Cybersicherheit und Compliance

Warum Excel und Word zum Haftungsrisiko werden

Viele Unternehmen setzen bei der Umsetzung von NIS2 und DORA zunächst auf Excel und Word – aus Gewohnheit, Kostengründen oder Pragmatismus. Für eine dauerhafte, revisionssichere Steuerung von Cyberrisiken reichen statische Office-Dokumente jedoch nicht aus. Warum das schnell zum Haftungsrisiko werden kann, zeigen fünf zent rale Schwachstellen im Umgang mit regulatorischen Anforderungen.

Die Idee ist naheliegend: Excel und Word kosten nichts extra, praktisch jeder im Unternehmen kann damit umgehen, und für eine erste Bestandsaufnahme sind sie schnell aufgesetzt. Doch was als pragmatischer Ansatz beginnt, entwickelt sich bei der dauerhaften Umsetzung von NIS2 oder DORA schnell zu einem unkalkulierbaren Risiko. Da Cybersicherheit durch die neuen regulatorischen Vorgaben endgültig zur Chefsache erklärt wurde – inklusive einer drohenden persönlichen Haftung der Geschäftsführung –, müssen Compliance-Prozesse auf einem soliden Fundament stehen.

Wer versucht, ein dynamisches Cybersicherheits-Niveau mit statischen Office-Dokumenten zu verwalten, stößt im Alltag unweigerlich auf fünf fundamentale Hürden.

1. Das »Version-Hell«-Dilemma: Aktualität bleibt auf der Strecke

Die NIS2-Verordnung zum Beispiel fordert kein einmaliges Projekt, sondern ein kontinuierliches Risikomanagement. In der Praxis kollidiert dieser Anspruch sofort mit der Natur von Excel-Tabellen. Da meist mehrere Abteilungen und Verantwortliche am Prozess beteiligt sind, entstehen unweigerlich lokale Kopien und mehrere Versionen kursieren parallel. Das Ergebnis: Intransparenz. Niemand kann am Ende verlässlich sagen, welche Version tatsächlich den aktuellen, realen Sicherheitszustand des Unternehmens abbildet. Geeignete Softwarelösungen nehmen diese Hürde, da sie dezentrale Dateien durch eine zentrale, relationale Datenbank ersetzen. Änderungen werden auf diesem Weg sofort für alle Beteiligten sichtbar.

2. Der Audit-GAU: Keine revisionssichere Dokumentation

Im Falle eines Audits durch Aufsichtsbehörden wie das BSI oder bei Sicherheitsüberprüfungen durch wichtige Kunden in der Lieferkette müssen Unternehmen lückenlose Nachweise erbringen. Hier stoßen Office-Dokumente an ihre Grenzen. Jede Zelle und jeder Textbaustein lassen sich rückwirkend verändern – ohne dass eine fälschungssichere, automatisierte Historie im Hintergrund mitschreibt. Für einen Auditor ist eine solche Tabelle somit kein revisionssicherer Nachweis oder gar ein Beweis für gelebte IT-Sicherheit. Eine passende Software schafft eine lückenlose Historisierung der Daten und loggt jede Änderung im Hintergrund mit. Damit schafft sie die erforderliche Revisionssicherheit.

3. Blindflug im Netzwerk: Starre Verknüpfungen statt dynamischer Abhängigkeiten

Ein funktionierendes Informationssicherheits-Managementsystem (ISMS) lebt von komplexen Beziehungen. Es muss transparent sein, welches IT-Asset an welchem kritischen Geschäftsprozess hängt, welche spezifische Maßnahme dieses Asset schützt und welche externen Lieferanten involviert sind. Solche mehrdimensionalen Abhängigkeiten lassen sich in flachen Excel-Strukturen kaum fehlerfrei abbilden. Ändert sich beispielsweise ein Risiko bei einem Zulieferer, müssten händisch dutzende Zellen über verschiedene Tabellenblätter hinweg aktualisiert werden. Fehler und blinde Flecken sind vorprogrammiert. Bei einer integrierten Softwarelösung liegen alle Assets, Bedrohungen, Schwachstellen und

Illustration: © magazinemaker.de, Microsoft


DOXA
WISSEN

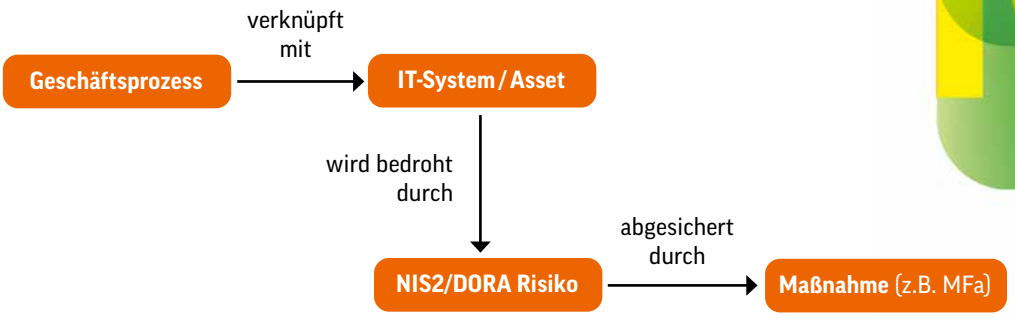

Abbildung: Sicherheitsprofile zeigt die Kreuzreferenzen zwischen den Bedrohungen die auf die Assets wirken zu deren risikominimierenden Maßnahmen.

