Week 3: October 18 – 24, 2015 - Defense in Depth

There are several ways in which everyday technology users can protect themselves. In the corporate world, network defenders use the principle of Defense in Depth (DID) to protect their systems and data. DID focuses on implementing several layers of security to protect against cyber threats, or to mitigate the effects of a successful cyber compromise. In the event of a cyber compromise (which is becoming all too common), users stand a better chance of protecting and recovering data as a result. Personal users can apply the same principles to protect their family's personal data, which might include years of family photos and film, financial information, and more.

Use out-of-band back-ups. Many people back up their information to external hard drives connected to their computer. As a result, if the computer hard drive fails, they still have the information on the external hard drive. Given recent trends in ransomware (such as CryptoLocker), backing up key information to an external hard drive may not work, as the adversary will encrypt both your computer and the external hard drive and demand a ransom in order for your data to be returned. The risk remains in the case of natural disasters, such as a house fire or flood; if the hard drive is physically in the house, a person can lose the data as a result of the event. Too many people have lifelong memories, photographs, and videos that are too invaluable to leave at risk. Backing up that information, and protecting the back-up, should not be viewed as an "expense," but instead as an insurance policy.

How can data back-ups be protected out of band? The data owner should assess the method that works best for them, but some techniques include:

- Physically keeping the back-up out of the residence or business, and at an alternate location.
    - The data back-up should be updated on a regular basis and then moved offsite.
    - Advantage: data is not connected to the Internet and has a low risk of exposure.
    - Disadvantage: having to consistently move data to an alternate location after updating the back-up system, and risk of physical theft.
    - If this method is used, data owners should consider encrypting the data to protect it in the event of physical loss.
- Utilizing well-known and well-protected cloud-based back-up services.
    - Advantage: real-time back-up of information keeps your data back-up up to date in the event of data loss from your computer.
    - Disadvantage (risk): information is now stored on an Internet-connected device.
    - It is important to always protect your username and password for any cloud service provider to ensure the confidentiality, integrity, and availability of the data and user account.
    - If your home computer is compromised by malware, you should immediately change your cloud back-up password (refer to the Week 1 post on the security advantages of using Two-Factor Authentication with cloud service providers).

Patch and update operating systems and software when vulnerabilities are identified. Hackers utilize vulnerabilities to deploy malware to systems, and then proceed to move laterally within a network (including home networks). Most operating systems and many software packages offer auto-update features, which should be used to download and apply those patches in a timely manner. Patching is important not only for home computers and laptops; other devices also need to be patched, including phones, tablets, webcams, home thermostats, etc., as they can provide a pathway into the rest of your home network. (Read more about these "Internet of Things" devices in the Week 2 Public Service

Announcement). Protective software, including anti-virus and personal firewalls, should be installed and kept up to date as well.

Manage your home user accounts, especially those with “privileged” access. It is convenient for home users to operate as the administrator on a home computer in order to install software as needed, but by always being logged in on an admin account, malware can be installed without a user’s knowledge. Utilize your administrative account when you intend to install software for a defined purpose, but do all your e-mail, web surfing, and social media activity from a standard user account. This way, if you click on a link to a nefarious website, your computer is less likely to be compromised in a way that offers the actor the ability to install malicious software. Similarly, always change the default username and password for your router or other Internet-connected devices. Hackers have become proficient at exploiting default usernames and passwords supplied by manufacturers on many devices, to compromise a home network. Ensure you are using strong passwords on those devices.

Think before you click. The most common method of cyber exploitation is phishing attempts. When a user clicks on a link to a website within an e-mail, they become vulnerable to credential theft or compromise by malware. If you receive an e-mail that asks you to click on a link to log in to your bank, social media account, or other online account, leave your e-mail and type the actual URL of the website into your browser. Cyber criminals can make it appear in an e-mail that you are visiting the right account, but instead they are collecting your username and password. Additionally, if you receive a document, spreadsheet, photograph, video, etc., via e-mail from an untrusted source, or even an unexpected message from a trusted source, first check with the source to ensure the e-mail is legitimate before clicking on the attachment.

Protect your mobile devices from cyber snoops in public places. If you log in to a Wi-Fi hotspot at your favorite coffee house, an airport, or a hotel, recognize that not all Wi-Fi hotspots implement strong security protections. In many cases it is easy for the person sitting next to you, in the vehicle outside, or in the room across the building, to “sniff” traffic as it passes through the network. By doing this, they can collect all the content of your communications and your login information to sensitive sites. You should avoid logging into sensitive accounts (such as banking, social media, and e-mail accounts), but when you must, you should utilize a well-known personal Virtual Private Network (VPN) service provider. A VPN encrypts your data and adds a layer of security to your communications, which makes it much more difficult for cyber snoops to steal.

If you sell or donate your computer, tablet, phone, or other device, use disk wiping and cleaning software to forensically clear your data before you release the device. Simply deleting information or performing certain types of formatting will not protect data from being recovered. By using commonly available wiping software, you can overwrite the data with random information and ensure your data cannot be recovered by those who might abuse it.