DORA-Compliance verstehen – IT Sicherheit gezielt prüfen

DORA: BRAUCHEN SIE EINEN PENTEST ODER THREAT-LED PENETRATION TESTING?

Wie Sie regulatorische Anforderungen erfüllen und gleichzeitig Ihre IT-Sicherheit strategisch stärken

Alle relevanten Informationen zu Cyber Security Assessments im Rahmen von DORA – inklusive Checkliste für Banken, Finanzinstitute und Versicherungen, die herausfinden wollen, ob ein Penetrationstest oder ein Threat-Led Penetration Testing für sie das Richtige ist.

ProSec
Security redefined.

ProSec
Security redefined.

Inhaltsverzeichnis

Was ist Threat-Led Penetration Testing (TLPT)?

Die DORA-Regulierung definiert neue Anforderungen für Cyber Security Assessments – darunter auch das Threat-Led Penetration Testing (TLPT), das für bestimmte Unternehmen mit besonders hohen Sicherheitsanforderungen verpflichtend ist. Doch was genau ist TLPT? Können auch Finanzunternehmen davon profitieren, die nicht explizit dazu verpflichtet sind?

Der Begriff TLPT wurde bereits 2018 von der G7 Cyber Expert Group eingeführt und sollte sicherstellen, dass Penetrationstests im Finanzsektor realistische Bedrohungsszenarien abbilden und Unternehmen gezielt auf Cyberangriffe vorbereiten. DORA greift dieses Konzept auf und fordert TLPT nun explizit für besonders kritische Instanzen des Finanzsektors.

Doch der eigentliche Kern von TLPT ist nichts grundlegend Neues – und genau hier setzen wir an: Jeder Penetrationstest von ProSec ist „threat-led“, denn wir orientieren uns immer an realen Angriffsvektoren und praxisnahen Risiken. **Der Unterschied liegt in der formalen Struktur**: TLPT erfordert eine noch detailliertere Dokumentation, eine präzise Bedrohungsanalyse und gegebenenfalls zusätzliche Workshops.

Was bedeutet das für Sie? Ganz gleich, ob Ihr Unternehmen explizit TLPT benötigt oder nicht – bei uns erhalten Sie immer einen praxisrelevanten, zielführenden Penetrationstest, der echte Sicherheitslücken aufdeckt und umsetzbare Maßnahmen liefert.

Pentest vs. TLPT: Was ist der Unterschied?

TLPT ist als feststehender Begriff – etwa in der DORA-Regulierung – ein regulatorischer Rahmen für eine Zielsetzung, die wir bei jedem Penetrationstest verfolgen:

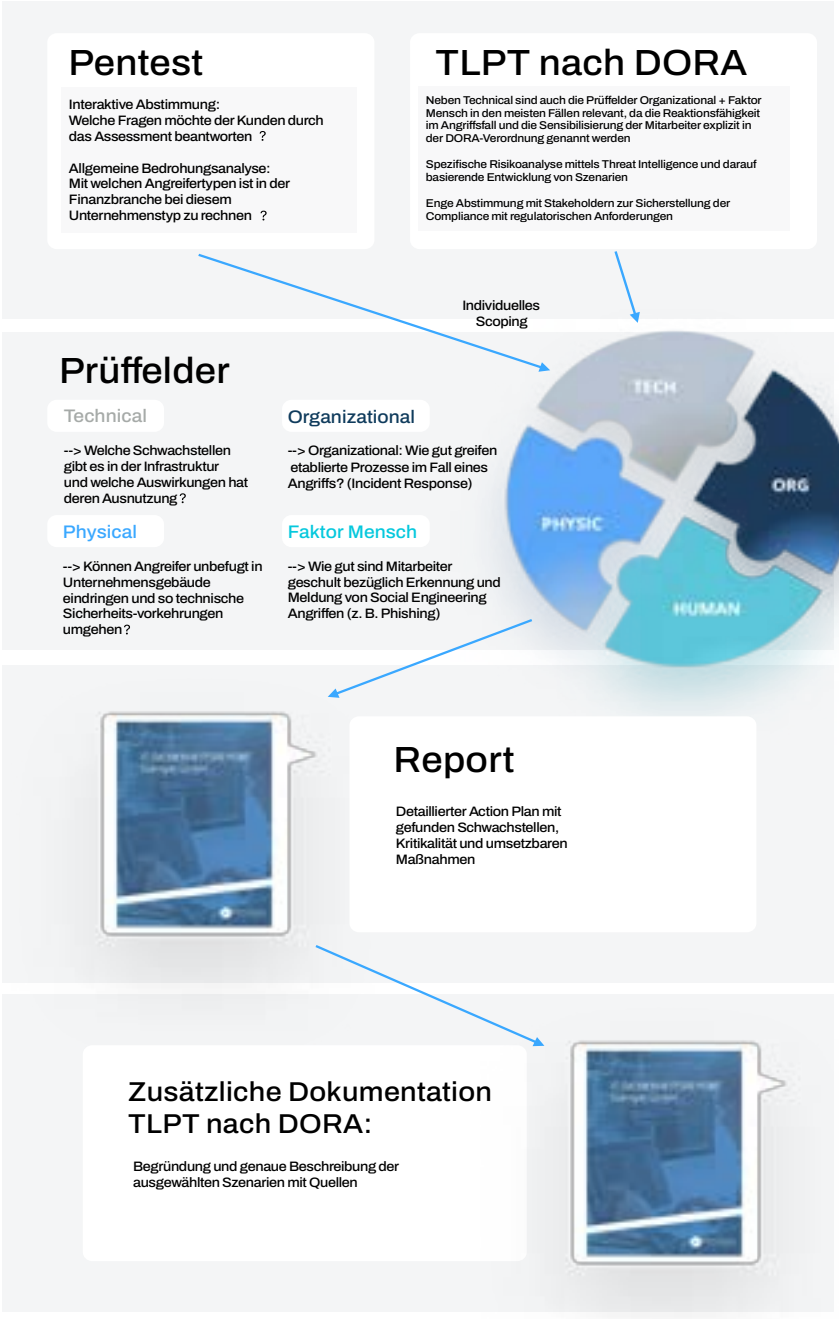
1. Wir identifizieren Schwachstellen, die von Angreifern mit hoher Wahrscheinlichkeit ausgenutzt würden.
2. Wir priorisieren Sicherheitslücken so, dass Unternehmen sie gezielt und effektiv schließen können.

Während alle unsere Penetrationstests praxisnah und „threat-led“ sind, erfüllt TLPT spezifische regulatorische Anforderungen und legt zusätzlich einen stärkeren Fokus auf formale Dokumentation und Bedrohungsanalysen:

- **Detaillierte Bedrohungsanalyse & Asset-Workshops:**
  TLPT setzt eine umfassende Analyse geschäftskritischer Systeme und möglicher Angriffsvektoren voraus.
- **Erweiterte Dokumentation & behördliche Abstimmung:**
  Die gewählten Bedrohungsmodelle müssen formal und nachvollziehbar begründet und dokumentiert werden.
- **Enge Ausrichtung an regulatorischen Rahmenwerken:**
  Internationale Best Practices wie TIBER-EU können hierbei als Referenz dienen – sind aber nicht automatisch verpflichtend.

Ein regulärer Penetrationstest von ProSec ist ebenfalls an TLPT-Prinzipien ausgerichtet, bleibt jedoch flexibler in Umfang und Methodik. Er eignet sich besonders für Unternehmen, die keine regulatorische Verpflichtung zu TLPT haben, aber dennoch ihre IT-Sicherheit realistisch testen möchten.

Nachdem wir die Unterschiede zwischen einem regulären Pentest und TLPT beleuchtet haben, stellt sich die Frage: Welche Schritte sind erforderlich, um eine realistische Angriffssimulation zu gewährleisten?



Wie läuft TLPT ab?

1. Informationssammlung:

Penetrationstester analysieren Unternehmensstrukturen, kritische Prozesse und verfügbare Dokumentationen (z. B. Netzwerkpläne, Bedrohungsberichte) sowie öffentlich zugängliche Informationen.

