

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



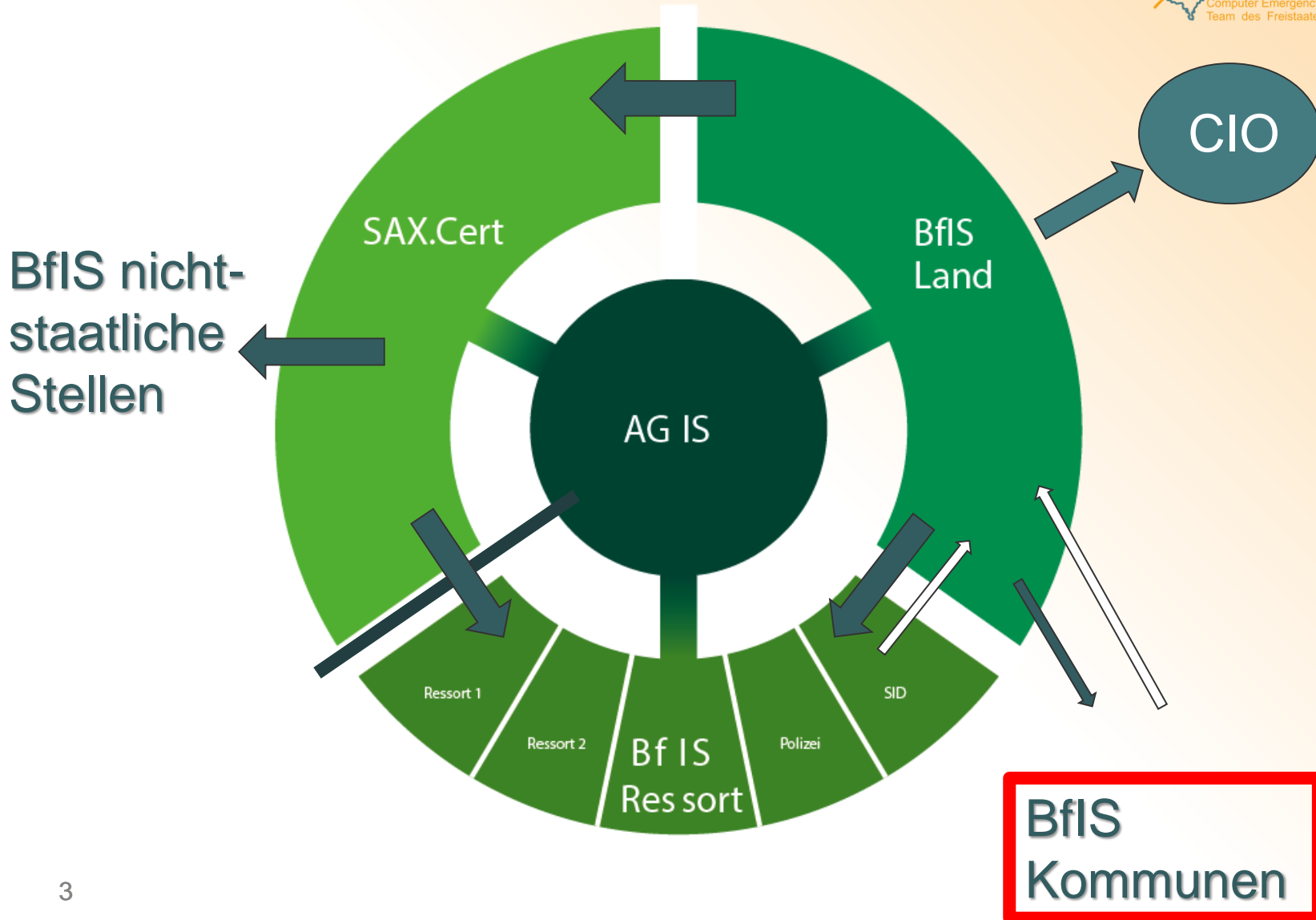
# SAX.CERT



