Business Continuity Management mit modernen Tools

NIS2: Excel wird zum Risiko für Unternehmen und Geschäftsführer

Mit der Einführung der NIS2-Richtlinie stehen Unternehmen in der EU vor verschärften Anforderungen in der Cybersicherheit. Eine elementare Änderung: Durch NIS2 werden Geschäftsführer persönlich haftbar, falls die erforderlichen Maßnahmen nicht umgesetzt werden. Business Continuity Management (BCM) spielt nun eine entscheidende Rolle, denn es trägt maßgeblich zur Resilienz und Sicherheit von Unternehmen bei. Doch viele Unternehmen setzen noch auf veraltete Technologien wie Excel, was erhebliche Risiken birgt.

Jedes Unternehmen ist potenziellen Bedrohungen wie Cyberattacken, technischen Betriebsunterbrechungen, Naturkatastrophen oder Feuer ausgesetzt. All diese Bedrohungen können schwerwiegende Folgen wie finanzielle Verluste, Rufschädigung oder sogar existenzielle Bedrohungen haben. Um auf solche Notfälle vorbereitet zu sein, reicht es nicht aus, nur über einen alten, ausgedruckten Notfallplan zu verfügen. Business Continuity Management geht darüber hinaus und stärkt die Widerstands- und Reaktionsfähigkeit eines Unternehmens strategisch, präventiv und operativ. Innerhalb des BCM werden geschäftskritische Bereiche identifiziert, Bedrohungen und deren Auswirkungen bewertet und Maßnahmen zur Bewältigung von Störungen implementiert. Hauptaufgaben von BCM sind die Identifikation von Risiken, die Durchführung von Business-Impact-Analysen, die Entwicklung von Notfallplänen und regelmäßige Tests und Übungen.

Excel vs. BCM-Tools. Obwohl Excel oft als kostengünstige und flexible Lösung wahrgenommen wird, erweist es sich im Rahmen der NIS2-Richtlinie als potenzielle Schwachstelle. Die Software ist nicht darauf ausgelegt, komplexe Prozesse im BCM zu verwalten, und bietet keine ausreichenden Mechanismen für die Nachvollziehbarkeit von Änderungen. Dies widerspricht den Anforderungen der NIS2, die eine lückenlose Dokumentation und Transparenz der Sicherheitsmaßnahmen fordert. Darüber hinaus bietet Excel nur begrenzte Sicherheitsfunktionen und ist anfällig für Fehler, die schwerwiegende Folgen haben können.
Inzwischen stellen auch KI-Tools ein zusätzliches Risiko dar, denn sie sind in der Lage, Excel-Dokumente auszulesen und zu analysieren. Diese Technologien können nicht nur sensible Daten extrahieren, sondern auch sicherheitskritische Muster erkennen. Solche Schwachstellen könnten Angreifern Einblicke in Unternehmensgeheimnisse gewähren und die Sicherheitslage eines Unternehmens erheblich verschlechtern.

BCM effektiv und NIS2-konform umsetzen. Die NIS2-Richtlinie legt einen starken Fokus auf Risikomanagement und BCM als zentrale Elemente der Cybersicherheit. Eine effektive Umsetzung dieser Richtlinie erfordert daher den Einsatz spezialisierter BCM-Softwarelösungen, die den neuesten Sicherheitsstandards entsprechen und die Anforderungen der NIS2 umfassend abdecken. Im Optimalfall wird eine Lösung eingesetzt, die als zentrale Schnittstelle für verschiedene sicherheitsrelevante Themen dient. Dazu zählen neben dem BCM auch Informationssicherheit, Datenschutz und Grundschutz. Im Gegensatz zu Excel lassen sich so Synergien nutzen, die durch eine gemeinsame Datenbasis entstehen.

Spezialisierte BCM-Tools bieten im Vergleich zu Excel weitere Vorteile:

- Integration verschiedener Datenquellen.
- Automatisierung von Prozessen.
- Zentrale Verwaltung.
- Kontinuierliche Aktualisierung von Notfallplänen.

Darüber hinaus gewährleisten BCM-Tools eine hohe Transparenz und Nachvollziehbarkeit durch die automatische Dokumentation aller Änderungen. Dies entspricht den Anforderungen der NIS2-Richtlinie, die auf eine strikte Einhaltung der Sicherheitsstandards drängt.

Wichtig ist jedoch immer, solche Tools nicht nur als »Richtlinien-Erfüller« anzusehen, sondern den echten Mehrwert für das eigene Unternehmen zu erkennen. Dazu zählen im Alltag zum Beispiel die Zeitersparnis für die Verantwortlichen und die Möglichkeit, mit einem Klick Berichte für das Management oder für Auditoren zu erstellen. Funktionen für die Risikoanalyse, Business-Impact-Analysen, das Notfallmanagement und Cyberkrisenübungen stellen sicher, dass Unternehmen auf mögliche Bedrohungen vorbereitet sind und ihre Geschäftsprozesse im Ernstfall schnell wiederherstellen können.

Persönliche Haftung und die Notwendigkeit einer modernen BCM-Strategie. Eine wesentliche Neuerung der NIS2-Richtlinie ist die verschärfte persönliche Haftung von Geschäftsführern, wenn die vorgeschriebenen Sicherheitsvorkehrungen nicht eingehalten werden. Diese Haftung erstreckt sich auch auf die Auswahl der eingesetzten Tools. Unternehmen, die weiterhin auf unsichere Lösungen wie Excel setzen, riskieren nicht nur finanzielle Schäden und Reputationsverluste. Sie riskieren auch rechtliche Konsequenzen und gefährden die persönliche wirtschaftliche Existenz der Geschäftsführer. Diese stehen nun mehr denn je in der Verantwortung, selbst die eingesetzten Werkzeuge zu prüfen und deren Risiken abzuwägen.

Investition in die eigene Zukunft. Die Einführung der NIS2-Richtlinie stellt Unternehmen vor die Herausforderung, ihre Cybersicherheitsstrategien zu überdenken und zu optimieren. Veraltete Technologien wie Excel bergen erhebliche Risiken und sind den Anforderungen moderner Cybersicherheitsrichtlinien nicht gewachsen. Durch den Einsatz spezialisierter BCM-Software können Unternehmen nicht nur die Sicherheit ihrer kritischen Infrastrukturen gewährleisten, sondern auch die persönliche Haftung ihrer Führungskräfte minimieren.

Die Investition in sichere und moderne BCM-Lösungen ist daher nicht nur eine Frage der Compliance, sondern auch eine strategische Entscheidung für eine gestärkte Unternehmensresilienz. Die NIS2-Richtlinie bietet die Chance, Cybersicherheit auf ein neues Niveau zu heben und das Unternehmen vor langfristigen Schäden zu bewahren.

Sascha Kreutziger,
Leiter Business Development,
HiScout