Isolation schlägt Detektion

Warum sensible Webportale einen eigenen Browser brauchen



CORONIC GmbH, Kiel

1 Zusammenfassung

Wer ein Webportal mit sensiblen Daten betreibt, hat ein Problem, das der Betreiber mit den technischen Mitteln des Portals nicht lösen kann: Der Computer, an dem der Nutzer arbeitet, gehört dem Betreiber nicht. Niemand administriert diesen Computer, niemand kennt seinen Zustand, und niemand weiß, was dort neben dem Portal noch läuft: veraltete Programme mit bekannten Lücken, ein Trojaner aus einem Mail-Anhang, ein Datendieb, der auf die nächste Anmeldung wartet. Der Nutzer surft auf demselben Computer privat, öffnet privat Anhänge, installiert privat Software. Für die Fehler der Nutzer nehmen die Gerichte trotzdem zunehmend den Betreiber des Portals in die Pflicht: Das Landgericht Berlin II hat im April 2026 eine Bank verurteilt, einem Phishing-Opfer über 200.000 Euro zu erstatten, weil sie hätte merken können, dass sich Kunde und Täter zur selben Zeit über völlig verschiedene Netzzugänge anmeldeten.[1]

Der übliche Weg für mehr Sicherheit heißt nach wie vor suchen, suchen, suchen. Schutzprogramme suchen Schadsoftware, suchen Auffälligkeiten, suchen Signaturen und aktualisieren ihre Virendateien. Der Fachbegriff dafür ist Detektion, und die Grenze liegt im Verfahren selbst, nicht in der Qualität der Produkte. Suchen heißt vergleichen, und ein Schutzprogramm vergleicht nur mit dem, was es schon kennt. Den jeweils allerneuesten Angriff kennt das Schutzprogramm nicht. Wer sucht, muss jedes Mal richtig liegen. Wer angreift, muss nur einmal zufällig richtig liegen.

Der einfachere Weg zur Sicherheit heißt Isolation. Isolation arbeitet wie der Airbag: kein Erkennen der Gefahr, kein rechtzeitiges Bremsen, kein Reißen am Lenkrad. Der Airbag tut gar nichts, bis es schiefgeht. Dann fängt der Airbag den Aufprall ab. Die Browser-Sitzung läuft ausgesperrt vom übrigen Computer. Was auf dem Computer liegt, kommt nicht in die Browser-Sitzung hinein. Was in der Browser-Sitzung passiert, kommt nicht hinaus. So einfach kann die Lösung sein.

Isolation ruht auf zwei Säulen. Die erste Säule ist die Härtung: Der Browser sperrt den PC aus, auf dem er selber läuft, und wehrt damit genau die Techniken ab, mit denen sich Schadsoftware typischerweise in ein laufendes Programm einklinkt. Die zweite Säule ist die Hardware-Isolation: Der Browser sperrt das Internet aus. Die Browser-Sitzung läuft in einer eigenen, wegwerfbaren virtuellen Maschine unterhalb des Betriebssystems, und die Trennung setzt der Prozessor selbst durch. Die Härtung ist bei Bank-Browsern seit Jahren etabliert, die Hardware-Isolation ist eine neue Entwicklung. Beide Säulen ersetzen Bremse und Assistenzsysteme nicht. Beide Säulen stehen dahinter und greifen, wenn die klassischen Sicherheitssysteme bereits versagt haben.

Die Banken sind mit dieser Lage seit über zwanzig Jahren vertraut. Banken betreiben seit den frühen Zweitausendern ein hochsensibles Webportal, auf das die Kunden mit privaten Computern zugreifen, die von der Bank nicht kontrolliert werden. Man nennt das Ganze Online-Banking. Die Banken haben dabei jede Stufe der Auseinandersetzung mit den Angreifern schon durchlaufen: erst aufklären, dann suchen, dann die Authentifizierung verstärken. Heute stehen Behördenportale, Kirchenportale und die Kundenportale von Versorgern und Versicherern an derselben Stelle wie die Banken vor zwanzig Jahren. Was die Banken gelernt haben, ist für andere Betreiber ein Blick in die eigene Zukunft.

[1] LG Berlin II, Urteil vom 22.04.2026, Az. 38 O 293/25: https://www.heise.de/news/Urteil-gegen-die-Apobank-Finanzinstitut-haftet-fuer-Phishing-Schaden-11288231.html

Die jüngste dieser Stufen verschärft die Lage noch einmal. Das europäische Zahlungsrecht verlangt von den Banken eine starke Kundenauthentifizierung. Der Nutzer weist sich mit zwei Faktoren aus drei Kategorien aus: Wissen, Besitz und Biometrie. Für den reinen Blick aufs Konto lässt das Recht der Bank viel Spielraum, aber viele Banken verzichten nach den ersten Urteilen freiwillig darauf und verlangen bei jedem Zugang zum Portal eine starke Kunden-Authentifizierung (SCA)[2]. Das ist sicherheitstechnisch richtig, aber für den Nutzer am PC ist es extrem lästig. Er muss bei jedem Schritt das Handy in die Hand nehmen und sich neben der Anmeldung am PC noch einmal mobil authentifizieren. Ein spezialisierter Bank-Browser mit eigener Hardwarebindung liefert die SCA-Nachweise vollautomatisch beim Start des Programms und ohne zweites Gerät. Der Betreiber gewinnt dabei mehr als der Nutzer: Der Betreiber sieht dann nicht nur, dass sich jemand mit gültigen Authentifizierungsdaten anmeldet, sondern auch, mit welchem Client. Und der Angreifer, der die abgefischten Daten in seiner eigenen Sitzung benutzt, scheitert am unbekannten Client.

