GANZ EINFACH

Cyber Security & Digitale Selbstverteidigung

Schluss mit der Angst vor Hackern



Danilo Sieren

Danilo Sieren

Ganz Einfach

Cyber Security und digitale Selbstverteidigung

Konten Geräte und eigene Server schützen
Angriffe erkennen und sicher reagieren

Überarbeitete und erweiterte
Neuauflage 2026

Willkommen zur Neuauflage 2026

Digitale Selbstverteidigung beginnt mit einem überschaubaren Ziel: Du möchtest deine Konten behalten, vertrauliche Informationen schützen und nach einer Störung wieder handlungsfähig werden. Dafür brauchst du verständliche Zusammenhänge und Verfahren, deren Wirkung du prüfen kannst. Ein einzelnes Produkt und eine lange Liste eingeschalteter Optionen reichen dafür nicht aus.

Dieses Buch führt dich vom persönlichen Konto über Geräte und Heimnetze bis zum eigenen Linux-Server. Du lernst, Phishing angemessen zu beurteilen, Passkeys und Wiederherstellungswege einzuordnen, Zugriffsgrenzen zu planen und Sicherungen tatsächlich zurückzulesen. Die technischen Kapitel erklären SSH, VPN, Container und Webanwendungen mit ihren jeweiligen Voraussetzungen.

Die Neuauflage richtet sich an interessierte Anwender und Betreiber kleiner eigener Umgebungen. Für die ersten Kapitel sind keine Programmierkenntnisse nötig. Die Server- und Python-Kapitel setzen Bereitschaft zum sorgfältigen Arbeiten in einer getrennten Testumgebung voraus. Du musst nicht jede Technik selbst betreiben: Die Entscheidung für einen betreuten Dienst kann zu deinen Möglichkeiten besser passen als ein eigener Server.

Der erfundene Lesegarten begleitet viele Beispiele. Zwei Menschen verwenden eine kleine Dokumentenablage und müssen ihre Konten, Geräte und Sicherungen zusammen denken. Der überschaubare Aufbau macht Abhängigkeiten sichtbar, ohne zu behaupten, dass dieselbe Architektur für jede Familie und jedes Unternehmen geeignet sei.

Weg durch das Buch

Lies zunächst die Kapitel 1 bis 5 für Schutzziele, Bestand, Phishing und Konten. Die Kapitel 6 bis 9 erklären Verschlüsselung, Zertifikate und sichere Alltagsgeräte. Die Kapitel 10 bis 18 vertiefen Netzwerke und den Betrieb eigener Dienste. Du kannst diese Teile entsprechend deiner Umgebung auswählen.

Die Kapitel 19 bis 26 behandeln Anwendungsgrenzen, Sicherungen, Beobachtung und kontrollierte Prüfungen. Die Kapitel 27 bis 30 verbinden die einzelnen Maßnahmen mit Vorfällen und Wiederanlauf. Die Anhänge enthalten einen ausgearbeiteten Plan, vollständige lokale Programme, Konfigurationsbeispiele, Notfallübungen und ausführliche Fehlerfälle.

Die Quellenkennungen wie D01 verweisen auf das Quellenverzeichnis. Dort findest du die offiziellen technischen Dokumentationen und die vorgesehenen weiterführenden Primärquellen. Das ausführliche Kapitelverzeichnis und das Stichwortverzeichnis helfen dir, einen bestimmten Ablauf später wiederzufinden.

Übungen mit einem klaren Auftrag

Verwende eigene Systeme und erfundene Testdaten. Ein Befehl mit Verwaltungsrechten verändert gegebenenfalls die ganze Maschine. Prüfe deshalb Voraussetzungen und Rückweg, bevor du eine Konfiguration übernimmst. Fremde Netze und Konten werden nicht ohne entsprechende Berechtigung untersucht.

