Abdulaziz Alsaif

Alfonso Haskins

Juman Aljahani

Gaming and gambling Industry

Abstract

The gaming industry is an industry that has transformed itself from just gaming to almost everything consumer related. Currently 30 states allow for any type of gambling commercial or tribal, out of those 30 states only 18 are commercial casinos. As some states are having difficulty balancing their budget increasingly they look towards the gaming industry to help remedy their budget woes.[1]

The United States commercial casino supported approximately $125 billion in spending and nearly 820,000 jobs in the U.S. economy in 2010 – roughly equivalent to 1 percent of the $14.5 trillion U.S. gross domestic product. This is the modern day casino where it's not just about gambling but also numerous auxiliary restaurant and hotel services. This industry includes standalone casinos, casino hotels, riverboat casinos, bingo halls, gambling machine manufacturers, lottery services, Internet gambling services, bookmaking and other gambling services. What are not included in this industry are horse and dog racetracks, and cruise lines with gambling operations. Just like with almost every other industry in the world the gaming industry is experience a shift from brick and mortar to online although it would be hard to say that the old brick and mortar would ever be fully replaced by online gambling. Online gambling itself is a growing industry, which has yet to reach its true potential.[2]

Convince is the name of the game, many gaming establishments as well as other industry's try to lure its customers in with the promise of convince comfort and a relaxed environment. One way this is accomplished is by making it extremely easy to wire money to the casinos and get lines of credit from the casinos so that the customer doesn't have to carry all that pesky cash around or go through the hassle of getting travelers checks. "Comps" short for compensations are another tool used to get customers in the door and firmly planted in a seat. With no windows or clocks and comps like free drinks free stays in their luxury hotels customers are sure to stay longer than they ever intended to. It is a sector based purely on entertainment with a side of gets rich quick.

In addition, in each casino, there should be a thousands of employees working in many different areas such as Gaming dealers, Surveillance officers, Gaming supervisors, Gaming managers, Maintenance, Cage cashiers, Slot technicians, Valet dispatchers, Cooks and sous chefs, Bartenders, Accountants, IT employees, IT Security employees, and Security. [3]

[1] (Villano, 2013)
[2] (American Gaming Association)
[3] (Peters, n.d.)

In this industry, the IT equipment's are similar to the other industries including PCs, servers, and workstations. Software needs system, utility, and application software. Furthermore, hardware equipment contains network server, computer printers, screens, projectors, cameras, and storage media. The numbers of the equipment that is needed for this industry depends on the size of this business.

With that in mind, securing all the aspects of this industry is very important in maintaining business operation. This means that we must implement a multifaceted system that includes physical security, personnel security, operations security, communications security, network security, and information security. These will allow us to protect the sovereignty of the state, in its assets, its resources, and its people. As for our aim, protecting information security in our industry is out top priority, and insuring that all information meets the critical characteristic, of Availability, Accuracy, Authenticity, Confidentiality, and integrity.

We must first understand ourselves and the threats that we face to better protect ourselves from any attacks. This means that we must know our information that needs to be protected and the system that stores, transport, and process it, to better understand what an attack might cause, and how it could be better secured.

Investigation

Management will be informed about the threats listed below to be able to better analyze them, and they would be the one to better understand the industries concerns. Below are the top four threats that the Gaming and gambling industry faces:

DDos attacks are a serious threat to online casino, brick, and mortar casinos alike. A DDoS is a attack to make online services unavailable by flooding it with traffic from a number of different sources it is very effective in taking down an online service. Hence, why this could be extremely bad news for online casinos and brick and mortar casino as well. While online casino is sort of self-explanatory if they where to be hit by a DDos attack it would cripple all online gambling until the attack was done. With conventional casinos, it seems to be a little different to the untrained eye but what one may not realize is that slot of conventional casinos host online high stakes card games. If a DDoS attack was to happen during our prior to a game starting it would damage the casino credibility and also a loss of customer confidence.