2 Das Grundproblem

Ein Portal ist dazu da, benutzt zu werden. Der Nutzer meldet sich an, lädt Dokumente hoch, ruft Auskünfte ab, gibt Daten ein. Der Nutzer tut das auf einem Computer, auf dem er auch privat surft, privat Anhänge öffnet und privat Software installiert. Genau darin liegt das Problem. Das Portal ist nur vermeintlich sicher, denn der Computer des Nutzers ist möglicherweise bereits kompromittiert.

Die Angreifer wissen das. Die Angreifer greifen deshalb nicht das Portal an, sondern die Browser-Sitzung des Nutzers. Der Angreifer klinkt sich in den Browser ein, übernimmt Sitzungsdaten und Zertifikate und benutzt den Browser des Nutzers als Sprungbrett. Der Angreifer wartet, bis der Nutzer sich angemeldet hat, und arbeitet in dessen Namen illegal weiter, auch an einer Zwei-Faktor-Authentifizierung vorbei.[3] Der Betreiber sieht in seinen Protokollen einen ordnungsgemäß angemeldeten Nutzer, der ordnungsgemäße Aktionen ausführt. Aus Sicht des Portals ist alles in Ordnung. Aus Sicht des Nutzers ist es das nicht, denn ihm werden gerade Geld, Daten oder noch wertvollere Informationen gestohlen. Dieser Weg lohnt sich. Die europäische Bankenaufsicht und die Europäische Zentralbank zählen für 2024 europaweit 4,2 Milliarden Euro Zahlungsbetrug, über 15 Prozent mehr als im Jahr davor. Bei Überweisungen entfällt über die Hälfte des Schadens nicht auf eine gebrochene Anmeldung, sondern darauf, dass der Nutzer selbst zur Freigabe gebracht wurde.[4] Der Angreifer bricht die Authentifizierung nicht mehr auf. Der Angreifer benutzt sie mit.

Das geschieht auf zwei Wegen, und die zwei Wege verlangen zwei verschiedene Antworten. Auf dem ersten Weg sitzt der Angreifer im Computer des Nutzers und arbeitet in dessen eigener, angemeldeter Browser-Sitzung mit. Auf dem zweiten Weg sitzt der Angreifer an seinem eigenen Computer, fischt die Zugangsdaten ab, öffnet damit eine zweite Sitzung parallel zur echten und lässt sich die Freigabe vom Nutzer liefern. Dieses zweite Muster lag dem Berliner

[2] SCA Strong Customer Authentication, starke Kundenauthentifizierung. Der Nutzer weist sich mit zwei Faktoren aus drei Kategorien aus: Wissen, Besitz, Biometrie.
[3] MITRE ATT&CK, Technik T1185: https://attack.mitre.org/techniques/T1185/
[4] EBA und EZB, 2025 Report on Payment Fraud: https://www.eba.europa.eu/sites/default/files/2025-12/1709846a-84d9-47cf-86a0-b155efb34d66/EBA%20and%20ECB%20Report%20on%20Payment%20Fraud.pdf

Urteil zugrunde. Gegen den ersten Weg helfen Härtung und Isolation. Gegen den zweiten hilft ein Browser, der sich gegenüber dem Portal zertifizieren kann.

Ehrlicherweise gibt es noch einen dritten Weg, und der ist so alt wie das Geld selbst: Der Angreifer ruft an und bequatscht den Nutzer so lange, bis der sein Geld selbst überweist. Nutzer, Computer und Freigabe sind echt. Gegen Trickbetrug schützt keine Technik. Hier hilft nur bessere Aufklärung.

Diese Lage ist nicht neu, und diese Lage ist auch nicht ungewöhnlich. Sie ist der Normalfall überall dort, wo ein Betreiber ein Portal anbietet, aber die Geräte seiner Nutzer nicht kontrollieren kann: bei Ehrenamtlichen, die von zu Hause für ihre Kirchengemeinde oder für einen Wohlfahrtsverband arbeiten, bei Bürgern an einem Verwaltungsportal, bei Privatkunden im Online-Banking, bei Mitarbeitern auf dem privaten Notebook.

3 Die Banken sind uns voraus

Wer wissen will, wie sich diese Lage entwickeln wird, muss sie nicht schätzen. Er kann bei den Banken nachsehen. Die Banken haben als Erste zwei Dinge zusammengebracht, die schlecht zusammenpassen: ein Portal mit hohem Schadenspotenzial (Online-Banking) und ein Endgerät, das der Bank nicht gehört (privater Computer, BYOD[5]). Seit vielen Jahren läuft dort dieselbe Auseinandersetzung, und diese Auseinandersetzung ist gut dokumentiert, weil viel Geld im Spiel ist und weil jeder Schaden gezählt wird.

