

Ein Test, der etwas findet, ist der einfache Teil.

Autorisierte Sicherheitsprüfungen für Web-Anwendungen und APIs — und drei Projekte, in denen der schwierige Teil danach kam.

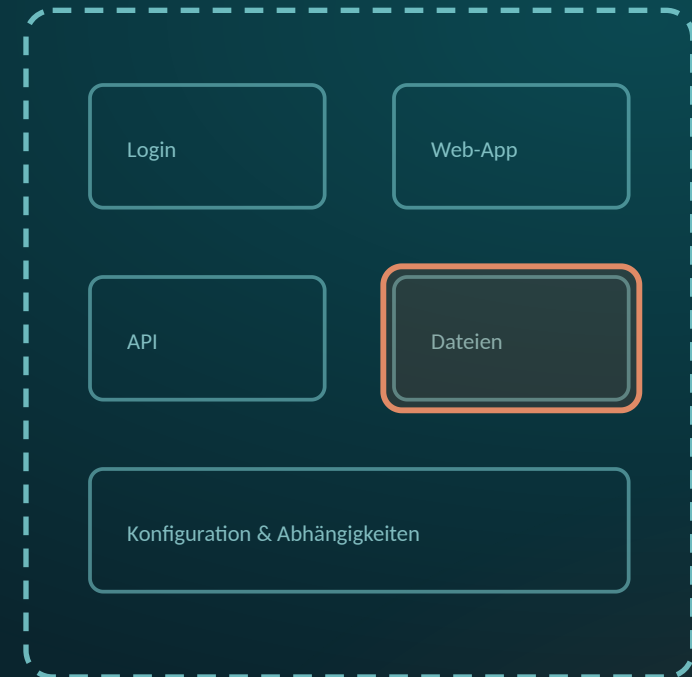
OWASP WSTG & ASVS

API Security Top 10

CVSS v3.1 / v4.0

Nur mit schriftlicher Freigabe

AUTORISIERTER SCOPE



Befund im Objektzugriff

Anonymisierte Referenzdarstellung · Systeme, Kennzahlen und Namen wurden zum Schutz der Auftraggeber verändert

Anirudh Chawla · Founder & Senior Software Engineer · Stand September 2026

Der Anlass steht im Gesetz. Der Auslöser selten.

Das **NIS2-Umsetzungsgesetz** gilt seit dem 6. Dezember 2025 — ohne Übergangsfrist, mit persönlicher Verantwortung der Geschäftsleitung. Seit dem **11. September 2026** greifen die ersten Meldepflichten des **Cyber Resilience Act**: 24 Stunden bis zur Frühwarnung. Für Finanzunternehmen läuft **DORA** seit Januar 2025.

In den Projekten, die bei uns landen, kommt der Anstoß trotzdem fast nie aus dem Gesetzblatt. Er kommt aus einem Lieferantenfragebogen mit 180 Fragen, aus einer Due Diligence, aus der Verlängerung der Cyberversicherung — oder daraus, dass es beim Wettbewerber passiert ist und jemand im Vorstand gefragt hat, ob das bei uns auch geht.

Das ist kein schlechter Anlass. Er führt nur oft zur falschen Frage — „Sind wir sicher?“ — statt zur beantwortbaren: Wo genau, gegen wen, und womit können wir das belegen?

01

Der Scan-Report

180 Seiten aus einem Werkzeug, sortiert nach CVE-Nummer. Kein Bezug zum eigenen System, keine Priorität, niemand zuständig.

02

Der Test ohne Nachtest

Geprüft, berichtet, abgelegt. Ob die Befunde je geschlossen wurden, weiß ein Jahr später niemand mehr.

03

Der zu große Scope

Alles ein bisschen geprüft heißt: nichts belastbar geprüft. Lieber drei Systeme richtig als dreißig oberflächlich.

WER INZWISCHEN FRAGT

NIS2UmsuCG seit 06.12.2025 in Kraft, keine Übergangsfrist
· rund 29.500 Einrichtungen betroffen

CRA Meldepflichten seit 11.09.2026 ·
Produktpflichten und SBOM ab Dezember 2027

DORA seit 17.01.2025 · Finanzunternehmen
brauchen ein Testprogramm, nicht einen Test

ISO 27001 A.8.8 und A.8.29 verlangen
Schwachstellenmanagement und
Sicherheitstests

KURZ GESAGT

Prüfungen sind nicht mehr die Frage. Die Frage ist, ob Sie hinterher etwas in der Hand haben, das Entwicklung, Geschäftsführung und ein Auditor gleichermaßen verstehen.

Rechtsstand September 2026. Übersicht zur Orientierung, keine Rechtsberatung — die Betroffenheit prüfen Sie bitte mit Ihrer Rechtsabteilung.

Was eine Prüfung leistet — und was ausdrücklich nicht

Diese Seite steht bewusst vorn. Die meisten Enttäuschungen in Sicherheitsprojekten entstehen hier, nicht im Test.

DAS LEISTEN WIR

Eine belastbare Momentaufnahme

Für einen klar abgegrenzten Bereich, zu einem festgehaltenen Zeitpunkt, mit dokumentierter Methode.

Nachweise, die Entwickler nachstellen können

Jedes Finding mit Testpfad, erwartetem und tatsächlichem Verhalten. Keine Behauptung ohne Beleg.

Eine Priorisierung, die zu Ihrem Geschäft passt

CVSS ist die Grundlage, nicht das Ergebnis. Eine 6,5 an der Zahlungsstrecke wiegt schwerer als eine 8,1 im Intranet-Wiki.

Einen Nachtest, der Befunde wirklich schließt

Jedes Finding einzeln: geschlossen, teilweise behoben oder bewusst akzeptiert — mit Datum und Unterschrift.

Etwas, das Sie weiterreichen können

An Kunden, Auditoren und Versicherer — ohne dass Sie erst übersetzen müssen, was drinsteht.

