SECURITY ASSESSMENT

SEATTLE PACIFIC UNIVERSITY

ISM-6331

INFORMATION SECURITY SYSTEMS

NICHOLAS CATANI

CHARAN SINGH

3/1/2023

Content

- Introduction Pag. 3
- Operating System Pag. 3
- Firewall Pag. 4
- Logs Pag. 5
- Incident Response Pag. 6
- Wireless Network Pag. 8
- Remote Access Control Pag. 9
- Compliance Pag. 10
- Disaster Management Pag. 11
- Patch Management Pag. 12
- Business Continuity Plan Pag. 13
- Recommendations Pag. 14
- Implementation Pag. 15

Introduction

Businesses are building more applications than ever and processing unprecedented amounts of data. While this can lead to amazing outcomes for customers, it also increases their exposure to cybersecurity threats. More data and code increase the threat surface, creating opportunity for malicious actors online.

The following assessment tends to reveal Seattle Pacific University's existing IT (Information Technology) vulnerabilities and suggest recommendations to improve its overall security posture. It is designed to reveal the immediate threats to IT security, show how to fix them, and ensure that they will not occur again.

Operating system

SPU has been using Windows in all the computers and laptops given to the staff. In some rare cases they have also used Linux. Windows is the best option for SPU as SPU has been using applications such as Microsoft 365, Outlook, Microsoft authenticator etc. and have been venturing Microsoft as its cloud provider.

Firewall

A network firewall is a network security tool that filters the traffic that is coming in and out of the network. Its purpose is to make sure that no unauthorized entity can enter the network. In our conversation with Mr. Gerard Duguay, he told us that for SPU's firewall, we work on the principle of blocking all traffic unless it is explicitly allowed. So, SPU decides what kind of traffic it would allow entering the network. They do not allow anyone to have an internet to connect to computer on the campus. The perimeter firewall is directly connected to SPU's server through which the web content passes. The perimeter firewall specifies what traffic is going to be accessed by what server.

Logs

SPU has distinct categories of logs and all of them are collected differently. We got a very extensive description of how the log system works at SPU. Server logs, Data transactional logs, Account logs are given to a third party that parses the logs and analyses them to find any kind of concerns that are there in those logs which is called the security operations center. On campus, there is a system called the DUDE and PRTG that monitors traffic going in and out of SPU's network. PRTG is a network monitor software made by a company named Paessler, making sure there are no outages and making the working seamless.

The DUDE and PRTG systems give them alerts if a switch in a building goes down the log collector has a graphical interface that will show us which switch it is and from what building. 3 staff members are always designated to look at all the logs and if needed, they will spend all their time reviewing them. SPU has contracted a third-party vendor that does artificial intelligence analytics which does cloud sourcing and has many locations and could understand threats a lot better as they deal with much more threats. It provides SPU with almost 10 alerts which they investigate on a weekly basis. They use a product called Vcentre which is a VMware product that tracks logs of the performance of the servers. SPU gets alerts if any of the servers is 15% below disk capacity, they are alerted via email so that they can increase the disk allocation. Working in a virtual environment makes it easier to increase allocations.

Incident response

A cybersecurity incident response refers to an enterprise's processes and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks. The goal is to prevent attacks before they happen, and to minimize the cost and business disruption resulting from any cyberattacks that occur. Seattle Pacific University's IRP (incident response plan) is outsourced from the ground up. Depending on the severity of the breach, it employs an End-point detection response (EDR) agent, the Security Operation Center (SOC), and Cyber Insurance coverage to contain cyberthreats and restore affected systems faster.

The first line of defense adopted is an EDR security solution that continuously monitors end-user devices – faculty members, alums, employees, students – to detect and respond to cyber threats like ransomware or malware. How does it work? It records the activities and events taking place on endpoints and all workloads, providing security teams with the visibility necessary to uncover incidents that would otherwise remain invisible. Moreover, the third-party agency offers advanced threat detection, investigation, and response capabilities - including incident data search and investigation alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment. <u>SPU receives a report periodically of all the activities performed.</u>

If the breach requires more attention, a security operations center takes over. The SOC is responsible for protecting the university from cyber threats. Analysts and Engineers perform around-the-clock monitoring of the SPU's network and investigate any potential security incidents. If a cyberattack is detected, analysts and engineers are responsible for taking any steps necessary to remediate it. The network, servers, computers, endpoint devices, operating systems, applications, and databases are continuously examined for signs of a cyber security incident. In addition, the team analyzes feeds, establishes rules, identifies exceptions, enhances responses, and keeps a look out for new vulnerabilities.

The final solution represents a Cyber Liability Insurance. It is an insurance policy that provides a combination of coverage options to help protect the company from data breaches and other issues such as costs for recovering compromised data, for repairing damages computer systems, or lost income due to a cyber event.

