EDSCOOP

Why university networks face heightened cyber-risks

The Internet of Things is poised to change our lives for all time in a wide range of different ways. According to a study conducted by Intel, the total number of devices and Internet-connected objects that make up the IoT will increase from two billion in 2006 to 200 billion by as soon as 2020.

This growth, unfortunately, also leads directly into one of the major challenges that the Internet of Things will bring with it: cybersecurity. And it's one that the education sector needs to pay attention to in particular.

The top three most targeted areas for cyber-hackers are the financial services industry, general businesses and education, according to the Identity Theft Resource Center.

If cybersecurity in an educational context was already difficult enough to maintain, just imagine how much more challenging it's about to become when there are suddenly billions of additional devices to worry about — each one representing a potential vulnerability just waiting to be taken advantage of by someone who knows what they're doing.

One of the most pressing challenges facing educational institutions in the wake of these changes has to do with delegation and control. The IT teams at universities are already having problems properly managing the workload of the huge IT infrastructures they're responsible for — to say nothing of the problems created when there are suddenly millions of additional devices to take into account.

Another major issue has to do with the ability to identify and prevent threats. Remember: someone can exploit every device connected to a network with the right tools and knowledge.

How do you possibly keep up when your infrastructure is expanding in the way the IoT is about to create? How to you respond when the total number of threats you're dealing with doubles, triples, quadruples and beyond – seemingly overnight?

DNS / DHCP Network Services: The 21st Century Battleground

Perhaps the biggest challenges in this regard that are somewhat unique to an educational environment are DNS and DHCP core network services. These are absolutely critical to the continued protection of digital information in an education context, yet at the same time are about to become a lot more challenging to handle due to the massive influx of additional volume they're about to experience.

Short for Domain Name System, DNS refers to the technology used to assign names to any device connected to the Internet — from smartphones to computers to tablets and everything in between. Think of it like a massive phone book — if your computer needs to access a resource on the internet, it uses DNS to find the appropriate name and to make sure that your request ends up in the right place. Cisco's 2016 Annual Security

Report notes that 91 percent of malware is using the DNS protocol, making it not only a target, but also a vector of cyberattacks.

The explosion of the Internet of Things also creates an issue related to the Dynamic Host Configuration Protocol, or DHCP. DHCP is what actually provides the IP addresses and all other required network information to any device trying to join the network.

Universities have the issue of delivering IP addresses to hundreds of thousands of devices on campus — most of which are connected wirelessly — in order to serve students, researchers, professors and visitors. DHCP must be able to keep up with capacity demands and focus on security at the same time, as it is often the single point of defense when things like denial of service (DoS) attacks occur.

Managing DHCP presents something of a double-edged sword. If you attempt to address DNS security issues in the wrong way, you could prevent legitimate user devices from connecting to a network and operating in the way that students and faculty members need them to. If you don’t place enough emphasis on security, you leave a network open to data breaches, illegitimate traffic and more.

Looking to the Future

All of these network and user issues, but DNS and DHCP in particular, create a mountain of potential headaches as the educational sector further embraces the Internet of Things with open arms. It is clear that the way these services are deployed, managed and used on a daily basis must evolve in response to bring forth as many of the advantages and as few of the potential downsides as possible.

Thankfully, while old, legacy solutions are not prepared to handle the attacks of today, there are technology solutions that integrate DNS, DCHP and IP Address Management (IPAM) in ways that can handle such attacks. Integrated DDI appliances, for instance, provide failover features to ensure service continuity on campus. They also can check that devices physically connected to the school LAN network meet, and are limited to, the set of devices that have been logically defined.

Security is always essential, particularly in the education field — but a balance must be struck to allow for the performance and availability needed to keep deployed infrastructures up and running. These modern security features are capable of doing exactly that, but it’s up to the educational institutions themselves to embrace them.

In today’s competitive educational environment, universities must be sure they have an infrastructure that will provide the high-level IT services that campus users have come to expect, in order to maintain the best matriculation rates and school rankings.

David Williamson is the CEO of EfficientIP, a DDI network services provider headquartered in Europe, Asia and North America. (DDI refers to three network services: Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and IP address management (IPAM).)