NEVERHACK

Your Cyber Performance Partner

/CASE_STUDY

Axinom case study

Validating Security. Enabling Trust

Elevating cyber resilience through web application penetration testing

NEXT PAGES TO KNOW MORE ↓

WWW.NEVERHACK.EE

axinom!

axinom!

Table of Contents

1. Security as a strategic lever

In a digital economy where speed is everything, web applications sit at the core of customer experience and business performance. But the same qualities that drive innovation—agility, rapid deployment, constant iteration—also expose systems to growing security risks.

Cyber threats have evolved. So must your defenses.

At NEVERHACK, we see security not as friction, but as force multiplication. It's how resilient companies move fast without compromise. Our Offensive Security team partners with forward-leaning organizations like Axinom to uncover hidden risks, validate defenses, and protect what matters most—before attackers even get a chance.

Security isn't just about preventing breaches. It's about building trust, continuity, and long-term competitive advantage

2. Inside Axinom: engineering for trust at scale

Axinom is no newcomer to high-stakes software. Founded in 2001 in Germany, the company delivers SaaS platforms and professional services tailored for the aerospace and media & entertainment sectors—industries where reliability, performance, and security aren't optional. They're mission-critical.

From Hollywood studios and global airlines to major broadcasters, Axinom serves organizations with some of the strictest security requirements in the world. Their platform powers everything from DRM (Digital Rights Management) systems trusted

With teams in Germany, Estonia, Sri Lanka, USA and a global footprint supported by a hybrid, multi-cloud architecture spanning Azure, AWS, and Google Cloud, Axinom builds with scale and resilience at its core.

But what truly sets them apart is how deeply cybersecurity is embedded into the company's DNA. For Axinom, security isn't a compliance checkbox—it's a competitive advantage and a prerequisite for doing business in sensitive, regulated environments.

They back this commitment with recognized certifications including ISO/IEC 27001:2022, Security Verified, and previously PCI DSS—reinforcing a culture where trust is built into the codebase, not just added on top.

3. The challenge

The decision wasn't driven by an incident. It was driven by foresight.

Axinom's leadership understood a simple truth: assumptions aren't protection. They wanted confirmation that no critical vulnerabilities were hiding in plain sight—and they wanted more than a checkbox report. They sought real, actionable insights to strengthen their position as a trusted technology partner.

"We assumed there were no major security holes... But we were also afraid of two extremes: either too many critical findings or none at all, which would feel like a waste." Grigory Grin | CISO at Axinom

Axinom turned to NEVERHACK Estonia's Offensive Security Team—a trusted partner from past engagements. They weren't looking for automation-heavy scans. They wanted deep manual testing, clear communication, and a framework-based approach grounded in OWASP ASVS Level 1.

Importantly, this initiative was driven by Axinom's commitment to achieving and maintaining ISO/IEC 27001:2022 certification, a key credential demonstrating their dedication to information security management. The penetration test provided vital evidence of control effectiveness and risk treatment—a cornerstone of ISO 27001 compliance.

In a bold but calculated move, Axinom opted to test in a live production environment. This meant working closely to manage risk, minimize disruption, and deliver results with full operational context.

This wasn't about compliance alone. It was about maintaining confidence—with customers, with partners, and with themselves.

In short: they wanted expertise. And that's exactly what they got.

4. What web application penetration test really delivers

At NEVERHACK, a Web Application Penetration Test isn't just about finding flaws—it's about delivering clarity, confidence, and control over your application's real-world security posture.

Our testing is designed to uncover vulnerabilities that could lead to data breaches, business logic abuse, privilege escalation, or full application compromise. We go beyond automated checks, applying advanced manual techniques that simulate how real-world adversaries think and operate.

The outcome is more than just a report—it's a playbook for remediation, improvement, and long-term resilience.

What you get: key deliverables

Detailed findings report :

Technical Findings: Comprehensive details of each identified finding, including its nature, location, and potential impact.

Risk Ratings – Severity levels based on likelihood and impact, following industry standards.

Proof of Exploitability: Demonstrations of how findings can be exploited, often including screenshots or detailed reproduction steps.

Security Standards Mapping – Clear references to OWASP ASVS, helping teams tie remediation to compliance.

