axians

THREAT-LED PENETRATION TESTING

VINCI ENERGIES

Inhalt

THREAT-LED PENETRATION TESTING

Was ist ein TLPT

Definition

Bei Threat-Led Penetration Testing werden Taktiken, Techniken, und Verfahren realer Angreifer auf Live-Produktionssystemen nachgestellt. Im Fokus liegen hierbei kritische Systeme, die essenzielle Funktionen für die Hauptgeschäftsprozesse einer Organisation liefern oder von gewisser systemischer Relevanz sind.

Das Ziel ist es ein faktengestützter Test-Bericht der Schwachstellen aufzeigt, die in einem realen Angriff von relevanten Angreifergruppen ausgenutzt werden könnten. Da ein TLPT von den Möglichkeiten deutlich über einen herkömmlichen Penetrationstest hinausgeht, können sich Testbefunde auf Schwachstellen in der operativen IT, Prozessen oder auch Personen beziehen.

Zur effektiven Durchführung eines TLPTs unter Berücksichtigung der sich aus der Vorgehensweise ergebenden Risiken gibt das TIBER 2.0-Framework einen hilfreichen Rahmen, der gleichzeitig auch die Vorgaben aus dem Digital Operational Resilience Act (DORA) und dem regulatorisch technischen Standard für TLPTs einhält.

Abgrenzung zum herkömmlichen Penetrationstest

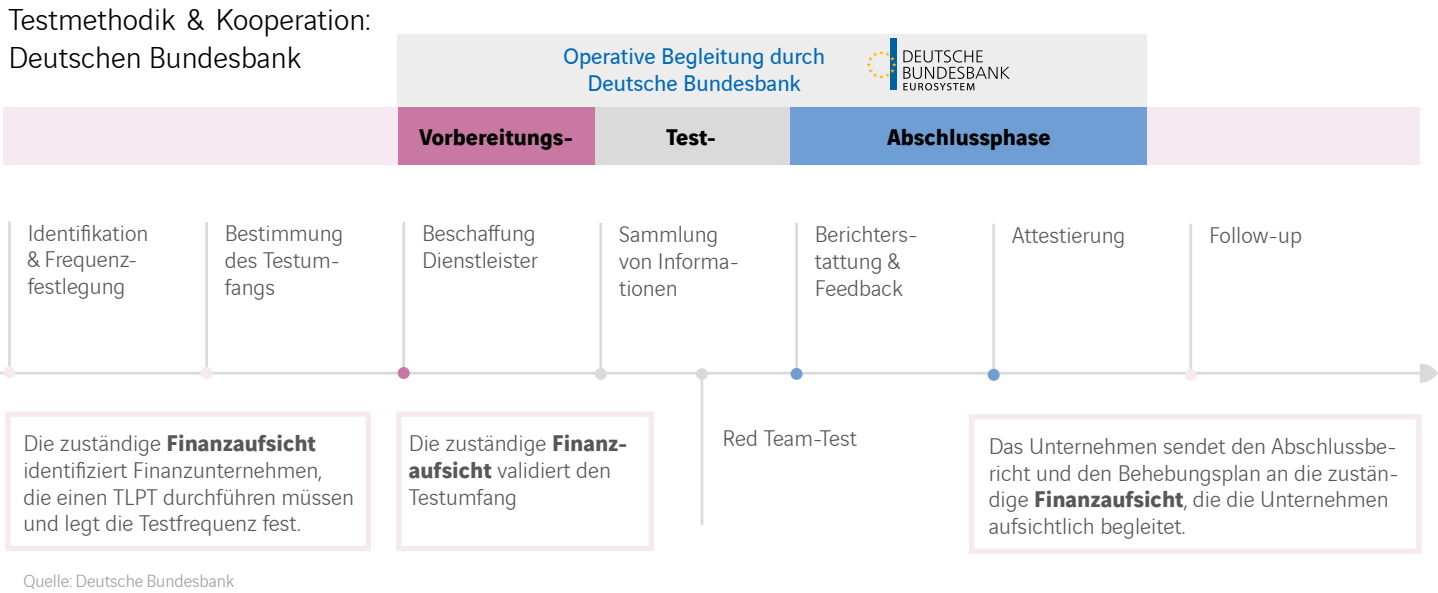
Basierend auf der Realitätsnähe der zu testenden Angriffsszenarien innerhalb eines TLPT gibt es eine deutlich erhöhte Anzahl an möglichen Vorgehensweisen in einem TLPT verglichen zu einem normalen Penetrationstest. Die Szenarien sind hochkomplex und werden auf Produktivsystemen durchgeführt. Auf dem Weg zum Testziel stehen nicht nur technische Erkenntnisse im Fokus, sondern auch: Prozesse, Entscheidungswege, Reaktionen und Teams.

