A Pragmatic Approach to Purchasing Information Security Products

InterWorks 2001

Session # 21

Ben Rothke, CISSP, CCO

Senior Security Consultant

Baltimore Technologies

ben.rothke@baltimore.com

About me...

- Who I am
  - Senior Security Consultant with Baltimore Technologies
  - Previously with Ernst & Young, Citibank
- Who Baltimore Technologies is
  - Leading e-security company
  - A global leader in e-security products, services & solutions
  - Over 1,200 employees worldwide

Session agenda

This session is:

- An attempt to show that information security is a process.
- a realistic approach in reviewing and analyzing information security products
- a discussion of the installation and deployment of security products in the context of security processes

This session is not:

- A vendor bashing session
- A comprehensive analysis of every security product

Today's infosec landscape

- Corporate networks are exceedingly complex, and are continuously becoming more Byzantine. Take an average Fortune 1000 MIS Department, add up all their:
  - Vendors
  - Topologies
  - Networks
  - Platforms
  - Add-ons
  - Custom written applications, etc.
- Now try to securely integrate them. If security was not designed into the original system architecture, how exactly do you expect these security products to work?
- Despite the fact that more and more is being spent on information systems security, things are getting more and more complex, and complex systems are much harder to protect.

What is pragmatic security?

Knowing that:

- Security is a process, not a product.
  - Just as Xenical doesn't = weight loss, so too security products don't automatically = security
- Products don't make good security, people do.
- Security Pixie Dust doesn't exist
- The need for security policies.
  - Which needs to be wrapped around a well thought-out strategy
- Remembering the word's of Milton Friedman
  - *There is no such thing as a free lunch*

Products can't do it alone

- Even if 98% of the hosts in your organization were secured, and 98% of those secured were configured correctly; that still leaves room for breaches.

- *Cool products* won't solve real problems. Do you want that *Air Gap* appliance because it's neat or you have defined its role?

- With the abundance of security products and mechanisms, there is a scarcity of management tools

Questions to ask

Before you buy a security product, ask yourself these questions:

- Do you have a CSO? CTO?
- Does the CSO have real power or it he simply a yes man to the CIO/CEO?
- Do the CSO/CIO understand the business?
- Do the CSO/CIO have a good relationship with the CIO/CFO?
- Does the CSO have trained staff?
- Are your developers trained in writing secure code?
- Will your company rollout an application if it has failed a security audit?
- Can a screaming SVP force your firewall admin to violate policy and open an unauthorized port?

- More than a few no's and you need a security strategy, not a product. If you buy a security product without the proper due diligence, then the product becomes theological, not practical.

Why buy security products without a strategy?

- Management wants a *product* to solve the *problem*
  - The product with the most bells and whistles win
- Similar to the weight loss industry. 99% of all diets end in failure. So why do people spend more money on diets?
  - Denial, hope, a way to transpose the problem.
  - I'm not fat. The medicine just didn't work properly
- If there is a security problem, then you can blame the product.
- Bottom line, if you don't have an information security strategy, then everything purchased becomes a reactive band-aid.

Security strategy

Security strategy incorporates comprehensive information security practices in the corporate process. A few of the myriad questions that must be posed are:

- What are you trying to accomplish within infosec?
- Do you have a information security mission statement?
- How does security fit into the overall business goal?
- Are staff members trained?
  - If you don't train them – how do you expect to have security?
  - Many people installing security software have little, and often, no background in infosec
- Have you taken significant time for research, planning, and designing a strategy for the product implementation
- Did you get all divisions involved and high level (CEO, CFO) support
- Are you able to sell this to management without using technical jargon

Don't look at the micro level of a product, look at the macro level of the security of the system

Security policy

- A comprehensive security policy is required to map abstract security concepts to *your* real world implementation of your security products.
- Policy defines the aims and goals of the business

Defense in depth

- There is a relationship between *prevention*, *detection*, and *response*. A comprehensive security strategy addresses all three.
- As an example:
  - Deadbolt on your front door
  - Security alarm
  - Police that respond to the alarm
- Defense in depth doesn't mean one of each type of product. Rather each aspect of protection needs to be throughout the enterprise, not just the front door.

Defense in depth

- If you just have a prevention strategy, and the prevention is not perfect, then you have real problems.
- Also, when everything works together, no single product has to bear the total responsibility for securing against an attack.
- While you can't *prevent* attacks, defense in depth ensures you can handle them when they do occur.

Risk analysis & assessment

- Without performing a comprehensive risk analysis, products operate in a vacuum.
- An effective risk assessment and analysis ensures that you are worrying about the right things.
- While most threats are internal, on the other side, you have to realize that the internal staff can be your greatest partners.
- The ultimate outcome of a risk analysis should be to see if you really can benefit from the product. Don't worry about *missing the bus*.

