STAATSBETRIEB SÄCHSISCHE INFORMATIK DIENSTE | Freistaat SACHSEN

Staatsbetrieb Sächsische Informatik Dienste
SAX.CERT-Team
Riesaer Str. 7
01129 Dresden
Tel.: 0351 79 997 799

IT-Vorfall TLP-Green

SAX.CERT Meldeformular

Formular ID:

Prüfsumme:

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:*

Bezieht sich die Meldung auf eine SAX.CERT Frühwarnung?

Referenznummern:* (aus dem Ticketsystem des Meldenden)

Meldungsnummer:

Beschreiben Sie den Vorfall:*

☐ Hat ein Mensch bewusst / vorsätzlich 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

Formular ID:

Prüfsumme:

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

Beeinträchtigung in Form: ☐ **einer Störung** ☐ **eines Ausfalls**

verursacht durch wen bzw. durch was:

Betroffene Komponenten

☐ Stromversorgung, USV	☐ Kühlung	☐ Datenverbindungen (Leitungsgebunden oder drahtlose Verfahren)
☐ Landesnetz (SVN)	☐ Betriebsräume	☐ Büroräume/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?

Drucken | Löschen | Speichern | Versenden

sid_saxcert

Stand: AKITEG-Beschluss 1/2016 vom 12.Januar 2016