Leitfaden zur Cybersicherheit

Barrierefreie Fassung

Cybersicherheitsagentur Baden-Württemberg (CSBW)

Mit uns. Mit Ihnen. Mit Sicherheit.

Inhalt

Cybersicherheit. Gemeinsam mit Ihnen

Cyberangriffe nehmen konstant zu. Die daraus resultierenden Schäden sind oft verheerend und existenzbedrohend. Im Zuge dieser Entwicklung stellt sich daher nicht die Frage, ob man Opfer einer Cyberattacke wird, sondern wann es passiert und wie gut man darauf vorbereitet ist.

Neben geplanten Angriffen, die strategisch vorbereitet und beispielsweise über gezielte Phishing-E-Mails initiiert werden, existieren auch weniger zielgerichtete Betrugsversuche, die wahllos an eine große Personengruppe versendet werden und somit jeden treffen können. Eine grundlegende Absicherung der IT-Systeme ist daher sowohl im beruflichen als auch im privaten Umfeld zwingend notwendig.

Doch auch die beste Absicherung der Systeme ist wirkungslos gegen den Faktor Mensch.

Informationssicherheit setzt daher ein Ineinandergreifen von technischen Maßnahmen und sicherheitsorientiertem Handeln voraus und muss als ganzheitliches Thema begriffen werden.

Um ein angemessenes Schutzniveau zu erreichen, müssen Anwenderinnen und Anwender fortwährend in sicherheitsbewusstem Handeln geschult und für Bedrohungen aus dem Cyberraum sensibilisiert werden.

Die Cybersicherheitsagentur Baden-Württemberg unterstützt das Land und seine Bürgerinnen und Bürger auf dem Weg zu mehr Cybersicherheit und gibt ihnen das notwendige Wissen an die Hand, um für den Ernstfall vorbereitet zu sein.

Prävention ist der beste Schutz gegen Cyberangriffe.

Mit uns. Mit Ihnen. Mit Sicherheit.

CSBW Cybersicherheitsagentur Baden-Württemberg

PASSWORT: Das Geheimnis guter Passwörter? Einzigartig, lang und komplex

Passwörter sind die Schlüssel zu unseren Daten und damit zu unserem digitalen Leben.
Schützen Sie Ihre beruflichen und privaten Daten zuverlässig vor ungewollten Zugriffen, indem Sie für jeden Ihrer Zugänge ein einzigartiges und komplexes Passwort verwenden.

Grundsätzlich gilt:

- Je länger und komplexer ein Passwort ist, desto schwieriger ist es zu knacken.
- Passwörter nicht notieren, nicht weitersagen und stets unbeobachtet eingeben.
- Doppelte, schwache oder geleakte (veröffentlichte) sowie Standard-Passwörter unverzüglich durch neue starke Passwörter ersetzen.

Empfehlungen:

- **Kombination verschiedener Zeichentypen**
  Nutzen Sie bei der Erstellung eines Passworts Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, um ein möglichst komplexes Passwort zu generieren.
- **Passwort-Manager nutzen**
  Ein Passwort-Manager ist eine Software, die Sie dabei unterstützt, komplexe Passwörter zu generieren und zu verwalten. Sie müssen sich nur noch ein komplexes Master-Passwort merken, mit dem Sie auf alle Ihre Passwörter zugreifen können.
- **Zwei-Faktor-Authentifizierung verwenden**
  Durch die Kombination von zwei unterschiedlichen Komponenten, wie PIN + EC-Karte, entsteht bei der Zwei-Faktor-Authentifizierung ein

Praxis-Tipps

Aus den Anfangsbuchstaben eines Satzes kann ein einprägsames Passwort erstellt werden: CSBW: Prävention ist der beste Schutz gegen Cyberangriffe! CSBW:PidbSgC!

Zusätzlich Buchstaben durch Sonderzeichen oder Zahlen ersetzen z.B. S=$, B=8: C$8W:Pidb$gC!

Passwort-Manager:

Einfacher geht es mit einem Passwort-Manager. Er generiert sichere Passwörter und speichert diese in einer Datenbank ab.

SICHERHEITSVORFALL: Sicherheitsvorfall im Büro? Jede Minute zählt!

Besteht der Verdacht auf einen Sicherheitsvorfall im Arbeitsumfeld, muss dieser schnellstmöglich gemeldet werden, um im Ernstfall Schlimmeres verhindern zu können. Informieren Sie unverzüglich die beauftragte Person für Informationssicherheit, die IT-Abteilung oder die Geschäftsleitung. Oftmals existieren auch IT-Notfallpläne, in denen geregelt ist, welche Personen zu welchem Zeitpunkt über den Vorfall in Kenntnis gesetzt werden müssen.

Schutzziele der Informationssicherheit:
Die wichtigsten Schutzziele der Informationssicherheit sind **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** von Informationen. Die Aufgabe der Informationssicherheit ist es, diese für alle Daten und Systeme geltenden Grundwerte angemessen zu schützen.

