

To Allow or Deny?
That is the question...



Do you have a Security Model?

Do you have a Security Model?

- Why do you need one?
- What is it supposed to protect?
- Who does it affect?
- Where is it in effect?
- How do you carry it out?

Do you have a Security Model?

- Why do you need one?
 - How do you identify problems?
 - What is allowed?
 - What is prohibited?
 - What is your action plan?



Do you have a Security Model?

- Why do you need one?
- What is it supposed to protect?
 - Data – Proprietary / Valuable / Irreplaceable
 - Property – Theft / Vandalism / Unauthorized Use
 - People – Misuse / Theft / Abuse

Do you have a Security Model?

- Why do you need one?
- What is it supposed to protect?
- Who does it affect?
 - Employees – Work Flow / Time Management
 - Visitors – Privacy / Theft / Vandalism
 - Technology – Control / Verification / Risk Assessment

Do you have a Security Model?

- Why do you need one?
- What is it supposed to protect?
- Who does it affect?
- Where is it in effect?
 - On-Site – Departments / Divisions
 - Off-Site – Remote Access / Verification / Authentication
 - Time of Day – Day / Night

Do you have a Security Model?

- Why do you need one?
- What is it supposed to protect?
- Who does it affect?
- Where is it in effect?
- How do you carry it out?
 - Technology – Configuration / Monitoring
 - Procedures – Documentation
 - Awareness – Understanding the Policies and Consequences

Allow or Deny

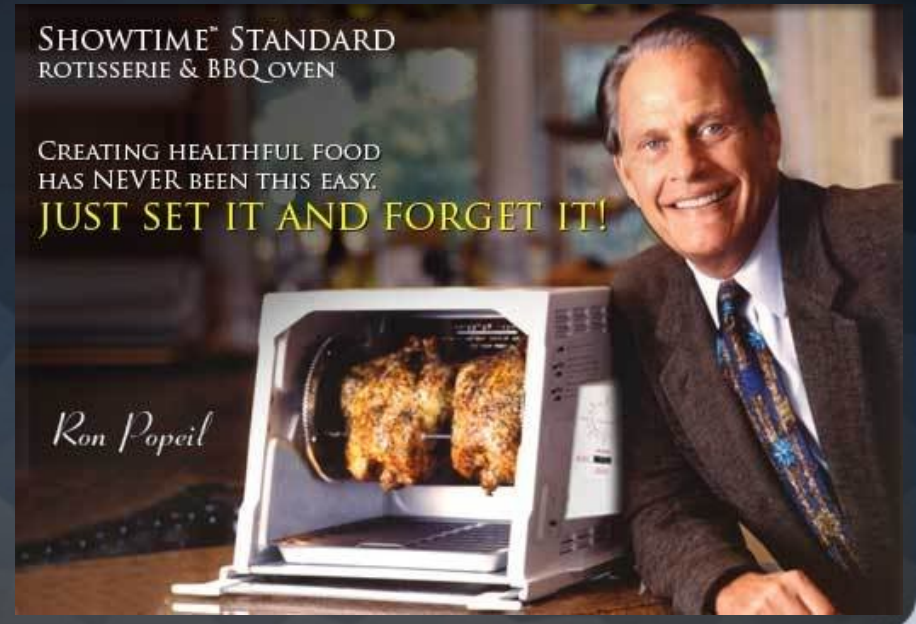
- Two different methods
 - Allow Everything, and Block Problems
 - Block Everything, Allow Applications



"Sorry, sir. Posers only."

Allow All, Deny Specific

- Easiest to Setup
 - Default for home equipment
 - Allows for easier testing of new services
 - Set it and forget it



Allow All, Deny Specific

- Easiest to Setup
- Easiest to Abuse
 - Abusive programs can run unchecked
 - Usually accompanied with poor logging and monitoring

Allow All, Deny Specific

- Easiest to Setup
- Easiest to Abuse
- Puts you into Reactive Mode
 - Problems don't normally get attention until they are out of hand
 - You're always putting out fires



Deny All, Allow Specific

- Requires full time administration
 - New policies must be approved and reviewed
 - Ongoing review of current policies to ensure compliance



Deny All, Allow Specific

- Requires full time administration
- Tighter Security
 - Easier to delay roll out until documentation is in place
 - Easier to implement logging

Deny All, Allow Specific

- Requires full time administration
- Tighter Security
- Can lead to hostility from Users
 - This never works
 - Review takes too long
 - Babysitting Users



Allow or Deny

- Which model do you think this is?



Allow or Deny – Onion Model



Allow or Deny – Onion Model

- Multiple Layer Networks
 - Allow All at higher levels
 - Global Policies that apply to Everyone
 - Deny All at lower levels
 - Department/Resource Specific

Allow or Deny – Onion Model

- Hosting Environment Example
 - Global Blocks – Apply to Everyone
 - BOGONs
 - SQL Attacks
 - Windows File Sharing
 - Customer Blocks – Apply to Specific Customer
 - Allow HTTP & HTTPS
 - Block everything else

Allow or Deny – Onion Model

- Physical Security Example
 - Global Security – Apply to Everyone
 - Timestamped Entry and Exit
 - Manually by Security
 - Key FOB
 - Recorded at Entrance
 - Cameras at Doorways
 - Parking Lot Cameras
 - Department Security – Varies by Department
 - Identity Verified and Recorded
 - Visitors Must be Escorted at All Times

Technology vs People



Technology vs People

- Technology can be compromised
 - Hacked – Intentional / Automatic
 - Misconfiguration – Default Config / Reset to Default / Missed Updates / Configuration Mistakes by Users
 - Failure – Power / Mechanical
 - Review and Mitigation – Security in Layers

Technology vs People

- Technology can be compromised
- People can be misled
 - Easy to Deceive
 - Peer Pressure
 - Inconvenient



Technology vs People

- Education of Policies
 - Explain the policies
 - Why the policy exists
 - What the policy protects
 - Who the policy applies to
 - Enforce policies
 - Technology can not do all the work
 - People are the weak link but can be stronger
 - Home is different from Work
 - This is Property Of:

Technology vs People

- Actual Ticket from User:

Please install dropbox on my desktop.

This program was deleted by the tech when my computer was being checked for virus.

I currently need this urgently to do my job.



URGENT

Technology vs People

- Actual Ticket Response:

Dropbox is a program which is commonly used to either backup files or to exchange files between multiple people.

<Company> routinely backs up <Company> servers and data using robust and proven methods. <Company> also provides FTP servers for use in exchanging files with customers in a secure and audited fashion.

Dropbox violates company policy by allowing proprietary and sensitive company data to be handled by a 3rd party with no control or auditing by <Company>.

Technology vs People

- Actual User Response:

Please give me an ftp site information so I can share it with our vendor to send me some training material.

Just an fyi, Dropbox is used by <VendorA> and <VendorB>. I have received a number of documents in the last couple of years in my Dropbox at <company> from those vendors but the information in the email below was never shared with me.

Thanks for the update.

Technology vs People

- Analysis of Ticket
 - User was using something convenient for them but violated company policy
 - User attempted to use peer pressure
 - *But VendorA uses it*
 - User did not know company policy
 - Once explained user accepted policy

Technology vs People

- Analysis of Ticket
 - Who is at fault?
 - User
 - Not complying with policies
 - Company
 - Not properly educating employee of policies

Security is a System

- Security works best when all involved work together
- All things in moderation



To Allow or Deny?

That is the question...

Presentation by:

Will @ WilliamGwin.Com

Dallas, TX - 2010 11 16