Phishing is another attack that can do harm to casinos. Phishing is where someone tries to acquire sensitive information like username and passwords by acting like a trustworthy entity. When done to online casinos one would be able to access player's account and steal virtual chips out of the compromised accounts, essentially, stealing money from other players or the casino itself. Conventional casinos are target for phishing as well. Almost in the same way, they affect online casinos. Accounts with the casinos can be hacked from phishing confidentiality broken players accounts compromised and with a little bit of luck, the hackers

would be able to steal chips out of the pockets of players hurting the casino by destroying the confident of the consumer.

Social engineering is the method that hackers used to trick people so they can break the security system through their error or failure. This is important threat in the gaming and gambling industry because the main goal in that industry is the money. Hackers can break into the system and steal many usernames and passwords of the customers. Also, credit card information while online casinos play big role in that industry. Human error or failure can cause a huge damage in gaming and gambling industry due to their sensitive security operation of the casinos. Casinos have many workstations, server, cables, and router that make the human error or failure riskier in that case. In addition, to avoid human error or failure the casinos must have solution to avoid all kind of threat in the security system, if any kind of threat happens they can solve it easily and in the shortest time to avoid more damage in the security system.

Deliberate software attacks are threats that are very harmful to the Gaming and Gambling industry and are most referred to as malicious code, malicious software, or malware. They are designed to damage, destroy, or deny service to the target system using viruses, worms, and other types of attacks. Viruses are malicious codes that affect an operating system when it takes control of the program. They can only be spread from computer to computer though physical media, e-mail, or any other form of computer data transmission. A Worm on the other hand is a malicious program that replicates itself without requiring a host program environment; they do so until all the resources are filled in the memory, hard drive, and network bandwidth. This does not only stop there but worms redistribute itself to all e-mail addresses and can deposit copies of itself onto all web servers infecting more an more as it goes. Any of those attacks are very harmful to the industry in that they can cause major loss of revenue, specially to online gambling in that if the system is either damaged, or destroyed, many valuable information will be vulnerable to loss its availability, confidentiality, and integrity.

Analysis

(a) Risk **identification**

DDos attacks are a serious threat to online casino, brick, and mortar casinos alike. A DDoS is a attack to make online services unavailable by flooding it with traffic from a number of different sources it is very effective in taking down an online service. Hence, why this could be extremely bad news for online casinos and brick and mortar casino as well. While online casino is sort of self-explanatory if they where to be hit by a DDos attack it would cripple all online gambling until the attack was done. With conventional casinos, it seems to be a little different to the untrained eye

but what one may not realize is that slot of conventional casinos host online high stakes card games. If a DDoS attack were to happen during our prior to a game starting it would damage the casino credibility and a loss of customer confidence. The website of the gaming industry is the asset that is under risk of DDos attack.

Deliberate software attacks are threats that are very harmful to the Gaming and Gambling industry and are most referred to as malicious code, malicious software, or malware. They are designed to damage, destroy, or deny service to the target system using viruses, worms, and other types of attacks. Viruses are malicious codes that affect an operating system when it takes control of the program. They can only be spread from computer to computer though physical media, e-mail, or any other form of computer data transmission. A Worm on the other hand is a malicious program that replicates itself without requiring a host program environment; they do so until all the resources are filled in the memory, hard drive, and network bandwidth. This does not only stop there but worms redistribute itself to all e-mail addresses and can deposit copies of itself onto all web servers infecting more an more as it goes. Any of those attacks are very harmful to the industry in that they can cause major loss of revenue, specially to online gambling in that if the system is either damaged, or destroyed, many valuable information will be vulnerable to loss its availability, confidentiality, and integrity. This can threat the OS that runs the web server, which may cause a lost of data such as customers credit cards numbers or customers requests and transactions using the website.