Ein Sicherheitsvorfall liegt vor, wenn mindestens eine der folgenden Situationen eingetreten ist:

- Die **Vertraulichkeit** von Daten ist verletzt, weil z.B. unberechtigte Personen Zugriff darauf haben.
- Die **Integrität** von Daten ist verletzt, weil z.B. Daten unberechtigt und unbemerkt verändert wurden.
- Die **Verfügbarkeit** von Daten ist gestört, weil z.B. ein System ausgefallen ist.

Generell gilt:

- Umgehend bei der IT-Abteilung melden, wenn sich Geräte wie Computer oder Handys anders verhalten als sonst.
- Je früher der Vorfall gemeldet wird, desto höher ist die Chance, schwerwiegende Schäden zu verhindern.
- Im Verdachtsfall besser einmal zu viel, als zu wenig melden: **Nur Mut!**

Am unteren Rand der Seite befindet sich zudem der Hinweis auf die Cyber-Ersthilfe BW der Cybersicherheitsagentur Baden-Württemberg:

Die **Cyber-Ersthilfe BW der Cybersicherheitsagentur** ist die zentrale und kostenfreie Kontakt- und Meldestelle für Cybersicherheitsvorfälle in Baden-

Württemberg. Unter der Telefonnummer **0711-137-99999** erhalten Sie von uns rund um die Uhr eine Ersteinschätzung sowie individuelle Handlungsoptionen zu Ihrem Verdachtsfall.

Titel des Infokastens: Mögliche Anzeichen für eine Cyberattacke

- Programme starten und beenden selbstständig.
- Dateien können nicht mehr verändert oder gespeichert werden.
- Die Darstellung der Programm-Icons ist verändert.
- Die Startseite im Webbrowser verändert sich.
- Das Webcam-Licht leuchtet trotz ausgeschalteter Kamera.
- Rechner fährt von selbst herunter.

Hinweis: Nicht jedes der oben genannten Symptome ist zwangsläufig auf eine Cyberattacke zurückzuführen.

HOMEOFFICE: Sicher von Zuhause aus arbeiten. Risikofaktoren erkennen und handeln

Das Arbeiten im Homeoffice ist inzwischen für viele zur Normalität geworden. Im Gegensatz zur geschützten Büroumgebung sind wir in den eigenen vier Wänden selbst dafür verantwortlich, dass der Schutz von Informationen gewährleistet ist.

Mit folgenden Handlungsempfehlungen lassen sich potenzielle Gefahren eingrenzen:

- Fenster und Türen schließen und nicht über Lautsprecher telefonieren, da dienstliche Gespräche nicht für fremde Ohren bestimmt sind.
- Papierunterlagen stets verschlossen aufbewahren.
- Informieren Sie Ihr direktes Umfeld, dass zufällig Mitgehörtes vertraulich behandelt werden muss.
- Geräte mit Sprachassistenz während der Arbeit ausschalten und aus dem Zimmer entfernen.
- Private Geräte nicht mit dem Geschäftsrechner verbinden und das Diensthandy nicht an den privaten Computer anschließen.
- Den Bildschirm beim Verlassen des Arbeitsplatzes sperren:
  Tastenkombination:
  Für Windows-Geräte: Windowstaste + L
  Für Apple-Geräte: Ctrl + Befehlstaste + Q
  Dies verhindert, dass unberechtigte Personen Einblick erhalten oder Haustiere versehentlich Daten löschen oder versenden.
- Vertrauliche Dokumente im Dienstgebäude und nicht im Hausmüll entsorgen.
- Ausgediente IT-Geräte wie USB-Sticks an die IT-Abteilung zurückgeben

Praxis-Tipps

Die **optimale Konfiguration des Home-Routers** erhöht die Sicherheit des Heimarbeitsplatzes signifikant, beispielsweise durch die Einrichtung eines Gast-Netzwerkes.

Ein **VPN (Virtual Private Network)** hilft dabei, im Internet anonym zu bleiben, die Privatsphäre zu wahren und geschützt auf Netzwerke zuzugreifen.

Software- und Virenscanner-Updates sollten zeitnah installiert und das System regelmäßig einem **Virenscan** unterzogen werden.

MOBILES ARBEITEN: Weit entfernt von Sicherheit? Worauf Sie unterwegs achten sollten

Auf Dienstreisen oder beim Arbeiten von unterwegs ist besondere Vorsicht im Umgang mit Dienstgeräten und vertraulichen Informationen geboten. Neugierige Mitmenschen, Diebe, öffentliche WLAN-Zugänge und verloren gegangene Geräte – die Gefahren sind vielfältig und stets präsent.

Unterwegs gilt es Folgendes zu beachten:

In der Öffentlichkeit

- Blickschutzfolie nutzen oder mit dem Rücken zur Wand sitzen, um ungewollte Einblicke auf den Bildschirm zu vermeiden.
- Ein Headset nutzen, möglichst keine sensiblen Informationen laut aussprechen oder das Telefonat auf einen späteren Zeitpunkt verschieben.
- Papierdokumente sind besonders kritisch, da diese unverschlüsselte Informationen enthalten und leicht eingesehen werden können.
- In manchen Situationen ist es ratsam, das Arbeiten auf einen späteren Zeitpunkt zu verschieben. Ob die Situation ein risikoarmes Arbeiten zulässt, obliegt der persönlichen Einschätzung.

