Netzwerkgrundlagen

Kryptografie-Grundlagen

Passwortsicherheit

Authentifizierung

Social Engineering

Websicherheit

Betriebssystemsicherheit

Endgeräteschutz

Datensicherung

Netzwerk- und Funkabsicherung

System- und Anwendungsabsicherung

Identitäts- und Zugriffsmanagement

E-Mail- und Kommunikationssicherheit

Web- und Browsersicherheit

Erkennung und Vorfallanalyse

Datenschutz und Informationsschutz

Datensicherheit und Governance

Incident Management

Schwachstellen- und Patch-Management

Netzwerkabsicherung

Kryptografie und Integrität

Bedrohungsanalyse

Dateiprüfung und Malware-Analyse

Cloud- & Datensicherheit

Endgerätesicherheit

Netzwerksicherheit und VPN

Kryptografie und Datenspeicher

Angriffsflächen und Schwachstellen

Incident Response & Governance

Datensicherung und Wiederherstellung

Eigene IP- und MAC-Adresse ermitteln

Ermittle auf deinem eigenen Computer die lokale IP-Adresse und die MAC-Adresse des aktiven Netzwerkadapters. Nutze die System-Netzwerkübersicht oder passende Bordmittel deines Betriebssystems.

Prüfe, dass die IP zum aktiven Adapter gehört und die MAC-Adresse als Hardwareadresse desselben Adapters angezeigt wird. Vergleiche keine Werte verschiedener Adapter.

Erreichbarkeit mit Ping testen

Teste mit dem Ping-Bordmittel, ob ein von dir gewählter, bekannter Host erreichbar ist, und beobachte die angezeigten Antwortzeiten oder Fehlermeldungen.

Wiederhole den Test und vergleiche die Antworten. Ausbleibende Antworten beweisen nicht allein, dass ein Host offline ist: Firewalls können ICMP blockieren.

DNS-Auflösung untersuchen

Frage mit nslookup einen bekannten Domainnamen ab. Notiere den abgefragten Namen, den verwendeten DNS-Server und die zurückgegebenen Adressen.

Prüfe, ob der Antwortname zur Anfrage passt und eine Adresse zurückgegeben wurde. Ergebnisse können je nach DNS-Server und Zeitpunkt abweichen.

Routing-Pfad nachvollziehen

Führe für einen bekannten öffentlichen Host tracert (Windows) oder traceroute (Linux/macOS) aus. Beobachte die angezeigten Zwischenstationen und Antwortzeiten.

Vergleiche die Hops und Zeiten innerhalb eines Durchlaufs. Sternchen oder fehlende Hops können durch Filterung oder ausbleibende Antworten entstehen und belegen keinen Defekt.

Netzwerkgrundlagen: Lokale Ports mit netstat prüfen

Nutze netstat, um auf deinem eigenen Rechner TCP-Ports im Zustand LISTENING sowie lokale UDP-Endpunkte zu untersuchen. Notiere bei TCP die zugehörigen Prozesse oder PIDs, sofern dein Betriebssystem diese anzeigt. UDP ist verbindungslos und hat keinen Listening-Zustand wie TCP.

Vergleiche die Ausgabe mit den Optionen deines Betriebssystems oder einer vertrauenswürdigen Systemübersicht. Prüfe, dass TCP-Listener als solche gekennzeichnet sind und UDP-Einträge nicht als wartende Verbindungen interpretiert werden.

SHA-256-Prüfsumme abgleichen

Lade eine beliebige Testdatei herunter und berechne lokal ihren SHA-256-Hash. Vergleiche ihn mit einem vom Anbieter veröffentlichten Prüfsummenwert. Verändere anschließend eine Kopie der Datei und berechne den Hash erneut.

Selbstprüfung: Der unveränderte Download stimmt mit dem veröffentlichten Hash überein; schon eine kleine Änderung an der Kopie ergibt einen anderen Hash. Ein Hash prüft Integrität, verschlüsselt die Datei aber nicht.

