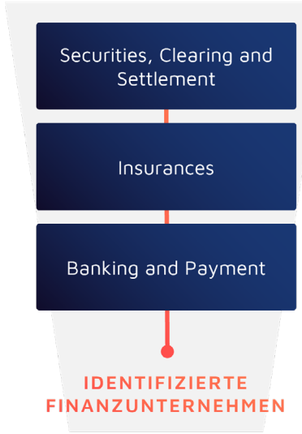
DIGITALE RESILIENZ IM FINANZSEKTOR

Was bedeutet Threat-led Penetration Testing (TLPT) unter DORA?

Die zunehmende Digitalisierung im Finanzsektor bringt zahlreiche Chancen – aber auch erhebliche Risiken. Cyberangriffe auf Finanzinstitute nehmen stetig zu, sowohl in Häufigkeit als auch in Komplexität. Um dieser Bedrohungslage zu begegnen, hat die Europäische Union mit dem Digital Operational Resilience Act (DORA) einen einheitlichen Rechtsrahmen geschaffen. DORA verpflichtet bestimmte Finanzunternehmen in der EU, insbesondere solche mit hoher Systemrelevanz oder besonderem IKT-Risikoprofil, dazu, ihre digitale Widerstandsfähigkeit aktiv zu stärken.

Ein zielgerichtetes Instrument dabei ist das sogenannte Threat-led Penetration Testing (TLPT). Es kombiniert Threat Intelligence, Penetration Testing und Red Teaming, um kritische Schwachstellen in der digitalen Infrastruktur frühzeitig zu erkennen und konkrete Maßnahmen zur Verbesserung der Cyberabwehr abzuleiten. Im Unterschied zu klassischen IT-Sicherheitsaudits simuliert ein TLPT einen echten, koordinierten Angriff durch Cyberkriminelle. Die Tests basieren auf realistischen Angriffsszenarien, die auf aktuellen, durch Threat Intelligence ermittelten Bedrohungsanalysen beruhen und zum Beispiel Informationen aus dem Darknet oder aus Berichten über kürzlich erfolgte Angriffe auf vergleichbare Unternehmen berücksichtigen. Es werden also besonders relevante Angriffsmechanismen, -wege und -szenarien herangezogen, um den versuchten Einbruch in kritische Systeme des Unternehmens oder das Ausnutzen relevanter Sicherheitslücken so realistisch wie möglich zu gestalten und damit die Reaktionsfähigkeit der Verteidigungsteams zu testen.

TECHNISCHER REGULIERUNGSSTANDARD (RTS) ZU TLPT



1 QUANTITATIVE KRITERIEN

Quantitative Kriterien für die Identifikation für bestimmte Arten von Finanzunternehmen wie

- Kreditinstitute *(Schwellenwerte)*
- Zahlungsinstitute *(Schwellenwerte)*
- E-Geldinstitute *(Schwellenwerte)*
- Zentralverwahrer
- Zentrale Gegenparteien
- Handelsplätze *(Schwellenwerte)*
- Versicherungsunternehmen *(Schwellenwerte)*

Verschiedene Kriterien und Schwellenwerte berücksichtigen die jeweiligen sektorspezifischen Besonderheiten

2 QUALITATIVE KRITERIEN & FLEXIBILITÄT

Qualitiative Kriterien ermöglichen der zuständigen Aufsichtsbehörde Besonderheiten zu berücksichtigen basierend auf

- **Auswirkungsbezogenen und den systemischen Charakter betreffenden Faktoren** (wie size, market share, interconnectedness, criticality or importance of services, complexity of the business model, group structure)
- **IKT-Risiko bezogenen Faktoren** (risk profil, threat landscape, dependence on ICT, complexity of ICT architecture, maturity, group structure)

3

Identifizierte Finanzunternehmen, die TLPT durchzuführen haben unter DORA

Abb. 1: Technischer Regulierungsstandard mit Kriterien zur Identifikation von Finanzunternehmen, die TLPT durchzuführen haben
Quelle: In Anlehnung an BaFin, 2024

Wer muss ein TLPT durchführen – und wie oft?

Nicht jedes Finanzunternehmen muss automatisch ein TLPT durchführen. Der technische Regulierungsstandard (RTS), der die Kriterien zur Identifikation von Finanzunternehmen festlegt, die ein TLPT durchführen müssen, wurde im Rahmen von DORA von den drei europäischen Aufsichtsbehörden ESMA, EBA und EIOPA entwickelt. Dieser RTS legt verbindlich fest, welche Unternehmen betroffen sind und unter welchen Voraussetzungen sie von der zuständigen Aufsicht zur Durchführung eines TLPT aufgefordert werden können (Abb. 1).

