**Defense in Depth**

**David V. Garlisch**

**Western Governors University**

**06/10/2024**

**Task 2**

**Table of Contents**

# Proposal Review…………………………………………………………………..3

1. Review of Other Works and B1 Relation of Artifacts to Project Development….9

1. Project Rationale………………………………………………………………….11
2. D. Current Project Environment………………………………………………….11
3. Methodology……………………………………………………………………………..14
4. Project Goals, Objectives, and Deliverables…………………………………………….14
5. Timeline………………………………………………………………………………….22
6. Outcomes………………………………………………………………………………...22
7. References……………………………………………………………………………….25

# Proposal Overview

## A.1 Problem Summary

Balrog Gaming is a rapidly growing company behind the hit game "The Mines of Mordor." The company faces increasing security challenges as it transitions from a small startup company to a significant player in the gaming industry. Initially, the company operated as a small team, sharing a building with another organization that was very lax in its security practices. This then led to several significant security issues.

Among these were physical security breaches such as tailgating, where unauthorized individuals gained access to secure or restricted areas by following employees through doors. That building didn’t have any badge readers in use. The shared building also lacked essential detective controls, such as surveillance cameras, which led to undetected and unresolved security breaches. There were even instances of theft being reported if you left your things out at your desk overnight.

The company's identity and access management (IAM) could have been better. Balrog Gaming has weak password policies and default credentials, making it easy for malicious actors to quickly gain unauthorized access to their systems. Phishing emails also posed a constant threat. The employees needed to be adequately trained to recognize and handle such attacks and even ran into many viruses that caused problems for the company. Since the company was small, most users wore many “hats,” so to speak, and did many jobs throughout the company. This led to privilege creep, where many users had permissions and access they shouldn’t. So, implementing access controls and end-point detection and response would help mitigate these issues.

With the company's recent success and anticipated rapid growth, these vulnerabilities have become even more crucial to address. The expansion to a new headquarters marks an essential time for Balrog Gaming to get these concerns taken care of. CEO of Balrog Gaming, Jim McGavin, understands that the current security practices must be improved for the larger, more complex organization they are becoming. The new headquarters presents an opportunity to establish a robust and comprehensive security strategy to safeguard their intellectual property, customer data, and employee safety.

Recognizing the heightened risks and the need for a more secure environment, Jim McGavin has taken proactive measures. He intends to hire a dedicated cybersecurity team tasked with developing and implementing a complete security plan tailored to the needs of Balrog Gaming. This team will focus on creating a multi-layered defense strategy known as Defense in Depth to address the company's vast array of threats. However, we will only cover some of the layers of defense in depth as Balrog Gaming excels at having a good network infrastructure and implementing good asset inventory practices.

By integrating multiple layers of security measures, Balrog Gaming aims to create a resilient security posture that will protect against current and emerging threats. This approach will involve enhancing physical security with turnstiles, badge readers, and security cameras, bolstering endpoint security with comprehensive antivirus solutions and regular software updates, and ensuring identity and access management are utilized with multi-factor authentication and user behavior analytics.

With a comprehensive Defense in Depth strategy tailored to Balrog Gaming, it will be ready to protect its assets, maintain customer trust, and ensure the safety and security of its growing workforce as it continues to innovate and lead the way in the gaming industry.

## A.2 IT Solution

Balrog Gaming has a few problems the cyber security team will need to address in their defense in depth strategy. The first one is with Physical Security. A well-known book titled Safeguarding Your Technology by Tom Szuba states, “Physical security is a vital part of any security plan and is fundamental to all security efforts” (Tom Szuba, September 1998), which is still very relevant today. When Balrog Gaming shared a building with another organization before purchasing a new building, the use of physical security was non-existent. Some people were caught tailgating through doors that had no business being there. This was often done at the front doors and server rooms. As the cyber security team, we can implement badge readers to ensure each individual has the right to enter the building or server room with the correct permissions. A turnstile at the front doors would also remediate the tailgating issue. Employees would often say their personal belongings were missing from their desks, and with no security cameras at the last facility, the act was never caught on camera. We can use security cameras in the building as a preventative and detective control.