Why do security products fail?

- Products are often incorrectly deployed, installed and managed
- Most products today ship out of the box in a default unsecured manner. The defaults are for usability and not security.
- Vendors bear no liability. All you can sue for is the replacement of the media.
- As an example, from section 11.9 of the VeriSign CPS:

  > VeriSign's public certification services are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

- Bruce Schneier writes at length that until software developers have some legal incentive to product secure products, they won't bother. There is no incentive for vendors to get it right from a security perspective the first time. Given that, beta code has priority over secure code.

Have you chosen a vendor?

- Don’t pick a vendor until you know your needs
- Don’t put too much faith in often exaggerated marketing material
  - We won’t even mention Press Releases
- Don’t get into religious wars (Entrust vs. VeriSign, NT vs. Unix) before performing a complete architecture and technology assessment.

Customer lists

- Vendors love to show off their customer lists
  - If Company X is using our product, shouldn't you?
  - Ask vendor how recent and involved the customers are
- But this is insignificant, since much of it ends up shelfware
- Fortune 100 companies own at least 1 of everything

Problem solving

- Don’t expect the product to solve all (or even most) of your security problems
  - Nonetheless, make sure your security problems are prioritized
- If you think product x will solve your security problems, then you don’t understand the product and you don’t understand your security problem.

Physical Security

- Did somebody say *physical security*?
- Every network operating system, from NetWare, Windows NT, Linux, Banyan Vines to Unix; place the foundation of their security architecture at the physical server level
  - Now about that firewall in the snack closet

Most products are similar

- As a general rule, most established commercial off the shelf security products are essentially indistinguishable from each other and can fundamentally achieve what most organizations require. Examples:
  - Checkpoint vs. PIX
  - Entrust vs. Baltimore
  - Cybercop vs. ISS
- A gourmet chef can take mediocre ingredients and make them edible. A lousy cook can turn the best ingredients into an unpalatable mass.
- Given that, don't obsess on the products. Focus on your staff, internal procedures, etc.
- After you have done the appropriate research and analysis, then you can obsess on the products.

A look at security products

- We are going to look at some major products and looks at problems in their common implementation.
- The bottom line is that no product can exist in a vacuum.
- We will look at a few examples, but this holds true for all products in our lives.

Firewalls

- Managements reaction to a hack “But we have a firewall!”
- But did they have a firewall policy?
  - Policy is a critical element of the effective and successful operation of a firewall. A firewall can’t be effective unless it is deployed it in the context of working policies that govern its use and administration.
  - Marcus Ranum defines a firewall as “the implementation of your Internet security policy. If you haven’t got a security policy, you haven’t got a firewall. Instead, you’ve got a thing that’s sort of doing something, but you don’t know what it’s trying to do because no one has told you what it should do”.
- Design must come before implementation
  - People in the construction business get this

Firewalls

Checkpoint is no longer just a firewall, via OPSEC a Firewall-1 box can have a lot of functionality:

- VPN
- Authentication
- Anti-virus checking
- Web site filtering
- High availability
- Encryption
- Intrusion detection
- Certificate server
- QoS
- Managed services/policy deployment

Marcus Ranum on firewalls

- “These days, the kind of plug-ins that come in your typical browser, combined with all the bizarre undocumented protocols used by new Internet apps, make it highly unlikely that a firewall is doing anything more complex than a thin layer of policy atop routing. As such, the apps behind the firewall are now more critical to security than the firewall itself. Which should scare the holey moley out of you.”

- “Eventually, if enough data is going back & forth through your firewall it is no longer a firewall.....it’s a router.”

For further information

- Marcus Ranum
  - http://web.ranum.com/pubs/index.shtml
    - Thinking about Firewalls: Beyond Perimeter Security
    - Are Firewalls Obsolete? Pro and Con of the Debate
    - Can we "certify" a firewall? On the Topic of Firewall Testing
    - The ULTIMATELY Secure Firewall - An Adaptive Packet Destructive Filter
- Building Internet Firewalls
  - by Elizabeth Zwicky
    - O'Reilly & Associates ISBN: 1565928717
- Firewalls and Internet Security
  - Bill Cheswick & Steve Bellovin
    - Addison-Wesley ISBN: 0201633574

Air Gap

- An air gap is essentially a firewall. But if you call yourself a firewall, then you are competing with Checkpoint & PIX – that's bad.
- A firewall is a logical separation of two physical networks, whereas an air gap device is a physical separation of two logical networks.
  - So they say. A firewall is a tunnel, an air gap is a tunnel. And a tunnel is a tunnel is a tunnel. Giving it another name doesn't mean it isn't the same.
- An air gap device basically re-packages the TCP layer header information, otherwise leaving the packet intact.
  - This limits the ability of protocol-based attacks on a host
  - But what about the myriad other types of attacks?

