Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

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 Präsens 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

INHALT:

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

1. Was ist „Stand der Technik?“

Dabei ist die Frage nach dem Stand der Technik und damit den Maßgaben zur IT-Sicherheit klar zu beantworten:

https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/

Information von ENISA und Teletrust:

https://www.teletrust.de/fileadmin/docs/presse/presse-docs/PM-190207-ENISA-TeleTrusT-Handreichung_Stand_der_Technik_DEU.pdf

Umfassende Dokumentation (Handreichung):

https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-02_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf

2. 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 "Fitnesstest zum Selbstcheck" für Verbraucher:

https://www.sicher-im-netz.de/it-fitnesstest-zum-selbstcheck

CISCO Networking Academy zur Schulung von Mitarbeitern als Anwender bis zum IT-Experten (Hinweise beachten zu Kursen!)

https://certnet.de/cisco/

Kursübersicht:

https://certnet.de/cna-kurse/

eval-U - Das Tool zur Kompetenzfeststellung:

„...eval-U wurde von Cisco entwickelt, um IT-Kompetenz realistisch und objektiv einzuschätzen. Der Test umfasst 20 Fragen aus den Bereichen Computergrundlagen, Netzwerke, Internet of Things und IT-Sicherheit. Nach Abschluss des Tests erhält jeder Teilnehmer eine Ergebnis-Urkunde. Die IT-Kompetenz wird in fünf Leveln geordnet, wobei Level 5 für ein großes Wissen im Bereich IT steht. Basierend auf dem erreichten Kompetenz-Level wird dem Teilnehmer ein passender kostenloser Kurs der Cisco Networking Academy empfohlen...!“

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

Cybersecurity-Test zur Feststellung über geeigneten Einstiegskurs:

https://www.eval-u.de/cybersecurity

CISCO ist Partner des „Haus des Stiftens“ für NGOs (Vereine, gemeinnützige Einrichtungen, etc.!)

https://www.hausdesstiftens.org/unser-partner/cisco/

Weitere Informationen:

https://www.cisco.com/c/de_de/training-events/networking-academy.html

Die Robert-Bosch-Stiftung ist Partner des „Haus des Stiftens“ für NGOs (Vereine, gemeinnützige Einrichtungen, etc.!)

Digital-Kamp 2019 – 10 Bausteine (Webinare) für „Non-Profits“

https://www.npo-digitalcamp.org

- Sozial + Digital = Genial?
- Kommunikation – was kommt nach Web 2.0 und Social Media?
- Datenanalyse – Potenziale und Nutzen
- Mit Algorithmen zu einer besseren Gesellschaft?
- Bildung und lernen in der digitalen Welt
- IT-Strategie – aus Struktur wird Strategie
- Digitale Wirkungsmessung – einfach gemacht
- Mehr als Geld – Online Unterstützung finden
- Digitalisierung & Ehrenamt – wie passt das zusammen?
- Bereit für die Digitalisierung – wirklich?

3. Ausgangslage:

Übersichten zu weltweiten Bedrohungen durch Viren, Trojaner, Würmer, Spam, Netzangriffe, etc.:

Infos von Kaspersky: https://statistics.securelist.com/de/

Honeypotarchitektur-Sicherheitstacho der Telekom und Partner über weltweite Angriffe in Echtzeit:https://sicherheitstacho.eu/start/main

Info zu "Honeypots": https://de.wikipedia.org/wiki/Honeypot

4. Warum entstehen so gravierende Schäden durch Internetgefahren?

"...Mehr als 99 Prozent der Cyberangriffe setzen dabei auf eine menschliche Interaktion und machen so den einzelnen Benutzer zur letzten Verteidigungslinie...!"

https://www.itsicherheit-online.com/blog/detail/sCategory/222/blogArticle/3473

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

5. Welche aktuellen Bedrohungen und Cybergefahren bestehen?

SIM-Swapping:

https://www.zeit.de/digital/2019-09/sim-swapping-technologie-hacking-soziale-medien-datenschutz

Fachmagazin IT-Sicherheit zum „Kampf der künstlichen Intelligenzen...!“:

Artikel: „Kampf der künstlichen Intelligenzen... wenn zukünftig nur noch Algorithmen das Schlachtfeld dominieren...!“ (Seite 3)