Next, we can look at Balrog Gaming needs help with endpoint security. The University of Tulsa says, “Endpoints are statistically the most likely access points for cyber attacks. According to IBM, up to 70% of successful data breaches and 90% of successful cyber attacks originate from endpoint devices” (University of Tulsa, 3/26/2024). This makes it a problem that needs addressing. None of the computers had any anti-virus or anti-malware solutions installed on them. There was also no way to know if each individual was keeping their PC patched to the latest version to at least keep them somewhat up-to-date. This was an issue because of the amount of phishing emails that would come in each week. Users would click on the links and share them, unknowingly spreading the malicious emails. User training and awareness sessions with the cyber security team can greatly reduce the effectiveness of these attacks. We also want to keep each computer patched and up-to-date as most computers used within the company are outdated and insecure. This could have led to ongoing undetected issues within the company. So, we want to make sure patch management is utilized.

Lastly, we want to focus on identity and access management. This was a problem because of the phishing emails and unauthorized users around the building. We want to make sure this doesn’t happen at the new headquarters. Implementing a strong password policy and not using default credentials combined with multi-factor authentication will be paramount to securing physical and digital assets in their environment. However, we will primarily use this for user accounts. The Cybersecurity and Information Security Agency says, “Using [Multi-Factor Authentication (MFA)](https://www.cisa.gov/mfa) is a powerful way to protect yourself and your organization. The use of MFA on your accounts makes you 99% less likely to be hacked”(Multifactor Authentication, n.d.). Balrog Gaming also had issues with users having permission creep since many employees held different titles. This leads to permission creep, leading to insider threats, data breaches, and increased security risks. The solution for this is utilizing the principles of least privilege.

## A.3 Implementation Plan

This section should contain the details of an implementation plan. First, provide details on the different phases (if applicable). Then, explain how the project will be carried out and why it will be carried out in that manner.

The implementation will be carried out in 3 phases. The first phase will be the Physical Security phase. We will start with this phase first because Balrog Gaming just purchased the building and is in the process of getting their computers, servers, and infrastructure set up. As they do that, we can work on securing access to the building with badge readers at the front door, and we can put some different badge readers for other restricted areas like the server room where only authorized personnel need to be. This will prevent anyone without a badge from entering the building or other areas of importance. These badges will be created with the user's name, photograph, and a unique RFID tag. Next, we can add a turnstile. As we know from Balrog Gaming's previous building, tailgating was common. Adding a turnstile to the main entrance will only allow one person at a time. This, combined with the bade readers, will make quick work of the tailgating issue and make sure only authorized individuals may enter. Lastly, we can add security cameras at the perimeter of the building, the entrances to the building, and areas where personnel work inside the facility to help protect the organization's assets. The cameras can be used as a deterrent for a potential threat actor, and they can be used as a detective control for incident response and evidence collection. The cameras will all link to a central hub for the Cybersecurity team to monitor in real-time.

In the second phase, we will want to move on to implementing Identity and Access Management. This will do away with weak passwords and default credentials and is also where we can fully implement multi-factor authentication. Implementing a good password policy from NIST and changing default credentials is very important. The updated guidelines emphasize the importance of password length, not password complexity. User-generated passwords should be at least eight (8) characters. Even though complexity is second to the length of the password, we will make sure to enforce that we change any default password and that no common passwords are used, such as qwerty or 12345. This will help prevent attacks like the Dictionary attack. As mentioned before by cisa.gov, multi-factor authentication helps reduce the risk of your accounts getting hacked by 99%. Multi-factor authentication uses at least two of these things. Something you know-passwords, pins, security questions. Something you have-smartphone, hardware token, or smart card. Something you are- biometric factors like a fingerprint or facial recognition. Somewhere you are, which is location-based. And finally, something you do which is a behavior factor based on how you interact with a system or device. We will implement something you know (username, password) with something you have(hardware token). If we feel we need to add another one as the company grows and increases its revenue, we can add something you are and use facial recognition or even an iris scan. Every employee will be given this hardware token and a one-time password (OTP) to be used when logging in to their computer.

