PwC Whitepaper

Die neue Rolle des CISO -

“Vom Verwalter zum Gestalter”

Maßnahme I

Die Rolle der CISOs: glaubwürdig, vertrauensvoll und umsetzungsstark

Wenn CISOs versuchen, eine neue Sicherheitskultur in Organisationen einzuführen, müssen sie die Bedeutung und deren Einfluss unternehmensspezifisch verstehen. Da diese Informationssicherheitsfunktion innerhalb der Organisationen an Größe und Umfang zunimmt, müssen CISOs gleichermaßen das Vertrauen ihrer Vorstände bzw. Geschäftsführer gleichzeitig aber auch das der Mitarbeiter gewinnen. Auf diese Weise können CISOs die Maßnahmen dieser Stakeholder zur proaktiven Minderung von Sicherheitsvorfällen „beeinflussen“ und sie gleichermaßen überzeugen, den Maßnahmen von CISOs im Umgang mit geschäftskritischen Vorfällen zu vertrauen.

Da CISOs kontinuierlich an Bedeutung für die Unternehmensleitung gewinnen und ihnen eine stetig größer werdende Rechenschaftspflicht auf Vorstandsebene zukommt, ist es darüber hinaus sehr wichtig, ihre mögliche Nachfolge und Stellvertretung zu planen, um die Kontinuität der Informationssicherheitsfunktion jederzeit zu gewährleisten. Auch ist die organisatorische Eingliederung der CISO-Rolle zu überdenken. Ein CISO, der dem IT-Leiter berichtet, kann nur schwer über die IT hinaus agieren und gestalten. Cybersecurity ist definitiv nicht nur auf IT Security beschränkt.

Das können Sie als CISO konkret tun:

- Streben Sie mit den unterschiedlichen Geschäftsbereichen ein gemeinsames Verständnis in Bezug auf Informationssicherheit-Standards und -Verfahren an.
- Verdienen Sie sich das Vertrauen Ihrer Unternehmensleitung durch glaubwürdige und regelmäßige Berichterstattung von Leistungskennzahlen.
- Setzen Sie auf ein starkes Führungsteam unter der CISO Rolle, dem Sie vertrauen können und das Ihnen eine entsprechende Nachfolgeregelung und Stellvertretung ermöglicht.

Maßnahme II

Die Beschleunigung der digitalen Transformation ist die größte Chance und zugleich die größte Gefahr für CISOs

Derzeit richten Unternehmen ihre Initiativen zur digitalen Transformation neu aus, um ihr Kernbusiness auch zukünftig zu ermöglichen. Aufgrund dieser schnellen Verfolgung digitaler Initiativen müssen CISOs ihre traditionellen Ansätze für das Sicherheits-, Risiko- und Compliance-Management erweitern, um sie an den Geschäftsbetrieb des nächsten „Normalfalls“ anzupassen. Während ein automatisierterer, agilerer und kollaborativerer Ansatz ein Muss ist, um Cyber--Risiko- und Compliance-Probleme zu vermeiden, müssen CISOs auch die sich nun bietende Gelegenheit nutzen, um eine standardisiertere und strengere Sicherheitskultur innerhalb von Organisationen zu entwickeln.

Das können Sie als CISO konkret tun:

- Etablieren Sie eine kontinuierliche Bewertung der Risiko- und Sicherheitslage, anstatt der weit verbreiteten anlassbezogenen Bewertung.
- Integrieren Sie Informationssicherheit in den traditionellen Ansatz des Informationsaustauschs innerhalb der Organisation, um sowohl Vertrauen als auch einfachen Austausch zu ermöglichen.
- Beschleunigen Sie die Identifikation und Einführung von Sicherheitstechnologien, um das Geschäftsmodell zu sichern.

Maßnahme III

Das Vertrauen der Kunden: ein kostbares Gut, das der CISO bewahren muss

Automatisierung, Künstliche Intelligenz (KI), Machine Learning (ML) und Internet of Things (IoT) ermöglichen es heute Unternehmen, ein individuelles Kundenerlebnis zu bieten, das ihre Fähigkeit, Kunden zu gewinnen und zu binden, erheblich beeinflussen kann. Kundenvertrauen ist auf lange Sicht der größte strategische Vorteil.
Es gibt jedoch auch eine entsprechende Kehrseite dazu: Die enormen Datenmengen, die diese neuen Technologien benötigen, um optimal zu funktionieren, erweitern kontinuierlich die Angriffsfläche und setzen das Unternehmen konstant neuen Cyberangriffen und neuen Bedrohungsvektoren aus. Daher ist es essenziell, dass ein CISO diese dynamischen Bedrohungsfelder versteht.

