# Das Passwort ist tot – es leben die Passkeys

# Das Passwort ist tot – es leben die Passkeys

Passwörter sind vom Konzept her kaputt, da helfen auch starke Passwörter und klassische Mehr-Faktor-Authentifizierung (MFA) nicht. Stattdessen brauchen wir konzeptionell sichere Authentifizierungsverfahren wie Passkeys.

Von Jürgen Schmidt

## -tract

- Die Authentifizierung mit Passwörtern ist inhärent unsicher: Auch die klassische Mehr-Faktor-Authentifizierung lässt sich mit Phishing aushebeln.
- Beim Passkey-Verfahren errechnet ein Authenticator für jede Domain einen eigenen Secret Key, mit dem er die Antwort auf eine Challenge des Servers signiert. Diese Antwort authentifiziert den Anwender.
- Passkey und Secret Key verlassen nie den Hoheitsbereich des Users.
- Der Authenticator kann ein externes Token oder im Betriebssystem integriert sein. Windows, macOS, Android und iOS bieten die Funktion bereits.

Das Grundproblem der Authentifizierung lösen Passwörter mit einem Geheimnis, dessen Besitz die Identität beweisen soll: Ich bin „ju“ und nur ich kenne das Geheimnis IM~qaaU0h!N5Z-:(UR~{H;8. Das ist noch nicht das Problem, sondern ein durchaus legitimes Konzept, mit dem sich prinzipiell bereits

eine recht hohe Sicherheitsstufe erreichen ließe. Das Problem beginnt an der Stelle, an der ich IM~qaaU0h!N5Z-:(UR~{H;8 einem Dienst als Antwort auf dessen Anfrage „Wie lautet dein Passwort?“ sende, um meine Identität zu beweisen.

Ich überspringe hier absichtlich die Klagen über 123456 und ficken123 als Passwörter, die sich viel zu einfach knacken oder erraten lassen. Denn das lässt sich durch entsprechende Policies, Awareness-Schulungen und den Einsatz von Passwort-Safes noch einigermaßen in den Griff bekommen. Doch auch mein Superpasswort, das ich nirgends anders benutze, ist eigentlich schon in dem Moment kompromittiert, in dem ich es in ein Passworteingabefeld eintippe respektive kopiere und abschicke.

## Abgephisht

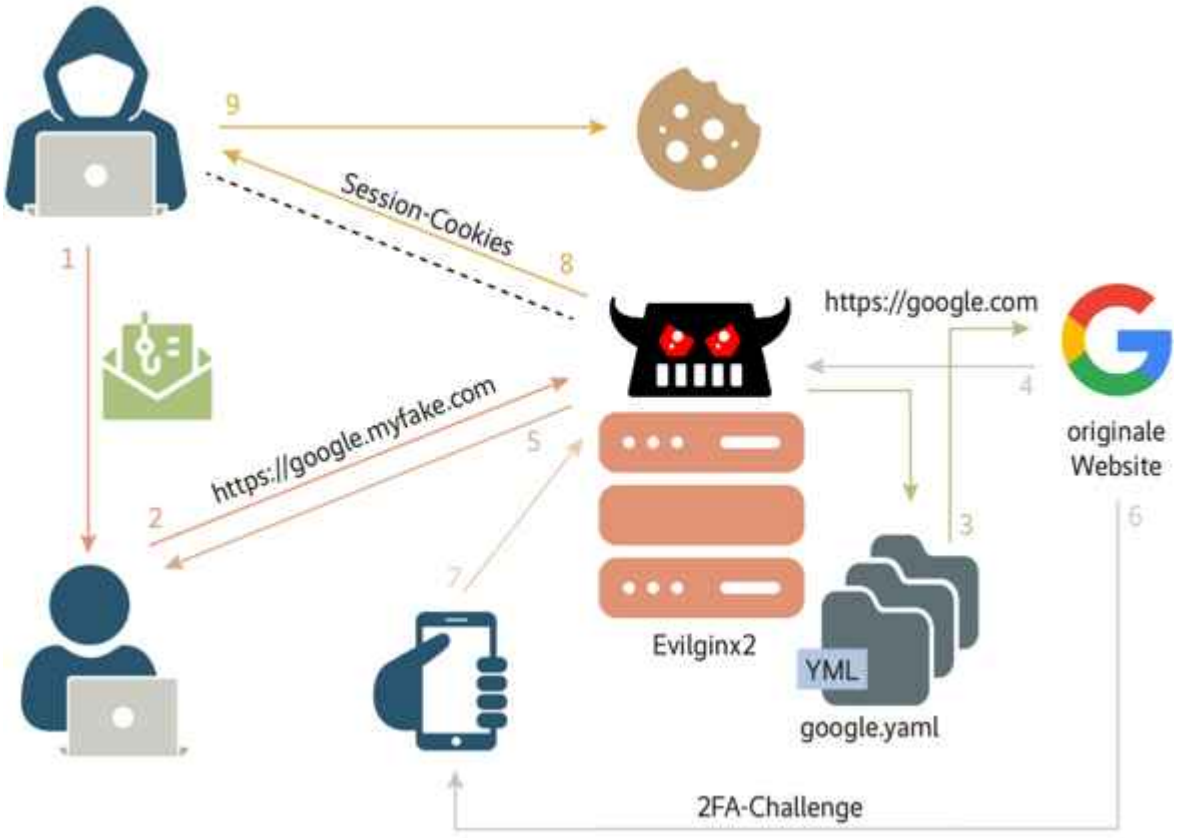
Denn damit ist das Geheimnis nicht mehr geheim. Letztlich weiß ich nicht, wer da auf der Empfängerseite mein geheimes Passwort bekommt und was der oder die dann damit macht. Phishing ist einer der wichtigsten Angriffsvektoren – und eine Gefahr sowohl für Privatpersonen als auch für Unternehmen. Das zeigen nicht nur Statistiken. Professionelle Penetrationstester erklären mir regelmäßig: „Wenn sonst gar nichts geht – Phishing geht immer.“ Und das gilt vermehrt auch für Zwei-Faktor-Authentifizierung.

Denn was bringt es, wenn ich zwei voneinander unabhängige Identitätsnachweise habe und dann letztlich zwei Zeichenketten an den Phisher schicke? Also beispielsweise mein normales Passwort und den Einmalcode, den ich via SMS oder von einer TOTP-App wie dem Authenticator bekommen habe? So gut wie nichts. Denn der Phisher muss nur schnell genug sein, sich während des Gültigkeitszeitraums mit den abgephishten Credentials beim Server anzumelden – und er ist drin.

## Echtzeit-Phishing

Wie leicht das geht, demonstriert das gern für Phishingtests

eingesetzte Tool Evilginx2 eindrucksvoll. Es funktioniert ähnlich wie der beliebte HTTP-Cache und Reverse-Proxy nginx. Damit setzen Angreifer mit wenigen Handgriffen eine Phishingseite auf, die dem Original gleicht wie ein Ei dem anderen. Denn alle Inhalte stammen von der echten Seite. Und die gesamte Kommunikation reicht der böse Ginx in Echtzeit in beide Richtungen durch.




Evilginx2 setzt sich als Man in the Middle zwischen Anwender und Webseite und kann die Websession nach dem Anmelden trotz Zwei-Faktor-Authentifizierung übernehmen (Abb. 1).
Allerdings nicht ganz direkt – zunächst protokolliert er alle Passwörter und auch das nach einer erfolgreichen 2FA ausgetauschte Session-Cookie. Da braucht es je nach dem von der Website eingesetzten Verfahren zum Session-Management etwas Anpassung – aber danach schreibt Evilginx2 dieses wichtige Token mit. Und damit hat der Phisher vollen Zugriff auf den Dienst. Da helfen weder SMS-PIN, TOTP noch Push-Authentication. Solange der Phisher die übertragenen Daten einfach weiterreichen und sich damit erfolgreich am Server anmelden kann, ist er drin.

Somit muss der Angreifer es nur noch schaffen, sein Opfer auf diese Phishingseite zu locken. Und dazu hat er beliebig viele Versuche und kann systematisch alle Mitarbeiter eines Unternehmens durchprobieren. Immer wieder. Irgendwann klickt eine oder einer auf den Link in der auf sie oder ihn zugeschnittenen Mail oder in dem als Waterhole zusammengezimmerten Forum. Natürlich kann man fordern, dass Anwender die URL einer Website prüfen müssen, bevor sie ihre Zugangsdaten eintippen. Aber immer öfter sieht man die URL gar nicht mehr – etwa auf Mobilgeräten oder bei Pop-up-Fenstern. Da hilft letztlich auch kein Awareness-Training, denn schon ein einziges unaufmerksames Opfer genügt. Wie die Pentester sagen: „Phishing geht immer."

## FIDO for the win

Um das zu ändern, hat die Alliance für Fast Identity Online (FIDO) ein konzeptionell besseres Authentifizierungsverfahren entworfen. Man hat dabei nach wie vor ein Geheimnis zum Nachweis der Identität – aber das gibt man nicht mehr Hinz und Kunz, sondern behält es immer unter seiner eigenen Kontrolle. FIDO ersetzt also das als Shared Secret fungierende Passwort, das man ständig durch die Gegend schickt, durch ein echtes Geheimnis – den Passkey.

Das ist keineswegs nur Wortklauberei, sondern ermöglicht den Einsatz moderner kryptografischer Verfahren, die viele Angriffe auf Passwörter praktisch unmöglich machen. Das Passkey-Konzept beruht auf asymmetrischer Kryptografie und einem Challenge-Response-Verfahren. Dazu benötigt man ein Stück Software, den sogenannten Authenticator, der den Authentifizierungsvorgang auf der Clientseite abwickelt. Er erzeugt für jeden Dienst ein eigenes Schlüsselpaar aus Public und Secret Key, indem er den geheimen Passkey mit dem Domain-Namen kryptografisch verknüpft (als Keyed-Hash Message Authentication Code, etwa HMAC-SHA256). Das bedeutet, dass der für Google verwendete Schlüssel ein anderer ist als der für

Microsoft oder Heise. Somit kann man Nutzer nicht über ihre Anmelde-Credentials tracken.

Den Public Key hinterlegt der Nutzer bei der Registrierung auf dem Server; den geheimen Passkey bekommt der Dienstbetreiber jedoch nie zu sehen – und kann ihn sich folglich auch nicht mehr stehlen lassen. Für die Anmeldung schickt der Server eine Challenge an den Authenticator. Der signiert diese mit dem passenden geheimen Schlüssel und schickt dies als Antwort an den Server. Der Anwender muss diesen Vorgang lediglich autorisieren – etwa durch das Berühren eines Sensors auf dem Token (User Presence).

In fortgeschrittenen Szenarien muss er seine Berechtigung etwa durch Eingabe einer PIN, Gesichtserkennung oder Fingerabdruck gegenüber dem Authenticator nachweisen (User Verification, UV). Dieser übermittelt dem Server lediglich das Ergebnis des UV-Tests; keinesfalls gehen dabei PINs oder gar biometrische Daten über die Leitung. Die gelegentlich anzutreffende Aussage, man melde sich mit seinem Fingerabdruck oder Gesicht an, ist also falsch oder zumindest irreführend verkürzt. Die Authentifizierung beim Server erfolgt mit dem Passkey, den man mit seinen biometrischen Merkmalen lokal freischaltet.

Das Challenge-Response-Verfahren verhindert herkömmliches Phishing mit nachgemachten Seiten und auch Replay-Angriffe sind nicht mehr möglich. Aber auch Echtzeit-Phisher mit Tools wie Evilginx2 bleiben außen vor: Die könnten zwar einen Anwender auf die Phishingseite www.he1se.de locken. Aber weil die Authentifizierung jetzt Domain-abhängig erfolgt, hilft ihnen das, was sie dort ergaunern, nicht beim Zugriff auf den echten Server www.heise.de.

## Die Bausteine

Das Ganze steht und fällt mit der Verfügbarkeit des Authenticators, der die ganzen Kryptooperationen abwickeln muss. Im ersten Schritt wurde er zusammen mit dem Passkey in

einen externen Security Key in Form eines Tokens gepackt. Der Browser kommuniziert dann über das Client to Authenticator Protocol (CTAP) etwa via USB mit diesem Token. Neuere Token unterstützen teilweise auch NFC; Bluetooth hingegen hat sich dafür nicht bewährt. Der geheime Schlüssel lässt sich nicht auslesen und verlässt dieses Token nie. Muss er auch nicht, denn alle kryptografischen Operationen damit erledigt das Token selbst. Somit kann nicht einmal eine Schadsoftware auf dem PC den Passkey aus- oder mitlesen.

In der nächsten Stufe haben die Betriebssysteme diese Authenticator-Funktion direkt eingebaut. So können Windows-PCs, Macs, Android-Smartphones und iPhones mittlerweile direkt als Authenticator agieren – ganz ohne externe Token. Den Passkey speichern sie dabei wo möglich in ihrem sicheren, nicht auslesbarem Speicher (bei Apple die Secure Enclave, bei Windows möglichst im TPM). Lediglich Linux-Desktop-Systeme können da noch nichts vorweisen, hier müssen dann reine Softwarelösungen einspringen. So kann man gemäß FIDO-Spec einen Authenticator auch als Browsererweiterung realisieren. Google etwa hat das in einigen Versionen des Chrome-Browsers eingebaut.

Der eigentliche Anmeldevorgang findet zwischen Browser und dem Webserver des Dienstes statt; im FIDO-Sprech ist Letzterer die Relying Party. Die beiden kommunizieren dabei über das Protokoll WebAuthn. Praktisch alle modernen Browser beherrschen das mittlerweile; auf der Serverseite sieht das allerdings noch eher dünn aus. Doch das ändert sich gerade.


Der Authenticator errechnet für jede Domain aus dem Passkey

einen eigenen Secret Key, mit dem er die Antwort auf eine Challenge des Servers signiert. Diese Antwort authentifiziert den Anwender (Abb. 2).

## Abstufbare Sicherheit

Dieses Passkey-Konzept kann man in verschiedenen Szenarien und für unterschiedliche Sicherheitsanforderungen umsetzen. Ursprünglich hatte es die FIDO Alliance als Universal 2nd Factor (U2F) spezifiziert. Die Idee dabei war, dass man die geheimen Schlüssel zusammen mit der notwendigen Software für die Challenge-Response-Authentifizierung in ein externes Token packt, wo sie auch vor Trojaner-Angriffen sicher sind. Die ersten Umsetzungen waren folglich Hardwaretoken wie die von Yubico, Feitian, SoloKeys und vielen anderen.