Stakeholder

Im Rahmen eines TLPT gibt es verschiedene Stakeholder, die es zu beachten gibt. Dazu zählen:

- **Control Team:**
  Mitglieder des Control Teams bestehen aus Mitarbeitern des getesteten Instituts. Das Team beinhaltet den Control Team Lead. Das Team bzw. der Lead ist der zentrale Ansprechpartner und für die Steuerung – also Entscheidungsträger sowie Risikomanagement - des Tests verantwortlich.
- **TLPT Cyber Team:**
  Das TCT ist der Deutschen Bundesbank (oder entsprechendem lokalen Äquivalent, z. B. Oesterreichische Nationalbank) zugeordnet und begleitet Finanzunternehmen bei der Durchführung eines TLPT.
  Zum Schluss des Tests attestiert das TCT die korrekte Durchführung, sofern alle formellen Vorgaben aus dem RTS eingehalten wurden. Falls das Risiko einer Nichteinhaltung während des Testverlaufes besteht, weist das TCT entsprechend darauf hin. Ein „Durchfallen" auf Grund von Red Teaming Resultaten ist nicht möglich.
- **Threat Intelligence Anbieter:**
  Der Threat Intelligence Anbieter muss nach Vorgaben aus dem RTS extern sein und liefert unternehmensspezifische Bedrohungsinformationen. Dies beinhaltet eine Analyse der externen Angriffsfläche des Zielinstitutes (z. B. Suche nach öffentlich verfügbaren, nutzbaren Informationen) sowie eine Identifizierung und Priorisierung relevanter Angreifergruppen.
  Aus der externen Angriffsfläche und den priorisierten Angreifergruppen erstellt der TI-Anbieter Angriffsszenarien, die im weiteren Testverlauf durchgeführt werden.
- **Red Teaming Anbieter:**
  Der Red Teaming Anbieter ist meist extern, kann unter Umständen allerdings auch aus einem internen Red Team bestehen. Der RT-Anbieter nutzt seine Expertise und die vom TI-Anbieter gesammelten Informationen, um die Angriffsszenarien durchzuführen.
- **Blue Team:**
  Im Kern besteht das Blue Team aus der Cyberabwehr des Zielinstitutes. Im Rahmen eines TLPT kann jeder Mitarbeiter, der nicht Teil des Control Teams indirekt ist als Teil des Blue Teams betrachtet werden. Das Blue Team darf nicht über die Durchführung eines Tests informiert werden.
- **IT-Dienstleister:**
  Sofern in den durchzuführenden Szenarien Zielsysteme vorkommen, die durch externe Dienstleister betrieben werden, kann es Sinn ergeben diese zum Start der Red Teaming Phase zu involvieren.

Testphasen und Timeline



Quelle: Deutsche Bundesbank

THREAT-LED PENETRATION TESTING

Die Testphasen im Detail

Vorbereitungsphase : Identifikation und Testnotifikation

Im ersten Schritt identifiziert die Finanzaufsicht Finanzunternehmen, die einen TLPT durchführen müssen. Darauf werden betroffene Unternehmen mit einer Testnotifikation angeschrieben und über die Auswahl zur Testdurchführung informiert. Mit der Notifikation beginnt die insgesamt sechsmonatige Vorbereitungsphase:

Benachrichtigung zum Start eines TLPT durch die TLPT-Behörden

Vorbereitung
inkl. Beschaffung, Risikomanagement

Einleitungsdokumente
(3 Monate)

Umfangsspezifikationsdokument
(6 Monate)

Quelle: eba.europa.eu

Bestimmung des Testumfangs (Scoping)

KRITISCHE FUNKTIONEN
Definition, Personen, Prozesse und Technologien, die das Unternehmen benötigt, um einen zentralen Dienst zu erbringen. Ein Szenario gilt als nachteilig auf die Stabilität, die Sicherheit und die Existenz des Unternehmens, dessen Kundenstamm oder Marktverhalten auswirken würde.

KRITISCHE SYSTEME
Anwendungen / Systeme, die zur Bereitstellung oder Aufrechterhaltung einer kritischen Funktion benötigt werden.

FLAGS
Ziele, die im Testverlauf erreicht werden sollen. Im Rahmen des Scope-Dokuments werden verschiedene Flags definiert, wovon eine Teilmenge innerhalb der finalen Szenarien aufgegriffen wird.

AUSSCHLÜSSE
Im Rahmen des Scopes können auch explizite Ausschlüsse definiert werden. Hierunter können kritische Funktionen, Angriffstechniken, Auslandseinrichtungen oder Tochtergesellschaften fallen.
Beispiele: Persönliche Geräte von Mitarbeitern, Personal (Kritische Funktion), DDoS (Angriffstechnik).

DAS SCOPE-DOKUMENT SETZT DEN GRUNDLEGENDEN RAHMEN FÜR EINEN TIBER-TEST / TLPT.
Es bildet durch die Definition und Testeinbindung von kritischen Funktionen, kritischen Systemen und möglichen Flags das Fundament eines TIBER-Tests.

