As I write this in the early afternoon of Monday, May 15, I just finished reading the latest bulletin from DHS on WannaCry, the ransomware virus that has become a lead news story since the weekend.

In what I read, it seems that WannaCry is not targeting overall critical infrastructures. For that, we can be thankful. But we were lucky this time. WannaCry was spread through phishing emails. Further, it gained speed by infecting computers that did not have the latest security patches.

WannaCry is showing that is it very possible to have a virus spread rapidly through security vulnerabilities. In other words, the lack of keeping network security up to date and the lack of education of the users, are the two factors that allowed this to happen and spread.

We've all heard about educating your employees about cyber hygiene. We trust that our network administrators will always be on top of the latest patches for the network. But WannaCry, like many other viruses, exploits the weakest link in the chain.

And there will always be a weak link. And as *Wired* magazine pointed out in an article released this afternoon, the WannaCry hackers weren't even that good!

As of the writing of this blog, the virus seems to be attacking IT systems. But will there be a WannaCry style ransomware that could attach industrial control systems? I'd like to say no, but the reality is that there are over 85,000 industrial control systems that are directly connected to the Internet. And that is just in the US. That is the weakest link, by far, for vulnerability in industrial control systems.

I'll close with some dark words from the same *Wired* article "Speculation aside, the hackers' sloppy methods also carry another lesson: A more professional operation could improve on WannaCry's techniques to inflict far worse damage. The combination of a network-based self-spreading worm and the profit potential of ransomware won't go away."

Print as PDF:

Topics

Security

Cybersecurity

Tags

Cybersecurity

WannaCry

Industrial Control Systems

Network Security