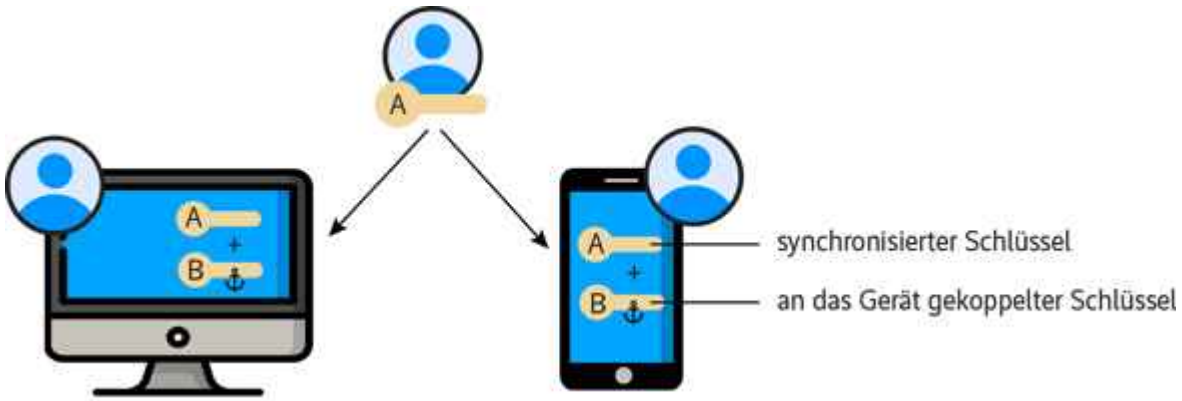
Mit FIDO2 hat die FIDO das Konzept erweitert und verallgemeinert, um Passkeys auch als einzigen Faktor zu erlauben und damit direkt das Passwort zu ersetzen, statt es nur zu ergänzen. Die Idee dabei ist: Passkeys sind auch ohne Passwörter so sicher, dass sie als alleiniger Schutz für die meisten Anwendungsfälle vollkommen ausreichen. Der Einsatz als zweiter Faktor gemäß U2F ist aber nach wie vor möglich und Teil der Spezifikation von FIDO2. Prinzipiell kann bei FIDO2 der Authenticator übrigens auch den bei einem Dienst verwendeten Benutzernamen speichern. Damit reduziert sich das sichere Anmelden im Wesentlichen auf einen Klick und den Blick in die Kamera. Praktisch wird das jedoch bisher kaum genutzt.

Trotzdem setzte sich Passkey-Authentifizierung immer noch nicht auf breiter Front durch. Das Problem: Die für höchste Sicherheitsansprüche geforderte Versiegelung der Passkeys in nicht auslesbaren Speicherbereichen verhinderte Backups und die Nutzung eines Passkeys auf mehreren Geräten. Man meldete sich mit seinem Smartphone ganz toll und komfortabel ohne Passwort bei einem Shop an, konnte dann aber auf dem PC nicht darauf zugreifen – oder umgekehrt. Und wenn man den hinterlegten Authenticator verlor, hatte man sich ausgesperrt.

## Synchron via Cloud

Das soll sich jetzt ändern. Mit einer 2022 gestarteten Initiative wollen FIDO, Apple, Google und Microsoft einen weiteren Stein aus dem Weg räumen: Die Passkeys sollen übertragbar werden. Beziehungsweise noch besser: Die Geräte eines Anwenders synchronisieren sich automatisch über die Cloud. Das ist wohlgemerkt optional. Ein Server kann auch weiterhin auf Passkeys bestehen, die fest an ein Gerät beziehungsweise Token gekoppelt und damit vor dem Zugriff durch Malware geschützt sind.

Am weitesten ist dabei aktuell Apple, wo die Cloud-Vision für Passkeys in iOS und macOS bereits weitgehend umgesetzt ist. So aktivierte ich kürzlich auf meinem iPhone endlich die Zwei-Faktor-Authentifizierung für meinen Bitwarden-Account. Ich klickte lediglich: „Ja, Passkey benutzen“, bestätigte meine Identität mit FaceID und der zweite Faktor war aktiv. Mit etwas flauem Gefühl versuchte ich dann, vom MacBook aus darauf zuzugreifen. Doch siehe da: Das klappte auf Anhieb. Ich bestätigte mit meinem Fingerabdruck, dass ich berechtigt bin, den Passkey zu nutzen (UV) – und schwups war ich drin. Apple hatte den Passkey bereits über die iCloud synchronisiert.




Mittlerweile lassen sich Passkeys über die Cloud zwischen mehreren Geräten synchronisieren (Abb. 3).
Google hat das zumindest für Android 9+ und Chrome bereits ähnlich umgesetzt; dabei läuft die Synchronisierung über den Google Password Manager. Microsoft arbeitet auf Hochtouren daran, das ebenfalls noch dieses Jahr auf die Straße zu

bekommen. Da wird es von beiden Herstellern im Lauf des Jahres noch größere Ankündigungen geben. Meine ursprüngliche Befürchtung, dass sich die Konzerne dabei selbst ebenfalls Zugriff auf die Passkeys der Anwender einräumen, hat sich übrigens nicht bestätigt: Apple synchronisiert die Passkeys Ende-zu-Ende-verschlüsselt. Das bedeutet in dem Kontext, dass für den Zugriff immer mindestens ein Geheimnis erforderlich ist, das nur der Anwender, nicht aber Apple im Zugriff hat. Google folgt offenbar diesem Beispiel, und wie es aussieht, wird auch Microsoft hier E2E-Technik einsetzen.

## Schöne passwortlose Welt

Damit ist die Authentifizierung mit Passkeys endlich nicht nur viel sicherer, sondern auch komfortabler als mit Passwörtern. Man meldet sich bei einem Dienst an, bestätigt, dass man den Passkey benutzen will, und kann sich künftig auf all seinen Geräten dort anmelden. Dazu muss man lediglich das jeweilige Gerät entsperren können (UV mit PIN, Fingerabdruck oder Gesicht) und das erledigt dann den Rest. Passwort braucht man keines mehr. Aber ja, Sie haben recht: Das ist zu schön, um wahr zu sein.

Ich habe mir nämlich letztlich mit meinem 2FA-Experiment bei Bitwarden doch ins Knie geschossen. Denn ich konnte zwar von iPhone und Mac aus problemlos auf das Bitwarden-Konto zugreifen. Doch auf meinen Linux- und Windows-Rechnern war ich ausgesperrt. Für die musste ich dann doch noch einen TOTP-Authenticator registrieren.

Und das wird auch noch auf absehbare Zeit hässlich bleiben. Denn die Passkey-Konzepte der Hersteller spezifizieren lediglich eine Synchronisierung im eigenen Cloud-Kontext. Als Workaround können Roaming Authenticators dienen, bei denen etwa ein iPhone eine Cross-Device-Authentifizierung für einen PC durchführt; die Kommunikation zwischen PC und Smartphone erfolgt dabei via Bluetooth.

Echte Passkey-Brücken zwischen Microsofts Azure, Googles Cloud Platform und Apples iCloud gibt es bislang aber nicht. Dabei wären APIs, die es etwa Drittanbietern erlauben, den Passkey-Sync über Plattformgrenzen hinweg durchzuführen, überaus wünschenswert. Zumindest Google und Microsoft haben diesbezügliche Absichten bereits anklingen lassen. Bis das spezifiziert, umgesetzt und ausgerollt ist, wird allerdings noch einige Zeit vergehen.

Trotzdem glaube ich, dass der Einsatz von Passkeys dieses Jahr einen großen Schritt nach vorne machen wird. Das größte Potenzial sehe ich dabei im Endanwenderbereich, wo allein die drei großen FIDO-Protagonisten Google, Microsoft und Apple so viel bewegen können, dass viele Dienstbetreiber ebenfalls auf den Zug aufspringen werden. Für den Einsatz in Unternehmen fehlen aktuell noch Konzepte für das unternehmensweite Passkey-Management. Dort hoffe ich vor allem auf verstärkten Einsatz von Passkeys als zweiter Faktor, wo FIDO2-Hardwaretoken deutlich mehr Sicherheit bieten als SMS oder TOTP. (odi@ix.de)

1. Quellen
2. Weitere Informationen zu Passkeys und FIDO2 sowie Evilginx2: ix.de/zfnt

---

# Zugangssicherheit-2FA, MFA und FIDO2

# Zugangssicherheit: 2FA, MFA und FIDO2

Das Passwort hat eigentlich ausgedient, weil mit FIDO2 ein phishingresistentes Log-in-Verfahren existiert. Wie das funktioniert und warum das eher eine Lösung für übermorgen als für morgen ist.

Von Jürgen Seeger

## -tract

- Zwei-Faktor-Authentifizierung (2FA) erhöht die Sicherheit signifikant, ist für Onlinekäufe und Finanztransaktionen sogar vom Gesetzgeber vorgeschrieben.
- Nicht alle 2FA-Verfahren sind sicher, so wurden Accounts, die durch eine per SMS gesendete PIN gesichert waren, Opfer von Phishingangriffen.
- Phishingresistent ist FIDO2, ein Standard, der statt der Übermittlung von Passwörtern ein sicheres Public-Key-Verfahren definiert.

Sicherheit und Zugänglichkeit sind bekanntlich konkurrierende Anforderungen: Je sicherer, desto unbequemer. Logisch also, dass viele – wenn nicht die meisten – Benutzer schlampig mit ihren Passwörtern umgehen. Seien es die berühmt-berüchtigten Zettel unter der Tastatur, Trivial-Passwörter à la „12345678“, immerwährend gleiche Phrasen für verschiedene Zugänge oder der Vorname der Tochter. Daran haben bislang auch erzieherische Maßnahmen wie der Welt-Passwort-Tag – jedes Jahr am ersten Donnerstag im Mai – wenig geändert.

Wer nationale Gedenktage mag, der kann am Änderere-dein-Passwort-Tag am 1. Februar alljährlich alle, so wirklich die Aufforderung, Passwörter ändern. Dabei ist das BSI von seinem

Rat, man möge Passwörter häufig ändern, bereits 2020 abgerückt. Denn das führe nur zu einfachen und somit unsicheren Passwörtern. Hintergrund: Ist ein Bruce-Force-Angriff auf ein zehn Zeichen langes Passwort aus dem Ziffernraum von 0 bis 9 in 10 Sekunden erledigt, dauert dies bei gleicher Rechenleistung bei einem Zeichenraum von 96 (Klein- und Großbuchstaben, Ziffern, Sonderzeichen) über 2000 Jahre. Dabei ist das „Erraten" von Passwörtern mittels automatisierten Ausprobierens oder Wörterbüchern nur eine Variante der Kompromittierung von Zugangsdaten. Sie können auch schlicht abgefangen oder via Social Engineering beziehungsweise Phishing ausspioniert werden. Hinzu kommt die Arbeitsbelastung auf der Serviceseite: Anrufe wegen vergessener Credentials, Mechanismen zum Übermitteln neuer Passwörter und so fort.

Langer Rede kurzer Sinn: Allein die Kombination von Accountnamen und Passwort ist weder sicher noch bequem oder effizient. Ein weiteres Kennwort oder Merkmal zu fordern ist zumindest aus der Sicherheitsperspektive betrachtet eine auf der Hand liegende Idee, also eine Zwei- oder Mehr-Faktor-Authentifizierung (2FA/MFA). Zudem sollte dieser zweite Faktor nicht dauerhaft kompromittierbar sein, weil er nur für ein Log-in oder für einen begrenzten Zeitraum gilt.

## Wenn es um Geld geht, ist 2FA vorgeschrieben

Das hat auch der deutsche Gesetzgeber erkannt und für den Zahlungsverkehr 2FA-Verfahren vorgeschrieben. Dabei wurden zum Teil offene Türen eingerannt, denn die Übermittlung einer Transaktionsnummer für Zahlungen ist seit Jahren nicht nur gängige Praxis der Kreditinstitute, sondern wurde schon am 14. September 2019 verpflichtend durch die EU-Zahlungsdiensterichtlinie PSD2. Jedenfalls ist seit dem 15. März 2021 2FA für alle Onlinezahlungen, also etwa auch beim Kauf im Webshop, obligatorisch, eine erste Stufe dieser

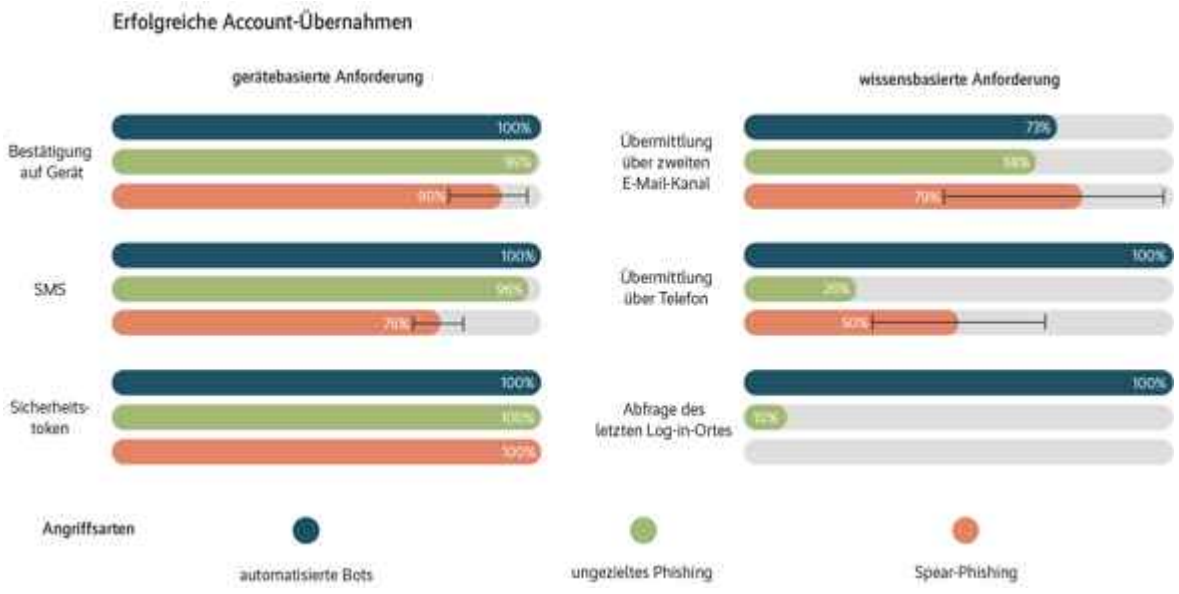
Vorschrift galt schon seit dem 15. Januar 2021. Ob und inwieweit der durch die DSGVO vorgeschriebene Schutz persönlicher Daten durch den Stand der Technik zwingend eine 2FA-Zugangssicherung nach sich ziehen wird, ist derweil noch Zukunftsmusik.

Zur konkreten Ausgestaltung des zweiten Faktors gibt es mehrere Möglichkeiten. Grob unterscheiden lassen sich Besitz eines Gerätes oder Merkmals, das Wissen um ein temporäres Geheimnis sowie Kombinationen davon. Biometrische Merkmale können durch einen Fingerabdruck- oder Iris-Scanner, Gesichts- oder Stimmerkennung verifiziert werden. Die diesen Verfahren inhärenten Risiken für den Anwender (Stichwort: abgeschnittener Finger) werden durch Lebenderkennung zu vermeiden versucht. Beim Faktor Besitz kann es sich um ein dediziertes Gerät handeln, das ein temporäres Passwort generiert. RSA stellte solch ein System unter dem Namen SecurID bereits 1986 vor; mittlerweile existieren zahlreiche Gerätchen, die zeitbasiert oder angestoßen durch zum Beispiel den Scan eines eigens dazu erzeugten QR-Codes ein Einmalpasswort generieren. Inzwischen sind diese Geräte oft durch das Mobiltelefon abgelöst worden, auf dem eine spezielle App läuft. Dass das zweite Merkmal nicht auf demselben Gerät, mit dem man sich einloggen will, erzeugt werden sollte, versteht sich von selbst (und wird auch vom BSI ausdrücklich empfohlen).

Der Vollständigkeit halber sei erwähnt, dass als eine Kombination von Besitz und Wissen auch die Übermittlung des zweiten Passworts über einen separaten Kanal gelten kann, also über eine zweite E-Mail-Adresse oder via SMS. Beides gilt als nicht sehr sicher, denn diese Nachrichten können abgefangen werden. So hat vor einer Übermittlung durch SMS-Nachrichten das für die Sicherheit von US-Behörden zuständige National Institute for Standards and Technology (NIST) bereits 2016 gewarnt. Die weithin bekannt gewordenen 2FA-Hacks betrafen denn auch SMS als zweiten Faktor: 2018 wurde das Portal Reddit

durch Abfangen einer SMS gehackt, 2021 die Kryptobörse Coinbase.

