secuvera

Cybersicherheit. Nachhaltig.

Penetrationstests als Teil eines ISMS

Grundlagen, Relevanz und mögliche Ansätze

23.02.2022

verinice.XP

Viktor Rechel

- seit 2019 bei der secuvera
- Tätigkeitsfelder, u. a.:
  - ISMS nach ISO 27001 (Umsetzung & Auditierung)
  - Sicherheitskonzepte nach IT-Grundschutz
  - Penetrationstests & Projektleiter
- Referent auf Fachkonferenz & Autor von Fachartikeln
- Zertifizierungen, u. a.
  - ISO 27001 Lead Auditor
  - Cyber Security Practitioner

Penetrationstest & ISMS

-

Das Zusammenspiel

secuvera

Informationen

secuvera

Zugang zu digitalen Informationen

„Die IT“

Informationen


Zugang zu digitalen Informationen
Soll Schutz sicher stellen
„Die IT“
Informationen
ISMS


Zugang zu digitalen Informationen
Soll Schutz sicher stellen
Stellt Anforderungen
„Die IT“
Informationen
ISMS
Standards

secuvera

„Die IT“

Informationen

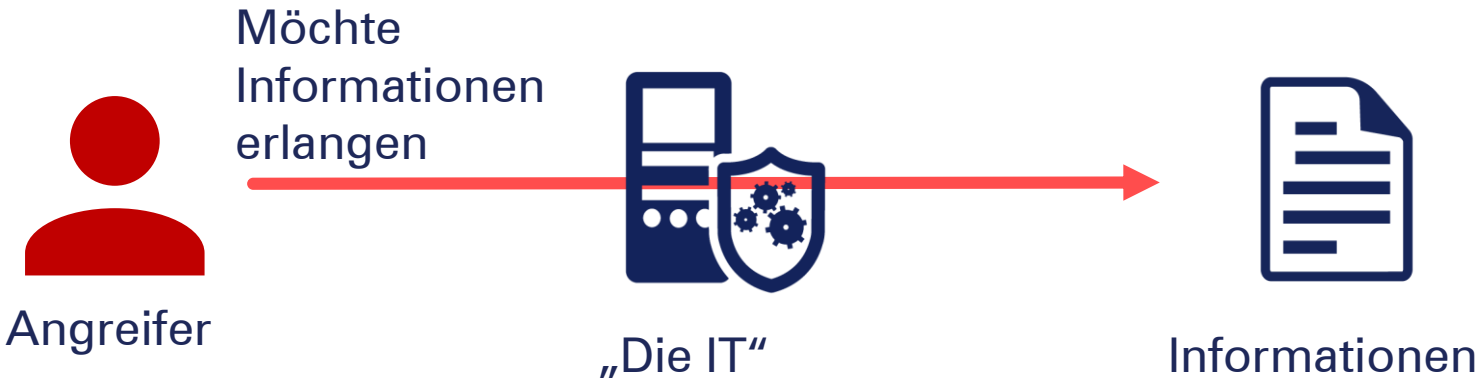
secuvera

Angreifer

„Die IT“

Informationen

secuvera


Möchte
Informationen
erlangen
Angreifer
„Die IT“
Informationen

secuvera

„Die IT“

Informationen

secuvera


Prüft auf
Sicherheit
Penetrationstest
Penetrationstester
„Die IT“
Informationen

Penetrationstest

„Die IT“

Informationen

ISMS

Penetrationstest

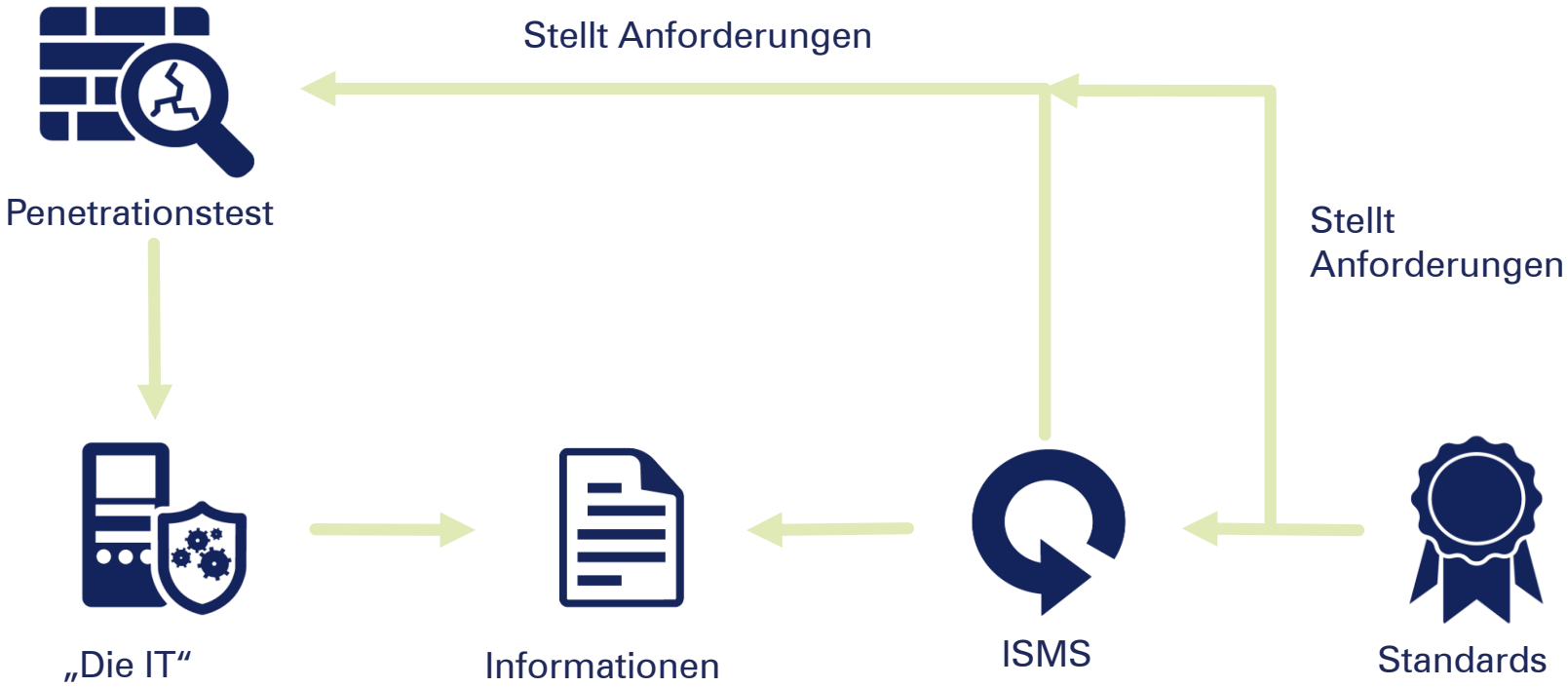
Stellt
Anforderungen

„Die IT“

Informationen

ISMS

secuvera


Stellt Anforderungen
Penetrationstest
Stellt
