2010 Annual Cybersecurity and Homeland Defense Symposium and Job Fair

Daniel Mintz
COO, Powertek Corporation

9420 Key West Avenue • Suite 210 • Rockville, MD 20850
Tel: 301.795.0400 • Fax: 301.795.0430
www.PowertekCorporation.com

powertek
Your success. Our mission.

Topics

- Context
- Security Thoughts/Emerging Threats
- Demand for Professionals
- Practical Advice

Context

First Principals

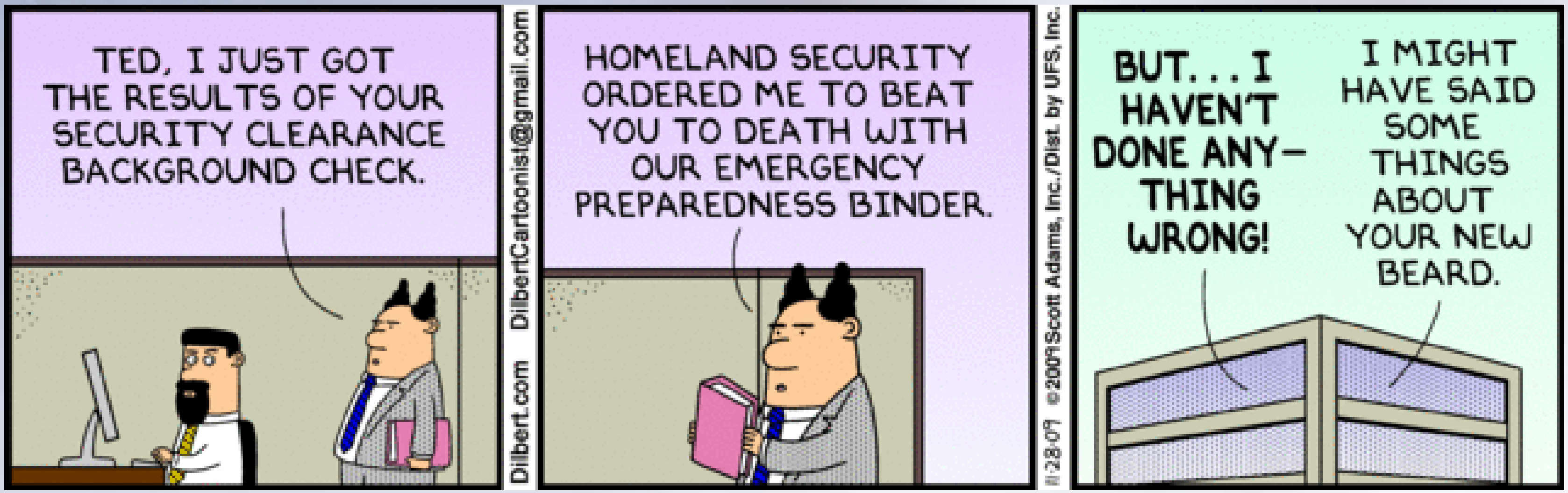
- Nothing from nothing leaves nothing – transactional cost economics
  - Makes it ~~advantageous~~ necessary to utilize external resources as much or more than internal

- Here come the clowns – management and implementation by crowd sourcing
  - The death of hierarchy

- Everybody needs somebody sometime – the Internet of Things
  - Fast sensors

- Ptolemy vs Copernicus vs Warhol, changing approaches to architecture: Earth -> Sun -> Nothing

Security Thoughts


TED, I JUST GOT THE RESULTS OF YOUR SECURITY CLEARANCE BACKGROUND CHECK.
Dilbert.com DilbertCartoonist@gmail.com
HOMELAND SECURITY ORDERED ME TO BEAT YOU TO DEATH WITH OUR EMERGENCY PREPAREDNESS BINDER.
11-28-09 ©2009 Scott Adams, Inc./Dist. by UFS, Inc.
BUT... I HAVEN'T DONE ANY-THING WRONG!
I MIGHT HAVE SAID SOME THINGS ABOUT YOUR NEW BEARD.

Factoids

- McAfee received > 34 million malicious code samples in 2009, will exceed that in 2010
- Operation Aurora, announced by Google, involved multiple high-tech companies probably attacked by Chinese operatives
  - Seems to have started when a Google employee clicked on a link in an instant message
- Cisco estimates that IP traffic will quintuple from 2008-2013, with 667 Exabytes of traffic in 2013
- According to Politico, by 2009, government agencies including Congress were attacked an average of 1.8 billion times/month

Homeland Security

Since the number of targets is essentially unlimited,

since the probability that any given target will be attacked is near zero,

since the number and competence of terrorists is limited,

since target-selection is effectively a near-random process, and

since a terrorist is free to redirect attention from a protected target to an unprotected one of more or less equal consequence,

protection seems to be sensible only in a limited number of instances.

