Pentest Factory GmbH

ZENTRALE
Walbecker Str. 53
47608 Geldern
Tel: +49 2831 12191 0

NIEDERLASSUNG BERLIN
Karl-Liebknecht-Str. 5
10178 Berlin
Tel: +49 30 4036367 60

NIEDERLASSUNG FRANKFURT
Olof-Palme-Str. 13
60439 Frankfurt
Tel: +49 69 9451569 50

KUNDENMITTEILUNG

Ergebnisse des Penetrationstests der Hintbox Webanwendung

für

lawcode GmbH

Universitätsstraße 3, 56070 Koblenz

DATUM
25.08.2021

VERSION
1.0

STATUS
FINAL

PENTEST-ID
LAWCODEPT-2
LAWCODEPT-5

PRÜFZEITRAUM
Juli / August 2021

Inhaltsverzeichnis

1. Management Summary

Dieses Dokument beschreibt die Ergebnisse des Penetrationstests für die lawcode GmbH (im Folgenden auch als „lawcode“ bezeichnet). Zweck des Penetrationstests war es, einen Überblick über den aktuellen Sicherheitsstatus der Hintbox Webanwendung sowie der unterliegenden IT-Infrastruktur von lawcode zu erhalten. Das Ziel bestand darin, Sicherheitsmängel zu identifizieren, eine Übersicht über die erkannten Schwachstellen zu erstellen sowie Empfehlungen zur Minimierung dieser Risiken zu geben.

Dieses Dokument beschreibt eine Zusammenfassung unserer Feststellungen des Penetrationstests. Den identifizierten Schwachstellen wird ein Risiko-Rating nach der OWASP-Risikobewertungsmethode[1] zugeordnet, welches auf Wahrscheinlichkeit und Auswirkung basiert.

Die folgenden Tests waren Bestandteil des Projekts:

» **Penetrationstest von Webanwendungen** aus der Perspektive eines externen Angreifers mit und ohne Zugangsdaten (Grey-Box), inklusive eines Infrastruktur-Scans mit dem folgenden Prüfumfang:

  – Hintbox Hinweisgebersystem; https://demo-pentest.hintbox.de

» **Wiederholungsprüfung (Re-Test)** des zuvor durchgeführten Penetrationstests, einschließlich der Prüfung von Mitigierungsmaßnahmen, die in Folge des ersten Penetrationstests durchgeführt wurden, um Schwachstellen zu beheben.

  – Hintbox Hinweisgebersystem; https://retest-pentest-demo.hintbox.de

1.1. Risikobeurteilung – Hintbox Webanwendung

Die nebenstehende Illustration stellt das Gesamtrisiko des getesteten Prüfobjekts nach Durchführung der Wiederholungsprüfung dar und basiert auf der höchsten Risikoeinstufung „**GERING**“ einer identifizierten Feststellung.

Während des Re-Tests wurden keine Sicherheitsprobleme mit einem mittleren, hohen oder kritischen Risiko identifiziert. Eine erfolgreiche Kompromittierung der Hintbox Webanwendung ist demnach unwahrscheinlich.

Pentest Factory GmbH – Geldern, 25.08.2021

Laurent Vetter
[Senior Penetration Tester]

Andres Rauschecker
[Senior Penetration Tester]

[1] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

2. Auftrag und Hintergrund

2.1. Projekthintergrund

Cyber-Angriffe stellen immer häufiger ein Hindernis dar, dem sich Unternehmen weltweit stellen müssen. Infolgedessen sind Unternehmen dazu gezwungen, ihre Sicherheitsmaßnahmen stetig zu verbessern, um sich effektiv gegen diese Bedrohungen zu verteidigen.

Die lawcode GmbH möchte die Vertraulichkeit, Integrität und Verfügbarkeit seiner IT-Assets innerhalb seiner IT-Infrastruktur sicherstellen. Zur Ermittlung des aktuellen Sicherheitsstands seiner Hintbox Webanwendung und unterliegenden IT-Infrastruktur wurde die Pentest Factory GmbH mit der Durchführung eines Penetrationstests inklusive Wiederholungsprüfung beauftragt.

2.2. Ziel, Umfang und Methodik des Projekts

Das Ziel des Tests bestand darin, mögliche Sicherheitsschwächen zu identifizieren, welche Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit der innerhalb der Hintbox Webanwendung und IT-Infrastruktur von lawcode verarbeiteten Informationen haben. Dieses Kapitel beschreibt die innerhalb des Projekts durchgeführten Leistungen.

