we all face. Here's what we learned by talking with a James M.T. Morrison, a Senior Computer Scientist at the FBI who is working to educate and empower companies to be mo

May. 22, 2018

"You won't make friends with tough security but you will protect the network."

In addition to securing your data, there are everyday network security concerns that we all face. Here's what we learned by talking with a James M.T. Morrison, a Senior Computer Scientist at the FBI who is working to educate and empower companies to be more secure.

[From the dataquest blog.]

Your #1 Source of Problems: Your own people

40% of all cyber threats to your company are from an internal source. And your

Cisco publishes guidance on educating employees here and there's always the SAN Tip of the Day that can act as a nice reminder to your teams.

Ransomware

According to the FBI, if you haven't seen ransomware on your network, it's probably coming. Ransomware is triggered by a user clicking on a link. This then encrypts all your files, or your entire hard drive, and you are instructed to call a number and pay a ransom. Ransoms can vary from $300 to $3,000 or more. You'll be instructed to pay the ransom (likely in bitcoin). Once you pay the ransom, a key is released to you which de-crypts your files. Your best defense for this is having a good backup on a separate hard drive in a different physical location. If you have this, you are able to restore from backup and avoid paying the ransom.

Phishing

70% of all attacks are phishing attacks. Phishing is a technique of sending emails that appear to come from a trusted source with the goal of getting the user to click a link or go to a website which will prompt a malware donwload. Phishing can also use a technique called domain twisting- replacing "l" with "1" or using two "v" letters to mimic a "w". This can be used to create a believable simulacrum of a trusted website such as a bank, where a hacker can collect the personal data entered on the banking website and use it. To prevent this, use caution before clicking links and hover over a link before you click it to determine whether domain twisting is being used.

Half of all companies who work with the FBI on this issue actually do phishing attack tests. The company sends a warning email to all users saying "we'll be doing a test and sending an email with a phishing link." What happens is that 20% of your people will just click the link. These are the people you really need to work with on network security.

SQL Injection Attacks

Make your Email servers Wary

Set up your email server to initially reject emails from domains under a certain age (say 6 months). This prevents 80% of malicious email attacks.

Restrict Access to Your network

Only let administrators have access to the remote RDP key. And work with the IT team to understand what "normal" traffic on your website looks like. Most companies do not have a current architectural drawing of their network. But if you have this documented, and understand what normal traffic is, you can detect a changes.

Require Better User Passwords

Implement password security policies and choose 2-factor authentication wherever you can.

Hold your business partners accountable

In contracts with contractors and subcontractors who access your network or data, require that they maintain a certain level of IT security.

Update Your Machines

Keep computers updated and patched, both the operating system and the browser.

If you need help

Register cyber crime incidents at the FBI's internet crime complaint center.
And remember the Tech Commandments:

Small Business