www.pipelinepub.com
Volume 18, Issue 1

CSPs and Cybersecurity Responsibility

By: Barry Spielman

Cybersecurity threats are on the rise for businesses and individuals alike. The Colonial Pipeline ransomware attack, which struck their networks, is just one recent example of the wide-reaching effects of cyber threats. The source of the hack, which eventually led to oil shortages and increased gas prices, was the leak of a single password. Despite its large-scale impact, the Colonial Pipeline ransomware attack demonstrated that not only the largest corporations are the targets of these attacks, but smaller businesses and even individuals are also vulnerable as well. Why?

If there's one thing you can rely on regarding cybersecurity, it's that people will always be the weakest link in their own defense. Whether it's clicking a suspicious link or giving away passwords and other personal information, people are gullible. By the time a threat reaches the domain of the end user, it is often too late to stop an attack or an infection.

Another common denominator in cybersecurity is that all Internet traffic must first go through the communication service provider (CSP). Therefore, it makes sense that CSPs should protect traffic before it is routed to their customers. This leads to several reasonable questions. How does this work? What can a CSP do? Could a 'clean' Internet be the next big differentiator among providers?

There are several factors to consider when evaluating the role that a CSP should play in protecting consumers from cyberattacks. According to a recent survey conducted for Allot by Coleman Parkes Research, a total of 90 percent of consumers believe their CSP should provide security solutions. Additionally, 64 percent of fixed broadband subscribers would pay up to $5 per month for a home security solution. The demand is there, but the question is whether CSPs can meet it.

Challenges facing consumers

With some notable examples, today CSPs are largely not involved in protecting their consumer customers from cyber threats. This leaves the responsibility for protection in the hands of the end user. There are several reasons why this is not a successful solution. When it comes to securing their devices and networks, many consumers are guilty of the same crime—default passwords. Most consumers do not use new or unique passwords for their routers and other devices. In fact, experts estimate that 81 percent of data breaches are caused by poor password security.

Additionally, many are unable to determine whether their phone performance has slowed due to software or space considerations, or if their central processing unit (CPU) has been hijacked in a crypto mining or botnet attack. This begs the question: how can they be expected to protect themselves from cyberattacks? Most consumers do not have the expertise or the resources to provide their own cybersecurity protection. This is true for small businesses as well, which often do not have dedicated staff protecting their digital assets. For small businesses, the inability to protect themselves is even more critical as their business assets are more valuable than that of consumers.

Furthermore, children are increasingly vulnerable to attacks on the Internet. With the COVID-19 pandemic and remote work and school the norm, securing the home network has never been more important. When it comes to cyber defense, consumers are on their own. They desperately need the right tools in place to defend their home networks.

Growing IoT and cybersecurity gaps

If the consumer is the weakest link in the cybersecurity chain, then IoT is the weakest link in the home network. A combination of weak password policies and little to no security on smart devices make the IoT a digital doorway for cyber criminals into connected homes. The number of smart devices available is booming, with billions of connected devices in use.

However, many of these devices were developed seven to 10 years ago, and therefore often lack up-to-date security features by design. This means they're left vulnerable toattackers, who can use them to access home networks. In fact, many people aren't even aware of every insecure device in their home, from cameras and baby monitors to smart TVs and more.

What does or doesn't work?

One option to prepare for cyberattacks is cybersecurity training, but this often falls short. Training usually does not offer enough encouragement to keep people from clicking on bad links. Additionally, this training is typically available in companies with abundant resources and where awareness of cyber threats is acute. It's not usually offered to consumers outside of the workplace.

Another option that is hard to rely on is endpoint solutions. While some endpoint protection apps are a great way to limit the damage that malware and cyberattacks can unleash, they're only useful when consumers install, update, and use them properly. This generally does not happen and leaves too much room for error. Probably due to the effort involved, and sometimes the cost, mobile subscribers who are offered endpoint solutions for their devices implement them a mere 8 percent of the time. Not only does that not bode well for consumers, but it does also not represent a particularly relevant business opportunity for the CSP.

Just ask your colleagues or friends what protections they've installed on their devices against cyberattacks and the answer will most likely be "I don't know" or "none." The same is true not only for laptops, but other smart devices as well.

Why rely on CSPs?

CSPs have the power to change the state of cybersecurity for consumers and small businesses. They are well-positioned to serve as the primary protection against cybersecurity threats. They can provide protection to the end-user network, connected devices and the home or business router itself. With network-based cybersecurity services, CSPs can block malware and attacks such as phishing and ransomware attempts inside the network, long before the threats reach the customer's devices or home network.

Network-based cybersecurity services refer to software solutions that are installed in the CSP's network and provide services to the CSP's customers. Because these services are deployed from within the CSP network, the customer does not need to think about installation and maintenance. They just accept the service offering and it starts to work. This is a critical element that has been missing in consumer-oriented cybersecurity. When the customer needs to fiddle with their cybersecurity software, they tend to avoid it in most cases, rendering it less than optimally effective—and that is when they have installed it in the first place, which, as stated earlier, is extremely rare in the case of CSP-offered solutions.

In addition to cybersecurity services such as virus protection and phishing and ransomware attack mitigation, CSPs can offer parental controls, which prevent children from accessing dangerous sites and can even limit their screen time. Given that they already provide their services to home and mobile users, CSPs should find it seamless to provision zero-touch and easy-to-use cybersecurity protection.

With the sophisticated nature of today's cyber threats, CSPs should take their customers' security into consideration and be held responsible for keeping networks and their users safe. What's more, with no-hassle cybersecurity services as part of the core offering, CSPs can differentiate themselves as security providers, and even generate a fair share of additional revenue as well. When consumers have an easy way to protect themselves and all their connected devices from cyberattacks, and CSPs can provide the services that their customers want, there can be a space where everyone wins—except for the cybercriminals.