RISK ASSESEMENT

Devonshire Deluxe (DD)

Eric Somogyi

CSEC 533 – 10/22/2024

Table of Contents

Executive Summary

Purpose

Following the recent data breach, Initek currently still faces security challenges involving our IT systems being compromised. This is due to the lack of updated enforceable security policies and procedures for users and employees, insufficient controls against malware, poor management of technical vulnerabilities, and failure to properly secure sensitive assets through encryption. These deficiencies leave Initek vulnerable to data breaches and other security incidents, which may lead to damage relating to operational integrity and reputation of the company, loss of data, and systems malfunctioning. If left unaddressed, these issues will impact Initek's ability to build and maintain a new solution to operating a secure environment.

Scope

Call to Action:

To address all the above, we recommend Initek invest the following: a new AV software, an Endpoint Detection and Response (EDR) software, produce new security policy documentation following COBIT 2019 and HIPAA compliance, adopt a Zero Trust architecture, and have the security team be trained on the new practices and applications. By supporting these recommended security measures, Initek will be able to protect sensitive data, ensure business continuity, and restore stakeholder trust all around.

Report

Purpose

The purpose of this assessment is to evaluate how the use of proper information technology software and hardware such as a next-generation firewall (NGFW), an Intrusion Detection System/prevention system (IDS/IPS), a Data Loss Prevention (DLP) solution, and a Security Information and Event Management (SIEM) system will strengthen DD's data center infrastructure security by reducing the risk of data center infrastructure vulnerabilities that can be exploited in cyberattacks. This will enable senior management to make informed decisions in managing the company with these identified available security controls.

Uncertainties

1. Software related uncertainties: There are several uncertainties in this risk assessment due to the nature of the data provided. Although we did confirm some of the software and hardware that is currently being used in the data center, there is limited information on what versions of the updated software and hardware installed are. We did confirm that there is a firewall and IDS/IPS system, but they were not configured properly. Allegedly, there was no logs to analyze due to improper configuration of the SIEM system so that has influenced the decision to make sure that senior management assign some of the employees to oversee and manage the SIEM system. Although this may be an uncertainty, we also confirmed that there was no DLP solution integrated in the data center infrastructure, so we recommend DD to make an investment into a solution similar to Forcepoint's Enterprise Data Loss Prevention Solution product.
2. Hardware related uncertainties: The list of current hardware is not made available to use however DD senior management has a list of what it is.

Analysis

In the table below are summarize the risk assessment results for the following risk tolerance inputs. These 6 inputs in the table are the same risk tolerance inputs that have been provided in the Situational Assessment which are being used as inputs to the assessment as requested by the senior staff and board of DD. In the table below in Column 1 is the identified Risk. In Column 4 and Column 5 is the Level of Impact and Overall risk.

In summary, these results in Table 1 display generally High Levels of Impact and High Overall Risk with a High Overall Likelihood of future breach if DD does not:

1. Correct their data center infrastructure's management procedures, implement the necessary patches in software or updated current versions of tools/software/hardware such as DLP, NGFW, SIEM, IPS/IDS.
2. Train members of the team to update entire systems and log management
3. Create and assign roles to members with specific tasks and job roles so there is a companywide understanding of how to respond to events relating to cyberattacks or to events relating to maintenance of system wide architecture.

Submission Feedback

Overall Feedback

--> Call for action is missing the executive summary

--> Some key risks mitigation aspects, such as the need for a Change management, Incident response plan, and Patch management were not addressed in the risk assessment.

