Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

IT-Sicherheitsleitfaden

Inhaltsverzeichnis

1 Einleitung

1 Einleitung

Die zunehmende Digitalisierung und Vernetzung verändern jeden Bereich unseres Lebens, sie haben also einen starken Einfluss auf unser Arbeits- und Privatleben. Ein Großteil unserer alltäglichen Kommunikation findet zunehmend in den sozialen Medien und Messenger-Diensten statt.

Dabei können Sie und Ihr Umfeld im Fokus möglicher Cyber-Angriffe stehen. Das Spektrum ist hier leider weit und reicht von Beschimpfungen über Cyber-Stalking bis hin zu Erpressung mit Verschlüsselung der gesamten IT und Veröffentlichung von gestohlenen Daten.

Ihre IT-Sicherheit in allen von Ihnen genutzten digitalen Kanälen zu steigern, ist wichtig, da die Auswirkungen fehlender IT-Sicherheit Ihnen, ihrer Familie und ihrem beruflichen Umfeld signifikanten Schaden zufügen kann.

Dieses Dokument dient der Bereitstellung von konkreten Hinweisen zur Steigerung Ihrer IT-Sicherheit und damit auch dem Schutz Ihrer elektronischen Daten und Identitäten.

Es gibt Ihnen einen Überblick über mögliche Handlungsfelder und bietet Ihnen neben konkreten Empfehlungen eine Reihe von Links zu weiterführenden Informationsangeboten. Die verlinkten Inhalte wurden teilweise in anderen Kontexten erstellt und können daher in Aufmachung, Ansprache und Stil voneinander abweichen. Aufgrund der erheblichen Dynamik in diesem Bereich kann es im Einzelfall vorkommen, dass Inhalte aktualisiert werden müssen.

Diese Empfehlungen helfen Ihnen dabei, Ihr IT-Sicherheitsniveau deutlich zu steigern.

Wir bitten Sie: Machen Sie Informationssicherheit zu Ihrer Priorität!

Wir wünschen Ihnen viel Erfolg beim Umsetzen der Maßnahmen!

2 Grundlegende Sicherheitsvorkehrungen

2 Grundlegende Sicherheitsvorkehrungen

2.1 Wie Sie Ihre Geräte und Software sicher einrichten und sicher halten

2.1.1 Halten Sie Ihre Software aktuell

Ihr Betriebssystem stellt die Basis für den Betrieb aller weiteren Programme dar und ist Grundlage für nahezu sämtliche Aktivitäten auf Ihrem Rechner, wie zum Beispiel die Ausführung weiterer Dienstprogramme (Apps). Daher sollten Sie darauf achten, dass sowohl das Betriebssystem als auch die Apps aktuell sind.

Verwenden Sie also die aktuelle Version des Betriebssystems und der installierten Programme. Nutzen Sie wenn möglich die Funktion zur automatischen Aktualisierung. Ob das Betriebssystem Ihres Computers auf dem aktuellen Stand ist, erfahren Sie in den Einstellungen unter „Update“. Achten Sie auch auf Hinweise zu neuen Versionen des Betriebssystems oder von Apps, und spielen Sie diese zeitnah ein.

Zugleich besitzen moderne PC-Betriebssysteme bereits ausreichend starke Virenschutzprogramme und Firewalls, die ebenfalls über Updates des Betriebssystems mit beispielsweise aktuellen Virensignaturen versorgt werden. Ein Grund mehr, regelmäßig – bestenfalls automatisiert – Updates einzuspielen. Sollten Sie nicht sicher sein, ob Virenscanner und Firewall aktiviert sind, lohnt sich ein Blick in die Einstellungen Ihres Systems.

Deinstallieren Sie Apps, die Sie nicht länger nutzen. Je weniger Anwendungen installiert sind, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.

Weiterführende Informationen:

2.1.2 So richten Sie Ihre Benutzerkonten sicher ein

Arbeiten Sie möglichst nicht mit Administratorrechten. Zunächst haben Schadprogramme die gleichen Rechte auf dem PC wie das Benutzerkonto, über das sie auf den Rechner gelangt sind. Als Administrator haben Sie vollen Zugriff auf fast alle Bereiche Ihres PCs. Daher sollten Sie nur dann mit Administratorrechten arbeiten, wenn es unbedingt erforderlich ist. Es ist somit zu empfehlen, für die tägliche Arbeit ein Standard-Benutzerkonto zu verwenden, das lediglich über eingeschränkte Systemrechte verfügt.

Richten Sie für alle Nutzerinnen und Nutzer des PCs unterschiedliche, passwortgeschützte Benutzerkonten ein. Je nach Betriebssystem ist dies über die (System-)Einstellungen oder die Systemsteuerung möglich. Vergeben Sie für diese Konten nur Berechtigungen, die die jeweilige Nutzerin oder der jeweilige Nutzer benötigt. So werden auch private Dateien vor dem Zugriff anderer geschützt. Surfen Sie im Internet mit einem eingeschränkten Benutzerkonto und nicht in der Rolle des Administrators. Der Aufwand für die Einrichtung der Konten rentiert sich für die damit erreichte Sicherheit.

Weiterführende Informationen finden Sie unter:

Tipps zum sicheren Umgang mit Apps finden Sie unter:

2.1.3 Nutzen Sie Schutzprogramme

In den gängigen PC-Betriebssystemen sind ein Virenschutz und eine Firewall integriert, die schon in deren Standardkonfiguration Angriffe aus dem Internet erschweren. Aktivieren Sie diese oder verwenden Sie ggf. ein (evtl. kostenpflichtiges) Virenschutzprogramm eines anderen Anbieters.

Eine Firewall kontrolliert den Datenfluss zwischen einem internen Computer oder Netzwerk und externen Netzwerken.

