

Aber sicher?!

Informationssicherheit und
Datenschutz





Informationssicherheit



1

Informationssicherheit

Sicherheitslage

2

Informationssicherheit

Rechtsgrundlagen und Begriffe

3

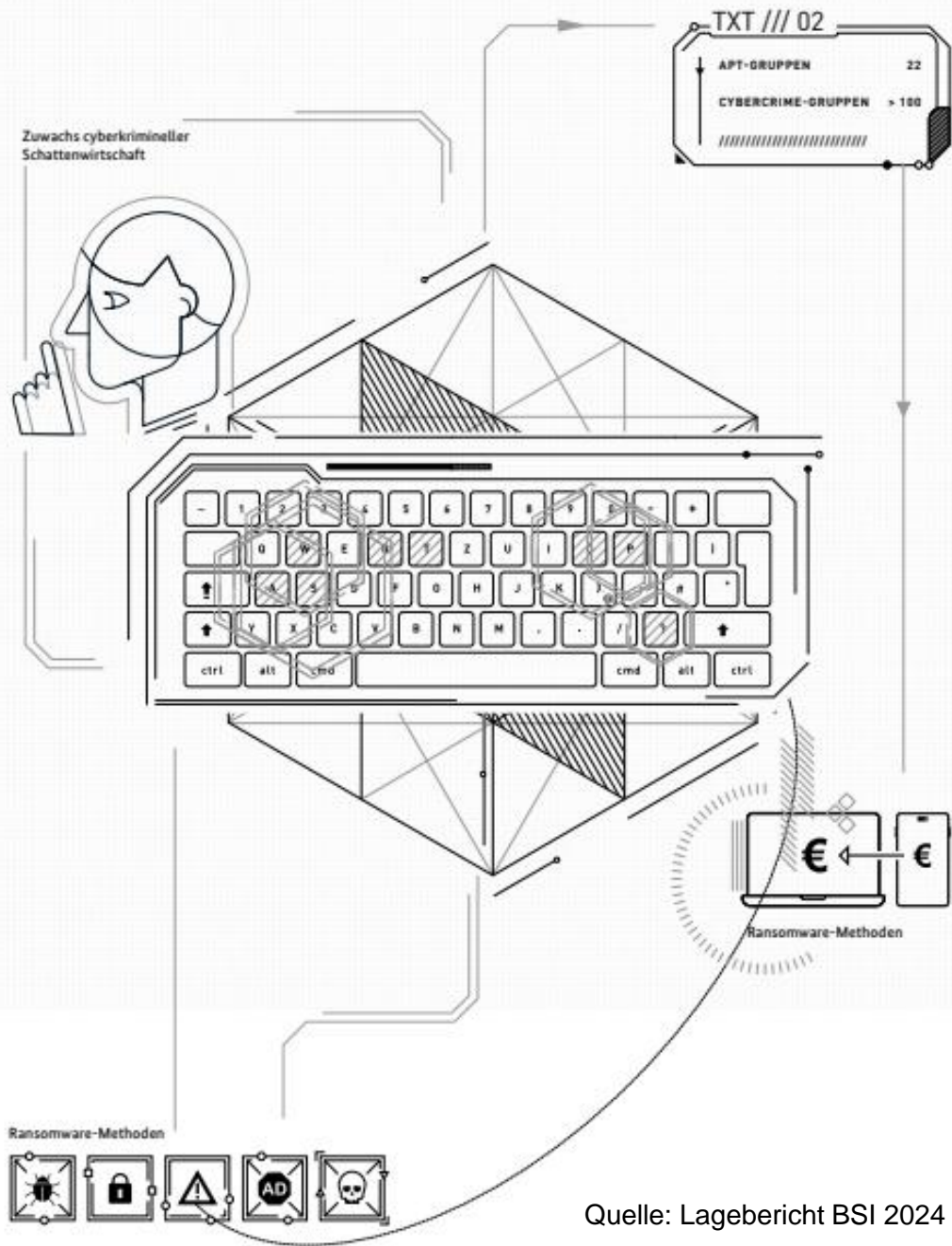
Informationssicherheit

Ganz praktisch

4

Informationssicherheit

Was müssen wir tun?



Sicherheitslage

Quelle: Lagebericht BSI 2024

Warum?

