IT-Sicherheit ist Chefsache!

IT-Sicherheit und das damit verbundene Unternehmensrisiko richtig einschätzen

HDH e.V. Webinar, 02. März 2021

Darf ich mich vorstellen?

Jan-Tilo Kirchhoff

- Country Manager Compass Security Deutschland GmbH
- verheiratet, zwei Kinder
- Werdegang: Von der TK-Security zur IT-Security
- Kompetenzen
  - Netzwerk Sicherheitsprüfungen
  - ICT- Security (VoIP, PSTN, GSM …)
  - IT-Forensik

CISSP® Certified Information Systems Security Professional

OFFENSIVE security (OSCP)®

Hobbys

- Meine Familie
- Musik (Trompete und Chor)
- Electronic Jazz, Jazz Funk
- Laufsport
- ICT-Security

Compass Crew

Was macht Compass?

seit 1999

Penetration Tests

Als Angreifer untersuchen wir Geräte, Netze, Dienste und Anwendungen auf Schwachstellen. Mittels Social Engineering und Red Teaming testen wir das Verhalten der gesamten Organisation.

Digital Forensics

Unsere Forensik-Experten helfen bei der Koordination von Vorfällen und Sofortmassnahmen sowie bei der gerichtsfesten Bearbeitung von Daten. Zudem bieten wir eine unkomplizierte und schnelle Ursachenforschung.

Security Reviews

Erfahrene IT Analysten unterstützen Sie mit Zweitmeinungen zu Security-Konzepten und prüfen nach Wunsch den Aufbau, die Konfiguration und den Quellcode Ihrer Lösung.

Security Trainings

Profitieren auch Sie vom Wissen unserer Analysten zu Penetration Testing, Netzwerkanalyse, sichere Apps und Anwendungen, Digitale Forensik und trainieren Sie in einem eigens dafür erstellten Labor.

Wir sind “nette” Hacker

Bild von Free-Photos auf Pixabay

Aktuelle Meldungen

Informationssicherheit – Um was geht es eigentlich?

C

- Confidentiality

I

- Integrity

A

- Availability

A

- Accountability

Vertraulichkeit

- Daten dürfen nur dem zur Verfügung stehen, der sie benötigt und berechtigt ist sie zu erhalten

Integrität

- Daten müssen unverfälscht gelagert und bereitgestellt werden

Verfügbarkeit

- Daten müssen verfügbar sein, wenn sie benötigt werden

Verbindlichkeit

- Zugriffe/Änderungen müssen eindeutig zugeordnet werden können (Nachweisbarkeit)

Gefährdungspotentiale



Höhere Gewalt

- Feuer, Wasser, Blitzschlag, Krankheit, ...

Organisatorische Mängel

- Fehlende oder unklare Regelungen, fehlende Konzepte, ...

Menschliche Fehlhandlungen

- "Die größte Sicherheitslücke sitzt oft vor der Tastatur„
- Fehlerhafte Einschätzung von Risiken

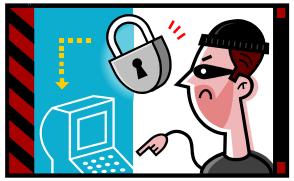
Technisches Versagen

- Systemabsturz, Plattencrash, ...

Vorsätzliche Handlungen

- Hacker, Viren, Trojaner, ...





