Defense in Depth

Securing Your Systems and Data

Brian Pallozzi, CISSP

Principal Sales Engineer

Sample Agenda

1. Security Myths
2. System and Data Risk
3. Changing Your Risk Profile
4. Protection Measures

Common Myths

- “We’re protected – we have a firewall.”
  - Mmmm; crunchy outside, chewy inside.
- “We don’t have anything anyone wants to steal.”
  - Then you won’t mind giving me an administrative account?
- “We’re too small for hackers to want to get in.”
  - You have users? You have data? They want in.
- “If someone tries to […], we would see it in the logs.”
  - Page down is not an effective data mining technique.
- “Our users aren’t allowed to […].”
  - And they always do what they’re told.
- “Microsoft SCEP (Forefront) is good enough.”
  - Sure, if you’re never attacked.

Common Myths

- “Why should I care, I have nothing to hide.”
  - Except passwords, credit cards, bank accounts, …
- “Why would anyone bother attacking my computer?”
  - Sometimes you’re a house, sometimes you’re just a step.
- “It’s too difficult for them to get access to my computer”
  - You use a browser, right? For that internet thing?
- “I made a really difficult password so I can use it on multiple sites.”
  - The good news is they only have to breach one of those sites to use it.
- “If someone tries to […], I would notice!”
  - And the last time you looked at the security logs on your system was …
- “I don’t need antivirus since I don’t go to bad sites.”
  - You might not, but your browser will happily redirect you at any time.
- “I have antivirus so I’m good.”
  - Antivirus is dead, long live endpoint protection.

Setting the Record Straight

- End goals
  - $$$
  - State sponsored
  - Hactivism
- Who/what is the target?
  - It might not be you or your company
    - What other systems/companies do you or your company have access to?
    - Where else might your credentials be valid?
  - You may be only the foot in the door
    - Recon
    - Zombie (Spam, DDoS)
    - Conduit (repository, exfiltrator)
    - Credential/system hopping

Setting the Record Straight

- All data is valuable to some degree
  - Technical use
    - User name, password, department
    - System naming and/or IP addressing conventions
    - Operating systems, service packs, hotfixes, applications
    - Security tools in use
  - Social engineering use
    - Who you are (name, nickname, family, pets, birthdate, SSN)
    - Where you work (company, department, floor, cubicle, remote)
    - Where you live (homeowner/renter, apt/single family, address, phone)
    - Interests (hobbies, organizations, friends (and *their* data))
    - What you have (CC#, bank accounts, identity (financial, online))

Points of Entry and Exfiltration

- Network
  - Internet, LAN, WAP, Rouge switches/WAP
  - Servers, Desktops, Laptops, NAS, Vendor/Guest system, BYOD
- Services
  - File access - HTTP(S), FTP(S/ES/SSL), SMB/CIFS
  - Email - SMTP, POP3, MAPI, IMAP, Webmail
- Endpoints
  - USB's
  - Applications
- Humans
  - Intentional vs. uninformed or oblivious

Tools of Entry

- Network
  - Redirection/Pharming
  - Infected hosts
- Email
  - Malicious attachments
  - Phishing, Spear Fishing, Whaling
- Endpoint
  - Malware on USB's
  - Application/OS vulnerabilities
  - Drive-by's and watering holes
  - User downloads (LAN, Web)
  - Program/Driver "updates"
  - Shared systems

Change Your Thinking

Start with new assumptions

- You are already compromised – you just haven't found it yet
- You are a viable target
- Security is not a "Set it and forget it" capability
- Depending on any single security feature/product is too risky
- 100% protection is an ostrich with its head in the sand
  - You don't know what you don't know
  - Attackers are continuously evolving
  - You don't have endless resources
  - You may be dependent upon other's diligence

Change Your Thinking

Start with new assumptions

- Balance security against acceptable business/personal risk
  - Definition of acceptable
    - Unique to every organization and person
    - Unique to the asset being protected
    - Unique to the threat level of the target
  - Avoid, transfer, reduce/mitigate/control, accept
  - Value of the asset vs. cost of protection
- You will need to expend resources to get and stay secure
  - Time, equipment, and/or money
  - Training (you, your family, your employees, your peers)