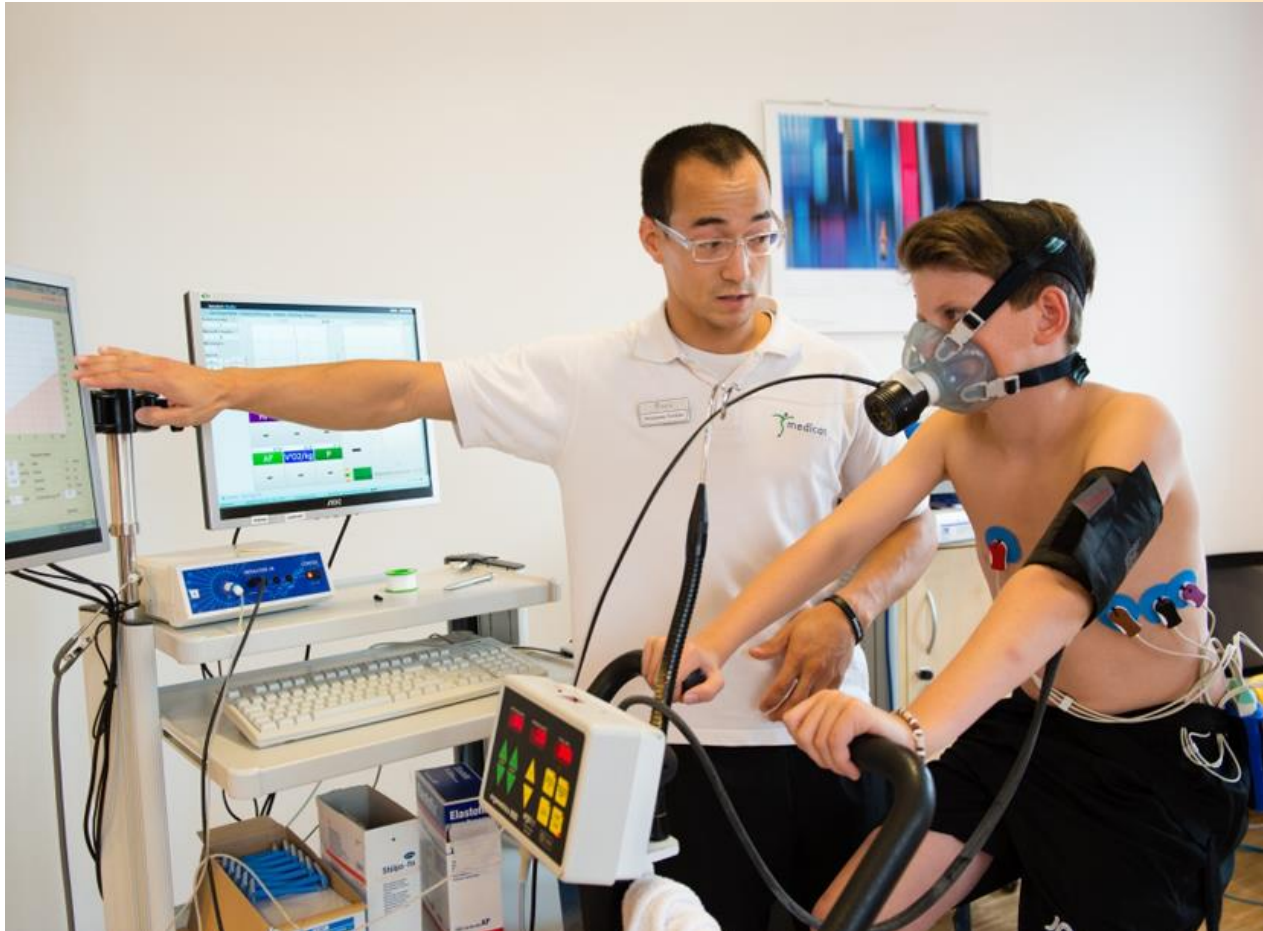
Das SAX.CERT ist das Sicherheitsnotfallteam (**Computer Emergency Response Team**) des Freistaates Sachsen.

