Cyber Security in Today's World

A Presentation for the Southwest Movers Association

September 13, 2018
David Mandala

Who is David Mandala & What Does He Know?

- I've worked in the Electronics and Computer Industries for 40+ years.
  - I've been with seven startups, the principal of three of them.
- I 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.
- I started **Secured by THEM LLC** to specifically help small businesses secure their business computers and networks.

What is Cybersecurity

Cybersecurity, computer security, or IT security is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

- Wikipedia

But my data is not worth anything……

Really?

Ka ching

- Stolen credit card info, paid for in untraceable cyber currency such as Bitcoin, can sell for anywhere from $5 to $250 each.
- Email addresses (useful for phishing campaigns) sell for $10 to $15 per thousand.
- Online bank accounts in the U.S. sell for two percent of the account balance.
- PayPal accounts can net six to 20 percent of the balance.
- Stolen health insurance information can bring in a whopping $1,300 per record.

According to Havocscope, the global black market price guide.

Cyber Attacks Occur by the Second

Cyber attacks are up all across the Internet, both personal and business networks. Business size is irrelevant, many attacks are by bots* that have no idea of size or even business type.

- Phishing & Spear-phishing both email and phone
- Brute force attacks on:
  - FIrewalls
  - Exposed Computers
- Port probing on Internet servers looking for exposed information
- SQL injection attack (drain your database information)
- Ransomware (the least of your problems)

* A piece of software that can execute commands, perform password or overflow attacks, either automatically or with minimal human intervention

Don’t Fall for Phishermen

The attacker tries to manipulate you into giving them either your information, or access to your computer’s so that they can get the information themselves. This can take place through many types of communication, including the telephone (vishing), email (phishing), text messages (smishing) or chats within games or apps. The aim of social engineering is to exploit human nature by targeting common human traits such as the fear of being attacked.

Don’t Feed the Phishermen

Social media can be a major source of information about you and your business.

- New hires proud of getting hired at a great company can give out lots of info by accident!
- You, your spouse, your kids can supply all kinds of information that can be used against you or your employees.
    - Don’t feed the phishermen, be careful of posts, have clear rules of what employees may and may not post.

Don’t Assume Any Email is Legitimate!

If you get an email that appears to come from a company you know, and it says that you owe money or you need to click HERE to verify your account **DON’T DO IT**.

This is an example of a **Phishing Email**.

These emails falsely claim to be from legitimate vendors and typically try to dupe the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information.

A good rule of thumb is to not click any links in an email. Instead go to the site by typing the address into your browser, or call the phone number on the company website. You can then verify if the email was legitimate.

It’s an Easy Trick

Criminals frequently send email that appears to come from someone you know. They’ll disguise malicious software as images or documents attached to these email messages.

Word to the wise: You should never open or download email attachments from any email without confirming with the person that supposedly sent it to you.

So how can customers know email is really from me?

Use a Secure Email certificate, this adds security and authenticity to your email communications. Encryption keeps your email private, digital signing ensures the integrity and authenticity of the message. It's easy to have all email from your company signed.

https://www.comodo.com/e-commerce/email-certificates/email-privacy.php

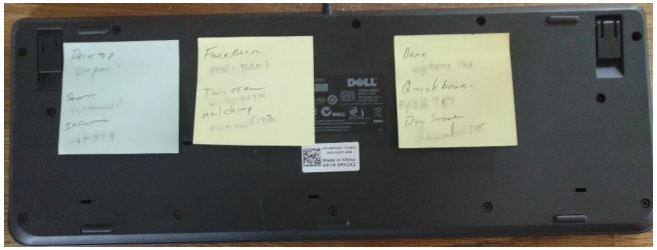
What to Do?

- Keep up to date on major security breaches. If you have an account on a site that's been impacted by a security breach, find out what the hackers know and change your password immediately.
- Be suspicious of unsolicited phone calls, visits, delivery people, or email messages from individuals asking about you, your employees, your colleagues or any other internal information.
- Use a VPN to Hide Your IP Address, your IP address can tell people geographical data and, with some digging, can be cross-referenced with online activity to reveal a rather disturbing amount of your information.

Have you ever seen this?

Do you know anyone that has a monitor like this?

