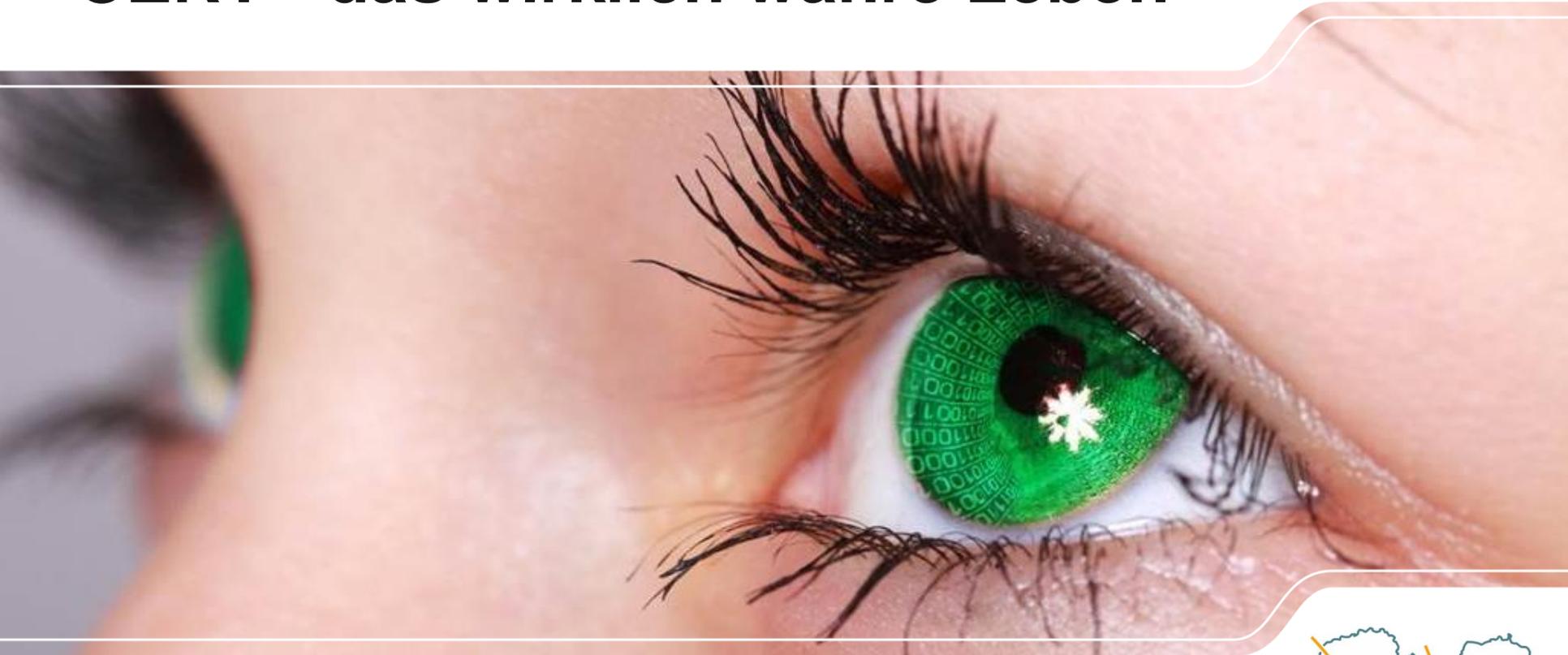


CERT - das wirklich wahre Leben



Agenda

1

Wie ist die Lage in der sächsischen Landesverwaltung?

2

Welche Maßnahmen werden ergriffen?

