Network security at the great widget company

Engineering, Computer Security

Great Widget Company TO: Network Administration Group FROM: Tonia Appleton, Manager of Network Services DATE: July 23, 2003 SUBJECT: Network Security Great Widget Company values the security and integrity of its data. In keeping with that policy the following information is provided to clarify the security level associated with each level of the OSI (Open System Interconnect) model. Please familiarize yourself with this information, we will discuss it in the next regular staff meeting scheduled for Monday, August 1, 2003. Physical Layer – Security protection at this level includes physical media, access to input devices, and power supply restoration. The server room will be locked at all times with only authorized team member having access. Entry to the server room will require both the scan of an authorized badge and the entry of the corresponding pin number. Anyone accessing the server room who is not an employee must be accompanied at all times by an authorized team member. All network hardware will be protected from loss of power by a UPC. Data Link Layer – Assurance and availability are the security goals for this OSI layer. One vulnerable area in this layer is alteration of the Address Resolution Protocol (ARP) cache causing MAC addresses to be matched up to incorrect IP's. MAC address filtering will be used to identify stations by address and cross-reference the physical port or logical access. Network Layer – The network layer is responsible for routing data, and the security vulnerabilities include routers, switches and bridges. All routers will utilize IPSEC technology to ensure confidentiality of data transmitted. The preferred mode if IPSEC encryption is tunnel to encrypt both the data payload and the header information. Transport Layer – The transport layer which assists the network layer in ensuring that data arrives

at the proper destination is vulnerable to security breaches. TCP and UDP can be used to obtain network information used for unauthorized access. Firewalls will have strict rules limiting access to specific transmission or protocol information. Firewalls must be capable of stateful inspection to prevent false packet profiles from entering the perimeter. In addition virus scanning software will be deployed for additional protection. Session Layer – All password exchange and storage will be encrypted. Three attempts to access with an invalid password will require a thirty minute time-out before access is authorized. Two such time outs in a 24 hour period will require permanent lock out of the user account until reinstatement is approved by the appropriate business unit contact. Presentation Layer – Secure Sockets Layer (SSL) protocol will be used to ensure private and secure transmissions. This is accomplished by a secure sockets layer handshake to authenticate the server and client, establish and encryption method and a unique session key. Application Layer – The application layer which is where the user interfaces with the system has its own set of security vulnerabilities. Viruses, Trojan horses and worms are among those introduced by the users through such applications as email. In addition to virus scans at this level intensive user education will be conducted to ensure network security. Any new processes or hardware, deemed to be non-compliant with this policy will require justification and the Director of IT approval to implement. Any current network processes or hardware, that violate this policy must be either changed or approved by September 1, 2003.