

**Inklusive Cyber-
Sicherheits-Check**

Im fehlenden Netz

Ein Psychothriller aus den Abgründen unserer
digitalen Alltagswelt

Einführung

Glauben Sie wirklich, dass Ihr Zuhause sicher ist, wenn Sie abends die Haustür abschliessen?

Wir leben in einer Welt, in der wir dem Digitalen mehr vertrauen als unseren eigenen Augen. Wir wischen über Bildschirme, um Türen zu öffnen. Wir scannen kleine schwarz-weiße Quadrate, um Bezahlungen abzuwickeln. Wir lassen Sprachassistenten unsere intimsten Gespräche belauschen und vertrauen darauf, dass das grüne Symbol auf dem Display uns die Wahrheit sagt.

Technik macht unser Leben komfortabel. Sie gibt uns das Gefühl von Kontrolle.

Doch Kontrolle ist eine Illusion.

Ein einziger unbedachter Moment, eine Unachtsamkeit von genau acht Sekunden reicht aus, um die Schutzmauer einzureissen. Wenn ein Fremder nicht mehr an Ihrer Haustür klopfen muss, sondern bereits in der Linse Ihrer Webcam sitzt, verwandelt sich die vertraute Technologie in ein lautloses Gefängnis.

Die Geschichte von Thomas Blaser ist erfunden. Aber die Methoden, die Waffen und die Fallstricke, die ihn und seine Familie an den Abgrund führen, sind zu einhundert Prozent real. Sie geschehen in diesem Moment. Auf Parkplätzen, in Cafés, an Heim-Routern und auf den Smartphones von Millionen von Menschen.

Schauen Sie auf Ihr Telefon, das gerade neben Ihnen liegt.

Sind Sie sich ganz sicher, wer es gerade benutzt?

Acht Sekunden

Regen peitschte quer über den Parkplatz. Thomas zog den Kragen hoch, Wasser lief ihm vom Kapuzensaum in den Nacken.

Blick aufs Armaturenbrett: 16:42 Uhr. Achtzehn Minuten bis Hortschluss.

Nur schnell das Ticket. Thomas hechtete zum Ticketautomaten am Rande des Areal. Das kleine Display der Säule blieb jedoch dunkel, der Münzeinwurf war mit einem Streifen Klebeband blockiert. Thomas unterdrückte ein Fluchen. Dann fiel sein Blick auf das Schild direkt über dem Display:

Bequem per Smartphone bezahlen.
QR-Code scannen, Kennzeichen eingeben, fertig.

Unter dem Text befand sich ein schwarz-weißes Quadrat. Ein Anblick, den Thomas hundertfach gesehen hatte. Auf Speisekarten, an Ladesäulen, auf Werbeplakaten.

Er zog sein Smartphone aus der Tasche, entsperrte es per Fingerabdruck und öffnete die Kamera. Der gelbe Rahmen auf dem Bildschirm erfasste den Code sofort. Ein kurzer Ton bestätigte den Scan. [\[Quishing & Gefälschte QR-Codes\]](#)

Acht Sekunden. Mehr Zeit brauchte der Vorgang nicht.

Eine Webseite öffnete sich im mobilen Browser. Das Logo des städtischen Parkbetriebs prangte gewohnt in Dunkelblau an der Spitze des Bildschirms. Darunter zwei simple Eingabefelder: Amtliches Kennzeichen und Zahlungsart wählen.

Thomas tippte mit klammen Fingern sein Kennzeichen ein und wählte die Bezahlung per Kreditkarte. Er drückte auf „Kostenpflichtig parken“.

Der Bildschirm wurde weiss. Der kleine Ladekreis in der Mitte drehte sich. Einmal. Zweimal. Dreimal.

Dann erschien ein rotes Ausrufezeichen: „Verbindungsfehler. Vorgang abgebrochen. Bitte versuchen Sie es erneut.“

„Verdammt nochmal“, knurrte Thomas. Er schaute auf die Uhr. Keine Zeit für einen zweiten Versuch. Er wühlte in seinen Hosentaschen, fand glücklicherweise doch noch eine Zwei-Euro-Münze und riss das Klebeband vom Münzeinwurf ab. Die Mechanik schluckte das Geld schabend. Der Automat spuckte das Papierticket aus.

Thomas rannte zurück zum Auto, warf den Zettel hinter die Windschutzscheibe und fuhr an.

Er dachte nicht mehr an die Fehlermeldung. Warum auch? Netzprobleme im Regen gehörten zum Alltag.

Was Thomas nicht sah, als er vom Parkplatz rollte: Auf dem Parkscheinautomaten lag das schwarz-weiße Quadrat nicht direkt auf dem Metall. Es war ein hauchdünner, witterungsbeständiger Aufkleber, der präzise über den echten QR-Code gepresst worden war.

Und was Thomas auf seinem Smartphone nicht sah: Die Fehlermeldung war kein Netzfehler gewesen. Sie war das geplante Ende eines Skripts.

In den acht Sekunden, in denen der Ladekreis rotiert hatte, war im Hintergrund ein verdeck-

tes Browser-Fenster geöffnet worden. Das Skript hatte nicht nur die Eingaben abgefangen, sondern auch die aktiven Session-Tokens seiner Banking-Apps und E-Mail-Konten aus dem Zwischenspeicher ausgelesen. Gleichzeitig war im Hintergrund eine unsichtbare Konfigurationsdatei heruntergeladen worden – ein digitales Schattenzertifikat, das dem Server eines Unbekannten vollen Lesezugriff auf die Systemmitteilungen des Smartphones gewährte.

[Session Hijacking & Böartige Profile]

Vierzig Minuten später war die Welt wieder in Ordnung. Seine Tochter sass auf der Rückbank und plapperte vergnügt über ein gemaltes Bild, während Thomas den Wagen in die Einfahrt ihres Einfamilienhauses steuerte. Das Haus wirkte warm und einladend. Die smarte Aussenbeleuchtung schaltete sich automatisch ein, als sein Auto die Koordinaten der Geofencing-Zone erreichte.

Thomas stellte den Motor ab und schnallte sich los. Er griff nach seinem Smartphone auf der Mittelkonsole.

Das Display leuchtete auf. Eine Benachrichtigung seiner Sicherheits- und Konto-App schwebte im Sperrbildschirm.

Sicherheitswarnung

Ein neues Gerät hat sich erfolgreich mit Ihrem Hauptkonto verknüpft.

Gerät: Linux/Chrome_Daemon_x86

Standort: Unbekannt

Zeit: Vor 1 Minute

Thomas runzelte die Stirn. Ein Fehler des Anbieters? Er wollte auf die Mitteilung tippen, um sie zu öffnen.

Doch noch bevor sein Finger das Glas berührte, verschwand die Benachrichtigung von selbst. Als hätte eine unsichtbare Hand sie einfach weggewischt.

Sein Herz machte einen kurzen, unwillkürlichen Stolperer.

DER CYBER-
SICHERHEITS-
CHECK

Quishing (QR-Code-Phishing)

Was im Buch passiert: Thomas scannt an einer Parkuhr einen präparierten QR-Code, der als Aufkleber über dem Original platziert wurde, und wird auf eine gefälschte Bezahlseite umgelenkt.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Sehr hoch (Immer häufiger an Parkuhren, Ladesäulen, Restaurant-Tischen oder öffentlichen Plakaten.)

Gefahrenpotenzial: Mittel bis Hoch (Führt zu Daten- und Finanzdiebstahl.)

So schützen Sie sich: Fühlen statt blind scannen: Prüfen Sie bei QR-Codes an öffentlichen Orten mit dem Finger, ob ein Sticker über dem Original klebt.

Vorschau prüfen: Nutzen Sie eine Kamera-App, die vor dem Öffnen die vollständige Ziel-Adresse (URL) anzeigt. Wenn die Adresse kryptisch oder ungewöhnlich aussieht, brechen Sie ab.

Session Hijacking & Böartige Profile

Was im Buch passiert: Das Skript der gefälschten Website stiehlt im Hintergrund Browser-Cookies und installiert ein Schattenzertifikat auf dem Smartphone, um Mitteilungen mitzulesen.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Mittel (Tritt meist als Folge von Phishing-Seiten auf.)

Gefahrenpotenzial: Sehr hoch (Ermöglicht dem Täter die vollständige Überwachung des Geräts.)

So schützen Sie sich: Keine unerwarteten Profile installieren: Unter iOS und Android fragen Konfigurationsprofile explizit nach einer Bestätigung. Installieren Sie niemals Profile von Websites, die Sie nicht zu 100 % kennen.

Regelmässig ausloggen: Melden Sie sich bei sensiblen Diensten (Online-Banking, E-Mail) nach der Nutzung manuell ab.

Kapitel 2

Schatten im Netzwerk

Thomas starrte auf den glatten, schwarzen Bildschirm seines Smartphones. War da eben wirklich eine Meldung gewesen? Oder bildete er sich vor lauter Hektik schon Sachen ein?

Er entspernte das Gerät, wischte die Mitteilungszentrale nach unten. Leer. Keine Warnung, kein Warnsymbol. Er schüttelte den Kopf, atmete tief durch und stieg aus. „Komm, Schatz, ab ins Warme“, sagte er zu seiner Tochter, nahm ihren kleinen Rucksack und schloss die Haustür auf.

Der Abend verlief scheinbar friedlich. Das Abendessen duftete nach frischer Pasta, seine Frau Nina erzählte von ihrem Arbeitstag, und die Kinder stritten sich wie gewohnt um die Fernbedienung. Doch das mulmige Gefühl in Thomas' Magen wollte nicht verschwinden. Es war wie ein leises, hochfrequentes Summen, das man erst bemerkt, wenn man versucht, zur Ruhe zu kommen.

Gegen 21:30 Uhr war das Haus ruhig geworden. Die Kinder schliefen, Nina las auf dem Sofa ein Buch. Thomas sass mit seinem Laptop am Esstisch. Er wollte nach den Finanzen schauen – die monatlichen Abbuchungen standen an.

Er rief die Webseite seiner Bank auf. Die Anmeldemaske erschien. Thomas tippte seinen Benutzernamen und sein Passwort ein. Als der Ladebalken stockte, griff er nach seinem Smartphone, um die Zwei-Faktor-Bestätigung per App freizugeben. Doch auf dem Handydisplay erschien keine Aufforderung.