Air Gap

- Well suited for niche areas
  - Backend database access from DMZ web server
- An air gap appliance mistakenly deployed, is a micro solution to a macro problem
  - Sort of like having a Diet Coke with your two Big Macs, onion rings and danish.
  - A half-duplex datastream with pico-second turnaround, coupled with a micrometer gap between two fiber connectors doesn't make a product any more or less secure than other firewalls. (Roger Marquis on the FW Wizards list)

For further information

- Secrets and Lies:Digital Security in a Networked World
  - Bruce Schneier
  - John Wiley ISBN: 0471253111
- Hacking Linux Exposed: Network Security Secrets and Solutions
  - Anne Carasik, George Kurtz, Saumil Shah
  - McGraw-Hill ISBN: 0072127732
- Hacking Exposed - Second Edition
  - Stuart McClure, Joel Scambray, George Kurtz
  - McGraw-Hill ISBN: 0072127481

PKI

- PKI in a nutshell - Establishing trust and maintaining that level of trusted assurance
- In the real world, trust is built through a complex web of social, legal, national, international and business interactions that often take years or decades to develop.
  - drivers license
  - ID badges
  - credit cards
  - Birth/marriage/death records
  - passports
  - treaties
- What the above provides is trust, underwritten by the providing authority. Unfortunately, that same level of trust is much harder to implement in the electronic world.

PKI/Digital certificates

- A digital certificate is simply an electronic credential.
- The value of the certificate is determined by the CA that issues it.
  - Just as it is possible to get a worthless identification card in Times Square, so is it possible to get a worthless, albeit cryptographically strong digital certificate.
- Your browser likely has at least 25 certificates loaded.
- In the future, people will have a plethora of certificates, just like they have a glut of credit cards.

PKI/Digital certificates

- Does a certificate = security? No!
  - Certificates are simply one aspect of a PKI. To the degree that the PKI is well-defined and configured, is to the degree that the certificate has value.
  - Have you ever checked the certificate on a web site to see if it belongs to the vendor you are about to give your credit card to?
- How do you know if you're ready to roll with your PKI?
  - Do you have a strategy on how to deal with the hundreds (thousands) of in-house applications that are not PKI compliant?
  - Do you have a strategy to deal with certificate rollout & revocation?
  - Do you understand what your CPS means?
- Non-repudiation
  - Mathematical definition vs. Practical definition
  - Dead men can sign documents

Certificate practice statement

1. Introduction
Overview
Identification
Community & Applicability
Contact Details
References
Definitions
2. General Provisions
Obligations
CA Obligations
RA Obligations
End User Obligations
Interpretation and Enforcement
3. Identification and Authentication
Initial Registration
Identity verification process
Identity Verification Check
Certificate Renewal
Revocation Request

4. Operational Requirements
Physical & logical controls
5. Technical Security Controls
Key properties
Key Strength
Private key distribution
Confidentiality key archive
Evidence required to retrieve a key
Compromise of CA keys
6. Certificate and CRL Profiles
Certificate Profile
CRL Profile
7. Specification Administration
Specification Change Procedures
Publication and Notification Procedures
8. Policy Status

From: www.baltimore.com/download/index.html
Also see Certificate Policies and Certification Practice Statements at: www.entrust.com/downloads/pdf/cps.pdf
www.verisign.com/repository/CPS/CPS-1_2-009.doc

For further information

- Understanding the Public-Key Infrastructure
  - Carlisle Adams, Steve Lloyd New Riders ISBN: 157870166X
- Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy
  - Stefan Brands MIT Press; ISBN: 0262024918
- Secure Electronic Commerce: Building the Infrastructure
  - Warwick Ford & Michael Baum Prentice Hall ISBN: 0134763424
- Ten Risks of PKI
  - www.counterpane.com/pki-risks.html
- Lockstar - www.lockstar.com
- Shym Technology - www.shym.com

Intrusion Detection Systems

- An IDS is purely reactive
- Contrary to popular belief, IDS aren't PnP. You can't simply plug in the IDS and expect it to work. You need a team.
- Does your team understand how to read, understand and interpret IDS logs? And logs from firewalls, routers, NT, Unix, other devices , etc.
- IDS should be considered as secondary systems designed to backup the primary security systems.
- After all of the false alarms, they often become ignored

Intrusion Detection Systems

- Common attacks against a typical IDS:
  - Blind the sensor
  - Blind the event storage
  - DoS (Denial of Service)
  - Fragmentation
  - Avoiding default port and services
  - Slow scans
  - Coordinated, low-bandwidth attacks
  - Address spoofing/proxying
  - Pattern change evasion
  - Complex evasion

Intrusion Detection Systems

Questions to ask an IDS vendor:

- How often is the product updated in order to account for newly released attack signatures?
- At what real-world traffic levels does the product become blind, in packets/second?
- How easy is the product to evade?
- How scalable is the IDS system as a whole?
- How many sensors does the system support? How big can the database be?
- What are the traffic levels when forwarding information to the management console?
- What happens when the management console is overloaded?
- How good is the reporting architecture?
- How easy is it to manage false positives?
- How long does it take to track down alerts and identify the situation?
- How many administrators does one need to care and feed for the IDS?
- What intrusion response features does the product have?

