Blog Post

Special Concerns for IT and Cybersecurity in Education

Published
Nov 18, 2020

Written by
John Headley

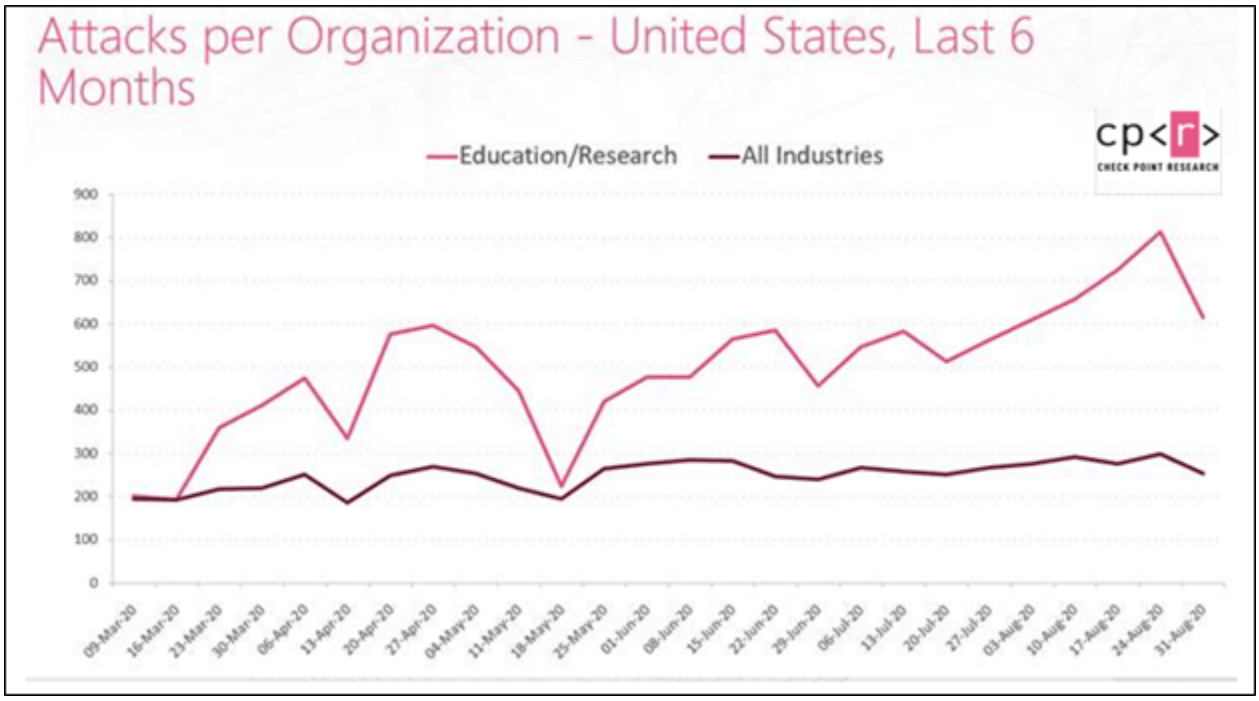
Filed under
Cybersecurity, Education

Even before the pandemic and the dramatic shift in both how students are learning and teachers are teaching, educational institutions have always had unique challenges when it comes to IT and cybersecurity. Not only does an educational institution have to secure a multitude of devices with different permission requirements, but it also has to ensure those devices always have reliable and high-speed access to required school resources.

The shift to work/learn from home has only compounded the challenges for the IT staff, as now these requirements for secure, high speed connectivity have extended to the homes of the students and faculty. This effectively places the majority of users outside of the secure perimeter that the IT staff has worked so hard to build on-prem.

Unsurprisingly with all these challenges, IT staff have a hard time securing the

organization against every possible attack vector, and the education sector continues to be a top target for attacks. In a blog post from September 2020, "researchers at Check Point found that in the last 3 months, there was a surge in hacker interest in topics related to education, research and going back to school." In addition, Microsoft reports Education as the most affected industry for enterprise malware encounters in the last 30 days.



In this blog post, we cover a few special concerns for IT and cybersecurity in education in detail with the recommendation that IT decision makers and their staff perform a self-assessment of their own organization in these areas.