Quelle: Unbekant

Initial Risk Assessment

Die Durchführung eines TLPT ist mit Risiken verbunden, die das betroffene Institut im Rahmen eines Initial Risk Assessments berücksichtigen muss. Hierbei ist es wichtig die Risiken inklusive Eintrittswahrscheinlichkeit und Schadenshöhe zu dokumentieren und entsprechende Gegenmaßnahmen zu definieren und dokumentieren. Beispiele für Risiken und zugehörige Maßnahmen sind:

- **Risiko: Aufdeckung des laufenden Tests durch das Blue Team**
  - Maßnahme: Verschlüsselte Kommunikationswege zwischen involvierten Stakeholdern
  - Maßnahme: Verwendung eines Projekt-Codenamens
- **Risiko: Schäden auf Produktivsystemen**
  - Maßnahme: Explizite Exklusion von Denial-of-Service-Angriffsmustern
  - Maßnahme: Einsatz eines nachweislich fachkundigen Red Teams
  - Maßnahme: Kontinuierlicher Austausch mit dem Red Team während der aktiven Testphase
- **Risiko: Verletzung der Vertraulichkeit von im Testverlauf zugegriffenen Informationen**
  - Maßnahme: Abschluss von Geheimhaltungsvereinbarungen mit TI- und RT-Dienstleister.
  - Maßnahme: Betrachtung streng vertraulicher Informationen nur nach Freigabe durch das Control Team.

Beschaffung Dienstleister

Im Rahmen der Vorbereitungsphase findet ebenfalls die Beschaffung des Dienstleisters statt. Für sowohl Threat Intelligence als auch Red Teaming Dienstleister gibt es Vorgaben. Das TCT (TLPT Cyber Team) der Bundesbank hat ein Veto-Recht, für den Fall, dass der Dienstleister die Anforderungen nicht erfüllen sollte.

Wir als axians security force erfüllen alle benötigten Anforderungen für die Durchführung von TIBER-Tests und Threat Led Penetration Tests (TLPT).

Welche Angreifergruppen sind für mein Unternehmen relevant?

Threat Intelligence Phase

Das finale Ziel der Threat Intelligence Phase ist die Erstellung und Auswahl von drei Angriffsszenarien, die in der Red Teaming Phase ausgeführt werden. Um zu den Szenarien zu gelangen, gibt es folgende Meilensteine in der TI-Phase:

Open-Source Intelligence (OSINT)

Im Rahmen der OSINT-Analyse werden Informationen über das Zielunternehmen gesammelt. Im Fokus hierbei liegen rein öffentlich verfügbare Informationen. Zum Beispiel von Social-Media-Kanälen, bekannten Leaks von Benutzerkennungen oder der allgemeinen Web-Präsenz einer Zielorganisationen.

In Kombination mit aktiven Scans gegen die öffentlich aufrufbare Infrastruktur des Ziels wird ein Profil aufgebaut, welches bereits auf mögliche Schwachstellen hindeuten kann und durch das Red Team in der Testdurchführung verwertet werden kann. Zusätzlich helfen die Ergebnisse bei der Priorisierung möglicher Angreifergruppen.

Bewertung der Bedrohungslage

Während die OSINT-Analyse einen Fokus auf die Sammlung von Eigenschaften und Informationswerten der Zielorganisation legt, werden bei der Bewertung der Bedrohungsanalyse relevante Angreifergruppen identifiziert und priorisiert.

Ausgangslage hierfür ist die allgemeine Bedrohungslage mit Details zu generellen Bedrohungen basierend auf beispielsweise geopolitischen, wirtschaftlichen oder technologischen Aspekten. In Kombination mit dem Profil der Zielorganisation wird die allgemeine Bedrohungslage spezifiziert. Ziel ist es „Targeted-Threat-Intelligence“ zu generieren damit das betroffene Zielunternehmen über allgemeine Trends hinaus informiert ist und die Angriffsszenarien im Test auf wirklich relevanten und wahrscheinlichen Angreifergruppen basieren.

Erstellung von Angriffsszenarien

Die Ergebnisse aus der OSINT-Analyse und der Targeted-Threat-Intelligence werden vom TI-Team verwendet, um neun bis zwölf grobe Angriffsszenarien zu entwickeln. Angriffsszenarien beinhalten:

- **Aus dem Scope-Dokument:**
  - Zielsysteme
  - Zugehörige Flags inkl. Schutzzielen (z. B. Verletzung der Vertraulichkeit)
  - Betroffene kritische Funktionen
  - Betroffene Dienstleister
- **Aus der TI-Phase:**
  - Nachzustellende Angreifergruppe
  - Motivationen der Gruppe
  - Fähigkeiten der Gruppe inkl. möglicher Angriffstechniken
  - Relevanter In-Vektor (z. B. Phishing)
  - Hilfreiche TI aus der OSINT-Phase (z. B. Domänen für das Phishing, Benutzerkennungen)

In einem Szenario-Workshop mit dem TI-Team, Red Team, TCT und Control Team werden schließlich drei Szenarien ausgewählt, die nochmal detailliert mit Angriffstechniken befüllt werden und an das Red Team zur Durchführung übergeben werden.