Artikel: „Wenn künstliche Intelligenz schiefgeht...!“ (Ab Seite 20)

https://www.itsicherheit-online.com/EPaper/index/active/1/epaper/8126

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

Malwarebytes-Bericht über „Gute und böse künstliche Intelligenz...!“

„...Fast-forward 10 years, however, and if we’re not proactive, we may be left in the dust. Best to develop this technology responsibly, with a 360-degree view on how it can be used for both good and evil, then to let it steamroll over us and move beyond our reach…!”

https://schwartzpr.de/website/uploads/AI_goes_awry.pdf

https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

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:

2019: 100 Milliarden Wirtschaftsschaden...!

https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr

2018: 43 Milliarden Wirtschaftsschaden...!

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

Bezugnahme zum „Haus des Stiftens“ , der Plattform www.stifter-helfen.de. Hier ist der Artikel der Robert-Bosch-Stiftung „Digitalisierung braucht Zivilgesellschaft“ für Zivilgesellschaft, gemeinnützige Organisationen und Vereine sehr zu empfehlen!

https://www.bosch-stiftung.de/sites/default/files/documents/2019-01/Summary_Digitalisierung_braucht_Zivilgesellschaft.pdf

und der komplette Report:

https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2019-01/Report_Digitalisierung_braucht_Zivilgesellschaft_2019.pdf .

Informationen des BSI zu gefälschten Mailadressen:

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

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.buerger-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

6. Allgemein:

a. 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

b. Hardware-Sicherheitslücken: Tests und Infos

https://www.ashampoo.com/de/eur/pin/1304/sicherheitssoftware/spectre-meltdown-cpu-checker

Sicherheitstipps von GData, Heise, Kaspersky, u.a.

https://www.gdata.de/tipps-tricks/meltdown-spectre-scanner

https://www.heise.de/thema/Meltdown-und-Spectre

https://www.kaspersky.de/blog/35c3-spectre-meltdown-2019/18332/

Informationen des Fraunhofer-Instituts zu Hardwaretrojanern:

https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HWT-Bericht/HWT-Bericht_Cover.pdf

Technische Informationen zu Meltdown und Spectre und den Hardwareherstellern von der Technischen Universität Graz:

https://meltdownattack.com/

c. Mailchecks auf Identitätsdiebstahl

Mailchecks auf Identitätsdiebstahl der eigenen Mailadresse(n):

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

https://haveibeenpwned.com

Die deutsche Webseite https://www.experte.de/email-check der Autoren der Firma vB Internet GmbH aus München unter Bezug zum Mail-Sicherheitscheck auf der englischsprachigen Webseite (https://haveibeenpwned.com).

https://breachalarm.com

d. Passwort-Check von Kaspersky

Ist das Passwort überhaupt sicher genug? **Achtung:** Auf keinen Fall das Originalpasswort eingeben, allenfalls ein Ähnliches...!

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

e. Passwortsicherheit: Erstellung und Umgang mit Passwörtern

Informationen des Bundesamtes für Sicherheit in der Informationstechnik:

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

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html

f. 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

https://datenklau.de/identitaetsschutz-in-schufa-qualitaet.html

Welche persönlichen Daten sind besonders gefährdet?

https://datenklau.de/gefaehrdete-daten-und-typische-faelle.html

g. 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

https://www.avira.com/de/free-antivirus-ios

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

h. Anti-Viren-Check der Betriebssysteme

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

https://www.eicar.org/?page_id=3950

i. Anti-Viren-Check des Mailprogramms

Sicherheitstests von Heise-Security:

"...E-Mail ist das zentrale Einfallstor für Viren und Würmer geworden. Die Postfächer sind voll mit infizierten Mails und täglich tauchen neue Schädlinge auf. Antiviren-Programme können diese Gefahr zwar reduzieren, aber nicht vollständig beseitigen. Deshalb ist es wichtig, seinen Umgang mit E-Mails und die dabei verwendeten Programme dieser Bedrohung anzupassen..."

