

Ausgabe 01/2025

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Seite 22

DATENVERARBEITUNG IM BESCHÄFTIGUNGS- KONTEXT

Dr. Inka Knappertsbusch

Seite 6

UMSETZUNG DER EPA 3.0

Prof. Ulrich Kelber

Seite 16

„WENN DIE EXECUTIVE ORDER AUFGEHOBEN WÜRDEN, WÄRE DAS EIN PROBLEM“

Interview mit Dr. Axel Spies



Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.



mastodon.social/@bvd@privacyofficers.social



linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BvD^{e.V.}
DATENSCHUTZ GESTALTEN

SCHWACHSTELLEN- UND PENETRATIONSTEST

Ihre Rolle in regulatorischen und normativen Vorgaben

Cybersicherheit wird immer wichtiger - und damit auch Maßnahmen zur frühzeitigen Identifizierung von Schwachstellen in den von Unternehmen betriebenen Netzwerken und Cloud-basierten Systemen zur Datenverarbeitung wie Schwachstellen- und Penetrationstests (Pentests). Teilweise werden solche Maßnahmen durch gesetzliche oder normative Vorgaben verlangt. Nachfolgend erläutern wir diese Vorgaben.

Zertifikat / Gesetz / Regelung	Notwendig weil?	Rhythmus	Pflichten	Gesetz
DS-GVO	Nur indirekt	regelmäßig	"geeignete technische ... Maßnahmen (TOMs)" und "Schutz personenbezogener Daten"	Art. 5, Art. 24, Art. 25
NIS-2	indirekte gesetzliche Vorgabe (nach aktueller Einschätzung)	regelmäßig	"...geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zur Risikominderung umsetzen" müssen. Gefordert werden „Cyberhygienemaßnahmen und -verfahren zur Prüfung und Bewertung der Wirksamkeit von Maßnahmen zur Bewältigung von Cybersicherheitsrisiken - Meldung bei kritischen Ereignissen"	Art. 21 Abs. 2, (Art. 21 Abs. 2 (f))
DORA	gesetzliche Anforderung	mindestens monatlich, öffentlich erreichbare Daten: wöchentlich	"über Mechanismen verfügen, um anomale Aktivitäten umgehend zu erkennen und potenzielle einzelne wesentliche Schwachstellen zu ermitteln."	Ref.: Art. 10.2 RTS 15_16 (Delegierte Verordnung (EU) 2024/1774 Art. 10, 17, 23, 25, 26
ISO 27001	Requirement der Norm	regelmäßig	Regelmäßige Überprüfung von Risiken	A, A.12.6.1 „Technische Compliance-Prüfung“ , Control 5.31 Einhaltung Sicherheitsanforderungen, Control 8.8 regelmäßige Identifikation und Bewertung von Schwachstellen, Control 8.16. regelmäßige Überprüfung der Sicherheit von IT-Systemen
TISAX	Requirement der Norm	risikobasiertes Intervall	Notwendige Prüfungen identifizieren und durchführen	TISAX Controls (5.2.6) und (5.3.1)

Abb. 1: Übersicht Pentesting: gesetzliche und normative Vorgaben

Regulatorische Vorgaben

DS-GVO

Die Datenschutz-Grundverordnung (DS-GVO) fordert keine direkte Verpflichtung zur Durchführung von Schwachstellen- und Pentests. Eine indirekte Verpflichtung lässt sich aber durchaus an verschiedenen Stellen ableiten. So fordert Art. 5 Verantwortliche beziehungsweise Unternehmen dazu auf, personenbezogene Daten vor unbefugtem Zugriff, Verlust oder Zerstörung zu schützen. Art. 24 fordert vom Verantwortlichen oder dem Unternehmen geeignete technische und organisatorische Maßnahmen (TOMs), um die Anforderungen der DS-GVO einzuhalten. Art. 25 fordert den Schutz personenbezogener Daten durch Technikgestaltung. Genau genommen müssen IT-Systeme so konzipiert sein, dass personenbezogene Daten standardmäßig geschützt sind.

NIS-2 Richtlinie

Nach dem derzeit vorliegenden Entwurf der Bundesregierung (Anmerkung: in Deutschland stand zum Zeitpunkt der Artikelveröffentlichung noch die Zustimmung des Bundestags aus) müssen sich Unternehmen, die unter die Vorgabe der NIS-2 Richtlinie fallen, mit diesem Thema verstärkt auseinandersetzen. Auch wenn die NIS-2 Richtlinie keine direkte Vorgabe zu Schwachstellen- und Pentests beinhaltet, finden sich die Vorgaben indirekt in Art. 21 der NIS-2 Richtlinie. Dort heißt es in Abs. 2, dass Unternehmen „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zur Risikominderung umsetzen“ müssen.