3

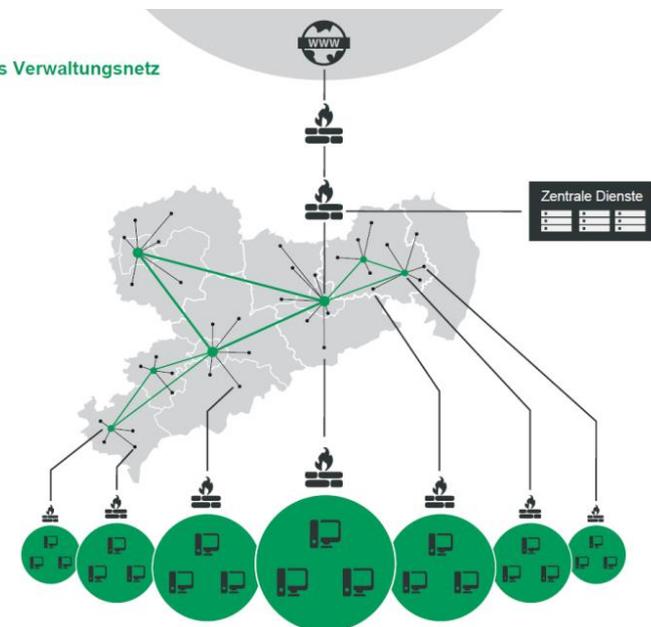
Bitte mitmachen!

Ausgangslage Sachsen

- **Daten- und Sprachnetz SVN** für alle 800 Landesbehörden (2.500 Standorte, über 40.000 Nutzer), 450 Kommunen + 1.300 Schulen
- Zentraler Internetübergang mit Firewalls, AV, Antispam, APT, IDS, DDoS...
- ISMS mit BfIS Land / CISO, BfIS Ressorts, CERT und AG IS



Sächsisches Verwaltungsnetz



Bedrohungslage

„Der Cyber-Krieg hat längst begonnen. Cybersicherheit ist DAS Trendthema der nächsten Jahre.“

vs.

„Kein Hacker interessiert sich für die öffentliche Verwaltung! Hier ist doch nichts zu holen. Es passiert ja auch nur selten mal was.“

Reale Probleme...

Parlament offline

Vorlesen

Trojaner im Landtag

Der Landtag ist durch Schadsoftware lahmgelegt worden. Abgeordnete und Mitarbeiter wurden angewiesen, Telefone und Computer vom Netz zu nehmen. Seitdem ist der Landtag offline und vom Telefonnetz genommen.



Gesamtes IT-Netz des Bundestages muss ausgetauscht werden



16 GB im Bundestag abgezweigt Hacker erbeuteten vertrauliche E-Mails

Bei der Cyber-Attacke auf den Bundestag wurde offenbar auch eine große Menge vertraulicher E-Mails von Abgeordneten erbeutet. Auch Terminkalender und Adressverzeichnisse waren Ziel der Hacker.

Gefährlicher Virus in Online-Bewerbung



Nach Wahlerfolg

Unbekannte veröffentlichen Mitgliederliste der AfD Sachsen

Kurz nach dem Wahlerfolg der AfD Sachsen haben Hacker vertrauliche Daten der Mitglieder veröffentlicht. Es geht um persönliche Informationen wie Telefonnummern und Geburtstage.

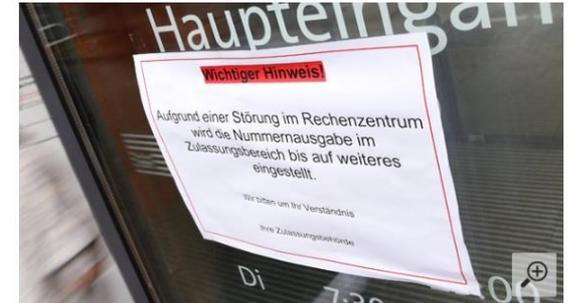
ERMITTLUNG

Computer-Virus: Verwaltung kann nur eingeschränkt arbeiten

Vorübergehend geschlossen

Autozulassungsbehörden melden Hackerangriff

23.06.2015, 08:14 Uhr | dpa



Wegen Hackerattacke geschlossen: Dutzende Kfz-Zulassungsstellen in Hessen und Rheinland-Pfalz sind lahmgelegt. (Quelle: dpa)

SICHERHEIT

Hackerangriff aufs Rathaus

Kryptomining-Angriff auf Server des Landesamts für Besoldung und Versorgung - Service sicherheitshalber eingeschränkt

Hacker spionieren die Bundesregierung aus

Hacker sind in das Netzwerk der Bundesregierung und der Bundesverwaltung eingedrungen. Vor allem das Außenministerium war wohl Opfer der Angreifer. Die Hacker konnten vermutlich bis zu einem Jahr lang Regierungsdaten kopieren oder mitlesen.