In the third and last implementation phase, we will provide Endpoint Security to the company and its users. In this phase, we want to focus on ensuring each computer has an anti-virus and anti-malware program installed on the machine and ensuring we do some system hardening by implementing patch management. Having an anti-virus and anti-malware solution will help prevent employees from being victims of phishing or anothersocial engineering attacks. We can even have some security awareness and training programs to educate the users of Balrog Gaming. Utilizing patch management will help ensure that all systems and applications are up-to-date with the latest security patches to mitigate vulnerabilities, as the company’s machines are wildly outdated and not patched. The cyber security team will provide patch management by testing patches before pushing out any update and creating a deployment strategy to push the updates to each machine easily.

Review of Other Works and B .1 Relation of Artifacts to Project Development  
  
Review of work 1

In the article titled “Defense In Depth: Stopping Advanced Attacks”, authors at Exabeam have shown us what defense in depth is and why it’s important. This article explains, "Defense in depth is a cybersecurity approach that uses layered defensive mechanisms to protect systems and data. With layering, if one defense fails, another is there to block an attack”("Defense In Depth," n.d.). This is the approach we are taking to finding the missing layers of security with Balrog Gaming’s company. The article then goes on to say why defense in depth is important. Each company has a wide array of attack vectors from which a malicious actor can attack. So, having multiple layers of defense is one of the best ways to reduce a single point of failure at your company. The article then briefly breaks down physical, administrative, and technical controls within defense and gives examples for each category. I chose this article because it shows the overall approach to what the cybersecurity team will do for Balrog Gaming by reducing the attack surface and proactively mitigating threats. It’s relevant because we will be using parts of the defense in depth strategy, and its importance is shown in this article.

# Review of work 2

# “What Is Endpoint Security? Definition, Types, and Importance“ is the title of the article The University of Tulsa produced. As the title states, it goes on to define endpoint security, talk about the different types within endpoint security, and also the importance of it (University of Tulsa, 03/26/2024). It mentions how endpoint attacks target unsecured devices and leverage them to compromise data or deliver malware to hardware and software, corrupting them. The article says that any device connected to a network is considered an endpoint. They show us how endpoint security is not only for external defense but also protects us from internal threats. Insider threats are always prevalent in any company, especially companies with privilege creep, like Balrog Gaming, which makes this article very relevant. It also tells us how the use of anti-virus is an important part of endpoint security, along with the use of sandboxing to test updates and patches.

# Review of work 3

# “Multifactor Authentication“ is the name of the next article. This one, though short, is important. It was also created by cisa.gov(“ Multifactor Authentication”, n.d.). The CISA (Cybersecurity and Infrastructure Security Agency) is a respectable and official governmental website aimed at cybersecurity. The article says that 123456 is the most common password used In the US today, and even if your password is more robust and complex, hackers can still find ways to get past it. This is where multi-factor authentication (MFA) comes into play. It states the importance of MFA and, if utilized, can make your accounts 99% less likely to be hacked by attackers. This article is relevant to our defense in depth strategy because Balrog Gaming can use MFA to help secure its devices and user accounts, especially with the phishing attacks it has been experiencing.

# Review of work 4

# Dataversity goes on to tell us the importance of identity and access management in the article “Understanding the Importance of Identity and Access Management (IAM) in Data Protection”(Thomas Kadar, 6/15/2023). The author explains the role of IAM when it comes to data protection. He then breaks down IAM, separating Identity Management and Access Management. Identity management basically confirms their identity with login credentials, for example, and Access Management checks the user's permissions within that organization. He then explains multifactor authentication and tools used within IAM. This article is really relevant to the cybersecurity team because they will implement some of these tools within Balrog Gaming, such as MFA to devices and user accounts. This is important to the company because of its previous issues with phishing emails, which could compromise the organization's systems.