Die Beispiele unterscheiden zwischen einem Modell, einer dokumentierten Konfiguration und einer beobachteten Wirkung. Ein Python-Modell verändert keine Firewall. Ein erfolgreicher Syntaxcheck bestätigt keinen erreichbaren Dienst. Ein gestarteter Dienst beweist keine korrekten Benutzerrechte. Diese

Unterscheidungen helfen dir, Ergebnisse angemessen zu bewerten.

Viele Übungen nennen einen bekannten positiven und einen negativen Fall. Prüfe beide. Ein erlaubter Zugriff zeigt, dass eine benötigte Funktion möglich ist. Erst der passende untersagte Zugriff hilft zusätzlich, die gewünschte Grenze zu beurteilen. Halte offene Fragen ausdrücklich fest.

Stand und Weiterentwicklung

Redaktionsstand dieser Neuauflage ist der 1. November 2026. Sicherheitsfunktionen, unterstützte Versionen und Herstellerangebote ändern sich. Kontrolliere vor einer produktiven Umsetzung die zum tatsächlich eingesetzten Stand gehörende Dokumentation und die aktuellen Sicherheitsmeldungen. Vermeide besonders die ungeprüfte Übernahme alter Installationsbefehle.

Das Buch verspricht keine vollständige Angriffsfreiheit. Es zeigt, wie du Risiken nachvollziehbar verringerst und auf Fehler vorbereitet bleibst. Bei einem erheblichen Sicherheitsvorfall, möglichen rechtlichen Pflichten oder unklaren forensischen Anforderungen sind die zuständigen geeigneten Fachleute einzubeziehen.

Inhalt

Willkommen zur Neuauflage 2026 2
1 Risiken verstehen und Schutzziele festlegen 7
2 Bestandsaufnahme und ein tragfähiger Sicherheitsplan 12
3 Phishing und Social Engineering erkennen 16
4 Identität Passwörter und Passkeys 20
5 Passwortmanager und Wiederherstellung organisieren 25
6 Kryptografie und Schlüssel richtig einordnen 31
7 HTTPS Zertifikate und Vertrauen 37
8 Sichere Geräte und verlässliche Updates 41
9 Browser E-Mail und Dateien im Alltag 45
10 Netzwerke IPv4 IPv6 und DNS verstehen 49
11 WLAN Router und vernetzte Alltagsgeräte 54
12 Segmentierung und Zugriffsregeln planen 58
13 Firewalls wirksam konfigurieren und prüfen 63
14 SSH mit einem sicheren Rückweg verwalten 68
15 VPN und Fernzugriff kontrolliert betreiben 73
16 Linux härten und Änderungen beherrschen 77
17 Container und Images sicher betreiben 83
18 Geheimnisse und Softwarelieferketten 88
19 Webanwendungen verstehen und schützen 93
20 Eingaben Sitzungen und Berechtigungen 98
21 Sicherungen nach dem Wiederherstellungsziel planen 103
22 Sicherungen erstellen und wirklich wiederherstellen 107
23 Protokolle und Integritätsprüfung 112
24 Monitoring und sinnvolle Alarme 116
25 Python für lokale Sicherheitsprüfungen 121

26 Schwachstellen und Freigaben kontrollieren 126
27 Sicherheitsvorfälle erkennen und eindämmen 130
28 Wiederanlauf und Ursachenanalyse 134
29 Datenschutz KI und zukünftige Verfahren 139
30 Ein durchgängiges Praxisprojekt.....143
Anhang A Einen vollständigen Sicherheitsplan aufstellen.....148
Anhang B Vollständige lokale Python Werkstatt 157
Anhang C Konfigurationen kontrolliert anwenden.....174
Anhang D Wiederherstellung und Notfallübungen 184
Anhang E Fehlerfälle systematisch lösen 194
Anhang F Begriffe und technische Orientierung 208
Ausführliches Kapitelverzeichnis.....213
Quellen und weiterführende Dokumentation.....223
Stichwortverzeichnis.....229
Impressum.....236

1 Risiken verstehen und Schutzziele festlegen

1.1 Was du eigentlich schützen möchtest

Informationssicherheit schützt nicht nur geheime Dateien. Vertraulichkeit bedeutet, dass Informationen nur für Berechtigte zugänglich sind. Integrität betrifft die beabsichtigte Richtigkeit und Unveränderтheit von Daten. Verfügbarkeit bedeutet, dass du benötigte Funktionen und Informationen rechtzeitig benutzen kannst.

