DORA-Readiness für Mainframe-Anwender

Sicherheitsmaßnahmen implementieren und Risikoprüfungen vorbereiten

Referent:

DR. STEPHEN FEDTKE

CTO, ENTERPRISE-IT-SECURITY.COM

ENTERPRISE-IT-SECURITY.COM

Kurz zu mir

Dr. Stephen Fedtke

- CTO von Enterprise-IT-Security.com
- Wirtschaftsingenieur Elektrotechnik, TH-Darmstadt
- Spezialist Mainframe, IT-Security, Penetration Tests, Compliance
- 20 Jahre technische Erfahrung in IT und Security

AGENDA

- Was bedeutet DORA für Mainframe-Anwender? Welche Themen müssen adressiert werden?
- DORA-Readiness für Mainframes durch Absicherung der Systeme und Instruktion des „Blue Teams“.
- Konkrete Schritte zur effizienten DORA-Readiness der Mainframe-Plattform - „be prepared“.

DORA – Digital Operational Resilience Act

DORA – neue EU Verordnung für die IT der Finanzwirtschaft

➔ **Ziel: Vermeidung IT-begründeter Katastrophen dank hoher Resilienz der IT**

Höchste IT-Sicherheit

Höchste IT-Verfügbarkeit

➔ **seit 17.01.2023 in Kraft**

➔ **Anwendung ab 17. Januar 2025**

Deutsche Umsetzung im Rahmen des Finanzmarktdigitalisierungsgesetzes (FinmadiG)

DORA – Digital Operational Resilience Act

DORA - Artikel 3, Absatz 1:

„digitale operationale Resilienz“

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck:

1. „digitale operationale Resilienz“ die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen;

Artikel 3, Abs. 1, VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

DORA - Herausforderungen an IT und Organisation

Wesentliche Elemente in DORA

IKT-Risikomanagement

- **Governance und Organisation**
- **IKT-Risikomanagement-rahmen**
- **IKT -Systeme, -Protokolle und –Tools**
- **Lernprozesse und Weiterentwicklung**
- **Kommunikation**

IKT-Drittpartei-risikomanagement

- **Allgemeine Prinzipien** (u. a. Informationsregister über IKT-Drittparteivertrags-beziehungen, Mitteilungen an die Aufsichtsbehörden, und Mindestvertrags-bestandteile)

EU-Überwachungs-rahmenwerk

- Überwachung von **kritischen IKT-Drittdienstleistern**

IKT-Vorfallmeldewesen

- Festlegung von **Definitionen** IKT-bezogener Vorfälle
- **Klassifikationskriterien** von IKT-bezogenen Vorfällen
- **Meldeprozess,** Berichtswesen von IKT-bezogenen Vorfällen und Cyberbedrohungen

Testen der digitalen operationalen Resilienz

- **Basistests**
- Gesamter Finanzsektor
- Schwachstellenscans, Quellcodetests, Performancetests etc.

TLPT

- **Fortgeschrittene Tests**
- TLPT: Threat Led Penetration Tests
- Nur „systemrelevante" Finanzunternehmen mit hohem IKT-Reifegrad
- TIBER-EU als „Blaupause"

Information Sharing & Cyberübungen

- Freiwilliger **Austausch von Informationen und Erkenntnissen** zwischen Finanzunternehmen zur Verbesserung der „Situational Awareness"
- Sektorübergreifende **Krisenmanagement- und Notfallübungen** mit Cyberbezug zur Verbesserung der Kommunikation und Stärkung der Resilienz im Finanzsektor

BaFin DORA - Digital Operational Resilience Act 05. Dezember 2023

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation1_Ueberblick_DORA.pdf?__blob=publicationFile&v=2

Technologisch zu lösende Kern-Herausforderungen

Was ist das IKT-Risikorahmenwerk nach DORA?

§ 5 Governance & Organisation

§ 6 IKT-Risikomanagementrahmen

§ 7 IKT-Systeme, -Protokolle und -Tools

§ 8 Identifizierung

§ 9 Schutz und Prävention

§ 12 Backup & Restoration

§ 11 Reaktion & Wiederherstellung

§ 10 Erkennung

§ 13 Lernprozesse & Weiterentwicklung

§ 14 Kommunikation

§15 Weitere Harmonisierung
von Tools, Methoden, Prozessen und Richtlinien für IKT-Risikomanagement

§16 Vereinfachter IKT-Risikomanagementrahmen

BaFin DEUTSCHE BUNDESBANK EUROSYSTEM

Was bedeutet DORA in der Praxis?
IKT-Risikomanagement

5. Dezember 2023 | 2

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation1_Ueberblick_DORA.pdf?__blob=publicationFile&v=2

Technologisch zu lösende Herausforderungen

SCHUTZ UND PRÄVENTION:

wirksames Vulnerability-Assessment

= intensive Schwachstellen-Analyse

Ziel:

Ein **über das Normalmaß hinausreichendes Niveau** an Schutzmaßnahmen und umfassender Compliance gegenüber IT-Sicherheits-, operationellen und Datenschutz-Risiken.

Technologisch zu lösende Herausforderungen

ERKENNEN UND REAKTION:

Wirksames Monitoring mit All-Phasen-Abdeckung

- **Vom „Anpirschen“, über die Tat, bis zur Flucht**
- **Vollständigkeit** in Bezug auf das Spektrum („schreiben alle relevanten Prozesse und alle detektionsrelevanten Raw-Events?“)
- **Detailstärke** („steht alles notwendige im Raw-Event?“)
- Stärke und Signifikanz der **Detektion**
  auch bezüglich der potentiellen **Unterschlagung von Events**
- Die Option zur gezielten **vorsichtigen Reaktion** und Verhinderung
- Unterstützung der **Forensik**

Technologisch zu lösende Herausforderungen

DAS GROSSE ZIEL

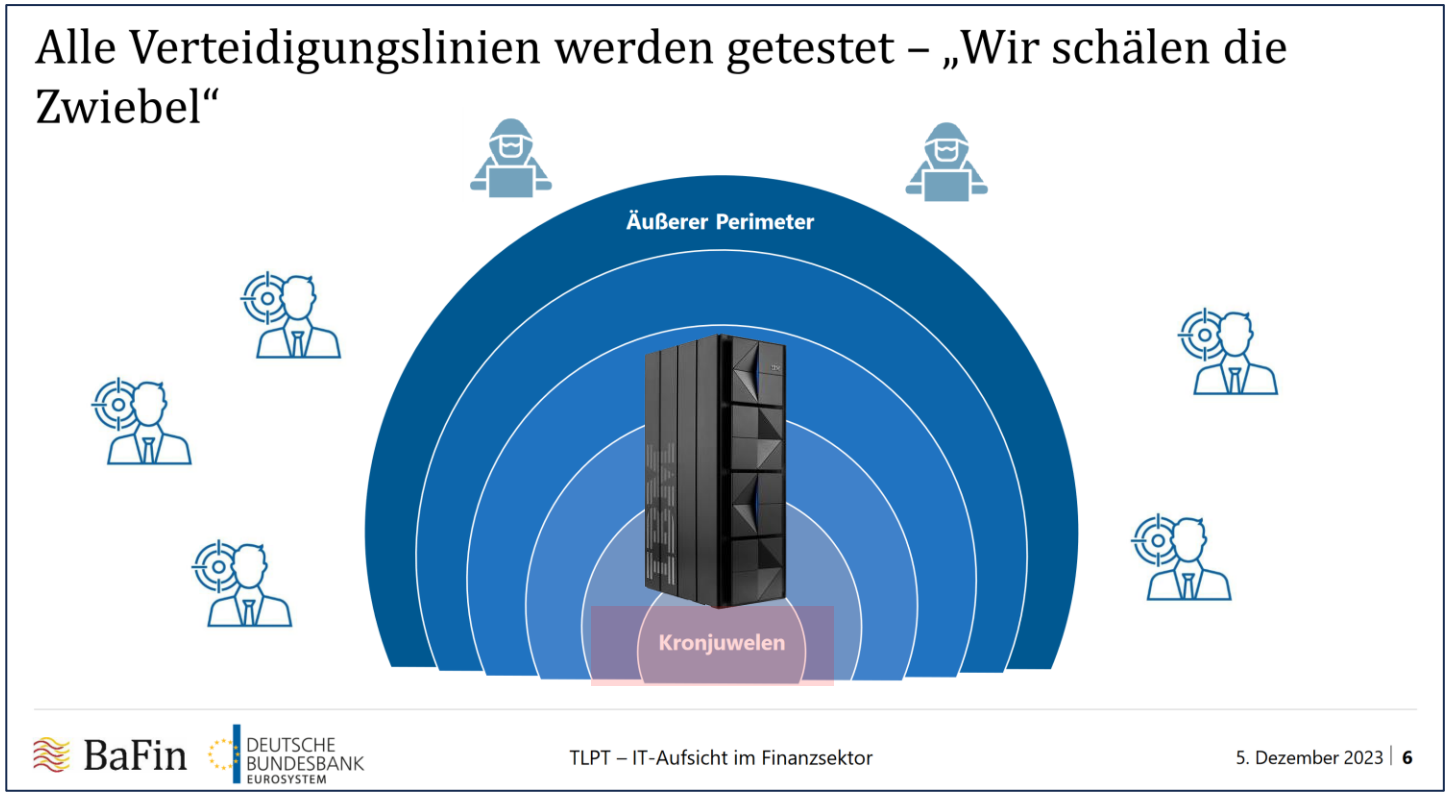
Am Ende den (Threat-Led) Penetration Test (TLP) mit „Bravour“ bestehen,

d.h. „das Spiel gegen die Red Sox“ gewinnen, oder höchsten „unentschieden spielen“.

