GAMECHANGER

RETHINKING HOW TECHNOLOGY IS USED IN EDUCATION

LOCK DOWN YOUR NETWORK

THIS TOP-SHELF LIST OF SECURITY PRACTICES AND PROTOCOLS IS A MUST-READ FOR PROPERLY SECURING YOUR NETWORK.

IF YOU'RE ASSESSING and tightening your institution's security profile, a good place to start is the CIS Critical Security Controls. The National Security Agency (NSA) created this list of 20 top security recommendations in 2008. Over time, it has been revised and updated by a consortium of U.S. and international agencies, including both government and private industry. The Center for Internet Security (CIS) currently manages the list and its contents.

The Cybersecurity Law Institute calls the CIS Critical Security Controls list "the de facto yardstick by which corporate security programs can be measured." See the complete list for more information. Here are short descriptions of the first five items on the list:

1: Inventory all Devices

The prioritized list starts with this important security control. This is clearly the No. 1 step you can take to improve your security posture. Do a full inventory of all authorized and unauthorized devices on your networks. This step is foundational and ranks "very high" for attack mitigation. There are a handful of asset discovery and vulnerability management tools commonly used for this step. This greatly reduces the ability of attackers to find and exploit unauthorized and unprotected systems.

2: Inventory all Software

Your institution may already have software change management, whitelisting and vulnerability management tools installed. If not, this is a good time to do so. The idea is to first gather information on installed software and patches. Then make that data available to security practitioners, along with tools that can calculate any changes in the data. Software inventory tools, CIS says, should "cover each of the operating system types in use, including servers, workstations and laptops." The software should also track the underlying version of the operating system; as well as installed applications, including software type, version number, and patch level.

3: Secure Configurations for Mobile Devices

This is a challenging security control on college campuses. The Bring Your Own Device (BYOD) movement has become the rule of the land. And most students tend to carry multiple devices at once. College campuses are inundated with new devices at the beginning of each semester. To prevent such abuses as installing unauthorized software, the CIS recommends limiting installations and limiting administrative privileges to "a very few users who have both the knowledge necessary to administer the operating system, and a business need to modify [the underlying configuration.]"

4: Continually Assess and Remediate Vulnerabilities

For institutions of higher education, this control entails regularly running automated vulnerability scanning tools against all systems, and quickly moving to fix vulnerabilities. Software that compares data from vulnerability scans to outside threat lists can help by generating an alert when it uncovers items on the threat list, such as malicious registry keys, IP addresses and domain names.

5: Control Admin Privileges

Two common types of attacks begin with enticing users to open a malicious e-mail, attachment or file or to visit a malicious web site. Then the attackers are often able to crack an administrative password to gain access to a target machine. To guard against this, CIS recommends, minimizing administrative privileges. Focus auditing on administrative privileged functions, the report further recommends, "and monitor for anomalous behavior."

To help implement and integrate the 20 security controls on the CIS list, consider a single integrated platform for overall security that can ingest, organize and analyze the data from silos across campus. Set up the software to verify incoming data from various programs, execute additional security requirements as needed, and support the activities of your IT security team. When all the data in your organization is indexed and available, security teams can instantly compare and analyze disparate data sources, making it easier to protect your organization.

LEVERAGE MACHINE DATA FOR SECURITY

shutterstock.com

BECAUSE OF ITS open nature, campus networks and infrastructure are at a high risk for attack. Recent statistics show the potential for abuse is growing. Higher education is no longer immune to serious attacks. A security incident strains network resources, consumes large amounts of the IT staff time, and can be embarrassing and costly to your institution.

Security experts counsel that good security doesn't happen in one place and through one tool. A secure network employs layers of protection across the system, and uses different approaches to block attackers where possible, detect intrusions quickly, and encrypt data to prevent loss if attackers do gain entry.

Given that, an essential component of your security strategy is an overall platform to help implement and organize security policies throughout the system. Your security teams need the ability to index, search and analyze data from across campus. By combining IT data with data from other departments, colleges, and "silos," you can gain deeper insights into software and hardware distribution, events, policies and performance. You can also significantly improve your security posture.

That sort of sophisticated platform must collect data from disparate sources, including the financial system, the student information and registration systems, the LMS, campus networks and web servers, remote sensors, mobile and online learning applications, legacy applications, application servers and structured databases. Centralizing all this data into a single console will provide unparalleled insight into the entire infrastructure and help expose any potential problems.

