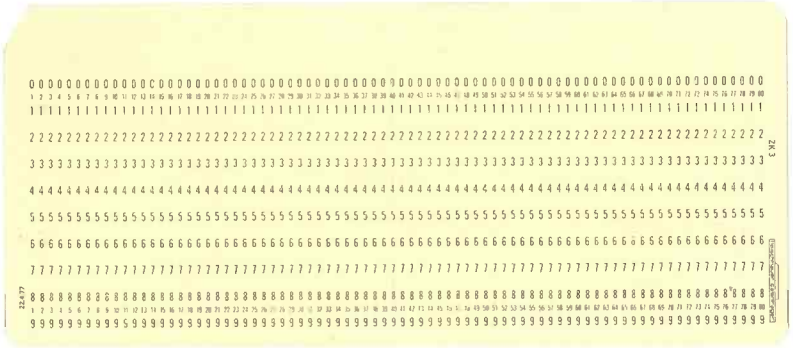
Informationssicherheit Hands-On

Ich bin motiviert, was kann ich zu Hause tun?

Markus Klingspor

Webmontag #63, 27.05.2019

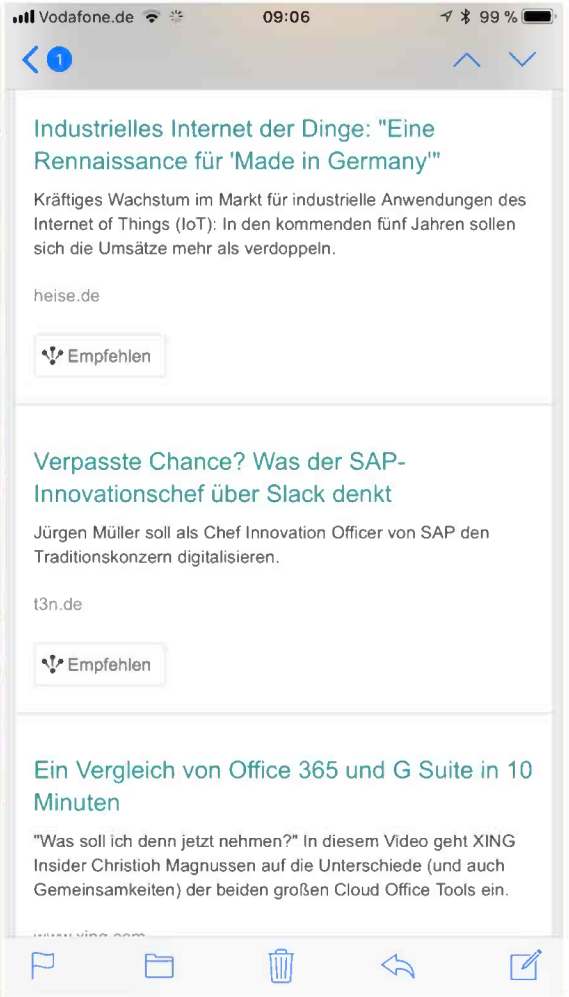


Quelle: https://upload.wikimedia.org/wikipedia/commons/thumb/7/7d/Lochkarte_Fleischhauer.jpg/2880px-Lochkarte_Fleischhauer.jpg
Quelle: https://upload.wikimedia.org/wikipedia/commons/3/33/ZXSpectrum48k.jpg
Quelle: http://techmattmillman.s3.amazonaws.com/wp-content/uploads/2014/04/ST500-01.jpg

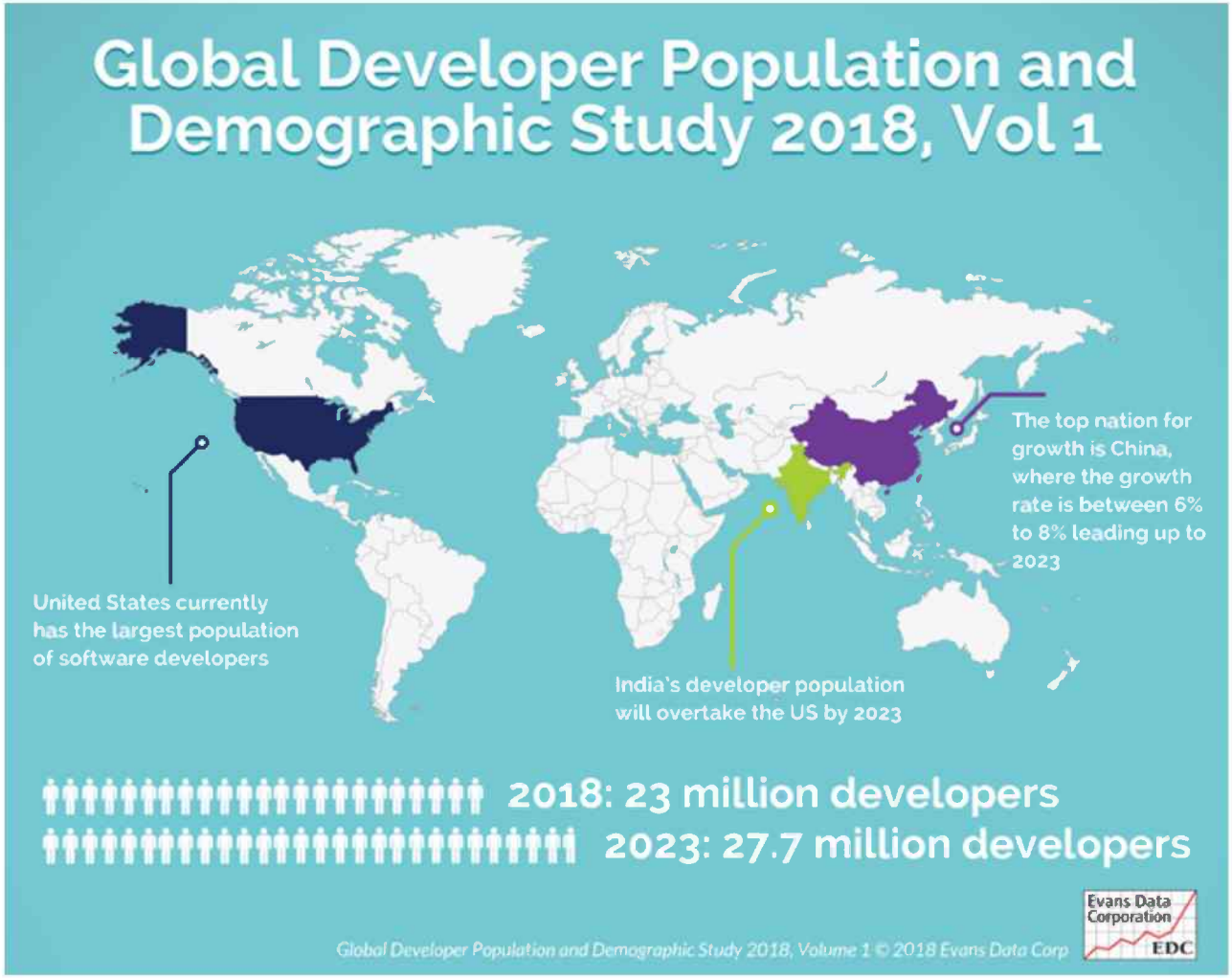
Quelle: https://taosecurity.blogspot.de/2005/08/soccer-goal-security-i-found-this-ad.html

Digitalisierungsstrategie als digitale Agenda

Die Digitalisierung umfasst alle Lebensbereiche. Deshalb widmet sich das Ministerium in seiner Strategie auch der Frage, wie die Digitalisierung zum Nutzen der Menschen gestaltet werden kann.