Öffentliche WLAN-Netzwerke

- Dritte können über öffentliche WLAN-Netzwerke Zugriff auf übermittelte Daten erlangen oder Malware einschleusen. Um dies zu vermeiden, sollte möglichst auf eine Nutzung verzichtet und das automatische Verbinden mit WLAN-Netzwerken auf den Geräten deaktiviert werden.
- Nur SSL-verschlüsselte Webseiten besuchen. Diese beginnen mit der Zeichenfolge http**s**://.
  Beispiel: https://cybersicherheit-bw.de
- Auf dienstliche Daten nur mit VPN-Verbindung zugreifen.

Praxis-Tipps

Grundsätzlich alle möglichen Schutzmaßnahmen gegen fremde Zugriffe aktivieren, wie z.B. Laptop und Handy mit Passwort oder biometrischem Merkmal sichern.

Sollte etwas verloren gehen, umgehend die IT-Abteilung und die Führungskraft informieren, um Zugangsmedien und Geräte deaktivieren zu lassen.

Vor Reisebeginn sicherstellen, dass Software- Updates installiert sind und das Betriebssystem auf dem neuesten Stand ist.

E-MAIL: Unbekannter Absender? Richtiger Umgang mit Phishing-E-Mails

E-Mails sind ein beliebtes Medium für Angreifende, um Schadsoftware zielgerichtet in Systeme einzuschleusen. Schätzungen zufolge werden mehr als 80 Prozent aller erfolgreichen Angriffe per E-Mail initiiert. Besonders Phishing-E-Mails, die dazu verleiten, auf Links zu klicken oder Anhänge zu öffnen, sind ein ernst zu nehmendes Sicherheitsrisiko.

Folgende Tipps können dabei helfen, Angriffe zu erkennen und erfolgreich abzuwehren:

- Bei unbekannten Absenderadressen ist grundsätzlich besondere Vorsicht geboten. Links und Anhänge sollten keinesfalls ungeprüft geöffnet werden.
- Aber auch E-Mails von bekannten Absendern sollten stets überprüft werden, wenn der Inhalt nicht zum Absender passt oder die Herausgabe von sensiblen Informationen gefordert wird.
- Oftmals wird mit Konsequenzen gedroht oder dringender Handlungsbedarf vorgetäuscht. Lassen Sie sich nicht unter Druck setzen und zu schnellen Handlungen verleiten.
- Melden Sie die E-Mail beim geringsten Verdacht der zuständigen Stelle und folgen Sie deren Anweisungen. Das kann beispielsweise die beauftragte Person für Informationssicherheit oder die IT-Abteilung sein.
- Die in der E-Mail angegebenen Kontaktdaten sind in vielen Fällen ebenfalls gefälscht und sollten nicht genutzt werden, um mit dem Absender in Kontakt zu treten. Es ist ratsam, die offiziellen Kontaktdaten im Internet zu recherchieren und den angeblichen Absender über den Phishing-Versuch zu informieren.
- Aufforderungen, beispielsweise zur Eingabe von Zugangsdaten, sollten nicht befolgt werden. Stattdessen sollte die entsprechende Webseite über den üblicherweise genutzten Zugangslink geöffnet werden, um zu prüfen, ob tatsächlich Handlungsbedarf besteht.

Titel des Infokastens: „Besonders wichtig!“

E-Mails vor dem Öffnen in der Vorschauansicht überfliegen.

Phishing-E-Mails sind mittlerweile weitestgehend fehlerfrei und kaum von echten E-Mails zu unterscheiden.

Immer öfter wird künst- liche Intelligenz (KI) bei der Erstellung von Phishing- E-Mails eingesetzt, um authentische Texte zu generieren.

Phishing findet über alle textbasierten Nachrichtenkanäle statt. Daher muss auch bei Messenger- Diensten und per SMS mit Angriffen gerechnet werden.

ARBEITSPLATZ: Risiken im Büro: Passwortzettel, unbekannte Personen, nicht aufgeräumte Schreibtische

Auch im Büro sind wir nicht völlig sicher vor Angriffen. Diese können entweder auf digitalem Wege erfolgen oder die angreifende Person versucht sich Zugang zum Bürogebäude zu verschaffen. Achten Sie daher stets auf Ihre Umgebung, identifizieren Sie fremde Personen und helfen Sie aktiv mit, Ihren Arbeitsplatz vor Angriffen zu schützen.

Empfohlene Schutzmaßnahmen:

- Bildschirm so positionieren, dass er vor ungewollten Einblicken geschützt ist oder eine Blickschutzfolie verwenden.
- Beim Verlassen des Arbeitsplatzes stets den Bildschirm sperren.
- Keine Dokumente im Drucker liegen lassen und nach Möglichkeit nur mit Transponder bzw. Zugangsdaten drucken.
- Unbekannte Datenträger wie USB-Sticks oder externe Festplatten keinesfalls an den Dienstrechner anschließen.
- Webcam des Computers bei Nichtbenutzung abdecken, beispielsweise mit einem Webcam-Cover.
- Beschriftete Tafeln, Flipcharts oder Whiteboards vor dem Verlassen des Raums vollständig reinigen.

