

# CERT Nord

## Unsere Leistungen für die kommunale Verwaltung in Schleswig-Holstein



Neumünster, 22.05.2025

# Vorstellung des CERT Nord - Überblick

1. Was ist ein CERT / das CERT Nord
2. Aufgaben des CERT Nord
3. Angebote des CERT Nord
4. Behandlung von IT-Sicherheitsvorfällen
5. Wie geht es weiter

# Was ist ein CERT?

→ Computer **E**mergency **R**esponse **T**eam

- **Aufgaben:**

- **Kommunikation**
- **Bewertung** und **Verarbeitung** aller eingehenden Informationen im Hinblick auf zu schützende Infrastruktur und interne Prozesse
- **Entgegennahme** von Sicherheitsvorfällen
- **Warnung** vor IT-Sicherheitsbedrohungen (offengelegte Schwachstellen)
- **Vorfallbearbeitung**
- **Lagebilderstellung**

# Was ist das CERT Nord?

- Gemeinsames, koordinierendes Länder-CERT der Bundesländer Bremen, Hamburg, Sachsen-Anhalt und Schleswig-Holstein
- Auftraggeber: Landes-CISOs (Chief Information Security Officer)
- Zielgruppe: CISOs, ISBs der Ministerien, Behörden und Kommunen
- CERT Nord ist grundsätzlich zuständig für die Landesverwaltungen ihrer 4 Trägerländer
- CERT Nord steht in dauerhaftem Kontakt mit BSI / CERT Bund sowie den CERTs der übrigen Bundesländer im sog. VCV (Verwaltungs-CERT-Verbund)
- CERT Nord arbeitet zusammen mit dem IT-Dienstleister aus dem Norden
- CERT Nord ist Meldestelle für Dritte (Chaos Computer Club, besorgte Bürger, andere CERTs, ...)

# CERT Nord – Erweiterung auf Kommunen

- Die CISOs der Flächenländer SH und S-T haben den Auftrag für das CERT Nord auf das kommunale Umfeld erweitert:
  - Bundesweite Angriffe auf Kommunen
  - Die Kommunen sind meist die direkten Ansprechpartner für die Bürger, Ausfälle haben damit direkte Auswirkungen auf die Bürger und die Dienstleistungen für die Bürger
  - Funktionierende Verwaltung und die Sicherheit der Bürgerdaten haben oberste Priorität
- Das CERT Nord wurde um Personal erweitert:
  - Zusätzliche 4 Personen für die Bereitstellung der CERT Dienstleistungen
  - 4 weitere Personen für Incident Response
  - Für die Kommunen in SH und S-T wurde ab 1.7.2025 eine Rufbereitschaft des CERT Nord beauftragt
  - Für Verdachtsfälle oder Vorfälle steht somit rund um die Uhr eine qualifizierte Ansprechperson zur Verfügung
- Das CERT Nord kann in Notfällen zusätzlich einen Dienstleister für Vor-Ort Einsätze beauftragen
  - Der Dienstleister wird in Notfällen innerhalb von 24 Stunden aktiv, wenn die Möglichkeiten der Incident Responder für eine Remote Aufklärung nicht ausreichen

# Kontaktmöglichkeiten zum CERT Nord

- Hotline: 040 / 428 46 – 1984 (innerhalb Servicezeit)
- Rufbereitschaft : 040 /428 99 6710 (außerhalb Servicezeiten)
- Fax: 040 / 428 46 – 3632
- eMail: [cert@certnord.de](mailto:cert@certnord.de)
- Öffentlicher PGP Schlüssel auf [Webseite](#) bzw. [Kundenportal](#):
  - <https://www.certnord.de/>
  - <https://kundenportal.dataport.de/websites/0108/SitePages/PGP-Schl%C3%BCssel.aspx>

# Vorstellung des CERT Nord - Überblick

1. Was ist ein CERT / das CERT Nord
2. **Aufgaben des CERT Nord**
3. Angebote des CERT Nord
4. Behandlung von IT-Sicherheitsvorfällen
5. Wie geht es weiter

