Essay Topic 2

Assume you are the Chief Information Officer (CIO)[1] of the company that you dream of (any company, real or hypothetical). Give a brief introduction to your company and identify a few types of internal, and external network threats that may endanger your company.

As a CIO, how to design your security policy and work with your IT department to provide the best protection to secure your company's network given the threats you just mentioned?

Daniel Lowry

10/26/2020

Hello, my name is Daniel Lowry. I am the Chief Information Officer for the company Misty Mountain Forge. We specialize in hand-forged Norse and Celtic jewelry along with useable reproductions of historical weaponry. We are a company that does a majority of its sales online, making several financial transactions daily through our secure portal with our customers. I write this letter to shine a light on some of the internal and external threats to our network that we, as a company, face on a day to day basis. We are a large company with several employees with multiple locations.

Being a large company with multiple locations opens many opportunities for us, but that fact does not come without some risks associated with it. One of these mentioned risks includes stack overflow. Stack overflow, as the name suggests, is a type of vulnerability related to data overflow. Say when we enter data into the data structure, if the data entered is more than the capacity of the data structure then the data overflows to adjacent memory locations and this might cause the application to crash. It is one form of denial of service (DoS) attack. This is one of the oldest vulnerabilities and is common when we use languages like C or C++ which use pointers. To mitigate this risk we use Data Execution Prevention to flag a certain area of the memory as an executable or non-executable memory, which will stop an attack from running the code.

Another risk we face is unauthorized access to the more secure areas of our systems. We work tirelessly with our IT department to employ “Multi-Layered Network Protection” to secure our network from unauthorized traffic. Some of these measures include, data encryption, firewalls, email security and archiving, digital certificates, and privacy controls to name a few. “Having multiple layers of security in place is crucial for businesses who protect data at all levels and across numerous applications and devices.” (SolarWinds MSP)

One thing that we try to not overlook is, “Sometimes external threats are successful because of an insider threat. The weakest link in data protection can be your own employees.” (The AME Group. 2017, August 17) We work closely with the IT department to ensure all of our employees understand the importance of network security and conduct bi-weekly training meetings to ensure our employees are up to date on certain threats we may face conducting business online.

With these measures in place, you can rest assured that the daily operations that are conducted within our organization are safe, and the risk of our network security being breached, either internally or externally, remains low. Thank you.

References

Multi-Layered Network Security Strategy. SolarWinds MSP, www.solarwindsmsp.com/content/multi-layered-security-approach.

Network Security Threats: 5 Ways to Protect Yourself. The AME Group. (2017, August 17). https://www.theamegroup.com/network-security-threats/.