Symmetrische Verschlüsselung verstehen

Eine Kollegin und du wollt eine vertrauliche Datei austauschen. Erkläre anhand des Szenarios, welche Rolle derselbe geheime Schlüssel beim Ver- und Entschlüsseln spielt und warum der Schlüssel über einen geschützten Weg geteilt werden muss.

Selbstprüfung: Deine Erklärung nennt einen gemeinsamen geheimen Schlüssel für beide Vorgänge und erkennt, dass dessen Offenlegung die Vertraulichkeit gefährdet. Moderne Verfahren wie AES-GCM bieten zusätzlich Integritätsschutz.

Öffentlichen und privaten Schlüssel unterscheiden

Ordne in einem Szenario mit einem öffentlichen und einem privaten Schlüssel zu: Was darf an alle verteilt werden, was bleibt geheim? Beschreibe, wie eine Person eine Nachricht vertraulich an den Schlüsselinhaber sendet.

Selbstprüfung: Die sendende Person verschlüsselt mit dem öffentlichen Schlüssel des Empfängers; nur dessen passender privater Schlüssel kann die Nachricht entschlüsseln. Der private Schlüssel wird nicht weitergegeben.

Passphrasen auf Stärke vergleichen

Vergleiche ein kurzes, häufig verwendetes Passwort mit einer längeren Passphrase aus mehreren zufällig gewählten Wörtern. Überlege, welche Merkmale die Schwierigkeit des Erratens erhöhen und warum ein leicht vorhersehbares Muster trotz Länge schwach sein kann.

Selbstprüfung: Eine gute Einschätzung berücksichtigt Länge und Unvorhersehbarkeit statt bloß Zeichenarten zu zählen. Zufällig gewählte Wörter sind meist stärker als ein bekanntes Zitat; nutze für Konten einzigartige Zugangsdaten.

TOTP-Zwei-Faktor-Authentifizierung prüfen

Aktiviere TOTP für ein eigenes Testkonto, sofern verfügbar. Scanne den Einrichtungscode mit einer Authenticator-App, gib einen angezeigten Einmalcode ein und bewahre die angebotenen Wiederherstellungscodes sicher auf.

> Selbstprüfung: Die Einrichtung gilt als erfolgreich, wenn das Konto einen aktuellen App-Code akzeptiert und einen abgelaufenen Code nicht als neuen Code annimmt. Teile Einrichtungscode und Wiederherstellungscodes nicht.

E-Mail-Authentifizierungsergebnisse lesen

Nutze eine harmlose Beispiel-E-Mail mit vollständigen Kopfzeilen oder eine eigens an dich gesendete Nachricht. Suche nach Return-Path sowie SPF- und DKIM-Ergebnissen und vergleiche die angezeigten Domains mit der sichtbaren Absenderadresse.

> Selbstprüfung: Notiere, ob SPF und DKIM bestanden haben und auf welche Domain sie sich beziehen. Ein positives Ergebnis allein beweist nicht, dass eine Nachricht harmlos ist; widersprüchliche Domains sind ein Anlass zur Prüfung.

Pretexting-Muster erkennen

Lies ein fiktives Szenario: Eine anrufende Person gibt sich als IT-Support aus, behauptet, ein Konto werde gleich gesperrt, und verlangt sofort einen Anmeldecode. Markiere die Hinweise auf Manipulation und formuliere eine sichere Reaktion.

> Selbstprüfung: Erkannt werden sollten künstliche Dringlichkeit, Autoritätstäuschung und die Forderung nach einem Geheimnis. Beende den Kontakt und verifiziere die Anfrage über einen unabhängig bekannten offiziellen Kanal.

QR-Code-Ziel vor dem Öffnen prüfen

Verwende einen selbst erstellten oder vertrauenswürdig bereitgestellten Test-QR-Code. Prüfe mit einer Vorschau die vollständige Zieladresse, bevor du sie öffnest. Achte auf Schreibvarianten der Domain und unerwartete Weiterleitungen.

