



Dokumentation zum Fachtag – Gemeinsam Prävention gestalten!

Cybersicherheit für Kommunen

Dipl.-Ing. Jörg Steinig



AssKomm

Allianz Sichere Sächsische Kommunen

www.asskomm.de



Cybersicherheit für Kommunen

Der Beauftragte für Informationssicherheit des Landes



14. September 2023 | Jörg Steinig

Agenda

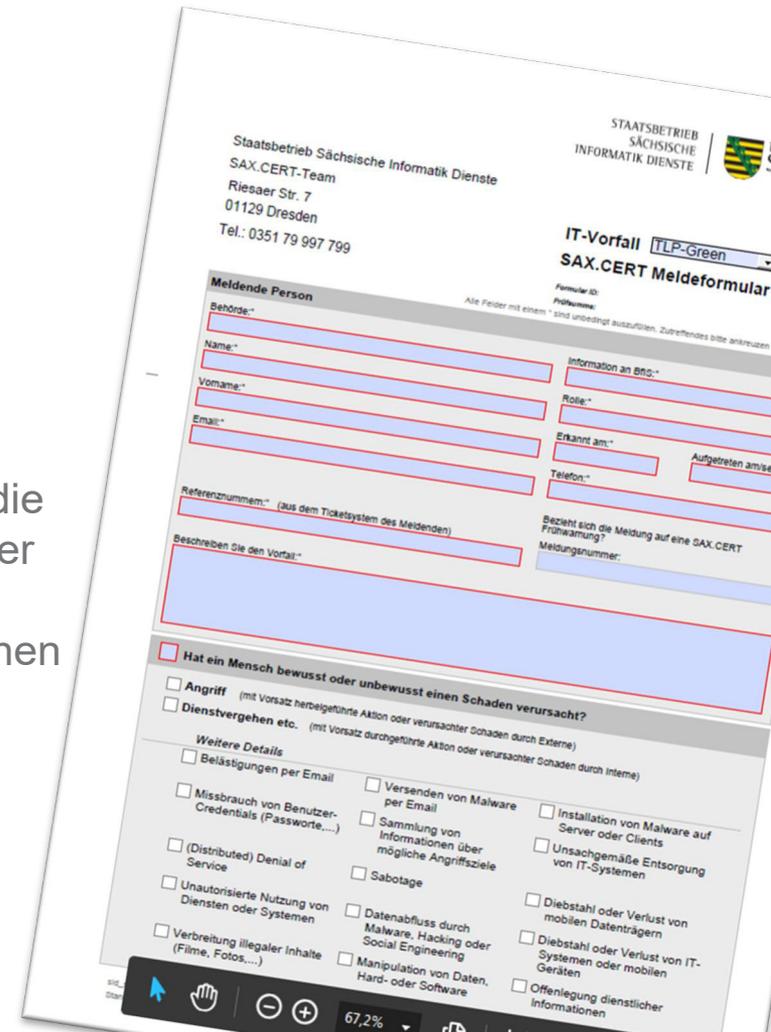
- Meldepflichten nach Sächsischem Informationssicherheitsgesetz
- Sicherheitsmeldungen 2023
- Schutzsysteme SVN und KDN
- Sicherheits-Services des Sicherheitsnotfallteam (SAX.CERT)
 - Schwachstellen-Warndienst
 - HoneySens
 - Identity Leak Checker
 - Webseiten-Scans
 - Monatlicher Lagebericht Kommunen
 - Passwortchecker
- E-Learning-Portal
- Schulungen zum IT-Grundschutz-Praktiker

Meldepflichten gemäß Sächsisches Informationssicherheitsgesetz

- Behördenübergreifende Meldepflichten
- Meldepflichten der staatlichen Stellen
- Meldepflichten der **nicht-staatlichen Stellen**, wenn mit dem SVN/ KDN verbunden:
 - Sicherheitsereignisse und Sicherheitsvorfälle an das Sicherheitsnotfallteam

Unverzüglich muss die Meldung erfolgen, wenn es sich um Sicherheitsvorfälle handelt, die

 - zu einer erheblichen Beeinträchtigung der Schutzziele geführt haben oder
 - behördenübergreifend zu einer erheblichen Beeinträchtigung der Schutzziele führen können.