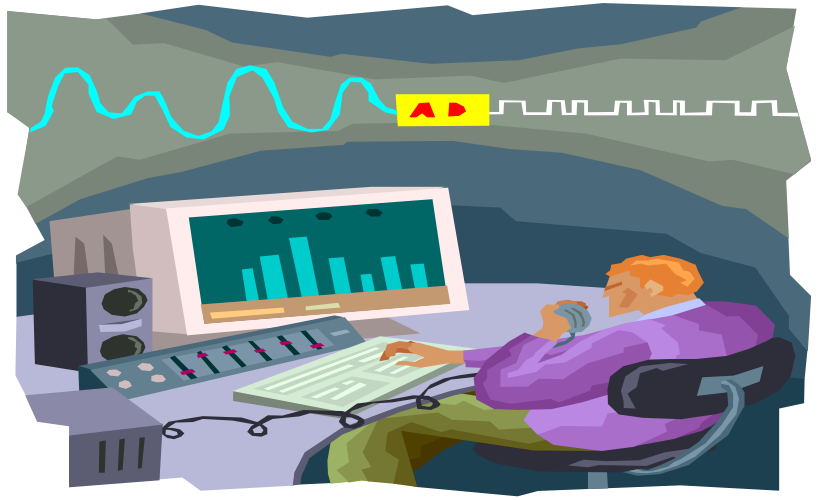
Verantwortlichkeiten

IT Compliance

- Einhaltung sämtlicher für ein Unternehmen relevanter gesetztlicher Pflichten, Vorschriften und Regeln

IT Governance

- Steuerungs- und Regelungssysteme innerhalb des Unternehmens



Compliance

Gesetzlicher Rahmen

- Allgemeines Recht
  - Grundgesetz
  - BGB
  - StGB
- Datenschutz
  - BDSG
  - LDSG
- Unternehmensrecht
  - KonTraG
  - Aktiengesetz/GmbH Gesetz
  - Handelsgesetzbuch
- Telekommunikation
  - TKG
  - TKÜV
- IT Sicherheitsgesetz
- Urheberrecht

Verträge

- Kreditkartengeschäft
  - PCI Compliance
- Servicel Level Agreements
- AGBs

Sicherheitstrategien

BSI Grundschutz

- Leitfaden IT-Sicherheit

ISO/IEC 27000

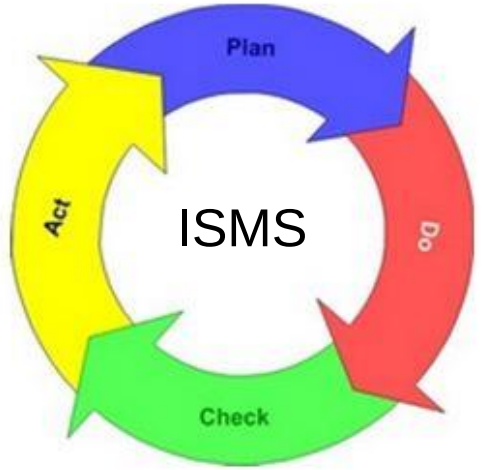
- Informationsicherheits Management System (ISO 27001 - ISMS)
- Risikomanagement (ISO 27005)
  - planmäßige Vorgehensweise zur Entdeckung, Analyse und Bewertung von Risikofaktoren

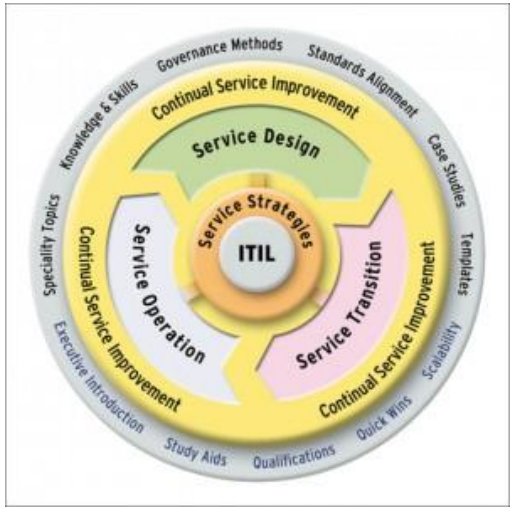
VdS 10000

- ISO 27000 light für KMU

ITIL

- Planung, Erbringung und Unterstützung von IT Serviceleistungen.





Wo fängt man an?

Andere erkennen ist weise. Sich selbst erkennen ist Erleuchtung.
- Laotse

https://commons.wikimedia.org/wiki/File:ThaySangLawCin.jpg

Wo fange ich an?

Mein Unternehmen

- Was ist der Kern meines Unternehmens?
- Welche Prozesse müssen laufen damit ich Geld verdiene?
  - Welche IT Systeme sind dafür notwendig?
  - Geht es auch ohne?
- Wo liegen die Kronjuwelen?
  - Betriebsgeheimnisse
  - Finanzdaten
    - Zugangsdaten zu Bankkonten etc.