„Kronjuwelen“ – Schutz, Prävention und Erkennung

Vulnerability-Assessment ➔ Monitoring ➔ Reaktion

mit 360-Grad-Sicht



Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation1_Ueberblick_DORA.pdf?__blob=publicationFile&v=2

DORA-Anforderung „Schutz und Prävention“

DORA - Artikel 9: Schutz und Prävention

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

Artikel 9

Schutz und Prävention

(1) Um einen angemessenen Schutz von IKT-Systemen zu gewährleisten und Gegenmaßnahmen zu organisieren, überwachen und kontrollieren Finanzunternehmen kontinuierlich die Sicherheit und das Funktionieren der IKT-Systeme und -Tools und minimieren durch den Einsatz angemessener IKT-Sicherheitstools, -Richtlinien und -Verfahren die Auswirkungen von IKT-Risiken auf IKT-Systeme.

(2) Finanzunternehmen konzipieren, beschaffen und implementieren IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools, die darauf abzielen, die Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen, insbesondere jener zur Unterstützung kritischer oder wichtiger Funktionen, zu gewährleisten und hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit, von Daten aufrechtzuerhalten, unabhängig davon, ob diese Daten gespeichert sind oder gerade verwendet oder übermittelt werden.

(3) Um die in Absatz 2 genannten Ziele zu erreichen, greifen Finanzunternehmen auf IKT-Lösungen und -Prozesse zurück, die gemäß Artikel 4 angemessen sind. Diese IKT-Lösungen und -Prozesse müssen

a) die Sicherheit der Datenübermittlungsmittel gewährleisten;

b) das Risiko von Datenkorruption oder -verlust, unbefugtem Zugriff und technischen Mängeln, die die Geschäftstätigkeit beeinträchtigen können, minimieren;

c) dem Mangel an Verfügbarkeit, der Beeinträchtigung der Authentizität und Integrität, den Verletzungen der Vertraulichkeit und dem Verlust von Daten vorbeugen;

DORA-Anforderung „Schutz und Prävention“

Pro-aktive
Überwachung ➔ Detektion ➔ Reaktion ➔ Härtung

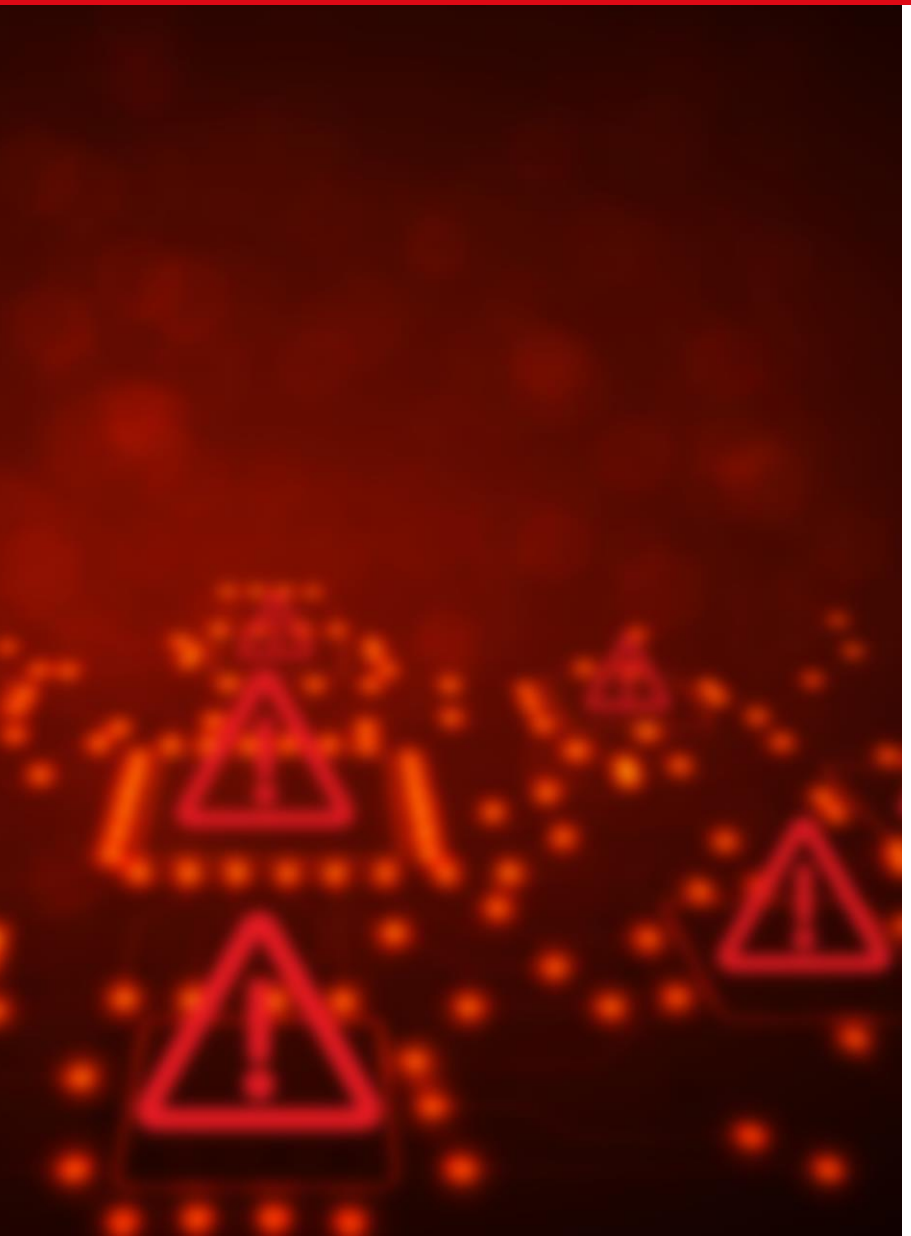
- **Kontinuierliches Assessment der Systeme**
  Fokus: sicherheits- und audit-bezogene sowie operationelle Risiken; Ausführung ist korreliert mit Änderungen und spezifischen Ereignissen im System (z.B. nach einem „parmlib change“).

- **Regelmäßige vollständige Prüfung**
  z.B. alle 24 Stunden zwecks zeitnahem Fixing der Schwachstellen

- **Permanentes zeitnahes Event-Monitoring**
  Gewinnung, Bereitstellung und Auswertung der Raw-Events

- **Kopplung zu SOC und SIEM**
  Ergänzung um Mainframe-spezifische Auswertungen, Korrelationen und Alarme; ferner Ermöglichung forensischer Aktivitäten

DORA-Anforderung „Anomalie-Erkennung“



Zusammenspiel zwischen Anomalie und Incident

- **FU müssen** eine **Anomalieerkennung implementieren**.
- Die Begrifflichkeiten **Events oder Problems werden in DORA nicht verwendet**.
- Der **Schwellenwert**, der einen durch eine **Anomalie** ausgelösten Alarm **zu einem Incident** werden lässt, **ist durch das FU zu bestimmen**.
  - **DORA nennt** hierfür **Trigger**, welche eine Behandlung im Incident-Management auslösen (**data loss, malicious activity, unavailiblity**...)

Draft RTS RMF:
Article 24 Anomalous activities detection and criteria for ICT-related incidents detection and response

[...] **detect anomalous activities** that can **result in ICT network performance issues and ICT-related incidents** [...] financial entities shall **implement detection mechanisms.**

[...] implement **tools generating alerts** for **anomalous activities and behaviour**, **at least for ICT assets and information assets supporting critical or important functions.** This shall include tools that provide automated alerts based on pre-defined rules to identify anomalies **affecting the completeness and the integrity of the data sources or, monitor thelog collection and issue an alert if the log collection failed** [...]