Google hat 2019 auf einer Webkonferenz die Ergebnisse einer Langzeitstudie zum Thema Sicherheit von 2FA-Verfahren veröffentlicht. Diese unterschied zwischen automatisierten Bot-Attacken, ungezieltem und gezieltem Phishing sowie zwei Arten von 2FA: geräte- und wissensbasiert. Das Ergebnis der Studie ist eindeutig: Bot-Attacken wurden durch fast alle 2FA-Verfahren vollständig abgewehrt (siehe Abbildung 1). Am schlechtesten schnitt die Übermittlung des zweiten Kennworts via E-Mail ab, aber auch die half schon gegen drei Viertel der Bot-Angriffe. Gegen ungezieltes Phishing lag die Abwehrrate der gerätebasierten Verfahren nahe bei 100 Prozent. Sogar gegen Spear-Phishing, gezielte Angriffe auf einzelne Accounts, erwiesen sich die gerätebasierten Verfahren als signifikant erfolgreicher, mit Abstand am besten schnitten Security-Token ab (siehe dazu auch den Test von vier ausgewählten Token im Artikel „Vier FIDO2-Token für den USB-Port“ ab Seite 50).




Klarer Sieger im Abwehrspiel: Security-Token konnten alle Arten von Angriffen abwehren (Abb. 1). *Google*

## HOTP und TOTP

Zur Generierung von Einmalpasswörtern existieren zwei Verfahren, bezeichnet als HMAC-based One-time Password (HOTP)

und Time-based One-time Password (TOTP). HOTP ist ereignisgesteuert, aus einem Server und Client bekannten gemeinsamen Geheimnis und einem bei der Registrierung synchronisierten Zähler wird auf beiden Seiten durch den Keyed-Hash Message Authentication Code ein Schlüssel erzeugt, der übereinstimmen muss. Der Zähler wird bei jeder Authentifizierung hochgezählt.

Durch HOTP generierte Passwörter haben kein inhärentes Verfallsdatum. Der Client kann den Zähler bei einem fehlgeschlagenen Log-in hochsetzen. Um sich weiterhin mit dem Server abgleichen zu können, geht dieser nicht von einem fixen Zählerstand aus, sondern von einem Bereich, dem Validierungsfenster. Ist dieses zu groß, gibt das Angreifern die Gelegenheit zum Erraten des OTP. Ist es zu klein, müssen Client und Server erneut synchronisiert werden.

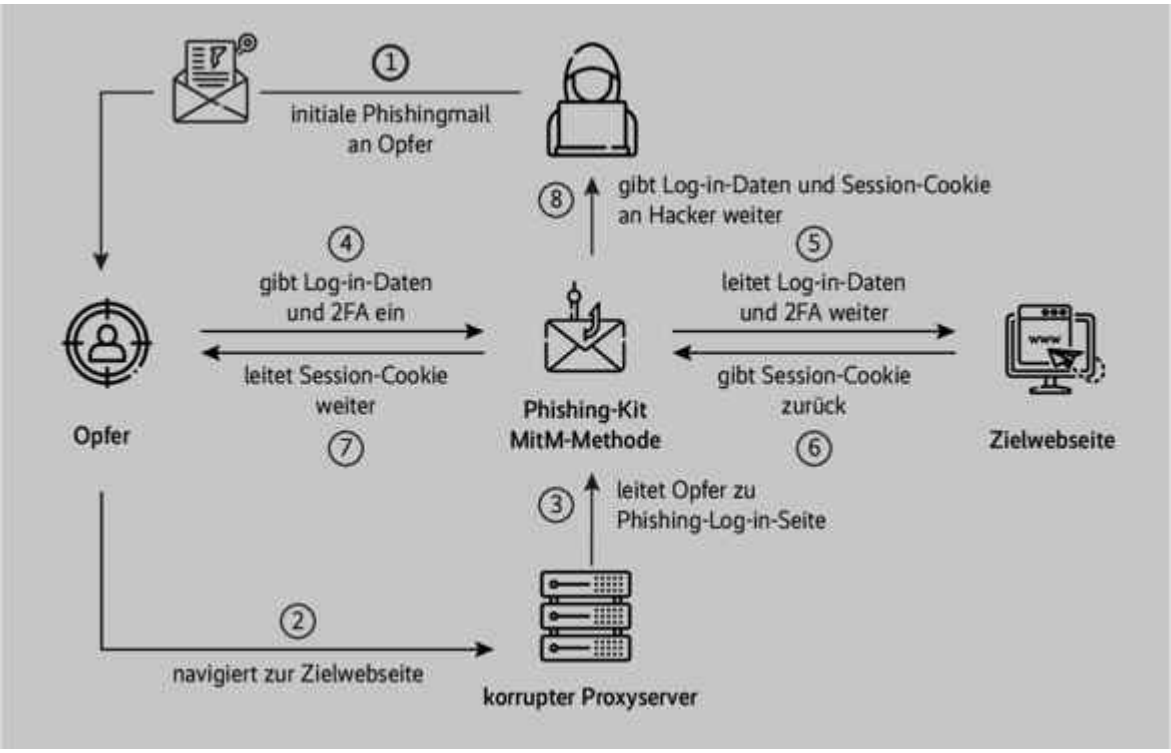
Beim neueren TOTP wird statt eines Zählers die Uhrzeit benutzt, die Gültigkeitsdauer des generierten Passworts ist implementierungsabhängig. Auch hier stehen sich Bequemlichkeit, also ein langer Zeitraum, und Sicherheit, eine kurze Gültigkeitsdauer, gegenüber. Laufen die Uhren auf Client und Server auseinander, steht eine neue Synchronisierung an.

Das generierte Einmalpasswort kann im Klartext angezeigt, via Telefon oder Mail übermittelt oder als QR-Code präsentiert werden.

## MFA hilft, ist aber kein Allheilmittel

2FA beziehungsweise MFA hilft also auf jeden Fall. Aber leider ist es kein Allheilmittel. Denn im ständigen Wettlauf zwischen Sicherheitsimplementierungen und Angreifern ist eine Schwachstelle im 2FA-Konzept aufgefallen: Was passiert eigentlich, wenn die den zweiten Faktor anfordernde Stelle nicht die ist, für die sie sich ausgibt? Es geht um eine Variante des Man-in-the-Middle-Angriffs (MITM), bei der eine zwischengeschaltete Stelle die Informationen abfängt, zwischen

Client und Server hin- und herleitet und zwischenspeichert (siehe Abbildung 2). Es gibt dafür seit ein paar Jahren fertige MITM-Pakete wie Evilginx, Muraena oder Modlishka. Eine Suche nach „2fa bypass“ bei GitHub ergab beim Schreiben dieser Zeilen über 40 Treffer, in einer Veröffentlichung der Sicherheitsfirma Malwarebytes Labs ist von 1200 Toolkits zum Umgehen von 2FA-Verfahren die Rede.




Kommunikation abgefangen: Das MITM-Tool leitet auch den zweiten Faktor hin und her (Abb. 2).

Man kann zwar den Erfolg von Phishingangriffen durch Schulungen und Aufmerksamkeitskampagnen unwahrscheinlicher machen. Also klarstellen, dass vor einem Mausklick das Ziel genau geprüft werden soll et cetera. Die grundsätzlichere Lösung besteht aber im Errichten einer Verbindung zwischen Client und Server, bei der sich beide Seiten ausweisen. Und genau das macht FIDO, aufgelöst Fast Identity Online, aktuell gilt FIDO Version 2 (FIDO2). Das „Fast“ hängt damit zusammen, dass man bei FIDO2 überhaupt kein Passwort mehr eingeben muss, sich also schnell einloggt und sich alle Debatten um sichere Passwörter erledigt haben. Damit hat sich das eingangs erwähnte Dilemma „je sicherer, desto unbequemer“ weitgehend in Wohlgefallen aufgelöst, FIDO ist sowohl sicher als auch

bequem.

## Public/Private Keys statt Passwörtern

Statt auf die Übermittlung von Passwörtern setzt FIDO2 auf ein Public-Private-Key-Verfahren. Dazu bedarf es eines Authenticator, Software mit Zugriff auf einen dedizierten Chip (Token), auf einem Mobiltelefon oder einem PC mit TPM-Baustein, derzeit unter Android und iOS beziehungsweise macOS und Windows 10/11. Dieser Authenticator identifiziert sich durch ein nicht extrahierbares Geheimnis, etwa eine Zahlenfolge, und ist gebunden an das Gerät. Aus einer Kombination dieser Zahlenfolge und der Internetadresse der Gegenstelle, des Servers, generiert er ein asymmetrisches Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel.

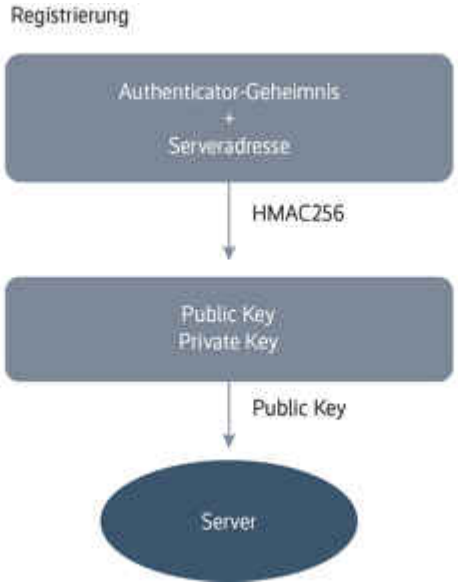
Bei der Registrierung speichert der Server des Dienstes den öffentlichen Schlüssel, nicht mehr wie bisher Accountname und Passwort. Der Server verwahrt also auch keine Geheimnisse mehr, die missbraucht werden können. Der private Key verlässt nicht den Authenticator und muss dort nicht einmal gespeichert sein, wahlweise kann das Schlüsselpaar bei jedem Kontakt zum Server neu erzeugt werden.

Bei einem Log-in-Wunsch schickt der Server eine sogenannte Challenge, eine sich bei jedem Log-in ändernde Zeichenfolge, die der Authenticator mit dem privaten Schlüssel signiert und zurückschickt. Der Server überprüft mittels des bei der Registrierung hinterlegten öffentlichen Schlüssels die Gültigkeit der Signatur und gibt im positiven Fall dem Log-in-Wunsch statt. Dieser Vorgang wird bei jedem Log-in-Wunsch wiederholt, es wird für jeden Server ein jeweils eigenes Public-Private-Paar generiert. Da die Serveradresse in die Schlüsselerzeugung eingeht, ist eine Umleitung auf einen anderen Server nicht möglich. Damit ist der übliche Weg für Phishingattacken versperrt.

Das Übersenden der signierten Challenge muss vom Benutzer bestätigt werden, durch einen biometrischen Abgleich oder eine PIN. Nichts davon geht über die Leitung, diese Daten verwendet nur der Authenticator als Sendegenehmigung. Worin diese besteht, wird beim Registrierungsprozess festgelegt. Bliebe die Möglichkeit, dass ein Trojaner den Authenticator steuert. Das ist bei einem dedizierten Token, das etwa einen Fingerabdruck zum Senden der signierten Challenge fordert, allerdings schwer vorstellbar. FIDO2 kann als alleiniges, passwortfreies Authentifizierungsverfahren eingesetzt werden oder zusätzlich zum vorhandenen Log-in-Prozedere, im letzteren Fall ist die Abfrage einer Sendegenehmigung optional.

Zur Generierung des Schlüsselpaars kommt wie bei HOTP und TOTP Keyed-Hash Message Authentication Code (HMAC-SHA256) zum Einsatz, für das Signieren der Challenge das auf elliptischen Kurven beruhende ECDSA P-256. Dass optional auch das veraltete RSA weiterhin mitspielen darf, wird in Sicherheitskreisen kritisiert.

FIDO2 wurde 2019 veröffentlicht und fasst die Standards FIDO und U2F (Universal Second Factor) zusammen. Definiert sind zwei APIs, WebAuthn auf Client- und Serverseite sowie CTAP, das Client-to-Authenticator Protocol zur Verbindung des Authenticators mit einem Webbrowser oder einem anderen Client. Für beide Standards ist der Code offengelegt und auf GitHub in verschiedenen Implementierungen und Programmiersprachen verfügbar, derzeit für Android, iOS, macOS und Windows 10/11 sowie die Browser Chrome, Edge, Firefox und Safari. Der Standard wird vom W3C und einer breiten Allianz von Behörden und Firmen unterstützt, von Apple und Amazon über Intel und Microsoft bis Visa und Yahoo. Auch das deutsche BSI und das US-Pendant NIST sind bereits seit 2015 Mitglied.




Mit FIDO2 gehen weder bei der Registrierung noch … (Abb. 3a) *ss*


… beim Log-in geheime Daten über die Leitung (Abb. 3b).

Genügend Gründe für einen baldigen Erfolg eigentlich. Wären da nicht die Beharrlichkeit von Benutzern und die notorische Sparsamkeit der Geschäftsführungen. Denn ein Log-in mit Benutzername und Passwort ist seit Jahren eingeübt und auch nicht langsamer als das passwortlose FIDO2-Verfahren, zumindest wenn man einen Passwortmanager nutzt. So ist bei einem Log-in via Webbrowser, der die Zugangsdaten gespeichert hat, häufig nicht einmal der Griff zur Tastatur nötig – zwei bestätigende Mausklicks reichen. Hinzu kommt die Angst vor Schlüsselverlust. Diese war in einer Untersuchung der Universität Bochum zur Akzeptanz von FIDO2-Token der von den Testpersonen meistgenannte Grund für ein Beharren auf den gewohnten Log-in-Verfahren. Hier kommt auch die Kostenfrage ins Spiel. Denn das Budgetargument ist nicht mit dem Verweis auf die relativ günstigen USB- oder NFC-Token vom Tisch, und auch nicht mit dem Hinweis auf die ohnehin vorhandenen

Smartphones oder PCs mit Authenticator-Funktionalität. Die eigentlichen Belastungen entstehen im Ausrollen von FIDO2 nebst Verfahren zum Ersatz verlorener Token, und eine firmen- oder behördeninterne Akzeptanzkampagne dürfte dazukommen.

## Passkeys – alles wird noch einfacher?

Mit FIDO2 muss man jeden Dienst auf einem Gerät mit Authenticator-Funktionalität registrieren, oder ein entsprechendes Token dabei haben, ein sogenanntes Roaming-Device. Hier kommt die im Mai 2022 von Apple, Google und Microsoft vorgestellte FIDO2-Erweiterung Passkeys ins Spiel (siehe Artikel „Das Passwort ist tot – es leben die Passkeys“ ab Seite 46, Demo-Site: Passkeys.io). Bei diesem Verfahren wird das bei der Registrierung erzeugte Schlüsselpaar in der Hersteller-Cloud hinterlegt, der private Schlüssel verlässt also den Authenticator-Client. So kann man dann einfach einen weiteren Dienst integrieren oder ein verlorenes Token ersetzen. Vorausgesetzt, man kennt noch die Credentials für die Hersteller-Cloud. Also Benutzername, Passwort und irgendeinen zweiten Faktor. Den FIDO-Segen erhielt das Verfahren durch die Erweiterung Multi-Device FIDO Credentials.