Für die Lesegarten-Terminliste sind alle drei Ziele relevant. Unberechtigte sollen die Kontaktdaten nicht lesen. Eine veränderte Kontoverbindung darf nicht unbemerkt zu einer falschen Zahlung führen. Nach einem Geräteausfall müssen Termine weiterhin verfügbar sein. Eine verschlüsselte, aber verlorene einzige Datei erfüllt den letzten Zweck nicht.

Schreibe für deine wichtigsten Daten auf, welche dieser Folgen besonders schwer wiegt. Eine öffentlich bestimmte Veranstaltungsankündigung braucht keinen Geheimnisschutz wie eine Teilnehmerliste. Ihre Integrität bleibt trotzdem wichtig: Eine manipulierte Ankündigung kann auf eine fremde Zahlungsseite führen.

1.2 Mit realistischen Szenarien arbeiten

Ein Risiko entsteht aus möglichen Ereignissen und deren Folgen. Die genaue Eintrittswahrscheinlichkeit lässt sich im privaten Alltag selten belastbar ausrechnen. Eine qualitative Einschätzung ist trotzdem nützlich, wenn du ihre Annahmen benennst. Frage beispielsweise, wie leicht ein verlorenes Smartphone ersetzt werden kann und welche Konten darüber erreichbar sind.

Verwechsle eine spektakuläre Angriffstechnik nicht mit deinem dringendsten Problem. Ein mehrfach verwendetes Passwort, ein ungepflegter Router oder eine einzige ungesicherte Fotobibliothek sind konkrete Ansatzpunkte. Deren Behebung verbessert deinen Zustand auch dann, wenn du keine individuelle Angriffswahrscheinlichkeit kennst.

Ein Gerät kann durch einen Angriff, einen Bedienfehler, einen Defekt oder ein verlorenes Konto ausfallen. Gute Schutzmaßnahmen berücksichtigen mehrere Ursachen. Eine unabhängige Sicherung schützt beispielsweise auch vor versehentlichem Löschen und nicht nur vor Erpressungssoftware.

1.3 Angriffsfläche und Vertrauensgrenzen

Angriffsfläche bezeichnet die erreichbaren Möglichkeiten, mit deinem System zu interagieren. Dazu gehören öffentliche Dienste, Anmeldemasken, Dateiuploads, installierte Erweiterungen und Verwaltungszugänge. Ein ungenutzter öffentlich erreichbarer Dienst vergrößert diese Fläche ohne betrieblichen Nutzen.

Eine Vertrauensgrenze liegt dort, wo Daten oder Befehle zwischen unterschiedlich kontrollierten Bereichen wechseln. Ein E-Mail-Anhang kommt von außen auf deinen Rechner. Eine Webanwendung greift mit eigenen Rechten auf eine Datenbank zu. Ein Administrationskonto verändert die Infrastruktur. An solchen Übergängen sind klare Regeln besonders wichtig.

Die Grenze verläuft nicht einfach zwischen Internet und Heimnetz. Ein kompromittiertes Smartphone kann bereits im eigenen WLAN stehen. Ein fremdes Dokument kann innerhalb einer vertrauten Cloudablage liegen. Entscheidend ist, welche Identität, welcher Zugriff und welcher Datenfluss tatsächlich erlaubt werden.

1.4 Schutz in mehreren Ebenen aufbauen

Mehrere Ebenen helfen, wenn eine einzelne Maßnahme versagt. Ein gepflegter Server begrenzt bekannte Schwachstellen. Ein eingeschränkter Zugang reduziert Erreichbarkeit. Gute Authentifizierung erschwert eine Kontoübernahme. Eine unabhängige Sicherung begrenzt bestimmte Folgen eines trotzdem erfolgreichen Angriffs.

