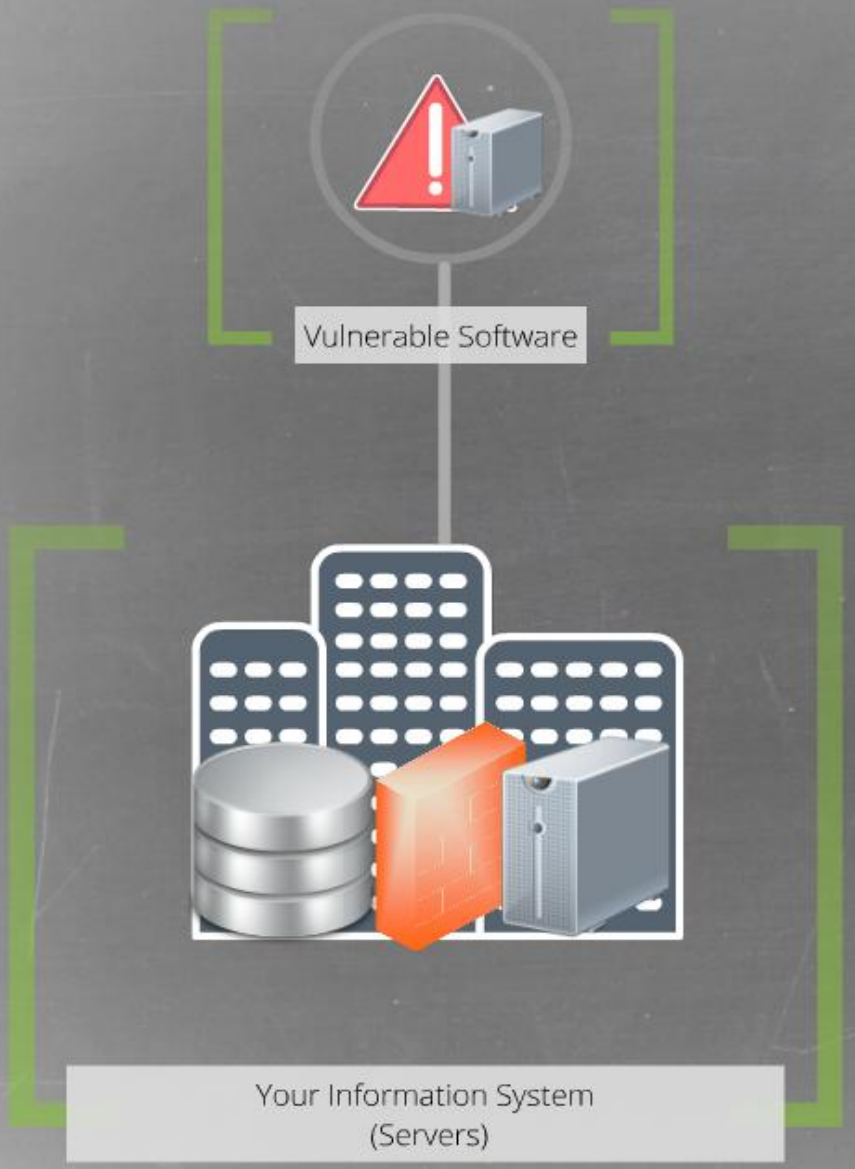
NDIA

Small Business Conference



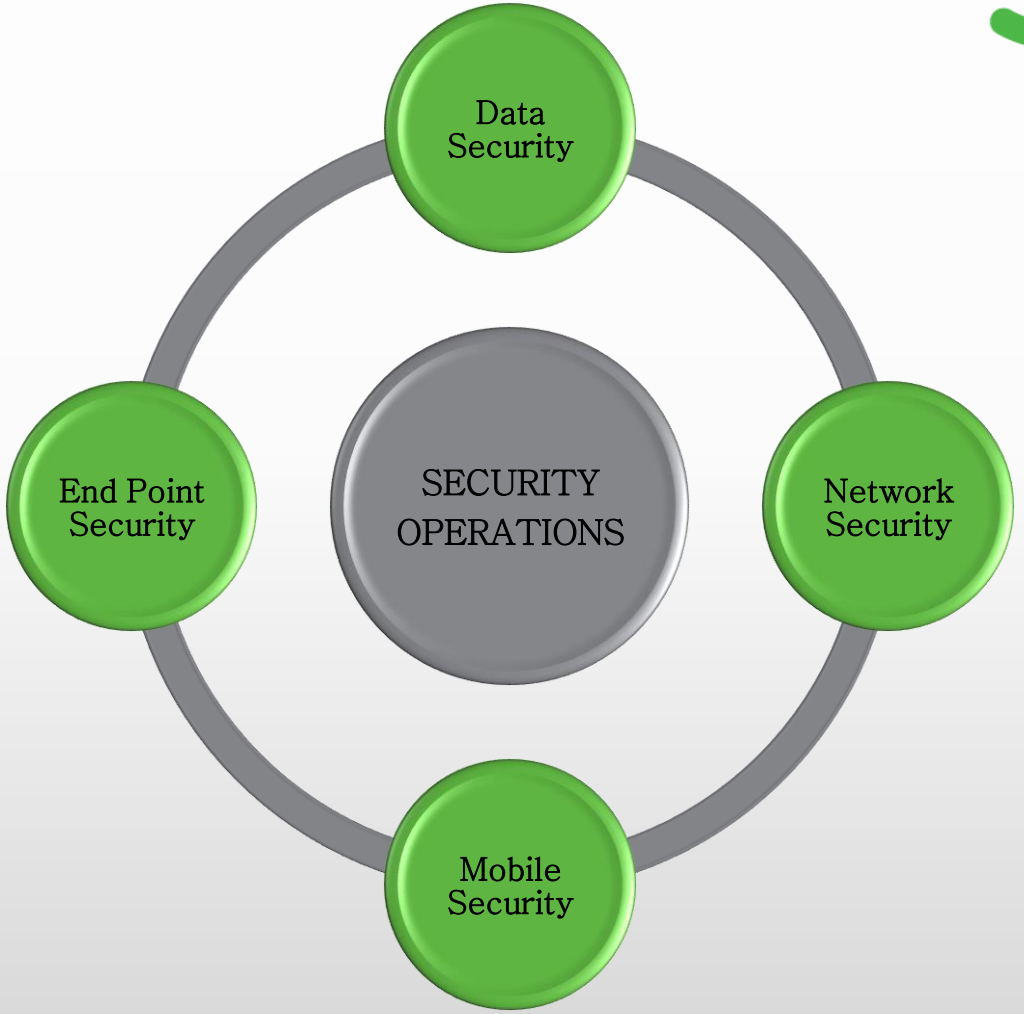
Hack Anatomy 101 – Discussion

WHAT IS ACTUALLY REQUIRED

- Security Intelligence
- Actionable Information
- Expertise and Experience
- Security Operations
- Incident Handling
- Event Management

SECURITY LANDSCAPE

- Attack Vectors
- Methods to Mitigate
- Security Tools
- Why isn't security done?



SECURITY AREA – DATA

DATA SECURITY		
ATTACK VECTORS	• Poor data security policies or no policies at all • No knowledge/inventory of existing sensitive data in the organization • Lack of awareness of who is using the data	• Lack of awareness of what the data is being used for • No sophisticated control structure to grant permissions to sensitive Data • Sensitive data on mobile and personal devices
MITIGATION	• Catalog and inventory data • Creation of established and enforced policies around sensitive data • Use of role based access control to limit unnecessary exposure and use of data	• Monitor the use of data by employees • Create awareness of how the loss of sensitive data can affect the company
SOLUTIONS	• Data Loss Prevention, Encryption , Device Control	
WHY ISN'T IT DONE?	• Budget concerns • Lack of trained talent/expertise	• Very complex to implement • Expensive and time intensive to manage

SECURITY AREA – INFRASTRUCTURE

INFRASTRUCTURE SECURITY		
ATTACK VECTORS	• Poorly managed network appliances and servers • No/infrequent security audits and vulnerability scans (awareness of weaknesses) • Improper password management • Lack of device/application inventory	• Weak or non existent network defense controls • Poorly coded applications • No established policies for security • No visibility as to who is doing what on the network
MITIGATION	• Scheduled security audits • Established secure configurations for devices and applications • Encryption of passwords • Secure code adoption in software lifecycle	• Establish the ability to view the information system "top down" and be able to drill down to examine faults and events
