Defense in Depth: Report

David V. Garlisch

Western Governors University

Task 3

06/15/2024

**Table of Contents**

Summary 3

Review of Other Work 7

Changes to the Project Environment 11

Methodology 13

Project Goals and Objectives 15

Project Timeline 29

Unanticipated Requirements 31

Conclusions 32

Project Deliverables 34

References 36

Appendix A 38

Appendix B 39

# Summary

Balrog Gaming was the client that needed a tailored defense in depth approach. Their recent success with their first game release, “The Mines of Mordor” allowed for the company to purchase their own building, as previously they shared a building as well as a multitude of security issues within that facility. Some of the issues they experienced in the last building they shared with another organization that they wanted to be remedied were physical security with security cameras to help prevent theft, turnstiles to eliminate tailgating, and badge readers only to allow authorized access to the building and server room. Next, they required identity and access management because of the lack of a password policy, common passwords in use, default credentials not changed, privilege creep with the employees in the company, and the need for multi-factor authentication. Lastly, Balrog Gaming had the need for endpoint security on their systems. No anti-virus or anti-malware was being used and with the amount of phishing attacks we knew adding endpoint security would go a long way. These phishing attacks also showed how the employees were not trained in how to spot and deal with these kinds of attacks. The machines also needed some system hardening, needing to be updated. So, patch management was needed to help secure their machines further.

Our cybersecurity team found the solution to each of Balrog Gaming’s issues and started creating a plan to remediate these issues for the company. For physical security, we knew we had to focus on detective control to collect evidence of theft. Even though they were going to a new building that wasn’t shared, an insider could have performed the theft. The cameras can also be a deterrent control, dissuading the attacker from performing the act. We thought about where the locations were needed for these cameras and moved on to preventing tailgating. The solutions to prevent tailgating and unrestricted access were badge readers at the main entrance doors and server room and turnstiles at the front entrance. With these two things combined, we will prevent unauthorized access and allow only one person at a time to enter the building through the turnstile.

Identity and access management (IAM) was our next solution for the company. We knew a few changes within IAM would go a long way in providing the kind of defense depth needed. First, we knew we had to enforce and enact a good password policy. We recommended that CEO Jim McGavin follow the NIST password guidelines, and he obliged. We also found and changed any default credentials that are being used within the company. We heard that since this is a small company, many employees have changed job titles or wear many hats, so to speak. This is where they had a privilege creep problem. The solution is to apply the principle of least privilege, ensuring each employee has the least permissions to do their job function. Lastly, we looked at implementing multi-factor authentication (MFA). In conjunction with new password policies, this will greatly reduce the likelihood of attack. The company was definitely being exploited through phishing attacks and default credentials, and we know that users were clicking on the links in those emails.

The last part of our solution for Balrog Gaming’s defense in depth is on endpoint security. The company was infected with generic malware and viruses as they currently do not use any software of that kind on their machines. Not only do they not use anti-virus and anti-malware solutions, but their machines were never up to date. They can push off updates and postpone or stop them from happening. This is a bad practice, leaving them even more vulnerable to attacks. We provided them with options for open-source anti-virus and anti-malware solutions so the company doesn’t have to spend additional money on this software after spending much of their budget on the building. We also used Microsoft Endpoint Configuration Manager for patch management, ensuring each machine is patched and up to date. Last but not least, we trained and educated the employees with our security training and awareness program. Educating users on security will not only help users with best security practices across the board but also greatly help reduce the likelihood of successful phishing attack attempts. This will also be beneficial for the CEO and other executives because of potential whaling/spear phishing attempts that could happen in the future. To make sure the company is learning, we simulated phishing attacks and re-educated users who are still struggling.

We started implementing physical security first as we thought this will take the longest time as it is a brand-new building that may need additional wiring or configuration. First, we outsourced and contacted a third party to set up a time to install the turnstiles. We implemented our security cameras, and we waited for the third party to install them a week later. Once the cameras were agreed upon and purchased after talking with the CEO, we got started. We located each spot at the facility's perimeter, the entrances, and areas of importance within the building. We had a few cybersecurity team members add the wiring for the cameras to link back to the central hub for live monitoring and a place for the recording of evidence to be obtained and we had the other remaining members of the team install and angle the security cameras in and around the building for the best view. By the time we were about done with installing the cameras, the third party installed the turnstiles. The team then took over and ensured they worked properly, only allowing one authorized user at a time. Everything was in order, and we had the remaining days for this phase of implementation to install the badge readers with RFID tags, create the badges with the correct permissions, and make sure we got the false positive rate to a minimum, which we think we eliminated the false positives by the end of this phase. We put a bade reader at the entrance, allowing everyone with badge permissions to enter, and a badge reader at the server room, where we only gave a few authorized personnel permission to enter. The badges were created with RFID tags and with pictures and names of the employees. This concluded the implementation of the company's physical security and made us confident that we had addressed all of their issues and concerns.

