# Securing your Business Office

How to add more security your business/home with today’s Internet risks

January 19, 2018
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.
- In 2017 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).
    - Equifax
    - 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.
  - Now we have discovered 20 year old computer CPU design failures that greatly expose our systems to being cracked.
    - Meltdown & Spectre

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

- Laptops are more prevalent, a lot of small business owners are both working from home and from a small office.
- Today most people, if not all business people have a very powerful pocket computer (they call it a smartphone).
  - Most don’t protect them at all.
  - Most everyone hunts for places offering free WiFi to save on data charges.
    - Some of those “free” WiFi points are hackers just waiting for you to log on so they can try to crack your device.  Remember “There is no such thing as a free lunch”.  There is ALWAYS a price.
  - Too many people trust caller ID.
    - Never ever trust caller ID, it’s very easy to spoof. NBC news showed on national TV exactly how easy it is to spoof.

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

- 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.

# What kinds of IoT can I buy today?

- 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

# What kinds of IoT might migrate to the office?

- There are more more than 43 classes of IoT devices sold on Amazon alone:
  - **Smart Lightbulbs**
  - Smart Door 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

# So there are a “Iot” of IoT things, who cares?

According to:

- James Lyne, global head of security research at Sopho:
  - "IoT devices are coming in with security flaws which were out-of-date ten years ago you wouldn't dream of seeing on a modern PC"
  - "Maybe that wireless kettle isn't an interesting target, but if it helps you see across to the PC where all the goodies are, that matters"
- Cybersecurity expert Bruce Schneier:
  - "Given how experts have repeatedly warned IoT devices do pose a potentially huge security risk, why isn't more care being taken by those producing and selling them? That's largely because the IoT is so new that standards don't exist and vendors are reluctant to spend money on security for products that might not take off anyway."

In short, since no one else cares, you should care for your own security.

# OK, some IoT devices are not secure, so what?

- Just because IoT devices are small does not mean the computers in them are small.  Many devices are very powerful computers.
  - They can be used to stage attacks on your network and PC's on your network.
  - They can monitor (sniff) traffic on your network.
  - Worse, they can be used to crack your PC's and installing ransomware to force you to pay up to gain access to your data.
  - Worse than that, they can be used to crack your PC's and steal your personal info including your banking info, and direct your bank to send money to them, and it looks like you ordered the money to be sent.  It's really hard to prove you did not send the transaction since it is coming directly from your own computer.
  - Finally imagine if all of your customer data was stolen and you had to tell all of your customers that their data had been stolen from your care!  Would you still be in business?

# What easy steps can I take to secure my network

- Check your firewall / Access Point
  - Make sure the firewall functions are turned on (shocking how many aren't).
  - Make sure to turn off all UPnP functionality. You don't want the risk in your office.
    - This was invented to make it easier to do network gaming, it was a bad idea.
  - If your WiFi Access Point is integrated into your firewall make sure to turn on guest network functions. If your firewall does not have a guest network option replace it.
  - Ideally if you provide WiFi for your customers the customer WiFi network should be in front of your private office network. If you can't do that at least have a private "guest" network for them.
    - Separate them from your primary office network. Remember their computers could be compromised and have viruses or already be cracked by criminals.
- Make sure your PC bios/firmware is up to date. Check the vendor website.
  - Do the same with tablets, printers, switches, and your firewall.

# What easy steps can I take to secure my network

- Make sure your anti-virus and anti-malware software is completely up to date and the latest version on ***ALL*** of your devices.
  - **Never turn it off**… Some Windows machines can be cracked in seconds…….
  - You say “But I have to turn it off to install new software.”
    - If there is absolutely no way to install the new software with your anti-virus and anti-malware software running, disconnect your network connection, then and only then disable your anti-virus and anti-malware software and install your new software. Then re-enable your anti-virus and anti-malware software. Then and only then reconnect your network connection.

# What easy steps can I take to secure my network

- 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.  Then criminals can’t use insecure IoT to steal from you.
- Make sure all of your guest networks have strong password protection.
- If you use a home office, it is even riskier, use guest networks to mitigate.
  - More IoT devices, more friends connecting unknown devices to your network.
- 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

- If you use a laptop you can greatly add to your data security by:
  - Encrypting the entire hard drive.
  - Adding 2 factor authentication (2FA)
- Your office desktop security likewise can be improved by encrypting the entire hard drive and 2FA
- 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?

- Large companies have entire departments focused on security, many hire expensive external companies to help small businesses don't have that luxury.  That said:
- 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.
    - Phishing is a real and significant problem, ***NEVER*** click on an email attachment until you talk to the person that supposedly sent it to you…. ***NEVER***.

# If I do everything you suggested will I be secure?

- In closing let me say 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).
- Additional layers can include:
  - **Firewalls with active deep packet inspection**
  - **Security Audits**
  - **Active Network Scanning**
  - **Penetration testing**
  - **24x7 Network monitoring**

# 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.

January 19, 2018
David Mandala


WHO'S ON YOUR NETWORK?