STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

# CERT - das wirklich wahre Leben

SAX.CERT

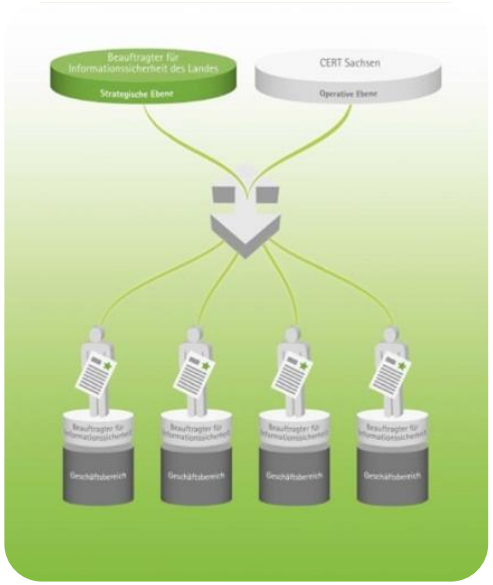
# Agenda

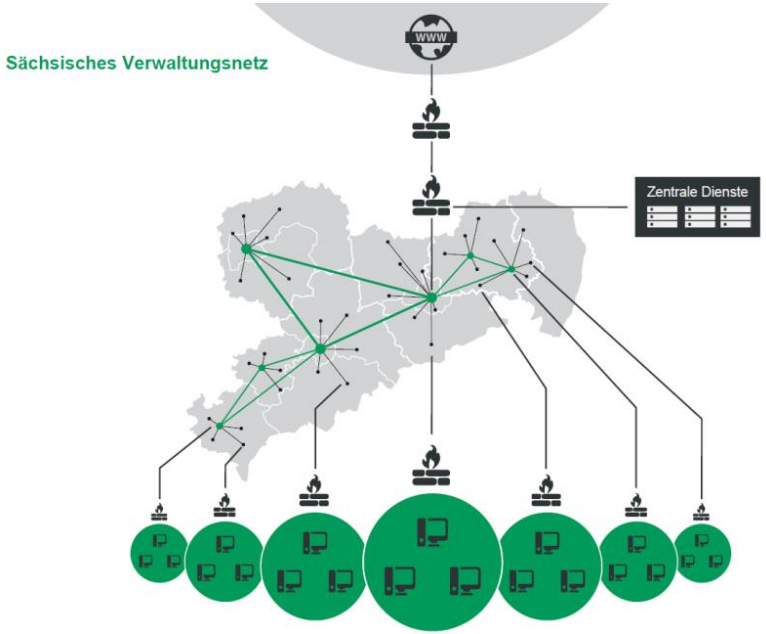
1. Wie ist die Lage in der sächsischen Landesverwaltung?
2. Welche Maßnahmen werden ergriffen?
3. Bitte mitmachen!

SAX.CERT

# 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



# 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

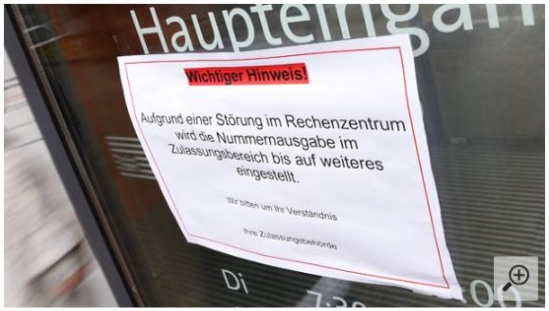
Der Landtag ist durch Schadsoftware lahmgelegt worden. Abgeordnete und Mitarbeiter wurden angewiesen, Telefone und Computer vom Netz zu nehmen. Seitdem ist der Landtag offline und vom Telefonnetz genommen.

## Gefährlicher Virus in Online-Bewerbung

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)

## Gesamtes IT-Netz des Bundestages muss ausgetauscht werden

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.

SICHERHEIT

## Hackerangriff aufs Rathaus

ERMITTLUNG

## Computer-Virus: Verwaltung kann nur eingeschränkt arbeiten

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

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.