Implementing identity and access management was next. We knew we had to change default credentials immediately, which we did. As some cybersecurity team members were working on that, other members were tasked with enacting a password policy to bring to the CEO for approval. We followed the NIST guidelines, which were approved after a meeting with Jim McGavin. We enforced this policy and had everyone change their password on the next login, not allowing 7 characters or less in the password, and it could not be in a list of common passwords. When the users changed their passwords, we had hardware security tokens ready for them to pair with the username and password, creating multi-factor authentication. This was a one-time password key-fob, which is something you have combined with their username and password, which is something you know. We were allowed to purchase the best ones we thought fit for the company and were able to get extra in case users lost theirs or when the company grew in employees. Lastly, we met with the CEO and executives to define and understand each employee’s job function and what was needed to perform it. We used this knowledge in creating the principle of least privilege for the company, only allowing users to have the least permissions necessary to perform their job duties. This remedied the privilege scope creep that was occurring within the company.

Finally, we implemented endpoint security for the company. We had yet another meeting with Jim McGavin and decided to go ahead with open-source anti-malware and anti-virus software to save money while helping protect each user's machine. We then installed both of the chosen software programs on each machine and updated them to the latest patch. We also updated each system using Microsoft Endpoint Configuration Manager. Since the company only uses Windows machines, this was a perfect way to implement patch management, ensuring each system can be patched and updated. We spent the remaining weeks in this phase creating and performing the security training and awareness program for everyone within the company. We made a PowerPoint presentation and encouraged communication and questions throughout the program. This taught everyone the best general security practices and much about how to spot and handle phishing attacks. We then simulated phishing attacks by crafting emails that looked very similar to the phishing attacks that users were falling with before, with plans to educate further any user who fell for it. This concluded the end of implementing our defense in depth for the company.

# Review of Other Work

**Review of work 1**

In the article titled “Defense In Depth: Stopping Advanced Attacks”, authors at Exabeam showed 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 took 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, and this is what we did for Balrog Gaming. Another article written by Spanning Cloud Apps, titled “Defense in Depth: Everything to Know About the Cybersecurity Model,” also further goes into the benefits of an in-depth defense approach and states, “Defense in depth is a cybersecurity strategy that utilizes multiple layers of security to holistically protect the [confidentiality, integrity and availability](https://www.unitrends.com/blog/cia-triad-confidentiality-integrity-availability) of an organization’s data, networks, resources and other assets”(Spanning Cloud Apps, n.d.). They mention controls we added for the company, physical security, endpoint security, and access controls. The article then briefly breaks down these controls in further detail within defense in depth and gives examples for each. I chose these articles because it showed the overall approach to what the cybersecurity team did for Balrog Gaming by reducing the attack surface and proactively mitigating threats. It’s relevant because we used parts of the defense in depth strategy specifically tailored to the company’s needs that were found 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. It mentioned 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 showed 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 made this article very relevant. “The Importance of Endpoint Security,” by Mark Knowles, also supports what the University of Tulsa says in this article. The author says, “Threats to your business’ information security come in many forms today, and advanced hackers are constantly changing their methods and exploiting unpatched software or lax employees”(Mark Knowles, 2024). This is another reason we need to implement endpoint security within our defense in depth approach for the company.  
  
 **Review of work 3**  
 “Multifactor Authentication“ is the name of the next article. This one, though short, is important. It was 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. Another article from the CISA titled “More than a password” says this to why an organization should use MFA, “Implementing MFA makes it more difficult for a threat actor to gain access to information systems—such as remote access technology, email, and billing systems—even if passwords are compromised through phishing attacks or other means”(More than a password, n.d.) was relevant to our defense in depth strategy because Balrog Gaming used MFA to help secure its devices and user accounts.  **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. Another supporting article is “Why is Identity and Access Management Important?”. Optimal IdM says in this article, “The concept of identity and access management technology makes it more difficult for an outside party to view, manipulate or steal sensitive data.(“Why is Identity and Access Management Important”, n.d.), showed us and the CEO the importance of why we used IAM in their defense in depth implementation. These articles were really relevant to the cybersecurity team because we implemented some of these tools within Balrog Gaming, such as MFA, to devices and user accounts. This was important to the company because of its previous issues with phishing emails, which could have compromised the organization's systems.

