Axians´ Penetration Testing

Our service enables you to continuously validate the security posture in your organization and present actionable findings to management so that informed decisions can be made.

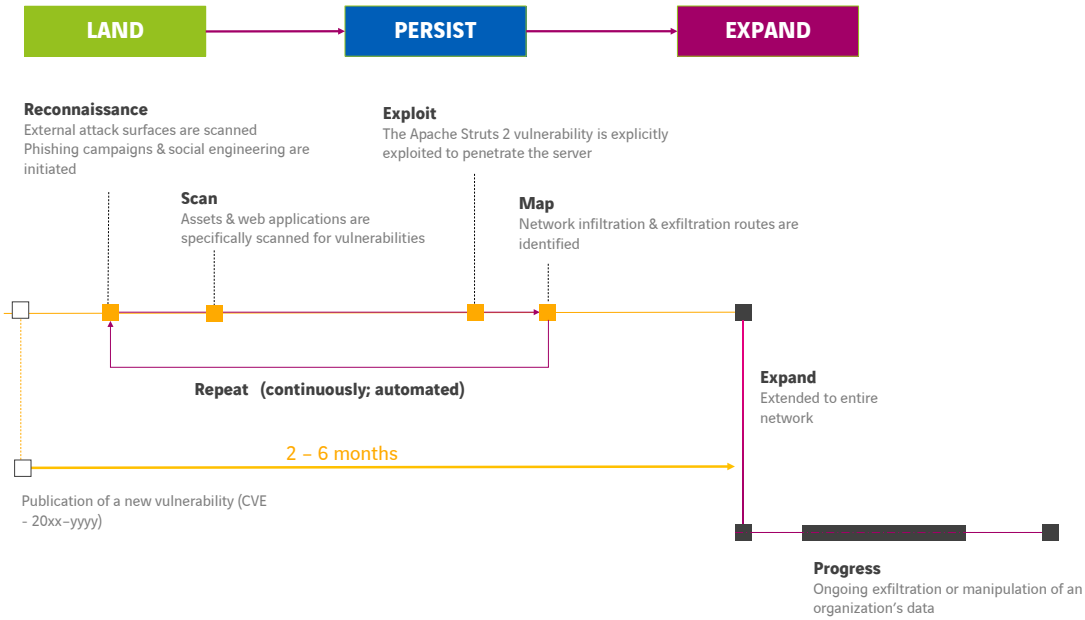
ARE YOUR CYBER SECURITY EFFORTS BEING UTILIZED TO FULL EFFECT?

Axians´ Penetration Testing

Data processing activities in agile cloud environments, web and business apps providing for mobile access, vulnerable end-points and workplaces — all create an unprecedented attack surface for organized cybercrime. Security experts and regulatory authorities alike urgently recommend adopting cyberdefense strategies that also enable an organization's infrastructure to be validated from an adversarial perspective and tested for vulnerabilities.

Pentesting is traditionally conducted by cyber security experts manually, the findings analyzed and presented in reports. Yet static, one-off security validation like this no longer satisfies the requirements posed by an IT infrastructure undergoing dynamic change. By the same token, restricting pentesting to critical data and environments no longer suffices since "successful" ransomware attacks show that they are prepared unnoticed in the network over the course of weeks or months and originate in seemingly non-critical systems.

Anatomy of a cyberattack: Land – Persist – Expand



Hackers prepare cyberattacks and ransomware attacks well in advance, observing an organization's infrastructure over extended periods of time in order to strike at just the right moment. What to do? Engage in continuous, long-term observation of your organizational infrastructure so that you, too, can strike at just the right moment!

Axians offers the right service for any challenge

Based on Pentera's automated pentesting platform, Axians enables you to subject your production environment to continuous security validation — in a controlled, secure and transparent manner.

