Cox Business

Education

Five Reasons K-12 Networks Can’t Wait on DDoS Mitigation

In recent years, we have borne witness to DDoS attacks against major service providers, financial institutions, government agencies and some of the largest businesses in the world. These high profile cases make it easy to obscure the fact that DDoS attacks are victimizing lower hanging fruit in the digital ecosystem too

In particular, K-12 school districts have continued to see an uptick in DDoS attacks against their networks in recent years. But just because these schools aren’t high-profile global corporations, it doesn’t mean the impact of succumbing to a DDoS attack doesn’t have very real consequences.

Here are five reasons that administrators for K-12 school districts cannot afford to wait on procuring DDoS mitigation software:

1 Student hackers: Unfortunately, it doesn’t take a professional hacker to conduct a DDoS attack. In many cases, students themselves have been able to perpetrate attacks. Because these students have access to the network, many have their own devices and a greater breadth of knowledge about computer programming than many of the faculty themselves, administrators must invest in DDoS mitigation to protect the student body from bad actors within the ranks.

2 Testing outages: DDoS attacks can do widespread damage to any educational operations that take place online. In many instances, testing is now done online. This includes homework assignments, exams and federally regulated standardized tests. Consider the case of Minnesota’s Board of Education, which had to renegotiate a contract with an ACT testing provider after the provider suffered DDoS attacks that prevented students from taking their exams.

3 Data loss: In some cases, DDoS attacks are simply smokescreens for larger attacks intended to target highly classified data stored on the network. While victims scramble to mitigate the DDoS attack, hackers can gain access to personal, financial and medical records of students or staff, putting affected individuals in a position to be exploited further.

4 Budgetary restrictions: Most K-12 school districts today do not get the funding they desperately need to resolve cybersecurity conflicts in-house. A robust cybersecurity plan requires a fully staffed IT department of highly skilled, experienced individuals. But tight budgets make it difficult to attract and retain IT talent, making it vital for administrators to seek help from an experienced third party.

5 Costly cleanup: As expensive as it can be to hire the personnel needed to prevent an attack, the cleanup after succumbing to a DDoS attack can be even costlier. According to one report, 36 percent of businesses reported that DDoS attacks cost them between $5,000-$19,999 per hour. Given these findings, it cannot be understated how much potential DDoS attacks have to devastate school districts.

Fortunately, K-12 administrators don’t have to resolve this challenge on their own. To learn how your district can protect itself against DDoS attacks, check out Cox Business here.

COX Business