# C. Project Rationale and D. Current Project Environment

Balrog Gaming has several reasons for needing the defense in depth approach for their company, and now more than ever before. Though they are a small company of 15 people, they know that with their newfound success and the amount of exposure their latest game release has given them, they need to expand. They expect to grow by at least triple within the year and with so many security-related issues in their last building, from physical to having no anti-virus, this led them down the path of needing to do things right regarding this new building they purchased. They actually have a say in certain security policies and can finally add security cameras, since they experienced theft on many occasions. It has more room for the company's impending growth and is the perfect place to apply defense in depth as they own the building now and have a say in more ways to secure the company’s assets. In their last building, they leased it and shared this space with another organization. That building had almost no security besides using WPA3, the most secure wireless network to date. They will use this along with a VPN for company remote users. They seem to have a good grasp of network security. So, the cybersecurity team is being hired to fill in the gaps everywhere else.

The company has had many physical security concerns because of theft, tailgating, and the lack of badge readers to prevent unauthorized access. This is where the cybersecurity team will first come into play and deploy security cameras around the perimeter, at the entrances, and within the organization to detect anything for evidence and possibly deter malicious actors from wrongdoing. The turnstiles will prevent tailgating, only allowing one person entry at a time, and the badge readers will ensure only those allowed in the building or in the server room, where we will have another badge reader requirement, are authorized to do so.

The cybersecurity team will also need to help with identity and access management for Balrog Gaming because of weak passwords and default credentials still being used within the company. It is easy for attackers to start getting into their systems and exfiltrating data or anything else they would like. The cybersecurity team would like to implement multi-factor authentication and change the user's password to at least 8 characters in length and any default credentials. Multi-factor authentication greatly reduces the likelihood of a user's account getting hacked. The company was unsure if any malicious actors had ever broken into their systems previously, but with the amount of exposure the company is getting now, it’s only a matter of time before more eyes will be on them. Simply equipping each employee with a hardware token on top of their stronger passwords and lack of default credentials now will only help mitigate future issues from occurring. The cyber security team doesn’t want to make it easy for the attackers.

Lastly, Balrog Gaming will need the use of Endpoint Security implemented within their organization. Each employee previously was responsible for their own machine, keeping it up to date with patches or updates, and for any anti-virus or anti-malware on the system. We know that some employees were clicking on phishing email links and sharing them with each other. They could have unknowingly installed a virus or a trojan on their machine that could spread throughout the network. These computers were also used for personal use, and no restrictions were placed to stop users from going to certain sites. The company was just asking for viruses and issues, but they were mostly unaware. This is where the cybersecurity team has to step in to do what they can to help prevent viruses, malware, or any vulnerability that is easily patched away. Implementing these things will only bolster the company's defense and make it harder for attackers to compromise any of the organization's systems without having to disallow their employees from going to social media sites or using these computers at home. Since they are still a smaller company, it still wants some of these benefits that come with being a smaller company and granting its users, whom they know very well, that kind of freedom. So, simply adding anti-virus and anti-malware and making sure each computer is up to date with the use of patch management would go a long way for the company.

# 

# E. Methodology and F. Project Goals, Objectives, and Deliverables

The best methodology to deploy this kind of defense in depth strategy with physical security, endpoint security, and identity access management for Balrog Gaming would be to implement an Agile methodology. The cybersecurity team will want to break down the project as a whole into 3 different parts, physical security, identity and access management, and endpoint security. Each part includes the analysis, design, implementation, testing, review, and feedback phases. With Balrog Gaming still being a small company and CEO Jim McGavin's importance on communication and collaboration already within his company, we believe the Agile framework would fit best.

AGILE FRAMEWORK:  
1. Analysis – evaluate the current state of physical security, identity and access management, and endpoint security

2. Design - develop a comprehensive plan ensuring optimal security

3. Implementation – start executing the plan by implementing the changes or installing deliverables

4. Testing – verify each system, change, or policy functions properly

5. Review and Feedback - Continuously monitor the performance of security controls, gather feedback from personnel, and identify areas for further improvement

Phase 1 for Physical security, we would want to start with the analysis part of the phase to evaluate the physical security posture, identify the requirements for it, such as the locations for the turnstiles, surveillance cameras, and badge readers, and then set clear objectives for the security improvements including preventing theft or unauthorized access. Next, we want to move to Design. This will include designing the badge reader system and the placement of the readers and the same goes for designing and the placement of the turnstiles and surveillance cameras. Now we move on to the implementation part of the phase. This is where we will actually install the badge readers, turnstiles, and security cameras according to the prior steps in finding their placements. In the Testing part of the phase, we will ensure each system functions properly. For example, we want the badge readers only to allow authorized access, turnstiles to work properly and allow authorized individuals only one at a time, and the cameras to work as they should, reporting back to a central hub with good image quality. Lastly is the Review and Feedback part of the phase. This is where we will monitor the performance of each one of these controls and gather any feedback from the personnel to see if we can improve on any of the physical security controls.