DAS LEISTEN WIR NICHT

Kein Zertifikat und kein Siegel

Ein Prüfbericht ist ein Prüfbericht. Wer Ihnen ein „Sicherheitszertifikat“ für einen Pentest anbietet, verkauft Ihnen etwas anderes.

Keine Vollständigkeit

„Keine Befunde“ heißt: in diesem Zeitfenster, mit diesem Aufwand, in diesem Umfang nichts gefunden. Nicht: es gibt nichts.

Keine Haltbarkeit über das Release hinaus

Ein Deployment, eine neue Abhängigkeit, eine geänderte Rolle — und die Momentaufnahme ist überholt.

Kein Ersatz für den Betrieb

Patchmanagement, Protokollierung, Backups, Rechtevergabe und Schulung bleiben Ihre Aufgabe. Wir können sie prüfen, nicht übernehmen.

Keine Prüfung fremder Systeme

Alles, was Ihnen nicht gehört oder wofür der Betreiber nicht unterschrieben hat, bleibt unberührt — auch wenn es technisch erreichbar wäre.

Warum wir das so deutlich sagen: In zwei von drei hier gezeigten Projekten lag vor unserem Angebot eines vor, das „umfassende Sicherheit“ versprach. Beides waren Scanner-Läufe mit Deckblatt. Ein ehrlich abgegrenzter Test ist nicht der schwächere Kauf — er ist der einzige, dessen Ergebnis Sie später verteidigen können.

Die Autorisierung ist die Rechtsgrundlage, kein Formular.

Ohne Einwilligung des Berechtigten sind das Ausspähen und Abfangen von Daten in Deutschland strafbar (§§ 202a–202c StGB). Deshalb beginnt bei uns kein Test vor der Unterschrift — auch kein „kurzer Blick“.

WAS IN DEN RULES OF ENGAGEMENT STEHT

01

Wer freigibt

Auftraggeber *und* — bei gehosteten Systemen — der Betreiber. Beide Unterschriften, sonst kein Test.

02

Was drin ist, was draußen

Domains, Hosts, Endpunkte, Testkonten — und die ausdrückliche Ausschlussliste, benannt statt mitgedacht.

03

Zeitfenster und Methoden

Wann geprüft wird, mit welcher Last, und was ausgeschlossen bleibt — etwa alles, was den Betrieb stören könnte.

04

Abbruchkriterien und Notfallkontakt

Eine Nummer, die während des Zeitfensters immer erreichbar ist. Auf beiden Seiten.

05

Umgang mit Daten

AVV nach Art. 28 DSGVO, verschlüsselte Ablage, Löschfrist für Nachweise — bei uns 90 Tage nach Nachtest.

WANN WIR STOPPEN UND ZUM TELEFON GREIFEN

01

Wir stoßen auf echte personenbezogene Daten. Wir sehen sie nicht an, wir dokumentieren nur, dass sie erreichbar waren.

02

Es gibt Hinweise auf einen fremden Zugriff, der nicht von uns stammt. Dann ist der Test beendet und es beginnt etwas anderes.

03

Ein System wird instabil oder verhält sich unerwartet. Wir halten an, auch wenn es wahrscheinlich nicht an uns liegt.

In dieser Reihenfolge, und immer telefonisch. Eine E-Mail um 22:40 Uhr ist keine Meldung.

AUS ERFAHRUNG

Zweimal haben wir erst am Testtag gemerkt, dass der Hoster nichts von der Prüfung wusste — und einmal hat dessen Schutzsystem uns nach elf Minuten ausgesperrt. Seitdem ist die erste Frage im Scoping-Gespräch nicht „Was sollen wir prüfen?“, sondern „Wem gehört die Maschine, auf der es läuft?“

WAS SIE VORBEREITEN SOLLTEN

- Testkonten je Rolle, vorab angelegt
- Eine Testumgebung, die der Produktion gleicht
- Ansprechpartner Technik *und* Fachbereich
- Ausnahmen in Schutzsystemen, falls gewünscht
- Klarheit, ob Protokolle ausgewertet werden

Sechs Schritte. Der letzte entscheidet, ob sich der erste gelohnt hat.

Dauern aus den drei hier gezeigten Projekten. Schritt 4 skaliert mit dem Umfang, alles andere bleibt weitgehend stabil.

01 · 1 WOCHE

Scoping

Ein Gespräch, kein Fragebogen. Welche Systeme tragen das Geschäft, welche Daten wären am teuersten, wo liegen die Kronjuwelen? Daraus entsteht der Umfang — nicht aus einer Preisliste.

02 · 3–5 TAGE

Rules of Engagement

Schriftlich, beidseitig unterschrieben, mit Ausschlussliste und Notfallkontakt. Parallel AVV und Testkonten. Dieser Schritt lässt sich nicht abkürzen.

03 · 3–8 TAGE

Aufklärung

Wir kartieren die Angriffsfläche innerhalb des Scopes und verstehen die Fachlogik. Ohne zu wissen, was ein Vorgang *bedeutet*, findet man keine Logikfehler.

04 · 5–15 TAGE

Prüfung

Manuell geführt entlang OWASP WSTG und ASVS, Werkzeuge unterstützen. Kritische Funde melden wir sofort telefonisch — nicht erst im Bericht.

Zugriff & Rollen

Sitzungen

Eingaben

Konfiguration

Abhängigkeiten

05 · 1 WOCHE

Bericht & Besprechung

Zwei Ebenen in einem Dokument: eine Zusammenfassung, die eine Geschäftsführung in zehn Minuten liest, und ein technischer Teil, mit dem ein Entwickler sofort arbeiten kann.

06 · NACH BEHEBUNG

Nachtest

Jedes Finding einzeln nachgestellt und einzeln abgeschlossen. Im Nachtestbericht steht pro Befund: geschlossen, teilweise behoben oder bewusst akzeptiert — mit Begründung.