https://www.heise.de/security/dienste/Emailcheck-2109.html

j. 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

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

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

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

http://iotscanner.bullguard.com/

http://iotscanner.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!)**

https://nmap.org/

Tools: https://seclists.org/

Schwachstellenscanner: https://sectools.org/tag/vuln-scanners/

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

www.wireshark.org

k. Schutzprogramme und Abwehr

Auswahl geeigneter Schutzprogramme für Privat und Unternehmen:

www.av-test.org

Getestete Schutzsysteme für Netzwerkumgebung mit Iot-Geräten:

https://www.av-test.org/de/internet-of-things/

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

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:

https://www.gdata.de/news/2018/11/31301-g-data-neuentwicklung-deepray-kunstliche-intelligenz-bringt-durchbruch-in-der-bekampfung-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/

Schutzprogramme für Mac und IOS-Geräte

z.B. https://www.avira.com/de/free-antivirus-ios

https://www.kaspersky.de/mac-security
https://www.gdata.de/mobile-internet-security-ios
https://www.av-test.org/de/antivirus/privat-macos/
https://www.av-test.org/de/antivirus/unternehmen-macos/

Absicherung von Iot-Geräten / Smart-Home / Abwehr von Cyberangriffen:

https://www.bitdefender.de/box/

https://www.securifi.com/de/smart-home

Cyberabwehr und Infektionsbereinigung / Schädlingsbereinigung:

https://www.botfrei.de

Hilfe bei Erpressung / Erpressungstrojaner etc.:

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

I. Digitale Mailsignaturen

Nutzung von digitalen Zertifikaten, dient der Sicherstellung über tatsächlichen Absender (Privat: kostenfrei – Laufzeit jedoch nur 30 Tage! Digitales Mail-Zertifikat und Verschlüsselung!)

https://ssl-trust.com/SSL-Zertifikate/Kostenloses-SSL-Zertifikat

Nutzung von kostenpflichtigen umfassenderen digitalen Zertifikaten, dient der Sicherstellung über tatsächlichen Absender (Mail- und Serverzertifikate):

https://www.sslplus.de/smime-zertifikate.html

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

https://www.thawte.de

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

Gemeinnütziges Projekt: https://letsencrypt.org/de/

m. 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/Verschluesselung.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.ionos.de/digitalguide/e-mail/e-mail-sicherheit/e-mail-verschluesseln-mit-ssl/

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

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/EMail_Verschluesselung/In_der_Praxis/EMails_verschluesseln_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

n. Webseiten verschlüsseln und Schutz vor Angriffen

Warum sollten Webseiten grundsätzlich verschlüsselt werden?

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

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

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

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:

1. Abwertung beim Ranking durch Google.
2. Warnung in Browsern vor unverschlüsselten Webseiten.
3. Warnungen in Sicherheitssuiten/Sicherheitssoftware vor dem Besuch unverschlüsselter Webseiten.
4. Sicherheitsrisiko für jeden Nutzer, der die Webseite besucht - aufgrund von Manipulation und Schadcodeübertragung.
5. 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/

Webseiten vor Angriffen schützen (Website Application Scan auf Sicherheitslücken):

https://www.ionos.de/hilfe/sicherheit/sitelock/was-ist-sitelock/

https://www.strato.de/faq/sicherheit/was-bietet-mir-sitelock/

- SQL-Injection Scan
- Cross-Site-Scripting (XSS)-Scan
- Malware-Scan
- Suchmaschinen-Blacklist Überwachung
- SSL-Verifikation der Webseite
- File Change-Monitoring
- Sitelock-Siegel mit Sicherheitszertifikat für die Webseite

o. 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...!)

p. Schufa – Informationen / Identitätsschutz / Tipps u. Tricks:

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

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

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

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

r. SocialBots erkennen:

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

s. 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

- **Vom Hessischen Innen- und Sportministerium „Cyber Competence Center“:**

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

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

t. Beschwerdestelle / Meldestelle der Bundesnetzagentur

Bei Fax-SPAM, belästigenden Anrufen, unverlangte SMS, unverlangte Werbenachricht per Messenger, Bandansage (Gewinnmitteilung, Spendenanruf), E-Mail-SPAM, Ping-Anruf, verwirrende oder fehlende Preisangabe, fehlende Preisansage, Warteschleife, hochpreisige Kundenhotline, Handy-/Internetdailer, unerlaubte Telefonwerbung, sonstiges...