Targeted Threat Intelligence Report

Der Targeted Threat Intelligence Report (TTI-Report) bildet das finale Übergabedokument aus der TI-Phase und beinhaltet:

- **Allgemeine Beschreibungen zum Testprozess und TI-Ablauf**
- **Ergebnisse aus der OSINT-Analyse**
- **Ergebnisse der Bedrohungspriorisierung**
- **Profile zu den bewerteten Angreifergruppen**
- **Drei detailliert beschriebene Angriffsszenarien**
- **Nützliche TI-Ergebnisse für das Red Team**
- **Weitere Empfehlungen basierend auf Beobachtungen aus der TI**

THREAT-LED PENETRATION TESTING

Red Teaming Phase

Erstellung eines Red-Team-Testplans (RTTP)

Basierend auf den drei im TTI-Report beschriebenen Szenarien erstellt das Red Team einen initialen Red-Team-Testplan. Dieser beinhaltet eine noch detailliertere Ausführung der drei Szenarien insbesondere bezüglich möglicher technischer Umsetzungsmöglichkeiten.

Ein weiterer, wichtiger Aspekt des RTTPs ist die Inklusion und Diskussion möglicher Leg-Ups. Bei Leg-Ups handelt es sich um potenzielle Hilfestellungen seitens des Control Teams, auf die das Red Team zurückgreifen kann, sofern es in einem der Szenarien stecken bleiben sollte.

Durchführung der Angriffsszenarien

Basierend auf dem RTTP werden die drei Angriffsszenarien mindestens zwölf Wochen lang vom Red Team durchgeführt.

Red-Team-Test-Report (RTTR)

Die Ergebnisse der Testdurchführung werden detailliert im Red-Team-Test-Report (RTTR) dokumentiert. Der RTTR dient als finaler Abschlussbericht seitens des Red Teams und wird nach dem aktiven Testen an das Control Team übergeben.

Schlussphase

Replay und Purple Teaming Workshops

Das Red Team führt im Rahmen der Abschlussphase Workshops durch, in denen dem Blue Team der Zielorganisationen gezeigt wird, wie genau die Angriffsszenarien durchgeführt wurden. Dies beinhaltet ein Nachstellen von den Angriffstechniken zu den wichtigsten Erkenntnissen aus der Testdurchführung und soll dem verteidigendem Blue Team dabei helfen greifbare Erkenntnisse basierend auf den Testresultaten zu erhalten.

Blue Team Test Report

Nachdem das Blue Team den RTTR erhalten hat, hat es laut Rahmenwerk sechs Wochen Zeit, um einen Bericht zu erstellen. Dieser sollte vor der Durchführung der Replay und Purple Teaming Workshops stattfinden. Der Bericht beinhaltet unter anderem eine Liste detektierter Angriffsaktivitäten, potenzielle Threat Hunting Aktivitäten und Timeline die BT und RT-Aktivitäten korreliert. Eine detaillierte Liste für Anforderungen an den Blue Team Test Report ist in Kapitel 2 der „TIBER-EU Blue Team Test Report Guidance" zu finden.

Finaler Abschlussbericht

Das Control Team erstellt abschließend einen finalen Abschlussbericht. Dieser beinhaltet im Kern die Erkenntnisse aus dem Red Team Test Report sowie geplante Gegenmaßnahmen.

Konkret gehören hierzu:

- Eine kurze Beschreibung der RT-Erkenntnis,
- eine Maßnahmenbeschreibung,
- die geplante Umsetzungsfrist pro Maßnahme,
- eine Root Cause Analyse,
- Verantwortlichkeiten für die Maßnahmenumsetzung,
- Risiken, sofern eine Maßnahmenumsetzung nicht erfolgt
- und falls relevant Risiken, die sich durch die Maßnahmenimplementierung ergeben.

Der finale Abschlussbericht wird neben dem TCT auch mit der jeweils relevanten Aufsicht (z. B. BaFin) geteilt.

Attestierung

Zum Schluss stellt das TCT dem getesteten Institut eine Attestierung aus. Dies bestätigt die erfolgreiche Testdurchführung unter Berücksichtigung regulatorischer Vorgaben.