- Sächsische Kommunen sind verpflichtet, die Sicherheit ihrer informationstechnischen Systeme zu gewährleisten. (§ 4 Absatz 2 SächsISichG)
- Der Behördenleiter trägt die Verantwortung dafür, dass gesetzliche Regelungen eingehalten werden und dass wichtige Geschäftsprozesse störungsfrei ablaufen. (§ 4 Absatz 3 SächsISichG)
- Pflicht, einen Beauftragten für Informationssicherheit (BfIS) in jeder Kommune zu benennen; ggf. in kommunaler Zusammenarbeit oder über Dienstleister. (§ 8 Absatz 1 SächsISichG)

Sächsisches Informationssicherheitsgesetz

Vollzitat: Sächsisches Informationssicherheitsgesetz vom 2. August 2019 (SächsGVBl. S. 630), das zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 22. Juli 2024 (SächsGVBl. S. 706) und durch das Gesetz vom 5. Juli 2024 (SächsGVBl. S. 590) geändert worden ist

⊕ Eingangformel

⊕ Inhaltsübersicht

⊕ Abschnitt 1 Allgemeine Vorschriften

⊕ § 1 Zweck des Gesetzes

⊕ § 2 Anwendungsbereich

⊕ § 3 Begriffsbestimmungen

⊕ § 4 Grundsätze der Informationssicherheit

⊕ Abschnitt 2 Organisation der Informationssicherheit

⊕ § 5 Beauftragte oder Beauftragter für Informationssicherheit des Landes

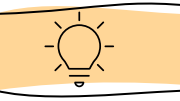
⊕ § 6 Sicherheitsnotfallteam

⊕ § 7 Beauftragte für Informationssicherheit der staatlichen Stellen

⊕ § 8 Beauftragte für Informationssicherheit der nicht-staatlichen Stellen

Was ist was?

Begriffe jonglieren



Informationssicherheit

Schutz jeglicher, **auch nicht elektronischer** Informationen

Cyber-Sicherheit

Schutz elektronischer Systeme
sowie unterstützender Prozesse

IT-Sicherheit

Schutz elektronischer Daten
und Systeme

Was ist was?

Bildet Zweiergruppen!

Welche Begriffe fallen Euch
im Kontext Sicherheit ein?

Schreibt je einen Begriff auf ein Post it
und ordnet ihn zu.



Wozu?

§ 3 Absatz 1
Sächs.
Informationssicherheits-
gesetz

Vertraulichkeit

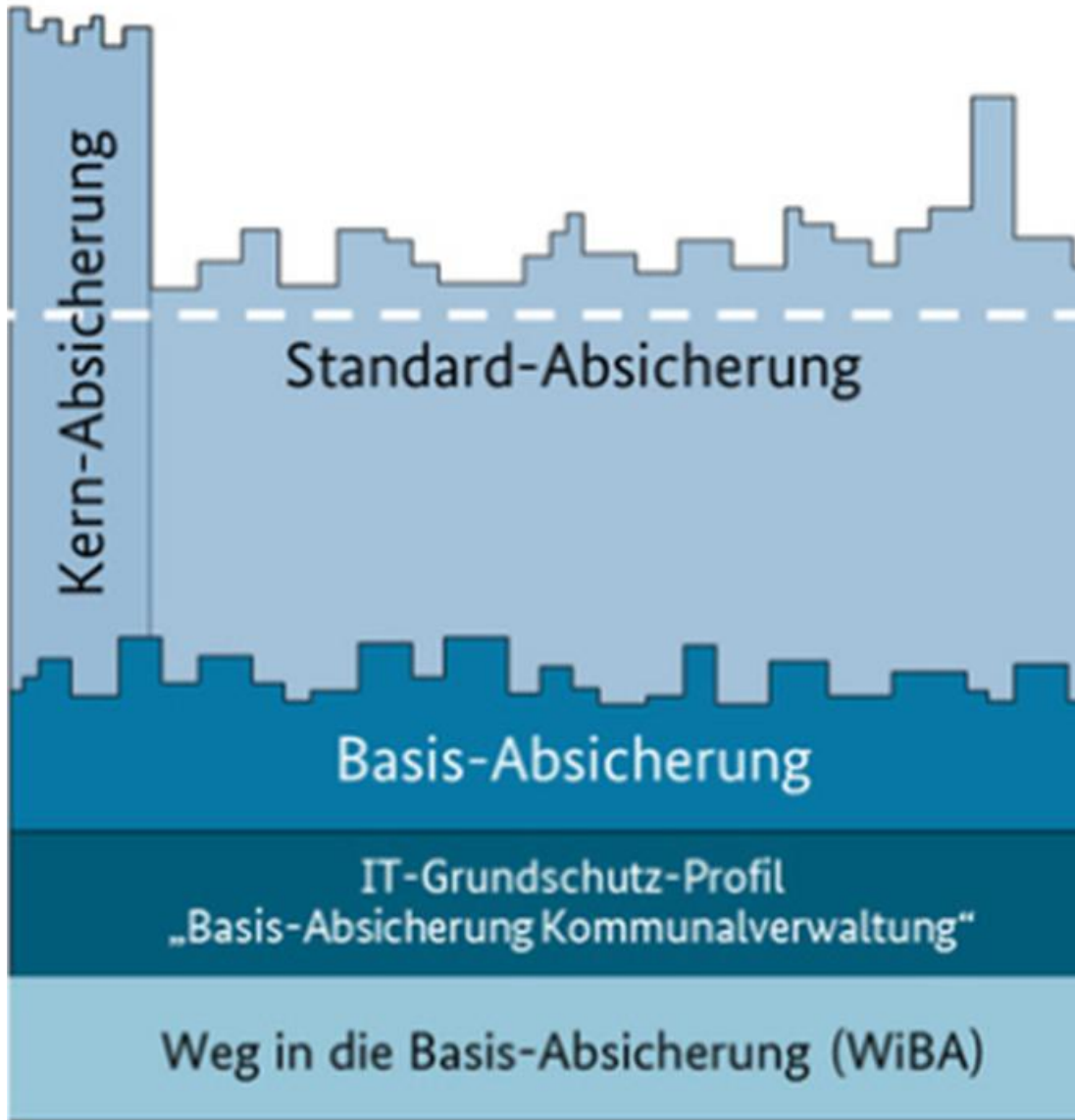
- Schutz von Objekten vor unbefugtem Zugriff