Gefordert werden „Cyberhygienemaßnahmen und -verfahren zur Prüfung und Bewertung der Wirksamkeit von Maßnahmen zur Bewältigung von Cybersicherheitsrisiken“ (Art. 21 Abs. 2 (f)). Dies kann nur mit regelmäßigen Schwachstellen- und Sicherheitstests gewährleistet werden.

Zu berücksichtigen ist in diesem Kontext Art. 34 (Sanktionen). Darin ist geregelt, dass sowohl gegen wesentliche als auch gegen wichtige Einrichtungen oder Unternehmen Bußgelder verhängt werden können, sofern diese gegen Art. 21 verstoßen.

DORA

Der Digital Operational Resilience Act (DORA) beinhaltet nach unserer Auffassung spezifische Anforderungen an Schwachstellen- und Pentests für Finanzunternehmen und deren IT-Dienstleister. Die Anforderungen lassen sich aus den Artikeln 10, 17, 23, 25 und 26 ableiten. Danach sollen die betroffenen Unternehmen unter anderem über Mechanismen verfügen, um anomale Aktivitäten umgehend zu erkennen und potenzielle einzelne wesentliche Schwachstellen zu ermitteln.

ISO 27001/27002

Die ISO 27001 fordert zur Risikobehandlung in Kapitel 6.1.3, dass Organisationen beziehungsweise Unternehmen Risiken bewerten und geeignete Maßnahmen implementieren müssen. Sowohl Schwachstellen- als auch Pentests können hier als geeignete Maßnahmen angesehen werden.

Kapitel 8.1 fordert beim Betrieb des ISMS, dass die implementierten Sicherheitsmaßnahmen regelmäßig überprüft werden sollten. Dazu gehören unter anderem regelmäßige Tests zur Identifikation von technischen Schwachstellen.

Die ISO 27002 beinhaltet in Kapitel 5.31 die Empfehlung, dass Unternehmen regelmäßig die Einhaltung von Sicherheitsanforderungen überprüfen sollten. Kapitel 8.8 beinhaltet die Anforderung zur regelmäßigen Identifikation und Bewertung von Schwachstellen.

Kapitel 8.16 fordert die regelmäßige Überprüfung der Sicherheit von IT-Systemen. Auch hier sind Schwachstellenscans und Penetrationstests ein geeignetes Mittel.

TISAX

Der vom Verband der Automobilindustrie (VDA) entwickelte Sicherheitsstandard TISAX (Trusted Information Security Assessment Exchange) orientiert sich sehr stark an den Vorgaben der ISO 27001/27002.

Ergänzt werden die von der ISO 27001/27002 abgeleiteten Anforderungen um für die Automobilwirtschaft spezifische Anforderungen, darunter der Umgang mit Prototypen.

Kapitel 5.2.6 beschreibt die Durchführung von Pentests sowie die Durchführung von Schwachstellenscans bei der Anforderung eines sehr hohen Schutzbedarfs als geeignetes Mittel zur Sicherstellung dieser Anforderungen und der damit einhergehenden Nachweisfähigkeit.

Bei neuen oder weiterentwickelten IT-Systemen wird in Kapitel 5.3.1 die Durchführung von Penetrationstests als angemessene Maßnahme genannt, sofern das Unternehmen die Anforderung eines sehr hohen Schutzbedarfs erfüllen muss.

Möglichkeiten der technischen Umsetzung

Die genannten Schwachstellen- und Pentests sind also essenzielle Maßnahmen, um die Einhaltung der oben genannten Anforderungen aus verschiedenen gesetzlichen und normativen Vorgaben zu erfüllen. Sie simulieren dabei Angriffe und helfen, Sicherheitslücken zu erkennen, bevor Angreifer sie ausnutzen können.

Damit solche Tests qualitativ hinreichend gut sind, sollten folgende Kriterien erfüllt sein:

1. Abdeckung der Sicherheitsscans (Tests)

Die Sicherheitsscans sollten alle relevanten Bereiche der IT-Infrastruktur abdecken:

- **Außen:** Externe Systeme wie Webanwendungen, VPNs und öffentliche Server, die für Angreifer zugänglich sind.
- **Innen:** Interne Netzwerke und Systeme, die von einem Insider oder nach einem erfolgreichen Eindringen gefährdet sein können.
- **Darknet:** Überprüfung von Daten, die im Darknet verkauft oder verbreitet werden, um mögliche Leaks zu erkennen.

2. Breite Abdeckung der Sicherheitslücken

- **Schwachstellenanalyse:** Automatisierte Tools scannen Systeme auf bekannte Sicherheitslücken, veraltete Software oder Fehlkonfigurationen.
- **Penetrationstests:** Hier wird aktiv versucht, Schwachstellen auszunutzen, um die tatsächliche Ausnutzbarkeit zu überprüfen und realistische Angriffsszenario zu simulieren.