> Selbstprüfung: Du kannst die angezeigte Domain mit der erwarteten offiziellen Domain vergleichen und öffnest keinen Link, dessen Ziel unklar ist. Ein QR-Code selbst bestätigt weder die Echtheit noch die Sicherheit des Ziels.

TLS-Zertifikat im Browser untersuchen

Öffne die Sicherheitsinformationen einer bekannten Website im Browser und prüfe das Zertifikat: Gültigkeitszeitraum, Ausstellerkette und ob der aufgerufene Hostname in den Subject Alternative Names (SAN) enthalten ist.

> Selbstprüfung: Das Zertifikat ist zeitlich gültig, die Kette wird vom Browser als vertrauenswürdig bewertet und der Hostname passt zu einem SAN-Eintrag. Das allein garantiert nicht, dass die Website vertrauenswürdig handelt.

HTTP-Sicherheitsheader prüfen

Untersuche mit den Entwicklerwerkzeugen oder einem HTTP-Header-Viewer die Antwortheader einer eigenen oder öffentlichen Website. Suche nach Strict-Transport-Security (HSTS), Content-Security-Policy (CSP) und X-Frame-Options.

> Selbstprüfung: Halte fest, welche Header vorhanden sind und welche Werte sie haben. HSTS erzwingt HTTPS für passende Anfragen; CSP begrenzt unter anderem erlaubte Inhaltsquellen. Fehlende Header sind nicht automatisch der Beweis einer ausnutzbaren Schwachstelle.

Cookie-Sicherheitsattribute beurteilen

Öffne die Entwicklertools für eine Website, bei der du angemeldet bist, und prüfe die Attribute eines Sitzungscookies. Suche nach Secure, HttpOnly und SameSite und notiere, ob sie gesetzt sind.

> Selbstprüfung: Secure beschränkt die Übertragung auf HTTPS, HttpOnly verhindert den direkten Zugriff durch clientseitiges Skript, und SameSite steuert die Mitgabe bei seitenübergreifenden Anfragen. Bewerte die Einstellungen im Kontext der Anwendung.

Standardkonto und Administrator trennen

Prüfe auf deinem eigenen Rechner, ob du ein Administratorkonto und ein separates Standardkonto verwenden kannst. Führe eine harmlose Systemänderung aus dem Standardkonto heraus aus und beobachte, ob eine gesonderte Berechtigungsbestätigung erforderlich ist.

> Selbstprüfung: Alltägliche Arbeit ist mit dem Standardkonto möglich; privilegierte Änderungen verlangen eine ausdrückliche Autorisierung. Ändere keine UAC- oder Systemrichtlinien, wenn du deren Wirkung nicht kennst.

Autostart-Einträge nachvollziehen

Öffne auf deinem eigenen Gerät die integrierte Autostart- oder Anmeldeverwaltung. Notiere einige Einträge samt Herausgeber und Zweck. Recherchiere unbekannte Namen, bevor du etwas deaktivierst.

Selbstprüfung: Du kannst für jeden notierten Eintrag eine plausible Anwendung oder einen nachvollziehbaren Herausgeber angeben. Unbekannt bedeutet nicht automatisch schädlich; entferne nichts, dessen Funktion unklar ist.

Eingehende Firewall-Regeln kontrollieren

Öffne die lokale Firewall-Verwaltung deines eigenen Rechners und prüfe, ob eingehende Verbindungen standardmäßig blockiert werden und welche Ausnahmen zugelassen sind. Verändere keine Regeln, die du für Verbindung oder Verwaltung benötigst.

Selbstprüfung: Du kannst die Standardaktion für eingehende Verbindungen sowie mindestens eine erlaubte Ausnahme benennen. Ein vorsichtiger Test beschränkt sich auf die Konfiguration; vermeide Scans fremder Geräte.

