OFFICE NETWORK SECURITY: HOW TO DO IT

There IS something you can do!

James M. Nachbar, MD, Esq.
ASPS Meeting, San Diego
September 2019

ASPS MEETING, SAN DIEGO SEPTEMBER 2019 RELEVANT INDUSTRY RELATIONSHIPS

I have the following relationships with **Practice Enhancement Specialists (formerly Inform Solutions/Mentor Solutions)**:

- Author of the InSched Scheduling Program & IntelliPract® Billing System and Paperless Charting
- Author of PatientConnection appointment reminder, lead management and patient portal
- I receive royalties for sales, maintenance, and operation of those systems

THE ONLY THING YOU NEED TO WRITE DOWN:

OfficeNetworkSecurity.Com

IMPORTANCE OF INTERNET SECURITY - 2019

- Quest Diagnostics -- June 2019 – 11.9 Million Records – medical info, financial info including credit cards and bank accounts, SSNs, etc.
- LabCorp -- March 2019 - 7.7 Million
- Dominion National dental and vision insurance -- June 2019 – 2.96 Million including SSNs, bank account numbers
- FEMA – Released far more personal info to its contractor than necessary
- Inmediata Health Group – January 2019 – Electronic Health Info was searchable on a public webpage

OCR CONCLUDES 2018 WITH ALL-TIME RECORD YEAR FOR HIPAA ENFORCEMENT

- Anthem $16,000,000
- MD Anderson $4,348,000
- Fresenius Medical $3,500,000
- Cottage Health $3,000,000
- Mass Gen Hospital $515,000
- Advanced Care Hospitalists $500,000
- (Ten total settlements or civil monetary penalties)

- Total: $28,683,400

IMPORTANCE OF INTERNET SECURITY

- HITECH Act requires notification of patients whose records may have been disclosed
- HITECH also provides penalties for unauthorized disclosure
- Viruses to encrypt your data and demand a ransom
- Burglars looking for personal information
- PCI rules for Credit Card security

YOU ARE A TARGET

- A hacker who gets patient information knows you are subject to substantial sanctions for disclosure, and subjects you to blackmail to prevent disclosure

- RANSOMWARE – Your staff opens one bad email attachment, and the next thing you know, your data is encrypted and you can't get it back without paying a ransom

- (hopefully the hackers are honest and give you back your data after you pay, but often they do not)

EVEN THE NSA GOT HACKED!

- The Biggest Risk:
  - **Social Engineering**
- Your staff may be accommodating and naïve
- Just trying to be helpful

TECHNICAL AND SOCIAL ISSUES

- Most computer consultants don't really understand the issues
- But if you tell them what you want, you are much more likely to get it

QUESTION 1

- 1) Are the staff in the office technically able to browse the web from their office computers running your EMR? If they click on a link on a webpage, will the computer load that link?
  - A) Yes, their computers can browse to any website, although they may have been told not to browse on their computers
  - B) Yes, they can browse to certain websites, but there are technical systems in place to prevent their computers from going to non-white-listed websites
  - C) No, their office computers are not connected to let them browse
  - D) I have no idea whether their office computers are set up to be able to browse.

QUESTION 2

- 2) Are the staff in the office technically able to open email attachments on their office computers connected to your EMR?
  - A) Yes, their computers can open email attachments, although they may have been told not to open some or all email attachments
  - B) No, their computers are prevented by technology from opening email attachments
  - C) I have no idea whether their office computers are set up to be able to open email attachments.

THE FUNDAMENTAL PROBLEM:

- You need your computer to do something
- You need your computer to be connected

- The only truly secure computer is the one that is turned off, disconnected, and locked in a guarded closet without power or network connectivity.

- **So, you need to find a balance: Security is not convenient**

THE FUNDAMENTAL PROBLEM:

- You need your computer to do something
- You need your computer to be connected

- The only truly secure computer is the one that is turned off, disconnected, and locked in a guarded closet without power or network connectivity.