So verlassen natürlich die privaten Schlüssel entgegen der ursprünglichen FIDO-Intention den Client, es liegen doch wieder sensible Daten in der Cloud. Immerhin haben sich kurze Zeit nach der Vorstellung von Passkey Apple und Google darauf verpflichtet, die privaten Schlüssel der Benutzer so zu speichern, dass die Konzerne darauf keinen Zugriff haben. Ende 2022 ist auch Microsoft mit diesem Versprechen nachgezogen.

Für den Zugang zum Firmennetz ist Passkeys (noch?) keine Option. Hier wird man mit dem Ausrollen von FIDO2-Mechanismen zum Umgang mit verlorenen oder zerstörten Schlüsseln aufsetzen müssen. (js@ix.de)

1. Quellen

2. Verweise auf die Dokumente der FIDO-Allianz, den Code bei GitHub, den Usenix-Talk zur 2FA-Akzeptanz und die Google-Studie zur Wirksamkeit von 2FA-Maßnahmen sind unter ix.de/zy24 zu finden.

---

# DSGVO-Bußgelder um 50 Prozent gestiegen

## DSGVO-Bußgelder um 50 Prozent gestiegen

**Die Bußgelder für DSGVO-Verstöße zogen im letzten Jahr deutlich an. Dabei baten die europäischen Richter Meta für Verstöße bei Facebook, Instagram und WhatsApp zur Kasse – jedoch um 4 Milliarden zu wenig, wie Datenschutzaktivist Max Schrems meint.**

Im Jahr 2022 ist die Zahl der Bußgelder in der EU wegen Verstößen gegen die Datenschutz-Grundverordnung stark angestiegen. Das belegt eine Studie der internationalen Anwaltskanzlei DLA Piper. Im Vergleich zum Vorjahr sind die Bußgelder um etwa 50 Prozent auf insgesamt 1,64 Milliarden Euro gestiegen. Dazu beigetragen haben insbesondere die Bußgelder gegen Facebook in Höhe von 210 Millionen Euro und Meta in Höhe von 180 Millionen Euro. Wegen dieser Verfahren führt die hierfür verantwortliche irische Datenschutzbehörde DPC das Ranking an. Im gleichen Zeitraum hat die Zahl der von Unternehmen gemeldeten Datenpannen signifikant abgenommen.

Der bekannte Datenschutzaktivist Max Schrems hat die irische Datenschutzbehörde für einen zu laxen Umgang mit Meta kritisiert. Seiner Meinung nach hätte das verhängte Bußgeld 4 Milliarden Euro höher ausfallen müssen – die Behörde legte

sich jedoch auf 390 Millionen Euro wegen DSGVO-Verstößen fest. Der Vorwurf lautete, dass Facebook rechtswidrig die gezielte Werbung gegenüber Nutzern als vertragliche Leistung ausgegeben hat, für die keine Einwilligung erforderlich sei. Ebenso fehlte es an einer wirksamen Einwilligung für das Tracking des Nutzerverhaltens. Laut Schrems hätte die DPC bei der Bemessung des Bußgelds die zusätzlichen Werbeeinnahmen durch den Datenschutzverstoß angemessen berücksichtigen müssen.


Auch WhatsApp ist derzeit im Fokus der irischen Datenschutzaufsicht. Hier lautet der Vorwurf ebenfalls mangelnde Transparenz über die Verarbeitung von Nutzerdaten sowie fehlende Rechtsgrundlage für gezielte Werbung und Tracking. Auf ein bereits 2021 verhängtes Bußgeld in Höhe von 225 Millionen Euro folgte nun ein weiteres über 5,5 Millionen Euro. Aber nicht nur Meta steht am Pranger: Die französische Datenschutzaufsichtsbehörde CNIL hat gegen TikTok eine Strafzahlung von 5 Millionen Euro angeordnet. Ihrer Meinung nach ist es unzulässig, dass für Nutzer die Ablehnung von Cookies nicht so einfach wie die Zustimmung ist. Apple wurde schließlich für die Verwendung von Gerätedaten für personalisierte Werbung im App-Store durch die CNIL mit einem Bußgeld über 8 Millionen Euro belegt.

Unterdessen verhandelt der Europäische Gerichtshof im

Bußgeldverfahren gegen die Deutsche Wohnen über Grundsatzfragen der Verhängung von Strafen nach der DSGVO. Konkret geht es darum, ob bei Datenschutzverstößen durch Unternehmen die hierfür verantwortlichen Personen namentlich ermittelt werden müssen oder ob es ausreicht, dass ein Verstoß begangen wurde. Die Richter prüfen zudem, ob Verstöße einer Leitungsperson zuordenbar sein müssen. Während dies nach deutschem Recht erforderlich ist, sieht die DSGVO diese Voraussetzungen nicht vor. Das Verfahren ist entscheidend für die künftige Bußgeldpraxis in Deutschland. *Tobias Haar* (pst@ix.de)

## Internationale ISO-Norm 31700 zu Privacy by Design in Kraft getreten

Am 8. Februar 2023 ist die ISO 31700 in Kraft getreten. Sie beschreibt Datenschutzgrundsätze von Privacy by Design im Zyklus von Produkten und Dienstleistungen, die deren Anbieter künftig vom Beginn des Entwurfs über Entwicklung und Vermarktung berücksichtigen sollen. Der erste Teil des Standards beschreibt Prinzipien der datenschutzfreundlichen Produktgestaltung. Es geht dabei um Fragen des Designs von Nutzerschnittstellen und Datenhaltung, der Kommunikation mit Verbrauchern, Risikoassessments oder Tests der Datenschutzeinstellungen.

Beispiele im zweiten Teil der Norm sollen das Verständnis für diese Standards und deren Umsetzung anschaulich verdeutlichen. Die Einhaltung des ISO-Standards 31700 ist nicht verpflichtend. Allerdings tragen solche Standards zur Weiterentwicklung des Standes der Technik insgesamt bei, der auch bei Datenschutzverstößen eine Rolle spielt. Der Download der Norm auf den Webseiten der internationalen Organisation für Normung ist gebührenpflichtig und kostet etwa 300 Euro. Der Standard konkretisiert Art. 25 DSGVO, der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen festschreibt. *Tobias Haar* (pst@ix.de)

## BAG: Keine Pflicht zur Stechuhr im Homeoffice

Seit einem Beschluss des Bundesarbeitsgerichts zur Arbeitszeiterfassung durch den Arbeitgeber wird über dessen Auswirkungen auf Arbeitszeitmodelle wie Homeoffice diskutiert. Die Erfurter Richter hatten verbindlich festgestellt, dass Arbeitgeber verpflichtet sind, „Beginn und Ende der täglichen Arbeitszeit der Arbeitnehmer zu erfassen“. Die Präsidentin des Bundesarbeitsgerichts hat nun erklärt, dass das Urteil diese Vertrauensarbeitszeitmodelle nicht abschaffe. Unter anderem hatte der Branchenverband Bitkom zuvor Zweifel hieran geäußert.

Die BAG-Präsidentin Inken Gallner stellte zudem klar, dass durch die Gerichtsentscheidung keine Pflicht zur Einführung von Stechuhren entstanden sei. „Das Wie der Arbeitszeiterfassung liegt in den gestaltenden Händen des Gesetzgebers“, so Gallner. Flexible Arbeitszeitmodelle sollen durch den Beschluss nicht abgeschafft werden. Aber auch bei solchen müsse beispielsweise die elfstündige Ruhezeit eingehalten werden. Die grundsätzliche Pflicht zur Arbeitszeiterfassung besteht bereits. Zusätzlich kündigte das Bundesarbeitsministerium an, Details der Zeiterfassung durch ein entsprechendes Gesetz regeln zu wollen. Wann dieses vorliegen und in Kraft treten wird, ist derzeit unklar. *Tobias Haar* (pst@ix.de)

## EU untersucht Wettbewerbsverstöße durch Microsoft-Lizenzierungspraxis

Cispe lässt nicht locker: Die Vereinigung von Cloud-Infrastruktur-Anbietern in Europa hatte bereits im November 2022 eine Beschwerde bei der Generaldirektion Wettbewerb der EU-Kommission gegen Microsofts Bündelungspraxis von Softwareprodukten und Cloud-Services eingereicht. Jetzt legte der Verband noch einmal argumentativ nach.

Wissenschaftler der privaten Hochschulen Frankfurt School of

Finance und European School of Management and Technology (ESMT) durchleuchteten im Auftrag von Cispe die ökonomischen Konsequenzen der Bündelung. In der 18-seitigen Untersuchung kommen sie zu dem Schluss, dass Preiserhöhungen, weniger Wahlmöglichkeit und geringere Innovationstätigkeit drohen.

Hintergrund ist der Verdacht, dass Microsoft die marktbeherrschende Stellung von zum Beispiel Windows oder Office als Hebel nutzen will, um sich im Cloud-Umfeld Vorteile zu verschaffen. Mittel zum Zweck sind die Lizenzbedingungen. Danach dürfen Kunden eine bereits erworbene Software auf Ressourcen externer Rechenzentren einsetzen, soweit diese von Microsoft als autorisierte Outsourcer zertifiziert sind – Amazon AWS, Google und Microsofts Azure selbst zählen nicht zu diesem erlauchten Kreis.

Allerdings offeriert der Konzern laut Studie diverse Optionen, bestehende Lizenzen auch ohne oder nur mit geringen Zusatzkosten in Azure zu nutzen. Diese Optionen stehen für AWS oder Google so nicht zur Verfügung. Ihr Einsatz wäre folglich die kostspieligere Alternative zur Microsoft-Cloud, da in der Regel neue Lizenzen zu erwerben sind. *Achim Born* (pst@ix.de)

## EU-Studie deckt Rechtsverstöße durch Dark Patterns in Onlineshops auf

Eine groß angelegte Studie von EU-Kommission und Verbraucherschutzbehörden aus 23 Mitgliedstaaten sowie Norwegen und Island hat weitverbreitete Rechtsverstöße in Onlineshops dokumentiert. Demnach setzen deren Betreiber in fast 40 Prozent der Fälle manipulative Praktiken zum Täuschen von Nutzern ein. Insgesamt wurden knapp 1400 Onlineshops untersucht. Verbreitet setzten die Anbieter laut Studie falsche Countdown-Zähler mit Fristen für den Kauf bestimmter Produkte ein. Viele Shops versuchten, Kunden durch visuelle Gestaltung oder sprachliche Mittel zum Abschluss von Abonnements zu bewegen. Bei 70 Anbietern fehlten im Kaufprozess entscheidende Informationen oder diese wurden nur

versteckt zur Verfügung gestellt. Bemängelt wurden auch Zwangsregistrierungen und „virtuelle Drängel- und Gängeleien“.

Die Behörden wollen die gerügten Shopbetreiber zunächst auffordern, die Rechtsverstöße kurzfristig abzustellen. Kommen sie dem nicht nach, drohen formale Verfahren und Bußgelder. Der Bundesverband Onlinehandel kritisiert, dass mit der Studie weniger als ein Prozent aller Onlineshops überprüft wurde. Auch fehlten große Plattformen und Marktplätze. Durch das im Digital Services Act verschärfte Verbot von Dark Patterns und ähnlichen Methoden dürfte der Fokus auf solche Praktiken weiter zunehmen. Verstöße können mit Bußgeldern von bis zu 6 Prozent des Jahresumsatzes sehr teuer werden. *Tobias Haar* (pst@ix.de)

## USA und EU arbeiten an gemeinsamem KI-Rahmen

Eine Verwaltungsvereinbarung zwischen den USA und der EU soll die Kooperation im Bereich des Einsatzes von künstlicher Intelligenz fördern. Ziel sei es, bestimmte Prozesse per KI zu verbessern. Gemeint sind unter anderem die Katastrophenprävention durch Vorhersage von Extremwettersituationen, aber auch die Gesundheitsvorsorge oder die Energieversorgung. Im Fokus steht dabei die gemeinsame Nutzung der vorhandenen sowie die Erschließung neuer Datenbestände im Einklang mit den geltenden datenschutzrechtlichen Bestimmungen. Ziel ist ein KI-Modell mit jeweils in der EU und den USA liegenden Daten zur gemeinsamen Nutzung. *Tobias Haar* (pst@ix.de)

## Kurz notiert

Der Verbraucherzentrale Bundesverband hat neun **Telemedizin- und Arzttermin-Portale** wegen DSGVO-Verstößen abgemahnt. Die Datenverarbeitung sei intransparent und es fehlten Einwilligungen der Betroffenen.

Das Landesarbeitsgericht Köln sieht die Beweislast für den **Zugang einer E-Mail beim Absender.** Weder deren Absendung noch

das Fehlen einer Unzustellbarkeitsnachricht begründen einen rechtlich relevanten Anschein für den Zugang einer E-Mail.

Die Schweiz hat zum Jahresanfang die **EU-Drohnenreglementierung** übernommen. Für Drohnen ab 250 Gramm gilt nun eine Registrierungspflicht. Piloten müssen zudem eine Onlineschulung nachweisen.

Der europäische Datenschutzausschuss EDSA sieht mögliche Rechtsverstöße bei **Cookie-Bannern.** Neben einem Akzeptieren-Button müsste es regelmäßig einen entsprechenden Ablehnen-Button geben, heißt es im Positionspapier. Auch die grafische Darstellung der Banner genügt oft nicht den Datenschutzvorgaben.

## Markt + Trends | IT-Recht & Datenschutz

# IT-Defense 2023 – Visionen und düstere Prognosen

# IT-Defense 2023: Visionen und düstere Prognosen

Mikko Hyppönen von WithSecure legte in seiner Keynote mit dem Titel „Scorched Earth“ am zweiten Konferenztag bemerkenswerte Ansichten zur Zukunft der KI dar.

Von Jörg Riether

Auf der IT-Defense 2023 reflektierte zunächst der finnische Sicherheitsexperte und Autor Mikko Hyppönen über die Vergangenheit, in der 1997 IBMs Deep Blue den seinerzeit amtierenden Schachweltmeister Garry Kasparov schlug. In seinen Augen ist die KI-Vision seitdem und bis heute gleichermaßen großartig wie angsteinflößend. Die Geschwindigkeit entwickele sich rasant und allein in den letzten sechs Monaten sei hier mehr passiert als in den letzten 30 Jahren zusammen, so Hyppönen.