Protection Paradigms

Bank Scenario: Teller

- Outside perimeter
  - Doors with deadbolts
- Inside perimeter
  - Guards
  - Surveillance cameras
- Asset access
  - Bulletproof glass
  - Teller conduit
  - Proof of identity

Bank Scenario: Vault

- Outside perimeter
  - Doors with deadbolts
- Inside perimeter
  - Alarm system
  - Surveillance cameras
- Asset access
  - Inner access door
  - Vault door
  - Access controls (time, people, combination/keys)

Protection Methodology

- Identify all assets requiring protection
  - Physical – computers, mobile devices, supporting systems (A/C, UPS)
  - System – OS, Applications, credentials
  - Data – PII, PHI, credit card data, identity data, personal data
- Assign risk level
  - Confidentiality – protect against disclosure
  - Integrity – protect against change
  - Availability – protect against loss of use
- Protect every point of entry
- Protect with an appropriate level of security
  - Attack resistance – how well does it protect asset and itself
  - Initial cost – acquisition, installation, implementation
  - Ongoing cost – maintenance, upkeep, monitoring

Physical Protection

- Prevent against theft
  - Although “noisy”, it gives attackers plenty of time to work on it
  - May provide access to other systems directly or through data on the system
  - May be the only copy of data or latest data
- Prevent against “hands-on”
  - Risk of discovery higher, but allows for unanticipated direct attacks
    - Brute force at keyboard
    - Autorun
    - Hardware sniffers and loggers

Physical Protection

Protect against theft

✓		Dedicated server room
✓	✓	Lock doors/windows
✓		Building/room access controls
✓		Surveillance system
✓	✓	Alarm system (if not 24x7)
✓	✓	Cable lock downs
✓	✓	Don’t walk away from unsecured systems

Physical Protection

Protect against “hands-on”

✓		Dedicated server room
✓	✓	Building/room access controls
✓		Surveillance system
✓	✓	Don’t share the system (alternatively, set up a limited guest user)
✓	✓	Use strong passwords
✓	✓	Use screensaver with timeouts and passwords
✓	✓	Periodically inspect for unauthorized devices
✓	✓	Don’t walk away from unsecured systems

System Protection

- Prevent or limit system access
  - Every other system does not need access to yours
  - Your system may be the end target or just a conduit or attack platform
- Limit access from compromise
  - Limit damage that can be done to your system
  - Stop attacker from gaining access to other systems
  - Don’t be a zombie or conduit

System Protection - Products

Prevent or limit system access

✓	✓	Hardware firewall/UTM/NextGen device
✓		Network Access Control, IDS/IPS
✓		Server and client management system
✓	✓	Desktop antivirus
✓	✓	Desktop firewall
✓	✓	Desktop IDS/IPS
✓		Application, process, and device controls
✓		SIEM and/or MSS

System Protection - Products

Set up your firewall/router properly

✓	✓	Change default logins (**every** default login **everywhere**)
✓	✓	Use WPA2 – only downgrade to WPA if absolutely necessary
✓	✓	Use a strong passphrase/key
	✓	Set up a separate network for WEP-only devices (Corp: buy new ones)
✓		Use certificate/VPN access control
	✓	Set up wireless MAC filtering – use a separate network for guests
✓	✓	Disable UPnP – use a separate network for consumer devices (see WEP)
	✓	Only give out the guest network key – never yours

System Protection – Local System Behavior

Prevent or limit system access

✓	✓	Patch early, patch often (OS and applications)
✓	✓	Install only the applications you need
✓	✓	Remove any unneeded applications
✓	✓	Use a current and supported OS
✓	✓	Use a current and supported browser
✓	✓	Put only truly trusted systems in the trusted sites and only if necessary
✓	✓	Do not reuse your username/password
✓	✓	Do not give your username/password to anyone

System Protection – Online Behavior

Prevent or limit system access

✓	✓	Every site should get its own password (use a password manager)
✓	✓	Use two-factor authentication where offered
✓	✓	Provide/collect the minimum personal details necessary
✓	✓	Download files directly from the author's or manufacturer's site
✓	✓	Verify the file you are downloading is the same type you asked for
✓	✓	Don't click links in email – go to the site directly
✓	✓	Disable Java
	✓	Disable Java Script as a default (enable only if and as needed)

