Radware Solutions for Education

Education Concerns and Challenges

Educational institutions have changed the way they operate and teach. Virtual classes are now the norm, causing an increase in network bandwidth. Online content, applications and services are more exposed and vulnerable to compromise. Educational institutions have seen a growth in DDoS attacks that take their networks offline, particularly during scheduled testing sessions, and increases in application attacks that compromise student and faculty PII. Since cybersecurity is typically not an area of expertise, educational institutions value automated and managed DDoS protection and application protection services.

Radware's 2019-2020 Global Application and Network Security Report provides insight into the cybersecurity threats and challenges specific to the education vertical and summarizes perspectives from education security professionals, including business concerns, the types of attacks experienced and their impact, and trends in attack landscape and threats. Educational institutions are concerned about their service online availability, protecting sensitive data and their lack of expertise and resources to manage cybersecurity protection.

Staying Open for Business

In a post-pandemic world, educational institutions depend upon their websites and online services more than ever. Networks and applications must be available 24x7 to allow students and faculty to access remote classes, resources and content. Educational institution respondents to the aforementioned survey reported they are challenged by malware and bots, socially engineered attacks (including phishing), and distributed denial-of-service (DDoS) attacks.

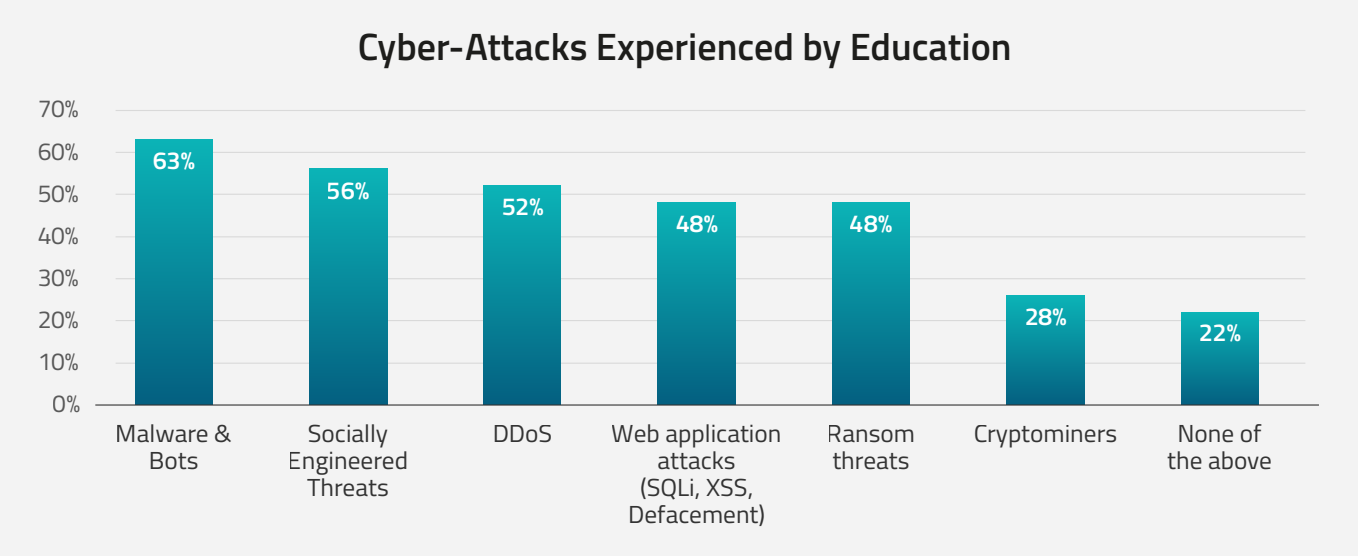

Figure 1: Types of attacks experienced[1]

