Permission to Attack – Penetration Test Agreement

Autor	Datum	Version	Klassifizierung	Prüfzyklus	Nächste Prüfung	Kommentar/ Änderungen
Dipl.-Ing. Daniel Mrskos, Bsc	11.06.2024	1.0	**streng geheim**	Jährlich	Juni 2025	Active Directory und Webshop

Diese Vereinbarung wird geschlossen zwischen der Firma

Your Name Here GmbH
AT-1234 Your City Here
Your Street Here 123

Von nun an Auftraggeber genannt.
und der Firma

Security mit Passion
Peygarten-Ottenstein 2/a/7
3532, Rastenfeld

Von nun an Penetration Tester genannt.

Kontaktinformationen:

Projektleitung Ziel Organisation (Solution Architecture):

Kontakt: Max Musterman
Telefon: +43 664 12 34 56 7
E-Mail: max.mustermann@idontexist

Sekundär-Projektleitung Ziel Organisation (Security Engineer):

Kontakt: Max Musterman
Telefon: +43 664 12 34 56 7
E-Mail: max.mustermann@idontexist

Management Kontakt Ziel Organisation (CISO):

Kontakt: Max Musterman
Telefon: +43 664 12 34 56 7
E-Mail: max.mustermann@idontexist

Primärer Kontakt SMP (Penetration Tester & Projektleitung):

Kontakt: Dipl.-Ing. Daniel Mrskos, BSc
Telefon: +43 664 12 34 56 7
E-Mail: daniel.mrskos@security-mit-passion.at

Sekundärer Kontakt SMP (Penetration Testing und Quality Assurance):

Kontakt: Julia Mrskos
Telefon: +43 664 12 34 56 7
E-Mail: julia.mrskos@security-mit-passion.at

Ablauf des Penetration Tests

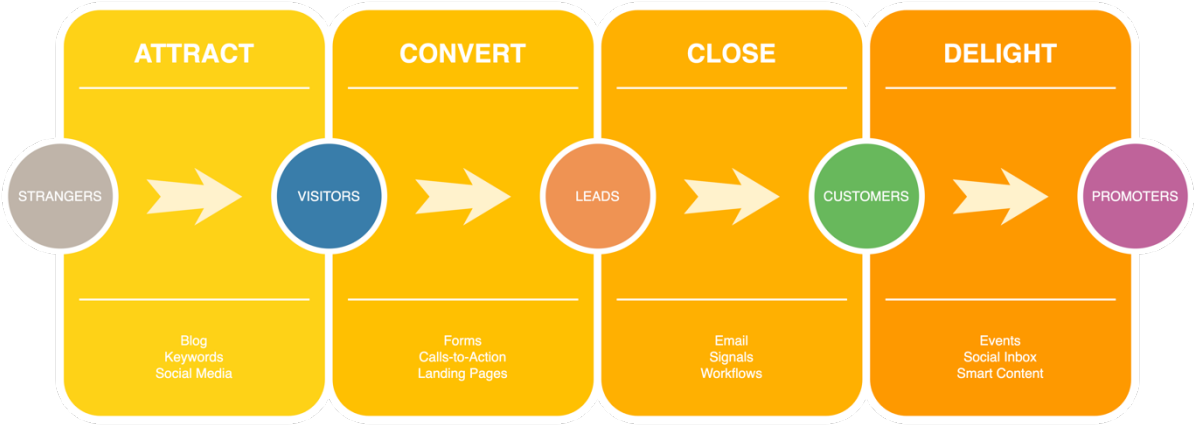
Vertraulichkeit

Dieses Dokument ist als streng vertraulich anzusehen.

Ziel des Penetration Tests

*Im Allgemeinen ist es das Ziel dieses Penetration Tests, die neuentwickelten Webshop-Komponenten und Active Directory Komponenenten der Firmeninfrastruktur von der **Your Name Here GmbH** zu prüfen. Dazu müssen im Rahmen eines Penetration Tests Angriffe durchgeführt werden, als würden echte Hacker die IT-Systeme penetrieren. Es ist daher maßgeblich erforderlich die Permission to Attack rechtsgültig ausgefüllt und unterschrieben zu haben. Der Penetration Tester handelt im Auftrag und vor allem unter dem Motto der Verbesserung der IT-Sicherheit des Auftraggebers. Am Ende des Penetration Tests ist ein Abschlussbericht mit den Findings und Empfehlungen zur Behebung dieser Sicherheitsrisiken vorgesehen. Es kann ebenso eine Abschlusspräsentation vereinbart werden.*

Visualisierung des Scopes/Business Prozesses



Permission to Attack

Mit dieser Vereinbarung wird der Penetration Tester beauftragt, IT Security Penetration- und/oder Social Engineering Tests, einerseits zur Erhebung der Sicherheit der IT-Systeme und andererseits des Sicherheitsbewusstseins der MitarbeiterInnen von dem Auftraggeber durchzuführen.

