IT-Sicherheit ist nie fertig – Ein persönlicher Weg über viele Jahre

1. Der Hallo-Wach-Moment

Wenn ich heute auf die letzten Jahrzehnte meines Umgangs mit IT-Sicherheit zurückblicke, wirkt vieles wie ein langsames Abschälen alter Gewohnheiten und Bequemlichkeiten. Die wirklich groben Patzer liegen weit zurück – allen voran der Moment, in dem ich mir als Jugendlicher aus purer Neugier einen Virus (getarnt als nützliche Software) auf meinen Gaming-PC geladen habe, der anschließend die komplette Festplatte ausgelöscht hat. Kein Backup, keine Sicherung, alles weg: Spielstände, Dokumente, Fotos. Heute ist das eine Anekdote, damals war es ein Schock. Und doch war genau dieser Vorfall der Augenblick, an dem mir zum ersten Mal dämmerte, dass »wird schon nichts passieren« kein Sicherheitskonzept ist, sondern ein Selbstbetrug, den man erst erkennt, wenn es zu spät ist.

Interessant ist rückblickend weniger dieser einzelne Auslöser als das, was danach kam: Kein plötzlicher Wechsel vom »naiven Nutzer« zum »Security-Nerd«, sondern eine lange Reihe kleiner Entscheidungen. Ein Passwort hier umgestellt, einen Account dort gelöscht, später den E-Mailserver umgebaut, dann das Heimnetz segmentiert, das Smartphone gewechselt, Backups automatisiert. Nichts davon war spektakulär. Aber in der Summe hat es meine gesamte digitale Infrastruktur verändert. Und genau daran sieht man gut, dass IT-Sicherheit kein Zustand ist, den man erreicht und dann konserviert, sondern ein fortlaufender Prozess.

Im Folgenden möchte ich einzelne Bereiche herausgreifen und sie gemeinsam mit euch betrachten – so, wie sie früher bei mir aussahen, welche Gedanken mich zum Umdenken gebracht haben und wie ich heute damit umgehe. Es war keine Revolution über Nacht, sondern ein langsamer, manchmal unbequemer Übergang: von einer Art digitalen Steinzeit, in der vieles einfach »mitlief«, hin zu einer Infrastruktur, die ich verstehe, hinterfrage und selbst gestalten kann.

2. Passwörter: Vom ausgedachten System zur kontrollierten Unmerkbarkeit

Es ist lange her, dass ich meine Passwörter nach einem Schema gebaut habe, auf

das ich damals sogar ein wenig stolz war. Ich hatte ein paar Grundbestandteile, etwa einen festen »Code«, und habe ihn mit Elementen des Dienstnamens kombiniert, manchmal eine Jahreszahl hinten dran, ab und zu ein Sonderzeichen dazwischen. Das fühlte sich »individuell« und »schwer zu erraten« an, war aber letztlich ein systematisches Muster. Und Muster sind genau das, womit Angreifer arbeiten.

Der eigentliche Denkfehler lag darin, dass ich die Perspektive verwechselt hatte: Ich dachte in meinem Kopf, der diese Regeln kennt. Ein Angreifer sieht aber nicht das, was ich mir ausgedacht habe, sondern nur ein geleaktes Passwort in irgendwelchen Datensätzen. Sobald er eine Handvoll davon analysiert, sind die Regelmäßigkeiten oft offensichtlicher, als einem lieb ist: Bestimmte Zeichenfolgen, die immer wieder auftauchen, Domainbestandteile, die sich wie Mosaiksteine wiederholen. Aus Sicht eines Angreifers reduziert ein solches »System« die Suche, statt sie zu erschweren.

Der Umstieg auf einen Passwort-Manager war deshalb weniger ein technischer Schritt als ein mentaler. Ich musste akzeptieren, dass ein wirklich sicheres Passwort für mich unmerkbar sein muss. Kein Bezug, kein Schema, keine Logik außer der Zufälligkeit. Das war anfangs ungewohnt. Man gibt die Illusion auf, die Dinge »im Kopf zu haben«. Heute liegt allerdings alles in KeePass, und genau dieses Nicht-merken-Können ist Teil des Sicherheitskonzepts: Die Passwörter existieren nur noch in einer verschlüsselten Datenbank, gesichert durch ein starkes Master-Passwort und ein Setup, das ich bewusst überschaubar gehalten habe.