Actionable recommendations:

Fix Instructions – Practical, platform-specific guidance to remediate each finding.

Best Practices – Insights to prevent similar issues in future sprints.

Workarounds – Temporary mitigation strategies when permanent fixes take time.

Executive summary:

High-Level Overview – Strategic insights for leadership, without the technical clutter.

Impact Assessment – Business risk evaluation of discovered vulnerabilities.

Live Findings Review – Interactive session with NEVERHACK testers to walk through results and next steps.

Scope, method, and testing levels:

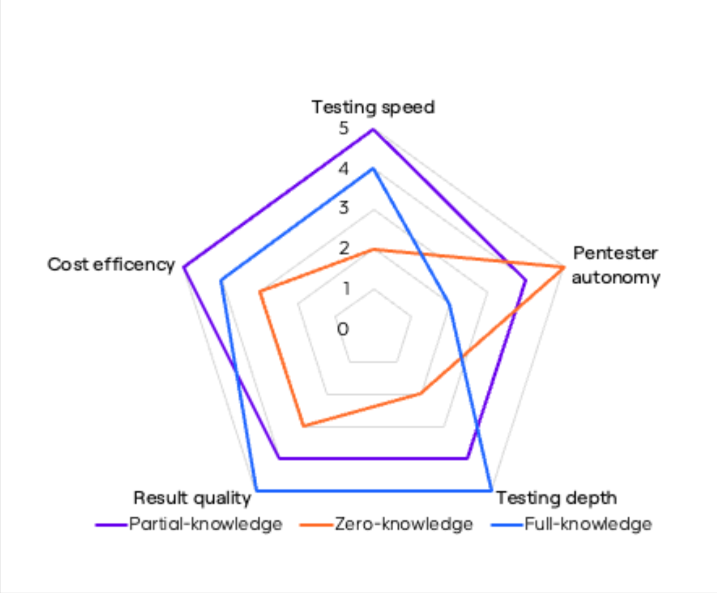
Every test is custom-tailored. Before we begin, scope is carefully defined—prioritizing what matters most, while excluding deprecated or overly sensitive areas if required.

We offer three engagement models:

Zero-Knowledge (black box) – Simulates an external attacker with no prior knowledge; only the URL and low privilege account are provided

Partial-Knowledge (gray box) – Penetration tester has partial knowledge about the application and data flow in addition to target URL.

Full-Knowledge (white box) – Deep-dive testing with access to source code and live logs



Methodology: built on standards that matter

Our approach is anchored in the OWASP Web Security Testing Guide (WSTG) and the Application Security Verification Standard (ASVS) the globally recognized framework for application security testing.

There are three ASVS testing levels: Level 1, intended for low-risk applications that can be fully penetration tested; Level 2, recommended for most applications as it covers sensitive data, authentication, and business logic; and Level 3, designed for high-assurance environments such as medical, financial, or safety-critical systems.

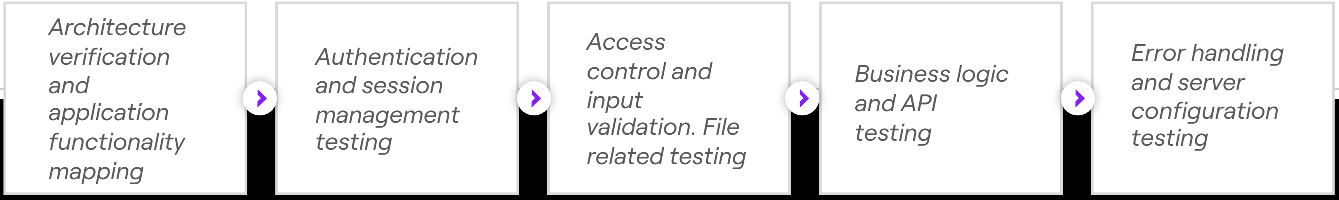
For Axinom, ASVS Level 1 was the right fit ensuring meaningful coverage without unnecessary overhead and aligning with their internal security maturity and compliance requirements.

5. The solution: focused, manual, and business-aware

For Axinom, precision mattered more than breadth. The testing scope was strategically pragmatic—targeting high-impact, business-critical components of the Axinom Portal while deferring less essential areas, like the admin UI, to stay within budget without compromising value.

