16. Account Monitoring and Control

- Why it's important:
  - Inactive accounts are often attacker's path into your system
  - Nobody's watching them
  - Sometimes even "left behind" by dishonest employees

Quick Wins

- Review your accounts and disable those with no current owner
- Set expiration date on all accounts
- Produce automatic daily report on all old/unused/expired accounts
- Create procedure to quickly delete accounts of departed employees

More Quick Wins

- Monitor account usage to find dormant accounts (disable them eventually)
- Encrypt and move off-line all files belonging to dormant accounts
- Lock out accounts after some modest number of consecutive failed login attempts

17. Data Loss Prevention

- Why it's important:
  - Many high impact attacks are based on your data being stolen
  - You need to know when critical data is leaving your custody
  - You need to understand how and why that happens

Quick Wins

- Use full disk encryption
  - On all mobile devices
  - On all devices holding particularly critical data
- Again, encrypt password files especially
- Other measures are more advanced

18. Incident Response Capability

- Why it's important:
  - Probably you'll be attacked, sooner or later
  - You'll be happier if you're prepared to respond to such incidents
  - Can save you vast amounts of time, money, and other critical resources

Quick Wins

- Create written response procedures, identifying critical roles in response
- Ensure you have assigned important duties to particular employees
- Set policies on how quickly problems should be reported
- Know which third parties can help you
- Make sure you employees know what to do when there’s a problem

19. Secure Network Engineering

- Why it’s important:
  - Attackers often break in at one place in your system
  - They then try to navigate to where they really want to go
  - Don’t make that easy

Quick Wins

- Use a DMZ organization
  - Connect private network to DMZ with middleware
- All machines directly contacting the Internet go in the DMZ
- No machines with sensitive data should be in the DMZ
- User education important for this problem, but not quick

20. Penetration Testing and Red Team Exercises

- Why it's important:
  - You probably screwed up something
    - Everybody does
  - You'll be happier finding out what if you do it yourself
  - Or have someone you trust find it

Quick Wins

- Regularly perform penetration testing
  - From both outside and inside your system boundaries
- Keep careful control of any user accounts and software used for penetration testing

Applying the Controls

- Understand all 20 controls well
- Analyze how well your system already incorporates them
- Identify gaps and make a plan to take action to address them
  - Quick wins first
  - Those alone help a lot

Creating an Ongoing Plan

- Talk to sysadmins about how you can make further progress
- Create long term plans for implementing advanced controls
- Think for the long haul
  - How far along will you be in a year, for example?

20 Controls Is a Lot

- What if you can’t take the time for even the quick wins on these 20?
- You have just a little time, but you want to improve security
- What to do?

The Australian Signals Directorate Controls

- A body of Australia’s military
- They have a list of 35 useful cybersecurity controls
- Well, if 20 is too many, 35 certainly is
- But they also have prioritized just 4 of them

The ASD Top 4 Controls

1. Application whitelisting
2. Patch your applications
3. Patch your OS
4. Minimize administrator privileges

- In ASD’s experience, handling these four stops 85% of attacks

1. Application Whitelisting

- Only allow approved applications on your machines
- Use a technology to ensure others do not get installed and run
- Identify apps you actually need to run to do your business
- Outlaw all the others

Enforcing Whitelists

- If running Windows, you can use Microsoft AppLocker
  - Available with post-Windows 7 OSes
- Prevents apps not on the whitelist from running
- More challenging if you're running Linux
  - MacAfee Application Control or configurations of SE Linux are possible

2. Patch Your Applications

- Apply patches to all applications you use
  - Especially those interacting with Internet
- Prefer up-to-date versions of software
  - Older versions may not have patches provided
- Ideally have a centralized method controlling patches for entire system
  - E.g., for Windows, Microsoft System Center Configuration Manager

3. Patch Your Operating System

- Go with most up-to-date releases of OS
  - E.g., desktop malware infections dropped 10x from XP to Windows 7
- Use system-wide tools that will apply patches to all machines you control
  - Microsoft System Center Configuration Manager, again
  - Similar tools available for Linux

4. Minimize Administrator Privilege

- Get rid of methods allowing users to alter their environments
  - Especially those allowing software installation
- Malicious intruders look for these capabilities
- Those allowing access to other machines especially dangerous

Further Controlling Administrator Privileges

- Use role based access control for admin privileges
  - If not available, separate accounts
  - Not normal administrator user accounts
- Avoid allowing admin accounts to have Internet access

Conclusion

- You can’t perfectly protect your system
- But you can do a lot better than most
  - And the cost need not be prohibitive
- At worst, you can make the attacker’s life hard and limit the damage
- These steps work in the real world