Verfügbarkeit

- Zugriff auf Dienstleistungen, Informationen oder Funktionen eines Systems zum gewünschten Zeitpunkt gewährleisten

Integrität

- vollständige Daten, die nicht verändert/manipuliert wurden



Absicherungsstufen nach BSI

Quelle: BSI

Auf dem Weg zum Level normal

WiBA-Werkzeugkasten



Themenseite der Digital-Lotsen-Sachsen: <https://InfoSic.Digital-Lotsen.de>



Wege in die Basisabsicherung

- [BSI – WiBA](#)
- Angebot der Digital-Lotsen-Sachsen: <https://WiBA.Digital-Lotsen.de/>

Auf dem Weg zum Level normal

IT-Grundschutz-Profil für Kommunalverwaltung



[vom BSI veröffentlichtes IT-Grundschutz-Profil:](#)



Auf dem Weg zum Level normal

BSI-Grundschutz



BSI-Standards zur Informationssicherheit

Informationssicherheit und IT-Grundschutz

BSI-Standard 200-1

Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-2

IT-Grundschutz-Methodik

BSI-Standard 200-3

Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 100-4

Notfallmanagement

IT-Grundschutz-Kompodium

Kapitel 1 Vorspann

Kapitel 2 Schichtenmodell und Modellierung

Elementare Gefährdungen

Schichten

Prozess-Bausteine:

- ISMS (Sicherheitsmanagement)
- ORP (Organisation & Personal)
- CON (Konzepte & Vorgehensweise)
- OPS (Betrieb)
- DER (Detektion & Reaktion)

System-Bausteine:

- IND (Industrielle IT)
- APP (Anwendungen)
- SYS (IT-Systeme)
- NET (Netze & Kommunikation)
- INF (Infrastruktur)

