May 3, 2019

The Dichotomy of Cybersecurity in Higher Education

CYBERSECURITY, HIGHER EDUCATION
BY SCHNEIDER DOWNS PROFESSIONAL

Cybersecurity in the higher education (Higher Ed) realm faces many challenges. Unlike corporate entities, there may be many groups outside of central IT and security that manage systems and data in a university environment. Individual colleges and departments frequently have their own systems and IT staff. These groups may have little interaction with the University's core security and IT teams. Consistency makes cybersecurity easier to implement, so what can you do if you are in an organization without it?

There are three high-level items that I consistently see in Higher Ed institutions that help when it comes to cybersecurity. Those are two factor authentication, relationship building between IT and security staff in different departments/colleges/etc. and treatment of the vast majority of the institution's network as hostile.

Two factor authentication is no longer considered simply a nice security add-on, it is a requirement for a base level of security at any size or type of organization. Having a physical token, cell phone app, Duo, or other solution must be required alongside a traditional password to gain access to organizational resources. As a penetration tester, my job becomes a lot simpler whenever I discover an organization is not using two factor authentication. However, two factor authentication is no silver bullet; there are ways to bypass it or trick people into giving up their SMS codes and etc., but boy is it a lot easier on me if I can send a simple phishing email, get a couple passwords and the next thing you know I'm on the inside of the network reading databases. Any organization using two factor authentication and implementing it properly is elevating the level of difficulty to break their shell. Next we move on to something less technical, that is relationship building.

The more that the core IT and security teams understand about their organization's systems—even those they don't control—the better they are able to secure them. Making partnerships between all IT assets in an academic environment can go a long way in ensuring that central IT and security departments understand the systems in use outside of their immediate control. This can happen through semi-regular meetings, seminars, lunches, etc. Free food is never a bad bet for getting people into a room. The goal is simple: get departments, colleges, IT and security talking and learning from one another.

Despite how well a higher Ed institution's two factor authentication and integration with central IT and security are, there is one security risk that will never change. Higher Ed institutions are places of freedom, exploration and learning. That means that you will never be able to take a corporate approach and say, "This is what everyone will do and this is how they do it, or else." Something like that would never fly in higher Ed and honestly it often doesn’t work well in the corporate world either. So what should institutions of Higher Ed do? It is most critical for them to treat their networks (both internal and external) like the warzones they are. The internal network is just the same as the Internet. Yes it is awesome, with big data, AI and ever increasing power, but it is still the Wild West and you need to carry a six shooter, even in the shower. There are a wide variety of ways to treat your internal network as hostile. At a minimum, network segmentation paired with attack detection and prevention capabilities should be standard. This could be in the form of micro segmentation, firewalls between the internal network and server segments, EDR solutions, SIEMs and so on. If you treat your internal network the same as you treat your Internet facing network, you are on the right path. Most orgs still do much better on the latter, so taking similar approaches from your Internet facing networks and shifting them inward can be very effective.

Higher Ed faces many unique challenges when it comes to security, but that does not mean it is impossible or impractical to secure a Higher Ed environment.

You’ve heard our thoughts… We’d like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we’re especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you’ll share it with us. After all, a dialogue is an exchange of ideas, and we’d like to hear from you. Email us at contactSD@schneiderdowns.com.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.