- **So, you need to find a balance: what are you (and your staff) willing to live with?**

HIPAA SECURITY RULE

- If you are a HIPAA covered entity (i.e., you bill insurance electronically), you must perform a security review
- You must conduct a risk assessment
- **You must decide what to do about the risks: what is an acceptable balance?**

PRACTICAL GUIDANCE – WHAT TO DO - BALANCE

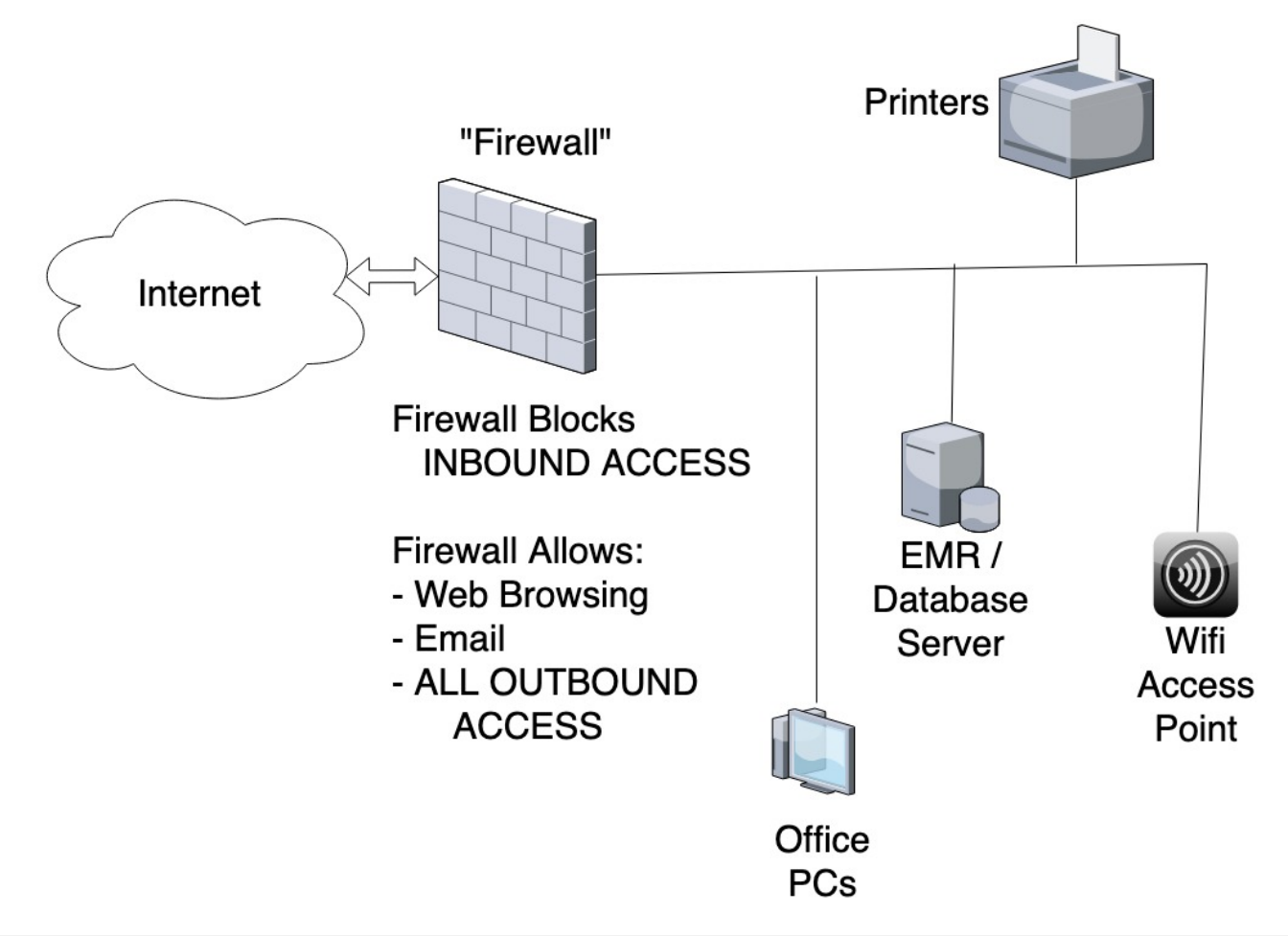
- Go to the HSS.GOV HIPAA website and review security rule information