https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Verbraucher/RumitelBeschwerde/beschwerde-node.html

u. Hilfe bei Diskriminierung /Hass im Netz / Strafverfolgung

https://hateaid.org/betroffenenberatung/

Hessen gegen Extremismus:

https://hke.hessen.de//

"...Die Meldeplattform "Hessen gegen Hetze“ wird durch das Hessen CyberCompetenceCenter des Hessischen Ministeriums des Innern und für Sport betrieben. Ziel ist es, Bürgerinnen und Bürgern die Möglichkeit zu bieten, potenzielle Hasskommentare einfach und schnell per Online-Formular, E-Mail oder Telefon zu melden...!"

https://hessengegenhetze.de/

https://www.bka.de/DE/KontaktAufnehmen/HinweisGeben/hinweisgeben_node.html

https://hessengegenhetze.de/fragen-antworten/meldestelle

https://hessengegenhetze.de/fragen-antworten/strafanzeige-strafantrag

v. DSGVO – Datenschutzmaßgaben

Datenschutzmaßgaben 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

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

7. Für Unternehmen zusätzlich:

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

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

Sicherheitscheck vom VdS für Unternehmen („Brandschutz des 21. Jahrhunderts: Cybersecurity“ - https://vds.de/cyber/):

https://www.vds-quick-check.de/

Kostenfreier Websitecheck für Unternehmen vom Ecoverband!

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

CISCO Networking Academy zur Schulung von Mitarbeitern als Anwender bis zum IT-Experten!

https://certnet.de/cisco/

Kursübersicht: https://certnet.de/cna-kurse/

a. Schwachstellensuche / Schwachstellenmanagment / Vulnerabilty Management / Beispiele

BSI - Cybersicherheit - Open Vulnerability Assessment System (OpenVAS)

Schwachstellen-Analyse in Netzen unter Einsatz von OpenVAS v2.0
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_007.pdf

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Tools/OpenVAS/OpenVAS_node.html

https://www.greenbone.net/

Vulnerability Management / Schwachstellenscanner
https://youtu.be/3z65oEoE2zA

"NESSUS" von TENABLE

Hinweis: Das Programm "NESSUS" zur Schwachstellenanalyse in IT-Netzwerken von Unternehmen wurde vormals auch vom BSI eingesetzt. NESSUS wird heute von dem Sicherheitskonzern "TENABLE" geführt und vertrieben.

https://www.security-insider.de/kostenloser-schwachstellen-scan-mit-nessus-essentials-a-838207/

https://de.tenable.com/blog/nessus-home-is-now-nessus-essentials

https://de.tenable.com/products/nessus/nessus-professional

https://de.tenable.com/webinars/schwachstellenmanagement-nach-bsi-it-grundschutz

On-Demand Webinar - Schwachstellenmanagement nach BSI IT-Grundschutz

https://de.tenable.com/webinars/schwachstellenmanagement-nach-bsi-it-grundschutz

"...Physische Geräte und Systeme aller Art – von Konferenzsystemen für Unternehmen bis hin zu Stromnetzen – sind heute vernetzt und programmierbar, wodurch sich noch mehr Möglichkeiten der digitalen Transformation eröffnen...

...Einige behaupten, diese digitalen Technologien seien die Zukunft. In Wahrheit ist die Zukunft jedoch bereits da. Bis 2019 werden in Unternehmen über 9 Milliarden IoT-Geräte im Einsatz sein, und über 90% der Unternehmen arbeiten heute mit Anwendungen in der Cloud...

...Während die digitale Transformation eine ganz neue Welt der Möglichkeiten eröffnet, stellt sie auch Ihre neue Cyber-Angriffsoberfläche dar, die es zu verteidigen gilt. Und diese wächst explosionsartig...!" Quelle: https://de.tenable.com/cyber-exposure

"...Cyber Exposure For Dummies is a must read for all InfoSec professionals responsible for protecting dynamic computing environments...!"

https://de.tenable.com/whitepapers/cyber-exposure-for-dummies

"... In den vergangenen 24 Monaten haben 50 % der Unternehmen einen Angriff auf ihre OT-Infrastruktur erlebt, der zu Ausfällen bei Anlagen und/oder operativer Ausrüstung geführt hat... Quelle: Cybersecurity für operative Technologien: 7 wichtige Erkenntnisse, Ponemon Institute, 2019.."

https://de.tenable.com/ponemon-report/cybersecurity-in-operational-technology

F-Secure - Schwachstellenscanning und -management

"...IT Security Manager müssen in der Lage sein, Schwachstellen von unterschiedlichen Perspektiven aus zu bewerten um eine genaue Beurteilung der Risiken zu erhalten, um Sicherheitsbedrohungen zu minimieren und den Gesetzesanforderungen zu entsprechen...!"

