CYBERSECURITY'S TOP FIVE ISSUES

BY CHARLES ANDERER

Casino networks are riddled with weaknesses and vulnerabilities. Here's what they are and how operators can protect themselves

When it comes to network security, casinos are often wide open to online attackers.

That's the basic finding of Bulletproof, a GLI company, which has completed network security assessments at more than 100 casinos. During the course of these evaluations, Bulletproof's team was routinely able to gain access to vast amounts of casino player and employee data in minimal amounts of time.

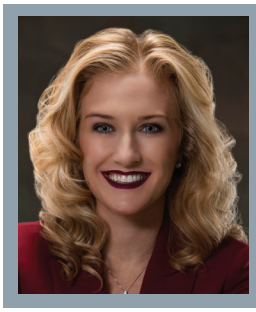
That's a problem, not least because the cost of an average data breach is just under $4 million and growing, per an IBM cost of data breach study 2017. "The damage from a security breach can wreak havoc to any organization beyond the financial loss of breach recovery and most importantly the organization's brand and reputation," said Melissa Aarskaug, vice president of business development USA at Bulletproof.

The good news, according to Cory Johnson, a Bulletproof management consultant who led the on-site assessments, is individual casinos currently don't figure high on the target list of network hackers, who are primarily in search of credit card and personal health data. "The breaches that we know of in gaming seem to have been through point-of-sale systems," said Johnson. "From what we can surmise, these attacks were not targeted at casinos, they were targeted at retailers."

The bad news is, given the scale and pace of cyber-attacks, it seems only a matter of time before all consumer-facing businesses including casinos will "get their turn," and that personal information, gaming operations, network infrastructure and company reputations could all be compromised. Citing data compiled by Verizon, Bulletproof notes that 2 billion records were compromised in the last year alone and there was an 8,350 percent increase in ransomware usage, i.e., people trying to extort money. All industries are struggling with this issue; the time between a security breach and its actual detection averages 197 days. With that in mind, there are far bigger, more attractive targets than casinos, but the clock is always ticking.

"As breach reporting for gaming is less regulated, there is little data on the extent of player data leakage. Additionally, it's likely that the affected casinos may not know that it was taken due to a lack of effective monitoring. What we do know, is that since the networks tend to have shared credentials and little the way of segregation, if there hasn't been loss of gaming data, it's due to sloppiness on the part of the attackers, rather than any inherent security in place."

Bulletproof has identified five key areas of network security threats and how to address them. A summary follows:



"The damage from a security breach can wreak havoc to any organization beyond the financial loss of breach recovery and most importantly the organization's brand and reputation."

—Melissa Aarskaug, vice president of business development USA, Bulletproof

UNPATCHED SYSTEMS

When a system has been attacked, the software provider usually issues a patch to resolve the vulnerability. Unfortunately, the latest and greatest operating system patches often fail to upgrade casino-based systems for a variety of reasons. For example, patching a server might mean breaking an application or service that's running on that server. Another issue is that the operating system may be patched, but a third-party service or application that's running on that server isn't patched, which introduces a new vulnerability. In addition, a lot of the third-party applications and services that casinos have implemented are on outdated legacy systems that won't allow those applications to be updated.

"We see many out-of-date systems in the field," Johnson said. "These aren't always vendor systems or workstations; these could literally fall into any part of the network. Recently we've still seen unpatched Windows XP boxes missing patches from back in 2008, as well as the ones that are highly publicized and critical like the Eternal Blue issue that was patched earlier this year after the CIA leak. We're still exploiting that one in the wild fairly consistently. "Secondarily, you have to have up to date anti-virus, even on gaming systems. At a couple of our customers' locations, we were able to gain access by exploiting the anti-virus itself. These are all issues that lead up to requiring a good patch management system."

Aarskaug and Johnson said casinos need to look beyond simply installing every new vendor-supplied patch and develop improved patch management systems. A patch management policy involves self-assessment and scanning systems environments on a regular basis; understanding what vulnerabilities currently exist within these environment and how they can be exploited. If casinos can at least identify where they might be attacked from and what some of those attack vectors might look like, they can start to protect themselves.