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



# Cybersicherheit für große Infrastruktur ist eine Strategie



# PRIORITÄTEN VON SAX.CERT

|                                    |                      |                   |                      |
|------------------------------------|----------------------|-------------------|----------------------|
| <b>A. Fitness<br/>(Prävention)</b> | <b>B. Monitoring</b> | <b>C. Notfall</b> | <b>D. Auswertung</b> |
|                                    |                      |                   |                      |



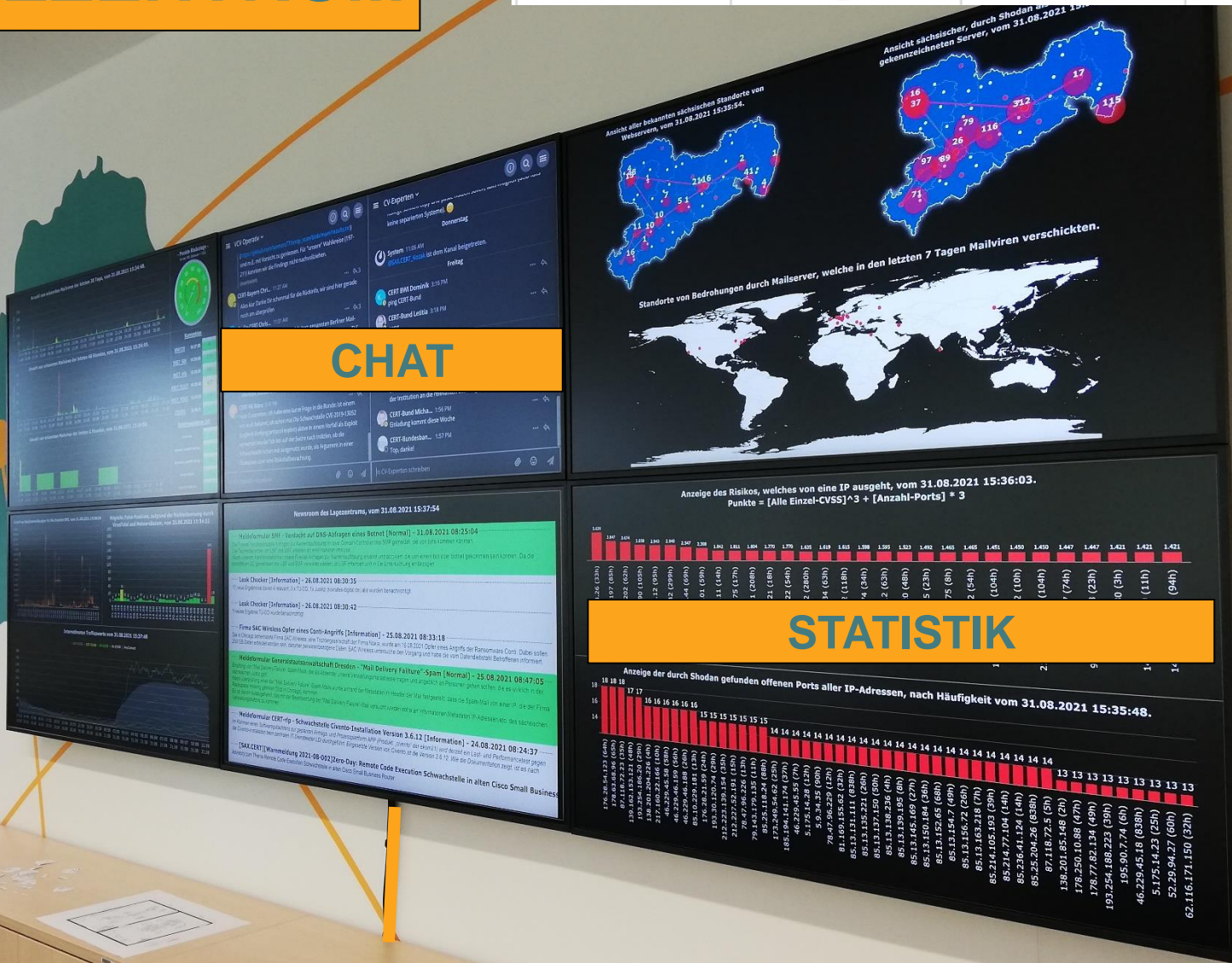
# LAGEZENTRUM

A. Fitness  
(Prävention)

B. Monitoring

C. Notfall

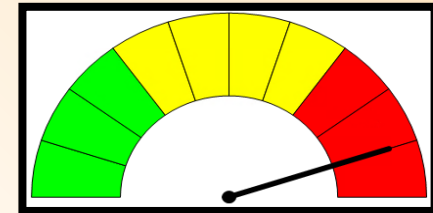
D. Auswertung





# 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.



# Technologie: CERT Komponenten

## SERVERRARUM



## LAGEZENTRUM



## DATENBANKEN



## RESPONSE TEAM





# CERT Portal

|                            |               |            |               |
|----------------------------|---------------|------------|---------------|
| A. Fitness<br>(Prävention) | B. Monitoring | C. Notfall | D. Auswertung |
|----------------------------|---------------|------------|---------------|