...auch in Sachsen.

Warning: Malicious Code Detected on This Website!

Website: www.███schule.de
 Status: **Infected With Malware.** Immediate Action is Required.
 Web Trust: **Not Currently Blacklisted** (10 Blacklists Checked)

Scan	Result	Severity	Recommendation
Malware	Detected	Critical	GET YOUR SITE CLEANED

ISSUE DETECTED	DEFINITION	INFECTED URL
Website Malware	majs-frame-injected6917v24	http://www.███schule.de (View Payload)
Website Malware	majs-frame-injected6917v24	http://www.███schule.de/fleischer.html (View Payload)
Website Malware	majs-frame-injected6917v24	http://www.███schule.de
Website Malware	majs-frame-injected6917v24	http://www.███schule.de
Website Malware	majs-frame-injected6917v24	http://www.███schule.de
Website Malware	majs-frame-injected6917v24	http://www.███schule.de

This URL is categorized as a security risk

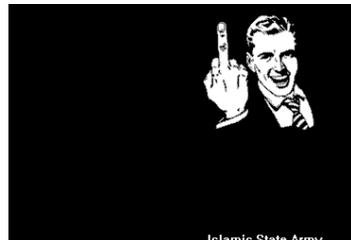
[Malicious Sources/Malnets](#) and [Reference](#)
 🕒 Last Time Rated/Reviewed: June 08, 2018 11:23:20 GMT

Hacked By Fallag Gassrini & darkshadow-tn

Fuck MuhmadEmad Fuck MuhmadEmad Fuck MuhmadEmad Fuck MuhmadEmad Fuck MuhmadEmad Fuck MuhmadEmad
 thank you [gassrini](#) for the tool



„Letzte Woche erzeugten Bots automatisch massenhaft Benutzerkonten auf unserer Webseite, um SPAM-Nachrichten mittels der Bestätigungsmails zu verbreiten. Die vorhandenen Captchas wurden automatisiert überwunden.“



Prophet S.A.W said, you will invade the Arabian Peninsula and Allah will grant it to you. Then (you will invade) Persia and Allah will grant it (to you). Then, you will invade Rome and Allah will grant it (to you). Then, you will invade The Dajjal and Allah will grant it (to you). Then, you will invade The Dajjal and Allah will grant it (to you).

[CB-Report#20180212-10001127] Schadprogramm-Infektionen in Ihrem Netzbereich

CERT-Bund Reports <reports@reports.cert-bund.de>

📧 Sie haben diese Nachricht am 13.02.2018 07:49 weitergeleitet.

Gesendet: Mo 12.02.2018 16:51
 An: SID SAX.CERT

System Warnung

⊗ Ihr Windows-System ist beschädigt Juni 6, 2018

Windows Version : Windows 7

Bitte beachten Sie: Ihre aktuelle Windows Security- Version ist beschädigt und veraltet. Dadurch werden Ihre gesamten Systemdateien automatisch gelöscht **202 Sekunden**

Erforderlich: Klicken Sie unten auf die Schaltfläche "Aktualisieren", um die neueste Software zum Scannen und zum Schutz Ihrer Dateien vor dem Löschen zu installieren.

Aktualisieren

„Auf den beiden betroffenen PC wurden ca. 8.000 mit Trojanern infizierte Dateien gefunden. Infektionsgründe waren ein unbedachter Klick auf eine Phishing-Mail und der Besuch einer suspekten Webseite.“

Site is Blacklisted
 9 Blacklists checked

Wie passiert das?

- I **Schadsoftware:** Immer dynamischere Schadsoftware ist unterwegs, Antivirus ohne APT-Schutz/Sandboxing lässt 25% der Viren durch, 50% aller Verbindungen sind verschlüsselt.
- I **Hackerangriffe:** Cyberspione und Hacker haben aufgrund der stärkeren Digitalisierung immer mehr Angriffsfläche.
- I **Schwachstellen:** Abwehrmaßnahmen sind bei weitem nicht der aktuellen Gefährdung angemessen.

