So betreibt die Allianz IT-Governance

Jens Dose (CIO-Redakteur)

Ralf Schneider ist Group CIO der Allianz SE.
Foto: Allianz SE

"Das Management, IT-Management und besonders die Cybersecurity vieler Unternehmen haben einen blinden Fleck," sagt Ralf Schneider, CIO der Allianz SE. Die Verantwortlichen sähen nicht, dass sie einem hierarchischen Paradigma folgen, das nicht mehr mit der Digitalisierung mithalten könne.

Starre Strukturen seien zu langsam, um Cybersecurity effektiv zu betreiben. Durch den Geschwindigkeitsschub, den die Digitalisierung allen Unternehmensbereichen beschere, steige auch das Risiko, dass digitale Assets schneller angegriffen, manipuliert oder zerstört werden.

Auf der Handelsblatt Jahrestagung "Strategisches IT-Management" berichtete Schneider über die Governance-Maßnahmen der Allianz. Der Versicherer habe weltweit 150.000 Mitarbeiter, mehrere 100.000 Geschäftspartner, Millionen Kunden, 50.000 Server, 200.000 Workstations, sechs Rechenzentren und diverse Cloud-Instanzen. Hinzu kämen Anwendungen, Betriebssysteme, Firmware, APIs, Serverless-Funktionen, Machine-to-Machine-Verbindungen und vieles mehr. Das alles müsse geschützt werden.

Bei so vielen Teilen könnten IT-Verantwortliche zwar schnell einschreiten, wenn etwas falsch laufe. Das Systemverhalten zentralisiert vorherzusagen, sei aber nicht mehr möglich. Schneider setzt daher auf Selbstorganisation, -regulierung und -steuerung - zusammengefasst im Begriff der "Kybernetik". Den Rahmen dafür bildet die "kybernetische Governance" des Versicherers.

Drei Governance-Bausteine

Der Allianz-CIO setzt auf einen Dreiklang aus Policy, Steuerung und Menschen:

Die **Policy** ist die gemeinsame Sprache im Konzern. Sie definiert keine Regeln, sondern Prinzipien, wie IT und Sicherheit im gesamten Konzern umgesetzt werden sollen. Diese Prinzipien wurden in sogenannte Controls übersetzt. Diese orientieren sich an den regulatorischen Vorgaben und beschreiben, wie IT sicher aufgebaut, betrieben und weiterentwickelt werden soll. Daraus leitet sich das Architektur- und Risikomanagement ab. Alles zu Security auf CIO.de

Alle 60 Fachbereichs-Vorstände weltweit und ihre Mitarbeiter müssen sich an dieses Schriftstück halten. Sie sind dafür verantwortlich, die Controls umzusetzen und deren Wirksamkeit zu messen. Der Governance-Bereich prüft über Compliance-Berichte, ob das passiert.

Daran anschließend hat Schneider ein **Steuerungsmodell** etabliert. Es beschreibt, wie CIOs und Security-Verantwortliche handeln sollten, um wirksame Sicherheitsmaßnahmen zu ergreifen und Angriffe abzuwehren. "Die zunehmende Komplexität der IT-Landschaft lässt sich nicht mehr in einem Eins-zu-eins-Modell abbilden. Daher greifen wir auf dieses Modell zurück," so Schneider.

Das funktioniert über ein IT-Security-Dashboard. Es führt zehn "Gesundheitsindikatoren" auf, die für jede Ländergesellschaft in Echtzeit überprüft werden. Darin ist etwa festgehalten, wie viele "toxische Komponenten", die veraltet sind und nicht mehr gepatcht werden können, betrieben werden. Davon ausgehend ergreifen die Verantwortlichen passende Schutzmaßnahmen.

Der dritte Governance-Faktor ist für Schneider der **Mensch**. Mitarbeiterinnen und Mitarbeiter erarbeiten beispielsweise, wie das Steuerungsmodell am besten umgesetzt werden kann und passen die Maßnahmen an. Die Steuerung und Verwaltung der Maßnahmen sind weitgehend automatisiert.

Dazu müsse die Belegschaft zum einen die notwendigen Tools kennen und beherrschen. Zum anderen sei es wichtig, dass die Zusammenarbeit mit Kollegen wie etwa Risikoanalysten klappt. Dazu setzt der CIO auf Schulungen und Trainings.

Integration

Um das Governance-Modell einzuführen, setzte Schneider auf den "Syntegration"-Asnatz von Managementberater Fredmund Malik. Demnach wird das notwendige Wissen über Schlüsselpersonen in die einzelnen Bereiche getragen und verbreitet.

Jedes Vorstandsmitglied muss einen IT-Compliance-Bericht unterschreiben, um zuzusichern, dass die rund 150 Compliance-Controls in dem jeweiligen Bereich eingehalten werden. Zudem wird automatisiert überprüft, ob diese Kontrollmechanismen aus dem Compliance-Statement auch tatsächlich effektiv implementiert sind.

Quelle: https://www.cio.de/a/so-betreibt-die-allianz-it-governance,3677634