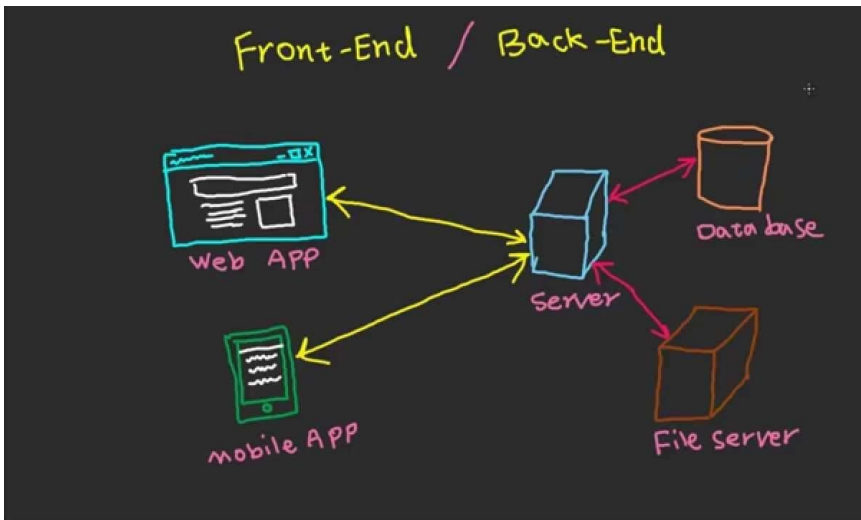


WOC - WorkingOnCert V0.14b [kozakka@SID-NOT-U14247]

Einstellungen und Informationen Listen SQL-Direktzugriff

Kontakte Kommunen Bedrohungen IPs SVN/KDN HTTP-Proxy-Liste Dokumentensuche ePO-Events IP-Liste Shodan Infos Newsroom

| Nr. | IP-Adresse | Port | Prot. | Produkt+Version        | CVE           | CVE-CVSS ↓ | CVE verified | CVE-Bes   |
|-----|------------|------|-------|------------------------|---------------|------------|--------------|-----------|
| 1   |            | 80   | tcp   | Apache httpd2.4.6      | CVE-2016-0705 | 10         | 0            | Double f  |
| 2   |            | 80   | tcp   | Apache httpd2.4.6      | CVE-2016-0705 | 10         | 0            | Double f  |
| 3   |            | 4443 | tcp   | Microsoft IIS httpd7.5 | CVE-2010-3972 | 10         | 0            | Heap-ba   |
| 4   |            | 21   | tcp   | ProFTPD 1.3.5          | CVE-2015-3306 | 10         | 0            | The mod   |
| 5   |            | 443  | tcp   | Microsoft IIS httpd6.0 | CVE-2017-7269 | 10         | 0            | Buffer ov |
| 6   |            | 80   | tcp   | Apache httpd2.4.6      | CVE-2016-2842 | 10         | 0            | The doap  |
| 7   |            | 80   | tcp   | Apache httpd2.4.6      | CVE-2016-0799 | 10         | 0            | The fmts  |
| 8   |            | 80   | tcp   | Microsoft IIS httpd5.0 | CVE-2007-2815 | 10         | 0            | The 'hit- |
| 9   |            | 443  | tcp   | Microsoft IIS httpd6.0 | CVE-2008-0075 | 10         | 0            | Unspecif  |
| 10  |            | 21   | tcp   | ProFTPD 1.3.5          | CVE-2015-3306 | 10         | 0            | The mod   |
| 11  |            | 80   | tcp   | Microsoft IIS httpd5.0 | CVE-2003-0224 | 10         | 0            | Buffer ov |



