STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Impfpflicht für alle –
Lagebericht des SAX.CERT

SAX.CERT

Agenda

1. Aktuelle Lage: Krankheiten und Epidemien
2. Erste Hilfe: Das Sicherheitsnotfallteam
3. Wie können Sie sich selbst schützen?

SAX.CERT

Hacker sind eine Krankheit…

Schadprogramm im Netzwerk der DRK-Trägergesellschaft

Massive Cyber-Attacke auf Krankenhäuser

TEAMVIEWER

Polizei warnt Firmen nach Hackerangriffen in Augsburg

Cyberangriff auf Messe Stuttgart größer als angenommen

Das Kommunikationsnetz der Stadtwerke Stuttgart, der Veranstaltungsgesellschaft in.Stuttgart sowie das der Stuttgart-Marketing ist zusammengebrochen, bestätigte ein Sprecher von in.Stuttgart. Dazu gehören

Meldungen VerwaltungsCERTVerbund:

Mailrelay versendet hundertausende SPAMs;
30 Server einer Behörde verschlüsselt;
Ausfall Landesnetz nach DDoS-Attacke;
Nach Virenwelle Infektionen in 12 Behörden;
Webseite KfZ-Wunschkennzeichen gehackt…

„Hacker sind bei einem deutschen IT-Dienstleister mit Kunden in 75 Ländern eingedrungen, haben alle IT-Systeme verschlüsselt und ca. 500 GB Daten (300.000 Dateien mit E-Mails, Verträgen und Tickets) abgezogen sowie im Internet frei veröffentlicht."

Hacker-Angriff legt lippische Arztpraxen lahm

Kreis Lippe. Die Praxen in Lage, Detmold und Lemgo sind besetzt, aber behandelt wird niemand. Im Verbund des Medizinischen Versorgungszentrums Lippe (MVZ) ist das Computersystem am Donnerstag durch einen Trojaner lahm gelegt worden. Das Klinikum

VIRENBEFALL: STADT GEHT VOM NETZ

Derzeit sind die Mitarbeiter nur noch telefonisch erreichbar, die Rechner sind komplett lahmgelegt. Auch das Buchungssystem ist betroffen. Die Stadt kann keine Zahlungen mehr anweisen. Onlinebasierte Dienstleistungen wie Ab-, An- und Ummeldungen, das Ausstellen von Personalausweisen und der Service der Kfz-Zulassungsstelle sind ebenso nicht mehr möglich. Die Verwaltung geht

…auch in Sachsen.

Innenministerium und Polizei warnen vor gefälschten Bußgeldbescheiden

Betrüger versenden per E-Mail gefälschte Knöllchen im Namen der Polizei und der Zentralen Bußgeldstelle

Trojaner legt Computersystem der Collm-Klinik lahm

Im Oschatzer Krankenhaus gab es jetzt einen Notfall der besonderen Art. Ein Computervirus, getarnt als E-Mail-Anhang, griff in das System der Collm-Klinik an. Nach Aussage der Geschäftsführerin konnte weitestgehend analog weiter gearbeitet werden.

CERT-Bund
@certbund
Folgen

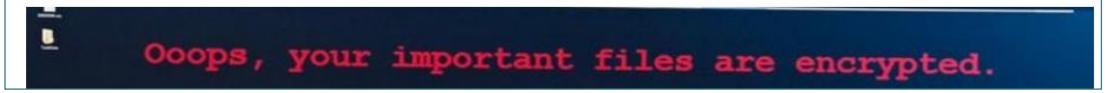
⚠️ Angreifer versenden aktuell gefälschte Bewerbungen im Namen von "Lena Kretschmer" zur Verbreitung der #Ransomware #GermanWiper. Nicht die Anhänge der Mail öffnen! ⚠️