Das können Sie als CISO konkret tun:

- Investieren Sie in eine hochmoderne (state-of-the-art) Infrastruktur zur Identifikation bzw. Verwaltung von Bedrohungen (Threat Intelligence).
- Erzwingen Sie einen Security-by-Design-Ansatz für technologische Implementierungen bzw. deren Einsatz.
- Bewerten Sie die Notwendigkeit Anwendungen und Sicherheitsprozesse neu zu evaluieren
- Stimmen Sie Ihre Fähigkeiten, Arbeitskräfte und Automatisierungsanforderungen auf die neuen Technologien ab.

Maßnahme IV

Abwägen alter und neuer Paradigmen der Technologie-entwicklung und -Implementierung

Während Unternehmen neuere Technologieplattformen rund um Infrastruktur als Service (IaaS) und Software als Service (SaaS) einsetzen, sollten die Altinvestitionen nicht an Wert und Bedeutung verlieren. Ein CISO muss einen doppelten Ansatz verfolgen, um sicherzustellen, dass Methoden zur Behebung und Minderung von Cybervorfällen sowohl neue als auch alte Technologieparadigmen gleichermaßen abdecken können. Anhaltende Sicherheitslücken in älteren Systemen, ältere Software-Update-Methoden und inkonsistente Patch-Versionen sind einige der größten Sicherheitsbedrohungen für Unternehmen. Ein CISO muss effektiv mit den Geschäfts- und Technologiefunktionen zusammenarbeiten, um die Nutzung und Implementierung alter und neuer Technologien in Einklang zu bringen und sicherzustellen, dass die Koexistenz beider nicht zu einer Schwäche wird.

Das können Sie als CISO konkret tun:

- Erstellen und verwalten Sie ein vollständiges Inventar von Cyber-Assets und -Prozessen, sowie deren Verknüpfungen mit bekannten Bedrohungen und Schwachstellen.
- Erheben Sie die Akzeptanz von Geschäftsrisiken beim Einsatz veralteter Technologien.
- Quantifizieren Sie Cyberrisiken, um die geschäftlichen Auswirkungen von Sicherheitslücken durch ältere Software aufzuzeigen.

Maßnahme V

Ausrichtung der Cyberziele und -Investitionen auf die Geschäftsziele

Die Fähigkeit, die richtigen Investitionspriorität auszuwählen und ihre geschäftlichen Auswirkungen zu rechtfertigen, ermöglicht es CISOs zukünftige Investitionen zu sichern und ihren Wert auf Management- und Vorstandsebene zu demonstrieren. CISOs müssen mit der gesamten Organisation zusammenarbeiten, um die traditionelle Methode zur Planung und Durchführung von Cyberinvestitionen zu überdenken.

Ein Top-Down-Ansatz bei der Durchführung einer Analyse der Geschäftsauswirkungen (BIA) als integraler Bestandteil der Konzeption und Implementierung einer Cyberstrategie sowie eine effektive Kommunikation der Auswirkungen an die Geschäftsleitung ist ein Muss für den „New-Age CISO“. Wenn CISOs beispielsweise Strategien in Bezug auf Notfallwiederherstellung und Krisenmanagement in dieser neuen Ära verteilter Arbeitskräfte und Daten überdenken, ist es wichtig, dass die Geschäftsprioritäten, Kontinuitäts- und Wiederherstellungspläne für das reibungslose Funktionieren des Unternehmens aufeinander abgestimmt sind.

Das können Sie als CISO konkret tun:

- Identifizieren und verstehen Sie die Geschäftsstrategien und ihre nachgelagerten Auswirkungen.
- Vereinfachen und kommunizieren Sie die Sicherheitstechnologie, die die Geschäftsleitung hinsichtlich der Auswirkungen auf das Geschäft verlangt.
- Investieren Sie in die Einführung eine kontinuierlichen Sicherheitsbewusstseins (Awareness) der Organisation.

Innovation und Transformation von Geschäftsmodellen: die Sicherheit darf dabei nicht in den Hintergrund rücken

Sicherheit von z.B. Kundendaten und Vertrauen in das Unternehmen)sind heute genauso essenziell wie eine individuelle Customer Experience.

Sicherheit wird heute als integraler Bestandteil jeder technologiegestützten Fertigkeit angesehen.

Dies ist der wesentliche Paradigmenwechsel, da Sicherheit vor einigen Jahren noch als Hindernis angesehen wurde.

Daher müssen CISOs von ihrem derzeitigen verwaltungsorientierten und reaktiven Compliance-Ansatz zu einem gestaltenden proaktiven Business-First-Ansatz übergehen.

Ihre Ansprechpartner

Haben wir Ihr Interesse geweckt? Oder haben Sie dazu noch Fragen?
Dann rufen Sie uns an oder schreiben Sie uns – wir nehmen uns gerne Zeit für Sie:

Georg Beham
Partner
Cybersecurity & Privacy Leader
Tel: +43 732 611750
georg.beham@pwc.com

Erik Rusek
Senior Manager
Cybersecurity & Privacy
Tel: +43 732 611750 4075
erik.rusek@pwc.com

PwC Österreich
Donau-City-Straße 7
1220 Wien

www.pwc.at