# Aufgaben des CERT Nord

1/15

## **Die wichtigsten Aufgaben im Überblick:**

- I. Informations- und Warndienst
- II. Schnittstelle zum BSI / CERT-Bund / VCV
- III. Unterstützung bei Behandlung von IT-Sicherheitsvorfällen und sog. UseCases
- IV. Statistiken / Lagebild

**Das CERT Nord nimmt noch weitere Aufgaben wahr. Darüber berichten wir gern in einer ausführlichen Präsentation.**

# CERT Nord – Informations- und Warndienst 2/15

## Kategorisierung:

### - **Information:**

- Hinweise auf Lücken und Schwachstellen, Bereitstellung auf dem CERT Nord Portal
- Handeln planen

### - **Warnung**

- Hinweise auf kritische Schwachstellen, Bereitstellung auf CERT Nord Portal und ggf. ergänzende Mail der CERT Nord (wenn Ausnutzung kurzfristig zu erwarten ist)
- Kurzfristiges Handeln einplanen

### - **Alarm**

- Kritische Schwachstellen werden aktiv ausgenutzt, Mail des CERT Nord
- Unverzögliches Handeln erforderlich, ggf. Abschaltung von gefährdeten Diensten

# CERT Nord – Informations- und Warndienst 3/15

## - Informationsdienst:

- Bereitstellung auf dem CERT Nord Portal
- Sicherheitsinformationen – Hinweise auf verschiedenen Quellen im Internet
- Tageslagebericht des BSI (tägliches Lagebericht ab ca. 15 Uhr)
- Schwachstellenmeldungen des BSI (WID-Meldungen, ca. 1000 pro Monat)
- Vorfallmeldungen von anderen LänderCERTs
- BITS-Meldungen (BSI-IT-Sicherheitsmeldungen) des BSI
- Patchday-Hinweise für Produkte von Microsoft, Adobe und Oracle

# CERT Nord – Informations- und Warndienst 4/15

## - Warndienst:

- Bereitstellung auf dem CERT Nord Portal und meist ergänzend per Mail
- Meist im Rahmen von BITS (ehemals Cybersicherheitswarnungen)
  - Oft auch Folgemeldungen von BITS mit neuen Erkenntnissen
- Besondere Hinweise vom BSI oder aus dem VCV Chat
  - zu besonderen Produkten, die innerhalb der Verwaltungen eingesetzt werden
  - zu Vorgehensweisen von Angreifern mit Fokus auf die Verwaltung
- Hinweise aus dem Lagezentrum
  - i.d.R. Erkenntnisse über spezifische Lücken bei Systemen einzelner Verwaltungen
  - aus eigenen Recherchen des BSI oder über Hinweise Dritter an das BSI

# CERT Nord – Informations- und Warndienst 5/15

- Informationen, Warnungen und Alarme werden anlassbezogen auch per eMail versandt
  - Soweit wie möglich zielgerichtet, ggf. nur an einzelne Empfänger
  - Ein standardisierter Kopf der Mail sorgt für einen schnellen Überblick
  - Soweit möglich, liefert das CERT Nord Handlungsempfehlungen, ggf. auch erweitert um Erkenntnisse vom Dataport SOC
    - Beispiele:
      - uns mitgeteilten Erkenntnissen zu Schwachstelle zu einem Produkt
      - IoC-Listen
      - Informationen und Bewertungen zu den Sicherheitspatches der Firmen Microsoft, Adobe und Oracle

# CERT Nord – Informations- und Warndienst 6/15

Antworten Allen antworten Weiterleiten Chat

Fr 04.04.2025 12:42



CERT

[alle CISO, alle ISB] [TLP:GREEN] [CERT Nord Warnung CN-W-2025-04-04-002]: Kritische Schwachstelle in Druckertreibern von Canon

An CERT

AK erl.