Trend 1: Phishing



Guten Abend,

bis Ende der Woche dürfte die Sache abgeschlossen sein. Nochmals sorry für die Verspätung, aber wenn die Mails in meiner Abwesenheit eintreffen, werden diese nicht automatisch weitergeleitet. Die Rechnung kann über den Link heruntergeladen werden.

>>> [Rechnung hier](#)

Herzliche Grüße,

Guten Morgen,

bitte unterschreiben und per Mail an mich zurücksenden.

>> <http://taltus.co.uk/FORM/Ihre-Rechnung/>

Viele Grüße
SID ServiceDesk

ich habe eine Frage zu der Rechnung im Anhang.
Diese ist nicht beauftragt und bei keinem anderen Vertrag vorhanden.

<http://wickedskinz.net/Fakturierung/Ihre-Rechnung/>

Bitte die gekennzeichneten Stellen ergänzen und unterschreiben, bitte mit Stempel außer das SEPA Formular.
Für die Abbuchung.

<http://nutrisea.net/Rechnungsanschrift/Rechnung/>

bezugnehmend auf unsere Telefonate vom 1. und 05. Juni möchten wir uns nach dem Stand unserer Rechnung erkundigen.
Falls der Betrag noch nicht angewiesen wurde, bitten wir um Überweisung auf unser Konto bei der Bank.

>>> <http://starcoimpex.com/FORM/Erinnerung-an-die-Rechnungszahlung/>

anbei die Steuerbescheide. Sie sind in Ordnung und entsprechen nun den eingereichten Steuererklärungen.
Das Guthaben wird Ihnen erstattet; bitte achten Sie auf den Zahlungseingang.

>>> <http://www.murciaterapia.es/DETAILS/Erinnerung-an-die-Rechnungszahlung-Nr052805/>

Wir bedanken uns für Ihr Vertrauen und wünschen Ihnen weiterhin viel Erfolg.

im Anhang dieser E-Mail erhalten Sie Informationen zu Ihrem Vertrag.
<http://avialution.com/Informationen/>

Freundliche Grüße
GM Schöneck - Winter - BM Kontakt ü. Fr. Riems

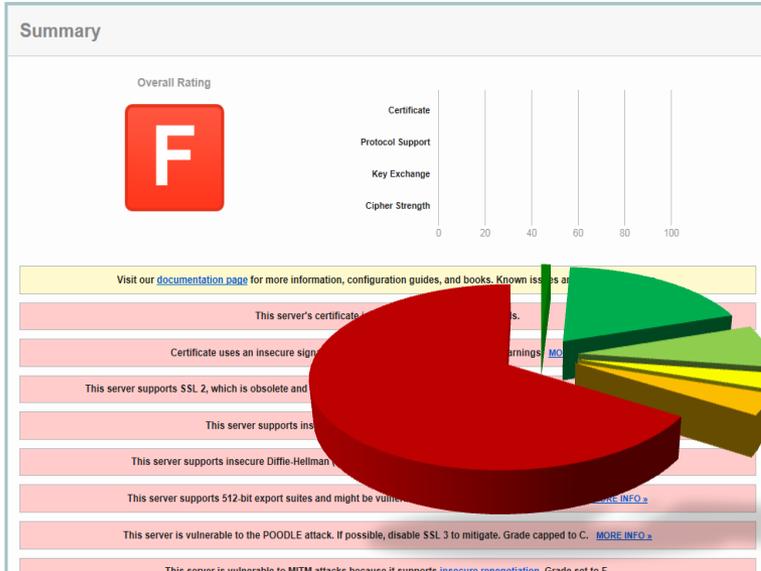
25 Mai

VG Bautzen,

mit dieser E-Mail schicke ich Euch zwei wichtige Dokumente.

<http://dekarlos.com/Zahlungserinnerung/Fakturierung/>

Trend 2: Webseiten



Site is Outdated

(using Joomla Version 1.5.18 to 1.5.26)

Joomla! 1.5 EOL (End of Life) notice - Sept 2012. All security patches have ceased.

