SECURING OPEN ACCESS

How higher education institutions can guarantee open networks and still keep data safe

June 2011

SPONSORED BY

BARRACUDA NETWORKS

1105 MEDIA Education Group

Higher education institutions can guarantee open networks and still keep data safe. The strategy simply requires a new way of thinking, and a commitment to flexibility that can help bolster defenses for the long-haul.

Introduction

Scan the headlines of security magazines these days and it seems as if hackers are taking on networks like never before. A perfect storm of dynamic Web applications (such as AJAX), social networking and mobile employees has created vulnerabilities these evildoers have jumped to exploit.

While the vast majority of these attacks are geared toward individual users and corporate networks, the world of higher education (with its characteristic open access networks), is not immune. Privacy Rights Clearinghouse, a non-profit consumer organization that tracks how technology affects personal privacy, reported there were 68 data breaches at educational institutions in 2010, up from the number of breaches in 2009. Perhaps the worst of the bunch: The December 2010 data breach at Ohio State University that potentially compromised personal data on 760,000 users and cost the institution $4 million.

Despite the overwhelming number of attacks, data security does not have to overwhelm education technologists any longer. With this in mind, the goals of this white paper are to:

- Describe current strategies behind data security breaches
- Identify common misconceptions about data security among academic technologists
- Analyze the challenges inherent in the higher education environment
- Provide technologists with a better understanding of where threats are coming from
- Offer suggestions for how academic technologists can protect their networks from these threats down the road.

Higher education institutions can guarantee open networks and still keep data safe. The strategy simply requires a new way of thinking, and a commitment to flexibility that can help bolster defenses for the long-haul.

The top four breaches of today

According to Paul Judge, chief research officer for Barracuda Networks, a security vendor based in Campbell, Calif., data security breaches in today's day and age generally fall into four basic categories.

Malicious Javascripts

This type of data security breach is by far the most prevalent, and comes in a variety of flavors. One, dubbed "malvertising," works through Web site ads. A hacker writes a program that he or she places behind an advertisement or other page on a perfectly legitimate Web site somewhere on the Internet. Users don't even have to click or hover over the ad to activate the malicious code; all they have to do is stop by. In many cases, these threats reside on perfectly trusted servers—servers that have been compromised at some time in the past.

Search engine malware

This strategy is a spin off malicious Javascripts—only instead of tricking users with a bad script on an otherwise harmless Web site, the approach feeds (the technical term is "poisons") search engines with malicious links. To get the biggest bang for their bucks, hackers stuff search engines with these links based on search topics that are trending (think "LeBron James," or "adjustable-height desks.") According to Judge, one in five search topics and one in 1,000 search results lead to malware of some kind.

Social attacks

In recent months, hackers also have exploited the social nature of social networking sites such as Facebook and Twitter. In the Facebook environment, attacks are designed to look like photo tags, chats and seemingly innocuous apps (a recent one promised users two free tickets on Southwest airlines). Another common iteration: a phenomenon known as "Likejacking," whereby a hacker makes it look as if a trusted confidante has "liked" something that's actually a malicious script. In the Twitter environment, attacks appear in the form of fake links.

Web Exploit Kits

Finally, exploit kits are ready-made tools designed to help hackers attack vulnerable software (and sometimes hardware) components. Anyone (including run-of-the-mill college students) can buy them. Anyone (again, including students) can use them. Most kits come

As hackers continue to evolve their strategies, so, too, must network administrators in every industry bolster their defenses and stay on top of what's coming next.

with dashboards that track the havoc a particular kit is wreaking. Perhaps most alarmingly, many kits are available on file-sharing sites—a kit named Blackhole was found on a number of these sites earlier this spring.

Identifying misconceptions in higher education

As hackers continue to evolve their strategies, so, too, must network administrators in every industry bolster their defenses and stay on top of what's coming next. Those tasks, however, can be tough. Half of the problem usually is perception; network administrators underestimate threats and their vulnerability to them. The world of higher education is plagued by three common misconceptions.

Misconception No. 1: Not me

With statistics like the ones from Ohio State, you'd think academic technologists would be downright paranoid about protecting their networks. In reality, however, it's precisely the opposite—most academic technologists think their networks aren't a priority for hackers, and that data security threats therefore usually are overblown. This comprises the biggest current misconception about data security in higher education as a whole; academic technologists simply don't think the bad news will happen to them.

Misconception No. 2: Who's hacking

Academic technologists—and much of the general public, actually—also have misconceptions about who's actually doing the hacking and breaching data security. Most people think all hackers are pros; indeed, in some cases, the masterminds of these threats are individuals who have crafted scripts or malware to hack hundreds of other networks and likely will use the same scripts and malware to hack hundreds more. But in many other cases, the hackers are students themselves—amateurs who are using nothing but a prefabricated Web exploit kit to wreak havoc. In these latter cases, snuffing out threats is as simple as staying on top of which exploit kits can foil certain set-ups. With the right kind of technology aid, it actually isn't that difficult.

