

Sicherheit „as a Service“ – Die Angebote des SAX.CERT für Behörden



Prof. Dr. Karol Kozak, Leiter SAX.CERT

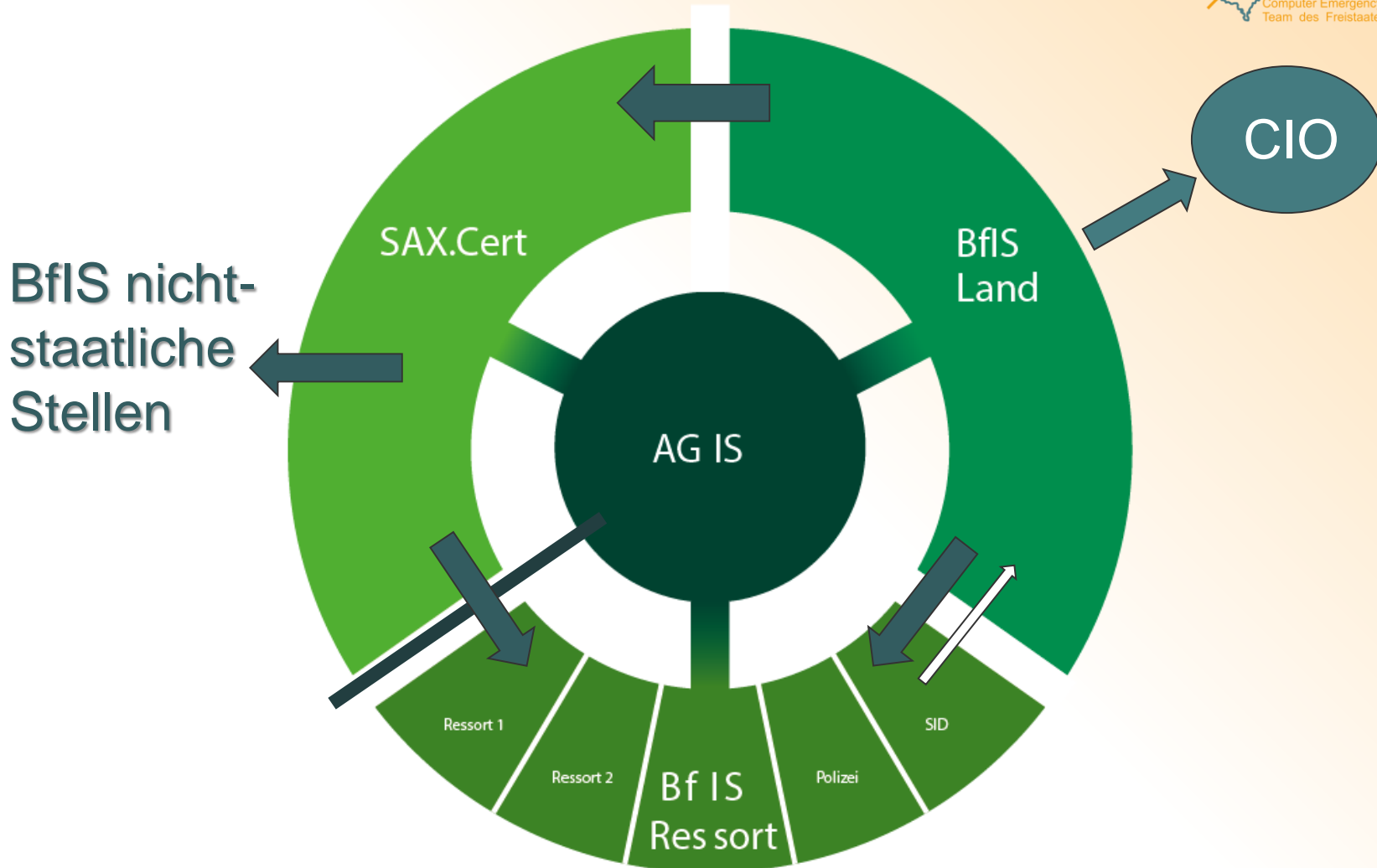
SAX.CERT



Das SAX.CERT ist das Sicherheitsnotfallteam (**Computer Emergency Response Team**) des Freistaates Sachsen.