## Warn- und Informationsdienst des CERT Nord

**Verteiler:** alle CISOs, alle ISBs aller Trägerländer sowie ST Kommunen, SH Kommunen, FHB BHV, Brekom, Governikus, Performa Nord, Wirtschaftsförderung Bremen, Kommunit, KID Magdeburg und Dataport

**Thema:** Kritische Schwachstelle in Druckertreibern von Canon

**Betroffene Treiberversionen:** Generic Plus PCL6, UFR II, LIPS4, LIPSXL und PS bis einschließlich Version 3.12

**CVE:** CVE-2025-1268

**CVSS-Score:** 9,4 – kritisch

**Bedrohungslage:** GELB

**Quelle:** BSI-Tageslagebericht

**TLP:** GREEN

**Patch:** Patches liegen vor

- **Entgegennahme** von Meldungen bis zur Einstufung VS-NfD
  - Aufbereitung und Weiterleitung an
    - betroffene Institutionen / Behörden / ISB
    - Fallweise Zusammenarbeit mit anderen Landes-CERTs, z.B. identisches Produkt im Einsatz
- **Weiterleitung** eigener Sicherheitsvorfälle an BSI / VCV
  - Kampagnen, (DDoS-)Angriffe, IoC-Listen, ...
- **Mitarbeit** im VCV
  - Teilnahme an Regeltreffen (2x p.a.)
  - Beteiligung an gemeinsamen Übungen mit Bund und Ländern (Lükex, ...)

# CERT Nord – III – Behandlung von SiVos 8/15

- Vorfallmeldungen von **außen**:  
BSI (Darknet-Überwachung), andere Länder-CERTs, Ermittlungsbehörden, ...
- Vorfallmeldungen von **innen**:  
aus Behörden und Organisationen unserer Trägerländer
- Sog. **UseCases**: durch SOC festgestellte **Auffälligkeiten** bzw. **ungewöhnliche Ereignisse** bei Endgeräten oder im User-Kontext
  - Beispiele für UseCases (Auszug)  
#4171442 UC 032.01 INT Häufung von Virenalarmen auf Endpoints  
#4144831 UC 109.01 INT RDP to Domain Controller

# CERT Nord – III – Behandlung von SiVos 9/15

- **Ermittlung** der betroffenen Institution zur Informationsweitergabe;  
**Dokumentation** gemeldeter Vorfälle
- **Empfehlung** von Maßnahmen und Workarounds
- *Option:*  
**Nachfrage im VCV Chat** nach weitere Betroffenenheiten oder Lösungen
- **Weiterleitung** an BSI und Länder-CERTs;  
ggf. **Warnung** anderer Organisationen (Kampfmittelbeseitigung)
- ggf. **Einschaltung** Notfall-/Krisenmanagements; ggf. **Koordination**
- Unterstützung durch **Mitarbeit vor Ort**
- **Erstellung** von Statistiken und Lagebildern

# CERT Nord –IV – Statistik / Lagebild

10/15

- Erstellung je einer **Monatsstatistik** pro Trägerland
- Erstellung **spezifischer Lagebilder** bei Anlass
- Statistiken / Lagebilder werden den jeweiligen Landes-CISOs übergeben
- Quellen:
  - Dem CERT Nord gemeldete Vorfälle
  - Dataport Incident System
  - Monatliche Berichte Antivirus- und Mail-Systeme
- Ziel:
  - Erschließung weiterer Quellen bzw. kundeneigener Installationen
  - Ausweitung auf weitere Kategorien

## Nutzen / Auswertung:

- Bedarf für Jahresberichte / Tätigkeitsnachweise
  - Monatliche Statistik pro Land an CISOs (geht in Jahresstatistik über)
  - Beantwortung der CISO-Nachfragen zu bestimmten Themen
  - Unterstützung der CISOs bei parlamentarischen Anfragen, Presseanfragen
- 
- Die Statistiken haben mittlerweile einen hohen Stellenwert bei den CISOs, da sie die Entwicklung der letzten Jahre nachzeichnen
- 
- **FATAL: „Wenn nichts gemeldet wird, ist auch nichts geschehen!“**