Bedenken Sie, dass diese Maßnahmen nur begleitend wirksam sein können. Deren Anwendung macht die übrigen Tipps dieser Broschüre nicht überflüssig. Lassen Sie sich also besser nicht durch einen aktivierten Virenschutz oder die Firewall zur Unvorsichtigkeit verleiten, diese garantieren keine vollständige Sicherheit.

Weiterführende Informationen zum Virenschutz:

Weiterführende Infos zu Firewalls:

2.1.4 Tipps zur Auswahl Ihrer Software

Seien Sie aufmerksam, wenn Sie etwas aus dem Internet herunterladen, insbesondere wenn es sich dabei um Programme handelt. Meiden Sie Quellen, bei denen Sie Zweifel an der Seriosität haben. Vergewissern Sie sich vor dem Download von Apps, ob die Quelle vertrauenswürdig ist. Nutzen Sie dafür Suchmaschinen, um ggf. mehr Informationen über den Hersteller zu erhalten oder Erfahrungsberichte von anderen Benutzerinnen oder Benutzern einzuholen.

Nutzen Sie zum Download nach Möglichkeit direkt die Webseite des jeweiligen Herstellers und dessen verschlüsselte Seiten, die Sie an der Abkürzung „https“ in der Adresszeile Ihres Browsers erkennen.

2.1.5 Einrichtung des Routers und sichere WLAN-Nutzung

Der Router bildet den Knotenpunkt für die Kommunikation aller internetfähigen Geräte im Büro und zu Hause – ob Computer, Fernseher oder intelligente Haustechnik. Er verbindet die Geräte sowohl untereinander als auch mit dem Internet. Deshalb kommt dem umfassenden Schutz des Routers eine besondere Bedeutung zu. Zur ganzheitlichen Absicherung gehören dabei die sichere Konfiguration des Routers als Basisschutz sowie die spezielle Konfiguration und der sichere Betrieb des WLANs.

Wenn Sie die Übertragungstechnologie Wireless LAN (WLAN) zum Surfen im Internet nutzen, achten Sie hier besonders auf die Verschlüsselung des Funknetzes. Wählen Sie in Ihrem Router den Verschlüsselungsstandard WPA3 oder, wenn dieser noch nicht unterstützt wird, bis auf weiteres WPA2. Wählen Sie ein komplexes, mindestens 20 Zeichen langes Passwort. Zugriff auf den Router erhalten Sie über eine festgelegte Internetadresse, die im Handbuch Ihres Routers vermerkt ist. Klären Sie, wer Zugriff auf dieses Netz hat (Kinder? Deren Freunde?) und halten Sie die Zugangsdaten geheim.

Hinweise zur sicheren Einrichtung des Routers sowie zum sicheren Umgang mit dem Medium WLAN finden Sie unter:

2.1.6 Wie Sie Cloud-Dienste kontrolliert nutzen

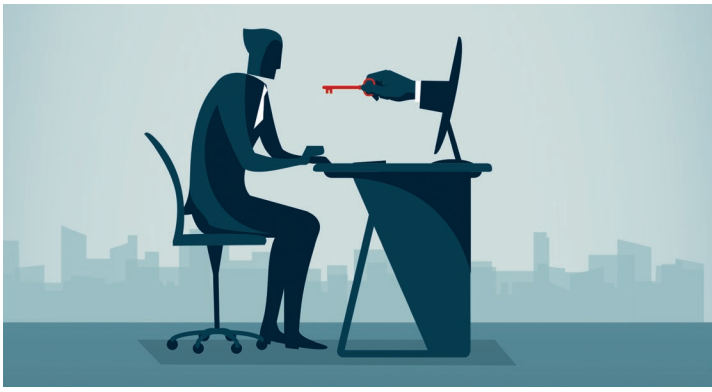
Ein Cloud-Dienst ist ein Onlinedienst, auf den Sie über das Internet jederzeit zugreifen können – egal mit welchem Endgerät. Die Daten werden also zumeist nicht auf Ihren Geräten gespeichert, sondern in der sogenannten Cloud.

Elf wichtige Tipps, die Sie für eine sichere Nutzung von Cloud-Diensten berücksichtigen sollten, haben wir hier für Sie zusammengefasst.

- Sorgen Sie für einen ausreichenden Basisschutz durch die sichere Konfiguration Ihres Zugangsgeräts gemäß den vorherigen Empfehlungen dieser Broschüre.
- Sichern Sie den Zugang zu Cloud-Diensten mit einem sicheren Passwort und wenn möglich mit einem zweiten Faktor ab; mehr dazu finden Sie in Kapitel 3.1. dieser Broschüre.

- Für den Cloud-Zugriff über mobile Geräte gelten die gleichen Sicherheitsvorkehrungen wie für stationäre Geräte.
- Prüfen Sie die Datenschutzbestimmungen des jeweiligen Cloud-Anbieters, damit Sie wissen, wie Ihre Daten verarbeitet werden.
- Informieren Sie sich über die Haftung des Anbieters im Falle eines Datenverlusts und erstellen Sie regelmäßige Backups Ihrer in der Cloud gespeicherten Daten.
- Überprüfen Sie in den Allgemeinen Geschäftsbedingungen des Anbieters, ob eine Weitergabe Ihrer Daten an Dritte zu kommerziellen Zwecken erfolgen könnte.
- Informieren Sie sich über die Sicherheitszusagen des Cloud-Anbieters zu Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten, etwa im Falle eines Ausfalls der Rechenzentren.
- Achten Sie bei der Auswahl Ihres Cloud-Anbieters unbedingt darauf, dass die Übertragung Ihrer Daten über eine sichere Verbindung wie https erfolgt.
- Wenn Sie sensible Daten in der Cloud speichern möchten, sollten Sie diese Daten verschlüsseln, bevor Sie diese in die Cloud laden.
- Wenn Sie Daten in der Cloud mit anderen Personen teilen, achten Sie auf die Art der Freigabe. Begrenzen Sie diese zeitlich und geben Sie nur so viele Daten wie nötig frei.
- Bevor Sie Ihre Daten einem Cloud-Anbieter anvertrauen, sollten Sie prüfen, wie aufwendig es ist, die Daten wieder aus der Cloud zu entfernen.