Backup-Plan nach 3-2-1 erstellen

Wähle wichtige Testdateien und entwirf einen einfachen Sicherungsplan nach dem 3-2-1-Prinzip: drei Kopien, auf zwei unterschiedlichen Medientypen und eine Kopie an einem getrennten Ort. Plane außerdem einen regelmäßigen Wiederherstellungstest.

Selbstprüfung: Der Plan zählt drei Kopien einschließlich Original, nennt zwei Medientypen und eine räumlich getrennte Kopie. Beim Test lässt sich eine Datei aus der Sicherung tatsächlich wiederherstellen.

WLAN-Sicherheit: Verschlüsselung und Pre-Shared-Key prüfen

Aufgabe: Prüfen Sie an Ihrem eigenen Router oder einem autorisierten WLAN, ob WPA2-AES (CCMP) oder WPA3 aktiviert ist. Kontrollieren Sie außerdem, ob ein Pre-Shared-Key (WLAN-Passwort) gesetzt ist und ob er ausreichend lang und einzigartig ist. Vermeiden Sie WEP und WPA-TKIP.

Selbstüberprüfung: Die Konfiguration zeigt WPA2-Personal mit AES oder WPA3-Personal, keinen veralteten Mischbetrieb und einen gesetzten, starken, nicht anderweitig verwendeten Schlüssel.

Gastnetzwerk: logische Isolation überprüfen

Aufgabe: Richten Sie auf Ihrem eigenen Router ein separates Gast-WLAN ein oder prüfen Sie eine vorhandene Konfiguration. Testen Sie von einem Gerät im Gastnetz nur gezielt und autorisiert, ob ein bekannter interner Drucker oder freigegebener Ordner erreichbar ist.

Selbstüberprüfung: Die Router-Einstellung weist eine Trennung vom privaten LAN aus. Ein gezielter, erlaubter Verbindungstest zum ausgewählten internen Gerät scheitert; prüfen Sie zusätzlich die dokumentierten Regeln, denn ein einzelner Test belegt keine vollständige Isolation.

Paketmitschnitt: DNS-Abfrage im eigenen Testnetz untersuchen

Aufgabe: Erfassen Sie mit Wireshark auf Ihrem eigenen Gerät oder in einem autorisierten Testnetz den Verkehr während einer ausdrücklich unverschlüsselten DNS-Abfrage. Filtern Sie die Anzeige mit „dns“ und betrachten Sie Anfrage und Antwort.

Selbstüberprüfung: Wenn die Abfrage tatsächlich unverschlüsselt erfasst wird, können Sie passende DNS-Pakete und den angefragten Domainnamen erkennen. Fehlen sie, prüfen Sie Schnittstelle und Filter; DNS kann auch verschlüsselt oder über andere Transportwege übertragen werden.

DNS-over-HTTPS im Client erkunden

Aufgabe: Aktivieren Sie DNS-over-HTTPS in einem unterstützten Browser oder Client und rufen Sie eine Website auf. Sehen Sie sich, falls verfügbar, die Client-Einstellung oder Statusanzeige für den verwendeten DNS-Dienst an.

Selbstüberprüfung: Bestätigen Sie, dass DoH aktiviert ist und der vorgesehene Anbieter angezeigt wird. Ein Mitschnitt ohne UDP-Port-53-Verkehr allein beweist weder, dass alle DNS-Anfragen verschlüsselt sind, noch schließt er andere DNS-Wege aus.

Schadsoftware-Prävention: Dateierweiterungen vollständig anzeigen

Aufgabe: Konfigurieren Sie die Explorer- bzw. Dateimanager-Einstellungen Ihres Betriebssystems so, dass bekannte Dateierweiterungen stets sichtbar sind. Erstellen Sie eine Testdatei 'rechnung.pdf.exe' und prüfen Sie die Darstellung.

Selbstüberprüfung: Die Dateiendung '.exe' wird unmissverständlich am Ende des Dateinamens dargestellt, sodass potenzielle Spoofing-Tricks sofort auffallen.