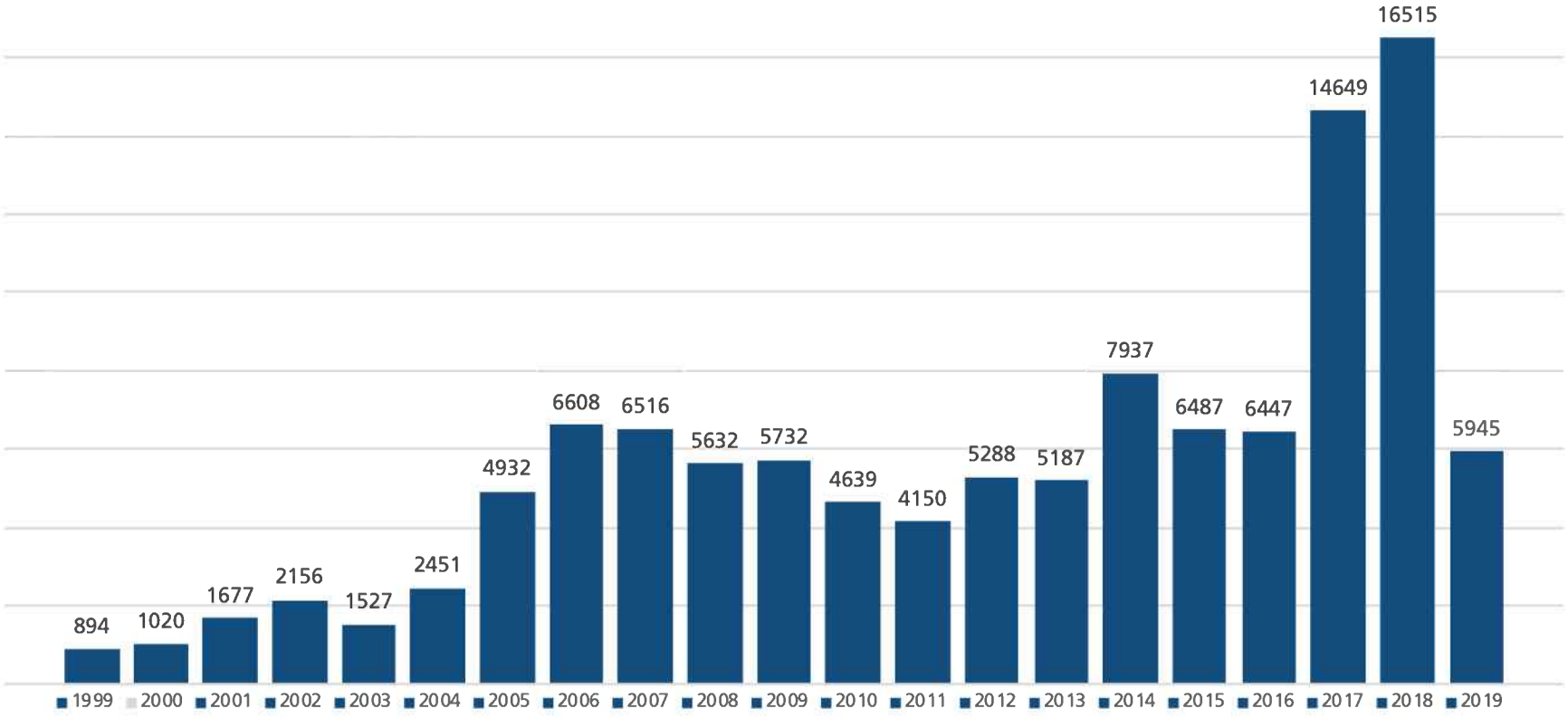


https://im.baden-wuerttemberg.de/de/digitalisierung/digitalisierungsstrategie/

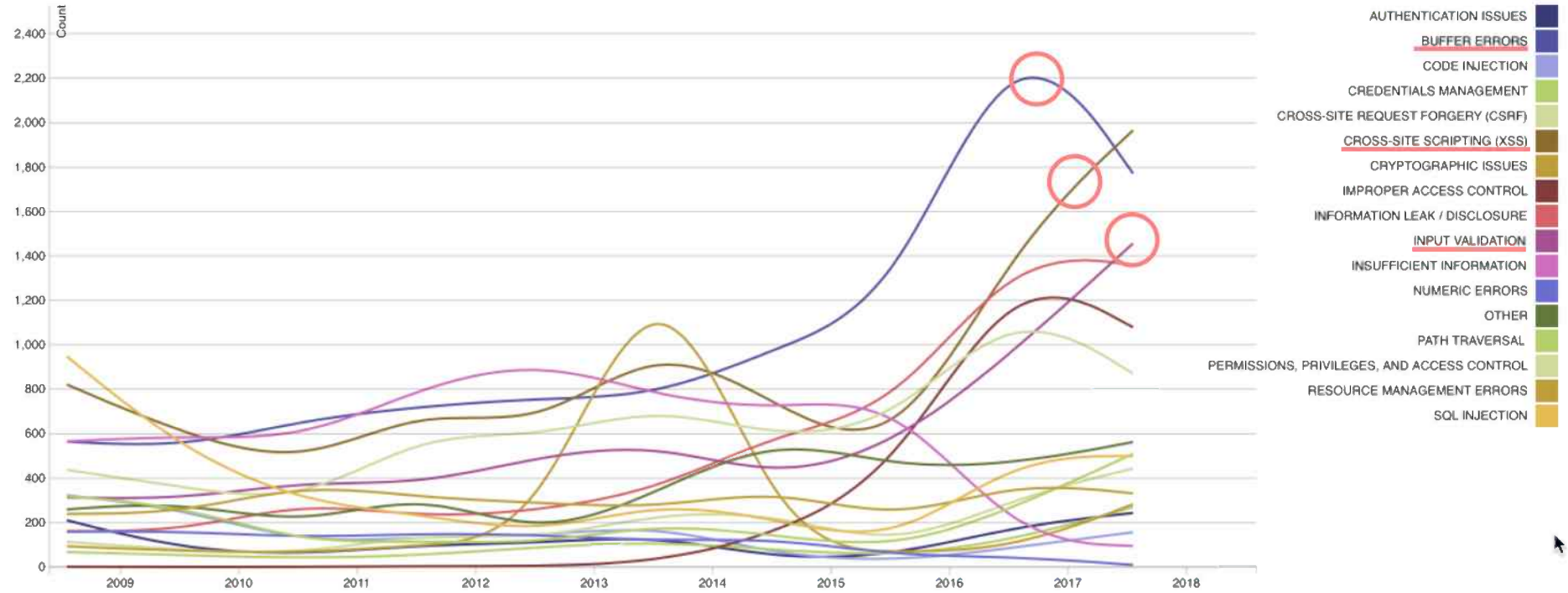


Quelle: https://evansdata.com/press/viewRelease.php?pressID=268

