1 Allgemeines

1.1 Ansprechpartner

1.2 Informationen

- Alle Inhalte, auch die dieses Gesprächs, werden vertraulich behandelt
- Schäden werden ausgeschlossen
- Ein Pentest hat nie einen Anspruch auf Vollständigkeit

1.3 Eingrenzung

Welche Art/en von Pentest/s sollen durchgeführt werden?

☐ Web-Application ⇒ Punkt 2 ausfüllen

☐ Network ⇒ Punkt 3 ausfüllen

☐ Social Engineering ⇒ Punkt 4 ausfüllen

☐ Wireless ⇒ Punkt 5 ausfüllen

☐ Physical ⇒ Punkt 6 ausfüllen

Die Punkte 1.4, 7 und 8 sollten immer ausgefüllt werden, unabhängig von der/den oben gewählten Art/en.

1.4 Allgemeine Fragen

Ist der Test für eine spezielle Compliance-Anforderung notwendig?	Ja	Nein
_____	☐	☐

Wann soll der Test statt finden?
_____

In welchen Zeiträumen soll der Test durchgeführt werden?		
Bürozeiten ☐	Feierabend ☐	Wochenende ☐

2 Web Application Penetration Test

Wird der Quellcode der Applikation/Webseite zugänglich gemacht?	Ja	Nein
	☐	☐

Wie viele Web-Applikationen sind In-Scope?

Wie viele Login-Systeme sind In-Scope?

Wie viele statische Seiten sind ca. In-Scope?

Wie viele dynamische Seiten sind ca. In-Scope?

Soll Fuzzing gegen die Applikation/en eingesetzt werden?	Ja ☐	Nein ☐

Soll der Penetrations-Test aus verschiedenen Rollen durchgeführt werden?	Ja	Nein
	☐	☐

Sollen Password-Scans auf die Webseite durchgeführt werden?	Ja ☐	Nein ☐

3 Network Penetration Test

Was ist das Ziel des Penetrations-Test?

Wie viele IP-Adressen sollen getestet werden?

Sind Techniken im Einsatz, die die Resultate verfälschen könnten? (WAF, IPS etc.?)	Ja	Nein
_____	☐	☐

Wie ist das Vorgehen bei einem gelungenen Angriff?
_____

Soll versucht werden lokale Admin-Rechte zu erlangen und tiefer in das Netz vorzudringen?	Ja	Nein
_____	☐	☐

Sollen Angriffe auf gefundene Passwort-Hashes durchgeführt werden?	Ja ☐	Nein ☐

4 Social Engineering

Gibt es eine vollständige Liste von E-Mail-Adressen, die für den Test verwendet werden können?	Ja ☐	Nein ☐
Gibt es eine vollständige Liste von Telefon-Nummern, die für den Test verwendet werden können?	Ja ☐	Nein ☐
Ist das Einsetzen von Social Engineering zum Überwinden physikalischer Sicherheitseinrichtungen erlaubt?	Ja ☐	Nein ☐

Wie viele Personen sollen ca. getestet werden?
_____

5 Wireless Network Penetration Test

Wieviele Funk-Netzwerke sind im Einsatz?

Gibt es eine Gäste WLAN? Wenn ja, wie ist dieses Umgesetzt?	Ja	Nein
	☐	☐

Welche Verschlüsselung wird für die Netzwerke genutzt?

Sollen nicht-firmen-Geräte im WLAN aufgespürt werden?	Ja ☐	Nein ☐

Soll Netz-Attacken gegen Clients durchgeführt werden?	Ja ☐	Nein ☐

Wie viele Clients nutzen das WLAN ca.?

6 Physical Penetration Test

Wie viele Einrichtungen sollen getestet werden?

Wird die Einrichtung mit anderen Parteien geteilt?	Ja ☐	Nein ☐

Muss Sicherheitspersonal umgangen werden?	Ja ☐	Nein ☐

Wird das Sicherheitspersonal durch einen Dritten gestellt?	Ja	Nein
	☐	☐

Ist das Sicherheitspersonal bewaffnet?	Ja ☐	Nein ☐

Ist der Einsatz von körperlicher Gewalt durch das Sicherheitspersonal gestattet?	Ja ☐	Nein ☐

Wie viele Eingänge gibt es zu der/den Einrichtung/en?
_____

Ist das knacken von Schlössern oder fälschen von Schlüsseln erlaubt?	Ja ☐	Nein ☐

Wie groß ist die Fläche ungefähr?
_____

Sind alle physikalischen Sicherheitsmaßnahmen dokumentiert und werden zur Verfügung gestellt?	Ja	Nein
_____	☐	☐

Werden Video-Kameras verwendet?	Ja ☐	Nein ☐

Werden diese Kameras durch Dritte verwaltet?	Ja	Nein
_____	☐	☐

Soll versucht werden, die aufgezeichneten Daten zu löschen?	Ja ☐	Nein ☐

Gibt es ein Alarm-System?	Ja ☐	Nein ☐

Gibt es einen Stillen Alarm?	Ja ☐	Nein ☐

Welche Ereignisse lösen den Alarm aus?	Ja ☐	Nein ☐

7 Questions for Systems Administrators

Gibt es Systeme, die als instabil angesehen werden (alte Patch-Stände, Legacy Systeme etc.)?	Ja	Nein
_____	☐	☐

Gibt es Systeme von Dritten, die ausgeschlossen werden müssen oder für die weitere Genehmigungen notwendig sind?	Ja	Nein
_____	☐	☐

Was ist die Durchschnittszeit zur Wiederherstellung der Funktionalität eines Services?
_____

Ist eine Monitoring-Software im Einsatz?	Ja ☐	Nein ☐

Welche sind die kritischsten Applikationen?
_____

Werden in einem regelmäßigen Turnus Backups erstellt und getestet?	Ja ☐	Nein ☐

8 Questions for Business Unit Managers

Ist die Führungsebene über den Test informiert?	Ja ☐	Nein ☐

Welche Daten stellen das größte Risiko dar, falls diese manipuliert werden?
_____

Gibt es Testfälle, die die Funktionalität der Services prüfen und belegen können?	Ja ☐	Nein ☐

Sind "Disaster Recovery Procedures" vorhanden?	Ja ☐	Nein ☐