A Pragmatic Approach to Purchasing Information Security Products

ACSAC - New Orleans

December 2000

Ben Rothke, CISSP

Senior Security Consultant

Baltimore Technologies

ben.rothke@baltimore.com

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

Products can't do it alone

- Even if 98% of the hosts in an 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/CEO?
- 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.

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

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.
- Many threats are internally based. But on the other hand, 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*.

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 (PIX vs. Checkpoint, NT vs. Unix) before performing a complete architecture and technology assessment.

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
- 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 a a few and 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

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 (Second edition due 1Q2001)

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.
  - 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)
- 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?

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

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.
  - 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.
- Security is a process, not a product

Thank You!!

Ben Rothke, CISSP, CCO

Baltimore Technologies

www.baltimore.com

ben.rothke@baltimore.com