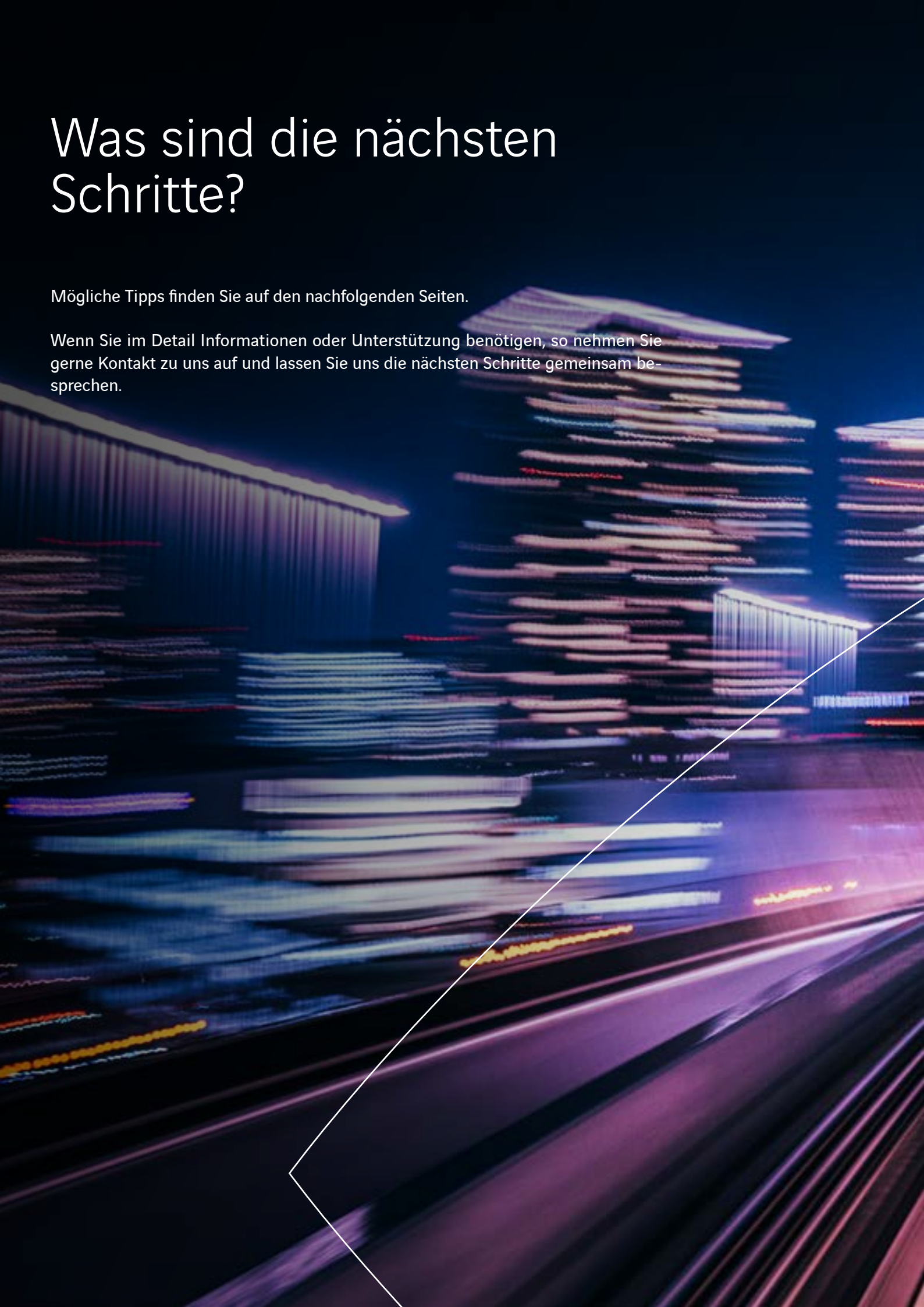
Erkenntnisse aus dem Red Teaming wie konkrete technische Schwachstellen oder Red Teaming Erfolge in den Szenarien fließen nicht mit ein. Der Fokus liegt ausschließlich auf der regelkonformen Durchführung.

Ein Grund für ein Fehlschlagen der Attestierung wäre zum Beispiel das Informieren des Blue Teams über den geplanten Testablauf.

Was sind die nächsten Schritte?

Mögliche Tipps finden Sie auf den nachfolgenden Seiten.

Wenn Sie im Detail Informationen oder Unterstützung benötigen, so nehmen Sie gerne Kontakt zu uns auf und lassen Sie uns die nächsten Schritte gemeinsam besprechen.



ERFOLGREICHE DURCHFÜHRUNG EINES TLPT

Unsere Tipps basierend auf mehrjähriger Erfahrung und einem ersten TIBER 2.0 Test.

Wer ist die Axians Security Force GmbH?

Die Axians Security Force GmbH (ehemals fernao security force GmbH) zählt zu den führenden Beratungsunternehmen in Deutschland mit Spezialisierung auf die Lösung komplexer Herausforderungen im Bereich der IT-Sicherheit. Unser Hauptsitz befindet sich in München, doch wir sind europaweit sowie in den USA tätig. Als ausgewiesene Experten für Security Assessments – etwa Penetrationstests und Red Team Assessments – sowie für Security Compliance, wie zum Beispiel das Informationssicherheits-Management nach ISO 27001, unterstützen wir unsere Kunden dabei, ihre Geschäftsprozesse, Anwendungen, (Embedded-)Systeme und Netzwerke effektiv abzusichern und sowohl vor internen als auch externen Bedrohungen zu schützen.

