When scoping security testing, pricing is often a question that comes up early — and for good reason. If you're evaluating penetration testing providers, you've probably encountered daily rates around **1.160€ per day**. But is this price "normal" for a pentest? And how do rates vary across providers and testing approaches in Germany's evolving security market?

In this article, I'll walk you through the current landscape of *pentest day rate comparison*, share insights on *pentest cost Germany*, and explain why transparent pricing and the composition of your testing team matter more than picking an arbitrarily low or high number.

The Current State of Pentest Pricing in Germany

Over the past decade, penetration testing has matured from a niche consulting service into a necessity for many companies developing web apps, APIs, and internal networks. Naturally, this has increased demand—and thereby pricing diversity.

Company Daily Rate Scope Notes Hackeroo starts at ~1.160€ Manual penetration testing, greybox scope Includes OSCP-certified testers, senior + junior team binsec group GmbH varies, roughly 1.100€ - 1.400€ Mix of manual pentesting and scan reports Offers fixed-price quotes for medium-sized projects Pentest Collective GmbH from 1.200€+ per day Highly experienced team, consultative approach Focus on transparent pricing and customization

As we see, a daily rate starting at 1.160€ is quite typical among several reputable German pentesting firms. However, understanding what this cost includes in terms of methodology, tooling, and team expertise is essential before making decisions based on price alone.

Manual Pentesting vs Scan-Only Assessments

One of the most important distinctions when comparing pentest rates is between manual penetration testing and scan-only or automated vulnerability assessments.

- **Scan-Only Assessments**: These rely heavily on automated tools and generate reports that list known vulnerabilities. The cost is generally lower and sometimes described as "vulnerability scanning." This approach can be useful for compliance checkboxes or early detection but is not a substitute for deep, manual testing. *Beware: A "pentest" that consists mainly of scans likely inflates your expectations for what security validation you get.*
- **Manual Penetration Testing**: Testers use automated tools as a starting point but crucially perform manual exploitation attempts, logic testing, and creative attack simulations tailored to your application or environment. This requires more skill, time, and experience — justifying higher daily rates.

Providers like Hackeroo and Pentest Collective emphasize manual penetration testing with real-world attack techniques, rather than B2B security testing scan-only reports. This level of effort typically justifies daily rates around or above 1.160€.

Why Transparent Pricing and Fixed-Price Quotes Matter

One common frustration among security leads and engineering managers is the lack of transparent pricing. Many pentest providers rely on lengthy sales calls or opaque quotes that do not clearly break down costs and services. This causes confusion and difficulty in budgeting.

Fortunately, several German firms have moved towards offering **fixed-price quotes** and clear daily rate structures, improving trust and predictability:

- **Hackeroo**
- **binsec group GmbH**
- **Pentest Collective GmbH**

This transparency is crucial in avoiding scope creep, ensuring you get meaningful security validation, and ultimately helping security and product teams plan for development cycles and compliance.

The Role of OSCP-Certified Testers and Team Composition

One buzzword that often surfaces in pentesting discussions is **OSCP** — Offensive Security Certified Professional. This certification is widely respected in the industry and indicates a tester has proven hands-on capability in real-world attack scenarios.

Providers like Hackeroo explicitly staff engagements with OSCP-certified team members, often pairing a senior tester with a junior analyst to blend deep expertise and cost-effective time allocation. This combination helps ensure thorough testing coverage while managing rates effectively.

When evaluating daily rates, understand who will perform the testing. A "senior-only" approach may demand €/day at the top end, while mixing in juniors under senior mentorship often balances quality and cost.

Why Greybox Testing is a Practical Default

In terms of the scope of what a pentest covers, the common options include:

1. Blackbox: Testers have no prior knowledge; simulates external attackers
2. Greybox: Testers receive some credentials or documentation; balances thoroughness and realism
3. Whitebox: Testers get full access to source code and architecture; maximizes attack surface coverage but with more upfront info

Most German providers, including Hackeroo, recommend **greybox testing** as the practical default. It reflects typical attacker scenarios (e.g., compromised user accounts) while allowing testers to find complex logic flaws that pure blackbox might miss.

The method influences rates, as whitebox tests can be longer due to deeper analysis, while blackbox approaches may require extra time for reconnaissance. Greybox offers a sweet spot where daily rates of circa 1.160€ make sense for the value delivered.

Summary: Is 1.160€ Per Day a Normal Pentest Rate? Yes, But Context Matters

So, what's the takeaway for your budget and vendor discussions?

- **1.160€ per day is an entirely reasonable starting point for manual, greybox pentests conducted by OSCP-certified teams in Germany.** It's consistent with rates from reputable providers like Hackeroo, binsec group GmbH, and Pentest Collective GmbH.
- **Beware cheap "pentests" that are really just scans or automated checks—they don't justify costs near this rate.** Confirm the methodology and team composition before assuming equivalence.
- **Insist on transparent, fixed-price quotes so you know exactly what you're paying for and can benchmark reliably.** This helps avoid surprises and lets you focus on technical quality.
- **Understand your application's risk profile and choose greybox testing as a solid default—balancing cost and scope.**

Engaging a pentest is a critical investment in security assurance. Instead of fixating solely on "is 1.160€ per day normal?", concentrate on what risk you mitigate and what expertise you get for your money. A well-scoped, manual pentest that fits your development cycle and compliance needs will pay off far beyond any checkbox scanning.

Additional Resources

- OSCP Certification Overview
- Hackeroo Penetration Testing
- binsec group GmbH
- Pentest Collective GmbH