3. Hohe Qualität durch gleiche Durchführung

Die Verwendung von standardisierten und wiederholbaren Testframeworks wie MITRE ATT&CK® gewährleisten eine konsistente und vergleichbare Qualität der Tests. Diese Vorgehensweise unterstützt die kontinuierliche Verbesserung der Sicherheitslage und ermöglicht eine präzise Messung von Fortschritten.

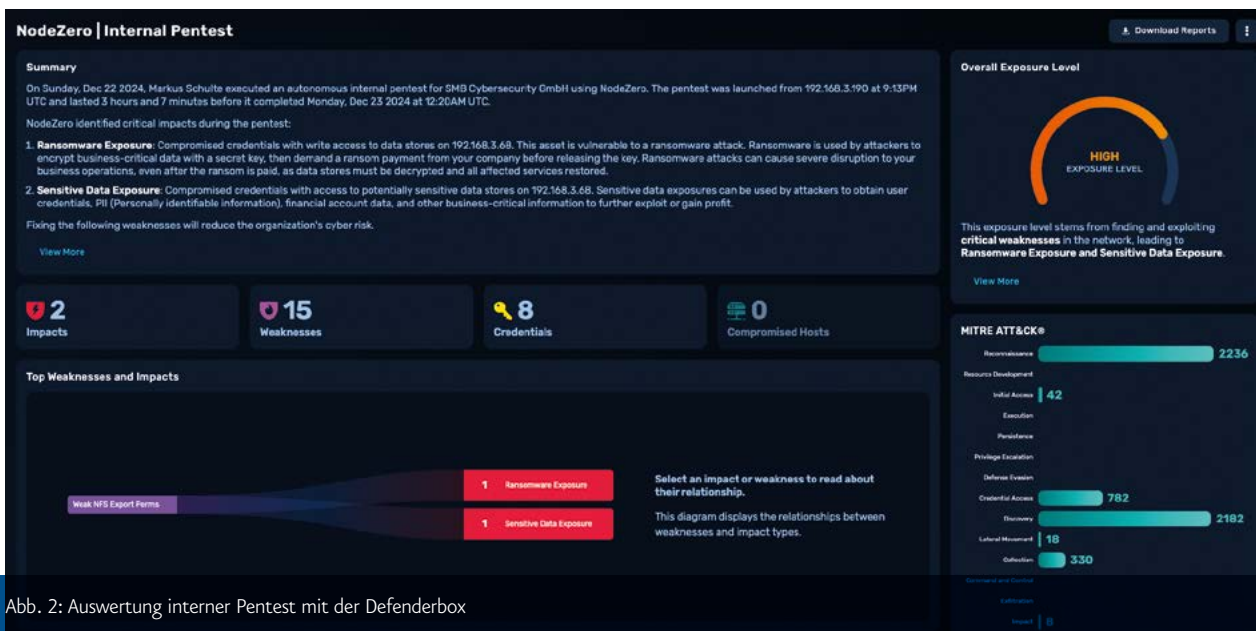


Abb. 2: Auswertung interner Pentest mit der Defenderbox

4. Automatisierung zur Senkung der Kosten

Automatisierte Schwachstellen- und Pentests bieten eine kostengünstige Möglichkeit, Sicherheitslücken regelmäßig zu identifizieren. Tools wie Nessus oder NodeZero® ermöglichen schnelle und skalierbare Sicherheitsscans. Sie sollten jedoch durch manuelle Pentests ergänzt werden, um komplexe Angriffsvektoren abzudecken.

5. Begleitung durch Cybersecurity-Experten

Idealerweise werden Schwachstellen- und Pentests von erfahrenen Cybersecurity-Experten begleitet, um die Ergebnisse korrekt zu interpretieren und Maßnahmen zur Risikominimierung zu entwickeln.

Dies kann durch interne Fachleute erfolgen. Externe Fachleute bieten mitunter zusätzlich neue Perspektiven auf bestehende Systeme.

6. Dokumentation der regelmäßigen Durchführung

Die Dokumentation sollte den Umfang der geprüften Systeme, die Qualität der identifizierten Schwachstellen und die Maßnahmen zu deren Behebung beschreiben.

Eine gründliche Aufzeichnung ist wichtig für die Nachverfolgbarkeit der Maßnahmen, um zu dokumentieren, dass gesetzliche Anforderungen erfüllt wurden und die IT-Sicherheit kontinuierlich verbessert wurde.

