ADVERTISEMENT

MEET MERIT'S NEW CISO - KEVIN HAYES

Merit is excited to have Kevin Hayes as our Chief Information Security Officer. We asked Kevin to share his insights on current security landscapes, predicting the next IT crisis and some tips to make your organization more secure.

Q: *What are your thoughts about the threat landscape? What is the single biggest threat to companies, governments and nonprofits now?*

KEVIN: Naturally, the threat landscape changes on a daily basis. Many of these changes directly reflect the changes we as IT professionals are making in our own environments. As we move to more cloud-based and web services, the attacks are focusing more and more there. As we go down this road, we are seeing attacks focusing on these web apps and the technologies that power them. A lot of this is due to the fact that we have mostly hardened our infrastructure so that attackers cannot easily hit things like our database servers and our Active Directory Servers. It's imperative to ensure the security of web application security (up to Layer 7); those areas of the security landscape are not as mature compared to most other practices. In short, securing your web apps is a really big deal for everybody!

Q: *What are some of the biggest lessons you learned from security in higher ed?*

KEVIN: The critical importance of fostering a culture of security. Higher education is filled with dedicated people that are coming up with unique solutions to fix problems that don't cost a lot of money. Many times these solutions don't take security into account as much as they should, or at all. A lot of people in higher education cannot grasp that there are people on the internet that want to do bad things. Trying to explain to employees that cyber attackers would deface your website and drop the tables on your databases is a challenge, mainly because this is a foreign concept to people who have dedicated themselves to make a positive impact in their community.

Q: *What's the next crisis on the horizon?*

KEVIN: Managing and securing the cacophony of non-standard IOT devices and services in our environments is proving to be an interesting challenge. Many of these devices are built for home use and *not* for enterprise environments. A good number of these non-standard IOT devices are using network stacks and libraries that have significant security holes in them, and the update cycles for these devices can be sparse or non-existent. My biggest worry is the next version of a Mirai botnet because the attackers will have learned from their mistakes and will make sure their attacks are both more invisible and persistent.

Q: *Low cost solutions – what's the number one thing people can do to improve their security posture?*

KEVIN: Learn scripting and leverage that to ensure that the basic things that we know we should be doing are applied to 100% of your IT landscape. Scripting helps make sure that there are no "loose ends" that you have forgotten about. Run those scripts on your entire IP space and take a look at the end report. That misconfigured printer or that old Windows Server 2003 box in the corner are going to be the ways attackers get in; they are the weak links in the chain you need to identify and prioritize fixing or getting rid of. Use scripting and let technology do the hard work for you!

Q: *What's the biggest tip to overcome end user/ human risk?*

KEVIN: You absolutely need to relate to what the end user is doing on a daily basis. While we have security videos and training to help teach the basics, to be most effective, you need to spend a small amount of time and sit down with individual groups. Give them actual examples of attacks they would expect to see, and make it relevant to their jobs. After you personalize these explanations, make sure that they have actionable information they can use. This involves watching what you click, hovering over URLs, and understanding how to read the URL popup. That level of personalized education and training will provide substantial results when a cyber attack actually does happen.

Q: *What are you looking forward to the most in your CISO role at Merit?*

KEVIN: I'm passionate about IT security, and I love helping people. I'm looking forward to being able to bring my knowledge, talents, and experience. There are countless dedicated technology professionals within our state and membership. Keeping Michigan on the map as an IT security leader in cybersecurity best practices is an honor I am excited to be part of.

Read the full interview at:
merit.edu/kevinhayes

merit