A patch management procedure also allows casinos to utilize network segregation, essentially grouping unpatched and previously exploited systems into a restricted network, thereby protecting systems that are patched and up to date. How this helps: casino systems are often designed for ease-of-use by players and operators—having a single, flat network where everything is connected and can talk to each other is easy to administer and popular with patrons and clients. However, such a setup also makes it easy for an attacker to gain access to other systems. These include things that one might not typically consider, such as building control systems that may be connected to the flat network for ongoing maintenance or support. An HVAC system or digital signage display for the building that's connected to the network, if compromised, can be a conduit into other systems. Segregating networks makes it very difficult for someone to get to those back-end and/or player management systems.

"We've been to a lot of places with very flat networks," Johnson said. "By that, I mean that every place on the network can get to every other place on the network. Setting aside how an attacker was able to get access to your network, you have to have a way to mitigate what they're doing once they're there."

By way of example, Bulletproof has been to casinos where digital signage is on Wi-Fi, and it wasn't particularly well-protected because the sign itself had a Wi-Fi access point built into it that people didn't know about.

"Because that Wi-Fi sign was actually on the casino network, we were able to break into the Wi-Fi on the monitor itself and use that as a launching point to attack the rest of the network," Johnson said. "Likewise, at the local network level, we've been able to abuse the authentication protocols in such a way that we could get sign-in credentials by just literally sniffing the network and lying to all the other hosts on that same local network. If segregation were in place, that would have been much less effective; instead of having credentials that we could use within five minutes, we would have to be there for hours doing it the old-fashioned way by scanning and looking for vulnerabilities such as missing patches. When your network is not segregated, it leaves the entirety of the organization open to attack. It's always best to have your network architected in as many small of pieces as you can physically manage."

A layered network architecture where important systems like gaming, player management, taxation and revenue, are as far away as possible from public-type access networks, such as Wi-Fi and building control systems, is one protection against cyber-attacks. This creates multiple layers to jump through in order to get from one system to another, which can frustrate attackers. Unfortunately, this also

An excessive number of admin accounts, weak passwords and loose controls on data access are all issues that can weaken systems.

Attackers often use social media sites to collect information about that person and try to form a bond with that person by pretending to be somebody from their past and then injecting some kind of malicious website into a link that the person is urged to click on.

makes casino systems more difficult to manage, but this is a small price to pay for better data protection.

USER MANAGEMENT & ACCESS CONTROL ISSUES

Bulletproof often goes into system environments that have been set up for ease of administration. The problem with this setup: to make their job easier, users with admin privileges often avoid precautions such as complex passwords, which creates a pathway for attackers to compromise systems and steal data. An excessive number of admin accounts, weak passwords and loose controls on data access are all issues that can weaken systems.

"User management is an extraordinarily complex thing to tackle; every single administrator you have in your environment is a target," Johnson said. "That can definitely become a problem if you're allowing your users to install software. We've been to some places where, via a group policy, every single user is a local administrator on their own computer, which seems harmless at first, but that allows users to turn off literally every control you have. It's very easy for an attacker to elevate from a local administrator user to a system-level user. At that point, they can do anything the operating system itself can do."

To illustrate the point, Bulletproof's field team has been able to go from having a single username and password to being an enterprise administrator in minutes. "You can make this as simple or as difficult as possible for an attacker by just keeping your users and groups constrained as far as possible," Johnson said. "Does a front-desk operator need to be able to install software on their computer? Chances are not. Hotel computer-operators really don't need access to anything other than the lodging management system they're using. Does your back-end system actually need to have a domain administrator account for your operations domain? Generally speaking, no. Failing to keep track of all of your user permissions as they spider out through the domain helps attackers actually gain more access."

It's important to know and manage who has access to what systems and under what conditions. Bulletproof has been able to access a supposedly secure system through a printer used by a domain administrator, due to poorly written software and a reliance on default passwords. "We could ask the printer nicely what username and password it was using to write to the sharer, found out that user for some reason had domain admin creds, so we went from typing 'admin admin' on a web page to complete control of an entire domain in a matter of minutes," Johnson said. "That's where default passwords and poor user group control can lead."

To counteract this problem, casinos need first and foremost to establish strong password protocols that include creating altered passwords on a regular basis. Meanwhile, on the administrative user front, it's not a great idea to give normal everyday users elevated admin privileges; if, for example, this person clicks on e-mail malware, it can spread throughout the entire system thanks to these admin connections. The privileges that most users have associated with their accounts should be limited.