# Changes to the Project Environment

ORIGINAL

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. 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.

NEW

We changed many things in this environment and I will compare it their old building as well. We changed the overall physical security of the environment by implementing security cameras that were not in use in their old building. We connected them throughout the building back to the central hub from monitoring. We installed and implemented badge readers at the main entrance doors and at the server room and added turnstiles. Both of these measures helped protect against unauthorized individuals gaining entry to the building and tailgating. None of these measures have taken place by Balrog Gaming before because of their previous restrictions on leasing part of the building they used before. We implemented all of these measures for the company for the first time. As far as Identity and Access Management, the company did not have a password policy, which we then created, added hardware tokens to create a multi-factor authentication that the company wasn’t using, changed default credentials that were still being utilized, and restricted permissions for each employee only to have the ability to perform their job function and nothing more. Lastly, we added anti-virus, and anti-malware, started using Microsoft Endpoint Configuration Manager for patch management, and created security training and awareness programs that the company was not doing as well.

# Methodology

The methodology used to deploy this kind of defense in depth strategy with physical security, endpoint security, and identity access management for Balrog Gaming was to implement an Agile methodology. The cybersecurity team broke down the project as a whole into 3 different parts, physical security, identity and access management, and endpoint security. Each part included 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 believed the Agile framework would fit best, and it did.

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

# Project Goals and Objectives

Phase 1 for Physical security, we wanted 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 we set clear objectives for the security improvements including preventing theft or unauthorized access. Next, we moved to Design. This included designing the badge reader system and the placement of the readers, and the same goes for the designing and the placement of the turnstiles and surveillance cameras. Now we moved on to the implementation part of the phase. This is where we actually installed the badge readers, turnstiles, and security cameras according to the prior steps in finding their placements. In the Testing part of the phase, we ensured that each system functions properly. For example, we wanted 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 was the Review and Feedback part of the phase. This is where we monitored the performance of each one of these controls and gathered any feedback from the personnel to see if we could improve on any of the physical security controls.

In Phase 2 we were concerned with Identity and Access Management. We used the same parts within each phase as we did for the prior phase. For the Analysis part of Phase 2, we reviewed if there were any existing password policies and access controls. We then focused on strengthening passwords, eliminating default credentials, and implementing multi-factor authentication for the company. Within the Design part of this phase, we developed a better, more comprehensive password policy based on NIST guidelines, which focused on the length of the password and avoiding common passwords. We also wanted to design the MFA implementation plan, including selecting authentication factors, such as hardware tokens for one-time passwords. Lastly, for design, we incorporated a framework for access control that used the principle of least privilege, which addressed the privilege creep the company was experiencing. We wanted to start implementing our new password policy, enforcing it on password changes and new account setups. We then distributed the hardware tokens to the employees to implement multi-factor authentication, and finally, we performed an access review of permissions. This was where we implemented the principle of least privilege. Testing in this phase ensured we set up the password policy correctly, and that it was being enforced properly. We then tested the multi-factor authentication setup to ensure users could authenticate themselves and log in properly. Lastly, we verified if each user's new permissions were set properly when adapting to the principle of least privilege. As we did in phase 1, we now moved on to Review and Feedback. This is where we monitored the identity and access management systems for compliance and effectiveness and collected feedback on anything we needed to improve upon or adjust.

In our final phase, Phase 3, we went over Endpoint Security. We started with Analysis. Here is where we did an endpoint assessment to evaluate the current state, or lack thereof, of the company’s endpoint security. We identified vulnerabilities and any outdated software. We also determined if there are any specific needs for anti-virus, anti-malware, and patch management solutions. The cybersecurity team designed the deployment plan for the anti-virus and anti-malware software for all of the endpoints within the company. We then designed a company patch management process and a security awareness and training program for employees, primarily focusing on phishing emails. Implementation is where we installed the anti-virus and anti-malware on each endpoint. We implemented the patch management process and scheduled regular updates that we pushed to each system. Moving on to testing. The cybersecurity team tested the effectiveness of the anti-virus and anti-malware solutions through simulated attacks and monitoring. The team validated that the patch management process successfully pushes updates to each endpoint as scheduled. As for testing with security awareness of the users, we simulated phishing attempts and helped those who are still falling for these attacks. In Review and Feedback, the team continued to monitor endpoints for threats and performance, collected feedback from users regarding any questions with their security awareness training, and made 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 individuals 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 need to 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 attempts. Also, new employees will have a mandatory session. |

