The Business of Security

How to Allocate Security Resources

Pete Lindstrom

petelind@spiresecurity.com

© 2002 Spire Security. All rights reserved.

Current State of Security

- Point products everywhere…
- Security is an art form…
- No clear guidance on how to secure an enterprise…
- No guarantee of success (even good security isn't impervious to attack)

SPiRE security

© 2002 Spire Security. All rights reserved.

Current State of Security

- Scarcity – never enough resources
- Too many risks – which are most important?
- Unclear objectives

SPiRE security

© 2002 Spire Security. All rights reserved.

Determine Attack Paths

- Public Connection (Internet)
- Private Connections
  - Business Partners
  - Customers
  - Maintenance

SPiRE security

© 2002 Spire Security. All rights reserved.

The First Round – Gut Check

- What are you trying to protect?
  - Asset/system prioritization.
- …from what?
  - Identification of the threats.
- …why?
  - Mission statement.

SPiRE security

© 2002 Spire Security. All rights reserved.

Asset Prioritization

- Apps/systems with valuable information.
- Apps/systems that are used most frequently by most people.
- Apps/systems that generate revenue.

SPiRE security

© 2002 Spire Security. All rights reserved.

Enterprise Threats

- Viruses
- Random attacks from Internet
- Malicious behavior
- Targeted attacks
- Denial-of-service attacks
- …and so on.

SPiRE security

© 2002 Spire Security. All rights reserved.

A Risk Equation

Risk = Threat x Vulnerability x Asset Value

R = T x V x A

(Peter Tippett, TruSecure)

- Basic equation, difficulty in details.
- Easy to understand letters, very difficult to determine the numbers.
- Asset value does NOT equal loss.

SPiRE security

© 2002 Spire Security. All rights reserved.

A Loss Equation

Annual Loss Expectancy = Probability x Value

ALE = P x A

(Insurance Industry)

- Basic equation, difficulty in details.
- Easy to understand letters, very difficult to determine the numbers.
- Asset value does NOT equal loss.

SPiRE security

© 2002 Spire Security. All rights reserved.

Types of Losses

- Information-centric Loss
  - Modified data (Integrity)
  - Copied data (Confidentiality)
  - Deleted data (Availability)
- System/App-centric Loss
  - Resource Availability (Productivity)
  - Resource Misuse (Liability)

SPiRE security

© 2002 Spire Security. All rights reserved.

The Elements of Loss

- Information Asset Value (Intellectual Property, Financial Assets)
- Direct Revenue (e-Commerce)
- Legal/Regulatory Costs (fines)
- IT Productivity Lost
- User Productivity Lost

SPiRE security

© 2002 Spire Security. All rights reserved.

Information Asset Value

- Stored Value (financial assets)
- Stored Knowledge (intellectual property)
- Market Cap (or equivalent) – Book Value = Goodwill (intangible assets)
- Some % of this Goodwill is attributable to information assets.
  - Professional services – higher percentage
  - Contract manufacturing or retail - lower

SPiRE security

© 2002 Spire Security. All rights reserved.

Productivity

- Where users and IT spend their time.
- Time is money philosophy.
- Often the only aspect of loss we quantify.
- Basic source of ROI.
- Hourly rate x lost/used hours.

SPiRE security

© 2002 Spire Security. All rights reserved.

Loss: Element by Type

	Read	Modify	Delete	Avail	Misuse
Asset Value	H	M	M	L	L
Revenue	M	H	H	H	L
Fines	M/H	H	L	L	?
IT Prod.	L	H	M	L	L
EU Prod.	L	L	M	H	L

SPiRE security

© 2002 Spire Security. All rights reserved.

Security Resources

A security model:

- The Four Disciplines of Security Management
- Identifies key activities and procedures
- Identifies key solutions

SPiRE security

© 2002 Spire Security. All rights reserved.

Four Disciplines
Major Functions

SPiRE security

© 2002 Spire Security. All rights reserved.

Four Disciplines
Objectives

SPiRE security

© 2002 Spire Security. All rights reserved.

Identity Management

- Identify and authenticate as many users as possible.
- Reduce the amount of unidentified sessions.
- Roots in enterprise security; we all do it.
- Authentication is a related beast.

SPIRE security

© 2002 Spire Security. All rights reserved.

Trust Management

- How we deploy resources in support of high-tech initiatives.
- Design and architect security solutions.
- Revolves around encryption and access control.
- Policy.

SPiRE security

© 2002 Spire Security. All rights reserved.

Threat Management

- Important due to large amount of unknown network traffic.
- Signature vs. Policy/rules (next slide)
- Intrusion Prevention
  - Config firewall
  - Inline

SPiRE security

© 2002 Spire Security. All rights reserved.