1. Der Penetration Tester ist berechtigt, mittels der im Scope definierten Techniken auf Basis von Penetration- und/oder Social Engineering-Tests oder forensischen Analysen vertrauliche Informationen wie Zugangsdaten abzugreifen, Schadcode ins Unternehmen einzuschleusen und/oder die IT-Systeme des Auftraggebers zu überprüfen. Je nach Definition der Techniken im Scope ist es dem Penetration Tester ausdrücklich erlaubt, die Organisation und die IT-Systeme des Auftraggebers über alle Extern und Intern erreichbaren Zutrittspunkte (bspw. Internet, WLAN, LAN, Remote Standorte, Webseiten- und Applikationen, etc.) zu testen, zu attackieren und gegebenenfalls Daten auszuspähen. Weiterhin ist es dem Penetration Tester je nach Definition der Techniken im Scope ausdrücklich erlaubt, die Organisation mittels Social Engineering Angriffs-Techniken zu testen.

2. Im Rahmen der im Scope definierten Tests und Maßnahmen kann es zu Abstürzen oder Fehlfunktionen von IT-Systemen des Auftraggebers kommen. Der Penetration Tester wird alles Zumutbare unternehmen, um Systemausfälle zu vermeiden. Der Penetration Tester haftet nicht für etwaige Ausfälle und daraus resultierenden Schäden welcher Art auch immer, soweit diese nicht grob fahrlässig oder vorsätzlich herbeigeführt wurden.
3. Dem Auftraggeber ist bekannt, dass die im Scope definierten Tests und Maßnahmen zu Ausfällen und Problemen bei der IT-Infrastruktur führen können mit allen damit verbundenen Folgen. Der Penetration Tester haftet nicht für etwaige Ausfälle und daraus resultierenden Schäden welcher Art auch immer oder Verlust von Daten, soweit diese nicht grob fahrlässig oder vorsätzlich herbeigeführt wurden. Sollte Dritten Schaden entstehen bzw. Dritte Ansprüche welcher Art auch immer geltend machen, hat der Auftraggeber den Penetration Tester gegenüber diesen Dritten schad- und klaglos zu halten.
    I. Penetration Test (extern und intern): Bei der Prüfung der Cybersecurity von extern wie auch von intern kann es zu unerwarteten Reaktionen des IT-Systems des Auftraggebers kommen, da eine aufgefundene Schwachstelle entsprechend ausgenutzt wird, um deren Auswirkung auf das IT- System beurteilen zu können. So ist es selbst bei sachgerechter Durchführung der im Scope definierten Tests und Maßnahmen nicht auszuschließen, dass etwa Produktionssysteme beeinträchtigt werden und Maschinen ausfallen. Der Auftraggeber ist sich dieses Risikos bewusst.
    II. Website Penetration Test: Bei der Prüfung von Websites und Online Shops können Dritte geschädigt werden, sofern die Systeme des Auftraggebers nicht im eigenen Rechenzentrum, sondern bei einem externen Provider gehostet sind und dieser am Webserver nicht nur die Website des Auftraggebers verwaltet. Diesfalls hat der Auftraggeber eine Abklärung mit dem Provider und allfälligen Dritten herbeizuführen und deren Zustimmung einzuholen.
    III. Social Engineering (z.B. Media Droping, Phishing Attacks, externe Dienstleister): Beim Media Droping ist vorgesehen, dass keine Rückschlüsse auf bestimmte Personen möglich sind. Wird dies vom Auftraggeber dennoch gewünscht, muss der Auftraggeber eine Abklärung mit diesem Dritten herbeiführen und dessen Zustimmung einholen. Bei der Prüfung externer Dienstleister hat der Auftraggeber eine Abklärung mit dem jeweiligen externen Dienstleister herbeizuführen und deren Zustimmung einzuholen.

IV. Cloud Security Tests. In Rahmen dieser Tests müssen vom Auftraggeber die notwendigen Einverständniserklärungen von den Cloud Anbietern eingeholt werden. Ebenso müssen diese vor dem Penetration Test informiert werden.

