terreActive
terreActive
terreActive
terreActive

Success
Story

Penetrationstest für Webapplikation
Vertrauen ist gut, Kontrolle ist besser

Validierung der Sicherheit durch unabhängige Dritte sorgt für mehr Vertrauen.

Wie kann ein Unternehmen nachweisen, dass es sein Versprechen in Bezug auf Datensicherheit einhält? Ein von unabhängiger Stelle durchgeführter Penetrationstest liefert klare Ergebnisse. Im Fall von LegacyNotes, dem Dienstleister für digitale Nachlassplanung, hat er gezeigt, dass die Kundendaten dort in guten Händen sind.

Die bei LegacyNotes hinterlegten Daten könnten persönlicher nicht sein. Es handelt sich um Kundeninformationen in Form von vorsorge- und nachlassrelevanten Daten wie Vorsorgeauftrag und Patientenverfügung, Bankkonten und Versicherungen, soziale Netzwerke oder auch Bestattungswünsche.

Sämtliche dieser Angaben und Anweisungen für den Nachlass liegen verschlüsselt an einem sicheren, zentralen Ort, sind auffindbar, jederzeit und von überall zugänglich und ggf. veränderbar. Sie können gezielt mit Angehörigen und sonstigen Vertrauenspersonen geteilt werden – entweder sofort oder erst nach dem Tod.

Freundliche Hacker am Werk

Bei einem gemeinsamen Kick-off-Meeting zwischen terreActive und LegacyNotes wurde der Ablauf und Umfang der anzuwendenden Tests für die öffentlich zugängliche Webapplikation definiert. Die darauf durchgeführten Penetrationsversuche zielten darauf ab, mögliche Schwachstellen im System aufzuspüren und zu identifizieren. Es wurde berücksichtigt, dass sowohl potenzielle externe Angreifer, als auch solche mit bestehender Kundenbeziehung versuchen, unerlaubt an fremde Daten zu gelangen. LegacyNotes wurde laufend über den Fortschritt informiert.

Parallel zu den Tests wurden die Ergebnisse sämtlicher Untersuchungsschritte analysiert und in einem Audit-Bericht dokumentiert.

Audit für Transparenz und Sicherheit

Nach Abschluss der Tests wurde der Audit-Bericht dem Kunden zur Vorbereitung der Abschlussbesprechung zugestellt. Anlässlich dieser Besprechung wurde das Projekt und die erzielten Resultate präsentiert und Fragen geklärt. Mit einer Massnahmenempfehlung zur Behebung von Risiken wurde das Projekt abgeschlossen.

«Der Pentest von terreActive bestärkt uns in unserem zentralen Kundenversprechen: 'Wir bieten Ihnen die Datensicherheit, die wir uns auch für unsere eigenen Daten auf LegacyNotes wünschen.'» – so Thomas Jaggi, Mitgründer und Geschäftsführer von LegacyNotes.

Die Cyberkriminalität nimmt ständig zu und deren Vorgehensweise wird immer raffinierter. Sensible Kundendaten sind ein wertvolles, uns anvertrautes Gut und dürfen nicht in falsche Hände geraten. Gerade bei von extern zugänglichen Webapplikationen empfiehlt es sich daher, regelmässig wiederkehrende Audits einzuplanen. So werden in strukturierter Form Schwachstellen identifiziert und fortlaufend behoben.

«Die langjährigen Geschäftsbeziehungen der terreActive im Umfeld mit hochsensiblen Daten von Banken, Behörden und Versicherungen gaben uns das Vertrauen, auf den richtigen Partner für die Auditierung zu setzen.»

Thomas Jaggi, Geschäftsführer

LegacyNotes

Ein gutes Gefühl

Penetrationstests gelten als effizientes Werkzeug, um die Sicherheit von Applikationen zu durchleuchten und den status-quo zu hinterfragen. Im Falle von LegacyNotes herrscht nun die Gewissheit, dass sowohl bei der grundsätzlichen Architektur als auch bei der technischen Umsetzung die richtigen Entscheide getroffen wurden.

Für die Kunden ist dies ein wichtiges Signal. Sicherheit versprechen ist einfach, Sicherheit liefern ist anspruchsvoll.

Zusatznutzen

- Im Zuge des Penetrationstests wurden en passant noch weitere sicherheitsrelevante Fragen in Bezug auf Zugriffsregeln von Kunden und deren eingesetzte Stellvertreter geklärt.
- Eine weitere positive Folgeerscheinung eines Audits bzw. eines Penetrationstests ist die gesteigerte Security-Awareness bei Mitarbeitenden.
- Die Einbettung der Online-Zahlung muss möglichst nahe an der Applikation bleiben, damit kein Zweifel an der Vertrauenswürdigkeit aufkommt. Gleichzeitig muss sie aber gut isoliert werden, um Angriffe über den Zahlungsdienstleister auszuschliessen. Beim Projektabschluss wurden Varianten besprochen, wie diese Anforderung umgesetzt werden kann.

Vorgehensweise Penetrationstest

ASVS (Application Security Verification Standard) gemäss OWASP (Open Web Application Security Project).

Der ASVS ist eine Sammlung von etablierten Best Practices für die sichere Implementation von Webapplikationen. Die Überprüfung kategorisiert die Umsetzung der Best Practices am Untersuchungsgegenstand in:

- Erfüllt oder nicht erfüllt.
- Nicht anwendbar, z. B. wenn die zu prüfende Funktionalität gar nicht vorhanden ist.
- Nicht prüfbar, z. B. wenn einzelne Themen von Beginn an vom Prüfumfang ausgeschlossen wurden.

LegacyNotes

Ist der persönliche, sichere und unabhängige Begleiter für die digitale Nachlassplanung. LegacyNotes erleichtert die administrative Arbeit und unterstützt die Liebsten, wenn man selber dazu nicht mehr in der Lage ist. Man kann auf einfache Art den Nachlass regeln, wichtige Daten sichern und die Handhabung seiner digitalen Accounts bestimmen.

Die Vision:
Kein Mensch verlässt diese Welt, ohne alles für seine Liebsten geregelt zu haben.

www.legacynotes.ch

Audits und ASVS Best Practice

Im Folgenden ein Ausschnitt einer möglichen Darstellung zum Erfüllungsgrad. Dieses Beispiel versteht sich losgelöst vom hier geschilderten Projekt.

ID	ASVS Best Practice	Rating
P1	Die Anwendung verfügt über ausreichende Anti-Automatisierungskontrollen um Datenexfiltration, übermässigen Gebrauch von Funktionen, übermässige Datei-Uploads oder Denial-of-Service-Angriffe zu erkennen und zu verhindern.	hoch
P2	Die Anwendung legt keine internen Informationen zu Infrastruktur oder Komponenten offen.	mittel
P3	Sicherstellen, dass eine Content Security Policy vorhanden ist, um Auswirkungen von XSS-Angriffen zu minimieren.	mittel
...	...	...