- Consider looking at the PCI (Payment Card Industry security standard) for specific guidance

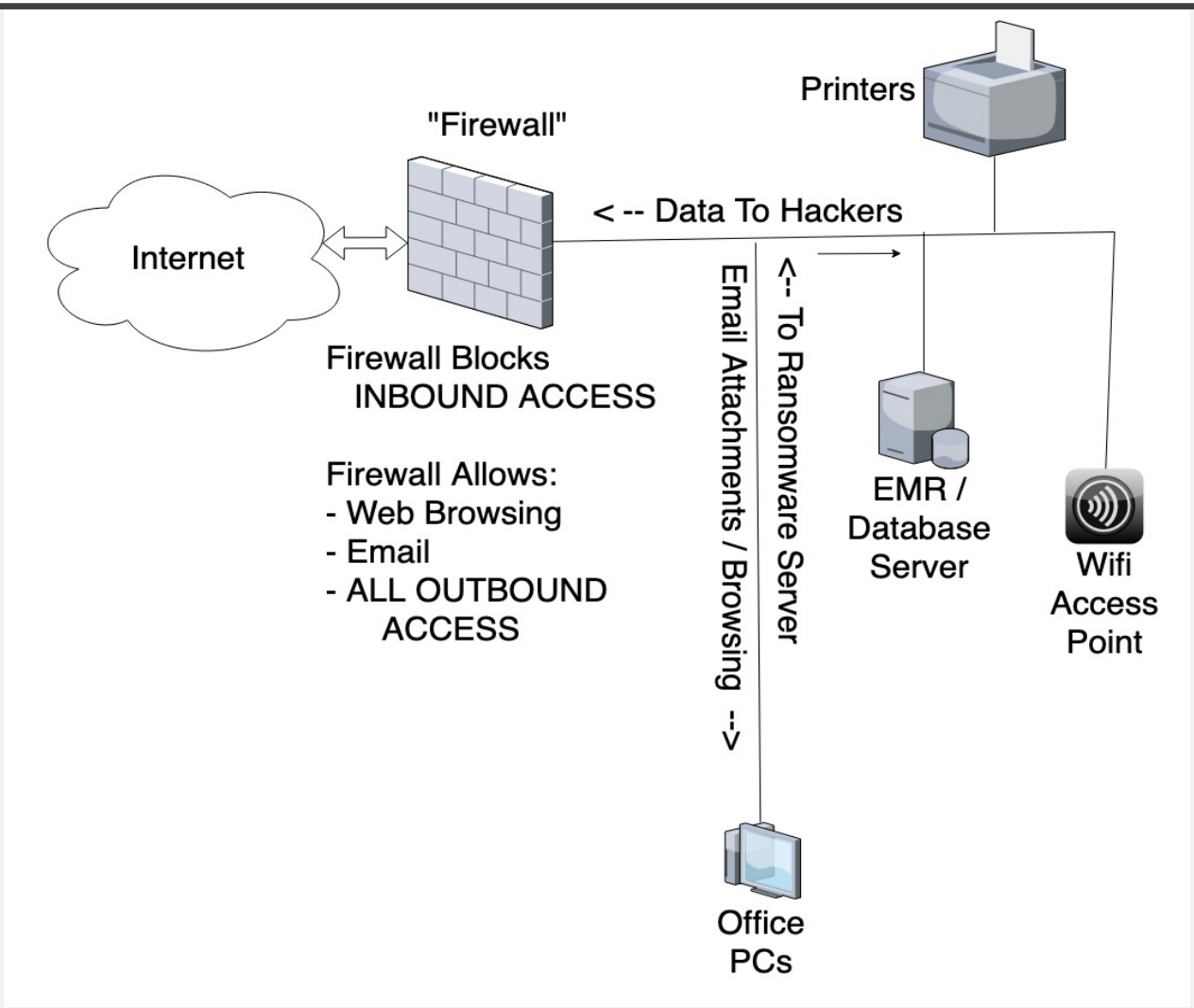
WHAT TO ASK YOUR CONSULTANTS AND VENDORS