In Phase 2 we will concerned with Identity and Access Management. We will use the same parts within each phase as we did for the prior phase. For the Analysis part of Phase 2, we will review if there are any existing password policies and access controls. We can then focus on strengthening those passwords, eliminating default credentials, and implementing multi-factor authentication for the company. Within the Design part of this phase, we will develop a better, more comprehensive password policy based on NIST guidelines, which will focus on the length of the password and avoiding common passwords. We also want to design the MFA implementation plan, including selecting authentication factors, such as hardware tokens for one-time passwords. Lastly, for design, we would want to incorporate a framework for access control that incorporates the principle of least privilege, which addresses the privilege creep the company is experiencing. Moving on to implementation for Phase 2. We want to start implementing our new password policy, enforcing it on password changes and new account setups. We can then distribute the hardware tokens to the employees to implement multi-factor authentication, and finally, we can perform an access review of permissions. This will be where we implement the principle of least privilege. Testing in this phase ensures we set up the password policy correctly and that it is being enforced. We can then test the multi-factor authentication setup to ensure users can authenticate themselves and login properly. Lastly, we can verify if each user's new permissions are set properly when adapting to the principle of least privilege. As we did in phase 1, we now can move on to Review and Feedback. This is where we can monitor the identity and access management systems for compliance and effectiveness and collect feedback on anything we may need to improve upon or adjust in this phase.

In our final phase, Phase 3. We will go over Endpoint Security. Let’s start with Analysis. Here is where we will do an endpoint assessment to evaluate the current state, or lack thereof, of endpoint security. We can identify vulnerabilities and any outdated software. We can also determine if there are any specific needs for anti-virus, anti-malware, and patch management solutions. With Design, the cybersecurity team will design the deployment plan for the anti-virus and anti-malware software for all of the endpoints within the company. We also would like to design a company patch management process and a security awareness and training program for employees, which can focus on phishing emails. Implementation is where we will install the anti-virus and anti-malware on each endpoint. We can now implement the patch management process and schedule regular updates that we can push to each system. Moving on to testing. The cybersecurity team will now test the effectiveness of the anti-virus and anti-malware solutions through simulated attacks and monitoring. We can also validate that the patch management process successfully pushes updates to each endpoint as scheduled. As for testing with security awareness of the users, we can simulate phishing attempts and help those who are still falling for these attacks. In Review and Feedback, we can continue to monitor endpoints for threats and performance, collect feedback from users regarding any questions with their security awareness training, and make any adjustments to the security awareness program as needed.