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

IT-Vorfall
SAX.CERT Meldeformular

Formular ID:
Protokollnummer:

Alle Felder mit einem * sind unbedingt auszufüllen. Zuhilfenahmendes bitte ankreuzen

Meldende Person

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

Information an Bsp.*
Rolle*
Erkannt am*
Telefon*
Aufgetreten am*

Bezieht sich die Meldung auf eine SAX.CERT
Meldungsnummer:

Hat ein Mensch bewusst oder unbewusst einen Schaden verursacht?

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

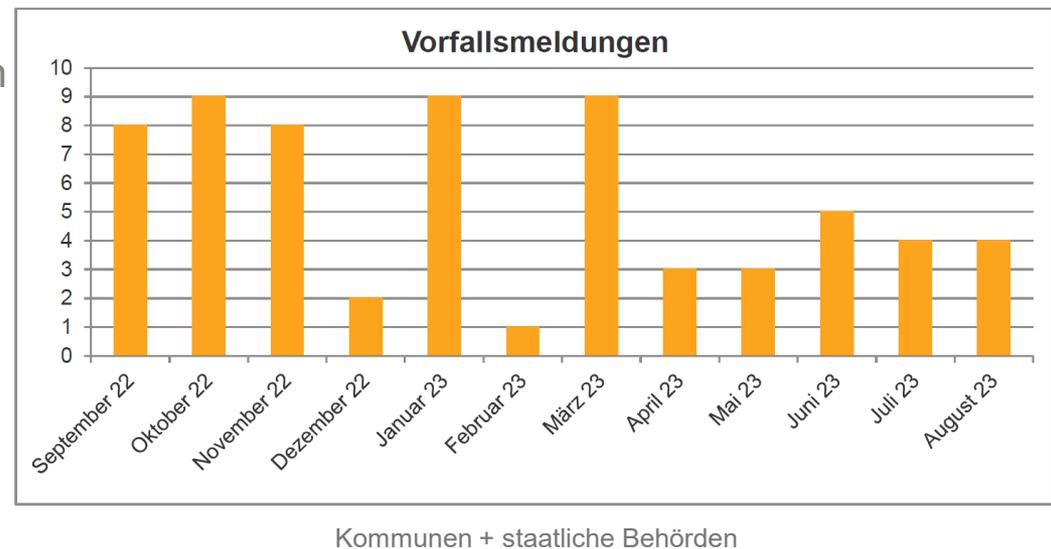
Dienstvergehen etc. (mit Vorsatz durchgeführte Aktion oder verursachter Schaden durch Interne)

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 (Passwörter,...)	<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 IT-Geräten
<input type="checkbox"/> Verbreitung illegaler Inhalte (Filme, Fotos,...)	<input type="checkbox"/> Manipulation von Daten, Hard- oder Software	<input type="checkbox"/> Offenlegung dienstlicher Informationen

Auszug Sicherheitsmeldungen aus den Kommunen in 2023

- September: Ransomware-Attacke auf Stadtverwaltung
- August: angebliches BM-Schreiben fordert zur Zahlung auf
- Juli: Kontaktformular wird mit Anfragen überschwemmt
- April: Massive IT-Störung einer Schule durch Innentäter
- März: Spammail-Kampagne und Spammails "Bitcoin-Erpressung" gegen Landkreis
- Januar: Schadsoftwarebefall im Schulverwaltungsnetz



Gemeinsame Schutzsysteme SVN und KDN

Mailaufkommen SVN und KDN						
Abgewiesene Mails aufgrund						
Monat	von Realtime Blacklists	von DNS-Checks	von ACLs	von Relay-Versuchen	von Greylisting	ungültige Adresse
Aug 23	747.964	916.222	39.648	162.083	2.902.520	145.618
Jul 23	861.427	1.592.913	72.568	72.802	3.022.637	123.042
Jun 23	1.076.146	1.858.947	37.198	87.100	2.851.948	136.991
Mai 23	609.755	1.275.709	18.908	41.395	2.566.766	115.101
Apr 23	899.335	2.400.547	24.053	33.205	2.555.463	126.735
Mrz 23	884.983	1.931.711	32.421	27.355	3.312.358	139.216