sachsen.de SAX.CERT Informationsportal

Meine Daten > Webseiten

+ Webseite hinzufügen Daten exportieren

Spalten ein-/ ausblenden Daten filtern

list Online

| Webseite                      | Online | inhaltl. Verantwortung   | Server IP      | Server Standort |   |
|-------------------------------|--------|--------------------------|----------------|-----------------|---|
| opal.sachsen.de               | ONLINE | sax.cert@cert.sachsen.de | 134.109.133.26 | DE Chemnitz     | ✓ |
| www.opal.sachsen.de           | ONLINE | sax.cert@cert.sachsen.de | 134.109.133.26 | DE Chemnitz     | ✓ |
| www.bildungsportal.sachsen.de | ONLINE | sax.cert@cert.sachsen.de | 134.109.133.26 | DE Chemnitz     | ✓ |
| bildungsportal.sachsen.de     | ONLINE | sax.cert@cert.sachsen.de | 134.109.133.26 | DE Chemnitz     | ✓ |
| ioer.de                       | ONLINE | sax.cert@cert.sachsen.de | 134.119.38.105 | DE Ismaning     | ✓ |
| www.ioer.de                   | ONLINE | sax.cert@cert.sachsen.de | 134.119.38.105 | DE Ismaning     | ✓ |
| saw-leipzig.de                | ONLINE | sax.cert@cert.sachsen.de | 136.243.80.202 | DE Falkenstein  | ✓ |
| www.saw-leipzig.de            | ONLINE | sax.cert@cert.sachsen.de | 136.243.80.202 | DE Falkenstein  | ✓ |
| www.leibniz-gwzo.de           | ONLINE | sax.cert@cert.sachsen.de | 139.18.16.156  | DE Markkleeberg | ✓ |
| oembed.leibniz-gwzo.de        | ONLINE | sax.cert@cert.sachsen.de | 139.18.16.156  | DE Markkleeberg | ✓ |

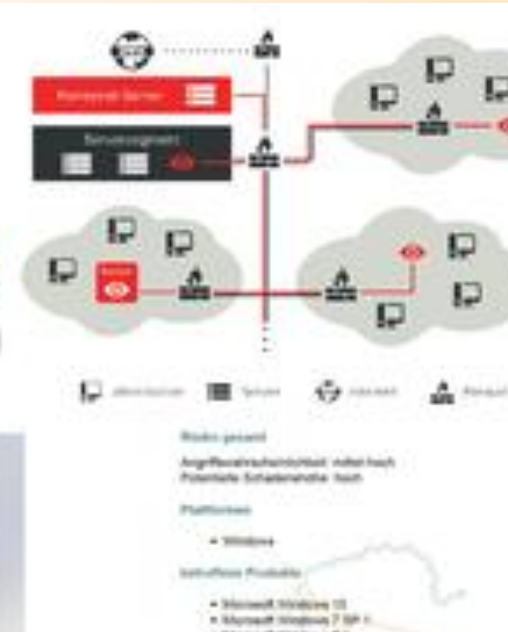
10 von 289

# Sicherheit „as a Service“ – kostenfrei für Kommunen

| A. Fitness<br>(Prävention) | B. Monitoring | C. Notfall | D. Auswertung |
|----------------------------|---------------|------------|---------------|
|                            |               |            |               |

## Produkte und Tools:

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

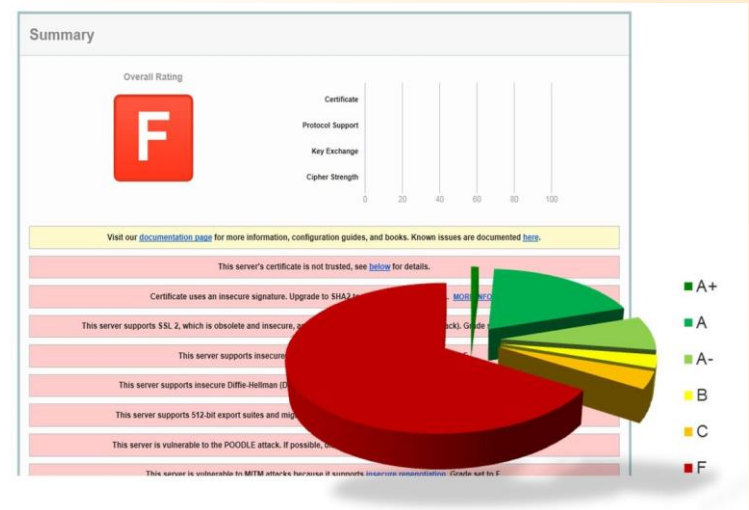


# WEBSEITENSCANS

|                            |               |            |               |
|----------------------------|---------------|------------|---------------|
| A. Fitness<br>(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.