Die Axians Security Force GmbH ist seit 2021 im TIBER-Umfeld aktiv und hat in dieser Zeit eine hohe Menge an Tests erfolgreich durchgeführt. Zu den getesteten Instituten zählen beispielsweise drei der zehn größten deutschen Banken nach Bilanzsumme. Zusätzlich hat die Axians Security Force GmbH auch bereits Erfahrungen bei der Durchführung freiwilliger Tests nach TIBER 2.0 sammeln können – und ist entsprechend auf TLPTs bestens vorbereitet.

Ein regelmäßiger Austausch mit der Deutschen Bundesbank und die Teilnahme an TCT-Events und Workshops sorgen für stets aktuelle Kenntnisse bezüglich erfolgreicher - das heißt attestierter - Testdurchführungen.

Wir haben eine Test Notification erhalten, was passiert jetzt?

Nach Eingang der Testbenachrichtigung für einen TLPT hat das betroffene Unternehmen sechs Monate Zeit, um die Vorbereitungsphase durchzuführen. Im weiteren Verlauf des Beitrages teilen wir unsere Erfahrungen aus fünf Jahren TIBER-Tests und einem TIBER 2.0 Test. Die Erfahrungen beziehen sich nicht nur auf die Threat Intelligence und das Red Teaming, sondern auch auf die Vorbereitungsphase.

Nach Erhalt der Testbenachrichtigung sind folgende Schritte für die Vorbereitung wichtig:

- Aufbau des Control Teams
- Definition eines Test-Scopes
- Durchführung des Initial Risk Assessments
- Dienstleisterbeschaffung

Die genannten Schritte müssen nicht konsekutiv erfolgen, sondern können auch parallel oder in einer anderen Reihenfolge erfolgen. Zum Beispiel: Das Initial Risk Assessment kann vor oder nach der Definition eines Test-Scopes durchgeführt werden.

Tipps für die Vorbereitungsphase

Aufbau eines Control Teams

Nach Eingang der Testbenachrichtigung sollten Verantwortlichkeiten innerhalb des Zielunternehmens definiert werden. Dies geschieht über die Aufstellung des für den Testverlauf eingeweihten Control Teams. Wichtig ist, dass ein Control Team Lead definiert wird, der zentraler Ansprechpartner für den durchführenden Dienstleister, sowie das TCT der Bundesbank ist. Darüber hinaus sollte es eine Vertretung geben. Weitere Teammitglieder können ebenfalls definiert werden – essenziell ist nur, dass niemand aus dem Blue Team über den geplanten Testablauf informiert wird. Es empfiehlt sich das Control Team initial klein zu halten (3 – 4 Mitglieder).

Control Team Mitglieder bestehen oftmals aus Mitarbeitern der internen Informationssicherheit (Compliance) oder des internen Risikomanagements. Für einen möglich effektiven Testverlauf sollten Mitglieder in das White Team aufgenommen werden, die einen Einblick in die Kritikalitätsbewertung von Prozessen und Systemen haben. Dies erleichtert die Definition des Testumfangs und das Beantworten möglicher Fragen seitens des durchführenden Dienstleisters während des Testverlaufs.

Definition des Testumfangs (Scope-Dokument)

Das Scope-Dokument bildet die Basis für den gesamten weiteren Testverlauf und wird insbesondere bei der Erstellung der Angriffsszenarien in der TI-Phase nochmal aufgegriffen. Entsprechend ist es ein sehr wichtiger Output aus der Vorbereitungsphase.

KRITISCHE FUNKTIONEN

Definition, Personen, Prozesse und Technologien, die das Unternehmen benötigt, um einen zentralen Dienst zu erbringen. Ein Szenario gilt als nachteilig auf die Stabilität, die Sicherheit und die Existenz des Unternehmens, dessen Kundenstamm oder Marktverhalten auswirken würde.

KRITISCHE SYSTEME

Anwendungen / Systeme, die zur Bereitstellung oder Aufrechterhaltung einer kritischen Funktion benötigt werden.

FLAGS

Ziele, die im Testverlauf erreicht werden sollen. Im Rahmen des Scope-Dokuments werden verschiedene Flags definiert, wovon eine Teilmenge innerhalb der finalen Szenarien aufgegriffen wird.

AUSSCHLÜSSE

Im Rahmen des Scopes können auch explizite Ausschlüsse definiert werden. Hierunter können kritische Funktionen, Angriffstechniken, Auslandseinrichtungen oder Tochtergesellschaften fallen.

Beispiele: Persönliche Geräte von Mitarbeitern, Personal (Kritische Funktion), DDoS (Angriffstechnik).

DAS SCOPE-DOKUMENT SETZT DEN GRUNDLEGENDEN RAHMEN FÜR EINEN TIBER-TEST / TLPT.

Es bildet durch die Definition und Testeinbindung von kritischen Funktionen, kritischen Systemen und möglichen Flags das Fundament eines TIBER-Tests.

Quelle: Unbekant

Organisatorischer Ablauf

1 ERSTELLUNG DES DOKUMENTS

Eine initiale Fassung des Testumfangs wird erstellt. Input hier ist das Template der Bundesbank (TCT).