Diese Ebenen sind nicht beliebig austauschbar. Zehn Warnprogramme ersetzen keine fehlenden Updates. Eine Sicherung ersetzt keine Zugriffskontrolle für vertrauliche Informationen. Wähle Maßnahmen nach der Aufgabe und prüfe ihre tatsächliche Wirkung.

Das NIST Cybersecurity Framework 2.0 ordnet Sicherheitsarbeit unter anderem nach Steuerung, Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Du kannst diese Perspektiven auch für eine kleine Umgebung nutzen, ohne daraus ein umfangreiches Verwaltungsprojekt zu machen. [D01]

1.5 Tarnung richtig einordnen

Ein anderer SSH-Port kann automatisiertes Hintergrundrauschen verringern. Er ist keine belastbare Authentifizierung. Ein entfernter Versionsbanner reduziert einzelne leicht ablesbare Informationen, schließt aber eine vorhandene Schwachstelle nicht. Gepatchte Distributionen können außerdem Sicherheitskorrekturen zurückportieren, ohne jede sichtbare Versionszeichenfolge grundsätzlich zu verändern.

Auch das Abschalten von Ping macht einen Rechner nicht unsichtbar. Andere Protokolle und erreichbare Dienste bleiben beobachtbar. Besonders IPv6 benötigt bestimmte ICMPv6-Nachrichten für wesentliche Netzwerkfunktionen. Pauschale Sperren können deshalb Verbindungen beschädigen. [D36]

Beschreibe eine Maßnahme mit ihrer wirklichen Wirkung: „Verwaltungsdienst nur über das VPN erreichbar“ ist überprüfbar. „Für Angreifer unsichtbar“ ist eine unzuverlässige Zusage. Du gewinnst Sicherheit durch weniger unnötige Zugriffe, belastbare Identitätsprüfung und gepflegte Systeme.

1.6 Einen eigenen Prüfrahmen festlegen

Übungen dieses Buchs beziehen sich auf deine eigenen Geräte, lokale Testdaten und Systeme, für deren Prüfung du verantwortlich bist. Lege vor einer Netzwerkprüfung Ziel, Umfang und Zeitpunkt fest. Ein Scanner für das eigene Testnetz wird nicht ungeprüft gegen einen fremden Dienst eingesetzt.

Trenne Beobachtung und Änderung. Eine Liste laufender Dienste ist eine Bestandsaufnahme. Das Stoppen eines Dienstes ist ein Eingriff mit möglichen Folgen. Eine lokale Simulation einer Firewallregel verändert die echte Firewall überhaupt nicht. Diese Unterschiede werden in den Praxisbeispielen ausdrücklich gemacht.

Halte einen bekannten Ausgangszustand fest. Bei einer Konfigurationsänderung brauchst du eine Sicherung, einen erreichbaren Rückweg und einen nachfolgenden Test. Ein zweiter funktionierender Verwaltungszugang kann im passenden Fall wichtiger sein als eine sofort besonders strenge Regel.

1.7 Werkstatt mit drei konkreten Risiken

Wähle E-Mail-Konto, Smartphone und einen wichtigen Datenordner. Beschreibe je einen möglichen Verlust und eine überprüfbare Gegenmaßnahme. Für das E-Mail-Konto kann das eine stärkere Anmeldung mit gesichertem Wiederherstellungsweg sein; für den Datenordner eine unabhängige Sicherung mit Rücklesetest.

Notiere, woran du den Abschluss erkennst. „Backup einrichten“ bleibt ungenau. „Eine gelöschte Übungsdatei in einen anderen Ordner zurückholen und öffnen“ ist ein überprüfbarer Erfolg.

2 Bestandsaufnahme und ein tragfähiger Sicherheitsplan

2.1 Geräte und Konten erfassen

Beginne mit einer Liste deiner regelmäßig verwendeten Geräte. Notiere Zweck, Betriebssystem, verantwortliche Person und den bekannten Updatezustand. Ergänze Router, Netzwerkspeicher und Smart-Home-Zentrale. Ein alter Mini-PC im Schrank kann weiterhin als öffentlich erreichbarer Server arbeiten, obwohl niemand ihn im Alltag beachtet.