Weitere Informationen:



2.2 Wie Sie Ihre Daten schützen und sichern

2.2.1 Sichern Sie Ihre Daten durch Backups

Kommt es trotz aller Schutzmaßnahmen zu einer Infektion mit Schadprogrammen, beispielsweise Ransomware, die Ihre Daten ungewollt verschlüsseln, können wichtige Daten verloren gehen, weil Sie in diesem Fall keinen Zugriff mehr auf diese haben. Dies gilt ebenso bei dem Verlust eines Geräts oder einem anderweitigen Defekt. Hier schafft ein Offline-Backup Abhilfe, um die Daten wiederherstellen zu können.

Weiterführende Informationen zum Thema Backup:

2.2.2 Datenverschlüsselung und verschlüsselte Internetnutzung

Besuchen Sie Internetseiten und geben Sie Ihre persönlichen Daten ausschließlich auf Internetseiten ein, die eine verschlüsselte Verbindung anbieten. Nutzt die Seite das sichere Kommunikationsprotokoll **https**, erkennen Sie dies an der aufgerufenen Internetadresse. Sie beginnt dann stets mit https, und in der Adresszeile Ihres Webbrowsers findet sich meist ein kleines geschlossenes Schlosssymbol oder eine ähnliche Kennzeichnung.

Auf einem gemeinsam genutzten Computer kann eine Verschlüsselung von Daten unbefugtes Lesen dieser Daten durch Mitbenutzerinnen und Mitbenutzer sowie durch Personen, die sich unberechtigt Zugang zu Ihrem Computer verschaffen, verhindern. Informationen auf mobilen Geräten wie Notebooks und USB-Speichermedien geraten nicht in falsche Hände (z. B. wenn das Gerät gestohlen wird oder verloren geht), wenn die Daten darauf verschlüsselt sind.

Weitere Informationen zur Verschlüsselung von Daten auf Computern:

Weitere Informationen zur Verschlüsselung der Datenübertragung durch VPN:

2.2.3 Seien Sie sparsam mit Ihren Daten

Angreifer im Internet steigern ihre Erfolgsraten, indem sie ihre Opfer individuell ansprechen: Zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, werden dazu genutzt, Vertrauen zu erwecken. Die ungeschützte Weitergabe persönlicher Daten in offenen, ungesicherten Netzen sollte vermieden werden.

Mit diesen vier Tipps schützen Sie sich und Ihr Umfeld – sowohl beruflich als auch privat:

- Nur erforderliche Daten speichern:
  Löschen oder archivieren Sie regelmäßig nicht mehr benötigte E-Mails und andere Dateien.
- Zu veröffentlichende Inhalte beurteilen:
  Überlegen Sie vor jeder Veröffentlichung, ob die Information öffentlich bekannt werden sollte. Bilder, Videos und andere Inhalte können in falsche Hände geraten. Liegen Angreifern bereits Name, Arbeitgeber oder Geburtsdatum vor, ist ein Identitätsdiebstahl deutlich einfacher.
- Motiv einer Bildaufnahme richtig wählen:
  Seien Sie besonders sensibel mit sozialen Medien im Umfeld Ihres Arbeitsplatzes. Finden Sie klare Regeln: (Wo) Dürfen Fotos und Videos gemacht werden?
- Regelmäßig überprüfen und sensibilisieren:
  Sie sollten Ihre Mitarbeiterinnen und Mitarbeiter sowie enge Vertraute immer wieder auf die Gefahren beim Umgang mit Informationen und IT hinweisen.

Weitere Informationen:

2.2.4 Identitätsdiebstahl: Der Fremde im eigenen Haus

Gestohlene Identitätsdaten sind vermehrt im Internet verfügbar und können für Angriffe missbraucht werden. Den Diebstahl Ihrer persönlichen Daten können Sie mit verschiedenen nationalen oder internationalen Leak Checkern überprüfen.

Sind Sie von einem Identitätsdiebstahl bei einem Ihrer Accounts (E-Mail, Social Media) betroffen, sollten Sie umgehend aktiv werden:

- Das Wichtigste: Zügig, aber besonnen reagieren.
- Ändern Sie das Passwort des E-Mail-Kontos, das im Profil hinterlegt ist und ändern Sie unverzüglich die Zugangsdaten für das betroffene Programm oder Social Media-Profil.
- Informieren Sie Ihre Kontakte am besten persönlich über den Identitätsdiebstahl.
- Bringen Sie den Vorfall bei der Polizei unter polizei-beratung.de zur Anzeige.

Hinweise zu Kontaktmöglichkeiten zum BSI für den Fall, dass doch etwas passiert sein sollte, finden Sie in Kap. 4 der Broschüre.

Weitere Informationen:

2.2.5 Empfehlungen zum Schutz vor Social Engineering

Social Engineering nutzt menschliche Beziehungen unter Vorspiegelung falscher Tatsachen aus. Die zentralen Merkmale von Angriffen mithilfe von Social Engineering bestehen in der **Täuschung über die Identität und der Absicht des Täters**. So gibt sich dieser beispielsweise als Technikerin bzw. Techniker oder als Mitarbeiterin bzw. Mitarbeiter eines Unternehmens wie PayPal, Facebook oder eines Telekommunikationsunternehmens aus, um das Opfer zur Preisgabe von Anmelde- oder Kontoinformationen oder zum Besuch einer präparierten Webseite zu verleiten.

