DIGITAL FUTURE CONGRESS 2026 · FACHVORTRAG

Papier beruhigt, der Ernstfall fragt nach

Resilienz jenseits von Zertifikat und NIS2-Checkliste

Kurzimpuls und Live-Simulation: 15 Minuten, drei Entscheidungen, Sie sind die Geschäftsführung.

DATUM & ORT

12. November 2026
SSI Schäfer IT Solutions, Peggau

REFERENT

DI Herwart Wermescher, MBA
Wermescher Advisory GmbH

IM RAHMEN VON

IT Community Styria
Leitung AK Cybersecurity

Seit 1. Oktober hat der Ernstfall eine Uhr

Das NISG 2026 setzt NIS2 in Österreich um: zwei Ziele, und klare Konsequenzen für die Geschäftsführung.

1 Die neue Realität › 2 Simulation › 3 Was trägt

ZIEL 1 · VORSORGE

Schützen

NIS2 motiviert Unternehmen, sich aktiv zu schützen.

Risikomanagement nach dem Stand der Technik.

Lieferkette und Schulung inklusive.

ZIEL 2 · RESILIENZ

Wiederanlauf

Falls doch etwas passiert: so rasch wie möglich wieder funktionieren.

§ 32 verlangt Incident-, Notfall- und Krisenmanagement.

Entscheidend ist, wie schnell der Betrieb wieder läuft.

DRUCKMITTEL · §§ 31, 34, 45

Verbindlich

Chefsache: Leitung verantwortet und schult sich selbst.

Meldepflicht: 24 h · 72 h · 1 Monat.

Strafen: bis 10 Mio. € oder 2 % des Umsatzes.

Das Gesetz verlangt nicht nur Vorsorge, sondern die Fähigkeit, Vorfälle zu bewältigen und den Betrieb wiederherzustellen (§ 32).

Quellen: NISG 2026, BGBl. I Nr. 94/2025 (§§ 31, 32, 34, 45); WKO NIS-FAQ. Keine Rechtsberatung.

Pläne funktionieren nur, wenn man sie übt

Ziel 2 im Detail: Nach einem Vorfall soll der Betrieb so rasch wie möglich wieder laufen.

1 Die neue Realität › 2 Simulation › 3 Was trägt

WAS IM PLAN STEHT	WAS DER ERNSTFALL FRAGT
Notfallplan ist freigegeben.	**? Findet ihn jemand, wenn Server und SharePoint verschlüsselt sind?**
Wiederanlaufzeiten sind festgelegt.	**? Wann haben Sie zuletzt alles auf leerer Infrastruktur wiederhergestellt?**
Krisenstab steht im Organigramm.	**? Wer entscheidet am Sonntag um 22 Uhr, und wer vertritt?**
Wiederanlauf-Reihenfolge ist definiert.	**? Welche Systeme kommen zuerst zurück, und wie arbeiten Sie bis dahin?**

Wer schnell wieder funktionieren will, muss den Ernstfall vorher geprobt haben. Genau das tun wir jetzt: eine Tabletop Exercise, mit Ihnen als Geschäftsführung.

Sonntag, 22:00 Uhr. Sie sind die Geschäftsführung.

Lageübersicht · Drei Schritte: Erkennung, Eindämmung, Wiederherstellung. Die Meldeuhr läuft mit.

1 Die neue Realität › **2 Simulation** › 3 Was trägt

SO 22:00 · LAGEÜBERSICHT

Lageübersicht

Ihre Rolle: Geschäftsführung eines steirischen Software- und IT-Service-Unternehmens mit 150 Mitarbeitenden und Kunden in Industrie und Handel.

Sonntag, 22:00 Uhr: Auf Servern und Clients erscheint eine Erpressernachricht.

Seit 1. Oktober 2026 gilt das NISG 2026. Die Meldeuhr läuft ab Kenntnis, auch am Wochenende.

Spielregeln

Sie entscheiden. Die IT berät, die Verantwortung liegt bei Ihnen.

Je Schritt: erst die Lage, dann die Optionen, dann Handzeichen.

Keine Musterlösung, aber gute und schlechte Gründe.

Saalmikrofon: kurze Wortmeldungen willkommen.

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende

JETZT · SO 22:00

So 22:00 Kenntnis

Mo 22:00 Frühwarnung fällig

Mi 22:00 Meldung fällig

Erkennung: Die ersten 15 Minuten

Schritt 1 von 3 · Sonntag, 22:00 Uhr. Die IT-Rufbereitschaft ruft an.