Erfasse außerdem zentrale Konten: E-Mail, Geräteplattform, Passwortmanager, Cloudspeicher, Domainverwaltung und gegebenenfalls Hosting. Bei diesen Konten kann eine Übernahme weitere Dienste betreffen. Die Liste selbst enthält keine Kennwörter oder Wiederherstellungscodes, sondern verweist auf deren geschützte Aufbewahrung.

Prüfe, welche Geräte und Konten wirklich noch benötigt werden. Ein ungenutztes Konto kann eine alte Freigabe oder ein weiterhin gültiges Anwendungstoken besitzen. Entferne solche Abhängigkeiten kontrolliert und bewahre benötigte Daten vorher auf.

2.2 Abhängigkeiten sichtbar machen

Ein Wiederherstellungsweg darf nicht im Kreis laufen. Wenn dein Passwortmanager nur über das E-Mail-Konto erreichbar ist und dessen einziges Passwort ausschließlich im gesperrten Passwortmanager liegt, brauchst du einen unabhängigen Notfallzugang.

Zeichne die wichtigsten Verbindungen auf. Welche E-Mail-Adresse empfängt Rücksetzlinks? Welches Gerät enthält den zweiten Faktor? Wer verwaltet Domain und DNS? Wo liegt der

Schlüssel der Sicherung? Die Antworten dürfen auf getrennte geschützte Aufbewahrungsorte verweisen, statt Geheimnisse in eine offene Übersicht zu schreiben.

Bei gemeinsam genutzten Diensten ist zusätzlich eine Vertretung nötig. Eine zweite berechtigte Person sollte den vorgesehenen Notfallweg kennen. Das bedeutet nicht, dass alle dasselbe Administratorkennwort erhalten. Eigene Konten und klar zugewiesene Rechte sind besser nachvollziehbar.

2.3 Daten nach Bedeutung und Empfängerkreis ordnen

Trenne öffentliche Informationen, interne Arbeitsdaten und besonders schützenswerte Inhalte nach ihrer tatsächlichen Verwendung. Eine Teilnehmendenliste gehört nicht allein deshalb in einen öffentlichen Ordner, weil sie in einer bekannten Cloud liegt.

Prüfe Freigaben aus Sicht der empfangenden Person. Ein Link mit weitreichender Berechtigung kann mehr erlauben als der sichtbare Dateiname vermuten lässt. Teste insbesondere Bearbeitung, Download, Weitergabe und Ablaufdatum, soweit der Dienst solche Einstellungen anbietet.

Bewahre nicht vorsorglich jede alte Kopie unbegrenzt auf. Weniger unnötige Daten bedeuten weniger zu pflegende Zugriffe und geringere mögliche Folgen einer Offenlegung. Die notwendige Aufbewahrung richtet sich nach dem tatsächlichen Zweck und gegebenenfalls anwendbaren Regeln.

2.4 Prioritäten nach Wirkung setzen

Bearbeite zuerst zentrale Konten und Wiederherstellung, dann aktuelle Geräte, anschließend Sicherungen und öffentliche Dienste. Diese Reihenfolge ist ein Ausgangspunkt, keine starre Rangliste. Ein gerade aktiv ausgenutzter erreichbarer Dienst kann sofortiges Handeln verlangen.

Schätze neben der Wirkung den Pflegeaufwand ein. Eine Schutzfunktion, die du nach zwei Wochen wegen ständiger Fehlalarme abschaltest, ist keine dauerhaft gute Lösung. Eine einfache gepflegte Konfiguration ist für eine kleine Umgebung oft wirksamer als ein kaum verstandener komplexer Überwachungsaufbau.

Plane auch laufende Aufgaben: Updates prüfen, Sicherungen kontrollieren, Wiederherstellung üben und Zugriffe bei einem Geräte- oder Personenwechsel anpassen. Sicherheit besteht aus einem bekannten Ausgangszustand und einem beherrschten Änderungsprozess.