Clean Desk-Prinzipien

Nicht aufgeräumte Schreibtische stellen ein Sicherheitsrisiko dar. Daher gilt:

- Vertrauliche Informationen stets einschließen.
- Passwörter niemals notieren und personenbezogene Daten nicht offen liegen lassen.
- Datenträger an einem sicheren Ort verwahren.

Übrigens: Die Clean-Desk-Prinzipien lassen sich auch problemlos auf dem Desktop anwenden.

Besucherinnen und Besucher

- Keine Personen ins Gebäude lassen, die sich nicht als berechtigt identifizieren bzw. ausweisen können.
- Fremde Personen zum Empfang geleiten.
- Besucherinnen und Besucher stets begleiten

Besonders wichtig!

Personenbezogene Informationen sind für Kriminelle äußerst wertvoll, um Angriffe gezielt zu planen und durchzuführen. Daher sollte mit Details zu internen Strukturen sowie den Urlaubs- oder Abwesenheitszeiten vorsichtig umgegangen werden.

Lassen Sie auch keine scheinbar unbedeutenden Informationen wie Telefon-nummern oder Netzwerkinformationen auf Ihrem Schreibtisch zurück.

Über Posts in sozialen Medien können Unbefugte sehr einfach an vertrauliche Informationen gelangen. Daher niemals Fotos vom Arbeitsplatz oder -umfeld in sozialen Netzwerken posten

INTERNET: Internet und Cloud. Fluch und Segen zugleich?

Das Internet ist das Tor zur Welt und eröffnet ungeahnte Möglichkeiten. Dies gilt auch für Cyberkriminelle, die im Netz ihr Unwesen treiben. Versteckte Schadsoftware, Trojaner oder Ransomware: die Bandbreite an Angriffsvektoren ist groß. Auch bei der Nutzung von Cloud- Diensten ist Vorsicht geboten, da sensible Daten im Netz besonderen Gefahren ausgesetzt sind.

Internet

- Regelmäßige Updates des Betriebssystems, des Browsers und der Antivirensoftware schützen vor Angriffen und schließen potenzielle Einfallstore.
- Ein SSL-Zertifikat zeigt an, dass es sich um eine verschlüsselte und damit sichere Verbindung handelt. Erkennbar ist das durch ein Schloss-Symbol in der Adressleiste und die Kennung „https“:
  Beispiel: https://cybersicherheit-bw.de
- Ungewöhnliche Website-Endungen, wie .ru, .pl oder .to, oder fehlerhafte Orthografie und Grammatik können Anzeichen für eine Fake-Website sein.
- Ein VPN (Virtual Private Network) hilft im Netz anonym zu bleiben und die Privatsphäre zu schützen
- Um die Nachverfolgung der Online-Aktivitäten zu verhindern, wird empfohlen, Cookies sowie Browserverläufe zu löschen und das Tracking in den Browsereinstellungen zu deaktivieren.

Cloud

- Es sollten nur die von Ihrer Institution freigegebenen Cloud-Services genutzt werden.
- Dienstliche Daten sollten nicht über freie Sharing-Anbieter getauscht werden. Welche Plattformen für den Datentransfer freigegeben sind, kann bei der IT-Abteilung in Erfahrung gebracht werden.
- Es wird empfohlen, private Daten zu verschlüsseln, bevor sie in der Cloud abgelegt werden.

Gut zu wissen:

Sprach-Übersetzungsdienste sind eine große Hilfe und erleichtern vielerlei Aufgaben. Vor der Nutzung sollte jedoch mit den Vorgesetzten geklärt werden, ob diese Dienste verwendet werden dürfen. Darüber hinaus sollten grundsätzlich keine vertraulichen Informationen in die Übersetzung gegeben und jeder zu übersetzende Inhalt anonymisiert werden.

Viele Suchmaschinen speichern und werten Nutzungsinformationen wie personenbezogene Daten und IP-Adressen aus. Um Datenspuren im Netz zu reduzieren, empfiehlt sich der Wechsel zu einer Suchmaschine, die Ihre Privatsphäre berücksichtigt.

SOCIAL ENGINEERING: Social Engineering. Manipulation, Täuschung und Betrug

Beim Social Engineering geben sich Angreifende als vertrauenswürdige Personen aus, die angeblich dazu berechtigt sind, Informationen von Ihnen zu erfragen. Die Opfer handeln im guten Glauben, das Richtige zu tun. Daher ist diese Betrugsmasche weiterhin sehr erfolgreich. +

Social Engineering kann auf verschiedenen Kanälen stattfinden: persönlich, am Telefon, via Messenger-Dienst oder in sozialen Netzwerken.

Taktiken und Strategien:

- Hilfsbereitschaft, Mitleid oder Angst: Angreifende nutzen Techniken der sozialen Manipulation, um bei der Zielperson bestimmte Emotionen auszulösen oder sie zu unüberlegten Handlungen zu bewegen.
- Fremde oder nicht eindeutig identifizierbare Personen fragen nach vertraulichen Informationen, internen Abläufen oder Zugangsdaten und drohen mit Konsequenzen, wenn die geforderten Informationen nicht preisgegeben werden.
- Selbst scheinbar unbedeutende Informationen wie Telefonnummern, Adressen, Namen oder Abwesenheitszeiten können einem Social Engineer helfen, einen Angriff zu planen und durchzuführen.