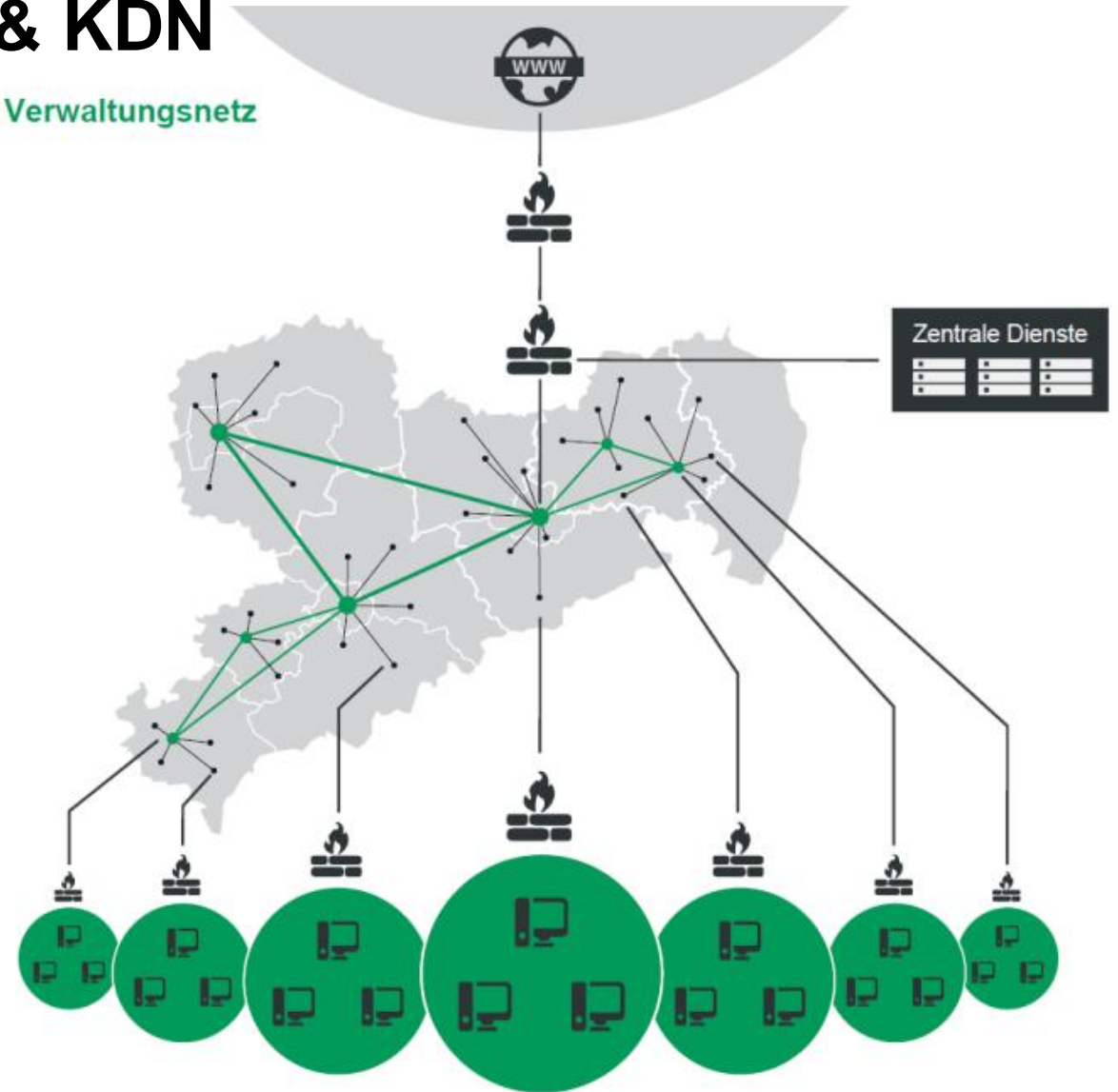
**Schulungen
zum
IT-Grundschutz-
Praktiker**

zentrales sicheres Netz

SVN & KDN

Sächsisches Verwaltungsnetz

- Daten- und Sprachnetz
SVN/KDN für alle 800
Landesbehörden
(2.500 Standorte, 40.000 Nutzer)
sowie 450 Kommunen + 1.300 Schulen
- Zentraler Internetübergang
mit Firewalls, Anti-Virenschutz, Anti-Spam,
dDoS ...
- 2028 weiterentwickeltes SVN NG / KDN IV



SAX.CERT für Kommunen

zentral finanzierte Dienste




- Individueller Warn- und Informationsdienst
- Auswahlmöglichkeit aus über 2.000 Produkten von 185 Herstellern
- Nutzerverwaltung über SAX.CERT





STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE



Advisory 2019-0021

Linux Kernel: Schwachstelle ermöglicht Offenlegung von Informationen

Datum: 2019-01-08
Stand: 2019-01-08

Risiko gesamt

Angriffswahrscheinlichkeit: mittel-hoch
Potentielle Schadenshöhe: gering-mittel

Sehr geehrte SAX.CERT-Kunden,

heute erhalten Sie, entsprechend ihrer getroffenen Produktauswahl, folgende Meldung:

Meldungsnummer	Titel	Bewertung (Ang)
2019-0021	Linux Kernel: Schwachstelle ermöglicht Offenlegung von Informationen	mittel-hoch / gering-mittel
2019-0020	IBM Rational Produkte: Mehrere Schwachstellen	mittel-hoch / hoch

SAX.CERT für Kommunen

Webseitenscans



- Seit Anfang 2018 monatlich zweimal Scans aller Internetseiten des Landes durch das SAX.CERT.
- Bewertung Integrität (HTTPS) und Softwareaktualität der Webseiten.
- Ableitung von Sicherheitsempfehlungen.

Auftrag des SAX.CERT

**Auch kommunale
Webseiten scannen**

Summary

Overall Rating

F

Certificate
Protocol Support
Key Exchange
Cipher Strength

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server's certificate is not trusted, see [below](#) for details.

Certificate uses an insecure signature. Upgrade to SHA2 to avoid browser warnings. [MORE INFO >](#)

This server supports SSL 2, which is obsolete and insecure, and can be used against TLS (DROWN attack). Grade set to F. [MORE INFO >](#)

This server supports insecure cipher suites (see below for details). Grade set to F. [MORE INFO >](#)

This server supports insecure Diffie-Hellman (DH) key exchange parameters (Logjam). Grade set to F. [MORE INFO >](#)

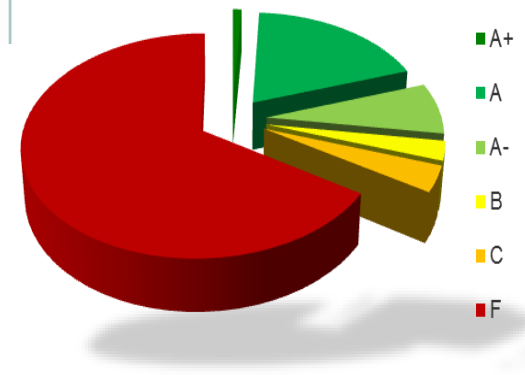
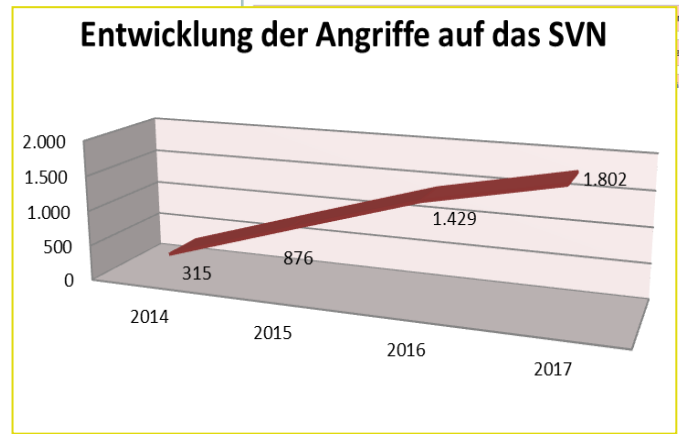
Grade set to F. [MORE INFO >](#)

capped to C. [MORE INFO >](#)

Grade set to F.

Apache 1.3.28 Released

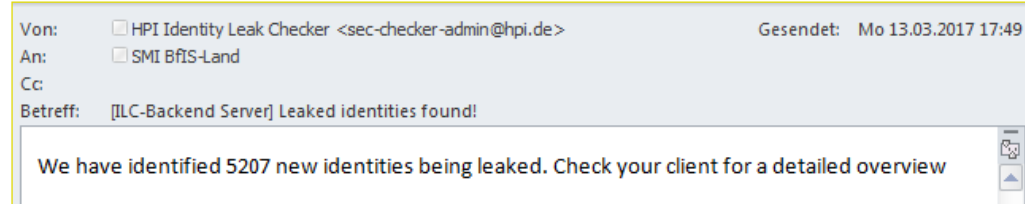
Apache 1.3.28 was released on 18th July 2003