Um das Risiko von Social Engineering zu mindern, sollten in jedem Fall die folgenden Grundregeln beachtet werden:

- Gehen Sie verantwortungsvoll mit sozialen Netzwerken um. Überlegen Sie genau, welche persönlichen Informationen Sie dort offenlegen, da diese von Kriminellen gesammelt und für Täuschungsversuche missbraucht werden können.
- Erwägen Sie, ggf. Ihre professionellen und privaten Profile getrennt zu halten.
- Seien Sie wählerisch bei Kontaktanfragen und nehmen Sie grundsätzlich nur Personen in Ihre Freundesliste auf, die Sie kennen.
- Geben Sie in privaten und beruflichen sozialen Netzwerken keine vertraulichen Informationen über Ihren Arbeitgeber oder Ihre Arbeit preis.
- Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Telefon oder E-Mail mit. Banken und seriöse Firmen fordern ihre Kundinnen und Kunden nie per E-Mail oder per Telefon zur Eingabe von vertraulichen Informationen auf. So gibt es z. B. eine seit Jahren bekannte Masche mit angeblichen Mitarbeiterinnen und Mitarbeitern des Microsoft Servicecenters, die Zugriff auf Ihren PC erlangen wollen: Ähnlich wie beim Enkel-Trick sollen Sie nach angeblichen Beweisen Software installieren oder Daten preisgeben.
- Lassen Sie bei E-Mails von unbekannten Absendern besondere Vorsicht walten: Sollte auch nur ansatzweise der Verdacht bestehen, dass es sich um einen Angriffsversuch handeln könnte, reagieren Sie im Zweifelsfall besser überhaupt nicht. Wenn es sich um falschen Alarm handelt, wird sich ein Absender ggf. über einen anderen Kanal bei Ihnen melden. **Nehmen Sie sich Zeit für den 3-Sekunden-Sicherheits-Check** - mehr dazu im untenstehenden Link.
- Nicht sorglos und unbedacht auf Links in E-Mails und Nachrichten klicken.
- Sollte eine Reaktion zwingend erforderlich sein, vergewissern Sie sich durch einen Anruf bei der Absenderin bzw. dem Absender, dass es sich um eine legitime und authentische E-Mail handelt.

Link zum 3-Sekunden-Sicherheits-Check:

Weitere Informationen:

2.3 Wie Sie Ihre Internet-einstellungen absichern

2.3.1 So sind Sie unterwegs sicher im Internet

Die folgende Übersicht fasst Vorsichtsmaßnahmen zusammen, die Ihnen helfen können, Ihre Smartphones, Tablets und anderen mobilen Geräte sowie die darauf befindlichen Daten vor Angriffen durch Cyberkriminelle zu schützen:

- Halten Sie Apps und Betriebssystem Ihres Geräts mit regelmäßigen Updates auf dem neuesten Stand.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die erteilten Zugriffsberechtigungen regelmäßig.

- Nutzen Sie Sperrcodes und Passwörter, um Ihre Geräte und Daten zu schützen. Die automatische Bildschirmsperre Ihres Smartphones und die PIN-Abfrage Ihrer SIM-Karte sollten stets aktiviert sein.

- Deaktivieren Sie Drahtlosschnittstellen, wie Bluetooth, WLAN oder NFC, wenn Sie diese nicht benötigen; es reichen bereits wenige Sekunden, um über AirDrop, Bluetooth, WLAN oder NFC unbemerkt Daten auf Ihr Gerät zu übertragen oder Daten von Ihrem Smartphone weiterzuleiten.

- Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht und achten Sie auf verschlüsselte Verbindungen des Browsers (https). Beachten Sie, dass bei öffentlichen Hotspots die WLAN-Verbindung häufig unverschlüsselt ist. Meiden Sie ggf. unbekannte Hotspots.

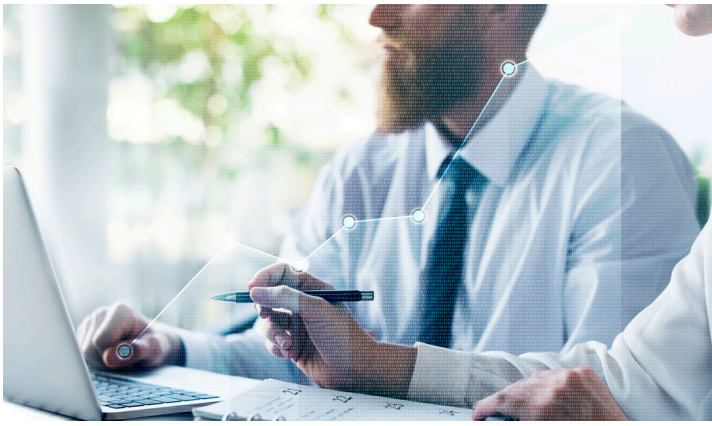
- Lassen Sie Ihr Gerät niemals unbeobachtet, um es vor unbefugten Zugriffen und Manipulation zu schützen. Seien Sie auch beim Aufladen des Akkus an fremden Anschlüssen aufmerksam.

- Prüfen Sie Nummern, die Sie nicht kennen, vor dem Rückruf. Hilfe gibt es auf www.bundesnetzagentur.de/Rufnummernmissbrauch.

- Sichern Sie die Daten auf Ihren mobilen Geräten regelmäßig und verschlüsseln Sie insbesondere sensible Daten.

- Löschen und formatieren Sie alle Speicher bevor Sie ein Gerät verkaufen, weitergeben oder entsorgen. Vergessen Sie nicht, die SIM-Karte(n) und zusätzliche Speicherkarten zu entfernen.

Weitere Informationen:



2.3.2 Richten Sie Ihre Browser sicher ein

Zum Surfen im Internet benötigen Sie einen Browser. Bei Erweiterungen, Add-Ons oder auch Plug-Ins handelt es sich um kleine Programme, die Ihren Browser mit zusätzlichen Funktionen ausstatten können.

- Deaktivieren oder deinstallieren Sie Add-Ons und Plug-Ins, die Sie nicht unbedingt benötigen.

- Die Einstellungen „Privater Modus“ oder die Funktion „Verlauf löschen“ verhindern beispielsweise, dass andere Nutzerinnen und Nutzer desselben Gerätes sehen, welche Internetseiten Sie besucht haben.