Anforderungen
„Die IT“
Informationen
ISMS
Standards

secuvera

Penetrationstests

-

Die Grundlagen

secuvera

Was ist ein Penetrationstest?

- (Technische) Prüfungen eines „Prüfgegenstands“
  - Innerhalb eines definierten Zeitraums technische Prüfungen gegen ein definiertes Ziel nach einem definierten Vorgehensmodell
  - Feststellung (aus Sicht eines Angreifers), welche Angriffspunkte erkannt (und potenziell ausgenutzt) werden können
- Feststellung des Sicherheitsniveaus von Systemen und Anwendungen
- Etablierung von nachhaltigen Sicherheitsmechanismen in Folge eines Penetrationstests

secuvera

Was ist ein Penetrationstest **nicht**?

- Penetrationstests sind **keine** Simulationen „echter Angreifer“
  - Angreifer haben spezifische Beweggründe und Ziele
  - Penetrationstest soll Schwachstellen identifizieren und grundlegend Informationen zum Sicherheitsniveau ermöglichen
- Einschränkende Aspekte
  - Time-boxed & risikobasierter Ansatz
- Wichtig: Der Penetrationstester ist Freund und Helfer.
  - Empfehlungen zu identifizierten Schwachstellen

secuvera

Vorbereitung

- Terminabstimmung
- Abstimmung der Ziele und des Vorgehens
- Vorstellung der Vorgehensweise und der Prüfungen durch Penetrationstester

Durchführung der eigentlichen Prüfungen / Tests

- Informationsbeschaffung und –auswertung
- Verifizierung der Schwachstellen
- Nach Absprache: Aggressivere Prüfungen

Abschluss

- Ergebnisbericht mit Bewertung der Schwachstellen
- Abschlussbesprechung

secuvera

Vorteile

- Feststellung existierender Schwachstellen
  - Angriffsfläche für potenzielle Angreifer kann geschmälert werden
  - Präventive Sicherheitsmaßnahmen
  - Empfehlungen zur Behebung im Rahmen des Penetrationstests
- Nachweisbarkeit eines bestimmten Sicherheitsniveaus
  - Kundenanforderungen
  - Rechtliche / regulatorische Anforderungen

secuvera

Fallstricke

- Penetrationstests sind stichtagsbezogen
  - Testgegenstand sollte realitätsnah sein
  - Testgegenstand sollte während den Prüfungen nicht verändert werden
- Wert eines Penetrationstests direkt von seiner Nachvollziehbarkeit abhängig
  - Achten Sie auf entsprechendes Know-How und ggfs. Referenzen
  - Relevant: BSI-Zertifizierungen für Penetrationstester und IT-Sicherheitsdienstleister

Ist eine Regelmäßigkeit notwendig?

- „Die Welt dreht sich weiter“
  - Neue Schwachstellen können bekannt werden
  - Neue Themen / Vorgehensweisen können erarbeitet werden
  - Die IT-Systeme entwickeln sich auch weiter
- Kontinuierliche Verbesserung des Sicherheitsniveaus durch regelmäßige Prüfungen

Penetrationstest & ISMS

-

Die Anforderungen

secuvera

ISO/IEC 27001

secuvera

ISO/IEC 27001 - Compliance

- A.18.2.3 „Überprüfung der Einhaltung technischer Vorgaben“
- Anwendung der Anforderung relativ spezifisch
- Grundsätzlich kann ein Penetrationstest als Überprüfung herangezogen werden und je nach Kontext und Reifegrad erwartet werden
- Notwendige Prüfung stark abhängig von Struktur, IT-Architekturen, etc.

Penetrationstest- bzw. Auditprogramm

secuvera

ISO/IEC 27001 - Softwareentwicklung

- A.14.2.8 „Testen der Systemsicherheit“
- A.14.2.9 „Systemabnahmetest“
- Softwareentwicklung bedingt eine entsprechende Prüfung der Software

(Web-)Anwendungsprüfung und/oder API-Prüfung

- Je nach Systementwicklung kann auch ein Penetrationstest als Abnahmetest bei komplexeren Systemen sinnvoll sein

Systembasierte Prüfung

BSI IT-Grundschutz

secuvera

IT-Grundschutz (Version 2022) – APP.1.4 Mobile Anwendungen

- APP.1.4.A15 Durchführung von Penetrationstests für Apps (H)
  - Vor Freigabe soll ein Penetrationstest durchgeführt werden, inkl. Backend und lokaler Speicherung
  - Regelmäßige und anlassbezogene Wiederholung des Penetrationstests

secuvera

IT-Grundschutz (Version 2022) – APP.3.2 Webserver

- APP.3.2.A16 Penetrationstest und Revision (S)
  - Regelmäßige Überprüfung auf Sicherheitsprobleme

Rein formal: Systembasierte Prüfung

Aus der Praxis: Verknüpfung von systembasierter Prüfung / Webanwendungsprüfung sinnvoll

secuvera

IT-Grundschutz (Version 2022) – SYS.1.1 Allgemeiner Server

- SYS.1.1.A24 Sicherheitsprüfungen für Server (S)
  - Regelmäßige Überprüfung auf Einhaltung von Sicherheitsvorgaben & etwaiger Schwachstellen (vor allem bei extern erreichbaren Systemen)
  - Durchführung auch mittels geeigneter Skripte realisierbar

Systembasierte Prüfung
(evtl. reine Port- & Schwachstellenscans)

secuvera

IT-Grundschutz (Version 2022) – NET.3.1 Router und Switches

- NET.3.1.A23 Revision und Penetrationstests (S)
  - Regelmäßige Überprüfung auf Sicherheitsprobleme

Systembasierte Prüfung

IT-Grundschutz (Version 2022) – NET.3.2 Firewall

- NET.3.2.A24 Revision und Penetrationstests (S)
  - Regelmäßige Überprüfung auf Sicherheitsprobleme

Systembasierte Prüfung

secuvera

IT-Grundschutz (Version 2022) – OPS.1.1.6 Software-Tests und –Freigaben & CON.8 Software-Entwicklung

- OPS.1.1.6.A14 Durchführung von Penetrationstests [Tester] (H)
  - Je nach Kritikalität sollte ein Penetrationstest durchgeführt werden
- CON.8.A5 Sicheres Systemdesign (B)
  - Erfüllung aller definierten Anforderungen muss überprüft werden
- OPS.1.1.6.A5 Durchführung von Software-Tests für nicht funktionale Anforderungen [Tester] (B)
  - Tests, u. a. zu sicherheitsspezifischen Anforderungen

(Web-)Anwendungsprüfung und/oder API-Prüfung

secuvera

IT-Grundschutz (Version 2022) – INF.13 Technisches Gebäudemanagement

- INF.13.A30 Durchführung von Penetrationstests im TGM (H)
  - Es sollten bedarfsorientierte Penetrationstests durchgeführt werden
- Implizite Anforderungen
  - INF.13.A11 Angemessene Härtung von Systemen im TGM (S)
  - INF.13.A12 Sichere Konfiguration der TGM-Systeme (S)
  - INF.13.A22 Durchführung von Systemtests im TGM (S) [Planer]

Systembasierte Prüfungen & (Web-)Anwendungsprüfung

secuvera

IT-Grundschutz (Version 2022) – Implizite Anforderungen

- Relationale Datenbanken
  - APP.4.3.A3 Basishärtung des Datenbankmanagementsystems (B)
    - Sicherstellung der Härtung
  - APP.4.3.A20 Regelmäßige Audits (S)
    - Regelmäßige Auditierung der Sicherheitsfunktionen
  - APP.4.3.A25 Sicherheitsprüfungen von Datenbanksystemen (H)
    - Regelmäßige Sicherheitsprüfungen der Sicherheitsfunktionen

Systembasierte Prüfung / Architekturanalyse

secuvera

IT-Grundschutz (Version 2022) – Implizite Anforderungen

- WLAN-Betrieb
  - NET.2.1.A13 Regelmäßige Sicherheitschecks in WLANs (S)
    - Untersuchung des WLANs auf Schwachstellen
    - Identifikation von Rogue-Access-Points
  - NET.2.1.A14 Regelmäßige Audits der WLAN-Komponenten (S)
    - Überprüfung der Einhaltung von Sicherheitsmaßnahmen bei den Komponenten

secuvera

IT-Grundschutz (Version 2022) – Implizite Anforderungen

- Industrie
  - IND.1.A17 Regelmäßige Sicherheitsüberprüfung (H)
    - Regelmäßige und anlassbezogene Prüfung der Konfiguration
  - IND.2.1.A19 Security-Tests [OT-Betrieb (Operational Technology, OT)] (H)
    - Regelmäßige Security-Tests der Sicherheitsmaßnahmen
  - SYS.4.4.A23 Auditierung von IoT-Geräten (H)
    - Regelmäßige Überprüfung

Zumeist Architekturanalyse

Penetrationstest & ISMS

-

Zum nachhaltigen Zusammenspiel

secuvera

Ansätze für ein „Penetrationstest-Programm“

- Regelmäßige Penetrationstests machen grundsätzlich Sinn
  - Techniken können sich ändern
  - Neue Schwachstellen und Vorgehensweisen können bekannt werden
- Vollumfängliche Penetrationstests (z. B. alle Systeme) sind aus Kostensicht nicht immer sinnvoll bzw. möglich
- Fokuspunkte können im Rahmen des ISMS bewertet werden (z. B. über Schutzbedarf oder Risikoanalyse)

➢ Kontinuierliche Verbesserung

secuvera

Ansätze für ein „Penetrationstest-Programm“

- Jährlich kritische Komponenten
  - Öffentlich erreichbare Systeme und Systeme mit höherem Schutzbedarf bzw. höherem Risiko
  - Öffentlich erreichbare und kundenbezogene Webanwendungen
- Z. B. 3-Jahres-Zyklus für allgemeine Komponenten (und entsprechende Anforderungen)
- Grundsätzlich auch Themen wie Clients, Mobilgeräte und Netzwerkstrukturen

secuvera

Ansätze für ein „Penetrationstest-Programm“

- Verbindung mit dem Auditprogramm für interne Audits
  - Interne Audits für organisatorische Themen
  - Penetrationstests für technische und tiefergehende Prüfungen
  - Entsprechende Themen können somit kombiniert und ergänzt werden

secuvera

Cybersicherheit. Nachhaltig.

Vielen Dank für die Aufmerksamkeit!

Fragen und Anregungen auch gerne persönlich im Nachgang

Ihr Ansprechpartner:

Viktor Rechel

vrechel@secuvera.de

+49 7032 9758 20