Die Stationen sind immer die gleichen. Zuerst klärt die Bank auf: Der Nutzer soll aufmerksamer werden. Dann sucht die Bank: Software auf dem Endgerät und Regeln im Portal sollen den Angriff bemerken. Dann verstärkt die Bank die Authentifizierung: aus einem Faktor mit Benutzername und PIN werden zwei, aus zwei werden drei, plus Gerätebindung oder plus Biometrie. Und am Ende steht die Frage, die alle anderen Wege übrig lassen: Was tun wir, wenn der Computer des Nutzers selbst nicht vertrauenswürdig ist?

CORONIC sieht Behördenportale, Kirchenportale und die Kundenportale von Versorgern, Versicherern und Kliniken auf demselben Weg wie die Banken, nur mit Verzögerung. Die Angriffe wandern dorthin, wo sich der Aufwand lohnt, und der Aufwand lohnt sich, sobald ein Portal genug wert ist. Das Problem Online-Banking zeigt damit, wie die nächsten zehn Jahre für die übrigen Betreiber laufen werden.

4 Warum Suchen immer hinterherläuft

Virenscanner, Mail-Filter und Systeme zur Angriffserkennung am Endgerät (Endpoint Detection and Response, EDR) arbeiten nach demselben Grundmuster. Sie vergleichen das Beobachtete mit Bekanntem: mit Signaturen, mit Mustern, mit Verhaltensregeln. Für die Masse der Angriffe funktioniert das, und darauf zu verzichten wäre unvernünftig. Die Stärke dieser Systeme liegt im Bekannten. Schwer tun sie sich mit unbekannten Schwachstellen (Zero-Days), mit frisch erzeugten Varianten desselben Schadprogramms und mit Angriffen, die sich unauffällig verhalten, bis sie ihr Ziel erreicht haben.

[5] BYOD Bring Your Own Device. Der Nutzer arbeitet mit seinem eigenen Gerät, das der Betreiber weder beschafft noch verwaltet und dessen Zustand er nicht kennt.

Auch die aufwendigeren Verfahren ändern dieses Grundmuster nicht. Detonations-Sandboxes öffnen Anhänge vollautomatisch in einer Prüfumgebung, bevor der Empfänger sie bekommt. Die besten davon beobachten dabei bis auf Prozessorebene, ob gerade eine Schwachstelle ausgenutzt wird. Das sind wirksame Werkzeuge, und sie gehören in jede gestaffelte Verteidigung. Aber sie alle beobachten und bewerten, und wer bewertet, lässt sich täuschen. Der Wettlauf bleibt derselbe, er wird nur auf höherem Niveau geführt.

Die Angreifer bauen ihre Werkzeuge gezielt so, dass die Werkzeuge durch diese Prüfung fallen. Der Angreifer erzeugt sein Programm bei jedem Abruf neu, damit es nie zweimal dieselbe Signatur hat. Der Angreifer lädt den schädlichen Teil erst nach, wenn die Prüfung vorbei ist. Und der Angreifer stellt die Arbeit ein, sobald er merkt, dass er gerade in einer Prüfumgebung läuft.[6]

Dafür gibt es ein Bild, das jeder kennt: Katze und Maus. Die Katze ist schnell, aufmerksam und oft erfolgreich. Und die Maus hat den Vorteil, dass sie sich aussuchen kann, wann sie versucht durchzukommen.



Aus „Suchen, suchen, suchen“ wird „Aussperren und Isolation“.

Die Konsequenz ist nicht, das Suchen abzuschaffen. Suchen fängt den größten Teil der alltäglichen Angriffe sicher ab, auf das Suchen zu verzichten wäre daher unvernünftig. Die Konsequenz ist, hinter das Suchen etwas zu stellen, das auch dann noch trägt, wenn das Suchen längst versagt hat.

5 Der Computer ist nicht sauber

Jede Sicherheitsarchitektur, die auf dem Endgerät aufsetzt, trifft stillschweigend eine Annahme: Der Computer des Nutzers ist dem Grunde nach sicher. Diese Annahme ist bequem, bei vielen Firmenrechnern im internen LAN mag sie zutreffend sein, aber bei privaten Geräten ist diese Annahme kaum zu halten.

Belastbare Zahlen über den Zustand privater Computer gibt es kaum, weil niemand sie flächendeckend messen kann. Was es gibt, weist in eine Richtung. Der Sicherheitsindex von Deutschland sicher im Netz steht 2025 mit 55,7 von 100 Punkten unverändert auf dem tiefsten Wert seit Beginn der Erhebung, während die erlebten Sicherheitsvorfälle mit 61,6 Punkten einen

[6] MITRE ATT&CK, Technik T1497: https://attack.mitre.org/techniques/T1497/

neuen Höchststand erreichen.[7] Erstmals liegt die Bedrohung der größten Nutzergruppe über ihrem eigenen Schutzniveau, und die Hälfte der Internetnutzer gilt der Studie als unzureichend geschützt. Das BSI zählt in seinem Cybersicherheitsmonitor 2026 jede zehnte Person als „im Vorjahr betroffen“[8], am häufigsten durch Betrug beim Onlineshopping, Fremdzugriffe auf Konten, Onlinebanking-Betrug und Phishing. Keine dieser Zahlen misst den Zustand eines einzelnen Computers. Zusammen genommen muss ein Betreiber den privaten Computer seiner Kunden aber als potenziell kompromittiert einschätzen.