1 2019-2020 Global Application and Network Security Report

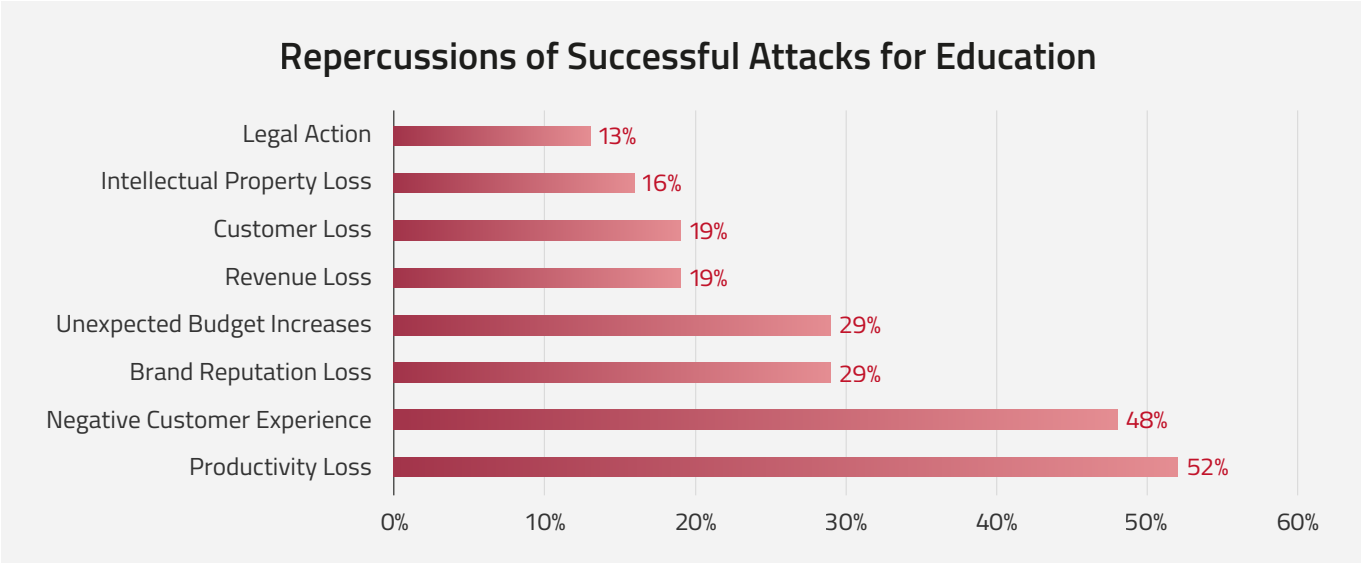

Figure 2: Repercussions of successful attacks[2]

Because educational institutions are dependent on applications, it comes as no surprise that application vulnerabilities were identified as the top threat (34%) concerning education IT managers. Students and faculty require ease of use and security of their applications/online services to be on par with standards set by Google, Amazon and Netflix

Protecting Sensitive Data

Remote learning has presented cybercriminals with new opportunities. This move has opened the door for different points of attack that most schools are not set up to support. "With more teachers and students online, particularly if they're doing it from less controlled environments outside of the school, the attack surface of the school community is increased," says Doug Levin, founder and president of EdTech Strategies, which runs the K–12 Cybersecurity Resource Center[3].

According to Levin, there have been at least 1,180 publicly disclosed cyber incidents nationally since 2016. These incidents, including phishing attacks, data breaches, ransomware attacks and denial-of-service attacks, have more than doubled from 122 in 2018 to 348 in 2019, with 408 incidents reported in 2020[4]. One possible explanation is that hackers are targeting the valuable PII available in schools and universities. "There are bad guys who are targeting [schools] because they've become successful," Levin said[5].

For a long time, school districts believed that they didn't have anything bad actors would find worthy of taking — which is incorrect. "They don't necessarily translate the concept of data into value," says Amy McLaughlin, cybersecurity project director for Consortium for School Networking[6].

Educational institutions have expedited moving applications and data to the public cloud for easier access, to improve the user experience and reduce costs, but now have less control and visibility to manage and secure cloud-based applications. Seventy-two percent rely on their public cloud provider to secure their cloud applications. One-third of respondents reported credential threats as the top cloud environment issue followed by web and application intrusion[7].

2 2019-2020 Global Application and Network Security Report

3 https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon

4 "State of K-12 Cybersecurity: 2020 Year in Review," Douglas A. Levin, March 10, 2021

5 https://www.edweek.org/leadership/coronavirus-compounds-k-12-cybersecurity-problems-5-areas-to-watch/2020/03

