Justifying the move beyond defense-in-depth

Ron Dilley

June 23, 2016

Agenda

- Threats (and a story)
- Defense-in-depth vs Interlocking Controls
- Security Controls
- How To Justify
- Next Steps

Security Threats – A quick story

- Why are you looking at this slide, you should be listening to my story

Defense-in-depth vs. Interlocking Controls

- Defense-in-depth
  - Back in the day . . . Castles . . .
  - When I started . . . Multiple layers of firewalls, A/V, etc.
  - Now . . . A list of products sold to us as point solutions
- Interlocking Controls (aka Overlapping Controls)
  - Broad influence (not a point solution)
  - Improves the effectiveness of other controls
  - Monitors for the effectiveness of other controls
  - Can be implemented incrementally

Security Controls

- Old-school may not be shiny, but . . .
  - Control the network
  - Control access
  - Control systems
    - Control applications
    - Control data
  - Detect threats
  - Harden users

How to justify: Define your goals

- Your plan will enable a secure and agile business, not limit it
- Your initiative will quickly enhance your defensible environment
- While strategically sustaining that posture as the threat-scape shifts
- It promotes a security aware culture
- It will progress incrementally on prioritized delivery
- It applies interlocking controls (not defense in depth)
- Your plan includes continual measurement and reporting as a foundational attribute

How to justify: Interlocking Controls

Segmentation

- Divide your networks into pieces
- Limit the scope of a breach

System Management

- Automated builds
- You can see and fix unauthorized changes
- Simple system recovery

Access Management

- The higher the privilege, the higher the control and monitoring

Runtime Management

- See and stop unknown and unsafe applications

IANS

How to justify: Before and After

	Segmentation	System Management	Access Management	Runtime Management
BEFORE	• Attackers exploit flat networks by obtaining a foothold using weak links • Many large breaches have included significant undetected horizontal movement	• Recovery from common malware is very expensive • A malware bloom impacting 500 machines will take months to return to normal operations	• Admin accounts give full access to everything • Attackers go there first	Someone clicks on a malicious phishing e-mail and exposes their computer and all the data they can access
AFTER	• Networks will no longer be flat, limiting exposure • More difficult for an attacker to move without making noise	• Systems will be controlled and managed so all changes are automated • Unauthorized changes will be detected and fixable through automation	Administrative access will be managed and monitored with two-factor authentication using gateways	• Unknown programs will not run on systems until they are confirmed to be non-malicious

Next Steps

- Time for a Columbo?
- Network Security: Reloaded – Marcus J. Ranum