4. Der Auftraggeber erkennt an, dass er die alleinige Verantwortung für den angemessenen Schutz und die Sicherung von Daten und/oder Geräten hat, die im Zusammenhang mit diesem IT Security Penetration Test verwendet werden.

5. Der Auftraggeber bestätigt, dass er berechtigt ist, IT Security Penetration Tests bei Systemen, welche sich nicht oder nicht ausschließlich in eigenständiger Befugnis befinden, durchzuführen bzw. ist dafür verantwortlich, ein solches Recht vom rechtmäßigen Eigentümer der Systeme einzuholen.

6. Sofern Systeme Bestandteil der Prüfungen sind, welche sich nicht oder nicht ausschließlich in eigenständiger Befugnis des Auftraggebers befinden, so ist der Auftraggeber über die Unterrichtung der Dritten Parteien allein verantwortlich. Der Auftraggeber hält diesbezüglich den Penetration Tester gegen jegliche Ansprüche Dritter schad- und klaglos.

7. Der Penetration Tester verpflichtet sich zeitlich unbefristet, weder im Zuge der Überprüfungen erlangte Daten, Informationen über das Netzwerk des Auftraggebers, noch die Ergebnisse der Überprüfung an Dritte weiterzugeben oder sonst irgendwie zu verwenden bzw. preiszugeben. Alle Ergebnisse gelten als streng vertraulich und werden als solche behandelt.

8. Der Penetration Tester verpflichtet sich, sämtliche erlangten personenbezogenen Daten nach der Datenschutzgrundverordnung und national geltenden Datenschutzgesetze zu behandeln.
   Insbesondere gelten die folgenden Bestimmungen:

   I. Der Penetration Tester verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden und ausschließlich dem Auftraggeber zurückzugeben oder nur nach dessen schriftlichem Auftrag zu übermitteln. Eine Verwendung der überlassenen Daten für eigene Zwecke des Penetration Tester bedarf eines schriftlichen Auftrages.

   II. Der Penetration Tester erklärt, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Einhaltung des Datenschutzes verpflichtet hat. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit dem Datenverkehr beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Dienstleister aufrecht.

   III. Der Penetration Tester erklärt, dass er ausreichende Sicherheitsmaßnahmen ergriffen hat, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden.

   IV. Der Penetration Tester trägt für die technischen und organisatorischen Penetration Tester Vorsorge, dass der Auftraggeber die gesetzlichen Bestimmungen (Auskunftsrecht, Recht auf Richtigstellung oder Löschung,

Recht auf Einschränkung der Datenverarbeitung, Recht auf Datenübertragbarkeit, Recht auf Widerspruch) gegenüber dem Betroffenen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.

V. Der Penetration Tester ist nach Beendigung der Dienstleistung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder auftragsgemäß zu vernichten.

VI. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht zur Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen, innerhalb eines angemessenen Zeitraums, eingeräumt. Der Penetration Tester verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

9. Der Auftraggeber nimmt zur Kenntnis, dass die Ergebnisse der IT Security Penetration Tests zwar hinreichend genauen Überblick über das aktuelle Sicherheitsniveau der getesteten Systeme bzw. von der IT-Sicherheits-Organisation oder Prozessen liefern, der Penetration Tester jedoch nicht für bestimmte Sicherheits- oder Konfigurationsprobleme der Zielsysteme bzw. organisatorische Mängel, welche während der Tests nicht zum Vorschein kamen, verantwortlich gemacht werden kann.

10. Sämtliche Informationen werden elektronisch auf einem AES 128-Bit verschlüsselten Datenträger, auf welchen nur die handelnden Personen des Penetration Testers Zugriff haben, aufbewahrt.

11. Nach Fertigstellung der Überprüfungen und Präsentation des Abschlussberichtes werden sämtliche Daten auf einem AES 128-Bit verschlüsselten Datenträger für 6 Monate aufbewahrt und nach Ablauf dieser Frist mit höchster Sicherheitsstufe (Stufe 5 – die Reproduktion der Daten ist nach Stand der heutigen Technik nicht möglich) vollständig vernichtet bzw. zerstört.

12. Der Penetration Tester nimmt zur Kenntnis, dass der Auftraggeber auf sämtliche IT Security Penetration Tests, die in den Monitoring-, Firewall-, Alarmsystem und der gleichen erkannt werden, in regulärer Weise bzw. wie es im Echtbetrieb geschehen würde, reagieren wird. Der Auftraggeber verpflichtet sich jedoch, eine Durchdringung von Schutzsystemen nicht an juristische oder öffentliche Stellen weiterzuleiten bzw. zu melden.

