IT–Security: Was braucht man wirklich?

Rainer Peipp

09. April 2018

Vorbemerkung

Die nachfolgende Präsentation ist in (enger) Anlehnung an eine Artikelserie der Zeitschrift c't, Ausgabe 01/2018 entstanden.

Allgemeine Überlegungen

- Security darf man nicht mit der Gießkanne verteilen → Nebenwirkungen
- Schlechte Security kann sehr wohl gefährlich und damit schlimmer sein als *gar nichts*.

  Beispiele:

  - Personal Firewall kappt Update–Mechanismus → Infektion mit Trojaner
  - Veraltete Verschlüsselung ermöglicht Angriff auf *Secret* und damit auch auf aktuelle Verschlüsselungsverfahren
  - Zu komplizierte Passwortregeln bringen Anwender dazu, sich die Passwörter auf unsichere Arten zu notieren (Zettel unter dem Schreibtisch)
  - Falsche Sicherheitsanforderungen (kein Zugriff auf USB–Ports) zwingen Anwender zu unsicheren Umwegen
  - Security muss mit den Befürfnissen der Benutzer abgewogen werden.
  - Maßvoller und zielgerichteter Einsatz von Security ist notwendig.

Abwehr von Schädlingen

Firewall

Filtert ein- und ausgehende Netzwerkverbindung anhand eines Regelsatzes. Wenn zwischen Computer und Internet ein Router hängt, übernimmt dieser meist die Aufgabe der Firewall. Ist der Computer direkt an ein öffentliches Netzwerk angeschlossen (z. B. Hotspot), kann eine *Personal Firewall* die Sicherheit verbessern. Ausgehender Datenverkehr lässt sich bei universell genutzten Computern kaum sinnvoll filtern.

Schütz

- vor unerwünschten Zugriffen auf lokale Dienste, etwa bei der Nutzung öffentlicher Hotspots.

Schütz nicht

- vor dem Abfluss persönlicher Daten
- zuverlässig vor der Infektion durch Viren/Trojaner

Risiken & Nebenwirkungen

- Störung von Programmen und Diensten, wenn erwartete Verbindungen blockiert werden
- Fehlkonfigurationen können Löcher in dies Sicherheit reißen

Adblocker

Sollen in Webseiten eingebette Werbung unterdrücken.

Schütz

- vor Tracking durch Werbung
- vor Schadcode, den Online-Kriminelle über Werbenetzwerke ausliefern

Schütz nicht

- vor Schadcode, der direkt in die Webseite eingebettet ist

Risiken & Nebenwirkungen

- einige Webseiten sperren Nutzer mit Adblockern aus
- Webseitenbetreiber werden um ihre (legalen) Werbeeinnahmen gebracht

Sicherheits–Updates

Schließen von bekannt gewordenen Sicherheitslücken. Besonders wichtig für Betriebssystem, Browser mit Plugins, PDF-Viewer, Office-Packet, Email-Client, Router

Schütz

- vor Angriffen auf bekannte Sicherheitslücken

Schütz nicht

- vor Schadcode, den der Nutzer selbst ausführt
- vor Zero-Day-Lücken (die im Geheimen enteckt und ausgenutzt werden, ohne dass der Hersteller informiert wurde)

Risiken & Nebenwirkungen

- durch den hohen Zeitdruck gibt es immer wieder Qualitätsprobleme bei den Updates

Virenschutz

Versucht Schädlinge anhand ständig zu aktualisierenden Signaturdatenbanken und Verhaltenüberwachung zu entdecken und auszuschalten.

Schütz

- vor der Infektion durch bekannte Schädlinge, die bereits seit einiger Zeit im Umlauf sind.
- oft vor bisher unbekannten Viren, die durch ihr schadhaftes Verhalten auffallen.
- vor der unabsichtlichen Weitergabe von Schadcode.

Schütz nicht

- vor der Ausnutzung ungepatchter Sicherheitslücken.
- vor allen Schädlingen. Insbesondere sehr frische Viren werden oftmals trotz Antivirenprogramm klaglos ausgeführt.

Risiken & Nebenwirkungen

- Nachrüstbare Schutzprogramme kosten meist Geld oder zeigen Werbung an.
- In Virenschutz-Programmen können Sicherheitslücken klaffen, die den Rechner angreifbar machen.
- Es kann zu Fehlalarmen kommen, die das System schlimmstenfalls lahmlegen.
- Die Schutzprogramme telefonieren häufig detaillierte Informationen über das System bis hin zu persönlichen Dateien nach Hause.
- Die Open–Source–Lösung ClamAV hat (noch) keine vergleichbare Erkennungsrate wie die kommerziellen Lösungen.

NoScript

Browser-Erweiterung, welche erlaubt, die Ausführung von JavaScript-Code stark zu reglementieren.

Schütz

- vor Angriffen, die Sicherheitslücken in Browser und Plug-ins ausnutzen.
- vor XSS-Angriffen (Cross-Site-Scripting).
- vor Clickjacking.
- vor Tracking durch eingebettete Skripte.