1 Die neue Realität › **2 Simulation** › 3 Was trägt

SO 22:00 · LAGE 1

Lage

Die IT-Rufbereitschaft meldet eine **Erpressernachricht auf Fileserver, ERP und Teilen der Virtualisierung.**

Der Umfang ist unklar.

Gefordert werden **2 Mio. € in Bitcoin**, die Angreifer behaupten, **Kunden- und Personaldaten kopiert** zu haben.

Ihr Handy läutet im Minutentakt.

2 Mio. € — Lösegeldforderung in Bitcoin

unklar — Umfang: Fileserver, ERP, Virtualisierung

24 h — bis zur NISG-Frühwarnung

JETZT · SO 22:00

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende

So 22:00 Kenntnis

Mo 22:00 Frühwarnung fällig

Mi 22:00 Meldung fällig

Entscheidung 1: Was tun Sie als Erstes?

Schritt 1 von 3 · Erkennung: Die ersten 15 Minuten

1 Die neue Realität › **2 Simulation** › 3 Was trägt

SO 22:15 · ENTSCHEIDUNG 1

A

Externe Hilfe holen

IR-Partner und Cyberversicherung anrufen, Forensik sichern.

B

Teams-Kanal öffnen

Führungskräfte zusammenholen, Lagebild von der IT einfordern.

C

Krisenfall ausrufen

Krisenstab nach Notfallplan aktivieren, Befugnisse und Budget freigeben.

Handzeichen: Wer wählt A? Wer B? Wer C?

JETZT · SO 22:15

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende

So 22:00 Kenntnis

Mo 22:00 Frühwarnung fällig

Mi 22:00 Meldung fällig

Alle drei sind nötig. Reihenfolge und Kanal entscheiden.

BEWERTUNG · C · OPTIMAL · A · AKZEPTABEL · B · UNZUREICHEND

1 Die neue Realität › **2 Simulation** › 3 Was trägt

AUFLÖSUNG 1

C 1. Krisenfall ausrufen

Erst der formelle Beschluss aktiviert Krisenstab, Mandate und Sonderbudget.

Entscheidungslog ab Minute 1 führen.

A 2. Hilfe in der ersten Stunde

Versicherung: Hotline und Obliegenheiten der Polizze beachten.

Forensik: Spuren sichern statt hektisch neu aufsetzen.

B 3. Kommunizieren, aber außerhalb

Ist M365 kompromittiert, liest der Angreifer im Teams-Kanal mit.

Out-of-Band-Kanal vorab festlegen und testen.

NISG-Falle: Die 24-Stunden-Frist läuft ab Kenntnis des Vorfalls, nicht ab dem Krisenbeschluss. Wer zögert, gewinnt keine Zeit.



Eindämmung: Wer zieht den Stecker, und wer spricht?

Schritt 2 von 3 · Montag, 08:30 Uhr. Aus dem IT-Problem wird ein Unternehmensproblem.

1 Die neue Realität › **2 Simulation** › 3 Was trägt

MO 08:30 · LAGE 2

Lage – Montag in der Früh

130 Endgeräte sind verschlüsselt, **ERP und Kundenportal** stehen.

Der Incident Responce-Partner empfiehlt, **alles vom Netz zu trennen**, auch die Kundenanbindungen. Das bedeutet **SLA-Bruch bei allen Kunden.**

Eine **Journalistin** will bis 10 Uhr eine Stellungnahme.

Mail und Teams sind abgeschaltet.

Die **NISG-Frühwarnung** ist noch nicht raus.

130	Endgeräte verschlüsselt
10:00	Die Presse will eine Stellungnahme
13,5 h	bis zur NISG-Frühwarnung

JETZT · MO 08:30

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende

So 22:00 Kenntnis — **Mo 22:00** Frühwarnung fällig — **Mi 22:00** Meldung fällig

Entscheidung 2: Wie entscheiden Sie?

Schritt 2 von 3 · Eindämmung: Wer zieht den Stecker, und wer spricht?

1 Die neue Realität › **2 Simulation** › 3 Was trägt

MO 08:30 · ENTSCHEIDUNG 2

A

Kontrolliert trennen

Inkl. Kundenanbindungen. Holding-Statement an Presse und Kunden, Frühwarnung heute absenden.