Meine Geschäftspartner

- Kunden
  - Datenschutz
  - Vertragserfüllung
- Lieferanten
  - Auftragsvergabe
  - Zahlungen
- Mitarbeiter
  - Datenschutz
- Investoren

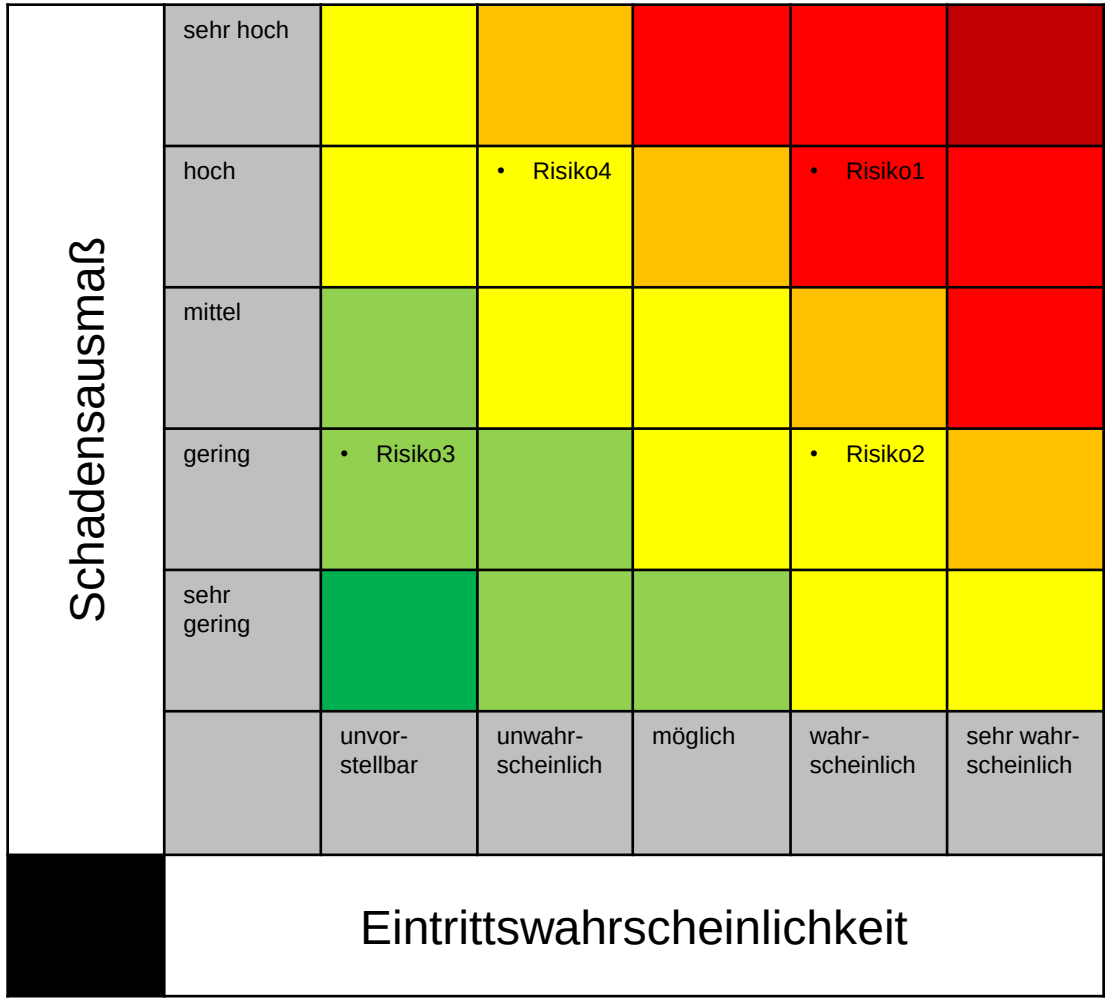
https://commons.wikimedia.org/wiki/File:Preussische-Kroninsignien.JPG

Threat Modelling

https://www.microsoft.com/en-us/download/details.aspx?id=20303

Risiko

Risikomatrix



Wie rechnet man?