Richtig reagieren:

- Ist die Person nicht eindeutig identifizierbar, sollten keine Informationen herausgegeben werden.
- Im Zweifelsfall die Unterhaltung freundlich beenden und anschließend mit der Führungskraft Rücksprache halten.

Praxis-Tipps:

Oftmals wird ein außergewöhnliches Szenario inszeniert, das die Herausgabe eines Passworts oder die Installation einer Software erforderlich macht. In diesem Fall nicht vorschnell handeln und Software-Installationen immer mit der IT-Abteilung abklären.

Vor allem in sozialen Netzwerken und Messenger-Diensten geben sich Angreifende gerne als Freunde oder Familienmitglieder aus. Mit persönlichen Fragen, die nur von der realen Person beantwortet werden können, lässt sich die Identität verifizieren.

VIDEOKONFERENZEN: Videokonferenzen. „…dann teile ich mal meinen Bildschirm“

Videokonferenzen ermöglichen uns, auch über Distanzen im Team zusammenzuarbeiten, Daten zu teilen und Inhalte zu präsentieren. Vor allem beim Teilen des Bildschirms (Screensharing) sollte man darauf achten, dass keine sensiblen Informationen sichtbar sind. Nicht alle Videokonferenzsysteme sind gleichermaßen sicher und innerbetrieblich zur Nutzung freigegeben. Welche Konferenzsysteme erlaubt sind und wie mit Einladungen zu nicht zugelassenen Konferenzsystemen umgegangen werden sollte, kann in der Regel die Führungskraft beantworten.

Generell gilt:

- Nach Möglichkeit einen virtuellen Hintergrund oder Weichzeichner verwenden, um die eigene Privatsphäre zu schützen.
- Sprachassistenz-Systeme können mithören. Deshalb sollten diese während der Arbeit ausgeschaltet und aus dem Büro entfernt werden.
- Teilnehmende ohne eingeschaltete Kamera und per Telefon teilnehmende Personen müssen sich zu Beginn identifizieren.

Beim Screensharing gilt:

- Sensible Informationen könnten von anderen eingesehen oder mit Screenshots festgehalten werden.
- Keine Passwörter eingeben, während der Bildschirm geteilt wird.
- Nicht benötigte Tabs und den Passwort-Manager vor dem Screensharing schließen.
- Pop-Up-Benachrichtigungen von E-Mail- Programmen, Konferenzsystemen und Messenger-Diensten deaktivieren.

Titel des Infokastens: Praxis-Tipps:

Viele Videokonferenzsysteme bieten die Möglichkeit, Unterhaltungen aufzuzeichnen. Vor der Aufzeichnung sollte unbedingt die Einwilligung aller Betroffenen eingeholt und über den Zweck der Aufzeichnung aufgeklärt werden. Zudem muss

gewährleistet sein, dass die Aufnahmen sicher verwahrt und nach Erfüllung ihres Zweckes ordnungsgemäß gelöscht werden.

In den Einstellungen sollten alle nicht benötigten Tracking-, Protokoll- und Aufzeichnungs-Funktionen sowie die Funktion „Nutzung der Daten zur Verbesserung der Dienste“ deaktiviert werden.

Glossar

A

Antivirensoftware
Computersoftware, die Schadprogramme wie Viren, Trojaner und Malware erkennt, blockiert und entfernt, um die Sicherheit des Computers und der darauf gespeicherten Daten zu gewährleisten.

B

Betriebssystem
Ein Betriebssystem umfasst und verwaltet alle grundlegenden Hardware-und Softwarekomponenten, die den Betrieb des Systems steuern und überwachen.

Blickschutzfolie
Eine dünne, transparente Folie, die auf den Bildschirm eines Geräts wie einem Computer oder Smartphone aufgebracht wird. Damit werden unerwünschte Einblicke von der Seite oder von oben verhindert.

Browser
Softwareanwendung, die es ermöglicht, Webseiten und Webinhalte im Internet anzuzeigen und mit ihnen zu interagieren.

Browserverläufe
Chronologische Auflistung der besuchten Webseiten und Suchanfragen, die im Hintergrund automatisiert von einem Webbrowser erfasst werden.

C

Clean-Desk-Prinzip
Prinzip des aufgeräumten Arbeitsplatzes. Vertrauliche Dokumente und Gegenstände werden stets weggeräumt. Dadurch wird verhindert, dass Unbefugte an vertrauliche Informationen gelangen.

Cloud/Cloud Computing

Cloud Computing, oftmals als Cloud abgekürzt, ist ein Modell, das es erlaubt, Computing-Ressourcen (z.B. Datenbanken, Server, Speicher) über das Internet abzurufen. Aus Nutzersicht ist es damit bspw. möglich, Fotos oder Dateien in eine Cloud auszulagern und abzurufen.