Systemhärtung: Dienste vor Änderungen sicher beurteilen

Aufgabe: Sehen Sie auf Ihrem eigenen Rechner laufende Dienste durch. Wählen Sie einen Dienst nur dann zur Deaktivierung aus, wenn Sie seine Funktion geprüft haben und er nachweislich nicht benötigt wird; ändern Sie nichts an unbekannten oder systemkritischen Diensten. Prüfen Sie bei SMBv1 gezielt, ob das optionale Feature aktiviert ist.

Selbstüberprüfung: Nach einer begründeten Änderung ist der ausgewählte Dienst beziehungsweise das SMBv1-Feature deaktiviert, und die benötigten Systemfunktionen arbeiten weiterhin. Bei Unsicherheit lassen Sie die Einstellung unverändert.

SSH-Zugang mit Schlüsseln absichern

Aufgabe: Richten Sie auf einem eigenen Linux-Testsystem ein SSH-Schlüsselpaar ein und testen Sie die Anmeldung mit dem öffentlichen Schlüssel. Ändern Sie Authentifizierungseinstellungen nur mit Konfigurationsprüfung und funktionierendem Konsolenzugang, damit Sie sich nicht aussperren.

Selbstüberprüfung: Testen Sie in einer zweiten Sitzung ausdrücklich, ob eine Passwortanmeldung abgewiesen wird, während der Schlüsselzugang funktioniert. Prüfen Sie die aktive Serverkonfiguration; andere Authentifizierungswege können weiterhin erlaubt sein.

Berechtigungsmanagement: Least-Privilege-Prinzip im Arbeitsalltag umsetzen

Aufgabe: Richten Sie auf Ihrem primären Testsystem ein Standard-Benutzerkonto ohne lokale Administrationsrechte ein. Arbeiten Sie über dieses Konto und protokollieren Sie, wann UAC-Prompts die Eingabe von Admin-Credentials fordern.

Selbstüberprüfung: Der Befehl 'whoami /groups' listet für den aktiven Benutzer keine Mitgliedschaft in der lokalen Administratorengruppe mit administrativen Rechten auf.

Passwortsicherheit: Leaks sicher prüfen

Aufgabe: Prüfen Sie Ihre eigene E-Mail-Adresse auf einer seriösen Datenleck-Prüfseite. Geben Sie dort niemals ein Passwort ein. Ermitteln Sie, welche Konten betroffen sein könnten, und ändern Sie deren Passwörter direkt beim jeweiligen Dienst.

Selbstüberprüfung: Notieren Sie die betroffenen Dienste und bestätigen Sie, dass deren Passwörter geändert wurden; verwenden Sie jeweils ein einzigartiges Passwort.

Notfallzugriff im Passwortmanager planen

Aufgabe: Prüfen Sie, welche Notfallzugriffs- oder Wiederherstellungsoption Ihr Passwortmanager bietet. Falls Sie einen Export erwägen, beachten Sie, dass er sensible Zugangsdaten enthalten kann, und sichern Sie ihn nur verschlüsselt und angemessen geschützt.

Selbstüberprüfung: Sie können den vorgesehenen Wiederherstellungsweg erklären und wissen, wo die dazugehörigen Informationen sicher verfügbar sind. Prüfen Sie die Funktion anhand der Dokumentation des Anbieters; Master-Passwort, Wiederherstellungscodes und Notfallkontakte sind nicht bei allen Diensten gleich.

E-Mail-Sicherheit: SPF-Eintrag im DNS validieren

Aufgabe: Überprüfen Sie mit dem Befehl 'nslookup -type=TXT domain.de' den SPF-Eintrag einer beliebigen Unternehmensdomain. Analysieren Sie die angegebenen Mechanismen (z. B. include, ip4, ~all, -all).

Selbstüberprüfung: Die Ausgabe liefert einen validen TXT-Record, der mit 'v=spf1' beginnt und autorisierte Sender-IPs sowie die Enforcement-Richtlinie deklariert.