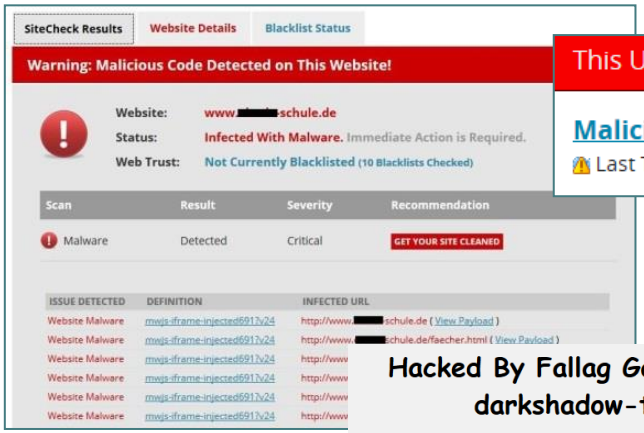
## Hacker spionieren die Bundesregierung aus

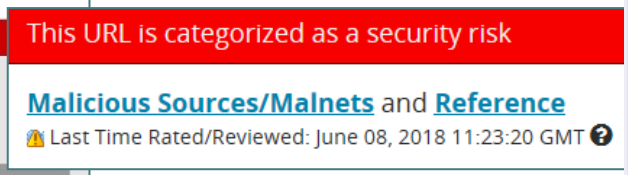
Hacker sind in das Netzwerk der Bundesregierung und der Bundesverwaltung eingedrungen. Vor allem das Außenministerium war wohl Opfer der Angreifer. Die Hacker konnten vermutlich bis zu einem Jahr lang Regierungsdaten kopieren oder mitlesen.

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

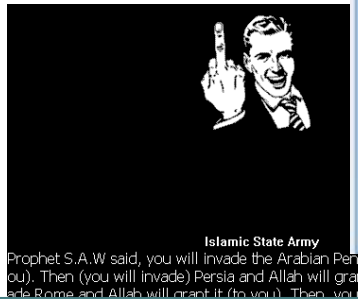
Freistaat
SACHSEN

# …auch in Sachsen.

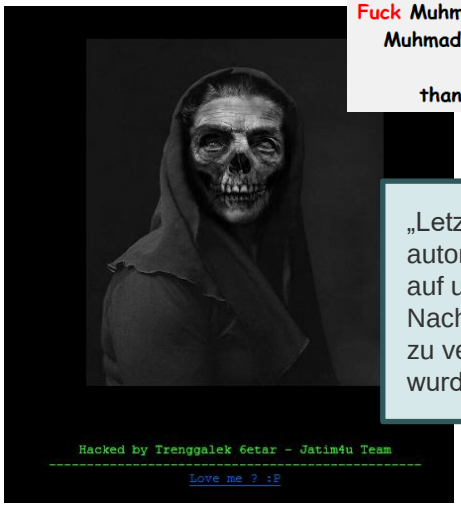




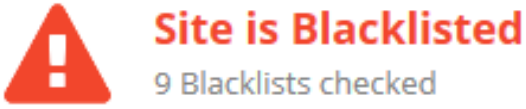








„Letzte Woche erzeugten Bots automatisch massenhaft Benutzerkonten auf unserer Webseite, um SPAM-Nachrichten mittels der Bestätigungsmails zu verbreiten. Die vorhandenen Captchas wurden automatisiert überwunden.“

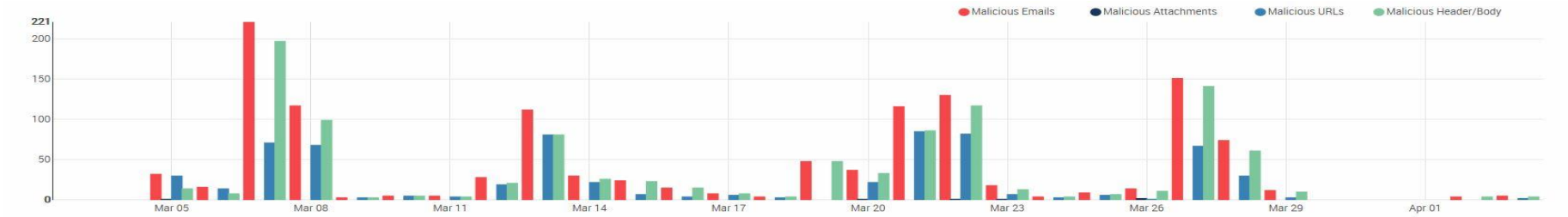



„Auf den beiden betroffenen PC wurden ca. 8.000 mit Trojanern infizierte Dateien gefunden. Infektionsgründe waren ein unbedachter Klick auf eine Phishing-Mail und der Besuch einer suspekten Webseite.“

# Wie passiert das?

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

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/

Von: SID ServiceDesk <1914@
An: SMI Beteiligungsportal
Cc:
Betreff: Rechnungs Details 917991

Guten Morgen,

bitte unterschreiben und per Mail an mich zurücksenden.