Warum der Nachtest im Preis steckt: Ein Bericht ohne Nachtest sagt nur, wie es einmal war. In zwei der drei Projekte war mindestens eine Korrektur unvollständig — nicht aus Nachlässigkeit, sondern weil dieselbe Prüfung an einer zweiten Stelle fehlte, an die bei der Behebung niemand gedacht hatte.

WIEDERHOLUNG

Sinnvoll jährlich und zusätzlich nach größeren Änderungen an Authentifizierung, Rollenmodell oder Zahlungsstrecke. Ein fester Turnus allein reicht nicht.

AUSGANGSLAGE

Eine Logistiksoftware, ursprünglich als Einzelinstallation für einen Kunden gebaut, inzwischen als SaaS mit **240 Mandanten auf einer Instanz**. Auf dem Tisch lag der Sicherheitsfragebogen eines Großkunden: 180 Fragen, davon rund 40 zur Trennung der Mandanten. Beantworten konnte man sie — belegen keine einzige.

Getestet worden war vorher zweimal. Beide Berichte waren Scanner-Läufe mit Deckblatt: Bibliotheksversionen, fehlende Header, ein abgelaufenes Zertifikat. Zur Frage, ob Mandant A an die Daten von Mandant B kommt, stand in beiden Berichten nichts.

DER AUFTRAG

Die Mandantentrennung belastbar prüfen, vor der Vertragsunterschrift mit dem Großkunden — Zeitfenster: vier Wochen. Danach ein Bericht, der als Anlage zum Fragebogen taugt.

RAHMEN

Grey-Box, 6 Testkonten

Eigene Testumgebung, produktionsnah

Freigabe von Auftraggeber & Hoster

Keine Lasttests

Quellcode-Einsicht punktuell

AVV nach Art. 28 DSGVO

DIE DREI HARTEN STELLEN

01 Mandantentrennung ist keine Funktion

Sie ist eine Eigenschaft, die an *jeder* Stelle gelten muss. Ein Endpunkt, der die Zuordnung nicht prüft, hebt die Trennung für das ganze System auf. Geprüft worden war bis dahin, was man in der Oberfläche sieht — und die Oberfläche zeigt nur das, was sie ohnehin anzeigt.

OWASP API1 · Objektzugriff

1.400 Endpunkte

02 Vierzehn Rollen, die niemand mehr erklären konnte

Historisch gewachsen, teils für einzelne Kunden angelegt. Es gab keine Matrix, wer was darf — also konnte es auch keine geben, gegen die man prüft. Wir haben sie in den ersten sechs Tagen mit dem Team erst aufgebaut. Dieser Schritt stand nicht im Angebot und war der wichtigste.

03 Vier Wochen reichen nicht für 1.400 Endpunkte

Das haben wir vor der Beauftragung gesagt, nicht danach. Statt alles oberflächlich zu prüfen, haben wir den Scope auf drei Bereiche begrenzt — Aufträge, Exporte, Dateien — und schriftlich festgehalten, was **nicht** geprüft wurde. Genau dieser Satz steht heute auch im Bericht an den Großkunden.

Befunde, die jemanden haben — und ein Datum

Laufender Befundstand, für den Auftraggeber jederzeit einsehbar.
Nachweise verbleiben verschlüsselt im Anhang, nicht in der Übersicht.

1

Autorisierter Scope aktiv · Freigabe v2 vom 03.06.2026, unterzeichnet von Auftraggeber und Hostler · 3 Hosts, Module Aufträge / Exporte / Dateien · **nicht im Scope:** Zahlungsdienstleister, Partner-Portal, Produktionsdaten

2

Sofort gemeldet
10.06., 11:42 Uhr — SEC-003 telefonisch an M. Berger, schriftlich um 11:58.
Behelfsmaßnahme noch am selben Tag aktiv.

4

SEC-2026-003 · Mandantenübergreifender Objektzugriff
RISIKO IN KLARTEXT
Ein angemeldetes Konto eines Mandanten konnte Auftragsdaten eines anderen Mandanten abrufen. Betroffen sind Kundennamen, Lieferadressen und Preise.

3

Nachweis · Testpfad
1 Anmeldung
Rolle Sachbearbeiter
Mandant ████████
2 Abruf eines Objekts außerhalb der Zuordnung
3 Ergebnis
erwartet 403 · erhalten 200
4 Inhalt ██████████
Vollständiger Nachweis im verschlüsselten Anhang.
Löschung 90 Tage nach Nachtest.

5

Nachtest 22.06.
Gleicher Testpfad, gleiche Konten.
Ergebnis: 403 wie erwartet.
Zusätzlich an vier weiteren Endpunkten stichprobenartig geprüft.

Befunde · 23 gesamt

Kritisch

Hoch

Mittel

Niedrig

2

5

9

7

Nach Modul

Aufträge

Exporte

Dateien

Anmeldung

9

6

5

3

Nicht geprüft: ~1.050 Endpunkte außerhalb des Umfangs.

ID	BEFUND	SCHWERE	CVSS	VERANTWORTLICH	FRIST	STATUS
SEC-2026-003	Mandantenübergreifender Objektzugriff im Auftragsmodul	KRITISCH	8.6	Team Plattform	14.06.	✓ Nachtest ok
SEC-2026-007	Berechtigung nur in der Oberfläche geprüft, nicht serverseitig	KRITISCH	8.1	Team Plattform	20.06.	Nachtest offen
SEC-2026-011	Sitzung bleibt nach Rollenwechsel mit alten Rechten gültig	HOCH	7.4	Team Identity	27.06.	In Behebung
SEC-2026-019	Dateiabruf ohne erneute Prüfung der Mandantenzuordnung	HOCH	7.1	Team Plattform	27.06.	In Behebung
SEC-2026-023	Wiederholte Anmeldeversuche werden nicht begrenzt	MITTEL	5.3	Team Identity	11.07.	Offen
SEC-2026-028	Interne Pfade in Fehlermeldungen sichtbar	MITTEL	4.3	Team Betrieb	11.07.	Offen

1

Der Scope steht über allem. Auf jeder Ansicht und auf jeder Berichtsseite — samt Ausschlussliste. So kann niemand später behaupten, etwas sei mitgeprüft gewesen.