- „Cookies nicht für Drittanbieter zulassen“ sorgt dafür, dass nur Webseiten Ihr Surfverhalten verfolgen können, die Sie tatsächlich besucht haben.

- Achten Sie auch darauf, dass Ihr Webbrowser immer auf dem aktuellsten Stand ist. Mit Aktualisierungen werden regelmäßig auch Sicherheitslücken geschlossen. Nutzen Sie ein Programm zum Blockieren von Werbung, um sich vor Malvertising, also der Verbreitung von Schadsoftware über Werbeeinblendungen, zu schützen.

- Tragen Sie die Adressen für besonders sicherheitskritische Webseiten, z. B. die Login-Seiten Ihrer Social Media Accounts, zunächst sorgfältig von Hand in die Adresszeile des Browsers ein und speichern Sie die eingegebene Adresse als Lesezeichen, das Sie dann für den sicheren Zugang nutzen. Durch kopierte URLs können Links auf gefälschte Seiten unentdeckt bleiben.

Weitere Informationen:

2.4 Ihr Arbeitsplatz: Sicherheit durch Organisation

2.4.1 Treffen Sie Sicherheitsregelungen

Zu den verschiedenen Angriffszielen zählen auch der Büroarbeitsplatz und das Homeoffice. Die folgende Checkliste fasst wichtige Tipps für eine sicherheitsbewusste Organisation im Team zusammen.

- Klar geregelt:
  Treffen Sie deutliche, unmissverständliche und verbindliche Regelungen zur IT-Sicherheit und zur Sicherheit Ihrer Daten in Papierform. Kommunizieren Sie diese schriftlich an alle Beteiligten.

- Hier gibt es nichts zu sehen:
  Ergreifen Sie an Ihrem Arbeitsplatz zu Hause wenn möglich Maßnahmen, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist. Verschließen Sie die Türen, wenn Sie den Arbeitsplatz verlassen, und geben Sie Dritten keine Chance durch einsehbare oder gar geöffnete Fenster. Sperren Sie beim Verlassen Ihres Arbeitsplatzes auch Ihr Gerät, um unerwünschte Einblicke und Handlungen unbefugter Personen zu vermeiden.

- Eindeutige Verifizierung:
  Sorgen Sie für eindeutige Kontaktstellen und Kommunikationswege, die von den Beschäftigten verifiziert werden können.

Weitere Informationen:

2.4.2 Sensibilisieren Sie Ihre Mitarbeitenden

Der Faktor Mensch spielt in der Informationssicherheit nach wie vor eine wichtige Rolle. IT-Sicherheit ist nur so gut wie der Mensch, der die Systeme bedient. Der Mensch ist dabei nicht Teil des Problems, sondern Teil der Lösung.

- Der Aufbau eines entsprechenden Problem- und Sicherheitsbewusstseins sowie regelmäßige Schulungen sind wichtige präventive Maßnahmen, um den Sicherheitsfaktor Mensch zu stärken.

- Relevante Gefährdungen müssen bekannt sein, und die Erwartungshaltung hinsichtlich der Informationssicherheit sollte im Team klar kommuniziert werden.

Weitere Informationen:

2.4.3 Rechte und Rollen Ihrer Mitarbeitenden

Achten Sie auf eine klare Rollentrennung: Welcher Mitarbeitende benötigt welche Rechte, um seine Aufgaben auszuführen. Seien Sie auch hierbei grundsätzlich sparsam.

Eine Konzentration vieler oder aller Zuständigkeiten in einer Rolle sollte vermieden werden.

- Definieren Sie die technischen und organisatorischen Rollen Ihres Teams.

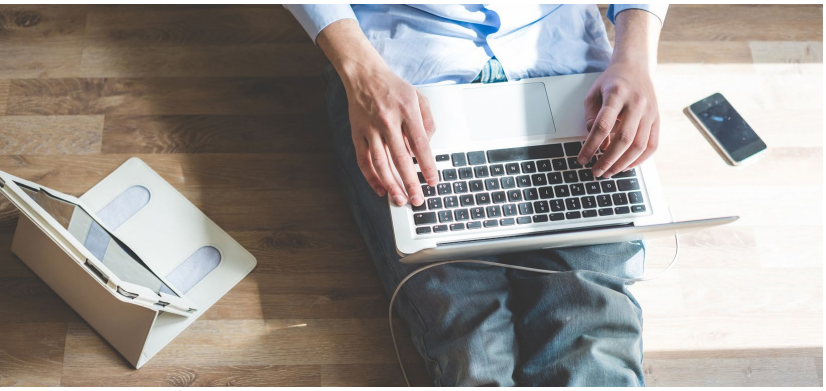
- Klären Sie die Verantwortlichkeiten eines jeden Mitarbeitenden.

- Legen Sie Zuständigkeiten fest (auch unter Einbeziehung externer Dienstleister).

3 Sichere Nutzung sozialer Netzwerke, E-Mail & Co.

3 Sichere Nutzung sozialer Netzwerke, E-Mail & Co.

Soziale Medien, E-Mail & Co spielen für viele von uns im Alltag eine zentrale Rolle. Vertrauenswürdige und private Gespräche finden vermehrt digital statt. Umso wichtiger ist es, dass Sie verantwortungsvoll mit diesen hilfreichen, aber auch missbrauchsanfälligen Kommunikationstools umgehen.



