

IT-Vorfall

SAX.CERT Meldeformular

Alle Felder mit einem * sind unbedingt auszufüllen. Zutreffendes bitte ankreuzen bzw. ausfüllen!

Meldende Person		
Behörde:*	Information an BfIS:*	
Name:*	Rolle:*	
Vorname:*	Erkannt am:*	Aufgetreten am/seit:*
Email:*	Telefon:*	
Referenznummern:*	Meldungsnummer:	
Bezieht sich die Meldung auf eine SAX.CERT Frühwarnung? (aus dem Ticketsystem des Meldenden)		
Beschreiben Sie den Vorfall:*		

Hat ein Mensch bewusst oder unbewusst einen Schaden verursacht?

Angriff (mit Vorsatz herbeigeführte Aktion oder verursachter Schaden durch Externe)

Dienstvergehen etc. (mit Vorsatz durchgeführte Aktion oder verursachter Schaden durch Interne)

Weitere Details

Belästigungen per Email	Versenden von Malware per Email	Installation von Malware auf Server oder Clients
Missbrauch von Benutzer-Credentials (Passworte,...)	Sammlung von Informationen über mögliche Angriffsziele	Unsachgemäße Entsorgung von IT-Systemen
(Distributed) Denial of Service	Sabotage	Diebstahl oder Verlust von mobilen Datenträgern
Unautorisierte Nutzung von Diensten oder Systemen	Datenabfluss durch Malware, Hacking oder Social Engineering	Diebstahl oder Verlust von IT-Systemen oder mobilen Geräten
Verbreitung illegaler Inhalte (Filme, Fotos,...)	Manipulation von Daten, Hard- oder Software	Offenlegung dienstlicher Informationen

Gab es einen unbeabsichtigt herbeigeführten Schaden oder eine negative Auswirkung oder waren höhere Gewalt oder Umwelteinflüsse im Spiel?

Beeinträchtigung in Form: **einer Störung** verursacht durch wen bzw. durch was:
eines Ausfalls

Betroffene Komponenten

Stromversorgung, USV	Kühlung	Datenverbindungen (Leitungsgebunden oder drahtlose Verfahren)
Landesnetz (SVN)	Betriebsräume	Bürräume/Gebäude
Endgeräte	Server, Storage, Cluster, etc.	Netzwerkkomponenten, Sicherheitsinfrastruktur
Eigene Fachverfahren	Landeseigene Fachverfahren	Fachverfahren Bund
Internet- / Telekommunikationsanbieter	Housing / Hosting-Anbieter	IT-Dienstleister, Dienstanbieter, Clouds

Handelt es sich um ein anderes meldewürdiges Ereignis?

Zum Beispiel:

Technische Schwachstelle in z.B. Software	Organisatorische Schwachstellen	Physikalische Schwachstellen
Operative Schwachstelle in Konfigurationen oder RZ	Bisher unbekannte Angriffsverfahren oder -werkzeuge	Bisher von Anti-Virus-Tools nicht erkannte Malware
Hinweise auf neue Tätergruppe(n)	Hinweis auf akute Bedrohung, z.B. durch Drohbrief	Information über Systeme, die für Angriffe verwendet werden, z.B. Bot-C&C-Server, Upload-Server

Andere:

Einschätzungen und Bewertungen bzgl. des Ausmaßes und der Folgen:
(Angaben nach bestem Wissen und Gewissen)

Betroffen ist: (maximal)

- Person
- Referat
- Abteilung
- kritischer Prozeß
- Fachverfahren
- Behörde

Vorfall/Schäden sind:

- vermutet
- gemeldet, unbestätigt
- gemeldet, bestätigt
- selbst festgestellt

Auswirkung auf Daten:

- Einsichtnahme
- Abfluss
- Manipulation
- Verlust
- unbekannt
- keine

Bei bekannten Auswirkungen:

Wurde dadurch der Datenschutz verletzt?