Cybersicherheit für Kommunen

Dipl.-Ing. Jörg Steinig

SÄCHSISCHE STAATSKANZLEI | Freistaat SACHSEN

Cybersicherheit für Kommunen

Der Beauftragte für Informationssicherheit des Landes

14. September 2023 | Jörg Steinig

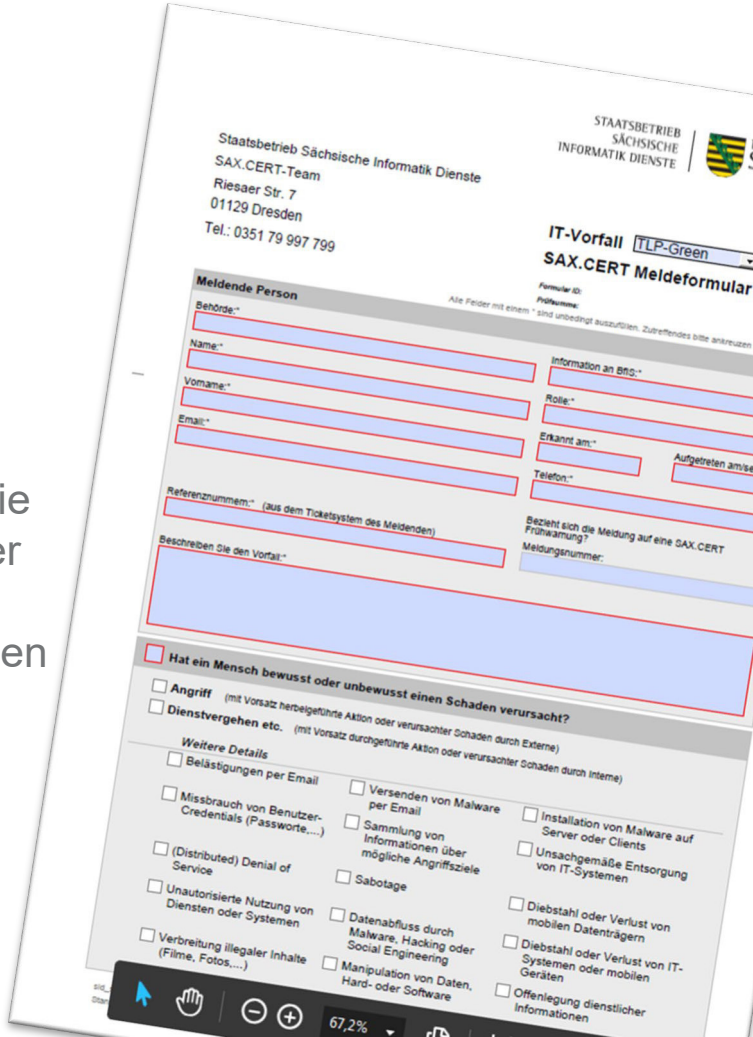
Freistaat SACHSEN

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

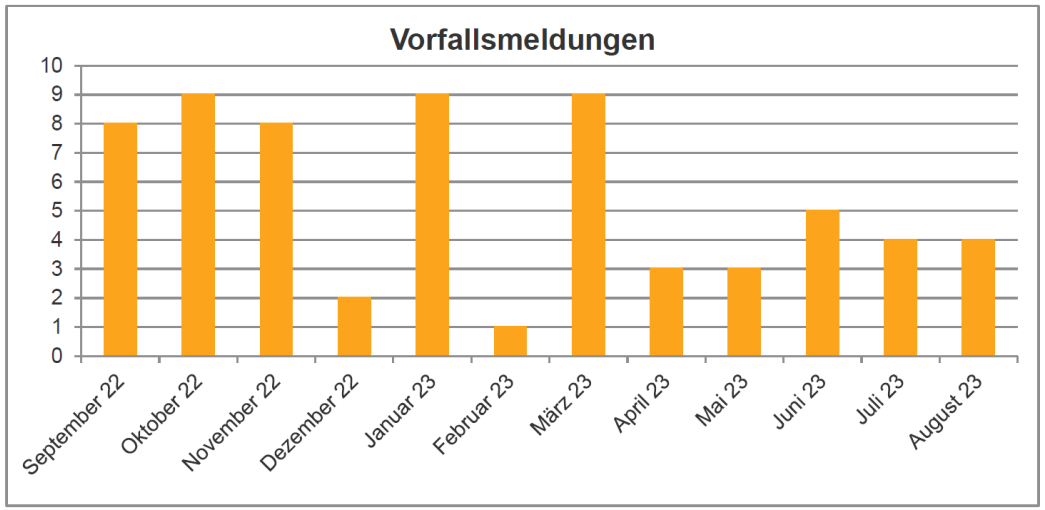
- Behördenübergreifende Meldepflichten
- Meldepflichten der staatlichen Stellen
- Meldepflichten der **nicht-staatlichen Stellen**, wenn mit dem SVN/ KDN verbunden:
  - Sicherheitsereignisse und Sicherheitsvorfälle an das Sicherheitsnotfallteam
    Unverzüglich muss die Meldung erfolgen, wenn es sich um Sicherheitsvorfälle handelt, die
    - zu einer erheblichen Beeinträchtigung der Schutzziele geführt haben oder