Monitor the Machine

This includes collecting and monitoring "machine data." This term refers to the large volumes of data generated automatically across campus via sources such as log files, web site monitoring tools, mobile devices, and embedded sensors located on campus. Because of its sheer volume, it can be a challenge to monitor machine data. However, it is immensely valuable in revealing security and compliance breaches because you can continually scan for anomalies across the entire institution.

For example, in order to break down traditional data silos within its data center, a large university in Ohio is correlating data from multiple systems. The university's network infrastructure generates huge amounts of machine data from more than 55,000 students across 14 colleges. To help reach into the many data silos within its datacenter, the institution is using software that helps analyze complex events from many software systems across its campuses. In the process, it is not only keeping university data safe, but also improving network performance.

At a medical college in upstate New York, using a software platform to index and analyze different data types has reduced the university's incident investigation to minutes instead of hours. Proactive searches of incoming data head off any issues on a routine basis. This also reduces downtime. The security solution has had a direct impact on the bottom line, making incident response an order of magnitude faster and more effective.

Using machine data and a software solution that can read and interpret that data, along with the metrics, reports and dashboards to present the findings, your IT department can harness that data to ensure security and compliance, detect and manage network abuse, and enhance campus services. Correlating machine data across a wide variety of sources can help detect patterns of abusive activity as they occur, instead of after the fact.

GAMECHANGER

RETHINKING HOW TECHNOLOGY IS USED IN EDUCATION

RAISE YOUR SECURITY PROFILE

VISIBILITY AND REAL-TIME INSIGHTS ARE KEYS TO ENSURING A ROBUST SECURITY POSTURE.

TODAY'S HIGHER EDUCATION landscape is changing. Universities and colleges remain focused on enrollment and retention, but face increased competition and tightening budgets. Many universities have essentially become small cities that aim to provide their students with a fully connected and secure experience. As each semester begins, thousands of students converge on campus carrying multiple devices ranging from laptops to tablets to mobile phones. With this reality, ensuring the security of campus networks is one of the critical challenges faced by higher education institutions.

While commercial entities can limit access to their networks and control how those networks are used, colleges and universities don't have that luxury. Schools must adhere to the needs of their students, making it much more difficult to educate and manage users, set and enforce universal policies, and keep diverse networks secure.

Despite growing awareness on college campuses about security issues, huge challenges remain including a lack of standardization in university IT departments. Some institutions have a centralized IT department, while others have individual IT groups for each department or school. These departmental IT silos often are more difficult to manage. The constant flow of new users and unregulated devices makes securing campus networks increasingly difficult. Universities need to give students easy access to the network, create a positive user experience, and ensure their campus environment is secure.

What Campus Networks Need Today

Campuses need a comprehensive solution that provides visibility into their complex environment to maintain network security. Every user, device and activities on the network generate data. This *machine data* offers tremendous value, whether it is for the security group, or any other network management or operations center. Real-time analysis of this data will not only improve security, it can also give schools insights into student behavior, so they can provide better services to them moving forward.

Splunk software offers higher education a comprehensive platform that can deliver powerful insights by combining and analyzing university data from every imaginable source – registration software, financial systems, student information and learning management systems, web services, mobile apps, remote sensors and network activity. Rather than dealing with silos of information, Splunk centralizes data collection and aggregation without the overhead of traditional data stores. Providing university security and IT leaders with this "single pane-of-glass" perspective enables usage patterns, potential vulnerabilities, malicious threats, and general trends to be detected in real time so university leaders can make informed decisions.

Splunk offers the capabilities universities need to break down what's happening across their "small city" environments to better protect and serve students. Collecting machine data and correlating it across a wide variety of sources is critical to reliable network security. Intelligent analytics can shed light on who is accessing campus networks, what and how they are accessing, as well as help institutions identify unauthorized or 'hidden' devices.

Imagine an institution-wide system that can ensure security and compliance throughout the campus, detect network abuse instantly, and reveal ways to enhance the institution's IT services to better serve students. Universities can achieve this by better managing, analyzing and protecting campus systems and networks, thereby creating an enhanced environment for recruiting and retaining today's fully connected student.