Shadow IT

What you don’t know can hurt you

ISSA New England Chapter Meeting

November 7, 2019

Presented by: Djilpmh Pi

Disclaimers

- Note that any ideas described in this writing are of a general nature and you should consult a security professional you can trust to evaluate its applicability to your specific situation.
- I am not compensated by any of the products mentioned, and the material presented here is intended to be a tickler to stimulate your own thinking and assessment of your information systems and networks.
- Mention of a product or company does not mean I endorse those products, I am making an independent observation only.
- You are responsible for your own actions. And your own inaction.
- If you do have any questions or wish to discuss these points feel free to send a note to djilpmh@ protonmail.com and I will attempt to answer as my resources and availability allow.
- All information presented in this book are found on the public internet; there are no secrets nor proprietary information.
- No animals were harmed during the production of this information. Except maybe the tuna sandwich.

Today: who likes to be right?

- I hope this will be less of a lecture and more of a conversation.
- Call me out if something just doesn't seem righ: Make me defend my point.
- **Turn on your bullshit detector** and set it to "sensitive".

- Later I'll remind you that what we do to support technology has to be an ongoing conversation among people you trust – as with any scientific statement it has to be continuously challenged and TESTED.
- Static statements of "fact" become outdated and irrelevant.

Malicious Compliance vs. Radical Truthtelling

- Term comes from Wsj, October 28, 2019: page R3
- Many (most?) workers just want to get their work done and go home.
- If you impose inflexible policies and rules, those become irrelevant.
- If an adversarial relationship develops between IT and users, the divergence between compliance and security can be aggravated.

- Compare to another term in the article “Constructive Defiance”

Mark Twain is credited with the saying:

"***It Ain't What You Don't Know That Gets You Into Trouble. It's What You Know for Sure That Just Ain't So.***"

If you believe the reports that are sent to management to justify your budget, that is the first sign you're in trouble.

Carl Jung

Carl Jung is quoted (via Jordan Peterson's talks, although Jung might well be referring to an ancient dictum):

"that which you need most is where you least want to look."

What if … ?

- A company issued laptop connecting to company network over VPN is able to host a
  - Internet (directly) accessible web server that bypasses company firewalls
  - Dark Web (TOR) hidden service – web server, ssh server, or IP camera
- File transfers of unlimited size between internal systems and external systems bypassing the security controls that should be enforced by the internet firewall ...
- An internal web server or RDP session is able to be accessed using a proxy (portal, gateway) from anywhere on the public internet …
- Users can run their own copy of portable applications without installation (no administrative privileges needed)

Do you think it's too hard for your people?

In contemporary work environments, if you believe these methods are too difficult for your employees, contractors, and vendors to figure out,

You need better employees and contractors who have more imagination, initiative, and willingness to try new things.

An ordinary day in the office

- You've been working on a project with a customer for a year, building a relationship on a high wire.
- Boss says "I want you to do ONE thing today: send this file to X, I've promised it will be delivered.
- Email fails, the company file transfer caps at 2 Gig, and HelpDesk "will call you back"
- At lunch you express some frustration, and someone says "try this program (e.g., onionshare) on my USB drive". It works.
- Does anyone really want to know if firewalls have been bypassed?

Some examples of Shadow IT

- Onionshare
- IPFS
- Open Archive
- QUIC
- Ngrok

Onionshare

- https://onionshare.org/
- No limit on file size (transfer via streaming)
- Auto shut down of server after one xfer, or can stay running

- Receiver can run TOR browser from USB: https://www.maketecheasier.com/install-tor-browser-usb-drive/
- Onionshare can run in "receive mode" so sender only needs a TOR browser
- When this succeeds, a door is open to TOR (dark web)

Inter Planetary File System

- https://ipfs.io/
- Distributed file storage / sharing

- IPFS is the platform on which D.Tube https://d.tube/ is built
- Initial objective is "anti-censorship" and "anti-centralized control"

- If your confidential information is published to public, it will be very hard to eliminate

Open Archive: a different risk

- https://open-archive.org/
- Secure media preservation: documenting events as citizen journalists with digital proofs – opposite of "fake news"