Mit der Zeit hat sich daraus eine Ordnung entwickelt, die weit über reine Logins hinausgeht. Konten sind sauber gruppiert, kritische Zugänge markiert, Hinweise für den Notfall ergänzt. Ich habe mich bewusst damit beschäftigt, wie jemand nach meinem Tod auf den Passwort-Manager zugreifen könnte, ohne gleich die gesamte Struktur zu kompromittieren. Digitaler Nachlass ist kein angenehmes Thema, aber er gehört zur Realität, wenn immer mehr Lebensbereiche online stattfinden. Die Passwortdatenbank ist heute nicht nur ein Werkzeug für den Alltag, sondern ein zentrales Element, das mir dabei hilft, den Zugang zu meinem digitalen Leben zu organisieren.

Natürlich bringt das alles nur etwas, wenn es praktisch nutzbar bleibt. Der nächste Schritt war deshalb die Frage: Wie bekomme ich diese Datenbank auf mehreren Geräten synchron, ohne sie in irgendeinen x-beliebigen Cloudspeicher zu kippen? Die Lösung war Syncthing. Statt anonyme Server in irgendwelchen Rechenzentren als Zwischenstationen zu nutzen, synchronisiere ich die Datenbank direkt zwischen meinem Linux-Desktop und meinem Android-Gerät. Das passiert so zuverlässig im Hintergrund, dass ich im Alltag gar nicht mehr darüber nachdenke – genau so, wie es sein soll. Komfort und Kontrolle schließen sich nicht aus, sondern müssen nur bewusst selbst gestaltet werden.

3. Accounts: Von »für alles ein Konto« zu »so wenig wie möglich«

Noch bevor ich mich ernsthaft mit Aliasen, Löschanfragen und Datenminimierung beschäftigt habe, war mein Umgang mit Accounts ziemlich typisch: Man stolpert über einen Dienst, registriert sich schnell, legt ein Profil an, probiert etwas aus – und verschwindet irgendwann wieder. Das Konto bleibt trotzdem bestehen. So sammeln sich im Laufe der Jahre zig Zugänge an, die man nicht mehr aktiv nutzt, von denen man aber auch nicht mehr genau weiß, welche Daten dort eigentlich liegen und wie lange sie noch irgendwo in Backups herumliegen.

Die Veränderung kam nicht über Nacht. Am Anfang war es eher ein Unbehagen: die Erkenntnis, dass jeder Account potenziell ein weiterer Datensatz ist, der irgendwann in einem Leak auftauchen kann. Also habe ich zunächst angefangen, bei neuen Diensten anders zu denken: Brauche ich das wirklich? Muss ich mich dafür registrieren oder gibt es eine Möglichkeit, die Information auch ohne Konto zu bekommen? Und wenn ich mich registrieren muss: Ist das ein langfristig relevanter Dienst oder eher eine zeitlich begrenzte Sache, die in einem Jahr keine Rolle mehr spielt?

Parallel dazu habe ich begonnen, alte Konten systematisch zu hinterfragen. Das ist kein besonders spannender Prozess – eher eine Art digitaler Frühjahrsputz –, aber er wirkt. Viele alte Forenlogins, kaum genutzte Social-Media-Profile und Testaccounts habe ich entweder gelöscht oder, wo das nicht möglich war, so weit anonymisiert, wie der Dienst es zugelassen hat. Je mehr davon verschwindet, desto überschaubarer wird der eigene »digitale Fußabdruck«.

Ein wichtiger Schritt, um mich digital zu organisieren, war die Nutzung von E-Mail-Aliasen. Statt überall dieselbe Adresse einzusetzen, trenne ich heute stärker nach Zweck und Vertrauensgrad. Kurzfristige Registrierungen, Foren, in denen ich nur mitlese, oder Dienste, denen ich nicht vollständig vertraue, laufen über addy.io-Aliase mit Weiterleitung. Meine eigentliche Hauptadresse – also die eigene Domain – nutze ich nur noch an wenigen, ausgewählten Stellen.

Mit der Zeit ist daraus eine Haltung geworden, die ich fast automatisch anwende: Ein Account ist nicht bloß ein Formular, sondern eine Art Austauschbeziehung. Deshalb stelle ich mir bei jeder Registrierung die Frage: Welche Daten gebe ich her – und was bekomme ich dafür zurück?