Misconception No. 3: Open means open

The third and final misconception surrounds the very nature of academic networks. For generations, higher education leaders have strived to make access to their resources as open as possible. In the world of IT, this means that network administrators have been tasked with keeping access to online resources as open as possible. Many of these administrators are so concerned with keeping access open that they've opted out of providing any security for users. Here, the misconception is fundamental—just because a network is open doesn't mean it can't also be secure.

The challenges

In addition to these misconceptions, academic technologists face a number of specific challenges in handling data security and managing threats.

Challenge No. 1: Mixed technologies are messy

The first challenge relates to this notion of an open network. Many schools have addressed concerns in this area by building two separate networks—a relatively open one for students and a more closed and traditionally secure system in place for faculty and administration. On paper, the solution works wonderfully. But in practice, deploying mixed technologies often results in coverage gaps and difficult administration and reporting as well as other problems

Challenge No. 2: Candy to hackers

Whether they realize it or not, another problem for academic technologists is that higher education institution networks are big targets for hackers who've done the whole hacking thing before. From a hacker's perspective, universities provide two of the most important ingredients for a "successful job." The ingredients: An open line and fast servers. These tools are like candy to hackers; with them, the evildoers can do almost anything. (Of course

Traditionally, most security strategies have been deployed at the network edge. Today, however the very best vendor monitoring solutions sit in the middle—always between the user and the web.

hackers also appreciate higher education networks for the preponderance of users who have credit cards at their disposal.)

Challenge No. 3: Educating users

Finally, users need a better idea of what they're up against. Attackers have gotten much more sophisticated in the department of social engineering (this is a fancy term for the way hackers now make threats look innocuous). Because these attacks change every day, it's imperative for users to stay abreast of potential threats on the horizon and educate users how to deal with them. Some schools do this masterfully, tipping users at the mere moment of a threat. Other schools don't prepare at all, opting to react only after the problems have sprouted.

The solution

Solving the problems of phishing, malicious Javascripts, worms, and other Web-based threats requires technologists to think differently about the way they scan traffic. Currently, most schools are focused on inbound stuff: Stopping spam as it comes over the transom or blocking known threats at the firewall. While this strategy does indeed keep some data safe, there is a better way: Protecting a network by searching both inbound and outbound traffic for known threats. This approach takes nothing for granted; assuming that at some point, even the most legitimate Web sites could become compromised and host malicious software. In short, it insures safety on both sides of the data equation.

Like most higher education security strategies, this particular version of Web security hails from the corporate world, and had its roots in a science previously known as Web filtering. In the olden days, corporate network administrators would use the technology to monitor user behaviors and dictate (based on threat levels) where the users could and couldn't surf. Gradually, protecting traffic—i.e., only looking for specific threats—became part of the game. Initially, higher education IT leaders were skeptical of the technology because they didn't want to even run the risk of monitoring user network behavior. Over the last few years, however, academic technologists have identified the dichotomy, and have warmed to the idea of protecting as a compromise.

Think of this approach like a home security system. If a homeowner needed to protect his house from being broken into, he could hire a security service to protect the house by keeping tabs on potential threats around windows and doors. The homeowner doesn't need the security service to monitor or record every single event of the day; he or she just needs protection. Web security works the same way—it's yet hands-off, ensuring security in a non-invasive way.

Traditionally, most security strategies have been deployed at the network edge. Today, however the very best vendor monitoring solutions sit in the middle—always between the user and the web. Some sit on appliances; others work in the cloud. These solutions serve as gateways for data on two separate occasions, scanning all traffic first as it comes in from the Internet, and again before it leaves and goes back out into the world. All of the scanning happens in seconds, which means users don't know the technology is even there unless network administrators have to protect them from something. With this in mind—especially from the user perspective—the access to the network stays open.

Barracuda's take

A handful of new solutions have come onto the market in recent months to grapple with these problems head-on. One such solution is the Barracuda Web Security *Flex*.