6 https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon

7 2019-2020 Global Application and Network Security Report

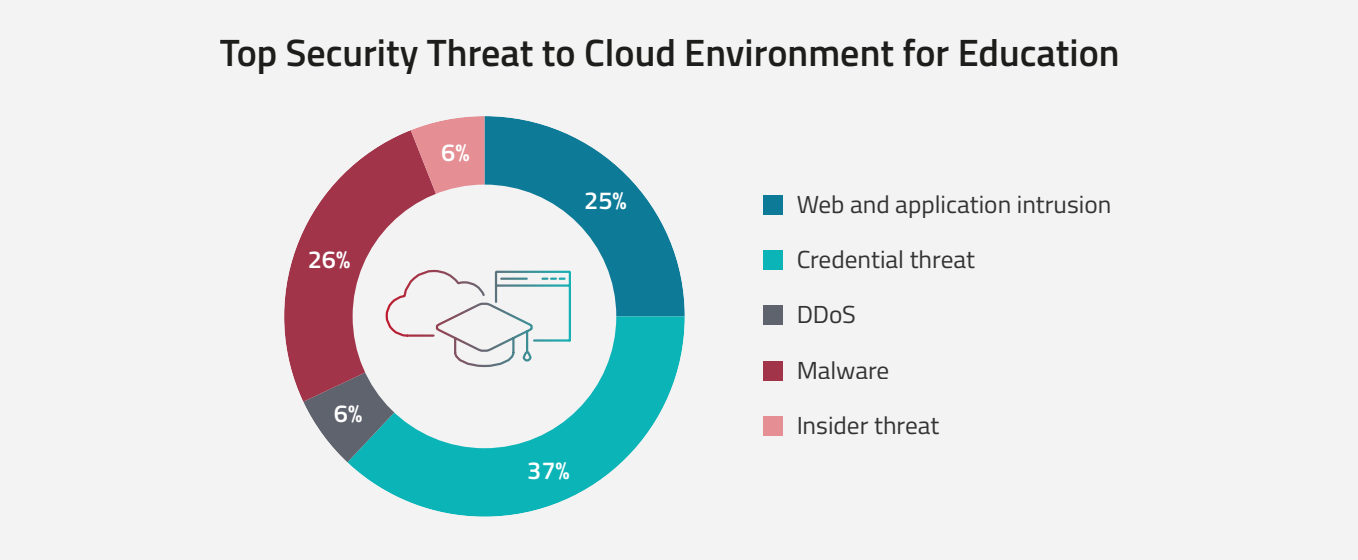

Figure 3. Top security threats to Education cloud environment[8]

Schools and higher education institutions have to comply with evolving regulations and standards, such as PCI and General Data Protection Regulation (GDPR). Encryption protocols are required to secure student transactions, but attacks using encryption are also a concern. Visibility was identified as a growing issue by 46% of respondents, who said that they don't know if they have experienced SSL- or TLS-based attacks on encrypted traffic, according to the 2019-2020 Global Application and Network Security Report

Lack of Expertise and Resources to Handle Complex Threats

Keeping digital assets secure is critical, but it has become more difficult given the increasing sophistication and size of attacks. "Many school districts lack the resources needed to build a strong cybersecurity program," says Linnette Attai, founder and president of PlayWell, a compliance consulting firm, and project director for Consortium for School Networking's privacy initiative and trusted learning environment program[9].

"In many school systems, you don't even have a full-time employee who is dedicated to cybersecurity," Attai says. "Oftentimes, you have someone who is also responsible for the technology or responsible for privacy." This resource challenge also comes with a knowledge and experience gap. Some districts don't have employees who have the expertise to effectively manage cybersecurity and develop engaging and ongoing training for the rest of the school or district[10].

8 2019-2020 Global Application and Network Security Report

9 https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon

10 https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon

Solution Summary — What You Should Consider

Educational institutions face many operational and security challenges. Radware has more than 20 years of experience leveraging cybersecurity research to provide solutions that solve business and technology challenges. Radware solutions have the industry's most expansive set of compliance certifications, including PCI, HIPAA, GDPR and advanced ISO regulations, to address data security in the cloud, including application and malware protection and encrypted traffic inspection.

For concerns with staying in business, Radware offers fully managed behavioral-based attack mitigation services in the cloud, which protect against volumetric, application and multivector attacks. These include keyless SSL attack mitigation that defends against encrypted attacks without impacting legitimate traffic. Radware's application delivery controller (ADC) ensures availability and disaster recovery for local and globally dispersed applications while providing a scalable architecture and automation across multiple heterogeneous environments.

To protect sensitive data as well as mission-critical web applications and APIs, Radware's cloud-based web application firewall (WAF) solution uses a positive security model and machine learning algorithms to provide adaptive defense against the OWASP Top 10 and other threats. Radware's cloud WAF integrates with Radware's Bot Manager, which provides precise bot mitigation and management.

For security and control over assets in multiple public cloud environments, Radware's Cloud Native Protector Service provides one solution to identify exposed assets and remove excessive permissions, detect misconfiguration issues and detect and defend against data breaches.

To assist with resources and expertise, Radware's attack mitigation and WAF solutions use machine learning, real-time signature creation and auto-policy generation to automate the attack protection life cycle to shorten time to mitigation by automatically mitigating attacks.

Radware's Emergency Response Team (ERT) offers a fully managed network and application security service 24x7, which includes immediate response, onboarding, consulting, remote management and reporting. The ERT offers threat intelligence subscriptions designed to provide actionable real-time data for immediate protection against active suspicious attacks and attackers.

Case Study

This Midwest school system was experiencing DDoS attacks from students eight months out of its nine-month school year. It was losing federal education funding because it couldn't administer required testing. The school's one-person IT department was overwhelmed trying to handle these attacks, and its ISP provider could only black hole both good and bad traffic to stop the attacks.

The competition proposed a standard solution that didn't solve the school's problem: either always-on or on-demand DDoS protection.

Radware was chosen for offering an affordable, flexible solution of always-on cloud DDoS service for the school's critical eight-month testing period with on-demand protection for the remainder of the school year. The school solved its attack and budget problem and has been a positive reference for Radware's capabilities with other businesses and educational institutions.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.