    - behördenübergreifend zu einer erheblichen Beeinträchtigung der Schutzziele führen können.



Freistaat SACHSEN

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



Kommunen + staatliche Behörden

Freistaat SACHSEN

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

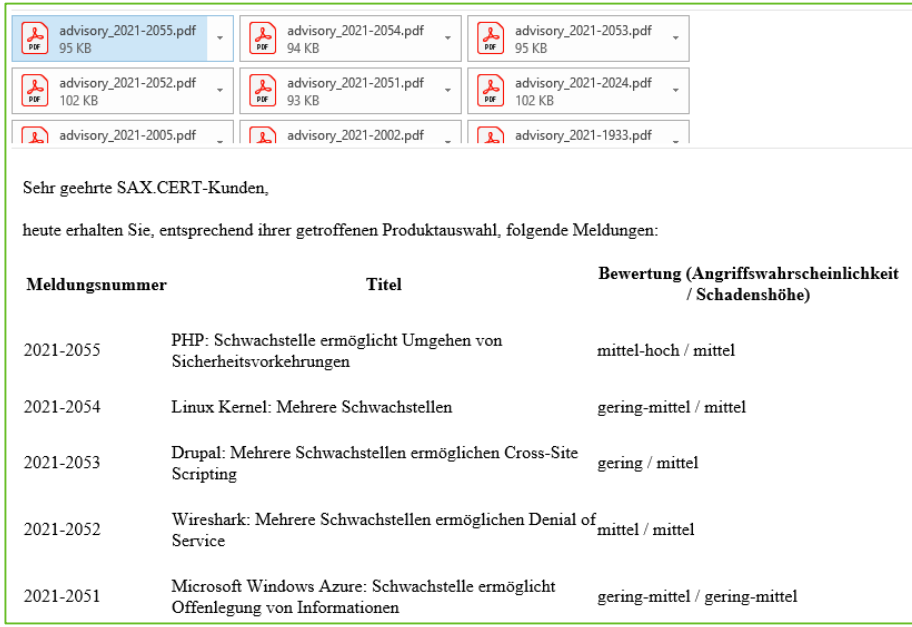
Mailaufkommen SVN und KDN			
Angenommene Mails			
Monat	unmarkiert	als Spam markiert[3]	mit Link-Reputation markiert
Aug 23	3.039.101	589.620	152.373
Jul 23	3.560.197	491.018	107.756
Jun 23	3.297.504	409.077	106.338
Mai 23	3.188.796	389.177	107.911
Apr 23	2.938.035	353.656	90.616
Mrz 23	3.508.612	471.482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

Mailaufkommen SVN und KDN – angenommene Mails

Freistaat SACHSEN

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.