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

Viele Grüße
SID ServiceDesk

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

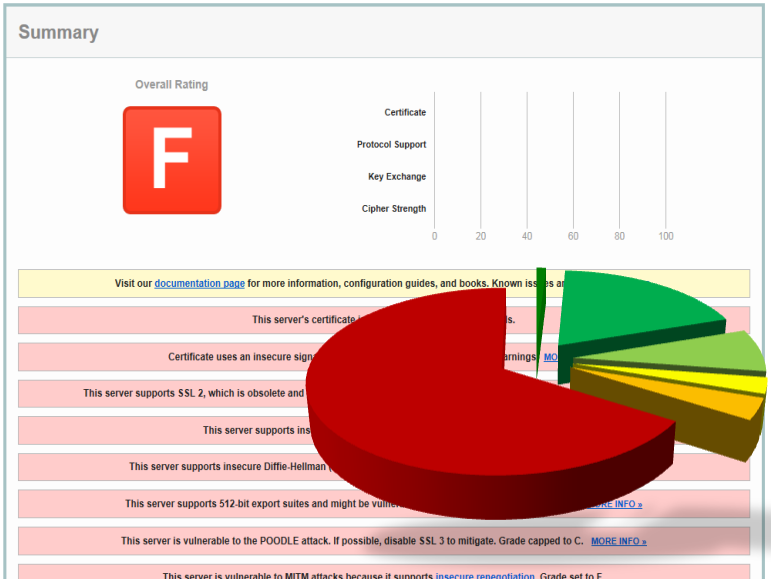
h 25 Mai

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.**

## Hack auf Bundesregierung erfolgte über Lernplattform Ilias

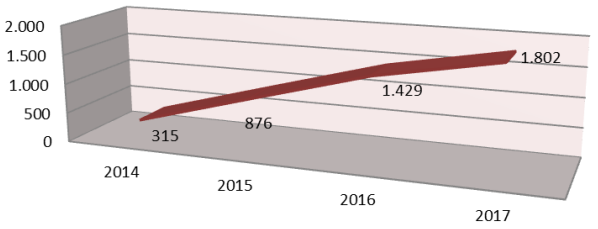
Die Bundesregierung wurde über die Lernplattform Ilias gehackt, die an der Hochschule des Bundes zu Weiterbildungszwecken genutzt wird. Die Einrichtung nutzte eine alte Version mit zahlreichen Sicherheitslücken.

```
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/1.28 FrontPage/
110/tcp  open     pop3         Courier pop3d
143/tcp  open     imap         Courier Imapd (released 2003)
```

**Apache 1.3.28 Released**

Apache 1.3.28 was released on 18th July 2003

**Entwicklung der Angriffe auf das SVN**

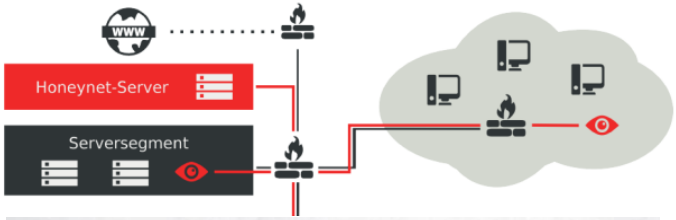


# …und was jetzt?

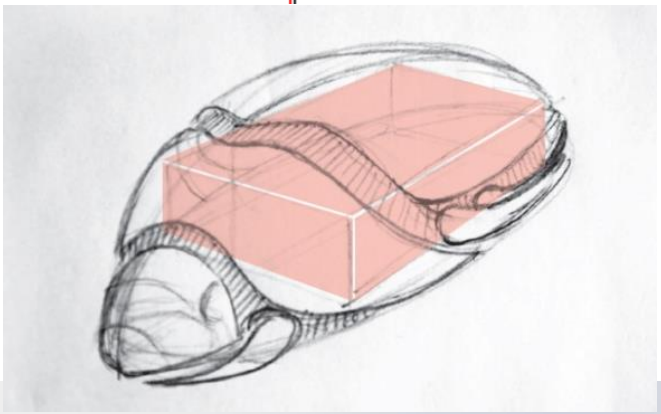
- **Priorität 1: aktuelle Lageübersicht** auf Basis gesicherter Daten:
  - **technische Bestandsaufnahme** der Infrastruktur,
  - Durchführung **monatlicher Sicherheitserhebungen**,
  - **verbindliche Meldepflicht** Sicherheitsvorfälle seit 2016.