E-Mail-Sicherheit: DKIM- und DMARC-Einträge abfragen

Aufgabe: Rufen Sie per DNS-Abfrage den DMARC-Record einer Domain ab ('nslookup -type=TXT _dmarc.domain.de'). Bestimmen Sie, ob die Richtlinie auf 'none', 'quarantine' oder 'reject' gesetzt ist.

Selbstüberprüfung: Das Feld 'p=' im DMARC-String ist klar identifiziert und definiert die Behandlungsweise nicht-authentifizierter E-Mails durch empfangende Mailserver.

Browser-Sicherheit: Tracking-Schutz einstellen

Aufgabe: Aktivieren Sie im Browser den Schutz vor websiteübergreifendem Tracking und, falls verfügbar, das Löschen von Cookies beim Schließen. Prüfen Sie anschließend eine vertraute Website und beachten Sie mögliche Funktionseinschränkungen.

Selbstüberprüfung: Kontrollieren Sie die Browser-Einstellungen und vergleichen Sie die Ergebnisse eines Privacy-Tests vor und nach der Änderung. Ein Test bildet nur bestimmte Tracker und Fingerprinting-Merkmale ab.

Prozesse mit Process Explorer untersuchen

Aufgabe: Öffnen Sie Process Explorer auf einem eigenen Testrechner und betrachten Sie Prozessnamen, Herausgeber und Dateipfade. Ein Virustotal-Abgleich kann Dateien an einen Drittanbieter übermitteln; nutzen Sie ihn nur, wenn das datenschutzrechtlich vertretbar ist.

Selbstüberprüfung: Sie können für ausgewählte Prozesse erklären, zu welchem Programm sie gehören. Einzelne Erkennungen sind Hinweise, kein Beweis für Schadsoftware; prüfen Sie sie im Kontext und isolieren Sie nichts allein aufgrund eines Scores.

Systemprotokolle: Fehlgeschlagene Anmeldeversuche im Event Viewer finden

Aufgabe: Öffnen Sie die Windows-Ereignisanzeige (eventvwr.msc) unter 'Sicherheit'. Filtern Sie nach der Ereignis-ID 4625 (Fehlgeschlagene Anmeldung) und erzeugen Sie durch eine absichtliche Falscheingabe einen Eintrag.

Selbstüberprüfung: Das Log verzeichnet einen neuen Eintrag mit ID 4625, inklusive Timestamp, betroffener Kontobezeichnung und Anmeldetyp.

Sensible Dokument-Metadaten prüfen

Aufgabe: Untersuchen Sie eine eigene DOCX- oder PDF-Datei mit den verfügbaren Dokumenteigenschaften auf Autor, Organisation oder weitere unerwünschte Angaben. Entfernen Sie sensible Metadaten mit einer passenden Funktion oder einem geeigneten Werkzeug.

Selbstüberprüfung: Prüfen Sie die bereinigte Datei erneut mit einem Metadaten-Viewer. Halten Sie fest, welche Angaben tatsächlich entfernt wurden; die verfügbaren Felder und Ergebnisse hängen von Dateiformat und Werkzeug ab.

Speichermedien: Vollverschlüsselung von Datenträgern verifizieren

Aufgabe: Überprüfen Sie den Verschlüsselungsstatus aller lokalen Laufwerke mit BitLocker (manage-bde -status) unter Windows oder LUKS/FileVault auf anderen Plattformen. Stellen Sie sicher, dass das Betriebssystemlaufwerk verschlüsselt ist.

Selbstüberprüfung: Die Konsolenausgabe zeigt 'Verschlüsselungsprozentsatz: 100,0 %' und 'Schutzstatus: Ein' für alle relevanten Systemvolumes.

Notfall-Kontakt- und Meldeplan erstellen

Aufgabe: Erstellen Sie für Haushalt oder Kleinbetrieb eine kurze, offline verfügbare Liste mit zuständigen IT-Ansprechpersonen, Internetanbieter und gegebenenfalls Bank oder weiteren Stellen. Notieren Sie, wie ein Vorfall intern gemeldet wird und welche Isolierungsschritte nach dem vorab festgelegten Plan gelten.

