VANTARION

Pentest & technische Prüfungen

Was wirklich hilft und wie Sie Ergebnisse auditfähig machen

Ein Praxisleitfaden für
IT-Leitung, ISB & Geschäftsführung

MANAGEMENT SUMMARY

Technische Sicherheitsprüfungen gehören heute in vielen Branchen zum Standard. Kunden fordern Penetrationtests (Pentests) als Vertragsbestandteil, Versicherer stellen Fragen zur technischen Absicherung und Auditoren erwarten Nachweise über Wirksamkeit.

Trotzdem werden Pentests häufig falsch verstanden.

Pentests werden beauftragt, ein Bericht wird erstellt und danach beginnt hektische Aktivität. Maßnahmen werden umgesetzt, aber selten strukturiert priorisiert. Verantwortlichkeiten sind unklar. Nachverfolgung erfolgt punktuell. Im nächsten Audit stellt sich die Frage: „Was wurde daraus?"

Ein Pentest ist kein Zertifikat. Er ist kein Ersatz für Governance. Und er ist kein einmaliger Nachweis. Er ist ein Instrument innerhalb eines funktionierenden Informationssicherheitsmanagementsystems.

Dieses Whitepaper zeigt:

- ☑ **wie sich Pentest, Vulnerability Scan und Audit unterscheiden,**
- ☑ **wann welche Prüfart sinnvoll ist,**
- ☑ **wie der Scope realistisch definiert wird,**
- ☑ **wie Findings systematisch in das Risikomanagement integriert werden,**
- ☑ **und wie technische Prüfungen in ein auditfähiges Steuerungssystem überführt werden.**

Ziel ist nicht nur eine technische Momentaufnahme. Ziel ist nachhaltige Risikoreduktion, nachvollziehbar, dokumentiert und steuerbar.

Tobias Frank,
Gründer und CEO

Als **Head of IT und Verantwortlicher für Informationssicherheit** in Handelsunternehmen und Fertigungsindustrie und habe ich in allen Facetten erlebt, wie aufwändig Informationssicherheit für CxO und Teams im Alltag ist. 20 Jahre lang.

Aus diesem persönlichen Antrieb heraus entwickelten wir VantarIS und gründeten Vantarion.

VantarIS nimmt die Bürokratie aus Normen wie NIS2 und bringt kompetente Sicherheit.

VANTARIS

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

WARUM TECHNISCHE PRÜFUNGEN ALLEIN NICHT GENÜGEN

Ein Pentest simuliert Angriffe.
Er zeigt Schwachstellen auf.
Er erzeugt Transparenz.

Doch Transparenz allein reduziert kein Risiko.

Ohne Governance-Struktur entstehen typische Probleme:

- ☑ **Findings werden isoliert behandelt**
- ☑ **Prioritäten werden nach technischer Schwere statt Geschäftsrisiko gesetzt**
- ☑ **Maßnahmen werden umgesetzt, aber nicht dokumentiert**
- ☑ **Wiederholungstests fehlen**
- ☑ **Management wird nicht eingebunden**

ISO 27001, NIS2 und vergleichbare Normen beschreiben ein ganzheitliches Managementsystem. Zuerst entsteht die Governance-Struktur, sie schafft Klarheit über Verantwortung und Prioritäten. Auf dieser Basis werden technische Prüfungen sinnvoll eingesetzt und deren Ergebnisse risikoorientiert verarbeitet.

Ein Pentest ersetzt kein Risikomanagement - Er ergänzt es.

VULNERABILITY SCAN, PENTEST ODER AUDIT?

Die drei Prüfarten werden oft vermischt, obwohl sie unterschiedliche Ziele verfolgen.

Vulnerability Scan – systematische Schwachstellenerkennung

Ein Vulnerability Scan ist automatisiert und regelmäßig einsetzbar. Er identifiziert bekannte Schwachstellen auf Basis öffentlicher Datenbanken.