Schütz nicht

- vor Phishing.
- vor dem Download von Viren.
- vor Angriffen, bei denen eine eigentlich vertrauenswürdige Website, die auf der Whitelist steht, kompromittiert wurde.
- vor Angriffen, die komplett ohne browserseitige Skripte auskommen.

Risiken & Nebenwirkungen

- Viele Websites funktionieren beim ersten Besuch nicht oder nur teilweise, weil die Erweiterung die Ausführung des JavaScript-Codes blockiert. Erst nachdem man die Site auf die Whitelist gesetzt hat, funktioniert alles, wie es soll.
- Es ist häufig ein Eingreifen des Nutzers notwendig, was dazu führen kann, dass die Ausnahmen zu lasch konfiguriert werden oder die Erweiterung gar nach kurzer Zeit komplett ausgemustert wird.

Internetkommunikation gegen Lausch- und andere Angriffe schützen

Transportverschlüsselung

Verschlüsselung der Übertragung von Daten (TLS, SSL, https://, ...).

Schütz

- vor Massenüberwachung im Internet
- vor dem Mitlesen von Emails während des Sendens und Empfangens
- vor dem Mitlesen von Inhalten zwischen Webserver und Browser

Schütz nicht

- vor gezielter Überwachung einzelner Personen
- vor Spionage
- vor Zugriff auf die gesuchten Daten beim Provider

Risiken & Nebenwirkungen

- Vorspielen falscher Sicherheit: Die Daten werden nur für den Transport verschlüsselt und liegen dann beim Provider unverschlüsselt vor.
- Erfolgreiche Man-in-the-Middle-Attacken hebeln den Schutz aus.
- https:// allein gibt keinen Hinweis auf die Vertrauenswürdigkeit der Gegenseite.

Mailverschlüsselung

Ende-zu-Ende-Verschlüsselung mittels PGP oder S/MIME.

Schütz

- vor dem Zugriff Dritter (auch beim Provider) auf den Inhalt der Emails.

Schütz nicht

- vor Sicherheitslücken beim Sender oder Empfänger.

Risiken & Nebenwirkungen

- Schwache Verbreitung und komplizierte Handhabung (Schlüsselverwaltung bei PGP).
- S/MIME erfordert kostenpflichtige Zertifikate.
- Alltagstaugliche Verschlüsselung bieten Messenger wie Threema, Signal oder WhatsApp.

Tor

Netzwerk zur Anonymisierung von Verbindungsdaten. Zur Nutzung ist spezielle Client-Software notwendig.

Schütz

- vor der Analyse des Datenverkehrs durch Dritte.

Schütz nicht

- vor den Spuren, die man auf den besuchten Servern hinterlässt.

Risiken & Nebenwirkungen

- z. T. erschreckend schlechte Performance
- eine Reihe von Webseiten funktioniert nicht über Tor
- Beim Übergang von Tor-Netzwerk ins *normale* Internet passieren die Daten einen Exit Node. Auf diesem kann der Netzwerkverkehr mitgelesen werden. Geheimdienste betreiben daher bewusst solche Exit Nodes.

Virtual Private Network (VPN)

Zusammenschluss mehrerer Kommunikationsnetze über *unsichere* Netze zu einem neuen virtuellen Netz. Dazu wird der Datenverkehr transportverschlüsselt.

Schütz

- vor Schüfflern zwischen den Endpunkten einer VPN-Verbindung
- vor der einfachen Lokalisierung des Nutzers

Schütz nicht

- vor allem anderen.

Risiken & Nebenwirkungen

- Der VPN-Dienstleister hat Zugriff auf sämtliche Daten, die er durchleitet.

Kinderschutz

Einschränkung der Nutzung (Zeitbeschränkungen) und Inhalte (Filterfunktion, Protokollierung), die Kinder zu Gesicht bekommen sollen.

Schütz

- vor dem Zugriff auf viele bedenkliche Inhalte und exzessiver Nutzung, insbesondere für kleinere Kinder bis 12 Jahre ohne technisches Detailwissen.

Schütz nicht

- bei der Nutzung von Fremdgeräten, etwa bei Freunden.
- vor technisch versierteren Kindern, die Schutzmechanismen aushebeln können.

Risiken & Nebenwirkungen

- Technische Lösungen ersetzen nicht das notwendige Erlernen von Medienkompetenz und die Begleitung der Nutzung durch die Eltern.

Privates Browsing

Im Modus *Privates Fenster* (Firefox) oder *Inkognito-Fenster* (Chrome) speichert der Browser keine Daten, die Aufschluss über die besuchten Seiten geben.

Schütz

- vor anderen Nutzern des Browsers/Rechners, die nicht mehr nachvollziehen können, welche Webseiten man besucht hat.

Schütz nicht

- vor Verfolgung im Internet
- vor Protokollierung der Nutzung im Firmennetz
- vor Spuren wie Downloads oder selbst gesetzte Lesezeichen

Risiken & Nebenwirkungen

- Massiver Komfortverlusst: Man startet die Sitzung, als wäre man noch nie im Internet gewesen.

Webdienste–Passwörter

Viele Webdienste erfordern ein Login mit persönlichem Benutzernamen/Passwort. Dazu sollte pro Webdienst ein individuelles Passwort mit ausreichender Stärke gesetzt werden!