Drupal-Lücke mit dramatischen Folgen

Alert! 29.10.2014 19:52 Uhr - Ronald Eikenberg

Jede Drupal-Installation, die am 15. Oktober nicht binnen Stunden gepatcht worden ist, muss man als kompromittiert betrachten. Mit dieser drastischen Einschätzung wendet sich das Drupal-Team an die Öffentlichkeit. Wohl dem, der ein Backup hat.

- A+
- A
- A-
- B
- C
- F

Hack auf Bundesregierung erfolgte über Lernplattform Ilias

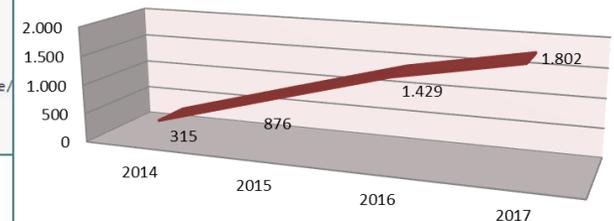
Die Bundesregierung wurde über die Lernplattform Ilias gehackt, die an der Hochschule des Bundes zu Weiterbildungszwecken genutzt wird. Die Einrichtung nutzte eine alte Version mit zahlreichen [Sicherheitslücken](#).

Apache 1.3.28 Released

Apache 1.3.28 was released on 18th July 2003

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 1.2.0
22/tcp	filtered	ssh	
23/tcp	filtered	telnet	
25/tcp	open	smtp	Postfix smtpd
80/tcp	open	http	Apache httpd 1.3.28 ((Linux/SuSE) mod_ssl/2.8.15 OpenSSL/0.9.7b PHP/4.3.3 mod_perl/1.2.8 FrontPage/
110/tcp	open	pop3	Courier pop3d
143/tcp	open	imap	Courier Imapd (released 2003)

Entwicklung der Angriffe auf das SVN



...und was jetzt?

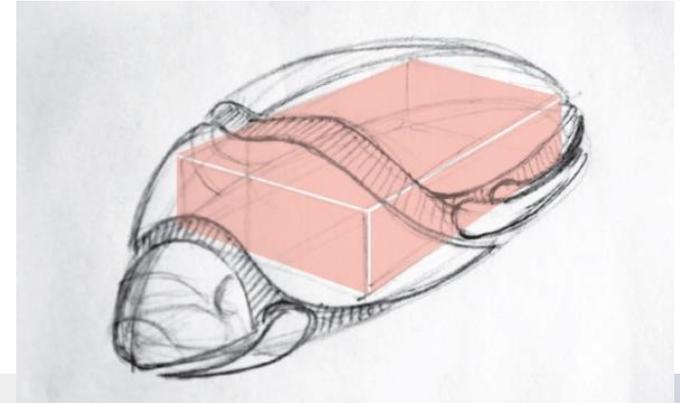
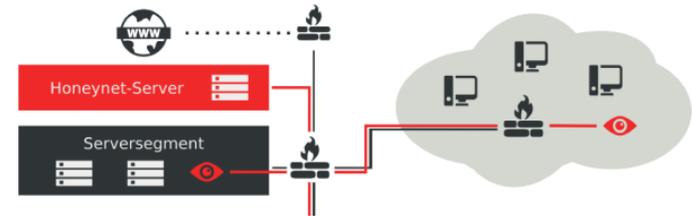
- I **Priorität 1: aktuelle Lageübersicht** auf Basis gesicherter Daten:
 - **technische Bestandsaufnahme** der Infrastruktur,
 - Durchführung **monatlicher Sicherheitserhebungen**,
 - **verbindliche Meldepflicht** Sicherheitsvorfälle seit 2016.

- I **Ziel:** Ableitung und Controlling der wichtigsten Basismaßnahmen für eine **reale Erhöhung der praktischen Sicherheit**.