# CERT Nord – IV – Statistik / Lagebild

12/15

Jahresstatistik 2024		Musterland											
Ereignistyp	Januar	Februar	März	April	Mai	Juni	Juli	August	September	Oktober	November	Dezember	Summe
Anzahl der monatlich vom Virenschutz betreuten Endgeräte	57.534	57.095	53.646	54.986	54.854	54.762	55.612	54.863	55.481	55.695	55.714	56.358	
2. Erfolgreiche Installation eines Schadprogramms	x			x	x		x					x	5
3. Systemeinbruch				x							x		2
4. Unautorisierte Systemnutzung							x						2
5. Datenabfluss durch Schadprogramme oder Hacker													0
6. Manipulation von Hard- oder Software													0
7. DDoS		x			x		x	x					4
8. Diebstahl oder sonstiger Verlust IT-System	x	x	x	x	x	x	x	x	x	x	x	x	271
9. Diebstahl oder sonstiger Verlust Datenträger		x							x	x	x	x	6
10. Unsachgemäße Entsorgung													0
11. Offenlegung durch unautorisiertes Personal													0
12. Sicherheitslücke	x	x	x	x	x	x	x	x			x	x	34
13. Schwerwiegender Ausfall von Betriebsmitteln													0
14. Schwerwiegende fehlerhafte Funktion						x	x				x		5
15. Schwerwiegende Überlastsituationen													0
16. Widerrechtliche Aktion, Verstoß IT-Sicherheitsrichtlinie	x	x	x	x	x	x	x	x	x	x	x	x	103
17. Interne Ursachen			x	x		x		x				x	6
18. Naturgewalten													0
19. Beschädigung					x								1
20. Besondere Erkenntnisse				x	x	x	x	x		x	x	x	17
21. UseCase	x	x	x	x		x	x		x	x	x	x	16
22. Fehlkonfiguration	x	x	x	x	x	x	x	x	x	x	x	x	72
23. Fremddaccountnutzung	x	x			x		x		x			x	11
24. Phishing	x	x	x	x	x	x	x	x	x	x	x	x	118
25. Wirtschaftsunternehmen	x		x		x		x			x	x	x	9
<b>Summen:</b>	<b>42</b>	<b>28</b>	<b>48</b>	<b>83</b>	<b>51</b>	<b>44</b>	<b>47</b>	<b>54</b>	<b>102</b>	<b>57</b>	<b>60</b>	<b>66</b>	<b>682</b>

# Vorstellung des CERT Nord - Überblick

1. Was ist ein CERT / das CERT Nord
2. Aufgaben des CERT Nord
3. Angebote des CERT Nord
4. Behandlung von IT-Sicherheitsvorfällen
5. Wie geht es weiter

# CERT Nord - Angebote

## 1. SPOC gemäß RFC 9116

- Ablage einer ASCII-Datei auf einem Webserver in einem definierten Verzeichnis mit Kontaktdaten Richtung CERT Nord

<https://MeinWebService.de/.well-known/security.txt>

- Whitehat Hacker kann darüber Kontakt aufnehmen

## 2. CERT-Bund Meldungen

- Dem CERT-Bund können externe IP-Bereiche gemeldet werden
- CERT-Bund scannt diese IP-Bereiche auf Verwundbarkeiten und meldet Funde dem CERT Nord
- CERT Nord kontaktiert Betroffene und gibt Hinweise zu Behebung der Lücken

# Vorstellung des CERT Nord - Überblick

1. Was ist ein CERT / das CERT Nord
2. Aufgaben des CERT Nord
3. Angebote des CERT Nord
4. **Behandlung von IT-Sicherheitsvorfällen**
5. Wie geht es weiter

