LANDTAG VON
BADEN-WÜRTTEMBERG

Webmontag Stuttgart #63

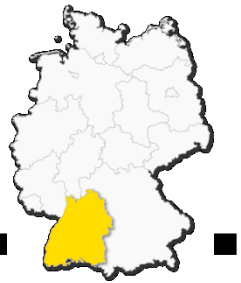
Networking und Vorträge rund ums Web

Informationssicherheit - Alles hoffnungslos?

Aus dem Alltag eines Informationssicherheitsbeauftragten

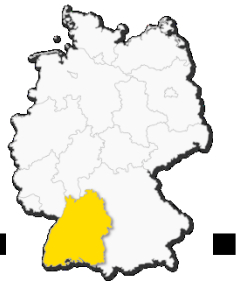
Rolf Häcker

27.05.2019 im Landtag von Baden-Württemberg



Informationssicherheit

- Informationssicherheit ist mehr als IT-Sicherheit
- Infos in
  - IT-Systemen
  - Auf Papier
  - In den Köpfen
  - …



Britischer Antiterrorchef Bob Quick tritt zurück

Informationssicherheit

https://iconicphotos.wordpress.com/2009/05/22/bob-quick-exposes-secret-documents/

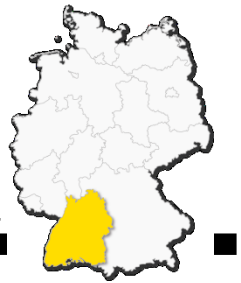
Informationssicherheit ist nicht nur IT-Sicherheit!

Bob Quick exposes secret documents

On April 9th, 2009, Bob Quick, the most senior counter-terrorism officer in the United Kingdom, was photographed in Downing Street carrying two folders and a briefing paper for the Prime Minister, Gordon Brown. As he exited the car, the picture taken of Mr. Quick and the exposed document information about “Operation Pathway”, an attempt to thwart “suspected AQ (al-Qaeda) driven attack” and the immigration status of the eleven suspects and the location of the targets to be raided, seven addresses in Manchester, Merseyside and Lancashire.

Aktuelle Situation - informationsverarbeitende Systeme

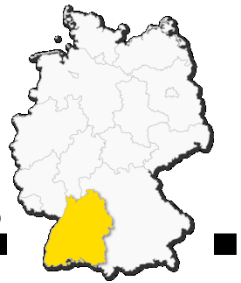
- Die globale Digitalisierung schreitet unaufhaltsam voran
- Wir alle nutzen Informationen und informationsverarbeitende Systeme



Aktuelle Situation - informationsverarbeitende Systeme

- Smartphones
- Online-Banking
- Online-Einkäufe
- Navigationssysteme
- Just in Time Fertigung
- Industrie 4.0

- Kritische Infrastruktur im Netz
- Fitnesstracker, Pulsuhren
- Heimautomation
- Internet of Things
- autonomes Fahren
- …



Fitness-App

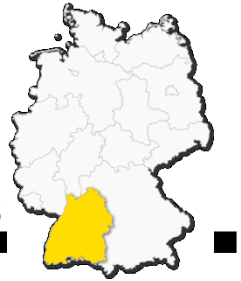
www.scinexx.de Das Wissensmagazin

Spion am Handgelenk

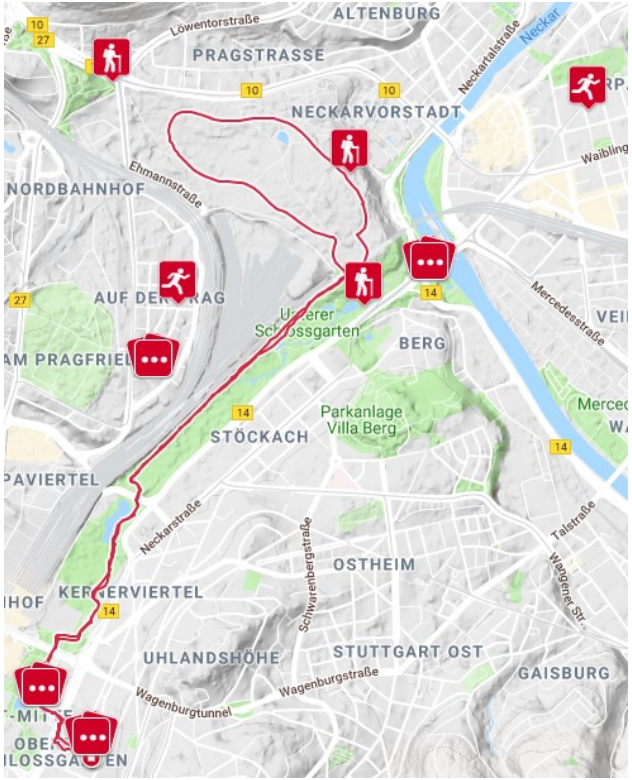
Smartwatch und Fitness-Tracker können unsere PINs und Passwörter verraten

Fatale Sicherheitslücke: Der Mini-Computer am Handgelenk weiß mehr als wir ahnen - und kann einem Hacker sogar unsere Passwörter und Bank-PINs verraten. Denn ihre eingebauten Bewegungssensoren registrieren unsere Tippbewegungen und aus diesen Daten lassen sich die PINs rekonstruieren, wie ein Experiment nun belegt: Ein Algorithmus erreichte dabei schon im ersten Anlauf eine 80-prozentige Trefferquote.

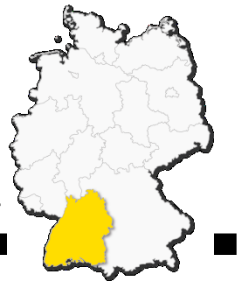
Wenn wir am Geldautomaten unsere PIN eingeben, registrieren die Sensoren des Fitnesstrackers oder der Smartwatch millimetergenau unsere Bewegungen.



Fitness-App



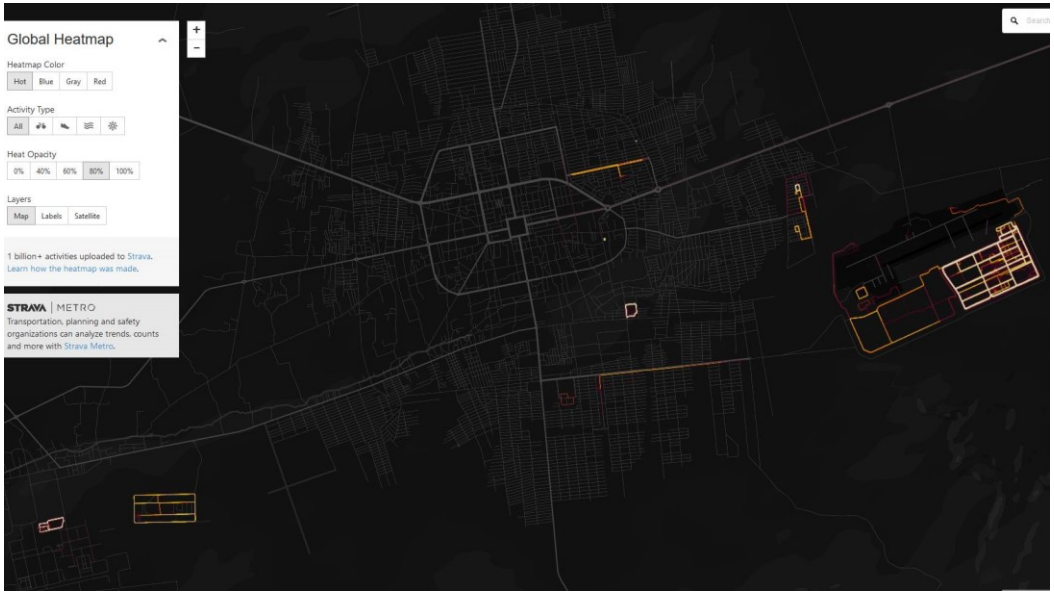
- Trainingseinheiten
- Geolokation
- Fitness-Daten
- Datum, Dauer
- Geschwindigkeit
- Höhe
- Puls