For further information

- Network Intrusion Detection: An Analysts' Handbook
  - Stephen Northcutt New Riders Publishing ISBN: 0735708681
- Intrusion Detection
  - Rebecca Bace Macmillan ISBN: 1578701856
- Digital Evidence and Computer Crime
  - Eoghan Casey Academic Press ISBN: 012162885X
- Network Flight Recorder
  - www.nfr.net
- Network Ice
  - www.networkice.com

Honey pots

A honey pot is a system designed to look like something that an intruder can hack. Examples can be:

- Installing a machine on the network with no particular purpose other than to log all attempted access.
- Install special software designed for this purpose. It has the advantage of making it look like the intruder is successful without really allowing them access.
- Any existing system can be *honeypotized*. For example, on WinNT, it is possible to rename the default "administrator" account, then create a dummy account called "administrator" with no password.
- WinNT allows extensive logging of a person's activities, so this honeypot will track users attempting to gain Administrator access and exploit that access.

Honey pots

- The real function of a Honey Pot should be to test the efficacy of your security infrastructure. If you deploy a honey pot with the intention of prosecuting hackers, get a life.
- Honey Pots can act as an early-alarm that will trip only upon hostile activity. This means that all traffic to a honeypot system is already suspect.
- Honey pots often present themselves as easily hacked systems.
- Remember that Bill Cheswick and Cliff Stoll had lots and lots of time. Your staff likely doesn't.
- Even if you can capture the hacker, odds are that you're his lawyer could get the evidence thrown out.
  - Your logs sync to NTP, don't they?

Honey pots

Setting up honey pots is really easy. When preparing to setup a Honey pot, make sure to:

- Documentation, documentation, documentation
  - Documentation is the first step in any network management endeavor (actually, the last step when people discover the pain of not having done it in the first place).
- How do you plan on maintaining it?
- How do you plan on receiving alarms from the system?
- What do you plan on doing when an alarm goes off?

Honey pots

- Most companies don't want to prosecute due to the bad publicity.
- For prosecution to succeed, staff needs to understand how to secure the evidence.
  - Remember this was a key strategy in O.J's defense
- Remember, honey pots do not *prevent attacks*, they assist in the detection
- Can your staff identify an active attack?
  - Problem with false positives

For further information

- Firewalls and Internet Security
  - Bill Cheswick & Steve Bellovin
    - Addison-Wesley ISBN: 0201633574 (Second edition due 1Q2001)
- The Cuckoo's Egg : Tracking a Spy Through the Maze of Computer Espionage
  - Clifford Stoll
    - Pocket Books 1990 ISBN: 0743411455
- An Evening with Berferd, In Which a Cracker is Lured, Endured, and Studied
  - Bill Cheswick, AT&T Bell Labs
    - http://cm.bell-labs.com/who/ches/papers/berferd.ps

So what's the solution?

- Stop buying products and develop a strategy
  - Develop a realistic, enforceable security policy
  - Create a security organization
    - If you have a small IT shop, give security responsibilities (and training!) to existing staff
    - At the very least, make sure you have a full-time CSO-equivalent with real power
  - All IT staff needs to be on the security bandwagon – it takes only one rotten apple to spoil the pie.
    - An anal-retentive system administrator is worth their weight in gold
  - Have information security involved from the inception of all new projects; security as an afterthought is invariably poor

What's the solution?

- Another solution is to outsource information security.
  - Banks outsource their money-handling to armed guards.
- Given the dearth of people who have experience in security, the complexity in securing it all and the difficulties in staffing a 24x7x365 security operations center (SOC), Managed Security Providers (MSP) are growing in popularity.
  - Counterpane Internet Security
  - RIPTech
  - Guardent
  - myCIO.com
  - ISS
- Nonetheless, outsourcing isn't a panacea. It doesn't solve the problem that the organization didn't get correct from the start.

Conclusions

- Real change takes time
- There are no silver bullets, no pixie dust solutions. Y2K clearly showed that.
- Complex distributed systems don't always need complex solutions. But elegant solutions take time and effort to effectively and properly develop, test and rollout.
- Information security must be seen as a process, not a product.

Thanks for attending

- Any questions? comments? jokes?
- Please fill out your evaluation sheets

Ben Rothke, CISSP, CCO
Senior Security Consultant
Baltimore Technologies
ben.rothke@baltimore.com
973/202-7921