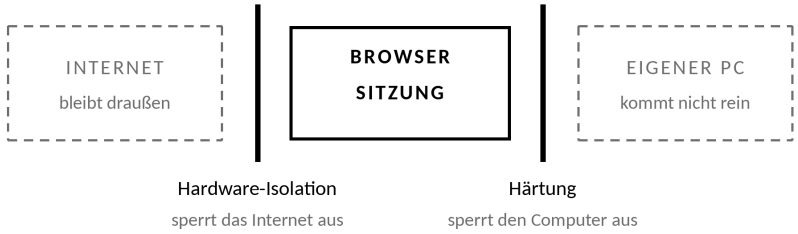
Wie ein übernommener Computer benutzt wird, zeigt die europäische Cybersicherheitsagentur ENISA in ihrem Threat Landscape 2025. Beim Schadcode, den Angreifer nach erfolgreichen Eindringversuchen nachgeladen haben, entfielen rund 87 Prozent auf Erpressungssoftware, Banking-Trojaner und Datendiebe.[9]

Der Datendieb ist dabei der unangenehmste Fall, weil der Datendieb die Anmeldung gar nicht angreift. Der Datendieb nimmt sich, was nach der Anmeldung zu sehen ist: die Daten aus der laufenden Browser-Sitzung. Wie stark der Nutzer sich authentifiziert hat, spielt für den Datendieb keine Rolle. Der Datendieb wartet einfach, bis die Anmelde-Arbeit getan ist und greift dann zu.

Die Betreiber eines Webportals stehen damit vor einer unangenehmen Aufgabe: Sie können das Portal beliebig gut absichern und haben den Teil der Strecke, auf dem der Schaden wahrscheinlich entsteht, trotzdem nicht in der eigenen Hand. Obendrein haftet der Portalbetreiber zunehmend für genau diesen privaten Teil der Strecke.

6 Zweimal aussperren

Isolation heißt, die Browser-Sitzung so zu führen, dass der Zustand des Computers für die Browser-Sitzung keine Rolle mehr spielt. Das gelingt in zwei Säulen, und die beiden Säulen tun Verschiedenes.



Die Hardware-Isolation sperrt das Internet aus, die Härtung den eigenen Computer.

6.1 Erste Säule: Härtung

Bei der Härtung sperrt der Browser den Computer aus, auf dem er selber läuft. Technisch ist das Laufzeitschutz im eigenen Prozess (RASP)[10]: Der Browser prüft beim Start und im Betrieb

[7] DsiN-Sicherheitsindex 2025: https://www.sicher-im-netz.de/dsin-sicherheitsindex-2025/
[8] BSI, Cybersicherheitsmonitor 2026: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Digitaler-Verbraucherschutz/Digitalbarometer/digitalbarometer_node.html
[9] ENISA Threat Landscape 2025: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
[10] RASP steht für Runtime Application Self-Protection: Schutzfunktionen, die im Programm selbst mitlaufen und Manipulationen zur Laufzeit erkennen, statt sie von außen zu suchen.

seine eigenen Programmdateien und den geladenen Code gegen Manipulation, überwacht die Einsprungpunkte der Systemfunktionen, die er benutzt, und erkennt, wenn ein fremder Prozess sich dort eingeklinkt hat.

Die Techniken, gegen die der Browser dabei arbeitet, sind bekannt und abzählbar: das Umbiegen von Systemaufrufen (API-Hooking), das Einschleusen fremder Bibliotheken in den laufenden Prozess (DLL-Injection), das Mitlesen der Tastatur unterhalb der Anwendung, das Auslesen des Prozessspeichers von außen und das Abfotografieren des Fensterinhalts. Die Daten der Browser-Sitzung hält der Browser verschlüsselt und ausschließlich im Arbeitsspeicher. Auf der Festplatte liegt kein Klartext, den ein Datendieb einsammeln könnte. Seine Schlüssel bindet der Browser an Merkmale des Computers, sodass eine kopierte Installation auf einem anderen Computer nicht arbeitet.