3.1 Die Grundlage: Sichere Logins nutzen

3.1.1 Der Anker: Ihr E-Mail-Account als Schlüssel zu weiteren Diensten und Konten

Zu den wichtigen Accounts gehören vor allem Ihre E-Mail-Konten. Wenn Dritte Zugang zu diesen erhalten, können sie großen Schaden anrichten. Einerseits könnten sie auf Ihre E-Mail-Daten und den gesamten Mail-Verlauf der Vergangenheit zugreifen und darüber hinaus auch in Ihrem Namen z. B. Sie diskreditierende Nachrichten versenden. Andererseits könnten vor allem Angreifer mit Zugriff auf Ihr E-Mail-Konto weitere Onlinedienste übernehmen, indem sie Passwörter zu diesen Diensten zurücksetzen und den Zugang für eigene Zwecke missbrauchen. Daher kann die Einrichtung eines separaten E-Mail Accounts ausschließlich mit der Funktion des „Anker-Accounts“, ggf. sogar separat pro Social-Media-Account, empfehlenswert sein.

Beachten Sie in diesem Zusammenhang auch, dass Ihr Smartphone, wenn es einmal gestohlen, verloren und entsperrt ist, ein mögliches Einfallstor für den direkten Zugriff auf Ihre E-Mails und andere Konten sein kann. Achten Sie daher auf sichere Sperrcodes und eine automatische Bildschirmsperre nach einem kurzen Zeitintervall.

Aufgrund dieser zentralen Bedeutung von E-Mail-Accounts als Anker für weitere Konten sollten Sie die folgenden Empfehlungen berücksichtigen.

3.1.2 Verwendung sicherer Passwörter

Vergeben Sie für jedes Online- und Benutzerkonto ein eigenes, sicheres Passwort und ändern Sie schnellstmöglich alle Passwörter, wenn diese in falsche Hände geraten sein könnten. Ändern Sie auch die von den Herstellern oder Dienstanbietern voreingestellten Passwörter nach der ersten Nutzung.

Dort wo eine Zwei-Faktor-Authentisierung (2FA) angeboten wird, sollten Sie damit den Zugang zu Ihrem Onlinekonto zusätzlich absichern. Ein Passwortmanager-Programm kann zudem die Handhabung unterschiedlicher, starker Passwörter erleichtern.

Besonders wichtig:
Geben Sie Ihre Passwörter niemals an Dritte weiter.

Weitere Informationen zu Erstellung und Nutzung von sicheren Passwörtern:

3.1.3 Nutzung eines Passwortmanagers

Im Alltag fällt es vielen Menschen schwer, sich komplexe und lange Passwörter zu merken. Einige Nutzerinnen und Nutzer haben daher die Strategie entwickelt, sich ein besonders komplexes Passwort für alle Accounts zu merken. Ist dieses jedoch einmal geknackt, können Cyberkriminelle auf alle sensiblen Daten zugreifen. Aus diesem Grund ist es sicherer, für jeden Account ein eigenes, komplexes Passwort zu verwenden – wenngleich das bedeutet, mehrere Dutzend von Zugangsdaten zu verwalten. Wer da den Überblick verliert, für den kann ein Passwortmanager Abhilfe schaffen.

Für Ihre hochsensiblen Inhalte sollten Sie in einem solchen Passwortmanager am besten einen erweiterten Schutzmechanismus einsetzen. Dieser lässt sich durch die Einrichtung eines zweiten Faktors realisieren.

Weitere Informationen finden Sie unter:

3.1.4 Mehr Sicherheit durch Zwei-Faktor-Authentisierung

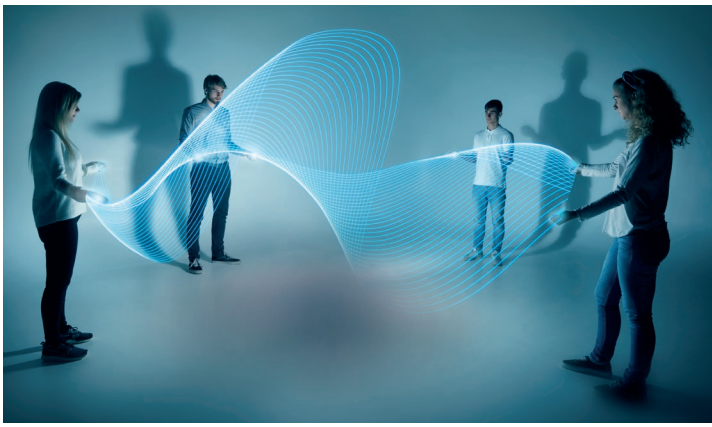
Zwei-Faktor-Authentisierung bietet eine wirksame Möglichkeit, die Sicherheit der von Ihnen verwendeten Accounts beträchtlich zu erhöhen.

Mittlerweile bieten viele Online-Dienstleister Verfahren an, mit denen sich die Nutzerinnen und Nutzer zusätzlich bzw. alternativ zur Passworteingabe identifizieren können, wenn sie sich in ein Konto einloggen.

Eine Authentisierung mittels mehrerer Faktoren beginnt in vielen Fällen mit der gewohnheitsmäßigen Eingabe eines sicheren Passworts. Das System, in das sich Nutzende einloggen möchten, bestätigt daraufhin die Richtigkeit des eingegebenen Kennworts. Dies führt jedoch nicht - wie bei einfachen Systemen üblich - direkt zum gewünschten Inhalt, sondern zur Prüfung des zweiten Faktors. Auf diesem Weg wird verhindert, dass unbefugte Dritte allein deshalb Zugang zu Nutzerdaten oder Funktionen erhalten, weil sie in den Besitz des Passworts gelangt sind.

- Wenden Sie, wenn möglich, eine Zwei-Faktor-Authentisierung an.
- Viele Dienste haben die Zwei-Faktor-Authentisierung nicht standardmäßig aktiviert, bieten sie aber dennoch an. Eine entsprechende Überprüfung lohnt sich.
- Gelangt Ihr Passwort oder Ihre PIN in die falschen Hände, sind Ihre sensiblen Daten dennoch gut gesichert, da diese durch die weitere Barriere des zweiten Faktors vor fremdem Zugriff geschützt werden.
- Als zweiter Faktor kann z. B. ein zusätzliches Gerät (Authentisierung über einen Sicherheitstoken) oder ein zeitlimitiertes Einmalkennwortverfahren (TOTP / Authentisierungs-App) genutzt werden.
- Aufgrund möglicher Angriffsszenarien in Mobilfunknetzen sollten Sie bei der Zwei-Faktor-Authentisierung besser auf SMS-basierte Verfahren verzichten und ein Hardware-Token bevorzugen.
- Es gibt zudem Verfahren der Zwei-Faktor-Authentisierung, die sich auch im Team nutzen lassen, wenn Ihr Account von mehreren Personen und verschiedenen Standorten / Geräten verwaltet werden soll.