3

Jeder Befund hat eine Person und ein Datum. Ein Bericht ohne Zuständigkeit ist eine Lektüre, keine Maßnahmenliste.

5

Nachweise sind geschwärzt und getrennt abgelegt. In der Übersicht steht nur der Testpfad: was getan wurde, was erwartet war, was tatsächlich kam. Vollständige Belege liegen verschlüsselt im Anhang, für benannte Personen, mit Löschfrist — ein Prüfbericht, der frei herumliegt, ist selbst ein Risiko.

2

Kritische Funde gehen sofort raus. Telefonisch, dann schriftlich, mit Uhrzeit protokolliert. Bis zur Behebung wird eine Behelfsmaßnahme vereinbart.

4

Risiko in Klartext, Maßnahme konkret. Nicht „Zugriffskontrolle härten“, sondern an welcher Stelle im System die Prüfung fehlt und wo sie hingehört.

EaseWerk Digital · easewerk.de · anirudh@easewerk.de · Projekt 01 SaaS-Plattform

07

Belegbar statt beteuert — und ein Satz, der wehtut

Prüfzeitraum 08.–26.06.2026, Nachtest in zwei Wellen bis 24.07.2026. Alle Angaben anonymisiert.

KRITISCH & HOCH NACH NACHTEST

7 → **0**

Alle sieben einzeln nachgestellt und geschlossen.

BEFUNDE GESAMT

23 in 3 Modulen

2 kritisch • 5 hoch • 9 mittel • 7 niedrig

BIS ZUM ERSTEN KRITISCHEN FUND

6 Std.

Zwei vorherige Scanner-Prüfungen hatten ihn nicht.

FRAGEN DES GROSSKUNDEN

0 → **38**

von 40 jetzt mit Beleg beantwortbar.

MITTLERE BEHEBUNGSZEIT

9 Tage

Kritische Befunde im Schnitt nach 3 Tagen.

„Der unangenehmste Satz im Bericht war nicht der über den kritischen Befund. Es war der darüber, wie viele Endpunkte wir nicht geprüft haben. Den haben wir dem Kunden trotzdem so weitergegeben.“

CTO • SaaS-Anbieter, 240 Mandanten

WAS DER NACHTEST ZUSÄTZLICH ERGEBEN HAT

01

Die Korrektur zu SEC-003 war an der Hauptstelle richtig — und fehlte im Export, der dieselben Daten über einen anderen Weg holte. Gefunden nur, weil wir im Nachtest auch Nachbarendpunkte stichprobenartig mitgeprüft haben.

02

Zwei mittlere Befunde wurden bewusst akzeptiert statt behoben — mit Begründung, Risikoträger und Wiedervorlage. Das ist eine legitime Entscheidung, solange sie jemand trifft und unterschreibt. Nicht dokumentiert ist sie nur eine Lücke.

Offen geblieben: Die Rollenmatrix existiert jetzt — aber drei historische Rollen aus Einzelverträgen ließen sich in vier Wochen nicht auflösen. Sie sind dokumentiert, eingeschränkt und terminiert. Die Konsolidierung ist ein eigenes Vorhaben und kein Sicherheitsbefund, sondern eine Altlast. Das im Bericht auseinanderzuhalten war dem Auftraggeber wichtig — zu Recht.

AUSGANGSLAGE

Eine Partner-Schnittstelle, über die 60 Unternehmen Zahlungen anstoßen und Abrechnungen abholen. Sechs Rollen, 90 Endpunkte, gewachsen über sieben Jahre. Die Aufsicht fragt seit DORA nicht mehr, *ob* getestet wurde, sondern nach dem **Programm** dahinter: Was wird wann geprüft, nach welchen Kriterien, und wie werden Befunde nachverfolgt?

Ein Programm gab es. Es bestand aus einem jährlichen Termin und einem PDF. Auf die Frage, welche der 540 Kombinationen aus Rolle und Endpunkt je geprüft worden waren, konnte niemand antworten — nicht aus Nachlässigkeit, sondern weil die Frage so noch nie gestellt worden war.

DER AUFTRAG

Die Autorisierung auf Objektebene systematisch prüfen — nicht stichprobenartig — und ein Prüfverfahren hinterlassen, das die interne Revision selbst wiederholen kann.

RAHMEN

Produktion ausgeschlossen

Spiegelumgebung, 6 Testpartner

Freigabe inkl. Cloud-Betreiber

Begleitung durch Interne Revision

Kein Social Engineering

Protokolle wurden mitausgewertet

DIE DREI HARTEN STELLEN

01 540 Kombinationen lassen sich nicht erraten

Sechs Rollen mal 90 Endpunkte. Wer hier stichprobenartig prüft, findet genau die Fehler, die er zufällig trifft. Wir haben die Soll-Matrix mit dem Fachbereich aufgeschrieben und dann jede Zelle gegen das tatsächliche Verhalten gehalten — das war der Großteil des Aufwands und der Grund, warum überhaupt etwas gefunden wurde.

OWASP API1 & API5

540 Prüfwerten

02 „Was, wenn ein Partner kompromittiert wird?“

Die Antwort im ersten Gespräch lautete: *Dann rufen die uns an*. Zugänge liefen sehr lange, ein sofortiger Widerruf war nicht vorgesehen, und niemand hätte im Nachhinein sagen können, was in der Zwischenzeit abgerufen wurde. Das war kein einzelner Befund, sondern ein fehlender Prozess.