Er liefert:

- ☑ **CVE-Referenzen**
- ☑ **Schweregradbewertungen**
- ☑ **technische Detailinformationen**

Er beantwortet die Frage: „Wo bestehen bekannte technische Schwachstellen?“

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

Er ist besonders geeignet für:

- ☑ kontinuierliche Überwachung
- ☑ Patch-Management-Kontrolle
- ☑ Basissicherheitsniveau

Was er nicht leistet: Er simuliert keine komplexen Angriffsketten und bewertet keine realistische Ausnutzbarkeit im Unternehmenskontext.

Penetrationstest – realistische Angriffssimulation

Ein Pentest geht deutlich weiter. Hier versuchen Sicherheitsexperten, Schwachstellen aktiv auszunutzen.

Dabei werden:

- ☑ Angriffspfade kombiniert
- ☑ Privilegien eskaliert
- ☑ Zugriffsmöglichkeiten ausgebaut
- ☑ reale Angriffsszenarien simuliert

Er beantwortet die Frage: „Was ist einem realen Angreifer tatsächlich möglich?"

Ein Pentest ist daher keine technische Prüfung, sondern eine Bewertung der Angriffsresistenz.

Er eignet sich besonders:

- ☑ für externe Angriffsflächen
- ☑ für geschäftskritische Anwendungen
- ☑ vor Markteinführung neuer Systeme
- ☑ bei erhöhtem Schutzbedarf

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

Audit – Prüfung der Steuerungslogik

Ein Audit bewertet nicht primär Technik, sondern:

- ☑ **Prozessreife**
- ☑ **Dokumentationsstruktur**
- ☑ **Managementsteuerung**
- ☑ **Wirksamkeit des ISMS**

Es beantwortet die Frage: „Ist das Sicherheitsmanagementsystem strukturiert und normkonform?"

Ein Audit kann einen Pentest fordern, ersetzt ihn jedoch nicht.

DEN SCOPE REALISTISCH UND STRATEGISCH FESTLEGEN

Ein Pentest ohne klaren Scope ist weder effizient noch aussagekräftig. Die Definition des Prüfbereichs sollte sich an folgenden Kriterien orientieren:

- ☑ **Kritikalität der Systeme**
- ☑ **Schutzbedarf der verarbeiteten Informationen**
- ☑ **Externe Erreichbarkeit**
- ☑ **Geschäftsrelevanz**
- ☑ **Komplexität**

Ein häufiger Fehler ist die pauschale Formulierung „Gesamtes Netzwerk". Dies führt zu unklaren Erwartungen und nicht priorisierbaren Ergebnissen. Stattdessen sollte der Scope präzise definieren:

- ☑ **Welche Systeme sind enthalten?**
- ☑ **Welche sind ausgeschlossen?**
- ☑ **Welche Testmethodik wird angewendet (Black-Box, Grey-Box, White-Box)?**
- ☑ **Welche Zielsetzung wird verfolgt?**

Ein klarer Scope schafft:

- ☑ **Erwartungssicherheit**
- ☑ **Budgettransparenz**
- ☑ **belastbare Ergebnisse**

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

FINDINGS SYSTEMATISCH IN DAS RISIKOMANAGEMENT ÜBERFÜHREN

Ein Pentest-Bericht enthält technische Bewertungen. Doch nicht jedes „kritische Finding" ist geschäftskritisch – und nicht jedes „mittlere Finding" ist harmlos. Deshalb ist die Einbindung in das bestehende Risikomanagement entscheidend.

1. Kontextbewertung

Jedes Finding sollte im Kontext bewertet werden:

- ☑ **Welcher Geschäftsprozess ist betroffen?**
- ☑ **Welche Vertraulichkeit, Integrität oder Verfügbarkeit ist berührt?**
- ☑ **Welche realistische Auswirkung hätte eine Ausnutzung?**

Erst durch diese Bewertung entsteht eine unternehmensbezogene Risikoeinschätzung.