Stattdessen meldete der Laptop-Browser schlicht: Sitzung bereits aktiv. **[Unbefugte Kontositzungen]**

Thomas runzelte die Stirn. Sitzung bereits aktiv? Er war seit gestern nicht mehr im Online-Banking gewesen.

In diesem Moment ertönte ein leises, mechanisches Surren aus dem Flur.

Thomas blickte auf. Das kleine, blaue LED-Licht der smarten Türklingel an der Wand leuchtete auf. Das Display der Gegensprechanlage aktivierte sich und zeigte das Videobild des Hauseingangs. Die Strasse vor dem Haus war stockdunkel, der Regen hatte nachgelassen. Niemand stand vor der Tür. Kein Postbote, kein Nachbar, nicht einmal eine Katze.

Pling-Plong.

Die Türklingel schellte durch das stumme Haus.

Nina schreckte auf dem Sofa hoch. „Wartest du noch auf ein Paket?“

„Nein“, antwortete Thomas langsam. Sein Puls beschleunigte sich. Er stand auf, ging zur Haustür und blickte durch den Spion. Der Vorgarten war leer.

Er öffnete die Tür einen Spaltbreit. Die kühle Nachtluft schlug ihm entgegen. Nichts. Er schloss wieder ab und sah auf das Display der Gegensprechanlage. Das Videobild war plötzlich verzerrt, durchzogen von bunten Störstreifen.

Dann sprang der Smart-TV im Wohnzimmer von selbst an. Der Bildschirm blieb schwarz, aber aus den Lautsprechern drang ein Geräusch. Ein rhythmisches, schabendes Atmen. Als stünde jemand direkt im Raum und würde den Lautsprecher als Megafon nutzen.

„Thomas... was ist das?“, fragte Nina, ihre Stimme gezinkt von plötzlicher Angst. Sie stand auf und trat einen Schritt zurück.

„Ich... ich weiss es nicht“, stammelte Thomas. Er rannte zurück zum Esstisch, griff nach seinem Laptop und öffnete das Konfigurationsmenü seines WLAN-Routers. Seine Finger zitterten, als er das Admin-Passwort eingab.

Die Benutzeroberfläche schlug fehl, baute sich nur langsam auf. Als die Liste der verbundenen Geräte endlich erschien, fror Thomas das Blut in den Adern.

Normalerweise hingen in ihrem Heimnetzwerk genau elf Geräte: zwei Smartphones, zwei Laptops, der Fernseher, die Türklingel, das Smart-Meter und ein paar smarte Lampen.

Jetzt zeigte die Liste vierundzwanzig aktive Verbindungen.

Ein Dutzend unbekannter IP-Adressen hatte sich in sein privates Netzwerk geschlichen. Sie trugen kryptische Namen wie Device_Unknown_99, Proxy_Node_Alpha und IoT_Bridge. Der Feind sass nicht mehr nur auf seinem Handy – er war im Haus. Er hatte sich über die ungeschützten Port-Weiterleitungen seiner smarten Kameras und Lampen durch das gesamte Heimnetz gefressen. **[Smart-Home-Infiltration (IoT)]**

„Ich trenne den Router vom Strom!“, rief Thomas und griff nach der Steckerleiste unter dem Tisch.

In genau diesem Augenblick klackte es in den Wänden.

Das Licht im gesamten Haus erlosch schlagartig. Die Notbeleuchtung der Rauchmelder an der Decke blitzte einmal kurz rot auf. Die elektrischen Rollläden an den Fenstern fuhren mit einem lauten, unerbittlichen Surren nach unten und sperrten die Dunkelheit der Nacht vollends ein.

Aus der smarten Sprachbox auf der Anrichte ertönte nicht mehr das Atemgeräusch. Stattdessen erklang eine synthetische, mechanisch verzerrte Stimme, die den Raum wie Eis umklammerte:

„Zu spät, Thomas. Ich sehe euch.“

Dreimal.

Dann erschien ein rotes Ausrufezeichen: „Verbindungsfehler. Vorgang abgebrochen. Bitte versuchen Sie es erneut.“

„Verdammt nochmal“, knurrte Thomas. Er schaute auf die Uhr. Keine Zeit für einen zweiten Versuch. Er wühlte in seinen Hosentaschen, fand glücklicherweise doch noch eine Zwei-Euro-Münze und riss das Klebeband vom Münzeinwurf ab. Die Mechanik schluckte das Geld schabend. Der Automat spuckte das Papierticket aus.

Thomas rannte zurück zum Auto, warf den Zettel hinter die Windschutzscheibe und fuhr an.

Er dachte nicht mehr an die Fehlermeldung. Warum auch? Netzprobleme im Regen gehörten zum Alltag.

Was Thomas nicht sah, als er vom Parkplatz rollte: Auf dem Parkscheinautomaten lag das schwarz-weiße Quadrat nicht direkt auf dem Metall. Es war ein hauchdünner, witterungsbeständiger Aufkleber, der präzise über den echten QR-Code gepresst worden war.

Und was Thomas auf seinem Smartphone nicht sah: Die Fehlermeldung war kein Netzfehler gewesen. Sie war das geplante Ende eines Skripts.

In den acht Sekunden, in denen der Ladekreis rotiert hatte, war im Hintergrund ein verdecktes Browser-Fenster geöffnet worden. Das Skript hatte nicht nur die Eingaben abgefangen,

DER CYBER-
SICHERHEITS-
CHECK

Unbefugte Konto-Sitzungen (Session-Klau)

Was im Buch passiert: Der Täter nutzt gestohlene Sitzungs-Cookies (Session Tokens), um sich ohne erneute Passwordeingabe beim Online-Banking einzuloggen.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Hoch (Sehr verbreitet bei Infektionen durch Schadsoftware oder unverschlüsselte Sitzungen.)

Gefahrenpotenzial: Sehr hoch (Hebelt das normale Passwort aus.)

So schützen Sie sich: Aktive Sitzungen beenden: Prüfen Sie in den Einstellungen Ihrer Konten (Google, Banking, Social Media) regelmässig die Liste der „Aktiven Geräte/Sitzungen“ und melden Sie fremde Geräte ab. Browser-Daten löschen: Leeren Sie in regelmässigen Abständen Ihren Browser-Verlauf und die Cookies.

Smart-Home-Infiltration (IoT-Sicherheit)

Was im Buch passiert: Der Hacker dringt über veraltete, schlecht gesicherte Smart-Home-Geräte (wie smarte Kameras und Lampen) in das gesamte Heimnetzwerk ein.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Hoch (Unzählige günstige Smart-Home-Geräte hängen ungepatcht im Netz und werden automatisiert gescannt.)

Gefahrenpotenzial: Sehr hoch (Das gesamte private Heimnetzwerk wird kompromittiert.)

So schützen Sie sich: Gast-WLAN nutzen: Richten Sie an Ihrem WLAN-Router ein zweites Netzwerk (Gast-WLAN) ein. Verbinden Sie alle Smart-Home-Geräte ausschliesslich mit diesem Netz. So bleiben Laptops, Handys und PCs isoliert.

Standard-Passwörter ändern: Ändern Sie bei der Einrichtung jedes Smart-Home-Geräts sofort das herstellerseitig vorgegebene Passwort.

Kapitel 3

Vertraute Stimmen

Die Dunkelheit im Wohnzimmer fühlte sich bleischwer an. Nur das hektische, rote Blinken der Rauchmelder an der Decke warf Dämmerlicht auf Ninas erbleichtes Gesicht.

„Thomas, mach das aus! Mach es aus!“, schrie sie, die Hand fest auf die Brust gepresst.

Thomas stolperte durch die Finsternis, trat gegen einen Stuhl, tastete sich zur Anrichte vor und riss das Stromkabel der Smart-Box mit einem gewaltsamen Ruck aus der Steckdose. Die synthetische Stimme verstummte schlagartig. Stille legte sich über den Raum, unterbrochen nur vom schweren Atmen der beiden.

An Schlaf war in dieser Nacht nicht zu denken. Thomas verbrachte die verbleibenden Stunden bis zum Morgengrauen damit, den Hauptschalter des Routers manuell umzulegen, die Sicherungen für die Smart-Home-Komponenten herauszudrehen und die elektrischen Rollläden mühsam über die mechanische Notentriegelung hochzukurbeln.

Als die erste Morgensonne durch die Fenster brach, schien das Haus wieder normal. Doch der Schein trog. Das Gefühl von Sicherheit war endgültig zerstört.

Samstagmittag, 13:15 Uhr.

Der Duft von frisch gemähtem Gras lag über dem Rasensportplatz der Gesamtschule. Pfiffe, Anfeuerungsrufe von den Rängen und das Klatschen von Händen hallten über das Gelände. Thomas' vierzehnjähriger Sohn Leo nahm an einem regionalen Fussballturnier teil.

Thomas hatte darauf bestanden, Leo persönlich hinzufahren. Das Handy des Jungen lag – nach heftigen Diskussionen – stummgeschaltet im Sportbeutel. Thomas wollte verhindern, dass irgendwelche ominösen Nachrichten das Smartphone seines Sohnes erreichten.

Während Leo auf dem Feld dem Ball nachjagte, stand Thomas am Spielfeldrand, die Arme

verschränkt, die Augen unruhig wandern lassend. Jede Person, die vorbeiging, jeder Passant mit einem Smartphone in der Hand wirkte plötzlich verdächtig.

Plötzlich spürte Thomas ein sanftes Vibrieren an seinem Handgelenk. Seine Smartwatch.

Ein eingehender Anruf.

Auf dem kleinen Display leuchtete der Name auf: Leo.

Thomas erstarrte. Er schaute auf das Spielfeld. Leo trug das grüne Trikot mit der Nummer 7 und sprintete gerade der Mittellinie entgegen. Sein Handy lag garantiert in der Umkleidekabine.

Warum raste Leos Name auf seinem Display? [Caller-ID-Spoofing]

Thomas nahm ab und drückte die Uhr an sein Ohr. „Hallo?! Wer ist da?“

Aus dem Lautsprecher drang Nebengeräusch. Strassenlärm. Und dann eine Stimme, die Thomas bis ins Mark erschüttern liess. Es war nicht die Stimme eines Fremden. Es war seine eigene.

Die Frequenz, der Tonfall, das leichte Nusseln bei den Konsonanten – es war exakt seine Stimme, die da glasklar aus dem Lautsprecher sprach.