Eintrittswahrscheinlichkeit x Schadensausmaß

oder (Schwachstelle x Bedrohung x Konsequenz)

Eintrittswahrscheinlickeit

- Erfahrungswerte
- Zeitlicher Aufwand für einen Angreifer
- Technisches Know-How des Angreifers

Schadensausmaß

- Technisch
- Finanziell
  - Direkter Schaden
  - Indirekter Schaden
    - Reputation

Wer sind die Angreifer?

Wie gehen sie vor und welche Ziele verfolgen sie?

https://upload.wikimedia.org/wikipedia/commons/c/c4/Backlit_keyboard.jpg

Lagebilder des BSI und des BKA

Cyber-Sicherheitslage für Deutschland 2020

Aktion und Reaktion

117,4 MIO. neue Schadprogramm-Varianten

2019: 114 MIO.

durchschnittlich **322.000** neue Schadprogramm-Varianten pro Tag

in Spitzenwerten **470.000**

76 % ist der Anteil unerwünschter SPAM-MAILS an allen in den Netzen des Bundes eingegangenen Mails

▶ 2019: 69 % ◀

24,3 MIO. Patientendatensätze waren Schätzungen zufolge international frei im Internet zugänglich

täglich bis zu **20.000** BOT-INFEKTIONEN deutscher Systeme

419 KRITIS-Meldungen

▶ 2019: 252

▶ 2018: 145

52.000 WEBSEITEN wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt

35.000 Mails mit Schadprogrammen wurden durchschnittlich pro Monat in deutschen Regierungsnetzen abgefangen

109.000 Abonnenten Bürger-CERT

▶ 2019: 105.000

▶ 2018: 100.000

rund **100** Produkte und Standorte hat das BSI im Bereich Common Criteria zertifiziert

4.400 mehr als Mitglieder der Allianz für Cyber-Sicherheit

▶ 2019: 3.700

▶ 2018: 2.700

rund **1.700** registrierte KRITIS-Anlagen

knapp **7 MIO.** Meldungen zu Schadprogramm-INFEKTIONEN übermittelte das BSI an deutsche Netzbetreiber