Schütz

- vor dem Zugriff Dritter auf eigene Daten, die auf dem betreffenden Webdienst liegen
- vor der Nutzung kostenpflichtiger Funktionen durch Dritte

Schütz nicht

- vor Angriffen auf Sicherheitslücken beim Anbieter (Yahoo-Attacke)
- vor schlecht implementieren Passwort-Rücksetzmechanismen (z. B. Frage nach dem Mädchennamen der Mutter)

Risiken & Nebenwirkungen

- Beim Speichern von Login-Daten im Browser können ggf. andere diese Daten abgreifen.
- Viele Dienste nutzen den Email-Account zur Verifiaktion oder zum Zurücksetzen vergessener Passwörter. Daher muss der Email-Account besonderes geschützt werden.
- Für wichtige Accounts (z. B. Google, Facebook, Apple, Microsoft) sollte die oft angebotene Zwei-Faktor-Authentifizierung genutzt werden.

Sensible Daten gegen Verlust absichern

RAID

Festplattenverbund mehrere Festplatten zur Steigerung der Performance, Kapazität und Verfügbarkeit.

Schütz

- vor Datenverlust bei Ausfall einzelner Festplatten. Die maximale Anzahl hängt von RAID-Art und der Anzahl der beteiligten Laufwerke ab, bei den kleinsten Verbünden darf nur eines ausfallen.
- vor Zeitverlust: Während des Beschaffens der Ersatzplatte und während des Wiederherstellens der Daten kann man weiterarbeiten.

Schütz nicht

- vor Datenverlust bei Ausfall zu vieler Laufwerke gleichzeitig, etwa durch Brand, Überschwemmung, Diebstahl, ... Ein RAID ist also kein (!) Backup, sondern kann allenfalls Teil einer Backup–Strategie sein.
- vor Datenverlust bei Fehlbedienung oder Kryptotrojanern.
- bei Wahl der falschen RAID-Art. Ein RAID 0 etwa liest und beschreibt die Laufwerke zwecks Temposteigerung abwechselnd, was die Ausfallwahrscheinlichkeit sogar steigert, weil die Daten weg sind, sobald auch nur eine der Platten kaputt geht. Auch ein JBOD (Just a bunch of disks) bietet keinen Ausfallschutz, denn hier werden die Platten einfach nacheinander vollgeschrieben.

RAID

Risiken & Nebenwirkungen

- Den erhöhten Ausfallschutz erkauft man sich mit einem erhöhten Preis pro GByte Speicherplatz, einem etwas höheren Stromverbrauch, einem komplizierterem Systemwechsel und manchmal auch mit mehr Lärm.
- Nach einem Rechnerwechsel kann man auf die Daten nur noch zugreifen, wenn die nötige Hard- und Software auch dort läuft.
- Betrifft Hardware-RAID: Wenn der Controller ausfällt und sich nicht mehr nachkaufen lässt, droht Datenverlust.
- Betriebssystemwechsel können unmöglich werden, wenn keine Treiber erhältlich sind oder wie bei Storage Spaces die Software nur unter Windows läuft.
- Wenn man versehentlich die falsche Platte tauscht, können RAID-Controller beziehungsweise -Software so durcheinander kommen, dass Probleme bis hin zum Datenverlust folgen.

Backup/Image

Jedes Backup ist besser als kein Backup!
Anzustreben: 3-2-1-Regel: 3 Kopien, auf mindestens 2 Systemen, davon 1 außer Haus

Schütz

- vor Datenverlust durch Fehlbedienung, Kryptotrojaner, Hardware-Defekten, ...
- vor Datenverlust durch Diebstahl, Feuer, Überschwemmung und ähnlichem, wenn das Backup in einem entsprechend sicheren Tresor oder außer Haus liegt.

Schütz nicht

- wenn man es nicht macht – klingt absurd banal, ist aber erfahrungsgemäß trotzdem der häufigste Grund, warum Daten nach einem Ernstfall nicht wiederherstellbar sind.
- die Daten, die seit dem letzten Backup neu hinzukamen oder verändert wurden.
- bei Feuer oder Diebstahl, wenn das Back up-Medium neben dem Gerät mit den Originaldateien liegt.
- wenn es nur ein Backup-Medium gibt und ein Krypto-Trojaner genau dann zuschlägt, wenn das Medium gerade angeschlossen ist.

Backup/Image

Risiken & Nebenwirkungen

- Der erforderliche Aufwand (Einrichten, regelmäßige Erfolgskontrolle, alle paar Jahre Tausch der Speichermedien) kann dazu führen, dass es irgendwann unterbleibt.
- Datenklau: Wer geheime oder private Daten stehlen will, dem reicht auch das Backup davon. Ein NAS lässt sich zudem einfacher raustragen als der Big-Tower-PC.
- Mancher denkt so lange über die richtige Backup-Strategie nach, bis es zu spät ist.
- Backup-Speicher kosten Geld.

USV

Eine unterbrechungsfreie Stromversorgung soll bei einem Stromausfall das geregelte Herunterfahren der Rechner ermöglichen.