(b) **Risk assessment**

	Web-server 1	Credit card info 2	Customer data 3	Payment data 4	Total
DDos attacks 1	0.8	1.0	0.7	1.0	3.5
Phishing 2	0.7	0.5	0.9	0.6	2.7
Social Engine	0.8	1.0	0.6	1.0	3.4

ering 3					
Deliberate software attack 4	1.0	1.0	0.8	1.0	3.8

(c) **Risk control**

DDoS Attack

DDoS Attack control can be by setting a firewall that filter out the unwanted flow. And this is a defend strategy.

Deliberate Software attacks

The first risk control is to Mitigate and by doing so; we will create a business continuity plan that will encompass the continuation of the business activities, even if a catastrophic event were to occur. This will include the secondary data centers, hot sites, or recovery sites, which will keep the company running with minimal disruption. The other strategy is to defend, and we will implement the security control by adding the safeguards to deflect attacks on the system and minimize the attacks that will succeed. The design will include the layered protection and administrative control to minimize the risk.

Logical design

1) DDos attacks
2) Deliberate software attacks

Policy:

SySP will be used to set new standards and procedures to insure that neither DDos attacks, nor deliberate software attacks become a very easy subject of attack toward the gaming and gambling industry. This policy provides levels of control access for authorized users in that if we have a firewall, the engineers follow a statement of intent from the manager for guidance to select, configure, and operate on a firewall. The SySP then has two groups one of, which is managerial guidance, and technical specification.

Managerial Guidance will provide the new guide to implement and configure the technology to address the high risk from the two threats that we face that are DDos attacks, and Deliberate software attacks. This will be the document that the managers will create who have a clear understanding of human behavior to provide a better structure to securing the information.
The Technical Specifications will then include the access control lists and the configuration rule policies. Access control lists will provide the access lists, matrices, and capabilities that will govern the right and the privileges of users. The configuration rule policies will list the new rules that govern the many component of the security system from firewalls, to intrusion detection, to proxy servers, which will be update continually so that it will allow the system to handle each data element they process.
The Documents are also important in that they are managed well. These documents are important and must be properly disseminated, in that they are correctly distributed, read, understood, agreed to, and lastly applied. ISSP will cover emails, use of the Internet, and specific minimum configuration of computers to defend against worm and viruses. The Gaming and Gambling industry need to write statement of policy, authorized access and usage of equipment, prohibited usage of equipment, statement management, violation of policy, policy review and modification, and limitation of liability.

Design:

For design, the industry must build a security architecture design. In addition, the sphere of security will have to protect the information for the customer in Gaming and Gambling industry like their usernames, passwords, and credit card information. The system will use multiple firewalls to filter the incoming and out coming traffic network in many ports. Defense in depth is very important on our security system because it has many layers to highly protect the network from hacking to the software. Security perimeter defines the boundary between the outer limit of the organization's security system and the beginning of the outside world. We also need a security domain so the trust user can freely communicate to the system because the users have authorized access to all systems with it. DMZs and Proxy Server are in the security system need because DMZs provide access to the organizational Web pages without allowing Web requests to enter the interior networks.

Education:

SETA, the security education, training, awareness program is very helpful for the employees who works in the security system in Gaming and Gambling industry because all of them is necessary for their knowledge and excellency. We could do three months training in the beginning, then some workshop to

get them acknowledge in some lacking areas, and of course awareness should be everywhere and all the time.