https://www.f-secure.com/de/business/products/vulnerability-management/radar

"...F-Secure Countercept verteidigt Unternehmen gegen sehr gezielte Angriffe. Wir leben in einer Welt, in der hochentwickelte Angreifer Unternehmen, Organisationen und Regierungen kompromittieren um Daten zu entwenden. Unser Ziel ist es, die Auswirkungen eines Cyberangriffs zu verhindern...!"

https://www.f-secure.com/de/business/products/advanced-threat-protection/countercept

Kaspersky - Vulnerability und Patch Management

"...Cyberkriminelle nutzen nicht gepatchte Schwachstellen in Betriebssystemen und häufig genutzten Programmen (darunter Java, Adobe, Internet Explorer, Microsoft Office usw.) aus, um Unternehmen aller Größen zielgerichtet anzugreifen. Dieses Risiko wird durch die zunehmende Komplexität von IT-Umgebungen noch verschärft – wenn Sie nicht wissen, welche Komponenten überhaupt vorhanden sind, wie sollen Sie diese dann schützen?"

https://www.kaspersky.de/small-to-medium-business-security/systems-management

https://www.kaspersky.de/small-to-medium-business-security/total

https://www.kaspersky.de/small-to-medium-business-security/endpoint-advanced

b. Cyberabwehrtraining für Unternehmen von Sicherheitsspezialisten mit Awareness-Training:

GData-Security-Awareness-Training

Cyberabwehrtraining für Mitarbeiter in Unternehmen, umfassendes Schulungsprogramm mit Lernmodulen für nachhaltigen und regelmäßigen Lernerfolg und fortlaufende Sensibilisierung der Mitarbeiter.

https://www.gdata.de/business/security-awareness-training

Kaspersky-Security-Awareness-Program (ASAP)

Kaspersky Automatisiertes Security Awareness Training

"...Ein einfach zu verwaltendes Online-Tool, das die Cybersicherheitskompetenz Ihrer Mitarbeiter stufenweise aufbaut... Die Kaspersky Automatisierte Security Awareness Platform (ASAP) wurde von führenden Cybersecurity-Experten mit dem Ziel entwickelt, Ihr Unternehmen zu schützen...!"

https://asap.kaspersky.com/de/

https://www.kaspersky.de/enterprise-security/security-awareness

c. Grundschutzprofile für Handwerksbetriebe, Handwerkskammern, IT-Dienstleister…

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/Profile/itgrundschutzProfile_Profile_node.html

IT-Grundschutz-Profil für Handwerksbetriebe:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Handwerksbetriebe.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Handwerksbetriebe.pdf

Routenplaners des BSI als Leitfaden zum IT-Schutz für Handwerksbetriebe:

https://www.bsi.bund.de/SharedDocs/Downloads/ACS/routenplaner_print.html

https://www.bsi.bund.de/SharedDocs/Downloads/ACS/routenplaner_print.pdf

Allianz für Cybersicherheit:

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/Routenplaner/routenplaner_node.html

Kompetenznetzwerk des Handwerks:

https://handwerkdigital.de

und

https://handwerkdigital.de/newsroom/aktuelles/it-grundschutz-profil-fuer-handwerksbetriebe/

IT-Dienstleistungen – aber sicher! Kriterienlisten für Auswahl geeigneter IT-Dienstleister:

https://www.ihk.de/it-sicherheits-kriterien

Bei DSGVO-Verletzung - Abmahngefahr für Handwerksbetriebe:

https://www.handwerk-magazin.de/so-sollten-handwerker-auf-dsgvo-abmahnungen-reagieren/150/381/372827

8. Ausblick / Hinweise zu Technologien

Technologische Entwicklungen z.B. um Künstliche Intelligenz, Big Data, Machine Learning, Deep Learning, Language Processing und Quantensystemen revolutionieren Gesellschaft und Märkte, im lokalen und globalen Wettbewerb. Und es entstehen Fragen z.B. über digitale Sicherheit, Verantwortung und Ethik...!

