Case Study:

Assessing Human Risk With Penetration Testing

This case study looks at how a company, frustrated with repetitive pen test results, collaborated with experts for a deeper security review. Were their annual pen tests giving them a false sense of security? Follow them on their journey to uncovering more realistic security insights.

Cyber Security isn't just about the latest tech: It's about your people too.

Challenges

A UK tech company was questioning the effectiveness of their routine penetration tests against real-world attacks. Despite high-tech defences like advanced firewalls and encryption, they realised a key component was overlooked: **the cyber awareness of their team.**

As phishing scams surged, it became evident that employee awareness was under-tested. They realised that their penetration testing efforts had concentrated on their security strategy's strongest aspect: their high-tech defences. Meanwhile, the human element, a hacker's favoured entry point, had been overlooked.

Solution

They decided it was time to revamp their penetration testing approach to get a true understanding of their security posture. They knew their servers were fortresses, but what about the people running them?

They needed a test that mirrored a real hacker's approach — targeting not just systems, but people too.

At a Glance

The Company: A UK-based tech company

Team Size: 150 employees

Established in: 2012

The Statistics

The UK's National Cyber Security Centre (NCSC) reports that an overwhelming **70% of cyber breaches are due to phishing attacks.**

Hackers exploit our daily routines and instincts, manipulating us into making mistakes. It's a stark reminder of the crucial role our day-to-day decisions have in keeping our online world secure.

Real attackers don't just use software glitches, they use psychology..

The annual security review raised a crucial question: **were their penetration tests providing realistic security insights?** While their servers were well-protected, the **human factor needed assessment too.** They needed a test that mirrored actual hacker tactics, targeting both systems and people.

The Decision: 1

The team agreed: it was time to see how they'd fare in a real cyber-attack. They needed a test that would go beyond the usual checks — one that would probe both their infrastructure and their team.

Partner Selection: 2

The partnership with Equilibrium was motivated by our reputation for realistic attack simulations. They were looking for a firm who could mimic real-life attacker paths, and test their team's reactions to targeted social engineering tactics.

The Set up: 3

We started with social media, quietly identifying key IT staff, especially those with admin privileges. We crafted personalised phishing emails — a realistic touch that could trick even the wary.

The Attack: 4

The emails went out. Some were regular updates, others looked like important messages from the bosses. Simultaneously, our team of penetration testers began probing their external defences, looking for any cracks.

The Breach: 5

A few clicks — that's all it took. Some of their staff fell for the phishing emails. Soon, the testers had admin credentials. They started exploring the internal network, moving towards the company's critical data

The Discovery: 6

Our penetration team found their way to sensitive information — the "network crown jewels." They encountered few internal barriers. What was more alarming: no detection systems caught their movements.

Unlocking Real World Insights

Discover the **response** from Equilibrium's penetration testing

They learned that in Cyber Security, falling into a "business as usual" mindset can be risky. To truly secure your systems, you need to think like a hacker, uncovering vulnerabilities which could expose your business. By partnering with Equilibrium, they probed their security gaps using social engineering and penetration tests, uncovering clear insights into both tech and human vulnerabilities.

Facing Reality:

When presenting the findings, the room was tense. "You have strong external defences, but internally, and in your team's awareness, there are gaps."

Response Plan:

We provided a detailed plan. It included targeted awareness training for staff, particularly around phishing. We also suggested strengthening internal security layers and improving detection systems.

Taking Action:

They implemented the plan, bolstering internal defences, and implementing new detection protocols. The team embraced the mantra of 'Always double-check your emails.'

Continuous Journey:

They understood that Cyber Security isn't a one-time fix. They planned regular tests, updates, and training. The mindset shifted from feeling secure to staying vigilant.

Equilibrium Security & Penetration Testing

Building a More Secure Future

Getting The Balance Right

They found that whilst it's essential to guard against external threats, it's just as important to ensure internal security is solid. They needed a balanced approach to achieve optimal security.

Importance of Employee Awareness

Their success stemmed in part from their commitment to staff awareness training, particularly regarding phishing attacks. They realised regularly training their team on the latest risks and best practice greatly reduced the chance of hackers exploiting human behaviour.

Cultural Shift Towards Vigilance

Their experience highlights the need to bolster internal security, educate your team on threats, and maintain constant vigilance. It's a strong reminder that varying security tactics is essential to uncover and address vulnerabilities we might overlook by relying solely on the same approaches.

Don't Take Our Word For It: Check Out Our 5 Star Google Reviews ★★★★★

Get Your Free Penetration Test Quote Today

T: 0121 663 0055

E: enquiries@equilibrium-security.co.uk