Threat Management

What we look at (madness):

- Layer 2 – MAC Address
- Layer 3 – IP Addresses
- Layer 4 – TCP/UDP Headers
- Payload
  - High-level protocol info
  - Data
  - Commands
  - Variables
- Reassembled Packets
- Traffic Flows
- Ports
- System State
- System Activity
- Audit Logs
- Alerts & Events

How we look (method):

- String search
- Protocol compliance
  - RFC
  - Reference Implementation
- Rule compliance
- Lexical analysis
- Command search
- Statistical Analysis
- Trend Analysis
- System activity analysis
- …more (?)

SPiRE security

© 2002 Spire Security. All rights reserved.

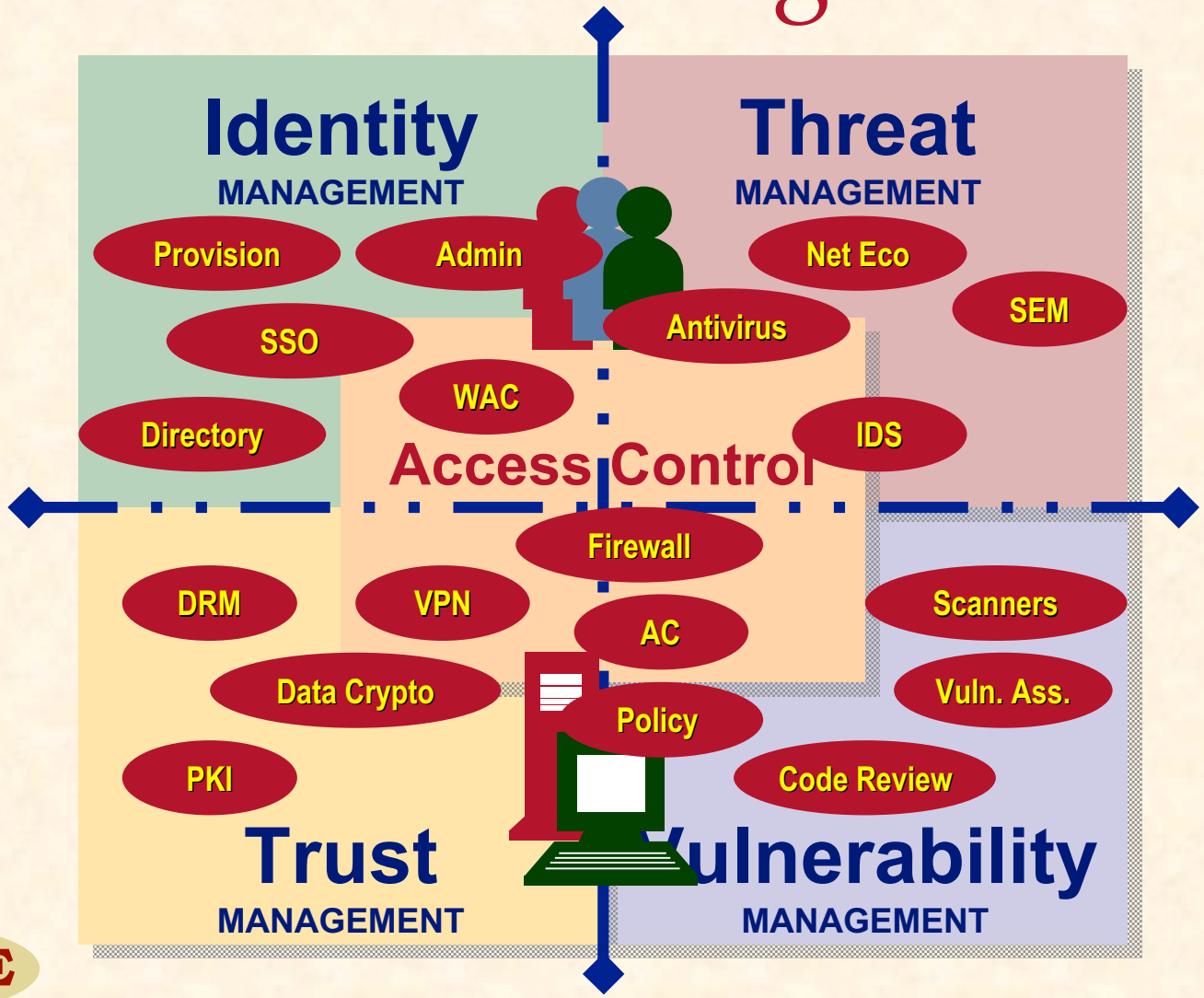
Vulnerability Management

- Psychologist's dream: look within ourselves.
- The fundamental aspect of risk.
- Scan, penetrate, review, config…

SPiRE security

© 2002 Spire Security. All rights reserved.

Four Disciplines
Product Categories



SPiRE security

© 2002 Spire Security. All rights reserved.

Resource Allocation

- Highest impact = combination of highest anticipated loss and biggest risk.
- Reduce anticipated loss.
- Increase productivity.

SPiRE security

© 2002 Spire Security. All rights reserved.

Thank You

Agree? Disagree?

Pete Lindstrom

petelind@spiresecurity.com

www.spiresecurity.com

© 2002 Spire Security. All rights reserved.