2 SCOPING WORKSHOP

Durchführung eines Workshops mit dem TCT, TI-Provider und optional RT-Provider.

Im Workshop wird das Scope-Dokument dem TCT vorgestellt. Das TCT gibt Feedback, welches eingearbeitet werden kann.

3 FREIGABE - BAFIN / EZB

Nach Verarbeitung des TCT-Feedbacks wird das Scope-Dokument zur Freigabe durch die Bafin weitergeleitet.

In den meisten Fällen wird das Scope-Dokument ohne weiteres Feedback / Änderungswünsche freigegeben.

4 FREIGABE - VORSTAND

Final wird das Scope-Dokument von einem Vorstandsmitglied freigegeben.

Eine Freigabe kann beispielsweise per Mail erfolgen und muss keinem festen Prozess / Freigabe-Template folgen.

Mögliches Vorgehen bei der Erstellung

Eine Vorgehensweise zur Identifikation kritischer Funktionen und Systeme kann die Betrachtung des ISMS Asset Managements sein.

KRITISCHE FUNKTIONEN

Aus Geschäftsprozessen mit höchstem Schutzbedarf können kritische Funktionen abgeleitet werden.

Alternativ können kritische Funktionen auch über generelle Umrisse identifiziert werden.

Bsp. aus dem Kreditgeschäft: das Großteil des generierten Umsatzes stammt aus, dann die Haupttaufgabe als kritische Funktion gewertet werden.

Beispiele für kritische Funktionen sind:

- Kreditgeschäft
- Zahlungsverkehr
- reasury
- Fördergeschäft

KRITISCHE SYSTEME

Systeme, die einen Prozess unterstützen und ebenfalls den höchsten Schutzbedarf haben, können als kritische Systeme klassifiziert werden.

Beispiele für kritische Systeme, die für den o.g. Kreditprozess typisch sind:

- LoanIQ (Kreditgeschäft)
- CORONA (Handelsgeschäft)
- Pega (Prozesssteuerung)
- OSPlus (Transaktionsgeschäft)

FLAGS

Für die kritischen Systeme werden im letzten Kapitel Flags definiert. Flags sind mögliche Ziele, die im Testverfahren erreicht werden sollen.

Die Erreichung der Flags bedeutet im Rot- Teaming durchgeführtem Angriffssimulationen ein Szenario, das von den ISAs für jedes kritische System 1–3 Flags zu definieren. Hierbei kann der Schutzziel-Verletzung Vertraulichkeit, Integrität, Verfügbarkeit ausgegangen werden.

Beispiele für Flags sind auf Seite 6 zu finden.

Weitere wichtige Punkte

Neben Geschäftsprozessen können unterstützende Prozesse (z. B. IT) explizit im Scope aufgenommen werden und mit kritischen Systemen (z. B. Active Directory) versehen werden.

Auf Grund des organisatorischen Ablaufs inkl. Freigaben empfehlen wir mindestens zwei Monate vor dem geplanten Kickoff mit dem Verfassen des Scope-Dokuments zu starten. In den drei finalen Testszenarien müssen die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit betrachtet werden. Dies bedeutet, dass pro Szenario ein Schutzziel vorkommen muss.

Entsprechend sollten Flags nicht zu eng definiert werden, bzw. sollten ausreichend Flags für eine weitere Auswahl definiert werden. Mögliche Dienstleister sollten bereits bei der Auflistung der kritischen Systeme berücksichtigt und erfasst werden.

Im weiteren Testverlauf können Dienstleister ggf. involviert werden sofern eines der durch den Dienstleister bereitgestellten kritischen Systeme Ziel eines Szenarios wird.

Risikomanagement (Initial Risk Assessment)

Die Durchführung eines TLPT ist mit Risiken verbunden, die das betroffene Institut im Rahmen eines Initial Risk Assessments berücksichtigen muss. Hierbei ist es wichtig die Risiken inklusive Eintrittswahrscheinlichkeit und Schadenshöhe zu dokumentieren und entsprechende Gegenmaßnahmen zu definieren und dokumentieren. Beispiele für Risiken und zugehörige Maßnahmen sind:

- **Risiko: Aufdeckung des laufenden Tests durch das Blue Team**
  - Maßnahme: Verschlüsselte Kommunikationswege zwischen involvierten Stakeholdern
  - Maßnahme: Verwendung eines Projekt-Codenamens
- **Risiko: Schäden auf Produktivsystemen**
  - Maßnahme: Explizite Exklusion von Denial-of-Service-Angriffsmustern
  - Maßnahme: Einsatz eines nachweislich fachkundigen Red Teams
  - Maßnahme: Kontinuierlicher Austausch mit dem Red Team während der aktiven Testphase
- **Risiko: Verletzung der Vertraulichkeit von im Testverlauf zugegriffenen Informationen**
  - Maßnahme: Abschluss von Geheimhaltungsvereinbarungen mit TI- und RT-Dienstleister.
  - Maßnahme: Betrachtung streng vertraulicher Informationen nur nach Freigabe durch das Control Team.