4. E-Mail: Von der Freemail zur kontrollierten Adresslandschaft

E-Mail war am Anfang meines Weges etwas, über das ich nicht groß nachgedacht habe. Ein web.de-Konto, irgendwann mal eingerichtet, weil man eben eins braucht. Gefühlt war das nicht anders als eine Telefonnummer. Man gibt die Adresse an, bekommt Nachrichten, fertig. Erst mit der Zeit wurde mir klar, dass E-Mail im

Netz oft die zentrale Identität ist: Mit der Adresse loggt man sich ein, setzt Passwörter zurück, verknüpft Konten. Wenn diese eine Adresse überall genutzt wird, ist sie das Bindeglied, das alles zusammenhält – und im Zweifel für Dritte auswertbar macht.

Der Schritt zum eigenen E-Mailserver war damals der Versuch, die Kontrolle zurückzugewinnen. Auf einem Debian-System einen E-Mailserver hochzuziehen, fühlte sich an wie ein großes Stück Unabhängigkeit/Freiheit. Plötzlich war ich nicht mehr nur Nutzer einer Infrastruktur, sondern Betreiber. Ich habe mich mit TLS-Einstellungen beschäftigt, SPF- und DKIM-Einträgen, mit Spamfiltern, Blacklists und der Tatsache, dass man als kleiner E-Mailserverbetreiber schnell in Situationen kommt, in denen große Anbieter einen faktisch blockieren, weil man nicht in deren Sicherheits- und Reputationsschema passt. Es war eine lehrreiche Zeit, die mir technisch viel gebracht hat – und auch ein besseres Verständnis dafür, wie fragil der E-Mail-Verkehr ist, wenn man eine Komponente vernachlässigt.

Irgendwann stand ich aber vor der nüchternen Abwägung: Möchte ich langfristig Energie in die Pflege einer E-Mailserver-Infrastruktur stecken, oder möchte ich die gleiche Zeit in andere Sicherheitsaspekte investieren? Die Antwort war relativ klar. Ich habe mich für mailbox entschieden, eigene Domains eingebunden und den technischen Unterbau in professionelle Hände gelegt, während ich die Hoheit über meine Adressen behalten habe. Das war kein Rückschritt, sondern eher eine Verschiebung der Verantwortlichkeiten: Der Dienst kümmert sich um Verfügbarkeit, Spamfilterung und aktuelle Standards, ich kümmere mich darum, wie Adressen genutzt werden.

Der eigentliche Paradigmenwechsel kam mit der konsequenten Einführung von Dienst-spezifischen Adressen. Statt eine oder zwei Hauptadressen zu haben, die ich überall hinterlasse, bekommt heute jeder Dienst seine eigene E-Mail. Ein Händler, bei dem ich Hardware bestelle, bekommt etwa `online-shop@meine-domain.de`. Ein Forum, das ich teste, tritt unter einer eigenen Adresse mit mir in Kontakt, ein Newsletter bekommt ebenfalls eine individuelle Adresse. Dieses Konzept ist erstaunlich wirksam: Sobald irgendwo Spam auftaucht oder eine Adresse plötzlich in anderen Kontexten auftaucht, ist sofort sichtbar, woher sie stammt. Sollte ein Anbieter unseriös wirken, deaktiviere ich einfach den Alias. Der Kontakt ist für ihn weg, ohne dass ich meine eigentliche Adresse ändern muss.

Aus einer einzelnen Freemail-Adresse ist über die Jahre somit ein fein strukturierter Adressraum geworden, in dem ich bestimmen kann, wer welchen Zugang bekommt, wer ihn behält und wer ihn wieder verliert. E-Mail ist dadurch nicht mehr der alles verbindende Identifikator, sondern ein Werkzeug, das gezielt eingesetzt wird.

5. Heimnetz: Vom »Router aus der Box« zur eigenen Infrastruktur

In meinem Heimnetzwerk war lange Zeit eine Fritz!Box das Tor zur digitalen Welt – wie in vielen anderen deutschen Haushalten auch. Das Gerät kam vom Provider, wurde angeschlossen, lief – und damit war das Thema für die meisten erledigt. Diese All-in-one-Lösung war praktisch: Modem, Router, WLAN, DHCP, DNS in einem. Aber je mehr ich mich mit Netzwerken beschäftigt habe, desto unwohler wurde mir bei der Vorstellung, dass diese eine Kiste gleichzeitig alles macht und ich nur eingeschränkt sehe, was tatsächlich passiert.