Ransomware

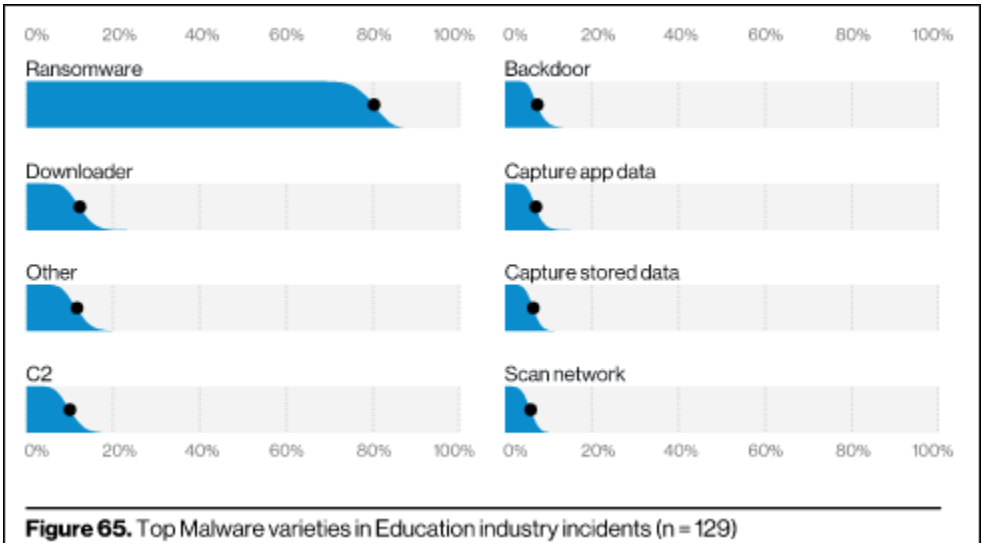


Figure 65. Top Malware varieties in Education industry incidents (n = 129)

According to Verizon's 2020 Data Breach Incident Report, "Ransomware is really taking hold of Education vertical incidents, and has been responsible for 80% of the

Malware-related incidents, up from 48% last year." Edscoop also wrote a recent article in which they listed 9 high profile ransomware attacks in the education sector this year – quite an eye-opening read.

As we discussed in a previous blog post titled How to Prevent Ransomware – A Technical Checklist, a defense in depth approach must be used to protect an organization against ransomware. Note that this is only a technical checklist and it is not exhaustive. Our recommendation here is to go through the checklist, but also to consider having a security assessment performed on your organization against a trusted set of security controls, like NIST 800-53, CIS 7.1, or the ISO 27000-series, as these assess both technical controls as well as administrative controls, such as ensuring you have the correct IT and cybersecurity processes and procedures in place.

Granular Visibility & Control

Granular visibility and control is a cornerstone security capability for all verticals, but the education sector has always had one of the most challenging environments to pull this off properly in because of the wide variety of users. Faculty vs staff vs students, and all at different grade levels that have different access requirements, can leave IT staff pulling their hair out.

Luckily, there are solutions out there that simplify providing granular visibility and control even in these challenging environments. We recommend vetting your security posture for implementation of these concepts below, and if you don't have them all in place, or you aren't sure if you do, then please reach out to us and we'd be glad to discuss your environment in more detail.

Network Access Control

- Only approved devices can connect to the network, whether connecting on-

prem or remote
- Multifactor authentication is implemented at a minimum for remote network access

Granular Policy Enforcement

- Users of all devices are properly identified in real-time and grouped as specifically as possible, e.g. Elementary Students
- Security policies, such as firewall policies and web content filtering policies, are applied per group with the necessary restrictions, whether the users/devices are on-prem or remote
- Security policies, such as firewall policies, are applied based on identified applications (OSI Layer 7), not simply based on ports and protocols (OSI Layers 3 and 4)

Visibility

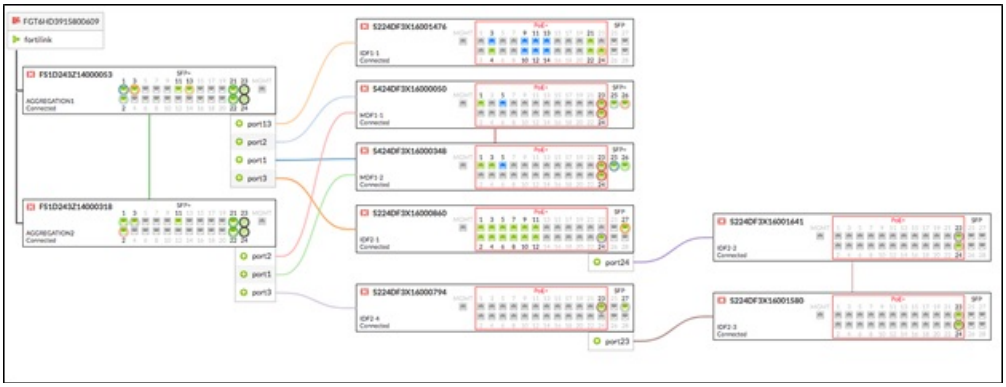
- IT staff has visibility, both past and present, into what users and devices have connected to the network and by what method
- IT staff has visibility, both past and present, into the websites and web applications that the users are accessing and the applications that the users are running on the devices, including cloud applications

High-Speed, Centralized Security & Network Access

Even more true in today's unique learning environment is that education requires high speed network access, and security should not be a bottleneck. The latest generation of network hardware supports unprecedented throughput. On the LAN access side, WiFi 6 APs (802.11ax) have been released along with new "multigigabit" switches to support them, which sport 2.5/5/10 Gbps Ethernet connections.