03 Die Kopie war nicht die Produktion

Produktion war zu Recht ausgeschlossen. Die Spiegelumgebung wich aber an elf Stellen ab — andere Konfiguration, ältere Abhängigkeiten, ein fehlendes Schutzsystem. Diese Abweichungen zu dokumentieren war ein eigener Arbeitsschritt und steht als Einschränkung im Bericht. Ohne diesen Absatz wäre das Ergebnis mehr wert, als es ist.

Jede Zelle einmal angefasst, nicht jede dritte

Soll-Matrix mit dem Fachbereich erstellt, Ist-Verhalten dagegen geprüft.
Das Verfahren bleibt beim Auftraggeber und ist wiederholbar.

Rollen- und Objektzugriffsmatrix • Spiegelumgebung540 Zellen • 540 geprüft

1

Lesart: ● erlaubt und korrekt • – nicht vorgesehen und korrekt abgewiesen • ▲ Abweichung zwischen Soll und Ist

ENDPUNKTGRUPPE	Partner lesen	Partner buchen	Partner Admin	Support	Revision	System
Zahlungen anlegen	–	●	●	–	–	●
Zahlungen abrufen	●	●	●	▲	●	●
Abrechnungen	●	●	●	–	●	–
Stammdaten Partner	–	–	●	●	–	▲
Exporte	–	–	●	–	●	–
Protokolle	–	–	–	●	▲	●
Zugänge verwalten	–	–	●	–	–	●
Webhooks	●	●	●	–	–	●

2

Drei Abweichungen — jede mit eigenem Befund

Support konnte Zahlungsdaten abrufen, obwohl die Rolle nur Metadaten sehen sollte • **System** durfte Partnerstammdaten ändern, was nirgends vorgesehen war • **Revision** hatte Schreibzugriff auf Protokolle — das hebt den Zweck von Protokollen auf.

Die Matrix ist Teil der Übergabe. Sie wird bei jeder neuen Rolle und jedem neuen Endpunkt ergänzt und lässt sich als Prüfliste wiederverwenden — auch ohne uns.

3

Zugänge, Gültigkeit und Nachvollziehbarkeit

Gültigkeit der Partnerzugänge • Ist-Aufnahme

Zugriffstoken		24 Stunden
Erneuerungstoken		unbefristet
Sofortiger Widerruf		fehlt
Bindung an Partner		vorhanden

Empfehlung: kurze Laufzeit für Zugriffstoken, befristete und einzeln widerrufbare Erneuerungstoken, ein Widerrufsweg mit Wirkung in Minuten statt Tagen.

4

Könnten Sie einen Missbrauch nachträglich belegen?

- ✓ Anmeldungen werden protokolliert
- ✓ Schreibende Zugriffe werden protokolliert
- ✗ Lesende Zugriffe auf Zahlungsdaten: nicht protokolliert
- ✗ Aufbewahrung: 14 Tage, rollierend überschrieben
- ▲ Protokolle für die Rolle Revision beschreibbar

Ohne Protokoll lesender Zugriffe ist die Frage „Welche Daten hat der kompromittierte Partner gesehen?“ nicht beantwortbar — weder für die Aufsicht noch für betroffene Kunden.

Was daraus wurde

Aus drei Befunden wurde ein Arbeitspaket: Laufzeiten, Widerrufsweg und Protokollierung zusammen — weil einzeln behoben jedes davon wirkungslos geblieben wäre.

- 1

Erst das Soll, dann das Ist. Ohne aufgeschriebene Soll-Matrix gibt es keinen Maßstab — dann ist jedes Verhalten irgendwie erklärbar.
- 2

Abweichungen sind einzelne Befunde. Auch die, bei denen zu viel erlaubt ist, ohne dass es je jemand genutzt hätte.
- 3

Ein Zugang ohne Ablauf ist ein Zugang ohne Ende. Geprüft wird nicht nur, wer hereinkommt, sondern wie lange und wie man ihn wieder schließt.
- 4

Nachvollziehbarkeit gehört zur Sicherheit. Die meisten Prüfungen hören beim Zugriff auf. Für DORA und NIS2 zählt aber genauso, ob Sie einen Vorfall im Nachhinein rekonstruieren und innerhalb von 24 Stunden melden können. Eine Protokollierung, die lesende Zugriffe auslässt und nach 14 Tagen überschreibt, trägt diese Pflicht nicht.

Aus einem Termin im Jahr wurde ein Verfahren

Prüfzeitraum sechs Wochen, Nachtest in drei Wellen. Begleitet von der Internen Revision, Ergebnis Teil der DORA-Dokumentation des Auftraggebers.

GEPRÜFTE ROLLE-/ENDPUNKT-ZELLEN

~~unbekannt~~ → **540**

Dokumentiert, wiederholbar, ohne uns fortführbar.

BEFUNDE

17 davon 3 kritisch

3 kritisch · 4 hoch · 6 mittel · 4 niedrig

GÜLTIGKEIT ERNEUERUNGSTOKEN

~~unbefristet~~ → **30 Tage**

Einzel widerrufenbar, Wirkung unter 2 Minuten.

AUFBEWAHRUNG DER PROTOKOLLE

~~14 Tage~~ → **12 Monate**

Lesende Zugriffe jetzt eingeschlossen, Schreibschutz aktiv.

WAS DIE AUFSICHTSFRAGE EIGENTLICH WAR

01

Gefragt war nie ein besseres Testergebnis, sondern ein nachvollziehbares Verfahren. Der Bericht ist inzwischen der kleinere Teil der Übergabe — die Matrix, die Prüfliste und der Turnus sind das, was die Revision zweimal jährlich selbst durchläuft.

