illume

highlighting cyber risk

Case Study

illume cyber-security tests help another law firm remain secure

Crown Commercial Service Supplier

CYBER SCHEME

CSP

GLOBAL CYBER ALLIANCE

Member CyberExchange

A SUCCESSFUL LAW FIRM FOLLOWING ITS OWN PATH

Our client is an award-winning law firm, employing over 200 people, across offices in the West Midlands. Over its long history, the firm has developed a reputation for consistently delivering exceptional standards of legal service to businesses and individuals.

Bringing together specialists in many disciplines, the firm provides genuine value by striving to constantly think from a client's point of view, understanding their issues and responding to their particular needs.

Like all law firms, our client recognises it will continue to grow by attracting and nurturing the best people to meet clients' changing needs, but always with an eye on security and confidentiality.

REMOTE, RELAXED AND VULNERABLE

Recognising the growing threat of cyber-crime, the firm invests significant resources in securing the firm's infrastructure against hackers and undertake regular penetration testing to uncover potential vulnerabilities in the systems.

Understanding the need for a comprehensive penetration test, given the challenge presented by accommodating so many remote workers in 2020, the firm's IT Director sought recommendations for a specialist cyber-security firm to undertake the work.

highlighting
cyber risk

Although a relative newcomer, Illume is already building an enviable reputation for delivering a range of digital security services that make it easy for organisations to protect against cyber-attacks.

Following a scoping call to understand the firm's requirements, Illume undertook an external penetration test to assess the infrastructure accessible via the internet, this is usually firewalls, VPN's etc., but the comprehensive test covers far more.

The test is designed to assess the risk of a malicious actor identifying those services and attempting to leverage any vulnerabilities in them. The tests performed depend on what is exposed by the business, which has changed significantly for most with the move to Cloud and adoption of O365.

Respecting the client's confidentiality, the tests performed will only be discussed in general terms. The test will have included, but not necessarily limited to the following:

Open Source Intelligence Gathering - It is surprising what can be found on the internet by those who know where to look and what to look for. The tester will have attempted to find out as much about the business and the staff as possible, with relevant finds, such as reused passwords, or metadata stored in documents, recorded.

Social Engineering - The most common entry point into an organisation is through the use of targeted phishing attacks. All external tests include a phishing attack, though clients can choose to opt-out, designed to discover an entry point. If found, the Illume team will typically use social engineering tactics to try and obtain credentials from users within the firm.

> *Penetration testing of systems and infrastructure is a valuable exercise to identify vulnerabilities, which can go unnoticed by in-house IT teams, that have a lot of other responsibilities. The external assessment demonstrates the reality of what they believe to be the situation and delivers peace of mind for insurers and stakeholders.*
>
> *The phishing element of the assessment helps expose the weakest link in any system, the people. By highlighting the tactics used and the risks associated with phishing emails, we can educate a workforce and help them to understand that cyber security is everyone's responsibility.*
>
> **Daniel Woolgar**
> Managing Director, Illume

Service and Vulnerability Identification - Port and service scans are used to identify the service that is listening on the address. That service is then checked for known vulnerabilities. There are over 131,000 ports on an address, so this process usually takes a couple of hours to complete.

Exploitation - An experienced Illume tester will verify the presence of a vulnerability by attempting to exploit it, in much the same way that a malicious attacker might. Often vulnerabilities can be 'chained' together to give the tester a greater level of access. This process also weeds out false positives ensuring an accurate report.

EXPERIENCE MAKES IT REAL

Whilst some security checks can be automated, to replicate the intensity of an attack a business will suffer on an almost daily basis from malicious actors, requires experience and detailed knowledge of the challenges faced by particular sectors, like those providing legal services.

Understanding the failures that have compromised law firms around the world in recent years, allows the Illume team to tailor the tests and use language familiar to those working within law firms, which can make it far easier to phish the unwary.

RESULTS IN REAL TIME

Apart from experience in the sector, one major reason for choosing Illume was the promise of the results of the test being delivered through an innovative portal developed in-house by the Illume team almost immediately, rather than waiting weeks for a pdf report.

Not only does the dashboard deliver results, it allows clients to observe the test as it happens, showing the testers' findings in near real time and highlighting the attack vector being used. The client can also interact directly with the testers, if they have any questions.

All penetration test data is fed straight into the dashboard, providing a single view for any identified vulnerabilities on the network. This ensures work to resolve any issues can begin immediately, with advice form the Illume team if necessary to address more challenging problems.

The portal allows clients to assign specific vulnerabilities to colleagues to be resolved as soon as they are identified, ensuring no vulnerabilities are missed or forgotten about, which could leave the firm open to an attack. If Illume find a vulnerability, chances are so will the cyber-criminals.

> *As a law firm, we recognise the importance of regular penetration testing and chose Illume in part, thanks to their unique portal that allowed us to get involved with the test, as it happened and see the results in near real-time, rather than waiting weeks for a report.*
>
> *Changes in working practices, more Cloud and more remote working have increased the workload on our IT team significantly, so using a specialist like Illume to perform the penetration test makes perfect sense, especially given their experience in the legal sector.*
>
> *Their work post-assessment to help resolve any identified vulnerabilities is a big plus for the service they supply and just instils confidence. We knew we were secure, but we now have the results to prove it.*
>
> **IT Director**
> Top 150 UK law firm

POST ASSESSMENT ACTIONS AND IMPROVEMENTS

Illume leveraged their experience to provide meaningful suggested resolutions, to assist the in-house team to remediate the problems.

The phishing and spear-phishing elements of the assessment, also help the firm identify individuals within their business who responded to the fake emails, not for any disciplinary action, but to understand why the email worked and why they were fooled.

This then allows more focussed training to be rolled out across the firm to reduce the future risk of users being duped by real phishing campaigns. Just one successful attack could deliver untold reputational damage, to say nothing of the immediate financial consequences.

Annual penetration testing is a growing requirement from insurers, as they recognise the increasing threat from cyber-attacks. On a commercial level, they also demonstrate a business understands the importance of identifying and resolving potential risks, which makes them a more attractive partner.

Project Stats

36 Publicly available credentials identified

4 Phishing campaigns

312 Phishing emails sent

When Illume find a vulnerability, the client receives a report to read not a ransom demand to pay.

For reasons of confidentiality, we do not name clients in our case studies, but they are happy to personally endorse the quality of our work. Please contact us for further details. support@illumesecurity.co.uk

illume