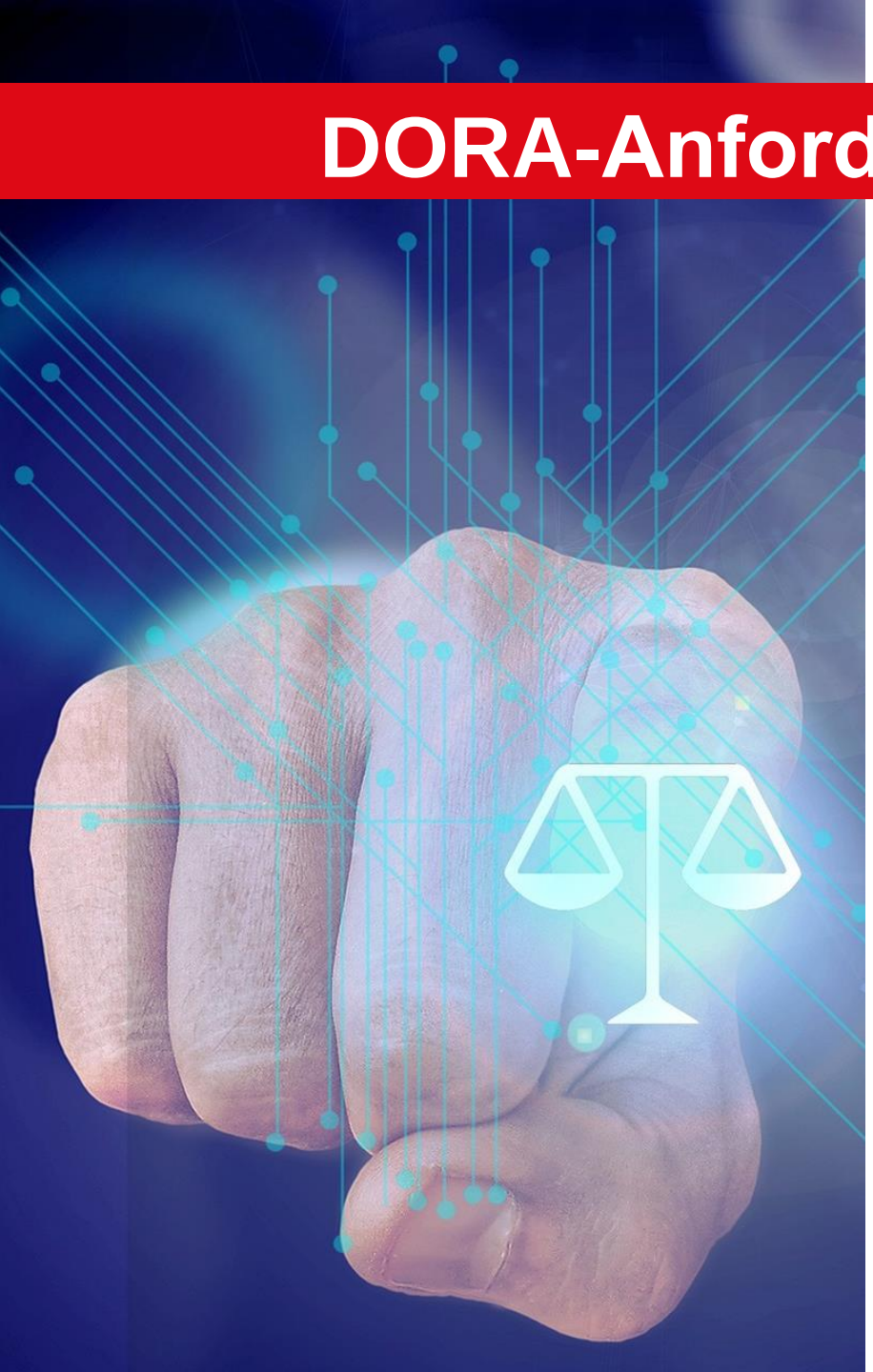
BaFin DEUTSCHE BUNDESBANK EUROSYSTEM

Was bedeutet DORA in der Praxis?
IKT-Risikomanagement

5. Dezember 2023 | 9

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation1_Ueberblick_DORA.pdf?__blob=publicationFile&v=2

DORA-Anforderung „Anomalie-Erkennung“



DORA - Artikel 10: Erkennung

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

Artikel 10

Erkennung

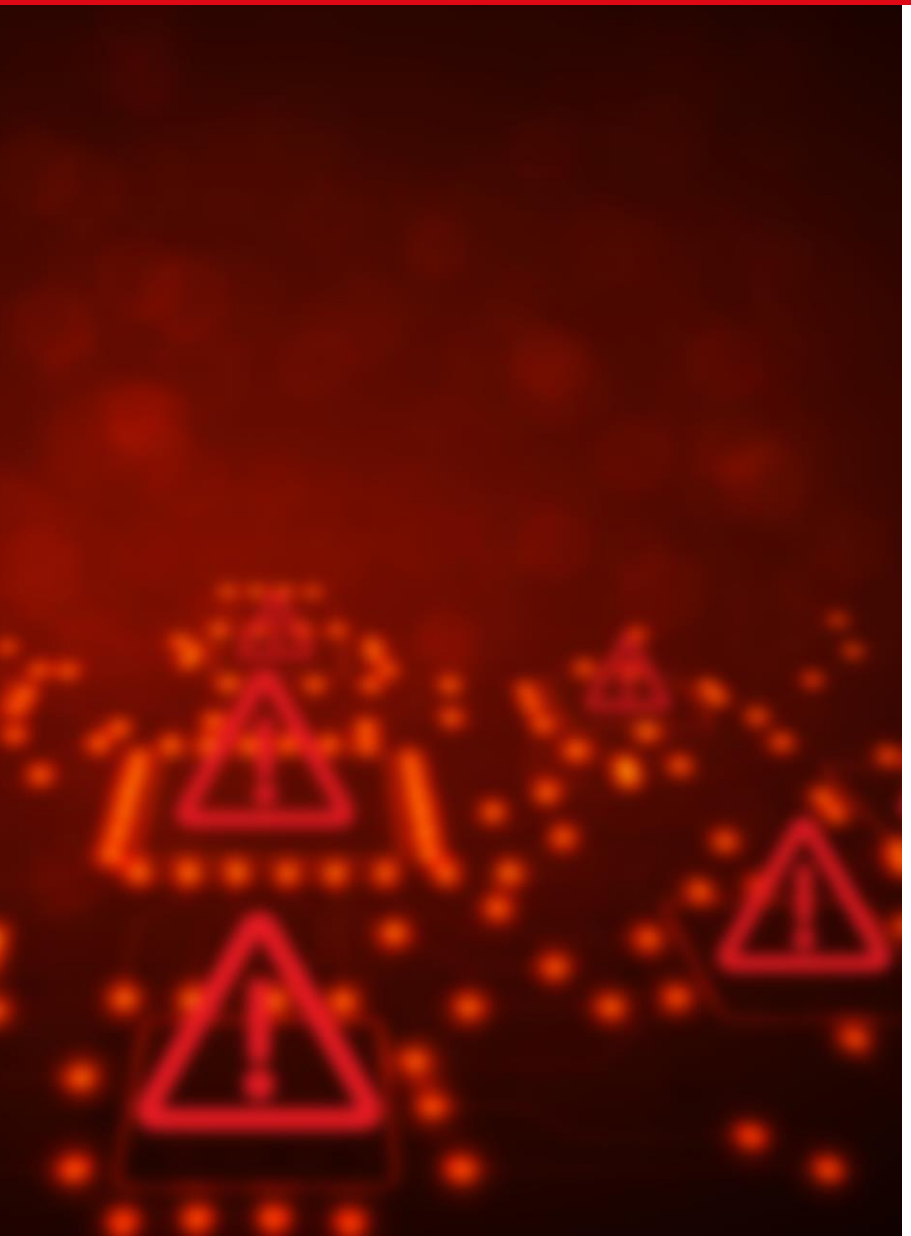
(1) Finanzunternehmen verfügen über Mechanismen, um anomale Aktivitäten im Einklang mit Artikel 17, darunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle, umgehend zu erkennen und potenzielle einzelne wesentliche Schwachstellen zu ermitteln.

Alle in Unterabsatz 1 aufgeführten Erkennungsmechanismen werden gemäß Artikel 25 regelmäßig getestet.

(2) Die in Absatz 1 genannten Erkennungsmechanismen ermöglichen mehrere Kontrollebenen und legen Alarmschwellen und -kriterien fest, um Reaktionsprozesse bei IKT-bezogenen Vorfällen auszulösen und einzuleiten, einschließlich automatischer Warnmechanismen für Mitarbeiter, die für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen zuständig sind.

(3) Finanzunternehmen stellen ausreichende Ressourcen und Kapazitäten bereit, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogenen Vorfällen, darunter insbesondere Cyberangriffe, zu überwachen.

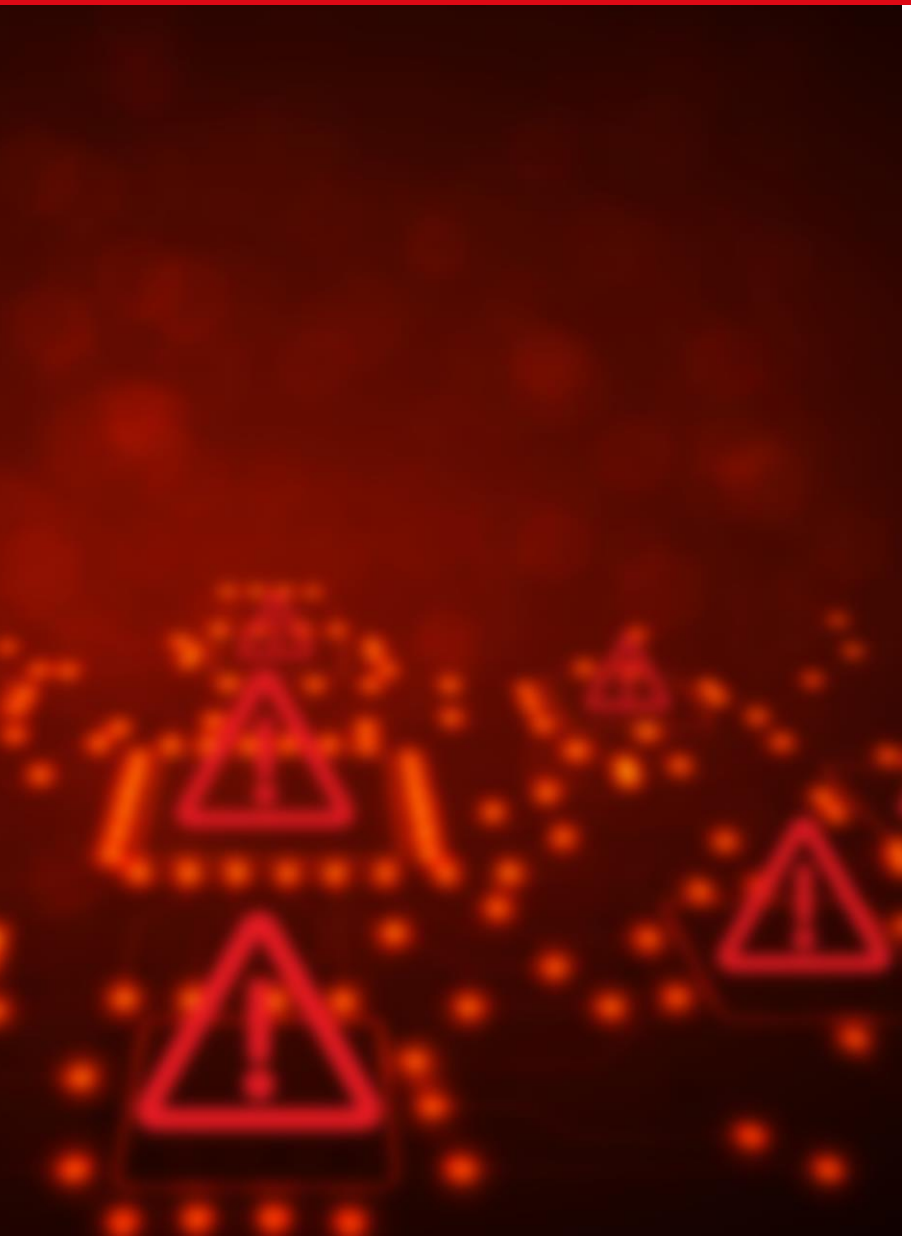
DORA-Anforderung „Anomalie-Erkennung“ (1)



Anomalie-Detektoren für den Mainframe:

- **Zeitnahe Auswertung und Korrelation** der Events bereits auf dem Mainframe (unabhängig von der Weiterleitung an ein SIEM, wie z.B. Splunk, oder an das SOC).
- **Mitschnitt und direkte Weiterleitung** von Events und Alerts **an SIEM und SOC.**
- Die Konfiguration auf Anomalien und Risiken überprüfen – im Rahmen des **kontinuierlichen Assessments.**
- Für DORA notwendige **360-Grad-Abdeckung** sämtlicher z/OS-Subsysteme und -Komponenten: Basis-MVS, aber auch USS, RACF, DB2, CICS, IMS, MQ, TCP, VTAM, etc.
- Option zum lokalen Entscheiden, auf dem Mainframe, zwecks einer besonders **zeitnahen Reaktion** („Cancel“ oder „Blockade“).