Hinweise hierzu geben u.a.:

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

https://www.bosch-stiftung.de/sites/default/files/documents/2019-01/Summary_Digitalisierung_braucht_Zivilgesellschaft.pdf

Wirtschaftswissenschaftlerin Frau Prof. Soshana Zuboff, Autorin des Buchs „Das Zeitalter des Überwachungskapitalismus“:

https://de.wikipedia.org/wiki/Shoshana_Zuboff

https://www.sueddeutsche.de/digital/shoshana-zuboff-ueberwachungskapitalismus-google-facebook-1.4198835

Wirtschaftsinformatikerin Frau Prof. Sarah Spiekermann :

https://www.tagesspiegel.de/politik/wirtschaftsprofessorin-sarah-spiekermann-digitalisierung-entzweit-uns-macht-uns-suechtig-und-passiv/24382456.html

Universitätsprofessor Dr. Klaus Mainzer der TU-München zum Thema "Natürliche und Künstliche Intelligenz - wann übernehmen die Maschinen?"

https://youtu.be/L8ab3b1zzms

Quellverweise zur Beschleunigung des digitalen Wandels/Transformationsprozesses:

Umgang von Unternehmen mit KI:

https://www.handelsblatt.com/adv/newrealities/kuenstliche-intelligenz-wie-unternehmenslenker-verantwortungsvoll-mit-ki-umgehen/24260170.html

Erster kommerziell nutzbarer Quantencomputer von IBM:

https://t3n.de/news/ibm-praesentiert-quantencomputer-1136607/

Quantencomputer von Google:

https://www.zeit.de/digital/datenschutz/2019-09/quantencomputer-google-technik-fortschritt-supercomputer/komplettansicht

https://pastebin.com/RfUMXJZE

Hinweise:
Die Liste erhebt keinen Anspruch auf Vollständigkeit.
Sie dient in erster Linie als Orientierungshilfe! Weitere Informationen zu Digitalisierung, IT-Sicherheit, IT-Datenschutz, IT-Haftpflicht, IT-Recht, Webseitenverschlüsselung, etc. auf www.webservice-schmitz.de

Umkehrung des Gesetzes der Thermodynamik:

https://www.scinexx.de/news/technik/physiker-kehren-die-zeit-um/

Teleportation von Quantenbits:

https://www.scinexx.de/news/technik/physiker-teleportieren-quantenoperation/

Quantenwirtschaft – neue Technologie durchdringt Wirtschaft:

https://www.handelsblatt.com/arts-und-style/literatur/buchtipp-quantenwirtschaft-gluckseligkeit-statt-konsumstreben-ein-neues-betriebssystem-fuer-die-wirtschaft/24469968.html

Forschung und Entwicklung zu Mensch-Maschine-Schnittstellen:

https://www.humanbrainproject.eu/en/

https://www.it-business.de/mensch-maschine-interaktion-via-gedankenuebertragung-a-813626/

https://www.handelsblatt.com/technik/digitale-revolution/digitale-revolution-wir-werden-irgendwann-alle-ablaeufe-im-menschlichen-gehirn-algorithmisch-fassen-koennen/24440082.html

Facebook-Entwicklerteam arbeitet an Hirn-Computer-Schnittstelle:

https://www.computerwoche.de/a/facebook-bastelt-an-hirn-computer-schnittstelle,3330572

Elon Musks Firma „Neuralink“ arbeitet an BCIs – Brain-Computer-Interfaces:

https://www.neuralink.com/

https://www.handelsblatt.com/technik/forschung-innovation/neuralink-elon-musk-will-hirn-vernetzung-mit-computern-bereits-2020-testen/24669968.html

„Brainhacking“:

https://www.handelsblatt.com/arts_und_style/kunstmarkt/buchtipp-mein-kopf-gehoert-mir-brainhacking-neurokapitalismus-das-21-jahrhundert-wird-das-jahrhundert-des-gehirns-sein/21064270.html

https://www.derbrutkasten.com/brain-hacking-technologie-startups/

Künstliche neuronale Netze:

https://de.wikipedia.org/wiki/Künstliches_neuronales_Netz

Neuromorphe Chips:

https://tu-dresden.de/tu-dresden/newsportal/news/computer-lernen-das-lernen

"BDA - Brain Data Agreement"...?