Schütz

- vor Verlust oder Veränderung ungesicherter Daten bei Stromausfällen.
- manchmal auch vor Überspannungen im Stromnetz (Bursts, Surges).

Schütz nicht

- Geräte, die an einer normalen Steckdose hängen, also nicht an die USV angeschlossen sind.
- gegen Bedienungsfehler: Wenn Sie oder jemand anderer den Stromnetzstecker des PCs rausziehen (oder rausstolpern), sind ungesicherte Daten weg.
- Geräte, die an einer USV-Steckdose hängen, die nur gefiltert ist, aber nicht gestützt wird (siehe Handbuch).

Risiken & Nebenwirkungen

- Regelmäßige USV-Funktionstests sind unverzichtbar, können aber zum Abschalten der USV-Ausgänge führen.
- USV-Akkus sind Verschleißteile und müssen regelmäßig (alle 3 bis 5 Jahre) erneuert werden.
- An die USV sollten auch alle für die Bedienung und zum Herunterfahren des Rechners unverzichtbaren Peripheriegeräte (Monitor, USB–Hub, KVW–Switch) angeschlossen werden, jedoch keine starken Verbraucher wie z. B. Laserdrucker.

Überspannungsschutzgeräte

Schutz von Elektronik-Geräten durch Spannungsspitzen.

Schütz

- gegen moderate Überspannungen.
- Blitztreffer bei entfernten Nachbarn.

Schütz nicht

- bei direkten Blitztreffern.
- vor Fehlbedienung und Fehlern im Stromnetz.
- gegen geräteinterne Überspannungen durch Defekte.

Risiken & Nebenwirkungen

- Die Bauteile in ÜSG am Stromnetz verschleißen mit der Zeit, wodurch der Schutzpegel sinkt. Wenn eine Fehlerleuchte ein Problem signalisiert, wechseln Sie das ÜSG aus.
- Manche ÜSG für Datenleitungen beeinträchtigen die Datenrate. Beispielsweise sinkt dann bei einem besonders schnellen DSL–Anschluss der Download–Durchsatz um ein paar Prozent, selten auch mehr. Bei LAN-V-erbindungen bekommt man unter Umständen keine Gigabit–Verbindung über die Maximaldistanz von 100 Metern mehr hin.

Sensible Daten vor fremden Augen verbergen

Dateiverschlüsselung

Soll verhindern, dass unbefugte den Inhalt von Dateien lesen können. Bekannte Programme: AxCrypt (Windows, macOS), Cryptomator (Windows, macOS, Linux), SecurStick (Windows, macOS, Linux)

Schütz

- den Inhalt von Dateien, auch beim Diebstahl des Datenträgers.

Schütz nicht

- die Datei selbst. Sie kann kopiert, verändert oder gelöscht werden. Verschlüsselung ersetzt also kein Backup.
- vor weiterer Verschlüsselung, etwa durch Krypto–Trojaner.
- die Metadaten, zum Beispiel Erstell-/ -Änderungsdatum, Speicherort, je nach Programm auch nicht die Dateinamen.
- vor dem Öffnen der Datei durch Unbefugte. Der Unbefugte sieht dann aber nur Datensalat. Ausreichend Zugriffszeit erlaubt zwar Brute-Force-Angriffe, die aber aussichtslos sind, wenn man ein starkes Passwort verwendet hat.
- Sobald die Datei zum Lesen oder Bearbeiten beim Öffnen entschlüsselt wird, kann ein Screenshot-anfertigender Schädling oder eine hinter Ihnen stehende Person den Inhalt ebenfalls lesen oder ein Trojaner die Datei unverschlüsselt kopieren.

Dateiverschlüsselung

Risiken & Nebenwirkungen

- Schlüssel oder Passwort muss man unbedingt sichern. Schlüsselverlust oder Passwort vergessen bedeutet Datenverlust.
- Nur selbst erzeugte und nie weitergegebene Schlüssel sind wirklich geheim.
- Verschlüsselung erschwert Backups: Entweder muss man unverschlüsselt sichern oder zusätzlich Schlüssel oder Passwort plus Entschlüsselungssoftware.

Container–Verschlüsselung

Verschlüsselung von Datei-Containern (z. B. VeraCrypt) oder Archiven (z. B. Zip-Archive).

Schütz

- den Inhalt der Dateien.
- die Metadaten der Dateien.

Schütz nicht

- die Metadaten des Containers.
- Container kann kopiert, verändert oder gelöscht werden. Verschlüsselung ersetzt also kein Backup.
- vor zusätzlicher Verschlüsselung etwa durch Kryptotrojaner.

Risiken & Nebenwirkungen

- Wenn der Container beschädigt wird, sind ohne Backup alle verschlüsselten Dateien verloren.
- Schlüssel oder Passwort muss man unbedingt sichern. Schlüsselverlust oder Passwort vergessen bedeutet Datenverlust.
- Nur selbst erzeugte und nie weitergegebene Schlüssel sind wirklich geheim.
- Verschlüsselung erschwert Backups: Entweder muss man unverschlüsselt sichern oder zusätzlich unbedingt den Schlüssel oder das Passwort plus die Entschlüsselungssoftware.