13. Im Falle eines Vorfalls oder unbeabsichtlichen Denial-of-Service-Angriffs, ist umgehend der Zuständige Kontakt bei dem Auftraggeber zu informieren.

14. Wenn ein Penetration Test auf ein oder mehrere Cloud Systeme vorgesehen ist, dann verpflichtet sich der Auftraggeber schon im Vorhinein die Erlaubnis von den Cloud Anbietern in schriftlicher Form einzuholen.

15. Ist dritte Software oder Software von Drittanbietern Teil des Penetration Tests muss im Vorhinein von dem Auftrageber eine schriftliche Erlaubnis der Dritten eingeholt

werden.

16. Werden BYOD-Geräte (Bring your own Device) oder Dienstnotebooks mit Erlaubnis zur privaten Nutzung ebenso im Penetration Test analysiert, so ist eine schriftliche Erlaubnis des Besitzers im Vorhinein vom Auftraggeber einzuholen.

17. Wenn forensische Analyse Bestandteil des Penetration Tests ist, so verpflichtet sich der Auftraggeber für die Integrität (Unveränderlichkeit) und korrekte Übergabe des zu analysierenden Geräts/Mediums zu sorgen. Der Penetration Tester haftet nicht im Falle eines in der forensischen Analyse auftretenden Datenverlusts oder Schadens an dem zu analysierenden Gerät/Medium.

18. Im Rahmen des Social Engineerings ist der Penetration Tester verpflichtet keine ungesitteten Anrufe/Gespräche zu tätigen (z.B.: vorgetäuschter Tod eines Angehörigen). Er ist ebenso verpflichtet, dass er niemanden durch seine Social Engineering Angriffe gefährdet (z.B. Kündigung eines Mitarbeiters).

19. Es gelten die allgemeinen Geschäftsbedingungen des Penetration Testers.

20. Sämtliche Punkte, welche sich für den Penetration Tester aus dieser Vereinbarung ergeben, gelten gleichermaßen für die MitarbeiterInnen und Sub-Unternehmer des Penetration Testers.

Ort, Datum	*Unterschrift des Auftraggebers*
Ort, Datum	*Unterschrift Penetration Tester*

Scope – Inhalt des Penetration Tests

Berichterstattung gewünscht?	Ja
Häufigkeit der Berichterstattung	Bei Critical/High, Info an Max Mustermann Am Schluss ein Abschlussbericht und eine Abschlusspräsentation
Zeit & Ort der Berichterstattung	Angestrebt wird der 20.06.2024
An wen soll die Berichterstattung erfolgen?	Asset Owner, Projektleitung und mit dem Asset in direktem Kontakt stehende Mitarbeiter
Gibt es spezielle Anforderungen/Ziele für diesen Penetration Test?	Quality Gate für das Go-Live
Start des Penetration Tests	10.06.2024 – 8:00 Uhr
Ende des Penetration Tests	20.06.2024 – 08:00 Uhr
Testzeiten/Zeitpunkt des Penetration Tests	Die Tests dürfen 24/7 stattfinden
Zeitpunkt des letzten Tages/Deadline	10.06.2024 – 08:00 Uhr
Zeitbudget des Penetration Tests	8 Projekttage
Schutzbedarf | Motivation für die Durchführung des Penetration Tests	Quality Gate vor dem Release
Welche Unternehmensprozesse werden durch diesen Penetration Test überprüft?	Webshop in dem alle Kunden bestellen können
Was ist das Risiko/der Impact bei einem Ausfall oder einer Kompromittierung der geprüften Assets?	Kein Kunde kann im Webshop bestellen
Wie geschäftskritisch sind die geprüften Assets?	Sehr kritisch
Wer ist verantwortlich für die geprüften Assets?	Max Mustermann
Gibt es ein Issue Tracking Tool für Projektmanagement, in dem die Befunde zugeordnet werden können?	Ja, Jira. - EPIC: WEBSHOP-123
Wie ist die Risikostrategie des Unternehmens?	Kritische und hohe Risiken werden behoben, ab mittleren Befunden wird im Security Board über eine Risikostrategie gesprochen.
Sollen Personen vor dem Penetration Test verständigt werden?	Nein
Wenn ja, welche Personen (vor Pentest)	-
Sollen Personen bei einem Vorfall während des Penetration Tests verständigt werden?	Ja
Wenn ja, welche Personen (bei Vorfall)	Auf jeden Fall an: Max Mustermann
Penetration Testing Ansatz (Blackbox, Greybox, Whitebox)	Blackbox stufenweise auf Greybox bis Whitebox inklusive Source Code Audit
Verfügen Zielsysteme über einen Schutzmechanismus, der den Penetration Test beeinflussen kann?	Nein
Wenn ja, welche Schritte sind zu tätigen um mit dem Penetration Test fortzufahren?	Melden bei Projektleitung / Stv. Projektleitung

