Helping operators keep players safe

The most common types of attack facing an operator include APT (advanced persistent threat) which is when hackers steal information by using sophisticated techniques such as malware to exploit vulnerabilities in systems to extract data from a specific target operator

Shemer Katz,
SafeCharge

1. APT – An advanced persistent threat is a network attack in which an unauthorised person gains access to a network and stays there undetected for a long period of time.
2. AET – An advanced evasion is a type of network attack that combines several different evasion methods to create a new technique that's delivered over several layers of the network simultaneously.
3. IP Spoofing – An hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a website, hijack browsers, or gain access to a network
4. DDoS – A distributed denial-of-service attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the system.
5. Phlashing – A permanent DoS attack that exploits a vulnerability in network-based firmware updates. Such an attack is currently theoretical but if carried out could render the target device inoperable.
6. Malware – Any program or file that is harmful to a computer user
7. Phishing – A form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.
8. Spear phishing – An e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorised access to confidential data.
9. Whaling– A type of fraud that targets high-profile end users such as C-level corporate executives, politicians and celebrities.
Phlashing – A permanent denial of service (DoS) attack that exploits a vulnerability in network-based firmware updates.

Another worrying type of attack is the dreaded Distributed Denial of Service (DDoS) attack which is where the site is subjected to a massive attack by a multitude of compromised systems, using many computers affected by malware, botnets etc, which potentially can slow down and in extreme cases shut down an operator's site.

Other security threats include internal data leakage – not necessarily from an employee but often from a co-worker, supplier, contractor etc. and Frontend Application Penetration which is when a hacker tries to find holes in applications.

The potential consequences of a breached security system can be catastrophic. Some of the effects include: data leakage, penetration of networks and applications, reputation damage, financial loss, game downtime.

All online gaming operators who process, transmit or store customer credit cards need to comply with the Payment Card Industry Data Security Standard (PCI DSS, or as its more commonly known PCI compliance), which is a complex and demanding set of requirements for payment data protection. It is time consuming, costly and risky for online gaming operators to manage their own PCI compliance. If an operator is holding customers' credit card details on file it makes that company far more vulnerable to malicious hackers, whereas if the operator has outsourced PCI compliance and there are no customer credit card details on its system for a hacker to attempt to steal then risks are greatly reduced. As all the card data is processed and stored by a third-party provider, hackers are far less likely to target the operators themselves.

Outsourcing PCI compliance to a third-party payment provider has become an attractive option for gaming operators seeking to minimise the liability of their compliance responsibilities. A key factor in an operator's decision making has been the overwhelming complexity of PCI compliance. Time spent working on compliance also means time spent away from profitable activities. We estimate that the cost of an assessment and implementation of in-house Level 1 PCI-related work can cost between $500,000 and $1m per year. Return on investment is why many gaming operators have begun to look for alternatives.

For an online gaming operator it is important to reduce the red tape involved with PCI, to minimise risk and to reduce PCI scope (the regulatory protocols regarding the handling of customer card data). If properly done, outsourcing reduces or eliminates PCI scope, and minimising scope is the simplest way for an operator to achieve PCI compliance.

Gaming operators need to choose an outsourcing PCI partner carefully, otherwise they may not achieve the PCI benefits they were intending. If an operator's outsourcing partner itself fails to meet PCI standards, the operator is still responsible for PCI. Operators need to make sure they are working with a reputable PCI outsourcing provider which is properly certified and uses the latest technology. Ideally an operator needs to take all its IT infrastructure out of PCI scope, as any part of the operator's IT system which processes, stores or transmits cardholder data comes under the scope of the PCI regulations.

Another way in which an outsource provider can remove an operator from PCI scope is by the use of tokenisation whereby a customer's card details (the primary account number – PAN) are replaced by a token that has no exploitable meaning or value, and takes the place of the card details. With tokenisation if a hacker were to gain entry to the operator's system all he/she would get would be the token which is going to be of no use as the hacker has no means of de-tokenisation.

On 1st June 2015 the new PCI 3.0 standard became mandatory. There is a raft of new and stricter regulatory procedures for operators to follow from this date.

If a merchant is currently outsourcing their PCI compliance to a trusted third party they can let them worry about this. At SafeCharge we have a PCI descoping team that is well versed in the regulations and keeps all our gaming clients safe in the knowledge that all their confidential customer data is secure in the hands of the PCI descoping experts.

Most of the changes being introduced with PCI 3.0 are clarifications and tweaks to existing requirements, however operators that are undertaking their own PCI requirements will realise that there are many changes to be made. The regulation refinements cover everything from the definition of scope and methods of documentation to new ways of preventing fraud at the point of sale.

For operators that do not outsource their PCI requirements they will find an ever-increasing amount of their technology systems will come under the scope of version 3.0. It's not only workstations that handle the credit card data that are included in the scope, it's now more defined in the regulations that any potentially vulnerable server or workstation that touches the operator's network has to be PCI DSS compliant. This extension of the scope has been brought about as a hacker could get into a network by a lesser protected workstation and subsequently gain access to a operator's customer data on the supposedly more secure parts of the network.

Other perils for operators undertaking their own PCI Regulations lurk ahead in the new scoping regulations for PCI 3.0 for example all third parties that handles customer credit card data on behalf of an operator will be included in the scope.

This is often out of the operator's control, but ironically still part of his liability. It is now known that the well-publicised breach of customer data by the U.S. retailer Target was caused by a an initial intrusion into its systems which was later traced back to network credentials that were stolen from a third party vendor.

It's simple. If a merchant doesn't have any customer credit card data touching its system, it is not going to be a target for commercial hackers. Reduce the risk, shift the risk onto an expert company that is fully PCI compliant and undertakes PCI descoping for some of the largest companies in the gaming industry. As well as peace of mind it will save merchants an awful lot of money, and enable them to do what they do best – run their business!