B

Hart abschalten

Sofort alles abschalten (Strom aus) und der Presse „kein Kommentar“ geben.

C

SLAs halten

Kundenanbindungen offen lassen. Presse und Behörde erst informieren, wenn die Fakten vollständig sind.

Handzeichen: Wer wählt A? Wer B? Wer C?

JETZT · MO 08:30

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende

So 22:00 Kenntnis

Mo 22:00 Frühwarnung fällig

Mi 22:00 Meldung fällig

Isolieren, informieren, melden: Chefsache

BEWERTUNG | A · OPTIMAL | B · UNZUREICHEND | C · UNZUREICHEND

1 Die neue Realität › **2 Simulation** › 3 Was trägt

AUFLÖSUNG 2

Kontrolliert isolieren

Netzsegmente und Internet trennen, nicht einfach Strom aus.

Flüchtige Spuren wichtiger Systeme vorher sichern.

Befugnis und Kriterien vorab festlegen, inkl. Kundenanbindungen.

Vorbereitet sprechen

Holding-Statements für Presse, Kunden und Mitarbeitende vorab freigeben.

Nur gesicherte Fakten, nichts dementieren, was man nicht weiß.

Belegschaft erreichen ohne Firmen-IT, mit Betriebsrat geklärt.

Früh melden, nicht perfekt

Frühwarnung: Verdacht auf böswillige Handlung? Grenzüberschreitend?

Zugang und Vertretung für das Meldeportal klären.

Parallel: DSGVO-Meldung an die DSB (72 h), Anzeige bei der Polizei.

„Wir haben einen IT-Sicherheitsvorfall festgestellt, arbeiten mit Spezialisten und Behörden und informieren, sobald gesicherte Erkenntnisse vorliegen."

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende



So 22:00 Kenntnis

Mo 22:00 Frühwarnung fällig

Mi 22:00 Meldung fällig

Wiederherstellung: Zahlen oder neu aufbauen?

Schritt 3 von 3 · Tag 3. Die Lage hat sich nicht entspannt, sie ist teurer geworden.

1 Die neue Realität › **2 Simulation** › 3 Was trägt

MI 10:00 · LAGE 3

Lage

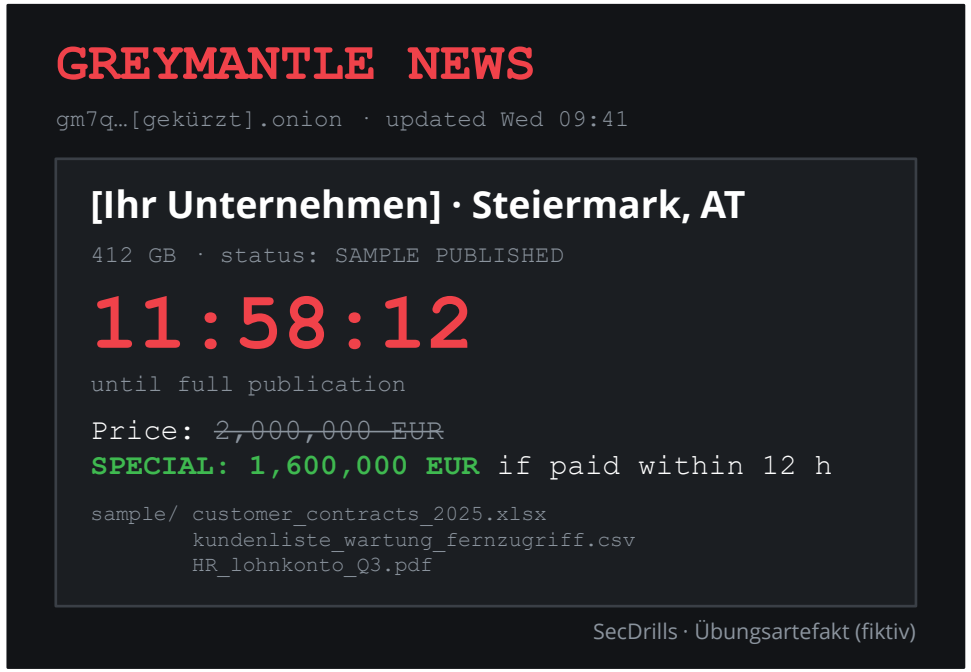
Der **saubere Wiederaufbau** dauert drei bis vier Wochen.

