Orange
Cyberdefense

Customer stories

One of the largest trade associations in the UK, representing over 1000 companies were keen to find out where they might be vulnerable to improve their security rating.

Customer profile

Industry: Transport
Location: Kent, UK

Solutions provided

- External Penetration Test

Business results

- They can now supply members with a clear demonstration of their compliance in a concise executive summary
- Assistance in the process of achieving Cyber Essentials and ISO 27001 compliance
- Confidence to move forward with compliancy projects including removing an outdated server and vulnerability patching.
- Maintenance of regulatory security compliance.
- Vulnerabilities were found which had not been highlighted before, allowing them to secure their systems.

Background

This organisation is one of the largest trade associations in the UK and represents over 1000 companies with links to delivery and transport including Morrisons, Veolia, FedEx and G4S. They represent the needs of the logistics industry at all levels including campaigning to raise awareness of the freight industry and helping companies stay compliant with the latest regulations.

The challenge

This organisation work with a number of large companies who are increasingly looking for partners and suppliers who share the same level of concern about Cybersecurity. Many customers were asking for Cybersecurity reports to be filled out before signing up with the association. The IT team needed to make sure they could fill in security surveys with confidence, knowing that they had no major vulnerabilities. Some companies even asked to see the results of a Penetration Test so having a clear summary was also important.

The organisations' IT Team were aware of vulnerability scanning technologies online that would allow their customers to test their systems for flaws. They were keen to find out where they might be vulnerable to improve their security rating. They are also working towards a number of accreditations including Cyber Essentials and ISO 27001 and know that a Penetration Testing on their publicly facing systems would help towards the gap analysis for these achievements.

The solution

The Network Manager, established that an up-to-date Penetration Test was needed to assure customers that security was a primary concern. In line with good practice, they looked to move to a different provider to ensure that a different range of tests were used in case new vulnerabilities could be found.

Orange Cyberdefense has reporting that was clear and organised which made our security remediation easier for our team.

Network Manager,
Leading Logistics
Company

As they had worked successfully with Orange Cyberdefense's sales team in the past over the supply of other Cybersecurity products, they knew Orange Cyberdefense had the knowledge and experience to carry out a comprehensive test. The Penetration Testers work completely independently of the account management team so they have a fresh perspective when undertaking a new test.

Orange Cyberdefense's dedicated Penetration Testing team never undertake a project before reviewing the scope of the work to establish what parts of the network need to be tested. They aimed to make this scoping discussion as simple as possible for the customer and because this was a grey box test (where the analyst is given only minimal information about the company before testing begins) the IT team only needed to supply a list of IP addresses. This made the process of setting up the test very staightforward.

The association were in contact with their hosting company before testing began who advised that there were certain shared service IPs they wanted excluded from the test. The Orange Cyberdefense analysts were very conscious of this while the work took place. Orange Cyberdefense Penetration Testers did a full range of tests using the most up to date tools and technology. This included both automated Vulnerability Scanning and manual Penetration Testing. Once the testing was completed in the agreed time scales, reports were compiled that detailed all of the individual vulnerabilities, rated with the standard Common Vulnerability Scanning System (CVSS). CVSS ranks all vulnerabilities as either critical, high, medium or low meaning that companies can address any issues in a systematic way, dealing with the most important vulnerabilities first.

The outcome

The whole test was delivered on time, with no disruption caused to the business which meant the remediation stage could begin. The IT team were keen to address the vulnerabilities in house, so clear and actionable reports from the Orange Cyberdefense Analysts were vital. Orange Cyberdefense were able to identify a critical vulnerability that had not been picked up in earlier tests, which was quickly remediated by the IT team. The comprehensiveness of the results allowed them to resolve or patch the vulnerabilities in order to fix them. The results of Orange Cyberdefense's test allowed the organisation to secure their infrastructure from external attacks.

Because of this, their security rating on external scanning sites has increased across the network, which provides visible proof to their members that protection of their data is being taken seriously. Further to this, the executive summaries of vulnerabilities can be given to members to prove that regular Penetration Tests are being undertaken and that their network is secure.

Finally, the tests have allowed the company to maintain their regulatory compliance and highlighting any problems is helping them move towards further certifications including ISO 27001 and Cyber Essentials, a government backed scheme to improve Cybersecurity across all sectors.

About Orange Cyberdefense

In 2019 SecureData UK & SecureLink UK were acquired by Orange Group to be part of Orange Cyberdefense, the Group's expert cybersecurity business unit. Today Orange Cyberdefense is Europe's leading managed security, threat detection and threat intelligence services provider. We help customers anticipate threats, identify risks, protect their IT assets, detect breaches and respond to security incidents. With a 25+ years track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world, we can offer a global protection with local expertise.