Selbstüberprüfung: Die Liste ist ohne Zugriff auf betroffene Geräte erreichbar, enthält aktuelle Kontaktdaten und benennt, wen Sie bei Ransomware-Verdacht zuerst kontaktieren. Trennen Sie Geräte nicht pauschal vom Netz, sondern folgen Sie dem vereinbarten Plan.

Software-Updates und Schwachstellen unterscheiden

Aufgabe: Lassen Sie sich auf Ihrem eigenen Rechner verfügbare Software-Updates anzeigen. Wählen Sie ein veraltetes Programm und prüfen Sie anhand einer verlässlichen Hersteller- oder Sicherheitsquelle, ob bekannte Sicherheitslücken behoben werden.

Selbstüberprüfung: Sie können die verfügbaren Updates und eine geprüfte Sicherheitsmeldung benennen. Eine Update-Liste allein ist kein CVE-Scan und belegt nicht, dass sämtliche installierten Programme aktuell oder frei von Schwachstellen sind.

SMB-Dienste im eigenen Netz prüfen

Aufgabe: Listen Sie unter Windows mit „net share“ die Freigaben des eigenen Computers auf. Scannen Sie ein eigenes oder ausdrücklich freigegebenes lokales Netz mit einem geeigneten Werkzeug nach Hosts mit offenem TCP-Port 445.

Selbstüberprüfung: Unterscheiden Sie lokale Freigaben von erreichbaren SMB-Diensten anderer Hosts. Ein offener Port 445 weist nicht alle Freigaben oder deren Berechtigungen nach; prüfen Sie Freigaben und Zugriffsrechte separat.

Kryptografie: Dateivertraulichkeit mit GnuPG (GPG) absichern

Aufgabe: Erzeugen Sie ein lokales GPG-Schlüsselpaar. Verschlüsseln Sie eine Textdatei mit dem öffentlichen Schlüssel und entschlüsseln Sie die resultierende .gpg-Datei anschließend mit Ihrem privaten Schlüssel.

Selbstüberprüfung: Die verschlüsselte Datei ist im Texteditor unleserlich; nach dem Befehl 'gpg -d datei.gpg' stimmt der Klartext exakt mit dem Original überein.

IP-Adressen mit Abuse-Datenbanken einordnen

Aufgabe: Wählen Sie eine öffentliche IP-Adresse aus einem eigenen Log oder einer vertrauenswürdigen Übungsquelle. Suchen Sie sie in einer öffentlichen Reputationsdatenbank und notieren Sie verfügbare Meldungen sowie gegebenenfalls Informationen zum Netzwerkbetreiber.

Selbstüberprüfung: Trennen Sie beobachtete Meldungen von Vermutungen. Ein Score oder ASN kann fehlen; einzelne Meldungen beweisen nicht, dass die Adresse bösartig ist. Berücksichtigen Sie Zeitpunkt, Quelle und den Zusammenhang Ihrer Beobachtung.

Datei-Hash ohne Upload nachschlagen

Aufgabe: Berechnen Sie den SHA-256-Hash einer nicht vertraulichen Übungsdatei und suchen Sie ausschließlich den Hash in einer öffentlichen Analyseplattform, ohne die Datei hochzuladen.

Selbstüberprüfung: Vergleichen Sie den berechneten Hash mit der Suchanfrage und notieren Sie, ob Ergebnisse angezeigt werden. Ein fehlender Datensatz ist nicht aussagekräftig genug, um auf eine frühere Analyse zu schließen; Scannergebnisse sind Hinweise, keine definitive Diagnose.

Cloud-Sicherheit: Öffentliche Freigaben und Sharing-Links auditieren

Aufgabe: Prüfen Sie die Freigabeeinstellungen in einem Cloud-Speicherdienst (z. B. Google Drive, OneDrive). Identifizieren Sie alle Dateien mit dem Status 'Jeder mit dem Link kann zugreifen'.