2.5 Maßnahmen überprüfbar beschreiben

Eine Maßnahme braucht einen Gegenstand, eine verantwortliche Person und einen Prüfschritt. „Der Server soll sicher werden“ ist kein Arbeitsauftrag. „Die Verwaltungsoberfläche soll aus dem Internet nicht erreichbar sein; Zugriff nur über den getesteten Verwaltungsweg“ ist konkreter.

Tabelle 2.1 Ein kleiner Maßnahmenplan

Aufgabe	Nachweis	Zuständigkeit
Zentrales Konto absichern	Zweiter Zugang und Wiederherstellung getestet	Kontoinhaber
Geräte aktualisieren	Unterstützter Stand und Neustart geprüft	Gerätenutzer
Sicherung prüfen	Übungsdatei erfolgreich zurückgelesen	Datenverantwortliche
Freigaben bereinigen	Nicht benötigte Links widerrufen	Dateieigentümer
Fernzugriff begrenzen	Zugriff von außen und innen geprüft	Serververwaltung

Ein Nachweis beschreibt einen konkreten Test. Ein grünes Symbol allein kann auf einen veralteten Stand oder einen zu engen Prüfbereich zurückgehen. Notiere deshalb bei wichtigen Prüfungen auch Zeitpunkt und Umfang.

2.6 Änderungen und Rückwege planen

Vor einem Eingriff in Router, Firewall oder SSH legst du fest, wie du zurückkommst. Ein physischer Konsolenzugang oder eine geeignete Providerkonsole kann einen ausgesperrten Fernzugang retten. Prüfe diesen Weg vor dem Eingriff, nicht erst danach.

Ändere möglichst einen zusammenhängenden Sachverhalt. Wenn du gleichzeitig DNS, Zertifikate, Firewall und Container austauschst, wird eine Störung schwer zuzuordnen. Halte die letzte Änderung kurz fest und prüfe danach die beabsichtigte Funktion.

Ein Rollback ist nicht immer eine geeignete Sicherheitslösung. Eine alte Version mit ausgenutzter Schwachstelle darf nicht dauerhaft wieder öffentlich betrieben werden. Der Rückweg muss deshalb Funktion und verbleibendes Risiko berücksichtigen; vorübergehende Abschaltung kann die richtige Zwischenlösung sein.

2.7 Werkstatt mit einem erreichbaren Wochenziel

Erstelle eine Bestandsliste mit fünf wichtigen Konten oder Geräten. Suche eine bislang unbekannte Abhängigkeit, etwa eine alte Wiederherstellungsadresse. Wähle daraus eine Maßnahme, die du vollständig ausführen und prüfen kannst.

Bewahre die Übersicht so auf, dass sie im Notfall erreichbar bleibt und keine offenen Geheimnisse enthält. Kontrolliere nach einer Woche, welche Punkte abgeschlossen, ungeklärt oder durch eine neue Erkenntnis verändert sind.

3 Phishing und Social Engineering erkennen

3.1 Die geforderte Handlung untersuchen

Social Engineering beeinflusst Menschen, damit sie eine für den Angreifer nützliche Handlung ausführen. Das kann eine Zahlung, eine Anmeldung, die Freigabe eines Codes oder die Installation eines Programms sein. Die Nachricht muss keine Schadsoftware enthalten, um Schaden anzurichten.

Frage zuerst, was du tun sollst und ob dieser Vorgang zu deiner tatsächlichen Situation passt. Zeitdruck, eine angebliche Weisung und ein ungewöhnlicher Ausweichkanal sind wichtige Hinweise. Sie sind keine Beweise für Betrug, rechtfertigen aber eine unabhängige Prüfung.

Gute Sprache, ein bekanntes Logo und persönliche Angaben beweisen keine Echtheit. Öffentliche Informationen und gestohlene Nachrichten können eine Anfrage glaubwürdig machen. Auch automatische Text- und Sprachwerkzeuge senken den Aufwand für überzeugend formulierte Täuschungen.