Fitness-App

Fitnesstracker: Strava-Aktivitätenkarte legt Militärbasen und Soldaten-Infos in aller Welt offen

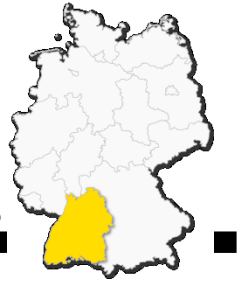
UPDATE 29.01.2018 10:13 Uhr



heise online heise+

Nicht nur Zivilisten, sondern auch Soldaten tracken offenbar fleißig ihre Bewegungen. Eine von Strava erstellte Weltkarte aller Aktivitäten legt deshalb teilweise geheime Militärbasen offen und zeigt beispielsweise regelmäßige Jogging-Routen.

Von Martin Holland



https://www.heise.de/newsticker/meldung/Fitnesstracker-Strava-Aktivitaetenkarte-legt-Militaerbasen-und-Soldaten-Infos-in-aller-Welt-offen-3952875.html

Fitness-App

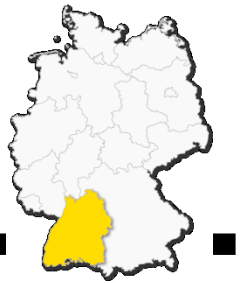
n-tv

Dienstag, 30. Januar 2018

Bewegungsprofile von US-SoldatenPentagon überprüft Fitness-Tracker-Nutzung

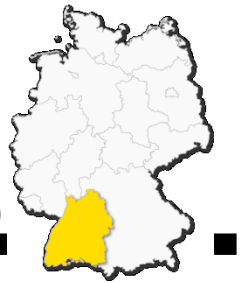
Fitness-Tracker liegen im Trend - auch bei US-Soldaten. Eine nun veröffentlichte Karte eines App-Anbieters ruft das US-Verteidigungsministerium auf den Plan, denn die Karte zeigt die Bewegungen ihrer Nutzer weltweit und liefert so Hinweise auf geheime US-Stützpunkte.

Nach der Veröffentlichung einer Karte mit Bewegungsprofilen von US-Soldaten auch in Konfliktgebieten durch eine Fitness-App überprüft das US-Verteidigungsministerium die Nutzung sogenannter Fitness-Tracker durch Armeeangehörige. Die Veröffentlichung der Daten zeige die Notwendigkeit eines stärkeren Bewusstseins, sagte Pentagon-Sprecher Rob Manning.



Aktuelle Situation - informationsverarbeitende Systeme

- Wir verlassen uns täglich darauf, dass diese Systeme **zuverlässig** und **sicher** für uns arbeiten und Kommunikationspartner verantwortlich mit unseren Daten umgehen
- Es trifft uns hart, wenn unerwartete Ereignisse eintreten, wenn wir etwa feststellen müssen, dass Dritte unsere Onlinekonten angreifen und über unsere Daten verfügen



Hacker zwacken Rechenleistung von Behörde ab, um Kryptogeld zu schürfen

heise online News › 01/2018 › Hacker zwacken Rechenleistung von Behörde ab, um Kryptogeld zu…

10.01.2018 15:08 Uhr Dennis Schirrmacher

(Bild: Landesamt für Besoldung und Versorgung Baden-Württemberg)

https://www.heise.de/newsticker/meldung/Hacker-zwacken-Rechenleistung-von-Behoerde-ab-um-Kryptogeld-zu-schuerfen-3938113.html

Das Landesamt für Besoldung und Versorgung Baden-Württemberg ist Opfer einer Hackerattacke geworden. Dabei sollen die Angreifer aber keine Daten abgezogen haben.

Bislang unbekannte Hacker sind mehrmals erfolgreich in das Computersystem des Landesamts für Besoldung und Versorgung Baden-Württemberg eingestiegen. Die Übergriffe fanden seit Herbst 2017 bis Anfang dieses Jahres statt, erklärte die Behörde.

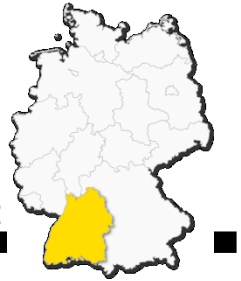
Dabei sollen die Angreifer Rechenleistung von Servern in Anspruch genommen haben, um so Krypto-Währung wie beispielsweise Monero zu schürfen. Das heimliche Schürfen von Krypto-Währung auf Computern von Opfern ist aufgrund explodierender Kurse von Bitcoin & Co. derzeit ein Trend in der Malware-Szene.

Hackerangriff in Baden-Württemberg

Hackerangriff auf Landesamt für Geoinformation und Landentwicklung

Am 24. April 2018 wurde in einer gemeinsamen Pressemitteilung der Staatsanwaltschaft Stuttgart und des Landeskriminalamts Baden-Württemberg von einem Hackerangriff auf Server des Landesamts für Geoinformation und Landentwicklung berichtet.

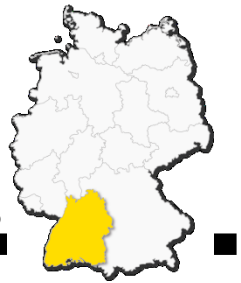
https://www.stuttgarter-nachrichten.de/inhalt.rems-murr-kreis-polizei-verdaechtigt-25-jaehrigen-nach-hackerangriff-auf-landesamt.aa20023e-3bd2-4ee7-bcee-8691e988c1c3.html



Hackerangriff in Baden-Württemberg auf KRITIS-Unternehmen

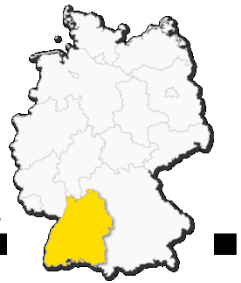
Große Anfrage 24.01.2018; Drucksache 16/3345

- Aus dem Bereich Energie liegen aus den polizeilichen Ermittlungen Erkenntnisse zu einem Sicherheitsvorfall im Jahr 2017 in einer Kritischen Infrastruktur vor.
- Das Landesamt für Verfassungsschutz (LfV) berichtet: 2017 gab es einen Angriff mit mutmaßlich nachrichtendienstlichem Hintergrund gegen baden-württembergische Unternehmen aus dem KRITIS-Bereich, der als IT-Sicherheitsvorfall zu werten ist.
- Betroffen war die Netcom BW, eine Tochter der EnBW



Situation bei E-Mail und Schadsoftware im Jahr 2018

- **Über 90 % als unerwünschte oder schädliche E-Mails erkannt**
- **Bei mehreren 100 E-Mails explizit Schadsoftware identifiziert**



heise online heise+

Gehackte Websites: 620 Millionen Accounts zum Verkauf im Darknet

12.02.2019 11:03 Uhr

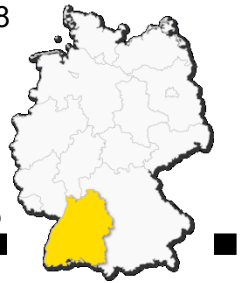
(Bild: geralt)

Eine riesige Datenbank mit Mail-Adressen und Passwörtern steht zum Verkauf. Bei einigen Websites war bislang nicht bekannt, dass sie gehackt wurden.