Cloud/Cloud-Dienst

Internet-Service, der es ermöglicht, Daten und Anwendungen auf entfernten Servern zu speichern, zu verwalten und darauf zuzugreifen, anstatt diese lokal auf dem eigenen Rechner zu speichern.

Cookies

Cookies sind kleine Textdateien, die von einer Website auf dem jeweiligen Computer oder Gerät gespeichert werden und Informationen über Interaktionen mit der Website enthalten. Es gibt verschiedene Formen von Cookies, die einen unterschiedlichen Zweck erfüllen. Neben technischen Cookies, die die Funktionalität einer Webseite garantieren, existieren auch Werbe- und Analyse-Cookies, um das Nutzerverhalten zu analysieren und dementsprechend Angebote zu steuern.

Cyber

Der Begriff „Cyber“ bezieht sich auf alles, was mit Computern, dem Internet und digitalen Technologien in Verbindung steht. Er wird eingesetzt, um allgemeine Themen wie Sicherheit und Kriminalität spezifisch auf den digitalen Raum zu beziehen (bspw. Cybersicherheit und Cyberkriminalität).

Cyberangriff/Cyberattacke

Kriminelle Handlung, bei der in ein Computersystem oder ein Netzwerk eingedrungen wird, um z.B. Daten zu stehlen, zu manipulieren oder zu beschädigen.

D

Datenspuren
Digitale Informationen, die von einem Benutzer oder einer Benutzerin im Internet hinterlassen werden, wie z.B. Suchanfragen, besuchte Webseiten, Online-Käufe oder Social-Media-Interaktionen.

Datenträger
Physisches Medium zur Speicherung und Übertragung von Daten. Beispiele für Datenträger sind Festplatten, USB-Sticks, CD-ROMs, DVDs, Blu-ray-Discs und Speicherkarten.

F

Fake-Website
Gefälschte Website, die das Erscheinungsbild einer originalen Website imitiert. Ziel ist es, eingegebene Login-Daten bzw. persönliche Informationen abzugreifen oder Geld für Produkte und Dienstleistungen zu kassieren, ohne die entsprechende Gegenleistung zu erbringen.

G

Gastnetzwerk
Separates WLAN-Netzwerk, das parallel zum Hauptnetzwerk eingerichtet wird. So können Gäste dennoch über das WLAN auf das Internet zugreifen und das Hauptnetzwerk bleibt geschützt.

H

Hacker/Hackerin
Der Begriff Hacker (auch Computer- Hacker) bezeichnet zumeist Personen oder Personengruppen, die unautorisiert in fremde IT-Systeme eindringen. Sie verfolgen das Ziel, Systeme anzugreifen, zu manipulieren oder zu infiltrieren, um sich selbst zu bereichern oder Chaos zu stiften.
Es gibt jedoch auch Hacker, die gute Absichten verfolgen: Sie decken Schwachstellen auf und melden diese bei offiziellen Stellen oder führen legale Tests an Systemen durch, um Einfallstore zu identifizieren.

Home-Router
Ein Router ist ein Hardwaregerät, das als Verbindungspunkt zwischen einem lokalen Netzwerk und dem Internet dient. Der Router zuhause wird als Home-Router bezeichnet.

https
HTTPS (Hypertext Transfer Protocol Secure) ist ein Protokoll zur sicheren Übertragung von Daten im Internet. Im Gegensatz zu HTTP (Hypertext Transfer Protocol) ist die Verbindung bei der Nutzung von HTTPS verschlüsselt und die gesamte Kommunikation zwischen Nutzendem und Server von außen nicht einsehbar. Das ist vor allem dann wichtig, wenn vertrauliche Informationen verarbeitet werden.

I

Informationssicherheit
Informationssicherheit hat das Ziel, Informationen vor unbefugtem Zugriff, vor Veränderungen oder vor Vernichtung zu schützen. Zeitgleich gewährleistet sie die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen.

Internet
Weltweites Netzwerk miteinander verbundener Computer, über das Informationen und Daten ausgetauscht und aufgerufen werden können.

IP-Adresse
Eine IP-Adresse ist eine eindeutige numerische Kennung, die einem Gerät zugewiesen wird, damit es in einem Netzwerk kommunizieren und eindeutig identifiziert werden kann.

ISB (Informationssicherheitsbeauftrage/r) Die mit der Informationssicherheit beauftragte Person ist für alle Fragen rund um die Informationssicherheit innerhalb einer Organisation zuständig.

IT

Die Abkürzung IT steht für Informationstechnologie. Sie umfasst die komplette elektronische Datenverarbeitung und die dafür verwendete Hard- und Software-Infrastruktur.

K

KI

KI steht für Künstliche Intelligenz und bezieht sich auf Maschinen und Systeme, die in der Lage sind, menschenähnliche Intelligenz zu zeigen. Dazu gehören Fähigkeiten wie Sinneseindrücke wahrzunehmen und darauf zu reagieren oder Informationen zu sammeln und auf deren Grundlage selbstständig Probleme zu lösen.

M

Master-Passwort

Komplexes Passwort mit einer Länge von mindestens 14 Zeichen, das benötigt wird, um auf die Datenbank des Passwort-Managers zuzugreifen. Bei Verlust des Master-Passwortes kann nicht mehr auf die im Passwort- Manager hinterlegten Passwörter zugegriffen werden.