3.2 Links und Domains richtig lesen

Lies bei einer Adresse den tatsächlich verwendeten Hostnamen. Bei konto.beispiel.example gehört konto zur Domain beispiel.example. Bei beispiel.example.anmeldung.invalid ist die vertraut aussehende Zeichenfolge dagegen nur ein vorderer Teil eines anderen Namens. Die reservierten Beispieldomains hier bezeichnen keine echten Dienste.

Ein Schlosssymbol oder HTTPS bedeutet nicht, dass ein Unternehmen hinter einer Seite vertrauenswürdig ist. Es betrifft zunächst die Verbindung und das Zertifikat für den aufgerufenen

Namen. Auch eine betrügerische Seite kann ein gültiges Zertifikat besitzen.

Für einen wichtigen Vorgang öffnest du die bekannte App oder eine selbst gespeicherte Adresse. Ein aus der Nachricht übernommener Link wird nicht dadurch unabhängig, dass du ihn in ein anderes Browserfenster kopierst. Bei verkürzten URLs fehlt zusätzlich die unmittelbare Sicht auf das Ziel.

3.3 E-Mail-Prüfungen richtig einordnen

Die angezeigte Absenderbezeichnung ist frei gestaltbar. Eine ähnliche E-Mail-Adresse kann leicht übersehen werden. Bei einer unerwarteten Änderung von Zahlungsdaten überprüfst du deshalb den Vorgang über einen bereits bekannten Kontaktweg.

SPF, DKIM und DMARC helfen empfangenden Maildiensten, bestimmte technische Absender- und Domainbeziehungen zu prüfen. Ein bestandener Test beweist nicht die Gutartigkeit des Inhalts. Eine kontrollierte oder übernommene Domain kann formal korrekt authentifizierte Betrugsmails verschicken. [D34]

Auch ein echtes übernommenes Postfach kann eine glaubwürdige Nachricht senden. Eine laufende Unterhaltung und bekannte Anhänge ersetzen deshalb keine Prüfung ungewöhnlicher Zahlungs- oder Zugriffsanforderungen. Trenne die Echtheit eines technischen Versandwegs von der Berechtigung der konkreten Handlung.

3.4 Telefonbetrug und synthetische Stimmen

Ein angezeigter Name oder eine Rufnummer ist kein belastbarer Identitätsnachweis. Stimmen und Videos können manipuliert oder synthetisch erzeugt werden. Suche nicht nur nach sichtbaren Fehlern wie unnatürlichen Händen oder Lippenbewegungen; solche Merkmale verändern sich und können ganz fehlen.

Bei einer überraschenden Zahlungsanforderung beendest du das Gespräch und rufst über eine dir bereits bekannte Nummer zurück. Verwende nicht einfach die Nummer, die dir die anrufende Person diktiert. Wenn eine angebliche Führungskraft keinen unabhängigen Rückruf zulässt, bleibt die Anfrage ungeklärt.

Ein vereinbartes Familienkennwort kann in manchen Situationen helfen, ist aber kein unfehlbarer Faktor. Es kann weitergegeben oder mitgelesen werden. Für wichtige finanzielle Vorgänge sind ein bekannter Rückkanal und ein abgestimmtes Freigabeverfahren belastbarer als ein einziges wiederverwendetes Wort.

3.5 Anmeldecodes und Zustimmung schützen

Gib Einmalcodes nicht an eine Person weiter, die dich überraschend kontaktiert. Ein Code kann gerade den Zugriff eines Angreifers bestätigen. Eine unerwartete Push-Anfrage lehnst du ab und prüfst das Konto anschließend über den bekannten Zugang.

Auch eine scheinbar harmlose Zustimmung kann eine Anwendung zum Lesen von E-Mails oder Dateien berechtigen. Lies bei einer Kontoverknüpfung die angeforderten Rechte und den tatsächlichen Anbieter. Entferne nicht benötigte Anwendungen in der Kontoübersicht.