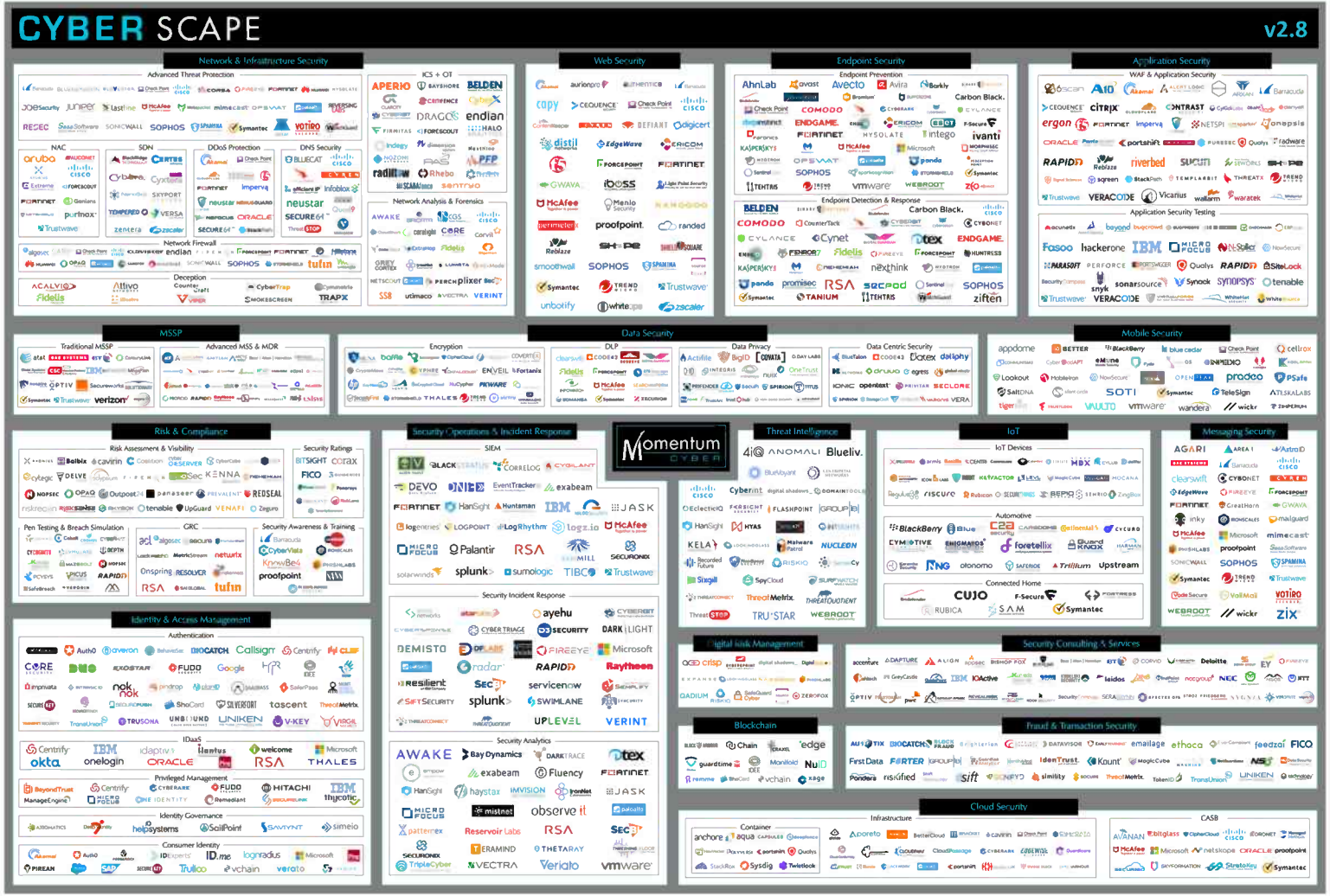
Vulnerabilities By Year



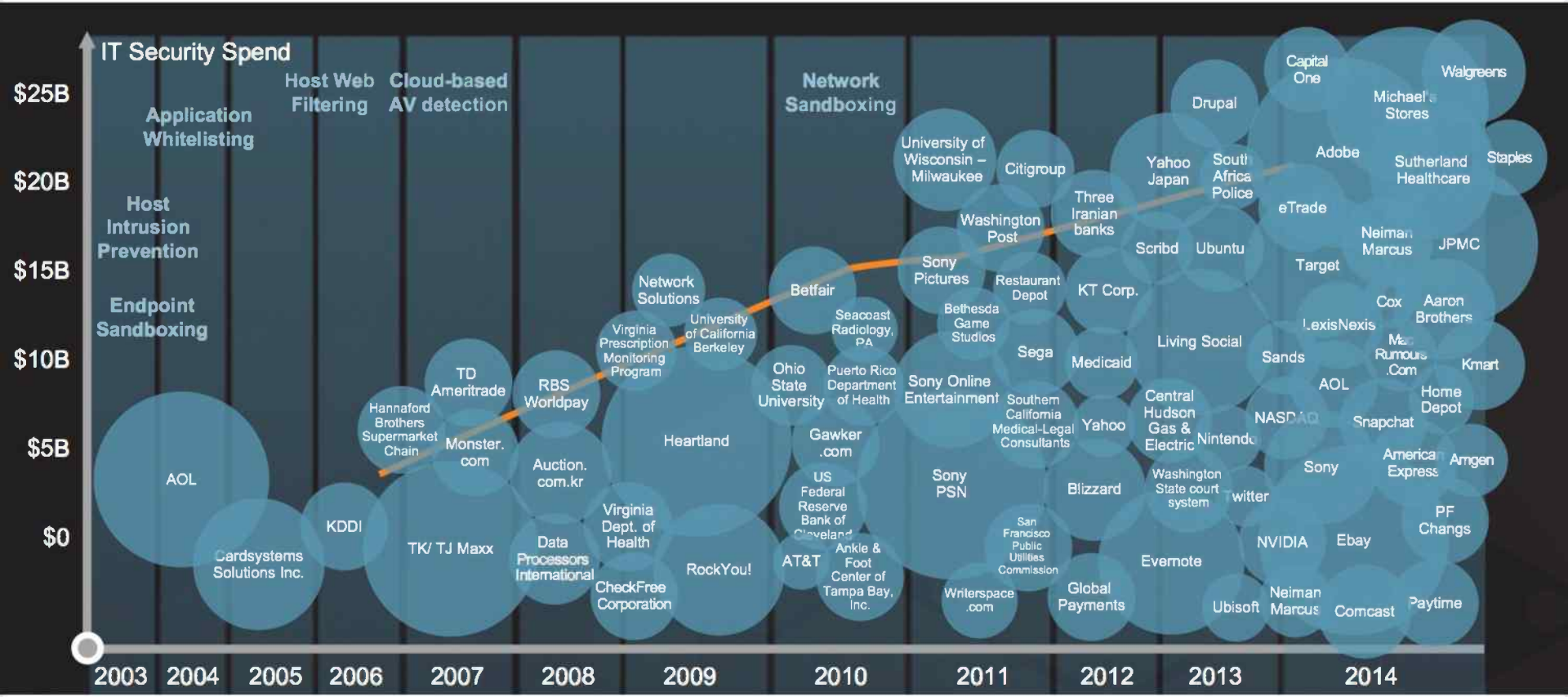
Quelle: https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all