Die offizielle Verpflichtung erfolgt durch einen sogenannten **Identifikationsbescheid**, der von der zuständigen Aufsichtsbehörde – in Deutschland ist das meist die BaFin, auf europäischer Ebene die Europäische Zentralbank (EZB) – ausgestellt wird. Betroffen sind in der Regel Unternehmen mit besonders hohem Risiko oder systemischer Relevanz, etwa große Banken, Zahlungsdienstleister:innen oder Betreiber:innen zentraler Marktinfrastrukturen.

Sobald ein Unternehmen benannt wurde, ist es gesetzlich dazu verpflichtet, **mindestens alle drei Jahre ein TLPT durchzuführen**. Die Durchführung erfolgt nach klaren Regeln, die im Einklang mit europäischen Standards wie dem TIBER-EU-Framework stehen (TIBER = Threat Intelligence-based Ethical Red Teaming) (Abb. 2).

Die Rolle externer Threat Intelligence Provider (TIPs)

Ein elementarer Bestandteil eines TLPT ist die Beteiligung eines externen Threat Intelligence Providers. Diese spezialisierten Dienstleister:innen analysieren das aktuelle Bedrohungsumfeld eines Unternehmens und identifizieren mögliche Angriffsvektoren – etwa durch Einblicke in kriminelle Aktivitäten im Darknet, geleakte Datenbanken oder Hackerforen. Auf dieser Grundlage entwickeln sie individuelle Angriffsszenarien, die im Rahmen des Tests durch Red Teams umgesetzt werden.

DORA schreibt genau vor, welche Anforderungen solche Anbieter:innen erfüllen müssen: Sie dürfen nicht Teil des Unternehmens sein, müssen umfangreiche Erfahrung im Finanzsektor vorweisen und über relevante Zertifizierungen (z. B. ISO 27001, CREST oder OSCP) verfügen. Ziel ist es, Objektivität, Unabhängigkeit und ein hohes Maß an Fachkompetenz sicherzustellen.

Warum TLPTs gerade jetzt wichtiger denn je sind

Die Bedrohungslage im digitalen Raum verändert sich rasant. Mit dem Einsatz neuer Technologien, insbesondere **künstlicher Intelligenz (KI)**, werden Cyberangriffe immer ausgefeilter. Gleichzeitig steigen die regulatorischen Anforderungen:

TLPTs sind längst **kein freiwilliges Sicherheits-Upgrade mehr, sondern in vielen Fällen eine gesetzliche Verpflichtung.** Und selbst dort, wo noch keine Pflicht besteht, lohnt sich die frühzeitige Vorbereitung. Und dies nicht nur um im Fall einer Einstufung durch die Aufsicht schnell und souverän reagieren zu können.

Ein TLPT ist jedoch nur ein Baustein in einem umfassenden Sicherheitskonzept. Unternehmen, die ihre digitale Resilienz ernst nehmen, kombinieren solche Tests mit kontinuierlichem Bedrohungsmonitoring, regelmäßigen Schwachstellenanalysen und einem proaktiven Umgang mit Sicherheitslücken. Nur so lässt sich sicherstellen, dass kritische Systeme auch langfristig widerstandsfähig bleiben.

Der Ablauf eines Threat-led Penetration Tests (TLPT) folgt einem klar strukturierten Prozess, der sicherstellen soll, dass realistische, gezielte und wirkungsvolle Angriffssimulationen durchgeführt werden. Ziel ist es, zu testen, wie gut ein Unternehmen auf fortschrittliche Cyberangriffe vorbereitet ist – aus Perspektive eines tatsächlichen Angreifers. Die typischen Phasen eines TLPTs orientieren sich an bewährten Frameworks wie TIBER-EU, das auch als Grundlage für DORA-konforme TLPTs dient.