Der erste Schritt war nicht, alles auf einen Schlag umzubauen, sondern die Rolle der FritzBox zu reduzieren. Sie blieb am Anschluss als Modem und einfache Routerinstanz, aber die eigentliche Netzwerklogik habe ich nach hinten verlagert. Eine FritzBox 4040, die ich mit OpenWrt geflasht habe, übernahm die Aufgaben, die mir wichtig wurden: Segmentierung, feinere Firewallregeln, eigene DNS-Konfiguration, Trennung von Zonen. Aus einem homogenen Heimnetz wurde nach und nach eine Sammlung verschiedener Bereiche, in denen nicht jedes Gerät alles sehen und ansprechen kann.

Dieser Umbau hat meine Perspektive auf das Heimnetz grundsätzlich verändert. Plötzlich war es nicht mehr »mein WLAN«, in dem alles gleichberechtigt herumfunkt, sondern eine Art kleiner Baukasten, in dem ich entscheiden konnte, wo ich Geräte hinstelle. Ein Smart-TV oder sonstige IoT-Spielzeuge kommen nicht mehr in das gleiche Netz wie mein Arbeitsrechner oder mein Server. Gäste erhalten ein eigenes Segment, das isoliert bleibt. Die Frage, ob ein Gerät wirklich ins Kernnetz gehört, stellt sich heute automatisch.

Der Pi-hole, den ich ergänzend als DNS-Filterinstanz ins Netz geholt habe, hat dann sichtbar gemacht, was vorher nur im Verborgenen ablief. Es ist schon erstaunlich, wie viele Anfragen im Hintergrund gestellt werden, ohne dass man aktiv etwas tut. Mit einem Blick auf die Logs sieht man, welche Domains permanent kontaktiert werden – von Fernsehern, Smartphones, Druckern, und natürlich von Apps. Viele dieser Anfragen haben mit echter Funktionalität nichts zu tun, sondern dienen Telemetrie, Tracking oder reiner Bequemlichkeit der Hersteller. Mit Pi-hole lässt sich das nicht komplett stoppen, aber deutlich einschränken. Vor allem schärft es den Blick dafür, was »normales« Verhalten ist und was nicht.

Über die Jahre hat sich das Heimnetz dadurch von einer Blackbox, die »halt funktioniert«, zu einem System entwickelt, das sich bewusst steuern lässt. Und mit jeder Anpassung wird klarer, dass es kein Luxus ist, sein eigenes Netz zu verstehen – sondern eine Grundlage dafür, dass andere nicht mehr wissen als man selbst.

6. Smartphone: Vom Lifestyle-Gadget zum kontrollierten

Werkzeug

Mein Smartphone hat vermutlich die deutlichste Wandlung durchgemacht. Das erste iPhone war damals vor allem eines: ein faszinierendes Stück Technik. Es stand für Freiheit, für neue Möglichkeiten, für permanentes Online-Sein. Dass es gleichzeitig auch ein exzellenter Sensor für Daten war, der fleißig nach Hause telefonierte, blieb lange im Hintergrund. Später, mit dem Wechsel zu Android, änderte sich daran zunächst wenig. Ja, das System war offener als iOS, ja, man konnte mehr einstellen, aber im Kern blieb die Rolle gleich: Das Gerät war Teil eines Ökosystems, das von Datenerfassung und Profilbildung lebt.

Der Wechsel zu Custom-ROMs wie LineageOS war der erste Versuch, dieses Verhältnis geradezurücken. Plötzlich verschwanden vorinstallierte Apps, Google-Dienste konnten reduziert werden, das System fühlte sich leichter an. Trotzdem blieb ein Unbehagen. Man merkte dem Gerät an, dass die ursprüngliche Plattform nicht dafür gebaut war, dem Nutzer echte Kontrolle über Datenflüsse bzw. Datenschutz zu geben. Analysen zum Datenfluss – etwa welches System wohin funkt, auch wenn der Nutzer nichts aktiv tut – haben diesen Eindruck verstärkt. Irgendwann war klar, dass ich ein System möchte, das von Anfang an mit Sicherheit und Kontrolle im Fokus entwickelt wurde, nicht erst im Nachhinein zurechtgebogen werden muss.