Or a keyboard like this:



Fix the easy things first

Your first line of defense against hacking is the easiest your password and your employees passwords

- First use STRONG passwords, 15 char or greater (I like 50+) totally random
  - Since no one can remember long random passwords use a password manager, there are some very good ones out there:
    - dashlane https://www.dashlane.com/
    - RoboForm https://www.roboform.com/
    - StickyPassword https://www.stickypassword.com/
    - keeper https://keepersecurity.com/
    - LastPass https://www.lastpass.com/
    - zoho https://www.zoho.com/vault/
    - 1Password https://1password.com

Password Manager? How do I protect THAT!!!

- How do I protect the password manager? After all if the hackers crack that they have ALL of my passwords!
  - Use a USB hardware password manager key like ONLYKEY
    - It locks when powered off
    - Take a 7-10 pin number to unlock
    - Can store
      - Up to 24 long random passwords,
      - An ssh private key
      - PGP/GPG keys
      - 2FA Bits (U2F, YubiKey OTP, Google auth)
    - It erases itself if too many attempts at unlocking it
    - Can be purchased from Amazon!

Brute Force Attacks

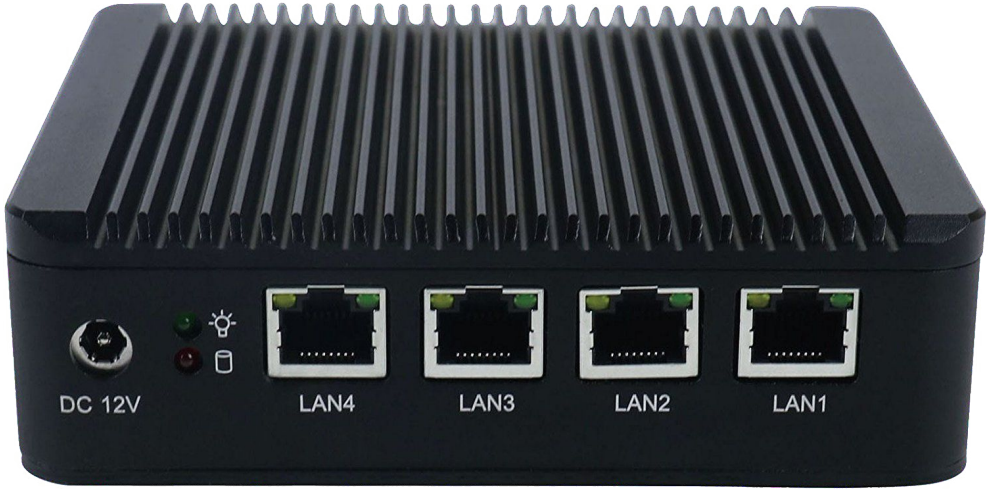
You can't really stop them from trying but you can take steps to protect yourself and your systems. **Know if you are under attack:**

- Read your firewall and computer logs regularly or pay someone to do so for you e.g., Managed Services
- Install a real multi-zone firewall, don't trust or rely on your ISP (business or home).
  - Don't have a single zone flat network, network segregation is critical today, even on your home network.
    - Have multiple zones, internal, internal shared, external. If one zone is violated the others are still safe.
    - Devices that come and go on your network need to be in a separate zone, after all they could get infected at a coffee shop or at some other network

Brute Force Attacks

What is a multi-zone firewall?

- It’s a device that has several Ethernet Ports, 1 to the Internet, several to the networks inside.



Brute Force Attacks

You can't really stop them from trying but you can take steps to protect yourself and your systems. **Know if you are under attack:**

- If you have *authorized* people that remote into your computers (CPA's, Remote employees, External Accountants,) make sure that you are using VPN's or at least restricting access by geo-location. Open ports on your firewall is an invitation to being hacked
- Monitor your network for unauthorized access
  - If you have WiFi turned on and you are not using it, turn it off.
    - If you do use your WiFi and you allow customers/friends to use your WiFi then have private and public zones.
  - Your network should only allow known computers on it. (MAC address restrictions)
  - Purchase or lease an IDS or IPS system for your business, after all you secure your physical premises with a alarm system do you want to do less with your data and finances?
- Have a security audit run, make sure you don't have visitors already

Easy Things to Avoid

- Avoid using public networks; Hackers love public networks
- Don’t use public computers for any business; Could have keyloggers installed
- Avoid downloading unknown applications
- Do not use pirate software, ie software downloaded from unsafe sources, including torrents and other peer-to-peer file sharing. It is not about morality or ethics – it is simply unsafe.

Video Surveillance

- Most of you have some sort of warehouse storage with video surveillance of the space.
  - If you are using direct video cameras into a digital recorder you are in good shape.
  - If you are using a commercial alarm company like “ADT” and they handle your video storage you are also in good shape.