DORA-Anforderung „Anomalie-Erkennung“ (2)



Mainframe-spezifische Filter und Detektoren für breites Funktionsspektrum

- Ausschließlich **APF**, das „Mainframe-Heiligtum“, zu betrachten ist **nicht ausreichend** für höchste DORA-Sicherheit.
- Wichtig: Überwachung von **„Malicious Activities“** mit Zielen wie RACF-Umgehung, Event-Unterdrückung (z.B. SMF oder Syslog), oder Fake- bzw. Flood-Event-Erzeugung.
- Detektion kritischer Events um die sog**. „Privilege Escalation“**. Das für DORA notwendige Monitoring geht über das Thema „ACEE Manipulation“ hinaus.
  => RACF-Klasse ACEECHK nicht ausreichend für DORA
- Die Option, Operationen über das Normalmaß hinaus durch **Blockaden** abzusichern, z.B. spezifische RACF-Kommandos oder Crypto-Funktionsaufrufe verhindern, etc.
- Und einiges mehr - „whatever happens“.

DORA-Anforderung „Schwachstellen-Erkennung“

Zeitnahe Erkennung und Behandlung von Schwachstellen

- FU müssen über die sie betreffenden Schwachstellen bei ihren **Dienstleistern** informiert werden und auch **selbst** ihre Schwachstellen an Kunden und Partner **angemessen kommunizieren**.
- Anforderungen an **automatisierte Schwachstellenscans** und die Behebung von Schwachstellen sind gestiegen, ICT-Assets, die kritische oder wichtige Funktionen unterstützen, müssen **wöchentlich gescannt** werden.
- Bei der Behebung von Schwachstellen sind **Patches prioritär** gegenüber anderen Maßnahmen zu installieren.
- FU müssen die **Priorisierung** nach **Kritikalität** der **Schwachstelle** und des betroffenen **Assets** durchführen.
- **Fremdbezogene Softwarekomponenten** sind ebenfalls regelmäßig auf **Schwachstellen** zu **überprüfen** (Lieferkettenrisiko).

Draft RTS RMF:
Article 10 Vulnerability and patch management
2. (b) […] performance of automated vulnerability scanning […] for those supporting critical or important functions it shall be performed **at least on a weekly basis**.
(c) […] ensure that **ICT third-party service providers handle** any **vulnerabilities** related to the ICT services provided to the financial entity and report them to the financial entity. […]
(d) track the **usage of third-party libraries**, including open source, monitoring the version and possible updates;
(e) establish procedures for responsible **disclosure of vulnerabilities to clients** and counterparts as well as to the public, as appropriate;
(f) deploy **patches** to address identified vulnerabilities. If no patches are available for a vulnerability, financial entities shall identify and implement other mitigation measures;

BaFin | DEUTSCHE BUNDESBANK EUROSYSTEM

Was bedeutet DORA in der Praxis?
IKT-Risikomanagement

5. Dezember 2023 | 11

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation1_Ueberblick_DORA.pdf?__blob=publicationFile&v=2

DORA-Anforderung „Schwachstellen-Erkennung“

Erkennung Mainframe-spezifischer Schwachstellen (nicht nur genereller Schwachstellen)

- Es geht um mehr als „offene Ports“.
- Ganzheitliche 360-Grad-Schwachstellen-Prüfung über alle z/OS-Komponenten hinweg: MVS, USS, RACF, DB2, CICS, IMS, MQ, TCP, VTAM, etc., inkl. Fremdsoftware
- Permanentes störungsfreies Assessment aller System-Elemente, insbesondere nach detektierter Änderung.
- Life-Elemente des Systems („Hauptspeicher“).
- Intensives Assessment in 24h-Intervallen, z.B. jede Nacht.
- Password- und Phrase-Qualitätsprüfung.

DORA-Anforderung „All-Phasen-Verschlüsselung“

Verschlüsselung von Daten auch während der Verarbeitung

- Daten sind entsprechend ihrer **Kritikalität** in allen Zuständen zu **verschlüsseln** (at rest, in transit & in use).
  - Falls Verschlüsselung während der Verarbeitung nicht möglich ist, müssen die Daten in **separierten und besonders Geschützen** Umgebungen verarbeitet werden oder **anderer geeigneter Maßnahmen** getroffen werden.
- Regeln für die Verschlüsselung von internem und externem Netzwerkverkehr sind zu treffen.
- Für **kryptographische Schlüssel** ist ein Lifecycle-Management einzurichten.

Draft RTS RMF:
Article 6 Encryption and cryptographic controls
2. (a) [...] rules for the encryption of data at **rest**, in **transit** and, where relevant, in **use**, taking into account the results of the approved data classification [...] **If encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment or take other equivalent measures**[...]
b. [...] encryption of internal network connections and traffic with external parties [...]

Article 7 Cryptographic key management
1. [...] cryptographic key management policy [...] requirements for **managing** cryptographic **keys through their whole lifecycle**, including generating, storing, backing up, archiving, retrieving, transmission, retiring, revoking and destroying keys [...]

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation1_Ueberblick_DORA.pdf?__blob=publicationFile&v=2

DORA-Anforderung „All-Phasen-Verschlüsselung“

Verschlüsselung der Daten auf dem Mainframe in allen Zuständen und Verarbeitungsphasen

- Fundament der All-Phasen-Verschlüsselung:
  „Pervasive Encryption“-Technologie des z/OS durch leistungsstarke Crypto-Funktionalitäten

- **Komplettverschlüsselung** in allen Phasen möglich

- „There is no free lunch“:
  All-Phasen-Verschlüsselungsfunktionen des z/OS
  = **interessantes Angriffsziel**

DORA-Anforderung „Schutz der Daten“

DORA - Artikel 9 Abs. 2: Vertraulichkeit von Daten

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

Artikel 9

Schutz und Prävention

(1) Um einen angemessenen Schutz von IKT-Systemen zu gewährleisten und Gegenmaßnahmen zu organisieren, überwachen und kontrollieren Finanzunternehmen kontinuierlich die Sicherheit und das Funktionieren der IKT-Systeme und -Tools und minimieren durch den Einsatz angemessener IKT-Sicherheitstools, -Richtlinien und -Verfahren die Auswirkungen von IKT-Risiken auf IKT-Systeme.

(2) Finanzunternehmen konzipieren, beschaffen und implementieren IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools, die darauf abzielen, die Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen, insbesondere jener zur Unterstützung kritischer oder wichtiger Funktionen, zu gewährleisten und hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit, von Daten aufrechtzuerhalten, unabhängig davon, ob diese Daten gespeichert sind oder gerade verwendet oder übermittelt werden.

DORA-Anforderung „Schutz der Daten“

Schutz sämtlicher Daten auf dem Mainframe in allen Zuständen und Verarbeitungsphasen

- **Fundament des All-Phasen-Schutzes: RACF**
- Voraussetzung für die **Wirksamkeit von RACF:** Sämtliche an User und Gruppen (Rollen) erteilten Berechtigungen basieren auf dem „need to have“-Prinzip.
- Ferner darf kein User (Angreifer) **RACF umgehen** können.

