

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Vorwort:

In der digitalen Welt kann niemand mehr eine Insel oder Burg als Rückzugsort oder Schutz bauen, denn Anhand des Spektrums an verfügbaren und kompromittierbaren Technologien, Daten und Informationen lösen sich die Insel und die Burg in transparente binäre Muster auf...- wie die unten stehenden und die PDF-Liste mit IT-Sicherheitschecks mit weiteren Informationen aufzeigen!

Die Präsenz oder auch Existenz wird komplett transparent und spiegelbar. Internetfähige Geräte, die Mitbürger, Mitarbeiter und Kollegen mitbringen, aber auch Geräte, mit denen von außerhalb des eigenen Netzwerks Zugriff oder eine Spiegelung der Daten und Gegenstände eines Gebäudes, Person, Vereins, Unternehmens, etc. immer dynamischer und progressiver technisch möglich ist, erübrigen einen nur partiellen Schutz.

Aufgrund der Dynamik der Technologien, Cyberangriffsformen, und dementsprechend anhand der Informationen von Sicherheitsanbietern, Behörden, Verfassungsschutz, Universitäten und Fachverlagen, ist es eine gesamtgesellschaftliche Herausforderung, Sicherheitsstrategien in einem größeren Bezug zu bewerten.

In unserer realen Welt sind uns „IQ“ und „EQ“ bekannt und Orientierung für Intelligenz und Empathie. Doch wie steht es in der digitalen Welt um „CQ“ („Cyber-Quotient – Gefahrensensibilisierung im Netz) und „DQ“ (Digitaler Quotient – Umgang und Etikette)...?

Beispielsweise: Ein Fachanwalt für IT-Recht ist nicht zwangsläufig auch ein Spezialist für Gefahrenabwehr im Internet, ein Informatiker nicht zwangsläufig auch ein Spezialist für Datenschutz und Recht...!

Hintergrund ist die Tatsache, dass gefährliche Wissenslücken bei IT-Anwendern und Verbrauchern bestehen.

Tatsache ist aber auch, dass internetfähige Geräte mit unzureichendem Schutz vermarktet werden:
„...“

Ist es erlaubt Produkte mit solchen Sicherheitsmängeln in Deutschland zu verkaufen? Das Bundesinnenministerium teilt auf Anfrage mit: Geräte mit bekannten Sicherheitslücken seien in Deutschland "legal".

Zitat: "Bislang ist die Frage der IT-Sicherheit der Produkte keine verpflichtende Voraussetzung für die Verkehrsfähigkeit und mithin den Marktzugang."

...“

Quelle:

<https://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/internet-der-dinge100.html>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Und wie sieht es mit Ihnen aus, wie kompetent sind Sie im Umgang mit internetfähigen Geräten und dem Internet?

Da Wellness, Fitness, Work-Life-Balance auch Gesellschaftsthemen sind, wie steht es um Ihre „digitale Fitness?“

Empfehlung: Starten Sie mit einem Fitness-Test in die digitale Welt...!

Digitaler "Fittestest zum Selbstcheck" für Verbraucher:

<https://www.sicher-im-netz.de/it-fittestest-zum-selbstcheck>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Ausgangslage:

Warum entstehen so gravierende Schäden durch Internetgefahren?

Studie offenbart gefährliche Wissenslücken bei deutschen IT-Anwendern:

<https://www.itsicherheit-online.com/blog/detail/sCategory/222/blogArticle/2457>

Mehr als die Hälfte der Verbraucher übernimmt keine Verantwortung für die Sicherheit der eigenen Geräte:

<https://www.itsicherheit-online.com/blog/detail/sCategory/222/blogArticle/2691>

IoT-Botnetze nutzen weiterhin erfolgreich Standardpasswörter aus:

<https://www.itsicherheit-online.com/blog/detail/sCategory/222/blogArticle/2428>

Welche aktuellen Bedrohungen und Cybergefahren bestehen?

