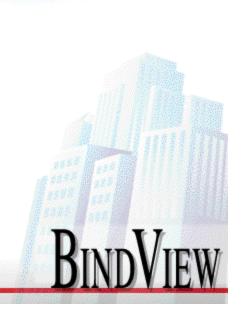
Trust No One Successfully Defending Your Network

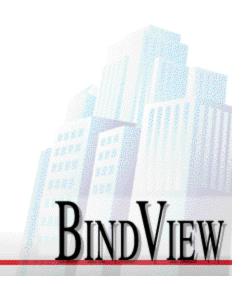
Scott Blake Datastream Cowboy



Overview

Security and networks

- Threats
- Defenses
- Learn about problems and solutions
 - Policies
 - Tools

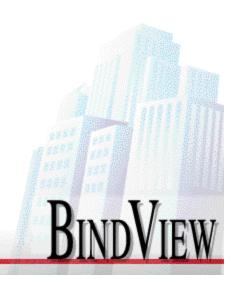


Technology and Policy

Problem specifics change at internet speed

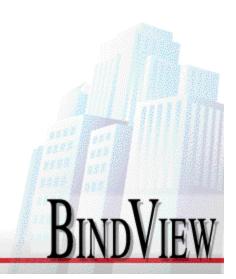
Ways of coping don't

This talk is about how to think about security



Policies

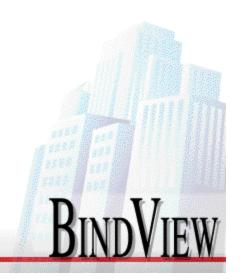
Know what you want to protect, and why
This lets you do cost benefit analysis
Know who you want to protect it from
This lets you design your defenses



Policies

Involvement

- Managers to focus on business case
- Technical staff to focus on what's possible, effective
- Everyone to commit to goals



Who might attack you?

BINDVIEW

Hackers

- A few talented people provide tools for thousands of kids
- rootshell.com, insecure.org contain hundreds of tools
- Opportunity targets
- Customers
 - Themselves
 - Through stolen/guessed passwords

Who else?

BINDVIEW

Insiders

- Through malice
- Carelessness
- Overwork
- Competitors
 - "Denial of Service" attacks make you look bad
 - Customer lists for marketing

How Outsiders Attack

- Look for known weaknesses
- Misconfigured Software
- Lots of sw has "more secure" configuration which is not turned on out of the box
- Outdated software with known problems
- Bad passwords



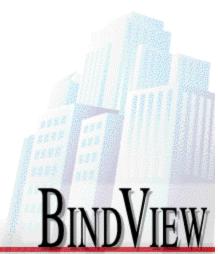
How outsiders attack (2)

Scanning tools (SATAN, sscan)
Make finding problems easy
Exploit tools

Make taking advantage of problems easy

Stealth tools

Make erasing logs easy



What to do

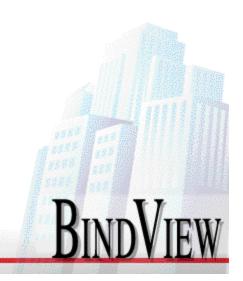
BINDVIEW

Policies and Procedures for Security

- What are you protecting?
- What's in place to protect it?
- Training and knowledge throughout the organization
 - Do system managers know that security is a priority?
 - Do they have the skills and training to execute?

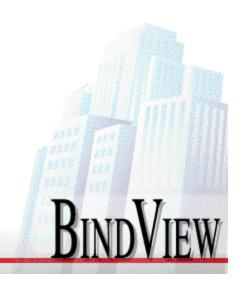
What are you protecting?