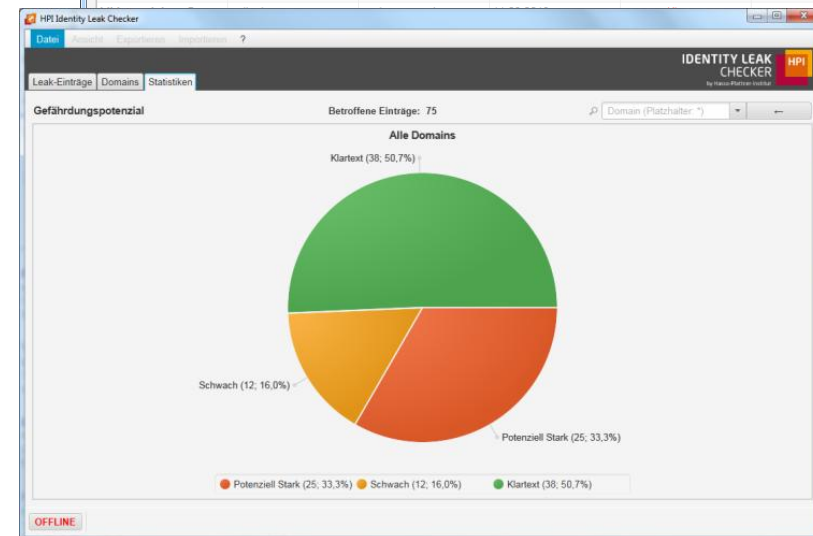
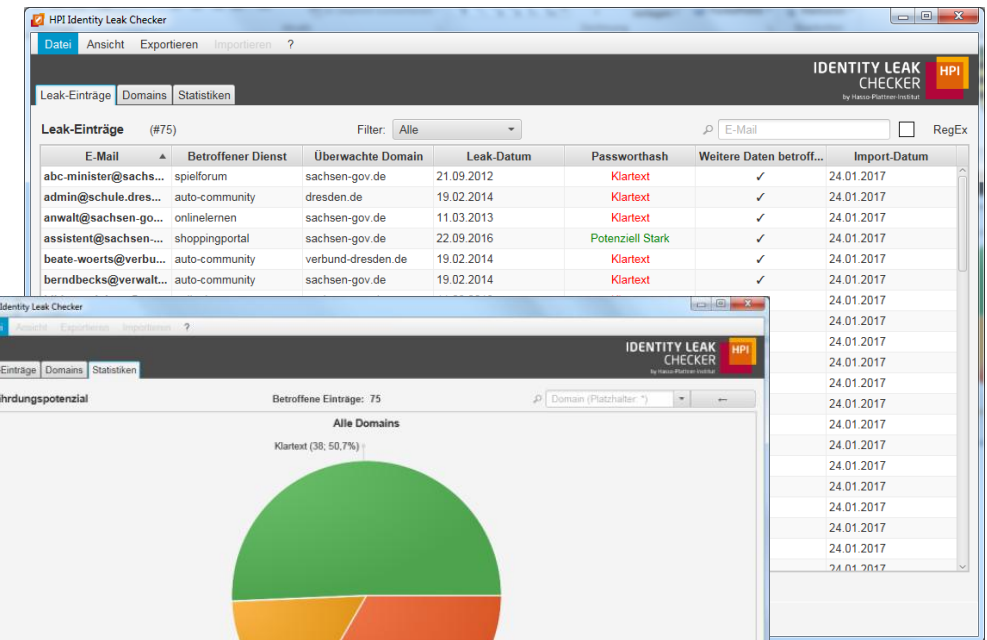
Site is Outdated
(using Joomla Version 1.5.18 to 1.5.26)

SAX.CERT für Kommunen

Identity Leak Checker



- Hasso-Plattner-Institut: Leak Checker und Zusammenarbeit mit dem Freistaat Sachsen.
- Bis heute: über 9,4 Mrd. gestohlene Identitäten gefunden.
- ILC-Client warnt SAX.CERT bei neuen Veröffentlichungen.