Messenger-Dienst

Online-Dienst, mit dem Nutzende in erster Linie schriftliche Nachrichten, aber auch multimediale Inhalte (Fotos, Videos usw.) über das Internet austauschen können.

N

Netzlaufwerk

Speicherbereich auf einem entfernten Computer oder Server, der über ein Netzwerk zugänglich gemacht wird und wie ein lokales Laufwerk auf dem eigenen Computer angezeigt wird.

P

Passwort

Ein Passwort ist eine geheime Kombination aus Zeichen, Zahlen und Symbolen, die zum Schutz von Daten, Konten oder Geräten verwendet wird.

Passwort-Manager
Software, die es Benutzern ermöglicht, Passwörter zu generieren, zu speichern und sicher zu verwalten.

PC Sperren-Tastenkombination
Für Windows-Geräte: *Windowstaste* + *L*
Für Apple-Geräte: *Ctrl* + *Befehlstaste* + *Q*

Personenbezogene Daten
Informationen, die sich auf eine Person beziehen, wie beispielsweise Name, Adresse, Geburtsdatum, E-Mail-Adresse oder IP-Adresse.

Phishing
Phishing setzt sich aus den englischen Begriffen „password“ und „fishing“ zusammen (dt.: nach Passwörtern angeln) und ist eine Form des Internetbetrugs. Kriminelle geben sich am Telefon, via E-Mail und anderen textbasierten Nachrichtenkanälen als vertrauenswürdige Person oder Organisation aus. Sie versuchen durch geschickte Manipulation an vertrauliche Informationen wie Passwörter oder Kreditkartendaten zu gelangen.

PIN
Abkürzung für „Personal Identification Number“. Diese Geheimzahl wird für den Zugriff auf persönliche Konten oder Daten benötigt.

Pop-up-Benachrichtigung
Kurz am Bildschirmrand auftauchende Meldungen, die beispielsweise auf den Erhalt einer Nachricht hinweisen und eine Vorschau des Inhalts zeigen.

Post (soziale Medien)
Nachrichten oder Inhalte, die auf einer Social-Media-Plattform veröffentlicht werden.

Programm-Icons

Kleine Symbole, die Programme, Dateien und Ordner auf dem Desktop repräsentieren. Mit einem Doppelklick wird die dem Icon zugeordnete Aktion ausgeführt.

R

Ransomware
Schadsoftware, die das System infiziert und daraufhin Daten oder das System verschlüsselt. Für die Entschlüsselung wird ein Lösegeld gefordert.

S

Schadsoftware
Bösartige Software, die entwickelt wurde, um Schaden an einem Computer, Netzwerk oder anderen Geräten zu verursachen. Sie kann unautorisierte Aktivitäten und schädliche Aktionen ausführen, Daten stehlen sowie zerstören oder Systemressourcen beeinträchtigen.

Screensharing
Möglichkeit, in einer Videokonferenz den eigenen Bildschirm in Echtzeit mit anderen Personen zu teilen.

Screenshot
Bildschirmaufnahme des angezeigten Inhalts auf dem Bildschirm eines Computers oder mobilen Geräts.

Sharing-Anbieter
Unternehmen, die Plattformen bereitstellen, über die Nutzende auf eine Vielzahl von Dienstleistungen, Produkten und Ressourcen zugreifen können (bspw. zum Transfer von Daten).

Shoulder Surfing
Eine Person versucht, sensible Informationen zu stehlen, indem sie über die Schulter einer anderen Person auf deren Bildschirm schaut (z.B. in der Bahn) oder die Eingabe der PIN beim Geldautomaten beobachtet.

Social Engineering
Taktische zwischenmenschliche Beeinflussung von Personen, um diese für die eigenen Zwecke zu instrumentalisieren. Personen sollen so beispielsweise zur Freigabe von sensiblen Informationen bewegt werden. Als Social Engineer bezeichnet man die Person, die Social Engineering durchführt.

Spam
Spam bezeichnet unerwünschte und oft massenhaft versendete Nachrichten (meist per E-Mail), die in der Regel Werbung oder betrügerische Inhalte enthalten.

Sprachassistenz
Technologie, die es ermöglicht, per Sprachbefehl mit einem Computer oder einem digitalen Gerät zu interagieren, um Aufgaben auszuführen oder Informationen abzurufen.

SSL-Verschlüsselung
Bei einer sogenannten „SSL-Verschlüsselung“ (Secure Sockets Layer) wird die Verbindung zwischen einem Server und einem Client verschlüsselt, um eine sichere Kommunikation über das Internet zu gewährleisten.

SSL-Zertifikat
Ein SSL-Zertifikat (Secure Sockets Layer) ist eine digitale Datei, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wird. Sie bestätigt die Identität einer Webseite und ermöglicht eine verschlüsselte Datenübertragung zwischen Server und Browser.

Standard-Passwort
Vorgegebenes Passwort, das dazu dient, den ersten Zugriff auf ein Konto oder eine Anwendung zu ermöglichen. Benutzerinnen und Benutzer werden in der Regel aufgefordert, das Standard-Passwort nach der ersten Anmeldung zu ändern.

