DDoS Defense from AT&T shields Pike County schools from crippling network attacks.

Enterprise-level threat protection keeps mission-critical systems up and running.

Having more secure and reliable Internet access is mission-critical for Kentucky’s Pike County Schools, and it is as necessary to the district’s day-to-day operations as any other utility. To help safeguard its network, Pike County employs a number of security tools and strategies—including DDoS Defense from AT&T, which helps protect the district from increasingly common Distributed Denial of Service (DDoS) attacks that can cripple vital network services.
This rural district of about 8,500 students relies on Internet connectivity for so many of its functions, including daily instruction, online state testing, communication through email and a Voice Over IP system, monitoring of IP-based surveillance cameras, and other operations. Teachers use cloud-based services such as Edmodo, a learning management system, and Google Apps for Education to assign digital content, deliver classroom instruction, assess students’ understanding of a topic, and enable online collaboration.

“Technology is embedded throughout education now,” said Director of Technology Clayton Potter. “It’s just as essential as electricity or water. Teachers rely on the Internet for their lessons. You might as well close the school down if you don’t have a reliable connection.”

Pike County has invested heavily in its network infrastructure, with 1 Gigabit-per-second (Gbps) connections between buildings and a 10 Gbps pipeline to the Internet. What’s more, wireless connectivity is available throughout every building. Keeping this network safe from disruption is a key priority for Potter and his staff.

“We have to make sure we have technologies in place to keep intrusion out,” he said. “We need enterprise-level threat protection.” And AT&T’s DDoS Defense system is an important aspect of this security plan.

**DDoS Explained**

A DDoS attack occurs when a hacker takes control of thousands of computers and aims them at a single server, overwhelming that network with traffic and ultimately knocking it offline.

DDoS attacks are fairly common; about one in five businesses reportedly have been hit with a DDoS attack, resulting in several hours of downtime. Recently, schools have become increasingly popular targets as well.

“Students are now able to buy their own DDoS attacks online and attack their own schools on any day they choose,” said Terry Hect, Director of Security Practice for AT&T. “We’re seeing it frequently happen near test time; students will attack their school’s network so the tests are postponed.”

A large higher Education institution in New Jersey, has had to deal with a series of expensive DDoS attacks that have debilitated its network services. The attacks were launched by a hacker who calls himself “Exfocus,” and he claims to have been paid by someone with an axe to grind against the university. After four such attacks during the 2014-15 school year, this institution spent $3 million to upgrade its network security and was forced to raise tuition by 2.3 percent. But the upgrades failed to protect the university from another attack in September 2015, which once again prevented students and staff from accessing the Internet or any e-learning tools.
The biggest problem that schools face in shielding their networks from such attacks is a “talent shortage,” Hect said: “They have very limited assets to identify and remediate problems in a timely manner. Additionally, the security technologies they use typically require a lot of care and feeding. Network security doesn’t just require a lot of skill; it also requires a significant amount of time.”

That’s where AT&T can help. DDoS Defense blocks and removes malicious traffic in the cloud, before it even reaches a school district’s network. The system helps thwart attacks in near real time and keep network services up and running.

The Kentucky Department of Education has supplied AT&T DDoS Defense for all of its K-12 districts. AT&T monitors the traffic flowing to each district’s network, and when there is evidence that an attack might be starting, the district is put into mitigation. All of this occurs so efficiently that Potter has not had to worry about a DDoS attack since the service began.

“There have been a few instances where AT&T has notified us of a broadcast storm and has done some throttling or restriction for us,” he said. “But this all happens in the background, and we haven’t had to give it another thought.”

Other Security Measures
DDoS Defense from AT&T is one of several measures that Pike County uses to help protect its network, along with firewalls, antivirus software, and more.

“As a school district, we’ve got several security challenges that are inherent to our business operations,” Potter said. “We have to guard against phishing schemes, viruses, and other malicious actions where people try to intrude on our network. Security of our endpoints is critical. We have to have a comprehensive admin setup where we have user IDs, and then we grant different levels of network access based on those user IDs.”

Another key aspect of network security is educating users.

“We tell our staff and students, ‘Don’t click on this, don’t click on that, because if you do, this is what’s going to happen,’” he said. “We make sure they know that if they get a suspicious-looking email, they should delete it immediately. We tell them not to look at messages in a preview pane, because there might be links that can activate an executable file just by previewing the message.”

In fact, educating end-users “is more of a challenge for us than other security aspects,” Potter said. “It’s this end-user factor that we really worry about.”

Security services such as DDoS Defense from AT&T, on the other hand, “aren’t as much of a challenge for us,” he said, “because we have confidence that once we have them set up, they’re running in the background.” He concluded: “We’ve been really pleased with the service.”