Ist dann die Zeit gekommen, um über ein "BDA - Brain Data Agreement" zu entscheiden, auch um eine DSGVO hier zu ergänzen...? Nicht nur das Strategiepapier der Bitkom wirft hier Fragen zum Umgang und Implementierung u.a. von Ethik bei der Entwicklung von künstlicher Intelligenz auf, sondern auch Fragen hinsichtlich der stetig weiter entwickelnden Kybernetik...!

https://www.aerztezeitung.de/medizin/krankheiten/neuro-psychiatrische_krankheiten/article/955099/hirn-computer-schnittstelle-neurowissenschaftler-fordern-umfassenden-datenschutz.html

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

https://www.spektrum.de/lexikon/neurowissenschaft/kybernetik/6831

https://www.heise.de/newsticker/meldung/Missing-Link-Die-Kybernetik-schlaegt-zurueck-4036974.html

https://blogs.hu-berlin.de/muwimewi/2018/04/17/18-19-04-18-gemeinsame-konferenz-der-humboldt-universitaet-und-der-technischen-universitaet/

9. 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, Multimediareceivers, Alarmanlage, etc.) und weiteren Schutzmechanismen abhängig (z.B. **Zwei-Faktor-Authentifizierung**, **Authentifikations-App**, 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?

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

10. Orientierungshilfen

Für größere Einrichtungen und Unternehmen sind Systemhäuser empfehlenswert, da hier über die gesamte Palette der Leistungen und Service von IT-Sicherheit, Datenschutz, Netzwerktechnik, Qualifikation, Datensicherung, Software und Hardware, Unterstützung angeboten werden kann.

Dies ist insofern sinnvoll, als eine komplette schlüssige Lösung insbesondere für Wirtschaftsbetriebe einen echten Mehrwert an IT-Sicherheit, Datenschutz, Stabilität, Ausfallsicherheit, Recovery Management bietet.

Die nachfolgenden Informationen sind erfahrungsgemäß relevant für Privatpersonen und bei der Verwendung in kleinen Netzwerken von gemeinnützigen Einrichtungen und Kleinunternehmen.

Auf der Webseite www.av-test.org werden Testergebnisse vom renommierten Magdeburger Testinstitut zu zertifizierter Sicherheitssoftware und Technik veröffentlicht.

Beachten Sie folgende Punkte bei der Einrichtungen und Konfiguration Ihres Netzwerks:

- Passwortrichtlinien/Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik beachten: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html
- Umgang mit Passwörtern: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html
- **Wo verfügbar, einsetzen: Zwei-Faktor-Authentifizierung. Wenn nicht verfügbar, Sicherheitsoptionen des Logins prüfen!** https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/2FA-zwei-faktor-authentisierung.html
- Weitere Informationen vom BSI: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html
- Ihr Router wird vom Hersteller/Provider mit Firmware unterstützt. **Ist dies nicht mehr der Fall, ist ein neuer Router angeraten!** (Hier bietet sich auch gleich eine Tarifprüfung an, z.B. über www.check24.de, www.verivox.de.)
- Router regelmäßig auf aktuelle Firmware prüfen.
- Router: Sicheres Anmeldepasswort für Anmeldung am Router wählen: Passwortrichtlinien beachten!
- Router: Sicheres WLAN-Passwort wählen: Passwortrichtlinie beachten!
- Router: Unnötige Dienste abschalten.
- Netzwerkgeräte/Iot-Geräte: Jedes Gerät sicher konfigurieren mit jeweils individuellem Passwort (Passwortrichtlinie beachten!) und regelmäßig auf aktuelle Firmware prüfen. Nur (sicherheits-)zertifizierte Geräte einsetzen. Ist hier ein Gerät nicht sicher besteht Gefahr für das gesamte Netzwerk!
- Betriebssysteme, Treiber und Programme aktuell halten und regelmäßig auf Updates prüfen.
- Alle Betriebssysteme - vor allem bei Windows: Nicht als Administrator das Internet nutzen. Hierfür ein "Standardkonto" als Benutzer anlegen und auch mit einem Passwort schützen (Passwortrichtlinie beachten!).
- Sicherheitsprogramme: Auch hier ein separates Passwort (Passwortrichtlinie beachten!) einrichten und die Konfiguration auf Sicherheitseinstellungen und Funktionen prüfen. Ein EICAR-Test zeigt, ob der Viren-Scanner auch anschlägt!
- Weitere Informationen auf der Webseite unter www.webservice-schmitz.de/it-sicherheit/..!