Mailaufkommen SVN und KDN – abgewiesene Mails

Mailaufkommen SVN und KDN			
Angenommene Mails			
Monat	unmarkiert	als Spam markiert ³	mit Link-Reputation markiert
Aug 23	3.039.101	589.620	152.373
Jul 23	3.560.197	491.018	107.756
Jun 23	3.297.504	409.077	106.338
Mai 23	3.188.796	389.177	107.911
Apr 23	2.938.035	353.656	90.616
Mrz 23	3.508.612	471.482	95.309

Mailaufkommen SVN und KDN – angenommene Mails

Schwachstellen-Warndienst

- Mit dem Schwachstellenwarndienst stellt das SAX.CERT in Zusammenarbeit mit dem technischen Dienstleister tagesaktuelle Informationen zu Schwachstellen und Sicherheitslücken in IT-Systemen zur Verfügung.
- Über das SAX.CERT kann kostenfrei ein eigenes Nutzerkonto angelegt werden, mit dem sich der Kunde aus aktuell mehr als 2.000 Hard- und Softwareprodukten eine individuelle Zusammenstellung auswählen kann.
- Der Warndienst wurde Stand Juli 2022 von 148 Einrichtungen im Bereich Kommunen genutzt.

 advisory_2021-2055.pdf 95 KB	 advisory_2021-2054.pdf 94 KB	 advisory_2021-2053.pdf 95 KB
 advisory_2021-2052.pdf 102 KB	 advisory_2021-2051.pdf 93 KB	 advisory_2021-2024.pdf 102 KB
 advisory_2021-2005.pdf	 advisory_2021-2002.pdf	 advisory_2021-1933.pdf

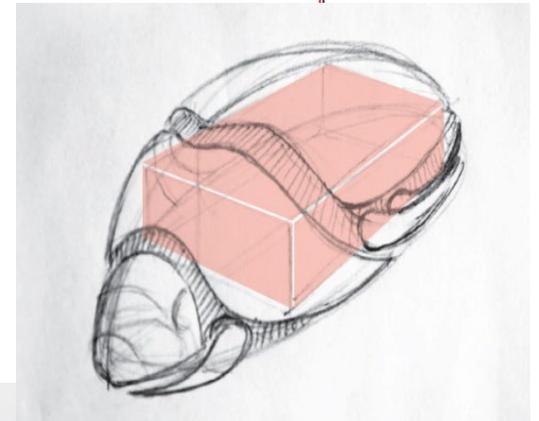
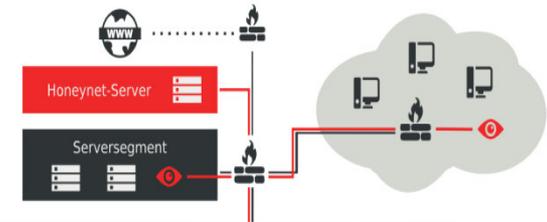
Sehr geehrte SAX.CERT-Kunden,

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

Meldungsnummer	Titel	Bewertung (Angriffswahrscheinlichkeit / Schadenshöhe)
2021-2055	PHP: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen	mittel-hoch / mittel
2021-2054	Linux Kernel: Mehrere Schwachstellen	gering-mittel / mittel
2021-2053	Drupal: Mehrere Schwachstellen ermöglichen Cross-Site Scripting	gering / mittel
2021-2052	Wireshark: Mehrere Schwachstellen ermöglichen Denial of Service	mittel / mittel
2021-2051	Microsoft Windows Azure: Schwachstelle ermöglicht Offenlegung von Informationen	gering-mittel / gering-mittel