Von **Dennis Schirrmacher**

Auf der Schwarzmarkt-Website Dream Market bietet ein Verkäufer eine mehrere Gigabyte große Datenbank mit aus Hacks erbeuteten persönlichen Daten für 20.000 US-Dollar an. Der Marktplatz befindet sich nicht im öffentlichen Internet – er ist über das Tor-Netzwerk erreichbar.

The Register berichtet in einer Meldung über das Datenleak. Stichproben zufolge seien die Daten echt. Sie sollen von 16 verschiedenen Websites aus den Jahren 2016 bis 2018 stammen. Bei einigen Seiten war bis zum Auftauchen der Datenbank nicht bekannt, dass sie Opfer einer Hacker-Attacke waren.



https://www.heise.de/security/meldung/Gehackte-Websites-620-Millionen-Accounts-zum-Verkauf-im-Darknet-4305517.html

INFOSECURITY MAGAZINE HOME » NEWS » FRAUD ATTACKS FROM MOBILE SPIKED 300% IN Q1

info security
STRATEGY | INSIGHT | TECHNOLOGY

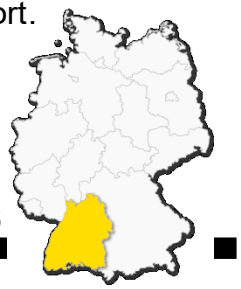
22 May 2019

Fraud attacks from mobile apps spiked by 300% in the first quarter of 2019, according to new researcher from RSA. Published today, the *Fraud Attack Trends: Q1 2019* report found that the total fraud attacks from rogue mobile applications on January 1 was 10,390 but had jumped to 41,313 by March 31.

Rogue mobile apps are those designed to duplicate legitimate apps of trusted brands, which are a fast-growing phenomenon among cyber-criminals and a huge digital risk for consumers and businesses, according to the report.

Kacy Zurkus News Writer

https://www.infosecurity-magazine.com/news/fraud-attacks-from-mobile-spiked-1/



heise online heise+

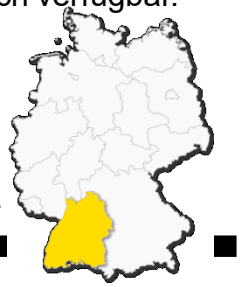
Möglicherweise Kontaktdaten von 49 Millionen Instagram-Nutzern öffentlich

22.05.2019 11:57 Uhr

(Bild: dpa, Tobias Hase)

Kontaktdaten von 49 Millionen Instagram-Nutzern sollen öffentlich im Netz gestanden haben – darunter auch Infos zum Marktwert mehrerer Millionen Influencer.

Eine Datenbank mit persönlichen Kontaktdaten von mehr als 49 Millionen Instagram-Nutzern soll zeitweise öffentlich im Internet abrufbar gewesen sein. Neben öffentlich verfügbaren Informationen zu den Inhabern der Accounts soll die Datenbank auch private Daten, unter anderem Telefonnummern und E-Mail-Adressen, enthalten haben, berichtet das Online-Tech-Magazin Techcrunch. Unter den betroffenen Konten sollen sich auch solche mehrerer Millionen Influencer – unter anderem bekannter Food-Blogger, Prominente und weiterer Social-Media-Beeinflusser – befunden haben. Ihnen war teilweise ihr Marktwert zugeordnet. Die Datenbank ist mittlerweile nicht mehr öffentlich verfügbar.



https://www.heise.de/newsticker/meldung/Moeglicherweise-Kontaktdaten-von-49-Millionen-Instagram-Nutzern-oeffentlich-4428378.html

heise online heise+

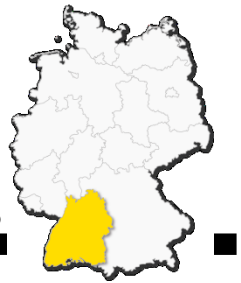
Daten-Leak: US-Immobiliendienstleister stellt 885 Millionen Unterlagen online

25.05.2019 13:18 Uhr

(Bild: pixabay.com)

Vertrauliche Vertragsunterlagen zu Immobilienkäufen in den USA waren frei zugänglich. Dafür genügte ein simples Ändern der Vertragsnummer in der URL.

Ein Dienstleistungsunternehmen für die US-Immobilienbranche hat hunderte Millionen Datensätze zu Vertragsabschlüssen mit vertraulichen Informationen offen auf seiner Website dargeboten. Die Datensätze waren über eine geeignete URL ohne Passwort zugänglich, die Vertragsnummer ließ sich beliebig ändern, berichtet IT-Sicherheitsspezialist Brian Krebs. Mittlerweile ist die Website offline genommen worden.



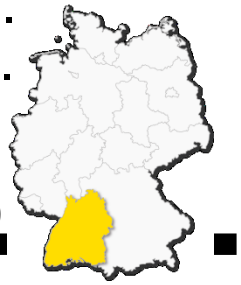
https://www.heise.de/newsticker/meldung/Daten-Leak-US-Immobiliendienstleister-stellt-885-Millionen-Unterlagen-online-4432042.html

Aktuelle Situation - informationsverarbeitende Systeme

Datenklau und Spionage:
Nicht nur große Unternehmen betroffen (02.01.2019)

Das Max-Planck-Institut für ausländisches und internationales Strafrecht hat zusammen mit dem Fraunhofer-Institut für System- und Innovationsforschung und der Polizei herausgefunden: Fast **jedes zweite mittelständische Unternehmen hat bereits einen Angriff auf die eigenen Daten erlebt.** Besonders betroffen waren dabei Firmen aus dem Handel-, Bau- und Dienstleistungsgewerbe. Im Fokus der Studie standen 583 Unternehmen und 713 Strafakte.

https://www.e-recht24.de/news/it-sicherheit/11196-datenklau-und-spionage-nicht-nur-grosse-unternehmen-betroffen.html



Hacker-Angriff auf Staatstheater Stuttgart

Niemand ist mehr sicher

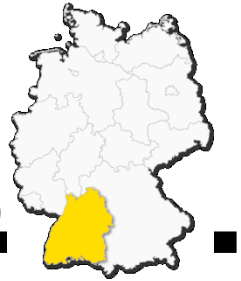
STUTTGARTER-ZEITUNG.DE StZ Plus

Von Andreas Müller 9. April 2019 - 16:14 Uhr

Die Hackerattacke auf die Staatstheater und Unternehmen ist eine Mahnung, noch mehr für die Sicherheit der Datensysteme zu tun, kommentiert StZ-Autor Andreas Müller.

Im Visier von Hackern: die Staatstheater Stuttgart *Foto: dpa*

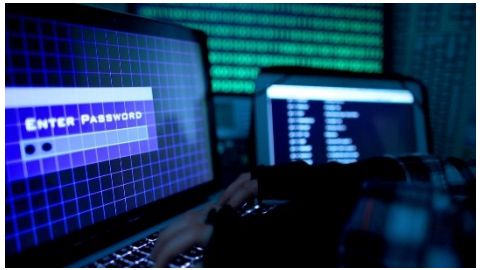
Stuttgart - Man darf annehmen, dass die Stuttgarter Staatstheater nicht gezielt von Hackern angegriffen wurden. Weder bei politischen noch bei wirtschaftlichen Motiven ergäbe dies Sinn: Die Kulturstätte ist – bei allem Respekt – nicht so systemrelevant, dass es den Staat destabilisieren würde, sie zeitweise lahmzulegen. Auch finanziell ist der auf hohe Zuschüsse angewiesene Betrieb sicher nicht prädestiniert, Opfer einer Erpressung zu werden.



