FORMATION TECH

CASE STUDY · INTERNAL PENETRATION TEST

Uncovering Hidden Risk

A leading UK recruitment organisation operating at scale across multiple locations, with a sophisticated internal IT environment supporting a large user base. Like many enterprises of its size, the business holds significant volumes of sensitive personal and commercial data, making the integrity of its internal network a critical priority.

IN THIS STORY

Following the success of automated external penetration testing, Formation Tech were engaged to extend the programme into the customer's internal network. The engagement uncovered a forgotten test switch on the core network, protected only by a basic administrative password, a single overlooked device that, if compromised, would have exposed the business far more widely than expected.

01

CHALLENGES

Validating the Internal Network

The customer had already secured its external-facing infrastructure, deploying automated penetration testing for regular visibility into new and existing threats. Having seen its value, **attention naturally turned to the internal network.**

The business went in with a high degree of confidence. Its internal environment was considered well secured, the result of years of investment, capable people and established processes. The question was less whether they were exposed and more **whether anything had been quietly overlooked over time.**

That confidence is common among well-run organisations, and it is exactly why internal testing matters. What it surfaces is rarely a headline misconfiguration, but forgotten infrastructure that rarely sits at the top of an IT team's radar. **Once authenticated, an attacker exploiting these "invisible" devices can travel a great deal further** than the business realises.

02

SOLUTION

A Thorough Test of the Internal Environment

Formation Tech extended their penetration testing programme into the customer's internal network, applying the same rigorous methodology that had already delivered value externally. The objective was straightforward: **validate the assumption that the internal environment was secure, and surface anything that had been missed.**

During the process, the testing identified a test switch installed in the customer's lab that had inadvertently ended up on the core network, protected only by a very basic administrative password. In isolation it looked unremarkable, **the kind of device set up for a short-term purpose and then forgotten**, but its position on the core network made it materially significant.

Once compromised, it would have exposed the network far more widely than the business expected. Formation Tech reported the finding, validated the impact with the customer, and supported the steps required to remediate the exposure and bring the device under proper control.

03

OUTCOMES

Visibility Where It Matters Most

The engagement delivered exactly what internal penetration testing is designed to: **independent validation, and the surfacing of overlooked exposure** that is almost impossible to identify from inside the team managing the environment. A single forgotten switch with a weak password was all it would have taken to give an attacker meaningful lateral access, and resolving it closed down a significant route into the business.

More broadly, it shows **why regular internal penetration testing has become essential for organisations of any scale**, particularly those operating across multiple sites or grown through acquisition. New devices, inherited infrastructure, temporary lab setups and IoT estates all change the internal attack surface in ways that are easy to lose track of.

Testing on a regular cadence is what lets businesses understand when those changes happen, rather than discovering them after a breach.

> For the customer, the outcome has been twofold: a specific, material risk addressed and resolved, and a broader programme of internal visibility that complements their existing external testing, on both sides of the perimeter.

RESULTS AT A GLANCE

Critical

Forgotten device identified on the core network

Increased Visibility

Full perimeter and internal visibility now in place

Ongoing Testing

Internal penetration testing cadence established

100%

Compromised device remediated