Phishingresistente Anmeldeverfahren verringern bestimmte Risiken einer gefälschten Anmeldeseite. Sie beseitigen aber nicht jede Form von Täuschung, etwa eine von dir selbst veranlasste falsche Überweisung. Identitätsschutz und Freigabe einer fachlichen Handlung bleiben unterschiedliche Aufgaben. [D07]

3.6 Wenn du bereits geklickt hast

Ein Klick allein bedeutet nicht automatisch eine vollständige Geräteübernahme. Entscheidend ist, was danach passiert ist.

Wurden Daten eingegeben, ein Programm gestartet, eine Zustimmung erteilt oder eine Datei heruntergeladen? Notiere den beobachteten Ablauf möglichst genau.

Wenn du ein Kennwort eingegeben hast, sichere das betroffene Konto über ein vertrauenswürdiges Gerät und den bekannten Dienstzugang. Beende unberechtigte Sitzungen und prüfe Wiederherstellungswege, Weiterleitungen und verbundene Anwendungen. Eine reine Kennwortänderung widerruft nicht bei jedem Dienst jede bestehende Sitzung.

Bei einer Zahlung kontaktierst du unverzüglich den zuständigen Zahlungsdienst beziehungsweise deine Bank über einen bekannten Weg. Bei einem verwalteten Arbeitsgerät informierst du die zuständige IT. Bewahre die Nachricht für die Untersuchung auf, ohne sie unkontrolliert an weitere Personen zu verteilen.

3.7 Werkstatt mit einem unabhängigen Rückkanal

Entwirf drei fiktive Anfragen: eine geänderte Bankverbindung, eine unerwartete Supportmeldung und eine Bitte um einen Anmeldecode. Bestimme für jede Anfrage die geforderte Handlung und den unabhängigen Prüfweg.

Erkläre anschließend, warum ein gültiges HTTPS-Zertifikat, eine bekannte Stimme und eine technisch authentifizierte E-Mail jeweils keine vollständige Freigabe der Handlung darstellen. Ziel ist ein wiederholbarer Entscheidungsweg, kein Wettbewerb beim Erkennen möglichst verdächtiger Formulierungen.

4 Identität Passwörter und Passkeys

4.1 Ein Konto ist mehr als sein Kennwort

Ein Konto verbindet Identität, Berechtigungen und Wiederherstellungswege. Prüfe neben der Anmeldung auch hinterlegte Geräte, aktive Sitzungen, Rücksetzadresse und verbundene Anwendungen. Ein starkes Kennwort schützt nicht gegen jeden bereits freigegebenen Zugriff.

Für ein Administrationskonto sind andere Rechte nötig als für eine gewöhnliche Benutzung. Verwende getrennte Konten, wenn die Plattform und dein Arbeitsablauf das sinnvoll unterstützen. Eine versehentlich gestartete Anwendung soll nicht selbstverständlich alle Verwaltungsrechte erhalten.

Beim Lesegarten darf die zweite Person Dokumente bearbeiten, aber nicht Domain und Sicherungsaufbewahrung verändern. Diese Trennung bleibt auch dann wichtig, wenn beide Menschen vertrauenswürdig sind. Sie begrenzt die Folgen von Fehlern und kompromittierten Konten.

4.2 Lange und eindeutige Kennwörter verwenden

Ein Kennwort gehört jeweils zu einem Dienst. Wiederverwendung verknüpft die Sicherheit deiner Konten: Eine gestohlene Kombination kann bei anderen Anbietern ausprobiert werden. Ein Passwortmanager erleichtert lange zufällige Kennwörter, ohne dass du sie alle auswendig lernen musst.

Bei einem selbst gewählten Hauptkennwort sind unabhängig zufällig ausgewählte Wörter möglich. Entscheidend ist die tatsächliche Auswahl, nicht eine hübsch klingende erfundene Wortkette. Übernimm niemals eine in einem Buch veröffentlichte Beispielpassphrase als eigenes Geheimnis.