Even though a user might need admin privileges to install software doesn't mean they need access to the back-end data itself. Make sure to keep track of

who has access to what and from where they can access data, and then control that in such a way that they can better protect themselves. Protect things like service accounts, database accounts or default application accounts and be sure not to use out-of-the-box or well-known passwords for all those accounts.

INEFFECTIVE LOGGING & ALERTING

A lot of casinos spend considerable time and money on logging and alerting systems, but often times those systems aren't very effective, according to Bulletproof. Among the issues: not understanding what should be logged and collected and not logging secondary pieces of information. Casinos might be looking at system events and errors instead of application events and game transaction logs that might indicate a breach. Systems also might not analyze things like security events. They're not necessarily picking up on things like multiple failed logins or brute-force type password attempts.

"We often see situations where events are being logged and information collected but not the instances where someone is actually trying to do something," Johnson said. "We've been spotted before we've been able to gain full access only twice in the last eight years or so, and that was really an outlier. The first time we were spotted was because they knew we were coming and they basically staffed someone who was supposed to catch us. The second time was simply because they were doing things correctly.

"Our engagements usually start first thing Monday morning or Sunday night if we're staying on property and 99.9 percent don't notice what we're doing the entire time we're there. By the time we're done we have the entire patron database; a copy of everyone's employment records; and in some cases, we have copies of everyone's passwords for stuff that has nothing to do with work, simply because they left it on a file share."

"It's not that we're trying to be sneaky, in fact, some of the tools we use are offensively loud," Johnson added. "But unless something actually breaks during the process of the engagement, most people don't notice anything happening at all."

Other events often overlooked include previously unused network ports that are suddenly saturated with data and login events that go from one computer to thousands of other company computers in the space of a minute. "The only thing that shows up in the logs, if they're bothering to log at all, is that somebody successfully authenticated," Johnson said. "And even when those things are logged, for instance, Windows active directory controllers log a variety of data by default, unless you have alerts set up for the things that they are logging (e.g., invalid logins), it's almost pointless to log it in the first place. Outside of gaming, there are requirements for logging, particularly within the PCI [payment card industry] space. Inside gaming, it

Configuring e-mails not to automatically download attachments is one way to counteract social engineering attacks. E-mail filters that scan attachments as they come in or go out, removing malware payloads, are another beneficial tool.

varies by jurisdiction, but 90 percent of the time those login requirements are to protect accounting data, not access. People are logging revenue but not when it was accessed, and not alerting when I decide to make myself a domain admin or promote somebody who's in HR to a domain admin. Those sorts of things can be logged, but if they're logged, they don't necessarily merit an alert."

"Often we end up in a position where we're under the radar and have the run of the entire enterprise as long as we don't make a mistake and knock a server over," Johnson added.

Aarskaug and Johnson emphasized that better handling of alerts in real-time needs to be a priority; if someone discovers a breach the next day or the next week, it's already too late. The longer the window between breach and detection, the more chance data has been opened and is out there for the world to see. Casinos also need to understand the sources of data collection. Talk to people who know the systems, applications and environments and are validating the data that they're collecting and monitoring. Understanding what certain types of alerts and events mean is essential, as is developing good processes on how to respond to them.

SOCIAL ENGINEERING ATTACKS

Social engineering attacks are scare tactics and threats of financial loss to target individual users. Common forms of this type of malfeasance includes:

- **Phishing:** Looking for things like usernames and passwords and/or financial account information, phishing includes whaling attacks or targeted phishing attacks aimed at C-level executives who have increased access to an organization's critical information, data and financial systems. These are often prolonged attacks that involve an attempt to gain the trust of the targeted person. Attackers often use social media sites to collect information about that person and try to form a bond with that person by pretending to be somebody from their past and then injecting some kind of malicious website into a link that the person is urged to click on.
- **Malware:** There are more and more malware attacks especially with ransomware being part of the mix. Bulletproof is seeing attachments being e-mailed to people that say, "Here's your invoice," or "If you don't click on this and respond you're going to go to jail," fear tactics that are designed to get people to do things they normally wouldn't do.
- **Non-IT attacks:** This involves perpetrators gaining physical access to office space through low tech means such as 'holding the door," which entails tailgating an actual employee into workspaces that have minimal or no security. "You may already be in a building wandering around the back of the house," Johnson said. "A lot of places require a badge but we've been to a places with no badge—opening doors, walking into places with nobody asking who we are and why we're there. We've had really good luck with USB drops, where we have a Word document that has malicious macros on it and put the USB drops in the break room. Eventually, someone will pick it up, plug it in and all the document does is open a connection back to our server so we can tunnel back in and use their access."

