DigitalXRAID
CYBER SECURITY EXPERTS

Breast Cancer Now Case Study

BREAST CANCER NOW The research & care charity

Service:
Penetration Testing

caseStudy

How Breast Cancer Now safeguarded its IT infrastructure with regular penetration testing

The Requirement

Breast Cancer Now combines the power of research and support to change the lives and build a brighter future for people affected by breast cancer.

The organisation funds 80 cutting-edge research projects to develop better treatments and prevent and diagnose breast cancer early.

It also leads change in treatments and care and offers trusted health information and specialist nurses, to support those navigating life with breast cancer.

As a best practice measure as part of a drive to continuously improve security, and in line with requirements from its regulators and insurers, Breast Cancer Now wanted to understand what its current security posture was in terms of internal and external infrastructure.

This would ensure that there were no vulnerabilities that could be exploited by a malicious actor.

DigitalXRAID
CYBER SECURITY EXPERTS

Breast Cancer Now Case Study

BREAST CANCER NOW The research & care charity

Service:
Penetration Testing

caseStudy

The Solution

Breast Cancer Now had worked with DigitalXRAID on other security projects, so engaged us to perform regular internal and external infrastructure penetration testing and also pen test some of its web applications, in order to identify any security weaknesses and potential exploitable vulnerabilities.

As a first step, DigitalXRAID's penetration testing consultants assisted Breast Cancer Now with effectively scoping the test. This was to ensure that maximum value would be achieved during the testing time.

DigitalXRAID delivered a thorough penetration testing service in line with the agreed scope. Over several days, the team conducted comprehensive tests which assessed the infrastructure, and determined whether any vulnerabilities existed across the network and applications that could be compromised.

DigitalXRAID used various tools and techniques as part of the penetration test, in line with industry best practice. Testing is performed using an advanced methodology, comprising years of experience.

The team thoroughly reviewed the IT infrastructure as part of the reconnaissance stage, including fingerprinting open ports or potential access points and active scanning techniques.

As a high-level overview of the attack simulation phase, the testers looked at areas such as the versions of software or hardware in use, passive monitoring of the network in internal environments, used active scanning techniques such as port scanning, and investigated identity authentication and authorisation in order to attempt to bypass processes and workflows.

DigitalXRAID
CYBER SECURITY EXPERTS

Breast Cancer Now Case Study

BREAST CANCER NOW The research & care charity

Service:
Penetration Testing

As part of the test, DigitalXRAID's penetration testers also assessed encryption security around the transmission of communication. This included checking for common weaknesses in SSL/TLS configurations and verifying that all sensitive data is securely transferred.

At the end of the testing period, DigitalXRAID supplied a comprehensive report, detailing the methodologies followed and highlighting and categorising any vulnerabilities found into low, medium, high and critical priorities. The report included a risk summary that explained how any vulnerabilities identified could be used by an attacker to affect the business.

caseStudy

"Feedback on the pen test from internal teams here was very positive and communication was responsive. We now have a much deeper visibility on our current security posture.

We're very happy with the reporting, which gave a thorough explanation of the findings and gave us clear solutions for remediation"

Brigid Macdonald, Head of IT, Breast Cancer Now

DigitalXRAID
CYBER SECURITY EXPERTS

Breast Cancer Now Case Study

BREAST CANCER NOW The research & care charity

Service:
Penetration Testing

caseStudy

The Results

Breast Cancer Now has taken steps to ensure its internal and external infrastructure is safeguarded effectively, with regular penetration testing. Even with updates to infrastructure, regular testing ensures that Breast Cancer Now remains secure.

With the results of the test outlined in the final report, alongside recommended remediation steps, Breast Cancer Now has the advantage of proactively addressing any gaps with an action plan, before potential vulnerabilities could be exploited.

Regular pen testing compliments other cybersecurity measures that Breast Cancer Now has taken, including achieving Cyber Essentials Certification and regular vulnerability scanning.

Pen Testing is able to uncover a far deeper level of issues than vulnerability scanning alone can achieve, so this has successfully increased the maturity of Breast Cancer Now's security posture.