New Miami Dade College Cybersecurity Center Gives Students Hands-On Experience Dealing With Attacks

ByALEJANDRA MARTINEZ • 14 HOURS AGO

Tweet Share Google+ Email

The Cybersecurity Center of the Americas' control room simulates a real-world security operations center.

COURTESY MIAMI-DADE COLLEGE

Miami Dade College's newCyberSecurity Center of the Americaswants to teach the next generation of South Florida's security professionals to detect, stop and remediate when under attack.

The Center launches this fall with a focus on training the future workers in cybersecurity and growing the state of Florida's cybersecurity competency. The school has a state-of-the-art control room that will simulate a real-world security operations center. Students will be given different scenarios of malicious software they will have to learn how to deal with.

Jorge Ortega, director of the new CyberSecurity program, says that cyber attacksare happening more frequently. The most common fall under malicious software. This threat typically has a financial motive. It locks up, encrypts files and gives a time limit to pay a ransom. Ortega says these attacks aren't just happening at an individual level but also at a larger scale to governments, businesses, and nonprofits.

"A huge bulk of attacks are user errors," says Ortega. In addition to real-world simulation, the new cybersecurity center will provide security awareness training, speaker eventsand forums. Ortega joined Sundial to discuss the impact of cybersecurity threats and how South Florida students are being prepared to address them.

Listen
17:21

Listen to the full interview.

WLRN: Take us inside the Cyber Security Center. What does it look like?

ORTEG: The room was created to mimic a security operation center or network operation center. Most people are familiar with them through ads or movies or TV where you see war-room type scenarios. In addition to having that facility, which will allow students and professionals to feel the true sense of being under attack, we also have a training platform. It's a really unique opportunity. And what this training platform does, which differentiates from a lot of training is that it simulates an actual network that has the size and scope that most professionals will find in the industry. It has all the different tools, servers, and traffic that you will have on a true corporate environment.

That platform we're talking about is a way to train people in that real-world experience. So you set up a simulation where a corporation is being attacked?

Correct. So this network will simulate what a corporation will have and then we will introduce real-world malware into that network. We have different attack scenarios like ransomware, man-in-the-middle [attack], sequel injection, these type of real-life attacks will be introduced to the network and the trainees will be forced to detect, neutralize and remediate the situation.

It's a little bit different from traditional training, which is more based on lectures and readings. Here, you're really forced to act and again that's really what we're aiming to do because when you get out in the industry and you get out into the organizational network, you need to understand how to respond to these cyber threats. Especially today where they're becoming more and more complex and advanced.

What are the differences between ransomware attacks and malware attacks?

Malware is essentially malicious software. There's a lot of different brands of that and ransomware is one of those. Ransomware has been very popular lately. It's been in the news a lot and essentially what it does is it locks up and encrypts your files or your network or parts of it and then it forces you with a time limit to pay a ransom to unlock those files otherwise, those files will be lost forever. That's a situation where there's clearly a financial motive. The person that is trying to launch that attack is looking to be paid for that attack.

Are a lot of the attacks still based on the simple mistakes that we make as individuals do when we open an e-mail, go to a link or are they finding other ways to get in?

I'd say that the bulk of the attacks are still very much what we would call rudimentary user error. That's why we also propose a lot of security awareness training and different exercises to get your security users. We're talking about everybody from your frontline admins all the way up to your c-level executives. They need to understand the repercussions of the actions they take and to be very cautious in what they do. A lot of which you see today is not a complex breach but rather user intervention or social engineering. Something that has nothing to do with the technical side but when someone writes their password on a post-it note and leaves it by their desk, now you have this person's credentials.

And sometimes people at the helpdesk give your information out.

Absolutely. Someone will call and especially today with social media everyone knows everybody's title, where they work and who their team is. They can call a helpdesk and say, 'I am this person and I forgot my credentials can you please give them to me?' And a lot of times they will be able to get it. In that case, it's even more complex because then the person's logging into the network with actual credentials but to do malicious activity. It's a complex issue and one that needs to have a lot of focus.