* **Introduced Robust Physical Security**: Introduced robust physical security greatly benefited the company by adding security cameras to prevent theft or deter malicious actors from attempting anything illegal, added 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 helped protect the company as a whole and added security the company hadn’t yet experienced previously.
  + **Security Cameras 1.a.:** Installed security cameras that 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.
    - **Installed Security Cameras 1.a.i**: Installed the security cameras in specific areas help prevent theft and deter others from doing anything illegal for fear of being recorded and caught. These locations were on the perimeter, entrances, and inside the facility to ensure the cybersecurity team could get a good view of everything they deem important.
    - **Central Hub for Cameras 1.a.ii.:** We linked 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.
    - **Installed Turnstiles 2.b.i**.: Installed turnstiles at the main entrance of the building will be the only area we need to put them. 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 Turnstiles 2.b.ii.:** Turnstiles were 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 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 restricts unauthorized personnel from entering areas they are not permitted. This helps with physical security by keeping people in the correct areas or not allowing those who are restricted from entering.
    - **Installed Badge Readers 1.c.i.:** The cybersecurity team ensured we added 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 created the badges with RFID tags where we added permissions for personnel to enter the main doors, and only those who need access have permission to enter the server room. This helped ensure the right permissions for each person and that their individual badge have 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, we knew we had to add IAM to the defense in depth strategy for the company.
  + **Created 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 was used to prevent a wide range of attacks.
    - **Strong Password Policy and No Common Passwords 2.a.i.:** We enacted a policy for strong password usage. By following NIST standards, which is common practice for creating a secure environment, we greatly reduced the likelihood of any password attack. NIST also recommends not using common passwords, such as 123456. This was also in the policy so we can prevent user accounts from being easily 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. We changed all default credentials.
  + **Principle of Least Privilege 2.b.:** This is where we eliminated the company’s privilege creep that has been occurring by only allowing the least amount of privileges to perform that employee’s duties.
    - **Checked User Permissions per Job Function 2.b.i.:** We assessed 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 gave 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 chose an anti-virus and anti-malware on each machine. We then found an open-source solution since the company is small still, but being armed with both can cover areas the other one misses.
      * **Installed Anti-virus and Anti-Malware 3.a.i:** After we chose these programs, we installed them on each machine. These dealt with anything from trojans, viruses, worms, spyware, ransomware, rootkits, and even phishing attacks, which are all relevant to bolstering the overall security posture of Balrog Gaming.
  + **Patch Management 3.b.:** Patch Management was 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.
    - **Scheduled Regular Updates and Patches 3.b.i.:** The cybersecurity team was able to push updates and patches when needed to each system with ease. We utilized Microsoft Endpoint Configuration Manager to push these updates and patches seamlessly. This was 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.:** Provided mandatory security programs that were invaluable to dealing with many types of attacks. This was very successful at dealing with phishing attacks as well, teaching our employees how to handle and spot these phishing attempts.
    - **Implemented the Security Program 3.c.i.:** The security program is mandatory at least once a year and for new hires. Educating the workforce on how to deal with these kinds of attacks went a long way and helped mitigate and prevent attacks on a regular basis. We went over many security concerns and questions throughout the program as well and encouraged communication. The cybersecurity team also simulated phishing emails to make sure our users are learning from these programs.

|  |  |  |  |
| --- | --- | --- | --- |
| Goals to Implement | Met | Objectives | Met |
| 1. Physical Security | Yes | 1.a.: Security Cameras | Yes |
| 1.b.: Turnstiles |
| 1.c.: Badge Readers |
| 1. Identity and Access Management | Yes | 2.a.: Password Policy | Yes |
| 2.b.: No Default Credentials |
| 2.c.: Multi-Factor Authentication |
| 2.d.: Principle of Least privilege |
| 1. Endpoint Security | Yes | 3.a.: Anti-virus | Yes |
| 3.b.: Anti-malware |
| 3.c.: Patch Management |
| 3.d.: Security Training and Awareness Program |

# 1. Physical Security: This goal was met by implementing several measures to strengthen this layer of defense in depth for Balrog Gaming. We used security cameras, badge readers, and turnstiles to cover issues like tailgating, theft, and unauthorized access

