Bellevue University Cybersecurity Program

Harry & Mae's Case Study

Instructions: Below are details about a fictitious business requiring improvements to its security. You have been hired as a security consultant for this business. Use the details from this case study according to the directions found in the various class assignments. The text in *italics* is the transcript from the video. The other text contains details on the hardware and software infrastructure in place at the client.

Video Transcript

Welcome! I'm Tom Pierce, the president of Harry and Mae's Inc. Recently, my company suffered a security breach where hackers obtained credit card data on over 25,000 of our customers. I need your expertise to ensure this doesn't happen again. Come on, let's get started. First, I'll give you a little background about my company and then I will go into detail about the security we currently have in place.

Harry and Mae's Inc. is a diner franchise that supports over 100 diners located in New York, New Jersey, Delaware, and Pennsylvania. Harry and Mae Pierce started the original Harry and Mae's diner with two railroad passenger cars back in 1954. Since then, his children and grandchildren have transformed the company from a single restaurant into a chain of restaurants, and, most recently, to a publicly traded franchise business. The franchise business provides restaurant owners with everything they need to open and run their own operation, including buildings, fixtures, restaurant products, support services, and food. As another service to franchise owners, we resell credit card payment processing services to them at competitive rates. Harry and Mae's reimburses, up front, for credit card transactions that are funneled through their payment processing system as an incentive for franchise owners to use our services.

As for location of the corporate headquarters, Harry and Mae Inc. call Windsor, Pennsylvania home. Both of the corporate headquarters and warehouses are located there. We built the campus from the ground up at that location because it was central to our operation and both the business climate and tax structure were favorable. The campus currently employs slightly over 400 people that see to the day to day business operations.

What about our physical security, you may be asking. Well, the campus' physical security system was designed by a retired Army general. Its main features include a perimeter fence, cameras, smart card access points, alarms, and a full-time security staff.

The campus also features a three-layer wired network infrastructure. Plus, it has full wireless access provided by an Aruba Networks grid. Comcast Business Solutions provides Harry and Mae's with Internet. We have a number of security appliances and devices already in place, but I'm not sure how effective they are. As for the active directory domain, there is a single one for the entire campus. It was configured using default settings, and uses the default domain group policy with one exception. Password history and complexity requirements have been disabled to make it easier for employees to use passwords they can remember and reuse them if they want. The rationale for making this change was that I had difficulty remembering my password, so I began to write it down. A member of the cleaning crew saw it and used my machine to view pornographic material. When I discovered the breach, I fired the person responsible and directed the password policy change.

Our headquarters also features servers, and web hosting; however, the specifics for each are a bit detailed. Next, let's focus on the on and off campus workstations. The company has over 400 Dell Optiplex 3020 workstations on campus. Each computer is installed with Windows 7. Plus, all computers are joined to the company's Active Directory domain. Off campus, the default configuration for new restaurants consists of a high speed Internet connection supplied by a local provider, a Network Address Translation firewall device that includes a wireless access point, an office computer, and two point-of-sale computer systems that include credit card processing software. Even though we try to stay up-to-date with the latest software and hardware, our system is not immune to failure. While all employees have user names and passwords for the system, there have been problems with computers becoming infected with malware because the point-of-sale software can be minimized.

Now that I've explained the history and background of my company as well as the infrastructure of our system, it's time to get to work. Visit your course site to check out your assignment. Be sure to ask your instructor any questions that arise. Good luck!

IT & Security Infrastructure

Below are details on the Information Technology and Security infrastructure, policies, and equipment currently in place at the client.

Physical security:

The campus physical security system was designed by a retired Army general. Its main features include a perimeter fence, cameras, smart card access points, alarms, and a full-time security staff. Access to all buildings on campus is restricted through smart cards. The server room is a 1600 square foot building within the main headquarters building. It has climate control, redundant uninterruptable power supplies (UPS), and a generator with enough capacity for 36 hours of uninterrupted operation. The walls, floor and ceiling are constructed of reinforced concrete and are two feet thick. In addition, the entire building is shielded against electromagnetic radiation. It has an outer set of vault doors and an inner door that is equipped with a biometric scanner. The interior of the room is equipped with fire, water, and motion sensors, as well as cameras. The sensor and video feeds from the campus are centrally monitored by a staff of three people 24 hours a day, seven days a week.