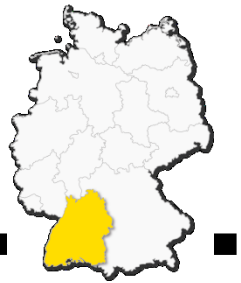
https://www.stuttgarter-zeitung.de/inhalt.hacker-angriff-auf-staatstheater-stuttgart-niemand-ist-mehr-sicher.ebc4f4ac-8113-4089-a73e-b8608b2828af.html?reduced=true

Die Trojaner-Attacke auf die Staatstheater Stuttgart war gravierender als bisher bekannt. Einfallstor war eine IT-Firma.

Stuttgart / Axel Habermehl 10.04.2019 - 19:10 Uhr



Der Hacker-Angriff, dem jüngst das IT-System der Württembergischen Staatstheater Stuttgart zum Opfer gefallen ist, ist offenbar deutlich umfangreicher als bisher bekannt. Der Landes-Datenschutzbeauftragte Stefan Brink sagte am Mittwoch dieser Zeitung, seine Behörde gehe derzeit von einer zweistelligen Zahl von betroffenen Institutionen und Personen aus. Auch habe der Angriff wohl schon früher als bisher berichtet begonnen. Erste Probleme habe es bereits Anfang März gegeben. „Aus unserer Sicht ist das ein schwerwiegender Vorfall, dessen Ausmaße wir noch nicht völlig abschätzen können“, sagte Datenschützer Brink.



https://www.swp.de/suedwesten/staedte/stuttgart/hacker-angriff_-viele-weitere-betroffene-im-land-30701652.html

Bericht: Hacker erpressen Citycomp mit gestohlenen Großkunden-Daten

30.04.2019 17:27 Uhr

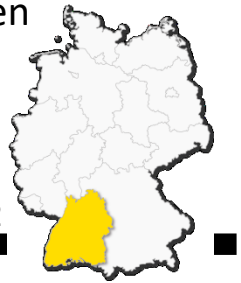
Die Stuttgarter IT-Firma Citycomp wird laut Medienbericht von Hackern erpresst. Über 516 Gigabyte an Daten großer Kunden sollen die Angreifer erbeutet haben.

von **dpa**

"312.570 Dateien in 51.025 Ordnern"

Dem Bericht zufolge behaupten die Hacker, im Besitz von "312.570 Dateien in 51.025 Ordnern" zu sein. In dem Datenbestand von über 516 Gigabyte befänden sich finanzielle und private Informationen. Zu den Kunden gehören demnach Ericsson, Leica, Toshiba, UniCredit, British Telecom, Hugo Boss, NH Hotel Group, Oracle, Airbus, Porsche und Volkswagen. Auch die Supermarktketten Rewe und Kaufland seien betroffen. (axk)

https://www.heise.de/newsticker/meldung/Bericht-Hacker-erpressen-Citycomp-mit-gestohlenen-Grosskunden-Daten-4410879.html



Trojaner im Landtag Sachsen-Anhalt

Parlament offline 30. August 2017

(Bildrechte: MDR/Katharina Buchholz)

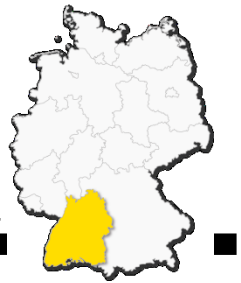
Der Landtag ist durch Schad-software lahmgelegt worden. Abgeordnete und Mitarbeiter wurden angewiesen, Telefone und Computer vom Netz zu nehmen. Seitdem ist der Landtag offline und vom Telefonnetz genommen.

Der Landtag ist weder über das Internet noch per Telefon zu erreichen. Laut Landeskriminalamt (LKA) wurde über einen schadhaften Dateianhang einer E-Mail ein Verschlüsselungstrojaner aktiviert. Betroffen sind nach jetzigem Ermittlungsstand sowohl der Rechner eines Mitarbeiters im Landtag als auch Teile eines angeschlossenen Netzlaufwerkes. Laut LKA-Sprecher Andreas von Koß müssen Experten nun klären, wer den Trojaner verschickt hat.

Meldung des MDR SACHSEN-ANHALT

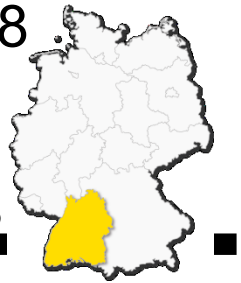
BSI-Bericht *„Die Lage der IT-Sicherheit in Deutschland 2018“*

- Gegen Ende des Jahres 2017 hat das BSI über das Nationale Cyber-Abwehrzentrum Hinweise auf einen erfolgreichen Cyber-Angriff erhalten, von dem einzelne Bundesbehörden betroffen sein sollten.
- *Primäres Ziel des Angriffs war das Auswärtige Amt.*
- *Der Angreifer war in der Lage,* ***einige Client-Systeme im Auswärtigen Amt erfolgreich zu infizieren und interne Dokumente in geringer Stückzahl auszuleiten****.*



Sicherheitslage laut BSI Bericht 2018

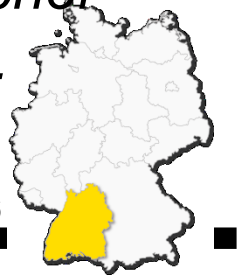
- Über **800 Millionen Schadprogramme** im Umlauf.
  Das sind 200 Millionen mehr als 2017
- Der **Zuwachs** der neuen Schadprogramm-Varianten pro Tag habe **von 280.000 auf 390.000 zugenommen**
- Pro Monat etwa 690.000 neue Android Schadprogramme
- Anstieg von Schadprogrammen für **Android** noch 2018 auf **über 30 Millionen** erwartet



Sicherheitslage laut BSI Bericht 2018

Das BSI schreibt zur **Update-Fähigkeit von Smartphones:**

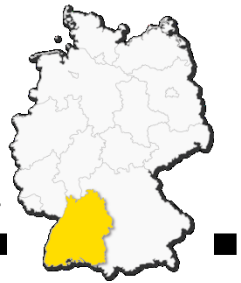
- *Auch Smartphones werden **mit öffentlich bekannten Schwachstellen im Handel als neu vertrieben**, **ohne** dass entsprechende **Sicherheitsupdates** zur Verfügung stehen.*
- *Dadurch existieren für Verbraucherinnen und Verbraucher bei der Nutzung teils **gravierende Sicherheitslücken**.*



Sicherheitslage laut BSI Bericht 2018

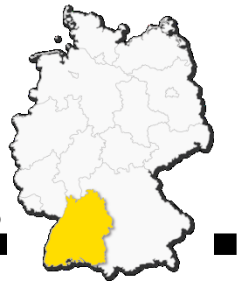
Das BSI schreibt zum Internet of Things (IoT):

- Die Bundesnetzagentur hat die Puppe "MyFriendCayla" 2017 als Spionagegerät eingestuft. Sie funktioniert via Sprachsteuerung – nur können weder Eltern noch Kinder uneingeschränkt beeinflussen, wann die Puppe Gespräche aufzeichnet. Über eine ungesicherte Bluetooth-Verbindung **kann IoT-Spielzeug gar zum Abhörgerät werden**



BITKOM Studie zur Spionage von 2017

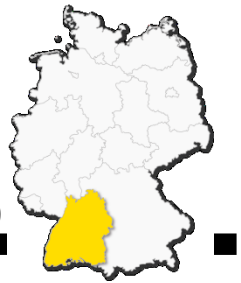
- Durch Spionage, Sabotage, Datendiebstahl **entsteht der deutschen Wirtschaft jährlich ein Schaden von 55 Milliarden Euro**. Mehr als die Hälfte der Unternehmen in Deutschland (53 %) seien in den vergangenen beiden Jahren Ofer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden.