2. Priorisierte Maßnahmenplanung

Maßnahmen sollten:

- ☑ **klar beschrieben**
- ☑ **mit Verantwortlichen versehen**
- ☑ **mit Fristen hinterlegt**
- ☑ **im Maßnahmenregister dokumentiert**

werden.

Nicht jedes Finding muss sofort umgesetzt werden. Entscheidend ist die dokumentierte Entscheidung, Umsetzung oder bewusste Risikoakzeptanz.

3. Wirksamkeitsprüfung und Nachweis

Nach Umsetzung muss dokumentiert werden:

- ☑ **Wann wurde die Maßnahme umgesetzt?**
- ☑ **Wie wurde die Wirksamkeit geprüft?**
- ☑ **Ist ein Wiederholungstest erforderlich?**

Erst hier entsteht Auditfähigkeit.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

EINBINDUNG IN MANAGEMENT & REPORTING

Technische Prüfungen dürfen nicht auf IT-Ebene verbleiben. Im Rahmen des ISMS sollten sie:

- ☑ **in das Maßnahmencontrolling integriert**
- ☑ **im Management-Reporting berücksichtigt**
- ☑ **im Management Review diskutiert**

werden.

So entsteht eine durchgängige Steuerungskette, die schützt nicht nur technisch, sie schützt auch organisatorisch.

ANFORDERUNGEN VON KUNDEN & VERSICHERERN

Kunden erwarten zunehmend:

- ☑ **regelmäßige technische Prüfungen**
- ☑ **Nachweis geschlossener Findings**
- ☑ **Transparenz über Maßnahmen**

Versicherer prüfen:

- ☑ **ob Pentests durchgeführt werden**
- ☑ **ob kritische Findings geschlossen werden**
- ☑ **ob strukturierte Nachverfolgung existiert**

Ein einmaliger Pentest-Bericht genügt selten. Versicherungsbedingungen enthalten häufig Klauseln zur Einhaltung von Sicherheitsstandards. Werden diese nicht erfüllt oder dokumentiert, kann dies im Schadensfall problematisch werden.

UMSETZUNGSUNTERLAGEN

1. Pentest-Scoping-Dokument

Dieses Dokument enthält:

- ☑ Zielsetzung
- ☑ Prüfbereich
- ☑ Ausschlüsse
- ☑ Testmethodik
- ☑ Verantwortlichkeiten
- ☑ Zeitplan

Es schafft Klarheit vor Beginn der Prüfung und verhindert Missverständnisse.

2. Findings-zu-Maßnahmen-Mapping

Dieses Dokument verbindet technische Ergebnisse mit dem ISMS:

- ☑ Referenz-Finding
- ☑ Geschäftsrisikobewertung
- ☑ Maßnahme
- ☑ Verantwortlicher
- ☑ Frist
- ☑ Status
- ☑ Nachweis

Es ist das zentrale Instrument zur Auditfähigkeit.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

FAZIT

Ein Pentest ist kein isoliertes Sicherheitsereignis. Er ist ein Instrument zur Validierung und Weiterentwicklung der Sicherheitsarchitektur. Richtig eingesetzt:

- ☑ **bestätigt er die Wirksamkeit technischer Maßnahmen**
- ☑ **identifiziert reale Angriffspfade**
- ☑ **stärkt er die Argumentationsbasis gegenüber Kunden**
- ☑ **unterstützt er das Risikomanagement**
- ☑ **verbessert er die Versicherbarkeit**

Falsch eingesetzt bleibt er ein technischer Bericht ohne nachhaltige Wirkung.

Der Unterschied liegt nicht im Test selbst, sondern in der systematischen Integration seiner Ergebnisse.

Erst wenn technische Prüfungen in Governance, Risikomanagement und Reporting eingebunden sind, entsteht aus einem Pentest ein strategisches Steuerungsinstrument.