Hackerangriff auf Alu-Konzern Norsk Hydro trifft auch Gießerei bei Leipzig

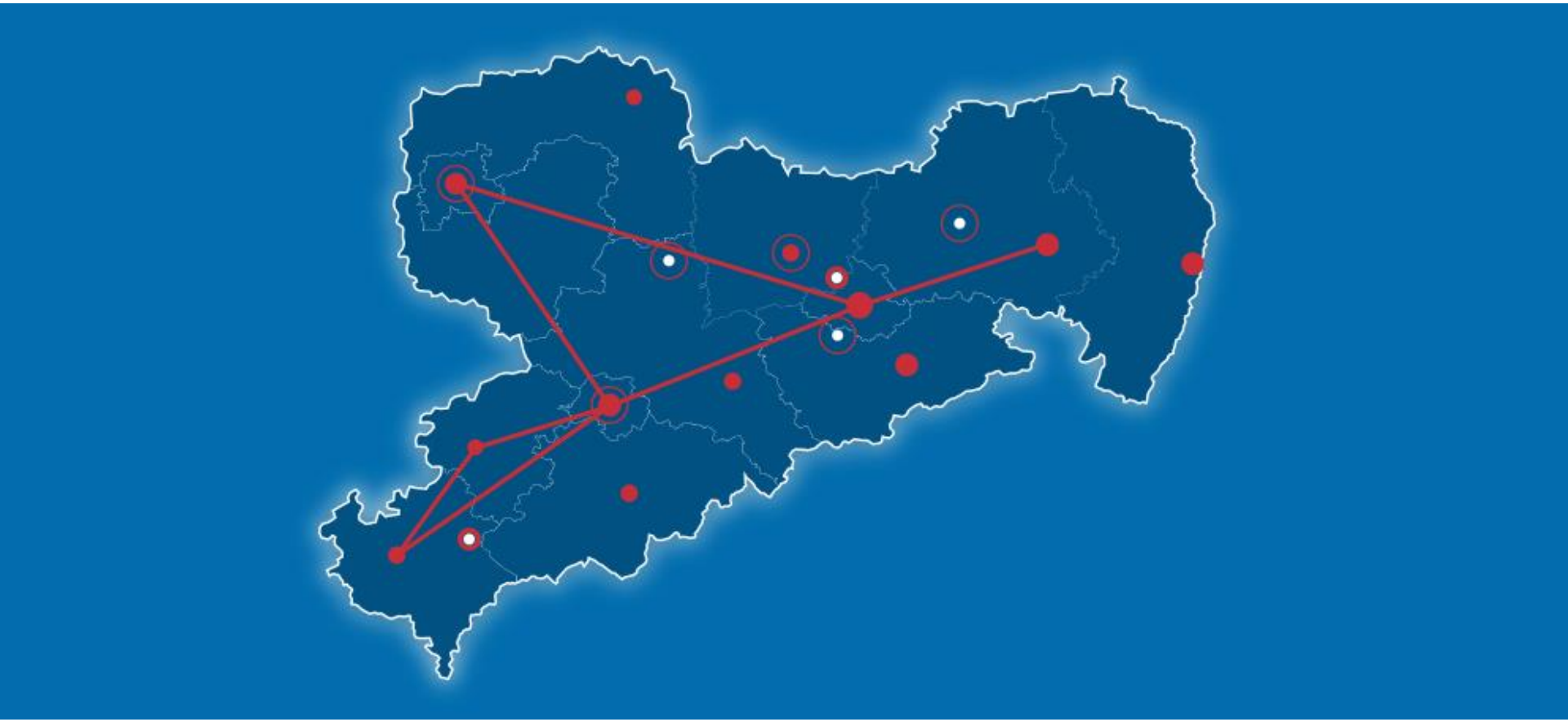
„Nach einem Hack der TK-Anlage wurden innerhalb weniger Tage 10.670 Auslands-verbindungen mit einer Dauer von 63.351 Minuten aufgebaut. Der Schaden wird auf mehrere zehntausend Euro geschätzt.“

„Durch die SVN-Sperrlisten fielen Verbindungen eines Smartphones in Richtung eines Spyware- und Botnetzes in China auf. Es besteht der Ver-dacht des Abfließens von SMS, Anruferlisten und anderen persönlichen Daten.“

Sachsens Verwaltung wird derzeit massiv von Hackern attackiert. In diesem Monat fand man bereits rund 26 000 E-Mail-Viren, teilte der Staatsbetrieb Informatikdienste am Freitag mit. Das zuständige Computer Emergency Response Teams innerhalb des Staatsbetriebes hält dagegen.