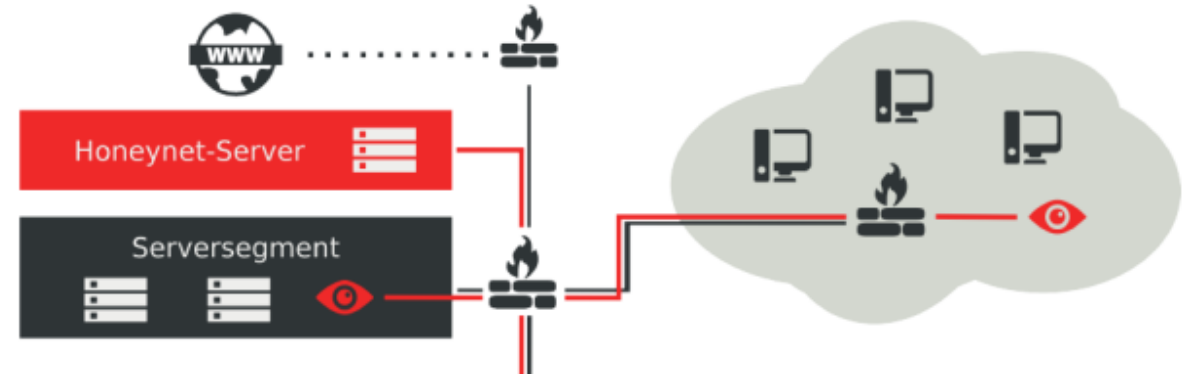


<https://www.cert.sachsen.de/identity-leak-checker-4000.html>

Honey Sens



- Warnsensor für Netzwerkeinbrüche und Anomalien
- Lösung:
 - Hackerfallen mit zentralem Management und Service, ideal für Kommunen und Landkreise.
 - Industriepartner: T-Systems MMS.

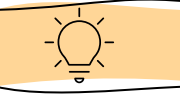


Veröffentlichungen:

- [„HSF im Blick“ Ausgabe März 2023](#)
- [SACHSENLANDKURIER 04/2019](#)
- [Flyer der Sächs. Staatskanzlei](#)



Weitere Informationen



- Unsere Themenseite Informationssicherheit: <https://InfoSic.Digital-Lotsen.de>
- [Sächs. Informationssicherheitsschein](#) (Selbstlerninhalt in der WVLP)
- Für kommunale BfIS – die Website der SAKD: https://www.sakd.de/index.php?id=is_methodische_herangehensweise
- Website zum Thema Informationssicherheit der Staatskanzlei (Referat 45): <https://www.egovernment.sachsen.de/informationssicherheit-in-den-kommunen.html>
- SAX.CERT-Sprechstunde für Kommunen; Anmeldung: BfIS-Land@sk.sachsen.de
- [Lagebericht 2024 zur Informationssicherheit in Sachsen](#)



**Was muss jede sächsische
Kommune mindestens tun?**

Was muss eine Kommune tun/getan haben?

- Beauftragte(n) für Informationssicherheit benennen und innerhalb eines Monats an BfIS-Land melden.
- Ist-Zustand / Absicherungsstufe bestimmen.
- Zielzustand definieren (WiBA, Grundschutzprofil Kommunalverwaltung etc.).
- Informationssicherheit auf der eigenen Digitalen Agenda verorten und priorisieren!
- Maßnahmen zur Informationssicherheit festlegen, umsetzen, dokumentieren und die Weiterentwicklung des Informationssicherheitsniveaus etablieren (ISMS).
- Notfallplan erstellen und den Notfall „üben“.
- Sicherheitsvorfälle immer an das SAX.CERT melden.
- Mitarbeitende (wiederkehrend) sensibilisieren und belehren.

Eure Checkliste als Digital-Navigatoren

- Ich kenne meinen Beauftragten für Informationssicherheit (BfIS).
- Ich habe das Sächsische Informationssicherheitsgesetz in meiner „Handakte“.
- Ich beziehe den BfIS aktiv in meine Digitalisierungsprojekte ein.
- Ich denke Informationssicherheit immer und von Anfang an mit!
- Ich habe einen Überblick über das bestehende Informationssicherheitsniveau und die Maßnahmen, die dieses erhöhen sollen sowie eventuell bestehende Risiken.
- Ich denke Informationssicherheit als Querschnittsaufgabe.

Checkliste

Informationssicherheit für Digital-Navigatoren



Beauftragte(r) für Informationssicherheit

- kenne ich

Sächsisches Informationssicherheitsgesetz

- in meiner „Handakte“

Überblick zu Informationssicherheitsniveau

- habe ich

Überblick zu bestehenden Risiken

- habe ich

Beauftragte(r) für Informationssicherheit

- beziehe ich in Digitalvorhaben ein

Informationssicherheit als Querschnittsaufgabe

- denke ich immer mit

zum Thema Informationssicherheit

- informiere ich mich regelmäßig

Meine Idee zu Informationssicherheit

.....