Es unterstützt den Beauftragten für Informationssicherheit des Landes und die Beauftragten für Informationssicherheit der staatlichen, nicht-staatlichen Stellen des Freistaates (auch **Kommunen**) in technischen Sicherheitsfragen.

Die Rolle des SAX.CERT in der Informationssicherheitsorganisation



Leistungen des SAX.CERT für die Kommunen



- das **Aufzeigen** von Lösungen bei konkreten Sicherheitsereignissen oder -Vorfällen
- die **Information** zu Sicherheitslücken
- die Erfassung und Analyse der **Lage** der Informationssicherheit
- **Meldestelle für Sachsen** im Verwaltungs-CERT-Verbund
 - Weitergabe von Infos, Warnmeldungen, und Frühwarnungen an Kommunen
- die **regelmäßige Information** über die Lage der Informationssicherheit im Freistaat Sachsen.

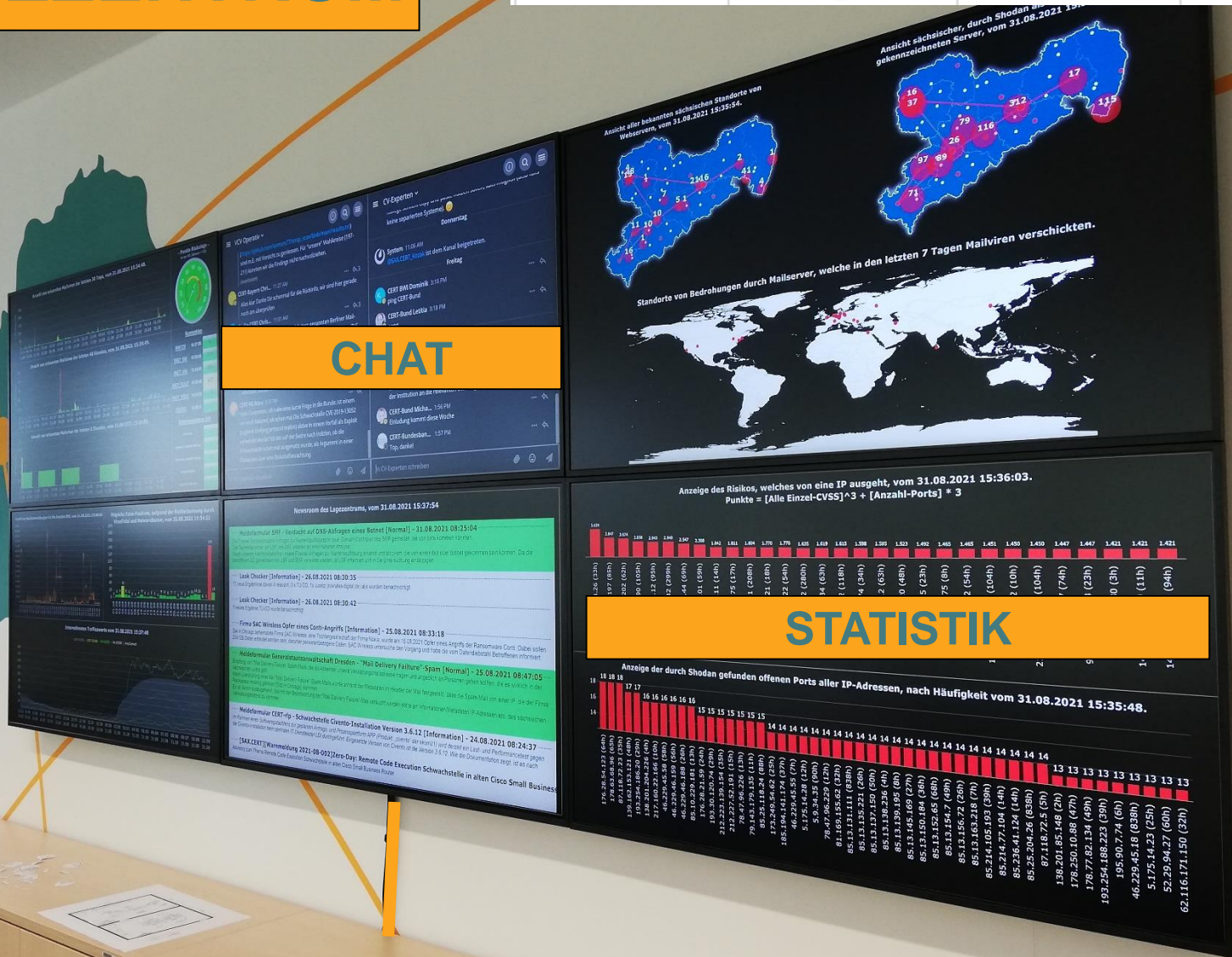
LAGEZENTRUM

A. Fitness
(Prävention)

B. Monitoring

C. Notfall

D. Auswertung



CHAT

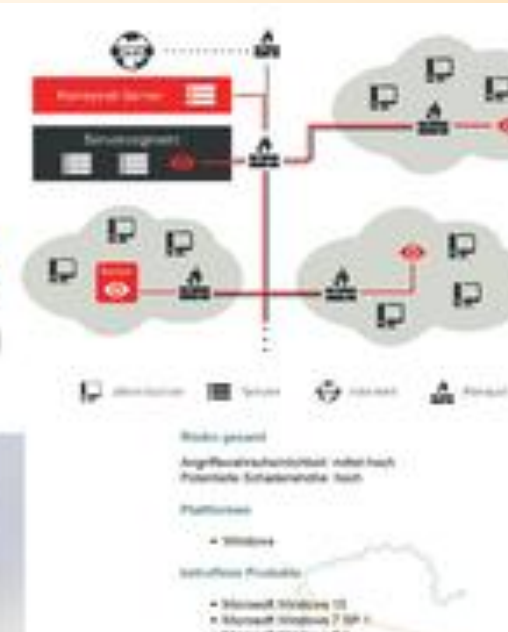
STATISTIK

Sicherheit „as a Service“ – kostenfrei für Kommunen

A. Fitness (Prävention)	B. Monitoring	C. Notfall	D. Auswertung

Produkte und Tools:

- Vulnerability Advisory Service
- HoneySens
- Webseitenscans
- Identity Leak Checker
- Meldeformular



WEBSEITENSCANS



A. Fitness (Prävention)	B. Monitoring	C. Notfall	D. Auswertung
✓	✓		

Das SAX.CERT führt monatlich mindestens zwei Sicherheitsscans aller bekannten Webseiten und Dienste durch. Dabei werden Sicherheitsmerkmale des verwendeten HTTPS-Protokolls geprüft und die eingesetzte Dienste-Software inklusive.