„Leo? Wo bist du? Mama hatte einen schweren Unfall. Du musst sofort zum Haupteingang des Sportplatzes kommen. Da steht ein schwarzer Transporter mit Warnblinker. Fahr mit ihnen ins Krankenhaus, ich bin schon dort. Schnell, Leo!“

Das Gespräch brach ab.

Thomas' Herz hämmerte gegen seine Rippen wie ein gefangener Vogel. Voice Cloning. Eine KI hatte aus seinen Sprachnachrichten und Videos der letzten Monate eine perfekte Kopie seiner Stimme synthetisiert. [KI-Voice-Cloning]

Er blickte panisch auf das Spielfeld.

Leo stand nicht mehr an der Mittellinie. Die Auswechselbank war leer. Die Umkleidekabinen – Leo musste sein Handy gehört und den Anruf entgegen genommen haben!

„LEO!“, brüllte Thomas und hechtete los. Er rannte, wie er noch nie in seinem Leben gerannt war, stiess Zuschauer zur Seite, ignorierte den verdutzten Blick des Schiedsrichters und stürzte um das Schulgebäude herum in Richtung Parkplatz.

Am Ende der Zufahrt stand ein schwarzer Kastenwagen. Die Schiebetür war einen Spaltbreit geöffnet.

Und dort, nur noch drei Meter vom Wagen entfernt, stand Leo. Verzweiflung im Gesicht, das Smartphone zitternd in der Hand. Er setzte gerade an, den Fuss auf die Trittstufe des Transporters zu heben.

„LEO! HALT! BEWEG DICH NICHT!“, schrie Thomas aus voller Kehle.

Der Junge wirbelte herum. Verwirrung spiegelte sich in seinen Augen. Er sah seinen Vater, der im Vollsprint auf ihn zustürzte – und dann blickte er zurück zu dem Mann im Fahrerhaus des Transporters, der eine dunkle Sonnenbrille trug.

Der Fahrer erkannte, dass die Falle aufgefliegen war. Die Schiebetür knallte zu, die Reifen quietschten auf dem Asphalt, und der schwarze Transporter schoss davon.

Thomas erreichte seinen Sohn, riss ihn an sich und schlang die Arme um den zitternden Jungen.

„Papa...“, stammelte Leo, tränenüberströmt. „Du... du hast mich doch angerufen? Du hast gesagt, Mama...“

„Ich war das nicht, Leo“, flüsterte Thomas, während ihm das Adrenalin eiskalt durch die Adern schoss. „Ich war das nicht.“

Erst jetzt wurde Thomas die grauenhafte Wahrheit klar: Der Täter hatte gewusst, wo Leo war. Er hatte gewusst, wie die Rollen verteilt waren, und er hatte in Echtzeit zugeschlagen.

Der unsichtbare Passagier fuhr nicht nur mit. Er bestimmte die Route.

DER CYBER-
SICHERHEITS-
CHECK

Caller-ID-Spoofing (Gefälschte Anrufer-ID)

Was im Buch passiert: Der Täter lässt auf dem Display von Thomas' Sohn die echte Telefonnummer des Vaters anzeigen.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Sehr hoch (Täglicher Standard bei Trickbetrügern, Schockanrufen oder angeblichen Bankmitarbeitern.)

Gefahrenpotenzial: Mittel bis Hoch (Baut enormen psychologischen Druck auf.)

So schützen Sie sich: Rufnummern sind nicht fälschungssicher: Verlassen Sie sich niemals allein auf die angezeigte Telefonnummer.

Gegenanruf tätigen: Legen Sie im Zweifel auf und rufen Sie die Person über eine Ihnen bekannte, fest abgespeicherte Nummer selbst zurück.

KI-Voice-Cloning (Geklonte Stimmen)

Was im Buch passiert: Der Täter nutzt eine per KI geklonte Stimme von Thomas, um den Sohn am Telefon in eine Falle zu locken.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Hoch (stark steigend) (Frei zugängliche KI-Tools machen Stimmklone aus wenigen Sekunden Online-Audio extrem leicht.)

Gefahrenpotenzial: Sehr hoch (Täuscht selbst engste Familienangehörige vollkommen.)

So schützen Sie sich: Skepsis bei emotionalen Notlagen: Je dringlicher und dramatischer der Anruf, desto eher sollten Sie inhalten misstrauen. Familien-Codewort nutzen.

Die digitale Umklammerung

Die Stille im Haus war nach der Rückkehr vom Sportplatz erdrückend. Leo sass verstört in seinem Zimmer, während Nina zitternd zwei Tassen Kaffee einschenkte.

„Wir müssen zur Polizei. Sofort, Thomas“, sagte Nina mit fester, aber brüchiger Stimme.

„Du hast recht“, erwiderte Thomas. Er griff nach seinem Smartphone auf dem Küchentisch, um die Nummer der lokalen Polizeidienststelle herauszusuchen.

Doch als er das Display aktivierte, starrte er auf ein leeres Empfangssymbol. Oben rechts in der Statusleiste prangte kein LTE, kein 5G, kein einziges Balkensignal. Stattdessen stand dort in grauen Buchstaben: Nur Notrufe.

Thomas runzelte die Stirn. Er startete das Gerät neu. Als der Ladebildschirm erlosch, erschien sofort eine Systemmeldung des Mobilfunkanbieters:

SIM-Karte deaktiviert

Ihre Rufnummer wurde erfolgreich auf Ihr neues Gerät (eSIM) übertragen.

Thomas entglitt die Farbigkeit aus dem Gesicht. SIM-Swapping.

Der Täter hatte nicht nur seine Web-Sessions abgefangen. Er hatte sich beim Mobilfunkanbieter als Thomas ausgegeben, ein Social-Engineering-Manöver durchgezogen und seine Handynummer auf ein eigenes Gerät gekapert. Damit gehörten ihm ab sofort alle Bestätigungs-SMS für Sicherheitscodes, Passwort-Rücksetzungen und Banktransaktionen. [SIM-Swapping]

„Mein Netz ist weg“, flüsterte Thomas. „Er hat meine Handynummer gestohlen.“

Er hechtete zu seinem Laptop, klappte ihn auf und stellte eine Kabelverbindung her, um über das Web-Portal seiner Bank die Konten sperren zu lassen. Er gab seine Zugangsdaten ein.

Fehler: Das eingegebene Passwort ist falsch.

„Nein, nein, nein!“, fluchte er und tippte auf Passwort vergessen.

Die Meldung, die folgte, war wie ein Schlag ins Gesicht:

Ein Link zur Passwort-Rücksetzung wurde an Ihre primäre E-Mail-Adresse sowie per SMS an Ihre Rufnummer gesendet.

Der Täter hatte die Passwörter längst geändert. Durch die Kontrolle über die SIM-Karte fackelte er nicht lange: Er fing die SMS-Bestätigungscode in Echtzeit ab, schloss Thomas aus seinen eigenen E-Mail-Postfächern aus und übernahm Schritt für Schritt seine gesamte digitale Identität. Thomas war von seinen eigenen Finanzen, seinen Daten und seinen Kommunikationsmitteln abgeschnitten.

Pling.

Das Smartphone seiner Frau, das auf dem Tresen lag, schlug an. Eine E-Mail-Benachrichtigung.

Nina griff danach. „Thomas... hier ist eine Nachricht von... von dir?“

Der Absender lautete auf Thomas' gehackte Mailadresse. Der Betreff war kurz: Ihr seid hübsch, wenn ihr euch sorgt.

Mit zitternden Fingern öffnete Nina die Mail. Im Anhang befand sich eine Reihe von Bild-dateien.

Thomas beugte sich über ihre Schulter und erstarrte.

Es waren Fotos. Live-Aufnahmen aus den letzten zehn Minuten. Man sah Nina, wie sie zit-ternd den Kaffee eingoss. Man sah Thomas, wie er verzweifelt auf seinen Laptop einprügelte. Die Perspektive der Kamera war leicht erhöht, von der Seite der Anrichte aus.

Thomas blickte langsam auf. Auf der Anrichte stand sein Dienst-Notebook, zugeklappt, aber mit dem Ladekabel verbunden. Am oberen Bildschirmrand der geschlossenen Klappe blink-te ein winziges, grünes Licht.

Die Webcam war aktiv. Der Täter schaute ihnen im eigenen Wohnzimmer zu. [Cam-Jacking]

In diesem Moment dröhnte ein gewaltiges Hämmern gegen die schwere Eichenholz-Haustür.

„POLIZEI! ÖFFNEN SIE SOFORT DIE TÜR!“, brüllte eine raue Männerstimme von draussen.

SIM-Swapping (Kaperung der Telefonnummer)

Was im Buch passiert: Der Hacker bringt den Mobilfunkanbieter durch Täuschung dazu, Thomas' Rufnummer auf eine neue eSIM zu übertragen, um SMS-Sicherheitscodes abzufangen.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Mittel (Tritt meist gezielt auf, wenn Täter bereits Zugänge oder finan-zielle Werte vermuten.)

Gefahrenpotenzial: Extrem hoch (Der Täter kapert den zweiten Faktor für Banken und Konten.)

So schützen Sie sich: Kunden-PIN beim Anbieter setzen: Richten Sie bei Ihrem Mobilfunkanbieter eine persönliche Kunden-PIN ein, ohne die keine Vertragsänderungen vorgenommen werden dürfen.

SMS nicht als 2FA nutzen: Steigen Sie von SMS-Codes auf App-basierte Authentifikatoren oder Hardware-Schlüssel um.

DER CYBER-
SICHERHEITS-
CHECK

Cam-Jacking (Webcam-Übernahme)

Was im Buch passiert: Der Angreifer aktiviert aus der Ferne die Webcam von Thomas' Notebook und spioniert die Familie im Wohnzimmer aus.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Mittel (Meist Folge von unbemerkt installierter Trojaner-Software.)

Gefahrenpotenzial: Sehr hoch (Massiver Eingriff in die Privatsphäre und Erpressungspotenzial.)

So schützen Sie sich: Physische Kamera-Abdeckung: Verkleben Sie Webcams an Laptops und Monitoren mit einer Schiebeabdeckung oder einem einfachen Stück Klebeband.

Zugriffsrechte prüfen: Kontrollieren Sie in den Einstellungen Ihres Betriebssystems regelmässig, welche Programme Zugriff auf Kamera und Mikrofon haben.

Kapitel 5

Das analoge Protokoll

Das Hämmern gegen die Eichenholztür war so heftig, dass der Rahmen vibrierte.