Laufwerksverschlüsselung

Verschlüsselung kompletter Partitionen, z. B. mittels LUKS oder VeraCrypt.

Schütz

- davor, dass Fremde etwas von dem ausgebauten Laufwerk lesen.
- schützt bei Entsorgung oder Weitergabe davor, dass sich ein Fremder Zugriff auf die Daten verschafft. Man braucht dazu nur das Passwort nicht mitzugeben.

Schütz nicht

- Kopien auf unverschlüsselten Laufwerken.
- davor, dass Fremde das komplette Laufwerk löschen.
- nicht vor weiterer Verschlüsselung, etwa durch einen Kryptotrojaner.
- im laufenden Betrieb. Während das Laufwerk entsperrt ist, können auch Datendiebe/Schädlinge darauf zugreifen.

Risiken & Nebenwirkungen

- Schützt nur nach Herunterfahren/Ruhezustand. Bei Suspend to RAM oder Bildschirmschoner wird das Laufwerk nicht gesperrt.
- Schlüsselverlust bedeutet Datenverlust.
- Nur selbst erzeugte und nie weitergegebene Schlüssel sind wirklich geheim.

Self–Encrypting Drive

Laufwerk, welches sämtliche Daten selbst verschlüsselt. Dazu nutzt es ein selbst erstelltes Geheimnis, welches das Laufwerk nie verlässt. Zum Löschen des Laufwerks genügt es, mittels *Security Erase* Befehl das Laufwerk ein neues Geheimnis erzeugen zu lassen.

Schütz

- vor dem Auslesen von Daten aus einer defekten Festplatte oder SSD.
- vor Klartext-Datenresten in Reservesektoren von Festplatten oder SSDs.
- im Verbund mit einem Schnittstellenpasswort vor Datendiebstahl.

Schütz nicht

- vor dem Lesen der Daten über die Schnittstelle, wenn dafür kein Passwort gesetzt wurde. Entweder per ATA Security Feature Set – das *HDD Password* in manchem BIOS-Setup –, nach TCG Opal oder mit dem eDrive-Konzept von Microsoft Bitlocker. Auch bei manchen USB-Festplatten lässt sich ein Passwort vergeben. Erst dann sind die Daten der SED ohne Passwort auf keinem Weg mehr lesbar.
- vor dem Lesen der Daten durch einen Trojaner – wenn das Betriebssystem läuft, muss das SED ja entsperrt sein.

Self–Encrypting Drive

Risiken & Nebenwirkungen

- Nicht mal Datenrettungsfirmen können etwas von einem SED retten, außer bei sehr speziellen Hardware-Defekten, wenn gleichzeitig ein ATA-Passwort gesetzt oder Bitlocker aktiviert wurde und Passwort/Wiederherstellungsschlüssel bekannt ist.
- Die proprietäre SED-Firmware kann Bugs oder Hintertüren (Zweitschlüssel) enthalten.

Zugriffsrechte

Beschränkung der Zugriffsmöglichkeiten einzelner Personen/Gruppen auf Dateien und Ordner durch den Administrator.

Schütz

- vor Zugriffen durch unberechtigte Benutzer/Gruppen.
- vor unberechtigten Handlungen berechtigter Nutzer: Wer als Recht lediglich *Nur Lesen* besitzt, kann die Datei weder löschen noch ändern.
- Wenn man sich selbst die Rechte an ausgewählten Dateien und Ordnern entzieht, sind diese vor Fehlbedienung und vor Zugriffen durch Schädlinge geschützt, die mit gleichen Rechten laufen.

Schütz nicht

- die persönlichen Dateien vor Schädlingen oder Fehlbedienung.
- wenn es einem Angreifer gelingt, auf dem PC ein Betriebssystem zu starten, in dem er Administrator ist. Das gilt auch, wenn er die Festplatte in einen anderen Rechner umbaut.
- wenn ein unberechtiger Nutzer sich einfach mit einem berechtigten Konto anmelden kann, etwa weil das nicht durch Passwort geschützt ist oder das Passwort auf einem Zettel steht.

Risiken & Nebenwirkungen

- Komplexe Konfiguration führt leicht zur Fehlkonfiguration.
- Fehlkonfigurationen erlauben unberechtigte Zugriffe.
- Bei Netzwerkfreigaben müssen auch die Dateisystemzugriffsrechte stimmen, damit der Zugriff klappt.

Authentifizierungs-Methoden

Zwei–Faktor–Authentifizierung

Login–Mechanismus, der zwei seaparate Identitätsnachweise benötigt, z. B.: TAN oder über Messanger/SMS übermittelten zusätzlichen Code

Schütz

- vor unmittelbarem Kontrollverlust über Geräte- oder Online-Konten, wenn Kriminelle in den Besitz des Passwortes kommen.

Schütz nicht

- vor ambitionierten Angreifern. Ein zweiter Authentifizierungsfaktor stellt zwar ein zusätzliches und im Regelfall auch durchaus hohes, aber eben nicht unüberwindbares Hindernis dar. Kommt als zweiter Faktor etwa ein per SMS verschickter Passcode zum Einsatz, könnten Kriminelle versuchen, die hinterlegte Mobilfunknummer zu ändern oder sich eine Ersatz-SIM-Karte zu beschaffen.

