Protecting Web Assets in Higher Education

(Challenges, and How to Overcome Them)

Introduction

Colleges and universities are faced with increasing and diverse threats to their web assets[1].

Sensitive information is increasingly targeted and stolen, exacting a high price from individuals to whom the information belongs as well as the learning institution entrusted to protect it. Online services can be brought down, defaced, and flooded with spam.

Institutions of higher learning face a double challenge:

- The growing sophistication of these threats are rendering traditional defences inadequate.
- Traditional defenses are not well suited for higher ed's unique IT environment.

This paper examines these challenges, and describes one solution designed to address them.

Advanced Persistent Threats

As financial and other incentives to steal private information grow, so does the sophistication of those attempting to steal it[2]. Advanced persistent threats (APTs) describe a new class of criminals that target specific institutions with a level of skills, patience, and ingenuity not seen before.

No longer satisfied with pre-packaged scripts that attempt to infiltrate a web site, hackers are now actively exploring their targets for weaknesses. Once a weakness is uncovered, it is often exploited to discover other ones, until, finally, the hackers manage to gain access to the coveted information.

Traditional approaches to securing online assets, while still important, are insufficient to stop APTs:

Installing patches regularly is insufficient. Keeping the system up-to-date is important, as it reduces its exposure to known vulnerabilities. However, a fast-moving APT may be able to leverage the delay from the time a vulnerability is made public and the time that a patch is made available and finally gets applied. And although rare, an APT may be exploiting a vulnerability that the public is not yet aware of.

[1] EdTech, EDUCAUSE 2014: Cyberattacks Are a Growing Problem for Higher Education
[2] SilliconANGLE, SQL Injection Attacks Rise as Hackers Go for the Money

Preventing known attacks is insufficient. Many "next generation" firewalls rely on a signature-based IPS. In many ways similar to an anti-virus, this approach works well for blocking publicly known attacks. However, this provides very little protection against APTs that can exploit the various third-party apps and modules whose vulnerabilities have not been publicly exposed. Critically, in-house developed services, which are of interest only to your institution, remain dangerously exposed.

Best coding practices are probably the best available defences from various application-level attacks that APTs may attempt, and should be encouraged. This requires a massive investment by the institution in keeping updated about the latest attacks and the best ways to defend against them, communicating this to all the development teams, and going back to secure the entire existing codebase. However, even if this can be perfectly achieved, any use of third-party apps and modules can leave the institution exposed.

Software and hardware solutions themselves have vulnerabilities. Security devices and software packages are continuously probed for vulnerabilities by hackers. Once discovered, these vulnerabilities must be immediately patched. If patching is a manual process, it can get delayed. IT staff may be busy with other important work, or there may be a policy of avoiding infrastructure updates during peak periods. Whatever the reason, as long as the security product is unpatched, the web assets remain vulnerable.

Threats are continuously evolving. As new classes of threats are discovered, security solutions need to be substantially modified. Vendors who operate with a purchase / upgrade business model may have an incentive to offer such modifications as a version upgrade for their products. Even if such an upgrade is made quickly available, making the decision to purchase and deploy the upgrade can take months for a large institution. Meanwhile, the security product used is not up to par.

Unintended Disclosures

Between 2005 and 2014, about 30% of data breaches in higher ed were the result of unintended disclosures.[3] Under these circumstances, a hacker doesn't need to work very hard to gain access to sensitive information, as it is made readily available.

Unintended disclosures on the web can include:

Posting sensitive information on a web site. Not all legitimate users of online services may be aware of the many concerns regarding sensitive information. If any post sensitive information online, a data breach becomes almost inevitable.

[3] EDUCAUSE. Data Breaches in Higher Education, page 6.

Passwords in the clear. There are many ways to handle use authentication online. Some readily-available ways to password-protect websites are not secure, with passwords flowing through the network unencrypted. These passwords can be harvested by hackers and used to gain illegitimate access to not only that service, but other services and information that are better protected as well.

Inadvertently publishing materials. Sensitive information can be uploaded to websites and remain hidden there unless it is explicitly linked to from other pages. The user who uploaded the information may have done so inadvertently and may be unaware that it is even there. However, a hacker that systematically traverses the site can gain access to this information.

Denial of Service

The reliable delivery of online services is a top priority for any institution. To guard from hardware and power failures, many institutions have invested in load balancing and failover solutions. Traditional application delivery solutions are not designed to prevent a denial of service attack from bringing down a service.