Stromausfall – Thriller

- Marc Elsberg: **Blackout**
- http://www.blackout-das-buch.de/
- „Piero Manzano“

https://www.randomhouse.de/Taschenbuch/BLACKOUT-Morgen-ist-es-zu-spaet-Roman/Marc-Elsberg/e411752.rhd

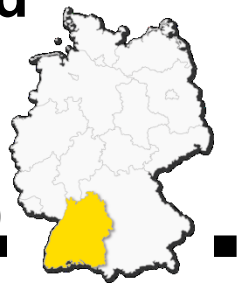


Stromausfall – Deutscher Bundestag Drucksache 17/5672

Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung (27.04.2011)

Technikfolgenabschätzung (TA)

TA-Projekt: **Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung**



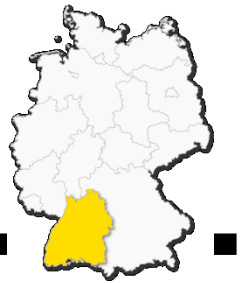
Stromausfall – Realität

Heise.de berichtete am 24.07.2018:

- ***Hacker sollen sich Zugriff zu Kontrollsystemen von US-Energieversorgern verschafft haben.*** *Die US-Regierung sieht Russland hinter den Angriffen.*

Heise.de berichtete am 24.08.2018

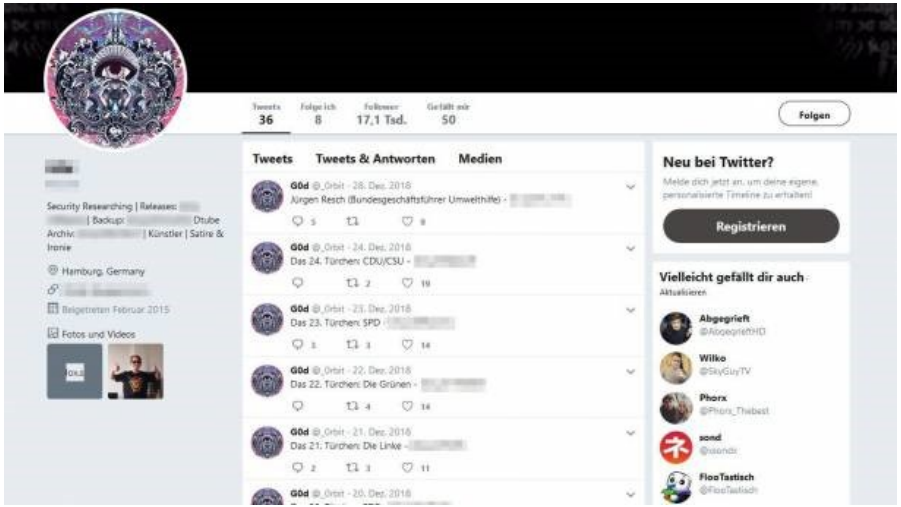
- ***Kritische Infrastruktur: Hacker könnten europaweiten Stromausfall auslösen***
  Cyberangriffe auf deutsche Stromversorger könnten verheerende Folgen haben, warnen Experten in einer vertraulichen Studie. Das berichtet der Spiegel.



heise online heise+

Hackerangriff: Persönliche Dokumente von deutschen Politikern und Promis veröffentlicht

04.01.2019 09:02 Uhr

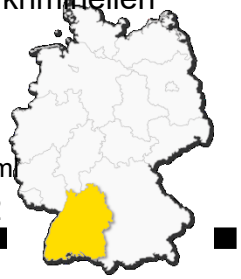


Screenshot des Twitter-Accounts, über den die gehackten Dokumente verbreitet wurden.

Unbekannte haben angebliche persönliche Daten und parteiinterne Dokumente deutscher Politiker und anderer Prominenter veröffentlicht.

Von **Oliver Bünte**

Unbekannte haben im Laufe des Dezembers persönliche Daten und parteiinterne Dokumente Hunderter deutscher Politiker und anderer Personen des öffentlichen Lebens in einem Twitter-Adventskalender veröffentlicht. Betroffen sind Politiker der CDU/CSU, SPD, Grüne, Linke und FDP. Wie die Informationen in die Hände der Cyberkriminellen gelangt sind, ist derzeit noch unklar.

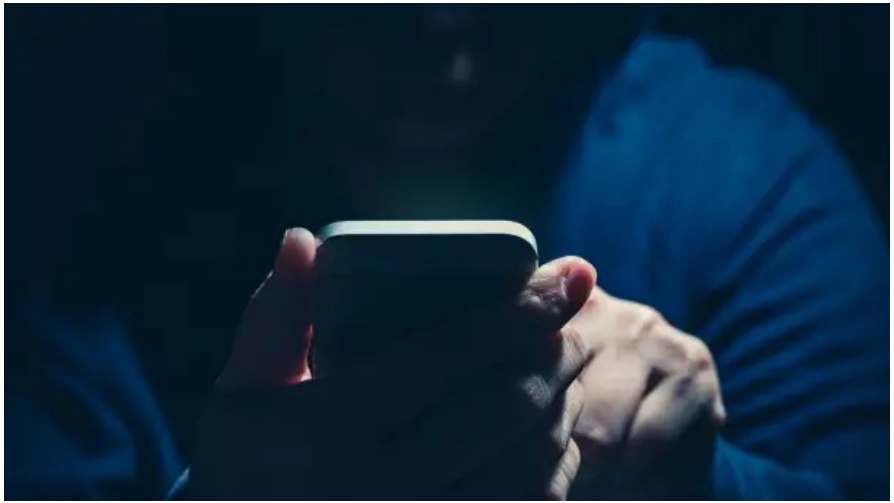


https://www.heise.de/newsticker/meldung/Parteihack-Persoenliche-Dokumente-Hunderter-deutscher-Politiker-veroeffentlicht-4265180.html

heise online heise+

Politiker- und Promi-Hack: Ehemaliges Twitter-Konto eines YouTubers missbraucht

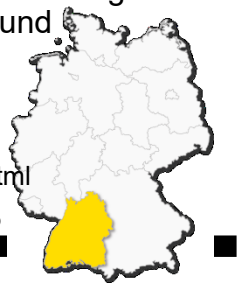
UPDATE 04.01.2019 13:46 Uhr



Der Twitter-Account, der Daten von Parteien und Prominenten veröffentlichte, gehörte früher einem Minecraft-Troll-YouTuber. Die Ziele sind weiter unklar.

