»Technik allein hält keinen Angriff auf«

NIS2 und Cyber Resilience Act verschärfen die Anforderungen an Unternehmen deutlich. Cyber Compliance wird damit endgültig zur Führungsaufgabe. Im Gespräch mit den drei Sompo-Experten René Ehlen, Björn Fehre und Maximilian Seidel wird deutlich, warum im Ernstfall Governance, Lieferkettensteuerung und trainierte Abläufe oft wichtiger sind als Technologie allein.

René Ehlen
Head of Cyber & Financial Lines, Insurance, Germany & Austria

Björn Fehre
Head of Claims, Insurance, Germany & Austria

Maximilian Seidel
Cyber Risk Specialist, Insurance, Continental Europe

v.l.n.r.: René Ehlen, Head of Cyber & Financial Lines, Germany & Austria, Malte Dittmann, Country Manager Germany & Austria, und Christian Kruppa, Head of Distribution & Client Relationship Management, Germany & Austria

»Cyber ist fast nie nur ein IT-Schaden. Es geht zugleich um Betriebsunterbrechung, regulatorische Fristen, Kommunikationsfähigkeit, Haftungsfragen und Reputationsrisiken.

Im Cyber-Ernstfall zeigt sich schnell, ob ein Unternehmen vorbereitet ist. Wer übernimmt die Führung? Wer entscheidet? Wer kommuniziert? Oft sind es genau diese Fragen, die in den ersten Stunden über das Ausmaß des Schadens mitentscheiden.

»Technik allein hält keinen Angriff auf«, sagt Björn Fehre, Head of Claims, Insurance, Germany & Austria bei Sompo. Der Satz bringt auf den Punkt, was die Schadenpraxis seit Jahren zeigt: Selbst gut ausgestattete Unternehmen geraten unter Druck, wenn Zuständigkeiten unklar sind, Krisenabläufe nicht eingeübt wurden oder Entscheidungen unter Zeitdruck ins Stocken geraten. »Die ersten Stunden sind entscheidend«, so Fehre. Umgekehrt kommen Unternehmen mit vergleichbarer technischer Ausstattung oft deutlich robuster durch einen Vorfall, wenn Organisation, Kommunikation und Wiederanlaufpläne funktionieren.

Mit NIS2 und dem Cyber Resilience Act verschärft sich diese Realität nun auch regulatorisch. Cybersecurity wird damit endgültig aus der IT-Ecke herausgelöst und zur Managementaufgabe. »Der größte Handlungsdruck liegt aus meiner Sicht in Governance, Lieferkettensteuerung und Nachweisfähigkeit«, sagt René Ehlen, Head of Cyber & Financial Lines, Insurance, Germany & Austria bei Sompo. Viele Unternehmen hätten Cyberrisiken in der Vergangenheit vor allem als IT- oder Informationssicherheitsthema behandelt. »Regulatorisch greift das nicht mehr. Cyber ist heute eine Frage der Unternehmenssteuerung.«

Wenn Cyber zur Chefsache wird

Für Vorstände und Geschäftsführerinnen und Geschäftsführer bedeutet das einen klaren Rollenwechsel. Es reicht nicht mehr, Budgets freizugeben und die operative Verantwortung an Fachabteilungen zu delegieren. Gefordert ist ein belastbares Bild darüber, welche kritischen Prozesse digital abhängig sind, wo die wesentlichen Bedrohungen liegen und wie widerstandsfähig das Unternehmen einschließlich seiner Dienstleister und Lieferketten tatsächlich ist. »Es geht nicht um absolute Sicherheit«, sagt Ehlen. »Aber es geht um eine angemessene Organisation und ein belastbares Überwachungssystem.«

Damit rückt auch die persönliche Verantwortung stärker in den Fokus. Nicht jeder Cybervorfall führt automatisch zu Haftung. Wohl aber steigt der Maßstab dafür, was als angemessene Unternehmensorganisation gilt. Besonders kritisch wird es dort, wo bekannte Schwachstellen über längere Zeit nicht adressiert, Warnsignale ignoriert oder Vorfälle organisatorisch nicht beherrscht werden.

Hinzu kommt ein Risikofeld, das viele Unternehmen noch immer unterschätzen: die Lieferkette. Die eigene Angriffsfläche endet längst nicht an der Unternehmensgrenze. IT-Dienstleister, Softwareanbieter, externe Service-Provider oder OT-Partner sind oft tief in die Betriebsabläufe eingebunden. »Viele Unternehmen schauen beim Thema Cyber noch stark auf interne Maßnahmen«, sagt Ehlen. »Weniger im Fokus stehen oft Abhängigkeiten, Konzentrationsrisiken und die Qualität von Zulieferern und Dienstleistern.« Gerade im Krisenfall zeigt sich, wie kritisch diese Abhängigkeiten sind: Wenn ein externer Dienstleister kompromittiert ist oder ein Produktionsstandort auf externe IT-Dienstleistungen angewiesen ist, wird aus einem IT-Vorfall schnell eine operative Krise.

Versicherbarkeit beginnt vor dem Schadenfall

Für die Versicherungswirtschaft hat das spürbare Folgen. Cyberversicherung ist heute weit mehr als finanzielle Absicherung im Ernstfall. »Das greift zu kurz«, sagt Ehlen. »Regulatorik verlangt heute nicht nur Reaktion, sondern Prävention, Resilienz, Governance und Nachweisbarkeit.« Versicherung funktioniere dauerhaft nur dann, wenn Risiken in einem gewissen Maß beherrschbar seien. Deshalb übersetzt Sompo regulatorische Anforderungen zunehmend in konkrete Underwriting-Kriterien.