Mit GrapheneOS habe ich dieses System gefunden. Seit einigen Jahren begleitet mich dieses Betriebssystem im Alltag, und es hat die Rolle meines Smartphones spürbar verändert. Es ist nicht mehr das Gerät, das »halt alles kann«, sondern ein Werkzeug, das genau das tut, was ich ihm erlaube – nicht mehr und nicht weniger. Die meisten Apps, die ich nutze, stammen aus dem Open-Source-Bereich und kommen über F-Droid oder vertrauenswürdige Repositories. Apps, die versuchen, mehr Daten zu sammeln, als für ihre Funktion notwendig ist, haben bei mir schlicht keinen Platz mehr.

RethinkDNS ergänzt dieses Konzept, indem es mir die feingranulare Kontrolle über den Netzwerkverkehr der Apps gibt. Anstatt im Dunkeln zu tappen, sehe ich, welche App welche Domains anfragt, zu welchen Zeiten und in welchem Umfang. Wo es keinen Grund gibt, eine Verbindung aufzubauen, wird sie blockiert. Ich kann Apps vollständig vom Netz nehmen oder ihnen nur den Zugriff auf bestimmte Ziele erlauben. Dadurch verliert das Smartphone den Charakter eines Dauer-Senders und wird zu einem Gerät, das wieder stärker mir dient als den Unternehmen, die die Plattformen und Infrastrukturen dahinter bereitstellen.

Diese Entwicklung war kein radikaler Schnitt, sondern das Ergebnis vieler kleiner Entscheidungen: eine App weniger, eine Berechtigung weniger, ein Dienst weniger, der auf dem Gerät läuft. Aber sie hat das Verhältnis komplett gedreht. Heute ist mein Smartphone nicht mehr das Datenleck in der Hosentasche, sondern

ein kontrollierter Baustein meiner Infrastruktur.

7. Backups: Verfügbarkeit als unterschätzte Säule

Der komplette Datenverlust auf meinem alten Gaming-PC steht sinnbildlich für den Punkt, an dem mir klar wurde, was Verfügbarkeit bedeutet. Damals war es ärgerlich, heute wirkt es fast banal: keine Backups, also keine Chance. Trotzdem hat es lange gedauert, bis Backups einen festen Platz in meinem Alltag bekommen haben. Wie bei vielen anderen Themen in der IT-Sicherheit ist das Risiko schwer greifbar, solange nichts passiert. Platten fallen nicht jeden Tag aus, Verschlüsselungstrojaner erwischen nicht jede Woche jemanden im Bekanntenkreis.

In den letzten Jahrzehnten hat sich das geändert. Ich habe mir bewusst eine Struktur aufgebaut, in der Daten nie nur an einem Ort existieren. Zentral ist dabei ein lokales RAID-System, das verhindert, dass der Ausfall einer einzelnen Festplatte gleich die gesamte Datengrundlage vernichtet. Das ist keine magische Lösung – auch ein RAID schützt nicht vor Bedienfehlern, versehentlichem Löschen oder massiven Hardwareproblemen –, aber es verschiebt die Verwundbarkeit an eine andere Stelle.

Der entscheidende Schritt war dann die Ergänzung durch verschlüsselte Offsite-Backups außer Haus bei Eltern und Freuden. Zusätzlich sichere ich mit Kopia regelmäßig in eine Nextcloud-Instanz, die sich außerhalb des eigentlichen Systems befindet. Die Backups selbst sind verschlüsselt, die Struktur ist automatisiert. Ich muss mich nicht mehr erinnern, »jetzt mal schnell zu sichern«, sondern kann mich im Alltag darauf verlassen, dass die relevanten Daten in definierten Zyklen an einen anderen Ort kopiert werden. Ebenso wichtig wie das Sichern ist das Testen der Wiederherstellung. Es reicht nicht, bunte Statusmeldungen zu sehen. Man muss einmal durchgespielt haben, was passiert, wenn man eine Datei oder ein Verzeichnis wirklich zurückholen muss.

Backups sind für mich heute kein Zusatzmodul mehr, das man »irgendwann mal einrichtet«, sondern ein integraler Bestandteil des Gesamtkonzepts. Ohne sie wäre jeder noch so gut gehärtete Server letztlich eine Schönwetterlösung.