Aktuelle Epidemien



Leaks

„In den letzten 5 Monaten 93 neue Leaks mit 443 Mio. Datensätzen im Identity Leak Checker aufgenommen, davon über 1.000 Adressen aus der öffentlichen Verwaltung in Sachsen."

Betroffener Dienst	Kategorie	Import-Datum	Leaks gesamt	Leaks Sachsen
myfitnesspal.com	Health	20.06.2019	143.343.877	338
sabiosciences.com	Shopping	18.07.2019	158.395	175
animoto.com	Entertainment	20.08.2019	22.439.713	110
dubsmash.com	Entertainment	17.08.2019	161.548.687	67
strongholdkingdoms.com	Gaming	12.06.2019	5.180.955	61
armorgames.com	Gaming	22.07.2019	10.108.727	54
wibdesign.de	Art & Design	07.08.2019	268.779	27
cardmarket.com	Shopping	17.06.2019	709.137	26
8tracks.com	Music	12.08.2019	17.973.604	22
jagex.com	Gaming	23.08.2019	1.556.187	18
catiacommunity.com	Community	18.07.2019	316.441	18
mgmresorts.com	Travel	19.07.2019	3.079.857	14
blankmediagames.com (Town of Salem)	Gaming	17.05.2019	7.569.669	11
Mastercard (Priceless Specials)	Finance	20.08.2019	89.386	10

Emotet-Leakmails

Liebe Kunden,

aufgrund eines Viren/Trojaner Befalls (Name: Emotet) auf einer unserer Systeme wurde das Mailsystem der Firma [redacted] am 31.05 zwischen 10:05-10:33 übernommen. Hierbei wurde auch Ihre Mailadressen entwedet, um Ihnen sogenannte Fake Mail's mit einem verseuchten Anhang zu senden. Insgesamt wurde ca 2000 Mails versendet.

Gesendet: Donnerstag, 6. Juni 2019 14:32
An: SID SAX.CERT
Betreff: AW: Sicherheitsvorfall

Sehr geehrter Herr Damm,

am 21.05.2019 habe ich eine E-Mail von einem Lieferanten bekommen welcher wohl Opfer einer Trojaner Mail wurde. Im guten Glauben habe ich den Anhang, eine DOC Datei, geöffnet, da ich eine Rechnung vermutete. Leider habe ich wohl so auch meinen PC infiziert.

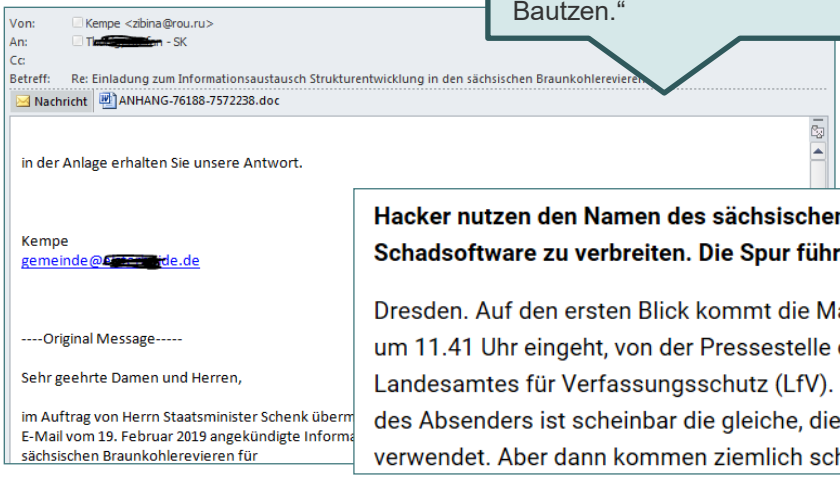
Am 22.05.2019 erhielt ich eine ABUSE E-Mail von meinem Hoster mit dem Hinweis, dass meine E-Mail-Adresse massiv für den Versand von Spammails missbraucht werden.

