TANIUM Public Sector | carahsoft

Q&A with An Expert

A Recap of Doug Thompson's Panel at Carahsoft's Annual EdTech Talks

Doug Thompson,
Director of Technical Solutions Engineering and Chief Education Architect,
Tanium

What's the latest advice on how to respond to a ransomware attack? We keep hearing more and more about institutions who are hit with ransomware. Do institutions' security response plans need to change to keep up with the current trends?

The way that you will respond to ransomware is very much like you'd respond to a breach in that what you really want to do now is just sort of isolate it put it on island and prevent it from spreading. The initial reaction I see from a lot of people is hey we're just going to turn the server off and you know we're going to go ahead and delete the malware. We're going to try to use our backups which are still on premises but they're getting infected too. It reminds me of back in the days when backups were done on tapes, and we shipped them off site. You did that in case you had a fire. Well, this is a fire, this is an electronic fire that's coming. You need to have those things backed up and just assume that you're going to get ransomware. Work through those tabletop exercises where you know what you're going to do in case there's a ransomware attack so it's just simply automatic, it's reactionary. You don't have to think about it, you know what to do. It's the urgency and the speed at which you can find it and remediate it is key to minimizing the damage.

Another part of digital transformation, the move to remote or hybrid or flexible models of work and learning has really blurred the borders of networks. What are some key considerations there, Doug?

We learned a lot when COVID hit. We got to enable remote learning and security was sort of a secondary concern. And now we've had time to sort of digest and work security back in there. We have to identify the things that are critical the crown jewels of what you have: research data, student information, etc. and harden the area around that. The fundamental question is where are all your end points? Where are they at any given time? Reliance on having to be on the VPN sort of limits what I can do. Like if I'm at Starbucks or something because I still have documents, I still have other things that are here then when I reconnected the VPN the floodgates are open the dam is gone and I can infect the entire network. So, knowing where those things are all the time and being able to have a conversation with them needs to be top of mind.

The cybersecurity landscape is just changing at such a rapid pace, some people are being denied premiums, insurance companies are adding more and more restrictions, limiting their payouts for certain types of losses. What do you think needs to change in order for higher education institutions to keep up with the new and ever-changing threats?

Automation! You just don't have enough manpower to stay on top of it anymore. But a lot of the breaches a lot of things that happen are exploits that there are patches and stuff for. You just don't get out and patch on a timely basis because you've got 85 other things to do. So how can you automate some of these to get these things patched and verifying that they are installed and more importantly did you reboot the machine. I've seen cases where over 3/4 of the machines were requiring a reboot which means they were not patched. They thought they were patched but because they needed to reboot, they weren't. It's just simple hygiene like that which will save you the blocking and tackling. Then you can focus on the higher risk things. the things that need a human intelligence to get in and do those things.