- **Definition: Ein Sicherheitsvorfall kann vorliegen**

- wenn die Verfügbarkeit, Vertraulichkeit oder Integrität von IT-Systemen, Diensten oder Verfahren gestört sind (auch in der Rufbereitschaft zu melden, wenn Verdacht auf eine Aktion Dritter als Ursache anzunehmen ist)
- gegen bestehende Regelungen/Anweisungen verstoßen wird (i.d.R. für Statistik interessant, kein Ereignis für Rufbereitschaft)
- durch ein Ereignis ein Schaden für die Institution entstehen kann (auch in der Rufbereitschaft zu melden, wenn Verdacht auf eine Aktion Dritter in Bezug auf IT-Systeme, Dienste oder Verfahren als Ursache anzunehmen ist)

- **Beispiele:**

- Eine im Internet betriebene Anwendung wurde manipuliert
  - Vorfallmeldung erforderlich, eine anonymisierte Weitermeldung an den VCV mit Informationen zu Anwendungsnamen, Hersteller und Problemlösung
- Durch einen Serverausfall steht eine wichtige Fachanwendung länger nicht zur Verfügung
  - Vorfallmeldung, wird für Statistik aufgenommen
- Kompromittierung Postfach – Phishing
  - Vorfallmeldung mit Hinweisen zu kompromittierter Adresse. Statistik und ggf. Warnung im VCV-Chat bzw. wichtige Kommunikationspartner
  - Möglichst initiale Phishing-Mail bereitstellen

# CERT Nord – Behandlung von IT SiVo

3/4

- Grundsätzlich gilt:  
**alle Sicherheitsvorfälle müssen dem CERT Nord gemeldet werden.**
- Meldung erfolgt über das Meldeformular via Mail an [cert@certnord.de](mailto:cert@certnord.de)
- Bei Unsicherheiten oder Fragen: **bitte Hotline (Durchwahl – 1984) anrufen**  
**oder per Mail an [cert@certnord.de](mailto:cert@certnord.de) um Kontaktaufnahme bitten**
- Keine Angst!
  - Es erfolgt kein Fingerprinting
  - Das CERT Nord stimmt die Meldung mit Ihnen ab

- Relevante Sicherheitsvorfälle werden an den VCV und ans BSI in Abstimmung weitergeleitet
  - anonymisiert
  - eine Weiterleitung kann auch untersagt werden, sofern nicht Anforderungen gem. NIS2 dazu verpflichten
- Warum sollen Vorfälle gemeldet werden?
  - Warnung Dritter (auf Wunsch ohne Nennung der Quelle)
  - Unterstützung / Information
  - Statistik / Lagebild
  - **Vermeidung den Trugbilds:**  
**„Wenn nichts gemeldet wird, ist auch nichts geschehen.“**

# Vorstellung des CERT Nord - Überblick

1. Was ist ein CERT / das CERT Nord
2. Aufgaben des CERT Nord
3. Angebote des CERT Nord
4. Behandlung von IT-Sicherheitsvorfällen
5. Wie geht es weiter

# CERT Nord – Wie geht es weiter?

1/6

- Das CERT Nord richtet die Ansprechpartner auf dem Portal ein
  - Die ISBs (Informationssicherheitsbeauftragte) sind die Ansprechpartner des CERT Nord. Das CERT Nord berechtigt die ISBs auf dem Portal und richtet Mailverteiler für den Versand von Meldungen ein.
  - Die Anmeldung erfolgt über Herrn Weidemann vom ITVSH, Herr Weidemann leitet die Anträge nach Prüfung an das CERT Nord weiter.
  - Für die Anmeldung wird eine TLP-Erklärung benötigt, das Formular liegt Herrn Weidemann vor.
  - Nach der Einrichtung im Portal erhält die/der ISB eine Mail mit dem Link zum Portal und einigen Hinweisen.