## F1. Goals, Objectives, and Deliverables Table

|  |  |  |  |
| --- | --- | --- | --- |
|  | Goal | Supporting objectives | Deliverables enabling the project objectives |
| 1 | Introduce Robust Physical Security | 1.a. Security Cameras. | 1.a.i. Install security cameras on the perimeter, inside the facility, and at the entrances to prevent theft and gather evidence |
| 1.a.ii. Make sure the cameras link back to a central hub for live review by the cybersecurity team with recording enabled for evidence collection |
|  |
| 1.b. Turnstiles | 1.b.i. Install turnstiles at the entrance to prevent tailgating |
| 1.b.ii. Only allow one authorized individual at a time to enter at a time |
| … |
| 1.c. Badge Readers | Install badge readers at the entrances and the server room to prevent any unauthorized individual entry |
| Create badges with RFID tags will be created with the badges to grant access and then add permissions for only allowing people to enter the facility, but only allow certain individuals access to the server room |
| Check permissions for only allowing certain indivduals access to the server room. |
| 2 | Implement Identity and Access Management to the company | 2.a. Create a Password Policy with no default credentials | 2.a.i. Enforce the creation of strong passwords by NIST standards. Make sure each device and user doesn’t use a common password like 123456 |
| 2.a.ii. Make sure no default credentials are used for any user or device |
| … |
| 2.b. The Principle of Least Privilege | 2.b.i. Go through each individual's permissions and only allow them to have the least amount of privileges to do their job. Eliminate scope creep |
|  |
| … |
| 2.c. Multi-Factor Authentication | 2.c.i. Implement and enforce each user to use multi-factor authentication by having something you know combined with something you have |
| 2.c.ii. Obtain and give each employee a hardware token for a one-time password used with MFA |
| … |
| … | Provide Endpoint Security | 3.a.Anti-virus and Anti-malware solutions | 3.a.i. Choose and install a trusted anti-virus and anti-malware program that can be utilized throughout the company |
| … |
| … |
| 3.b. Patch Management | 3.b.i. Utilize patch management by scheduling regular updates and critical patches that must be pushed out to each machine. We can use Microsoft Endpoint Configuration Manager to do so |
| … |
| … |
| 3.c. Security training and awareness program | 3.c.i. Create a mandatory security awareness program for all employees for the first and those who need it if they fail on simulated phishing attemps. Also, new employees will have a mandatory session. |