Die Härtung schützt nicht gegen alles, aber die Härtung schützt gegen das, was tatsächlich passiert: gegen Schadsoftware, die schon läuft und die Browser-Sitzung auslesen will. Die Härtung funktioniert auf handelsüblichen Computern, ohne besondere Ausstattung und ohne zusätzliche Administratorrechte, d. h. der Nutzer braucht dafür nichts zu tun und nichts zu kaufen. Bei Bank-Browsern ist die Browser-Härtung seit Jahren im Einsatz.[11]

6.2 Zweite Säule: Hardware-Isolation

Bei der Hardware-Isolation sperrt der Browser das Internet aus. Die Browser-Sitzung läuft nicht mehr im Betriebssystem des Nutzers, sondern in einer eigenen virtuellen Maschine, der Micro-VM. Diese Maschine verwaltet kein Programm des Betriebssystems, sondern eine schmale Schicht darunter, die auf den Virtualisierungsfunktionen des Prozessors aufsetzt. Unter Windows heißt der Unterbau dafür Hyper-V. Es ist eine Hardware-Virtualisierung und technisch kaum zu vergleichen mit den üblichen Browser-Sandboxes oder sonstigen Software-Virtualisierungen. Die Micro-VM startet immer neu, wenn die Browser-Sitzung beginnt, und wird stets verworfen, wenn die Browser-Sitzung endet. Was auf dem Computer liegt, erreicht die Micro-VM nicht, und was ein Angreifer in der Micro-VM anrichtet, verschwindet mit jedem Neustart.

Der Unterbau dafür ist ein Typ-1-Hypervisor, der direkt auf den Virtualisierungsfunktionen des Prozessors aufsetzt, etwa Intel VT-x oder AMD-V. Beim Start der Browser-Sitzung fährt kein vollständiges Betriebssystem hoch. Der Hypervisor klont eine Micro-VM aus einer vorbereiteten, schreibgeschützten Vorlage. Verfahren wie Copy-on-Write sorgen dafür, dass dieser Klon in Sekundenbruchteilen bereitsteht und zunächst kaum zusätzlichen Speicher belegt. Die Speichertrennung erzwingt der Prozessor selbst, über eine zweite Ebene der Adressübersetzung (Second Level Address Translation): Der Hypervisor konfiguriert die Grenzen, die CPU setzt sie durch.

Die Verbindung der Micro-VM zum Wirtssystem beschränkt sich auf wenige, klar definierte Kanäle: Bildausgabe, Tastatur und Maus sowie einen kontrollierten Übergabepunkt für Dateien und Zwischenablage. Diese Kanäle sind die kritischen Stellen des Entwurfs, denn jede Komfortfunktion, also gemeinsame Zwischenablage, Ordnerfreigabe oder direkter Gerätezugriff, vergrößert die Angriffsfläche wieder.

[11] BankInformation 09/2020, gehärtete Banking-Browser: https://www.coronic.de/wp-content/uploads/2020/10/Artikel-BankInformation-BVR-Onlinebanking-direkt.pdf

Der Unterschied zu allem, was im Betriebssystem selbst ansetzt, ist einfach zu benennen: wenn der Angreifer einmal drin ist, sitzt er selbst im Betriebssystem, also auf derselben Ebene wie die Software-basierte Abwehr. Bei der Hardware-Isolation sitzt der Angreifer eine Ebene darüber, und die Hardware-Grenze darunter kann der Angreifer nur schwer durchbrechen: Der Hypervisor bietet ihm kaum Angriffsfläche, denn seine Schnittstellen sind schmal und streng definiert, alles gut zu kontrollieren.

6.3 Was eine normale Browser-Sandbox nicht kann

Die Software-Sandbox des Browsers leistet das nicht. Jeder moderne Browser führt Webinhalte in eigenen, beschnittenen Prozessen aus, und das ist einer der wichtigsten Sicherheitsfortschritte der letzten fünfzehn Jahre. Die Grenze zieht dort aber das Betriebssystem. Sandbox und übrige Programme laufen im selben Betriebssystem. Ausbrüche aus Browser-Sandboxes werden regelmäßig vorgeführt und gehandelt. Die Micro-VM unterscheidet sich in beidem. Die Grenze erzwingt der Prozessor, und die Umgebung wird mitsamt allem weggeworfen, was sich darin eingenistet hat.

Der andere Weg wäre, die Browser-Sitzung ganz aus dem Haus zu geben. Bei der Cloud-Isolation läuft der Browser im Rechenzentrum eines Anbieters, zum Nutzer geht nur noch das Bild. Das wirkt, hat aber Folgen, die die Anbieter selbst dokumentieren: Hardware-Sicherheitsschlüssel und Passkeys arbeiten in bestimmten Betriebsarten nicht mehr, weil die Browser-Sitzung unter einer fremden Adresse ausgeliefert wird und damit die Domänenbindung bricht, auf der WebAuthn beruht. Kamera, Mikrofon und 3D-Grafik fallen aus, jede Eingabe kostet Laufzeit, und die Betrugserkennung des Portals sieht statt des Nutzers die Adressen des Isolationsanbieters.[12] Für einen Betreiber, der den Browser gerade als Ausweis benutzen will, ist das der falsche Weg: Das Portal sieht dann nicht mehr den Nutzer, sondern den Isolationsanbieter. Die Isolation muss lokal bleiben.

6.4 Warum beide Säulen nötig sind

Die Antwort ist unromantisch: weil die Hardware-Isolation Voraussetzungen hat und die Härtung nicht. Die Hardware-Isolation braucht einen Prozessor, der sie beherrscht, und ein Betriebssystem, das sie freigibt. Wo das fehlt, muss die Härtung allein tragen. Wo beides vorhanden ist, sitzt die Härtung innen und die Hardware-Isolation außen. Ein Angreifer müsste beide Säulen nacheinander überwinden. Das ist der ganze Gedanke: nicht besser suchen, sondern lieber zweimal richtig aussperren.