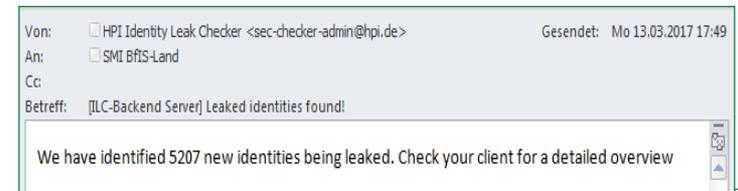
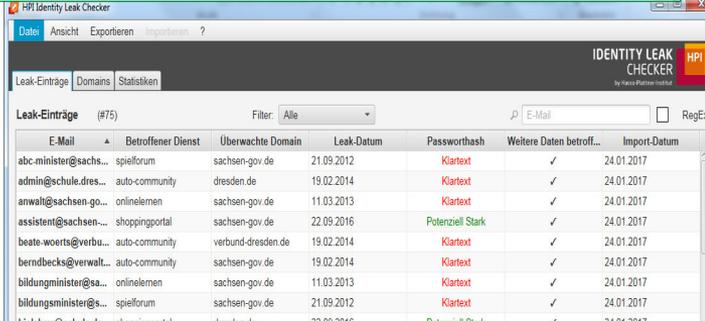
HoneySens

- 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.
- Bei sicherheitsrelevanten Zugriffen wird der Nutzer per E-Mail und visuell über die Sensoren alarmiert. Damit kann schneller auf Angriffe reagiert, bzw. das Vorgehen des Angreifenden besser nachvollzogen werden.
- Im Juli 2022 waren insgesamt 19 Sensoren in Kommunen im produktiven Einsatz.

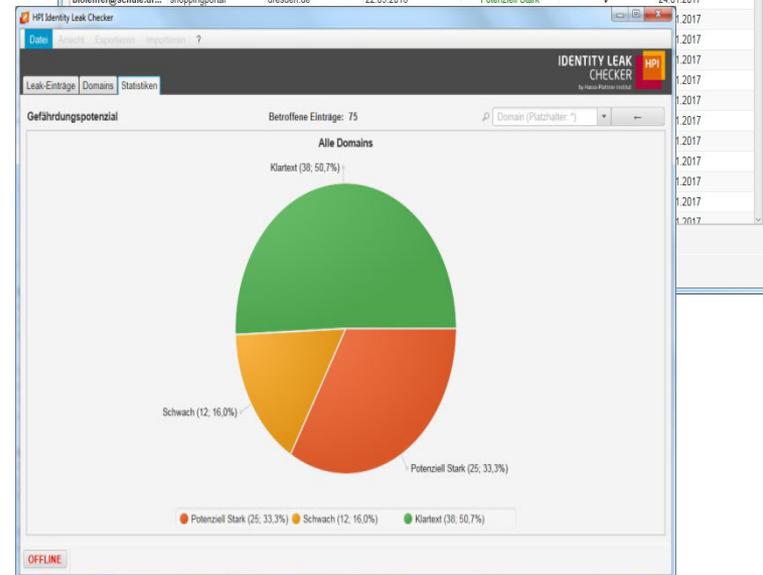


Identity Leak Checker

- Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen.
- Mit dem Identity Leak Checker bietet das SAX.CERT in Zusammenarbeit mit dem Hasso-Plattner-Institut (HPI) einen individuellen Dienst zur Überprüfung von E-Mail-Adressen an.
- Auf Antrag können über das SAX.CERT weitere Mail-Domains in den Dienst aufgenommen werden, was von 35 Nutzern außerhalb der Landesverwaltung genutzt wird.

E-Mail	Betroffener Dienst	Überwachte Domain	Leak-Datum	Passworts hash	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
anwalt@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



E-Learning-Portal

- Fortbildungsveranstaltungen zur Informationssicherheit in Präsenz sind kein alleiniges Heilmittel – deshalb: E-Learning.
- In Zusammenarbeit mit TU Dresden Weiterentwicklung eines bestehenden E-Learning-Angebots der BAKöV
- Bis September gut 20.000 Absolventen, davon über 8.500 aus den Kommunen

Informationssicherheit am Arbeitsplatz
Start ins Programm – Einstiegsszenario (1/7)



Hallo, mein Name ist Florian Sibe.
Meine Aufgabe ist es, für mehr Sicherheit am Arbeitsplatz zu sorgen.
Und das hier ist mein Assistent @gar. Er wird Sie zuverlässig durch das Programm führen und an vielen Stellen nützliche Tipps und Zusammenfassungen rund um das Thema Informationssicherheit geben. Bist du bereit für den Rundgang durch das Programm, @gar?

