axians

Axians
Security Validation Platform

Die Schäden sind sofort sichtbar, die Angreifer nicht!
Begegnen Sie den Angreifern auf Augenhöhe
mit dem Service sowie dem Know-how von
Axians und der Technologie von Pentera.

DEM ANGREIFER EINEN SCHRITT VORAUS

Die Herausforderung

Hacker werden immer raffinierter, daher sind sich die Sicherheitsbeauftragten der Unternehmen und die Aufsichtsbehörden immer mehr der Notwendigkeit bewusst, die Perspektive der Angreifer in ihre laufende Security-Abwehrstrategie zu integrieren.

An diesem Punkt kommen Penetrationstests ins Spiel. Manuelle Penetrationstests, wie wir sie heute kennen, sind zeitaufwändig, für den Betrieb des Netzwerks störend, kostspielig, stellen nur eine Momentaufnahme dar und werden dem Bedarf an kontinuierlicher Sicherheitsüberprüfung in einer dynamischen IT-Umgebung nicht gerecht.

Sicherheitslücken rechtzeitig erkennen und wertvolle Daten schützen

Mit **Axians Security Validation Platform (ASVP)** setzen wir auf eine Variante, welche als Übungsangriff auf Ihre Schutzmaßnahmen dient, ohne das tatsächlich „echte" Schäden entstehen. Hierdurch werden die Verwundbarkeiten sichtbar und Handlungsempfehlungen gegeben.

Die Kombination aus unseren hochzertifizierten Cyber-Security-Consultants und der innovativen Softwarelösung Pentera ermöglicht es, in einem relativ kurzen Zeitraum einen umfangreiche Überprüfung der Security Abwehrmechanismen zu günstigen Konditionen durchzuführen. Dabei konzentrieren wir uns auf die Bedrohung von innen und ahmen den Hackerangriff nach. Wir führen ethische Exploits automatisiert aus, wobei der ungestörte Netzwerkbetrieb gewährleistet bleibt.

Alle Highlights im Überblick

- **Agentenlos**
- **Minimale False Positives**
- **Unschädliche Exploits**
- **Angriffs-Checkpoints**
- **Priorisierte Handlungsempfehlungen**
- **Aktuellste Hacker-Techniken**
- **Angepasste Prozess-Alarme**
- **Sichtbarkeit von Angriffsvektoren**

SO FUNKTIONIERT´S

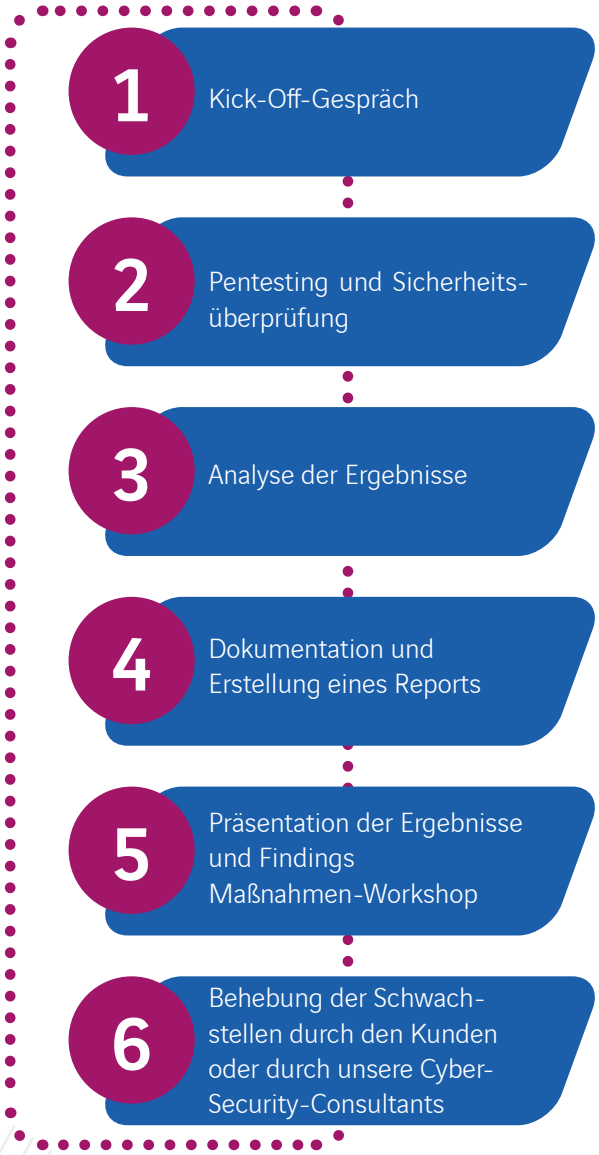
Axians Security Validation Platform

Zuerst findet ein Kick-Off-Gespräch statt. Hier wird die Vorgehensweise besprochen, der Scope definiert (IP-Ranges und -Adressen) und Maßnahmen für einen ungestörten Betrieb festgelegt (z. B. Information an Kollegen, die das SOC/SIEM-System betreiben, etc.).
Die Sicherheitsüberprüfung wird gestartet und läuft größtenteils automatisiert ab.

Folgende Tests werden durchgeführt:

- **Blackbox-Test** (Keine Kenntnisse über das Netzwerk vorhanden)
- **Password-Cracking**
- **Greybox-Test:** „was wäre wenn"-Szenarien
- **Active Directory Password Assessment:** Passworthygiene, Passwortrichtlinien, Fehlkonfigurationen, User ohne Passwort, umkehrbare Verschlüsselung
- **Pentera RansomwareReady Prüfung:** Durchführung eines Ransomware-Angriffs, sehr realitätsnahe Prüfung mit den Ransomwarevarianten REvil, Maze und Conti

Nach dem durchgeführten Pentest werden die Ergebnisse **analysiert, aufbereitet** und in einem Report **zusammengefasst.** In der anschließenden Ergebnispräsentation werden **Vorgehensweisen für die Behebung der Schwachstellen** besprochen. Diese Art der Überprüfung von Schwachstellen sollte in regelmäßigen Abständen durchgeführt werden, zumal stetig neue Angriffsvarianten aufkommen und die Software Pentera ständig weiterentwickelt wird.



ANZAHL PENTESTS/ SICHERHEITS-ÜBERPRÜFUNGEN	EINMALIG PRO SEGMENT	QUARTALSWEISE 4 x IM JAHR PRO SEGMENT	MONATLICH 12 x IM JAHR PRO SEGMENT
ANGEBOTSPREIS	Auf Anfrage	Auf Anfrage	Auf Anfrage
EINMALIGE HARDWARE-KOSTEN	Im Angebotspreis enthalten (Leihgerät)	Auf Anfrage	Auf Anfrage
OPTIONALES DIENSTLEISTUNGS-KONTINGENT ZUR BEHEBUNG DER FINDINGS ▸ Abrechnung nach Aufwand ▸ Geschätzter Aufwand ca. 5 Tage	Auf Anfrage	Auf Anfrage	Auf Anfrage

09/2022

axians

Axians IT Security GmbH · Christoph-Probst-Weg 27 · 20251 Hamburg
Tel.: +49 40 271661-0 · Fax: +49 40 271661-44
E-Mail: info-itsecurity@axians.de · www.axians.de