Er führte als Beispiele den Text-zu-Bild-Generator Stable Diffusion sowie die Textgeneratoren und Dialogsysteme ChatGPT und Bard an. Seine Prognose mutet unerhört an: Schon in naher Zukunft würden Computer bessere Kunst als Menschen erschaffen. Computer würden die besseren Poeten, die besseren Musiker, die besseren Programmierer und die besseren Maler sein, so Hyppönen. Das, was Computer dann produzieren, würde die Menschen tiefer und intensiver berühren als das, was ein Mensch jemals zustande bringen könnte. Er würde diese

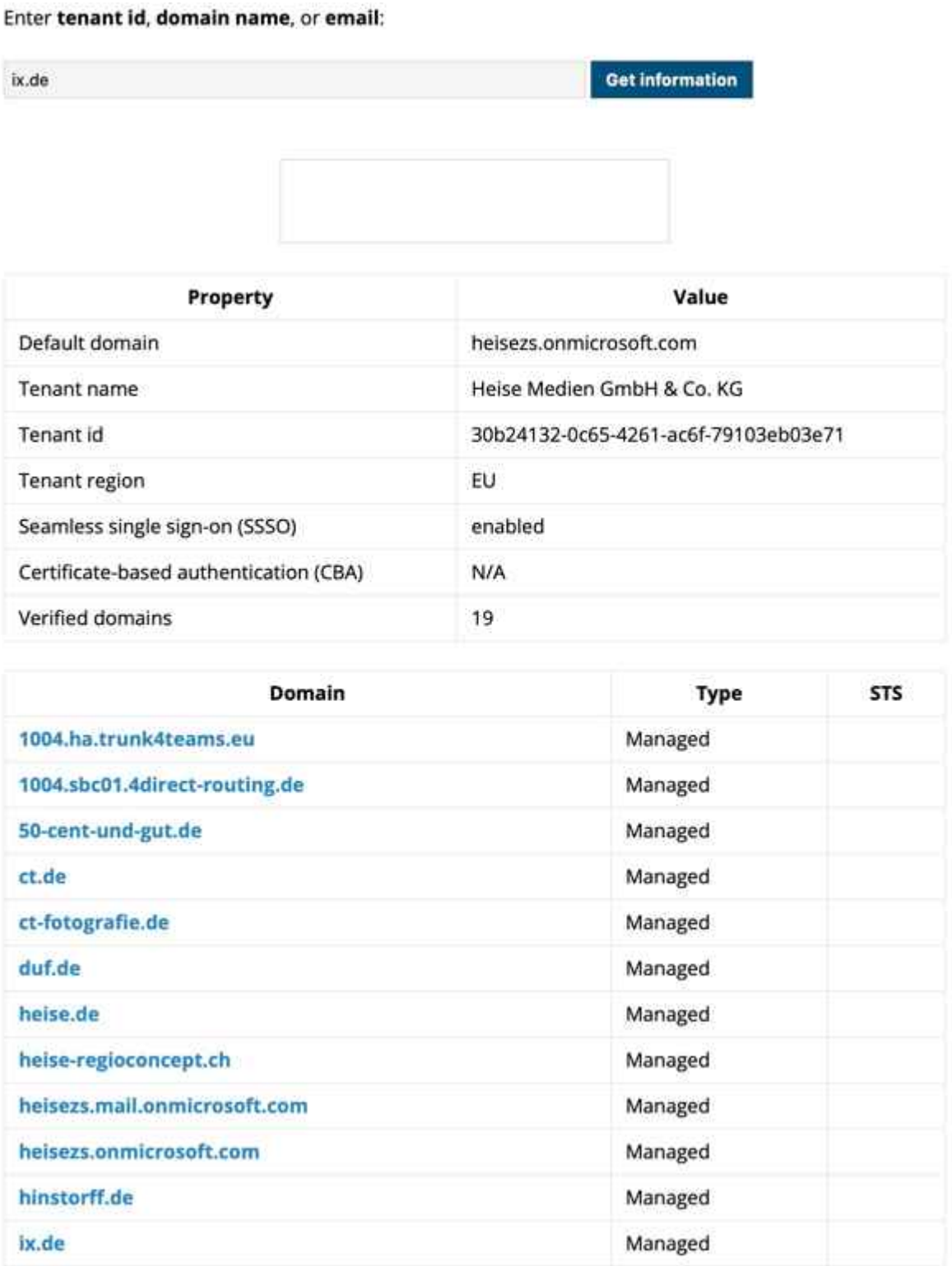
Vorstellung hassen. Es ändere aber nichts an der Realität und genau so werde es kommen, dies sei für ihn klar. Mehr noch: Wenn die Entwicklung so weitergehe wie aktuell, könnten Computer in 100 Jahren menschliche Intelligenz stimulieren.


Hyppönens radikale Zukunftsvision: Computer werden in fast allem besser als Menschen sein (Abb. 1).

## Gesprächige Tenants

Azure-AD- und Microsoft-365-Experte Nestori Syynimaa sprach über das Vertrauen in M365-Umgebungen. In diesem Zusammenhang stellte er seine eigenen Tools vor. Diese beinhalten neben diversen PowerShell-Abfragewerkzeugen auch ein Web-GUI (siehe ix.de/zyfa), das über öffentlich zugängliche Quellen zahlreiche Tenant-Informationen einsammeln kann. Dass diese durchaus detailliert sein können, zeigt ein Versuch des Autors mit der Domain ix.de (Abbildung 2).

Es offenbart sich auf einen schnellen Klick, dass ix.de zur M365-Standarddomain heisezs.onmicrosoft.com gehört, die in der EU-Region beheimatet ist, außerdem gibt es im Tenant 19 verifizierte Domänen. Darunter gibt es auch Einträge wie „1004.ha.trunk4teams.eu“, „50-cent-und-gut.de“ sowie „heisezs.mail.onmicrosoft.com“. Die Seamless-Single-Sign-on-Technik (SSSO) ist aktiviert und zertifikatbasierte Authentifizierung (Certificate-based Authentication, CBA) ist nicht vorhanden, dies kann man mit einer gültigen Mailadresse optional prüfen.




Nestori Syynimaas Werkzeuge haben es in sich und können sowohl zur Informationssammlung in M365-Umgebungen, wie hier bei ix.de, als auch aktiv-offensiv benutzt werden (Abb. 2).
Dieses Beispiel ist noch relativ harmlos. Spannend ist, dass all diese Informationen „per Design“ öffentlich verfügbar sind. Es lohnt sich, mit dem Werkzeug selbst ein wenig mit der eigenen Unternehmensdomain oder anderen bekannten Domains zu spielen. Man könnte das Tool auch dazu missbrauchen, valide

Mailadressen herauszufinden. So gab das Web-GUI im Test bei einer vermutlich gültigen Microsoft-Mailadresse aktivierte CBA an, während es bei einer erfundenen Mailadresse aus vielen zufälligen Zeichen „nicht vorhanden“ ausgab. Es lassen sich also möglicherweise mehr Informationen ableiten, als dem einen oder anderen Unternehmen lieb sein könnte.

Auch die PowerShell-Werkzeuge sind mächtig. Neben der passiven Informationsbeschaffung gibt es hier sogar ein Phishingmodul, mit dem man live einen Angriff durchführen kann, der einen bei Erfolg direkt ins Outlook Web Access des Opfers führt. Syynimaa macht sich hier die Azure Device Code Authentication zunutze (siehe ix.de/zyfa).

## Aus dem Tesla-Nähkästchen

Der IT-Sicherheitsforscher Martin Herfurt stellte in seinem Vortrag Details zum Projekt TEMPA vor, das Werkzeuge und Details zum proprietären VCSEC-Protokoll bereitstellt. Gewonnen hat er diese Informationen durch Analyse der dekompilierten offiziellen Tesla-Android-Anwendung – und konnte so Einblicke in die Angreifbarkeit des Protokolls und damit des Fahrzeugs erhalten (mehr Details siehe ix.de/zyfa).

Herfurt berichtete, dass er die Relay-Verwundbarkeiten, über die mit zwei Raspberry Pis und Telefonen ein Tesla entwendet werden konnte (siehe ix.de/zyfa), an den Hersteller gemeldet hatte. Tesla ließ verlauten, dass man dies nicht ändern werde und die Kunden doch bitte PIN2Drive einsetzen sollen, also eine zusätzliche PIN-Abfrage, bevor man das Fahrzeug starten kann. Dazu rät auch Herfurt, denn leider seien die Relay-Angriffe auf Teslas immer noch sehr einfach möglich. (ur@ix.de)

## IT-Defense 2023: Visionen und düstere Prognosen

Mikko Hyppönen von WithSecure legte in seiner Keynote mit dem Titel „Scorched Earth“ am zweiten Konferenztag bemerkenswerte Ansichten zur Zukunft der KI dar.

---

# Kurz notiert – März 2023

## Kurz notiert

Die Linux Foundation hat mit der **Open Metaverse Foundation** eine neue Unterorganisation gegründet. Die Stiftung soll Standards für ein herstellerneutrales Metaverse entwickeln.

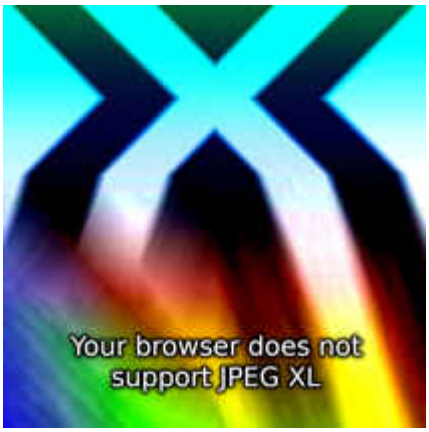
Die **Abmahnwelle wegen Google Fonts** hat in Österreich Schäden von mehr als 5 Millionen Euro verursacht. Darauf deutet die Einschaltung der Wirtschaftsstaatsanwaltschaft (WKSta) hin, die erst ab diesem Betrag aktiv wird.

Das **World Wide Web Consortium (W3C)** hat seine Umwandlung in eine gemeinnützige Non-Profit-Organisation abgeschlossen. Zuvor war das Konsortium ein Zusammenschluss von Bildungs- und Forschungseinrichtungen ohne eigenen Rechtsstatus.

Bei der aktuellen Firefox-Version 109 hat Mozilla die wegen Einschränkungen für Adblocker umstrittene **Plug-in-Schnittstelle Manifest V3** als Standard aktiviert. Manifest V2 ist aber noch vorhanden und wird von Mozilla unterstützt.

## Mozilla Firefox: JPEG XL muss draußen bleiben

**Wie bereits Chrome soll auch Firefox das Grafikformat JPEG XL nicht unterstützen. Mozilla hält dies nicht für notwendig, da es im Vergleich zu anderen Formaten zu wenig Vorteile biete.**




Firefox wird das vielseitige und ressourcensparende Grafikformat JPEG XL in absehbarer Zeit nicht darstellen. Das gab Mozillas Distinguished Engineer Martin Thomas auf der GitHub-Seite des Projekts bekannt. Man sei gegenüber dem Format „neutral“ – was bedeute, dass man es in stabilen Firefox-Versionen nicht erlaube, auch nicht optional, obwohl dies technisch mit wenig Aufwand möglich ist.

Mozilla unterstütze neue Formate nur, wenn sie Bedürfnisse der Nutzer und Websitebetreiber adressieren, so Thomas. JPEG XL

habe zwar einige potenzielle Vorteile, sei aber gegenüber Mitbewerbern wie AVIF nicht so viel performanter und vielseitiger, dass es die Aufnahme in den Browser rechtfertige. Damit übernimmt Thomas das Argument, das bereits führende Chrome-Entwickler ins Feld führten. Google hatte sich im Herbst 2022 dagegen entschieden, das Format in seine Browser-Engine aufzunehmen.

Befürworter argumentieren damit, dass JPEG XL die bessere Alternative sowohl für klassische Pixel-Formate wie JPEG und PNG als auch für die von Videocodecs abstammenden animationsfähigen Standards wie WebP oder AVIF sei. Auch hatten sich in der Vergangenheit Unternehmen wie Intel, Adobe, Meta oder Shopify hinter das Format gestellt. Bisher können bei den Browsern nur Nischenprodukte JPEG-XL-Dateien anzeigen, darunter Firefox-Derivate wie Waterfox oder Pale Moon. (ulw@ix.de)

## Browser-Engine Servo mit neuer Finanzierung nach langer Pause wiederbelebt

Nach über zwei Jahren ohne nennenswerte Aktivitäten hat das Entwicklerteam der Browser-Engine Servo die Arbeit wieder aufgenommen. In einem Blogbeitrag kündigten die Entwickler eine neue externe Finanzierung an, die die Fortführung ermögliche – ohne jedoch die Geldgeber zu nennen. Bereits im Dezember hatte die Entwicklergenossenschaft Igalia bekannt gegeben, dass sich vier ihrer Mitarbeiter künftig der Weiterentwicklung von Servo widmen werden. Bei Igalia arbeiten renommierte Browserspezialisten, die zu den verbreiteten Engines Chromium und WebKit wichtige Beiträge leisten.

Servo ist eine in Rust implementierte Browser-Engine, die 2012 als Mozilla-Projekt an den Start ging. Sie sollte im Rahmen des Projekts Quantum in Firefox integriert werden, dazu kam es jedoch nie. 2020 wanderte Servo in der Folge einer Entlassungswelle bei Mozilla zur Linux Foundation, aber auch dort schlief die Aktivität bald wieder ein.

Jetzt gibt es eine neue Roadmap für 2023. In diesem Jahr sollen neben Aufräumarbeiten bei den Dependencies das Layoutsystem und die Umsetzung von CSS2 im Fokus stehen. (ulw@ix.de)

## Malvertising-Welle bei Google-Suchen

Mehrere Sicherheitsforscher beobachten einen starken Anstieg von Malvertising über Google Ads. Immer mehr der bei Google-Suchen eingeblendeten Anzeigen verlinkten auf Schadsoftware statt auf beliebte Programme wie Adobe Reader, Slack, Gimp oder Thunderbird. Securityexperten bei Spamhaus vermuten, dass eine Cybercrime-Gruppe damit begonnen hat, Malvertising als Service zu vermarkten. Ein Hinweis darauf sei unter anderem, dass bei gleichlautenden Suchbegriffen Links auf unterschiedliche Schädlinge auftauchen.

Die Securityfirma SentinelOne hat eine Malware-Kampagne identifiziert, die auf bösartige Loader für .NET verlinkt. Am häufigsten versuchen die Angreifer derzeit, XLoader zu installieren, einen Nachfolger von FormBook, der Passwörter, Kontaktdaten und andere sensible Informationen stiehlt. (ulw@ix.de)

## Chrome-Updates nur noch ab Windows 10

Mit dem Erscheinen von Chrome in Version 110 bekommen die Versionen für Windows 7, 8 und Windows Server 2012 keine Sicherheitsupdates mehr. Microsoft hat den erweiterten Support für diese Betriebssysteme bereits ab Januar eingestellt. In Chrome 110 hat Google 15 Sicherheitslücken geschlossen, drei davon mit Risikoeinstufung „hoch“.

Mit Version 110 von Chrome kommt es zu einer Änderung im Releasezyklus. Künftig gibt es für ausgewählte Nutzer eine Early-Stable-Version, die eine Woche vor dem eigentlichen stabilen Release erscheint. Google will damit in der Lage sein, noch vor dem Veröffentlichen der stabilen Version auf Probleme bei Anwendern zu reagieren. (ulw@ix.de)

**Markt + Trends | World Wide Web**

---

# Cybervorfälle-Top-Gefahren für Unternehmen

Im neuen Allianz-Risk-Barometer 2023 (ix.de/zh1v) belegen wie im vergangenen Jahr Cybervorfälle und Betriebsunterbrechungen die ersten beiden Plätze der **Top-Gefahren für Unternehmen.**

*ix.de/zh1v*

- **Vollständiges Programm der Kongressmesse SecIT**
- **Allianz-Risk-Barometer 2023**
- **Wissenschaftscomics von CASA**
- **BSI-Grundschutzkompendium**
- **WithSecure-Forschungsbericht „Creatively malicious prompt engineering“**
- **heise-Artikel zu ChatGPT-Versuchen von WithSecure**
- **Pressemitteilung Check Point zum Umgehen der Zugangsbeschränkungen von ChatGPT**
- **Pressemitteilung von Sophos zur Jagd nach Cyberkriminellen mit ChatGPT**

---

# ChatGPT und Co.-KI als Gamechanger für Gut und Böse?

## ChatGPT und Co.: KI als Gamechanger für Gut und Böse?

**Seit Veröffentlichung des smarten Chatbots von OpenAI überschlagen sich die Meldungen, was man damit alles machen kann – aber auch die Warnungen, gerade in Sachen IT-Sicherheit.**

Sicherheitsforscher von Check Point hatten kürzlich den ersten durch ChatGPT erstellten Angriffscode im Darkweb entdeckt (siehe auch iX 2/2023, Seite 20). Nun gibt es weitere Erkenntnisse: In Untergrundforen tauschten sich russische Kriminelle darüber aus, wie sie die von OpenAI für Russland vorgesehenen Beschränkungen – Kontrolle von IP-Adressen, Zahlkarten und Telefonnummern – umgehen können. Die Forscher stießen auf Nachfragen, wie man mit gestohlenen Zahlkarten an

einen leistungsfähigeren OpenAI-Account gelangt, außerdem auf zahlreiche halblegale russische Online-SMS-Dienste, die Anleitungen zum Registrieren bei ChatGPT geben.

