The Key to Good Cybersecurity: You

Did you know that your organization and you can be a cyber criminal's target even if you do not have much valuable information? Imagine that it is the morning of February 3rd, 2020. Frigid temperatures extend as far south as Texas and are expected to stay in place for at least the next 6-8 days. As you are getting ready for work you hear the local fire company's siren begin to wail. A few seconds later your whole house goes dark. You pull out your phone to turn on the flashlight app and it starts wildly chirping and buzzing. There is an alert from the Federal Emergency Management Agency ("FEMA") advising everyone of a nearly nation-wide blackout and recommending that everyone stay off the streets and at home while emergency crews work to assess and address the situation.

Your Wi-Fi is out, so try connecting your laptop to the Internet via your phone but the phone has trouble keeping you online. So, you E-mail your office that you will try again in a bit when the power comes back on, then change into warmer clothes and settle in on your couch armed with a heavy blanket, a book, and the old AM/FM radio that you found buried at the back of your closet.

By noon the news begins reporting that the blackout was the result of a coordinated attack. The attackers created malicious software (malware) that overwhelmed the protective switches, called relays, which are used by power companies to keep their electrical distribution equipment from being damaged. The malware kept the relays from working properly, causing transformers and other equipment to overheat and, in some cases, to catch fire. Officials are still assessing the damage, but they are warning that although there is some inventory of spare parts and equipment, much of the equipment will need to be newly manufactured which could take months.

As the day progresses you accept the fact that the power will be out a while and that the fire-and-blanket approach is not a long-term strategy. You are about to hop in the car to buy a generator when your phone rings. It is the CEO of your company. The FBI called her moments ago and told her that they traced the problem back to an individual E-mail account at your company: your account. Foreign agents gained access to your E-mail account and used it to send infected E-mails to select customers of your company. These infected E-mails allowed the foreign agents to gain control of other systems, and to eventually work their way up to a company that has access to the electrical grid. From there, they were able to infect the grid and cause the nation-wide blackout. The FBI assured the CEO that they will not publicly name your company, but cautioned that given the scope of the damage and the number of agencies involved it may not be long before the company's name, your name, and your collective role in the blackout are leaked. You hang up and collapse onto your couch, your head spinning at the thought that your world has forever changed.

Could This Really Happen?

While this scenario may sound far-fetched, cyber criminals target victims for a variety of reasons, and most aspects of this scenario have already occurred. For example, according to the Wall Street Journal, agents of the Russian government gained access to an excavating company's E-mail systems in 2018[1]. They exploited the excavating company's trusted relationship with its customers and moved up to larger, more sophisticated companies, eventually gaining access to the US electrical grid. "They got to the point where they could have thrown switches" and disrupted power flows, said Jonathan Homer, chief of industrial-control-system analysis for DHS[2]. "Some companies were unaware they had been compromised until government investigators came calling, and others didn't know they had been targeted until contacted by the Journal." Thankfully, investigators from the FBI and DHS were able to stop the foreign agents before damage could be done to the US electrical grid. Otherwise, the US may have suffered the same fate as Ukraine in 2018, when an attack on its electrical grid caused massive equipment failures and lengthy power outages[3].

1 - https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112
2 - https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/
3 - https://dragos.com/wp-content/uploads/CrashOverride-01.pdf

Fathom Cyber
Defensible Cybersecurity Strategists
215-648-1950
P.O. Box 1235, North Wales, PA 19454

Top 7 Tips for Improving Individual Cybersecurity

Here are our top 7 tips for keeping yourself safe at home and at work:

1) Stop and Think Before You Click a Link - Before you click on a link or open an attachment in an online message (i.e., an E-mail, text message, instant message, etc.), ask yourself if you were expecting the message, even if it was from someone you know and trust. If you weren't expecting the message, contact the sender via another means (e.g., call or text them) to see if they truly sent the message. A few extra seconds of effort can save you a lot of headaches later. For more information about common online messaging-based attacks, visit Stay Safe Online (https://staysafeonline.org/blog/5-ways-spot-phishing-emails/). Think you have the skills to spot a fake online message? Try Google's phishing quiz at https://phishingquiz.withgoogle.com/.

2) Avoid Less Reputable Websites - Although some websites pay attention to cybersecurity and attempt to keep their sites safe, many sites do not. Their primary focus is to drive viewers to the site to increase advertising revenue or sales, and the maintenance and security of the site often take a back seat. Regardless of whether the link is in an online message, search engine result, or other source, before you click on the link you should ask yourself whether the site is likely to be secure, and if you are unsure, don't visit the site. Advertising-laden sites are also more prone to unintentionally posting advertisements that can push malware down to your device and should therefore be avoided where possible.

3) Back up your data - Ransomware is one of the biggest threats facing organizations and individuals today. Ransomware will encrypt your locally stored data and online storage, such as Carbonite, OneDrive or Drobox. Some online storage companies keep multiple older versions of your data, helping to improve your chances of recovering unencrypted versions of your files. However, we recommend that you back up your data to offline sources such as external hard drives that you keep unplugged from your computer except when backing up your data to them. This allows you to successfully recover your data in the event the online backup provider is the victim of a ransomware attack or otherwise goes offline.

4) Use Antivirus and Firewall Software – Old antivirus software used to bog down computers, but today's antivirus software is both highly efficient and effective. If you don't want to pay for antivirus software, Microsoft Windows even comes with its own antivirus software called Windows Defender that consistently receives high ratings in independent reviews. Similarly, Windows Firewall does a good job of helping to keep attackers at bay. If you need help enabling Windows Firewall or Windows Defender, visit https://www.microsoft.com/en-us/windows/comprehensive-security. Several well-known companies, including McAfee, Norton, BitDefender, and AVG also make antivirus software for Android devices, and if you own an Android device you should consider installing one of those. We also recommend downloading and running an alternative antivirus program, such as Malwarebytes, as a safety precaution every few months.

5) Enable Automatic Software Updates – Most operating systems, such as iOS, Android, and Windows, and most commercial software, such as Microsoft Office, Adobe Acrobat, Google Chrome, and Mozilla Firefox are regularly updated by their manufacturers. Almost every update contains fixes for security vulnerabilities that were found in the operating system or software. Most of these tools can automatically install the latest updates from the manufacturer, and it is a good idea to enable automatic updates.

6) Use Multifactor Authentication Where Possible – Usernames and passwords are not enough to keep attackers at bay. A third form of authentication, called multifactor authentication, is a necessity and should be used whenever available. Multifactor authentication can take different forms, including text messages or synchronized pseudo-random numbers that change frequently. Although some forms of multifactor authentication are stronger than others, any multifactor authentication is better than none.

7) Use a Password Manager – Password mangers such as 1Password, Dashlane, and LastPass store your passwords in an encrypted form that only you can access and can automatically log you into your favorite websites. The stored passwords can be synchronized across your mobile and desktop/laptop devices. Password managers are safer than storing passwords in your browser, and they allow you to use unique passwords on every website.

For more practical cybersecurity news and tips, subscribe to our newsletter at: https://FathomCyber.com/

Fathom Cyber
Defensible Cybersecurity Strategists

215-648-1950
P.O. Box 1235, North Wales, PA 19454