Risiken & Nebenwirkungen

- Fällt der Kommunikationsweg oder das Gerät für den zweiten Faktor aus, ist ein Login nicht mehr ohne Weiteres möglich. Für viele Konten lassen sich deshalb zusätzliche Backup-Kontaktwege hinterlegen – etwa eine alternative Mailadresse oder Handynummer.
- Zwei–Faktor–Authentifizierung geht zu Lasten der Bequemlichkeit: Versand und Eingabe des zweiten Faktors erfordern zusätzliche Zeit, Tipperei und oft ein zweites Gerät.

UEFI Secure Boot

Ein solches System startet nur digital signierte Bootloader, die sich über eine im BIOS hinterlegte kleine Datenbank verifizieren lassen.

Schütz

- vor speziellen Formen von Malware, die schon vor dem Start des Betriebssystems die Kontrolle übernehmen soll.

Schütz nicht

- vor sonstigen Viren, Trojanern & Co.
- vor Angriffen auf Firmware-Funktionen wie Intels Management Engine.

Risiken & Nebenwirkungen

- Ein installiertes Betriebssystem könnte durch Ändern der Schlüsseldatenbank den Start anderer Betriebssysteme unterbinden.
- Betriebssysteme ohne signierten Bootloader booten nicht mit Secure Boot. Das betrifft in erster Linie einige LinuxDistributionen. Ein Problem ist das aber nur bei Rechnern, bei denen sich Secure Boot nicht von Hand im BIOS abschalten lässt. Das ist nach unseren Beobachtungen vor allem bei einigen Windows10-Tablets der Fall.
- Viele PC-Hersteller hinterlegen ausschließlich Microsoft-Signaturen in der Secure-Boot-Schlüsseldatenbank der Firmware.

Sicherheitsfragen für Accounts

Sollen in der Regel den Zugriff bei vergessenem Passwort wiederherstellen (Passwort–Reset).

Schütz

- vor Gelegenheits-Kriminellen.

Schütz nicht

- vor ambitionierten Angreifern, die die korrekten Antworten auf die Sicherheitsfragen auf irgendeine Art zusammentragen können – sei es per Social Engineering oder schlicht durch googeln, weil Sie neulich ganz stolz ein Foto Ihrer ersten CD für die ganze Welt sichtbar bei Instagram gepostet haben.

Risiken & Nebenwirkungen

- Viele Antworten auf Sicherheitsfragen kann ein Angreifer oft mit mäßigem Aufwand herausfinden. Eigentlich sollten Sie deshalb besser andere Noteingänge in Ihren Account haben, etwa eine Recovery-Mail-Adresse. Sind die Sicherheitsfragen zwingend, empfiehlt es sich, falsche Antworten einzugeben. Für den Fall, dass Sie sie wirklich einmal brauchen, notieren Sie die Antworten und verwahren Sie sie sicher.

ATA Security Password

Festplattenpasswort, das bei jedem Booten vom BIOS abgefragt wird. Ohne korrekte Eingabe wird die Festplatte nicht entsperrt und es ist kein Systemstart möglich.

Schütz

- vor unbefugtem Zugriff auf eine Festplatte oder SSD, etwa nach deren Ausbau.

Schütz nicht

- vor dem Auslesen der gespeicherten Daten in einem Datenrettungslabor, denn dabei wird die Elektronik auf der Festplatte umgangen, die für den Abgleich des Passwortes und Erlaubnis des Zugriffs zuständig wäre. Deshalb ist ein ATA Security Password nur für selbstverschlüsselnde Laufwerke sinnvoll.

Risiken & Nebenwirkungen

- Wenn das BIOS nach der Übergabe des Passworts den ATA-Befehl *Freeze Lock* nicht übergibt, kann Malware die Festplatte im laufenden Betrieb sperren.
- Hat man das Passwort vergessen, lassen sich die Daten höchstens im Datenrettungslabor noch auslesen – und das auch nur, wenn sich das Laufwerk nicht selbst verschlüsselt.

Trusted Platform Module (TPM)

Sicherer Speicherchip für digitale Geheimnisse wie Signaturen, Schlüssel und Prüfsummen.

Schütz

- vor der Manipulation digitaler Schlüssel.
- im Verbund mit Verschlüsselungstechnik auf vielen Firmen-PCs Datenbestände davor, von Angreifern ausgelesen, kopiert oder manipuliert zu werden.

Schütz nicht

- vor Datenverlust.
- vor Viren.

Risiken & Nebenwirkungen

- Mit einem TPM lassen sich auch starke Maßnahmen für Zugriffs- und Kopierschutz umsetzen, also Digital Rights Management (DRM).
- Zusammen mit der Technik *Measured Launch* kann das TPM verhindern, dass das vom Hersteller vorgesehene BIOS durch eine alternative Firmware wie Coreboot oder Libreboot ersetzt wird.
- Das Betriebssystem kann das TPM nutzen, um digitale Signaturen von Software zu prüfen, und verweigert dann das Starten unsignierter Software. Google Chromebooks tun genau das.

