CASE STUDY

Higher Education

University tackles cyber security challenges with Wavenet*

Situation

A university invited organisations to quote to carry out a penetration test. The university had put together an initial scope of work stating their expectations for the exercise.

Universities have thousands of student users who require access to their network, in addition to hundreds of employees and support functions requiring varying levels of access, and multiple and remote users. This means they are faced with a huge task when it comes to their cyber security. Their networks need to be accessible for long hours and, because of the nature of their student user-base, unusual activity is hard to pinpoint.

As part of the initial project, Wavenet* conducted some research into the university and found data containing vital contact information for 3000 users, including phone numbers and email addresses, accessible to anyone from the internet. This was alarming for our tester to discover, knowing the implications from an access perspective; however, it is not unusual for large organisations.

The university chose Wavenet to carry out their penetration test based on the quotation and Wavenet's long standing security credentials. Having worked with a number of UK universities to help improve their cyber security meant we had a greater understanding of their network complexity and user needs.

At a glance

Industry:
Higher Education

Solutions/services taken:
Penetration Testing

Length of relationship:
5 years

*The initial engagement was with ECSC, acquired by Daisy in 2023. Daisy was acquired by Wavenet in 2024.

Solution

Penetration tests are carried out by an accredited security tester according to a scope defined by the customer. We helped the university to further refine the scope of their testing project and developed an understanding of their specific network complexities.

We carried out further investigation, using the previously acquired contact details to conduct a brute force attack against multiple external portals. The sheer number of usernames already available gave our tester a high chance of gaining access; our Wavenet tester gained access easily to an account where the privileges were then escalated. Full control of the university network was then gained, including access to over 100,000 hashed passwords. The hashes were put through a password cracking process and within the allocated testing time over 60,000 were cracked.

Had this easily exploitable vulnerability been identified by a malicious attacker rather than in the course of a penetration test commissioned by the university, the resulting reputational damages, financial losses and fines imposed by regulatory bodies could have been catastrophic. The remediation activity required to reduce the risk of this happening included:

- A review of information storage, process and access rights
- Putting protective measures in place regarding access to contact information
- Educating users on the use of more complex passwords
- Re-testing to ensure remediation activities have been effective

Wavenet continues to work with the university to improve their cyber security posture. By developing a relationship with this customer we help to ensure the most effective use of budget and prioritise areas of improvement.

Benefits

- Customer gained insight into their security vulnerabilities, empowering them to take action
- Helps to maintain contractual obligations and standards such as payment card industry data security standard (PCI DSS) and ISO 27001