Was sind die größten Sicherheitsbedenken der zu testenden Firma?	Initial Infektion der Infrastruktur, Verbreitung über Infrastruktur, Stehlen von Sensiblen Daten
Wie soll mit sensiblen Daten umgegangen werden?	Laut DSGVO und NDA
Werden Penetration Tests überwacht?	Nein
Sind Clients/Endsysteme Inhalt des Penetration Tests?	Nein
Sind Denial of Service Attacken erlaubt?	Nein
Wenn Nein, wer soll im Falle eines unbeabsichtigten DoS-Angriffs informiert werden?	Auf jeden Fall: Max Mustermann
Sind gefährliche Checks/Exploits erlaubt?	Ja, da es sich um ein Testsystem handelt und somit das Restrisiko gering ist.
Welche speziellen Hosts, Systeme oder Applikationen sollen getestet werden?	- https://webshop-that-does-not.exist - Domain „ynh-gmbh“
Welche speziellen Hosts, Systeme oder Applikationen sollen NICHT getestet werden?	- Restliche Infrastruktur
Welche Systeme stammen von Dritten oder werden von Dritten gehostet? (Erlaubnis von Dritten ist zwingend notwendig!)	-
Werden die Tests gegen ein Testsystem oder das Produktivsystem durchgeführt?	Testsystem
Werden Penetration Tests intern oder extern ausgeführt?	Extern
Wenn intern, wie wird der Zutritt erteilt?	-
Gibt es Test Accounts/Credentials?	Lieferanten Account für VPN Zugriff Start ohne Zugang, danach Freischaltung mit Domain-Account
Gibt es Dokumente, die den Penetration Test unterstützen können?	Ja ein Auszug aus Confluence und Zugriff zu Jira Epics

Methoden des Penetration Tests

Network Penetration Test	Nein
Web Application Penetration Test	Ja
Mobile Application Penetration Test	Nein
Cloud Penetration Test	Nein
Software Penetration Test	Ja
Physical Penetration Test	Nein
SAP Penetration Test	Nein
OT Penetration Test	Nein
IoT Penetration Test	Nein
Container Penetration Test	Nein
IaC Penetration Test	Nein
Social Engineering	Nein
WLAN Penetration Test	Nein
Red-Teaming-Angriffe	Nein
Vulnerability Assessment	Ja
Threat Modeling	Nein
Application-Level Manipulation	Nein
Client-seitiges Reverse Engineering	Nein
Source Code Audit	Ja
Konfigurationsaudit	Nein
SOC-Wirksamkeitsprüfung	Nein
IT-Forensische Test	Nein
Compliance Gap-Analyse	Ja
Phishing Kampagnen	Nein
Andere	-