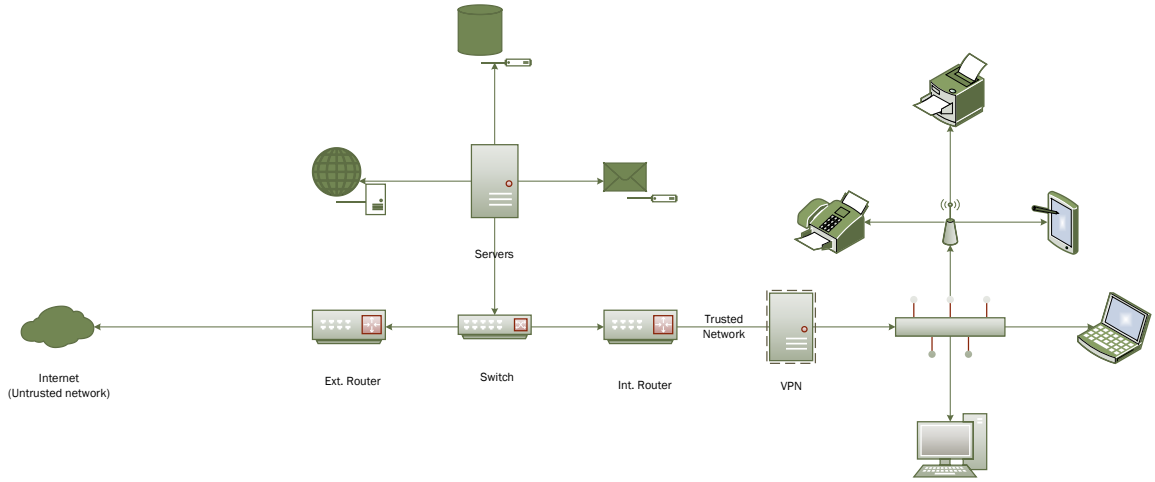
After a successful DDos attack the victim's computer, system would be at a crawl in the best scenarios, and at a standstill in most cases. What happens is the servers are so overloaded from request from who ever is trying to bring down your websites, that it stops processing new request. User of the computer system would start getting an error message. This is the only way one can begin to detect an attack if they do not have the necessary monitoring software. To combat this check your web site regularly and check your web stats. So, what is next? Something needs to be done to stop the attack, and the first person on the list should be your network admin he/she will have the tools to monitor and verify that an attack is taking place. They would then monitor the users and see who is running the attack, and block them from accessing the site or sending request to your server. The only time a DDos attack would turn into a disaster type situation is if the network admin or the system admin was unable to stop the attack, which could happen various ways. One being the Admins might not have the software they need to monitor the system correctly, so that they may single out the attacker. If the DDos attack brought down the system and the admin are unable to stop the attack then it would be consider a disaster keeping the certain casino/ gaming entity from conducting business. The only real way to get back to somewhat of a working environment is to stop the attack so the admins would need to get certain software that can block/drop questionable packets. In the future the best move would be to properly defend the network, site, and, servers. By using firewalls and monitoring software and new software design to prevent such attacks or at the minimum mitigate an attack and keep it from becoming a disaster.