LAN core switches now come standard with 10/25/40/100 Gbps ports, and firewalls with the same port density and speed are replacing legacy core switches in some environments. Even without venturing into chassis-based firewalls, single boxes can reach numbers of 1.2Tbps of firewall throughput and 240 million concurrent sessions, facilitating internal network segmentation and the same granular visibility and control for both north-south and east-west traffic. This is especially important for large educational institutions like school districts with a centralized firewall topology.

In addition to secure devices that support the ever-growing demand for bandwidth, management of the switches, APs, firewalls, and other infrastructure to support this goal should be painless. IT staff have a lot on their plate and the management complexity of devices can lead to a lack of standardization, misconfiguration, and ultimately a data breach.



We recommend evaluating if your current network and security infrastructure is performing up to the mark for the new demands placed upon the organization this year. Your IT staff may be spending valuable time in managing disparate and isolated infrastructure. Cost-effective solutions are available that centralize management of switches, APs, and even firewalls into one on-prem or cloud dashboard, providing a single pane of glass visibility and control into your IT infrastructure.

VPLS, a Trusted Partner in Education

VPLS has a proven track record of success within the education vertical, such as our data center migration to the VPLS Cloud for El Segundo Unified School District. Whether you want to dive deeper into the special concerns we discussed above, or you have other IT or cybersecurity items on your 2021 agenda, please don't hesitate to reach out to us and we'd be happy to provide a free consultation.

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

More from this Author

PREVIOUS
Evocative (now VPLS) Ranks 13th on the Fastest-Gr...

NEXT
VPLS's Hawaii Team Bridges Services and Support...

If you enjoyed this article, you'll probably like:

5 Reasons SOC-as-a-Service Features Help You

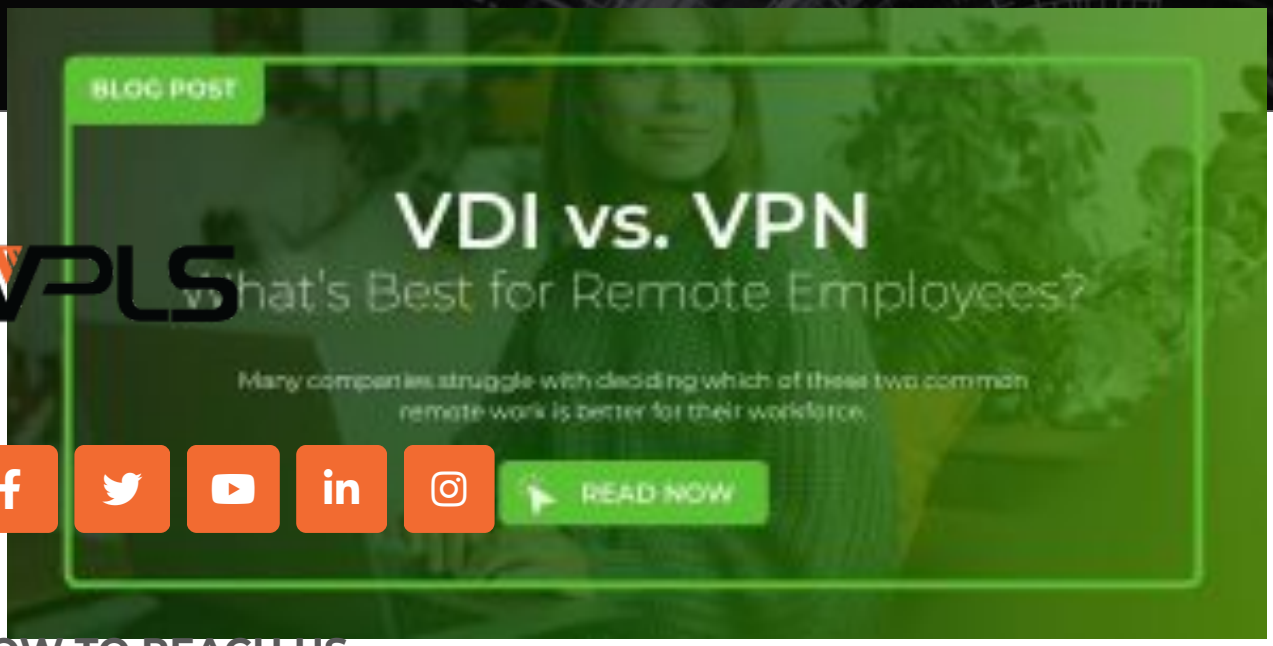
March 29, 2022

Read More »

What Is SOC-as-a-Service?

March 28, 2022

Read More »



VDI vs. VPN: What's Best for Remote Employees?

March 28, 2022

Read More »

HOW TO REACH US

Corporate Headquarters

600 West 7th Street, Suite 510
Los Angeles, CA 90017

24/7/365 Customer Service

+1 (888) 365-2656

support@vpls.com

Sales Inquiries
+1 (888) 365-2656
sales@vpls.com

WHAT WE DO

Cloud
Hosting
Colocation
Network Services
Managed Services
Professional Services
VAR

WHO WE SERVE

Financial Services
Healthcare and Life Sciences
Media & Entertainment
Telecom
Startup
Enterprise
Public Sector