert. Komplett verhindert werden können Cyber-Angriffe nicht. Ziel soll aber sein, deren Auswirkungen auf ein Minimum zu reduzieren.

Um den finanziellen Schaden (Eigenschaden, Schadensersatzansprüche, Krisenmanagement) eines Angriffs abzufedern, kann eine Cyber-Versicherung sinnvoll sein. Aber auch dafür müssen vorab diverse Massnahmen zum Schutz der versicherten Daten getroffen werden. Sind diese Hausaufgaben nicht erledigt, kann die Haftung abgelehnt werden.

Ein erfolgreicher Cyber-Angriff kann zudem sehr grosse Auswirkungen auf die Reputation einer Organisation haben und einen Vertrauensverlust bei Kunden und Partnern auslösen. IT-Sicherheit muss deshalb zwingend ins Risikomanagement einfliessen und auf der Agenda des Stiftungsrats einen festen Platz haben.

Fünf-Punkte-Check für Stiftungsräte

1. Starke Sicherheitskultur aufbauen
2. Technische und organisatorische Massnahmen implementieren
3. Mitarbeitende sensibilisieren und schulen
4. IT-Systeme und Netzwerke überprüfen lassen
5. Für den Notfall vorsorgen