2. Sicherheitskritische Systeme & Daten identifizieren:

Fokus auf zentrale Systeme (z. B. Zahlungssysteme, Kundendatenbanken). Eine Business Impact Analysis bewertet mögliche Folgen eines Angriffs.

3. Bedrohungsmodellierung:

Entwicklung eines unternehmensspezifischen Angriffsmodells auf Basis interner Risiken und Schwachstellen (z. B. Angriffsvektoren wie Social Engineering oder Insider-Bedrohungen).

4. Threat Intelligence nutzen:

Analyse aktueller Bedrohungen durch externe Quellen wie CrowdStrike oder ENISA-Berichte, um branchenspezifische Risiken zu identifizieren und das Bedrohungsmodell zu schärfen.

5. Szenarien entwickeln:

Penetrationstester simulieren realistische Angriffe (z. B. Phishing oder Insider-Bedrohungen), die gezielt Schwachstellen des Unternehmens testen. Diese Szenarien werden dokumentiert und begründet.

6. Workshops und Abstimmung:

Zusammenarbeit mit internen Stakeholdern (z. B. IT-Leiter, Compliance-Teams) sowie, falls erforderlich, Aufsichtsbehörden, um sicherzustellen, dass regulatorische Anforderungen abgedeckt werden.

7. Durchführung des Tests:

Simulation der Angriffsszenarien, um Schwachstellen in technischer Infrastruktur, Prozessen und organisatorischer Resilienz aufzudecken.

8. Berichterstellung und Analyse:

Erstellung eines detaillierten Berichts mit identifizierten Schwachstellen, Begründung der Angriffsszenarien und priorisierten Handlungsempfehlungen. Ergebnisse werden gemeinsam mit dem Unternehmen analysiert.

TLPT legt zusätzlich zur technischen Prüfung einen verstärkten Fokus auf regulatorische Anforderungen sowie die organisatorische Resilienz. Ein regulärer Pentest kann je nach Bedarf ähnliche Elemente enthalten, bietet jedoch mehr Flexibilität in der Umsetzung. **Wie können Sie herausfinden, welche Variante für Sie die richtige ist? Im nächsten Abschnitt erfahren Sie, welche Kriterien eine Rolle spielen.**

Was ist die richtige Variante für Ihr Finanzunternehmen?

Variante 1: Sie haben Post

Ein klares Zeichen, dass Ihr Unternehmen TLPT-konform geprüft werden muss: Sie haben ein offizielles Schreiben von der BaFin oder der Deutschen Bundesbank erhalten.

In diesem Fall gibt es keinen Interpretationsspielraum – die Anforderungen müssen erfüllt werden. Wir stellen sicher, dass Ihr TLPT die DORA-Vorgaben vollständig erfüllt. Mit unserer Erfahrung im Testen kritischer Infrastrukturen sorgen wir für eine praxisnahe Umsetzung, die behördliche Vorgaben und Ihre Sicherheitsstrategie sinnvoll ergänzt.

Variante 2: Sie haben keinen Brief erhalten – aber ist TLPT trotzdem sinnvoll?

Falls Ihr Unternehmen kein offizielles Schreiben der BaFin oder Bundesbank erhalten hat, bedeutet das nicht automatisch, dass TLPT für Sie irrelevant ist. Während bestimmte Unternehmen zur Durchführung verpflichtet sind, kann TLPT für andere Organisationen eine sinnvolle Maßnahme zur Stärkung ihrer Cyber-Resilienz sein. Ob Ihr Unternehmen sich für einen regulären Penetrationstest oder TLPT entscheiden sollte, hängt von Ihrer individuellen Sicherheitsstrategie ab.

Ein regulärer Penetrationstest von ProSec ist bereits stark an TLPT-Prinzipien ausgerichtet: Sie erhalten eine realistische Einschätzung der Sicherheit Ihrer IKT-Systeme, inklusive umsetzbarer Optimierungsmaßnahmen.

Wann ist TLPT dennoch eine sinnvolle Wahl?