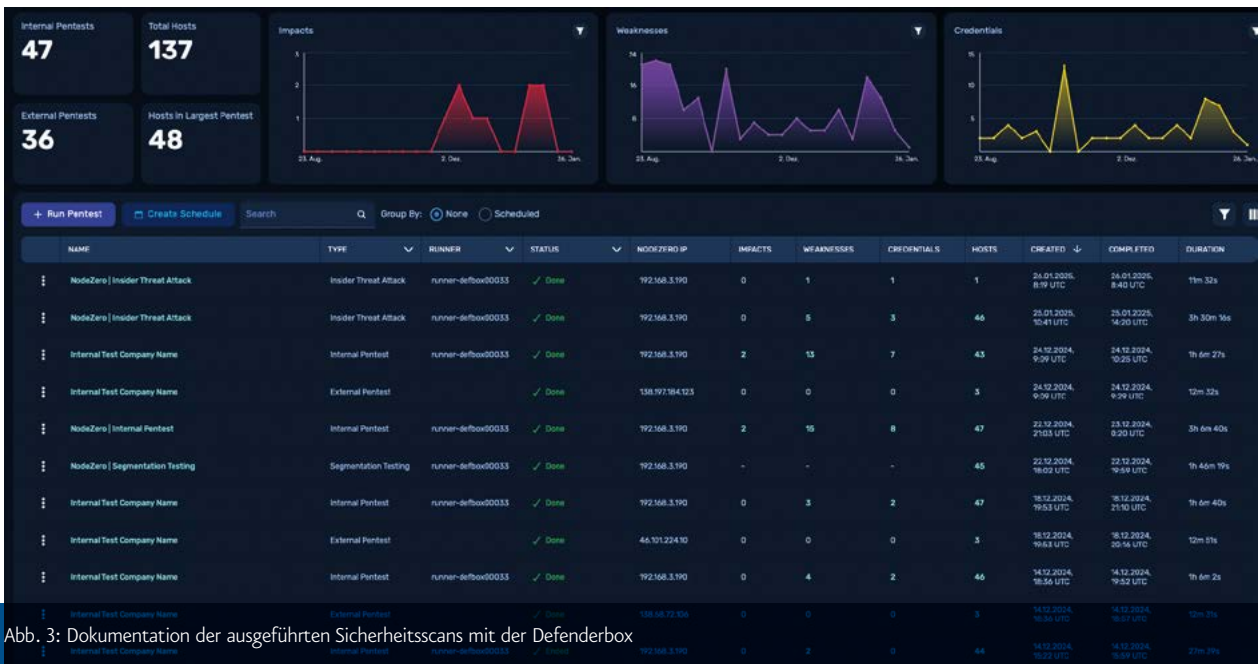


Abb. 3: Dokumentation der ausgeführten Sicherheitsscans mit der Defenderbox

Fazit

Die regelmäßige und systematische Durchführung von Penetrations- und Schwachstellentests ist unverzichtbar, wenn die Risiken eines Cyberangriffs nachhaltig minimiert werden sollen und Unternehmen ihre Cyber-Resilienz stärken wollen. Dabei müssen die Unternehmen nicht nur entsprechende Sicherheitsscans und Überprüfungen durchführen, sondern auch das Ergebnis nachvollziehbar dokumentieren und in ihre zukünftige Sicherheitsstrategie integrieren. Dabei ist zu beachten, dass es sich hier nicht nur um ein einmaliges beziehungsweise zeitpunktbezogenes Sicherheitsmonitoring, sondern um ein regelmäßiges Sicherheitsmonitoring handeln sollte.



Abb. 4: Der Defenderbox X Mini Computer im Plug & Play-Einsatz für interne und externe Sicherheitsscans inkl. Darknet-Recherche.

Über die Autoren

Markus Schulte

ist Gründer und Geschäftsführer der Defenderbox. Seine Karriere begann er in der IT-Branche, bevor er sich der IT-Sicherheit widmete. Nach einigen Jahren in der Beratung entstand bei ihm der Wunsch, eine einfach zu installierende und budgetfreundliche Cybersicherheitslösung für kleine und mittelständische Unternehmen zu schaffen. Mit zwei Mitbegründern entwickelte er die Defenderbox.



Ralf Zlmal

ist Geschäftsführer der IITR Cert GmbH, Datenschutzbeauftragter, Informationssicherheitsbeauftragter und Auditor. Er ist technischer Betriebswirt und verfügt über mehrjährige Erfahrung in den Bereichen Management, Datenschutz und Informationssicherheit. Ralf Zlmal unterstützt Firmen bei der Einführung, Aufrechterhaltung und Auditierung des betrieblichen Datenschutzes, der Informationssicherheit (ISO 27001, NIS-2, DORA etc.) sowie bei der Zertifizierung der VDA-Vorgaben im Rahmen von TISAX.



► <https://defenderbox.de/>