- Proofmode to establish authenticity of media https://github.com/guardianproject/proofmode/blob/master/README.md
- If your confidential information is published to public, it will be very hard to eliminate

QUIC

- Google Chrome feature – how many of you allow Chrome at work?
  - And have you blocked QUIC?
- https://www.fastvue.co/fastvue/blog/googles-quic-protocols-security-and-reporting-implications/
- Since 2015 https://www.chromium.org/quic
- UDP, encrypted, firewalls can find it problematic to view – not easy like SSL inspection https://blog.sonicwall.com/en-us/2018/09/how-everyone-can-implement-ssl-decryption-inspection/

- "benefits" of using UDP – VPN software uses it for enhancing delivery of packets (higher level protocols check for drops anyway)

ngrok

- Tutorial at https://danielmiessler.com/study/ngrok/
- Docs https://ngrok.com/docs

Example of conflict between policy and current needs

- It is a traditional / legacy policy to prevent internet based systems owned and controlled by non-employees to have administrative access to internal systems (servers, switches, routers).
- Vendors can be allowed inbound but usually through established secure gateways and portals where the vendor's actions are logged and visible. These are typically under specific support contract agreements. Example: Avaya SAL (secure access link)
- In violation of these legacy policies are Cisco Meraki and Juniper Mist cloud based WiFi controllers, which can change configuration of in house WiFi via direct internet connections; you have no idea what vendor staff has access.

What is the long term answer?

- Leadership over the opposing interest groups: the fighting has to stop between:
  - IT, Security enforcing proper standard rules
  - Developers, workers supporting innovative customers and creating new services, apps
- Declare a vision of future and steps to get there

What Can You Do Right Now? Part 1

- Educate and explain:
- basic communication security
- network isolation concepts

- and their importance:

What Can You Do Right Now? Part 1a

Network Architecture – why you have any VLANs in the first place

- Application developers are focused on making their product work. What do they care if your internal IDAM (identity and access management) core servers are protected in your innermost rings of security or exposed to the public internet?
- Explain the corporate network architecture and the reasons for keeping the segments separate.
- Contractors hired to just do a few apps have no idea and the managers who hire them just want them to make the app work; they don't want contractors to waste time trying to understand the network architecture.

What Can You Do Right Now? Part 1b

Network Isolation / Segregation --

- Pet peeve: using the same interface and same subnet for both clients and administrative functions. The reason should be obvious: if systems admin is not accessible (to general purpose network, to public internet), it is harder to attack (but not impossible; for example, see "Stuxnet" and "VLAN hopping").
- IPMI variants such as DRAC or ILO are critically important because they control your server right down to the hardware. See "security vulnerabilities [ilo | drac]"

What Can You Do Right Now? Part 2

- Modern science is not static knowledge: everything is subject to question, testing and 3rd party verification and confirmation of results.
- Challenge everything:
- Challenge more strongly those things that don't make sense – there was a report of interstellar movement 5x the speed of light. So some things are really just journalists trying too hard to be provocative without understanding scientific fundamentals.
- **FIND PEOPLE TO TALK WITH – to do a sanity check without judgment**

What if your internal Domain Controllers …

- Your internal domain controllers and Id/AM servers were compromised?
- Can’t email, Skype, or call with VoIP phones. Or worse, you can, and all your plans are in plain sight to the attackers.
- See Wired story on “Olympic Destroyer” (October 17) –

- Maybe it’s a good idea for a small core team to practice using an alternative communication platform that cannot be monitored by corporate IT and Security tools. Check with your tools to verify it is actually invisible.

Did I Say IT and Security Weren't Important?

IT and Security are more important than ever

- I do apologize that the tone was rather harsh.
- DO continue the basic and appropriate (best?) practices

But

- **DON'T BELIEVE that's all you have to do**

Plus

- IT, Security, Users, Developers, Contractors, all need to work together to create a plan to work together under guidance from leadership.

?

- Questions / Comments

- Let's continue the conversation
- Other projects:
  https://about.me/djilpmh/
- Or email: djilpmh@protonmail.com

- Coupon for free copy: ISSA-New England (Nov 7th until end of Nov 2019)

http://leanpub.com/shadowit/c/dDf7c7ZDwIs9