Wireless Network

Seattle Pacific University offers both wired and wireless options for connecting personal computers and mobile devices to the campus network and internet. A single access point (a device that creates a wireless local area network, or WLAN, usually in an office or large building. It connects to a wired router, switch, or hub via an ethernet cable, projecting a WIFI signal to a designed area.) runs three SSID (Service Set identifier) such as, **SPU-GUEST**, **SPU-BUSINESS**, AND **SPU-WIRELESS.**

The "SPU-Guests" wireless network is available to campus guests only and many Seattle Pacific University resources are inaccessible via this network. Students, faculty, or staff members need to use the "SPU-Wireless" network. In addition, the university makes no guarantee concerning the security, availability, reliability, or confidentiality of transmissions made via this network.

The "SPU-Wireless" is available throughout campus for current faculty, students, and staff members. The user needs valid SPU credentials (username & password) to connect to the network with the device. Each device connected to the network is allotted 20 Mbps. Moreover, the Computer and Information System department constantly integrates new wireless technology to take advantage of industry innovations, increasing coverage and performance.

Remote Access Management

The University provides multiple tools to allow employees to access on-campus services and resources while working remotely and to manage security performances of SPU devices. We report three accesses: VPN, AOVPN, and Citrix.

There are several Virtual Private Networks configured to allow faculty and staff to connect securely to on-campus technology resources from SPU devices while off the perimeter such as Matthew, My Docs synchronization, EMS, or StarRez. - **no longer in use**

The SPU always on VPN was launched during the 2021-2022 school year and is being deployed to workstation computers throughout the environment. It is installed automatically on SPU devices allotted to faculty and staff. It is powered by Microsoft's always on technology and is designed to always be connected. The AOVPN connectivity for remote computers is necessary for CIS to centrally manage programs and applications, keep them updated. Also, it provides the user with direct access to DFS (Depts File Server) departmental files shares.

Citrix is an online service for faculty and staff that allows them to access SPU My Documents, Departmental File Shares, and other SPU specific applications form a personal device with internet access. It can also be used to connect to on-campus desktop devices. - **it will be decommissioned**

Compliance

There are several compliance requirements for SPU network, and we are going to talk about some of them. The most impactful one is GLBA which is Gramm-Leach Bliley Act requires some privacy protocols so that users' information stays safe and protected. It means risk assessment needs to be done wherever third parties are involved and can get access to the data. SPU has a separate network that has students' health insurance details that is HIPAA compliant. They had to keep it on a separate network as making the whole network HIPAA complaint is an expensive and lengthy process.

SPU also follows the 800 171 guidelines which are a set of standards for all kinds of different things about what you do with your logs, how you control access your physical access and virtual access. SPU uses third party provider Sodexo for all its transactional processes which is PCI DSS Compliant and they themselves do not have to make the whole network compliant to PCI.

DMCA or Digital Mollett Millennial Copyright Act which is used to prevent illegal peer-to-peer sharing like torrents as piracy violates copyright laws. Another old compliance that SPU follows is FERPA which is that any student or staff information should not be leaked or even its presence should not be acknowledged by anyone or even by the network.

Disaster management

SPU's disaster management involves the process of preventing, mitigating, and eliminating disasters even before they occur. SPU focus is on 2 things that is 1) Data, 2) systems to protect their data they have a very extensive back up process and store their back up data at isolated locations within the campus. Everyone with a SPU issued device their sensitive and important documents are backed up through file share. We also have data that is stored in the cloud transferred using VEEAM that is a powerful back up engine.

Every night 3 batches of back up are sent to Microsoft Azure cloud provider and another company called Back Blaze. They use the best practices, including the 321, which means making 2 different copies of back up, 2 different storage places and 1 offsite location. Along with this they have a diesel generator that provides power to the server room and the PBX ROOM, so processes of the system are not interrupted, and the system is never down.

Patch Management

A patch policy is comprised of a set of steps and procedures aimed at managing and mitigating vulnerabilities in your environment through a regular and well-documented patching process. It lists the guidelines and requirements for the proper management of vulnerabilities and involves various phases such as testing, deployment, and documentation applied to the university. A vulnerability appears when a released software's code is flawed, which means that malicious actors can exploit it. Every time that is discovered, it may publicly be disclosed or not.

Seattle Pacific University has implemented a period schedule where assures that all the software is up-to-date and secured from future risks and be able to decide when is being installed. The first patch occurs every Wednesday from 4am to 6pm. Whereas the second patch occurs generally during the breaks.

Business continuity plan

SPU has made some managerial preparations for business continuity in case of a system failure or after been stricken by a disaster. SPU sees its single point of failures so they can mitigate them for example SPU has two internet connections and both are running on separate lines so that if one breaks the other stays independent and the operations could continue.

They have backups stored in different isolated locations with VEEM helping to store them. 3 batches of back up are sent up on the cloud every night. SPU practices its back up, so in case of a disaster they already know how to do things to know what machines depend on different variables. SPU has a wiki offsite which is a knowledge base that consists of all the instructions and encryption keys so that if everything is lost, they can still rebuild the entire system using the instructions and steps stored in the wiki but having an educated work force to imply that recovery is of equal importance. SPU is moving towards Microsoft 365 and will start doing backups on it.