8. Raus aus den Datensilos der Konzerne

Ein roter Faden, der sich durch meinen Weg zieht, ist die schrittweise Loslösung von den großen Datenkonzernen. Wie die meisten habe auch ich lange Zeit WhatsApp genutzt – schlicht, weil es alle nutzen. Es war bequem, kostenlos und überall erreichbar. Die Frage nach den Konsequenzen stellt man am Anfang kaum. Genauso selbstverständlich waren Google-Dienste, Microsoft-Konten oder Facebook: Dienste, die sich unbemerkt in den Alltag einschleichen und irgendwann wie eine Grundversorgung wirken, obwohl sie auf einem Modell

basieren, das vom Sammeln und Verwerten von Daten lebt.

Mit der Zeit – und durch viele unabhängige Analysen zur massenhaften Datensammelei – wuchs bei mir ein Unbehagen, das sich nicht mehr wegerklären ließ. Spätestens die Snowden-Enthüllungen haben diesen Eindruck endgültig zementiert: Die großen Plattformen waren nicht einfach nur bequem, sie waren Teil eines Systems, das auf umfassende Überwachung und Profilbildung setzt. Ab diesem Punkt war klar, dass ich mich daraus Stück für Stück lösen muss. WhatsApp ist daher schon lange Geschichte; an seiner Stelle nutze ich Signal (Die großer Messenger-Übersicht). Das verändert nicht die Welt, aber es verändert die Abhängigkeiten. Ich bevorzuge einen Dienst, dessen Geschäftsmodell nicht darauf basiert, aus jedem Nutzer ein möglichst vollständiges Profil zu formen.

Ähnlich lief es im Bereich Browser und Suche. Statt einem Standard-Firefox, der mittlerweile auch gerne eigene Experimente fährt und Telemetrie mit sich bringt, setze ich auf LibreWolf mit strengeren Voreinstellungen. Ich möchte nicht bei jeder Neuinstallation wieder die selben Schalter suchen, um meine Ruhe zu haben. Das Web bleibt auch so ungemütlich genug – da muss nicht auch noch der Browser selbst zusätzliche Daten generieren.

Dasselbe Muster habe ich nach und nach auf andere Bereiche übertragen: Konten bei Microsoft-Diensten, Logins bei Google, Abhängigkeiten von Facebook – all das spielt in meinem Alltag keine Rolle mehr. Es gibt Alternativen. Manchmal sind sie etwas unbequemer, manchmal muss man sich umgewöhnen, aber der Gewinn an Unabhängigkeit ist spürbar. Ich habe gelernt, dass es nicht nur möglich ist, ohne diese Konzerne auszukommen, sondern dass man sie irgendwann auch nicht mehr vermisst.

9. Virenscanner: Abschied von der Sicherheitsillusion

Einer der letzten großen Denkfehler, die ich abgelegt habe, betrifft klassische Virenscanner. Bis in die frühen 2000er Jahre hinein waren sie für mich nahezu gleichbedeutend mit »Sicherheit«. Ein System ohne Antivirus fühlte sich »verwundbar« an, eines mit einer Suite wirkte geschützt. Werbung, Tests, Charts – all das suggeriert, man könne sich mit einem Produkt gegen die Gefahren des Netzes abschirmen.

Je tiefer ich mich mit Angriffsszenarien, Softwarearchitektur und den tatsächlichen Fähigkeiten dieser Programme beschäftigt habe, desto deutlicher wurde, dass dieser Eindruck trügt. Viele Virenscanner hängen tief im System, installieren eigene Treiber/Dienste, prüfen permanent Dateien, scannen Netzwerkverkehr – und vergrößern damit selbst die Angriffsfläche. Zudem reagieren sie in der Regel auf bekannte Muster. Für einfache Malware mag das ausreichen, für gezielte Angriffe oder moderne Techniken weit weniger.

Viel schwerer wiegt allerdings die psychologische Komponente. Wer sich auf einen Virenscanner verlässt, ist geneigt, an anderen Stellen nachlässiger zu werden. »Ich habe ja Schutz installiert« ist ein gefährlicher Satz. In der Praxis sind es andere Maßnahmen, die wirklich tragen: eine möglichst kleine Angriffsfläche durch wenige, gut gewartete Dienste, aktuelle Software, ein gehärteter Browser in einer Sandbox, ein kontrollierter E-Mail- und Dateiumgang, klare Trennung von Systemen. Ein Virenscanner kann im Einzelfall ein zusätzliches Werkzeug sein, aber er ist kein Ersatz für ein Konzept.

Heute sehe ich die meisten dieser Produkte als das, was sie für viele Hersteller sind: Geschäftsmodelle bzw. Snakeoil, die von Angst leben. Für meinen Alltag spielen sie keine Rolle mehr. Stattdessen investiere ich Zeit in das Verständnis der eigenen Systeme – und in deren Reduktion.

