What is on your Business Network

How to secure your business with today’s Internet risks

June 20, 2017
David Mandala

Who is David Mandala?

- I’ve worked in the Electronics and Computer Industries for 40+ years.
  - I’ve been with 7 startups, the principal of 3 of them.
- Spent the last 10 years developing embedded computer operating systems or improving them.
  - Ubuntu Linux for ARM System on Chip (SoC).
  - Improving Linux for the ARM SoC’s with Linaro.
  - Standardization of the 96Boards platform so that binaries run on any board without recompilation of source code.
- Started **Secured by THEM LLC** to specifically help small businesses secure their business computers and networks.

I’ve come to talk to you about office network security

- Today the Internet is pervasive, nearly every business has an Internet connection.
  - Weekly you see in the news new computer ransomware or leeching attacks (data loss).
    - Target
    - Chipotle & Pizzeria Locale
    - The Buckle Inc. 450 stores hit between Oct. 28, 2016 and April 14, 2017
    - InterContinental Hotel Chain
      - 1,175 properties on the list: Holiday Inn Express (781), Holiday Inn (176), Candlewood Suites (120), Staybridge Suites (54), Crowne Plaza (30), Hotel Indigo (11), Holiday Inn Resort (3)
    - Other hotel chains: Kimpton Hotels, Trump Hotels (2x), Hilton, Mandarin Oriental, and White Lodging (2x). Card breaches also have hit hospitality chains Starwood Hotels and Hyatt.
  - Laptops are more prevalent, a lot of small business owners are both working from home and from a small office.

I’ve come to talk to you about office network security

- Today the Internet is pervasive, nearly every business has an Internet connection.
  - Smart low cost Devices are widely available, they are connected to the Internet. They are called Internet of Things or IoT for short. 6.4 Billion were connected to the Internet at the end of 2016, 20.8 Billion expected by 2020.
    - These devices can easily end up in your office providing points behind your firewall to attack your business computers and network from.
- If you use a home office, it is likely to be even riskier.
  - More IoT devices, more friends connecting unknown devices to your network.

Some of the smart devices available

- There are more more than **43 classes** of IoT devices sold on Amazon alone:
  - Smart Lightbulbs
  - Smart Locks
  - Smart Wall Plugs
  - Smart Light Switches
  - Smart Wall Touchscreen
  - Smart Thermostat
  - Smart Garage Door Opener
  - Smart Blinds
  - Smart Curtains
  - Amazon Alexa
  - Amazon Dot
  - Smart Keyrings
  - Smart Egg Minder
  - Smart Blu-Ray Player
  - Smart TV
  - Smart Outdoor Switch/Plug
  - Smart Trackers (keys, luggage, etc)
  - Smart Speakers
  - Smart Cameras (security)
  - Smart Alarm Systems
  - Smart Pet Feeder
  - Smart Smoke Detector
  - Smart Carbon Monoxide Detector
  - Smart Air Quality Detector
  - Smart Landscape Lighting
  - Smart Home Controller
  - Smart Doorbell
  - Smart Pet Treat Feeder / Camera
  - Smart Weather Station
  - Smart Plant Watering Device
  - Smart Garden Sensors
  - Smart Picture Frames
  - AeroGarden with WiFi
  - Smart Plant Pots
  - Smart Sprinkler Controller
  - Smart Crock Pot
  - Streaming Media Player
  - Smart Coffee/Tea Pot
  - WiFi Video Projector
  - Smart Robot Vacuum
  - Smart Range
  - Smart Microwave
  - Smart Dishwasher

How can we tell what is on a network

- To protect a network we need to know what is on the network, how do we do that?
  - Use NMAP to do scans of the network
    - A fast lightweight ping scan can be done in seconds, but does not tell us much about devices attached to the network. So use to identify hosts that need deeper scanning. We log the results to the cloud.
    - A deeper OS fingerprinting scan is run based on the ping scan. We get info on what OS the device runs. This is also logged to the cloud.
    - A deeper full port scan is run on discovered devices. This is also logged to the cloud.
  - We build a map of the machines on the network, the ports they use over time. This becomes the baseline of the network.

How can we tell what is on a network

- Once we build a map of the machines on the network, and the ports they use over time.
  - Compare this to a manual inventory of the network, they never match.
    - Have to locate the extra hardware and determine what is actually needed.
  - We run continuous scanning of the network. All sent to the cloud.
    - We compare the current scan to the baseline scan,
      - We do not alert if machines are missing, it's a normal condition. Machines come and go all the time.
      - If extra machines are found alarms are sent.
        - Most alarms are false, business added more machines, forgot to call.
      - If new ports on an existing machine are opened we alert.
        - Usually caused by software upgrade or new software added to the machine.