Social Engineering Inhalte

Angriff	Erklärung	Teil des Pentests?
CEO Fraud	*Vom Auftraggeber werden zahlungsberechtigte Personen preisgegeben. Anschließend werden Pretexte, in welchen bspw. Firmenübernahmen, Kauf von Immobilien oder Firmenwagen, etc. angegeben werden, erstellt. Diese werden per E-Mail an zahlungsberechtigte Personen übermittelt und es wird versucht eine Überweisung ausführen zu lassen. Ggf. kann es vorkommen, dass Personen zusätzlich angerufen werden. Vom Auftraggeber ist ein Bankkonto zur Verfügung zu stellen – ist dies nicht gewünscht, kann ein fiktives Konto verwendet werden.*	Nein
Phishing (Spear Phishing) Attacks	*Vom Auftraggeber wird eine Mitarbeiterliste mit E-Mail Adressen ausgehändigt, an die ein Phishing Mail, mit der Absicht Zugangsdaten abzugreifen, versendet wird. Es wird das Webmail Portal des Auftraggebers geklont und auf einem eigenen Webserver mittels eigener Domäne bereitgestellt. Anschließend wird ein Pretext, welcher die Betroffenen auf das geklonte Portal locken sollte, verfasst und versendet. Abgegriffene Zugangsdaten werden ggf. mitprotokolliert. Als Absender wird entweder eine allgemeine Support E-Mail Adresse verwendet oder eine Identität – sofern sich diese online recherchieren lässt – verwendet. Die jeweilige Identität wird vorab mit dem Auftraggeber abgesprochen. Zusätzlich ist vom Auftraggeber eine schriftliche Zusage von der Dritten Partei einzuholen.*	Nein
Tailgating	*Zutrittsbereiche an den Standorten, wie in der Auftragsbestätigung angegeben, werden einem Audit unterzogen. Dafür werden Firmenabläufe vorab inspiziert und anschließend mögliche Schwachstellen ausgenutzt um unberechtigt ins Unternehmen zu gelangen. Bei den Zutrittsversuchen wird zusätzlich versucht, sensiblest Eigentum wie Notebooks oder ähnliches zu entwenden.*	Nein
Media (USB) Dropping	*Für die Media Dropping Attack werden USB Sticks mittels Dateien versehen, welche non destruktive Trojaner (Memory only – not-persistent) enthalten. Für die Erstellung eines funktionierenden Trojaners ist vom Auftraggeber die Angabe des eingesetzten Antivirenschutz inkl. Bereitstellung einer Install Source dessen notwendig. Es wird bei der Erstellung der Dateien darauf geachtet, dass keine Personenrückschlüsse gezogen werden können. Sollte es sich trotzdem aus irgendeinem Grund anbieten, wird dies vorab mit dem Auftraggeber abgesprochen, da dieser ggf. eine schriftliche Zusage der Dritten Partei einzuholen hat. Die erstellten USB Sticks werden teilweise an den Standorten, wie in der Auftragsbestätigung angegeben, verteilt bzw. per Post versendet.*	Nein

Network Implant Platzierung	*Für Network Implant Platzierungen werden vorgefertigte Netzwerkimplantate von einem Penetration Tester erstellt und danach im Netzwerk eingebaut. Ziel dieses Angriffs ist es, dass man automatisiert Daten im Netzwerk abgreift und gleichzeitig das Netzwerk auf Schwachstellen abscanned.*	Nein
Vhishing Attacks	*Vom Auftraggeber wird eine Mitarbeiterliste Telefonnummer ausgehändigt. In die Mitarbeiterliste ist zusätzlich die Funktion anzugeben. Wahllos werden anschließend Mitarbeiter durchgerufen und es wird versucht, vertrauliche Informationen (Passwörter, sensible Daten, Firmengeheimnisse, etc.) abzugreifen. Für die Anrufe wird ein Pre-Paid Handy verwendet und entweder mittels Call ID Spoofing die Rufnummer gefälscht bzw. anonym angerufen. Weiters werden für die Telefonanrufe Identitäten aus dem Unternehmen, welche recherchiert werden können, verwendet. Dies wird vorab mit dem Auftraggeber abgestimmt, da ggf. eine schriftliche Zusage der Dritten Partei einzuholen ist.*	Nein
Whaling Attacks	*In sämtliche Angriffe werden auch Vorstände, Geschäftsführer, mittleres Management bzw. andere leitende Funktionen mit einbezogen.*	Nein
Dumpster Diving	*Sofern es die Gelegenheit zulässt wird versucht, über Restmüll an vertrauliche Informationen zu gelangen.*	Nein
Quid Pro Quo Baiting Attacks	Bei Quid Pro Quo Baiting Angriffen wird durch das tun von Gefallen versucht, sich einen Gefallen von der Person, der man geholfen hat zurückzugewinnen. Der gewonnene Gefallen wird dann für schadhafte Angriffe oder vertrauliche Informationen eingesetzt.	Nein
Shoulder Surfing	Beim Shoulder Surfing wird gezielt einem Mitarbeiter beim Tippen auf der Tastatur, am Smartphone oder bei der Eingabe etwaiger vertraulicher Informationen über die Schulter geschaut.	Nein
Lock Picking	Durch Lock Picking wird das Aufbrechen von Türschlössern ohne dass dadurch Schaden entsteht mit sogenannten Picks ausgeübt. Ziel ist es, die Sicherheit des Schließmechanismus zu überprüfen.	Nein
Pretexting	Ein Angreifer erstellt eine fiktive Situation oder Identität, um Personen dazu zu bringen, vertrauliche Informationen preiszugeben oder Handlungen auszuführen, die normalerweise nicht durchgeführt würden. Zum Beispiel kann ein Angreifer vorgeben, ein IT-Support-Mitarbeiter zu sein, um Zugangsdaten oder Systemeinstellungen zu erhalten.	Nein
Social Media Reconnaissance	Nutzung von Informationen, die aus sozialen Medien und anderen öffentlichen Quellen gewonnen wurden, um gezielte Angriffe durchzuführen. Hierzu gehört das Sammeln von Informationen über Mitarbeiter, Firmenabläufe und andere relevante Details.	Nein