DORA-konformer Umgang mit IT-Diagnose-Daten

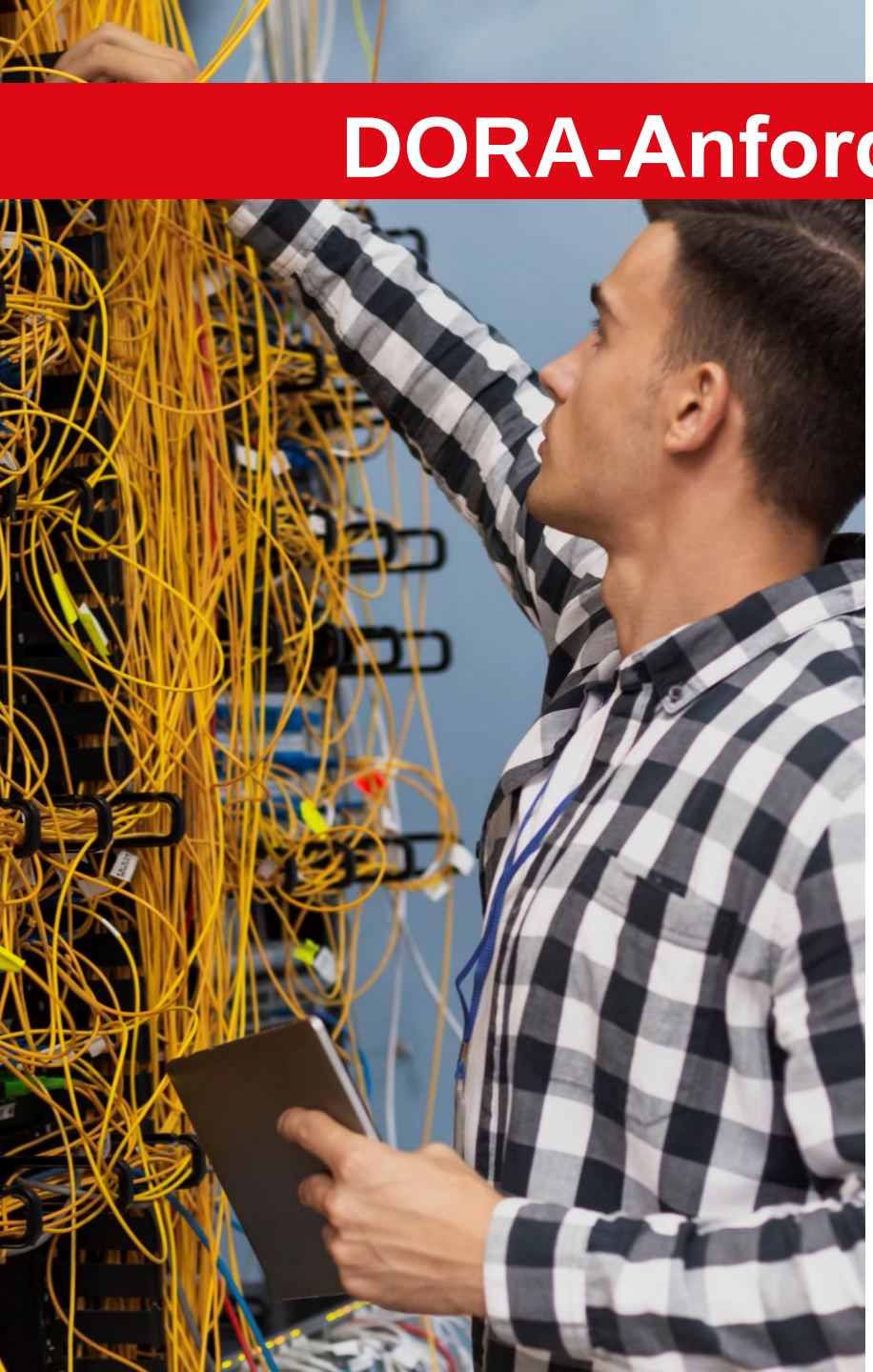
IT-Diagnose-Daten, d.h. Dumps, Logs und Traces, sind ein gravierendes Sicherheits- und Datenschutz-Risiko

- Das Risiko sind die **versteckt eingelagerten** sicherheitssensiblen und personenbezogenen Daten.

- **Diese sensible Daten** verlassen das Haus, können extrahiert und anschließend gestohlen, verkauft oder missbraucht werden (siehe Microsoft Fall, 2023).

Ein Upload von IT-Diagnose-Daten **ohne vorherige lokale Anonymisierung** verletzt DORA-Obliegenheiten in Bezug auf den Schutz der Daten.

DORA-Anforderung „Netzwerk-Sicherheit“



Netzwerksicherheit stärken

- **Detaillierung**, welche Arten von Netzwerkverkehr zu **verschlüsseln** sind, bspw. auch lokale Netzwerke.
- Für **Firewallregeln** ist ein **Lebenszyklus** einzurichten, Firewallregeln, die den Netzwerkverkehr von kritischen oder wichtigen Funktionen steuern, sind **halbjährlich** zu **rezertifizieren**, alle anderen jährlich.
- Die gesamte **Netzwerkarchitektur** ist mindestens einmal im Jahr einem **vollständigen Review** zu unterziehen.
- Möglichkeiten zur **temporären Isolation von Subnetzen**, Netzwerkkomponenten und Geräten sind zu schaffen.

Draft RTS RMF:
Article 13 Network security management
(e) [...] encryption of network connections passing over corporate networks, public networks, domestic networks, third party networks and wireless networks [...]
(g) [...] **securing the network traffic** between the internal networks and the internet and other external connections; [...]
(h) [...] definition, implementation, approval, change and review of **firewall rules and connections filters**. [...] perform the review on a regular basis [...] ICT systems supporting critical or important functions, [...] perform this review at least every six months;
(i) [...] reviews of the network architecture and of the network security design once a year [...]
(j) [...] **measures to temporarily isolate**, where necessary, subnetworks and network components and devices;

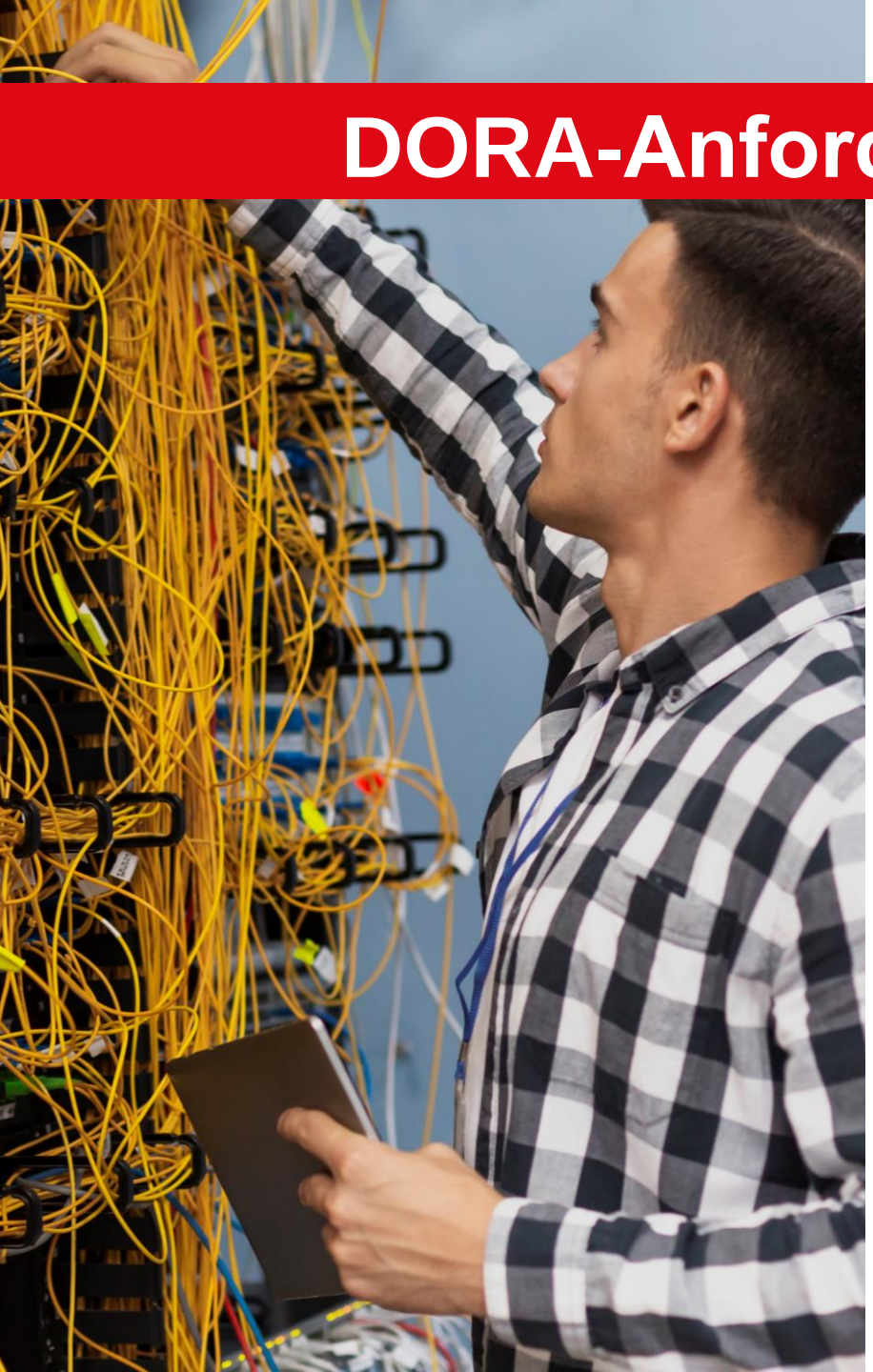
BaFin | DEUTSCHE BUNDESBANK EUROSYSTEM

Was bedeutet DORA in der Praxis?
IKT-Risikomanagement

5. Dezember 2023 | 12

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation1_Ueberblick_DORA.pdf?__blob=publicationFile&v=2