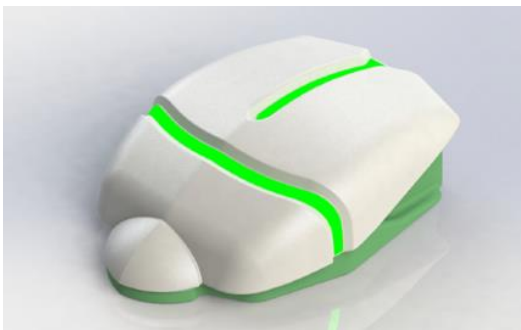


Hackerfalle HoneySens



A. Fitness (Prävention)	B. Monitoring	C. Notfall	D. Auswertung
	✓		

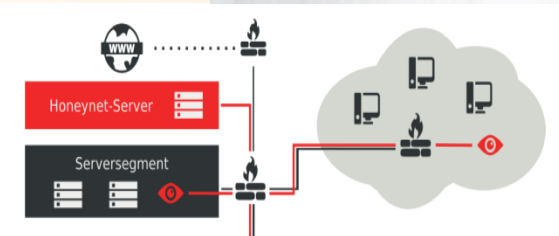
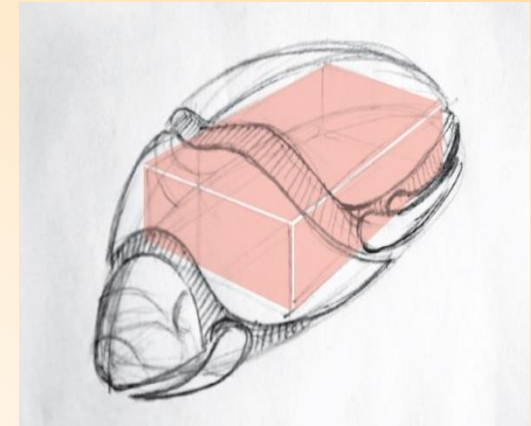
HoneySens ist eine Sicherheitslösung zur Erkennung von Hacker-Angriffen in internen Netzwerken, bestehend aus Sensoren/Clients zur Überwachung des Netzwerks sowie einer zentralen Serverinstanz, an die die Clients verdächtige Zugriffsversuche melden



Hackerfalle HoneySens

- Hohe Bedeutung der Innenerkennung von Schadsoftware und Hackern.
- Lösung: Hackerfallen mit zentralem Management und Service, ideal auch für KMU und Kommunen.
- Industriepartner: T-Systems MMS.

Rundum-Betrieb oder Open Source.



VULNERABILITY ADVISORY SERVICE



A. Fitness (Prävention)	B. Monitoring	C. Notfall	D. Auswertung
	✓		

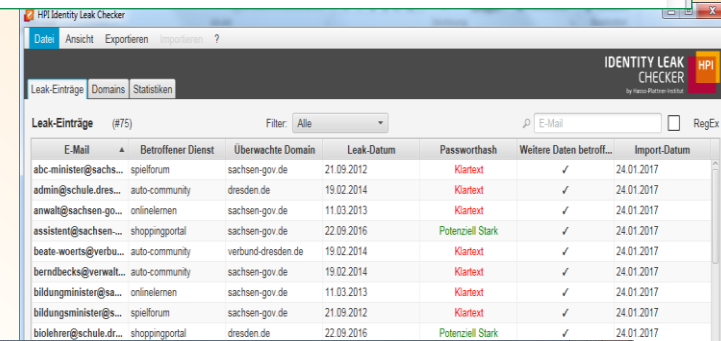
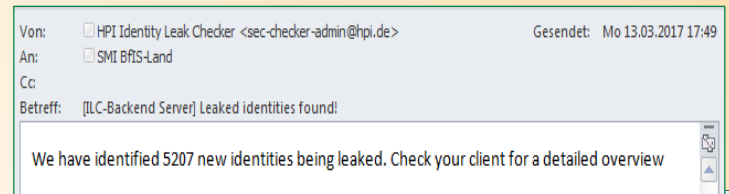
- „Software enthält Schwachstellen“
„Ohne Gegenmaßnahmen stellen sie ein Risiko dar“
- 2000 Hard- und Softwareprodukte in der Überwachung
- Per E-Mail werden die Abonnenten des Dienstes täglich über Schwachstellen in der Software informiert und Gegenmaßnahmen dargestellt.



