



CERT Nord Services

- **Informationsdienst**
- **Bereitstellung von Informationen** per Mail und auf dem **CERT Nord Portal**
- Meldungen zu **Schwachstellen, Patches, Hinweisen**
- **Tageslagebericht** des BSI
- **Warndienst**
- Bereitstellung der **WID-Meldungen** des **CERT Bund**: Warnungen zu über 1000 Produkten
- Bereitstellung von **BSI-IT-Sicherheitsmitteilungen**
- **Eigene Bewertung** von Sicherheitslücken
- Versand von **Warnmeldungen**
- **Alarmmeldungen**
- **Alarmierung bei akuten Gefahrensituationen** z.B. ausgenutzte Lücken von Hard- und Software

Was ist neu?

Der CISO Ihres Landes hat das **CERT Nord** beauftragt, die **CERT Nord Services** auf das **kommunale Umfeld zu erweitern**.

Zusätzlich kann bei einem IT-Sicherheitsvorfall auch **Incident Response Unterstützung** bereitgestellt werden.



Schutz für Ihre IT-Infrastruktur

Kompetente Unterstützung und aktuelle Sicherheitsinformationen für Kommunen, Behörden und öffentliche Einrichtungen

CERT Nord

Postfach 1780
24016 Kiel

Telefon +49 40 428 46-1984
E-Mail cert@certnord.de

certnord.de



Computer Emergency Response Team

CERT Nord ist das gemeinsame LandesCERT der Bundesländer:

- Bremen
- Hamburg
- Sachsen-Anhalt
- Schleswig-Holstein

Das **CERT Nord** ist Teil des bundesweiten Verwaltungs-CERT-Verbundes (VCV) und steht in Kontakt mit dem BSI.

Das CERT Nord

- **Zentrale Meldestelle** für IT-Sicherheitsvorfälle
- **Prüft und bewertet** mit den Meldenden die aktuelle Situation
- **Gibt Hinweise** für weitere Aktionen
- **Unterstützt** die Erstellung von IT-Sicherheitslagebildern



Erreichbarkeit

CERT Nord Services zu Bürozeiten und Incident Response Unterstützung:

Mo – Do	08:00 – 16:00 Uhr
Fr	08:00 – 15:00 Uhr
Telefon: +49 40 428 46-1984	

Incident Response Unterstützung

- **Annahme** von IT-Sicherheitsvorfällen
- **Qualifizierung** des Vorfalls
- **Erste Hilfestellung** für weiteres Vorgehen
- **Bei Bedarf:** Unterstützung Remote oder ggf. vor Ort (durch IT-Dienstleister)

Was sind IT-Sicherheitsvorfälle?

Beispiele und Merkmale



Verschlüsselung von Dateien
(Ransomware)



Manipulation von Daten



Langwierige
Beeinträchtigung / Ausfall

Vorfallmeldung

1. **Wer meldet den Vorfall?**
2. **Welche Funktionen sind gestört?**
E-Mail, Bürgerservice, Fachverfahren
3. **Wie wurde er bemerkt?**
Mitarbeitende, Monitoring, externe Hinweise
4. **Wann wurde der Vorfall entdeckt?**
Datum, Uhrzeit
5. **Wo befindet sich das betroffene IT-System?**
Gebäude, Raum, Arbeitsplatz
6. **Was ist betroffen?**
PCs, Server, Netzlaufwerke, Dienste, ...

Identitätsdiebstahl



Kriminelle Angriffe



Vireninfektion

