NAVIRO

PROTECT WHAT MATTERS. EMPOWER WHO MATTERS.

Cyber-Resilienz aus einer Hand

Naviro verbindet die operative Stärke eines Systemhauses mit der Tiefe einer Informationssicherheitsberatung – von der Infrastrukturhärtung bis zum belastbaren ISMS.

Unsere Mission: „Wir machen Organisationen und Menschen *handlungsfähig*, statt sie nur abzusichern.
Wir arbeiten *partnerschaftlich*, statt nur Dienstleister zu sein. Wir denken *nachhaltig*, weil es nicht nur um kurzfristige Sicherheit, sondern um das langfristige Gedeihen der digitalen Gesellschaft geht. Wir schützen, was morgen zählt.“

Warum Unternehmen
uns wählen

Ganzheitlicher Ansatz

Technische Umsetzung und strategische Beratung aus einer Hand. Wir empfehlen nur, was wir selbst geprüft und im Alltag erprobt haben.

Schnell wirksam

Wir starten mit messbaren Quick Wins, reduzieren Risiken sofort und bauen darauf strukturiert weiter.

Wir sprechen KRITIS

Praxiserfahrung in Energie, Transport und Gesundheit mit hohen Compliance- und Verfügbarkeits-anforderungen.

Vertrauen durch Zertifizierung

- BSI-zertifizierter Partner (DIN-SPEC 27076)
- ISO 27001 Information Security Officer
- ISO 22301 Business Continuity Manager

Unsere Werte

- **Verantwortung & Gemeinwohl**: *Wir übernehmen Verantwortung – nicht nur für unsere Kunden, sondern für alle, die von einem sicheren, digitalen Miteinander profitieren.*
- **Befähigung & Partnerschaftlichkeit**: *Wir machen Menschen und Organisationen stark, damit sie selbst die Zukunft gestalten können.*
- **Vertrauen & Stabilität**: *Für uns zählt echter Mehrwert statt schneller Versprechen. Wir begegnen auf Augenhöhe statt in einem Lieferantenverhältnis.*
- **Nachhaltigkeit**: *Unser Blick richtet sich immer nach vorne – denn wir wollen morgen noch genauso erfolgreich schützen wie heute.*

Die größten Irrtümer

> „Wir sind zu klein für Cyberangriffe"

> „Bei uns gab es noch nie einen Einbruch"

> „Wir besitzen keine wertvollen Informationen"

Realität: Jedes datenverarbeitende Unternehmen ist Ziel. Ein fehlender Vorfall bedeutet nicht fehlende Schwachstellen.

Der Druck steigt – die Zahlen sprechen

Die Bedrohungslage verschärft sich kontinuierlich. Mittelständische Unternehmen stehen unter zunehmendem regulatorischem Druck (NIS2, KRITIS), kämpfen mit Fachkräftemangel und einem steigenden Betriebsunterbrechungs-Risiko. Die Verantwortung liegt bei IT-Leitung und Management.

bis zur Entdeckung

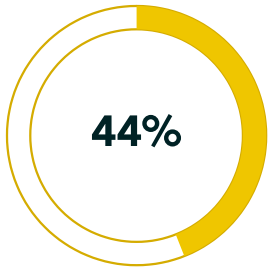
Durchschnittliche Zeit, bis ein Sicherheitsvorfall erkannt wird (IBM)

bis zur Eindämmung

Durchschnittlicher Zeitspanne von Entdeckung bis zur vollständigen Eindämmung (IBM)

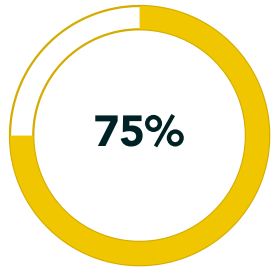
Ransomware-Kosten

Durchschnittliche finanzielle Belastung pro Vorfall (NinjaOne)



Passwort-Wiederverwendung

Mitarbeitende nutzen identische Passwörter über mehrere Systeme (Keeper Security)



Anstieg Cloud-Angriffe

Zunahme gezielter Attacken auf Cloud-Infrastrukturen (National University US)

Quelle: https://segura.security/post/cybersecurity-stats-you-cant-ignore

Ihr Fundament für nachhaltige Resilienz

Warum ein Fundament?
Ohne Basis-Schutz bauen Sie auf Sand: kleine Vorfälle werden zu Krisen, Maßnahmen verpuffen, und Compliance bleibt Zufall statt System.

Ist-Zustand transparent erfassen

Verstehen, wo Sie heute stehen: Systeme, Prozesse, Schwachstellen. Nur wer die Lage kennt, kann gezielt handeln.

Kritische Lücken sofort schließen

Akute Risiken zuerst beseitigen – ungeschützte Webserver, frei zugängliche Admin-Zugänge oder veraltete Systeme. Das ist wie die Haustür zu schließen, bevor man die Alarmanlage installiert.