# CERT Nord – Wie geht es weiter?

2/6

- Zum 1.7.2025 ist das CERT Nord außerhalb der Servicezeiten über eine Rufbereitschaft erreichbar
  - Besteht der Verdacht eines IT-Vorfalles, führt das CERT Nord mit einem kompetenten Ansprechpartner eine Vorklärung durch
    - Zur weiteren Klärung bindet das CERT Nord Incident-Responder (IR) ein
    - Sofern durch den Vorfall die Informationstechnik weiterhin betriebsfähig ist, erfolgen weitere Analysen durch einen Remote-Incident-Responder. Ein Mobile-Incident-Responder steht zur Verfügung, wenn keine Remote-Analysen möglich sind
    - Remote-Incident-Responder (R-IR) stehen während der Servicezeit zur Verfügung, über einen Dienstleister kann ein Mobile-Incident-Responder (M-IR) innerhalb von 24 Stunden eingebunden werden
    - Vor dem Einsatz eines IR muss die Erklärung zur Datenverarbeitung unterzeichnet werden

# CERT Nord – Wie geht es weiter?

3/6

- Das CERT Nord und die Incident-Responder von Dataport erarbeiten Dokumente und Hinweise zur Vorbereitung möglicher Einsätze
  - Registrierte Ansprechpartnerinnen und Ansprechpartner erhalten demnächst Anleitungen und Hinweise, damit bei einem möglichen Vorfall Informationen zu wichtige Fragen vorbereitet werden können
- Das CERT Nord bietet an, in Abstimmung auch vor Ort (z.B. auf Kreisebene) ausführlicher über Leistungen zu berichten und weitergehende Fragen zu klären
  - Sprechen Sie uns dazu einfach an
  - Selbstverständlich klären wir Einzelfragen auch an der Hotline (Durchwahl - 1984)

## Traffic Light Protocol

- Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des FIRST (Forum of Incident Response and Security Team). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
- TLP-eingestufte Dokumente (außer TLP:CLEAR) **dürfen nicht** auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) **hochgeladen werden**, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.

# CERT NORD – Kurz erklärt: TLP

5/6

TLP-Einstufungen	Weitergabe
<b>TLP Clear</b>	<b>Unbegrenzte Weitergabe</b> Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen dieser Stufe ohne Einschränkungen frei weitergegeben werden. Hinweis: TLP:CLEAR entspricht der Kennzeichnung TLP:WHITE der früheren Version 1.0 des TLP.
<b>TLP Green</b>	<b>Organisationsübergreifende Weitergabe</b> Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe, wie beispielsweise Angehörige der Cybersecurity-Community, angehören.
<b>TLP Amber</b>	<b>Eingeschränkte interne und organisationsübergreifende Weitergabe</b> Der Empfänger darf die Informationen dieser Stufe an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisation gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.
<b>TLP Amber+Strict</b>	<b>Eingeschränkte interne Weitergabe</b> Die Einstufung dieser Stufe beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers, jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.
<b>TLP Red</b>	<b>Persönlich, nur für bekannte Empfänger</b> Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/ Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

## Traffic Light Protocol

- TLP ist kaskadierend aufgebaut:
  - Die Mitarbeiterinnen und Mitarbeiter des CERT Nord haben sich gegenüber dem BSI verpflichtet, die Regelungen von TLP einzuhalten
  - Sie erklären sich gegenüber dem CERT Nord, die Regelungen von TLP einzuhalten
  - Wenn Sie in Ihrem Verantwortungsbereich TLP eingestufte Meldungen weitergeben, müssen Sie Ihre Mitarbeiterinnen und Mitarbeiter entsprechend verpflichten
    - Die entsprechende Dokumentation verbleibt in Ihrem Hause
- Die Einstufungen nach TLP sind unbedingt zu beachten, eine Nichtbeachtung führt zu einem Ausschluss zum Zugang zu TLP-eingestuften Dokumenten!

# Gibt es noch offene Fragen?



Vorstellung des CERT Nord  
Neumünster, 22.05.2025