Die Angreifer hatten **Admin-Zugriff** und haben **Backups teilweise gelöscht.**

Auf der **Leak-Seite** steht eine Stichprobe Ihrer Kundendaten, dazu **20 % Rabatt** bei Zahlung binnen 12 Stunden.

Ihr **größter Kunde** droht mit Kündigung.

Heute um 22:00 ist die **72-Stunden-Meldung** fällig.



JETZT · MI 10:00

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende

So 22:00 Kenntnis

Mo 22:00 Frühwarnung fällig

Mi 22:00 Meldung fällig

Entscheidung 3: Wie gehen Sie mit der Forderung um?

Schritt 3 von 3 · Wiederherstellung: Zahlen oder neu aufbauen?

1 Die neue Realität › **2 Simulation** › 3 Was trägt

MI 10:00 · ENTSCHEIDUNG 3

A

Rabatt nutzen

Sofort zahlen, um schnell wieder lieferfähig zu sein.

B

Kategorisch ablehnen

Jeden Kontakt zu den Angreifern verweigern und nur neu aufbauen.

C

Verhandeln lassen

Verhandler über die Versicherung einschalten, parallel neu aufbauen, Entscheidung dokumentieren.

Handzeichen: Wer wählt A? Wer B? Wer C?

JETZT · MI 10:00

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende

So 22:00 Kenntnis

Mo 22:00 Frühwarnung fällig

Mi 22:00 Meldung fällig

Lösegeld kauft einen Schlüssel, kein sauberes Netz

BEWERTUNG | C · OPTIMAL | B · AKZEPTABEL | A · UNZUREICHEND

1 Die neue Realität › **2 Simulation** › 3 Was trägt

AUFLÖSUNG 3

Was Zahlen nicht löst

Netz bleibt kompromittiert: Hintertüren bleiben, Neuaufbau ist ohnehin nötig.

Entschlüsselung ist oft langsam und unvollständig.

Löschung der Daten ist nicht überprüfbar.

Wer zahlt, gilt als zahlungsbereit.

Was die Geschäftsführung braucht

Informiert und dokumentiert entscheiden (Business Judgment Rule, § 25 Abs. 1a GmbHG).

Sanktionslisten prüfen, mit Versicherung und Polizei abstimmen.

Verhandeln ist nicht zahlen: Profis gewinnen Zeit und Information.

≈ 50 % der Betroffenen zahlten **1 Mio. USD** Median der Zahlungen *Quelle: Sophos, State of Ransomware 2025 (n = 3.400, 17 Länder)*

NISG-MELDEUHR

§ 34 · ab Kenntnis, auch am Wochenende



So 22:00 Kenntnis — **Mo 22:00** Frühwarnung fällig — **Mi 22:00** Meldung fällig

Was echte Resilienz ausmacht: vier Fähigkeiten

Nichts davon ist exotisch. Es muss nur vor dem Ernstfall existieren und geübt sein.

1 Die neue Realität › 2 Simulation › **3 Was trägt**

1 Entscheiden

Krisenstab aus GF, IT, Recht, Kommunikation und HR. Mandate, Budget, Vertretungen vorab. Entscheidungslog ab Minute 1.

2 Wiederherstellen

Unveränderbare, getrennte Backups mit eigenen Admin-Konten. Wiederanlauf auf leerer Infrastruktur getestet.

3 Kommunizieren

Out-of-Band-Kanäle, Kontaktlisten offline, Holding-Statements. Meldewege mit Zugang und Vertretung.

4 Üben

Tabletop mit der GF mindestens jährlich. Erkenntnisse zurück in den Notfallplan, das erfüllt zugleich § 32.

Notfallpläne beruhigen den Auditor. Ob sie funktionieren, zeigt nur die Übung.

Wer übt, ist schneller wieder da.

DREI FRAGEN FÜR IHRE NÄCHSTE GF-SITZUNG

1. **Wer entscheidet bei uns außerhalb der Dienstzeiten oder am Wochenende?**
2. **Wann haben wir wichtige Systeme zuletzt komplett wiederhergestellt?**
3. **Wer schickt binnen 24 Stunden die Frühwarnung ab, und mit welchem Zugang?**

WEITERDISKUTIEREN IM WORLD CAFÉ

Themeninsel „Cyber Security und NIS2“

Bonus: „7 Fragen an Ihren Krisenstab“. Sprechen Sie mich an.

DI Herwart Wermescher, MBA
Wermescher Advisory GmbH
herwart@wermescher.com