„Betroffen waren: 7.6. KMU in Königstein, 6.6. Anwaltskanzlei in Berlin, 6.6. und 3.6. 4x KMUs in Sachsen, 4.6. Gemeinde in Sachsen, 4.6. Schule in Leipzig, 4.6. und 31.5. 5x Landesverwaltung Sachsen-Anhalt, 30.5. und 28.5. 2x KMUs aus Dresden, 28.5. Wirtschaftsprüfer in NRW, 26.5. und 17.5. 2x Landesverwaltung Niedersachsen, 24.5. Bildungseinrichtung in Hoyerswerda, 21.5. Landesverwaltung Hamburg, 20.5. Stadt in Sachsen, 15.5. Schule in Niedersachsen, 14.5. Rechtsanwalt in Dresden, 7.5. Schule bei Bautzen.“

Stand heute sind 18 Vorfälle in Folge der Virusinfektion in der Gemeinde bekannt. Betroffen sind 7 Behörden in 4 verschiedenen Ministerien:

- 11x Daten zu Veranstaltungen, z.B. Einladungen und Schriftverkehr
- 3x Daten zu einem Fachverfahren (Informationsschreiben)
- 3x Daten zu einem Newsletter
- 1x Grußschreiben

Bei jedem dieser Fälle sind die von den Mitarbeitern der Landesverwaltung versandten Informationen komplett aus der Gemeinde abgeflossen und wurden auf weltweit verteilte gehackte Postfächer kopiert, die dann die Phishingmail im Namen der Gemeinde an das SVN versendeten (hier u.a. in Russland, Polen, Ecuador, Großbritannien, Simbabwe und Brasilien; aber auch z.B. auf einen gehackten Schulserver eines anderen Bundeslandes).


Von: Kempe <zibina@rou.ru>
An: [redacted] - SK
Cc:
Betreff: Re: Einladung zum Informationsaustausch Strukturentwicklung in den sächsischen Braunkohlerevieren
Nachricht ANHANG-76188-7572238.doc

in der Anlage erhalten Sie unsere Antwort.

Kempe
gemeinde@[redacted]de.de

----Original Message-----

Sehr geehrte Damen und Herren,

im Auftrag von Herrn Staatsminister Schenk überm
E-Mail vom 19. Februar 2019 angekündigte Informa
sächsischen Braunkohlerevieren für

Hacker nutzen den Namen des sächsischen Geheimdienstes, um Schadsoftware zu verbreiten. Die Spur führt nach Russland.

Dresden. Auf den ersten Blick kommt die Mail, die am Mittwoch um 11.41 Uhr eingeht, von der Pressestelle des sächsischen Landesamtes für Verfassungsschutz (LfV). Die E-Mail-Adresse des Absenders ist scheinbar die gleiche, die auch das Amt verwendet. Aber dann kommen ziemlich schnell Zweifel. Schon

Forensikbericht aus dem Landesnetz: „Der Dropper, Loader und der Emotet-Trojaner kamen unter den Nutzerrechten des Anwenders zur Ausführung und konnten sich im System persistent einrichten und zumindest eine Zeit lang nach außen kommunizieren.“

Erste Hilfe


ERSTE HILFE
Edition
...AUCH KLEINE WUNDEN
SOFORT VERSORGEN !
SAX.CERT
Made in Germany

SAX.CERT - Das Sicherheitsnotfallteam

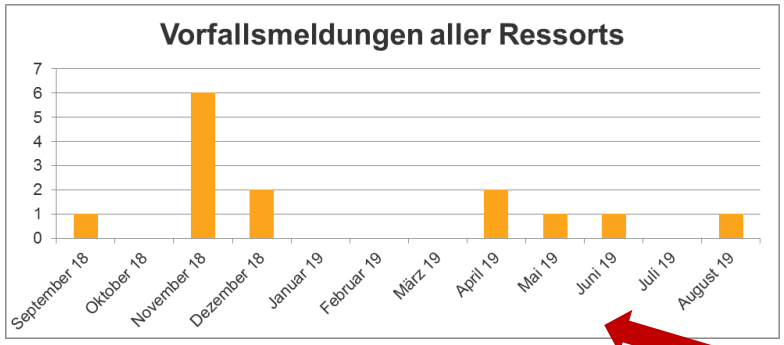
- Derzeit **Sachgebiet im SID,** kürzlich verstärkt auf jetzt **6 Mitarbeiter** und Sitz in der **Außenstelle Glacisstraße im Regierungsviertel.**

- **Zuständigkeiten:** Information, Unterstützung bei **Sicherheitsvorfällen und Virenverdacht**, Erstellung **Lagebild**, zentrale Meldestelle, regelmäßige **Sicherheitstests.**

- **Ansprechpartner** für **alle Ressorts und Landesbehörden**, für **alle Kommunen** (neu seit 31.8.2019) und für **KRITIS-Unternehmen** in Sachsen (ebenfalls neu seit 31.8.2019).