„Thomas Blaser! Öffnen Sie sofort, oder wir brechen die Tür auf!“, schallte es von draussen.

Nina presste die Hände auf den Mund. Thomas stürzte zum Flur, entsicherte das Schloss und riss die Tür auf. Auf der Veranda standen zwei Polizeibeamte in schusssicherer Kleidung, die Hände auf den Holstern ihrer Dienstwaffen. Dahinter blitzte das blaue Signallicht zweier Streifenwagen durch die Dämmerung.

„Was... was ist denn los?“, stammelte Thomas, während er die Hände unwillkürlich anhob.

„Thomas Blaser? Sie sind vorläufig festgenommen“, sagte der ältere der beiden Beamten mit eisalter Stimme. „Gegen Sie liegt ein dringender Tatverdacht wegen gewerbsmässiger Erpressung, schwerer Computerkriminalität und der Verbreitung von Drohschreiben an städtische Einrichtungen vor.“

„Was?! Das ist ein Irrtum! Ich wurde gehackt!“, rief Thomas.

„Sparen Sie sich das“, unterbrach ihn die jüngere Beamtin. „Von Ihrer IP-Adresse und unter Nutzung Ihrer verifizierten E-Mail-Signatur wurden in den letzten zwei Stunden mehrere Erpresserschreiben an die Stadtparkasse und das Schulamt verschickt. Inklusive Sperrkonten-Forderungen. Wir haben einen richterlichen Beschluss zur Beschlagnahme aller Speichermedien.“ [Digitaler Identitätsdiebstahl]

Thomas fühlte, wie ihm der Boden unter den Füßen weggezogen wurde. Der Täter hatte ihn nicht nur ausgespioniert – er benutzte Thomas' Identität als Schutzschild für seine eigenen Verbrechen. Während Thomas hilflos im Wohnzimmer gesessen hatte, liefen auf seinen Namen schwere Straftaten.

„Hören Sie mir zu!“, schrie Thomas verzweifelt und deutete auf den Laptop auf dem Küchentisch. „Sehen Sie sich die Webcam an! Jemand spioniert uns live aus! Mein Handy wurde

gekapert, meine SIM-Karte übernommen! Der Täter sitzt da draussen und lacht sich ins Fäustchen!"

Der ältere Polizist zögerte. Er trat einen Schritt in den Flur und blickte auf das blinkende Licht der Webcam. Dann sah er in die verängstigten Gesichter von Nina und Leo, der zitternd auf der Treppe sass. Die Professionalität des Beamten schlug in skeptische Wachsamkeit um.

„Wenn das stimmt, Blaser, dann sind Sie und Ihre Familie in Lebensgefahr“, sagte der Polizist leise. „Aber wir müssen die Geräte mitnehmen. Zur spurensichernden Analyse.“

„Nehmen Sie alles mit!“, sagte Thomas sofort. „Nehmen Sie die Laptops, die Tablets, die Handys. Hauptsache, dieses Zeug ist aus diesem Haus!“

Eine Stunde später war die Polizei weg. Sie hatten alle Speichermedien verpackt und versiegelt. Eine Festnahme hatten die Beamten vorerst ausgesetzt, doch Thomas stand unter strenger Beobachtung und durfte die Stadt nicht verlassen.

Das Haus war nun vollkommen stumm. Keine Lichter blitzten mehr, keine Displays leuchteten.

Thomas versammelte Nina und Leo am massiven Holztisch in der Küche. Auf dem Tisch lag nichts Digitales mehr. Nur ein Zettel und ein Bleistift.

„Wir müssen komplett analog werden“, sagte Thomas leise. Seine Stimme war ruhig geworden, getrieben von einer neuen, klaren Entschlossenheit. „Er kontrolliert alles, was ein Signal sendet. Unser WLAN, unsere Handys, unsere Autonavigation. Solange wir digitale Geräte nutzen, ist er uns immer einen Schritt voraus.“

Thomas zog den Bogen Papier zu sich heran und schrieb in grossen Druckbuchstaben ein einzelnes Wort auf das Blatt:

PANTHER

„Was ist das?“, fragte Leo leise.

„Das ist unser Familien-Codewort“, erklärte Thomas eindringlich und blickte seine Frau und seinen Sohn an. „Egal wer ab jetzt anruft, egal wer eine Nachricht schickt, egal wie sehr die Stimme nach mir, nach Mama oder nach dir klingt: Wenn die Person dieses Wort nicht im ersten Satz nennt, ist es ein Fake. Ein KI-Cloning. Ein Betrug.“ [Das analoge Notfall-Codewort]

Nina nickte langsam, während ihr die Tränen über die Wangen liefen. „Und wie wehren wir uns jetzt, Thomas? Ohne Computer? Ohne Handy?“

Thomas sah auf das Papier vor sich. Ein Lächeln ohne jede Freude stieg in ihm auf.

„Der Täter glaubt, dass er uns im Netz gefangen hat. Er denkt, wir sind blind und taub, weil er uns die Bildschirme weggenommen hat“, flüsterte Thomas. „Aber genau das ist jetzt unser Vorteil. Ab jetzt hinterlassen wir keine digitalen Spuren mehr. Wir locken ihn auf analoges Terrain.“

In diesem Moment ertönte ein lautes Poltern vom Dachboden des Hauses. Als würde jemand mit Stiefeln über die Holzbohlen gehen.

Obwohl sämtliche Türen und Fenster verriegelt waren.

Digitaler Identitätsdiebstahl

Was im Buch passiert: Der Täter nutzt Thomas' gekaperte E-Mail-Adresse und IP-Adresse, um Straftaten in dessen Namen zu begehen.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Sehr hoch (Passiert täglich millionenfach durch Datenlecks bei Online-Shops und Plattformen.)

Gefahrenpotenzial: Extrem hoch (Führt zu rechtlichen Problemen, Rufmord und finanziellen Schäden.)

So schützen Sie sich: Sicheres Haupt-E-Mail-Postfach: Sichern Sie Ihr primäres E-Mail-Konto mit einem starken Passwort und Hardware-Schlüsseln ab.

Datenlecks prüfen: Überprüfen Sie auf Plattformen wie haveibeenpwned.com, ob Ihre Daten in Lecks aufgetaucht sind.

Fehlendes analoges Familien-Codewort

Was im Buch passiert: Die Familie vereinbart ein geheimes, nicht digital festgehaltenes Wort, um Fälschungen und KI-Klonstimmen sofort zu entlarven.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Sehr hoch (die Sicherheitslücke) (Fast keine Familie nutzt heutzutage ein solches Notfall-Codewort.)

Gefahrenpotenzial: Sehr hoch (Macht die Familie anfällig für Social-Engineering-Tricks.)

So schützen Sie sich: Ein Wort für den Notfall: Vereinbaren Sie innerhalb der Familie ein einfaches, unvergessliches Codewort (z. B. ein Begriff aus der Kindheit).

Konsequente Anwendung: Wer das Codewort bei verdächtigen Notfall-Anrufen nicht nennen kann, ist nicht die echte Person.

Schatten auf dem Dachboden

Das Poltern über ihren Köpfen verstummte so abrupt, wie es begonnen hatte. Die Stille, die folgte, war beinahe noch unerträglicher.

Thomas stand starr am Küchentisch. Er sah zu Nina, die ihren Sohn fest an sich drückte. In ihren Augen lag pure Angst.

„Bleibt hier“, flüsterte Thomas. „Abschliessen. Wenn ihr irgendetwas hört, nutzt die Pfeife aus dem Notfallset.“

Er griff nach der schweren Metall-Taschenlampe aus dem Flurschrank. Seine Hände waren feucht, sein Puls raste. Schritt für Schritt schlich er die Holztreppe hinauf in den ersten Stock und weiter zur schmalen Klapptreppe, die auf den Dachboden führte.

Der Geruch von altem Holz und Staub schlug ihm entgegen, als er die Luke vorsichtig nach oben drückte. Er schob den Kopf durch die Öffnung und leuchtete mit dem hart gebündelten Strahl der Taschenlampe in die Finsternis.

Nichts. Nur ausrangierte Umzugskartons, alte Kindermöbel und die Dämmwolle zwischen den Dachbalken.

Thomas stieg vollends nach oben. Die Holzbohlen knarzten leise unter seinen Sohlen. Er leuchtete die Winkel ab. Am hinteren Ende des Raumes, gleich neben der Wand zum Nachbarhaus, verlief der Kabelstrang, den Thomas vor zwei Jahren für die Netzwerkdosen im Haus verlegt hatte.

Dort blinkte etwas. Ein winziges, blaues Licht.

Thomas stockte. Er trat näher und kniete sich in den Staub.

Direkt an der Hauptnetzwerkdose, kurz bevor das Kabel in den Router im Erdgeschoss führte, hing ein schwarzes, etwa zigarettenstachelgrosses Plastikgehäuse. Es war mit einem Kabelbinder fachmännisch am Balken befestigt und schmarotzte den Strom direkt von einer Notstrom-Abzweigdose.

Thomas brauchte keinen IT-Abschluss, um zu verstehen, was er da vor sich hatte. Es war ein autarker Mini-Computer – ein Rogue Access Point. Der Täter hatte den Schutz des Routers gar nicht aus der Ferne knacken müssen. Er war irgendwann physisch auf diesem Dachboden gewesen und hatte die Hardware direkt in Thomas' Heimnetz eingeplant. Ein Trojanisches Pferd aus Plastik und Silizium, das dem Hacker von aussen dauerhaften, ungefilterten Zugriff gewährte. [\[Rogue Access Points\]](#)

Wut kochte in Thomas hoch. Der Kerl war in meinem Haus.

Er griff nach dem schwarzen Gehäuse, um das Netzkabel herauszureissen.

Klack.

Ein mechanisches Geräusch im Inneren der Dose löste aus. Ein leises Zischen folgte, und eine scharf riechende, chemische Flüssigkeit versprühte sich aus einem feinen Ventil an der Seite. Thomas wich hustend zurück und wischte sich über die Augen.

Gleichzeitig surrte ein winziger Thermodrucker, der in der Unterseite der Box verbaut war. Ein schmaler Papierstreifen – wie ein Kassenbon – schoss heraus und fiel auf die staubigen

Holzbohlen.

Thomas hob den Streifen mit zitternden Fingern auf und leuchtete ihn an. Darauf stand in gestochen scharfen, schwarzen Buchstaben:

Glaubst du wirklich, mit dem Router ist es vorbei?