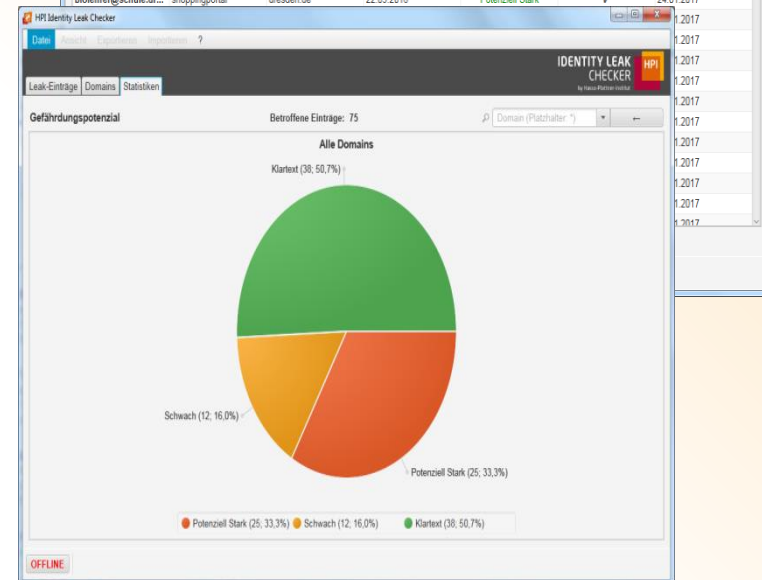
Identity Leak Checker

- 2014: BSI findet 18 Mio. Identitäten, HPI startet Leak Checker und die Zusammenarbeit mit Land Sachsen.
- Im Jahr 2021 891 (391 sachsen.de, 500 Kommune) gestohlene Identitäten im Freistaat gefunden.
- ILC-Client warnt Abonnenten bei neuen Veröffentlichungen.

Lösung für alle Kommunen nutzbar!



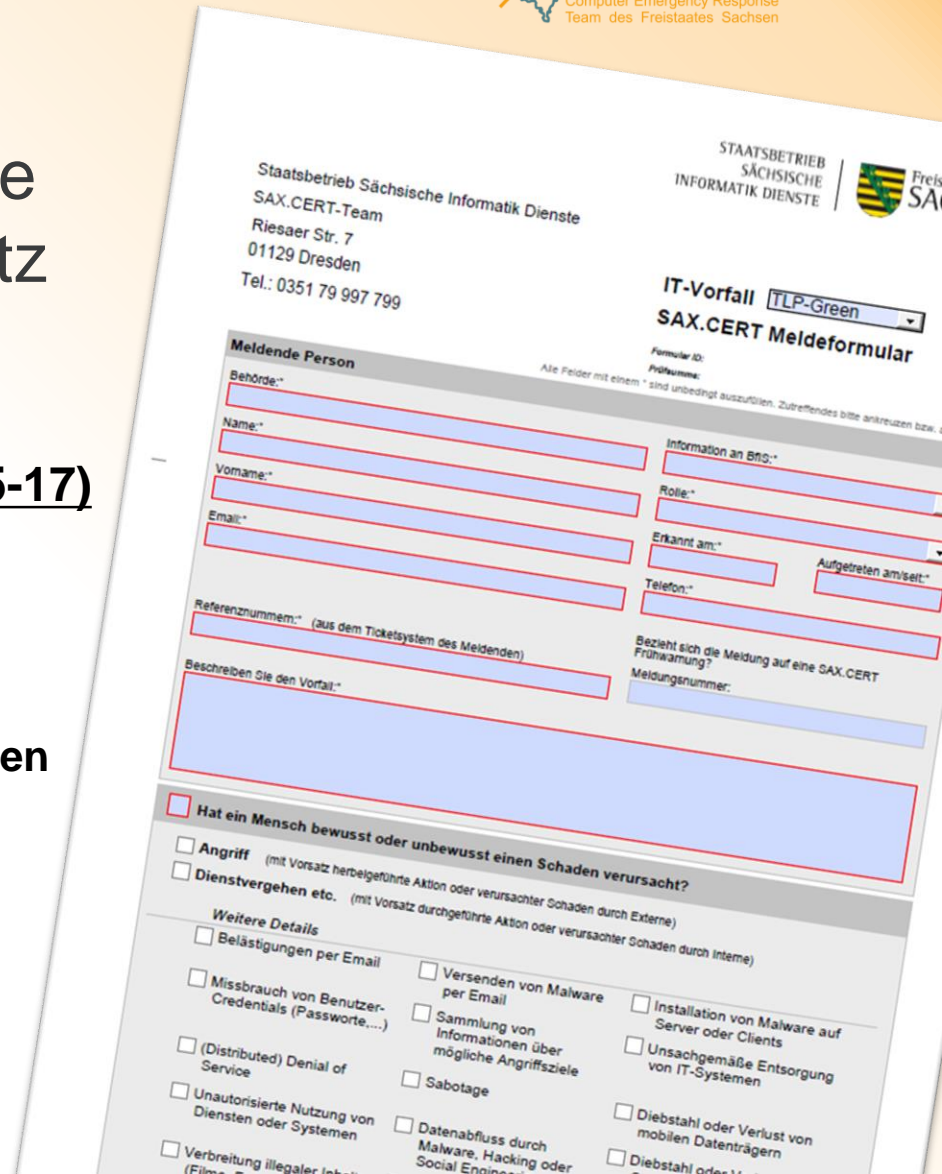
E-Mail	Betroffener Dienst	Überwachte Domain	Leak-Datum	Passwortshash	Weitere Daten betroff...	Import-Datum
abc-minister@sachs...	spielforum	sachsen-gov.de	21.09.2012	Klartext	✓	24.01.2017
admin@schule.dres...	auto-community	dresden.de	19.02.2014	Klartext	✓	24.01.2017
anwahl@sachsen-go...	onlinelernen	sachsen-gov.de	11.03.2013	Klartext	✓	24.01.2017
assistent@sachsen...	shoppingportal	sachsen-gov.de	22.09.2016	Potenziell Stark	✓	24.01.2017
beate-woerts@verbu...	auto-community	verbund-dresden.de	19.02.2014	Klartext	✓	24.01.2017
berndbecks@verwalt...	auto-community	sachsen-gov.de	19.02.2014	Klartext	✓	24.01.2017
bildungsminister@sa...	onlinelernen	sachsen-gov.de	11.03.2013	Klartext	✓	24.01.2017
bildungsminister@s...	spielforum	sachsen-gov.de	21.09.2012	Klartext	✓	24.01.2017
birolehrer@schule.dr...	shoppingportal	dresden.de	22.09.2016	Potenziell Stark	✓	24.01.2017