02

Drei Befunde ließen sich nur gemeinsam beheben. Kurze Tokenlaufzeiten ohne Widerrufsweg hätten nur genervt; ein Widerrufsweg ohne Protokoll wäre nicht belegbar gewesen. Wir haben sie deshalb als ein Arbeitspaket geschrieben, gegen die Gewohnheit, jedes Finding einzeln zu ticketieren.

03

Die elf Abweichungen der Spiegelumgebung stehen als Einschränkung im Bericht. Vier davon wurden anschließend in der Testumgebung angeglichen — nicht wegen eines Befunds, sondern weil die nächste Prüfung sonst wieder weniger wert gewesen wäre.

„Am nützlichsten war die Frage, ob wir einen Missbrauch im Nachhinein überhaupt belegen könnten. Darauf hatten wir keine Antwort — und das war schlimmer als jeder einzelne Befund.“

Leiter Interne Revision · Zahlungsdienstleister

Offen geblieben: Geprüft wurde die Spiegelumgebung, nicht die Produktion. Das war richtig und ist zugleich die größte Einschränkung des Ergebnisses — ein Befund, der nur aus einer Abweichung der Umgebungen entstünde, hätten wir nicht gefunden. Ein bedrohungsgeleiteter Test auf der Produktion nach TIBER-Vorbild ist ein eigenes Vorhaben mit eigener Freigabe; wir haben ihn empfohlen und nicht als Nachtrag angeboten.

Neun Jahre gewachsen · 60 Extensions, davon 11 eigene · 340 Composer-Pakete · anonymisierte Referenzdarstellung

AUSGANGSLAGE

Der Anlass war kein Gesetz und kein Fragebogen. Beim Wettbewerber hatte es einen Vorfall gegeben, drei Tage Stillstand, und die Geschäftsführung wollte wissen, ob das hier auch ginge. Eine unpräzise Frage — aber die ehrlichste, die wir in den drei Projekten bekommen haben.

Vorgefunden haben wir eine über neun Jahre gewachsene Plattform: zwei Entwickler, von denen einer seit 2023 nicht mehr da ist, 60 Extensions, ein Deployment-Prozess mit manuellen Schritten und eine Liste installierter Pakete, die seit Jahren nur länger geworden war.

DER AUFTRAG

Keine tiefe Anwendungsprüfung, sondern das Fundament: Konfiguration, Zugänge, Abhängigkeiten, Protokolle, Backups. Drei Wochen, feste Obergrenze — und danach eine Liste, die zwei Entwickler realistisch abarbeiten können.

RAHMEN

Konfigurations- und Härtingsprüfung

White-Box, mit Repository-Zugang

Staging + Produktion (lesend)

Wiederherstellungstest vereinbart

Keine Prüfung der Shop-Zahlungsanbindung

DIE DREI HARTEN STELLEN

01 340 Pakete, die niemand bestellt hat

Direkt installiert waren 60 Extensions. Mitgekommen sind 280 weitere Pakete als Abhängigkeiten. Zu keinem einzigen gab es eine Entscheidung — sie waren einfach da. Wir haben zuerst eine Stückliste erzeugt, bevor überhaupt bewertet werden konnte, was fehlt.

Lieferkette

SBOM als Nebenprodukt

02 Die meisten Befunde standen nicht im Quelltext

Sie standen in Einstellungen: Debug-Ausgaben, die in der Produktion aktiv waren, ein Redaktionszugang aus 2019 ohne zweiten Faktor, zu weit gefasste Schreibrechte auf einem Sicherungsverzeichnis. Nichts davon ist spektakulär. Zusammen war es der kürzeste Weg ins System.

03 Backups gab es. Geprüft hatte sie seit 2021 niemand.

Wir haben einen echten Wiederherstellungstest verlangt, gegen anfänglichen Widerstand. Der erste Versuch scheiterte an einem fehlenden Datenbankbenutzer, der zweite gelang — nach **neun Stunden**. Kein Sicherheitsbefund im engeren Sinn und der wertvollste Tag der gesamten Prüfung.

Das Fundament prüft man nicht mit einem Scanner

Konfiguration, Zugänge, Abhängigkeiten und Wiederherstellung — je Umgebung getrennt bewertet.



Eine Liste, die zwei Entwickler tatsächlich abarbeiten können

Prüfzeitraum drei Wochen, Nachtest nach sechs Monaten. Das Team hat 24 von 31 Befunden ohne externe Unterstützung geschlossen.

WIEDERANLAUFZEIT

~~9:10 Std.~~ → **2:40 Std.**

Im Nachtest erneut geübt, jetzt halbjährlich terminiert.

BEFUNDE

31 · 24 geschlossen

1 kritisch (in Kombination) · 6 hoch ·
13 mittel · 11 niedrig

HÄRTUNGSSTAND PRODUKTION

~~58 %~~ → **89 %**

17 von 19 Kontrollen erfüllt.

PAKETE OHNE PFLEGE

~~17~~ → **4**

Sechs Extensions ganz ausgebaut statt
ersetzt.

ZUGÄNGE OHNE ZWEITEN FAKTOR

~~23~~ → **0**

Inklusive vier Konten, die niemandem
mehr gehörten.

WARUM DAS TEAM ES SELBST GESCHAFFT HAT

01

Die Liste war nach *Aufwand* sortiert, nicht nur nach Schwere. Neun Befunde waren in einem halben Tag erledigt. Damit beginnt man, und der Rest wirkt danach machbar.

02

Zu jedem Befund stand nicht nur, was zu tun ist, sondern *wo* — Datei, Einstellung, Verantwortlicher. Zwei Entwickler haben keine Zeit, sich das aus einer Empfehlung herzuleiten.

03

Sieben Befunde haben wir ausdrücklich als „später“ markiert, mit Begründung. Eine Liste, auf der alles dringend ist, wird nicht abgearbeitet — sie wird weggelegt.