Beide Säulen setzen dasselbe voraus: einen eigenen Browser. Härten lässt sich nur eine Software, die man selbst baut, und echte Hardware-Isolation bekommt man in einen Standard-Browser nicht hinein. Wer diesen eigenen Browser aber einmal hat, bekommt das Dritte fast geschenkt: Eine eigene Software kann sich gegenüber dem Portal zertifizieren und die Faktoren der starken Kundenauthentifizierung gleich mitliefern. Die beiden Säulen wehren den Angreifer im Computer des Nutzers ab, und sie tragen die Antwort auf die parallele Sitzung des Angreifers huckepack mit sich.

[12] Cloudflare, Remote Browser Isolation, Known Limitations: https://developers.cloudflare.com/cloudflare-one/remote-browser-isolation/known-limitations/

7 Starke Kundenauthentifizierung ohne zweites Gerät

7.1 Was das Recht verlangt

Europäisches Recht schreibt für Zahlungsdienste eine starke Kundenauthentifizierung vor. Der Nutzer weist sich dabei mit zwei Faktoren aus drei Kategorien aus: etwas, das der Nutzer weiß (Wissen: PIN, Passwort), etwas, das der Nutzer hat (Besitz: Telefon, EC-Karte), und etwas, das der Nutzer selber ist (Inhärenz: Biometrie, Fingerabdruck, Gesicht). In der Praxis heißt das für die meisten Nutzer: Passwort am PC, Biometrie auf dem Smartphone.

Das Gesetz lässt dabei etwas Luft. Für den reinen Blick auf Kontostand und Umsätze muss der Nutzer die starke Anmeldung nicht jedes Mal durchlaufen. Eine Verordnung der Europäischen Kommission erlaubt einen Abstand von 180 Tagen zwischen zwei starken Anmeldungen.[13] Diese Ausnahme war der Grund, warum Online-Banking am PC die letzten Jahre einfach nutzbar war. Die komplexe zwei Faktor Anmeldung war für den Kontoblick nur jedes halbe Jahr verpflichtend, dazwischen konnte man sich ganz einfach mit Username und PIN anmelden.

7.2 Warum die Banken nachschärfen

Viele Banken rudern jedoch inzwischen zurück und verlangen bei jedem Loginprozess eine starke zwei Faktor Authentifizierung und der Grund liegt in der aktuellen Rechtsprechung. Das Landgericht Berlin II hat 2026 eine Bank verurteilt, einem Phishing-Opfer über 200.000 Euro zu erstatten.[14] Über die Entscheidung hinaus hielt das Gericht der Bank vor, die Bank habe die Verknüpfung eines neuen Geräts ohne hinreichende Besitzprüfung zugelassen, obwohl Einwahl und Geräteregistrierung über verschiedene Netzzugänge liefen.

Für die Banken ist die Botschaft eindeutig. Wenn der Kunde bei einer Täuschung nicht mehr grob fahrlässig handelt, bleibt der Schaden bei der Bank hängen. Wer haftet, sichert sich ab. Also verlangt die Bank ab sofort immer die starke Authentifizierung, auch dort, wo das Gesetz sie nicht explizit fordert. Den Preis dafür zahlt der Nutzer am PC: Er tippt seine Zugangsdaten ein und greift dann zusätzlich zum Smartphone, bei jedem Login und bei jedem Auftrag. Am Smartphone selbst fällt dieser Preis nicht an, weil dort das Gerät selbst der Besitzfaktor ist und die Biometrie gleich mitbringt.

7.3 Hardwarebindung im Browser

Ein Browser, der dem Betreiber gehört, bringt beide fehlenden Faktoren zusammen. Den Besitz liefert die Bindung an die PC-Hardware: Der Browser erzeugt bei der Einrichtung ein Schlüsselpaar, das an Merkmale genau seines Computers gebunden ist und sich auf einem anderen PC nicht verwenden lässt. Wo ein Sicherheitschip vorhanden und sauber eingebunden ist, legt der Browser den privaten Schlüssel dort ab, sodass er den Chip nie verlässt. Der Aufwand liegt nicht in diesem Normalfall, sondern in den anderen: auf Computern ohne brauchbaren Sicherheitschip oder auf älteren Systemen.

Die Biometrie liefert oft schon das Betriebssystem. Unter Windows koppelt der Browser den Zugriff auf den Schlüssel an Windows Hello und sein TPM, auf Macs mit Touch ID an den

[13] Delegierte Verordnung (EU) 2022/2360: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2360
[14] LG Berlin II, Urteil vom 22.04.2026, Az. 38 O 293/25: https://www.heise.de/news/Urteil-gegen-die-Apobank-Finanzinstitut-haftet-fuer-Phishing-Schaden-11288231.html

Fingerabdruck. Dort liegt der Schlüssel in der Secure Enclave. Der Nutzer startet sein Programm, mehr tut er nicht.