Von **Fabian A. Scherschel**

Am gestrigen Donnerstag wurden Mitarbeiter des Berliner Rundfunks RBB auf ein Twitter-Konto aufmerksam, das im Laufe des Dezembers die Daten mehrerer Politiker, YouTuber und Musiker im Rahmen einer Art Adventskalenders veröffentlicht hatte. Das Twitter-Konto @_0rbit, welches im Laufe des heutigen Freitagvormittags gesperrt wurde, kommt angeblich aus Hamburg und hat fast 19.000 Follower.



https://www.heise.de/newsticker/meldung/Politiker-und-Promi-Hack-Ehemaliges-Twitter-Konto-eines-YouTubers-missbraucht-4265608.html

heise online heise+

Massen-Doxxing: Datenklau möglicherweise nicht von Hacker alleine

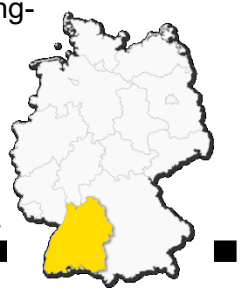
16.01.2019 17:07 Uhr

(Bild: dpa, Silas Stein)

Der Schüler, der auf Twitter private Daten von Politikern und Prominenten illegal veröffentlicht hat, handelte möglicherweise nicht allein.

Von **dpa**

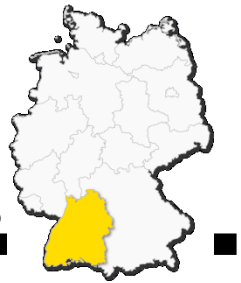
Die Ausspähung und illegale Veröffentlichung privater Daten von Politikern und Prominenten ist möglicherweise nicht von dem tatverdächtigen Schüler alleine begangen worden, wie der rbb und das ARD-Magazin Kontraste berichten. Im Zuge der Ermittlungen zum Datenklau seien Zweifel aufgekommen, ob es sich tatsächlich um einen Einzeltäter handelt. Nach Informationen aus Sicherheitskreisen sei der mutmaßliche Täter trotz eines vollumfänglichen Geständnisses nicht in der Lage gewesen, den Ermittlern zu zeigen, wie er die Daten im Netz erbeutet hatte.



https://www.heise.de/newsticker/meldung/Massen-Doxxing-Datenklau-moeglicherweise-nicht-von-Hacker-alleine-4278619.html

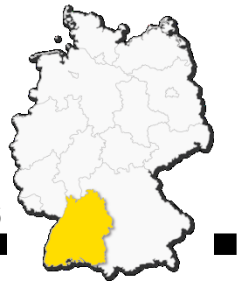
Aktuelle Situation - Kontaktdaten und persönliche Dokumente

- 4. Januar 2019 aus der Presse bekannt:
- **Kontaktdaten und persönliche Dokumente** von deutschen Politikerinnen, Politikern, Journalistinnen, Journalisten und Prominenten veröffentlicht
- → **Datenschutz und Informationssicherheit** sind sehr zentrale und wichtige Themen, die **uns alle** berühren.



Aktuelle Situation - Kontaktdaten und persönliche Dokumente

- ca. 1.000 Betroffene bundesweit, davon ca. 50 stärker
- 54 Abgeordnete aus dem Landtag Baden-Württemberg
- 39 CDU
- 15 GRÜNE
- davon 2 stärker betroffen

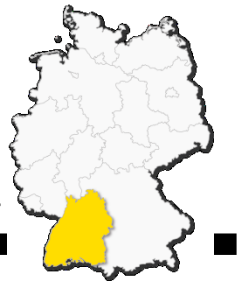


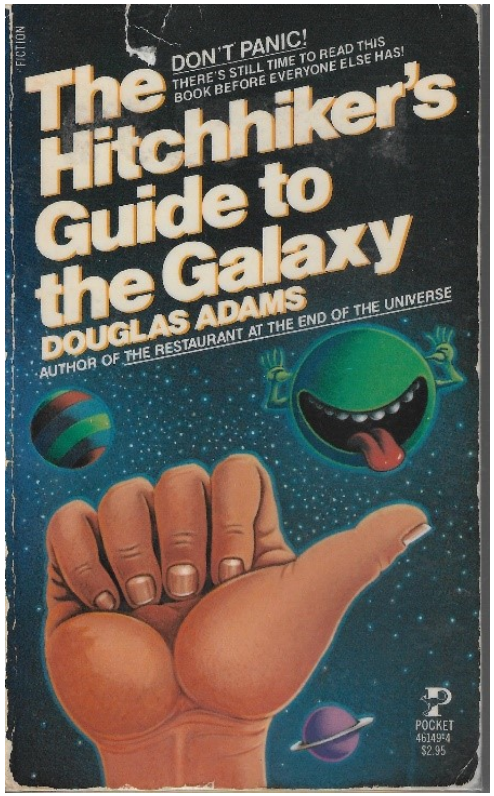
Aktuelle Situation - Der Hacker-Hunter

Troy Hunt und der riesige Passwort-Fund „Collection #1 bis #5“

- **2,2 Milliarden Passwörter** zu Onlinekonten sind im Netz aufgetaucht. Woher kommen die Daten und wer muss jetzt mit Angriffen auf seine digitale Identität rechnen? Der australische Sicherheitsforscher Troy Hunt hat Antworten darauf.
- **Mailadressen prüfen: HavelBeenPwned.com**
- Identity Leak Checker des deutschen HPI nutzen: **sec.hpi.uni-potsdam.de/ilc/**

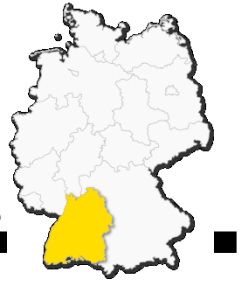
https://www.heise.de/select/ct/2019/04/1550227129581885





Was ist zu tun?

DON‘T PANIC



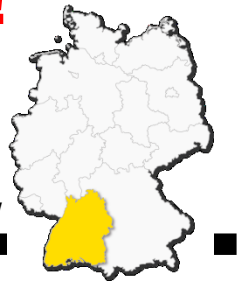
Was ist zu tun?

Cliff Stoll

Schachbuch

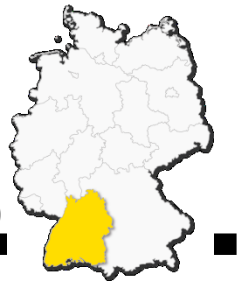
- **Regel 1:**
- **Regel 2:**
- **...**
- **Make the best possible move!**

http://www.kleinbottle.com/index.htm



Maßnahme – für vom Datenleak Betroffene

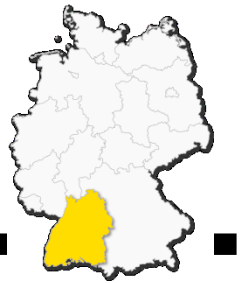
- Betroffene Abgeordnete wurden vom Innenministerium informiert
- Passwörter der betroffenen Systeme unverzüglich ändern!
- Dabei Reihenfolge beachten; E-Mail-Systeme zuerst!
- BSI Hinweis: *IT-Sicherheitsmaßnahmen im Rahmen des aktuellen „Politleaks“*
- Kompletter Scan mit einem aktuellen Virenscanner



Maßnahmen – Empfehlungen des BSI

Weitere Infos:

https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_zum_Schutz_vor_Datendiebstahl_060012019.html



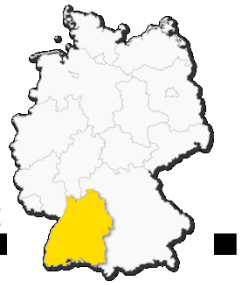
IT-Sicherheitsmaßnahmen; BSI Empfehlungen

Auswahl von Leak-Datenbanken zur Recherche:

- https://sec.hpi.de/ilc/
- https://haveibeenpwned.com/
- https://monitor.firefox.com/
- https://beachalarm.com/

