

## 1 Allgemeines

### 1.1 Ansprechpartner

- 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 den oben gewählten Art/en.

### 1.4 Allgemeine Fragen

Ist der Test für eine spezielle Compliance-Anforderung notwendig?	Ja	Nein
_____	<input type="checkbox"/>	<input type="checkbox"/>

Wann soll der Test statt finden?
_____

Unternehmen	Pentester
Straße Nr	Tel
PLZ Ort	E-Mail
USTID	Webseite

## 2 Web Application Penetration Test

Wird der Quellcode der Applikation/Webseite zugänglich gemacht?	Ja	Nein
_____	<input type="checkbox"/>	<input type="checkbox"/>
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?		
_____		
In welchen Zeiträumen soll der Test durchgeführt werden?		
Bürozeiten <input type="checkbox"/>	Feierabend <input type="checkbox"/>	Wochenende <input type="checkbox"/>
Soll Fuzzing gegen die Applikation/en eingesetzt werden?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Soll der Penetrations-Test aus verschiedenen Rollen durchgeführt werden?	Ja	Nein
_____	<input type="checkbox"/>	<input type="checkbox"/>
Sollen Password-Scans auf die Webseite durchgeführt werden?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>

Unternehmen	Pentester
Straße Nr	Tel
PLZ Ort	E-Mail
USTID	Webseite

### 3 Network Penetration Test

Was ist das Ziel des Penetrations-Test?		
In welchen Zeiträumen soll der Test durchgeführt werden?		
Bürozeiten <input type="checkbox"/>	Feierabend <input type="checkbox"/>	Wochenende <input type="checkbox"/>
Wie viele IP-Adressen sollen getestet werden?		
Sind Techniken im Einsatz, die die Resultate verfälschen könnten? (WAF, IPS etc.?)	Ja	Nein
	<input type="checkbox"/>	<input type="checkbox"/>
Wie ist das Vorgehen bei einem gelungenen Angriff?		
Soll versucht werden lokale Admin-Rechte zu erlangen und tiefer in das Netz vorzudringen?	Ja	Nein
	<input type="checkbox"/>	<input type="checkbox"/>
Sollen Angriffe auf gefundene Passwörter durchgeführt werden?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>

### 4 Social Engineering

Gibt es eine vollständige Liste von E-Mail-Adressen, die für den Test verwendet werden können?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Gibt es eine vollständige Liste von Telefon-Nummern, die für den Test verwendet werden können?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Ist das Einsetzen von Social Engineering zum Überwinden physikalischer Sicherheitseinrichtungen erlaubt?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>

Unternehmen	Pentester
Straße Nr	Tel
PLZ Ort	E-Mail
USTID	Webseite

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

☐

☐

Unternehmen	Pentester
Straße Nr	Tel
PLZ Ort	E-Mail
USTID	Webseite

Wird das Sicherheitspersonal durch einen Dritten gestellt?	Ja	Nein
_____	<input type="checkbox"/>	<input type="checkbox"/>
Ist das Sicherheitspersonal bewaffnet?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Ist der Einsatz von körperlicher Gewalt durch das Sicherheitspersonal gestattet?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Wie viele Eingänge gibt es zu der/den Einrichtung/en?		
_____		
Ist das knacken von Schlössern oder fälschen von Schlüsseln erlaubt?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Wie groß ist die Fläche ungefähr?		
_____		
Sind alle physikalischen Sicherheitsmaßnahmen dokumentiert und werden zur Verfügung gestellt?	Ja	Nein
_____	<input type="checkbox"/>	<input type="checkbox"/>
Werden Video-Kameras verwendet?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Werden diese Kameras durch Dritte verwaltet?	Ja	Nein
_____	<input type="checkbox"/>	<input type="checkbox"/>
Soll versucht werden, die aufgezeichneten Daten zu löschen?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Gibt es ein Alarm-System?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Gibt es einen Stillen Alarm?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>

Unternehmen	Pentester
Straße Nr	Tel
PLZ Ort	E-Mail
USTID	Webseite

Welche Ereignisse lösen den Alarm aus?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
--	--------------------------------	----------------------------------

## 7 Questions for Systems Administrators

Gibt es Systeme, die als instabil angesehen werden (alte Patch-Stände, Legacy Systeme etc.)?	Ja	Nein
_____	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es Systeme von Dritten, die ausgeschlossen werden müssen oder für die weitere Genehmigungen notwendig sind?	Ja	Nein
_____	<input type="checkbox"/>	<input type="checkbox"/>
Was ist die Durchschnittszeit zur Wiederherstellung der Funktionalität eines Services?		
_____		
Ist eine Monitoring-Software im Einsatz?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Welche sind die kritischsten Applikationen?		
_____		
Werden in einem regelmäßigen Turnus Backups erstellt und getestet?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>

## 8 Questions for Business Unit Managers

Ist die Führungsebene über den Test informiert?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
Welche Daten stellen das größte Risiko dar, falls diese manipuliert werden?		
_____		
Gibt es Testfälle, die die Funktionalität der Services prüfen und belegen können?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>

Unternehmen	Pentester
Straße Nr	Tel
PLZ Ort	E-Mail
USTID	Webseite

Sind "Disaster Recovery Procedures" vorhanden?	Ja <input type="checkbox"/>	Nein <input type="checkbox"/>
--	--------------------------------	----------------------------------

<i>Unternehmen</i>	<i>Pentester</i>
<i>Straße Nr</i>	<i>Tel</i>
<i>PLZ Ort</i>	<i>E-Mail</i>
<i>USTID</i>	<i>Webseite</i>