The Real World

by Andrew Cardno

The following discusses a real-world cyber-attack on an online casino group and translates this into a scenario showing what this might look like in the highly regulated space of Indian gaming. Details of the real events surrounding the online information leaking was reported on by *ZDNet* in January 2019 – it makes for a sobering read.

Hacked

A casino has leaked information to the internet on over 100 million bets; including details about customers' personal information, deposits, and withdrawals. The data was leaked from a database server connected to the internet for the purpose of providing real time marketing services. The data was stored in a high-performance database, which allows companies to provide rapid response to queries for information relatingn to online marketing initiatives. The database was left open to the internet and could be directly accessed to see specific customer information and had access to an interface to generate promotional dollars, also known as freeplay.

On further investigation, researchers found that data from the on reservation engine was replicated into a hybrid cloud environment and co-mingled with data from other gaming facilities. This co-mingling of data was used to provide overall gaming market statistics and was even used as the basis for an online gaming operation.

Deeper analysis of the URLs on the cloud server environment, security investigators found a large number of online gaming facilities that were being run where users could place bets on slot games and online table gaming operations. The database was taken down from the internet as soon as the leak was discovered, however, it was exposed for a sizeable period of time, meaning any number of things could already have been done with the available data.

Fallout

What does this mean for you? In this scenario your customer data has been exposed to the world, but you are still lacking in information. The next questions should be about the immediate fallout of the situation, who will be responsible for the event in question, and how you prevent this from happening again?

The immediate fallout is a hard question to quantify, your first duty after patching up the wholes in your security on learning of an attack like this one is to your customers, making sure that you remove the database from the internet, and subsequently inform them of the breach so that they can take steps to secure their personal information. These customers, particularly ones with recent sizeable winnings, are at risk of being the targets of various scams and attacks so it is important to notify them as soon as possible.

Next, there is accounting to be done for those responsible, because in the eyes of regulators, you are one of the key responsible parties. Your data being leaked due to an attack is something that is ultimately your responsibility according to regulators, and if your casino did not do its part to secure your customer info, then there could be consequences. The security and isolation of your servers is a large part of this responsibility, in addition to making sure that outside vendors that come in contact with your databases are vetted and have the correct licenses – something required by gaming regulators.

Cyber criminals are increasingly sophisticated, they can move freely between countries and no place that is connected to the internet is completely safe. They are highly connected and can create sophisticated attacks on many kinds of databases. They have been known to impersonate people over the phone in order to get employees to click on phishing e-mails. They have even stolen physical identification keys that are used for secure logins.

Response

You have been the victim of a cyberattack, now what? The first steps from an organizational point of view are quite simple – figuring out how the breach occurred and patching that specific hole in your security network. This will, however, not solve all of your problems. Cyber security is a complex beast and it requires the participation of quite literally every single member of your organization to maintain. It has many layers each one highly important in keeping out potential attackers.

Layer 1: Your firewall is the first line of defense against a malicious outside attack – there are a few different implementations, with the use of a dual firewall being quite popular in the modern era. Dual firewalls literally are two firewalls from two different vendors, creating a demilitarized zone putting internet facing servers on a less restricted, less secure network that can freely communicate with the internet. It also puts internal servers on a secure network that is not reachable by outside networks and can only send information to the DMZ in the middle. Security incident and event monitoring software is highly important to the security of your network as it looks at security incidents and evaluates the associated threat levels in real time, and is a key partner to your effective firewall.

Layer 2: Your next line of defense relates to your internal programs and backups. Even with a firewall in place, it is possible that your network could suffer from a breach, so it is important to have anti-virus and malware reporting tools on your servers and internal computers. It is also important that you keep your devices up to date via a patch management tool that monitors and reports to your IT team. Lastly, backups are the critical last resort in cyber security. Should your network become infected, it may be necessary to scrap it and the infected databases. If this is the case, then a backup will likely save your business.

Layer 3: People are the final layer of your security. One of the most frequent ways in which breaches occur is internally via an employee that clicks an unknown link allowing hackers onto your network. There are several things you can do to mitigate this risk. Using a specific e-mail format is a good way to ensure that outsiders do not get onto your network as any e-mail not following the format can be subject to further verification by users. Penetration testing, wherein your internal IT team sends benign phishing e-mails to team members to test responses. Follow up and discussion are two of your most important tools – talk to the members of your organization about the importance of cyber security and make sure that any lapses are specifically addressed.

Conclusion

Cyber security is a very real issue and casinos are prime targets for hackers as their databases are loaded with sensitive personal information that can be used for all sorts of nefarious things. As for the actual steps you can take to make your company more secure, while several are listed here, one of the most important is that you take the threat seriously. ♣

Andrew Cardno is CEO & Founder of Innovation Gaming Group. He can be reached by calling (858) 254-0412 or email andrew.cardno@innovationgaminggroup.com.