7000 Seiten  
SVN und  
Kommunen

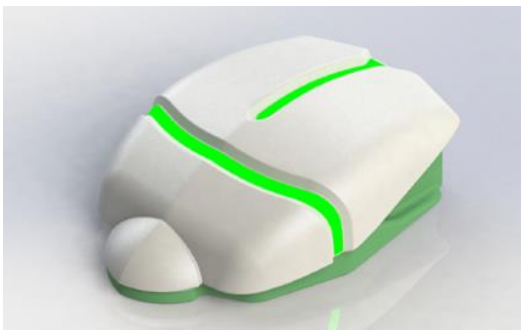


# Hackerfalle HoneySens



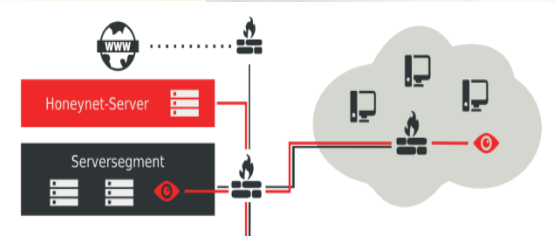
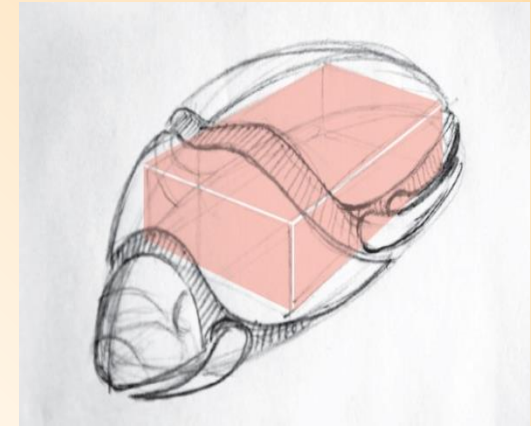
| A. Fitness<br>(Prävention) | B. Monitoring | C. Notfall | D. Auswertung |
|----------------------------|---------------|------------|---------------|
|                            | ✓             |            |               |

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.

**24 Nutzer mit 29 Sensoren, davon sind 15 Sensoren in Kommunen**



# VULNERABILITY ADVISORY SERVICE



| A. Fitness<br>(Prävention) | B. Monitoring | C. Notfall | D. Auswertung |
|----------------------------|---------------|------------|---------------|
|                            | ✓             |            |               |

- „Software enthält Schwachstellen“  
„Ohne Gegenmaßnahmen stellen sie ein Risiko dar“
- 2000 Hard- und Softwareprodukten  
106 Abonnenten im Freistaat Sachsen aktiv genutzt (83 im Bereich Land, 20 im Bereich Kommunen).
- Per E-Mail werden die Abonnenten des Dienstes täglich über Schwachstellen in der Software informiert und Gegenmaßnahmen dargestellt.