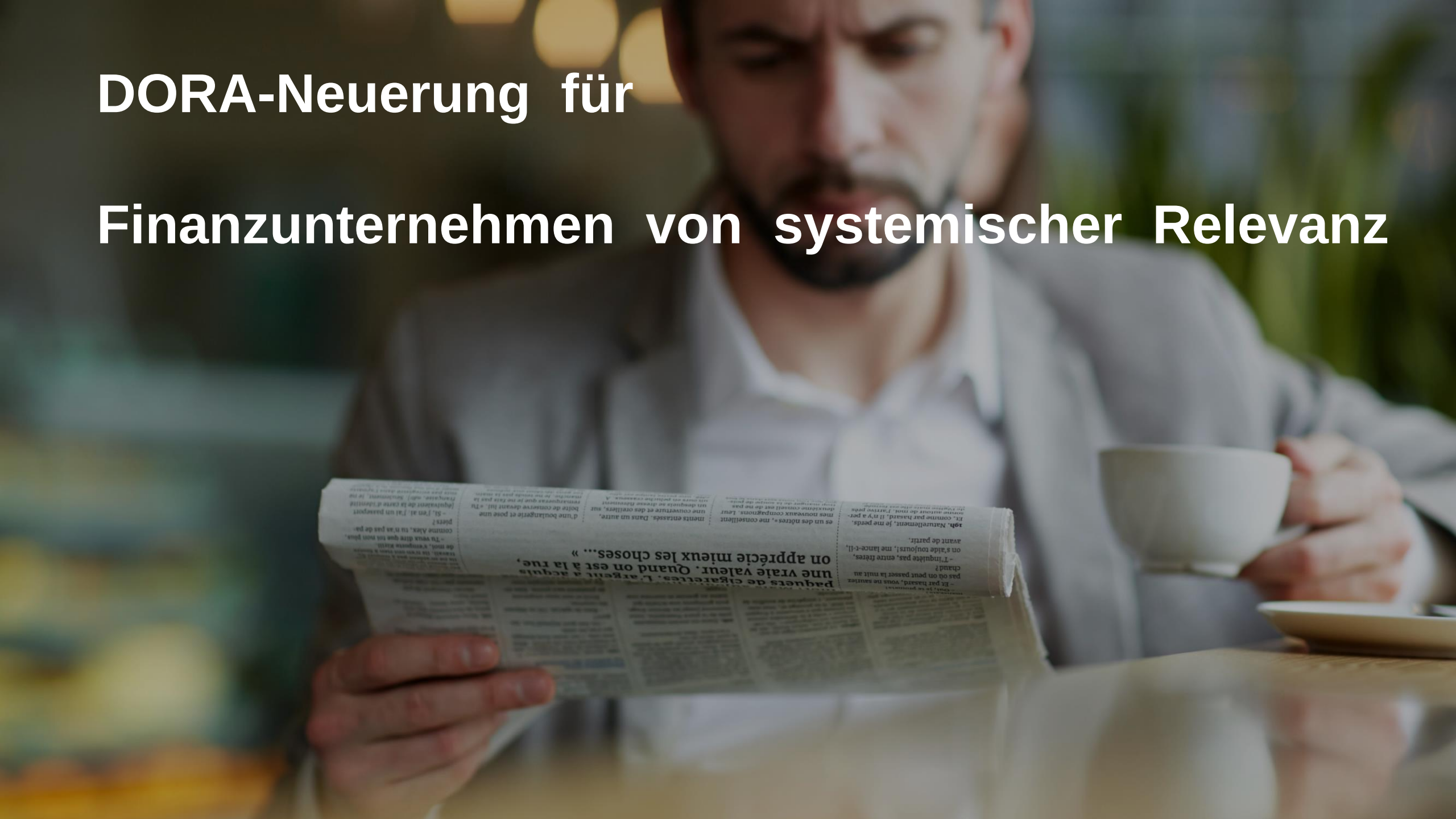
DORA-Anforderung „Netzwerk-Sicherheit“



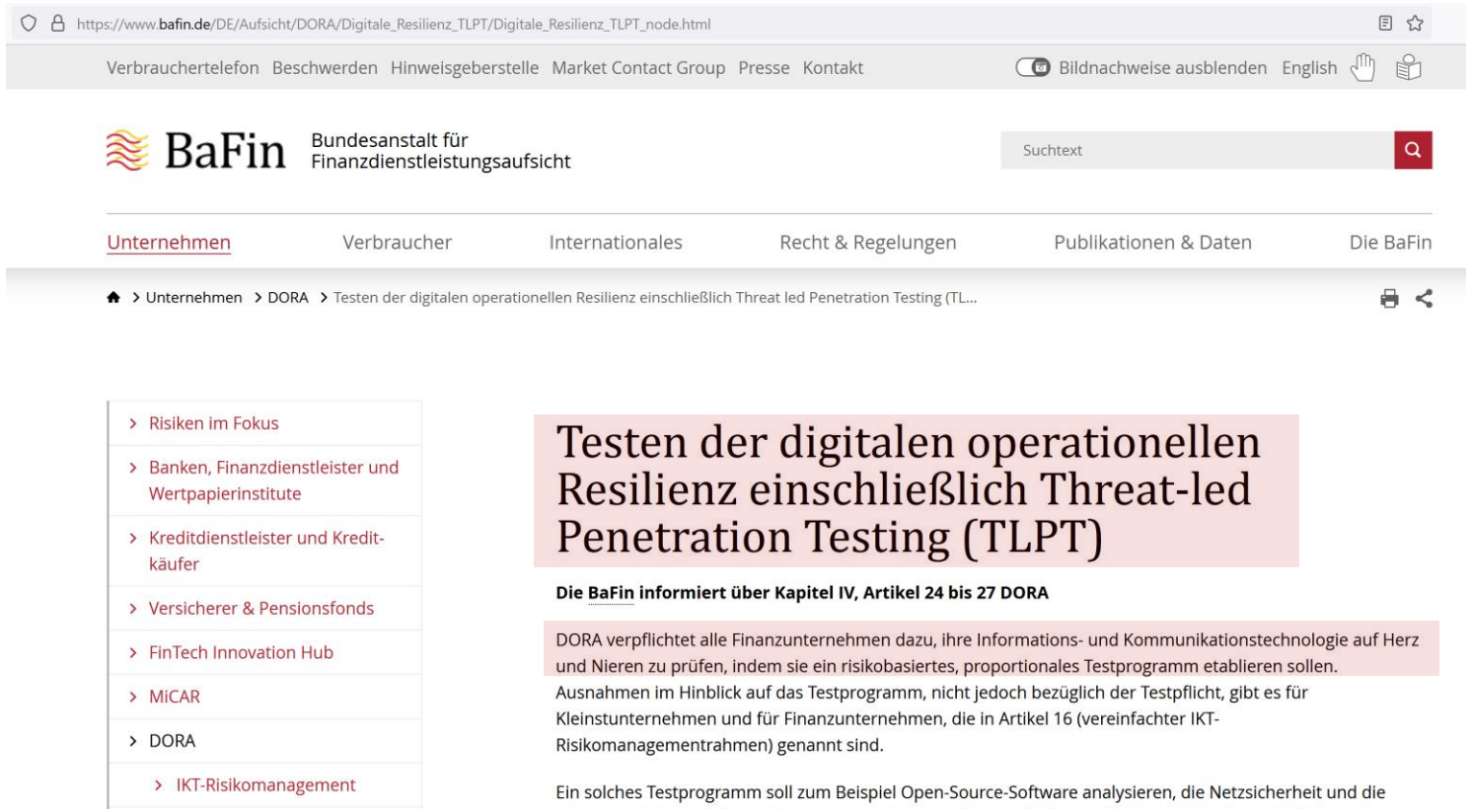
Netzwerk-Schwachstellen und -Angriffe erkennen: allgemein und Mainframe-spezifisch

- Grundschutz durch Firewall vor dem bzw. durch den z/OS Policy Agent auf dem Mainframe
- Fundament für Detektionen:
  - TCP-bezogene Audit-SMF-Records vom Typ 119
  - Crypto-Statistiken
  - DB2-Distributed-bezogene SMF Records
  - weitere
- Aufdeckung neuer bzw. unplausibler „Listener“
- Individuelle Security-Prüfung der einzelnen Stacks
- Klassische TCP-bezogene Schwachstellen: Ports, DNS, FTP statt sFTP, etc.

DORA-Neuerung für Finanzunternehmen von systemischer Relevanz



DORA fordert den regelmäßigen Nachweis - per TLPT



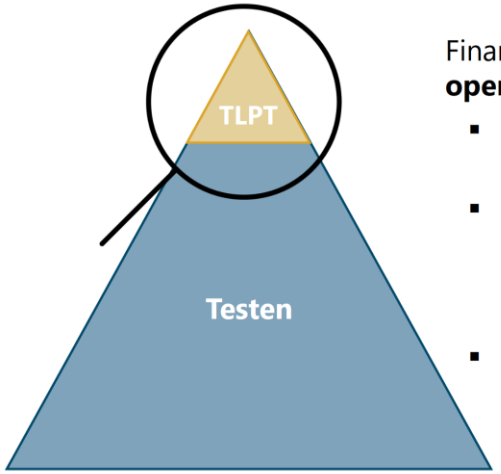
Bisher war ein Penetrationstest eher eine freiwillige, eigen-motivierte Maßnahme - nach dem Motto „Schönheit, die von innen kommt“.

DORA macht aus der Tugend eine Pflicht.

Quelle: https://www.bafin.de/DE/Aufsicht/DORA/Digitale_Resilienz_TLPT/Digitale_Resilienz_TLPT_node.html

Test-Niveaus - „1. und 2. Liga“

Was fällt unter „Testen der digitalen operationalen Resilienz“ im Kontext von DORA?



Finanzunternehmen haben ein **Programm für Tests der digitalen operationalen Resilienz** zu etablieren und zu pflegen. Das Testprogramm

- ist **integraler Bestandteil** des Risikomanagementrahmens für Informations- und Kommunikationstechnologien (IKT) (Art. 6(5) DORA)
- hat das **Ziel** IKT-Systeme, -Prozesse und Mitarbeitende auf die Effizienz der Fähigkeiten für Prävention, Erkennung, Reaktion und Wiederherstellung zu testen, um potentielle Schwachstellen aufzudecken und zu beseitigen
- umfasst eine **breite Palette** von Instrumenten und Maßnahmen:
  - von **grundlegenden Tests** von Schwachstellenbewertung und -scans, bis Penetrationstests für alle Finanzunternehmen (Art. 25 DORA)
  - bis zu **erweiterten Tests** wie TLPT - nur für Finanzunternehmen, die aus IKT-Perspektive ausgereift genug und von gewisser systemischer Relevanz sind (Art. 26 DORA)

DORA Kapitel IV (Artikel 24 bis 27) widmet sich exklusiv dem Testen

BaFin DEUTSCHE BUNDESBANK EUROSYSTEM

TLPT – IT-Aufsicht im Finanzsektor

5. Dezember 2023 | 3

Installationen mit Mainframes sind meistens so groß, dass sie in der „1. Liga spielen“, d.h. „erweiterten Tests“ gerecht werden müssen, wie einem TLPT.

