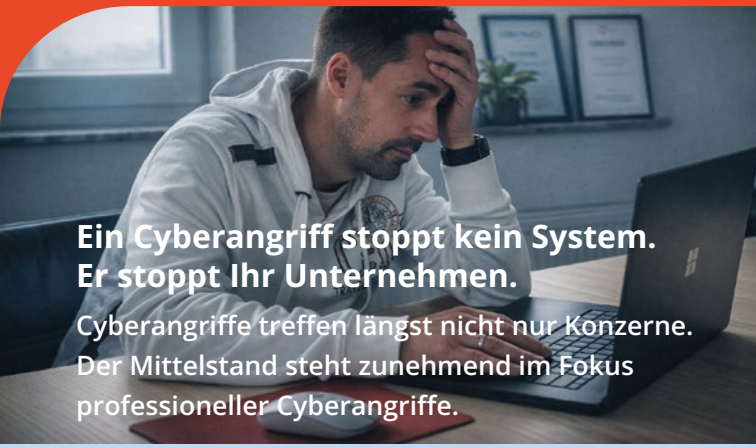
OESTERLING.IT



Ein Cyberangriff stoppt kein System. Er stoppt Ihr Unternehmen.

Cyberangriffe treffen längst nicht nur Konzerne. Der Mittelstand steht zunehmend im Fokus professioneller Cyberangriffe.

IT Sicherheit ist heute unternehmerische Verantwortung.

Digitalisierte Prozesse, vernetzte Systeme und mobile Arbeitsplätze erhöhen Effizienz – und gleichzeitig die Angriffsfläche.

Ein erfolgreicher Angriff kann innerhalb weniger Stunden operative Abläufe vollständig zum Stillstand bringen.

Was Sie in diesem Info-PDF erfahren

- Wie stark Cyberangriffe in den letzten 10 Jahren zugenommen haben
- Welche realen Schäden mittelständische Unternehmen tragen mussten
- Warum strukturierte IT Sicherheit wirtschaftlich sinnvoller ist als Reaktion
- Was ein Vorfall tatsächlich kostet

Cyberkriminalität erreicht Rekordschäden

Fakten zur aktuellen Lage

- Über 90% der Unternehmen waren bereits Ziel eines Angriffs
- Ransomware ist häufigste Ursache für Betriebsunterbrechungen
- Angriffe erfolgen automatisiert – jedes erreichbare System wird systematisch gescannt
- Professionelle Tätergruppen agieren arbeitsteilig

Realität in Deutschland

2020 - Universitätsklinikum Düsseldorf
IT-Ausfall durch Ransomware - Patientenverlegung notwendig

2021 - Landkreis Anhalt-Bitterfeld
Kompletter Verwaltungsstillstand - Katastrophenfall ausgerufen

2022 - Industrieunternehmen Krones AG
Produktionsunterbrechung durch Cyberangriff

Was bedeutet das für ein mittelständisches Unternehmen?

Typisches Szenario (50 bis 150 Mitarbeitende):

Produktionsstillstand:	**20.000 - 100.000** € (pro Tag)
IT-Wiederherstellung:	**30.000 - 150.000** €
Forensik & Rechtsberatung:	**10.000 - 50.000** €

Mögliche DSGVO-Strafen und Vertrauens- und Reputationsschaden

Gesamtschaden schnell: **100.000 - 500.000 €** (und mehr)

IT Sicherheit ist kalkulierbar

Wenn es zum Angriff kommt:

- 100.000 - 500.000 € direkte Schäden
- Produktions- oder Dienstleistungsstillstand
- Externe Forensik & IT Wiederherstellung
- Rechtliche Risiken & DSGVO-Thematik
- Vertrauens- und Reputationsverlust
- Unkalkulierbar. Unplanbar. Existenzgefährdend.

Strukturierte IT Sicherheit bedeutet:

- Analyse der Sicherheitslage nach **NIS2** und **CISIS12**
- Technischer Schutz (Firewall, Endpoint, Backup)
- Notfall- und Wiederanlaufkonzept
- Mitarbeitersensibilisierung
- Regelmäßige Überprüfung

Typische Investition:

- 5.000 - 20.000 € pro Jahr
- Planbar. Kontrollierbar. Nachhaltig.

Ein einziger Vorfall kostet häufig mehr als zehn Jahre strukturierte Prävention.

IT Sicherheit braucht Struktur

1 Analyse

Sicherheitscheck & Risikobewertung

2 Strategie

Individuelles Konzept und Priorisierung

3 Umsetzung

Technische Maßnahmen und Notfallkonzept

4 Begleitung

Monitoring braucht Schulung und kontinuierliche Optimierung

Warum OESTERLING.IT ?

- **Spezialisierung auf mittelständische Unternehmen**
- **Wirtschaftlich sinnvolle, praxistaugliche Lösungen**
- **Nachhaltige Sicherheitsstrategie statt Einmal-Projekt**
- **Unterstützung bei der Identifikation und Beantragung von Fördermöglichkeiten**

Lassen Sie uns Ihre IT Sicherheit strukturiert bewerten.

Vereinbaren Sie einen unverbindlichen Sicherheits-Check

IT Kompetenz für Ihr Business

Nehmen Sie mit uns Kontakt auf: rufen Sie uns einfach an oder senden Sie uns eine Mail.
Wir sind für Sie da.

+49 6071 739573-0
vertrieb@oesterling.it

OESTERLING.IT

OESTERLING.IT

Am Schlangensee 36 - 64807 Dieburg

https://oesterling.it
linkedin.com/company/oesterling-it
info@oesterling.it
facebook.com/christoph.oesterling
+49 6071 739573-0
@christophoesterling