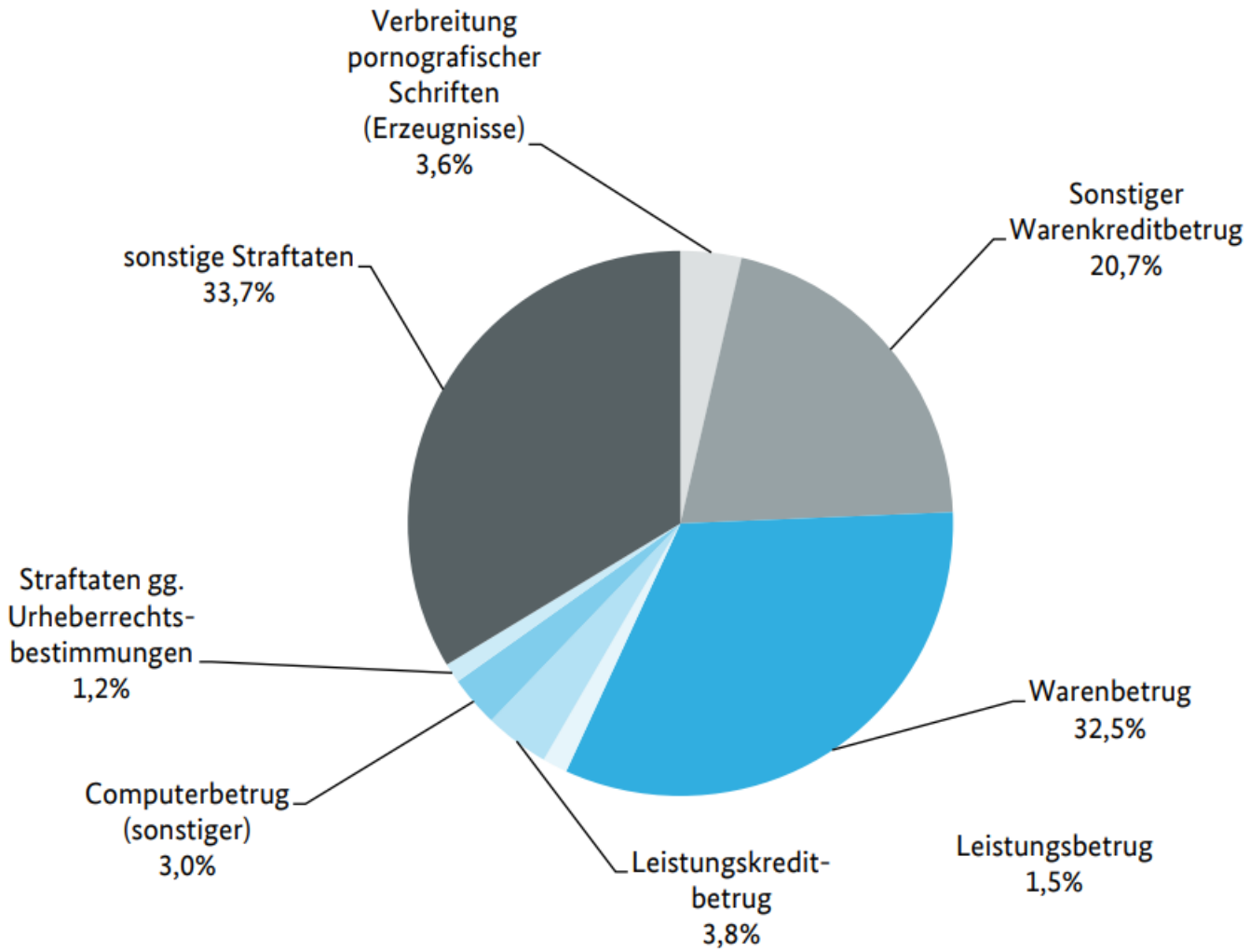
3 Cybercrime in Deutschland

- Die Professionalität von Cyberkriminellen steigt weiter an.
- Cybercrime erschafft und basiert auf kriminellen Wertschöpfungsketten.
- Ransomware bleibt die größte Bedrohung für Wirtschaftsunternehmen.
- Anzahl und auch Intensität von DDoS-Angriffen steigen rapide an.
- Die Täter sind global vernetzt und agieren international, arbeitsteilig und höchst organisiert.
- Die wichtigsten Schutzmechanismen gegen Cybercrime sind weiterhin sensible Internetnutzer.