- **Kontakt:** Tel. **0351 79997799**, E-Mail **sax.cert@cert.sachsen.de**, Internet **www.cert.sachsen.de**

Achtung Praxis!



Beschluss 1/2016
71. Sitzung des AK ITEG am 12. Januar 2016

Der AK ITEG nimmt die Beschlüsse Nr. 07/2015 „Änderung GO“ und Nr. 08/2015 „Sicherheitsmeldungen“ der AG IS zur Kenntnis. Die Ressorts werden gebeten, das auf der Internetseite www.cert.sachsen.de bereitgestellte CERT-Meldeformular für Sicherheitsvorfälle umfassend zu nutzen.

In einem ersten Schritt soll bereits der Verdacht auf mindestens folgende Ereignisse in den Ressorts und den nachgeordneten Geschäftsbereichen unverzüglich gemeldet werden:

a. Schadwirkung durch ein Schadprogramm,
b. Einbruch in ein System oder Netzwerk,
c. nicht autorisierte Veränderung einer Internetseite,
d. schwerwiegende oder erfolgreiche Überlastungsangriffe auf eine Internetseite,
e. nachgewiesene Abflüsse / Verluste personenbezogener oder vertraulicher Daten,
f. schwerwiegende, über normale Wiederherstellungszeiten hinausgehende ungeplante Ausfälle von bedeutsamen IT-Verfahren.

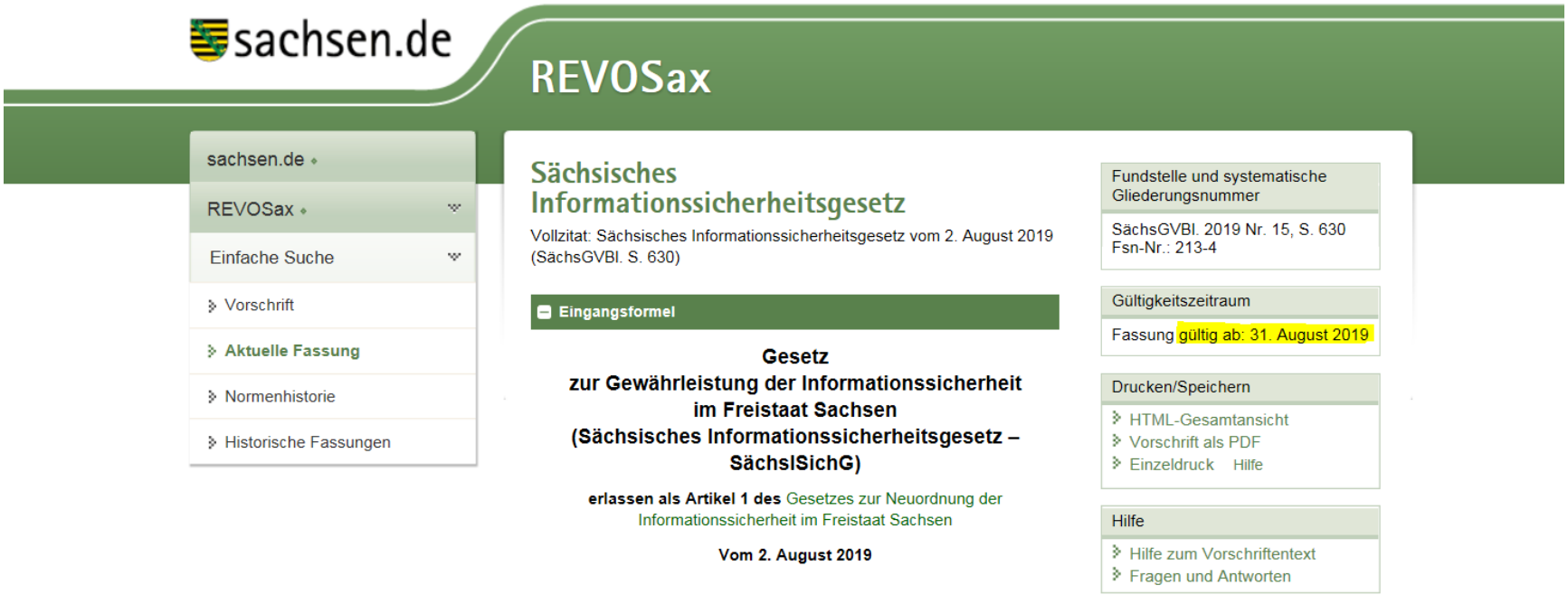
Auf Ihren Hinweis und nach Prüfung der vertraglichen Vereinbarungen bitten wir entsprechend des vereinbarten Berichtswesens, um Auswertung und Interpretation der Log-Files durch Sie dergestalt, dass die in der E-Mail an das BZ SVN vom 5. Juni 2019 übermittelten bekannten Absenderadressen von Schadsoftware im <Envelope from>-Feld im beschriebenen Zeitraum gesucht werden und alle auf diesen Filter zutreffenden Mails (Logfelder: Datum, Envelope-from, Anhang ja/nein, Envelope-to; falls verfügbar auch From) kurzfristig als Auswertung zusammenzustellen.