BSI für Bürger Schutzmaßnahmen & Risiken

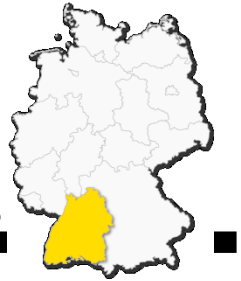
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/BasisschutzGeraet_node.html
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html



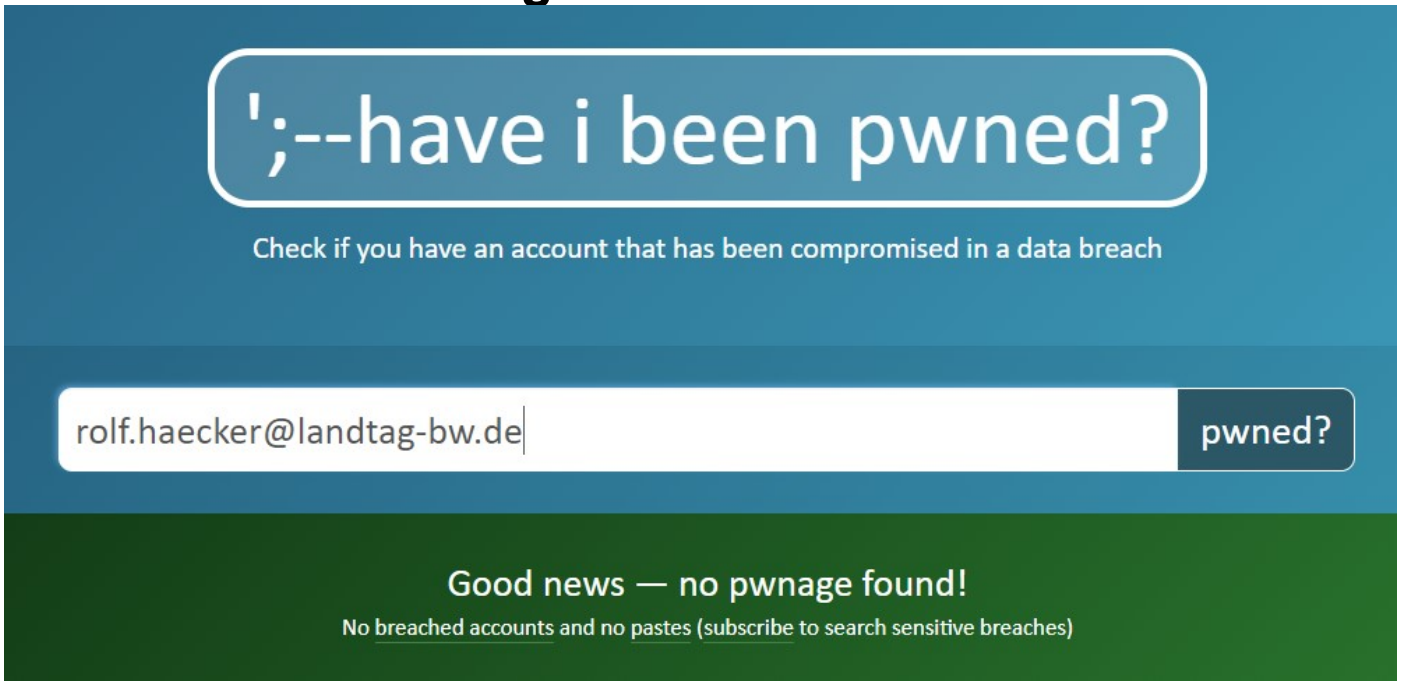
Maßnahme – Prüfung der Betroffenheit

- **Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker**
- **Glückwunsch: Ihre E-Mail-Adresse rolf.haecker@landtag-bw.de taucht nicht in unserer Datenbank auf. Das garantiert jedoch nicht, dass keine Ihrer persönlichen Informationen gestohlen wurden.**

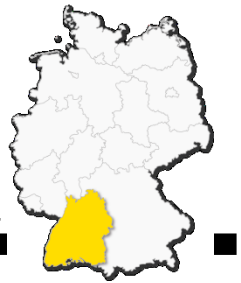
https://sec.hpi.de/ilc/search



Maßnahme – Prüfung der Betroffenheit

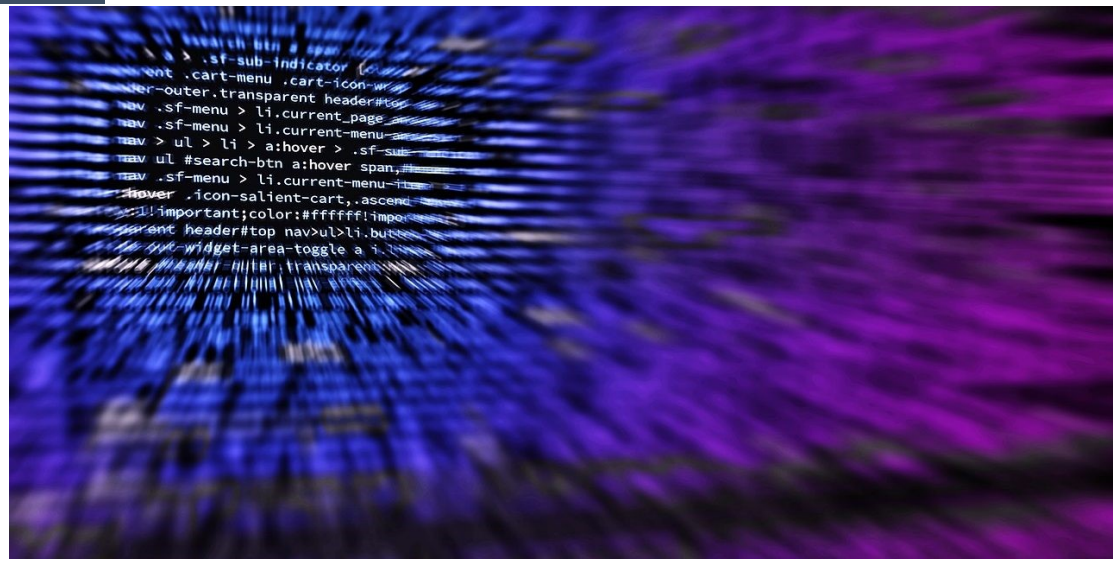


https://haveibeenpwned.com/

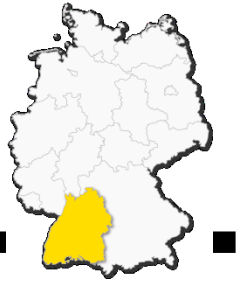


Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Hackerangriffe – Empfehlenswerte Maßnahmen nach erfolgreichen Angriffen



https://www.baden-wuerttemberg.datenschutz.de/category/datenschutz/



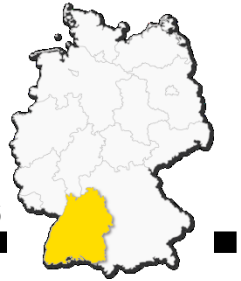
Maßnahme – für vom Datenleak Betroffene

- **Daten prüfen!**
  - hinterlegte E-Mail Kontaktadresse
  - Sicherheitsabfrage
  - berechtigtes Smartphone für M-TAN
  - … siehe auch:

Sicherheit im Postfach wiederherstellen

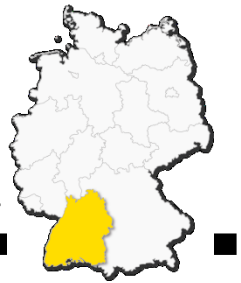
In nur 4 Schritten

https://web.de/email/sicherheit/postfach-schuetzen/#.pc_page.tipps.postfach-hack-erkennen.textlink.sicherheit_postfach-schuetzen



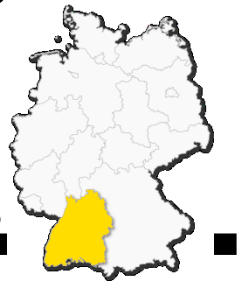
Maßnahme – für vom Datenleak Betroffene

- Ändern einer Mobilfunknummer notwendig?
- Ändern einer Festnetznummer notwendig?
- Neue E-Mail Adressen notwendig?