Informationssicherheit am Arbeitsplatz
Machen Sie Ihren Arbeitsplatz sicher – Informationssicherheit (3/8)

Verfügbarkeit

+ **Integrität**
korrekte, unverfälschte und vollständige Informationen

+ **Vertraulichkeit**
zugänglich nur für Befugte

= **Informationssicherheit**

Integrität bedeutet, dass die Informationen korrekt, vollständig und nicht verfälscht sind und Vertraulichkeit heißt, dass nur diejenigen darauf zugreifen können, die dazu befugt sind. Reicht das?



Erste Roadshow Kommunen des BSI in Sachsen

- Themenfindung
- Einbindung und Ansprache der Kommunen



Roadshow Kommunen

2. Mai 2022
10:00 - 14:15 Uhr
Agenda

10:00 Uhr	Keynote - Arne Schönbohm, Präsident des BSI
10:15 Uhr	Begrüßung - Thomas Popp, CIO des Freistaates Sachsen
10:30 Uhr	Begrüßung - Bert Wendsche, Präsident Sächsischer Städte- und Gemeindetag
10:35 Uhr	Vortrag Bedrohungslage - BSI
11:10 Uhr	Vortrag Sicherheit "as a Service" - SAX.CERT
11:45 Uhr	Pause
12:15 Uhr	Informationssicherheit für Kommunen - BSI
12:45 Uhr	Vortrag Rechte und Pflichten der Kommunen aus dem Sächsischen Informationssicherheitsgesetz - BfIS Land
13:15 Uhr	Vortrag OZG - BSI
	Vortrag Kommune - Erfahrungsbericht/ Best Practice aus einer Kommune zur

Die Roadshow als Ausgangspunkt für weitere Aktivitäten

- Seit Oktober 2022 jeden ersten Freitag im Monat um 10 Uhr Online-Sprechstunde des SAX.CERT für Kommunen
- Services des SAX.CERT werden im Detail erläutert
- Fragen und Bedarfe aus den Kommunen werden aufgenommen



Finanzierung von Schulungen (IT-Grundschutz-Praktiker)

- Seit Inkrafttreten des SächsISichG unterstützt BfIS Land die Kommunen bei der Weiterbildung von Mitarbeitern zum Beauftragten für Informationssicherheit
- Jährlich Schulungen zum „IT-Grundschutz-Praktiker“ in Zusammenarbeit mit SSG und SAKD inkl. Zertifikat
- Aktuell: 25.-27.9.23 in Chemnitz und 7.-9.11.23 online
- Weitere Termine in Planung

Basisschulung für den IT-Grundschutz-Praktiker Chemnitz 25. - 27.09.2023



Logo SAKD / Freistaat

Die 3-tägige Schulung wird den sächsischen Kommunen vom Freistaat Sachsen in Kooperation mit der Sächsischen Anstalt für kommunale Datenverarbeitung und der Stadt Chemnitz angeboten.

Sie richtet sich nach dem Curriculum des Bundesamtes für Informationssicherheit in der Informationstechnik (BSI) und versetzt die Teilnehmenden in die Lage, in ihrer Behörde ein Information-Sicherheits-Management-System (ISMS) entsprechend der IT-Grundschutz-Methodik aufzubauen. Die Schulung behandelt die Themenfelder:

- Einführung und Grundlagen der IT-Sicherheit und rechtliche Rahmenbedingungen
- Normen und Standards der Informationssicherheit
- Einführung IT-Grundschutz
- IT-Grundschutz-Vorgehensweise (Überblick)
- Kompendium (Überblick)
- Umsetzung der IT-Grundschutz-Vorgehensweise
- IT-Grundschutz-Check