Polizeiliche Kriminalstatistik 2019

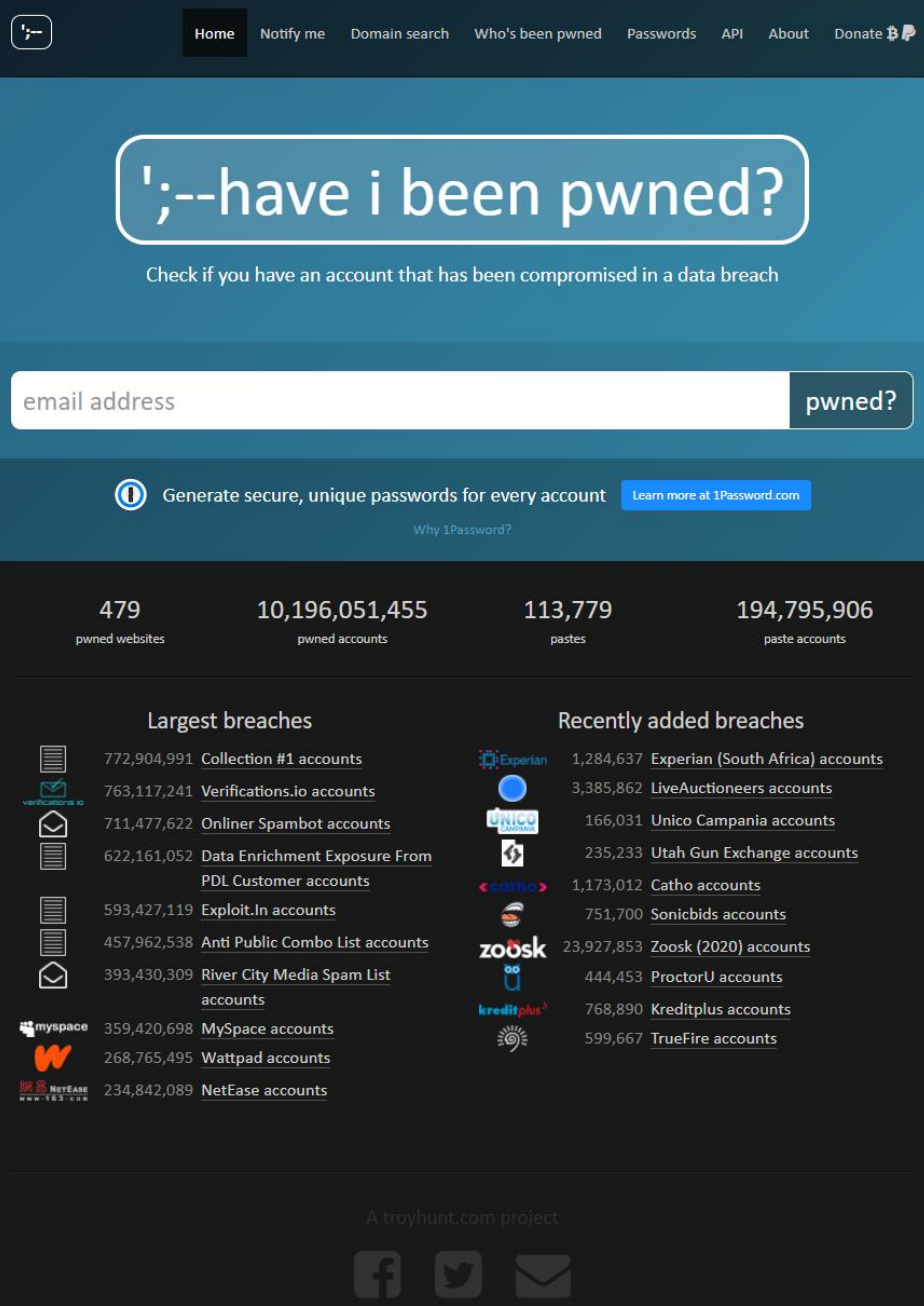
Straftatenanteile an Straftaten mit Tatmittel „Internet“ = 251.617 Fälle

1 - 2.4.2 – G01



Quelle: BKA

Demo


Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?
479
pwned websites
10,196,051,455
pwned accounts
113,779
pastes
194,795,906
paste accounts
Largest breaches
772,904,991 Collection #1 accounts
763,117,241 Verifications.io accounts
711,477,622 Onliner Spambot accounts
622,161,052 Data Enrichment Exposure From PDL Customer accounts
593,427,119 Exploit.In accounts
457,962,538 Anti Public Combo List accounts
393,430,309 River City Media Spam List accounts
359,420,698 MySpace accounts
268,765,495 Wattpad accounts
234,842,089 NetEase accounts
Recently added breaches
1,284,637 Experian (South Africa) accounts
3,385,862 LiveAuctioneers accounts
166,031 Unico Campania accounts
235,233 Utah Gun Exchange accounts
1,173,012 Catho accounts
751,700 Sonicbids accounts
23,927,853 Zoosk (2020) accounts
444,453 ProctorU accounts
768,890 Kreditplus accounts
599,667 TrueFire accounts
A troyhunt.com project

Passworte etc.

Gute Passworte

- Werden nicht mehrfach verwendet
- Sind lang
  - Passphrasen statt Passworte
  - Komplexität ist gut, länger ist besser
  - Nutzen Sie Passwort Manager
    - z.B. Keypass, LastPass, OnePassword

Multifaktor Authentisierung

- Wird von den meisten Online Plattformen unterstützt
- Geht auch ohne Token
  - z.B. Google oder Microsoft Authenticator
  - SMS TAN

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html

Der Mensch steht im Mittelpunkt

Sie könnnen helfen Angriffe abzuwehren

- Cyberkriminelle nutzen Corona/COVID19
- Vorsicht bei
  - Mails von Unbekannten
  - Links zu angeblicher Software für Videokonferenzen
  - Fragen nach persönlichen Informationen
    - Zugangsdaten
    - Kontodaten
  - Aufforderungen zur Überweisung von Geldern
- Hinterfragen Sie die Nachricht und Prüfen Sie die Indentität des Absenders
- Lassen Sie sich unter Druck setzen
- Bitten Sie Kollegen, Vorgesetzte oder die IT-Abteilung um Unterstützung.
- Achtung! Angreifer nutzen auch das Telefon.