- Specific recommendations for how to set up your network
- Even if you don't know how to do these things, you should know to ask about them
- And even if you don't know how to ask them, you need to understand the tradeoffs
- **The Doctor should be the one deciding the balance**

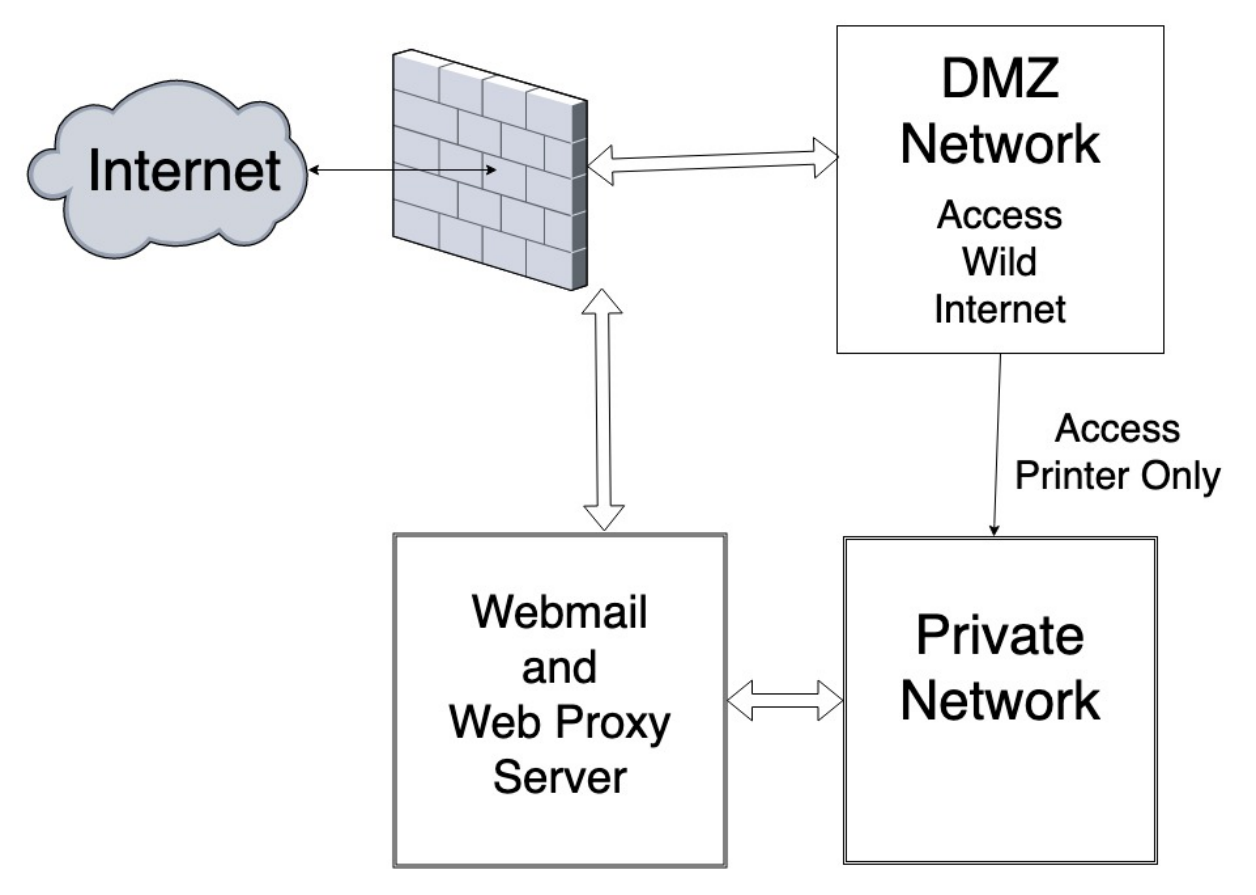
TRADITIONAL OFFICE NETWORK



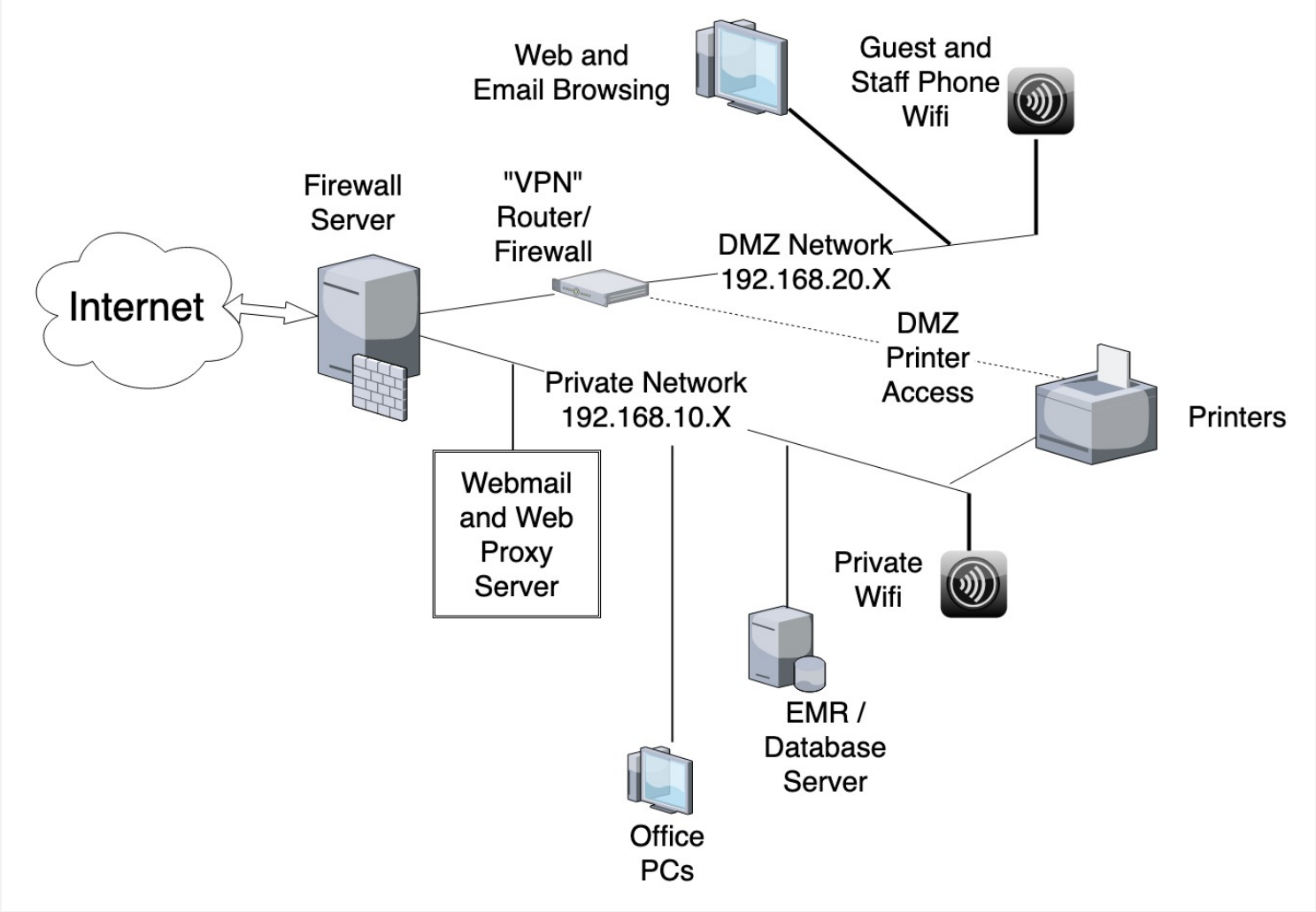
FAIRLY EASY TO ATTACK



HIGH-LEVEL DESIGN – TWO NETWORKS



DETAILED DESIGN – TWO NETWORKS



EMAIL – THE BIGGEST RISK

- Probably the most common way for viruses and other malware to enter your office
- If you let your staff read email on your office network, you are at risk
- They don't know what to look for.
- Subject: "Is this you in this picture?"
- They click on the link, and the virus is installed

EMAIL – THE BIGGEST RISK

- Should not allow staff to read email with attachments on your office network
- One solution: separate network for email