Verfassungsschutzberichte:

<https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte>

Allianz für Cybersicherheit / BSI:

<https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Lageberichte/lageberichte.html>

Allianz für Cybersicherheit / Register aktueller Cyberbedrohungen:

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/BSI-CS_026.pdf

Bitkom (Digitalverband Deutschlands)/Studie Wirtschaftsschutz:

<https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf>

Bitkom /Handlungsempfehlungen zur Umsetzung der Strategie Künstliche Intelligenz der Bundesregierung: Gipfelpapier zum digitalen Wandel und Transformation / Künstliche Intelligenz

<https://www.bitkom.org/sites/default/files/file/import/171012-KI-Gipfelpapier-online.pdf>

Informationen des BSI zu gefälschten Mailadressen:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/GefaelschteAbsenderadressen/gefalschteabsenderadressen_node.html

Hinweise des BSI zum gefährlichen Trojaner "Emotet" (Gefälschte Mailadressen, Mails mit Schadcode!)

<https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html>

Deutschland sicher im Netz (Schirmherrschaft: Bundesinnenministerium)

<https://www.sicher-im-netz.de/siba-aktuelle-meldungen>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Sicherheitsbarometer: Aktuelle Sicherheitsinfos / Apps für Windows-, Apple- und Android-Systeme:
<https://www.sicher-im-netz.de/siba>

Bundesamt für Sicherheit in der Informationstechnik / "Computer Emergency Response Team"
www.buenger-cert.de

EU-Initiative für mehr Sicherheit im Netz (...für Kinder, Eltern, Lehrer,...!)
<https://www.klicksafe.de/service/aktuelles/news/>

Bedrohungshinweise von Sicherheitsspezialisten Kaspersky:
<https://www.kaspersky.de/blog/category/threats/>

Hinweise der Schufa zum Datenklau und Identitätsdiebstahl:
<https://datenklau.de/gefaehrdete-daten-und-typische-faelle.html>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Allgemein:

Check für Computer, Smartphone, Tablet

Volksbank-Computercheck:

„Der VR-ComputerCheck der VR-NetWorld GmbH und des Sicherheitsspezialisten Coronic GmbH kann die auf Ihrem Computer, Tablet und Smartphone installierten Programme und Plug-ins auf Aktualität und bekannte Sicherheitsprobleme prüfen und Ihnen bei der Behebung von Sicherheitslücken helfen...!“

<https://www.wvb.de/banking-service/sicherheit/vr-computercheck.html>

Mailchecks auf Identitätsdiebstahl

Mailchecks auf Identitätsdiebstahl der eigenen Mailadresse(n):

<https://sec.hpi.de/ilc/search?lang=de>

<https://haveibeenpwned.com>

<https://breachalarm.com>

Passwortcheck

Kaspersky-Passwort-Check:

Ist das Passwort überhaupt sicher genug? Achtung: Auf keinen Fall das Originalpasswort eingeben, allenfalls ein Ähnliches...! **Bitte unbedingt Hinweise zur Passwortsicherheit im Anhang beachten...!**

<https://password.kaspersky.com/de/>

Schufa – Identitätsschutz

Schufa: Schutz vor Identitätsdiebstahl – IdentSafe und Alarmierung bei Missbrauch (kostenpflichtig, aber sehr sinnvoll!)

https://www.meineschufa.de/index.php?site=22_1&via=menu

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

<https://datenklaue.de/identitaetsschutz-in-schufa-qualitaet.html>

Welche persönlichen Daten sind besonders gefährdet?

<https://datenklaue.de/gefaehrdete-daten-und-typische-faelle.html>

Check auf Schadcode und verseuchte Webseiten

Tests/Scan von Dateien, Webseiten, IP-Adressen auf verseuchte und infizierte Inhalte:

www.virustotal.com

Hinweise für Mac- und IOS-Systeme

z.B. <https://www.kaspersky.de/mac-security>

und <https://www.gdata.de/mobile-internet-security-ios>

Testvirus

Webseite für Download des Testvirus zum Testen und prüfen, ob überhaupt eine installierte Sicherheitssoftware anschlägt (Empfehlung: Testweise auf Virustotal hochladen zu Verifizierung!):

<https://www.etes.de/downloads/eicar-testvirus/>

Router- , Netzwerk- und Computer-Checks

Router- , Netzwerk- und Computer-Checks auf offene Ports und Datenverkehr:

<http://www.heise.de/security/dienste/Netzwerkcheck-2114.html>

http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=13091&article_id=56032&psmand=48

https://www.f-secure.com/de_DE/web/home_de/router-checker

- **Netzwerkprotokoll/Datenverkehr im Netzwerk prüfen:**

<https://www.pcwelt.de/ratgeber/So-entlarven-Sie-WLAN-Schnueffler-7685086.html>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

https://praxistipps.chip.de/fritzbox-datenverkehr-mitschneiden_9989

- **Iot-Scanner für internetfähige Geräte (Router, TV, Alarmanlage, Telefon, Netzwerkdrucker, PC, Smartphone, Tablet, Laptop, Notebook, etc.):**

<http://iots scanner.bullguard.com/>

<http://iots scanner.bullguard.com/deep-scan/>

<https://www.bitdefender.de/solutions/home-scanner.html>

- **Sicherheitstests/Informationen des BSI:**

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/sicherheitstest_02112018.html

- **Prüfung auf Herkunft und Identität von Webadresse, IP-Adressen (Hinweis: Jede Webseite und jede Mail enthält IP-Adressen mit Herkunftsinformationen!)**

www.network-tools.com

- **Scan von jedem internetfähigen Gerät im internen, eigenen Netzwerk auf offene Ports (Achtung: Nur im internen, eigenen Netzwerk verwenden!)**

www.nmap.org

- **Überwachung von sämtlichen Datenverkehr im internen, eigenen Netzwerk über die Schnittstellen im Router:**

www.wireshark.org

Schutzprogramme und Abwehr

Auswahl geeigneter Schutzprogramme für Privat und Unternehmen:

www.av-test.org

Hinweise: Beispielsweise nutzen nachfolgende Anbieter künstliche Intelligenz zur Cyberabwehr. Nach offiziellen Schätzungen von ca. 400.000 (Quelle: BSI) neuen digitalen Schädlingen täglich (!) eine Herausforderung für jeden Sicherheitsanbieter:

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

<https://www.gdata.de/news/2018/11/31301-g-data-neuentwicklung-deeplay-kunstliche-intelligenz-bringt-durchbruch-in-der-bekämpfung-von-cybercrime>

<https://www.avira.com/de/press-details/nid/1171/news/avira-antivirus-2018-remastered-and-redesigned-for-todays-digital-world>

<https://news.sophos.com/de-de/2018/08/08/ki-sollte-kein-solist-sein-sondern-teil-eines-mehrschichtigen-ensembles/>

Hinweise für Mac und IOS-Geräte

z.B. <https://www.kaspersky.de/mac-security>

und <https://www.gdata.de/mobile-internet-security-ios>

Cyberabwehr und Infektionsbereinigung / Schädlingsbereinigung:

<https://www.botfrei.de>

Hilfe bei Erpressung / Erpressungstrojaner etc.:

<https://www.nomoreransom.org/de/index.html>

Digitale Mailsignaturen

Nutzung von digitalen Zertifikaten, dient der Sicherstellung über tatsächlichen Absender (Privat: kostenfrei! Digitales Mail-Zertifikat und Verschlüsselung!)

<https://www.instantssl.com/ssl-certificate-products/free-email-certificate.html>

Nutzung von kostenpflichtigen umfassenderen digitalen Zertifikaten, dient der Sicherstellung über tatsächlichen Absender:

<https://www.globalsign.com/de-de/>

<https://www.thawte.de>

<https://www.geotrust.com/de/signing-products/secure-email/>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Mailverschlüsselung

Mailanbieter nach DSGVO/Mailverschlüsselung und digitale Mailsignatur/Kennzeichnung sicherer Kommunikation im Verbund von Telekom, 1und1, Strato, GMX, Web.de, Freenet:

<https://www.e-mail-made-in-germany.de/index.html>

<https://www.e-mail-made-in-germany.de/Verschlusselung.html>

<https://www.e-mail-made-in-germany.de/Outlook-Plugin.html>

Office365-DKIM für digitale Signatur von Mails:

<https://docs.microsoft.com/de-de/office365/securitycompliance/use-dkim-to-validate-outbound-email>

Warum überhaupt verschlüsseln?

https://www.bsi.bund.de/DE/Themen/Kryptografie_Kryptotechnologie/Kryptotechnologie/Gpg4win/gpg4win_node.html

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschlusselung/EMail_Verschlusselung/In_der_Praxis/EMails_verschlusseln_in_der_Praxis_node.html

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05063.html

Freies Verschlüsselungs- und Signaturprogramm:

<https://www.gpg4win.de>

Webseiten verschlüsseln

Warum sollten Webseiten grundsätzlich verschlüsselt werden?

<https://www.website-check.de/blog/datenschutzrecht/update-zur-dsgvo-muss-die-komplette-website-ssl-verschlusselt-werden/>

<https://www.deutsche-handwerks-zeitung.de/firmen-webseiten-ssl-verschlusselung-ist-pflicht/150/3101/360639>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

<https://www.zeit.de/digital/datenschutz/2019-01/mail-daten-ueberwachung-ip-adresse-speicherung-bundesverfassungsgericht>

<https://www.ionos.de/digitalguide/websites/webseiten-erstellen/wie-stelle-ich-meine-seite-auf-ssl-und-https-um/>

...weitere Gründe: Abwertung beim Ranking durch Google; Sicherheitsrisiko für jeden Nutzer, der die Webseite besucht - aufgrund von Manipulation und Schadcodeübertragung, Abmahngefahr und Verletzung der DSGVO, weil jeder Provider personenbezogene Daten übermittelt und speichert (IP-Adresse, etc....!).

Webseitencheck auf SSL-Verschlüsselung:

<https://www.ionos.de/tools/ssl-check>

SSL-Server-Check (Sehr umfangreich, ggf. mit Hinweisen zu Bugs!):

<https://www.ssllabs.com/ssltest/>

Schutz vor Internetbetrug

Webseiten mit Informationen zum Schutz vor Internetbetrug:

<https://www.sicher-im-netz.de>

<https://www.bsi-fuer-buerger.de>

<https://www.buerger-cert.de>

<http://www.klicksafe.de>

<https://secuso.aifb.kit.edu/642.php> (SECUSO – Forschungsgruppe des KIT mit Informations-, Schulungs- und Abwehrmaßnahmen für Sicherheitsbeauftragte...!)

Schufa – Informationen:

<https://datenklau.de/identitaetsschutz-tipps-tricks.html>

<https://datenklau.de/die-methoden-der-betrueger.html>

„Fake-News“ / gefälschte Informationen erkennen in sozialen Medien:

<http://faktenfinder.tagesschau.de/tutorials/fakenews-erkennen-tutorial-101.html>

SocialBots erkennen: <http://faktenfinder.tagesschau.de/tutorials/social-bots-erkennen-101.html>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Vom Hessischen Innen- und Sportministerium:

<https://innen.hessen.de/sicherheit/cybersicherheit/cert-hessen/erreichbarkeit-und-dienstleistungen>

<https://innen.hessen.de/sicherheit/cybersicherheit/cert-hessen/informationen-fuer-buerger>

Meldestellen bei Internetbetrug

Informations- und Meldestellen bei erfolgtem Internetbetrug:

<https://www.allianz-fuer-cybersicherheit.de/>

<https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.html>

- **Polizeidienststellen:**

<https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/ZAC/polizeikontakt.html>

- **Informationen des BKA:**

https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html

https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/internet_node.html

DSGVO – Datenschutzmaßnahmen

Datenschutzmaßnahmen nach DSGVO / Datenschutzgeneratoren für Webseitenbetreiber: (Achtung: Lizenzrechte der Betreiber unbedingt beachten!)

<https://datenschutz-generator.de>

<https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de>

Informationen der hessischen Datenschutzbehörden:

<https://datenschutz.hessen.de>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Datenschutzhinweise und Muster:

<https://datenschutz.hessen.de/infothek/hinweise-und-muster-ds-gvo>

Verfassungsgemäße Datenschutz-Rechte der Bürger in Hessen:

<https://www.verfassung-hessen.de/datenschutz-in-die-verfassung>

Für Unternehmen zusätzlich:

Sicherheitscheck für Unternehmen von „Deutschland sicher im Netz“ unter Schirmherrschaft des Bundesinnenministeriums:

<https://www.dsin-sicherheitscheck.de/sites#Home-show>

Kostenfreier Websitecheck für Unternehmen vom Ecoverband!