Im Kern geht es um drei Fragen: Wie wahrscheinlich ist ein Schaden? Wie schwer könnte er ausfallen? Und wie beherrscht ist das Risiko insgesamt? Technische Mindestkontrollen wie z. B. Multi-Faktor-Authentifizierung, Patch-Management oder E-Mail-Sicherheit bleiben wichtig. Doch zunehmend zählt das Gesamtbild: Ist Cyber-Governance auf Leitungsebene verankert? Gibt es belastbare Incident-Response-Prozesse? Sind Wiederanlaufpläne getestet? Ist das Management von Drittparteien strukturiert und nachweisbar? »Der Markt entwickelt sich weg von der punktuellen Abfrage einzelner Controls hin zur Bewertung des gesamten Cybersteuerungsmodells«, sagt Ehlen.

Wo Unternehmen besonders anfällig bleiben

Wo in der Praxis besonders häufig Schwachstellen liegen, erlebt Maximilian Seidel, Cyber Risk Specialist, Insurance, Continental Europe bei Sompo, regelmäßig in Risk-Assessments. Handlungsbedarf sieht er vor allem im Business-Continuity-Management und im Third-Party-Risk-Management. »NIS2 fordert ein umfassenderes Risikomanagement der Lieferanten«, sagt Seidel. Während Sicherheitsanforderungen früher oft nur bei neuen Verträgen oder in einmaligen Prüfungen berücksichtigt wurden, gehe es heute um kontinuierliche Bewertungen und belastbare vertragliche Standards.

Auch das Schwachstellen- und Patch-Management bleibe ein zentrales Thema – gerade weil sich die Bedrohungslage dynamisch weiterentwickelt und künstliche Intelligenz Angriffe zusätzlich beschleunigen kann. Gleichzeitig arbeiten viele Unternehmen in historisch gewachsenen IT- und Produktionslandschaften. Die Herausforderung besteht dann nicht im idealtypischen Neustart, sondern in der realistischen Härtung bestehender Strukturen. Seidel beobachtet zudem, dass Unternehmen mit Standorten in Deutschland oder der EU, aber Hauptsitz im Ausland, die Relevanz von NIS2 teils noch unterschätzen.

Im Ernstfall zählt das Zusammenspiel

Wie stark sich organisatorische Defizite im Ernstfall auswirken, zeigt sich im Schaden. »Es ist selten die Technik, an der Cyberresilienz scheitert«, sagt Fehre. »Häufiger fehlt ein belastbares Konzept – oder es existiert nur auf dem Papier.« Die entscheidenden Fragen seien im Vorfall oft erstaunlich basal: Wer beruft den Krisenstab ein? Wer entscheidet über einen Produktionsstopp? Wer spricht mit der Kundschaft, den Behörden, den IT-Forensikerinnen und -Forensikern oder dem Versicherer? Unklare Verantwortlichkeiten und falsche Reaktionen könnten die Folgen eines Cyberangriffs zusätzlich verschärfen und die Schäden deutlich erhöhen.

Denn Cyber ist fast nie nur ein IT-Schaden. Es geht zugleich um Betriebsunterbrechung, regulatorische Fristen, Kommunikationsfähigkeit, Haftungsfragen und Reputationsrisiken. Wenn etwa ein Werk vorsorglich stillsteht, weil nicht klar ist, ob Systeme sicher weiterlaufen können, Liefertermine reißen und Kunden keine belastbare Information erhalten, wird aus einem technischen Angriff binnen Stunden ein unternehmensweiter Krisenfall. Wie belastend und langwierig solche Situationen für Unternehmen sind, zeige sich immer wieder: Nach einem schweren Angriff dauert es oft lange, bis Betriebe organisatorisch und operativ wieder vollständig auf die Beine kommen. Genau deshalb muss Reaktionsfähigkeit ebenso konsequent trainiert werden wie Prävention. Fehres Empfehlung ist entsprechend klar: Vorfälle üben, Back-ups realistisch testen, Incident-Response-Pläne nicht nur dokumentieren, sondern kennen, externe Ansprechpartner vorab kennen. »Nicht nur in Prävention investieren, sondern mindestens genauso konsequent in Reaktionsfähigkeit.«

Wie Sompo Underwriting, Risk-Engineering und Claims verzahnt

Die zentrale Botschaft ist klar: Cyber Compliance ist kein Projekt der IT-Abteilung mehr. Sie ist Teil wirksamer Unternehmensführung. Wer regulatorisch belastbar, versicherbar und im Ernstfall handlungsfähig sein will, braucht mehr als gute Technologie: klare Verantwortlichkeiten, belastbare Prozesse, Transparenz über Abhängigkeiten und den Nachweis, dass all das auch unter Druck funktioniert.

Sompo setzt dabei auf ein Modell, in dem Underwriting, Risk-Engineering und Claims eng zusammenarbeiten. Erkenntnisse aus realen Vorfällen fließen in Risikobewertung und Prävention zurück; technische Analysen helfen, operative Schwachstellen früh sichtbar zu machen.

»Wir sind als Schadenexperten meist schon beim ersten Treffen mit dem Kunden dabei«, sagt Björn Fehre. »Uns ist es wichtig, persönlich aufzutreten und unsere Expertise schon zu Beginn einer Partnerschaft mit ins Spiel zu bringen.« Diese enge Verzahnung zählt auch im Schadenfall – von Forensik über Rechtsberatung bis Krisenkommunikation.

So schließt sich der Kreis: Resilienz entsteht weder in technischen Silos noch erst im Schadenfall. Sie entsteht dort, wo Menschen, Funktionen und Entscheidungen ineinandergreifen – im Unternehmen selbst ebenso wie in der Zusammenarbeit mit dem Versicherer.

Weitere Informationen unter:
sompo-intl.com

SOMPO