Sehr geehrte SAX.CERT-Kunden,

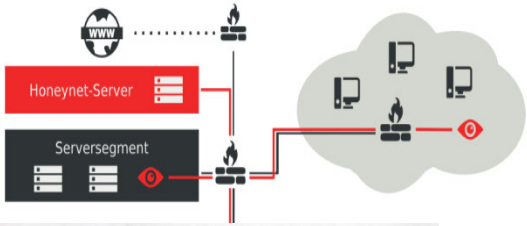
heute erhalten Sie, entsprechend ihrer getroffenen Produktauswahl, folgende Meldungen:

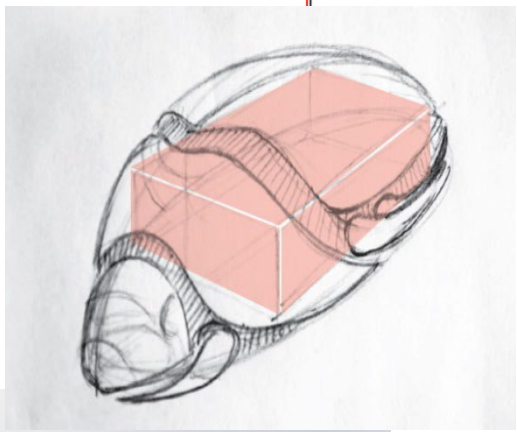
Meldungsnummer	Titel	Bewertung (Angriffswahrscheinlichkeit / Schadenshöhe)
2021-2055	PHP: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen	mittel-hoch / mittel
2021-2054	Linux Kernel: Mehrere Schwachstellen	gering-mittel / mittel
2021-2053	Drupal: Mehrere Schwachstellen ermöglichen Cross-Site 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

Freistaat SACHSEN

HoneySens

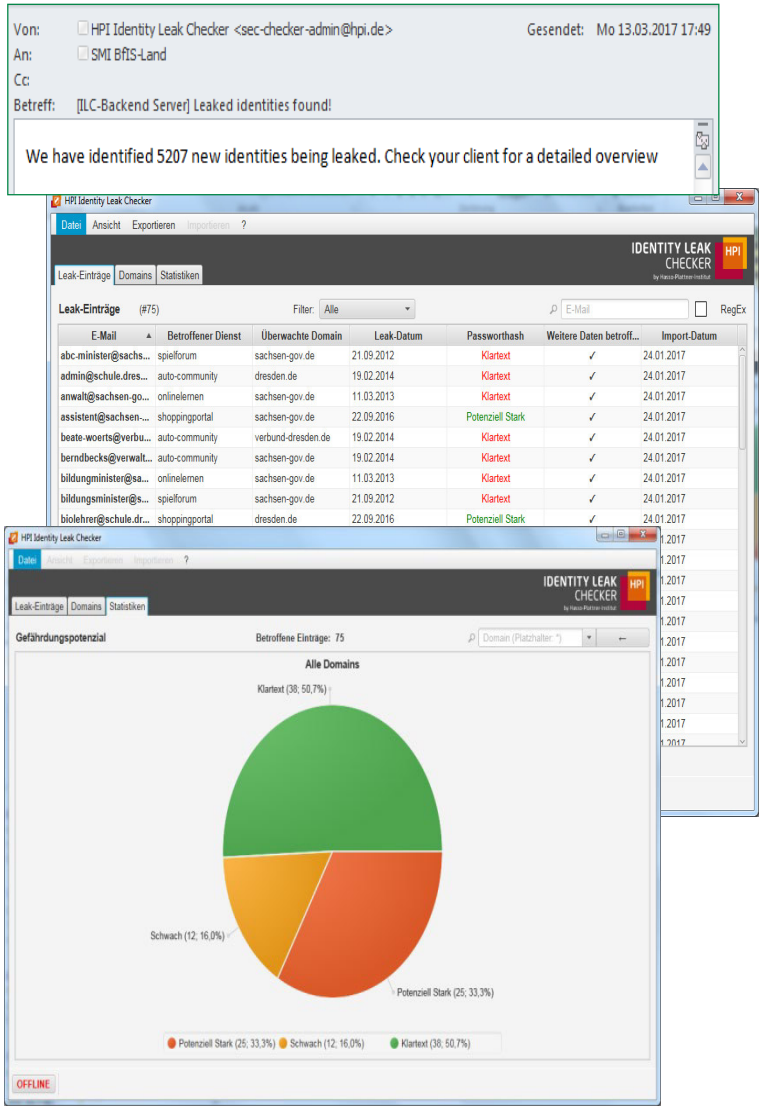
- HoneySens ist eine Sicherheitslösung zur Erkennung von Hacker-Angriffen in internen Netzwerken, bestehend aus Sensoren/Clients zur Überwachung des Netzwerks sowie einer zentralen Serverinstanz, an die die Clients verdächtige Zugriffsversuche melden.
- Bei sicherheitsrelevanten Zugriffen wird der Nutzer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