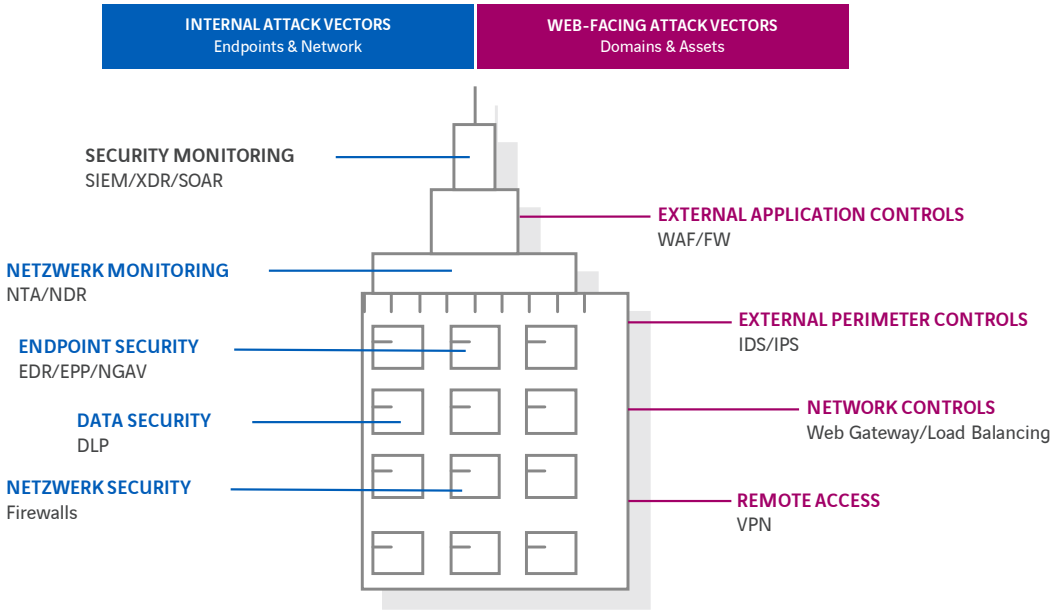
Axians shows you the real-world consequences a cyberattack would have on your mission-critical data & processes and supports you in answering the following questions:

- **Can my organization be comprised by a ransomware attack?** If so, what would the direct impact be and how can specific security gaps be plugged?
- **Have cyber security software and solutions been expertly deployed** to provide for sufficient protection against attacks?
- **Are escalation processes followed in the event of an attack?** Do internal and external service providers comply with their SLAs?

What Axians offers you

We continuously test your organizational structure in its entirety for security gaps and vulnerabilities without disrupting the productivity of your employees or tying up enormous resources of your IT department. You receive up-to-the-minute, detailed reports and recommendations for action that address your actual vulnerabilities.

End-to-end security validation & penetration testing service



Comprehensive security validation of all attack vectors and digital resources

The following pentesting scenarios are examples: during a consultation with you, scenarios are individually adapted to your specific needs.

- Security validation of your **production data processing systems** (e.g. servers, clients, endpoint security solutions)
- Security validation of your **cyber security solutions and controls** (e.g. firewalls, remote access & VPN, cloud environments, SOC services)
- Security validation of your **web-facing services and applications** (e.g. online shops, e-banking, web services & online applications)

Our pentesting services at a glance

Internal or external penetration testing, web app pentesting, one-off or continuous security gap testing: Our services cover various types of penetration testing so that no security gap gœs undetected. They can also be combined per project, as needed. Let us show you what we can do for you.

Web application pentesting

- Testing of web applications (including the server infrastructure on which the application is run) from the perspective of an experienced hacker
- Pentesting is based on the OWASP Web Security Testing Guide (WSTG)
- Pentesters perform ethical exploits and expand testing following a structured approach by mounting specific attacks gleaned from their wealth of experience

Web API pentesting

- Testing of the Web API (including the server infrastructure on which the API is hosted) by an experienced hacker
- Pentesting is based on the OWASP Web Security Testing Guide (WSTG) and the OWASP API Top 10 security threats
- Pentesters perform ethical exploits and expand testing following a structured approach by mounting specific attacks gleaned from their rich experience

Mobile app pentesting

- Validation of mobile applications applying the OWASP Mobile Application Security Verification Standard (MASVS)

Internal pentesting

- Continuous security validation based entirely on the MITRE ATT&CK Framework

Our range of services are available on an ongoing basis or as a one-off starter package.
Don't hesitate to contact us for advice and a quotation tailored to you.

- Ransomware emulation and AD security assessment

External attack surface pentesting & critical asset identification

- Continuous security validation of defensive perimeter controls like external application control (WAF), remote access (SSL/VPN) and perimeter controls (FWs), including leaked credentials monitoring (powered by Pentera)

Have we piqued your interest?

Take advantage of a personal consultation at no obligation to you: this enables us to precision-adapt our pentesting services to your organization.

YOUR CONTACT

Renata Rekic (Presales Consultant)

Email: renata.rekic@axians.com

07/2023

Axians IT Services AG · Arlesheim · Lausanne · Zürich
Phone: +41 61 716 70 70
Email: info-ch.security@axians.com · www.axians.ch