

Sunderland Council

“The relationship I have built with Sapphire allows me to place my faith in them and know that the level of service I will receive will match that of my expectations.”

Howard Smith, Information Security Manager, Sunderland Council

About Sunderland Council

The City of Sunderland has a population of just fewer than 300,000 and is the largest city between Edinburgh and Leeds. It is situated on the north east coast of England.

Sunderland Council is one of the most prominent local government authorities in the country, employing over 14500 people. The council has over 5000 users, 3500 of which are desktop or mobile users. To manage this, Sunderland has an IT department staffed with 106 employees. The council's main offices are based at the Civic Centre, Sunderland.

Background

Previously Sunderland Council had commissioned a vulnerability assessment of its network. The individual responsible for initiating this was Howard Smith, then employed as Data Protection Officer, now Information Security Manager. At that point the council had never carried out a vulnerability assessment on either their external or internal networks. Howard saw this as a major concern and immediately set out to test the robustness of the council's infrastructure.

“I immediately saw the need for an assessment of council's network” comments Howard. “Getting an outside organisation in to test the vulnerabilities of the infrastructure, would enable the security team at Sunderland to gauge just how impenetrable their systems were... or not, depending upon the results.”

Howard approached a number of organisations to carry out the test. Four companies submitted their specification documents.

It was a tough call for Howard, however one organisation had the experience and certification the council was looking for and that company was Sapphire.

“The result of the initial assessment highlighted few vulnerabilities.” Howard said “Even though these results were encouraging I realised that to maintain this level of security on the network, testing was going to have to be a regular activity. At the time I did want to continue with further tests but due to work being carried out on the council's infrastructure was unable to do so.”

The Driving Force

Howard implemented many new working practices, one of which is the council gaining ISO27001 certification. Industry best standards such as the new ISO27000 series encourage organisations to take a responsible approach to information security at all levels including that of higher management.

“The number of government agencies and outside organisations the council deal with is phenomenal.” Howard said. “We liaise regularly with social services, the police and NHS. It is of the utmost importance that Sunderland Council offers a high level of assurance to these associated organisations.”

Following the initial assessment in 2002 the council wanted to continue carrying out regular tests. However due to other commitments this is something that was put on the back burner, until Howard reached a point where BS7799 was driving the need to carry out another assessment.



Howard hoped that the vulnerability test carried out would prove that the council's infrastructure was secure and polices and procedures implemented as part of BS7799 were working effectively.

Once again Howard went out to tender for the provisioning of an external vulnerability assessment and finally narrowed down the applicants to three organisations. Howard was looking for two main criteria from the testers: experience and certification.

Having looked through all supporting paperwork Howard once again chose Sapphire over the other security companies in the tendering process.

"The reasons I chose Sapphire were pretty similar to those in 2002" commented Howard. "Firstly, Sapphire was able to provide a number of reference sites, all of which were local government authorities. This gave me confidence in their reliability and sector specific knowledge. Another contributing factor was that the Sapphire security team is CHECK certified and Sapphire itself is qualified to ISO27001. This gave me a high level of confidence in their integrity. I also had first hand experience of their services as we used them back in 2002. Above all trust is crucial to a relationship, many of the suppliers who quoted had not carried out work for Sunderland before, nor were they able to provide the calibre of references Sapphire produced. The relationship I have built with Sapphire over the years allows me to place my faith in them and know that the level of service I will receive will match my expectations."

The Assessment

Sapphire was approached by Sunderland Council to carry out an external vulnerability assessment on their network. Howard Smith, Information Security Manager at Sunderland wanted the assessment to be carried out in as realistic an environment as possible, without jeopardising the functionality of the council's network.

To ensure the test would be as pragmatic as possible only one individual within the council knew the exact dates the assessment would be carried out.

Sapphire was given a time period in which they could test the vulnerabilities of a specified number of IP address.

Howard was adamant that the test needed be as thorough as possible and therefore there was only one limitation applied. At no point was the infrastructure to go down.

The assessment ran for seven days within the given time period; it ran smoothly and, as requested, caused no disruption to Sunderland Council. The assessment highlighted no serious vulnerabilities on the council's network although there were several areas that needed minor improvements.

Out of the range of IP addresses tested only 3 key areas of concern were highlighted. These related largely to one application requiring an upgrade. A higher level of authorised access being applied to one of the anti-virus solutions and further levels of security being applied to the ICMP timestamps.

A low-level vulnerability provides an attacker with network and system information. Overall, Sapphire reported a total of eleven low-level vulnerabilities, nine of which needed the re-configuration of systems and 2 of which required patching. The assessment also highlighted five medium-level areas of concern which related largely to systems needing re-configuration. The definition of a medium risk being a vulnerability that can be combined with at least one other medium vulnerability to compromise the host.



The Benefits

“Sunderland Council achieved four things by commissioning an external vulnerability assessment of its network” said Howard. The test showed Sunderland’s perimeter security structure was safe and working reasonably well. It also pinpointed areas which enabled the council to take further action to rectify the problems. The assessment was comprehensive. This meant Sunderland had no need to carry out further tests.

The project did however prove to higher management the benefits of carrying out vulnerability tests. As a result of which the council are now looking to deploy assessments on their internal network and applications. The assessment assisted the council to meet the criteria required to maintain their BS7799 certification.

The Future

Sunderland Council realises the importance of regular penetration testing. As a result of which it is now part of the organisation’s Information Security Strategy to carry out an assessment of their external networks annually. This is a project that Howard Smith will be driving personally. Following advice from the security team at Sapphire, Howard will be alternating suppliers for any future assessments. The council is also beginning to run assessments on their internal applications.

In the future Howard would like to take the network assessments one step further and test the organisations business continuity plans as well as the defence methods for the infrastructure. During this assessment Howard specifically requested that at no point was Sunderland Council’s network allowed to fail or prevent everyday working. This is however something that Howard is considering doing in the future in a controlled environment.

Testimonials

“Sunderland Council takes a responsible attitude to protecting the information stored on its corporate infrastructure. By building on relationships with trusted partners such as Sapphire the council can share information and continue to raise awareness of information security issues within the organisation. I would fully recommend Sapphire’s penetration testing services to any organisation from either the public or private sectors.”

Howard Smith, Information Security Manager, Sunderland Council



For more information about Sapphire’s vulnerability assessment service please contact <mailto:info@sapphire.net> and quote 'Pen Test' in the subject header.