- Each component of the network
- Web servers
- Routers
- Accounting systems
- Mail Servers
- Modem Banks



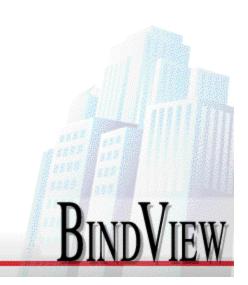
Design Defensively

- Don't build a Maginot line
- A firewall is not a complete defense
 - Attackers can easily be on the inside
- Each component may be interesting in itself
- Or as a stepping stone



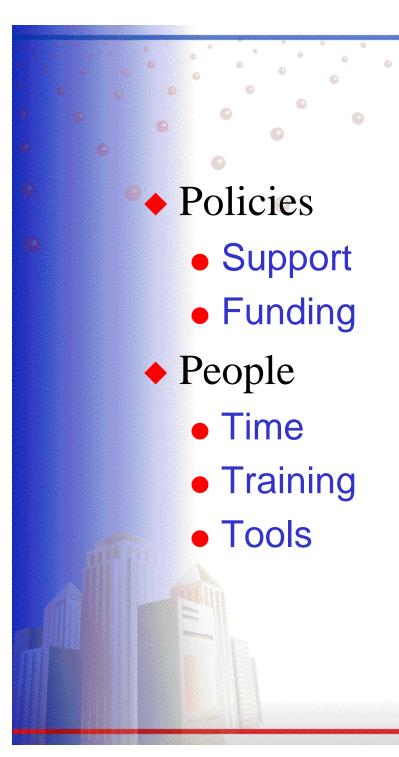
What can be wrong?

- Poor software configuration
- Missing patches
- Bad passwords
- No logs
- No sysadmin attention



Run Defensively

Run only those services you need Out of the box is not secure Vendor has a security manual Who in your organization has read it? Log extensively Once the information is gone, its gone Expect attacks Probes happen all the time Good defenses prevent escalation

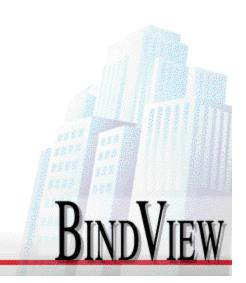


What to do about it?

BINDVIEW

What to do about it (2)

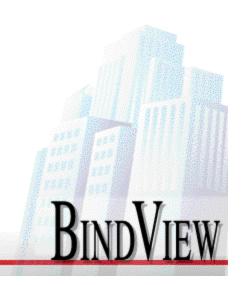
♦ Tools Firewalls VPN Anti-Hacker Intrusion Detection System Admin tools Backup



Firewalls

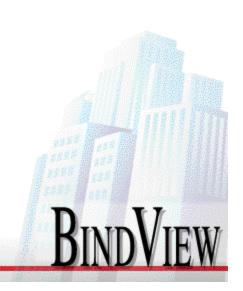
• Provide a wall between us and them

- Let some things through
- Can be walked around
- Very useful line of defense



Virtual Private Networks (VPN)

- Let you communicate securely over the Internet
- Look for IPSec compliant
- Remember that the endpoints must be secure
- Very useful if done right



Anti-Hacker Software

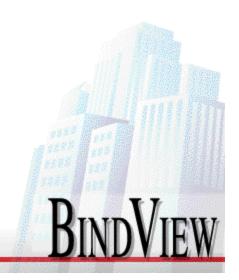
- Examines your network and hosts to find holes
- Not a replacement for systems management
- Look for ease of use, frequent updates
- Very useful if you respond
 - Act on reports
 - Use auto-correction features

Intrusion Detection

- Watches network or host logs to find attacks in progress
- A hard problem
 - Networks are getting faster, segmented, and encrypted
- Many have high false positive rates
- Some have auto-response features

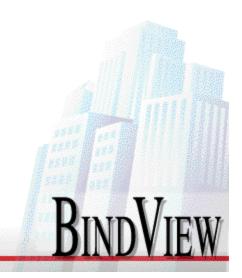
System Administration Tools

Managing a modern network is hard
Need tools to do it right
Backup/restore is a security tool



Conclusion

Understand the risks
Manage the risks with
Policies
People
Tools



Trust No One Successfully Defending Your Network

Scott Blake Datastream Cowboy