Impersonation	Ein Angreifer gibt sich physisch oder online als eine vertrauenswürdige Person oder Dienstleister aus, um Zugang zu sensiblen Bereichen oder Informationen zu erhalten. Dies kann durch das Tragen von Uniformen, Erstellen von gefälschten Ausweisen oder das Versenden von täuschenden E-Mails geschehen.	Nein
Watering Hole Attack	Der Angreifer identifiziert Websites, die häufig von Zielpersonen besucht werden, und kompromittiert diese Seiten, um Malware zu verbreiten. Ziel ist es, durch legitime Websites die Sicherheitsmechanismen zu umgehen und Zugriff auf das Netzwerk oder die Systeme der Zielpersonen zu erlangen.	Nein
Baiting	Ein Angreifer lockt das Ziel mit einem verlockenden Angebot, um Malware zu verbreiten oder vertrauliche Informationen zu erhalten. Dies kann durch das Platzieren von USB-Sticks oder das Anbieten von kostenlosen Downloads geschehen.	Nein
Reverse Social Engineering	Der Angreifer lässt das Ziel auf ihn zukommen, indem er eine Situation erzeugt, die das Ziel dazu bringt, den Angreifer selbst zu kontaktieren und dabei vertrauliche Informationen preiszugeben oder schädliche Handlungen durchzuführen.	Nein
Consent Phishing	Der Angreifer versucht, das Opfer dazu zu bringen, einer Anwendung oder einem Dienst Zugang zu sensiblen Daten oder Systemen zu gewähren, oft durch den Missbrauch legitimer Funktionen von Plattformen wie OAuth.	Nein
Honey Trap	Der Angreifer stellt eine attraktive Person dar, die versucht, das Opfer in eine Beziehung zu verwickeln, um Informationen zu sammeln oder bestimmte Handlungen durchzuführen. Dies kann sowohl online als auch offline geschehen.	Nein
Help Desk Scams	Der Angreifer gibt sich als legitimer Help Desk oder Support-Mitarbeiter aus, um Zugang zu Systemen oder vertraulichen Informationen zu erhalten. Dies wird häufig durch telefonische Anfragen oder gefälschte Support-Webseiten durchgeführt.	Nein
Scareware	Der Angreifer verwendet gefälschte Warnungen und Bedrohungen, um das Opfer zu überzeugen, bestimmte Handlungen durchzuführen, wie z.B. das Herunterladen von Malware oder das Preisgeben von persönlichen Informationen.	Nein
Man-in-the-Middle (MitM) Social Engineering	Der Angreifer schaltet sich in die Kommunikation zwischen zwei Parteien ein und fängt die Informationen ab, ohne dass die Parteien dies bemerken.	Nein

Zutrittskontrolle umgehen	Der Angreifer versucht mittels Flipper Zero die Zutrittskontrolle zu umgehen und sich somit Zugriff zu nicht-gestatten Räumen oder Gebäuden zu verschaffen	Nein

Informationen zu den Social Engineering Tests

Sind Social Engineering Angriff auf externe Mitarbeiter/Dienstleister vorgesehen (Erlaubnis muss eingeholt werden!)	Nein
Sind spezifische Personen aus den Social Engineering Angriffen auszunehmen?	-
Welche Personen sind in den Social Engineering Tests eingeweiht?	-
Wer ist im Falle einer Aufdeckung als Kontaktperson zu nennen und zu informieren?	-

Informationen zu den IT-Forensik Tests im Rahmen des Penetration Tests

Ist IT-Forensik im Rahmen des Penetration Tests enthalten?	Nein
Sollen IT-forensische Tests auf Dienstnotebooks durchgeführt werden?	-
Welche Geräte und Systeme müssen von IT-forensischen Tests ausgenommen werden?	-
Wer ist im Falle eines Vorfalls in einer IT-forensischen Analyse zu informieren?	-