Prüfbar wird der Nachweis über WebAuthn, den Standard, über den ein Portal heute schon Sicherheitsschlüssel und Passkeys annimmt.[15] Das Portal schickt eine Zufallsaufgabe, der Browser signiert sie mit dem gerätegebundenen Schlüssel und vermerkt in der signierten Antwort, ob der Nutzer sich vorher am Gerät ausgewiesen hat. Wer WebAuthn bereits unterstützt, hat die Schnittstelle im Haus. Zu bauen bleiben die Registrierung des Browsers als bekannter Client und die Entscheidung, welche Nachweise das Portal anerkennt.

Die Europäische Bankenaufsichtsbehörde hat 2019 ausdrücklich festgestellt: App, Browser oder Schlüsselpaar weisen Besitz nach, sofern eine eindeutige Bindung an das Gerät besteht. Ohne diese Bindung nicht.[16]

Für Banken kommt ein zweiter Weg in Betracht. Jede europäische Bank betreibt seit der Zahlungsdiensterichtlinie PSD2 eine Schnittstelle, an der sich zugelassene Drittanbieter mit Zertifikaten ausweisen. Die Rechenzentren verarbeiten dort täglich genau solche Nachweise. Ein Browser, der sich mit einem technisch vergleichbaren Zertifikat als Client registriert, könnte diesen vorhandenen Weg mitbenutzen, statt einen neuen zu bauen. Die Zertifikate dieser Schnittstelle setzen eine aufsichtsrechtliche Zulassung voraus und sind auf Unternehmen ausgestellt, nicht auf einzelne Geräte. Die Schnittstelle und die Technologie ist aber in jedem Rechenzentrum vorhanden und kann benutzt werden, auch um einzelne Clients zu zertifizieren.

Die Berlin Group, das europäische Gremium, das die Schnittstellen der Zahlungsdiensterichtlinie technisch standardisiert, hat einen solchen Zugang für Nicht-Drittanbieter selbst vorgesehen. „Direct Access“ öffnet dieselben Schnittstellen für die eigenen Kunden der Bank, beschrieben für Firmenkunden und Händler. An die Stelle der aufsichtsrechtlichen Zulassung tritt ein Vertrag mit der kontoführenden Bank. Das Rahmenwerk beschreibt dafür ausdrücklich eine Verwaltung von Nutzern, Konten und Zertifikaten, bis hinunter zu persönlichen Zertifikaten einzelner Zeichnungsberechtigter.[17] Und genau da ist auch der Raum für eine einzelne zertifizierte Browser-Installation eines einzelnen Nutzers.

7.4 Der erkennbare Client

Ein Browser, der sich ausweisen kann, ist ein erkennbarer Client. Der Betreiber sieht dann nicht nur, dass sich jemand mit gültigen SCA-Daten anmeldet, sondern auch, mit welchem Client. Die parallele Sitzung des Angreifers läuft über einen Client, den niemand registriert hat, und scheitert, bevor der Nutzer eine Freigabe erteilt. Genau das war die Lücke in dem zitierten Gerichtsurteil.

Für den Nutzer verschwindet dabei das, was ihn stört. Für den Zugang zum Portal liefert der Browser die Faktoren beim Programmstart, ohne zweites Gerät. Die Freigabe einzelner Zahlungen bleibt davon unberührt: Sie muss an Betrag und Empfänger gebunden bleiben, und das soll sie auch. Der Gewinn liegt beim Zugang, und der Zugang findet jeden Tag statt.

---

[15] W3C, WebAuthn Level 2: https://www.w3.org/TR/webauthn-2/

[16] EBA, Opinion on the elements of strong customer authentication under PSD2, EBA-Op-2019-06: https://www.eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

[17] The Berlin Group, openFinance API Framework Workplan 2026: https://www.berlin-group.org/_files/ugd/c2914b_bbc2887475d54da38b7c61854ab3db4e.pdf

8 Wer diesen Weg geht

Härtung ist seit 2010 ein Thema bei deutschen Banken und wird bei vielen Regionalbanken zum Standardprogramm. Isolation ist technisch weder neu noch exotisch. Die Marktforscher von Gartner erwarten, dass 2028 etwa 25 Prozent der Organisationen die vorhandenen Werkzeuge um mindestens einen abgesicherten Unternehmensbrowser ergänzen. Zum Zeitpunkt der Prognose lag der Anteil noch unter zehn Prozent.[18]

Das britische National Cyber Security Centre nennt in seinen Grundsätzen für besonders schützenswerte Arbeitsplätze die Virtualisierung als Weg, riskante Tätigkeiten vom Arbeitsplatz auszusperren, wenn sich diese Tätigkeiten nicht vermeiden lassen.[19] Das BSI führt in Version 3.0 seines Mindeststandards für Webbrowser virtualisierte Systeme und ferngesteuerte Browser-Umgebungen als erweiterte Lösung für hohen und sehr hohen Schutzbedarf.[20]

In der modernen Verwaltung ist Isolation längst im Betrieb. Dataport, der IT-Dienstleister mehrerer norddeutscher Länder, hat 2025 europaweit einen gekapselten Internetbrowser ausgeschrieben, ausdrücklich als Lösung auf dem Computer des Nutzers, mit Hardware-Virtualisierung und on Premises.[21]