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



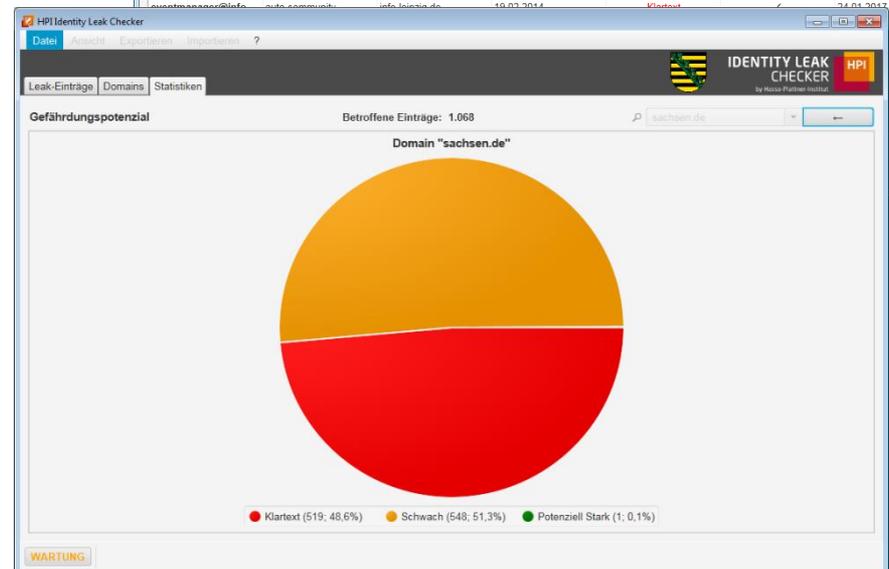
Identity Leak Checker

- 2014: BSI findet 18 Mio. Identitäten, HPI startet Leak Checker und die Zusammenarbeit mit Land Sachsen
- Bis heute: über 5,3 Mrd. gestohlene Identitäten gefunden...
- ILC-Client warnt Sachsen bei neuen Veröffentlichungen

Lösung für alle Länder nutzbar!



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@verwal...	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@...	spielforum	sachsen-gov.de	21.09.2012	Klartext	✓	24.01.2017
biolehrer@schule.dr...	shoppingportal	dresden.de	22.09.2016	Potenziell Stark	✓	24.01.2017
bjoern-streier@land...	shoppingportal	sachsen.de	22.09.2016	Potenziell Stark	✓	24.01.2017
dariuskalter-aktien...	clouddienst	info-leipzig.de	06.06.2016	Potenziell Stark	✓	24.01.2017
direktor.schul@lan...	de-nachrichten	sachsen.de	31.12.2008	Schwach	✓	24.01.2017
direktionschef@info...	auto-community	info-leipzig.de	19.02.2014	Klartext	✓	24.01.2017



Security Dashboard

I Bietet Lageüberblick aus **Managementsicht**:

- Bericht zu Sicherheitsvorfällen
- Sensordaten, z.B. HoneySens
- Scans: Lücken im Zeitverlauf
- Zuordnung Behörde / Ort
- Aktuelle Angriffslage

I Basis für **Maßnahmenplanung**



Maßnahmen

I Umgesetzte **Maßnahmen in Sachsen:**

- Sensibilisierungsveranstaltungen,
- E-Learning-Plattform Info-Sicherheit,
- Grundverschlüsselung SVN2.0,
- Handlungsempfehlungen Verschlüsselung,
- DDoS- und APT-Schutz, SSL-Schutz geplant.



I Maßnahmenbündelung: **IT-Sicherheitsgesetz in Arbeit**

Zusammenfassung

- I Bei begrenzten Ressourcen: **Fokus auf Praxis** notwendig.
- I Wichtigste Grundlagen: **Sensibilisierung und regelmäßige Sicherheitstests** für reales Lagebild.
- I Und: **nie aufgeben!**

Live Hacking Tour:
lsnq.de/hacking

Alle Lösungen zur **Nachnutzung** verfügbar.

Kontakt: sax.cert@cert.sachsen.de

Vielen Dank für Ihr Interesse!



Erfahren Sie mehr...

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

Besucheradresse:
Glacisstraße 4
01097 Dresden

Telefon 0351 3264 6630

Telefax 0351 3264 6209