Nina ist gerade in der Kanzlei angekommen. Ihr PC steht offen.

Acht Minuten, Thomas.

DER CYBER-
SICHERHEITS-
CHECK

Rogue Access Points (Hardware-Hacks)

Was im Buch passiert: Der Täter platziert heimlich einen Mini-Computer auf dem Dachboden, der sich direkt mit dem Heimnetzwerk verbindet.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Gering (Erfordert physischen Zugang zum Gebäude; wird meist nur bei gezielter Spionage eingesetzt.)

Gefahrenpotenzial: Extrem hoch (Umgeht die Sicherheitsregeln des Routers vollkommen.)

So schützen Sie sich: Physische Sicherheit: Lassen Sie fremde Handwerker oder Dienstleister nicht unbeaufsichtigt in sensible Hausbereiche.

Netzwerk-Scans: Prüfen Sie in der Benutzeroberfläche Ihres Routers regelmässig die Liste der verbundenen Geräte.

Kapitel 7

Falle im öffentlichen Netz

„Sieben Minuten!“, knurrte Thomas, während er die Stufen der Dachbodentreppe hinunterstürzte.

Er rief Nina und Leo im Vorbeigehen zu, dass sie im Haus bleiben und die Tür verriegeln sollten. Er riss seine Jacke vom Haken, schnappte sich eine alte Umhängetasche, in der seit Jahren ein ausrangierter Ersatz-Laptop ohne SIM-Slot und ohne jegliche persönliche Daten lag, und rannte nach draussen.

Er konnte Nina nicht anrufen – sein Handy war tot, ihre Verbindung unsicher. Er musste an einen Ort mit schnellem Internet, um sich über einen gesicherten Tunnel auf den Server der Kanzlei einzuwählen oder ihren IT-Leiter zu kontaktieren.

Drei Strassen weiter lag das Café Central. Ein belebter Zufluchtsort mit ständiger Publikumsströmung.

Thomas stürzte durch die Tür, ignorierte die verdutzten Blicke des Kellners und setzte sich an einen kleinen Eck Tisch im hinteren Bereich. Er klappte den alten Laptop auf, fuhr das ver-

staubte System hoch und suchte nach verfügbaren WLAN-Netzen.

In der Liste erschien sofort ein Signal mit voller Stärke:

CafeCentral_Guest_Free

Perfekt, dachte Thomas. Er klickte auf Verbinden. Keine Passwortabfrage war nötig. Die Login-Seite des Cafés öffnete sich sofort im Browser mit dem gewohnten Logo und einem grossen Button: Jetzt kostenlos einwählen.

Thomas wollte bereits klicken, um die Kanzlei-E-Mail einzugeben. Doch kurz bevor seine Finger die Taste berührten, hielt er inne.

Sein Blick fiel auf die Adresszeile im Browser.

Da stand nicht cafecentral-bern.ch, sondern cafecentral-guest-login.net. Ein klitzekleiner Unterschied.

Thomas schluckte trocken. Er öffnete das erweiterte Netzwerkdiagnose-Werkzeug seines Laptops und prüfte das Sicherheitszertifikat des Hotspots.

Es war eine Falle. Der Täter hatte gewusst, wohin Thomas flüchten würde. Er hatte in Reichweite des Cafés einen eigenen, tragbaren WLAN-Sender platziert – einen sogenannten Evil Twin. Ein gefälschtes Netzwerk mit identischem Namen, das alle Daten der unbedarften Gäste abfing und durch seine eigenen Server leitete. Hätte Thomas sich eingeloggt, hätte er dem Hacker die Zugangsdaten zur Kanzlei auf einem Silbertablett serviert. [Evil-Twin-Angriffe]

„Nicht mit mir“, flüsterte Thomas und klappte die WLAN-Funktion augenblicklich wieder zu.

Er riss das Ladekabel heraus und stand auf. Doch als er das Café verlassen wollte, versperrte ihm ein Mann in einem dunklen Mantel den Weg, der unauffällig am Nachbartisch gesessen hatte. Der Mann hielt ein Smartphone hoch, auf dessen Display eine Textnachricht leuchtete:

Guter Blick für das Zertifikat, Thomas. Aber du bist zu langsam. Dein Forensiker-Freund hat eben meine Einladung geöffnet.

Evil-Twin-Angriffe (Gefälschte WLAN-Hotspots)

Was im Buch passiert: Im Café betreibt der Hacker ein gefälschtes WLAN mit einem zum Verwechseln ähnlichen Namen, um den Datenverkehr abzufangen.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Hoch (Beliebt an stark frequentierten Orten wie Flughäfen, Bahnhöfen, Hotels oder Cafés.)

Gefahrenpotenzial: Mittel bis Hoch (Ermöglicht das Abfangen unverschlüsselter Daten.)

So schützen Sie sich: Mobiles Netz bevorzugen: Nutzen Sie unterwegs primär das mobile Datennetz (4G/5G) statt öffentlicher Hotspots. VPN verwenden: Wenn Sie öffentliches WLAN nutzen müssen, schalten Sie stets eine verschlüsselte VPN-Verbindung ein.

DER CYBER-
SICHERHEITS-
CHECK

Der digitale Köder

Thomas wich einen Schritt zurück, stiess die Tür des Cafés auf und hechtete hinaus auf die Strasse. Der Mann im dunklen Mantel folgte ihm nicht – er blieb im Eingang stehen und lächelte nur matt. Er war kein Schläger, sondern lediglich ein Bote im digitalen Schachspiel.

Thomas rannte. Er schlug Haken durch zwei Seitengassen, um jeden Verfolger abzuschütteln, bis er vor einem unauffälligen Backsteingebäude im Gewerbegebiet stand. Hier lag die Werkstatt von Marc – einem ehemaligen Studienkollegen und freiberuflichen IT-Forensiker.

Ohne anzuklopfen, polterte Thomas durch die Tür.

Marc sass vor drei riesigen Monitoren, eine Kaffeetasse in der Hand. „Thomas? Was zum Teufel... du siehst aus, als hättest du einen Geist gesehen.“

„Schlimmer“, schnaufte Thomas und knallte die Umhängetasche auf den Tisch. „Jemand hat mein Leben übernommen. Und er war gerade dabei, deine Systeme zu scannen.“

Innerhalb von zehn Minuten hatte Thomas die Ereignisse der letzten 24 Stunden zusammengefasst. Marc hörte schweigend zu, während sein Gesichtsausdruck von skeptischer Überraschung in eiskalte Professionalität umschlug.

„Der Typ ist gut“, murmelte Marc und tippte blitzschnell Befehle in ein schwarzes Terminal-Fenster. „Er nutzt automatisierte Skripte, um deine Konten zu isolieren. Wenn wir ihn stoisch abwehren, sucht er sich einfach den nächsten Winkel. Wir müssen aufhören, Schildkröte zu spielen. Wir stellen ihm einen Köder.“

„Einen Honeypot?“, fragte Thomas.

„Genau. Wir servieren ihm ein saftiges Filetstück, das er unmöglich ignorieren kann.“ Marc öffnete einen Editor und erstellte eine gefälschte PDF-Datei mit dem Titel `Kanzlei_Notfall_Protokoll_Beweise.pdf`.

Die Datei sah aus wie eine verschlüsselte Sammlung von Protokollen, die den Täter entlarven könnte. Gesichert war sie mit einem simpel wirkenden Passwort. Doch im Code des Dokumentes war ein unsichtbares Signal eingebettet – ein digitaler Kanarienvogel. Sobald die Datei heruntergeladen und geöffnet würde, rief sie im Hintergrund eine neutrale Cloud-Adresse auf und übermittelte dabei unbemerkt die echte IP-Adresse und den Standort des Lesers. [\[Honeypots & Canary Tokens\]](#)

Marc lud die präparierte Datei auf einen ungesicherten Cloud-Ordner, der mit Thomas' gehackter Mailadresse verknüpft war, und schickte eine fingierte Statusnachricht ab.

Acht Minuten verstrichen.

Auf Marcs Hauptmonitor lief ein roter Graph. Thomas hielt den Atem an.

Plötzlich schlug der Graph aus. Ein gelber Punkt blinkte auf der digitalen Karte auf.

„Er hat angebissen!“, rief Marc. „Er lädt die Datei herunter... er öffnet sie.“

Ein Ladebalken füllte sich. Das Skript löste aus und umging die Anonymisierungsserver des Täters durch die direkte Interaktion im Dokument.

Auf dem Monitor sprangen grüne Zahlenzeilen an. Eine unverschleierte IP-Adresse baute

sich auf, gefolgt von einer geografischen Koordinate.

„Ich habe ihn!“, flüsterte Marc. „Er sitzt nicht im Ausland. Er ist hier in der Stadt. Industriegebiet Ost, Halle 12.“

Doch noch bevor Thomas jubeln konnte, wurde Marcs Bildschirm schlagartig rot. Eine Fehlermeldung nach der anderen kaskadierte über die Monitore.

„Scheisse!“, brüllte Marc und riss an den Tastaturkabeln. „Er hat den Köder bemerkt! Er fährt eine Gegenattacke über die Kanzlei-Server – er geht auf Ninas Firma los!“

Honeypots & Canary Tokens (Verteidigung)

Was im Buch passiert: Der IT-Forensiker erstellt ein gefälschtes Dokument mit einem unsichtbaren Tracking-Pixel, das bei Öffnen die IP-Adresse des Täters verrät.

Risiko-Analyse:

Einordnung: Experten-Verteidigungswerkzeug.

So nutzen Profis das: Unternehmen und IT-Spezialisten nutzen digitale Stolperdrähte (Canary Tokens), um unbefugte Zugriffe auf Dateien sofort zu bemerken und den Angreifer zu lokalisieren.

DER CYBER-
SICHERHEITS-
CHECK

Kapitel 9

Das Netz der Schatten

Die Sirenen der Notstromversorgung im Gewerbegebiet blieben stumm, doch das rote Blinken auf Marcs Monitoren war ohrenbetäubend genug.

„Er schlägt zurück!“, rief Marc, während seine Finger wie wild über die mechanische Tastatur flogen. „Er hat realisiert, dass der Honeypot eine Falle war. Er nutzt jetzt den bereits infizierten Zugang in Ninas Notariatskanzlei, um das gesamte Firmennetz mit einer Ransomware zu verschlüsseln!“

Thomas spürte, wie ihm die Kälte bis in die Fingerspitzen kroch. „Nina... sie ist mittendrin!“

Zeitgleich in der Notariatskanzlei Vogt & Partner.