Das Prinzip Hoffnung
ist keine
Informationssicherheits-
strategie!



Datenschutz



1

Datenschutz

Begriffe

2

Datenschutz

Rechtsgrundlage und Grundsätze

3

Datenschutz

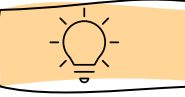
Was müssen wir tun?

4

Zusammenfassung

Was ist was?

Begriffe jonglieren



Informationssicherheit

Schutz jeglicher, **auch nicht elektronischer** Informationen

Cyber-Sicherheit

Schutz elektronischer Systeme
sowie unterstützender Prozesse

IT-Sicherheit

Schutz elektronischer Daten
und Systeme

Informationen
mit
Personenbezug
= personen-
bezogene
Daten

Datenschutz



Was ist Datenschutz?

Datenschutzgrundsätze

personenbez. Daten dürfen erhoben bzw. verarbeitet werden ...

- rechtmäßig, nach Treu und Glauben, transparent
- für festgelegte, eindeutige und legitime Zwecke
- auf das notwendige Maß beschränkt
- wenn sie sachlich richtig oder berichtigt sind
- nur solange der Zweck existiert
- wenn Sicherheit gewährleistet ist

Rechenschaftspflicht:

verarbeitende Stelle:

Grundsätze
einhalten
**und
nachweisen!**



DSGVO





**Was muss jede sächsische
Kommune mindestens tun?**

Was muss eine Kommune tun / getan haben?

- Datenschutzbeauftragte(n) benennen.
- System zum Datenschutz aufbauen (Konzept und TOM).
- Verzeichnis der Verarbeitungstätigkeiten erstellen und aktuell halten.
- Vorhandene Einwilligungen prüfen und ggf. neu einholen.
- „Meldekette“ festlegen, um bei Datenverlust informieren zu können.
- Bestehende Verträge überprüfen, ob die Vorgaben für Vereinbarungen mit Auftragsdatenverarbeitern eingehalten werden.
- Mitarbeitende sensibilisieren und belehren.
- Prüfen, ob gemeinsame Verantwortlichkeit mit anderen Stellen vorliegt. In diesen Fällen Verantwortlichkeiten festlegen (Informationspflichten etc.).

Checkliste

Datenschutz für Digital-Navigatoren



Beauftragte(r) für Datenschutz

- kenne ich

DSGVO

- in meiner „Handakte“

Überblick zu Datenschutzkonzept

- habe ich

Überblick zu technischen und organisatorischen Maßnahmen (TOM)

- habe ich

Beauftragte(r) für Datenschutz

- beziehe ich in
Digitalvorhaben ein

Datenschutz als Querschnittsaufgabe

- denke ich immer mit

zum Thema Datenschutz

- informiere ich mich
regelmäßig

Meine Idee zu Datenschutz

.....



Guter Datenschutz
hilft
Vertrauen zu bilden
– und nicht
Digitalisierung
zu verhindern!

Was sollt ihr heute mitnehmen?



- Informationssicherheit und Datenschutz gelten für die digitale und analoge Welt.
- Es sollte in jeder Kommune eine Ansprechperson geben, welche die Rolle BfIS und DSB wahrnimmt.
- Die Verantwortung für Informationssicherheit und Datenschutz trägt immer der Verantwortliche für den jeweiligen Bereich = Behördenleiter.
- Besser kleine Schritte gehen als gar nicht loslaufen!
- Starten! Jetzt!
Kostenlose Angebote und Best-Practices nutzen ...



Die Inhalte der Präsentation wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte können wir jedoch keine Gewähr übernehmen. Die Inhalte dieser Präsentation sind ausschließlich für Teilnehmer der Basisbefähigung des Digital-Lotsen Sachsen Projektes vorgesehen. Sie sind der Öffentlichkeit fernzuhalten und dürfen nicht ohne vorhergehende schriftliche Genehmigung des sächsischen Städte- und Gemeindetages e.V. verbreitet, kopiert, gespeichert oder anderweitig genutzt werden.

Digital-Lotsen-Sachsen
Sächsischer Städte- und Gemeindetag
Glacisstraße 3, 01099 Dresden
Tel.: 0351 8192-270

 www.digital-lotsen.de

 www.ssg-sachsen.de