Maßnahmen an einem einzigen Ort. Alles ist miteinander vernetzt und in webbasierten Ansichten nachvollziehbar.

4. Wettlauf gegen die Zeit: Das starre Reporting-Zeitfenster

Bei erheblichen Sicherheitsvorfällen gelten unter NIS2 und DORA strenge Fristen. Sie verlangen extrem schnelle Reaktionen – allen voran eine erste Meldung an die Behörden innerhalb von gerade einmal 24 Stunden, gefolgt von einem ausführlichen Bericht nach 72 Stunden. Wenn der dafür notwendige Notfallplan als statisches Word-Dokument irgendwo im Firmennetzwerk liegt, das im Ernstfall vielleicht gerade durch eine Ransomware-Attacke komplett verschlüsselt wurde, geht wertvolle Zeit verloren. Ein integriertes BCM mit Alarmierungs-, Melde- und Wiederanlaufplänen sorgt dafür, dass kritische Informationen auch im Krisenfall verfügbar bleiben.

5. Das Silo-Problem: Fehlendes Rollen- und Aufgabenmanagement

Compliance und Cybersicherheit sind Teamsache. NIS2 und DORA verlangen, dass Verantwortlichkeiten für technische Maßnahmen, regelmäßige Überprüfungen und Mitarbeiterschulungen glasklar zugewiesen und nachgehalten werden. Excel-Listen sind jedoch stumm – sie können keine automatischen Erinnerungen versenden, wenn eine Frist abläuft. Zudem fehlt Office-Dateien ein granulares Rechte- und Rollenkonzept. Es gibt meist nur die Wahl zwischen »Bearbeiten« oder »Schreibgeschützt«. Sensible Sicherheitsdaten erfordern jedoch ein präzises Berechtigungsmanagement, bei dem jeder Mitarbeiter nur das sieht und bearbeitet, was für seine Rolle relevant ist. Doch gerade in historisch gewachsenen IT-Landschaften gibt es häufig Insellösungen und unkoordinierte Workflows. Die Folge sind fehlende Übersicht, doppelte Arbeit und ein erhöhtes Risiko für regulatorische Lücken. Dadurch steigt nicht nur der Aufwand: Ohne durchgängige Strukturen wird echte NIS2- und DORA-Compliance praktisch kaum möglich. Auch hier bietet eine Tool-Lösung Abhilfe, denn sie steuert die Zusammenarbeit über ein integriertes Aufgaben- und Berechtigungsmanagement durch gezielte Zuweisung. Änderungen fließen nicht ungeprüft in den Gesamtbericht ein, sondern sie durchlaufen einen definierten Review-Prozess (etwa durch den CISO oder Risikomanager), bevor sie im Freigabeprozess als »gültig« markiert und in die Datenbank überführt werden.

NIS-2 und DORA softwarebasiert umsetzen. Wer Governance- und Sicherheitsprozesse softwarebasiert statt mit Excel und Word etabliert, schafft mehr Transparenz, effizientere Abläufe und kann interne Ressourcen gezielter einsetzen. Unternehmen reagieren dadurch schneller auf Risiken, reduzieren Ausfallzeiten und schaffen Vertrauen bei Kunden und Partnern. Das zeigt sich vor allem im Tagesgeschäft: Statt nur auf regulatorischen Druck zu reagieren, schaffen Unternehmen stabilere Abläufe und können neue Anforderungen deutlich schneller umsetzen.

In der Praxis geht es längst nicht mehr nur darum, einzelne Vorgaben abzuhaken. Unternehmen müssen Risiken konstant im Blick behalten und revisionssichere Nachweise jederzeit liefern können. Moderne GRC- und Compliance-Plattformen unterstützen Unternehmen dabei, NIS2- und DORA-Anforderungen strukturiert umzusetzen, Risiken frühzeitig zu erkennen und Nachweise jederzeit bereitzustellen. Das schafft Transparenz, reduziert Aufwand und erhöht die Reaktionsfähigkeit im Tagesgeschäft.

Silke Menzel ist Consultant bei HiScout und unterstützt Unternehmen in Business Continuity, Informationssicherheit, Compliance sowie Prozess- und Changemanagement. Als Agile Coach und Projektmanagerin begleitet sie Transformationsprozesse und stärkt effiziente, resiliente Organisationsstrukturen und die strukturierte Umsetzung von Sicherheits- und Compliance-Anforderungen.