Auch Sicherheitsexperten von WithSecure loteten die kriminelle KI-Kompetenz aus und ließen das Sprachverarbeitungsmodell GPT-3 in verschiedenen Bereichen wie Fake News, Social Media und Phishingmails agieren. Voraussetzung für die in der Regel gut lesbaren und glaubwürdigen Texte ist laut Ergebnisbericht (siehe ix.de/zh1v) ein präzises Briefing der KI. Wie bei echten Kriminellen wird eine maßgeschneiderte Spear-Phishing-Mail umso glaubwürdiger, je mehr Details über den Mitarbeiter, das Unternehmen und den Kontext bekannt sind.

Einen Gamechanger nicht nur für die dunkle Seite sieht das Sicherheitsunternehmen Sophos: Auch für die Jagd nach Cyberkriminellen entfalten die neuen KI-Tools Potenzial. So ließ sich GPT-3 per „Few-Shot Learning“ mit nur wenigen kommentierten Beispielen für Erkennung trainieren und wies nicht die Schwächen herkömmlicher maschineller Lernmodelle der Überanpassung und dadurch fehlender Verallgemeinerungen auf (Details siehe ix.de/zh1v). Einsetzen lässt sich das Werkzeug laut Sophos vor allem in der Spamerkennung und beim Reverse Engineering von Befehlszeilen, bei dem es eine Befehlszeile in eine verständliche Beschreibung übersetzen kann. In den Augen der Sophos-Forscher ist GPT-3 „ein Meilenstein für die Cybersicherheit“. (ur@ix.de)

---

# Das BSI hat den Entwurf des Mindeststandards zur

# Protokollierung und Detektion von Cyberangriffen Version 1.0a.4 als Community Draft veröffentlicht

Das BSI hat den Entwurf des Mindeststandards zur **Protokollierung und Detektion von Cyberangriffen** Version 1.0a.4 als Community Draft veröffentlicht (siehe ix.de/zwq6).

*ix.de/zwq6*

- **Sicherheitslücke in MatrixSSL**
- **Informationen der Telekom-Forscher**
- **Report von Atlas VPN**
- **Blogartikel von Checkpoint, wie Kriminelle GPT missbrauchen können**
- **Blogartikel von Checkpoit zu ersten Fällen des Missbrauchs von ChatGPT**
- **BSI Community Draft**
- **LKA-Warnung vor gefälschten Domain-Rechnungen**
- **Google OSV Scanner**

---

# gefälschten Domain-Rechnungen von D.D.N. Hosting.

Zum Jahreswechsel kommt es laut LKA Niedersachsen verstärkt zu **gefälschten Domain-Rechnungen** von D.D.N. Hosting. Ein

Beispielschreiben findet sich auf der LKA-Seite.

(siehe ix.de/zwq6)

*ix.de/zwq6*

- **Sicherheitslücke in MatrixSSL**
- **Informationen der Telekom-Forscher**
- **Report von Atlas VPN**
- **Blogartikel von Checkpoint, wie Kriminelle GPT missbrauchen können**
- **Blogartikel von Checkpoit zu ersten Fällen des Missbrauchs von ChatGPT**
- **BSI Community Draft**
- **LKA-Warnung vor gefälschten Domain-Rechnungen**
- **Google OSV Scanner**

---

# Hacking-Tools-Werkzeuge für Experten-2021

## Gute Tools, böse Tools

# Hacking-Werkzeug für Fortgeschrittene

Mit den Hacking-Tools von Penetrationtestern finden Sie Sicherheitslücken in Ihren Websites, Netzwerken und

Anwendungen, bevor es andere tun.

Von Ronald Eikenberg und Alexander Königstein

Hollywood weiß Hacker-Aktivitäten in Szene zu setzen: Vor unzähligen Monitoren mit monochromatischen Benutzeroberflächen sitzen Gestalten im Kapuzenpulli und brechen durch die Firewalls. In der Realität geht es weitaus nüchterner zu, denn die eigentliche Action spielt sich hinter den Kulissen ab. Das ist aber nicht weniger faszinierend, denn Hacking-Tools leisten erstaunliche Dinge, wenn man sie richtig einsetzt. Das setzt etwas Wissen und Erfahrung voraus, doch beides baut sich ganz von selbst auf, wenn Sie erst mal Feuer gefangen haben. In diesem Artikel stellen wir eine Auswahl interessanter Profi-Werkzeuge vor, die sowohl auf der dunklen als auch auf der hellen Seite der Macht genutzt werden. Stöbern Sie auch im Artikel „Hack Dich selbst“ auf Seite 18, der nützliche Problemlöser für den Alltag präsentiert.

Mit den im Folgenden vorgestellten Profi-Tools spüren Sie Sicherheitslücken in Ihren Websites, Netzwerken, Apps, IoT-Geräten und vielem mehr auf. Anschließend können Sie gezielt Schutzmaßnahmen ergreifen und die Schlupflöcher stopfen, bevor es zu spät ist. Die meisten Hacking-Tools laufen am besten oder ausschließlich unter dem Betriebssystem Linux. Eine gute Grundlage für die ersten Schritte ist **Kali Linux**, das von Haus aus bestens auf die Bedürfnisse von Hackern zugeschnitten ist. Auf Seite 30 erfahren Sie, wie Sie sich einen Kali-USB-Stick mit persistenter Datenpartition für Ihre Experimente erstellen. Download-Links und weiterführende Informationen zu allen vorgestellten Tools finden Sie online unter ct.de/ygg5. Aber genug der Vorrede – jetzt geht es in die Vollen!

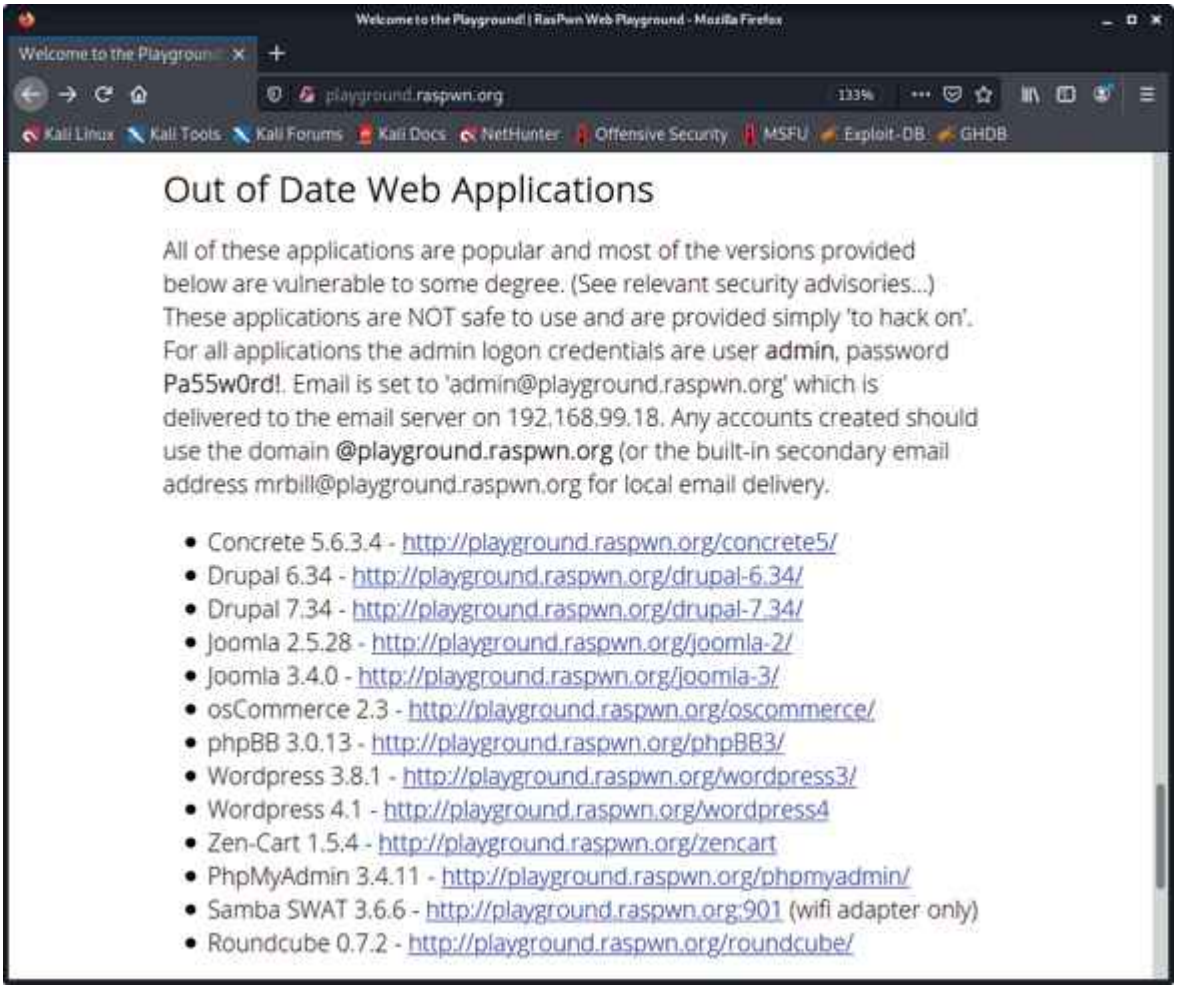
## Angreifen erlaubt

Die hier genannten Hacking-Tools sind nicht illegal, aber natürlich dürfen Sie damit nicht gegen geltende Gesetze verstoßen (siehe Seite 170). Damit Sie gar nicht erst in

Versuchung kommen, die Tools unerlaubt an fremden Servern zu testen, sollten Sie sich eine geeignete Übungsumgebung schaffen – zum Beispiel ein Testnetz, in dem sich ausschließlich Systeme befinden, die Sie attackieren möchten und dürfen.

Ein geeignetes Angriffsziel ist **RasPwn**, das ein ganzes Netzwerk voller verwundbarer Server simuliert, an denen Sie sich austoben können. Sie übertragen es einfach auf eine MicroSD-Karte, die Sie anschließend in einen Raspi-Kleincomputer stecken (mindestens Raspi 2B). Nach dem Booten meldet sich ein WLAN namens „RasPwn OS“, zu dem Sie mit dem Passwort „In53cur3!“ eine Verbindung herstellen. Aus dem Netz öffnen Sie http://playground.raspwn.org mit einem Browser Ihrer Wahl, wo Sie mit allen wichtigen Informationen über das virtuelle Netzwerk und die angreifbaren Server versorgt werden. Ein Netzwerkkabel darf nicht mit dem Raspi verbunden sein, andernfalls hat das hochgradig verwundbare Image unter Umständen Zugriff auf Ihr Hauptnetzwerk und das Internet – was Sie tunlichst vermeiden sollten.

Zu den möglichen Angriffszielen zählen verwundbare WordPress-Installationen, eine steinalte Version des Webshop-Systems osCommerce, das Datenbank-Tool phpMyAdmin, ein Mailserver, Samba und so weiter. Auch das Debian-Linux, auf dem RasPwn basiert, hat schon fast sieben Jahre auf dem Buckel und ist so löchrig wie ein Schweizer Käse. Obendrauf gibt es zahlreiche Web-Applikationen wie OWASP Bricks und Damn Vulnerable Web Application (DVWA), die nur mit dem Ziel entwickelt wurden, möglichst verwundbar zu sein, um typische Sicherheitslücken am lebenden Objekt zu demonstrieren. Viele dieser Projekte sind online dokumentiert, wodurch sie sich hervorragend zum Lernen eignen (siehe ct.de/ygg5).



Das Raspi-Image RasPwn enthält etliche verwundbare Web-Apps – und das mit voller Absicht.

## Netzwerk auskundschaften

Hat sich ein Angreifer Zugriff auf ein fremdes Netzwerk verschafft, etwa durch eine frei zugängliche Netzwerkbuchse im Aufenthaltsraum, eine per E-Mail eingeschleuste Malware oder ein schwaches WLAN-Passwort, dann wird er sich erst mal einen Überblick über die Geräte im Netz verschaffen, um mögliche Angriffsziele auszumachen. Hierbei ist der mächtige Netzwerkscanner **Nmap** (Network Mapper) die erste Wahl. Er spürt nicht nur die Rechner, Drucker, NAS, Server, Router und vieles mehr auf, sondern auch die darauf laufenden Dienste. Durch Skripte lässt sich der Scanner beliebig erweitern, etwa um die entdeckten Clients gleich noch auf Sicherheitslücken abzuklopfen. Das alles ist nützlich, um verwundbare Geräte im eigenen Netz aufzuspüren und sie anschließend entweder abzusichern oder aus dem Verkehr zu ziehen.

Nmap läuft auf Linux, macOS und Windows, bei Kali Linux ist er inklusive. Wenn Sie auf einer Shell nmap ohne Parameter eintippen, zeigt das Tool die wichtigsten Betriebsmodi an. Um einfach und schnell die offenen Ports eines bestimmten Hosts herauszufinden, hängen Sie einfach dessen IP-Adresse an den Befehl an, etwa nmap 192.168.178.1. Das müssen Sie zwar nicht als root ausführen, es lohnt sich aber: So finden Sie mehr über die Clients heraus, im konkreten Fall die MAC-Adressen. IPv6-Adressen scannen Sie mit dem Parameter -6.

Sie können den Scan auf einen IP-Bereich ausweiten, den Sie zum Beispiel mit 192.168.178.1-50 definieren (alle IP-Adressen, die mit 192.168.178 anfangen und mit .1 bis .50 enden). Oder Sie scannen gleich das gesamte /24-Subnetz (alle bis .255): nmap 192.168.178.0/24. Ist der Scan abgeschlossen, präsentiert Ihnen Nmap die Ergebnisse auf der Shell, vorher lässt das Tool nicht von sich hören. Wer ungeduldig ist, kann mit --stats-every 10s festlegen, dass Nmap regelmäßig ein Statusupdate ausgibt.