Nina sass an ihrem Schreibtisch im zweiten Stock. Die Atmosphäre im Büro war seit dem Morgen angespannt gewesen. Vor knapp zwanzig Minuten hatte Ninas Kollegin aus der Buchhaltung eine E-Mail erhalten, die scheinbar direkt vom geschäftsführenden Partner der Kanzlei stammte. Der Betreff: Dringende Aktualisierung der Sicherheitszertifikate – Bitte umgehend bestätigen.

Die Mail sah täuschend echt aus. Ein Klick auf den Link hatte die Kollegin auf eine Anmeldeseite geführt, die exakt wie das Microsoft-365-Portal der Kanzlei aussah. Sie hatte ihre Zugangsdaten eingegeben, ohne auf die feine Abweichung in der Webadresse zu achten. Ein klassischer Fall von gezieltem Spear-Phishing. [Spear-Phishing]

Plötzlich fror Ninas Bildschirm ein. Das Dokument, an dem sie gerade arbeitete, verschwand.

Stattdessen färbte sich der gesamte Monitor flammend rot. Ein riesiges, schwarzes Totenkopf-Symbol erschien in der Mitte des Bildschirms, darunter ein herunterzählender Timer: 59:59... 59:58...

SÄMTLICHE DATEN WURDEN VERSCHLÜSSELT

Alle Kundendateien, Verträge und Notariatsakten sind blockiert.

Lösegeld-Forderung: 15 Bitcoin.

Hinweis an die Belegschaft:

Dieser Angriff wurde ermöglicht durch den internen Systemzugang von Nina Blaser.

In allen Büros der Kanzlei begannen die Bildschirme gleichzeitig rot aufzuleuchten. Schockierte Schreie hallten durch den Flur. Kolleginnen und Kollegen traten auf den Gang, die Blicke voller Entsetzen und Beschuldigung auf Ninas Bürotür gerichtet.

„Nein... das stimmt nicht!“, flüsterte Nina, während ihr die Tränen in die Augen stiegen.

Der Täter nutzte nicht nur die Daten, die er über die Buchhaltungs-Mail erbeutet hatte – er schob den Schaden gezielt Nina in die Schuhe, um ihre Existenz und ihren Ruf vollkommen zu vernichten.

In diesem Moment knallte die Eingangstür des Büros auf.

Thomas stürzte herein, völlig aus der Puste, den blinden Fleck der digitalen Überwachung nutzend. Er sah Ninas rotes Display, sah die feindseligen Blicke der Kollegen im Flur und stürmte direkt zum Serverraum am Ende des Ganges.

„Thomas! Was machst du hier?“, rief Nina und rannte ihm nach.

„Keine Zeit!“, brüllte Thomas. Er riss die unverriegelte Tür des Serverraums auf, griff nach den dicken, blauen Haupt-Netzwerkkabeln an den zentralen Switches und riss sie mit aller Gewalt heraus.

Klack. Klack. Klack.

Die Lichter an den Server-Racks erloschen nicht, aber die Datenverbindung nach draussen war schlagartig unterbrochen. Der Verschlüsselungsprozess stockte. Thomas hatte die Ausbreitung der Ransomware im letzten Moment gestoppt, bevor die Sicherungs-Backups der Kanzlei überschrieben werden konnten.

Er drehte sich zu Nina um, während der Schweiß ihm von der Stirn tropfte.

„Wir wissen, wo er ist“, flüsterte Thomas, die Kabel noch immer in den Händen. „Marc hat seine echte Adresse geknackt. Er sitzt im Industriegebiet Ost. Halle 12.“

Spear-Phishing (Gezielte Phishing-Mails)

Was im Buch passiert: Eine Kanzlei-Mitarbeiterin erhält eine gefälschte E-Mail der Geschäftsleitung und gibt ihre Zugangsdaten auf einer nachgebauten Login-Seite ein.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Sehr hoch (Die Ursache für über 80 % aller erfolgreichen Cyber-Angriffe auf Firmen und Privatpersonen.)

Gefahrenpotenzial: Extrem hoch (Führt oft zum kompletten Befall mit Erpressungs-Software / Ransomware.)

So schützen Sie sich: Absender genau prüfen: Blicken Sie auf die tatsächliche E-Mail-Adresse hinter dem Namen (nach dem @-Zeichen). Keine spontanen Logins über Links: Rufen Sie Firmenportale oder Dienste immer direkt über Ihre abgespeicherten Lesezeichen auf.

Kapitel 10

Die unmaskierte Fratze

Der Regen hatte wieder eingesetzt, als Thomas und Nina den Kanzleikomplex durch den Hinterausgang verliessen. Sie nutzten keine Taxis über Apps und mieden die Hauptstrassen mit den automatischen Kennzeichen-Kameras. Sie bewegten sich wie Phantome durch das graue Industriegebiet Ost.

Vor ihnen ragte die Halle 12 auf. Ein verwitterter Flachbau aus Wellblech und rostigen Stahlträgern, umgeben von einem überwucherten Maschendrahtzaun. Keine Leuchtreklame, keine Schilder. Nur das leise, monotone Summen eines grossen Kühlaggregats an der Seitenwand verriet, dass im Inneren Unmengen an Elektronik liefen.

Thomas winkte Nina hinter einen Stapel alter Holzpaletten zurück. Er zog eine analoge Kompaktkamera aus der Tasche, die Marc ihm mitgegeben hatte. Kein WLAN, kein GPS, kein Bluetooth. Nur ein optischer Linsenverschluss und ein Film.

Er schlich an den Maschendrahtzaun heran, suchte eine Lücke im Blickfeld der unbemann-ten Aussenkameras und blickte durch das schmutzige Fenster im Hochparterre.

Im Inneren der Halle leuchteten Dutzende Bildschirme. Auf zwei Tischen stapelten sich Server-Racks, Kabelstränge zogen sich wie dickflüssige Adern über den Betonboden. An der Wand hingen ausgedruckte Fotos – Fotos von Thomas, von Nina, von ihren Kindern Leo und der kleinen Tochter. Rotstift-Markierungen verbanden die Bilder mit Stammbäumen, Arbeitsplätzen und Bankdaten.

Es war die Kommandozentrale eines besessenen Stalkers.

Ein Schatten bewegte sich im Raum.

Thomas hob die Kamera, legte das Auge an den Sucher und drehte am Zoomring. Der Fokus stellte scharf.

Der Mann drinnen wandte sich vom Hauptmonitor ab, nahm ein Headset ab und griff nach

einer Kaffeetasse. Das grelle Licht eines Monitors erhellte sein Profil.

Thomas fror das Blut in den Adern. Seine Hand begann so heftig zu zittern, dass das Kameragehäuse gegen die Zaunmaschen schlug.

Es war kein anonymmer Profi-Hacker aus dem Darknet. Es war kein Fremder.

Es war Julian.

Julian – Thomas' bester Freund seit Schultagen. Der Mann, der auf ihrer Hochzeit der Trauzeuge gewesen war. Der Mann, der vor zwei Wochen noch beim Grillen in ihrem Garten gesessen und gelacht hatte. Der Mann, dem Thomas die Schlüssel zum Haus anvertraut hatte, wenn sie in den Urlaub fuhren.

Plötzlich ergab alles einen schrecklichen Sinn: Der Zugang zum Dachboden, das genaue Wissen über ihre Tagesabläufe, die Leichtigkeit, mit der er die ersten Zugänge gelegt hatte. Julian benötigte keine komplizierten Hacking-Tools für den Erstkontakt – er hatte schlicht das absolute Vertrauen der Familie ausgenutzt. **[Insider-Bedrohungen & Social Engineering]**

Thomas' Herz hämmerte wie verrückt. Warum?

In diesem Moment knackte es hinter ihm im Gebüsch.

Bevor Thomas herumwirbeln konnte, legte sich eine schwere Hand von hinten auf seine Schulter. Eine metallische Mündung drückte sich hart in seinen Rücken.

„Du warst schon immer zu neugierig, Thomas“, flüsterte eine Stimme dicht an seinem Ohr.

**DER CYBER-
SICHERHEITS-
CHECK**

Insider-Bedrohungen & Social Engineering

Was im Buch passiert: Der Täter war Thomas' bester Freund, der jahrelanges Vertrauen ausnutzte und Alt-Passwörter kannte.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Hoch (Oft unterschätzt: Racheakte von Ex-Partnern, ehemaligen Mitarbeitern oder Bekannten mit Alt-Zugängen.)

Gefahrenpotenzial: Extrem hoch (Täter kennt die persönlichen Schwachstellen genau.)

So schützen Sie sich: Keine Passwort-Wiederverwendung: Nutzen Sie niemals dasselbe Passwort für mehrere Dienste. Zugänge entziehen: Ändern Sie Passwörter konsequent, wenn sich Lebensumstände oder Beziehungen verändern.

Das Motiv der Rache

Die Mündung des Revolvers drückte unerbittlich zwischen Thomas' Schulterblätter.

„Keine plötzlichen Bewegungen, Thomas. Geh rein. Langsam.“, flüsterte die Stimme hinter ihm.

Thomas wurde durch den Nebeneingang in die Halle gestossen. Die schwere Stahltür fiel hinter ihm mit einem satten Klacken ins Schloss. Der Geruch von Ozon, erhitzten Platinen und kaltem Rauch lag in der Luft.

Drinne drehte sich der Mann am Hauptpult langsam um.

Es war Julian.

Er trug ein schlichtes, schwarzes Hemd, die Ärmel hochgekrempelt. Kein Irrer mit wirrem Blick, sondern der Mann, mit dem Thomas noch vor zwei Wochen beim Grillen über die Bundesligaergebnisse diskutiert hatte. Genau diese alltägliche Normalität machte den Anblick so verstörend.

„Julian...“, brachte Thomas heraus. Seine Stimme war kaum mehr als ein Krächzen. „Warum? Was zum Teufel tust du hier?“

Julian legte den Kopf schief. Ein dünnes, freudloses Lächeln erschien auf seinen Lippen.

„Warum?“, wiederholte Julian leise. Er trat hinter dem Pult hervor und schob die Hände in die Hosentaschen. „Die Frage ist falsch, Thomas. Du solltest dich fragen, wie du so blind sein konntest. Jahrelang.“

Er deutete mit einer Handbewegung auf die Wand voller Fotos und Datenströme.