* **Introduce Robust Physical Security**: Introducing robust physical security will greatly benefit the company by adding security cameras to prevent theft or deter malicious actors from attempting anything illegal, adding turnstiles to stop tailgating by only allowing one authorized individual entry at a time, and badge readers for an additional layer of security to only allow entry to authorized individuals to the building and server room. This will help protect the company as a whole and add security the company hasn’t yet experienced previously.
  + **Security Cameras 1.a.:** Installing security cameras will help prevent theft and gather evidence as a detective controls if something does happen. It’s also a deterrent control dissuading a potential attacker. This is a must for physical security for any company.
    - **Installing Security Cameras 1.a.i**: Installing the security cameras in specific areas will help prevent theft and deter others from doing anything illegal for fear of being recorded and caught. These locations will be on the perimeter, entrances, and inside the facility to ensure the cybersecurity team can get a good view of everything they deem important.
    - **Central Hub for Cameras 1.a.ii.:** We would like to link the cameras up to a central hub for the cybersecurity team to review in real time and check recordings if needed. This can be used as evidence collection and live monitoring.
  + **Turnstiles 1.b**.: Balrog Gaming previously had issues at their last building that they shared with people tailgating that shouldn’t be allowed there. Turnstiles at the entrance will help prevent this by only allowing one individual entry at a time. This, coupled with the badge reader, will prevent unauthorized personnel from entering the building past the main entrance.
    - **Installing Turnstiles 2.b.i**.: Installing turnstiles at the main entrance of the building will be the only area we need to put them at. This is the main entrance for every person and guest, ensuring each person who tries to enter the building will go through one at a time.
    - **One At A Time 2.b.ii.:** Turnstiles will be added to prevent tailgating and only allow permitted personnel by letting a user through if they are authorized, one at a time.
  + **Badge Readers 1.c**.: Badge readers will greatly benefit the security posture of BalRog Gaming by only allowing entry to the entrances or restricted areas if the user has the correct permissions on their badge. This will restrict unauthorized personnel from entering areas they are not permitted. This will help physical security by keeping people in the correct areas or not allowing those who are restricted from entering.
    - **Installing Badge Readers 1.c.i.:** The cybersecurity team will ensure we add badge readers at the entrance of the building to prevent unauthorized personnel from entering the main doors and another badge reader will be installed at the door to the server room. Many people at the previous location would come and go anywhere they pleased and even were in the server room when they had no business being in there. This can cause great risk to a company by having an insider threat knowingly or unknowingly doing something wrong within that restricted area.
    - **Creating the Badges with RFID tags 1.**c.ii.: We can create the badges with RFID tags where we can add permissions for personnel to enter the main doors, and only those who need access have permission to enter the server room. This will help ensure the right permissions for each person and that their individual badge has the correct authorization.
* **Implement Identity and Access Management:** Implementing identity and access management is part of the defense in depth plan for Balrog Gaming because lack of password policy, default credential usage, privilege creep, and the need for multi-factor authentication. With the amount of phishing attacks and now widespread exposure, they will need to add security in these areas if they want to continue keeping their assets protected.
  + **Create a password policy with no default credentials 2.a.:** With the amount of attention Balrog Gaming is getting over the success of their recent game, they will have more eyes on them than ever. Some of that attention may lure potential attackers to the company as well. IAM will be used to prevent a wide range of attacks from any would-be malicious actor.
    - **Strong Password Policy and No Common Passwords 2.a.i.:** We can enact a policy for strong password usage. By following NIST standards, which is common practice for creating a secure environment, we can greatly reduce the likelihood of any password attack. NIST also recommends not using common passwords, such as 123456. This will also be in the policy so we can prevent user accounts from being compromised.
    - **No Default Credentials 2.a.ii.:** The company has said they have not switched many of their default credentials for ease of access. This is also an ease of access for any attacker to gain entry into a system or device. Once changing all the default credentials, we will be one step closer to having a secure implementation of IAM
  + **Principle of Least Privilege 2.b.:** This is where we would want to eliminate the company’s privilege creep that has been occurring by only allowing the least amount of privileges to perform that employee’s duties.
    - **Check User Permissions per Job Function 2.b.i.:** We will assess each employee’s permissions to do their job function. This is common practice for better security in a company, only allowing the least amount of permissions to do that person’s job and nothing more. This also needs to be looked at if a person is going from one job title to another by restricting and or granting them permissions yet again based on their current duties.
  + **Multi-Factor Authentication 2.c.:** The use of MFA as stated before, will reduce the likelihood of getting your user accounts hacked by 99%. This is a must-have in any company in the modern day, large or small.
    - **MFA with Something You Know and Something You Have 2.c.i.:** To implement MFA, the team has decided to utilize something you know combined with something you have. Something you know will be username and password, which will be a strong password as we would have implemented and enforced as well and something you have, which is something physical you have.
    - **Hardware Token for Something You Have 2.c.ii.:** For something you have, we will give each employee a hardware token. This hardware token will grant an OTP, which is a one-time password. This greatly protects user accounts and is very hard to bypass for an attacker.
  + **Provide Endpoint** **Security 3.a.:** Providing endpoint security for the company is an absolute must in any organization. Users having anti-virus, anti-malware, up-to-date systems and patches, as well as security awareness training, is paramount to a defense in-depth methodology. Every organization can protect a large variety of attacks with what we can do in endpoint security.
    - **Anti-virus and Anti-malware solutions 3.a.:** We want to choose anti-virus and anti-malware on each machine. We can find an open source solution since the company is small still, but being armed with both can cover areas the other one misses.
      * **Install Anti-virus and Anti-Malware 3.a.i:** After we choose these programs, we can install them on each machine. These can deal with anything from trojans, viruses, worms, spyware, ransomware, rootkits, and even phishing attacks, which are relevant to bolstering the overall security posture of Balrog Gaming.
  + **Patch Management 3.b.:** Patch Management needs to be utilized within the company for system hardening. Nothing was in place before to keep each system up to date, making each system more vulnerable to attacks.
    - **Schedule Regular Updates and Patches 3.b.i.:** The cybersecurity team would like to be able to push updates and patches when needed to each system with ease. We can use Microsoft Endpoint Configuration Manager to push these updates and patches seamlessly. This is an easy and efficient way to keep systems up to date and reduce the likelihood of a successful attack.
  + **Security Training and Awareness Program 3.c.:** Providing mandatory security programs are invaluable to dealing with many types of attacks. This is very successful at dealing with phishing attacks as well, teaching our employees how to handle and spot these phishing attempts.
    - **Implement the Security Program 3.c.i.:** The security program should be mandatory at least once a year and for new hires. Educating the workforce on how to deal with these kinds of attacks goes a long way and can help mitigate or prevent attacks on a regular basis. We can go over many security concerns and questions throughout the program as well and encourage communication. The cybersecurity team will also simulate phishing emails to make sure our users are learning from these programs.

