

ENTERPRISE AND PERIMETER SECURITY

HOST

- Some computing entities

Is made up of :

- OS software
- Hardware
- Network:
 - So what is in-between the application and network? Is the OS and hardware.

HOST

- It is interesting to know that some people trust things like :
 - Apple
 - MAC OS
 - WINDOWS
 - Distinct distribution of Ubuntu...
- Sensitivity of data:
 - Example: an AI expert or a student

HOST

- Example of host security
 - Mandatory authentication logon
 - Regular update
 - Malware scanner
 - Host base network firewall
 - Software – may implement firewall or not

Network Security

- INTERNAL PERIMETER
- EXTERNAL PERIMETER
- Internal Perimeter
 - we're talking about the LAN
 - What is going on, on the local area network.
 - LAN: switches, routers, hubs....in your organization that connects well to security host.
 - Security consideration
 - So if you have a back office network and there is no firewall, no isolation, no security boundaries.
 - Consider attacks that happens or begin inside the internal network

Scenario

- An employee (Joy) that brings a laptop from home to work and might have a worm on it and may be Joy uses a MAC book and her MAC book is immune to Windows based worm. But there are other window based computers on the network.
- So when she connects into the internal network, Joy is essentially unleashing this worm against all these window computers. If there is no firewall. If there is no firewall on the network on the back of her network, what happens? Absolutely, nothing is going to protect those window computers.
- That is a common scenario with wit portable devices. There is need for internal network protection.

Network Security

- How do you deal with internal network security
 - Internal Firewalls
 - Statefull Packet Inspection
 - IDS
 - Host base Protection
 - Application Base Firewall

Network Security

- If you do not consider the action of Joy bringing in her MAC book and unleashing the virus and what it will take to protect against that kind of attack, that is the failure(not considering that kind of scenario).
- Whether it protects it against it or whether it budgets a lot of money, little money, no money. That is the important bit you need to consider.

Network Security

External Perimeter

- Outside the perimeter, outside of the internal network.
- At the border between the this organization and the ISP or another organization we have our own perimeter.
- We also have the outside network, what is going on out there in the wide world.
- There is none as much control, there is not as many things that we can do to control security out there in the world, because that is where the bad guys lives.

Network Security



- Do we need to still worry about this guy? Or not?

Network Security

- yes we do need to worry about the external network.
- We do need to worry about applying some controls in considering.
- Considering that, there are a few things we can still do such as:
 - Communicating with the ISP
 - Public organizations to get best practices

Network Security