NEVERHACK responded with a tailored, methodical approach—engineered for depth, not noise.

Testing workflow



Architecture verification and application functionality mapping

Authentication and session management testing

Access control and input validation. File related testing

Business logic and API testing

Error handling and server configuration testing

Manual first. Always.

Over 90% of the assessment was conducted manually. Tools like Burp Suite were used with surgical precision only where they added value without disrupting the live production environment.

NEVERHACK Offensive Security Team combined technical depth with operational discipline. Their hands-on methodology allowed them to uncover nuanced issues that automated scans simply miss.

What truly set this engagement apart was the team's ability to decode complex business logic including Axinom's DRM infrastructure and auth flows. That understanding enabled them to spot vulnerabilities buried beneath layers of application logic, far beyond surface-level weaknesses.

Throughout the process, collaboration was tight. Communication was clear. And every finding came with context, not just code.

6. The results: validation with real impact

The assessment confirmed what Axinom had hoped and what their customers demand: a mature security posture, backed by real-world testing.

No critical vulnerabilities were identified. However, the test surfaced several lower-severity issues, including a noteworthy authentication bypass in the management system a risk created not by a single flaw, but by the subtle interplay of minor oversights.

This finding underscored a powerful truth: small missteps can stack up to create serious risk.

To support rapid remediation, NEVERHACK delivered an intermediate report mid-engagement, enabling Axinom's team to address the most important issues without delay.

"We liked the report format it had a clear management summary and detailed reproduction steps. Very actionable and easy to follow for our developers."

Grigory Grin | CISO at Axinom

Axinom's response was swift and structured:

- Findings were logged into the development backlog
- Key issues were remediated before the final report
- Internal workshops were held to share lessons across teams
- Secure coding guidelines were updated to prevent recurrence
- A follow-up retest confirmed all significant issues had been effectively resolved
- The result? Not just a stronger application but a stronger security culture.

7. Key takeaways: testing as a catalyst for growth

This wasn't just a technical exercise. For Axinom, the engagement served as a strategic checkpoint validating their security posture, proving compliance maturity, and sparking meaningful improvements across teams.

Lessons learned:

- Penetration testing delivers the most value when paired with internal ownership.
- Manual, context-aware testing uncovers what tools can't.
- Even small findings can have large implications—especially when chained.
- Security should evolve with the product. Axinom now plans recurring tests, rotating scope based on growth, risk, and customer expectations.

Based on experience across sectors and critical systems, we recommend:

- Apply OWASP ASVS Level 2+ across the software development lifecycle
- Fix small issues early—before they become exploitable chains
- Use layered defenses including MFA, WAFs, and robust access controls
- Embed testing into your release cycle and maintain a tested incident response plan

8. Business value delivered

The engagement provided clear, measurable outcomes both technical and strategic:

- Confirmed the resilience of a mission-critical application
- Delivered actionable findings that elevated developer practices
- Reinforced trust with stakeholders, partners, and auditors

Axinom walked away not just with a clean bill of health but with greater confidence, sharper processes, and a stronger security foundation to support ongoing growth.

Conclusion: security as a competitive edge

Axinom's case is a powerful example of how proactive security investments pay off. With the right testing partner and internal alignment, penetration testing becomes more than risk reduction it becomes a tool to accelerate innovation, earn trust, and lead with confidence.

8. Business value delivered

The engagement provided clear, measurable outcomes both technical and strategic:

- Confirmed the resilience of a mission-critical application
- Delivered actionable findings that elevated developer practices
- Reinforced trust with stakeholders, partners, and auditors

Axinom walked away not just with a clean bill of health but with greater confidence, sharper processes, and a stronger security foundation to support ongoing growth.

Conclusion: security as a competitive edge

Axinom's case is a powerful example of how proactive security investments pay off. With the right testing partner and internal alignment, penetration testing becomes more than risk reduction it becomes a tool to accelerate innovation, earn trust, and lead with confidence.

NEVERHACK

Your Cyber Performance Partner

/CASE_STUDY

Contact us for more

WWW.NEVERHACK.EE

axinom!