„Wir hatten mit einer Liste gerechnet, die uns zeigt, wie schlecht wir sind. Bekommen haben wir eine, bei der nach vier Wochen die Hälfte abgehakt war.“

IT-Leitung · Handelsunternehmen

Offen geblieben: Das Upgrade des TYPO3-Cores und der Umstieg auf eine gepflegte PHP-Version waren in drei Wochen nicht zu leisten und sind auch kein Prüfergebnis, sondern ein eigenes Projekt. Vier Befunde hängen daran und bleiben bis dahin offen — mit Behelfsmaßnahme und Termin. Wir haben das nicht als „behooben“ gezählt, auch wenn es die Zahlen auf dieser Seite freundlicher gemacht hätte.

Ein Bericht, der zwei Leser gleichzeitig bedient

Vorn zehn Minuten für die Geschäftsführung, hinten das Material für die Entwicklung. Beides im selben Dokument, beides prüfbar.

TEIL A • ZUSAMMENFASSUNG

Für Geschäftsführung und Auditoren

- Was geprüft wurde — und was nicht
- Lage in fünf Sätzen, ohne Fachbegriffe
- Verteilung der Befunde nach Schwere
- Die drei Dinge, die zuerst passieren müssen
- Aufwand und Reihenfolge, grob geschätzt
- Einschränkungen der Aussagekraft

TEIL B • BEFUNDE

Für Entwicklung und Betrieb

- Je Befund: Risiko, Nachweis, Maßnahme, Nachtest
- CVSS-Wert und fachliche Einordnung
- Betroffene Stelle, nicht nur betroffenes System
- Zuständigkeit und Frist
- Verweis auf den verschlüsselten Nachweisanhang

WAS WIR WEGLASSEN

Keine Anleitungen zur Ausnutzung, keine Produktivdaten, keine vollständigen Bezeichner. Ein Prüfbericht wandert durch Postfächer und Datenräume — er darf nicht selbst zur Gefahr werden.

Prüfbericht 2026-014 • Teil B, Befund 3 von 23

Vertraulich • nur für benannte Empfänger

SEC-2026-003

KRITISCH

CVSS 8.6

Mandantenübergreifender Objektzugriff im Auftragsmodul

RISIKO • WAS PASSIEREN KANN

Ein angemeldetes Konto eines Mandanten konnte Auftragsdaten eines anderen Mandanten abrufen. Betroffen sind Kundennamen, Lieferadressen und vereinbarte Preise. Ein Mandant könnte damit die Konditionen eines Wettbewerbers einsehen, der dieselbe Plattform nutzt.

MASSNAHME • WAS ZU TUN IST

Die Zuordnung zum Mandanten bei jedem Objektzugriff serverseitig prüfen — zentral in der Datenzugriffsschicht, nicht je Endpunkt. Die Prüfung in der Oberfläche bleibt bestehen, trägt die Sicherheit aber nicht.

Betroffene Stelle: Auftragsmodul, gemeinsame Abfrageschicht • **gleiche Ursache bei:** Export, Dateiabruf • **Zuständig:** Team Plattform • **Frist:** 14.06.2026

NACHWEIS • TESTPFAD

Vorbedingung
zwei Testkonten, verschiedene Mandanten

- 1 Anmeldung als Rolle **Sachbearbeiter**, Mandant 
- 2 Abruf eines Auftragsobjekts, das dem zweiten Mandanten zugeordnet ist
- 3 Erwartetes Verhalten **403 Forbidden**
Tatsächliches Verhalten **200 OK**
- 4 Inhalt der Antwort 

Zeitpunkt 10.06.2026, 11:31 MESZ
Beleg A-003 im verschlüsselten Anhang

NACHTEST • 22.06.2026

✓ **Geschlossen.** Gleicher Testpfad, gleiche Konten: 403 wie erwartet. Zusätzlich an vier benachbarten Endpunkten stichprobenartig geprüft — dabei wurde SEC-2026-019 gefunden.

Die Zeile, auf die es ankommt: „Gleiche Ursache bei Export und Dateiabruf.“ Ein Befund ohne diesen Hinweis wird an einer Stelle repariert und bleibt an zwei anderen bestehen. Genau das ist in Projekt 01 beinahe passiert.

CVSS allein entscheidet nicht. Die Einstufung als kritisch stammt aus der fachlichen Wirkung — Preiskonditionen zwischen Wettbewerbern — nicht aus der Zahl 8,6.

Wonach wir prüfen — und was davon wirklich Befunde liefert

BLACK BOX

ohne Vorwissen

Wir bekommen nur, was ein Außenstehender auch hätte. Nah an der Realität, aber teuer: Ein großer Teil der Zeit geht für Dinge drauf, die Sie uns in zehn Minuten hätten sagen können.

GREY BOX • UNSERE EMPFEHLUNG

Konten & Doku

Testkonten je Rolle, Architekturübersicht, Endpunktliste. Das beste Verhältnis von Aufwand zu Erkenntnis — in allen drei gezeigten Projekten so gewählt. Wer Rollen und Objektzugriffe prüft, muss die Soll-Rechte kennen.

WHITE BOX

mit Quelltext

Zusätzlich Repository- und Konfigurationszugriff. Sinnvoll bei Konfigurationsprüfungen und eigenen Komponenten — Projekt 03 lief so. Ersetzt keine Prüfung von außen.

EHRlich ZUR AUTOMATISIERUNG

Werkzeuge laufen bei uns mit. Sie finden veraltete Versionen und offensichtliche Fehlkonfigurationen zuverlässig — und liefern damit einen Teil der Befunde.

Autorisierung auf Objektebene, Mandantentrennung und Geschäftslogik finden sie nicht. In allen drei Projekten lagen genau dort die kritischen Befunde.

PRÜFBEREICHE UND IHRE GRUNDLAGE

BEREICH	GRUNDLAGE	WORAUF ES HINAUSLÄUFT
Zugriff & Rollen	OWASP API1/API5 · ASVS V4	Erreicht jede Rolle nur die für sie bestimmten Objekte?
Anmeldung & Sitzungen	ASVS V2/V3 · WSTG-ATHN, WSTG-SESS	Laufzeiten, Widerruf, Verhalten bei Rollenwechsel
Eingaben & Verarbeitung	OWASP Top 10 A03 · ASVS V5	Werden Inhalte sicher verarbeitet und ausgegeben?
Dateien & Ablagen	ASVS V12 · WSTG-BUSL	Berechtigung beim Abruf, Typprüfung, Ablageort
Geschäftslogik	WSTG-BUSL · fachliche Abstimmung	Lässt sich ein Vorgang in unzulässiger Reihenfolge führen?
Konfiguration	OWASP A05 · BSI IT-Grundschutz	Header, Zugänge, Fehlerausgaben, Trennung der Umgebungen
Abhängigkeiten	OWASP A06 · CRA-Stückliste	Was ist installiert, wer pflegt es, wie kommt ein Update an?
Nachvollziehbarkeit	NIS2 · DORA · ISO 27001 A.8.15	Könnten Sie einen Vorfall im Nachhinein belegen und fristgerecht melden?

Was Sie am Ende in der Hand haben: Prüfbericht in zwei Teilen, Befundliste mit Zuständigkeit und Frist, Nachweisanhang verschlüsselt, Nachttestbericht je Befund — und, wo es Sinn ergibt, ein Prüfverfahren, das Ihre eigene Revision wiederholen kann.

Drei Dinge, die wir nicht machen — auch auf Nachfrage nicht

01 Keinen funktionierenden Angriff vorführen

Nicht im Verkaufsgespräch, nicht im Vortrag, nicht als Video im Bericht — auch nicht auf Ihrem eigenen System, auch nicht wenn Sie ausdrücklich darum bitten. Eine Vorführung überzeugt kurzfristig und erzeugt ein Artefakt, das anschließend unkontrolliert weiterwandert. Was ein Befund bedeutet, lässt sich in drei Sätzen erklären; was er im Detail ermöglicht, gehört in den Testpfad und in den verschlüsselten Anhang.

02 Keinen Scanner-Report als Prüfbericht verkaufen

Ein Werkzeuglauf mit Deckblatt ist in zwei Stunden erstellt und sieht nach Arbeit aus. Zwei der drei hier gezeigten Auftraggeber hatten so etwas bereits — in beiden Fällen ohne einen einzigen Befund zur Zugriffskontrolle. Wenn eine Automatenprüfung für Ihren Zweck reicht, sagen wir das und nennen Ihnen ein Werkzeug. Dafür brauchen Sie uns nicht.

03 Keine Prüfung ohne Freigabe des Betreibers

Auch dann nicht, wenn Sie Eigentümer der Anwendung sind und es „nur kurz“ gehen soll. Ohne die Unterschrift desjenigen, dem die Maschine gehört, fehlt die Rechtsgrundlage — für uns und für Sie. Das kostet im Zweifel eine Woche. Diese Woche ist der Preis dafür, dass das Ergebnis hinterher belastbar ist.

WENN WIR ETWAS AUSSERHALB IHRES SCOPES FINDEN

Manchmal stößt man bei einer Prüfung auf eine Schwäche, die nicht Ihnen gehört — in einer Bibliothek, bei einem Dienstleister, in einem fremden Produkt.

Dann informieren wir zuerst Sie, dann den Hersteller, und setzen eine Frist. Veröffentlicht wird nichts — weder von uns noch mit Ihrem Namen. Das ist kein Entgegenkommen, sondern die einzige Vorgehensweise, die niemanden gefährdet.

Umgekehrt gilt dasselbe: Was wir bei Ihnen finden, erfährt niemand sonst.

UND EINE SACHE, DIE IMMER STIMMT

Die teuersten Befunde waren nie die kompliziertesten.

Ein Testzugang von 2019. Ein Erneuerungstoken ohne Ablauf. Ein Backup, das niemand zurückgespielt hat. Eine Berechtigungsprüfung, die es nur in der Oberfläche gab. Nichts davon erfordert besondere Fähigkeiten — nur jemanden, der einmal systematisch nachsieht.

Welches System trägt bei Ihnen das Geschäft?

Wir fangen nicht mit einem Angebot an, sondern mit dieser Frage. Daraus ergibt sich der Umfang — und meistens auch, dass er kleiner sein sollte als ursprünglich gedacht.

SCHRITT 1

Scoping-Gespräch

60 Minuten, unverbindlich. Am Ende steht ein Vorschlag für Umfang, Testart und Zeitfenster — oder die Empfehlung, es zu lassen.

kostenfrei

SCHRITT 2

Konfigurationsprüfung

Das Fundament: Zugänge, Härtung, Abhängigkeiten, Protokolle, Wiederherstellung. Der günstigste Einstieg mit dem höchsten Ertrag.

Festpreis • 2-3 Wochen

SCHRITT 3

Penetrationstest

Web-Anwendung oder API, Grey Box, mit Rules of Engagement, Bericht in zwei Teilen und Nachtest im Preis.

nach Aufwand • ab 4 Wochen

DANACH

Turnus & Verfahren

Prüfliste und Matrix bleiben bei Ihnen. Wiederholung jährlich und nach größeren Änderungen — begleitet oder eigenständig.

nach Vereinbarung

Anirudh Chawla

Founder & Senior Software Engineer • EaseWerk Digital

anirudh@easewerk.de +49 162 8893421 easewerk.de

OWASP • ASVS • API SECURITY • HARDENING • REPORTING • NACHTEST

Alle Projektdarstellungen sind anonymisiert; Systeme, Kennzahlen und Namen wurden verändert.
Prüfungen ausschließlich mit schriftlicher Autorisierung. Keine Rechtsberatung.