Video Surveillance

- Most of you have some sort of warehouse storage with video surveillance of the space.
  - If you are using cheap IP cameras be careful, many of the cheap cameras transmit all data to a remote website where you send your browser to see the video. Problem is many of these sites don’t have good security and people can see your warehouse and others.

Credit Card Readers - Stay Alert

- ATM's, gas pumps, any kind of a machine where you slide your credit card into the machine are potentially dangerous.
- Before you insert your card, reach out and pull on the card reader, try to pull it out of the device, see if your fingernails catch on any part of the reader and pull; Try to wiggle everything, real machines are solid, with no loose parts or "wiggle"
- ALWAYS cover your hand with your other hand if you have to enter a pin number. The supplied visual cover is not good enough, cameras are so small they can be pasted on the back of the visual cover!
- If at a gas station and you have any reason to be suspicious go inside and pay the clerk.

Credit Card Readers - Stay Alert

Credit Card Readers - Stay Alert

If you have an android phone download and install the “Skimmer Scanner” app it will spot some types of skimmers, but not all of them.

Web Browsing and Staying Secure

- Set your browser security high enough to detect unauthorized downloads
- Limit the use of browser plugins. Disable commonly exploited ones such as Flash Player and Silverlight when you're not using them. You can do this through your web browser under the plugin settings.
- Use a pop-up blocker (the links in pop-up ads are notorious sources of malware)
- When filling out personal information on a site, make sure they aren't asking for your social security number or excessive financial information. Both are telltale signs of a fraudulent website.

Web Browsing and Staying Secure

- Whenever possible use a credit card when paying for something rather than a debit card. Credit cards have limits on what you can spend whereas debit cards are tied directly to a bank account. Make sure and review your statements, to see if there are any unauthorized charges. If there is a discrepancy, it's important to report it immediately.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- When using websites that take info from you make sure they are using secure traffic layers (SSL) so the URL should start with https:// the **s** shows it is secure. Never provide information of any kind to a website that only uses insecure traffic layer: http://.

Your Pocket Computer (smart phone)

- Don’t trust caller ID, worthless anymore
- Don’t trust text messages, (same problem as caller ID)
- Install anti-virus, anti-malware and anti-spyware software. Keep the software active at all times and keep it updated to the most current.
- Avoid using public WiFi.

Your Pocket Computer (smart phone)

- If your devices battery life is suddenly and drastically shortened, malware or a virus could be running.
  - There is a new type of malware out there for phones, it watches the GPS and only starts running when the phone is moving at speed! Apparently the designer realized that most people don't pay much attention to their phone when in their car….

The IoT - Home/Work Automation

The Internet of Things (IoT) are devices that are useful, do things for you and have an embedded computer in them. Items such as video doorbells, thermostats, home audio/video devices, smart TVs, Google Home, Alexa, really any device that connects to Ethernet or WiFi to do something for you.

These devices:

- Generally lack security.
- Will upgrade themselves when they want to or not.
- Should **NEVER** be connected to your main home/office network..
    - WiFi devices should be on a Guest network,
    - Ethernet devices should be on an isolated network, either vlan or totally separate from your primary network. Yes this will take some work to set up.

SOME 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

Ransomware

Petya, WannaCry and NotPetya are all strains of ransomware that affected the computer systems of organisations worldwide. Ransomware is a type of malware that is delivered by social engineering and blocks access to the information stored on your device/system. Users will be denied access to their information unless they pay a ‘ransom’ to the attacker – usually in an electronic currency such as bitcoin.

If you are doing your backups regularly ransomware is an annoyance at best, no backups? Now you have a problem…..

Last but not least!

LOCK your credit report, this should have been done months ago but if you have not done it yet, get it done ASAP. A magic date is Sept 21st, after Sept 21, 2018 it will be ***FREE*** to freeze and unfreeze your credit file and those of your children/dependents throughout the US.

- TransUnion - https://www.transunion.com/
- Equifax - https://www.equifax.com/personal/
- Experian - http://www.experian.com/

I Listened, I Must Be Secure

Even if you do everything I suggest, being 100% securite is not possible.

You will certainly be more secure than before, but the truth is this presentation 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.

Everyone's situation is unique, and must be addressed individually.

Feel free to reach out and talk with me. (info@them.com)

Questions?

Reference Links

Secured by THEM

https://www.them.com/

info@them.com

(469) 298-8436

Thank you for your time.

February 22, 2018
David Mandala

WHO'S ON YOUR NETWORK?