* + 1.a Security Cameras.: The security cameras objective was achieved by installing cameras at strategic locations around and in the building. All of these cameras successfully linked back up to a central hub for the cybersecurity team to monitor
  + 2.b. Turnstiles: Turnstiles were successfully achieved by having a third-party being hired to install the turnstiles at the main entrance while the cyber security team worked on other tasks. This prevented tailgating and unauthorized access
  + 3.c. Badge Readers: Badge Readers were successfully implemented by installing them at the main entrance and at the server room door, preventing or granting access based on the permissions set within the RFID tag when creating the badges
* 2. Identity and Access Management: This goal was met by listening to the company's issues and knowing what we can implement to successfully remediate or strengthen the security of. We met these goals by enacting a password policy, changing default credentials, utilizing the principle of least privilege, and implementing multi-factor authentication.
  + 2.a. Password Policy: We followed NIST guidelines when it came to creating and using a password policy. The company was previously allowing any length and common passwords. We secured these issues by following NIST’s best practices and forced users to change their passwords
  + 2.b. No Default Credentials: This goal was easily met by changing any default credentials being used by any of the company’s devices
  + 2.c. Multi-Factor Authentication: This goal was met by combining something you know (user name and password) with something you have (hardware token). We bought hardware tokens that gave one-time passwords to each employee for logging into their system
  + 2.d. Principle of Least Privilege: This goal was met by meeting with the CEO and executives who know each employee's job function and then restricting them to have the least amount of permissions needed to perform their job. This provides security and helps prevent insider threats
* 3. Endpoint Security: This goal was met by implementing anti-virus, anti-malware, patch management solutions, and a security training and awareness program
  + 3.a. Anti-virus: We met this goal by finding an open-source software program and then installing it on each machine
  + 3.b. Anti-malware: We also met this goal by finding an open-source software program and then installing it on each machine along with an anti-virus
  + 3.c. Patch Management: We met this goal by using Microsoft Endpoint Configuration Manager to push updates and patches to each computer
  + 3.d. Security Training and Awareness Program: This goal was met by creating a PowerPoint presentation on security awareness and training users on how to deal with and spot phishing attacks

# Project Timeline

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Goal/Deliverable | Planned Duration | Actual Duration | Actual Start Date | Actual End date |
| Physical Security | 30 Days | 30 Days | 01/01/2024 | 01/31/2024 |
| Identity and Access Management | 30 Days | 28 Days | 02/01/2024 | 02/29/2024 |
| Endpoint Security | 29 Days | 30 Days | 03/01/2024 | 03/31/2024 |

# 

# Every goal/deliverable was met with each phase because we gave time to spare. We decided we had time to dedicate a month to each of the three phases while we originally could have done this in two to three weeks in hindsight. We did it this way because we used the Agile framework and wanted extra time for any review and feedback as time went on. This was approved by the CEO, who hired the cybersecurity team to implement this strategy. The company was also not in an immediate rush for everything as they were still in the process of getting all of their equipment set up in their new building. The physical security took the longest amount of time before we reached the review and feedback phase at 25 out of 30 days, but we still had time for any iteration if it was needed. The cameras took the longest to get implemented and placed, while the badge readers took the shortest amount of time. If we didn’t outsource installing the turnstiles we wouldn’t have met our goals for the month.

# As for Identity and Access Management, we also made the time with a week or two to spare, but we used that time for review and feedback. We met this timeline because we implemented a password policy that we had a guideline for already with NIST recommendations and changing default credentials to a secure password was relatively easy. What took the most time was figuring out everyone's job duties were so we can apply the principle of least privilege. We only waited 3 days for the hardware tokens to arrive after we ordered them and we implemented multi-factor authorization the day we received them.

Lastly, we met the goals for Endpoint security relatively comfortably as well. There were no hiccups in implementing Anti-virus and anti-malware once we agreed upon the software to use. Since all the computers were Windows machines, we quickly utilized Microsoft Endpoint Configuration Manager for patch management and got every machine up-to-date. What we spent the most time on was creating a PowerPoint presentation for the security training and awareness program. Afterward, we only had about a week to simulate phishing emails and see if anyone still needed to be reeducated on the topic.

