Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Tiratura: 4.500
Data: 21/11/2025 | **Pagina:** 22 | **Autore:** Stefan Laimer und Christian Feichter
Categoria: Waren- und Dienstleistungsgenossenschaften Print & Web

Von der Warnung zur Krise

CYBERSICHERHEIT – Ein kleiner Cybervorfall kann schnell zur Krise werden. Ab Januar 2026 müssen Unternehmen, die unter die NIS2-Richtlinie fallen, **schwere Cyberangriffe binnen 24 Stunden an die italienische Cyberbehörde ACN melden.** Wer unvorbereitet ist, riskiert Sanktionen und langfristigen Schaden.

Bozen – Ab dem 1. Januar 2026 gilt für Organisationen, die unter die NIS2-Richtlinie fallen, eine neue Meldepflicht: Schwerwiegende Cybersicherheitsvorfälle müssen künftig an die Nationale Agentur für Cybersicherheit (ACN) gemeldet werden. Das Verfahren ist dreistufig: Innerhalb von 24 Stunden erfolgt eine Vorabmeldung, innerhalb von 72 Stunden eine detaillierte Meldung und spätestens nach einem Monat ein Abschlussbericht.

Ein strukturierter Ablauf bei Cyberangriffen ist für alle Unternehmen essenziell – nicht nur für jene, die unter die NIS2-Richtlinie fallen. Von der ersten Einschätzung bis zur Nachbereitung entscheidet die Vorbereitung über die Wirksamkeit der Reaktion. Dieser Prozess lässt sich in drei Phasen gliedern:

1. Phase: Die erste Stunde nach dem Angriff: Cyberangriffe kündigen sich selten lautstark an. Erste Warnsignale wie verdächtige Systemaktivitäten oder Monitoring-Alerts müssen rasch bewertet werden. IT- und Security-Teams analysieren, welche Systeme betroffen und welche Daten gefährdet sein könnten. Verdächtige Geräte werden isoliert, Backups geprüft und erste Kommunikationsketten aktiviert. Dann folgt die Einordnung: Handelt es sich um einen IT-Zwischenfall oder um einen potenziellen Angriff? Trifft Letzteres zu, wird umgehend das vorbereitete Notfallteam aktiviert – mit klar zugewiesenen Rollen und Eskalationswegen.

2. Phase: Die Stunden danach: Zeigt sich, dass der Vorfall erhebliche Auswirkungen hat, wird das Notfallteam einberufen – bestehend aus IT, Management, Rechts- und Kommunikationsabteilung und eventuell externen Expertinnen und Experten. Nun gilt es, den Schaden zu begrenzen, den Umfang des Angriffs zu analysieren und betroffene Kundinnen und Kunden oder Partner:innen rechtzeitig zu informieren. Auch rechtliche Pflichten – wie die Meldung an die Cyberbehörde ACN – greifen jetzt. Die Entwicklung und Bewertung möglicher Lösungswege, etwa ein Notbetrieb oder die Datenwiederherstellung, erfordern fundierte Entscheidungen unter Zeitdruck.

3. Phase: Die Folgetage: Ist die akute Bedrohung eingedämmt, beginnt der Weg zurück zum Normalbetrieb. Systeme werden kontrolliert bereinigt und mit gesicherten Daten neu aufgesetzt. Ein Abschlussbericht dokumentiert Ursachen, Verlauf und Maßnahmen. Schwachstellen in Prozessen und


Foto: Shutterstock/ babar ali 1233

Technik werden analysiert, Verbesserungen angestoßen und gewonnene Erkenntnisse in die Organisationsentwicklung bzw. in den Krisenplan übertragen. Auch die Kommunikation nach außen ist jetzt entscheidend für das Vertrauen aller Beteiligten. Alle wichtigsten Erkenntnisse fließen schließlich in Trainings, Tests und künftige Präventionsmaßnahmen ein.

Prävention beginnt zuvor

Für den Fall aller Fälle sollten Unternehmen einen strukturierten Ablauf bereits ausgearbeitet haben. Aber: Effektive Prävention beginnt weit vor dem Cyberangriff – mit klaren Zuständigkeiten, durchdachten Prozessen und der passenden technischen Infrastruktur. Entscheidend ist, alle relevanten Bereiche ganzheitlich zu betrachten:

- **Prozessuale Prävention:** Notfallmanagement ist eine zentrale Führungsaufgabe. Unternehmen sollten mögliche Szenarien im Voraus durchdenken, klare Abläufe definieren und diese mit praxisnahen Checklisten hinterlegen. Ebenso unerlässlich sind vorbereitete Kommunikationspläne, die in Stresssituationen eine schnelle, abgestimmte und transparente interne wie externe Kommunikation ermöglichen.
- **Organisatorische Prävention:** Ein genaues Verständnis geschäftskritischer Prozesse und ihrer IT-Abhängigkeiten ist essenziell. Unternehmen müssen wissen, welche Abläufe besonders zeitkritisch sind – eine fundierte Business Impact Analyse (BIA) liefert hier klare Antworten. Ebenso ist es von zentraler Bedeutung, zuverlässige externe Partner wie SOC-Dienstleister frühzeitig auszuwählen, die eine kontinuierliche Überwachung der IT-Sicherheit gewährleisten. Dabei sollten die Kriterien Qualität, Reaktionszeiten und vertragliche Rahmenbedingungen eindeutig definiert werden.
- **Technische Prävention:** Unternehmen sollten über ein getestetes Incident-Response-Konzept verfügen und regelmäßig unter realistischen Bedingungen üben. Damit Vorfälle nachvollzogen werden können, sollten Logdaten vollständig und zentral erfasst sowie ausgewertet werden. Ein lückenloses Asset-Management schafft Übersicht über alle Systeme und deren Schutzbedarf. Immutable Backups (unveränderliche Datensicherung) sorgen dafür, dass Daten im Ernstfall vom Angreifer weder verschlüsselt noch gelöscht werden können. Die Systeme sollten kontinuierlich optimiert, umfassend abgesichert und mindestens einmal jährlich durch externe Security-Assessments geprüft werden. Ergänzend stärken die Awareness-Trainings die Aufmerksamkeit der Mitarbeitenden für Bedrohungen und Social Engineering.

Ein klar strukturiertes Basis-Notfallkonzept hat mit überschaubarem Aufwand große Wirkung. Entscheidend ist jedoch, nicht bei der Theorie stehenzubleiben: Nur regelmäßige IT-Notfallübungen und Krisensimulationen zeigen, wie gut Abläufe tatsächlich funktionieren – und wo noch nachgebessert werden muss.

**Stefan Laimer
und Christian Feichter**

DIE AUTOREN Laimer ist Head of Security Operations und Security Manager bei Konverto. Feichter ist Senior Berater für IT und Cybersicherheit und Zertifizierter Auditor ISO 27001 und TISAX.