Umgang mit dem COVID-19-Erreger

18. März 2020 um 07:27

Sparkasse

Sehr geehrte Kundinnen und Kunden,

Ihre Sicherheit und Gesundheit und auch die unserer Mitarbeiter liegt uns sehr am Herzen.

Vor diesem Hintergrund haben wir uns dafür entschieden, unsere kleineren Filialen bis auf weiteres zu schließen.

Sehr gerne stehen wir Ihnen telefonisch, per E-Mail und in unserem Online-Banking auch im Chat persönlich zur Verfügung. Die SB-Bereiche sind uneingeschränkt nutzbar.

Bitte nehmen Sie sich deshalb die 2 Minuten Zeit, um

– Ihre Adresse(n)

– Ihre Telefonnummer(n)

– und Ihre E-Mail-Adresse(n)

zu überprüfen und gegebenenfalls zu aktualisieren, um weiterhin eine reibungslose Kommunikation bei anliegenden Fragen zu gewährleisten.

In diesen Tagen müssen wir es als Gemeinschaft dem Erreger so schwer wie möglich machen, sich schnell zu verbreiten.

Prävention ist keine Hysterie, und Ignoranz ist auch kein Mut! Wir hoffen sehr auf Ihre Solidarität und Ihr Verständnis.

Vielen Dank!

Mit freundlichen Grüßen

Ihr Sparkassenverband.

Jetzt prüfen >

Quelle: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/corona-falschmeldungen.html

