NIEDERSACHSEN DIGITAL

UVN Unternehmerverbände Niedersachsen

# BASISMAßNAHMEN IN DER IT-SICHERHEIT

## Empfehlungen von niedersachsen.digital

Das Risiko für Unternehmen, Opfer von Cyberangriffen, insbesondere von digitalem Betrug, zu werden, steigt.
Bei Cybersicherheitsvorfällen kommt immer häufiger die gesamte Geschäftstätigkeit zum Erliegen, wodurch den Unternehmen große Schäden entstehen. Analysen solcher Vorfälle zeigen, dass viele von ihnen vermeidbar wären oder in ihrem Ausmaß begrenzt werden könnten, wenn bestimmte **Basismaßnahmen** ergriffen würden.
In diesem Papier sind die wichtigsten Basismaßnahmen zusammengestellt, die von den Expertinnen und Experten des Digitalverbands **niedersachsen.digital** als Teil der **Unternehmerverbände Niedersachsen** empfohlen werden. Sie sollen Unternehmen dabei helfen, ihre IT-Sicherheit unbürokratisch zu verbessern und somit das Risiko eines erfolgreichen Angriffs zu senken bzw. im Notfall ihre Geschäftstätigkeit weitestgehend aufrechtzuerhalten.

## GRUNDSÄTZE DER IT-SICHERHEIT

Um die Basismaßnahmen sinnvoll umzusetzen, sind die folgenden **Grundsätze** zu beachten:

### Verantwortung der Geschäftsleitung

IT-Sicherheit ist Chefsache. Die Geschäftsleitung steht voll und ganz hinter diesem Thema und stellt ausreichende Mittel bereit, definiert Zuständigkeiten und setzt Prioritäten.

### Transparenz über Prozesse und Systeme

Ein Überblick über alle Systeme, Daten und Abläufe im Unternehmen ist die Voraussetzung für wirksame IT-Sicherheit.

### Ziel der IT-Sicherheit

Das Ziel besteht darin, erfolgreiche Cyberangriffe und IT-Ausfälle zu vermeiden bzw. die Geschäftstätigkeit in diesen Fällen möglichst aufrechtzuerhalten.

### Sicherheitsbewusstsein im Unternehmen

Alle Mitarbeitenden tragen zur IT-Sicherheit bei. Sie kennen die wichtigsten Regeln und wissen, wie sie im Notfall reagieren müssen.

Die folgenden Basismaßnahmen bieten bei minimalem Aufwand das größtmögliche Potenzial zur Schadensminderung.
Sie sind hersteller- und produktunabhängig und ersetzen nicht bestehende Normen oder regulatorische Vorgaben (wie NIS2, ISO 27001 oder BSI-Grundschutz).

## BASISMAßNAHMEN FÜR IT-SICHERHEIT

### 1. Krisenteam und Notfallplan

Es gibt ein festes Krisenteam, das allen bekannt ist. Ein IT-Notfallplan liegt vor und wird regelmäßig geübt.
**Ziel:** Betrieb im Ernstfall aufrechterhalten (Business Continuity Management).

### 2. Schulung und Übung

Mitarbeitende und IT-Verantwortliche werden regelmäßig, gezielt und nachweisbar geschult.
**Inhalte:** sicheres Verhalten, Erkennen von Phishing, Abläufe im Notfall. Notfallübungen und Phishing-Tests werden regelmäßig durchgeführt.

### 3. Datensicherung

Alle wichtigen Daten werden regelmäßig und **manipulationssicher** nach Stand der Technik gesichert.

### 4. System zur Detektion von Sicherheitsvorfällen

Ein zentrales System überwacht sicherheitsrelevante Ereignisse (z. B. SIEM. Oder IDS/IPS-Systeme). Logdaten werden gesammelt und ausgewertet. Bei Auffälligkeiten wird automatisch alarmiert.

### 5. Zugriffsschutz

Für Fernzugriffe (z. B. VPN) und Cloud-Dienste (z. B. Microsoft 365) wird **Mehr-Faktor-Authentifizierung** genutzt.

### 6. Updates und Patches

Es gibt feste Abläufe, um Software-Updates im Büro und in der Produktion **zeitnah einzuspielen.**

## 7. Netzwerksegmentierung

Der Datenfluss zwischen Büro- und Produktions-IT wird minimiert und gesteuert, um Schäden zu begrenzen.

## 8. Altsysteme absichern

Alte Systeme ohne Sicherheitsupdates werden **isoliert**, und ihr Ersatz ist **geplant.**

## 9. Externe Dienstleister kontrollieren

Zugänge externer Partner und Dienstleister werden **regelmäßig geprüft.**

## 10. IT-Dokumentation

Die IT-Infrastruktur ist dokumentiert (Netzwerkplan, Geräte- und Softwarelisten).

## 11. Sicherheitssoftware auf Endgeräten

Alle Computer und mobilen Geräte sind mit **aktueller Sicherheitssoftware** geschützt, überwacht und ggf. zentral gesteuert.

## 12. Online-Banking und Geschäftsprozesse

Es gelten klare Regeln, z. B. **Vier-Augen-Prinzip** beim Online-Banking und bei wichtigen Zahlungen.

## 13. Physische Sicherheit

Das Gelände ist geschützt (Zaun, Tor, Pförtner). Serverräume sind abgeschlossen. Fremde Personen dürfen nicht unbeaufsichtigt in Büro- oder Technikbereichen sein. Keine Technik oder Dokumente offen liegen lassen.

### Nächster Schritt: Kostenloser Risikodialog

Die obige Liste umfasst zentrale Basismaßnahmen, die Unternehmen mit überschaubarem Aufwand umsetzen können. Sie bildet den Einstieg in ein systematisches IT-Sicherheitskonzept.

Um einzuschätzen, inwieweit diese Maßnahmen im eigenen Unternehmen bereits umgesetzt sind oder wo konkreter Handlungsbedarf besteht, empfehlen wir einen kurzen Risikodialog der Geschäftsführung und/oder der IT-Verantwortlichen mit einem unabhängigen Berater.

Die unten genannten Autoren sind Mitglieder von niedersachsen.digital und bieten einen kostenlosen Risikodialog auf Basis gemeinsamer fachlicher Standards an. Vergleichbare Angebote sind auch bei anderen qualifizierten Anbietern am Markt verfügbar.

**Sprechen Sie uns an und vereinbaren Sie einen kostenlosen Risikodialog.**

# AUTOREN


**Torben Bues**
Unabh. Berater für Informationssicherheit
TBCS IT GmbH
torben.bues@tbcs.it

**Dr. Axel Ebers**
Leiter Digitalisierung, Mittelstand & niedersachsen.digital
Unternehmerverbände Niedersachsen e.V. (UVN)
ae@uvn.digital

**Carsten John**
Consultant IT-Sicherheit
Lampe & Schwartze Risk Management GmbH
c.john@ls-risk.de

**Klaus Mönikes**
Geschäftsführender Inhaber (Datenschutzbeauftragter, Berater für Cybersecurity)
privsec Klaus Mönikes Unternehmensberatung für Datenschutz und Datensicherheit
klaus.moenikes@privsec.de

**Markus Dietz**
Leiter Business Development, Vertrieb & Marketing
GRASS-MERKUR GmbH & Co. KG
markus.dietz@grass-merkur.de

**Achim Gärtner**
Geschäftsführer
GRTNR.IT GmbH
achim@grtnr.it

**Ron Kneffel**
Head of Information Security
BREDEX GmbH
ron.kneffel@bredex.de