- Another solution: modified webmail browser that does not download attachments – can use browser on separate network to view attachments if needed
- Either way, you need firewall/proxy server to prevent access around your system

EMAIL – THE BIGGEST RISK

- I use Roundcube (free), with the "download" button removed
- Roundcube runs on an office server and has access to an IMAP server for mail
- Firewall prevents email clients from accessing IMAP directly
- Proxy server prevents direct access to "non approved" webmail servers
- IMAP server can be accessed from outside the office network, if needed, using other webmail interfaces, to get the attachments if needed

WEB BROWSING

- Second most common way for viruses to enter your office
- Huge time waster
- But there may be sites your staff needs to use for their jobs
- Solution: Proxy server to limit web surfing
- Solution: Set up DMZ Network for web browsing
- Solution: Do browsing from a computer not on the office network – tablet / phone

PROXY SERVER

- Proxy server is a modified web server that runs in your office
- Requests for web pages are redirected to the proxy server (controlled by settings in your web browser to tell it about the proxy server)
- Firewall blocks direct access from your office computers to the Internet
- All of the software is free, but someone has to set it up

EXTERNAL FIREWALL

- Iptables system (free) within Ubuntu (free) is probably the most powerful – control incoming and outgoing
- Can be set to allow specific "ports" in or out to specific numeric "IP Addresses"
- Your vendors should cooperate by operating outside "standard" ports, like 80 and 443, so your firewall can block the standard ports without preventing their programs from working
- You have to ask which ports have to be opened when you sign up for a service – ironically, credit card processors are the worst, often requiring 443 (https) to be open in order to work!