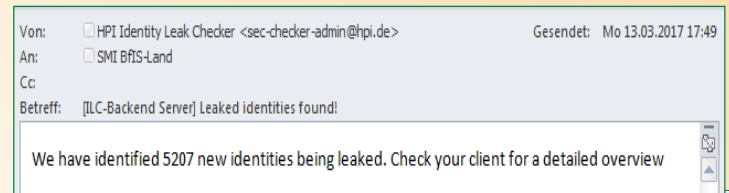


# Identity Leak Checker

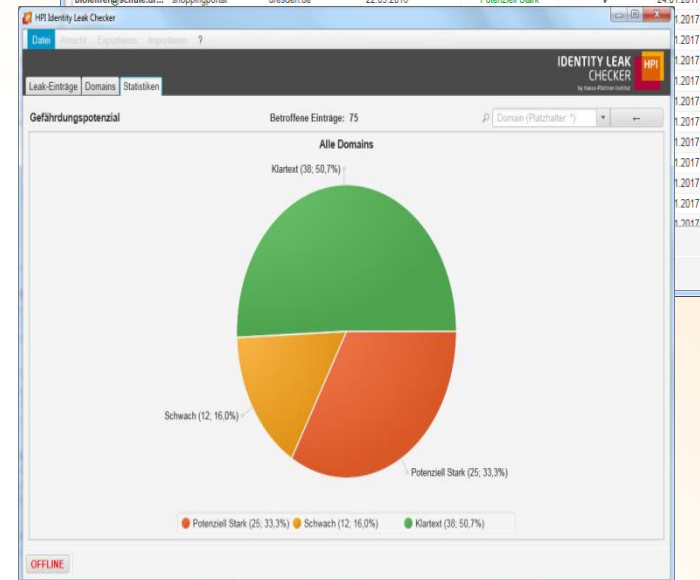


- 2014: BSI findet 18 Mio. Identitäten, HPI startet Leak Checker und die Zusammenarbeit mit Land Sachsen.
- Im Jahr 2021 **5800 (391 sachsen.de, 500 Kommune)** gestohlene Identitäten im Freistaat gefunden.
- ILC-Client warnt Abonnenten bei neuen Veröffentlichungen.

**Lösung für alle Kommunen nutzbar!**



| E-Mail                  | Betroffener Dienst | Überwachte Domain  | Leak-Datum | Passwortsch      | 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   |



# PASSWORTCHECKER

|                            |               |            |               |
|----------------------------|---------------|------------|---------------|
| A. Fitness<br>(Prävention) | B. Monitoring | C. Notfall | D. Auswertung |
| ✓                          |               |            |               |

Einer der wichtigsten Sicherheitsaspekte einer IT-Landschaft sind Passwörter!

- <https://apps.sachsen.de/cert/passwortcheck/>

Der Passwortchecker berechnet aus einem eingegebenen Passwort einen Gesamtpunktwert, welcher die Passwortstärke messbar darstellt.

*Nur Land SVN Netz  
Extern – in Diskussion*

### Passwortchecker v1.0.0

Passwort:   sichtbar

| Kriterium   | Messung   | Punkte     |
|---|---|------------|
| Länge des Passwortes  | 5 Punkte pro Zeichen<br>=> 34 Zeichen   | 170        |
| Wörterbuch  | -2 Punkte pro Übereinstimmung pro Zeichen<br>[Ein,sicheres,Passwort,ist,wichtig] => 5 Teile => 29 Zeichen | -58        |
| Bewertung der übrigen Zeichen, welche nicht in der Wörterbuchliste vorkommen. |   |            |
| Kleinbuchstaben   | 15 Punkte, falls Kleinbuchstaben vorhanden  | 0          |
| Großbuchstaben  | 15 Punkte, falls Großbuchstaben vorhanden   | 0          |
| Zahlen  | 10 Punkte, falls Zahlen vorhanden   | 0          |
| Sonderzeichen   | 10 Punkte, falls Sonderzeichen vorhanden  | 10         |
| Sonderzeichen am Ende   | -10 Punkte, falls ein einfaches Sonderzeichen [#!?=+&] am Ende steht                                      | 0          |
| Passwortlänge kleiner 12  | -20 Punkte, falls die Passwortlänge kleiner 12 Zeichen beträgt  | 0          |
| <b>Gesamtpunkte</b>   |   | <b>122</b> |

Ein Angreifer würde **mehrere Jahrtausende** benötigen, um Ihr Passwort per Brute-force zu überwinden. Um diesen Aufwand in Zeit zu schätzen, wird angenommen, dass ein Angreifer fünf Milliarden Versuche pro Sekunde durchführen kann. Dies entspricht der Rechenleistung eines guten Heim-PC.