Quelle: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cwe-over-time



Quelle: https://momentumcyber.com/docs/CYBERscape.pdf



Quelle: http://www.infosecurityeurope.com/__novadocuments/85293?v=63

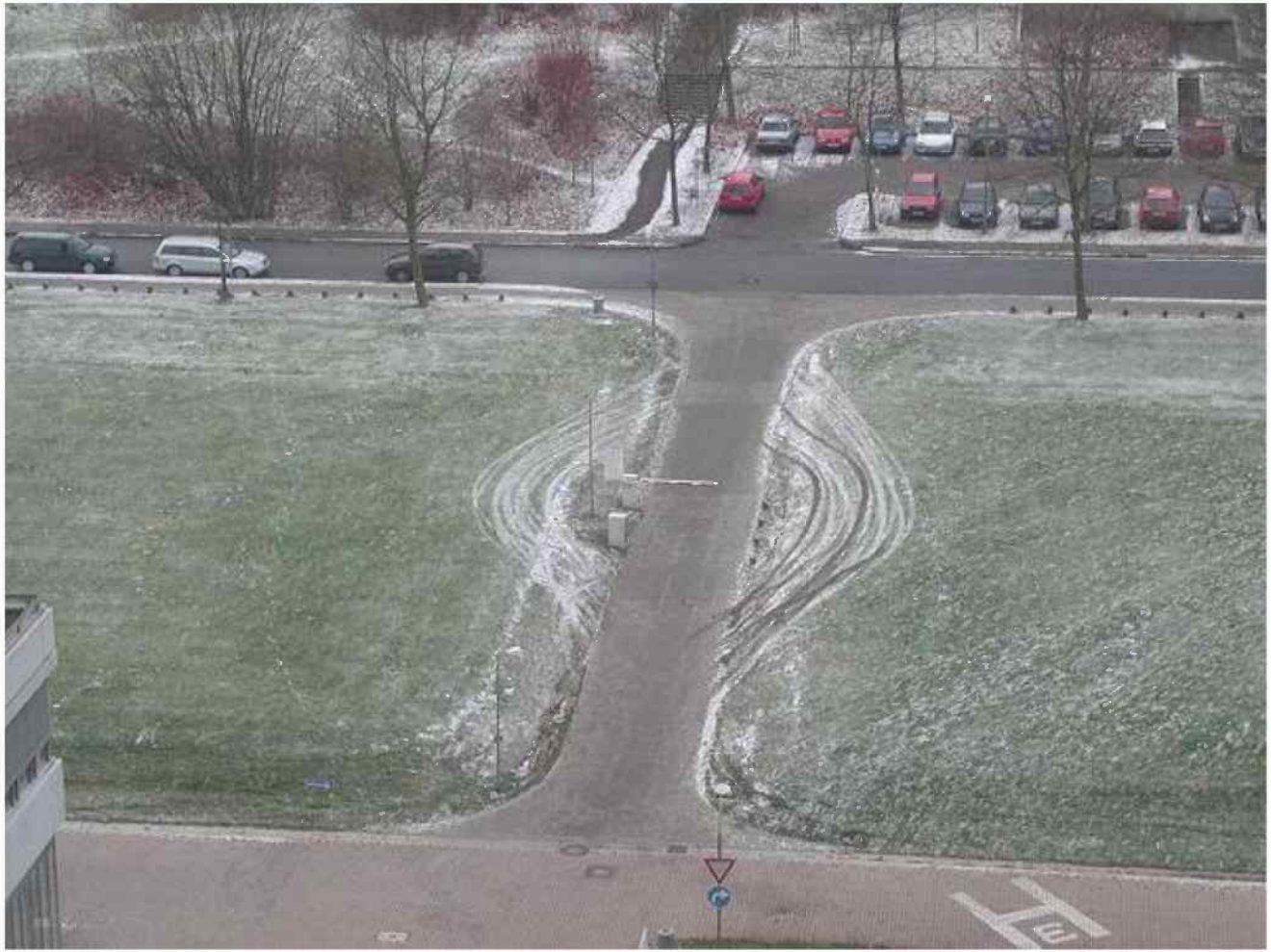
Crypto-Gram
May 15, 2000

Computer Security: Will We Ever Learn?

If we've learned anything from the past couple of years, it's that computer security flaws are inevitable. Systems break, vulnerabilities are reported in the press, and still many people put their faith in the next product, or the next upgrade, or the next patch. "This time it's secure," they say. So far, it hasn't been.

Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. **The trick is to reduce your risk of exposure regardless of the products or patches**.

Quelle: https://www.schneier.com/crypto-gram/archives/2000/0515.html



Quelle: https://www.studycheck.de/media/images/blog/witzige-bilder/parken-uni-bielefeld.jpg
Quelle: https://goo.gl/maps/A5q8hotQm9M2

Cybersecurity 1975

- Economy of mechanism: So einfach wie möglich.
- Fail-safe defaults: Was nicht erlaubt ist, ist verboten.
- Complete mediation: Jeder Zugriff wird auf Berechtigung überprüft.
- Open design: Keine Security by Obscurity.
- Separation of privilege: Vier-Augen- / Zwei-Schlüssel-Prinzip.
- Least privilege: Nur was unbedingt benötigt wird, ist erlaubt.
- Least common mechanism: Möglichst wenig gemeinsame Nutzung.
- Psychological acceptability: Die Benutzung muss einfach sein. Keine Überraschungen.
- Work factor: Der Angriff muss teurer sein als der Nutzen für den Angreifer.
- Compromise recording: Angriffe müssen aufgezeichnet werden.

Quelle: https://en.wikipedia.org/wiki/Saltzer_and_Schroeder%27s_design_principles

Economy Of Mechanism

Keep the design as simple and small as possible. *This well-known principle applies to any aspect of a system, but it deserves emphasis for protection mechanisms for this reason: design and implementation errors that result in unwanted access paths will not be noticed during normal use (since normal use usually does not include attempts to exercise improper access paths). As a result, techniques such as line-by-line inspection of software and physical examination of hardware that implements protection mechanisms are necessary. For such techniques to be successful, a small and simple design is essential.*

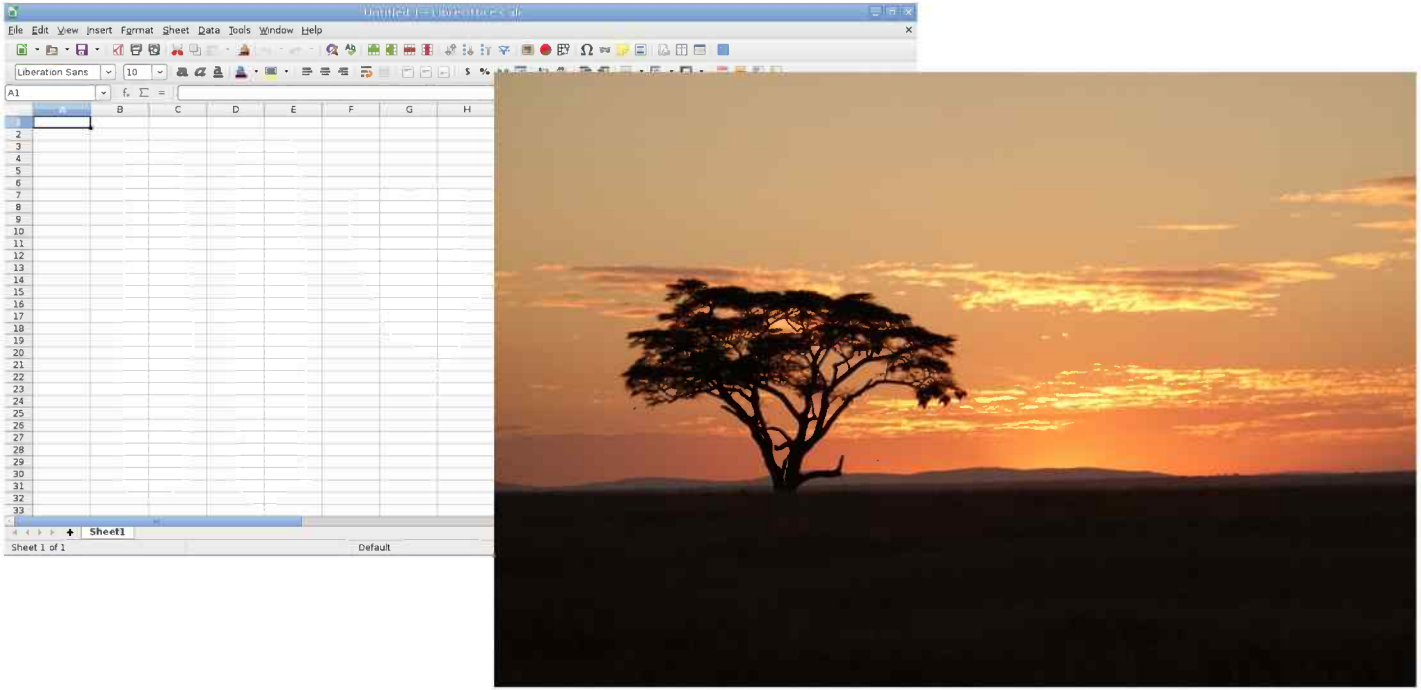
Quelle: https://adam.shostack.org/blog/the-security-principles-of-saltzer-and-schroeder/

Complete Mediation

Complete Mediation *Every access to every object must be checked for authority. This principle, when systematically applied, is the primary underpinning of the protection system. It forces a system-wide view of access control, which in addition to normal operation includes initialization, recovery, shutdown, and maintenance. It implies that a foolproof method of identifying the source of every request must be devised. It also requires that proposals to gain performance by remembering the result of an authority check be examined skeptically. If a change in authority occurs, such remembered results must be systematically updated.*

Quelle: https://adam.shostack.org/blog/the-security-principles-of-saltzer-and-schroeder/