System Protection – Behavior for the Wary

✓	✓	Being on the first page of the search results doesn't mean it is a safe site
✓	✓	Remember even good sites get compromised – don't update flash, reader, or codecs just because the site said you had to
✓	✓	If a site tries to download a file to you when you visit, just leave
✓	✓	The big download button is probably an ad – look for the real one
✓	✓	Look for third-party software in your downloads
✓	✓	That popup window may not really be a popup window
✓	✓	Neither Symantec nor Microsoft are going to call and tell you you're infected and offer to clean it up
✓	✓	The FBI, IRS, DMV, and Interpol is not going to let you pay a fine for viewing that pornography, paying your overdue taxes, or driving on the toll road

System Protection – Behavior for the Paranoid

Prevent or limit social engineering

✓	✓	"Unsubscribing" may add you to the list of valid emails
	✓	Do not respond to questionnaires and surveys*
	✓	Do not list what you own(ed) in your forum signature block
	✓	Limit who can see what on your social site posts
✓		If IT calls and asks for your password, tell them to just reset it
✓	✓	Don't offer company, personal, coworker, or friends details
	✓	If the bank or credit card company is calling you and asking you to verify your account or access details first, call them back at their 800 number
✓	✓	Just because you're paranoid doesn't mean they're not out to get you

*Some exceptions may include web site performance, professional inputs, customer service metrics if they don't violate other rules.

Data Protection

- You have to know what data you're trying to protect
- You have to know where that data resides
- You have to decide what "protect" means
  - At rest, in motion, in use
  - Actions you'll take
    - Notification only
    - Automatic/manual remediation
    - Blocking
- You have to decide what it's worth

Data Protection

- DLP is significantly impacted by access control
  - Least privilege
    - Systems
    - Users
  - Privilege de-escalation
- DLP and backups
  - Ransomware

Data Protection

PII, PHI, credit cards, research, employee/student identities

- Actors
  - Insiders
  - Malicious Insiders
  - Malicious Outsiders
- Options
  - Data at rest – storage
    - Full drive encryption
    - File and Folder encryption
  - Data in motion – email, web
    - Email encryption
  - Data in use – file copy, print, cut/paste
    - DLP agent

Data Protection

PII, PHI, credit cards, research, employee/student identities

- Data Loss Prevention program
  - Policy
  - Discovery
  - Monitoring
  - Notification
  - Remediation

Data Protection

PII, PHI, credit cards, personally private data

- Actors
  - Family/Friends with access
  - Malicious Family/Friends with access
  - Malicious Outsiders
- Options
  - Data at rest – storage
    - Full drive encryption
    - File and Folder encryption
    - Software or hardware based USB encryption
  - Data in motion – email, web
    - Email encryption
    - Secure web storage/sharing

Data Protection – DLP

✓	✓	Data Loss Prevention doesn't stop at discovery; it starts there
✓	✓	Implement least privilege
✓	✓	Encrypt data at rest
✓	✓	Don't send sensitive data through email unencrypted
✓	✓	Don't make an unencrypted copy of sensitive data to "work on at home"
✓	✓	Treat credit card information like cash (your cash)
✓	✓	Beware phishing email
✓	✓	Start dealing with this today; you may already be compromised

Data Protection – Backups

✓	✓	RAID is not a backup solution
✓	✓	Snapshots are only a short-term option
✓	✓	Backups can contain private information; consider encryption
✓	✓	A backup stored onsite is probably useless after a fire, flood, or burglary
✓	✓	A single backup device is a single point of failure

Data Protection – Be Aware

Things to ponder

✓	✓	SMTP is seldom encrypted
✓	✓	Full disk encryption only helps data at rest
✓	✓	Pieces of data can be spread over multiple locations and combined
✓	✓	Your cloud provider may be able to read your data – where is the encryption taking place?
✓	✓	Encryption is only as good as the protection of the key
✓	✓	Deleted data can often be recovered – even from a USB

Final Thoughts

- Trust no one
  - You're about 50 milliseconds from every creep on the planet
  - Yes, some people really are that [mean|greedy|corrupt|depraved|…]
  - Friends today, but …
  - If it's not the NSA, then it's China, or hackers, or …
  - Would you leave your door unlocked? Your wallet on the street?
- Security is
  - Hard
    - You have to be right 100% of the time
    - The bad guys only have to be right once
  - Constantly changing
  - Successful when nothing happens

Thank you!

Brian Pallozzi

brian_pallozzi@symantec.com