Defense in Depth

Layered Information Security Strategy

Defense in Depth

What is security strategy and why do we need one?

Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat. – Sun Tzu

- If we view security "tactics" as the activities we undertake and tools we acquire and use…
- Strategy is how we ensure that each activity and tool work together toward the common goal.

The Old Model – The Walled City

- As in antiquity, we built walls and gates (firewalls, ACLs) to keep the badguys out.
- We put guards on the walls to keep watch (IDS).
- Based on "hierarchy of trust" which places internal users at the top and external users at the bottom
  - Activities inside the boundaries not truly segmented or restricted
  - User policy almost non-existent, geared more towards acceptable use, not security
  - Low levels of awareness training – little emphasis on security outside of Network and System administration roles
- Troy had walls. How'd that work out for them?

What Changed?

- The accidental traitors among us!
  - Modern attack vectors transform users into unwitting accomplices.
  - 49% of data breaches reported in 2010 incorporated malware
  - 11% employed social tactics
  - Hackers figured out that Admins were catching on…so they switched to attacking users

What Changed?

- The badguys changed
  - 83% of victims appear to be targets of opportunity (i.e. Drive by hacking)
    - They don't know or care who you are
  - Most hacking attempts now utilize automated tools – search for vulnerable systems, then exploit, then report back
    - The average hacker is not as technically savvy as in the "good old days"

What Changed?

- Why hack?
  - Money is the new draw
- Often backed by organized crime
  - Identity Theft - a stolen credit card number commanded between $10 and $16 in mid-2007. A year and a half later, the price had fallen to 50 cents. The price drop is due to increased supply.
  - Child Pornography is often served from compromised machines
  - Spammers often utilize compromised machines
  - Distributed Denial of Service Attacks (DDOS) are launched from huge "botnets"
    - The Mariposa botnet controlled 12 million machines in 100 countries before being neutralized by law enforcement in 2009

What Changed?

- The network we were defending changed
  - The lines got blurry
    - Wireless
    - Mobile devices (trusted users on un-trusted hardware)
    - Deeply interconnected organizations sharing data
    - The cloud
- Where is our “boundary” really?
- Defensive strategy had to change.

What is Defense in Depth?

- Concept adapted from military strategy
- Has become accepted best-practice for cyber security worldwide, across industries
- Defenses are layered throughout the network
- Coupled with extensive monitoring
- The Goal - delay an attacker until detection results in a coordinated response

What is Defense in Depth?

- Put simply – Build an *acceptable* level of security into each node and application on the network.
- As any individual security mechanism is compromised…
  - Damage is contained
  - Attacker success is met with yet another hurdle
  - With each compromise, the possibility of detection is increased

Defense in Depth

What are some benefits of Defense in Depth?

- Security is distributed – no single points of failure
- Security can be tailored to business needs
  - Allows your ISO to use the word "NO" less often – We can find other ways to compensate for a vulnerability introduced by a legitimate business need
- Very widely recognized and accepted (i.e. auditors love it)

How you fit in…

- Defense in Depth depends on people
  - Heavy emphasis on training and awareness
  - Recognizes that users are key to good security