Meldepflichten auf Grundlage Informationssicherheitsgesetz

Abschnitt 4: Meldepflichten (§ § 15-17)

- Behördenübergreifende Meldepflichten
- Meldepflichten der staatlichen Stellen
- **Meldepflichten der nicht-staatlichen Stellen**



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

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

IT-Vorfall **TLP-Green**
SAX.CERT Meldeformular

Formular ID:
Prüfnummer:

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

Meldende Person

Behörde: *
Name: *
Vorname: *
Email: *

Information an BfS: *
Rolle: *
Erkannt am: *
Aufgetreten am/seit: *
Telefon: *

Referenznummer: * (aus dem Ticketsystem des Meldenden)

Bezieht sich die Meldung auf eine SAX.CERT Frühwarnung?
Meldungsnummer:

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 Daten
 Verbreitung illegaler Inhalte (Filtern)

MELDEPLICHT – Meldekategorien



Kategorisierung durch die meldende Person

- | | | | | |
|---------------------------------------|---------------------------------------|--|---|--|
| <input type="checkbox"/> Ransomware | <input type="checkbox"/> Drohbrief | <input type="checkbox"/> DDoS | <input type="checkbox"/> Geräteverlust | <input type="checkbox"/> Datenverlust |
| <input type="checkbox"/> Einbruch | <input type="checkbox"/> Störung | <input type="checkbox"/> Diebstahl | <input type="checkbox"/> Naturgewalten | <input type="checkbox"/> Schadprogramm |
| <input type="checkbox"/> Datenabfluss | <input type="checkbox"/> Manipulation | <input type="checkbox"/> Unberechtigte Nutzung | <input type="checkbox"/> Social Engineering | <input type="checkbox"/> Datenmissbrauch |
| <input type="checkbox"/> andere | <input type="text"/> | | | |
| <input type="checkbox"/> andere | <input type="text"/> | | | |
| <input type="checkbox"/> andere | <input type="text"/> | | | |

Betroffen ist (maximal):

Personen

Kritischer Prozess

Vorfall/Schäden sind:

FRAGEN?

Sie finden uns unter:
www.cert.sachsen.de

SAX.CERT

im Staatsbetrieb Sächsische Informatik
Dienste

Telefon (+49) 0351 79 99 77 99

E-Mail: sax.cert@cert.sachsen.de



Kooperationen



- Allianz für Cyber-Sicherheit
- CERT-Bund
- CERT-Verbund
- Verwaltungs-CERT-Verbund