# Unanticipated Requirements

We didn’t deal with a lot of the personnel on a daily basis because they were still in the process of transferring everything to this new facility, but we did run into a gentleman who gave a lot of pushback on the badge readers. We had to explain to him that security is paramount, not just for the building but for everyone's safety. Other unanticipated requirements were learning how to wire these cameras through this new building back to the central hub. Looking back, we should have used wireless cameras, but we got it done, and it did save the company money, which they appreciated. We had to educate ourselves on creating badges with the correct permissions as well as learning everyone's job function. This only took time as the cybersecurity team hasn’t created badges in the past, and learning everyone's job function is something we had to get up-to-date on to apply the principle of least privilege as well as who has authorization to the server room. The team also was lucky enough to have enough foresight to know the camera setup could take a while so outsourcing the installation to a third party saved us on an unanticipated outcome there. The last technical issue we had was getting the false positives to show up anymore when using the badge reader. One of the techs lowered the sensitivity of the scan and definitely lowered the false positive rate to where we didn’t see it again.

# Conclusions

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. The CEO said the reports of theft and tailgating stopped from what we implemented, which was a big accomplishment. Physical security did take a long time to implement though and this was due to wiring issues we had 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. We saw an immediate decrease in successful phishing attacks and no one fell for our simulated phishing emails, which was another big win for the success of this endeavor.

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.

Some of the signs and metrics we used for success were seeing the decrease in successful phishing attacks and with our simulated phishing attacks, theft not occurring again, nor tailgating being reported. There was also no false positives reported again and no one entered the facility or server room without a badge and without those correct permissions. This was a great success and the CEO was very happy with the defense in depth strategy we implemented.

# Project Deliverables

The PowerPoint presentation was one of the most successful parts of the defense in depth methodology we used for Balrog Gaming. It demonstrated users being trained successfully on preventing and mitigating phishing attacks by being able to spot them and to not simply click on links or pass around these suspicious emails to others. This was a big part of endpoint security in phase 3 and was found even to be successful in providing other general best security practices in a fun and encouraging environment.

Next is the methodology we used in implementing physical security, identity and access management, and endpoint security in a successful and timely manner for a company of Balrog Gaming’s size. It is the agile framework. This allowed us to be able to go through each phase of the agile framework when implementing the deliverables in each phase. Analysis allowed us to gather and prioritize the requirements needed to reach our goals. Design helped create the actual design for the solution, focusing on flexibility and simplicity. Implementation had the team actually implement and put to work our goals and deliverables by installing what is needed for example. Testing is where we make sure everything is working successfully. Review and feedback is the final stage, where we can monitor and take in any feedback. This framework was the key to our success in meeting the company's goals with defense in depth and doing it on schedule.

# References

"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.).

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

Retrieved on June 15, 2024 from <https://www.exabeam.com/explainers/information-security/defense-in-depth-stopping-advanced-attacks-in-their-tracks/>

“Defense in Depth: Everything to Know About the Cybersecurity Model,” also further goes into the benefits of an in-depth defense approach and states, “Defense in depth is a cybersecurity strategy that utilizes multiple layers of security to holistically protect the [confidentiality, integrity and availability](https://www.unitrends.com/blog/cia-triad-confidentiality-integrity-availability) of an organization’s data, networks, resources and other assets”(Spanning Cloud Apps, n.d.).

Spanning Cloud Apps(no author, n.d.). Defense in Depth: Everything to Know About the Cybersecurity Model.

Retrieved on June 15, 2024 from <https://spanning.com/blog/defense-in-depth/>

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>

“Threats to your business’ information security come in many forms today, and advanced hackers are constantly changing their methods and exploiting unpatched software or lax employees”(Mark Knowles, 2024)

Mark Knowles(2024). “The Importance of Endpoint Security”

Retrieved on June 15, 2024 from <https://hyperproof.io/resource/endpoint-security/>

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

Retrieved on June 15, 2024 from <https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication>

“Implementing MFA makes it more difficult for a threat actor to gain access to information systems—such as remote access technology, email, and billing systems—even if passwords are compromised through phishing attacks or other means”(More than a password, n.d.)

Cisa.gov(no author, n.d.) “More than a password”

Retrieved on June 15, 2024 from <https://www.cisa.gov/MFA>

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

Retrieved on June 15, 2024 from <https://www.dataversity.net/understanding-the-importance-of-identity-and-access-management-in-data-protection/>

“The concept of [identity and access management technology](https://optimalidm.com/solutions/technology/) makes it more difficult for an outside party to view, manipulate or steal sensitive data.”Optimalidm(no author, n.d.)

Optimalidm(no author, n.d.) “Why Is Identity and Access Management Important?”

Retrieved on June 15, 2024 from <https://optimalidm.com/resources/blog/importance-of-iam/>

# Appendix A

# Security Training and Awareness Program – PowerPoint



# Appendix B

# Agile Framework