Risiko Datenverlust



Quelle: https://upload.wikimedia.org/wikipedia/commons/3/35/LibreOffice_5.1_Calc_%28Tango%29.png

Quelle: http://www.sv-hjotto.de/media/images/brand-it-raum-2.jpg

https://upload.wikimedia.org/wikipedia/en/1/18/Wana_Decrypt0r_screenshot.png

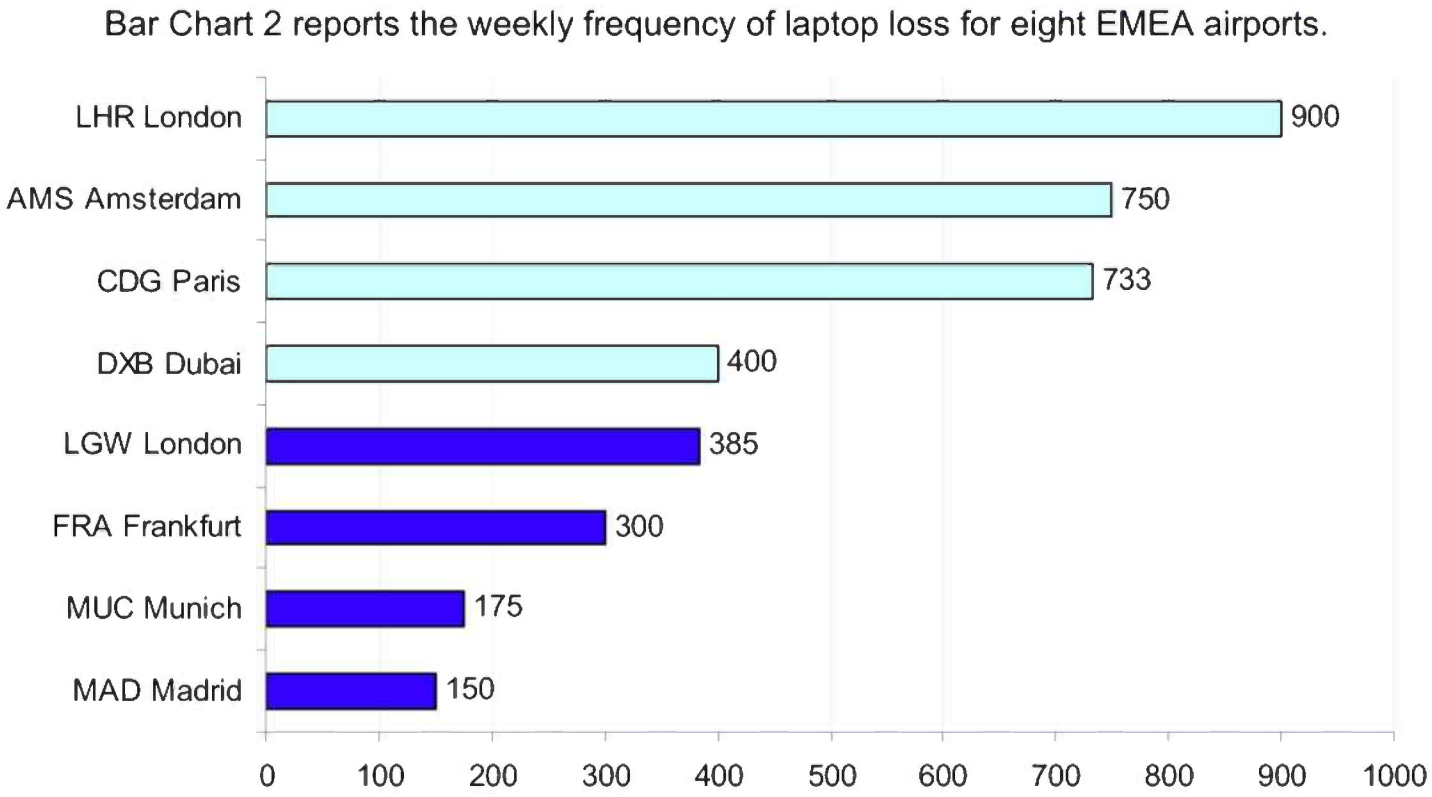
Daten, die nicht mindestens dreimal gesichert sind, sind gar nicht gesichert!

- Backupstrategie planen.
- Backup regelmäßig durchführen.
- Backups verschlüsseln.
- Backup testen!!!
- Malware kann auch Backups zerstören.

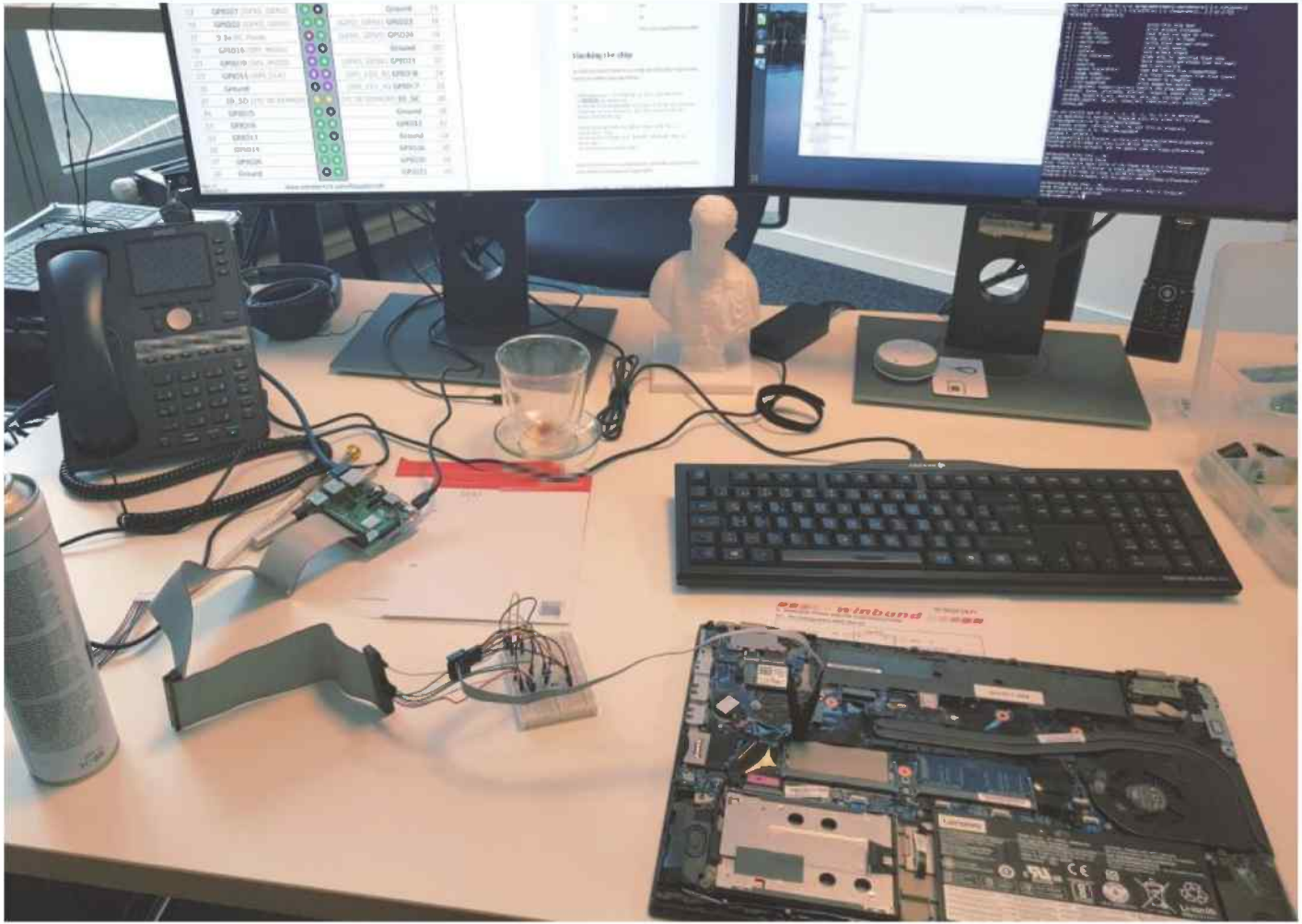
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Datensicherung/datensicherung_node.html
https://www.heise.de/select/ct/2018/20/1537842151930716