Wired network Infrastructure:

The wired network infrastructure consists of three layers. The innermost layer consists of consists of two Cisco Nexus 7000 switches populated with M1-Series 8-port fiber optic switches running NX-OS Release 5.0. These switches provide fully redundant 10Gbit connectivity between servers, to the Internet, and to the second layer. The second layer consists of a 10 Gbit dual fiber ring that provides connectivity between the core network and 2 Cisco ME 3600X Series Ethernet Access Switches located in each building on campus. The third layer consists of Gigabit copper local area networks that connect computers and Power over Ethernet (PoE)

phones with Cisco 2960-S PoE switches that are located in communication closets in close proximity to their users. Each subnet in the third layer is connected to the second layer through both Cisco ME 3600X Series Ethernet Access Switches that provide access to the fiber ring for the building. Layers 1 and 2 are fully redundant. Layer 3 doesn't provide redundant connections, but less than 50% of the available ports are used on each switch. The communication closets are equipped with patch panels that would permit network administrators to manually bypass a defective switch.

Wireless connectivity on the campus:

The campus has full wireless access provided by an Aruba Networks grid. There are two Aruba 6000 Modular Mobility Controllers serving over 100 Aruba Networks AP-125 wireless access points. The wireless network interfaces directly with the corporate headquarters wired network. The mobility controller has the ability to serve as a firewall, but the default settings currently allow all traffic in both directions. In addition, the president of the company has directed that the current wireless system be configured to provide open access without logon capability because he wants to make it as easy as possible for employees to use their mobile devices. When asked about potential security issues, he said that the convenience of mobile devices outweighs the risk. He is emphatically supporting BYOD throughout the company. He had his physical security consultant walk the perimeter with a mobile device to confirm that the signals from wireless devices on the campus were too weak to register.

BELLEVUE UNIVERSITY

Internet:

The Internet connection for the company is provided by Comcast Business Services. Comcast provides a fully redundant 1000Mbps down and 50Mbps up fiber connection to the campus on a fully redundant dual fiber ring consisting of two fiber pairs.

Security appliances:

The campus network has two Dell SonicWAll NSA 4600 Firewall Security Appliances that connect the Comcast Internet connections to the core network. These two devices are currently configured to allow all traffic in both directions. These devices are capable of up to 1000 VPN connections each. However, the company chooses to forward VPN traffic through the firewalls and handle it using a Microsoft PPTP solution.

The campus also has two Barracuda Spam & Virus Firewall 300 appliances. These devices are located on the core network, and all mail traffic is forwarded through them. However, the company has not activated the subscription that updates the signature files, and some users are

complaining about excessive SPAM. Other users (especially Sales and Accounts) are complaining about missing email.

Active Directory Domain:

There is a single Active Directory domain for the entire campus with two Domain Controllers. It was configured using default settings, and uses the default domain group policy with one exception: password history and complexity requirements have been disabled to make it easier for employees to use passwords they can remember and reuse them if they want. The rationale for making this change was that Tom Pierce had difficulty remembering his password, so he began writing it down. A member of the cleaning crew saw it and used Tom's machine to view pornographic material. When Tom discovered the breach, he fired the person responsible and directed the password policy change. There are five members of the IT group with domain administrative privileges.

There is a second AD Organization Unit set by the Chief Financial Officer for the Accounting and Finance Group. In this OU, all administrative assistants are also administrators in order to quickly add or remove user accounts. This OU has full password complexity turned on.

