Your Partner For Success

Securing Your Business for the Future

SECURING THE UNIVERSITY NETWORK

Client's Challenge

Universities have been targets for computer hacking since computers first arrived on campuses. Universities have a unique challenge in protecting their digital assets. One challenge facing universities is a large number of hackers reside on the university network. There are many reasons why students can be perfect hackers: their curiosity and high-levels of intelligence; plenty of motivation and an abundance of free time; and the university network generally has an open usage policy, limited staff, and is designed to promote creativity and openness not restriction and control.

One university client challenged TBG Security to identify weaknesses specific to their Student Information System and their Financial Aid System. These systems were all third party developed applications. Management was suspicious of these applications due to specific lack of security guidance during deployment and subsequent maintenance. There was a general "feeling" that these vendors were focused purely on functionality and not necessarily security.

TBG Security Solution

Our approach for assessing security of our university clients has been to take on the role of a hacker. Our hacker role puts us directly on the network; we take on the identity of the would-be attacker. We deploy a number of tools that are well known in hacker circles and we have leveraged these tools and coupled them with our knowledge of hacking techniques.

These applications were assessed from several different standpoints. The Student Information System had both internal (thick client) and external (browser based) components. We assessed each component both as an unauthorized user and an authenticated user. When authenticated, we took on the identity of users with various levels of access. This approach allows us to go beyond testing just authentication, but also allows us to test authorization controls.

When assessing thick client components of a client / server application, we look closely at 4 distinct areas: security of the client, security of the network, security of the server and security of the database. We will look carefully at how each component of the application interacts with the environment overall.

TBG understands, as do the hackers, the old security maxim: "You are only as secure as your weakest link".

Impact on client's business

We identified very serious weaknesses in each of the systems we reviewed including:

- Flaws in the web portal of the Student Information System which allowed for complete compromise of the supposedly protected database.
- We found ways for authenticated users (students) to subvert security controls and change their grades.
- We identified weaknesses in the design of the Financial Aid System which could allow any user on the network to directly access the backend database and pilfer or alter important financial data.

By engaging TBG Security, our client positioned themselves to be in a proactive situation with regards to identified vulnerabilities on their critical systems. As a trusted advisor, we worked closely with the management team and the 3rd party vendors to assist them in remediating their security flaws. By giving our client the necessary leverage to negotiate with their vendors, they were in a much better position to dictate the terms and conditions of their agreements and to insist that certain level of security be provided and maintained by their vendors.