Weitere Informationen:



3.2 Unterwegs in sozialen Netzwerken

3.2.1 Sicherheitstipps für die Nutzung sozialer Medien

Die Berücksichtigung nachfolgender Sicherheitstipps hilft Ihnen, die Nutzung sozialer Medien abzusichern.

- Beachten und prüfen Sie die Sicherheitseinstellungen und nutzen Sie Sicherheitsfragen:
  - Beim Einrichten eines Social Media Accounts ist häufig eine Sicherheitsfrage zu beantworten. Der Grund: Im Falle eines vergessenen Passwortes wird diese Sicherheitsfrage erneut vom Social Media-Anbieter abgefragt. Die Sicherheitsfrage sollte im Sinne eines zweiten Passwortes beantwortet werden - wenn z. B. nach dem Geburtsnamen einer verwandten Person gefragt wird, sollte dort statt des Geburtsnamens ein starkes Passwort genutzt werden.
  - Die Sicherheitseinstellungen des Social Media Accounts sollten regelmäßig überprüft werden. Oft gibt es neue Optionen, die die Sicherheit ihres Accounts erhöhen können. Besonders die Verknüpfungen zu anderen Konten sollten regelmäßig geprüft werden.

- Account-Verifizierung:
  - Die Angebote einiger Social Media-Anbieter für eine Account-Verifizierung sollten genutzt werden. Der Grund: Ein verifizierter Account ist für andere Nutzerinnen und Nutzer über ein spezielles Symbol erkennbar (z. B. Blue Badge) und gilt als authentisch. Damit können Fake Accounts mit ähnlichem Namen von anderen als nicht authentisch identifiziert werden.
  - Auf Anfrage stellt das BSI ein eigenes Dokument zum Thema Account-Verifizierung zur Verfügung.
  - **Wichtig:** Eine Verifizierung verknüpft Ihre Identität oder die Identität Ihrer Organisation eindeutig mit Ihrem Account. Entsprechend werden Beiträge dieses Accounts von den meisten Nutzenden als öffentliche und glaubwürdige Äußerung von Ihnen oder Ihrer Organisation verstanden. Durch die höhere Glaubwürdigkeit des verifizierten Accounts ist dessen Account-Sicherheit sogar noch wichtiger als bei einem nicht verifizierten Account.
- Überwachen Sie Geräte und Drittanbieter mit Zugriff auf den Social Media Account:
  - Prüfen Sie regelmäßig die Übersicht erlaubter Geräte und aktiver Sessions. Löschen Sie Geräte und Sessions, die Sie nicht zuordnen können.
  - Aktivieren Sie den Benachrichtigungsmodus, der meldet, wenn sich bisher unbekannte Geräte in den Account einloggen. Der Grund: Der Social Media-Anbieter versendet eine Warnnachricht z. B. an das hinterlegte Referenzkonto, falls Unbefugte versuchen, sich über andere Geräte an dem Account anzumelden. Falls Sie eine Benachrichtigung über ein Ihnen bisher unbekanntes Gerät erhalten, prüfen Sie diese Meldung sorgfältig.
  - Achten Sie auch darauf, dass Sie dieses Referenzkonto bzw. die Nachrichten und E-Mails dieses Anker-Accounts regelmäßig lesen.
  - Oft besteht die Möglichkeit, den eigenen Account mit Drittanbieter-Apps zu koppeln. Prüfen Sie, ob es solche Verknüpfungen gibt und ob diese tatsächlich notwendig sind. In der Vergangenheit gab es immer wieder Vorfälle, in denen solche verknüpften Dienste als Einfallstor missbraucht wurden.
  - Achten Sie darauf, dass Drittanbieter-Apps eventuell nicht alle gewünschten Aktionen 1:1 abbilden können. Beispielsweise könnten Direktnachrichten in einer App gelöscht werden, aber weiterhin in Ihrem Account vorliegen.

Weitere Informationen:

Hinweise und Hilfestellungen, weiterführende Links:

3.3 Ihre sichere digitale Kommunikation

3.3.1 Sicher in Kontakt bleiben durch Messengerdienste

Einige bekannte Instant-Messengerdienste sind WhatsApp, Threema, Telegram, Signal, Wire und der Facebook Messenger. Solche geschlossenen Systeme erlauben den Chat zwischen Personen, die denselben Messenger verwenden.

Worauf Sie bei solchen Messengern achten sollten:

- Halten Sie die Messenger-App aktuell, indem Sie Updates umgehend installieren.
- Achten Sie auf die Vertrauenswürdigkeit des Anbieters. Bedenken Sie dabei auch, dass andere Länder andere Datenschutzgesetze haben und die Anbieter nur den lokalen Gesetzen unterworfen sein können. Gesetze zum Schutz der Privatsphäre unterscheiden sich weltweit.

- Messenger werden wiederholt auf Verschlüsselung und die Einhaltung des Datenschutzes getestet. Beziehen Sie die Ergebnisse solcher Tests bei der Entscheidungsfindung für einen Dienst mit ein.

- Bedenken Sie, dass Messenger auf Mobilgeräten häufig umfassende Rechte auf Ihren Geräten einfordern und danach weitgehenden Zugriff auf die Ressourcen Ihres Gerätes haben, z. B. auf die komplette Kontaktliste. Versuchen Sie nach Möglichkeit, diese Rechte einzuschränken.

