Zwischen Regulierung und Realität

NIS-2 und DORA verlangen Transparenz

Viele Organisationen setzen Informationssicherheit mit der Anzahl ihrer Security-Tools gleich. Für die Anforderungen von NIS-2 und DORA reicht das nicht: Gefragt ist ein durchgängiges Lagebild, das den Sicherheitsstatus nachvollziehbar bewertbar macht.

Bild: vecstock/Magnific.com

Von Agnes Graf, AMPEG GmbH

Mit NIS-2 und dem Digital Operational Resilience Act (DORA) erreicht die europäische Cybersecurity-Regulierung eine neue Qualität. Beide Regelwerke formulieren klare Anforderungen an Risikomanagement, Resilienz und Berichtsfähigkeit. In vielen Organisationen folgt die Umsetzung jedoch einem wiederkehrenden Muster: Die Diskussion bleibt auf der Ebene von Compliance und Dokumentation, während die operative Sicherheitslage fragmentiert ist.

Dabei ist die eigentliche Botschaft beider Regelwerke deutlich weitreichender. Es geht nicht primär darum, zusätzliche Richtlinien zu erfüllen oder bestehende Prozesse zu dokumentieren. Es geht darum, jederzeit in der Lage zu sein, den eigenen Sicherheitsstatus realistisch zu bewerten, Risiken frühzeitig zu erkennen und fundierte Entscheidungen zu treffen – auf operativer wie auf Managementebene.

Viele Tools, wenig Gesamtbild

Genau hier liegt in der Praxis die größte Herausforderung. Viele Unternehmen verfügen heute über eine Vielzahl spezialisierter Security-Tools: Endpoint-Detection-and-Response-(EDR)-Lösungen, Schwachstellenmanagement, Patch-Management, Netzwerküberwachung. Jedes dieser Systeme liefert wertvolle Informationen – aber immer nur im eigenen Kontext. Was fehlt, ist das übergreifende Lagebild, um das tatsächlich erreichte Sicherheitsniveau zu bewerten.

So entstehen typische Symptome moderner IT-Sicherheitslandschaften: eine hohe Anzahl an anwendungsbezogenen Dashboards, widersprüchliche Kennzahlen, iso-

lierte Risikobetrachtungen. Für technische Teams bedeutet es einen erheblichen Mehraufwand, ein übergreifendes Lagebild zu erstellen. Für das Management entsteht ein noch größeres Problem: Entscheidungen müssen getroffen werden, ohne dass ein belastbares Gesamtbild vorliegt.

NIS-2 und DORA adressieren genau diesen Punkt – indirekt, aber sehr klar. Beide Regelwerke fordern kontinuierliche Risikobewertung, nachvollziehbare Steuerung und eine klare Verantwortlichkeit auf Leitungsebene. Besonders DORA macht deutlich: Auch ausgelagerte IT-Services entbinden nicht von der Verantwortung. Die Resilienz muss jederzeit messbar, überprüfbar und steuerbar sein.

Das lässt sich nicht allein über Prozesse mit veralteten Reports abbilden. Erforderlich ist ein durchgängiges, aktuelles Lagebild der gesamten IT- und Sicherheitslandschaft. Eines, das nicht nur technische Details aggregiert, sondern diese in eine Form übersetzt, die steuerungsrelevant ist: verständlich, vergleichbar und priorisierbar.

Einzelindikatoren führen in die Irre

In diesem Kontext gewinnt ein Aspekt zunehmend an Bedeutung, der in vielen Diskussionen noch unterschätzt wird: die Fähigkeit zur objektiven Bewertung. Sicherheitsentscheidungen basieren häufig auf Einzelindikatoren – etwa der Anzahl offener Schwachstellen oder dem Patch-Status bestimmter Systeme. Doch diese Kennzahlen sind isoliert nur begrenzt aussagekräftig. Erst im Zusammenspiel verschiedener Faktoren entsteht ein realistisches Bild des tatsächlichen Risikos.

Ein nicht gepatchtes System in einem isolierten Netzwerk ist anders zu bewerten als ein vergleichbares System mit direkter Internetanbindung und zusätzlichen Konfigurationsschwächen. Ohne kontextuelle Einordnung bleiben solche Unterschiede unsichtbar. Die Aufgabe besteht also nicht nur darin, Daten zu sammeln, sondern sie sinnvoll zu korrelieren und daraus belastbare Aussagen abzuleiten.

In vielen Organisationen verschiebt sich deswegen der Fokus derzeit weg von der reinen Tool-Perspektive hin zu einem übergreifenden Verständnis der eigenen Sicherheitslage. Relevant ist dieser Ansatz auch im Kontext von „Security made in Germany“. Denn neben technologischen Fähigkeiten rücken Aspekte wie Datensouveränität, Nachvollziehbarkeit und Kontrollierbarkeit stärker in den Vordergrund. Gerade in einem kritischen Umfeld stellt sich zunehmend die Frage, wo sicherheitsrelevante Daten verarbeitet werden, wie transparent die zugrunde liegenden Bewertungsmechanismen sind und in welchem Maß Organisationen die Kontrolle über ihre eigenen Sicherheitsprozesse behalten. On-Premises-Ansätze oder hybride Modelle gewinnen in diesem Zusammenhang wieder an Bedeutung – nicht als Gegenmodell zur Cloud, sondern als bewusste Entscheidung für unabhängige Steuerbarkeit und Transparenz.

Neue Prioritäten für CISOs

Für CISOs bedeutet das eine klare Verschiebung der Prioritäten. Die Frage ist nicht mehr, ob ausreichend Security-Tools vorhanden sind. Das ist in den meisten Fällen längst gegeben. Entscheidend ist vielmehr, ob mit dem Betrieb der Tools das erforderliche Sicherheitsniveau für das eigene Netzwerk erreicht wird. Abhilfe schaffen kann ein Lagebild, das nicht nur den Status beschreibt, sondern konkrete Handlungsoptionen aufzeigt. Das Lücken sichtbar macht. Eines, das es erlaubt, Schutzmaßnahmen gezielt zu steuern und deren Wirkung in einem stets aktuellen Security-Dashboard nachzuvollziehen.

Genau darin liegt der Kern von Resilienz im Sinne von NIS-2 und DORA: Sicherheit nicht über implementierte Tools als erledigt abzuhaken, sondern aktiv zu steuern. Ohne diese Transparenz bleibt Security-Management reaktiv; mit ihr wird es steuerbar. Oder anders formuliert: Ohne aktuelles Lagebild gleicht Security-Management einer Fahrt im Nebel – man hofft, dass die Richtung stimmt, weiß es aber nicht. ■

Bild: Vecstock / Vecteezy.com – KI-generiertes Ausgangsbild, redaktionell bearbeitet