

**Meldung IT-Vorfall an CERT Nord**cert@certnord.de

Tel. 040 42846 1984

Vertraulichkeit:	TLP Clear	(bitte auswählen)	Zur Einstufung der Vertraulichkeit nach TLP (Traffic Light Protocol) siehe Anhang oder Merkblatt des BSI
Behörde:	Bezeichnung, Ort		
Meldender:	Vorname Nachname	Telefon	eMail
Rückfragen: sofern anderer Kontakt als der des Meldenden	Vorname Nachname	Telefon	eMail
Datum:	Datum	Uhrzeit	Tag und Zeit des Vorfalls
Sachverhaltsbeschreibung bitte beschreiben Sie den Sachverhalt			Ggf. Verweis auf beigefügte weitere Dokumente

Leitfragen:

- Wie ist der Vorfall aufgefallen?
- Was ist belegbar (und darüber hinaus vermutlich) passiert?
- Wer bzw. was ist betroffen? Welcher Schaden wurde festgestellt?
- Ist eine Kompromittierung weiterer Systeme in anderen Organisationen wahrscheinlich?
- Wurden bereits (Gegen)Maßnahmen ergriffen? Wenn ja, welche?
- Wurden bereits weitere Stellen informiert?
- Wird Ihre Infrastruktur von Dataport betreut? Wenn ja, melden Sie den Vorfall bitte an den Dataport UHD (das CERT Nord wird von Dataport über den Vorfall informiert).

Falls Sie sich bei der Formulierung unsicher sind, rufen Sie uns gerne an. CERT Nord Hotline 040 42846 1984

Hinweis bei Hardwareverlust:

Bei Hardware, die von Dataport verwaltet wird (z.B. StaPI, Basis, +1), melden Sie den Diebstahl/Verlust bitte sofort an den Dataport UHD, der hierfür einen Sicherheitsvorfall eröffnen wird.

Eine ergänzende Meldung an das CERT Nord ist dann nicht mehr erforderlich, da das CERT Nord von Dataport über diesen Sicherheitsvorfall informiert wird.

Klicken Sie hier, um Text einzugeben.

Erwartete Reaktion durch das CERT Nord: falls Sie unsicher sind, rufen Sie uns bitte an: 040 42846 1984



Bitte um möglichst sofortigen Rückruf durch CERT Nord In diesem Fall sind die weiteren Angaben nicht erforderlich
Alles Weitere wird im Telefonat besprochen



Zur Kenntnisnahme



Bitte um Einschätzung / Stellungnahme
(Rückruf durch CERT Nord erfolgt)



Unterstützung erwünscht
(Rückruf durch CERT Nord erfolgt)

Weitergabe an BSI:

Freigabe zur Aufnahme in den
BSI Lagebericht



Keine Freigabe zur Aufnahme
in den BSI Lagebericht



Freigabe der anonymisierten
Endfassung zur Aufnahme in
den BSI Lagebericht



Explizite Freigabe der
Endfassung zur Aufnahme in
den BSI Lagebericht durch
Meldenden erforderlich

Erläuterungen

Einstufung der Vertraulichkeit

TLP-Einstufung	Weitergabe
TLP Clear	Unbegrenzte Weitergabe 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.
TLP Green	Organisationsübergreifende Weitergabe 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.
TLP Amber	Eingeschränkte interne und organisationsübergreifende Weitergabe 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.
TLP Amber+Strict	Eingeschränkte interne Weitergabe 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.
TLP Red	Persönlich, nur für bekannte Empfänger 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.