Auf die von Ihnen als Inhaltsdaten eingeordneten Betreffzeilen würden wir in diesem Schritt insofern verzichten.

Diese Daten sind von TKG geschützt und dürfen laut Konzernvorgaben nicht ohne richterlichen Beschluss herausgegeben werden.
Diese Daten sind von SAX CERT zur Aufklärung von 61 Sicherheitsvorfällen angefordert worden.
Wir haben zwar ein Register der datenschutzrechtlichen Verfahren definiert und in der Vergangenheit abgestimmt. Er beinhaltet kein solches Verfahren zur Herausgabe von Mailheader Information.

Das Informationssicherheitsgesetz

- Zum **31. August 2019** in Kraft getreten - das neue **SächsISichG: https://recht.sachsen.de/vorschrift/18349**



Wie können Sie sich selbst schützen?

Infektionen schon bei Verdacht melden!

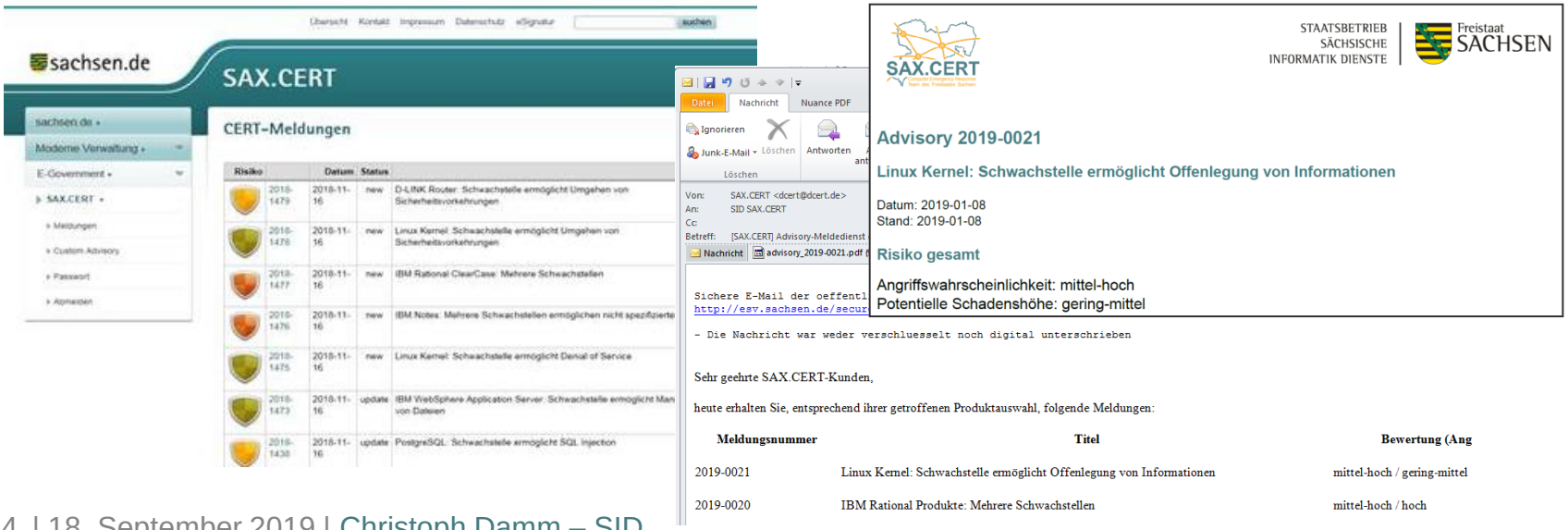
- Nur bei einer Meldung kann geholfen und eine **Infektion anderer Stellen** verhindert werden. Allgemein: geringer Mehraufwand für Betroffene, aber **große Hilfe für andere…**