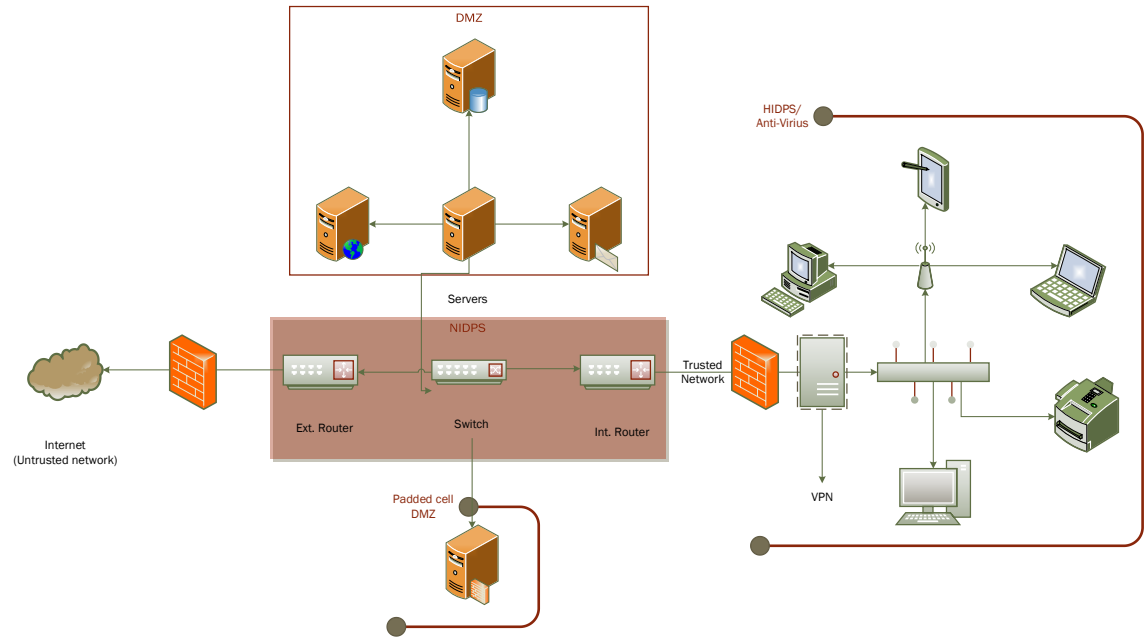
Another major attack that could happen to the gaming industry is a deliberate software attack. The malicious code could affect all aspect of the business. Spotting an attack can be difficult unlike a DDos attack there may not be any tell sign of an attack. You may find out only after the attack is finished or as private documents are released to the public or put up for sell. Coincidentally the best way to find out if you are under attack is to use updated antivirus, which would be the same way you defend against an attack. Letting the admins know about your hypothesis would be the best place to start. They can deploy the necessary software to stop the attack or keep the attack from spreading. Once again, a disaster would be classified as a complete inability to continue normal business practices. If this were the case then you would be detrimental to the business and could result to a loss of consumer confidence. In this industry consumer, confidence is extremely important. If this was the case there would be no other choice then all hands

on deck to stop the attack, by getting the necessary software making sure it is up to date, or taken affected systems offline till they were completely scrubbed of the malicious code.

Physical Design A

Our design is composed of a variety of routers with firewalls, IDPS, DMZ, application level firewalls, application level anti-virus software strategically placed throughout the network to create as many levels of defense as possible as demonstrated below.





Our standard network includes element used by most business to include the gaming industry. Those components are external and internal routers, a hub switch leading to the multiple servers. Which consist of an email, web, and, database server. Lastly VPN connected to a trusted network which includes an array of different devices such as fax machines, laptops, tablets, and, workstations. To protect our assets and devices we have issued policies and education on allowed uses of the network. Now is the time we implement technology to help protect our network. To protect our servers we have placed them in a DMZ in conjunction with a NIDPS and firewalls on the external and internal routers. This leaves us with 3 levels of protection for our servers. Our next assets is the VPN and trusted network which has been protected by HIDPS and anti-virus software installed on the individual devices, they also are protected by the firewalls installed on the network. Lastly we installed a protected honey pot also known as a padded cell so it would give hackers another target and hopefully we can figure out how they infiltrated our network so we can setup new policies and technology to keep them out of our more important assets.

Physical Design B

Physical security is one of the most important components of security. There are many ways we can state it. In our project we have plan to use cameras around the building for monitoring purposes. One of the seventh losses of physical security is extreme temperature like heat or cold, so we have decided to use sensors for it to protect our machines. In addition, we will have sprinkle water system and fire detections in different spots. Also, we have to secure the pipeline system in that building, so the gases will not affect the machines. Furthermore, to protect our machines we have to used alarms and locks in the gates such as manual, mechanical, and electronic locks, so in that way we can limit the people who can access to these workstation and servers. Mantrap and electronic monitoring would fit perfectly in our physical security system.

Implementation and Maintenance

This implementation will and maintained will be the next necessary step to maintain the system that we set out to secure. It is in that we identified the threats, that we believed to be the top threats on the gaming and gambling industry, we identified the top two threats to Asses wither it became a risk based on the exposure. Then, it allowed as us to control the risk and create a logical design based on what was necessary from us to create the policy, design, and provide the education. We then created the physical design, which included all the components, the will better protect the network that this system operates on. Lastly we, included all the needed physical security systems that protect the hardware from sprinkles to sensors, and cameras.