How to protect your data from cyberattacks

May 25 2017, by Leah Becerra, The Kansas City Star

Credit: George Hodan/Public Domain

The malware attack known as WannaCry (or Wcrypt) has quickly become one of the worst cyberattacks in recent memory. But the damage could've been prevented.

"Go home tonight and open your door and leave it open all day," said Kevin Cardwell, a computer security architect and online instructor for Udemy. "Now let's see if anyone comes into your house."

Obviously, leaving the door to your home wide open isn't a great idea. But Cardwell points out that many individuals and even businesses leave the door to their personal networks wide open all the time.

"You leave the door open, and things are going to come in," he said.

The Federal Trade Commission offers advice on how to protect computers from Malware. Malware is short for "malicious software" and includes viruses and spyware installed on your computer or mobile device without your consent.

The WannaCry attack preyed on digital doors left open and was able to breach at least 200,000 computer terminals in 150 countries since Friday. The particularly nasty ransomware locked people out of their systems while demanding payment.

The malicious code was emailed to its victims inside a zip file. Once the file was opened, it compromised a weakness in older versions of Microsoft's operating system, which led to the proliferation of the WannaCry worm.

"The patch was out in March for the WannaCry ransomware, but all these machines were still infected," said Cardwell. Meaning a lot of those who've been impacted by WannaCry weren't practicing basic cyber defense tasks like keeping their operating systems updated.

The security patch released in March didn't cover older and unsupported versions of Windows like XP. But when WannaCry started causing havoc, Microsoft released a patch to close the wide-open front doors of those machines, too.

"The reality is, the patch system's broken," Cardwell said. "Yes, you have to patch, but unfortunately sometimes your systems, your applications, you can't patch them. Because of mission or business needs. So, because of that, you have to mitigate the risk."

While individuals should take steps to defend their digital lives, by backing up, installing updates and running antivirus software, it's arguably more important for small businesses to set up proper defenses.

"Small business are usually the easier attack. And when you're an attacker, you're going to look for the weakest link," said Cardwell. "You don't go after the large corporate network that has all those resources usually. You find the people they do business with and attack them."

Cardwell says the best way for small businesses to protect their clientele, whether those clients are individuals or corporate giants, is to deploy network segmentation. This means businesses should not be connecting their most sensitive information to the same internet employees use.

"To give you an analogy, you've got all this data - say it's like a vault that has data, money, jewels or whatever in it. And you put it in the same room as all your workers. That makes no sense."

Account numbers, Social Security numbers and all other types of data a company wants to keep safe can still be networked internally. Separating the important stream of information from, for example, the network where employees get emails, could prevent malware from breaching the really important stuff.

At the end of the day, Cardwell notes that "no product will make you secure." What's important is setting up a process of defenses because he says, "everyone is a target."

Citation: How to protect your data from cyberattacks (2017, May 25) retrieved 18 April 2024 from https://phys.org/news/2017-05-cyberattacks.html