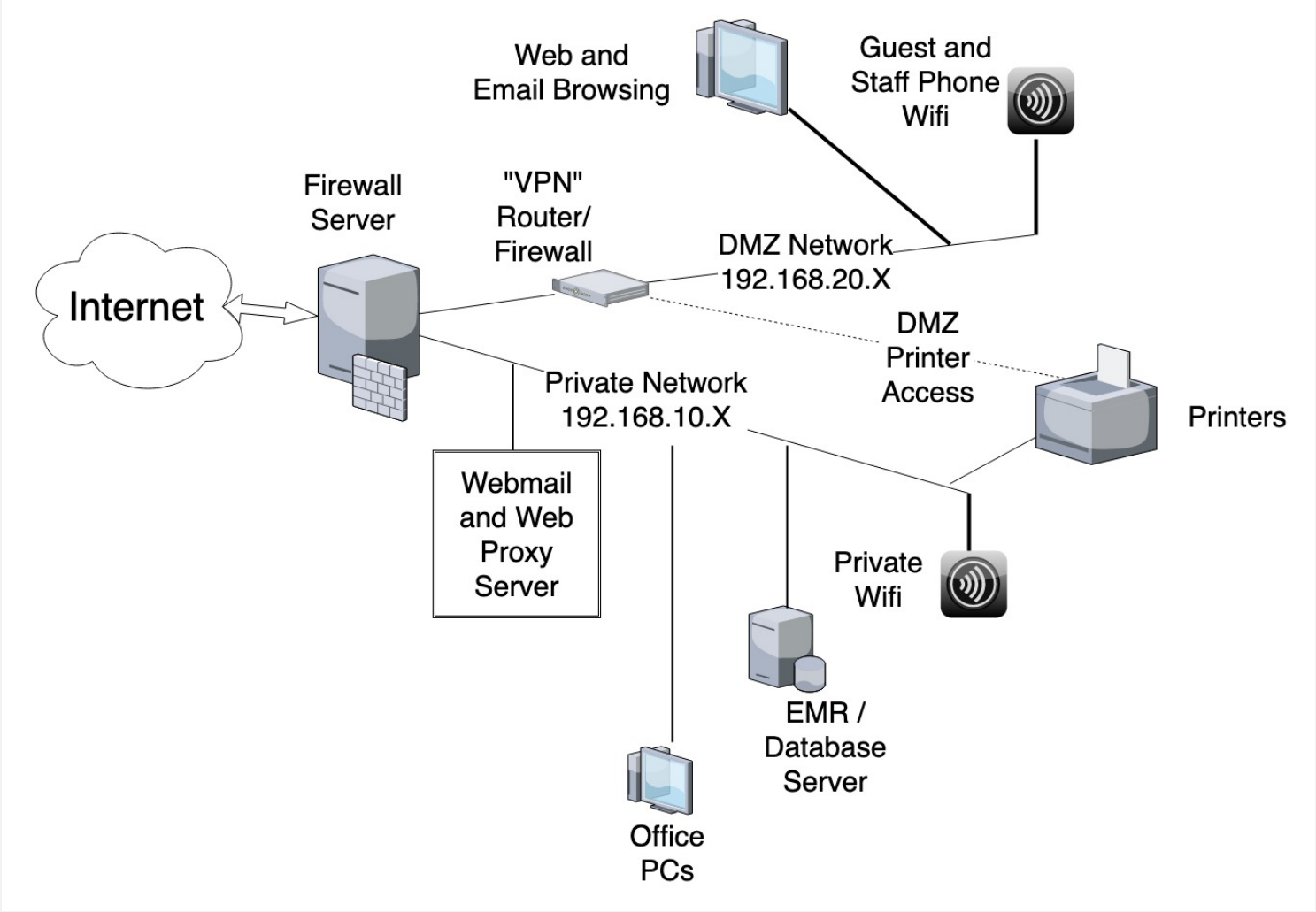
SEPARATE BROWSING NETWORK

- A simple solution might be to block all surfing from office computers – they can surf on their phones!

INTERNET ADDRESSING

- DNS Address: like www.google.com - shortcut for IP Address
- IP (Internet Protocol) Address (IPV4) – like 24.240.80.40 – like a street address for a computer
- Multiple computers inside an office can share a single public IP address via a router
- There is also an IPV6, but not generally usable yet
- "Port" – a number between 1 and 65535 – like a "Suite Number" inside your address – by convention, indicates which service you want
- Standard ports for standard services: 80 for HTTP, 443 for HTTPS, 25 for outgoing email
- You have to block outgoing access to those ports to block access to those services
- It is practical (and recommended) to block ALL outgoing access to ports, so all communications can be controlled by your firewall server, with only specific exceptions as needed

DETAILED DESIGN – TWO NETWORKS



PASSWORD MANAGEMENT

Mark Zuckerberg Hacked!!

His password: dadada

LinkedIn breach, "encrypted" passwords taken & cracked

Same password used for Twitter and Pinterest

PASSWORD MANAGEMENT – "ENCRYPTION"

- Proper password security (since at least the 1980's) is for server system to save only "salted and hashed" passwords
- The actual password itself is never stored
- Rather, an extra and different-for-each-password sequence (the "salt") is added to the password, and then the resulting string is put through a one-way "hash" function
- Then, both the salt and the hashed password are stored.