Folgende Faktoren sprechen dafür, über einen TLPT nachzudenken:

- Sie führen regelmäßig Penetrationstests durch und setzen empfohlene Maßnahmen konsequent um. Das bedeutet, dass bei einem Retest oder einer Prüfung durch einen anderen Dienstleister nicht wiederholt dieselben Schwachstellen ausgenutzt werden können.
- Ihr Unternehmen hat bereits einen hohen Reifegrad in Sachen IKT-Sicherheit. TLPT könnte die nächste Stufe sein, um gezielt Ihre Resilienz gegen realistische Bedrohungsszenarien zu testen.

- Sie verfügen über eine aktuelle und umfassende Dokumentation Ihrer sicherheitskritischen Systeme und Daten.
- Sie verfolgen ein konkretes Ziel mit dem nächsten Penetrationstest. Beispielsweise möchten Sie gezielt die Sicherheit der für Ihr Unternehmen kritischsten Systeme prüfen oder sich auf zukünftige regulatorische Anforderungen vorbereiten.

Lassen Sie uns gemeinsam herausfinden, was für Ihr Unternehmen sinnvoll ist!

IT-Sicherheit ist keine isolierte Compliance-Aufgabe, sondern ein geschäftskritischer Faktor. Unternehmen, die proaktiv handeln, können nicht nur regulatorische Risiken minimieren, sondern auch finanziellen Schaden durch Cyberangriffe vermeiden und das Vertrauen von Kunden und Investoren stärken. Lassen Sie uns gemeinsam herausfinden, welche Sicherheitsstrategie für Sie die beste ist.

Jetzt Beratungsgespräch vereinbaren

Welche Voraussetzungen müssen Finanzunternehmen erfüllen, um TLPT sinnvoll nutzen zu können?

TLPT geht weit über die reine technische Prüfung hinaus. Er testet nicht nur IT-Sicherheitsmaßnahmen, sondern auch die organisatorische Resilienz, interne Abläufe und den Faktor Mensch – Aspekte, die bei realen Angriffen oft entscheidend sind.

TLPT beantwortet unter anderem folgende Fragen:

- **Detektion:** Wird der Angriff erkannt? Wenn ja, wie schnell?
- **Reaktion:** Werden die richtigen Maßnahmen zur Eindämmung ergriffen?
- **Kommunikation:** Sind interne und externe Eskalationswege klar definiert und effektiv?
- **Wiederherstellung:** Wie gut funktioniert die Schadensbegrenzung und die Rückkehr zum Normalbetrieb?

Diese Fragen können auch durch einen klassischen Penetrationstest beantwortet werden, wenn das Prüffeld „Organizational“ im gemeinsamen Scoping als sinnvoller Bestandteil ermittelt wurde (siehe Abb. S. 05). Beim TLPT gehören sie in jedem Fall zu den Kernfragen des Tests.

Damit TLPT aussagekräftige Erkenntnisse liefert, müssen bestimmte Prozesse, Tools und Experten im Unternehmen vorhanden sein. Falls hier noch Lücken bestehen, unterstützen wir Sie gerne:

- Schrittweise Heranführung an TLPT-Niveau: Unsere regulären Penetrationstests sind bereits stark an TLPT-Prinzipien ausgerichtet. Sie eignen sich ideal, um Unternehmen auf ein höheres Sicherheitsniveau zu bringen.
- Reifegradgerechte Testansätze: Wir passen Umfang und Angriffslevel immer an die bestehende Sicherheitsstrategie an. Dadurch erhalten Sie genau die Rückmeldung, die Sie für den gezielten Ausbau Ihrer IT-Resilienz benötigen.

Nutzen Sie die Checkliste auf der nächsten Seite, um einzuschätzen, ob Ihr Unternehmen bereit für TLPT ist – oder ob ein regulärer Penetrationstest aktuell die sinnvollere Wahl darstellt.

Ist Ihr Unternehmen bereit für TLPT?