How can we tell what is on a network

- Also use NMAP to do scans of the firewall from the outside.
  - If the company has a stateful firewall sometimes sets off alarms.
  - Can spot misconfigured firewalls sometimes.
- Do a manual review of the firewall, make sure security holes are turned off.
  - Shocking how many firewalls have UPnP turned on by default. This is a mistake.
    - What are the problems with UPnP?
      - **Programming Errors –** there are oversights in the actual code for UPnP implementations that can be exploited by malicious users, allowing them to execute harmful code through injection.
      - **Unintended Exposure** – the purpose of UPnP is to make devices on a network easily discoverable by other devices on that network. Unfortunately some UPnP control interfaces can be exposed to the public Internet, allowing malicious users to find and gain access to your private devices.
      - If a malicious device gets installed behind your firewall it can open holes in your fireall.

How can we tell what is trying to access the network

- We make use of managed switches to setup a monitor port on the firewall
  - Allows use of Snort to see attacks on machines that access the internet.
    - Using Open Source rulesets, could use commercial rulesets if desired.
    - If Snort alerts we send alarms specific to the machine that was attacked.
  - Allows logging of every data packet that traverses the firewall.
    - Packets are stripped of the data load and IP and port info is logged for 90 days
      - Outside IP addresses are matched against a GEO-IP database to determine who/what each data packet connects to.
      - Daily traffic reports are generated. Particularly useful if Snort warned that a machine was attacked but attack was thought to be unsuccessful. Can watch the traffic for a few days just to make sure nothing unusual is happening.
      - Can also see if large amounts of data are going to “odd” places.

What easy steps can I take to secure my network

- For wired devices use managed switches to setup vlans (virtual lans) to isolate classes of devices from other devices.
  - Flat networks are old school, with the advent of low cost managed switches even small businesses can afford to have a layered network.
  - Put wired IoT devices on their own vlan, if you have enough IoT devices out classes of devices in vlans (they are cheap to create).
- Put all of your “Smart” IoT WiFi devices on their own “guest” network. By doing that they don’t share your office network and they can’t reach anything in your office.

What easy steps can I take to secure my network

- If you provide WiFi access for your customers when they visit your office, have a private “guest” network for them, separate from your primary network and separate your “IoT” network. Remember their computers could be compromised and have viruses or already be cracked by criminals.
- Make sure all of your guest networks have strong password protection.
- If you don’t need WiFi for your office network, don’t set it up, the safest network requires physical access, if the only way to access your network is via wire it’s more secure. Remember WiFi goes through walls and ceilings, someone could be in the parking lot or in a multistory building above or below you trying to access your network.

What easy steps can I take to secure my network

- Where possible you can greatly add to your data security by:
  - Encrypting the entire hard drive.
  - Adding 2 factor authentication (2FA)
  - Turn off devices when not in use.
- You can use 2FA with many social sites, if they offer it, use it.
- Some mobile phones offer 2FA making use of the fingerprint scanner some mobile phones have built in. Better than nothing but not a great idea, you leave copies of your fingerprints EVERYWHERE! They can be copied and used against you.

What easy steps can I take to secure my network

- Backup your data daily. This should be part of your daily process, do work, backup work. If you don't you have no one to blame except yourself if you lose data in a ransomware attack.
- Finally most importantly use STRONG PASSWORDS on all of your computer systems. Use password manager software if you can't remember long passwords, then protect the password manager software with a long passphrase, 60 - 120 characters long.
  - LastPass 4.0
  - RoboForm 8 Everywhere
  - And don't write down passwords EVER.

If I do everything you suggested will I be secure?

- You'll be more secure than if you don't, but the truth is this only scratches the surface. There is no such thing as a completely secure device, only levels of security.
- Security is like an onion, the more layers you have the more secure you are.
- Criminals can still crack your firewall, or infiltrate via email attachment.
- Everyone's network is different, I can't address exact issues in a general talk. Feel free to reach out and talk with me. (info at them dot com)

Questions?

Reference Links

Password Vault:

https://www.lastpass.com

https://www.roboform.com/

Whole disk encryption:

https://www.veracrypt.fr/en/Home.html

https://www.microsoft.com/en-us/store/d/windows-10-pro/df77x4d43rkt/48DN

Comparsion of veracrypt and bitlocker: http://lifehacker.com/windows-encryption-showdown-veracrypt-vs-bitlocker-1777855025

Secured by THEM

https://www.them.com/ or info@them.com or (469) 298-8436

Thank you for your time.

June 20, 2017
David Mandala

WHO'S ON YOUR NETWORK?