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation4_TLTP_unter_DORA.pdf?__blob=publicationFile&v=2


In den „TLPT Finals“ spielen
„Red Socks“ gegen „Blue Socks“
nach den TIBER-Regeln

TLPT - Red Team & Blue Team

Die Testmethodik sieht in der Testphase die Einbindung diverser Stakeholder vor

TLPT Cyber Team – Gutachter (TIBER-DE)
- Bestätigt die regelkonforme Testdurchführung
- Fachliche und prozessuale Betreuung
- Ansprechpartner für das Control Team
- Hält Kontakt zu externen Stellen

Threat Intelligence-Anbieter - Spion
- Sammelt unternehmens-spezifische Bedrohungs-informationen
- Erstellt Angriffsszenarien

Tester- Angreifer
- Führt Angriffsszenarien auf das Unternehmen durch
- nutzt durch den TI-Anbieter gesammelte Informationen

Getestetes Unternehmen

Control Team - Manager
- Zentraler Ansprechpartner und Entscheidungsträger
- Monitoring und Risikomanagement

Blue Team - Verteidiger
- Cyberabwehr (SOC/CERT)
- Alle Mitarbeiter außerhalb des Control Teams
- Nicht über die Durchführung des Tests informiert

BaFin | DEUTSCHE BUNDESBANK EUROSYSTEM

TLPT – IT-Aufsicht im Finanzsektor

5. Dezember 2023 | 8

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation4_TLTP_unter_DORA.pdf?__blob=publicationFile&v=2

TLPT - „Red Team gegen Blue Team“

ChatGPT

Ein "Red Team" ist eine Gruppe von Sicherheitsexperten, die in einem Penetrationstest die Rolle von Angreifern übernehmen. Ihr Ziel ist es, Sicherheitslücken in einem System oder Netzwerk zu identifizieren, indem sie versuchen, es zu durchdringen.

Das "Blue Team" repräsentiert die Verteidigungsseite und arbeitet daran, Angriffe zu erkennen und abzuwehren. Die Zusammenarbeit zwischen Red Team und Blue Team ermöglicht eine umfassende Sicherheitsbewertung und stärkt die Verteidigungsmechanismen von Organisationen.

TLPT - „Spiel in der Profi-Liga“

Wofür steht die Abkürzung TLPT in DORA?

T hreat-
L ed
P enetration
T esting

„bedrohungsorientierte Penetrationstests (TLPT – Threat-Led Penetration Testing)“ beschreibt einen Rahmen, der **Taktik, Techniken und Verfahren realer Angreifer**, die als echte Cyberbedrohung empfunden werden, **nachbildet** und einen **kontrollierten**, maßgeschneiderten, erkenntnisgestützten **(Red-Team-) Test** der kritischen **Live-Produktionssysteme** des Finanzunternehmens ermöglicht“*

*Quelle: DORA, Art. 3 (17) Definitionen

BaFin DEUTSCHE BUNDESBANK EUROSYSTEM

Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation4_TLTP_unter_DORA.pdf?__blob=publicationFile&v=2

TLPT - „Profi-Liga, -Regeln und -Schiedsrichter“

3.2 Drafting principles: DORA and the TIBER-EU framework

3.2.1 The TIBER-EU framework

8. TIBER-EU is a European framework for threat intelligence-based ethical red-teaming. It provides comprehensive guidance on how authorities, entities, threat intelligence and red-team providers should work together to test, maximise learning and improve the cyber resilience of entities by carrying out controlled cyberattacks. Inspired by and taking account of the lessons learned from similar initiatives in the United Kingdom (CBEST) and the Netherlands (TIBER-NL), it was developed jointly by the ECB and the EU’s national central banks and published in May 2018.

Aus Sicht des Red Teams gibt es im **Kern des Spiels nur wenige Regeln:** die Hauptsache „der Ball geht ins Tor, und das Tor selbst steht danach noch“.

https://www.esma.europa.eu/sites/default/files/2023-12/JC_2023_72_-_CP_on_draft_RTS_on_TLPT.pdf

TLPT - „Profi-Liga, -Regeln und -Schiedsrichter“

TIBER-EU: „Intelligence-led red teams …“

https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf

EUROPEAN CENTRAL BANK
EUROSYSTEM

TIBER-EU White Team Guidance

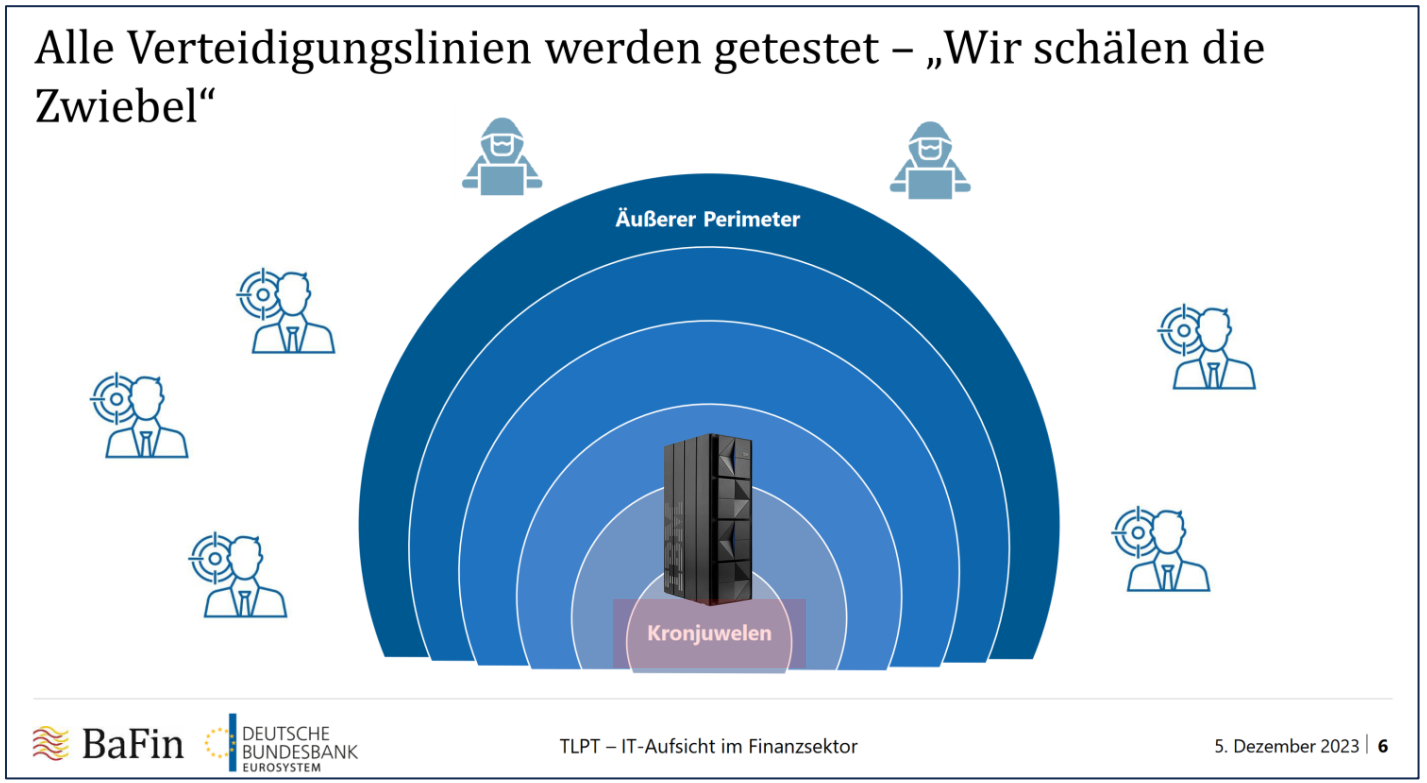
The roles and responsibilities of the White Team in a Threat Intelligence-based Ethical Red Teaming test

1.1 What is TIBER-EU?

TIBER-EU is a framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. Intelligence-led red team tests mimic the tactics, techniques and procedures of real-life threat actors who, on the

TLPT-Konsequenz: Training und Fitness sind gefragt

Man kann es sehen wie man möchte: DORA‘s TLPT fokussiert die Kronjuwelen und fordert beim Blue Team stetiges Training und hohe Fitness.



Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Praesentation1_Ueberblick_DORA.pdf?__blob=publicationFile&v=2

„Threat-Szenarien“ – Ransom, „> 1d Ausfall“, …

Digitale operationale Resilienz klingt recht abstrakt, konkret geht es um „Threat Level“-, d.h. durchaus Worst-Case-Szenarien:

1. Erkennung unzulässiger „Karrieren“: „Privileged Escalation“ via dynamischer Manipulation, z.B. zur sog. „Privileged STC“, „Special User“, …
2. Aktivierung und missbräuchliche Anwendung von Encryption:
   - ➢ Missbräuchliches bzw. zerstörerisches Verändern und Anwenden von Crypto-Schlüsseln
   - ➢ Aufbau eigener trusted Signing-Keys und Root-Zertifikaten.

„Threat-Szenarien“ – Ransom, „> 1d Ausfall“, …

- Man sollte sich vor Augen halten: ein Ransom-Angriff hängt nicht von der z/OS-Crypto-Facility ab. Der Angreifer kann eigene Crypto-Routinen mitbringen und anwenden, zum Lesen, Verschlüsseln und Zurückschreiben.

- Weitere „Threat-Zielrichtungen“: die Zerstörung von Daten oder des Mainframe-Betriebssystems.

FAZIT:

- Nahezu **unendlich viele Szenarien** sind denkbar.

- Für eine effiziente kontinuierliche DORA-Readiness bedarf es eines Plans auf Basis einer Serie von sich steigernden **„Muster-Threat-Szenarien“**.