10. Ihr könnt das auch

Wenn man so einen Text liest, kann leicht der Eindruck entstehen:

> Das ist alles viel zu viel, das schaffe ich nie.

Genau das Gegenteil möchte ich eigentlich zeigen. Mein Weg bestand nicht aus einem einzigen radikalen Schritt, sondern aus vielen kleinen Entscheidungen, die sich über Jahre summiert haben. Es gab keinen Masterplan, keine perfekte Strategie, sondern immer nur den nächsten Schritt, der sich sinnvoll angefühlt hat.

Wichtig ist: Man muss nicht alles auf einmal umwerfen. Niemand steigt morgens auf, schmeißt alle Konten raus, migriert seine E-Mails, baut das Heimnetz um, wechselt das Smartphone-System und richtet nebenbei noch Backups ein. Realistisch ist eher: Man fängt an einer Stelle an – zum Beispiel bei den Passwörtern –, zieht das konsequent durch und nimmt sich danach das nächste Thema vor. Jeder einzelne Bereich, den man verbessert, reduziert Angriffsfläche und Abhängigkeiten.

Wenn ihr also irgendwo anfangen wollt, würde ich drei Dinge vorschlagen: Erstens einen Passwort-Manager einführen und nach und nach alle wichtigen Zugänge auf lange, zufällige Passwörter umstellen. Zweitens die eigene E-Mail-Struktur überdenken, Alias-Adressen nutzen und nicht mehr überall die gleiche Adresse hinterlassen. Drittens das Smartphone und den Browser hinterfragen: Welche Apps brauche ich wirklich, welche Berechtigungen sind nötig, welche Alternativen gibt es zu Google-Diensten, Apple-Cloud und den üblichen Standard-Apps? Der Weg weg von Google und Apple muss nicht mit dem radikalen Schnitt beginnen. Man kann zunächst quelloffene Apps aus F-Droid einsetzen, Standard-Apps austauschen und Schritt für Schritt Dienste ablösen. Wer einen Schritt weiter gehen will, kann sich ein Gerät zulegen, auf dem sich ein freieres System wie etwa GrapheneOS installieren lässt, um die Kontrolle über das eigene Gerät und die

Datenflüsse deutlich zu erhöhen. Schon diese drei Baustellen bringen enorm viel.

Dabei geht es nicht darum, alles »perfekt« zu machen. Perfektion ist ein guter Vorwand, um gar nicht erst anzufangen. Viel wichtiger ist, ins Tun zu kommen und Schritt für Schritt mehr Kontrolle zu gewinnen. Jede App, die ihr löscht, jedes Konto, das ihr schließt, jede E-Mail, die ihr durch einen Alias ersetzt, ist ein kleiner Rückgewinn von Selbstbestimmung. Und irgendwann merkt man, dass sich die Perspektive geändert hat: weg von »Ich habe nichts zu verbergen« hin zu »Ich entscheide, wer was über mich weiß.«

Mein Weg ist nur ein Beispiel, kein Maßstab. Ihr müsst nicht die gleichen Werkzeuge nutzen, nicht die gleichen Systeme und auch nicht die gleiche Konsequenz. Aber ihr könnt euch Bausteine herausgreifen, die zu eurem Alltag passen, und sie nach und nach einbauen. IT-Sicherheit ist kein exklusives Thema für Fachleute, sondern eine Sammlung von Entscheidungen, die jede und jeder treffen kann – mit dem Ziel, weniger ausgeliefert zu sein und die eigene digitale Umgebung bewusster zu gestalten.

Empfehlungsecke

Wer tiefer einsteigen möchte oder konkrete Alternativen sucht, findet in der Empfehlungsecke eine kompakte Übersicht zu datenschutzfreundlicher Software, sicheren Apps und hilfreichen Werkzeugen. Die Sammlung wird regelmäßig aktualisiert und bietet einen guten Ausgangspunkt, um eigene Entscheidungen bewusst und informiert zu treffen.

Du kannst den Blog aktiv unterstützen!

Unabhängig. Kritisch. Informativ. Praxisnah. Verständlich.

Die Arbeit von kuketz-blog.de wird vollständig durch Spenden unserer Leserschaft finanziert. Sei Teil unserer Community und unterstütze unsere Arbeit mit einer Spende.