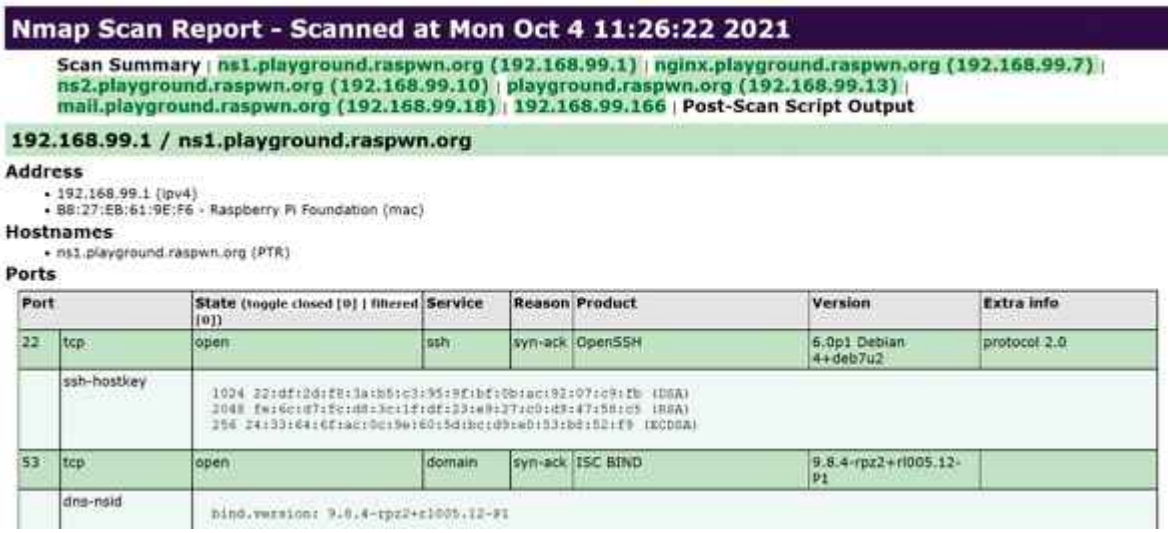
Wirklich komfortabel lesbar ist der Bericht auf der Shell nicht. Sie können jedoch leicht einen formatierten HTML-Report erstellen, indem Sie zunächst Nmap mit -oX ergebnis.xml anweisen, einen XML-Export der Ergebnisse zu schreiben. Anschließend bauen Sie daraus mit dem unter Kali vorinstallierten Tool xsltproc eine HTML-Datei, die Sie mit jedem Browser öffnen können: xsltproc ergebnis.xml -o ergebnis.html

Mit dem einfachen Scan kratzen Sie erst an der Oberfläche der Möglichkeiten. Mehr können Sie Nmap über verschiedene Scan-Optionen entlocken (siehe ct.de/ygg5). Sehr umfangreich ist der Modus -A, der unter anderem die Betriebssystem- und Versionserkennung (Fingerprinting) scharf schaltet. Diesen Modus sollten Sie mit sudo starten, damit Ihnen nichts entgeht. Aber aufgepasst: Nmap greift in diesem Fall aktiv auf die entdeckten Server zu, um Informationen einzuholen. Das kann zu unerwarteten Effekten führen, unser Epson-Drucker etwa

spuckt bei jedem Scan eine spärlich bedruckte Seite aus. Sie sollten Ihre ersten Schritte daher besser im oben erwähnten Testnetz machen.

Hardcore

Eine Übersicht über die mitgelieferten Skripte finden Sie in der Dokumentation von Nmap (siehe ct.de/ygg5). Praktisch ist etwa das vulners-Skript, das zu den ermittelten Serverversionen bekannte Schwachstellen aus einer Online-Datenbank heraussucht. Eigene Skripte können Sie in der Programmiersprache Lua entwickeln.

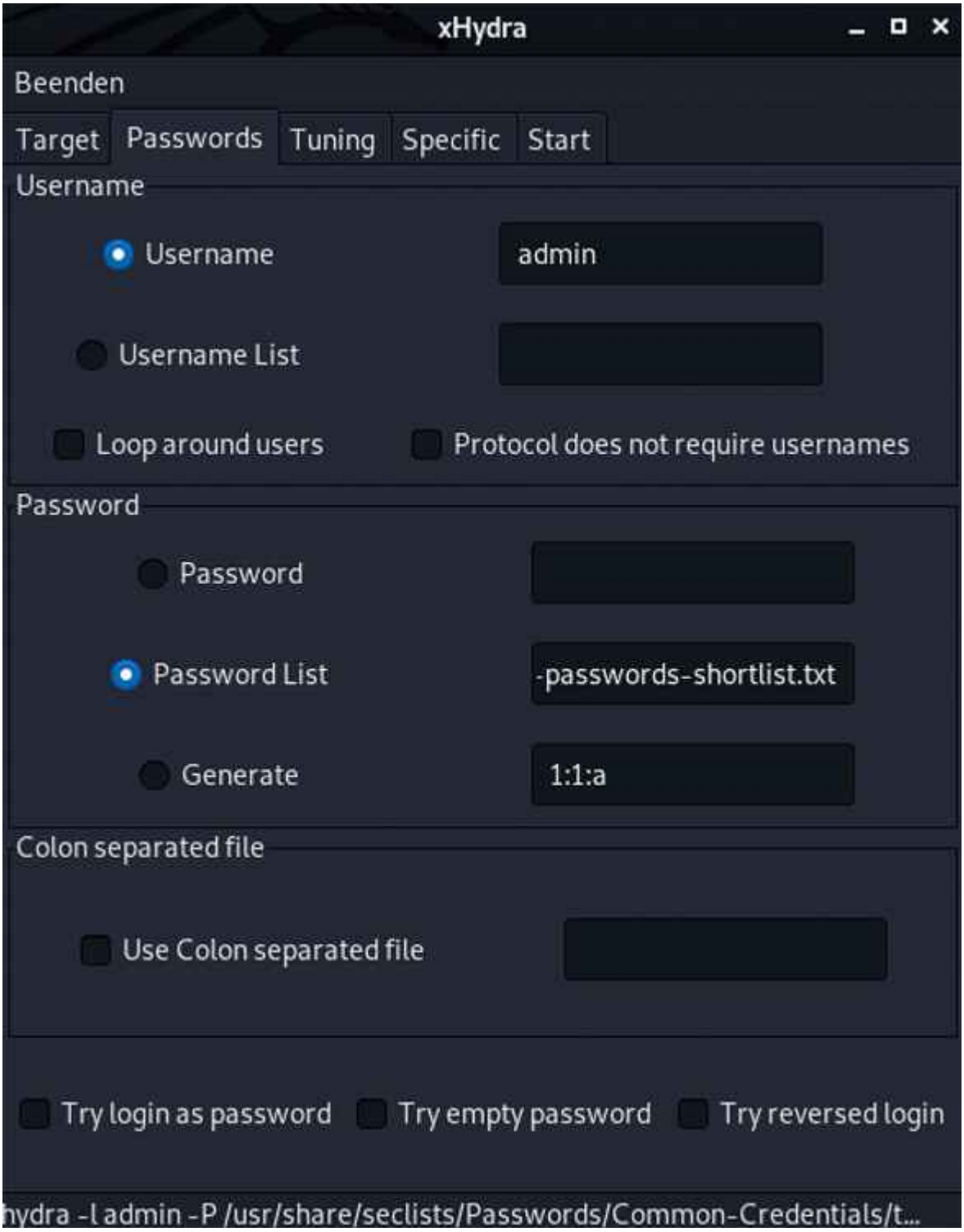


Was ist los im Netz? Der Netzwerkscanner Nmap liefert einen HTML-Bericht über alle Geräte und Dienste.

## Zugriff auf Server

Vernetzte Geräte wie WLAN-Kameras oder Smart-Home-Komponenten sind oft für eine Überraschung gut: Auf manchen Exemplaren laufen unerwartete Dienste, die im Worst Case sogar mit einem Standardpasswort für Gott und die Welt aus dem Internet erreichbar sind. Die entdecken Sie zum Beispiel mit einem Nmap-Scan (siehe „Netzwerk auskundschaften“). Doch dann stehen Sie erst mal vor verschlossener Tür, denn das Zugriffspasswort ist häufig ebenso wenig dokumentiert wie der Dienst selbst. Solche Dienste sind ein unkalkulierbares Sicherheitsrisiko.

Fehlt Ihnen das Passwort, können Sie versuchen, es zu erraten – oder Sie überlassen dem Login-Cracker **Hydra** die ganze Arbeit. Er unterstützt viele gängige Protokolle wie FTP, HTTP(S), SMB, SSH, Telnet und VNC, wodurch er universell einsetzbar ist. Sie können Hydra wahlweise auf der Shell benutzen oder mit xHydra eine grafische Oberfläche starten, um ein paar Parameter einzustellen und die Passwortsuche zu starten. Wichtig sind das Ziel, der Port und das richtige Protokoll im ersten Tab. Danach folgt die Konfiguration des Nutzernamens und einer Passwortliste. Falls Sie gerade keine zur Hand haben, können Sie unter Kali das Paket seclists installieren, das diverse Listen unter /usr/share/seclists/Passwords ablegt. Im letzten Tab ist der Output des Tools zu sehen, also im besten Fall das gesuchte Passwort.




Sesam, öffne Dich: Hydra probiert, sich mit beliebig langen Passwortlisten bei einem Server einzuloggen.

## IPv4-Traffic umleiten

ARP-Spoofing (auch ARP-Poisoning genannt) ist ein alter, aber nach wie vor effektiver Trick, um IPv4-Netzwerkverkehr umzulenken. Ein Angreifer im gleichen Netzwerk kann so den Datenverkehr anderer Teilnehmer ohne deren Zutun mitlesen und

manipulieren, etwa um sensible Daten abzugreifen oder Schadcode zu verbreiten. Das Ziel des Angriffs sind die ARP-Tabellen der Netzwerkclients. Darin ist vermerkt, unter welchen MAC-Adressen die IPs im lokalen Netz erreichbar sind. Durch gefälschte Nachrichten im Address Resolution Protocol (ARP) kann ein Angreifer die Tabellen verändern und Traffic umleiten, mitlesen und manipulieren. Eine solche Umleitung ist aber auch praktisch, um den Netzwerkverkehr einzelner Clients zu untersuchen, zum Beispiel, um herauszufinden, mit welchen Servern ein Smart-Home-Gerät spricht und ob die übertragenen Daten verschlüsselt sind.

Mit dem Sniffing-Tool **Ettercap** ist ARP-Spoofing sehr einfach, weil es alle nötigen Schritte vereint. Kali-Nutzer starten es über den Launcher („Sniffing & Spoofing/ettercap-graphical“). Wählen Sie zunächst das gewünschte Netzwerk-Interface. Anschließend müssen Sie noch die beiden IPs einstellen, zwischen denen Sie lauschen möchten, zum Beispiel Router-IP und die IP des Clients, für den Sie sich interessieren. Klicken Sie hierzu auf den Menüknopf (drei Punkte), „Targets“ und „Current Targets“. Über die Add-Buttons tragen Sie die IPs als Target 1 und 2 ein. Alternativ können Sie auch erst mal im lokalen Netz nach Clients scannen. Klicken Sie dafür im Menü unter „Hosts“ auf „Scan for hosts“. Kurz darauf können Sie die Netzwerkteilnehmer unter „Hosts/Host list“ einsehen und per Rechtsklick als Target hinzufügen.


Verkehrsumleitung: Ettercap nutzt ARP-Spoofing, um den Datenverkehr anderer Rechner über sich umzuleiten.
Jetzt müssen Sie das ARP-Spoofing nur noch auslösen: Klicken Sie oben rechts auf den Knopf, der an eine Weltkugel erinnert („MITM menu“) und auf „Arp poisoning…“. Über das Menü und „View/Connections“ können Sie live beobachten, wie die Daten durch Ihr System fließen. Sie erfahren dort unter anderem IP-Adresse, Hostname und Land der Gegenstelle, den genutzten Port und den Datenumfang. Ein Doppelklick auf eine Verbindung zeigt die übertragenen Daten an. Interessant sind zum Beispiel unverschlüsselte HTTP-Verbindungen auf Port 80, weil Sie deren Inhalt ohne weitere Hilfsmittel als Klartext lesen können.

Ettercap bringt einige interessante Plug-ins mit, die Sie im Menü unter „Plugins/Manage plugins“ durchstöbern und per Doppelklick aktivieren können. Darunter findet sich auch ein Gegengift für ARP-Spoofing: Der „arp_cop“ soll ARP-Manipulationen anzeigen. Wenn Ihnen die Analysefunktionen von Ettercap nicht ausreichen, können Sie Werkzeuge wie Wireshark nutzen, denn der angezapfte Traffic ist auf dem anfangs eingestellten Netzwerk-Interface sichtbar. Mit den Linux-Werkzeugen iptables oder nftables können Sie den Datenverkehr

zudem beliebig umleiten, zum Beispiel an einen lokalen Server.

## WLAN auf dem Prüfstand

Funknetzwerke müssen viel aushalten, denn jeder in Reichweite kann sie attackieren. Wenn Sie sich nicht darauf verlassen möchten, dass Ihr WLAN schon sicher genug sein wird, können Sie mit Hacking-Tools die Probe aufs Exempel machen. Kali hat mehrere davon an Bord, die unterschiedliche Angriffsszenarien durchspielen. Zur Nutzung benötigen Sie ein WLAN-Interface, das sich in den „Monitor Mode“ schalten lässt und zudem gut von Linux unterstützt wird. Solche gibt es als USB-WLAN-Adapter schon für weniger als 20 Euro, zum Beispiel von CSL Computer (Modell 27395) oder Alfa Network. Ob Ihr Interface den nötigen Modus unterstützt, erfahren Sie über eine Google-Suche nach dem Chipsatz, etwa „Ralink RT5572 monitor mode“.

Um die gängigsten Angriffsarten zu simulieren, können Sie zu **wifite2** greifen, das diverse WLAN-Hacking-Werkzeuge für Sie ansteuert, um Sicherheitsprobleme aufzuspüren. Sie starten es wie folgt:

```
sudo wifite --random-mac --kill
```

Die Option --random-mac sorgt dafür, dass die genutzte Geräteadresse des WLAN-Adapters zufällig ausgewürfelt wird und --kill beendet störende Prozesse, die dem Tool in die Quere kommen könnten. Wifite fragt Sie zunächst, welches WLAN-Interface genutzt werden soll und macht sich anschließend sofort an die Arbeit. Kurz darauf listet es alle Netze in Reichweite auf.


Mit wifite2 finden Sie heraus, wie sicher Ihr WLAN wirklich ist. Im ersten Schritt zeigt es alle Netze in Reichweite samt Verschlüsselung und WPS-Status an.
Sobald Sie Ihr WLAN gefunden haben, beenden Sie den Scan mit Strg+C und geben die Indexzahl des Netzes ein. Wifite testet anschließend die wichtigsten Angriffsmöglichkeiten der Reihe nach durch, allen voran WPS-Attacken (Pixie Dust und Brute Force auf die PIN), die bei anfälligen Routern am schnellsten zum Ziel führen. Danach nimmt sich das Tool WPA(2) zur Brust und schließlich das steinalte WEP-Verfahren. Gegen WPA3 kommt es derzeit nicht an.

Der WPA(2)-Angriff läuf relativ simpel ab: Zunächst zwingt wifite die Clients per Deauthentication-Paket, die Verbindung zum Router zu trennen. Bei der anschließenden Neuanmeldung zeichnet es den Handshake auf und setzt anschließend den Passwort-Cracker hashcat darauf an. Der probiert eine Reihe von Passwörtern aus einer langen Liste durch, bis er fündig wird. Die wichtigsten Schutzmaßnahmen in aller Kürze: Nutzen Sie lange WPA-Passwörter (mindestens 16 Zeichen, besser mehr), aktivieren Sie möglichst WPA2/3 (Mixed Mode) und die geschützte Anmeldung von WLAN-Geräten (Protected Management Frames, PMF).