Risiko Geräteverlust

> 3000 verlorene Laptops / Woche



Quelle: https://www.ponemon.org/local/upload/file/LostLaptopsDell%20EMEA%20Final%208.pdf



Quelle: https://aramido.de/blog/datensicherheit/cold-boot-angriff-festplattenverschlusselung-ade

Schutz vor „Hardware Verlust“

- Festplatten verschlüsseln (auch externe)
- Firmware-Passwort setzen

- Secure Boot konfigurieren
- Booten von externe Medien verbieten
- Unbeaufsichtigten Rechner abschalten

- Backups verschlüsseln!!!

https://www.cpsd.at/bitlocker-massnahmenkatalog-2018/
https://www.heise.de/select/ct/2018/15/1532047372835191

Eine einfache Frage

„Linda ist 31 Jahre alt, Single, freimütig und sehr intelligent. Sie hat Philosophie im Hauptfach studiert. Als Studentin interessierte sie sich sehr für Themen wie Diskriminierung und soziale Gerechtigkeit, und sie nahm auch an Anti-Atomkraft-Protesten teil."

Was ist wahrscheinlicher?

„Linda ist 31 Jahre alt, Single, freimütig und sehr intelligent. Sie hat Philosophie im Hauptfach studiert. Als Studentin interessierte sie sich sehr für Themen wie Diskriminierung und soziale Gerechtigkeit, und sie nahm auch an Anti-Atomkraft-Protesten teil."

a) „Linda ist Bankkassiererin."
b) „Linda ist Bankkassiererin und in der feministischen Bewegung aktiv."

https://www.schneier.com/blog/archives/2007/02/the_psychology_2.html
https://de.wikipedia.org/wiki/Schnelles_Denken,_langsames_Denken
ka-it-si_160421_ist-der-dau-wirklich-dumm.pdf

Beispiele für Social Engineering

Mit Warnweste kommst du überall umsonst rein

DAVID ALLEGRETTI

Eine Warnweste ist dein Schlüssel zur Welt. Zoo, Kino, Coldplay? Alles ist möglich. Das zeigt auch ziemliche Sicherheitslücken auf.

Phishing-Test bei der Berliner Polizei

heise Security 01.12.2015 11:32 Uhr – Dennis Schirrmacher

Die Berliner Polizei will das Sicherheitsbewusstsein ihrer Mitarbeiter sensibilisieren. Dafür hat sie gefälschte E-Mails in Umlauf gebracht, um Log-in-Daten der Beamten abzugreifen.
252 Polizeibeamte sind auf einen Phishing-Test der Berliner Polizei hereingefallen und haben eine gefälschte E-Mail mit einem Link geöffnet. 35 Beamte haben die Anweisungen befolgt und verschiedene Nutzerdaten hinterlegt, berichtet der Tagesspiegel.

Fan mogelt sich mit Wikipedia-Eintrag in Backstage-Bereich

heise online 03.12.2015 10:33 Uhr – Axel Kannenberg

CEO-FRAUD

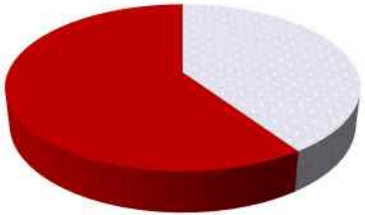
Autozulieferer Leoni um 40 Millionen Euro betrogen

http://www.heise.de/newsticker/meldung/Fan-mogelt-sich-mit-Wikipedia-Eintrag-in-Backstage-Bereich-3030041.html
http://www.heise.de/newsticker/meldung/Phishing-Test-bei-der-Berliner-Polizei-3028064.html
https://www.vice.com/de/article/mit-warnweste-kommst-du-uberall-umsonst-rein?utm_source=vicefbdeads&utm_medium=link&utm_campaign=internal
https://www.golem.de/news/ceo-fraud-autozulieferer-leoni-um-40-millionen-euro-betrogen-1608-122741.html

Achtung Warnhinweis

Bitte schalten Sie jetzt WLAN bei ihrem Smartphone aus, wenn Sie nicht gehackt werden wollen!

SPAM Mails + Malware



- 12 Mrd. "gute" Mails

- SPAM: unerwünschte Post

- Werbung



- Phishing / Malware

11.06.2015: T-Online: http://www.t-online.de/computer/sicherheit/id_65864362/falsche-dhl-paketankuendigung-enthaelt-trojaner.html
06.10.2014: Die Welt: http://www.welt.de/finanzen/verbraucher/article132960353/Wer-nicht-zahlt-wird-mit-dem-Tod-bedroht.html
06.03.2015: Spiegel Online: http://www.spiegel.de/netzwelt/web/dhl-warnt-vor-spam-mails-mit-infizierter-zip-datei-a-1022213.html

Arbeiten Sie auch noch als Admin?

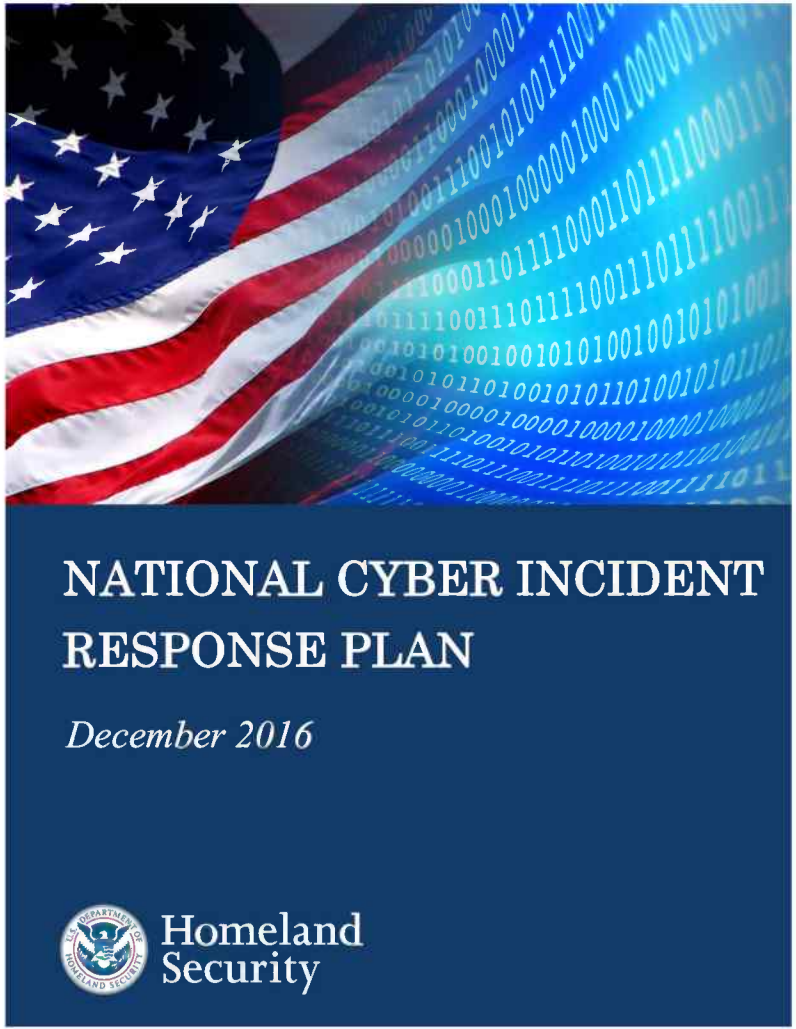
Quelle: https://[illegible]files.wordpress.com/2015/0[illegible]/img_3969.jpg

Maßnahmen

- Regelmäßige Software Updates.
- Keine Adminrechte als Benutzer.
- Augen auf beim Email-Empfang.
- Browser Adressleiste prüfen.
- SSL und Zertifikate prüfen.
- Virenscanner benutzen.
- Keine fremden USB-Sticks benutzen.
- Gehen Sie vorsichtig mit Ihren Daten um.
- Nicht ist kostenlos!