- Professor John Mueller, Ohio State University

SCADA Systems

- They have historically been stand-alone systems operated by the business, not IT
- Moving to common system designs and protocols as corporate IT functions
- Integrated into business systems for real-time information
- Typically distributed physically and logically; more opportunities for data interception, spoofing, and denial of service

A tip of the hat to CSC, which this was adapted from

Summary of Key Challenges

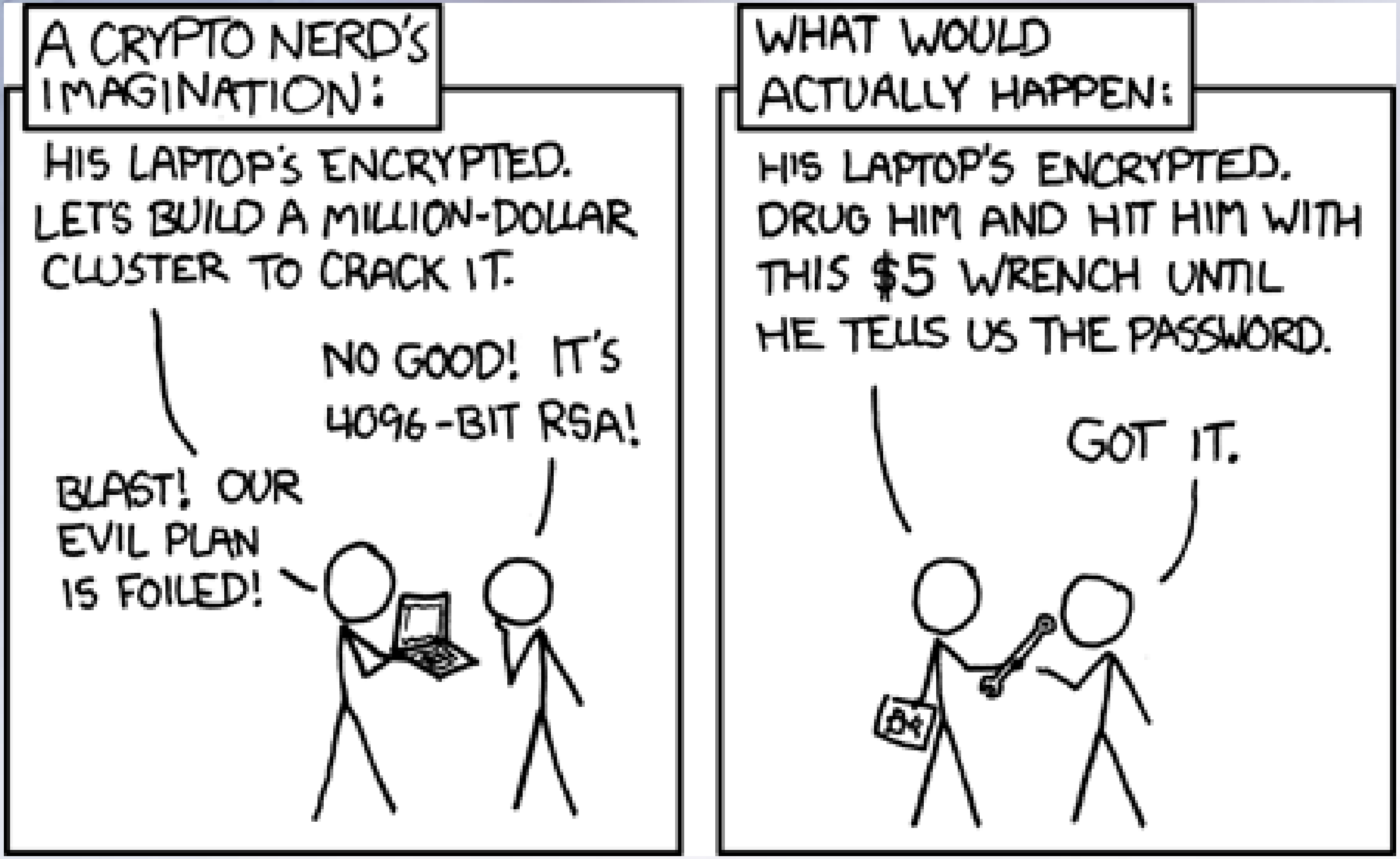
- Need for Public/Private cooperation
- Cloud Computing
  - Inability to quantity security status or define Service Level Agreements (SLA’s)
- Social networking – especially by younger employees
  - Increasing power of commercial ‘end-points’
  - Increasing interconnection to an internet of things
- False positives
- Whack-a-mole approaches to security
  - Inability to prioritize
  - Overemphasis on perimeter security, under emphasis on resiliency
- Difficulty for security professionals to understand or communicate with mission owners

Demand for Professionals

Federal Requirements

- Booz Allen Hamilton Report
  – 76 % of Federal respondents said recruiting skilled cyber security talent a “high” or “top” priority
  – TechAmerica found Federal CIO’s in 2009 rated IT security the top CIO challenge
- Estimates are that having cyber-skills can have as much as a 20% salary premium

Practical Advice


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Goals

- Automated Situational awareness
  - If you do not know what is happening you cannot improve it

- Transparency of status
  - If no-one knows the situation, they can’t help implement the objectives

- Walk and chew gum (e.g. Federal Desktop Configuration Control-like activities)
  - Without these it’s like putting steel plates on a house while leaving the windows open

- Take Business (Enterprise) Architecture seriously

- Build security into the process

Some Advice

- Steve Martin used to tell a joke about how to become a millionaire and not pay taxes
  - Beware the “First, find a million dollars” step 1
- Keep in mind that security is rarely the goal of your organization
  - How do you measure security and risk
  - How do you justify security investments compared to mission investments
  - Understand your organizational culture

Powertek Corporation
9420 Key West Avenue, Suite 210
Rockville, MD 20850

www.powertekcorporation.com

Daniel Mintz, Chief Operating Officer

301-795-0418/o
301-332-0717/c
DMintz@PowertekCorporation.com

Twitter: www.twitter.com/technogeezer
Facebook: www.facebook.com/technogeezer