Solide Basis für nachhaltigen Schutz schaffen

Erst wenn elementare Sicherheitsmaßnahmen greifen, kann man darauf aufbauen: Governance, kontinuierliches Monitoring, Automatisierung und echte Resilienz.

> **Die Realität in vielen Unternehmen:**
>
> **Der Schlüssel steckt noch von außen in der Tür. Ein solides Fundament bedeutet, diese Tür endlich abzuschließen – und das Haus sicher zu machen, bevor man es erweitert.**

Einstiegsangebote für schnellen Nutzen

CyberSprint 16h

In zwei Arbeitstagen messbar sicherer: schlanke Analyse, Auswahl der 8–12 wirksamsten Quick Wins, unmittelbare Umsetzung mit dokumentierten Nachweisen für Management und Auditoren.

Alle Maßnahmen sind praxiserprobt, messbar und sofort wirksam.

NIS2-Gap-Analyse + ISMS-Umsetzungsplan

Kompakter Abgleich der NIS2-Anforderungen mit priorisiertem Umsetzungsplan für Ihr ISMS nach ISO/IEC 27001 oder BSI-Standard 200-1.

Cyber-Resilienz-Strategie

Entwicklung einer unternehmensweiten Cyber-Resilienz-Strategie zur Verbesserung der Widerstandsfähigkeit inkl. Überblick zu relevanten Handlungsfeldern, klarer Roadmap und priorisiertem Maßnahmenkatalog.

Unsere Leistungen im Überblick

Von strategischer Beratung bis zur technischen Umsetzung – wir decken das gesamte Spektrum moderner Cyber Security ab. Unsere Kompetenzfelder sind praxiserprobt und orientieren sich an den höchsten Sicherheitsstandards.

ISMS & Compliance

Risiko-/Gap-Analysen, NIS2-Beratung und Umsetzung, ISMS-Einführung nach ISO 27001 und BSI-IT-Grundschutz, Umsetzungsplan, Bereitstellung eines vCISO/ISB

Awareness & Training

Security-Awareness-Programme und Computer-Based Training zur Stärkung des menschlichen Faktors in Ihrer Resilienzstrategie

IT & Security Management

IT Asset Management, Monitoring, Patch- und Schwachstellenmanagement, Fernwartung sowie Automatisierung von IT-Prozessen

Identity Management

Identity & Access Management (IAM), Benutzer-Life-Cycle, Multi-Faktor-Authentifizierung, Zugriffs-steuerung, Privileged Access Management (PAM)

Incident Response Management

Incident-Response-Begleitung und proaktive Bedrohungsabwehr rund um die Uhr durch Endpoint Protection mit Managed Detection & Response (XDR/MDR) als SOC-Service, SIEM-Bereitstellung

Business Continuity Management, Cloud Backup & Disaster Recovery

Umfassende Konzepte für Geschäftskontinuität, Datensicherung, Test- und Notfallwiederherstellung sowie Krisenmanagement für gesicherten Betrieb

Pentesting & Hardening

Schwachstellenscans, Penetrationstests, Red Teaming und systematische Infrastruktur-Härtung für resiliente Systeme (Server, Netzwerk, Verzeichnisdienste, Cloud-Workloads)

Cloud & Network Security

Netzwerksegmentierung, konzeptionelle Gestaltung von Zero-Trust- und SASE-Architekturen sowie Implementierung und Betrieb

Mail & Microsoft 365 Security

Redundante Cloud Mail Gateways für Security, Archivierung, PGP-/SMIME-Verschlüsselung und Backup von Microsoft 365

Managed Security Services

Übernahme sicherheitsrelevanter Überwachungs- und Verwaltungsaufgaben, mit klaren Service-Levels.

Ihr Thema. Unsere Lösung. Individuell statt von der Stange.

Wir entwickeln die Lösung, die exakt zu Ihrer IT-Landschaft passt.

Ihr nächster Schritt zu mehr Sicherheit

Bereit für messbare Verbesserungen?

Wir stärken Ihre Cyber-Resilienz pragmatisch und nachweisbar. Als BSI-zertifizierter Partner (DIN-SPEC 27076) begleiten wir Organisationen, Unternehmen und KRITIS-Betreiber von der schnellen Bestandsaufnahme bis zur nachhaltigen Umsetzung, fokussiert auf Entlastung statt Bürokratie.

Mehrwertgespräch

Kostenloses Erstgespräch zur Analyse und Beratung Ihrer individuellen Ausgangslage.

Strategiegespräch

Wir zeigen und entwickeln die Lösung, die exakt zu Ihnen und Ihrer Situation passt.

Zusammenarbeit

Wir liefern. Sie sehen Wirkung. Der schnellste Weg zu messbarer IT-Sicherheit.

Jetzt Mehrwertgespräch buchen

Kontaktieren Sie uns

Steven Schilling - Naviro GmbH

E-Mail: steven.schilling@naviro.de

Telefon: +49 (0) 721 181290-92

Web: www.naviro.de