# Project Timeline with Milestones

|  |  |  |  |
| --- | --- | --- | --- |
| Milestone or deliverable | Duration  (hours or days) | Projected start date | Anticipated end date |
| Physical Security | 30 Days | 07/01/2024 | 07/31/2024 |
| Identity and Access Management | 30 Days | 08/01/2024 | 08/31/2024 |
| Endpoint Security | 29 Days | 09/01/2024 | 09/30/2024 |

# Outcome

Physical Security took the longest amount of time to complete, at 25 days, and only 5 days for any review and feedback until the team had to move on to the next phase. This was due to wiring issues within the building. It’s a new building and didn’t have a lot of the infrastructure their last building had. We also had trouble with one of the cameras not reporting back to the central hub that was positioned at the main entrance, but after replacing the security camera, we were able to move on. The Badge Readers were easily installed at the front entrance doors and the server room. The harder part was making sure the RFID tags had the right permissions and that we minimized the amount of false positives we received at the start. For the last part of physical security, we added 3 turnstiles right past the main entrance doors. We had a separate company come in and install the turnstiles for us to make sure the badge readers and security cameras were taken care of in a timely manner by the cybersecurity team. The only feedback that was given for physical security was some users having some peace of mind knowing they are more secure and a few disgruntled employees having to get used to having their badge ready when walking into the building.

Identity and Access Management was a breeze as everyone adapted to the new hardware tokens used for logging in without issue. We have extra ones at the ready for anyone who loses their tokens, which happened a time or two after implementing them. We enforced a policy with the company on strong passwords and what that entails and had the cyber security team change all of the default credentials on each device. The part that took the longest was meeting with the CEO and others in charge to make sure we knew each employee's role to start implementing the principle of least privilege. Overall, this was a good second month after implementing the security cameras, and we were able to have extra time to monitor and review how everything is going up until this point. We had a few days at the end of the month to prepare for the last phase.

The endpoint security phase was successful, but most of the time was spent getting each machine up to date and hardened. We met with the CEO and other executives and decided on the open-source anti-virus and anti-malware solution the company can use going forward. After that, the team installed them on each machine. Our cybersecurity team has never used Microsoft Endpoint Configuration Manager for patch management before, so there was a small learning curve. Once the team felt comfortable with it, we rolled out updates to each machine, making sure every user's computer was up to date and on the same page. The last couple of weeks were focused on creating and presenting our security training and awareness program. The team kept it fun and encouraged people to participate. This ended up being a great success, and the CEO would like to do this twice a year as he thinks it will be very beneficial going forward. Lastly, the team put together a simulated phishing email that everyone passed. The cybersecurity team will continue to educate and test the employees going forward.

The AGILE framework and allowing time for review and feedback worked really well with this small amount of people within the company and will be used going forward. Balrog Gaming is now ready to take on its newfound success with a multi-layered defense in depth approach to help mitigate and prevent many different attacks.

# References

Cisa.gov(no author, n.d.).Multifactor Authentication.

Retrieved from <https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication>

The University of Tulsa,(2024, March 26) Endpoint Security.

Retrieved from <https://online.utulsa.edu/blog/what-is-endpoint-security/#:~:text=By%20implementing%20a%20comprehensive%20endpoint,and%20the%20risk%20of%20insolvency>

Tom Szuba(1998, September).Protecting Your System: Physical Security.

Retrieved from <https://nces.ed.gov/pubs98/safetech/chapter5.asp>

Kharmela Mindanao(2024, April 2). NIST Password Guidelines: 9 Rules to Follow [Updated in 2024]

Retrieved from <https://www.itsasap.com/blog/nist-password-guidelines>

Exabeam(no author, n.d.). Defense in Depth: Stopping Advanced Attacks in their Tracks.

Retrieved from <https://www.exabeam.com/explainers/information-security/defense-in-depth-stopping-advanced-attacks-in-their-tracks/>

Tamas Kadar(2023, June 15) Understanding the Importance of Identity and Access Management in Data Protection

Retrieved from <https://www.dataversity.net/understanding-the-importance-of-identity-and-access-management-in-data-protection/>