„Du hast alles, Thomas. Die perfekte Familie, das schöne Haus, den Job, die Anerkennung. Und weisst du, wie du das bekommen hast? Auf meinem Rücken. Als wir damals die Firma gegründet haben, warst du das Gesicht. Der nette Thomas, den alle mochten. Ich war der Nerd im Keller, der die Arbeit gemacht hat. Und als es schiefging, hast du mich fallen gelassen wie eine heisse Kartoffel. Du hast dich sauber gewaschen, während ich ruiniert war.“

„Das stimmt doch nicht!“, rief Thomas. „Wir haben uns einvernehmlich getrennt! Du wolltest die Anteile ausbezahlt haben!“

„Weil du mich dazu gedrängt hast!“, schnauzte Julian, und zum ersten Mal blitzte der krankhafte Wahnsinn in seinen Augen auf. „Aber du hast vergessen, dass ich derjenige war, der eure Systeme aufgebaut hat. Ich kenne deine Passwörter, seit du 2012 dein erstes Online-Konto eröffnet hast. Du nutzt überall dieselben Schemata. Ein bisschen Social Engineering, ein paar Zeilen Code – du hast es mir lächerlich einfach gemacht.“ [Die Psychologie schwacher Passwörter]

Julian trat an einen der Bildschirme und tippte eine kurze Befehlskette ein.

„Ich wollte dir nicht einfach nur Geld stehlen, Thomas. Ich wollte dir dein Leben wegnehmen. Schritt für Schritt. Dich isolieren. Deine Frau, deine Kinder, deinen Ruf. Ich wollte, dass du spürst, wie es ist, wenn die Welt dich für ein Monster hält und du zusehen musst, wie alles verbrennt.“

Thomas schluckte schwer. Er hielt den Blick fest auf Julian gerichtet. Er wusste, dass er Zeit

gewinnen musste. Jede Sekunde, die Julian redete, war eine Sekunde, in der Nina da draussen reagieren konnte.

„Und der QR-Code am Parkscheinautomaten?“, fragte Thomas leise.

Julian lachte auf. „Ein reiner Katalysator. Ein kleiner Schubser, um den Prozess zu beschleunigen. Du hast nicht einmal geschaut, ob die Domain echt war. Ein Laye bleibt eben ein Laye, Thomas. Egal wie smart dein Haus ist.“

Plötzlich flackerte einer der Überwachungsmonitore an der Wand. Das Bild der Aussenkamera an der Nordseite der Halle zeigte eine dunkle Gestalt, die sich am Aussenverteilerkasten zu schaffen machte.

Julian erstarrte. Sein Lächeln schwand schlagartig.

Er riss die Waffe hoch und zielte direkt auf Thomas' Brust.

„Deine Frau“, knurrte Julian mit eiskalter Stimme. „Sie lernt es einfach nicht.“

DER CYBER-
SICHERHEITS-
CHECK

Die Psychologie schwacher Passwörter

Was im Buch passiert: Der Täter errät Thomas' Zugänge, weil dieser logische Abwandlungen alter Passwörter nutzt.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Extrem hoch (Der mit Abstand häufigste Nutzerfehler im Internet.)

Gefahrenpotenzial: Extrem hoch (Ein einziges Datenleck gefährdet alle anderen Konten.)

So schützen Sie sich: Nutzen Sie einen Passwort-Manager (z. B. Bitwarden, 1Password, KeePass). Dieser erstellt für jeden Dienst ein einzigartiges, zufälliges Passwort aus 20+ Zeichen.

Kapitel 12

Der physische Overkill

Julians Finger spannte sich am Abzug. Die Mündung des Revolvers ruhte unabänderlich auf Thomas' Brust.

„Sie hätte draussen bleiben sollen, Thomas. Jetzt muss sie zusehen, wie es endet.“

KLACK.

Ein dumpfer, metallischer Knall erschütterte die Aussenwand der Halle. Im selben Augenblick erlosch das grelle Licht der Leuchtstoffröhren. Das Summen der Kühlaggregate startete ab, die Dutzenden Monitore an den Wänden schossen in schwarze Finsternis.

Nina hatte am Aussenverteiler mit dem Brecheisen den Hauptsicherungshebel herumgerissen. Die Stromzufuhr der Halle war schlagartig gekappt.

Die Dunkelheit war absolut.

Thomas zögerte keine Zehntelsekunde. Er nutzte die plötzliche Blindheit des Täters, warf sich nach vorne und rammte Julian mit voller Wucht im Hüftbereich.

Beide Männer krachten zu Boden. Der Revolver schlug scheppernd auf den nackten Beton und rollte in die Finsternis. Julian fluchte, traf Thomas mit einem blinden Ellbogenstoss an der Schläfe, doch Thomas hielt ihn mit Verzweiflung am Kragen fest.

Plötzlich erfasste ein rotes Scheinwerferlicht den Raum.

Ein hohes, schrill pfeifendes Warnsignal ertönte. Entlang der Decke sprang die Notbeleuchtung an, und in den Server-Racks flammten grüne Status-LEDs wieder auf.

Julian lachte keuchend, während er Thomas von sich abstieß. „Glaubst du wirklich, ich bin so unvorbereitet? Meine Server laufen auf einer unterbrechungsfreien Stromversorgung. Eine industrielle USV – batteriegepuffert für zwanzig Minuten!“ **[USV-Systeme & Redundanz]**

Julian rappelte sich mühsam auf und hechtete nicht nach der Waffe, sondern zurück zum Hauptpult.

Auf seinem zentralen Monitor lief eine neongelbe Befehlszeile ab. Ein mechanischer Countdown war eingesprungen: 04:59 ... 04:58 ...

„Das ist mein Dead-Man-Switch“, keuchte Julian, während er sich das Blut von der Lippe wischte. „Ein digitaler Totmannschalter. Sobald die Hauptstromzufuhr unterbrochen wird, startet das Zerstörungsskript. Wenn ich mich nicht innerhalb von fünf Minuten mit meinem Biometrie-Schlüssel verifiziere, geht dein gehacktes Archiv an die Staatsanwaltschaft, an die Medien und an die Kontakte deiner Frau.“ **[#18: Dead-Man-Switches]**

In diesem Moment brach Nina durch die Seitentür der Halle. In der Hand hielt sie das schwere, verbogene Brecheisen.

„Thomas!“, schrie sie.

Julian griff mit zitternden Fingern in seine Hosentasche, zog einen kleinen, blauen USB-Sicherheits-Token – einen YubiKey – heraus und wollte ihn in die Konsole stecken, um den Countdown manuell abzublasen und die Daten freizugeben.

Doch seine Finger waren feucht von Schweiß. Der kleine Plastik-Schlüssel entglitt ihm und fiel exakt durch das schmale Lüftungsgitter unterhalb des Server-Racks.

Der Countdown tickte unbarmherzig weiter: 04:12 ... 04:11 ...

Julian starrte auf das Gitter. Panik trat in seine Augen. Er hatte sich in seiner eigenen digitalen Falle verfangen.

USV & Automatisierte Erpressung (Dead-Man-Switches)

Was im Buch passiert: Das Rechenzentrum des Täters läuft über Batterien weiter, und ein automatisierter Countdown droht Daten zu veröffentlichen.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Gering (Kommt vor allem bei professionellen Kriminellen und Ransomware-Banden vor.)

Gefahrenpotenzial: Extrem hoch (Setzt Opfer unter extremen Zeitdruck.)

So schützen Sie sich: Bewahren Sie bei Erpressungen Ruhe, trennen Sie betroffene Geräte sofort vom Netz und informieren Sie unverzüglich die Spezialisten der Polizei (Cybercrime-Dienststelle).

Kapitel 13

Wettlauf gegen die Zeit

03:45 ... 03:44 ...

Der rote Schein der Notbeleuchtung tauchte das Gesicht von Julian in ein fratzengleiches Profil. Er lag auf dem Bauch, drückte sein Gesicht auf den Betonboden und versuchte verzweifelt, mit den Fingern durch die engen Schlitze des Lüftungsgitters zu greifen.

„Nein! Nein! Scheisse!“, brüllte Julian. Der kleine blaue Hardware-Token lag unerreichbar auf dem tiefen Wannenboden unter dem Server-Rack.

„Schluss jetzt, Julian!“, rief Nina und trat mit erhobenem Brecheisen vor ihn. Julian hob abwehrend die Hände, die Augen weit aufgerissen vor Angst.

Thomas stürzte zum Hauptpult. Der gelbe Schriftzug brannte sich in seine Netzhaut ein:

CRITICAL AUTOMATION: EXFILTRATION IN PROGRESS

Verbleibende Zeit bis zur vollständigen Datenfreigabe: 02:15... 02:14...

„Marc! Bist du da?!“, brüllte Thomas in das kleine, analoge Walkie-Talkie, das er aus der Werkstatt mitgenommen hatte.

Das Funkgerät knackte lautstark. „Thomas! Ich höre dich! Was ist da los? Das Signal der Halle ist tot, aber die Skripte laufen auf dem externen Host!“

„Julian hat einen Dead-Man-Switch aktiviert! Der Hardware-Schlüssel liegt unerreichbar im Gehäuse! Wie stoppe ich das Skript ohne den Token?!“

„Verdammt!“, fluchte Marc durch das Rauschen. „Wenn es ein FIDO2-Hardware-Token ist, braucht die Konsole ein physisches Unterbrechungssignal! Du musst den Master-Reset-Schalter an der Rückseite der USV überbrücken – direkt an der Notfall-Konsole! Schneid das gelbe Steuerkabel durch!“ **[Hardware-Sicherheitsschlüssel]**

00:48 ... 00:47 ...

Thomas riss die Verkleidung an der Rückseite des Hauptservers ab. Dutzende bunte Kabel verliefen wirr in den Kabelkanälen.

„Welches gelbe Kabel?!“, schrie Thomas. „Hier sind fünf gelbe Kabel!“

„Thomas...“, flüsterte Nina, die auf die Zeitanzeige starrte. 00:22 ... 00:21 ...

Julian lachte am Boden plötzlich irre auf. „Es ist vorbei, Thomas. Wenn du das falsche Kabel durchschneidest, löst der Stromimpuls die sofortige Übertragung aus!“

Thomas blendete Julians Lachen komplett aus. Er atmete tief ein. Fokussieren. Nicht digital denken, sondern logisch.