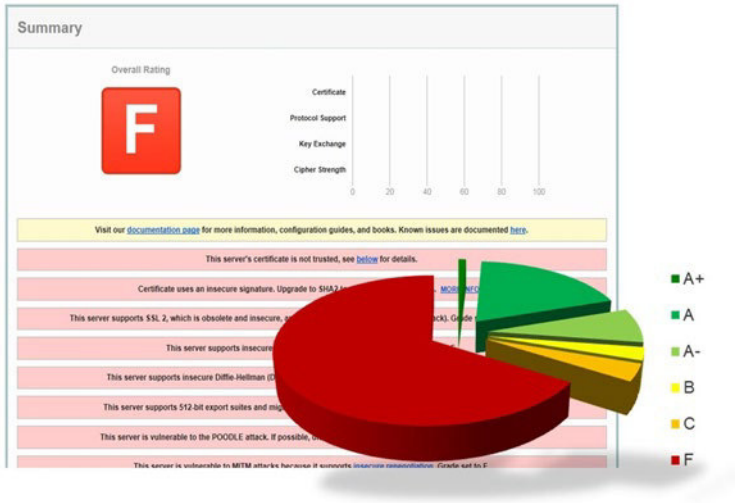
Identity Leak Checker

- 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.



Webseiten-Scans

- 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.
- Von den insgesamt über 7.300 gescannten Webseiten und –Diensten sind über 1.500 von Kommunen.



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

Erste Roadshow Kommunen des BSI in Sachsen

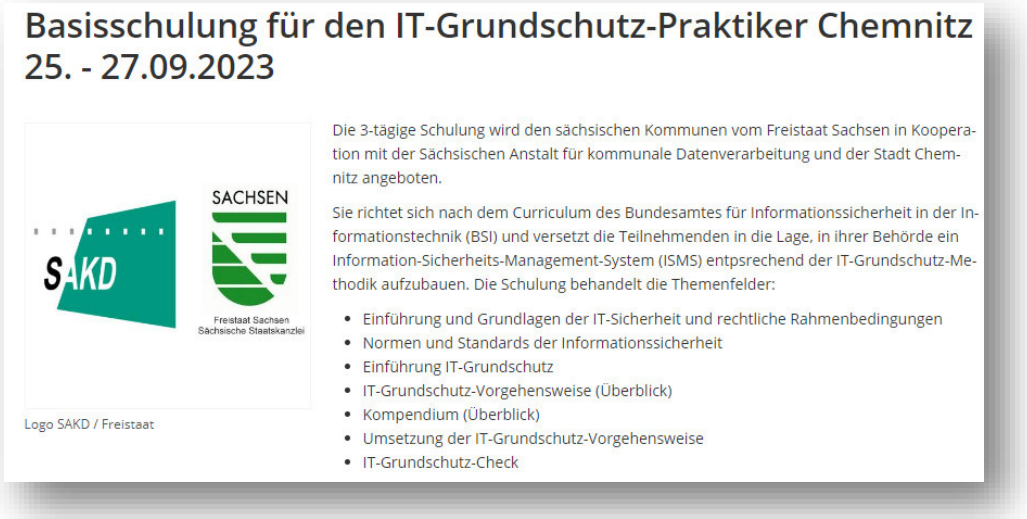
- Themenfindung
- Einbindung und Ansprache der Kommunen

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



Logo SAKD / Freistaat