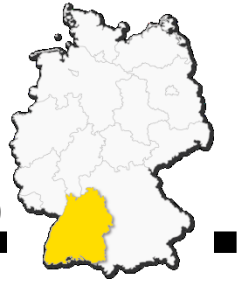
Maßnahme - Passwörter

- Nutzen Sie hinreichend lange und komplexe Passwörter und verwenden Sie diese **jeweils exklusiv**, d.h. für **jedes System** mit schutzbedürftigen Daten nehmen sie **ein anderes Passwort**.
- Dadurch sind auch bei erfolgreichen Angriffen nicht gleich alle Systeme betroffen.
- **Ändern Sie Ihre Passwörter unverzüglich**, wenn Sie den Verdacht haben, dass diese Dritten bekannt sein könnten.



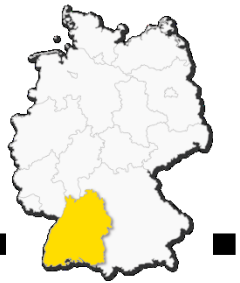
Maßnahme – Option: Passwortmanager benutzen

- Passwortmanager benutzen, der diese Passwörter für Sie verwaltet. Dann brauchen Sie sich **nur noch ein gutes Passwort** für den Passwortmanager zu **merken**.
- Beispiel: **Passwortmanger *KeePass***
  Es handelt sich um ein freies Programm, das Sie sich auch zur privaten Nutzung im Internet herunterladen können. Infos dazu unter:
  https://de.wikipedia.org/wiki/KeePass



Maßnahmen – Online-Zugänge

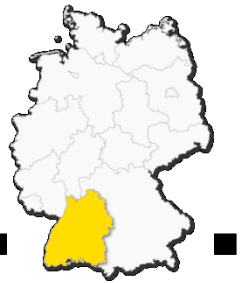
- Für Ihre Online-Zugänge verwenden Sie wenn möglich die **Zwei-Faktor-Authentifizierung**.
- Damit ist ein Missbrauch alleine mit Kenntnis des Passworts nicht mehr möglich.



Maßnahmen - Updates

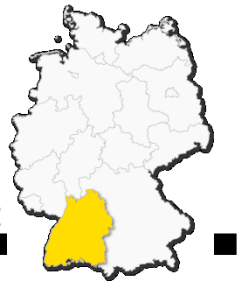
Updates von Software und Betriebssystemen

- Halten Sie Ihre Systeme möglichst zeitnah auf den jeweils aktuellen Softwareständen.
- Damit können Sie nicht mehr über Schwachstellen in veralteten Versionen angegriffen werden.



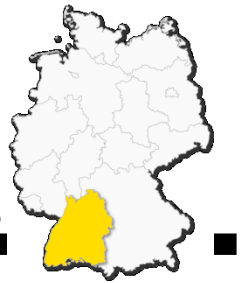
Maßnahmen - Backups

- **Sichern Sie** Ihre wichtigen privaten Daten regelmäßig auf externen Medien!
- **Stecken Sie** danach **das verwendete externe Laufwerk aus**, damit auch eine Verschlüsselungs-Malware nicht mehr darauf zugreifen kann und
- **Sicher Lagern**, möglichst in einem separaten Brandabschnitt.

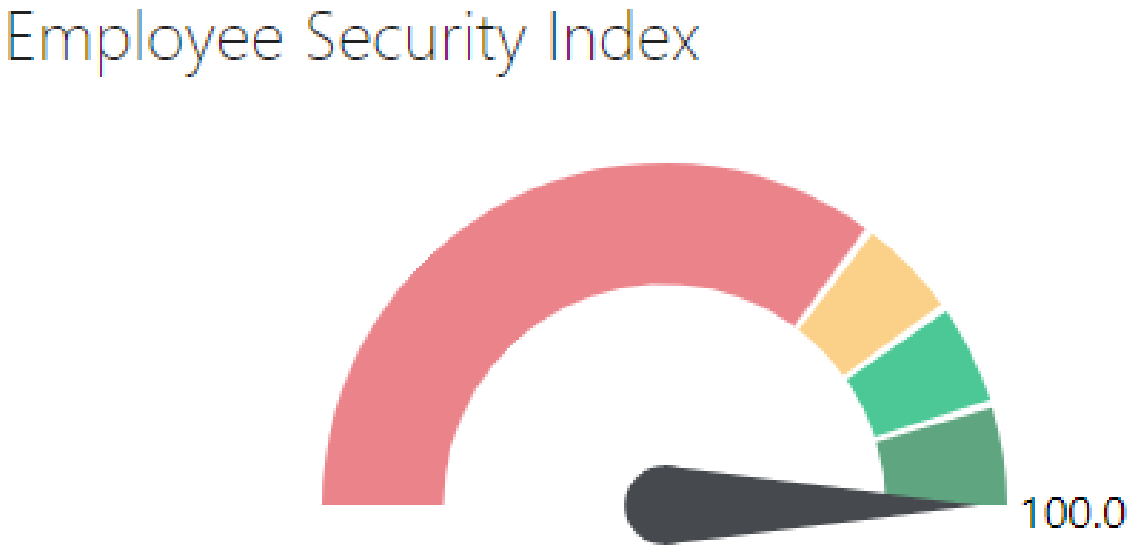


Sensibilisierungsmaßnahmen – Beispiele für ISBs

- E-Mails des ISB: <Informationssicherheit> XYZ
  mit aktuellen Hinweisen
- Vortragsveranstaltungen zur Informationssicherheit
- „Life-Hacking“ Veranstaltungen
- Respektvolle Angriffssimulation Spear-Phishing E-Mails
- Serious Gaming-Ansatz
  Zirkeltraining Informationssicherheit

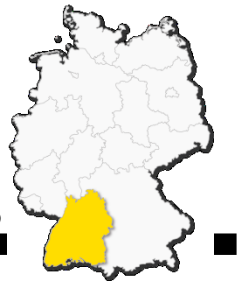


Respektvolle Angriffssimulation



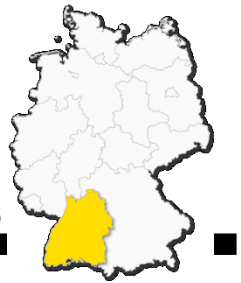
Sicherheit und Komfort ein Wiederspruch?

- *„Sicherheit behindert doch nur den Fortschritt!“*
- **Aber:**
- **Wäre es ohne Daten oder ohne Strom wirklich komfortabler und fortschrittlicher?**



Informieren Sie sich – Vernetzen Sie sich

- **Infos Ihres IT-SiBes**
- https://www.bsi-fuer-buerger.de/
- https://www.baden-wuerttemberg.datenschutz.de/
- https://www.heise.de/security/
- https://netzpolitik.org/
- www.secupedia.de
- Newsletter LKA
- Newsletter LfV
- …



Zentrale Ansprechstelle Cybercrime (ZAC)

Herzlichen Dank für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?