Top-down Cyber-Risk-Assessment by HiSolutions

Konzernweite Steuerung des Cyberrisikos bei innogy

Die Bestimmung des unternehmensweiten Cyberrisikos ist eine wichtige Voraussetzung für eine ganzheitliche Bewertung und globale Steuerung, um die Verteidigung verbessern und den Ressourceneinsatz optimieren zu können. HiSolutions hat mit innogy ein Top-down Cyber-Risk-Assessment-Vorgehen entwickelt, das einen aktuellen, zentralen und aggregierten Überblick über den gesamten Konzern inklusive aller Töchter ermöglicht und so als wertvoller Input für die Cybersicherheitsstrategie dient.

Von David Fuhr, HiSolutions AG und Thomas Krauhausen, innogy SE

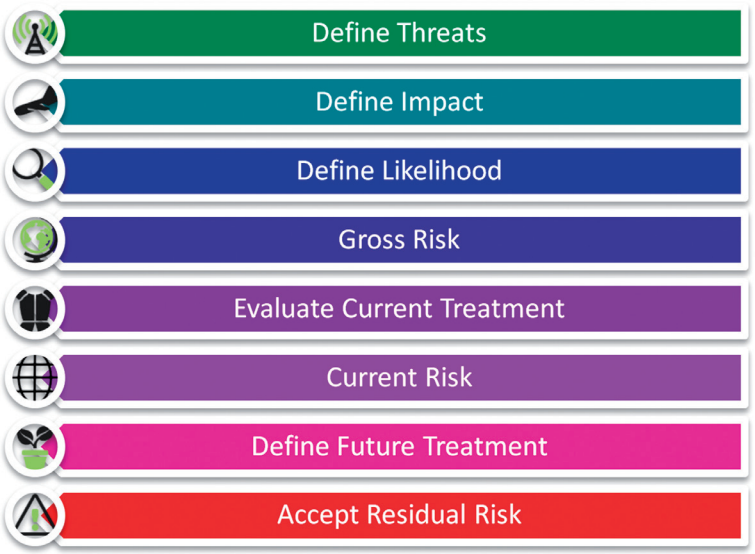
Die stetig zunehmende IT-Bedrohungslage lässt die Steuerung von Cyberrisiken immer wichtiger werden. Viele Unternehmen verfügen bereits über Methoden, um Schutzbedarf, Business Impact oder Restrisiken bestimmter Assets – einer Anwendung, einer Datenbank, eines Rechenzentrums – zu bewerten. Sehr häufig jedoch fließen die verschiedenen Ansätze, Skalen und Methoden nicht in ein kohärentes Gesamtbild ein. Es fehlt in der Regel ein konzernweiter, einheitlicher Blick auf das Cyberrisiko. Ein solcher wird jedoch heute zunehmend von Aufsichtsgremien, Regulierern, Wirtschaftsprüfern oder auch von externen Partnern wie etwa Cyberversicherern verlangt. Vor allem aber besteht ohne ein zentrales Cyber-Risk-Assessment die Gefahr, dass Ressourcen falsch allokiert werden oder nicht schlüssig begründet werden können.

Für die innogy SE ist das Thema Cybersicherheit eines der zentralen, um die Zukunftssicherheit der Netze und erneuerbaren Energien für 23 Millionen Kunden in Europa sicherzustellen. innogy ist das führende deutsche Energieunternehmen mit einem Umsatz von rund 44 Milliarden Euro (2016), mehr als 40 000 Mitarbeitern und Aktivitäten in 16 europäischen Ländern. Informationssicherheit hat für innogy von Beginn an Priorität. So wurde etwa neben dem großflächigen Ausrollen von Informationssicherheitsmanagement (ISM) und der erfolgreichen externen Zertifizierung nach IT-Sicherheitsgesetz und Sicherheitskatalog der Bundesnetzagentur auch ein Projekt zur Bestimmung des Umsetzungs- und Reifegrades der ISO 27001 durch die Konzernsicherheit der innogy entwickelt.

Cyber-Risk-Assessment

Was bisher noch fehlte, war eine zentrale, aggregierte und operationalisierbare Sicht auf das Cyberrisiko in allen Bereichen des Konzerns inklusive der Töchter. Zu dem Zweck haben innogy und HiSolutions gemeinsam eine szenariobasierte Methodik für ein Cyber-Risk-Assessment entwickelt und durchgeführt, als deren Herzstück Interviews mit den Top-50-Risikoträgern im Konzern fungierten. Darüber hinaus flossen Risiko- und Assetbewertungen aus unterschiedlichen Quellen in die automatisierte Aggregation und Bewertung mit ein. Die Cybersecurity-Experten der in-