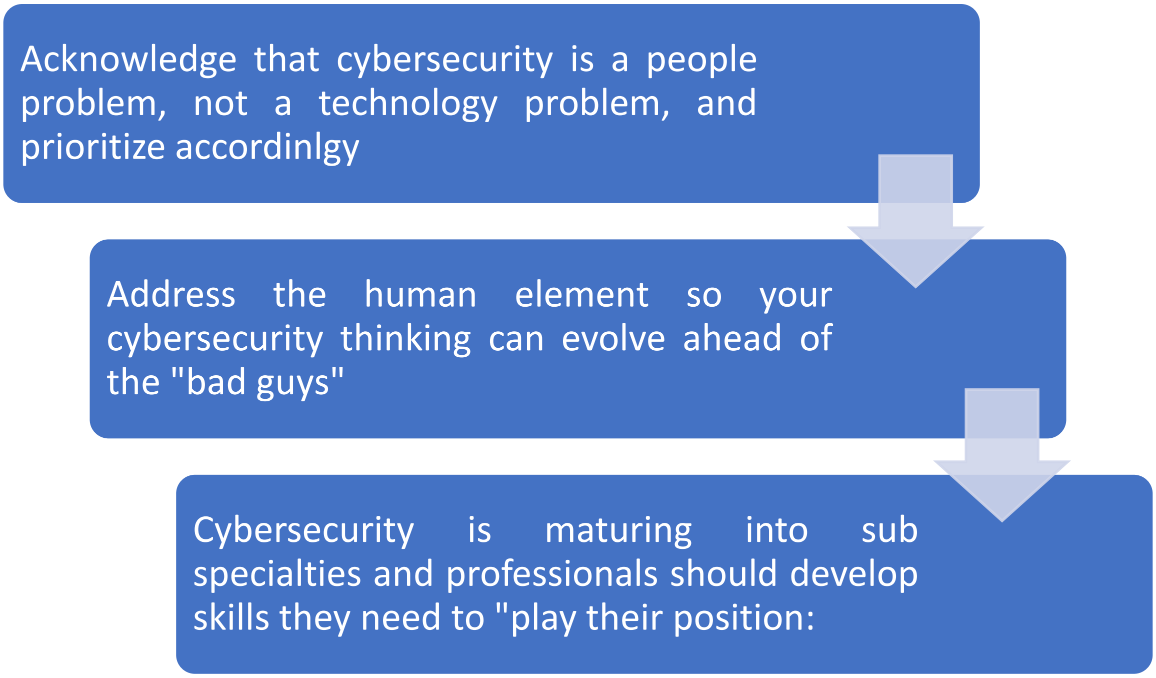
Recommendations

- The threat model for internal security differs from that of perimeter security. Perimeter security defends SPU networks from internet attackers, armed with zero-day exploits of common internet services like HTTP and SMTP. However, the access an employee has to the network, simply by plugging in to an ethernet jack, dwarfs the access a sophisticated hacker gains with scripts. Therefore, we recommend deploying hacker defenses at the perimeter and to enforce policy to address internal threats.
- The increase in volume and velocity of cyber attacks combined with the challenge of accommodating a hybrid or remote workforce in the modern enterprise, has compounded the need for SecOps. It generally refers to a highly skilled team made up of security and IT operations staff that mitigate risk in the perimeter. Unfortunately, Seattle Pacific University lacks a security team. Therefore, we recommend building a team that can support a combination of remote and on-premises work while maintaining security.
- The university lacks a consistent program to train employees on cyber threats. Having an extensive security awareness program, may teaches staff and faculty to understand vulnerabilities and threats to business operations. They need to be aware of their responsibilities and accountabilities when using a computer on the SPU network.

Implementations

- We think that when evaluating security measures on the perimeter, a level that's good enough can only be ever really determined by an accurate estimate of the university's needs and the threat landscape it must navigate through. Looking externally at what it faces, and internally at the specific needs, may help create a unique security architecture that is both adaptable and robust. Cisco NGIPS: Next-Generation Intrusion Prevention System - Study CCNP (study-ccnp.com) The NGIPS can make this architecture possible, in addition to other facets like a good security culture within SPU and a comprehensive knowledge of cyberthreat trends and evolving technologies.

- In terms of creating a security team, depending on SPU budget, we came up with three simple steps to build a robust security team.



Acknowledge that cybersecurity is a people problem, not a technology problem, and prioritize accordinlgy

Address the human element so your cybersecurity thinking can evolve ahead of the "bad guys"

Cybersecurity is maturing into sub specialties and professionals should develop skills they need to "play their position:

- Finally, for the cyber security awareness program, we thought to design an intuitive implementation plan…

Get a buy-in from top management

Perform risk assessment reports

Provide interactive training courses

Schedule simulated phishing attacks

Compile test results and improve

Implement and enforce new policies

Retrain employees regularly

Be consistent and stay informed