# Datenlecks im Webserver finden

Webserver sind prinzipbedingt meist für jeden erreichbar – und damit zwangsläufig auch für Angreifer, die nach Sicherheitslücken, Datenlecks und schwachen Passwörtern suchen. Das geschieht längst nicht mehr mühsam von Hand, sondern automatisiert. So können die bösen Buben tausende Websites innerhalb kurzer Zeit auf Schwachstellen abklopfen und müssen bei der Wahl ihres Angriffsziels nicht wählerisch sein.

Wenn Sie eine Website betreiben, müssen Sie also fest mit ungebetenem Besuch rechnen. Und wenn es eine Sicherheitslücke gibt, wird diese früher oder später auch ausgenutzt. Sie können den Angreifern jedoch die Petersilie verhageln, indem Sie sich deren Tools zu eigen machen, um etwaige Schwachstellen selbst frühzeitig zu finden. Auch diese Tools dürfen Sie nur gegen eigene Server und niemals unbefugt gegen fremde Systeme einsetzen, sonst drohen juristische Konsequenzen (siehe Seite 170). Beachten Sie, dass die Werkzeuge sehr viele Anfragen und damit potenziell auch eine hohe Last erzeugen, was die Erreichbarkeit des Servers beeinträchtigen kann.

Ein einfaches, aber effektives Werkzeug zur Suche nach Datenlecks ist **DIRB**. Es probiert eine lange Liste mit gängigen Verzeichnisnamen wie /admin, /backups oder /internal durch, um Ordner zu finden, die nicht für die Öffentlichkeit bestimmt, aber trotzdem für jeden zugänglich sind. Ferner kann das Hacking-Programm Verzeichnisnamen per Brute Force erraten. Gibt es einen Treffer, versucht DIRB auch noch mögliche Unterordner zu entdecken. Die Bedienung ist einfach:

```
dirb https://ihre-website.example
```

Unzureichend geschützte Verzeichnisse sind häufig die Ursache für Datenlecks, etwa wenn darin Backups der MySQL-Datenbank oder Konfigurationsdateien mit Zugangsdaten gespeichert sind.

Diese Blindgänger sollten Sie rechtzeitig entschärfen, zum Beispiel durch einen Zugriffsschutz auf dem Verzeichnis, sofern die Daten überhaupt auf dem öffentlichen Server liegen müssen.

## WordPress-Lücken aufspüren

Das Content-Management-System WordPress ist sehr verbreitet (siehe S. 60 ff.) und bei Angreifern entsprechend hoch im Kurs. Häufig wird es in veralteten – und somit verwundbaren – Versionen betrieben oder mit anfälligen Plug-ins und Themes. Auch Konfigurationsfehler begünstigen eine Fremdübernahme. Solche Schlupflöcher aufzudecken ist inzwischen ein Kinderspiel – zum Beispiel mit dem WordPress Security Scanner **WPScan**. Der kann Ihnen gute Dienste beim Absichern Ihrer Website leisten.

Auf der GitHub-Seite des Ruby-Tools erfahren Sie, wie Sie es unter Linux, macOS und als Docker-Container an den Start bringen (siehe ct.de/ygg5). Kali-Nutzer können sich das sparen, das Programm ist vorinstalliert. Um Ihre WordPress-Installation zu scannen, füttern Sie WPScan einfach mit der URL: wpscan --url https://ihre-website.example/wordpress

Bevor die Analyse beginnt, lädt der Security Scanner eine Datenbank mit aktuellen Infos aus dem Netz. Das geschieht normalerweise automatisch, wenn Sie es jedoch auf die verwundbaren WordPress-Installationen von RasPwn loslassen möchten (siehe „Angreifen erlaubt“), haben Sie keine Internetverbindung, solange Sie mit dem Raspi-Testnetz verbunden sind. In diesem Fall sollten Sie sich zunächst mit Ihrem normalen Netz verbinden und das Update mit wpscan --update manuell starten. Trennen Sie die Verbindung danach, ehe Sie schließlich den Scan aus dem RasPwn-Netz anwerfen.

Nach und nach gibt WPScan interessante Informationen über die WordPress-Installation aus, darunter die WordPress-Version samt Erscheinungsdatum und eine Einschätzung, ob diese Ausgabe

nach aktuellem Stand der Dinge sicher ist. Weiterhin identifiziert das Tool die Versionen von Webserver und PHP sowie Themes, Plug-ins und diverse Konfigurationsfehler. Prinzipiell kann man selbst im Netz recherchieren, welche Sicherheitslücken in den identifizierten Versionen klaffen. Aber auch das kann Ihnen WPScan abnehmen. Diese Informationen fragt das Tool über ein Web-API vom Server der Entwickler ab – dafür ist eine kostenfreie Registrierung nötig (siehe ct.de/ygg5).

## Datenbank-Lecks verhindern

Die Kronjuwelen einer Website sind häufig Kunden- oder gar Nutzerdaten. Diese können Onlinegauner im Darknet leicht zu Geld machen. In der Regel bewahren Webanwendungen solche Daten in einer Datenbank auf, die natürlich gut geschützt sein sollte. Die Betonung liegt auf sollte, denn allzu oft gelingt es Cyberkriminellen, Kundendaten im großen Stil aus Datenbanken abzugreifen.

Eine häufige Ursache sind sogenannte SQL-Injection-Lücken: Dabei spricht der Angreifer nicht direkt mit dem Datenbankserver, sondern versucht stattdessen, die Webanwendung dazu zu bringen, eingeschleuste SQL-Befehle auf der Datenbank auszuführen. Das Resultat ist häufig, dass die Datenbank über die Web-Anwendung massenweise sensible Datensätze ausspuckt.

Sie ahnen es vielleicht schon: Auch für solche Lücken gibt es ein Hacking-Tool, in diesem Fall **SQLmap**. Es unterstützt zahlreiche Datenbanken, unter anderem Oracle, MySQL, MariaDB, MS SQL Server, PostgreSQL und SQLite. Je nach Datenbanktyp und Berechtigungen kann es auch Dateien auf den Webserver schreiben. Hacker können so versuchen, eine Web-Shell hochzuladen, um den Server dauerhaft fernzusteuern.

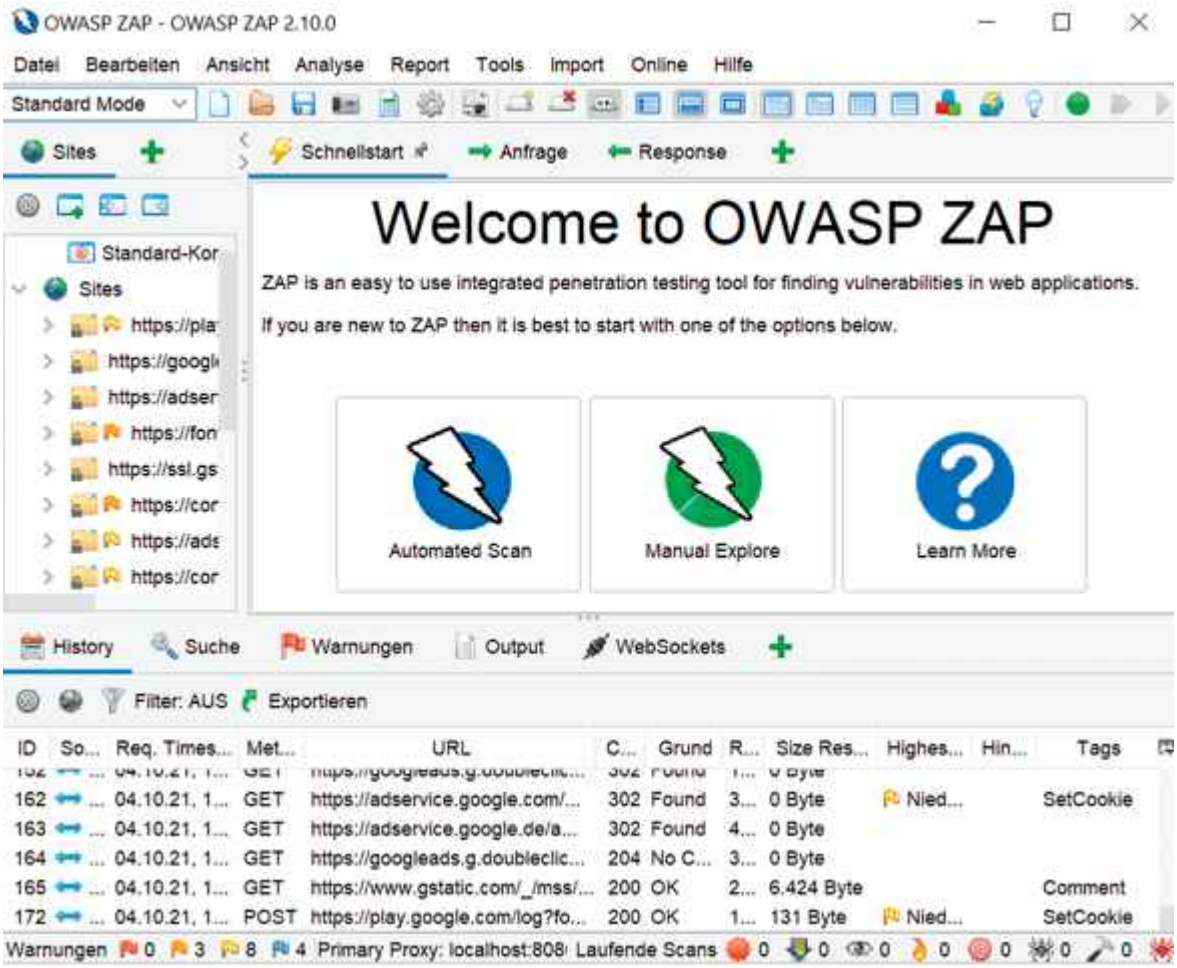
Für einen ersten Funktionstest können Sie die absichtlich anfällige „Wacko Picko“-Website von RasPwn mit SQLmap scannen.

Das Login-Formular der Website sendet beim Abschicken zwei POST-Parameter, nämlich „username“ und „password“, die der Schwachstellenscanner in diesem Beispiel in die Mangel nehmen soll. Um zu überprüfen, ob die Website bei der Auswertung dieser Parameter patzt, können Sie das Tool mit --data anweisen, genau das herauszufinden:

```
sqlmap -u "http://wackopicko.playground.raspwn.org/users/login.php" --data="username=1&password=1" --banner
```

Die Option „banner“ findet die Datenbankversion und das Betriebssystem des Servers heraus, wenn die Website verwundbar ist. Falls Sie den Datenbankinhalt gleich auslesen möchten, ersetzen Sie --banner einfach durch --dump.

Solche SQL-Injections vermeiden Sie, indem Sie Eingaben von außen konsequent überprüfen, bevor sie verarbeitet oder gar in Datenbankbefehle integriert werden. Weiterhin ist der Einsatz sogenannter „Prepared Statements“ sinnvoll, bei denen Sie zunächst den Aufbau des SQL-Befehls festlegen, ehe Sie darin einen Platzhalter mit den von außen angelieferten Werten füllen. Am besten basteln Sie die Datenbankbefehle nicht selbst zusammen, sondern setzen auf eine hinreichend getestete ORM-Bibliothek (Object-Relational Mapping), die bereits gegen alle Eventualitäten abgesichert ist.




Der Zed Attack Proxy (ZAP) macht verschlüsselten Datenverkehr im Klartext sichtbar und spürt Schwachstellen in Web-Anwendungen und APIs auf.

## Browser- und App-Traffic

Der **OWAP Zed Attack Proxy (ZAP)** ist ein universelles Werkzeug zur Analyse und Manipulation von Web-Traffic (HTTP/HTTPS). Sie können sich damit zum Beispiel zwischen Browser und Internet klemmen oder den Datenverkehr Ihres Smartphones durch den Proxy schleusen, um herauszufinden, welche Daten wohin übertragen werden. Eine Stärke des ZAP ist, dass es die identifizierten Gegenstellen, also Webanwendungen, API-Endpunkte und so weiter gleich noch auf Sicherheitsprobleme abklopfen kann. ZAP ist eine Java-Anwendung und läuft unter Windows, Linux und macOS.

Nach dem ersten Start klicken Sie am besten auf den Browser-Knopf in der Symbolleiste, um einen perfekt vorkonfigurierten

Webbrowser zu starten. Dessen Datenverkehr wird automatisch durch den Proxy geschleust. Öffnen Sie damit eine Website, um den Traffic in ZAP zu inspizieren. Wenn Sie den Browser auf diese Weise starten, schleust ZAP in die geöffneten Websites eine eigene Oberfläche namens ZAP HUD ein, über die Sie zahlreiche Funktionen direkt aus dem Browser steuern können. Klicken Sie auf den Knopf „Take the HUD Tutorial“, um eine Einführung zu erhalten und einige der nützlichen Funktionen kennenzulernen.

## Gemischtwaren

Dieser Artikel liefert Ihnen nur eine kleine Auswahl an Hacking-Tools. Das Angebot ist riesig und täglich kommen neue dazu. Einige davon sind sehr komplex oder nur für bestimmte Zielgruppen interessant. Dazu zählt das modular aufgebaute Pentesting-Framework **Metasploit**, das professionelle Penetrationtester nutzen, um einen kompletten Angriff zu simulieren: vom Aufspüren der Ziele über das Ausnutzen von Sicherheitslücken bis hin zum Ausleiten der Datenbeute. Falls Sie sich eingehender mit Hacking beschäftigen möchten, sollten Sie einen Blick darauf werfen. In eine ähnliche Kerbe schlägt **PowerShell Empire**, das Pentestern weitreichenden Rechnerzugriff verschafft, ohne verdächtigen Binärcode auf dem System zu hinterlassen – die Angriffsmodule bestehen aus Skripten für die Windows PowerShell.

Wer eine Windows-Domäne administriert, sollte Tools wie **mimikatz** kennen, das Anmeldeinformationen aus dem Arbeitsspeicher der Windows-Clients ausliest. Angreifer gelangen damit schlimmstenfalls an die Zugangsdaten eines Domänen-Administrators und können das gesamte Netzwerk übernehmen. Den Domänencontroller spüren die Eindringlinge vorher mit **AdFind** von joeware auf. Auch **PsExec** aus Microsofts SysInternals-Kollektion birgt ein gewisses Missbrauchspotenzial: Es wird genutzt, um Befehle auf anderen Rechnern im Netzwerk auszuführen. Angreifer nutzen es mit

zuvor erbeutete Anmeldeinformationen.

Das von der NSA entwickelte Reverse-Engineering-Toolkit **Ghidra** ist interessant, wenn Sie ausführbaren Code (wie EXE- und DLL-Dateien) bis ins letzte Bit auseinandernehmen und verstehen möchten. Es dekompiliert Binärdateien und kann sie auch wieder zusammenbauen, ähnlich wie der kommerzielle Disassembler IDA Pro. In c't 14/2020 haben wir Ghidra ausführlicher getestet (siehe ct.de/ygg5).

## Fazit

Die vorgestellten Hacking-Tools decken einen weiten Bereich ab. Manche Techniken sind erschreckend simpel, andere fordern viel Einarbeitung und Erfahrung. Sich damit zu beschäftigen lohnt sich aber: Sie lernen so, wie ein Angreifer zu denken und Ihre eigenen Sicherheitsprobleme und -lücken aufzuspüren. Das ist hilfreich – ganz gleich, ob Sie nur eine private WordPress-Site betreiben oder gar für die Sicherheit Ihrer Kunden verantwortlich sind. *(rei@ct.de)*

**Hacking-Tools & weitere Infos:** ct.de/ygg5