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 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

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

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

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 "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....!“

Cybersecurity-Test zur Feststellung über geeigneten Einstiegskurs:
https://www.eval-u.de/cybersecurity

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

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?

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

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 .

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

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

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

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

Welche persönlichen Daten sind besonders gefährdet?

https://datenklau.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://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!)**
  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-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/

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 – 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/

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/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

Webseiten verschlüsseln und Schutz vor Angriffen

Warum sollten Webseiten grundsätzlich verschlüsselt werden?

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

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

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: 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/

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

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

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

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

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

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

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

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

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

Für Unternehmen zusätzlich:

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

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

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/

Kaspersky-Security-Awareness (ASAP)
Interaktive Schulungsprogramme zum Aufbau der Sensibilität der Cyberumgebung für alle Unternehmensebenen
https://www.kaspersky.de/enterprise-security/security-awareness

Grundschutzprofile für Handwerksbetriebe, Handwerkskammern, IT-Dienstleister…
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/Profile/itgrundschutz-Profile_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:

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

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

Bei DSGVO-Verletzung - Abmahngefahr für Handwerksbetriebe:
https://www.handwerk-magazin.de/so-sollten-handwerker-auf-dsgvo-abmahnungen-reagieren/150/381/372827

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, 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:

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

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