Informationen zu den SOC-Healthchecks im Rahmen des Penetration Tests

Ist ein SOC-Healthcheck Rahmen des Penetration Tests enthalten?	Nein
Wer ist der externe SOC-Anbieter?	-
Welche Geräte und Systeme müssen von SOC-Healtchecks ausgenommen werden?	-
Wer ist im Falle eines Vorfalls während des SOC-Healthchecks zu informieren?	-

Informationen zu Compliance GAP-Analyse im Rahmen des Penetration Tests

Ist eine Compliance GAP-Analyse im Rahmen des Penetration Tests enthalten?	Ja
Welche/r Norm/Standard soll als Basis für die Compliance gelten?	CIS Controls V8, OWASP Top 10 und CWE Top 25
Gibt es interne Richtlinien oder Dokumente die im Rahmen des Penetration Tests herangezogen werden können?	-
Was ist die aktuelle Maturität (nach CMMI) ?	-

Informationen zu Konfigurations-Audits im Rahmen des Penetration Tests

Ist eines Konfigurations-Audits im Rahmen des Penetration Tests enthalten?	Nein
Welche Konfigurationen werden überprüft?	-
Wer ist der Verantwortliche für die Konfigurationen? (Intern/Extern)	-
Gibt es Prozessbeischreibungen oder Dokumente die den Konfigurationsaudit unterstützen können?	-

Informationen zu Red Teaming im Rahmen des Penetration Tests

Ist Red Teaming im Rahmen des Penetration Tests enthalten?	Nein
Wer ist der Notfalls-Kontakt im Rahmen einer Aufdeckung?	-
Gibt es No-Gos die beim zwingend Red Teaming vermieden werden müssen?	-
Gibt es Personen, die aus dem Red Teaming ausgenommen werden?	-

Ort, Datum *Unterschrift des Auftraggebers*

Ort, Datum *Unterschrift Penetration Tester*

NDA – Verschwiegenheitserklärung

Durch diese Geheimhaltungsvereinbarung wird zwischen dem Auftraggeber und dem Penetration Tester eine Verschwiegenheitspflicht bezüglich des Penetration Tests eingeräumt. In Anbetracht des Erhalts von vertraulichen Informationen aus dem Penetration Test erklären sich beide Parteien wie folgt einverstanden:

1. *Die Informationen werden streng vertraulich behandelt, dürfen nur im Rahmen dieser Geschäftsbeziehung verwendet werden, dürfen ohne vorherige schriftliche Zustimmung durch den Penetration Tester weder vom Auftraggeber noch von seinen Vertretern in irgendeiner Weise, ganz oder teilweise, weitergegeben werden und dürfen vom Auftraggeber oder seinen Vertretern nur im Zusammenhang mit ihrer durch den Penetration Tester beauftragten und definierten Tätigkeit verwendet werden. Der Auftraggeber ist für jede Verletzung dieser Vereinbarung durch seine Vertreter verantwortlich und stimmt zu, auf alleinige Kosten alle vernünftigerweise notwendigen Maßnahmen (einschließlich, aber nicht beschränkt auf Gerichtsverfahren) zu treffen, um seine Vertreter von der verbotenen oder unbefugten Offenlegung oder Nutzung der Informationen unter Verletzung dieser Vereinbarung abzuhalten oder diese rückgängig zu machen.*

2. *Der Penetration Tester verpflichtet sich zur Verschwiegenheit über Geschäfts- und Betriebsgeheimnisse, sowie personenbezogene Daten, die ihm während eines Penetration Test Auftrags bekannt werden. Von dieser Pflicht zur Verschwiegenheit sind insbesondere umfasst:*
   i. *Geschäfts- oder Betriebsgeheimnisse sowie ihm anvertraute Dokumente und Informationen i.S.d. § 11 österreichischen UWG.*
   ii. *Sämtliche personenbezogene Daten aus der Datenverarbeitung, die ihm ausschließlich im Rahmen des Penetration Tests anvertraut wurden oder zugänglich geworden sind.*

3. *Diese Vereinbarung kann nur durch eine schriftliche Vereinbarung geändert oder ergänzt werden, die vom Auftraggeber und dem Penetration Tester unterzeichnet wurde. Der Auftraggeber ist nicht berechtigt, diese Vereinbarung, ohne die ausdrückliche schriftliche Zustimmung von dem Penetration Tester abzutreten*

Ort, Datum	*Unterschrift des Auftraggebers*
Ort, Datum	*Unterschrift Penetration Tester*