Mitmachen ➡

11. Fazit: Sicherheit als Prozess, nicht als Zustand

Wenn ich die Entwicklung der letzten Jahre zusammenfasse, dann nicht in Form einer Liste von Tools, sondern als Änderung der Perspektive. Früher war IT-Sicherheit für mich etwas, das man »hat« oder nicht. Heute ist es eher eine Art Haltung: Misstrauen gegenüber einfachen Versprechen, Skepsis gegenüber »kostenlosen« Angeboten, der Wunsch nach Kontrolle über die eigenen Daten – und die Bereitschaft, dafür an manchen Stellen Bequemlichkeit aufzugeben.

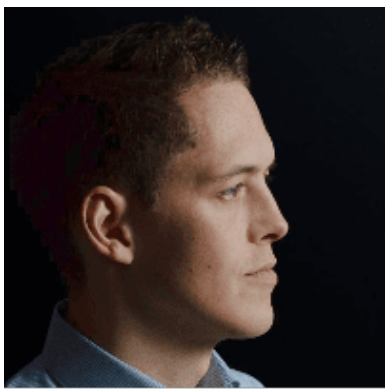
Die alten Fehler – keine Backups, wiederverwendete Passwörter, sorglos verstreute

Accounts – liegen lange hinter mir. Aber sie waren notwendig, um in Bewegung zu kommen. Was sich seitdem geändert hat, ist vor allem das Bewusstsein, dass dieser Weg kein Ende hat. Software wird sich weiterentwickeln, Dienste werden kommen und verschwinden, Bedrohungen verändern sich. Das Einzige, was konstant bleiben sollte, ist die eigene Bereitschaft, Entscheidungen immer wieder zu hinterfragen.

Es geht tatsächlich ohne Google, Microsoft, Facebook und Co. Es geht ohne zentrale Freemail-Adressen, ohne flache Heimnetze, ohne Smartphones, die im Hintergrund ständig Daten abgreifen. Es geht mit offenen, nachvollziehbaren Systemen, mit eigenen Strukturen und mit dem klaren Ziel, Kontrolle zurückzugewinnen. IT-Sicherheit ist für mich heute kein Spezialgebiet mehr, sondern ein durchgängiges Prinzip: so wenig Daten wie nötig, so viel Einsicht wie möglich, so wenig Vertrauen wie nötig – und so viel Selbstbestimmung wie möglich.

`Zum Abschluss möchte ich hervorheben`: Für diesen Weg muss man kein »Security-Nerd« sein. Er steht allen offen, die ihre digitale Umgebung bewusster gestalten wollen. Er beginnt nicht mit einem großen Schritt, sondern mit vielen kleinen – einer Entscheidung hier, einer Anpassung dort. Niemand muss über Nacht alles umwerfen. Aber jeder kann anfangen, Strukturen zu hinterfragen und Stück für Stück Kontrolle zurückzugewinnen. Der Weg vom unbedarften Nutzer zum selbstbestimmten Anwender besteht nicht aus einem großen Schritt, sondern aus vielen kleinen – und diese Schritte sind für jeden machbar.

Über den Autor | Kuketz



Mike Kuketz

In meiner freiberuflichen Tätigkeit als Pentester und Sicherheitsforscher bei Kuketz IT-Security überprüfe ich IT-Systeme, Webanwendungen und mobile Apps (Android, iOS) auf Schwachstellen. Als Lehrbeauftragter für IT-Sicherheit an der DHBW Karlsruhe sensibilisiere ich Studierende für Sicherheit und Datenschutz. Diese Themen vermittle ich auch in Workshops, Schulungen sowie auf Tagungen und Messen für Unternehmen und Fachpublikum. Zudem schreibe ich für die

Computerzeitschrift c’t und bin in Medien wie heise online, Spiegel Online und der Süddeutschen Zeitung vertreten. Der Kuketz-Blog und meine Expertise finden regelmäßig Beachtung in der Fachpresse und darüber hinaus.

Mehr Erfahren ➡

Unterstützen

Die Arbeit von kuketz-blog.de wird zu 100% durch Spenden unserer Leserinnen und Leser finanziert. Werde Teil dieser Community und unterstütze auch du unsere Arbeit mit deiner Spende.

Folge dem Blog

Wenn du immer über neue Beiträge informiert bleiben möchtest, gibt es verschiedene Möglichkeiten, dem Blog zu folgen: