secunet

Beginn: 15:00 Uhr

Pentest – Schwachstellenanalysen für Unternehmen jeder Größe

Björn Jansen

Dirk Reimers

Webinar, 6. März 2023

secunet Security Networks AG

secunet auf einen Blick

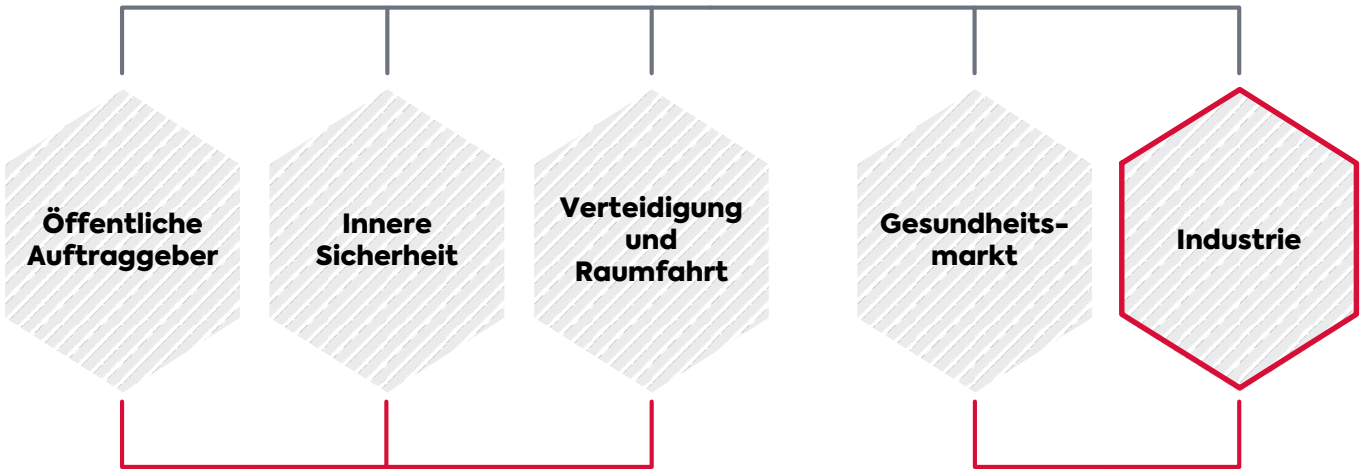
12 Standorte
in Deutschland

über 1000
MitarbeiterInnen

secunet.com

secunet auf einen Blick

secunet Security Networks AG

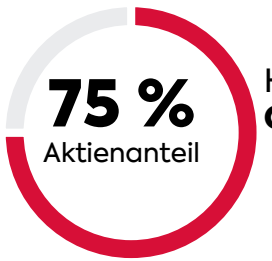


Division Industry Fokus

- **KRITIS-Betreiber / Versorger**
- **Digitale Infrastrukturen**
- **Industrielle Anlagen**
- **Automotive & Mobilität**

345m*
Euro Umsatz

47m*
Euro EBIT



Hauptaktionär:
Giesecke & Devrient

*vorläufig, im Jahr 2022

Schwachstellen in IT-Systemen – ein Presserundblick

TPM-2.0-Spezifikationen: Angreifer könnten Schadcode auf TPM schmuggeln

heise online, 01.03.2023

LastPass-Hack: Angreifer hackten Privat-PC von DevOps-Entwickler

heise online, 28.02.2023

BSI-Studie: Viele massive Sicherheitslücken bei Online-Shops

heise online, 27.02.2023

Hack wohl verantwortlich für Insolvenz von E-Bike-Hersteller

golem.de, 11.01.2023

Zahlenfolge „123456“ immer noch beliebtestes Passwort in Deutschland

heise online, 22.12.2017

IT-Sicherheit in Deutschland

Ein Bericht aus der Praxis

Konfiguration ungenügend

Triviale Standard-Passwörter

- Passwort zum Patienteninformationssystem ist „1“
  - USB-Tastatur anschließen und schon sind alle Patientendaten sichtbar

Sicherheit schafft Unsicherheit

- Überwachungskameras in Bank laufen auf internen Switch
  - Kamera ab / Laptop ran und schon im Banken-LAN
- Türöffnungsanlage im Gast-WLAN erreichbar
  - Mach‘ Dir die Tür selbst auf

Sichere auch die Hintertür

- Patientenüberwachungssystem
  - Standard-Passwort an der Kamera

Awareness mangelhaft

Mr. Hackermann

- E-Mail mit ZIP-Datei und Passwort
  - Schlechter Tausch: Eine Datei entschlüsselt, danach alle Dateien verschlüsselt.

„Hier haben wir Backups“

- Gefundene USB-Sticks
  - besser „auf Arbeit“ testen

Rouge Access Points

- Login im internen LAN
  - Warum muss ich auf einmal ein Passwort eingeben?

Patches nicht eingespielt

Veraltete Systeme

- Steuerung der Zutrittskontrolle auf Basis von Windows XP
  - Vom Besucher zum raumpflegenden RZ-Mitarbeiter

Veraltete Komponenten

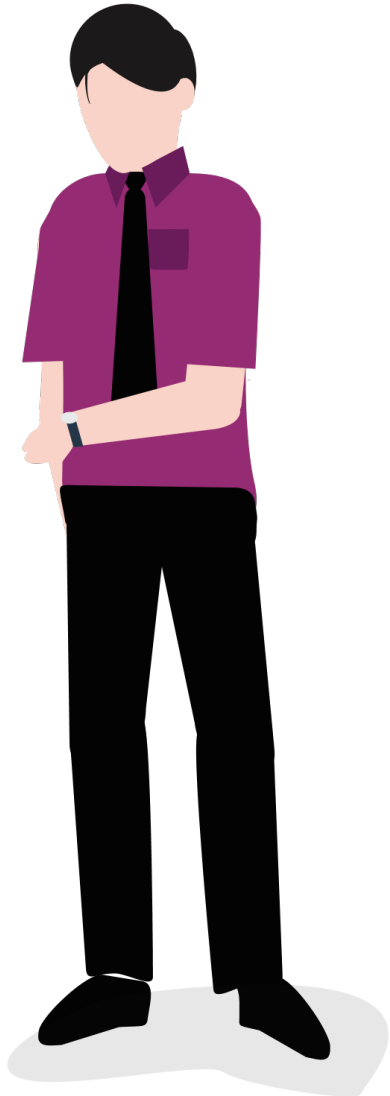
- PHP im Web-Portal
  - Web-Shell Upload
- SQLi in Bankenportal
  - Zugriff auf Kreditselbstauskunft
  - Klartextpasswörter

Unnötige Funktionen / nicht aktivierte Sicherheit

Härtung

- Festplatten im Büro müssen nicht verschlüsselt werden
  - Hier haben ja nur vertrauenswürdige Personen Zugang
- fehlende Systemhärtung
- veraltete/vergessene Systeme
- fehlende interne Schutzzonen
- fehlendes Sicherheitslagebild (temporär & dauerhaft)

Täter unbekannt?



Wer ist in diesen Szenarien kein Täter?

- Wie sicher ist Ihr Passwort wirklich?
- Wie häufig verwenden Sie Passwörter weiter oder ändern einfach eine Ziffer?
- Wer prüft bei einer E-Mail wirklich den Absender und die URLs
  - bspw. mit Virustotal oder Jotti.org
- Wer hat noch nie versucht, den automatischen Bildschirmschoner zu umgehen?
- Wer verschlüsselt vertrauliche E-Mails immer?

Unsere Lösungskomponenten

Prävention

Reaktion

Incident Readiness

Network Reconnaissance

Pentests

Incident Response

Wargaming

Detailanalysen

Red Teaming

IT-Forensic

Was ist ein Pentest und vor allem was nicht?

Wir suchen nach technischen und menschlichen Schwachstellen

- Wir suchen nicht nach dem Schuldigen im Unternehmen.

Wir wollen nicht Ihre knappen Ressourcen über die Maßen belasten

- Wir zeigen Ihre Schwachstellen auf, bevor sie jemand anderes ausnutzt.
- Wir geben eine Metrik, nach der Sie die Schwachstellen und die Behebung priorisieren können.
- Bei Bedarf stellen wir Security Administratoren, die Ihnen bei der Behebung helfen.

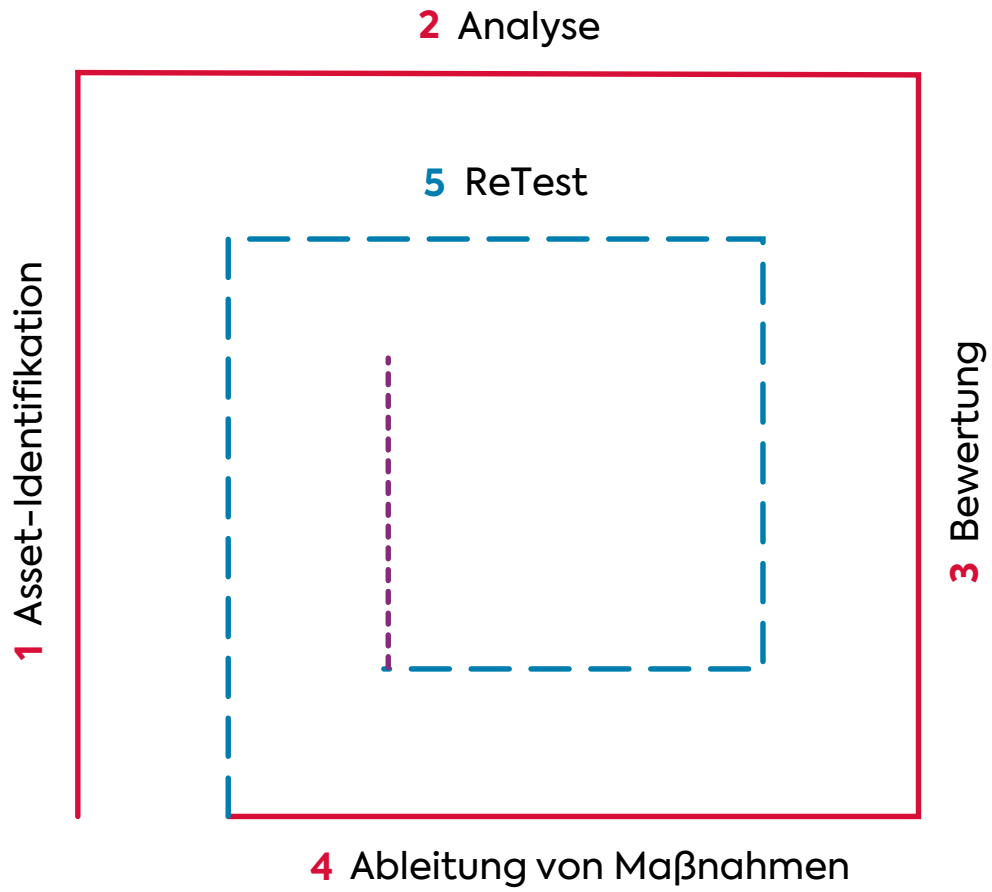
Wir helfen lieber vor einem Vorfall, als mit Ihnen die Scherben Ihrer IT aufzukehren

- Wer im Training viel schwitzt, schwitzt weniger während eines Vorfalls (wenn überhaupt).

Das typische Vorgehen bei Pentests

Vorgehen pro Arbeitspaket folgt grundsätzlich dem gleichen Schema

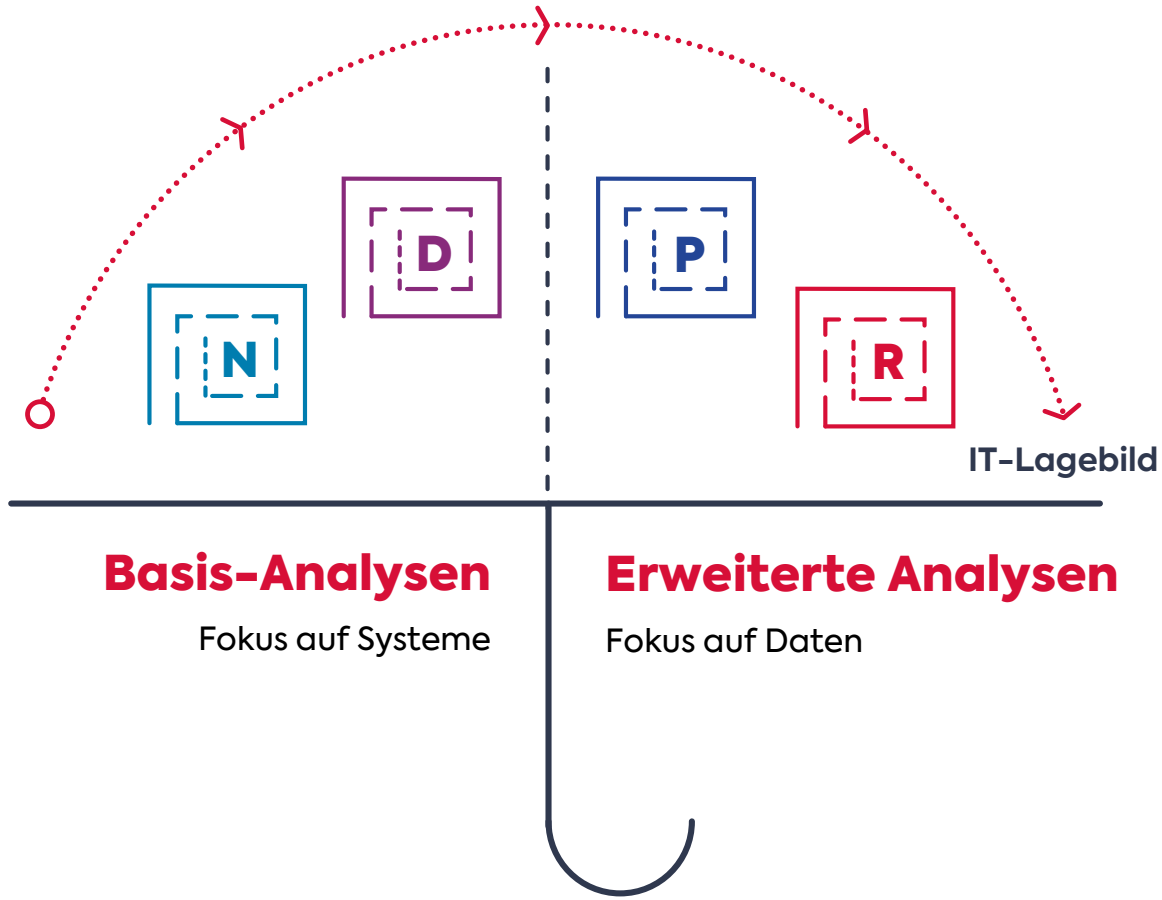
1. **Asset-Identifikation**
   - Auswahl von Analysetyp und Zielen
2. **Durchführung der Analyse**
   - Technische Prüfung
3. **Bewertung der Ergebnisse**
   - Überprüfung & Anpassung
4. **Ableitung von Maßnahmen**
   - Dokumentation empfohlener Maßnahmen
5. **ggf. ReTests (Sprung zu Schritt 2)**
   - Bei Bedarf erneute Analyse



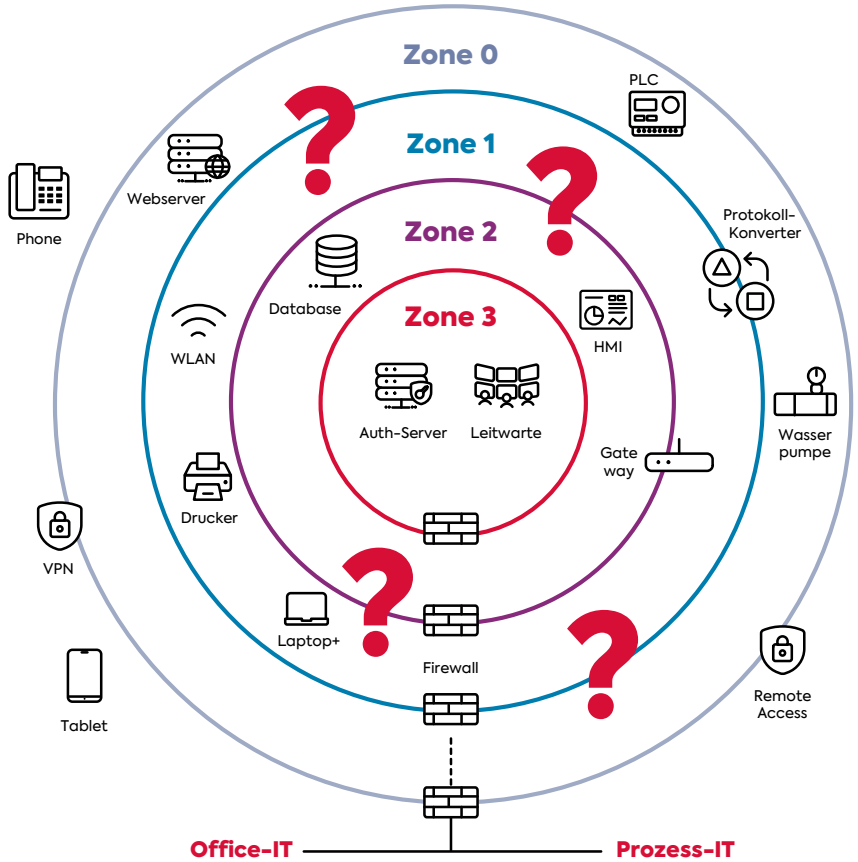
Vom Pentest …

Einzelne Pentests schaffen Momentaufnahmen

- Zielabsprache
- Durchführung
- Objektive Bewertung nach CVSS v3 Base Score
- Übergabe der Dokumentation
- Schwachstellen werden durch den Kunden bewertet
- Maßnahmen werden abgeleitet
- Waren Behebungen erfolgreich?



… mit verbindlichen ReTests …



Test der etablierten Maßnahmen

- 80% der Unternehmen führen keine ReTests durch.
- Es bleibt unklar, ob die Maßnahme wirksam ist.
- Wurden vielleicht neue Schwachstellen geschaffen?

Wiederholte Pentests schaffen Mehrwerte

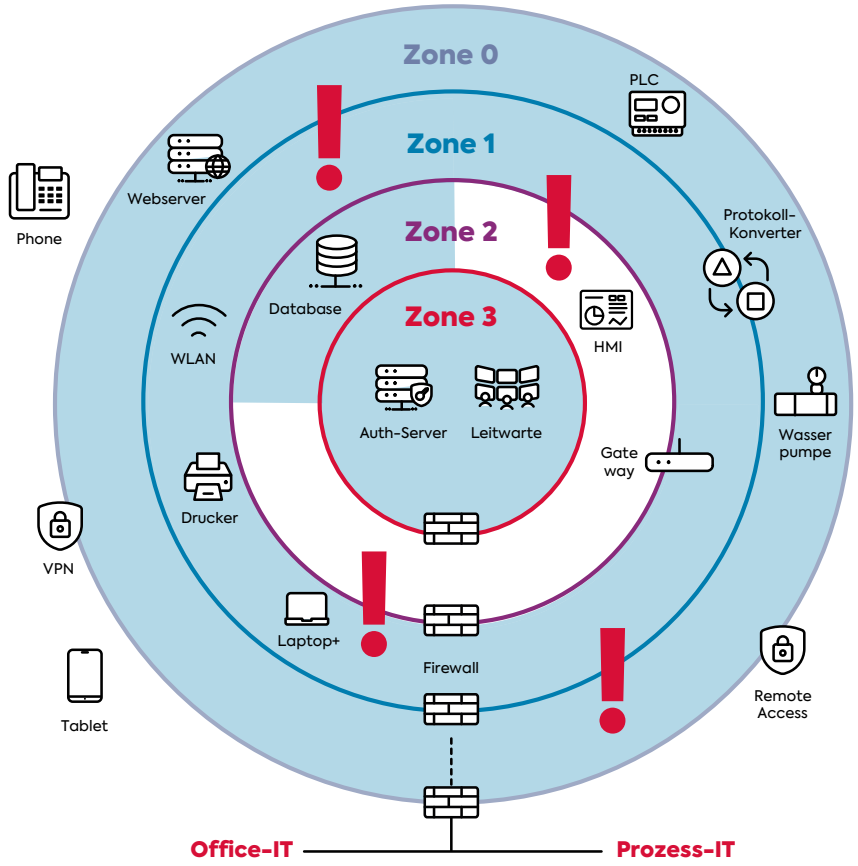
- ReTests bereits geprüfter Komponenten validieren Behebungen.
- Tests neuer Komponenten erweitern die Sicht: Sukzessive wird das ganze Unternehmen geprüft.
- Ein IT-Sicherheitslagebild entsteht.

… mit der Pentest-Wette …

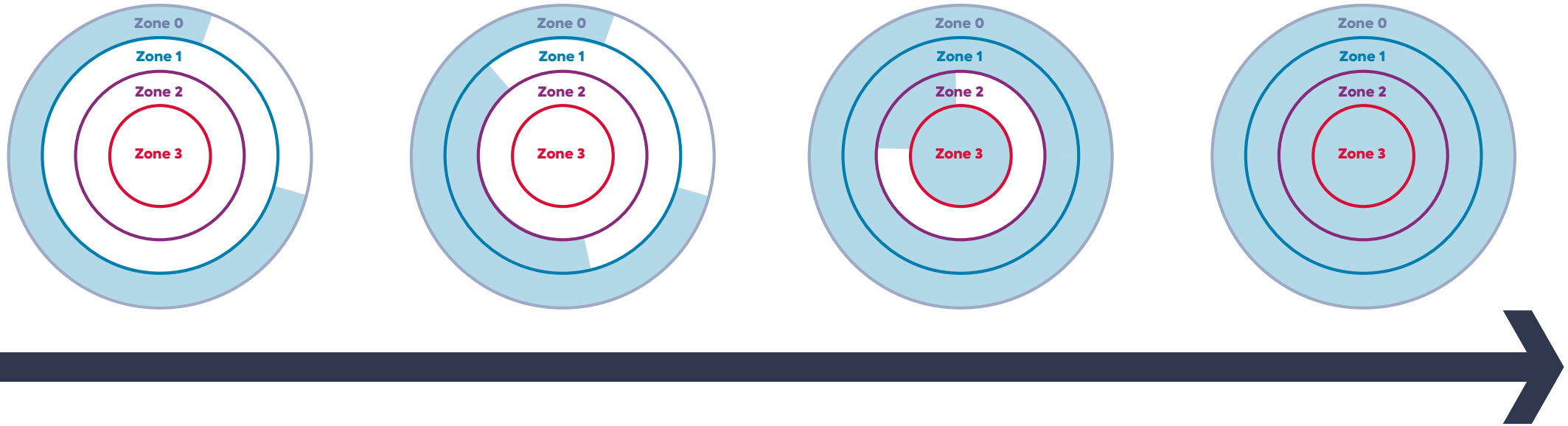
Wir wetten mit Ihnen

- Wir addieren alle Schwachstellen mit einem Base-Score >=7
  - Im ursprünglichen Pentest und
  - Im ReTest
- Ist die Summe im ReTest mindestens 30% geringer, bezahlen Sie 30% weniger für den ReTest.

Zeigen Sie uns, dass Ihr Security Prozess funktioniert!



...zur Pentest-Strategie im Unternehmenskontext



+ Start mit **Scans** + Im Internet erreichbare Systeme + Überblick über schwache Systeme	+ Überprüfung gefundener Schwachstellen + Interne Scans + Detailanalysen häufiger Systeme	+ Lagebild ist vorhanden + Fokuswechsel: Datenzugriff + Erweiterte Pentests mit Zugriffsziel	+ Alle Systeme in einem guten Zustand + Neues Ziel: Erkennung von Angriffen + Red-Teaming

Butter bei die Fische (wie man so sagt)

Welcher Schritt sollte der Erste sein?

