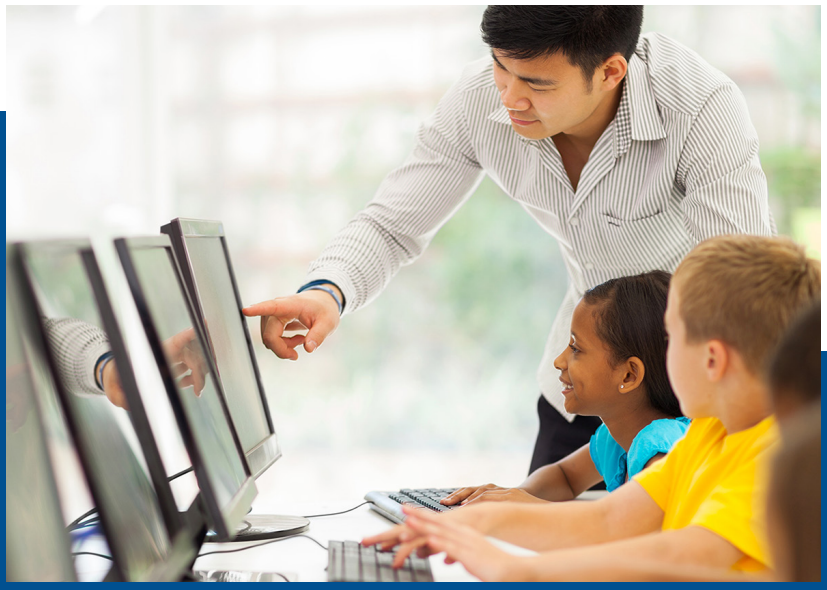
ena by zayo

SPOTLIGHT DISTRICT:
North Judson-San Pierre Schools

Adopting a Proactive Versus Reactive Approach to DDoS Attacks



Cybersecurity attacks are becoming commonplace in school districts across the nation. Many school leaders, already overwhelmed with their normal day-to-day tasks, are now having to proactively mitigate and prevent detrimental and extremely costly distributed denial-of-service (DDoS) attacks.

Plus, we are learning that hackers aren't just targeting large, well-known school districts. Rather, they are going after schools in all geographic locations and sizes. And the cyberattacks aren't just being launched from external sources—they are being generated internally as well.

DDoS attacks are easy and inexpensive cyberattacks that can be purchased to take down school networks and bring all operations relying on the Internet to a standstill. Many of these cyberattacks are purchased by the students themselves, and they don't understand the legal ramifications associated with these cyber events.

HOW IT BEGAN

Recently, Billy Russell, Technology Director at North Judson-San Pierre Schools in North Judson, Indiana, had to overcome this exact type of debilitating cyberattack.

Around March of 2020, Russell noticed a disturbing pattern.

Each day around 9:30 a.m., he logged into his myENA portal to check the district's bandwidth usage and saw that usage would suddenly max out and then drop to the floor just as quickly. This would occur in three-minute spurts followed by a minute of not receiving anything. The schools would lose Internet and voice services for nearly an hour at a time.

The downtime was devastating for teachers and principals alike. Discovering the source of the downtime quickly became a high priority.

> "People wanted to find an answer very quickly and we just weren't able to," explained Russell. "We went through a lot of struggles. We were losing testing ability, especially in our elementary schools, every single day."

Eventually, through a packet capture, Russell saw pages and pages of traffic asking for a peacecoprs.org DNS request, and he realized that was synonymous with a DDoS attack.

> "We would get a DDoS attack lasting about an hour in 30-second spurts and we would lose Internet for a full hour. If we did the packet capture at the correct time, we would have hundreds of pages filled up with the DNS requests. We would never have time to recover; we'd be down for a full hour," said Russell.

At the time, neither Russell nor his staff were sure which steps to take next.

"When this started, no one knew what a DDoS attack was. I had to explain how we were limited by the tools we had at the time," Russell continued. "We explained this would keep happening until we could purchase something or come up with a better plan. With the tools we had, we just weren't able to defend against it."

The staff, reeling from the constant disruptions, was surprised by how easy it was to order a DDoS attack and shut down a network.

> "I told them that, basically, for a couple bucks you can shut down our entire network," said Russell.

Russell and North Judson-San Pierre Schools, however, were determined to find a solution.

"When we started, I had no idea how to prevent an ongoing DDoS attack, so I looked on message boards, asked colleagues in other districts, and spoke to a former EdTech person who has been very helpful in the past. Ultimately, we landed on ENA NetDefender."

North Judson-San Pierre Schools has now been running ENA NetDefender for over a year. Although the DDoS attacks against the school corporation continue, with seven attacks since January 2021, the district experiences very limited downtime as ENA NetDefender mitigates the impact of the attacks.

"Instead of going down for an hour, we may see the network drop for three seconds, which is much more manageable for the teachers and principals than the hour we were dealing with," said Russell.

When asked what advice he would give to those who have been in his position, Russell said it was fairly simple:

> "The easiest answer would be just go back in time and buy ENA NetDefender!"

He also recommended having a plan in place before it happens, keeping a list of experts and any appropriate vendors that can be consulted, and ensuring you have easy and quick access to any IT portals and systems that could be required for a diagnosis or a fix.

To put it simply, as Russell said, "Adopt a more proactive approach."

If you would like help strengthening your school's defenses, **ENA NetDefender, our automatic DDoS mitigation and scrubbing service**, proactively scans and analyzes your network for attacks. When an attack is detected, ENA NetDefender reroutes your traffic to one of our scrubbing centers, removes the malicious packets, and leaves intact all desired traffic.