- Festlegung von 2016 weiter sinnvoll - neu: **auch für Kommunen!**

> In einem ersten Schritt soll bereits der Verdacht auf mindestens folgende Ereignisse in den Ressorts und den nachgeordneten Geschäftsbereichen unverzüglich gemeldet werden:
>
> a. Schadwirkung durch ein Schadprogramm,
> b. Einbruch in ein System oder Netzwerk,
> c. nicht autorisierte Veränderung einer Internetseite,
> d. schwerwiegende oder erfolgreiche Überlastungsangriffe auf eine Internetseite,
> e. nachgewiesene Abflüsse / Verluste personenbezogener oder vertraulicher Daten,
> f. schwerwiegende, über normale Wiederherstellungszeiten hinausgehende ungeplante Ausfälle von bedeutsamen IT-Verfahren.

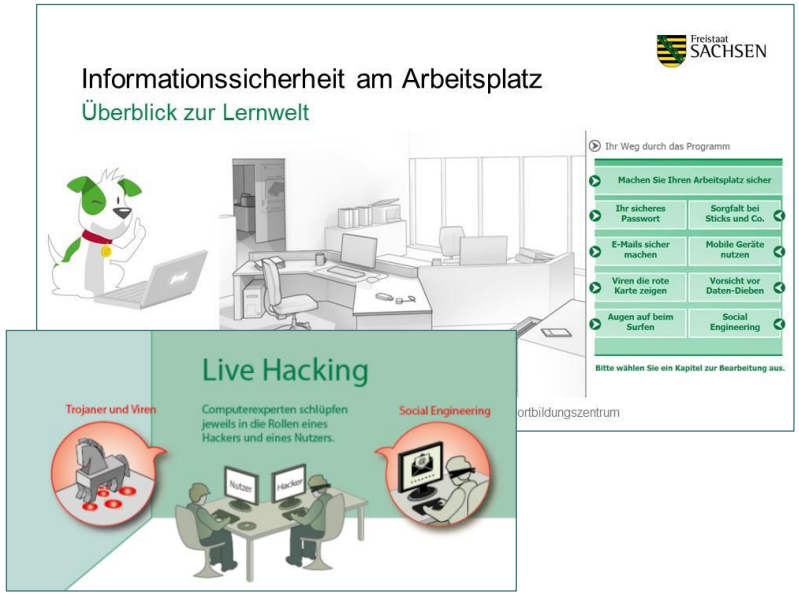
Pflaster (Patches) helfen!

- Das kurzfristige Einspielen von Softwareaktualisierungen (Patches) ist weiter eine der **wirkungsvollsten Schutzmaßnahmen**.
- Warn- und Informationsdienst des SAX.CERT für über 2.000 Produkte von 185 Herstellern – individualisierbar und **kostenfrei nutzbar!**



Wissen schützt!

- „INFOSIC – Die Hacker kommen 2019“ in 10 Städten in Sachsen: **https://lsnq.de/infosic2019** (Land), **https://lsnq.de/Hacking** (Bürger).
- E-Learning am Arbeitsplatz: **https://lsnq.de/InfosicAmAP**



Zusammenfassung

- Die Lage der Informationssicherheit **bleibt angespannt**.
- Dank SächsISichG unterstützt das SAX.CERT nun mit mehr Personal **alle Ressorts, Kommunen und KRITIS-Unternehmen** in Sachsen.
- Bitte dennoch selbst schützen:
  Melden, Patchen, Informieren!

Das SAX.CERT berät Sie dabei gern.

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