Servers:

The headquarters has a 200TByte HP StorageWorks Storage Area Network (SAN) that provides storage for 10 Hewlett Packard ProLiant DL380 G7 servers. The firmware and drivers was last updated in July 2013. The HP servers are running VMware vSphere Hypervisor (ESXi) version 5.1. On that virtual platform, the company currently hosts redundant virtual servers for their domain controllers, Inventory Tracking System (ITS) Point of Sale (POS) system, accounting system, payment processing system, email system, Web site with database support for active content, Windows Routing and Remote Access Server (used for VPN connections,) authentication services, and database management systems. All virtual machines are running Microsoft Windows Server 2012 Datacenter edition. The administrative staff elected to not install antivirus software on any of the virtual servers, as that would slow them down. After all, Web browsers are disabled on all servers and by policy administrators are not allowed direct access or email.

The Web servers (IIS) and Email servers (Microsoft Exchange Server 2010 SP3) have two network connections: an internal one and external one with a public IP address. There are no firewalls on the external connections. The Web Server uses SSLv3.0 for any sensitive pages along with certificates signed by Verisign. Web developers move web pages to the Web server using File Transfer Protocol (FTP). FTP is enabled for both internal and external networks, as some programmers access the Web server from home. Security is enabled, so they must log in using

their Active Directory user accounts. In addition, the system administrators have discovered that FTP is a convenient way to move files, and they often log in using their accounts, as well. Using the FTP server as a staging server, it is possible to move files from the outside to the Web server, and then from the Web server to a workstation.

Web hosting:

The Web server is used to host the company's web site. The site has two parts that are both hosted on the same server, a public part that is available over the Internet using the company's URL http://www.harryandmae.com, and a "private" part that is available on the internal network only that is accessible only by using the internal URL http://www.haryandmae.local. Employees can log into the "private" Web site using their Windows login credentials and view their pay statements, work performance reports, vacation time, and other personal information.

The franchise owner in Scranton, PA purchased and uses the domain www.HandMScranton.com for customers at his three restaurants. He also has an active Facebook page and Twitter and Instagram accounts. He often runs contest using these sites.

Campus workstations:

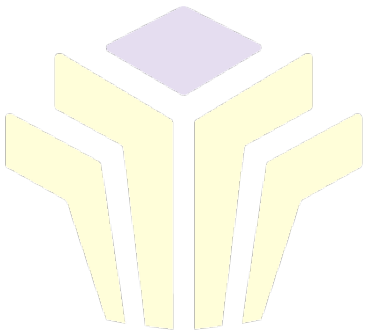
The company has over 400 Dell Optiplex 3020 workstations with Windows 7 Professional installed. All computers are joined to the company's Active Directory domain. These computers are configured for IPv4 only, and IPSec is disabled by group policy. All workstations have Symantec Endpoint Protection installed. About 1/3 of employees have local administrator access in order to install and run applications. The company uses WSUS to update Microsoft applications. There is no standard process for updating other programs.

In spite of the new relaxed password rules, some employees still write their passwords down, and they can be found taped to the inside of drawers, on the bottom of mouse pads, or on notes stuck to their monitors. The company uses a Web front end for all of its applications, and the workstations are capable of accessing them using Microsoft's Internet Explorer. IE10 is the company standard. Some employees have installed and use other browsers. Remote users have access to the same applications via the VPN.

Off campus:

The default configuration for new restaurants consists of a high speed Internet connection supplied by a local provider, a Network Address Translation (NAT) firewall device that includes a wireless access point, an office computer, and two point-of-sale computer systems that include

credit card processing software. The WAP router at each store is procured and set-up by the franchise owner. All franchises are supposed to have free Internet WiFi for customers. All computers are Microsoft Windows 7 machines with Norton Antivirus software. All employees have user names and passwords for the system. There have been problems with computers becoming infected with malware because the point-of-sale software can be minimized. Point-of-sale computers connect with the corporate headquarters for payment processing using Microsoft PPTP VPN clients on each machine.



BELLEVUE
UNIVERSITY