Protecting the Campus from the Outside In

DNS security provides a first line of defense, helping colleges and universities protect against bad traffic coming from a multitude of directions, way before it hits the network infrastructure.

Rufus Coleman
Director and General Manager for U.S. Education, Infoblox

IF THE SHIFT TO REMOTE LEARNING HAS TAUGHT the IT organization anything, it's that network protection doesn't begin and end at the campus borders. Rather than a corral, the perimeter for security is now an open range, with scattered endpoints put into existence by students, faculty and staffers from remote sites. Traditional lines of defense – next-generation firewalls, intrusion prevention and generic DDoS – have begun to look almost haphazard in the face of so much distributed activity.

Is it any wonder threats are on the rise? As the number of system and data breaches rack up in higher education, security experts have adopted a defense-in-depth stance.

Putting multiple defensive measures in place begins with a baseline security posture that wants to understand everything coming into and going out of the network, preferably in real time. The tricky part is achieving that level of visibility and response when the threats could originate from any one of the many thousands of devices accessing institutional resources.

One route is deploying domain name system (DNS) security. Let's think about DNS for a moment. It may be decades-old but it's still heavily relied upon; without it, the entire network is shut off from the internet. Regardless of their location, endpoints require DNS to connect to any application, service or data source. And so does malware, which uses DNS at multiple stages of an attack. That's why DNS is a marvelous transport system for malfeasance. Traditional security mechanisms don't police it well because there's so much of it – millions of DNS queries a day for the typical university.

And, unfortunately, most users don't know when their devices are infected. Once their compromised laptop or smartphone has gained entry to the network, flags don't necessarily begin waving. Quietly, the malware goes about its business looking for friendly neighbors willing to accept packets from something else also identified as being inside the network. Thereby does the malware start downloading an encryption key, possibly uploading a copy of data, all of which eventually can turn into a ransomware event.

A Million Points of Defense

Tackling the DNS challenge requires a dedicated solution. Stopping bad traffic from getting to central operations – the command-and-control server – enables IT to identify and quarantine the components making up attacks before they can assemble themselves and strike. The use of DNS security and its powerful algorithms reduces susceptibility to volumetric attacks, NXDOMAIN exploits, DNS cache poisoning, reflection and amplification attacks, and DNS hijacking, while still letting through legitimate queries.

A big benefit of the DNS security approach is that you can capture bad traffic early on, before it becomes a major issue, thereby making the rest of your security infrastructure more efficient. With the proper tools, DNS can provide the visibility needed for blocking attacks other defenses don't see, improving breach detection and helping facilitate faster and more effective incident response. Tapping DNS for a greater role in security is a low-risk investment with high potential.

> Unfortunately, most users don't know when their devices are infected. Once their compromised laptop or smartphone has gained entry to the network, flags don't necessarily begin waving.

When considering a DNS security solution, colleges and universities need to assess four key functional areas:

- **SINGLE PANE VISIBILITY,** the ability to monitor on-prem and remote DNS traffic through a single administration console, for full visibility, lower response time, and faster resolution and threat containment. Infoblox Advanced DNS Protection (ADP) supplies

a single view of attack points across the network along with attack sources, supplying the intelligence needed for threat management.

- **ADAPTATION,** for automatically updating protection against new and evolving threats as they surface. Threat Adapt, built into Infoblox ADP, applies independent analysis and research to evolving attack techniques, including what our own threat specialists have seen in customer networks, to update protection. That includes adaptation to reflect DNS configuration changes as well.
- **INTEGRATION WITH EXISTING CYBERSECURITY INVESTMENTS.** Defense-in-depth means overlapping layers of security and tools that work together. The institution already has existing defenses protecting the network. Why not increase the value of those products – whether from FireEye, Check Point, Fortinet, Cisco, Palo Alto Networks, Rapid7 or 70-plus other companies – by sharing threat and attacker information bi-directionally, in real time? That's the idea behind the Infoblox Cybersecurity Ecosystem and to work with other security and network providers in developing a highly interconnected set of integrations. The idea is not competing, but completing.
- **SECURITY COVERING OPERATIONS INSIDE AND OUTSIDE THE DATA CENTER.** DNS security needs to protect every connection, regardless of device or location, and secure infrastructure that stretches across physical, virtual and cloud systems. Infoblox BloxOne Threat Defense Advanced, a subscription-based hybrid cloud solution, becomes a linchpin in all IP-based communications, covering DNS, DHCP and all IP address management. When a DNS query is sent, BloxOne uses machine learning to inspect it, run it against any one of up to 40 million bad domains and indicators of compromise, to determine in real time whether the address is good or bad. BloxOne also accommodates custom filtering. Tired of having March Madness slow legitimate traffic to a crawl? Stop people from hitting the streaming domains via the network.

The higher ed network is growing exponentially in complexity. Users are becoming more distributed. But IT's job is the same: Protect everything and everyone, wherever they are. DNS security provides that first line of defense that helps tackle the job at scale.

Rufus Coleman *is the director and general manager for U.S.-based education and government at Infoblox.*