Quelle: https://upload.wikimedia.org/wikipedia/commons/6/61/Fallschirm_-_panoramio.jpg

https://media.licdn.com/mpr/mpr/p/2/005/095/08e/221325e.jpg



https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Identitäten und Passworte

Wie viele Accounts haben Sie?

STUTTGARTER-ZEITUNG.DE

Chaos Computer Club zu Politikern im Internet

„Selbst Schüler wissen mehr über Netzsicherheit“

Frankfurter Allgemeine

Inland

Schutz von Politikern ist nicht auf der Höhe der Zeit

STUTTGARTER-ZEITUNG.DE

Datensicherheit nach Hacker-Angriff

Vergibt Gmx inaktive Email-Adressen neu?

FOCUS ONLINE

"Maybrit Illner"

Zwei-Faktor-Authentifizierung: Im TV schockiert Ministerin mit Aussage über Kollegen

Quelle: http://www.dumfriesandgalwatch.co.uk/attachments/Image/SBRC_Password_poster.PNG

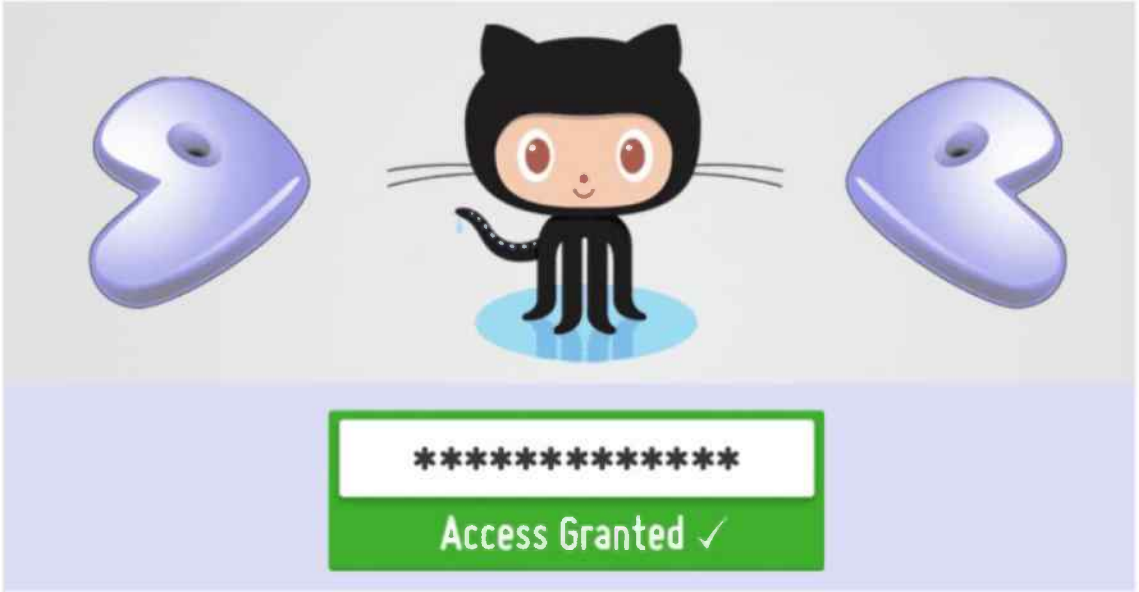
WcKGq]aLNg8GzPP*jpUht7QY

Ich werde mein Amazon Passwort nie vergessen!

Merkhilfe: I_w_m_A_P_n_v!

Password-Guessing Was Used to Hack Gentoo Linux Github Account

July 04, 2018 Swati Khandelwal



Maintainers of the Gentoo Linux distribution have now revealed the impact and "root cause" of the attack that saw unknown hackers taking control of its GitHub account last week and modifying the content of its repositories and pages.

https://thehackernews.com/2018/07/github-hacking-gentoo-linux.html
https://wiki.gentoo.org/wiki/Project:Infrastructure/Incident_Reports/2018-06-28_Github

KeePass Tutorial – Passwörter sicher verwalten

Am besten sollte man lange und komplexe Passwörter verwenden und dazu noch bei jeder Webseite und bei jedem Konto ein anderes. Aber wer soll sich die alle merken? Richtig, KeePass. In diesem Blogbeitrag erkläre ich mit Hilfe von Videos die Installation von KeePass und verschiedenen Plugins, die dabei helfen Passwörter sicher zu verwalten.

weiterlesen

Passwort-Management-Systeme – Warum Sie nicht darauf verzichten sollten

Wäre ich ein Hacker, würde ich versuchen irgendwie an die Identitäten eines Unternehmens zu kommen und dort Admin-Rechte zu erlangen. Beispielsweise über Bruteforce-Attacken lassen sich Identitäten automatisiert knacken und somit auch Zugang zu administrativen Accounts erhalten.

weiterlesen

Warum Passwörter Mist sind – Tipps zu sicheren Passwörtern

Passwörter sind großer Mist! Der jüngst veröffentlichte Mega-Hack bei Yahoo, in dem über 500 Mio. Zugangsdaten gestohlen wurden, zeigt mal wieder, dass Passwörter ein schlechter Weg sind, um Zugänge abzusichern. Leider gibt es für die meisten Online-Dienste keine brauchbaren Alternativen. Grund genug die Hintergründe und Zusammenhänge zu beleuchten. Wann ist ein Passwort gut?

weiterlesen

https://blog.to.com/?s=keepass

YouTube

KeePass Tutorial Nr. 1: KeePass Installation

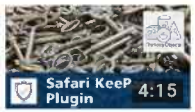
Thinking Objects GmbH

KeePass Tutorial Nr. 2: Kee für Firefox - Installation & Nutzung

Thinking Objects GmbH

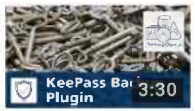
KeePass Tutorial Nr. 3: ChromeIPass für Chrome - Installation & Nutzung

Thinking Objects GmbH



KeePass Tutorial Nr. 4: Passafari für Safari - Installation & Nutzung

Thinking Objects GmbH



KeePass Tutorial Nr. 5: KeeAnywhere zur Cloud-Synchronisation

Thinking Objects GmbH

https://www.youtube.com/watch?v=gD8x2vHDS8k&list=PL8urNLbry_yO-wI3MStwRd8giQHy5FDya

WcKGq]aLNg8GzPP*jpUht7QY

Ich werde mein Passwort-Manager Passwort nie vergessen!

Merkhilfe: I_w_m_P-M_P_n_v!

Zweiter Faktor

https://www.wired.com/story/yubikey-series-5-fido2-passwordless/
https://www.yubico.com
https://www.ftsafe.com
https://en.wikipedia.org/wiki/Google_Authenticator
https://support.apple.com/en-us/HT204915
https://support.microsoft.com/de-de/help/12408/microsoft-account-how-to-use-two-step-verification
https://www.google.com/landing/2step/

Ach 0rbit... 😂 Bis heute auf der Suche nach Aufmerksamkeit, haha.

Donnerstag, 20:49

Naja wieso nicht, viele kleinere Youtuber (z.B News-Youtuber) suchen doch auch die Aufmerksamkeit :-)

Donnerstag, 21:48 ✓

Haha, kinda funny. Wie biste an Simons Zeugs gekommen?

Donnerstag, 21:49

Naja eig. hat Gmail eine Lücke und 2 Faktor kann man umgehen (Darauf gehe ich aber nicht näher ein) hab eig. auch gar nichts gegen Simon, aber er hat halt die perfekte Reichweite und darauf kann man gut Sachen loswerden, es wird auch nichts geleakt von Simon. Du hast ja die Nummer von ihm, vl will er ja mal reden, z.B über die Links.