- Damit keine Dritten den Inhalt Ihrer Kommunikation sehen können, sollten die ausgetauschten Nachrichten verschlüsselt sein. Achten Sie darauf, dass Ihr Messenger eine solche Funktion anbietet, und verwenden Sie möglichst einen Messenger, der eine Ende-zu-Ende Verschlüsselung nutzt.

- Blockieren Sie Kontakte, wenn Sie unsicher sind, um welche Person es sich handelt oder wenn Ihnen eine Person zusetzt. Zeigen Sie Beleidigungen, sexuelle Belästigungen, Nötigungen, Erpressungsversuche oder Bedrohungen unverzüglich bei der Polizei an.

- Prüfen Sie die AGBs und die Datenschutzbestimmungen vor allem mit Blick darauf, was mit Ihren Daten und Angaben geschieht. Werden sie verkauft, gespeichert oder verschlüsselt? Können Sie mit dem, was in den Bestimmungen steht, leben?

- Es gibt Messenger, die mit sozialen Netzwerken verknüpft sind. Solche Verknüpfungen können ggf. aus Sicht des Datenschutzes bedenklich sein. Durch die Verknüpfung können Sie zudem rasch den Überblick darüber verlieren, welchen Inhalt Sie gegenüber welchen Personen freigegeben haben.

Weitere Informationen:

3.3.2 Nutzen Sie E-Mail wirklich sicher?

Verzichten Sie, wenn möglich, auf die Darstellung und Erstellung von E-Mails im HTML-Format und verwenden Sie stattdessen ein reines Textformat. Die Nutzung des HTML-Formats können Sie über die Einstellungen Ihres Mailprogramms ändern. Seien Sie aufmerksam beim Öffnen von E-Mail-Anhängen oder beim Klick auf einen Link, denn Schadprogramme werden oft über in E-Mails integrierte Bilder oder Dateianhänge verbreitet oder verbergen sich hinter Links. Besonders zu beachten ist dies bei E-Mails, deren Absenderin oder Absender Ihnen nicht bekannt ist.

Falls Ihnen eine E-Mail von einer bekannten Absenderin oder einem bekannten Absender seltsam vorkommt, fragen Sie vor dem Öffnen bei der Absenderin oder dem Absender nach, ob die E-Mail tatsächlich von ihr oder ihm stammt. Nutzen Sie dabei besser nicht die Antwortfunktion für die in der E-Mail angegebenen Kontaktmöglichkeiten. Sie könnten gefälscht sein.

Unerwünschte oder gefährliche E-Mails können Sie häufig schon an wenigen Merkmalen identifizieren: Indem Sie mit der Maus über die Absenderin bzw. den Absender fahren oder auf diese bzw. diesen klicken, können Sie beispielsweise erkennen, ob der Absender gefälscht ist. Achten Sie dabei auf wirre Buchstabenfolgen, den Tausch durch optisch ähnliche Buchstaben oder eine ausländische Domain, also die Endung der E-Mail-Adresse. Überprüfen Sie auch die Betreffzeile und den Text der E-Mail auf Sinnhaftigkeit und Rechtschreibung. Betrüger machen hier oft Fehler. Seien Sie zudem skeptisch, wenn eine schnelle Reaktion von Ihnen eingefordert wird.

3.3.3 Vertrauliche E-Mails verschlüsseln

E-Mail-Anbieter nutzen für den Versand der Nachricht unterschiedliche Knotenpunkte im Web, an denen die E-Mail navigiert und weitergeleitet wird, bis sie zum empfangenden E-Mail-Programm gelangt. Auf dieser Strecke im - nicht generell verschlüsselten - Internet kann die E-Mail dann potentiell mitgelesen werden.

Vertrauliche E-Mails lassen sich verschlüsseln. Prüfen Sie dafür die Möglichkeiten Ihres E-Mail-Anbieters.

Weitere Informationen zu E-Mail-Verschlüsselungen:

3.4 Last but not Least: Nützliche Links zu Sicherheitseinstellungen für soziale Netzwerke und Messenger

Bereits beim Einrichten Ihres Kontos für das soziale Netzwerk können Sie bekannte Schwachstellen und Probleme vermeiden.

Weitere Informationen zu sicherheitsrelevanten Einstellungen verschiedener Plattformen und Dienste:

4 Und wenn dann doch etwas passiert ist

4 Und wenn dann doch etwas passiert ist.

Ergänzend zu den oben dargestellten Hilfen kann das BSI bei IT-Sicherheitsvorfällen zusätzlich unterstützen. Über unsere Hotline können unsere Mitarbeitenden Sie persönlich beraten und bei Verständnisfragen weiterhelfen.

Bitte beachten Sie aber, dass wir Ihnen aus rechtlichen Gründen leider keinen unmittelbaren Support für Ihr IT-Gerät und keine technische Hilfe im Einzelfall anbieten können. Hierzu sollten Sie sich an einen geeigneten Dienstleister wenden.

Kontaktmöglichkeit zur BSI-Hotline:

Einen Vorfall bewältigen, melden, sich informieren, vorbeugen:

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

E-Mail
bsi@bsi.bund.de

Internet
www.bsi.bund.de

Telefon
+49 (0) 22899 9582 – 0

Telefax
+49 (0) 22899 9582 – 5400

Stand
Version 1.0, Januar 2022

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bildnachweis
Titel: GettyImages ©Yuichiro_Chino-Moment,
S. 6: GettyImages ©D3Damon;
S. 8: GettyImages ©erhui1979; S. 10: GettyImages ©westend61;
S. 11: Freepik ©rawpixel.com; S. 14: AdobeStock ©Eugenio Marongiu;
S. 15: GettyImages ©Henrik Sorensen; S. 16: AdobeStock ©vegefox.com;
S. 18: AdobeStock ©thodonal; S. 20: AdobeStock ©oz

www.bsi.bund.de