- Analysen von innen oder von außen?
- Mit Wissen der IT oder ohne?
- Verdeckt oder Offen?
- Alles oder einzelne Systeme?

Wir empfehlen eines von zwei Standard Arbeitspaketen

- Technische Basisanalyse
- BSI Cyber Sicherheits-Check

Technische Basisanalyse

Ein erster technischer Eindruck über die wichtigsten Angriffsvektoren

- Kick-Off
- Scans von außen
- Scans von innen
- Detailanalysen der Firewall(s)
- Strukturbetrachtung der internen Netze
- Detailanalyse eines typischen Arbeitsplatzes
- Abschlussbesprechung
- Dokumentation

BSI Cyber Sicherheits-Check

Technische Basisanalyse

+

Organisatorische Betrachtung mit beleggestützten Interviews

- Organisation
- Physische Sicherheit
- Absicherung von Netzübergängen
- Abwehr von Schadprogrammen
- Inventarisierung der IT-Systeme
- Vermeidung offener Sicherheitslücken
- Sichere Interaktion mit dem Internet
- Logdatenerfassung und Auswertung

- Sicherstellung eines aktuellen Informationsstands
- Bewältigung von Sicherheitsvorfällen
- Sichere Authentisierung
- Gewährleistung der Verfügbarkeit notwendiger Ressourcen
- Durchführung nutzerorientierter Maßnahmen
- Sichere Nutzung von Sozialen Netzwerken
- Durchführung von Penetrationstests
- Active Directory

secunet T⁴
Tools, Techniken, Typen und Teams

Tools

- Freie Tools & Eigenentwicklungen
- Bieten schnell Überblick
- Low-Hanging-Fruits

Techniken

- A fool with a tool …
- Einsatz von Tools nicht ausreichend
- secunet entwickelt systemspezifische Techniken

Typen

- „Hacker“-Mindset
- Hohes persönliches Engagement
- Vertrauens-würdigkeit
- Kriminelles Denken ohne kriminelle Vorgeschichte

Teams

- 12 Pentester an drei Standorten
- Unterschiedliche Zertifikate wie OSCP, eCCP, BSI geprüfter Pentester, etc.
- Weltweite Einsätze sind möglich
- Backup mit 600 weiteren Experten unterschiedlichster Ausrichtung

Fazit

Fakt ist…	Sicherheitsniveau für geprüfte Bereiche aufrechterhalten	Was ist zu tun?
■ IT-Systeme werden permanent angegriffen. ■ Einzelne Pentests schaffen „nur“ Momentaufnahmen.	■ Nur regelmäßige Pentests schaffen ein vollständiges Sicherheitslagebild. ■ Unternehmen sparen Kosten durch frühe Planung & Einbindung von Pentests in den IT-Sicherheitsprozess.	■ Mit der secunet Pentest-Strategie werden die Werte des Unternehmens effektiv geschützt.

secunet berät und unterstützt Sie bei der Erstellung und Umsetzung Ihrer individuellen Pentest-Strategie

Save The Date – unsere Industrial Security Webinare

- **secunet monitor KRITIS – die Angriffserkennung gemäß IT-Sicherheitsgesetz 2.0“**

  09. März, 10:00 – 11:00 Uhr

- **Sichere Cloud-Anbindung in der Produktion**

  29. März, 10:00 – 11:00 Uhr

- **Cyberangriff – Notfallplan für den Ernstfall**

  24. April, 15:00 – 16:00 Uhr

- **Vorbereitung auf Cyberangriffe – Üben für den Ernstfall**

  15. Mai, 15:00 – 16:00 Uhr

Informationen und Anmeldung unter:
www.secunet.com/industrie

Kontakt

Dirk Reimers

Abteilungsleiter Pentest und Forensik

secunet Security Networks AG

dirk.reimers@secunet.com

Björn Jansen

Senior Sales Manager

secunet Security Networks AG

bjoern.jansen@secunet.com


secunet