aruba
a Hewlett Packard Enterprise company

AT A GLANCE

MODERNIZING CYBERSECURITY IN HIGHER EDUCATION

Every individual, organization and industry including higher education can be a cyberattack target. Educause, the largest community of IT leaders and professionals in higher education, listed "information security strategy" as the #1 most urgent issue to address for the last four years[1]. While general and industry specific cybersecurity reports can give us insight into threat trends and what threat vectors to pay most attention to, threats can come from anywhere anytime. Let's look at ways to stop cybercriminals as early as possible ideally before they gain access and definitely before they do any real damage to a university[2].

BROAD ATTACK SURFACE

University network infrastructures are complex and are driven primarily by the need for always-on, anytime and anywhere access – all in support of student learning and their university experience. With 15+ years of delivering secure, high performance networks to higher education institutions, Aruba understands the unique cybersecurity challenges associated with more open to the public yet secure networks, tech savvy students, students and faculty connecting a wide range of personal devices and unsecured IoT devices, the need for collaboration, technology enabled learning, securing research, institutional and student IP that is increasingly a target of cybercriminals, and more. All this widens the attack surface and makes the infrastructure more difficult to secure.

CLOSING THE GAPS

Although education institutions are increasing investments in cybersecurity, recent breach statistics suggest there are opportunities for improvement to stay ahead of threats. Most traditional Security solutions focus on securing the perimeter by detecting known attacks and malware by their patterns or signatures. Yet, never before seen threats, mutated threats and advanced targeted attacks, can often bypass these types of traditional solutions.

Let's investigate how modern security solutions from Aruba can help education institutions better:

[1] Educause 2019 Top 10 IT Issues
[2] Wired: The worst cybersecurity breaches of 2018 so far
[3] Moody's Investor Service, IBM Security
[4] 2018 Education Cybersecurity Report

- Gain visibility into everything connected to both wired and wireless networks
- Ensure that the appropriate IT access policies are applied to users and devices
- Detect and investigate attacks by malicious, negligent and compromised insiders

101 confirmed data disclosures 2017 at U.S. universities, up from just 15 in 2014[3]

- IBM Security

Alarmingly, out of 17 industries in the U.S., Education comes last in terms of total cybersecurity. This should be a cause for serious concern for the education industry as a whole.

Cyberattack incidents include:

- Phishing attacks and network breaches resulting in the disclosure of personal data
- Ransomware attacks
- Denial-of-service attacks
- Other cyber incidents resulting in school disruptions and unauthorized disclosures

- 2018 Education Cybersecurity Report[4]

SECURE INFRASTRUCTURE

For over 15 years, Aruba has delivered high performance networks that include many built-in security features.

- The newest Wi-Fi certified protocol WPA3™ was co-authored by Aruba experts and delivers a range of security and ease of use features.

- Secure boot delivers anti-tampering features for access points.
- Military grade encryption and VPN ensure traffic is secure.
- The Aruba Policy Enforcement Firewall (PEF) enables user/application visibility and policy enforcement based on user, role, application, device and location.

ACCESS CONTROLS

Security starts with visibility of who and what is connected to your network and what they are doing on the network at all times.

- **Know What is on the Network**
  Today, many IoT devices are built on standard hardware platforms. That can make it extremely difficult to know exactly what is on your network. For example, a security camera and smart thermostat could both be built on the same Linux platform. ClearPass Device Insight uses machine learning to identify devices based on multiple attributes, traffic destination, and communication frequency. Knowing what is on the network is the first step in protecting it.
- **"Zero Trust" Access to the Network**
  Aruba ClearPass NAC (Network Access Control) delivers discovery, profiling, authentication and authorization of users, their devices and IoT devices before letting them on the network or giving them access to IT resources. These pre-admission controls are critical because cybercriminals are adept at quickly advancing and moving laterally within seconds after gaining access to a network.
- **Precise Control of Access to IT Resources and Assets**
  ClearPass provides adaptive, granular policy-based access controls by user, device, role and location, including for applications. These controls ensure that each user, device or IoT only has access to the network and IT resources and assets they are approved for.
- **Intelligent Segmentation**
  Aruba Dynamic Segmentation leverages the Aruba secure infrastructure, PEF and ClearPass Policy Manager to deliver a network edge that securely isolates and separates user and device traffic across wired and wireless networks.

SECURE ON THE INSIDE

Protecting against advanced attacks that are active on the inside of a network is critical.

- **"Adaptive Trust" with Continuous Activity Monitoring**
  Aruba IntroSpect integrated UEBA (User and Entity Behavior Analytics) and NTA (Network Traffic Analysis) uses machine learning and analytics to continuously monitor behavior of users and "entities" (i.e, anything with an IP address such as a user device, server or IoT device) looking for indicators of unusual activity that indicates a gestating attack.
- **Advanced Attack Detection**
  Using a combination of self-learning and trained machine learning models, IntroSpect detects stealthy hidden attacks that traditional perimeter based security solutions have missed.
- **Accelerated Incident Investigation, Prioritization and Response**
  IntroSpect uses "Risk Scoring" to prioritize risk into a single number and comprehensive "Risk Profiles" to dramatically accelerate investigation. Incident response is orchestrated within IntroSpect and/or with third party solutions such as ClearPass, SIEMs and other security solutions.

NEXT STEPS FOR A HEALTHIER SECURITY POSTURE

With advanced access controls and security that addresses hidden attacks from the inside, and interoperability with over 140 multi-vendor network and security solutions, you can rest assured with the visibility and confidence that your security posture is in a much healthier state.

TO LEARN MORE

https://www.arubanetworks.com/solutions/higher-education/

aruba
a Hewlett Packard Enterprise company

AAG_SecurityInHigherEd_SK_093019 a00089536enw