Donnerstag, 21:55 ✓

Nachricht schreiben

Unge ✓
@unge

Follow

Danke Leute, habe den Twitter Account zurück!
Scheinbar wurde der #Hackerangriff durch eine Sicherheitslücke von Gmail verschuldet bei der man die 2-Faktor-Authentifizierung umgehen kann.
@solmecke & weitere News-Portale haben darüber berichtet, es sind einige Personen betroffen!

Unge ✓
@unge

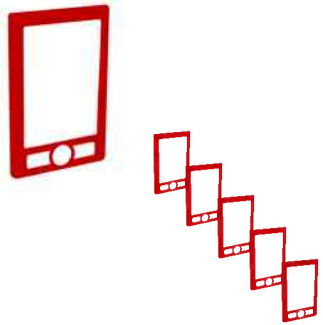
Follow

Mein Twitter Konto hatte 2FA aktiv allerdings nicht das Gmail Konto mit dem Twitter verknüpft war, über dieses Konto hatte der Hacker mit Twitter Email Kontakt und hat so Mitarbeiter davon überzeugt 2FA von meinem Twitter Account zu deaktivieren.
2/3

Zugriff auf Account

Verbundene Apps

Verbundene Geräte



Passwort

2. Faktor
Disconnected / OTP

Connected

Passwort zurücksetzen

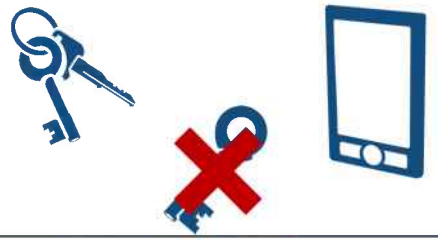
Verbundene E-Mail

- Frage 1
- Frage 2
- Frage 3

Pass ort

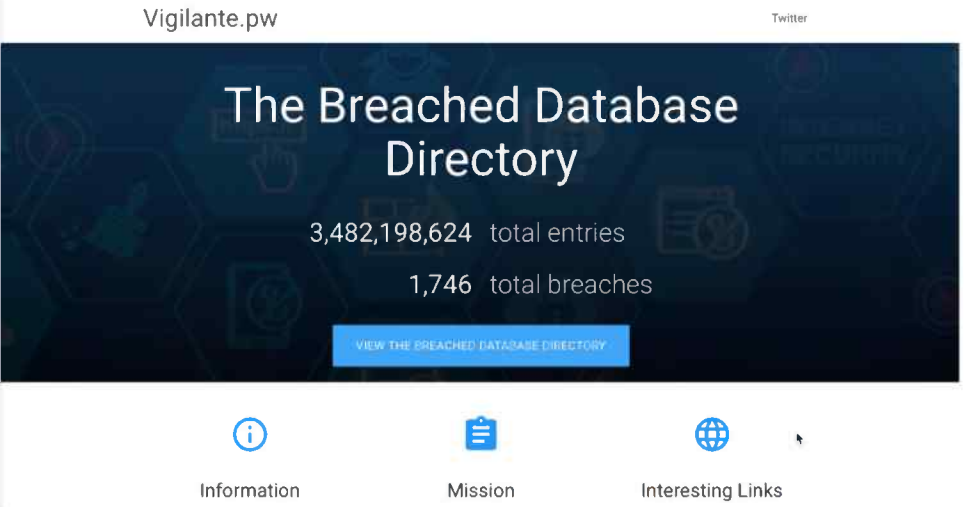
2. Faktor
Disconnected / OTP

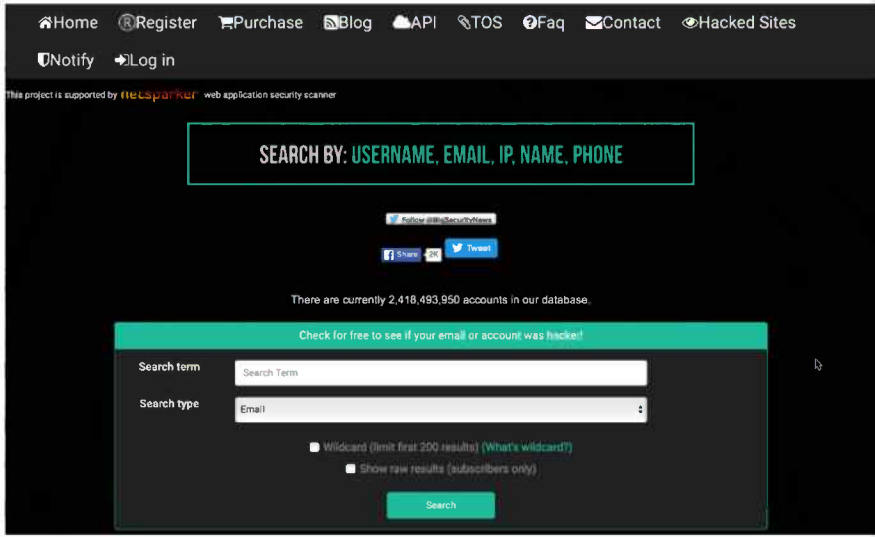
Connected

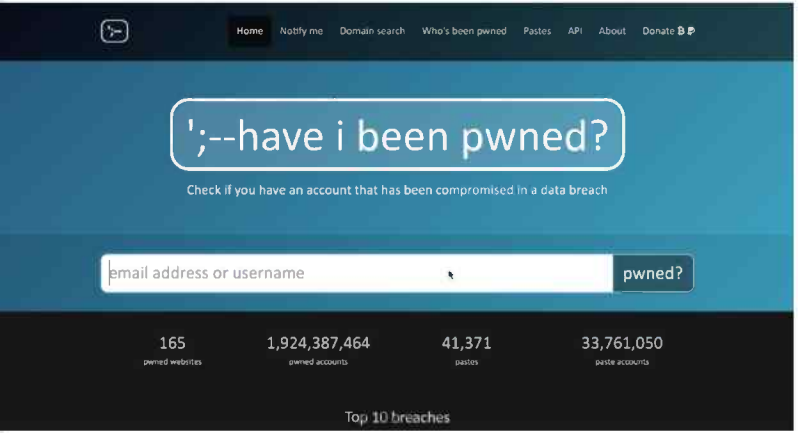


Maßnahmen

- Zweiten Faktor benutzen
- Passwort Manager verwenden
- Passwortlänge mindestens 12 Zeichen
- Passwortlänge am besten >> 16 Zeichen
- Nie mehrfach verwenden
- Von Accounts abmelden
- Keine Passworte per Email
- Verbundene Accounts überprüfen
- Passwort Leaks prüfen
- Sicherheitsfragen nie wahr beantworten







https://www.vigilante.pw/
https://www.leakedsource.com/
https://haveibeenpwned.com/
https://sec.hpi.de/ilc/

Weitere Maßnahmen

- Emailverschlüsselung nutzen.
- Messenger Verschlüsselung nutzen.
- WLAN absichern.
- Smart Home Netz separieren.
- Vor dem „Entsorgen“ Daten löschen.
- ...

Linksammlung

- BSI für Bürger Empfehlungen: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html
- BSI Bürger CERT: https://www.buerger-cert.de/ (Newsletter mit aktuellen Warnmeldungen, signiert)
- Heise Checklisten: https://www.heise.de/ct/artikel/Security-Checklisten-gratis-zum-Download-4163181.html
- Dateien auf Viren prüfen: https://www.virustotal.com/ (keine vertraulichen Daten)
- Beratungstellen der Polizei: https://www.polizei-beratung.de/opferinformationen/cybercrime/
- Tipps der Polizei: https://www.polizei-praevention.de/themen-und-tipps/basisschutz-hard-software.html

Thinking Objects

TOsecurity

Cyber Security von Anfang an

25 Jahre

Markus Klingspor

Tel. +49 711 88770-120
markus.klingspor@to.com

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal / Stuttgart

Tel. +49 711 88770400
www.to.com
blog.to.com