<https://www.eco.de/presse/63730/>

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Anhang:

In Sachen Passwortsicherheit:

Egal ob Router, Iot-Gerät, Banking, Mail, Social-Media, etc.: Überall, wo ein Login angezeigt ist, ist die Passwortsicherheit auch von der Programmatik der Firmware (Z.B. Betriebssystem des Routers, Fernsehers, Multimediereceivers, Alarmanlage, etc.) und weiteren Schutzmechanismen abhängig (z.B. Zwei-Faktor-Authentifizierung, Zugriffssperren, sukzessive Verlängerung der Sperrintervalle wie bei Routern, etc.).

Denn:

Ein langes alphanumerisches Passwort mit Sonderzeichen ist kein wirksamer Schutz mehr! Am Beispiel vom Kaspersky-Passwort-Check lässt sich dies einfach darstellen, da hier nur von einem Heim-PC als attackierendem Gerät ausgegangen wird.

<https://password.kaspersky.com/de/>

Wie im Artikel vom Spiegel von 2011 beschrieben, konnte damals mittels einem handelsüblichen PC 25 Millionen Passwörter pro Sekunde ausprobiert werden:

<http://www.spiegel.de/netzwelt/web/sichere-passwoerter-sindsieschongeknackt-a-790936.html> .

Heute kann ein einzelner PC mit moderner Grafikkarte und „Deep Learning“-Technologie (auch neuronale Chips!) bis über 60 Terraflops pro Sekunde ausführen, sprich über 60 Milliarden Berechnungen pro Sekunde!!!

Selbst ein neues Tablet von Apple mit neuartigen neuronalen Bionic-Prozessoren (<https://www.apple.com/de/ipad-pro/specs/> und <https://en.wikichip.org/wiki/apple/ax/a12x>) schafft hier bereits über 10 Milliarden Berechnungen pro Sekunde. Sind massenhaft PC's, Smartphones, Tablets zu Botnetzen verbunden, ist Passwortsicherheit nur anhand der Länge kein Sicherheitsargument mehr...! Bereits 2016/2017 wurden bereits ganze Länder testweise (!) über gekoppelte Botnetzangriffe durch kompromittierte Router und Iot-Geräte lahm gelegt:

<http://www.spiegel.de/netzwelt/web/botnet-mirai-unbekannte-werfen-liberia-aus-dem-netz-a-1119708.html> .

Auch ist es sinnvoll, zur Sicherheit vor Passwortverlust und Identitätsdiebstahl das Passwort und die Mail zum Postfach zum Passwortreset- und Verifizierung mindestens nach gleichen Sicherheitsstatuten einzurichten. Was hilft ein sicheres Login, wenn man mit dem Button „Passwort vergessen?“ direkt ein neues Passwort über das unsichere Referenz-Postfach gesandt bekommt?

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe!

Bei der Nutzung von verschlüsselten Mails sind auch diese kritisch zu betrachten. Sind die Mails nicht zusätzlich digital signiert, ist der Absender nicht als eindeutig verifizierbar zu bewerten. Die öffentlichen Schlüssel sind für jeden lesbar i.d.R. auf Key-Servern abgelegt. Damit ist auch eine verdeckte Schadcodeübertragung möglich und Schutzprogramme schlagen allenfalls dann an, wenn die Mail auf dem Endgerät (Computer, Smartphone, etc.) entschlüsselt wird! Auch die Form der Übertragung – im nur Text-Format spielt eine Rolle, wie nachfolgend beschrieben:

<https://www.zeit.de/digital/datenschutz/2018-05/pgp-s-mime-verschluesselung-e-mails-sicherheit>

<https://www.sueddeutsche.de/digital/exklusiv-verschluesselte-e-mails-sind-nicht-sicher-1.3978608>