1.0.0 ☰ Menu

Germany

Internet Exposure Dashboard

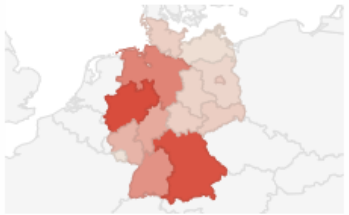
Module 1.1
Ports Open

27,083,499

Module 1.5
Industrial Control Systems

3,689

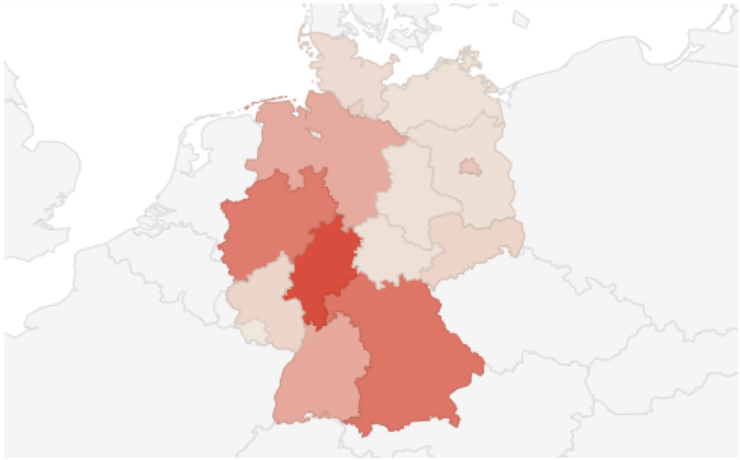
Module 1.8
Map of ICS



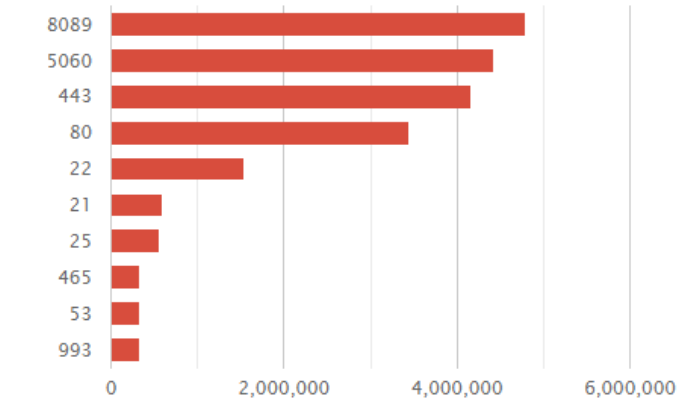
Module 1.5
EternalBlue Vulnerable

210

Module 1.3
Map of All Services



Module 1.2
Port Usage



Module 1.14
Top Vulnerability

CVE-2015-0204

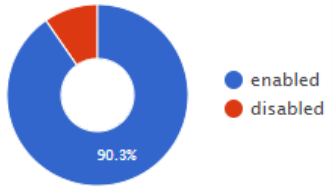
Module 1.5
BlueKeep Unpatched

2,761

Module 1.9
Compromised Databases

1,180

Module 1.11
SMB Authentication



Module 1.10
Vulnerable to Heartbleed

8,582

powered by Shodan ®

Sind Sie auf dem aktuellen Stand?

Schwachstellen in Remote Access Lösungen

CVE	Software	Rating	Threat
CVE-2019-11510	Pulse Connect Secure	10	Very High
CVE-2018-13379	Fortinet Fortigate SSL VPN	9.4	Medium
CVE-2019-1579	Palo Alto Networks GlobalProtect	9.2	High
CVE-2019-19781	Citrix Application Delivery Controller and Gateway	9.9	Very High
CVE-2019-0688	Microsoft Exchange Server	9.9	Very High
CVE-2019-0708	Remote Desktop Server	9.9	Very High
CVE-2017-11882	Microsoft Office	9.9	Very High
CVE-2020-1472	Windows	10	Very High

Patchmanagement

- Firmenrechner
  - Patchmanagement regeln
    - Auch für installierte Applikationen
  - Prüfen das Patches auch per VPN installiert werden
- Private Rechner / BYOD
  - Nur aktuelle Betriebsyteme erlauben
  - Sandboxing Lösungen prüfen
    - Mobile Device Management Lösung
    - Virtuelle Maschinen

Wo finde ich Unterstützung

Werkzeuge

DSIN
- https://www.dsin-sicherheitscheck.de/sites
- Bottom-Up: https://www.dsin-berufsschulen.de/
- Sicherheitsbarometer: https://www.sicher-im-netz.de/sicherheitsbarometer

ISMS
- VdS 10000
  - https://shop.vds.de/de/download/c7ef8c4c9f529185a75474671c74ff8a/
  - https://www.3473-wiki.de/doku.php?id=vorlagen_public:checklisten

- Dokumentationstools
  - Grundschutztool
  - ISO 27000
  - VdS 10000

- Handwerkskammern
  https://www.handwerkdigital.de/RoutenplanerCyber-Sicherheitf%C3%BCrHandwerksbetriebe

Dienstleistungen

- IHK

- ZVEH
  - https://www.zveh.de/e-check-it/der-e-check-it.html

- Digitalisierungsberater

- IT Sicherheitsberater
  - ISMS
  - Penetrationstests
  - Digital Forensics & Incident Response

- IT Systemhäuser

- Versicherungsunternehmen

Weiterführende Angebote und Informationen

https://www.sicher-im-netz.de/it-sicherheit-mittelstand-workshop-reihe

https://www.teletrust.de/kostenfreie-it-sicherheitsloesungen/

https://hk2-corona-recht.de/

Quickcheck Ihrer IT durch Compass Security

- Kostenloses Beratungsgespräch (1-2h) und kurze Konzeptanalyse
- Optional: Einfache technische Prüfung der externe Infrastruktur
  - Schwachstellen Scan und manuelle Verifikation (bis zu zehn Systeme)
  - Evaluation der Ergebnisse
  - Kurzbericht mit Hinweisen zur Verbesserung der Sicherheit
  - Kostenpflichtig (1300,00 EUR)

Compass Security Deutschland GmbH
Tauentzienstraße 18
10789 Berlin

+49 30 2100 253 0
Team.CSDE@compass-security.com