Selbstüberprüfung: Reduzieren Sie die Berechtigung sensibler Testdateien auf 'Nur bestimmte Personen'. Der Link darf in einem Inkognito-Fenster ohne Login nicht mehr abrufbar sein.

USB-Massenspeicher-Richtlinien prüfen

Aufgabe: Prüfen Sie auf einem eigenen Testgerät die Betriebssystemeinstellungen oder Richtlinien für Wechseldatenträger. Finden Sie heraus, welche konkrete Einstellung den Zugriff oder die Installation von USB-Massenspeichern einschränkt, bevor Sie sie testweise ändern.

Selbstüberprüfung: Notieren Sie die Richtlinie und ihre dokumentierte Wirkung. Testen Sie nur mit einem entbehrlichen Medium und stellen Sie sicher, dass Sie die Einstellung zurücksetzen können; Laufwerksbuchstaben und Zugriffsverhalten hängen von System und Richtlinie ab.

DNS-Anfragen bei aktiver VPN-Verbindung prüfen

Aufgabe: Verbinden Sie sich mit Ihrem VPN und führen Sie einen DNS-Leak-Test durch. Vergleichen Sie die angezeigten Resolver mit den DNS-Angaben Ihres VPN-Anbieters; dieser kann auch Resolver Dritter einsetzen.

Selbstüberprüfung: Prüfen Sie, ob die Ergebnisse zu den Angaben des Anbieters passen. Ein abweichender Resolver kann auf ein DNS-Leak hindeuten, ist allein aber kein Beweis. Testdaten können unvollständig sein.

Einen verschlüsselten Dateicontainer testen

Aufgabe: Erstellen Sie mit VeraCrypt einen kleinen Testcontainer, speichern Sie eine harmlose Testdatei darin und hängen Sie den Container anschließend aus. Verwenden Sie nur eigene Testdaten.

Selbstüberprüfung: Ohne den Container zu entsperren, lässt sich die darin gespeicherte Datei nicht öffnen. Nach dem korrekten Entsperren sollte sie wieder zugänglich sein.

Eigene öffentliche Angriffsfläche recherchieren

Aufgabe: Prüfen Sie in Shodan ausschließlich eine öffentliche IP-Adresse, deren Untersuchung Ihnen gehört oder für die Sie eine ausdrückliche Berechtigung haben. Notieren Sie gefundene Dienste und den Erfassungszeitpunkt; nehmen Sie keine aktiven Tests vor.

Selbstüberprüfung: Ordnen Sie jeden Fund einem bekannten eigenen Dienst zu und prüfen Sie ihn anschließend direkt über autorisierte Verwaltungswege. Keine Treffer bedeuten nicht, dass die Angriffsfläche sicher oder vollständig erfasst ist; Shodan-Daten können veraltet sein.

Incident Response: Erstellung eines Post-Mortem-Berichts

Aufgabe: Verfassen Sie anhand eines simulierten Phishing-Vorfalls einen einseitigen Kurzbericht mit Zeitachse, Root-Cause-Analyse und drei konkreten Präventionsmaßnahmen.

Selbstüberprüfung: Der Bericht beantwortet Wann, Was, Wer und Wie präzise und definiert klare Verantwortlichkeiten zur Behebung der identifizierten Sicherheitslücke.

Eine Backup-Wiederherstellung praktisch testen

Aufgabe: Stellen Sie ausgewählte Dateien aus einem vorhandenen Backup in ein separates Testverzeichnis wieder her. Wenn Originaldateien und zuvor erstellte Prüfsummen verfügbar sind, vergleichen Sie die Hashwerte.

Selbstüberprüfung: Öffnen Sie die wiederhergestellten Dateien mit passenden Anwendungen. Stimmen vorhandene Prüfsummen überein, bestätigt das die Integrität der verglichenen Dateien; ohne Referenzprüfsummen lässt sich daraus keine Hash-Übereinstimmung ableiten.