Biometrie

Benutzerauthentifizierung mittels biometrischer Merkmale, wie z. B. Fingerabdruck oder Gesichtserkennung

Schütz

- vor Passwortdieben, die den Besitzer während der Eingabe bespitzeln.
- vor vergessenen Passwörtern oder verlorenen Tokens.
- verbessert durch hohen Komfort die Sicherheit, falls der Nutzer sonst aus Faulheit gar kein (oder ein schwaches) Passwort verwenden würde.

Schütz nicht

- vor Attacken durch ausdauernde und gut ausgestattete Angreifer.

Biometrie

Risiken & Nebenwirkungen

- Fingerabdrucksensoren lassen sich meist mit mehr oder weniger Aufwand austricksen, sobald der Angreifer einen Fingerabdruck der Zielperson ergattern konnte.
- Gesichtserkennung mittels eines einfachen, also zweidimensionalen Bildes lässt sich oft schon mit einem Foto vom Besitzer austricksen.
- Gesichtserkennung mit einer Tiefenkamera (etwa Intel RealSense oder Face ID im iPhone X) ist deutlich schwieriger zu überlisten, versagt aber mitunter auch – etwa bei allzu ähnlichen, eineiigen Zwillingen.
- Ein kompromittiertes Passwort kann man ändern – sein Gesicht nicht.
- Weil ein biometrisches Merkmal spontanen Veränderungen unterliegen kann (Verletzungen des Fingers oder des Gesichts, Rasur, Verlust einer Brille . . .), verlangen die allermeisten Systeme das Anlegen einer alternativen Entsperrmethode. Für Smartphones ist es sinnvoll, mehrere Fingerabdrücke einzurichten; auch um das Gerät in vielen Lebenslagen bequem entsperren zu können.

User Account Control (UAC) *nur Windows!*

Schützt in der Windows-Welt vor ungewollten Änderungen am System. Auch ein Administrator muss bei sicherheitsrelevanten Änderungen eine Nachfrage abnicken.

Schütz

- die Windows-Komponenten sowie das Gros der installierten Software vor ungewollten Manipulationen durch Schädlinge.

Schütz nicht

- vor Erpressungstrojanern, Viren und sonstigen böswilligen Programmen, die ohne besondere Rechte aus dem Benutzerordner heraus lauffähig sind. Zum Verschlüsseln der eigenen Dateien sind zum Beispiel gar keine Administratorrechte erforderlich.
- vor Malware, die darauf ausgelegt ist, mit ausgefeilten Techniken die UAC Abfrage zu umgehen.
- wenn die UAC-Abfrage tatsächlich von einem böswilligen Programm herrührt und man sie einfach gedankenlos bestätigt.

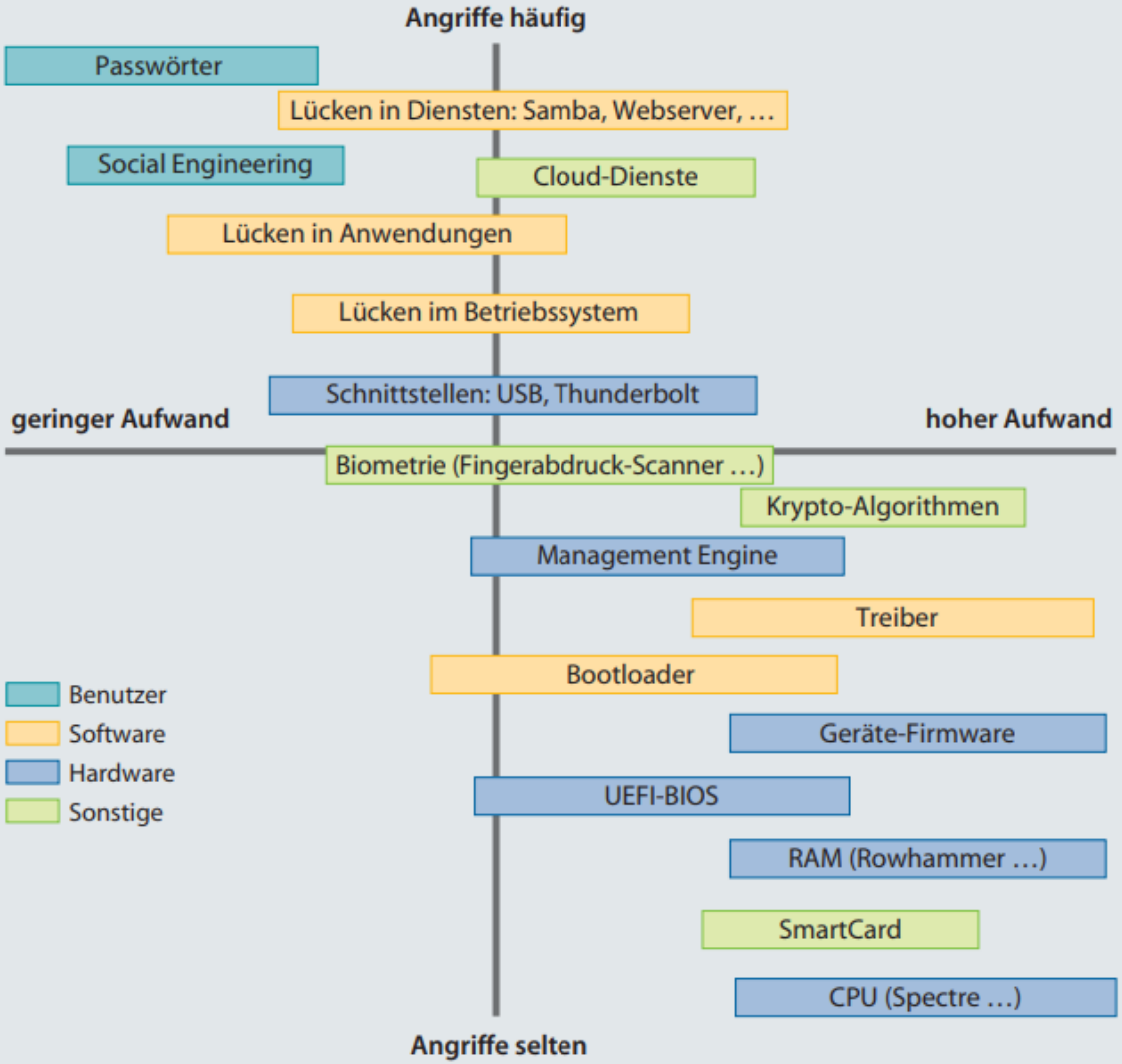
User Account Control (UAC) *nur Windows!*