ABLAUF EINES THREAT-LED PENETRATION TESTINGS UNTER DORA

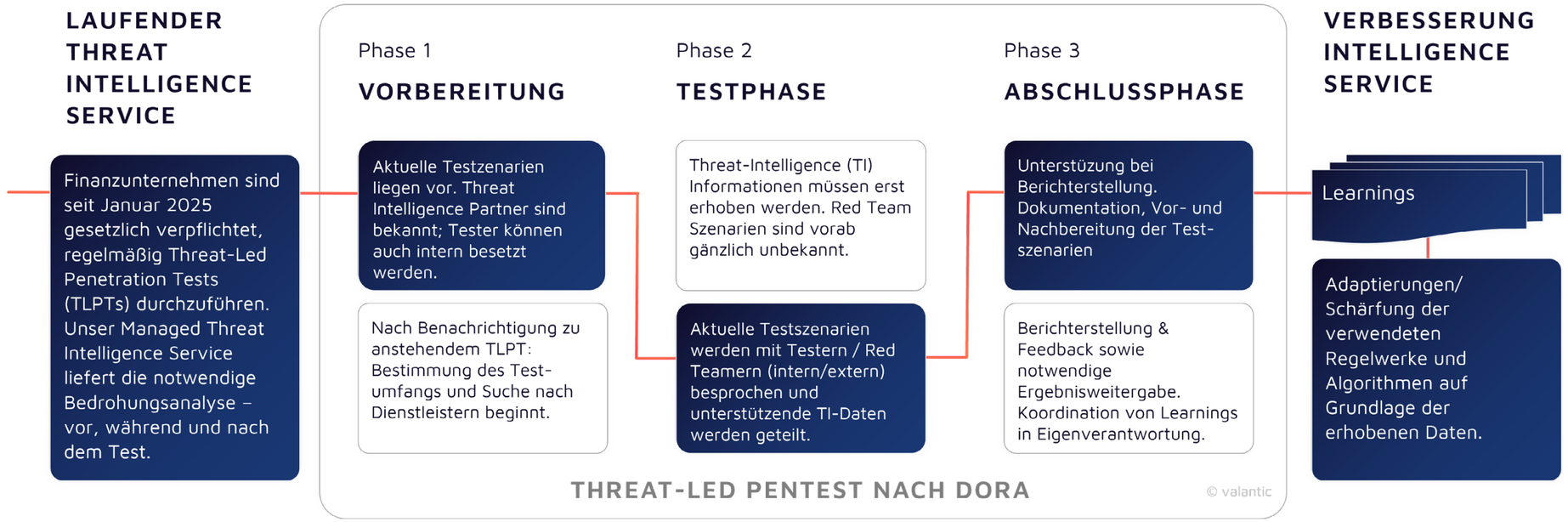


Abb. 2: Testmethodik für TLPT unter DORA
Quelle: Eigene Darstellung

Unterstützung entlang des gesamten TLPT-Prozesses – und darüber hinaus

Wir begleiten Sie auf dem gesamten Weg zur DORA-Konformität: von der ersten Bedrohungsanalyse bis zur strategischen Umsetzung der Erkenntnisse. Als externer Threat Intelligence Provider erfüllen wir sämtliche regulatorischen Anforderungen und verfügen über langjährige Erfahrung im Finanzumfeld. Unsere Leistungen umfassen unter anderem:

- Die Durchführung umfassender Bedrohungsanalysen auf Basis aktueller Informationen aus dem Darknet und anderen Quellen,
- die Entwicklung realistischer Angriffsszenarien für TLPTs,
- das kontinuierliche Monitoring sicherheitsrelevanter Entwicklungen,
- die enge Zusammenarbeit mit erfahrenen Red Team- und Pentest-Partnern für die reibungslose Umsetzung,
- sowie die strukturierte Nachbereitung mit konkreten Maßnahmenempfehlungen.

Ob als punktuelle Unterstützung oder als langfristiger Sparringspartner – mit unserem Managed Threat Intelligence Service helfen wir Ihnen nicht nur, die Komplexität von TLPTs pragmatisch und zielgerichtet zu bewältigen, ohne das Tagesgeschäft zu blockieren. Wir sorgen auch dafür, dass Ihr Unternehmen jederzeit gut informiert, vorbereitet und widerstandsfähig bleibt, weit über die verpflichtenden Tests hinaus.

Wir unterstützen sie gerne in jeder Phase. Kontakieren Sie uns.

Über valantic

valantic berät Unternehmen seit vielen Jahren kompetent und umfassend im Bereich der Cybersicherheit – vom Information Security Management über Regulatory Compliance bis hin zu präventiven Maßnahmen wie Threat Intelligence Analysen und Darknet Monitoring. So stellen wir sicher, dass unsere Kunden den Bedrohungen im digitalen Zeitalter einen Schritt voraus sind. Denn Sicherheit beginnt vor der Krise.

Thomas Lang
Partner
valantic GmbH

Ulf Bernhardt
Director
valantic GmbH