Penetrationstest von Webanwendungen

Der „Penetrationstest von Webanwendungen“ beinhaltete eine umfassende Sicherheitsanalyse der „Hintbox“ Webanwendung auf Anwendungs- und Netzwerkebene. Unsere Tests auf Netzwerkebene beinhalteten einen automatisierten Schwachstellenscan sowie eine manuelle Analyse aller vom Anwendungsserver bereitgestellten Netzwerkdienste aus der Perspektive eines externen Angreifers (Black-Box). Die Tests auf Anwendungsebene wurden mit einem semi-manuellen Ansatz mit und ohne gültige Nutzerzugangsdaten (Grey-Box) durchgeführt.

Die folgenden URLs wurden im Projektumfang des Penetrationstests untersucht:

» https://demo-pentest.hintbox.de

Wiederholungsprüfung (Re-Test)

Der Re-Test beinhaltete die Verifizierung durchgeführter Maßnahmen zur Behebung identifizierter Schwachstellen des zuvor durchgeführten Penetrationstest von Webanwendungen.

Das folgende Prüfobjekt wurde im Projektumfang der Wiederholungsprüfung untersucht:

» https://retest-pentest-demo.hintbox.de

2.3. Testzeitraum

Die einzelnen Tests wurden im folgenden Zeitraum durchgeführt:

Penetrationstest	Startdatum	Enddatum
Penetrationstest von Webanwendungen – LAWCODEPT-2	26.07.2021	30.07.2021
Wiederholungsprüfung (Re-Test) – LAWCODEPT-5	24.08.2021	25.08.2021

Tabelle 1: Zeitfenster für die Durchführung der Penetrationstests

2.4. Angewandte Methodiken bei der Durchführung des Penetrationstests

Bei der Durchführung von Penetrationstests orientiert sich die Pentest Factory GmbH an bewährten Testvorgaben von OWASP und OSSTMM.

Innerhalb von Infrastrukturtests wurden die folgenden Tests durchgeführt:

» Passive Analyse von öffentlich verfügbaren Informationen über die Zielorganisation

» Identifikation von verfügbaren Netzwerkdiensten

» Manuelle Sicherheitsanalyse der identifizierten Netzwerkdienste

» Automatisierte Schwachstellenscans der im Umfang des Projekts definierten Infrastruktur

» Manuelle Verifizierung der im Schwachstellenscan identifizierten Feststellungen

Für Anwendungstests wurden alle typischen Tests durchgeführt, die im OWASP Testing Guide[2] (Version 4) beschrieben sind:

» Informationsbeschaffung

» Testen des Konfigurations- und Bereitstellungsmanagements

» Testen des Identitätsmanagements

» Tests der Authentifizierungsverfahren

» Tests der Berechtigungen

» Tests des Session-Managements

» Tests der Eingabe- und Ausgabevalidierung

» Kryptographie

» Fehlerbehandlung

» Plausibilitätsprüfung

» Tests der Client-Seite

[2] https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

3. Anhang

3.1. Methodik der Risikobewertung

Auswirkung

Die Abschätzung der Auswirkungen eines erfolgreichen Angriffs basiert auf zwei Faktoren. Zum einen den „technischen“ Auswirkungen (Technical Impact), welche mögliche Auswirkungen eines erfolgreichen Angriffs auf die vom Zielsystem/Anwendung verarbeiteten Daten widerspiegeln:

» Vertraulichkeit: Wie viele Daten könnten offengelegt werden und wie sensibel sind diese?

» Integrität: Wie viele Daten könnten manipuliert werden?

» Verfügbarkeit: Könnte das Problem zu Datenverlust oder Unterbrechung des Dienstes führen?

» Nachvollziehbarkeit: Ist es möglich den Angreifer zurückzuverfolgen?

Zum anderen den Auswirkungen auf die Organisation (Business Impact), welche mögliche Auswirkungen widerspiegeln, die ein erfolgreicher Angriff auf das Unternehmen selbst haben könnte:

» Finanzieller Schaden: Würde ein erfolgreicher Angriff finanzielle Schäden verursachen?

» Reputationsschäden: Würde ein erfolgreicher Angriff Reputationsschäden verursachen?

» Compliance-Probleme: Führt die identifizierte Schwachstelle zu Problemen bei der Compliance?

» Verletzung der Privatsphäre: Werden durch die identifizierte Schwachstelle personenbezogene Daten offengelegt?

Einige Faktoren, insbesondere welche Auswirkungen die identifizierten Schwachstellen auf die Organisation haben könnten, erfordern zusätzliche Informationen wie finanzielle Hintergründe, Reputationsrisikobewertung, rechtliche Konsequenzen usw., welche über den Umfang eines Penetrationstests hinausgehen. Aus diesem Grund werden die Auswirkungen auf Grundlage bisheriger Projekterfahrungen bewertet.