Eine feste Vorgabe oder eine offizielle Vorlage für das Initial Risk Assessment existiert nicht. Hier können Vorgaben aus dem bereits existierenden Risikomanagementprozess des jeweiligen Zielunternehmens aushelfen.

Dienstleisterbeschaffung

Im Rahmen der Vorbereitungsphase findet ebenfalls die Beschaffung des Dienstleisters statt. Für sowohl Threat Intelligence als auch Red Teaming Dienstleister gibt es Vorgaben. Das TCT (TLPT Cyber Team) der Bundesbank hat ein Veto-Recht, für den Fall, dass der Dienstleister die Anforderungen nicht erfüllen sollte.

Das TCT agiert marktneutral und stellt keine Dienstleisterempfehlungen aus. Bei der Beschaffung von Dienstleistern können Rückfragen zu bisherigen Testerfahrungen aushelfen. Außerdem gibt es seitens TCT organisierte Events für getestete Unternehmen und Control Teams, die einen Erfahrungsaustausch ermöglichen.

Wir als axians security force erfüllen alle benötigten Anforderungen für die Durchführung von TIBER-Tests und Threat Led Penetration Tests (TLPT).

Tipps für die Threat Intelligence Phase

Transparenz und Kommunikation

Nach Eingang der Testbenachrichtigung sollten Verantwortlichkeiten innerhalb des Zielunternehmens definiert werden. Dies geschieht über die Aufstellung des für den Testverlauf eingeweihten Control Teams. Wichtig ist, dass ein Control Team Lead definiert wird, der zentraler Ansprechpartner für den durchführenden Dienstleister, sowie das TCT der Bundesbank ist. Darüber hinaus sollte es eine Vertretung geben. Weitere Teammitglieder können ebenfalls definiert werden – essenziell ist nur, dass niemand aus dem Blue Team über den geplanten Testablauf informiert wird. Es empfiehlt sich das Control Team initial klein zu halten (3 – 4 Mitglieder).

Control Team Mitglieder bestehen oftmals aus Mitarbeitern der internen Informationssicherheit (Compliance) oder des internen Risikomanagements. Für einen möglich effektiven Testverlauf sollten Mitglieder in das White Team aufgenommen werden, die einen Einblick in die Kritikalitätsbewertung von Prozessen und Systemen haben. Dies erleichtert die Definition des Testumfangs und das Beantworten möglicher Fragen seitens des durchführenden Dienstleisters während des Testverlaufs.

Hilfreiche Informationen

Annex 1 des „TIBER-EU Targeted Threat Intelligence Report Guidance" beinhaltet hilfreiche Informationen, die das Zielunternehmen dem TI-Team vor Start der TI-Phase bereitstellen sollte. Dies beinhaltet zum Beispiel:

- Details zu Domänen und IP-Adressen
- Details zu Nischenmärkten in denen das Zielunternehmen aktiv ist
- Liste an Ländern in denen das Unternehmen eine Marktpräsenz hat
- Liste an Beispielen vergangener Cyber-Vorfälle
- Kundensegmente, die interessant für ausländische Geheimdienste sein könnten

Ein Teilen der Informationen ermöglicht es dem TI-Team weniger Ressourcen für die Suche nach Unternehmensrisiken aufzuwenden und stattdessen einen größeren Fokus auf technische Erkenntnisse oder Detailanalysen zu legen.

Tipps für das Red Teaming

Tagesaktueller Austausch

Während des aktiven Red Teamings besteht ein täglicher, direkter Austausch mit dem Control Team. Dies erfolgt durch ein tägliches Jour Fixe sowie durch Instant-Messaging-Nachrichten (Signal) und ermöglicht es dem Control Team stets über aktuelle Aktivitäten informiert zu sein.

Detaillierte Dokumentation

Das Red Team erstellt detaillierte Ergebnisdokumentationen in Form von Folien für die wöchentlichen Jour Fixe und die Workshops in der Testabschlussphase. Diese beinhalten Key-Performance-Indikatoren und können vom Control Team als Statusbericht oder Testablaufprotokoll für beteiligte Stakeholder verwendet werden.

Kooperation über aktive Testphase hinaus

Nach der zwölfwöchigen, aktiven Testphase behält das Red Team einen guten Kontakt zum Control Team sowie auch Blue Team und setzt die Zusammenarbeit im Nachgang fort. Hierbei bietet das Red Team insbesondere Unterstützung beim Briefing des Blue Teams und des Vorstands.

In den Workshops während der Abschlussphase versucht das Red Team alle Beteiligten abzuholen und auch Variationen der erfolgten Angriffe in einer entspannten, aber lebhaften Atmosphäre durchzuführen. Dies soll den Erkenntnisgewinn für das Blue Team maximieren.

Gemeinsame Stärken: Red Teaming für mehr Resilienz mit Axians

09/2025

axians

Axians Security Force GmbH · Landsberger Str. 346 · 80687 München
Tel.: +49 89 889518190
E-Mail: info-asf@axians.de · www.axians.de