Modern techniques have dramatically increased the risk of denial of service (DOS) attacks for the following reasons:

Scripts are readily available, requiring little or no technical skills to operate. Anyone can download them and use them to target a web site of their choice.

Low-resource, high-impact techniques. The cost of launching an effective attack is now very low. Today, a hacker wielding very simple tools can tie up your server's resources, effectively bringing down a significantly more powerful web site.

A Complicated IT Environment

Colleges and universities strive in an atmosphere of collaboration and innovation. Faculty and staff introduce new online services at a rapid pace. Over the years, this has produced a highly complicated IT environment, one with unique challenges to keep it secure.

Dozens if not hundreds of web sites. The sheer number of online services that higher ed institutions offer its students, faculty, and staff is impressive. Whether developed by a third party or in-house, each may have unique vulnerabilities that require protection.

Decentralized development makes enforcing security best practices a greater challenge. New services may be brought online with little notice, giving the information security team little time to test it for vulnerabilities.

Diverse platforms, tools, and development languages. Higher ed institutions typically deploy a wide range of technologies, requiring the security staff to be up to date with a large spectrum of vulnerabilities.

Limited Resources. Security teams across higher ed are reporting that they are understaffed, typically for lack of budget.[4] Many modern web application firewalls have a steep up-front cost, ongoing support fees, and non-obvious upgrade cycles. But even if an institution can ignore these financial considerations, many web application firewalls, to be effective, require a prohibitive amount of the security team's time to set up, review logs, and maintain a security policy.

A Proposed Solution for Higher Education

In order to overcome these challenges, a new approach to securing higher ed's web assets is required. Hermetric's *eduWAF* is a secure application delivery solution designed with these considerations in mind. Unlike traditional approaches, Hermetric's *eduWAF* has three main components that build on and strengthen one another:

- **A reverse proxy** that scans and protects your network in real time.
- **Monthly reports** that help your information security team gain insights about, and take proactive steps to neutralize, dangerous vulnerabilities.
- **A professional security team** that monitors the reverse proxy and tailors a security policy for each protected web site.

These three components are designed to maximize each other's potential and work in tandem to secure your networks.

Hermetric's *eduWAF* can help fend off APTs by offering:

- **Real-time protection** from online hackers. Deployed between your web servers and the rest of the world, *eduWAF* can identify and block hackers before they reach your web sites.
- **Tailored, positive security policies** for each web application. Employing modern big-data analysis techniques, Hermetric can identify and differentiate legitimate traffic from hacking attempts. Online services are protected not only from known vulnerabilities,

[4] SANS Institute. Higher Education: Open and Secure?, pages 16-17

but also from zero-day attacks and vulnerabilities which may be unique to your institution.
- **Hassle-free updates and upgrades**. Hermetric ensures that its platforms are kept up to date with the latest exploit patterns, bug fixes, and security engines, all while ensuring that traffic continues to flow to the web servers without disruptions.
- **Vulnerability reports that expose broken pages**, which can become gateways to future intrusion attempts.

Unintended disclosures can be discovered and neutralized. Hermetric's monthly vulnerability reports expose:

- Publicly posted sensitive information, including social security and credit card numbers.
- Unencrypted passwords flowing through the networks.
- Services vulnerable to systematic traversal.

Denial of service attacks can be stopped. Hermetric's *eduWAF* includes:

- Real-time application-aware inspections that identify and block attempts to hog your server's resources.
- Vulnerability reports that expose slow-to-respond pages, which can become targets of future DOS attacks.
- Real-time packet drops of unrelated network-level communication.

Hermetric's *eduWAF* is designed to fit well in higher ed's complicated IT environment by offering:

- **Security as a service,** requiring no upfront costs or lengthy commitments.
- **Technology-agnostic protection** that can secure all your web applications.
- **A scalable solution** that can be deployed incrementally, giving your institution the control over which web sites Hermetric protects.
- **A hassle-free solution** that can be deployed on your VMware infrastructure in about an hour. Your security team will be spared from tedious log reviews and from the time-consuming task of tailoring a security policy for each web site. Hermetric's security team will do that for you!

Some additional benefits for deploying Hermetric's *eduWAF* include:

- **Integrated load-balancing and failover capability**. Hermetric's reverse-proxy can serve multiple web-server clusters reliably and securely. Should a power failure bring down one instance, another one will quickly assume all relevant IP addresses and continue to deliver your web services.
- **Reduced spam**. Hermetric identifies and blocks spambots that attempt to flood your web services with spam.

Hermetric offers an innovative new approach to securing web assets in higher education. To learn more, visit hermetric.com.