Suchmaschine

Anwendung, die das Internet basierend auf der eingegebenen Suchanfrage nach Webseiten und anderen digitalen Inhalten durchsucht und die relevantesten Ergebnisse liefert.

T

Tab
Ein Tab ist ein Reiter innerhalb des Webbrowsers, in dem eine Webseite geöffnet ist. Nutzende können somit mehrere Webseiten innerhalb eines Browsers öffnen und zwischen diesen beliebig navigieren.

Tracking-Funktion
Tracking-Funktionen ermöglichen es, die Internet-Aktivitäten einer Person nachzuverfolgen und zu überwachen.

Transponder
Elektronisches Gerät, das Signale empfangen und senden kann. Beispiel hierfür ist eine Zugangskarte, mit der sowohl der Drucker betätigt, als auch die Türe geöffnet werden kann.

Trojaner
Schadprogramm, das sich als legitime Software ausgibt, um unbemerkt in ein Computersystem zu gelangen und es zu manipulieren oder Daten abzugreifen.

U

Update
Aktualisierung des Betriebssystems oder von Software, um Fehler zu beheben, Sicherheitslücken zu schließen oder neue Funktionen hinzuzufügen.

USB-Stick
Kleines, tragbares Speichergerät, das an einen Computer angeschlossen werden kann, um Daten zu speichern und zu übertragen.

V

Videokonferenzsystem
Plattform oder Anwendung, die eine videobasierte Online-Kommunikation mit mehreren Personen in Echtzeit ermöglicht.

Virenscanner
Programme, die elektronische Geräte vor Schadsoftware schützen, indem sie nach Viren suchen und diese entfernen. Da täglich neue Virenvarianten hinzukommen, bietet auch der beste Virenscanner keine vollständige Sicherheit.

Virtueller Hintergrund
Digital generierter Hintergrund, der zum Schutz der Privatsphäre in Videokonferenzen genutzt werden kann. Er erfüllt dieselbe Funktion wie ein Weichzeichner, zeigt jedoch statt des verwischten Hintergrunds ein beliebiges Foto.

Vorschauansicht
Da bereits das Öffnen einer E-Mail eine Infektion des Systems zur Folge haben kann, bietet das E-Mail-Programm eine auszugsweise Vorschau des Inhalts, ohne dass die eigentliche E-Mail geöffnet wird.

VPN
Ein VPN (Virtual Private Network) ist ein virtuelles Netzwerk, das es Benutzenden ermöglicht, sicher auf das Internet zuzugreifen. Es hilft im Netz anonym zu bleiben, die Privatsphäre zu schützen und sichert die Nutzung öffentlicher WLAN-Netzwerke.

W

Webcam-Cover
Integrierter Schieberegler oder Aufkleber, der die Kamera (engl. Webcam) eines Geräts verdeckt. Das Ausspionieren über die Kamera wird somit verhindert.

Webcam-Licht
Kleines Licht neben der Webcam, das anzeigt, ob die Kamera gerade aktiv ist.

Weichzeichner

Filter, die in Videokonferenzen verwendet werden, um den Hintergrund des eigenen Videobildes zu verwischen oder zu verblassen und so die Privatsphäre zu schützen.

WLAN-Zugang
WLAN-Zugang (Wireless Local Area Network) ist ein drahtloser Zugang zu einem Netzwerk, wie z.B. dem Internet.

Z

Zugangslink
Über den Klick auf einen Zugangslink werden Nutzende zur Zieladresse weitergeleitet und erhalten Zugang zu einer Website, Datei oder Plattform (z.B. zu einer Videokonferenz).

Zwei-Faktor-Authentifizierung
Methode zur Erhöhung der Sicherheit, bei der zwei unterschiedliche Identifikationsmerkmale verwendet werden, um den Zugriff auf ein Konto zu autorisieren. Ein typisches Beispiel für eine Zwei-Faktor-Authentifizierung ist die Nutzung der Bankkarte zusammen mit der dazugehörigen PIN-Nummer, um am Bankautomaten Geld abzuheben.

Notfallkarte: Verhalten im Cybersicherheits-Notfall

IT-Notfallnummer:

Bitte Notfallnummer in das Feld eintragen:

➔ **Ruhe bewahren!**

➔ **Arbeit am betroffenen Gerät/System einstellen**

➔ **Cyberangriff melden:**
Meldung an ISB, IT-Abteilung oder Führungskraft, gemäß Ihrer IT-Notfallplanung

1. **WER meldet? (Name, Stelle etc.)**
2. **WELCHES IT-System ist betroffen?**
3. **WIE und in welchem Umfang haben Sie vor dem Vorfall am betroffenen System gearbeitet?**
4. **WAS haben Sie beobachtet? Ist Ihnen am System etwas aufgefallen?**
5. **WANN ist das Ereignis eingetreten?**
6. **WO befindet sich das betroffene Gerät/System? (Gebäude, Etage, Raum, Arbeitsplatz)**

➔ Erst nach der Meldung **weiterführende Maßnahmen in Absprache mit der zuständigen Stelle einleiten.**