SF-Sherlock

SF-SafeDump

Penetrationtest auf Simulationsbasis

bewährte Lösungen und Dienstleistungen für höchste Mainframe-Security und -Compliance

„Anomalie-Erkennung“ mit SF-Sherlock

SF-Sherlock bietet genau das notwendige breit ausgelegte **360-Grad-Spektrum an vordefinierten Anomalie-Detektionen** und deckt die relevanten **Privilege-Escalation- und Manipulations-Szenarien** für den Mainframe ab.

SF-Sherlock ist spezialisiert auf die gravierenden Risiken der **professionellen Tricks eines Mainframe-Angriffs**, um diese innovativ zu entschärfen, und wurde diesbezüglich stetig fortentwickelt. Wir wissen definitiv, was es für DORA auf dem Mainframe zu implementieren gilt.

„Schutz und Prävention“ mit SF-Sherlock

SF-Sherlock – DORA Readiness durch:

+ Kontinuierliches, tiefgreifendes Assessment
+ Intelligentes Monitoring
+ Punktgenaues Reaktionsvermögen
+ Abdeckung der für den Mainframe relevanten Privilege-Escalation-Szenarien:
  Annäherung ➔ Privilegien-Aneignung ➔ Tat ➔ Flucht
+ Jahrelange Erfahrung mit gefährlichen Angriffsmustern
+ Permanente Fortentwicklung und Innovation
+ DORA-Härtung und DORA-Readiness

„Schwachstellen-Erkennung“ mit SF-Sherlock

SF-Sherlock – Schwachstellen-Erkennung durch:

+ kontinuierliche Prüfung der Systeme
+ DORA notwendige **360-Grad-Schwachstellen-Erkennung**
+ Schließt ein: neben RACF **sämtliche Subsysteme und Bereiche des Mainframes**
+ Alleinstellungsmerkmale: z.B. Passwort- und Phrase-Cracking im Ramen der **simulierten störungsfreien Penetration** trotz verschlüsselter RACF-Datenbank.
+ Das Thema **„Malicious Code“** in Modulen wird vom VIDELA-Scanner übernommen.
+ etc.

„All-Phasen-Verschlüsselung“ und SF-Sherlock

SF-Sherlock – DORA-gerechte Verschlüsselung:

+ Überwachung der eingeschalteten Verschlüsselungen
+ Detektion **inkorrekter** oder nicht mehr möglicher **Entschlüsselungen**
+ Erkennung **unplausibler oder „tödlicher“ Verschlüsselung**, z.B. von System-Bibliotheken und System-Dateien
+ Monitoring zentraler **kritischer Crypto-Ereignisse**, wie u.a. „Set Master-Key“ als „Königs-Event“

„Schutz der Daten“ und SF-Sherlock

SF-Sherlock bietet umfassende Unterstützung beim Schutz der Daten

+ Überwachung der administrativen Vorgänge im RACF, und Detektion von Auffälligkeiten bzw. negativen Konsequenzen
+ Härtung des RACF durch Assessment und potentielles Bypassing
+ Überwachung auf Techniken der Datenflucht

„Netzwerk-Sicherheit“ mit SF-Sherlock steigern

SF-Sherlock – DORA-Unterstützung für ein sicheres Mainframe-Netzwerk:

+ Assessment der **TCP-Konfiguration** Mainframe
+ Zahlreiche Standard-Filter zwecks Erkennen von **Anomalien und unzulässigen Verbindungen**
+ Detektion neuer bzw. **unplausibler „Listener“**
+ Durch eine Gruppe von **Standard-Event-Filter** können für sog. „Privileged User“ (z.B. System-Programmierung) unzulässige „Login-Wege bzw. -Formen“ detektiert werden - das sog. „CyberArk Bypass Monitoring“.
+ etc.

TLPT-Readiness mit SF-Sherlock

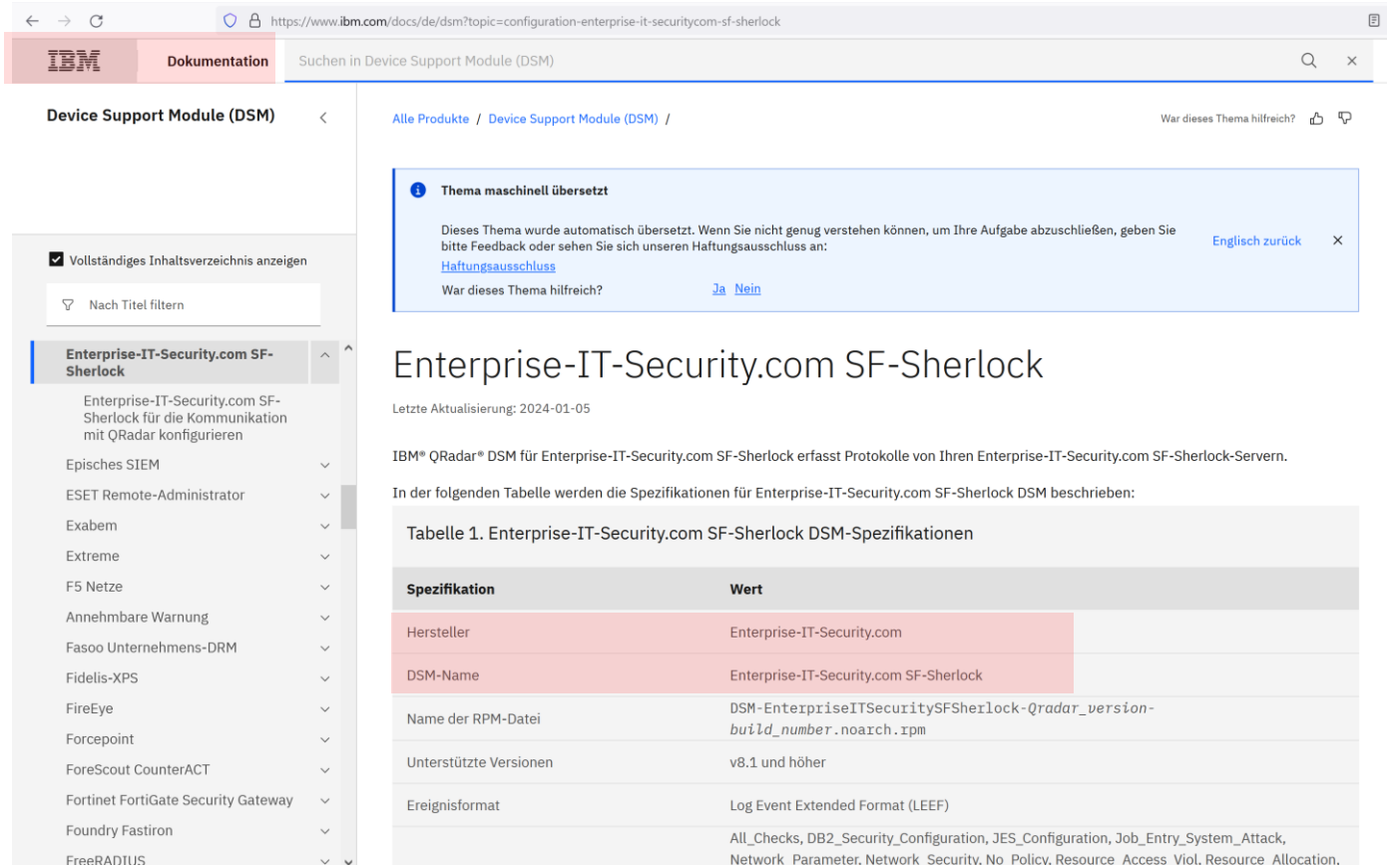
- Der notwendige **DORA-Aktivierungsplan für den Mainframe** ist mit Sherlock erprobt vorbereitet, erfolgt in strukturierten Stufen des „fiktiven Threats“, und ist stressfrei machbar.

- Egal wie die DORA-Teams und Detailregeln des TLPTs heißen: Sherlock unterstützt das **Mannschaftsspiel** (Sysprog, RACF, etc.), denn jeder muss auf seiner Spielfeld-Position den notwendigen Beitrag leisten.

- Zielsetzung ist die **generelle All-Phasen-Abdeckung:** von der frühzeitigen Erkennung des „Anpirschens“, und versuchten Angriffsversuchen, über das konkrete Vergehen, bis hin „zur Flucht“. Alle Wege werden jetzt versperrt oder mit Kameras und Sensoren versehen.

Anerkannte SF-Technologien

Die SF-Lösungen genießen eine hohe Reputation und erlauben die schnelle Integration, z.B. in Splunk, Qradar und ArcSight



DORA-konforme IT-Diagnose-Daten mit SF-SafeDump

SF-SafeDump erlaubt für alle Plattformen die **lokale, revisionsgerechte, automatisierte Anonymisierung von IT-Diagnose-Daten** vor dem Upload, zwecks Bereinigung von sicherheitssensiblen Daten und solchen mit Personenbezug.

SF-SafeDump for z/OS läuft zu >=95% auf zIIP.

Master-Key-Diebstahl aus Crash-Dump bei Microsoft:

https://www.enterprise-it-security.com/it-governance-isaca-artikel-dez-2023

Info-Video für mehr Awareness im IT-Betrieb:

https://www.enterprise-it-security.com/isaca-awareness-video-it-diagnose-daten


Ihr Blue Team soll das Spiel entscheiden!

ENTERPRISE-
IT-SECURITY.COM

Vielen Dank für Ihr Interesse!

Bei weiteren Fragen, zögern Sie nicht, mich persönlich zu kontaktieren:

Telefon: **+41 (0) 41 710 4005**
E-Mail: **stfedtke@enterprise-it-security.com**

Gerne unterstützen wir Ihr Unternehmen auf dem Weg zur DORA-Readiness des Mainframes:

https://www.enterprise-it-security.com/dora-readiness-of-the-mainframe