9 Grenzen

Isolation ist keine Unfehlbarkeit. Das NCSC schreibt selbst, dass Hardware-Virtualisierung kein unfehlbares Sicherheitsmerkmal ist und Angreifer versuchen können, über Schwachstellen der Umgebung auf das Wirtssystem zu gelangen.[22] Microsoft hat im Januar 2025 drei aktiv ausgenutzte Rechteausweitungen in Hyper-V geschlossen. Es waren keine Ausbrüche aus der Micro-VM, aber Fehler in genau der Komponente, auf der die Hardware-Isolation ruht.[23] Der Unterschied zur ungeschützten Browser-Sitzung bleibt trotzdem groß: Der Angreifer muss eine zusätzliche, gut beobachtete Grenze überwinden, statt nur irgendein Schutzprogramm unterlaufen.

Die Hardware-Isolation braucht Ausstattung. Einen Prozessor, der sie beherrscht, ein Betriebssystem, das sie freigibt, und etwas mehr Arbeitsspeicher. Die Hardware-Virtualisierungsfunktion muss im Bios eingeschaltet sein, was ab Werk nicht zwingend der Fall ist, und der exklusive Zugriff auf sie kollidiert mit anderer Virtualisierungssoftware auf demselben Computer. Auf Geräten ohne diese Voraussetzungen steht deshalb nur die Härtung zur Verfügung. Eine Architektur, die beide Säulen kennt, kommt damit zurecht. Eine Architektur, die nur auf die Hardware-Isolation setzt, nicht.

Isolation endet an Tastatur und Bildschirm. Beide gehören weiter dem Computer des Nutzers. Gegen einen Angreifer, dessen Schadsoftware auf dem Computer bereits läuft, arbeitet die

[18] Gartner, Pressemitteilung 29.04.2025: https://www.gartner.com/en/newsroom/press-releases/2025-04-29-gartner-predicts-25-percent-of-organizations-will-use-secure-enterprise-browsers-to-enhance-remote-access-and-endpoint-security-by-2028

[19] NCSC, Principles for secure PAWs: https://www.ncsc.gov.uk/collection/principles-for-secure-paws/isolate-high-risk-activity-from-paw

[20] BSI, Mindeststandard Webbrowser V3.0: https://www.bsi.bund.de/dok/MST-Browser

[21] Bekanntmachung TED 364417-2025: https://ted.europa.eu/de/notice/-/detail/364417-2025

[22] NCSC, Principles for secure PAWs: https://www.ncsc.gov.uk/collection/principles-for-secure-paws/isolate-high-risk-activity-from-paw

[23] The Register, 15.01.2025: https://www.theregister.com/2025/01/15/patch_tuesday_january_2025/

Härtung. Das ist kein Nachteil der Hardware-Isolation, sondern der Grund, warum es beide Säulen braucht.

10 Fazit

Für den Betreiber eines sensiblen Portals lassen sich die Überlegungen auf drei Sätze bringen.

- Der Computer des Nutzers wird nicht sauber, egal wie gut das Portal ist. Wer seine Architektur auf einen sauberen Computer stützt, stützt sie auf eine Annahme, die im Alltag nicht hält.
- Suchen bleibt nötig und reicht trotzdem nicht aus. Dahinter gehört die Härtung, die auch dann trägt, wenn das Suchen versagt hat. Wo die Ausstattung es erlaubt, liegt die Hardware-Isolation darüber.
- Sicherheit muss nicht unbequem sein. Was den Nutzer heute stört, ist das zweite Gerät. Ein Browser, der die Faktoren selbst mitbringt und sich ausweisen kann, nimmt dem Betreiber die Unsicherheit und dem Nutzer den Aufwand.

CORONIC baut seit über 20 Jahren gehärtete Browser für Portale mit hohem Schutzbedarf. Hunderte von Banken und Sparkassen haben CORONIC-Produkte eingesetzt. Bei Browserüberweisungen mit diesen Produkten ist bei CORONIC kein Schadensfall dokumentiert. Die zweite Säule, die Hardware-Isolation, entsteht in einem Forschungsprojekt, das aus Mitteln der Europäischen Union und des Landes Schleswig-Holstein gefördert wird.

Wo ein Betreiber die starke Authentifizierung nicht über den Browser führen will oder kann, liefert CORONIC sie als eigene Anwendung: SIGN Connect ist eine europäische Multifaktor-Lösung mit App und WebAuthn. Sie lässt sich privacy-konform als Docker-Container im eigenen Rechenzentrum oder hybrid als White-Label betreiben, für beliebige Browser und ganz ohne US-Akzent.

Widerspruch erwünscht

Wir bauen Browser, keine Banking-Portale und keine Paymentlösungen. Was hier über die Portalwelt steht, ist die Sicht des Browserbauers, aus Projekten mit Banken. Wenn Ihre Wahrnehmung eine andere ist oder wenn Sie beim Lesen auf einen Fehler stoßen, sagen Sie uns gerne Bescheid. Die nächste Fassung erscheint dann inklusive Ihrer Anregungen.