Pentest

Pre-Assessment Checklist

automITe engineering GmbH

Version vom 28. Juli 2021

Im Rahmen des Penetrationstest simulieren wir einen Angreifer, der versucht in Ihr System einzudringen. Im Vergleich zu einem echten Angreifer gehen wir dabei aber nicht rücksichtslos vor, sondern arbeiten im Hinblick darauf Ihr System und Ihren Tagesablauf so wenig wie möglich zu beeinträchtigen. Damit uns dies zusammen mit Ihnen gelingt, und für den Fall das es doch zu Komplikationen kommt, benötigen wir im Vorfeld einige Informationen. Wir möchten Sie daher bitten diesen Bogen so gut wie Ihnen möglich ist auszufüllen. Wissen Sie einmal nicht weiter, so lassen Sie das Feld leer oder kontaktieren Sie uns unter den unten angegeben Kontaktdaten.
Schicken Sie uns bitte den ausgefüllten Bogen zurück, damit wir mit Ihnen das weitere Vorgehen abstimmen können.

---

1 Allgemeine Informationen

Aktuelles Datum:

Name des Unternehmen:

1.1 Autorisierungsberechtigung

Kontaktdaten der Person, die uns autorisiert ihr System zu testen:
Hinweis: Dieses Dokument dient **nicht** der Autorisierung zum Testen. Diese erfolgt später separat und muss von der hier genannten Person unterzeichnet werden.

Name:

E-Mail:

Telefon:

1.2 Ansprechpartner (organisatorisches)

Kontaktdaten der Person, die bei organisatorischen Fragen zur Verfügung steht:

Name:

E-Mail:

Telefon:

1.3 Ansprechpartner (technisches)

Kontaktdaten der Person, die bei technischen Fragen zur Verfügung steht:

Name:

E-Mail:

Telefon:

1.4 Notfallkontakt

Kontaktdaten der Person, die bei Notfällen zur Verfügung steht:

Name:

E-Mail:

Telefon:

1.5 Abschließender Bericht

Die E-Mail Adresse an die der abschließende Bericht geschickt werden soll:

Soll diese E-Mail verschlüsselt werden? Ja ☐ Nein ☐

1.6 Weiteres

Wurde bereits früher ein Pentest durchgeführt? Ja ☐ Nein ☐

Falls ja, wann war der letzte Pentest?

2 Scope (Webanwendung)

Unter Scope versteht man die zu testende Anwendung. In dieser Sektion wird dieses genauer bestimmt.

Beschreibung der Webanwendung u.a. auch Komplexität

Verwendete Technologien:

Hier ist Platz für sonstige Anmerkungen zu Dingen, die getestet werden sollen. Gibt es etwa Teile der Webanwendung, welche ausgeschlossen oder explizit getestet werden sollen:

3 Technische Fragen

In dieser Sektion versuchen wir im Vorfeld einige technische Fragen zu Ihrer Anwendung zu klären. Dies erleichtert uns und Ihnen im späteren Verlauf das Vorgehen. Sollten Sie die Antwort auf eine Frage nicht wissen, so lassen Sie das Feld leer.

Wird den Testern ein Backend der Webanwendung zum Testen zur Verfügung gestellt? (Nein, sofern das Backend lokal von den Testern aufgesetzt werden soll.) Ja ☐ Nein ☐

Die folgenden Fragen sind nur relevant, wenn das Backend zum Testen von Ihnen bereit gestellt wird, Sie also obige Frage mit Ja beantwortet haben.

Hosten Sie das Backend selber? Ja ☐ Nein ☐

Falls nein, bitte den Namen des Hostinganbieters eintragen

Falls nein, bitte den Namen des Hostinganbieters eintragen

Bitte kreuzen Sie an, ob Sie eine der folgenden Technologien einsetzen.

Web Application Firewall	Ja ☐	Nein ☐	Weiß nicht ☐
Intrusion Detection System (IDS)	Ja ☐	Nein ☐	Weiß nicht ☐
Intrusion Prevention System (IPS)	Ja ☐	Nein ☐	Weiß nicht ☐
Load Balancer	Ja ☐	Nein ☐	Weiß nicht ☐

Listen Sie bitte hier (falls vorhanden) Drittanbieter auf, die Sie in ihrer Infrastruktur verwenden. Dazu zählen zum Beispiel Hoster, Cloud Anbieter, externe APIs etc.

Erstellen Sie regelmäßig Backups? Ja ☐ Nein ☐

Falls ja, wann wurde das letzte Backup erzeugt?

4 Testdurchführung

Während wir zwar einen echten Angreifer simulieren, liegt uns doch viel daran Ihren tägliche Arbeitsablauf nicht zu stören, daher benötigen wir einige Informationen für eine reibungslose Testdurchführung.

Wird den Testern Dokumentation der Webanwendung zur Verfügung gestellt und falls ja welche Form hat diese (bspw. Dokumentation der API):

Wird den Testern Sourcecode zur Verfügung gestellt und falls ja von welchen Komponenten:

Wann soll der Pentest stattfinden (der Zeitpunkt kann auch grob eingegrenzt werden, bspw. 4. Quartal):

Die folgenden Fragen sind nur relevant, wenn das Backend zum Testen von Ihnen bereit gestellt wird.

In welchen Zeiträumen (Uhrzeit und/oder Wochentag) ist die Testdurchführung ungünstig? (leer lassen, falls keine Präferenzen bestehen). Einflussfaktoren können Dinge sein wie tägliche Backups, Updatezyklen, Zeiten hoher Auslastung etc.

Ist ihr interner Systemadmin (oder falls sie keinen Systemadmin haben, die Person, die einem Systemadmin am nächsten kommt) über den Test informiert? Ja ☐ Nein ☐

Haben Sie eine Entwicklungsumgebung in der getestet werden kann? Ja ☐ Nein ☐

Falls den Testern Informationen oder Dokumente in anderer Weise zur Verfügung gestellt werden, diese bitte hier auflisten. Die könnten zum Beispiel VPN Zugänge, Zugangsdaten für Testaccounts oder Ähnliches sein.
Bitte keine Zugangsdaten oder Ähnliches hier notieren. Lediglich vermerken, dass diese weitergegben worden sind, damit nach dem Test alles wieder zurückgegeben bzw. zurückgesetzt werden kann.

5 Unsere Kontaktdaten

Sollten Sie Probleme beim Ausfüllen dieses Bogens oder andere Fragen rund um den Penetrationstest haben, zögern Sie bitte nicht uns unter den folgenden Kontaktdaten zu erreichen:

Adresse: automITe engineering GmbH
Isaac-Newton-Straße 8 - 23562 Lübeck

Telefon: 04 51 / 39 77 10

E-Mail: info@automite.de

---

automITe