Er folgte der Verlegung des Kabels nicht mit den Augen, sondern mit den Fingern. Vier der gelben Kabel führten zu den Festplatten-Adaptern. Nur ein einzelnes, etwas dickeres Kabel verlief direkt von der Notstrom-Platine zur Steuereinheit des Interfaces.

00:05 ... 00:04 ...

Thomas griff nach dem Brecheisen in Ninas Hand, nutzte die scharfe Kante des Metallfuss und klemmte das einzelne Kabel dazwischen.

00:02 ...

Er riss das Kabel mit einem gewaltsamen Ruck durch.

00:01 ...

Ein Funke blitzte auf.

Ein dumpfer Ton drang aus den Lautsprechern. Dann erlosch die gelbe Warnanzeige. Der Monitor sprang um.

SYSTEM TERMINATED BY PHYSICAL OVERRIDE.

Sämtliche ausstehenden Datenübertragungen abgebrochen.

Stille legte sich über die Halle. Nur das schwere Atmen von Thomas und Nina war noch zu hören.

DER CYBER-
SICHERHEITS-
CHECK

Fehlende Hardware-Sicherheitsschlüssel (Passkeys)

Was im Buch passiert: Thomas stellt sein digitales Leben auf physische Hardware-Schlüssel um, um künftige Angriffe abzuwehren.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Sehr hoch (die Lücke) (Die meisten Nutzer verlassen sich weiterhin auf reine Passwörter oder unsichere SMS-Codes.)

Gefahrenpotenzial: Sehr hoch (Reine Passwörter können jederzeit abgefangen oder erbeutet werden.)

So schützen Sie sich: Nutzen Sie Passkeys oder USB-Sicherheitsschlüssel (wie YubiKeys). Diese Anmeldemethode ist technisch immun gegen klassisches Phishing.

Das saubere Netz

Draussen zerschnitt das bläuliche Blitzlicht von einem Dutzend Einsatzfahrzeugen die regennasse Nacht.

Die schweren Eisentüren der Halle wurden aufgerissen. Beamte einer Spezialeinheit stürmten mit gezogenen Waffen und Taschenlampen herein. Marc hatte der Polizei über seinen eigenen gesicherten Notfallkanal die exakten Standortdaten und die Beweise übergeben.

Julian wurde in Handschellen abgeführt. Als er an Thomas vorbeigeführt wurde, blickte er stumm auf den Betonboden. Kein Hohn mehr, keine Überheblichkeit – nur die gebrochene Hülle eines Mannes, der sich in seinem eigenen digitalen Rachewahn verloren hatte.

Die Beamten der IT-Forensik sicherten sogleich die Server-Racks, die gefälschten Festplatten und die aufgetauchten Dokumente.

„Herr Blaser“, sagte der Einsatzleiter der Kriminalpolizei, während er sein Notizbuch schloss. „Wir haben die Datenströme gestoppt. Ihre Identität ist entlastet. Die gefälschten Erpresserschreiben an die Banken und Behörden wurden offiziell als Cyber-Angriff eines Dritten eingestuft. Sie und Ihre Frau sind reingewaschen.“

Thomas zog Nina fest an sich. Ein tiefer, befreiender Seufzer entfuhr seiner Brust.

Drei Tage später.

Die Sonne schien warm in die Küche der Familie. Das Haus war ungewohnt still. Die alten Smart-Home-Komponenten lagen verpackt in Kartons im Flur – Thomas hatte beschlossen, die billigen Kameras und ungesicherten WLAN-Steckdosen komplett zu entsorgen.

Am Küchentisch sass Thomas vor einem fabrikneuen, jungfräulichen Laptop. Kein einziges Backup aus der alten Zeit wurde eingespielt, um keine tief sitzende Schadsoftware einzuschleppen.

Gemeinsam mit Marc ging er nun Schritt für Schritt durch das digitale Aufräumprotokoll:

Kompletter Identitäts-Reset: Alle bestehenden E-Mail-Konten und Online-Zugänge wurden neu aufgesetzt.

Einsatz eines Passwort-Managers: Statt wie früher ähnliche Passwörter wiederzuverwenden, generierte Thomas ab sofort für jeden einzelnen Dienst zufällige, 24-stellige Zeichenketten, die in einem lokal verschlüsselten Vault lagen.

Hardware-Schlüssel statt SMS: Sämtliche Zwei-Faktor-Authentifizierungen wurden von SMS auf FIDO2-Hardware-Sicherheitsschlüssel (Passkeys) umgestellt. Selbst wenn ein Angreifer künftig eine SIM-Karte kapern sollte, blieb der zweite Faktor physikalisch in Thomas' Hosentasche. **[Mangelnde Digitale Hygiene]**

Leo kam in die Küche, legte sein neues Smartphone auf den Tisch und sah seinen Vater an. „Papa? Können wir den Familien-Kalender wieder einschalten? Aber... diesmal sicher?“

Thomas lächelte seinen Sohn an. „Ja, Leo. Diesmal machen wir es richtig.“

Er griff nach seinem neuen Smartphone, um die erste saubere Anwendung einzurichten.

Da vibrierte das Gerät in seiner Hand. Eine neue SMS ging ein.

Der Absender war eine unbekannte Nummer. Der Inhalt bestand nur aus einem einzigen Satz:

Ihr habt die Halle gefunden. Aber nicht meine Cloud.

Thomas' Lächeln fror auf den Lippen ein.

DER CYBER-
SICHERHEITS-
CHECK

Mangelnde Digitale Hygiene

Was im Buch passiert: Thomas reinigt sein digitales Leben von Grund auf und richtet saubere Systeme ein.

Risiko-Analyse:

Auftretenswahrscheinlichkeit: Extrem hoch (Trifft auf den Grossteil aller Internetnutzer zu.)

Gefahrenpotenzial: Sehr hoch (Bietet Angreifern dauerhaft offene Schlupflöcher.)

Ihre Checkliste für maximale Sicherheit: Software-Updates aktivieren: Halten Sie Smartphone, PC und Router immer auf dem neuesten Stand. Zwei-Faktor-Authentifizierung (2FA) überall einschalten: Ein Passwort allein reicht nicht mehr aus. Regelmässige Offline-Backups: Sichern Sie wichtige Daten auf einer externen Festplatte, die nach der Sicherung vom PC getrennt wird.

Kapitel 15

Das neugeborene Profil (Epilog)

Thomas starrte auf das Display seines neuen Smartphones. Das Herz klopfte ihm kurz bis zum Hals, während die Zeile „Ihr habt die Halle gefunden. Aber nicht meine Cloud.“ vor seinen Augen verschwamm.

Nina, die gerade zwei Tassen Tee an den Tisch trug, bemerkte sein Erstarren sofort. „Thomas? Was ist los?“

Thomas wischte sich über das Gesicht, atmete tief durch und reichte ihr das Telefon.

Nina las die Nachricht. Doch statt in Panik zu geraten, trat ein ruhiges, fast mitleidiges Lächeln auf ihre Lippen. Sie tippte auf das Absenderprofil der SMS, klickte auf die Details und zeigte Thomas den oberen Bildschirmrand.

Dort leuchtete in grünem Text die Meldezeile des neuen, installierten Sicherheits-Filters:

Automatisierter Spam- & Phishing-Köder abgefangen.

Sende-Server blockiert (Botnet-Massenmail).

„Ein alter, automatisierter Bot“, sagte Nina leise und legte die Hand auf seine Schulter. „Ein vorgefertigtes Skript, das irgendwo auf einem ausländischen Server hängen geblieben ist und zeitverzögert rausging. Julian sitzt in Untersuchungshaft, Thomas. Das Netz ist sauber.“

Thomas sah seine Frau an, nickte langsam und spürte, wie sich die monatelange Anspan-

nung endgültig aus seinen Muskeln verabschiedete. Er löschte die Nachricht mit einer einzigen Daumenbewegung.

Das Leben der Familie hatte sich verändert. Sie waren keine Technikverweigerer geworden – das Smart Home lief wieder, aber diesmal auf einem isolierten, vom Internet getrennten Gast-Netzwerk. Sämtliche Konten waren mit Hardware-Tokens gesichert, und auf den Smartphones liefen aktuelle Betriebssysteme ohne unbewilligte Schattenprofile.

Sie hatten nicht auf Komfort verzichtet, sondern die Kontrolle zurückgewonnen.

Zwei Wochen später.

Ein sonniger Dienstagmittag. Thomas stand auf dem Parkplatz vor der Notariatskanzlei, um Nina nach Feierabend abzuholen. Er genoss die warme Sonne im Gesicht und das leise Rauschen der Stadt.

Ein junger Mann mit einer Umhängetasche und einer Warnweste spazierte an ihm vorbei. Er steuerte auf die Ladesäule für Elektrofahrzeuge am Rande des Parkplatzes zu.

Der Mann wischte kurz über das Metall der Säule, zog ein kleines, schwarz-weisses Quadrat aus der Tasche und streifte die Schutzfolie von der Klebefläche ab. Er setzte an, den frischen Sticker präzise über den gedruckten QR-Code der Ladesäule zu kleben.

Thomas beobachtete die Szene aus zehn Metern Entfernung. Er spürte keinen Schrecken mehr. Nur eine kühle, wache Aufmerksamkeit.

Er griff in die Tasche seiner Jacke, zog sein Smartphone heraus und steuerte langsam auf den Mann zu.

„Schöner Tag zum Laden“, sagte Thomas mit ruhiger, fester Stimme.

Der Mann in der Warnweste zuckte zusammen, liess den Sticker fallen und blickte Thomas mit aufgerissenen Augen an.

Thomas blickte auf das kleine Quadrat am Boden, schaute dem Mann direkt in die Augen und lächelte dünn.

„Aber die Adresse auf dem Code... die kenne ich bereits.“

Über den Autor



Stefan Kammermann

Techniker & Sicherheitsspezialist, DM Informatik

Stefan Kammermann betreut seit vielen Jahren IT-Arbeitsplätze und unterstützt Privatpersonen bei Fragen rund um Computer, Internet und digitale Sicherheit. Er kennt die typischen Risiken im Alltag und zeigt einfache und verständliche Lösungen auf.

Copyright © 2026 Stefan Kammermann

Alle Rechte vorbehalten.

Herausgeber: D. M. Electronics AG