Die Bewertung von Auswirkungen wird wie folgt definiert:

Hoch: Schwachstellen, die es Angreifern ermöglichen, unbefugt auf hochsensible Informationen zuzugreifen, diese zu manipulieren (z. B. Finanzdaten, Zugangsdaten, Kundendaten) oder beliebige Befehle auf dem Zielsystem auszuführen. Diese Schwachstellen können es einem Angreifer ermöglichen, einem Unternehmen finanziellen Schaden oder Reputationsschäden zuzufügen, die zu Kundenunzufriedenheit führen können. Weiterhin können sie dazu führen, dass auf andere interne Systeme zugegriffen werden kann oder hohe Privilegien erworben werden können.

Mittel: Schwachstellen, die es Angreifern ermöglichen, die Reputation eines Unternehmens in begrenztem Umfang zu schädigen oder sich unbefugten Zugang zu sensiblen Funktionen oder Informationen zu verschaffen. Die Privilegien, die ein Angreifer durch Missbrauch dieser Schwachstellen erlangen kann, sind begrenzt.

Gering: Schwachstellen, die keine direkte Gefahr darstellen, jedoch eine Plattform für weitere Angriffe bieten könnten. Diese Schwachstellen können es einem Angreifer ermöglichen, Berechtigungen auf eine sehr beschränkte Ebene zu heben.

Eintrittswahrscheinlichkeit

Die Abschätzung der Wahrscheinlichkeit eines erfolgreichen Angriffs basiert ebenfalls auf zwei Faktoren. Die Threat Agent Factors, welche mit dem böswilligen Angreifer in Verbindung stehen, sowie die Eigenschaften der Schwachstelle.

Die Threat Agent Factors sind:

» Technische Fähigkeiten: Welche technischen Fähigkeiten sind erforderlich, um das Problem zu missbrauchen?

» Motiv: Welche Vorteile hat es für einen Angreifer, das Problem zu missbrauchen?

» Gelegenheit: Welche Ressourcen und Bedingungen sind erforderlich, um das Problem zu missbrauchen?

» Größe: Welcher Zugang ist notwendig, um das Problem zu missbrauchen?

Die Faktoren für Schwachstellen sind:

» Auffindbarkeit: Wie schwierig ist es, die Schwachstelle zu entdecken?

» Ausnutzbarkeit: Wie schwierig ist es, das Problem auszunutzen?

» Bekanntheitsgrad: Ist die Schwachstelle allgemein bekannt?

» Erkennbarkeit des Eindringens: Ist es möglich den Angriff zu erkennen?

Die Bewertung von Auswirkungen wird wie folgt definiert:

Hoch: Zur Entdeckung und Ausnutzung des Problems sind beschränkte technische Fähigkeiten erforderlich. Automatisierte Tools können zur Aufdeckung des Problems verwendet werden. Techniken zum Ausnutzen der Schwachstelle sind allgemein bekannt. Darüber hinaus ist die verwundbare Funktion für eine große Zahl von Nutzern zugänglich.

Mittel: Zur Entdeckung und Ausnutzung des Problems sind technische Fähigkeiten erforderlich. Das Problem kann mit manuellen Penetrationstests entdeckt werden. Um das Problem auszunutzen, muss ein Angreifer einen nutzerdefinierten Exploit erstellen, jedoch sind ähnliche Exploits allgemein bekannt.

Gering: Zur Entdeckung und Ausnutzung des Problems sind fortgeschrittene technische Fähigkeiten erforderlich, oder das Problem ist nur einer kleinen Nutzergruppe zugänglich. Die Entdeckung ist kompliziert und erfordert manuelle Testmethoden. Der Exploit ist schwierig und erfordert fortgeschrittene technische Fähigkeiten und zusätzliche Ressourcen.

Risiko

Unsere Risikobewertungen basieren auf der OWASP-Risikobewertungsmethodik[3]. Die folgende Tabelle zeigt den verwendeten Ansatz der Risikobewertung.

Risikobewertung				
Auswirkung	**HOCH**	Mittel	Hoch	Kritisch
	MITTEL	Niedrig	Mittel	Hoch
	NIEDRIG	Informativ	Niedrig	Mittel
		NIEDRIG	**MITTEL**	**HOCH**
		Wahrscheinlichkeit		

Tabelle 2: Matrix zur Risikobewertung

Wir empfehlen die Durchführung einer separaten Risikoanalyse, die sich an Ihrer Methodik für die Risikobewertung des Informationssicherheitsmanagements orientiert und tiefer auf die Erfordernisse des Geschäfts und interne organisatorische Faktoren eingeht.

3.2. Weitere Informationen

Konfigurationsstatus / Schwachstellen

Die vorgenommenen Risikobewertungen basieren auf der Systemkonfiguration und den öffentlich zugänglichen Schwachstelleninformationen zum Zeitpunkt der durchgeführten Tests. Täglich werden neue Schwachstellen identifiziert und Systemkonfigurationen unterliegen häufigen Änderungen.

[3] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_5:_Deciding_What_to_Fix