Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 6

Nightmare Network Threats

By Becky Bracken

The loyalty of your customer, your reputation, your bottom line — all can be destroyed in a matter of seconds by network security vulnerabilities. Security breaches like the all-too-common distributed denial-of-service (DDoS) attacks can overwhelm networks with fraudulent traffic and lead to service disruption. Thefts of large swaths of customer data are a real, everyday looming threat and could open up operators to extensive litigation. And worse, interception and penetration of networks have never been easier.

More people and data are traversing your network than ever before, and the opportunities for security breaches are exploding at an exponential rate. Broadly, the first culprits are the much-hailed next-generation networks (NGN) and their move toward an IP-based open standard, which has opened up and exposed tele-communications networks and the data they hold to the Internet and the security threats that lurk online. The amount of network real estate accessible by the Internet broadens the level of threat exposure.

Secondly, the sheer number of devices accessing a network increases its vulnerability to attack. Simply put, more devices, more problems. Smartphones, tablets and all of their capabilities have created efficiency — and services — that continue to evolve to make what was once impossible possible. But the proliferation of smartphones and their applications, not to mention their "always on" nature, are creating a security nightmare for CTOs at every level. Thanks to those two developments, if you're in charge of network security your task is bigger than ever. Below are a few of the specific security threats that should be keeping you up at night.

BYOD

Mobile security is where the cyberthreat action is, and where prudent network-security managers have to keep an eye out. Smartphones have enabled even the least tech-savvy network user to bring the apocalypse, just as fast as you can say "Angry Birds."

CTIA CEO Steve Largent warned in October at MobileCON that there is widespread concern about mobile security among IT professionals. In fact 86 percent of those surveyed say they worry about smartphones on their network and their vulnerability to attack. Now that BYOD uptake is practically feverish, more foreign mobile devices than ever have access to the network. Even if you think there aren't unauthorized devices on your network, there are. Now is the time to get serious about policy and network intelligence tools as well as wrangling rebel employees and devices.

One report, from Check Point, based on a global survey of 768 IT managers, found that 89 percent have mobile devices such as smartphones or tablets connecting to corporate networks, and 78 percent say there are now more than twice as many personal devices connecting to corporate networks than there were just two years ago.

All of those devices are creating a security nightmare. A hearty 71 percent of the IT managers surveyed say mobile devices have contributed to increased security incidents, and the Android mobile platform is considered to introduce the greatest security risks. Seventy-two percent also say careless employees are a greater security threat than hackers.

Employees

Lame passwords, quick and dirty workarounds and apps are by far the biggest threats to network security. Tight network policy controls are one thing, but strict corporate rule making about BYOD policies is the best place to start. Increasingly technical teams need to interface with legal and risk management teams to create sensible corporate policies regarding BYOD, because without governance employees are out there playing fast and loose.

Nearly 25 percent of mobile workers say they employ some sort of workaround on their smartphones to bypass IT controls and get at corporate data, while 12 percent of tablet users say they use similar tactics, according to the quarterly iPass Mobile Workforce Report. What seems like an easier way to conduct business as usual for the BYOD employee is a potential catastrophe for network administrators.

"Users can unwittingly create back doors around corporate security even as they're trying to improve their productivity with applications like LogMeIn, WebEx or even Dropbox," says Stephen Pao, vice president of product management at Barracuda Networks. "The intention of using these unauthorized applications might not be malicious but can create unintended security holes."

Security software like Cisco's Unified Access BYOD solutions take policy control to the device level to try and detect threats. But even the best policy controls and network intelligence aren't going to protect against sloppy employee supervision.

"IT's best strategy to deal with the rise of BYOD is to address it with a combination of policy, software, infrastructure controls, and education in the near term, and with application management and appropriate cloud services in the longer term," says Gartner's David A. Willis, who has written extensively about BYOD security.

"Friends"

First, a bit of good news: the threat of those mobile devices containing malware is relatively small. True, there are tons of devices out of the reach of IT, but a combination of regular updates and strict controls on the part of smartphone OS providers like Apple and Google are proving pretty effective at keeping malware at bay, acting quickly to thwart threats.

But social media is another animal altogether. With the click of a "like" button, a smartphone's entire identity can be exposed to theft. Telecom networks are prime real estate for phishing attacks and attempts to access sensitive information or gain access to the network.

More people and data are traversing your network than ever before, and the opportunities for security breaches are exploding at an exponential rate.

"While it is prudent to provide some insulation against mobile malware attacks, the threats emanating from botnets, social media and unauthorized application usage are real today, and most organizations do not have the right protections in place," Pao says. "The telecom provider's own internal networks should remain free of phishing attacks that attempt to steal user credentials, or downloadable malware that can be used to leak sensitive information or create back-door access to sensitive data. With new social engineering in Web 2.0 applications, even educated internal users can be easily fooled into compromising the security of their workplaces by 'friends.'"

Application-level attacks

Distributed denial-of-service, SQL injection, cross-site scripting attacks, and other threats are increasingly targeting the application layer rather than the network layer, Pao says. "The telecom provider's own Web presence should be insulated from application-level attacks that can steal sensitive data. Moreover, all of these attacks are automated through the same botnets that used to be directed at spam proliferation."

Network administrators of all stripes should look toward implementing beefier security to deal with these emerging threats, he adds, including application firewalls to protect online apps and advanced email and Web security to protect against social-media attacks.

Fraud

According to a Communications Fraud Control Association (CFCA) estimate of global telecom fraud, losses in 2011 totaled $40.1 billion, down 33 percent from the CFCA's 2008 survey, and equivalent to 2003 numbers. (Telecom fraud losses account for approximately 1.88 percent of revenues, a 1.66 percent decrease from 2008.) But the reason for the drop isn't because more fraud is being detected and stopped — it's that global revenue growth outpaced fraud losses. In fact 89 percent of operators surveyed said fraud losses had increased or stayed the same within their companies, a 13 percent increase from 2008.

The top five fraud-loss categories reported by operators were:

- Compromised PBX/voicemail systems ($4.96 billion)
- Subscription/identity theft ($4.32 billion)
- International revenue-share fraud ($3.84 billion)
- Bypass fraud ($2.88 billion)
- Credit card fraud ($2.40 billion)

Although service providers are focused on creating value-added services, as device uptake reaches saturation it's going to become more imperative to mitigate fraud losses.

Protecting a network these days is more complicated and high stakes than it's ever been. While it used to be standard for service providers to leave security up to the individual customer, more than ever the burden is on the shoulders of the provider.

A recent report from TCS's Niche Technology Delivery Group (NTDG) suggests that companies use rigorous risk assessment, reassessment and testing to constantly monitor the latest threats and their networks' potential vulnerability to those threats. It goes on to recommend a "Defense in Depth" approach to security, with protections in place to ensure that if one layer of the network is breached the others remain secure.

"Charity begins at home," says Stephen Pao. "The CTO of the network should first ensure that his/her own internal networks and customer-facing Internet presence are secure. While news of breaches or denial-of-service attacks hit ordinary victims every day, the telecom provider is held to a higher standard."

CTIA CEO Steve Largent warned in October at MobileCON that there is widespread concern about mobile security among IT professionals.