# 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. auswählen.

**Meldende Person**

Behörde: \*  
Name: \*  
Vorname: \*  
Email: \*  
Referenznummer: \* (aus dem Ticketsystem des Meldenden)  
Beschreiben Sie den Vorfall: \*

Information an BfSG: \*  
Rolle: \*  
Erkannt am: \*  
Telefon: \*  
Aufgetreten am/seit: \*  
Bezieht sich die Meldung auf eine SAX.CERT Frühwarnung?  
Meldungsnummer: \*

**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**

|   |  |   |
|---|--|---|
| <input type="checkbox"/> Belästigungen per Email                                    | <input type="checkbox"/> Versenden von Malware per Email                             | <input type="checkbox"/> Installation von Malware auf Server oder Clients |
| <input type="checkbox"/> Missbrauch von Benutzer-Credentials (Passworte,...)        | <input type="checkbox"/> Sammlung von Informationen über mögliche Angriffsziele      | <input type="checkbox"/> Unsachgemäße Entsorgung von IT-Systemen          |
| <input type="checkbox"/> (Distributed) Denial of Service                            | <input type="checkbox"/> Sabotage  | <input type="checkbox"/> Diebstahl oder Verlust von mobilen Datenträgern  |
| <input type="checkbox"/> Unautorisierte Nutzung von Diensten oder Systemen          | <input type="checkbox"/> Datenabfluss durch Malware, Hacking oder Social Engineering | <input type="checkbox"/> Diebstahl oder Verlust von Daten                 |
| <input type="checkbox"/> Verbreitung illegaler Inhalte (Filme, Musik, Software,...) |  |   |

# MELDEPLICHT – Meldekategorien

**Kategorisierung durch die meldende Person**

Ransomware   
  Drohbrief   
  DDoS   
  Geräteverlust   
  Datenverlust

Einbruch   
  Störung   
  Diebstahl   
  Naturgewalten   
  Schadprogramm

Datenabfluss   
  Manipulation   
  Unberechtigte Nutzung   
  Social Engineering   
  Datenmissbrauch

andere

andere

andere

Betroffen ist (maximal):  
 Personen  
 Kritischer Prozess

Vorfall/Schäden sind:

# FRAGEN?

Sie finden uns unter:  
[www.cert.sachsen.de](http://www.cert.sachsen.de)

## SAX.CERT

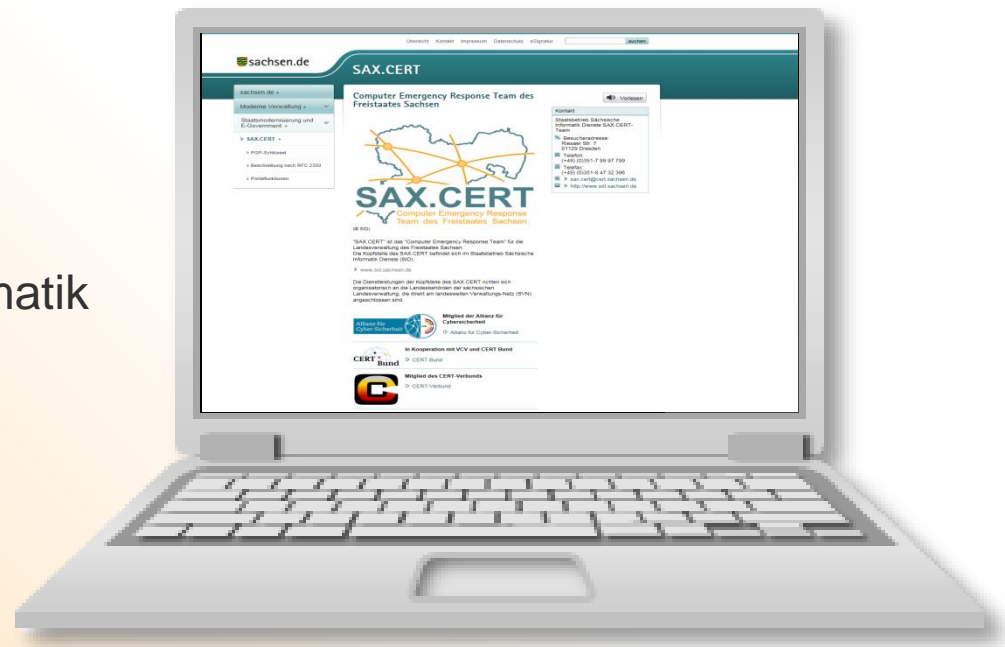
im Staatsbetrieb Sächsische Informatik  
Dienste

Glacisstr. 4

01099 Dresden

Telefon (+49) 0351 79 99 77 99

E-Mail: [sax.cert@cert.sachsen.de](mailto:sax.cert@cert.sachsen.de)



# Kooperationen



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