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

# HoneySens



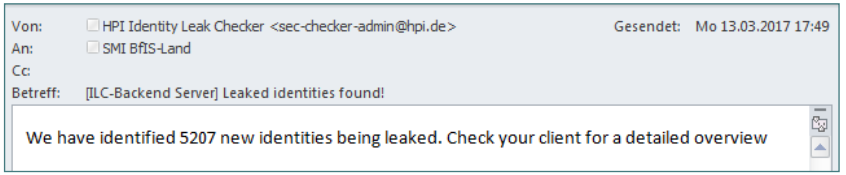

- Hohe Bedeutung der **Innenerkennung** von Schadsoftware und Hackern
- **Lösung: Hackerfallen** mit zentralem Management und Service, ideal auch für KMU und Kommunen
- **Industriepartner:** T-Systems MMS

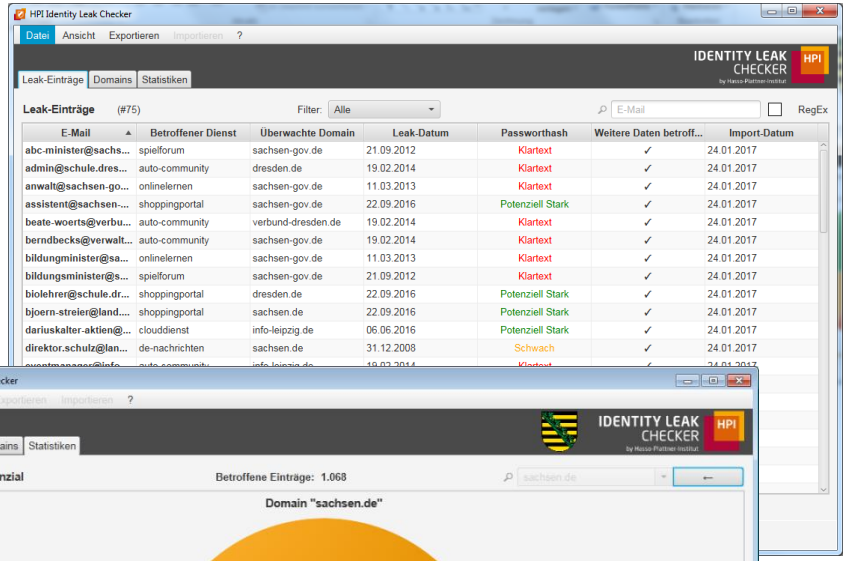


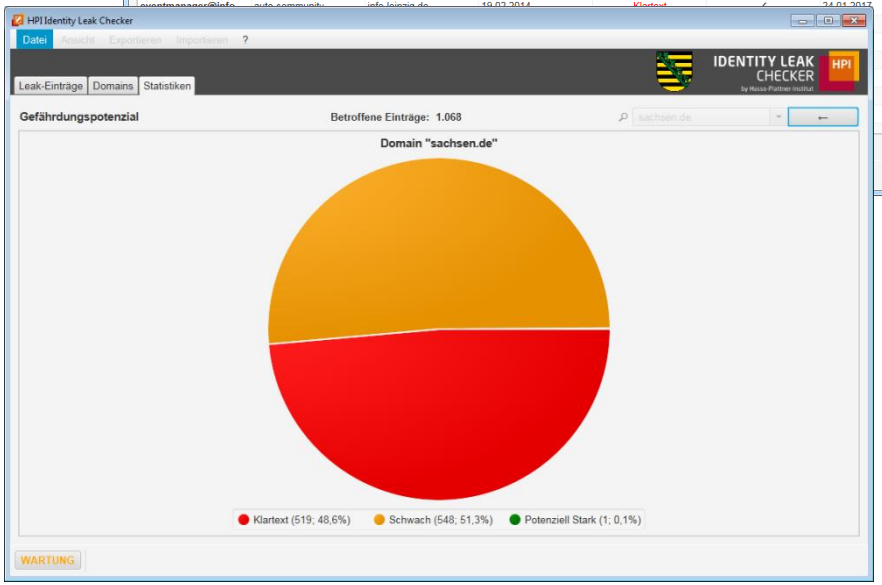
**Rundum-Betrieb oder Open Source**

# 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!**

# Security Dashboard

- Bietet Lageüberblick aus **Managementsicht:**
  - Bericht zu Sicherheitsvorfällen
  - Sensordaten, z.B. HoneySens
  - Scans: Lücken im Zeitverlauf
  - Zuordnung Behörde / Ort
  - Aktuelle Angriffslage
- Basis für **Maßnahmenplanung**

# Maßnahmen

- Umgesetzte **Maßnahmen in Sachsen**:
  - Sensibilisierungsveranstaltungen,
  - E-Learning-Plattform Info-Sicherheit,
  - Grundverschlüsselung SVN2.0,
  - Handlungsempfehlungen Verschlüsselung,
  - DDoS- und APT-Schutz, SSL-Schutz geplant.
- Maßnahmenbündelung: **IT-Sicherheitsgesetz in Arbeit**

# Zusammenfassung

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

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