This solution works for a variety of reasons. First, the service exists predominantly in a cloud proxy, essentially meaning traffic is scanned virtually while it crosses the DMZ. Next, the technology also can be administered from on-network appliances when needed for local enforcement. Finally, Barracuda Web Security *Flex* offers remote and mobile filtering as well, a feature that enables academic technologists to stay on top of student users who connect through Smartphones and faculty and staff members who frequently connect remotely. Specifically, Barracuda Web Security *Flex* delivers:

- Anti-virus signatures that update continuously for fast response to new and known threats

- Advanced heuristics block unknown Web viruses and spyware
- AJAX-aware analysis detects malicious Web apps and script-based attacks
- HTTP behavior analysis and intrusion detection blocks botnet communication, spyware and rogue anti-virus
- Advanced Anti-Spam Intelligence protects against blended email and Web threats
- Web filtering and application control for Web apps like IM, VoIP, P2P file sharing and streaming media
- Advanced policy management for Web filtering like file and content type control, data leak prevention and restrictions on bandwidth and time

What's more, this particular technology offers centralized multi-site management and reporting, and that there is unlimited deployment flexibility, meaning it's scalable for just about anything. That's where the flex part of the name comes into play. Barracuda Web Security *Flex* offers a number of deployment options to ensure total coverage. For deployments inside a firewall, gateway appliances—hardware or virtual—integrate with enterprise directory services, like Active Directory, to control user and group-based policies. A pure SaaS Web security service provides malware protection and Web filtering without directory service integration for remote locations and home-based users. Software agents extend malware protection and Web filtering to mobile user laptops. Administrators can select any combination of deployment options to satisfy their exact Web security needs.

Web Application Security

Another solution is the Barracuda Web Application Firewall. Think of any application in an educational institution and you will realize that it runs on the web. Traditional network firewalls do an excellent job of protecting ports and protocols but unfortunately cannot perform the deep inspection required to protect web traffic and prevent data leakage. Hackers know this better than anyone else and as a result the vast major of attacks today occur at the web application layer. With the number of readily available web exploit kits automating the vulnerability discovery process, it is not a matter of if but a matter of when an attack will occur against your web assets.

The Barracuda Web Application Firewall is a complete and powerful security solution for Web applications and Web sites. The Barracuda Web Application Firewall provides protection against hackers leveraging protocol or application vulnerabilities to instigate data theft, denial of service or defacement of your Web site. Beyond security, it provides load balancing and application acceleration capabilities that enhance delivery, reliability, and scalability of any web application.

Conclusion

Between malicious Javascripts, search engine malware, social attacks and the rise of kits to leverage Web exploits, the threats of data breaches impact every industry in today's computing environment. Academic technologists face particular challenges; because they operate in an environment that prides itself on open network access, administrators must provide seamless protection and ensure that protection is undetectable to users. A number of solutions exist to provide this protection; the best of them scan traffic as it comes and as it goes, protecting user data by monitoring it for threats repeatedly inside the firewall. As threats continue to evolve, the solutions also must be flexible, and must be able to react dynamically to new challenges as they arise. Hackers will stop at nothing to obtain data; network administrators—and the technologies they adopt—must be just as relentless in order to stay ahead.

BARRACUDA NETWORKS

About Us

About Campus Technology

The only monthly publication focusing exclusively on the use of technology across all areas of higher education, Campus Technology provides in-depth coverage of specific technologies and their implementations, including wireless networks and mobile devices; enterprise resource planning; eLearning and course management systems; 'smart classroom' technologies; telecom, Web, and security solutions—all the important issues and trends for campus IT decision makers.

Targeting administrators, IT professionals and tech-savvy faculty, Campus Technology provides direction, analysis and detailed coverage of emerging technologies to assist technology leaders in their specific roles on campus.

To learn more, visit www.campustechnology.com.

About T.H.E. Journal

THE Journal is dedicated to informing and educating K-12 senior-level district and school administrators, technologists, and tech-savvy educators within districts, schools, and classrooms to improve and advance the learning process through the use of technology. Launched in 1972, THE Journal was the first magazine to cover education technology.

THE Journal's franchise consists of the monthly print magazine (which is also available in digital format), the web site thejournal.com, six newsletters (THE News Update, T.H.E. Journal Insider, IT Trends, THE SmartClassroom, and School Security), and targeted list rental opportunities.

With a distribution of 100,000 circulation, T.H.E. Journal is the leading resource for administrative, technical, and academic technology leaders in K-12 education.

To learn more, visit www.thejournal.com

About Barracuda Networks

Barracuda Networks Inc. combines premises-based gateways and software, virtual appliances, cloud services, and sophisticated remote support to deliver comprehensive content security, data protection and application delivery solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

More than 130,000 organizations protect their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions.

To learn more, visit www.barracudanetworks.com

the JOURNAL

CAMPUS TECHNOLOGY

9201 Oakdale Ave.
Suite 101
Chatsworth, CA 91311

(818) 814-5277

BARRACUDA NETWORKS

Barracuda Networks, Inc.
3175 Winchester Blvd
Campbell, California 95008
United States

(408) 342-5400