SOLUTIONS	• Password/identity management, Continuous threat monitoring, Vulnerability management software, UTM (unified threat management) appliances, Code audit service, Centralized management platform, SIEM platform, Web application protection/firewall	
WHY ISN'T IT DONE?	• Centralized management platforms are costly and difficult to implement properly	• Security platforms "sell" simplified security but it they still require experienced resources for operations

SECURITY AREA – END POINT & MOBILE

END POINT & MOBILE SECURITY		
ATTACK VECTORS	• Poorly managed malware protection software • No ability to locate devices if they are stolen • No established or enforced AUP for devices • Sensitive data is often left "in the wild" (unencrypted)	• Poorly configured devices can be reimaged by a thief, leaving no trace • Workers working remotely with no secure transport method to use sensitive data
MITIGATION	• Use of malware solution that provides centralized management capability • Establish ability to remotely wipe/lock/track lost devices as standard configuration	• Create awareness of how devices should be used • Use of secure transmission methods for remote workers (VPN, SSH) • Standardized machine images for control
SOLUTIONS	• Malware protection suites (Symantec, McAfee, Kaspersky – no particular order), "LoJack" software for devices – bios level protection, Imaging and configuration management software (Microsoft), File and folder encryption	
WHY ISN'T IT DONE?	• Sophisticated solutions require operations and operators to maintain configurations and provide support	• Encryption can often become cumbersome if implemented improperly and inhibit productivity • Hard to ascertain which solution to purchase (decision paralysis)

C-Level Resources

- digitalhands.com
- iscanonline.com
- fcc.gov/cyberplanner
- csrc.nist.gov
- csoonline.com