Table 1:

1	2	3	4	5	
Risk	**Threat Sources**	**Vulnerabilities and Predisposing Conditions**	**Overall Likelihood**	**Level of Impact**	**Overall Risk**
Potential for an adversary to bring down DD's networks through intentional/unintentional actions	External Threat sources: Any unwanted public IP that gets through the Firewall Internal threat sources: untraining employees and lack of communication	Vulnerability: Missing patches, lack of hardware/software inventory, unsuccessful/lack-of Hardware Firewall, lack of Data Loss Prevention (DLP) security control tool. Predisposing condition: Panic of employees and management within company from having confusion of what to do.	High	Very High	High
Insufficient Logging and Monitoring	Internal threat sources: Insufficient software resources allocated to log management/analysis	Vulnerability: Lack of a real time monitoring tool/software, lack of logging (security control tool). Predisposing condition: Our data center has a high volume of data and lack of expertise to decipher security logs since they are nonexistent.	Low	High	Low

Deficient Patch Management	Internal Threat Sources: Lack of dedicated job role for processing patch management External Threat Sources: Attackers who exploit known vulnerabilities for outdated patches, Malware.	Vulnerability: Lack of testing software (security control tool) to confirm successful operational use, No vulnerability scanning. Predisposing condition: Confusion around patch management in a complex data center environment, "Vendors may take extra time to release patch updates for newly discovered vulnerabilities."	High	Very High	Medium
Inadequate asset management	Internal Threat Source: Lack of correct hardware/software tools not implemented and running properly.	Vulnerability: No known asset discovery process (aka no internal system for logging of new devices/software once installed), lack of use of inventory software	Medium	High	Medium
Inadequate Incident Response	Internal Threat Sources: Lack of documented procedure and understanding by employees of how to manage a cyberattack response External Threat: Risk of attackers repeating different cyberattacks to exploit the delayed incident response	Vulnerability: No established permanent communication channels, lack of trained personnel, lack of formal Incident Response Plan Predisposing condition: Data center being a complex IT environment.	Medium	Low	High
Vulnerability to DDoS attacks	External Threat Source: Attackers with ability to launch DDoS attacks to disrupt business operations at the data center.	Vulnerability: Lack of Intrusion Detection/Prevention System Software/Tool (security control tool) , Lack of Firewall Predisposing condition: DDoS attacks have occurred before in the recent data breach, data centers are more prone to attacks because they attract malicious actors because of the value of the data.	Low	High	Low

Mission and Functions of the Organization

The business processes supporting the mission of DD is to manage and keep the data center and system networks secure by providing 24/7 monitoring and maintenance. The interconnections that this function rely on are inventory management of hardware and software asses. Through not identifying these hardware/software assets in an inventory log file on a company computer, this becomes an inherent risk because the action of not creating this inventory is a risk to DD's business. Once identified, these software/hardware assets can be scheduled to be upgraded/updated if an update from a 3rd party vendor is made available. Another business process that DD must achieve is IT operations. By maintaining IT infrastructure and providing internal IT support to the necessary components of the system architecture, this will ensure availability of management properly operating the business's technical operation of the company's data center activities.

Organizational Information Systems

The systems that are lacking from DD is mainly network infrastructure management, which is part of the technical operations of the data center environment. The properly configured NGFW and SIEM system would help information flow of network traffic and logging on a daily basis every second. This data being properly managed would help management and employees facilitate communications from these shared services internally within the company. Any disruptions to these organizational processes would increase the likelihood DD's ability to maintain an unbreachable data center. Through the proper awareness and training of how to configure, read, and react to the implementation of the logging mechanism tools, DD will be able to mitigate the risk associated with situational data breaches.

Time frame

This risk assessment is valid for 60 days.

Conclusion

This risk assessment has reviewed all technical operations within DD's data center infrastructure. These vulnerabilities include DD's lack of proper security control tools, which include: training for incident response, logging and monitoring, patch management configuration, DLP, SIEM, NGFW, and an IDS/IPS system. In addition, DD's recent prior history in how they managed operations relating to this DDoS cyber-attack breach pose a high level of threat to their data center services. To mitigate these risks, DD must implement better security controls, proper operational and technical management by employees and senior management, enhance its logging/monitoring systems, and improve incident response procedures relating to outside cyber-attacks. DD must establish clear roles to all employees and their job responsibilities for security management and this can be done through proper training. Addressing these areas will strengthen DD's overall IT security infrastructure within the data center environment through ensuring continued availability, integrity, and confidentiality of its data center operations.