Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Three Steps To Protect Your Network From Hackers

By: Bernardo Lucas

According to a recent Technology, Media and Telecom Risk Index, c-level executives voted cyberattacks/hijacks as the fourth most pressing risk to their business. A perfect storm of legacy systems, complex hybrid networks, and the influx of data traffic is exposing vulnerabilities for hackers to not only breach the security perimeters of networks but also to commit fraud. And as the global smartphone penetration rate is expected to reach 44 percent by the end of 2017, CSPs must guard against new types of fraud made possible by the hyper-connectivity of an expanding array of networked devices. Bernardo Lucas, chief strategy officer at WeDo Technologies provides three steps that CSPs can implement to safeguard their networks.

1. Network security: your first weapon to win the battle against fraudsters

Like criminals who cross physical borders, hackers look for the places where border controls are the weakest and use fake IDs and false keys to hack their way inside. They may even corrupt border security, exploiting weaknesses in a firewall to hijack the network. Because borders can be compromised, it is vital to counter fraudsters through a deep and layered strategy that involves both detection and prevention, in the same way that national security does not stop when you pass through airport security.

Though your network borders will never provide the perfect barrier to fraudsters, CSPs must make access controls as effective as possible. Many good security controls are simple and unsophisticated. For example, you usually ask prospective customers to show an ID card or document every time they want to sign a new contract. However, where good fundamental protections like checking a customer's identity can be a robust and cost-effective way of obstructing fraudsters, analytical intelligence and the manipulation of information can cut both ways. We know that fraudsters often try to evade simple checks by making small changes to details, such as the spelling of their name or providing different middle initials.

When you allow a customer to pass through your borders and enter your network, you can still use your initial risk assessment to improve how you monitor network activity. This is where the concentration of access controls at the firewall and the gathering of data by Security Information and Event Management (SIEM) come together to provide both real-time insights and the forensic capability to determine who is sending which traffic, and what their objective is. An example of this is if somebody with a similar name to a known fraudster calls the same numbers that a fraudster previously called, you can safely suspect that they are one and the same person.

2. Intelligence is required to win the war

To win the war against fraudsters, intelligence cannot exist in a vacuum, but instead requires the collaborative sharing of information at every level within an organization, and also between organizations.

Within a single telco, different departments must pool their combined knowledge resources. Sales

staff, for example, may identify concerns with a customer whilst conducting credit checks. With corporate policies that encourage whistle-blowers, they will be encouraged to pass on the details and give fraud managers the ability to unveil fraud that may not have been otherwise detected. When data breaches occur, fraud managers need to play a heightened role in monitoring for fraud that exploits the data which was compromised.

The charging team can also provide intelligence of potential fraud from data collected by the Policy and Charging Rules Function (PCRF). Some operators offer their subscribers special bundles that allow free access to social networking sites. In this instance, the operator zero-rates the URLs it wants to provide for free. However, attackers may manipulate requests to make it appear as if they are visiting free sites, when they are not. This is called Free URL Bypass and gives the attacker free unrestricted access to the entire internet. CSPs can identify fraud by monitoring the charging rules, correlating them with the information coming from the deep packet inspection (DPI) system, and cross-referencing the free URLs to the destination server IP.

The DPI system can also play a role in identifying one-click billing fraud schemes that target smartphone users by tricking victims into registering and paying for a certain service after they have visited the fraudster's website. More recent variations of this fraud have plagued Android users who have downloaded malicious apps. Whilst closing the browser is enough to escape a fraudster's website, apps can repeatedly demand payment. By integrating your fraud management system with DPI and security information, CSPs can identify fraud by observing outlier trends for the user experience, such as apps which pop-up every few minutes.

In addition, your security information and event management (SIEM) logs can be used to support active fraud detection. For example, a PBX hacker will have typically written a script that crawls corporate firewalls looking for vulnerabilities, such as open ports. When an opening is detected, the scammer can punch requests at it, hoping to tease out information about system vulnerabilities. Eventually the hacker has enough information to force their way through the firewall. Once the firewall has been breached, the scammers can gain access to the PBX, build a back door into the system, and use it to route as much traffic as they want. However, by defining which events are of interest and how they should be responded to, the SIEM security logs can be used to temporarily adjust your thresholds in order to:

- impose channel limitations;
- enforce a cap on the maximum per-minute cost of a phone call; and
- restrict the amount of credit that a company is extended.

3. Context increases the value of intelligence

With so much information to share, technology plays a vital role in eliminating mistakes and reducing bureaucracy, whilst ensuring sensitive information is kept secure and only made available to the people who need to receive it.

Speed is of the essence – to stop the losses and because there is little benefit to identifying criminals after they have disappeared. But with so much information in the network, how can fraud managers quickly hone into the relevant information and focus on the real fraudsters?

To demonstrate the extent of the attacks that hackers are attempting, the antivirus company McAfee mapped and analyzed real-world attack patterns in order to further leverage the data inside McAfee Global Threat Intelligence (GTI) and better protect their customers. During a three month period, they found:

- Every hour, more than 6.7 million attempts were made to entice them into connecting to risky URLs (via emails, browser searches, etc.)
- Every hour, more than 19.2 million infected files were exposed to the networks of McAfee customers;
- Every hour there were 2.3 million attempts by McAfee customers to connect to risky IP addresses, or attempts by risky addresses to connect to customer networks; and
- Every hour, an additional 7 million Potentially Unwanted Programs (PUPs) attempted

installation or launch. The scale of the number of attempts underpins the notion that we can no longer depend solely on human judgment.

By implementing automated analysis, CSPs have the tools to combine data with context, and to synthesize the right decisions at the right time. Contextual analysis encourages optimal decisions by repeatedly adding the latest new data to the foundations of the accumulated history.

In addition, automated contextual analysis broadens our perspective when evaluating how to respond to suspicious behavior and provides helpful background information, exactly when it is needed. When fraudsters access your network, the challenge is to single them out of the crowd, especially when they seek to trick your controls by replicating the behavior of ordinary customers.

Conclusion

Telecom fraud managers are confronted with a growing responsibility. Armed with superior data intelligence helps them to reduce fraud, but the criminals are only responding by becoming more devious and by targeting a wider range of victims.

A communications service provider's first plan of action must be to develop intelligent anti-fraud measures that are built on the foundations of solid security. Instead of following a static policy, CSPs need to be flexible and scalable in order to respond to the current level of threats during normal levels of risk, but also have the ability to deploy more extensive countermeasures when risks are high.

And finally, in order to maximize your detection and prevention efforts, a unified approach to fraud that is tightly coupled with compliance and security is required. From here, CSPs can leverage security insights from first-and third-party applications in order to detect fraud from across multiple products and channels.

Over two hundred years ago Benjamin Franklin said, "An ounce of prevention is worth a pound of cure." This adage has become even more important in today's digital world.