Risiken & Nebenwirkungen

- Stellt man die UAC-Abfragehäufigkeit von der voreingestellten zweithöchsten Stufe auf die höchste um, erfordern schon einfache, mitunter völlig unkritische Systemaufgaben wie das bloße Öffnen des Task-Managers eine UAC-Bestätigung. Dafür werden aber bestimmte Angriffe verhindert.
- Stellt man die Abfragehäufigkeit niedriger ein oder deaktiviert UAC komplett, steigt das Risiko deutlich, dass Schädlinge unbemerkt Sicherheitsfunktionen manipulieren oder abschalten oder sich unbemerkt zur Tarnung mit eigenen Treibern im System verankern (Rootkit).

Angriffsmöglichkeiten auf PCs

Alle Komponenten von PCs bieten Angriffsmöglichkeiten, aber manche lassen sich leichter ausnutzen als andere. Wer einen PC gezielt angreift, versucht zuerst einfachere Attacken.



(aus c't 06/2018, S. 121)

Maßnahmen zum PC-Schutz

Maßnahme	Funktion
Büro abschließen	Zugriff auf Hardware verhindern
PC-Gehäuse abschließen	Manipulation und Diebstahl von Datenträgern erschweren
verschlüsseltes Backup	Daten sichern, vor allem bei Vollverschlüsselung
unnötige Funktionen abschalten	Risiken minimieren
unnötige Schnittstellen abschalten	unbefugten Zugriff erschweren
Boot-Reihenfolge festlegen	Booten anderer Betriebssysteme verhindern
Passwörter für BIOS-Setup und Systemstart	unbefugten Zugriff erschweren
Festplatten-Passwort	unbefugten Zugriff erschweren
Festplatte verschlüsseln	unbefugten Zugriff erschweren
sichere Passwörter wählen	unbefugten Zugriff erschweren
BIOS-/Firmware-Updates	Sicherheits-Patches schnell einspielen
Secure Boot	Risiken minimieren (manipulierte Bootloader)
Measured Launch mit TPM/Intel TXT	Risiken minimieren (manipuliertes BIOS)
Open-Source-Betriebssystem	Risiken minimieren
Open-Source-Treiber	Risiken minimieren
Betriebssystem sicher konfigurieren	unbefugten Zugriff erschweren
automatische Updates	Sicherheits-Patches schnell einspielen
Signaturen/Hashes von Software prüfen	Integrität und Authentizität von Software/Treibern
je Konto eigenes Passwort, 2FA	Risiken minimieren
Anwendungen in VMs isolieren	Angriffe einhegen
proprietäre Sicherheitsfunktionen meiden	Risiken minimieren
Ethernet statt WLAN	Belauschen von Datenpaketen erschweren
Glasfaser-LAN statt Kupferleitung	Belauschen von Datenpaketen erschweren
Passwörter auf SmartCard auslagern	Risiken minimieren, Zwei-Faktor-Authentifizierung (2FA)
PC mit Libreboot/Coreboot	Risiken durch UEFI, Intel ME, AMD PSP minimieren

(aus c't 06/2018, S. 123)

Und sonst ...

- Unbetrachtet sind z. B.:
  - Netzwerke, WLAN
  - Internet–of–Things
  - physischer Zugangsschutz
  - Smart–Phones, Tablets
  - und vieles mehr ...
- Strategie für sichere Passwörter
- Informiert bleiben (Meltdown, Spectre, ...)
- Veraltete Systeme ggf. ausmustern bzw. in unkritischen Anwendungsszenarien weiterbetreiben
- Der Geist ist willig, doch der Geist ist schwach ...
- TANSTAAFL: *there ain't no such thing as a free lunch*