PASSWORD MANAGEMENT – "ENCRYPTION"

- Both the salt and the hashed password are stored.
- For example: password "dadada", random salt "si28sge", combined = "si28sgedadada"
- Then, one-way hash function => "29diqc39sd3ke"
- No way to recover the password from the hashed string, but can repeat the process with login attempts to determine that password is correct

PASSWORD MANAGEMENT – "ENCRYPTION"

- No way to recover the password from the hashed string, but can repeat the process with login attempts to determine that password is correct
- The problem: if you have the salt and the hashed password (which are stored) and lots of time, you can try lots of passwords to see which work
- You can be sure you are doing it right by starting with your own password
- Many use "guessable" passwords, and many of those use the same password on multiple sites

PASSWORD MANAGEMENT – "ENCRYPTION"

Bottom line:

Some of the sites you use will be hacked

If you use a common or guessable or short password, the hackers will figure it out

If you use the same password on multiple sites, they will have access to ALL OF THEM

If one of the sites does not properly handle the passwords (e.g., ASAPS), it doesn't matter how good your password is

PASSWORD MANAGEMENT

- Don't use the same password for everything (or the name of the site plus a number) and don't use easy passwords
- The best passwords can't be remembered, and if you write them down, they can be found
- Use a password management program – 1Password and others – Apple has announced support in their new operating system
- Should encrypt the data on disk with a "master password". If you forget the master password, no power on earth can get it back.

SHARED NETWORK FOLDERS

- Check the permissions on your network servers
- If "executable" files are "writable" from the logins used by staff computers, a virus that gets into any one computer can easily copy itself into the writable executable files
- Ask what the "minimum required permissions" are
- The loosest security is the easiest to design and support
- If the vendors won't cooperate in your security …

ANTI-VIRUS SOFTWARE

- Microsoft Windows is defective
- Apple OS X is defective
- People have written programs that take advantage of those defects
- ZERO HOUR viruses – released as soon as new defects are discovered, and spread by email and websites before the anti-virus software has been updated to look for them

UPDATING YOUR SOFTWARE

- Especially need to update operating system software, email software, and browsers, because they are exposed to the Internet
- Defects in those programs are discovered and are the basis of new virus design
- Also need to update Anti-Virus programs frequently, so they know about new viruses

EXTERNAL ACCESS SOFTWARE

- Very convenient for your vendor support staff
- Can open an entry point into your system
- E.g., Citrix "GoTo" applications can run on port 8200 so you don't need to open standard ports
- Don't leave external access programs like "LogMeIn" running – turn them on when needed, and turn them off when they are done

CREDIT CARD NUMBERS

- Specific PCI rules for handling credit card numbers
- You can be liable for unauthorized charges if you were the source of credit card numbers
- DO NOT STORE CREDIT CARD NUMBERS (other than the last four digits, to ID the card)
- You are prohibited from storing the CVV ANYWHERE. If a vendor asks you to write the CVV on a piece of paper and fax it to them, you know that they know nothing about security, and should probably find another vendor

ENCRYPTION FOR NETWORK ACCESS

- Use https:, never http:, to access all systems

- Use encrypted access for email sending and receiving – e.g. do not use ports 25, 110, or 143 – they send usernames and password unencrypted (in "cleartext")

WIRELESS NETWORKS

- WiFi, in particular, is a risk for eavesdropping, especially if "unlocked", if WEP is used, or if the password is shared (for example, the hotel WiFi)
- WEP is broken (WPA is safe, as long as the password is good) – any script kiddie can break a WEP network
- Email clients automatically send usernames and passwords in cleartext when you connect
- Best defense is encryption – HTTPS, and encrypted SMTP and IMAP

SUMMARY

- INSIST ON SECURITY FROM THE VENDORS
- Firewall to prevent office computers from accessing the Internet directly
- Proxy Server to allow browsing to specific approved websites
- Do not allow access to email with attachments, and do not rely on email clients to block them – they must be blocked at the server
- Get a Password management program

OfficeNetworkSecurity.Com