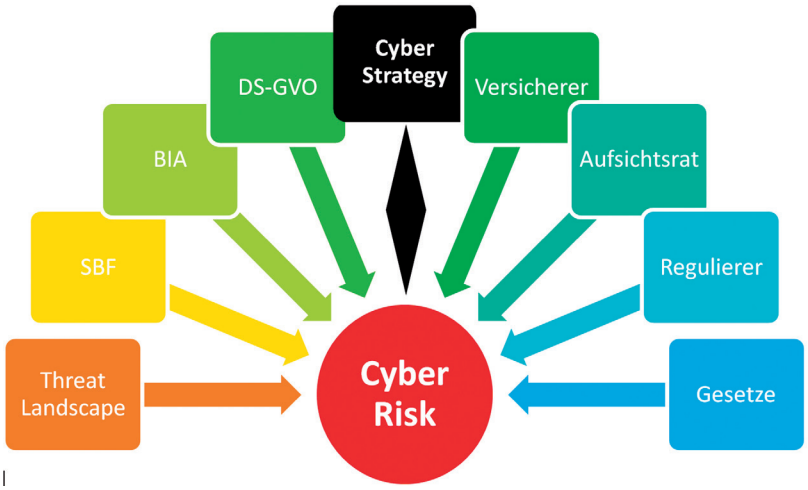
„Durch das Cyber-Risk-Assessment schaffen wir bei unseren Führungskräften die erforderliche Transparenz über die wesentlichen Cyberrisiken und unterstützen so direkt die Digitalisierungsstrategie unseres Konzerns. Zusammen mit unserer tool-basierten Reifegradmessung bildet es die Grundlage unserer Cyber-Sicherheitsstrategie." – Florian Haacke, CSO, innogy SE



nogy Konzernsicherheit bewerteten daraufhin als zentralen Arbeitsschritt die Eintrittswahrscheinlichkeit wesentlicher Gefährdungsszenarien – auch auf der Basis der Erkenntnisse bereits durchgeführter Sicherheitsprojekte. Die Analyse mündete in einer automatischen Auswertung und Darstellung nach Schutzziel, Risikotyp, Segment, Land, Sparte, IT-Dienstleister et cetera. Als Besonderheit wurde zusätzlich auch die Verteilung der Datenschutzrisiken nach DS-GVO im Konzern ermittelt und dargestellt. Das Management-taugliche Reporting für die Stakeholdergremien wurde ebenfalls teilautomatisiert, ohne die Notwendigkeit teurer spezieller Softwarelösungen.

Cyber-Strategie

Klassischerweise wurde IT-Security vor allem bottom-up aus der IT heraus angegangen. Zwar schreiben Standards wie ISO 27001 oder IT-Grundschutz eine Verankerung des Sicherheitsprozesses in der Leitungsebene vor, die geeignete und ausreichende Ressourcen bereitzustellen hat. Gelegentlich wird auch eine Integration von IT-Risiken in das Enterprise Risk Management angestrebt. In aller Regel wird jedoch die IT-Sicherheit traditionell weiterhin von „unten“ betrieben. Dies macht es aufwendig, IT-Risiken global und gleichzeitig agil zu steuern – und die effektive Unterstützung der Geschäftsziele durch das Sicherheitskonzept zum Glücksspiel. Die übliche Folge: Die Security wird ausschließlich als Bremserin wahrgenommen; um Budget muss gerungen werden und höchstens nach Vorfällen herrscht kurzfristiger Aktionismus, der nicht nachhaltig ist. Reine Lippenbekenntnisse von „Management Commitment“ und „Security als Enabler“ allein helfen hier nicht weiter.



Das Cyber-Risk-Assessment benötigt vielerlei Input und dient als Basis einer erfolgreichen Cyberstrategie.

Vielmehr muss Cyber-Security in Form einer Cyber-Sicherheitsstrategie integraler Teil der Unternehmensstrategie werden, um optimal zum Geschäftserfolg beitragen zu können. Das Cyber-Risk-Assessment bei innogy liefert hierzu die ideale Basis. ■

Die HiSolutions-Risikobewertungs-Methodik

Klassisch wird Risiko definiert als Eintrittswahrscheinlichkeit x Schadenshöhe (Worst Case) in den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit. HiSolutions nimmt weitere Dimensionen in den Blick, um ein realistischeres Ergebnis mit höherer Aussagekraft zu erhalten:

_____ Schutzziele sind nicht unabhängig voneinander: Höhere Verfügbarkeit etwa kann die Vertraulichkeit gefährden und umgekehrt. Die Vertraulichkeit von Kryptoschlüsseln etwa sichert die Integrität von Nutzdaten. Dies ist in die Berechnung und Behandlung systematisch einzubeziehen.

_____ Assets sind in der Regel durch verschiedene Schadensszenarien mit unterschiedlichen Wahrscheinlichkeiten und Schäden bedroht, das Risiko somit nicht nur ein Produkt von zwei Zahlen, sondern eine Summe beziehungsweise ein Integral.

_____ Wahrscheinlichkeiten wie mögliche Schadenshöhen ändern sich zudem stetig. Das erfordert aktuelle Daten (möglichst in Echtzeit) als Entscheidungsgrundlage.

_____ Die Schadensbewertung hat selbst einen zeitlichen Aspekt: Klar ist, dass ein längerer Ausfall in der Regel teurer wird. Aber auch bei manipulierten Daten ist entscheidend, wann sie wieder benötigt werden und wie lange die Korrektur dauert.

_____ „Schwarze Schwäne“ – sehr unwahrscheinliche, teure Schadensereignisse – müssen aus der Betrachtung ausgeschlossen werden, da sonst die Berechnung beliebig wird. Das sollte bewusst und dokumentiert erfolgen.

_____ Unterschiedliche Organisationen (z. B. Tochterunternehmen), Organisationseinheiten und Stakeholder benötigen ggf. maßgeschneiderte Blicke (Auswertungen) der Risikolandschaft.

Das alles lässt sich nur abbilden in einem formelbasierten Risikomodell mit Auswertungsautomatisierung. Die Risikobewertungs-Methodik von HiSolutions erlaubt es, den Überblick über die Methode und über die Ergebnisse zu behalten.

Kontakt
HiSolutions AG
Bouchéstraße 12
12435 Berlin
www.hisolutions.com