Ein TLPT liefert die besten Ergebnisse, wenn bestimmte Prozesse, Tools und Expertenstrukturen bereits vorhanden sind. Nutzen Sie die folgende Checkliste, um eine erste Einschätzung zu treffen:

Prozesse:

1. Notfall- und Wiederherstellungspläne:

- Gibt es dokumentierte Pläne zur Reaktion auf Sicherheitsvorfälle? ☐ Ja ☐ Nein
- Werden diese Pläne regelmäßig getestet? ☐ Ja ☐ Nein

2. Kommunikations- und Eskalationsketten:

- Sind klare Kommunikations- und Eskalationswege definiert? ☐ Ja ☐ Nein

3. Identifikation sicherheitskritischer Systeme und Bedrohungen:

- Sind die sicherheitskritischen Systeme, Daten und Prozesse des Unternehmens identifiziert? ☐ Ja ☐ Nein

4. Vorfallmanagement:

- Gibt es standardisierte Verfahren, um Vorfälle zu erkennen, zu analysieren und zu beheben? ☐ Ja ☐ Nein

Tools:

5. SIEM-System:

- Wird ein System zur Echtzeitüberwachung und Protokollierung von Sicherheitsvorfällen genutzt? ☐ Ja ☐ Nein

6. Threat Intelligence Feeds:

- Werden Bedrohungsinformationen genutzt, um aktuelle Angriffsmethoden zu identifizieren? ☐ Ja ☐ Nein

7. Backup- und Wiederherstellungssysteme:

- Sind Daten regelmäßig gesichert, und können diese im Ernstfall schnell wiederhergestellt werden? ☐ Ja ☐ Nein

8. Ticket- und Workflow-Management:

- Gibt es ein Tool zur Nachverfolgung und Dokumentation von Sicherheitsvorfällen? ☐ Ja ☐ Nein

9. Security Operations Center (SOC):

- Gibt es ein SOC, das Ihre Systeme und Netzwerke rund um die Uhr überwacht und auf Bedrohungen reagiert? ☐ Ja ☐ Nein

10. Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems (IPS):

- Nutzen Sie IDS/IPS, um verdächtige Netzwerkaktivitäten zu erkennen und Angriffe zu blockieren? ☐ Ja ☐ Nein

Experten:

11. Incident Response Team:

- Gibt es ein Team, das für die Erkennung und Reaktion auf Sicherheitsvorfälle zuständig ist? ☐ Ja ☐ Nein

12. Führungsebene:

- Sind Führungskräfte in Notfallpläne eingebunden und bereit, schnelle Entscheidungen zu treffen? ☐ Ja ☐ Nein

Wie auch immer Ihre Selbstevaluation ausfällt:

IT-Sicherheit ist keine Einmalmaßnahme, sondern ein kontinuierlicher Prozess. Falls Ihr Unternehmen keine regulatorische Verpflichtung zu TLPT hat oder nicht alle Punkte der Checkliste erfüllt, kann ein klassischer Penetrationstest eine sinnvolle Alternative sein. Er bietet flexible, praxisnahe Angriffssimulationen ohne den formalen Rahmen von TLPT. Wir passen jeden Test an Ihren aktuellen Reifegrad an – damit Sie genau die Erkenntnisse erhalten, die Sie für den Ausbau Ihrer Sicherheitsstrategie benötigen.

Sind Sie unsicher, ob ein klassischer Pentest oder ein TLPT für Sie der richtige Weg ist? Lassen Sie uns in einem unverbindlichen Erstgespräch gemeinsam Ihre Sicherheitsstrategie analysieren – praxisnah, compliance-konform und mit echtem Mehrwert.

Beratungstermin sichern

ProSec
Security redefined.

WHO WE ARE

2016
gegründet

50+
Team-Mitglieder

1000+
durchgeführte Assessments

100%
Systemübernahmen

UNSERE MISSION

Menschenleben retten und schützen, indem wir die digitale Infrastruktur von Unternehmen nachhaltig sicher machen.

UNSERE VISION

Wir wollen IT Security viral gehen lassen.

HOW WE SUPPORT YOUR INFORMATION SECURITY

Penetration Testing IT Security Consulting Ethical Hacker Courses

„IT Security aus der Eifel
für Kunden weltweit."