Whatever the format, the very nature of gaming properties and the types of people they employ can make them a constant target for social attacks. "The important thing to recognize is that social engineering almost always works some of the time; by that I mean it's not effective on everybody, but the people it's effective on, it's always effective on," said Johnson. "The more helpful a person is, the more likely they are to fall for these attacks.

"In our own social engineering engagements, we've done simple stuff like calling the help desk to get a password reset. In one case, we didn't even care about the password reset, we just wanted an admin to log-in to that particular box if possible because then we could steal the admin credentials. In another case, we did our own phishing attack where we set up a web server with a domain name that we bought that was one letter different from the real domain. And then we sent an e-mail to everyone on the e-mail list that we were trying a new webmail server and, if you're receiving this e-mail, go ahead and log in to the server and tell us what you think of it. The opening page just had a username and password box and then they'd be forwarded to the real

An HVAC system or digital signage display for the building that's connected to the network, if compromised, can be a conduit into other systems. Segregating networks makes it very difficult for someone to get to those back-end and/or player management systems.

authentication site. All we did was scrape everything they typed into the first page and we had 15 sets of valid credentials in five minutes. They stopped coming in after five minutes because apparently somebody noticed. But when we reported to IT afterward, only seven of the 15 people reported to IT that they had entered their information in that box. That left eight people standing with live accounts that we could use because they were embarrassed."

Configuring e-mails not to automatically download attachments is one way to counteract social engineering attacks. E-mail filters that scan attachments as they come in or go out, removing malware payloads, are another beneficial tool. Questionable attachments can be quarantined and go into a sandbox-type service or an isolated controlled environment and opened to see what happens.

INDUSTRY MISCONCEPTIONS

The casino industry does have some unique characteristics that increase its vulnerability to attacks. One that Johnson outlined is the regulatory framework. Security is almost never part of what regulators require of vendors. Most gaming regulations tend to focus on two things: fairness and accounting. Most jurisdictions are more concerned with Sarbanes-Oxley compliance than PCI compliance. In this market, anything that is not specifically required of vendors will not get implemented because development and compliance testing and certification is expensive. "People in most commercial settings don't do things that they aren't forced to do," Johnson said. "Because of the regulatory focus on game integrity the games themselves are reasonably secure; it's all the infrastructure that supports the games that is not."

That said, organizations vary. In the last six months, Johnson visited two completely different operations, one gaming, one not, with two completely different results. "At the gaming vendor, I couldn't do anything; they had their network nailed down," he said. "They were confident. I did eventually discover that under one circumstance if an individual found himself in one specific place, the whole thing was wide-open. They took it the right way and tried to fix it while I was there, which they were able to do after a few cycles. At the other, a non-gaming company, it took me 35 minutes to gain access to their entire global operation. Their response was not surprised, but they didn't feel they had enough people to resolve it. That's what I usually hear; we don't have enough IT people and we can't afford a security guy."

The attitude is common: IT doesn't produce any revenue, it's a cost center. "Saving money on IT is great until a breach happens and you spend $1 million on forensics," Johnson said.

In response, some organizations are turning to cybersecurity insurance for coverage. But in order to get that, a casino has to demonstrate that it has a security plan in place and is training employees in security procedures. If they did get breached and they didn't have those things in place, they could potentially not be reimbursed for those breaches.

As for vendors, the principal thing they can do is take security into their own hands, treat their systems as an enclave and cut back on the number of integrations that they support. "All things being equal, in casinos where gaming systems are fully integrated into the rest of the casino, there's a much greater likelihood of easy access to the gaming system or vice versa," Johnson said. "Where the gaming system is set up as its own separate tied-off entity, even if I could get into the point-of-sale system, if I can't get into the gaming system, then that data is safe. If, somehow, I manage to get into gaming the rest of the systems are safe—the attack complexity is greatly increased. Generally speaking, some systems are built more securely, while others are more worried about functionality and integration."

The bottom line is, yes, you could get breach insurance, yes, you could possibly eventually regain your customers' trust—however, prevention is always better than any cure," Johnson added. "Aggressive testing of your IT network is the best way to give you, your vendors and your customer's assurance that data is safe. And the time to do all that is now. Criminals aren't going to sit around and wait, and neither should casinos."