Juniper Hack: When Firewalls Fail

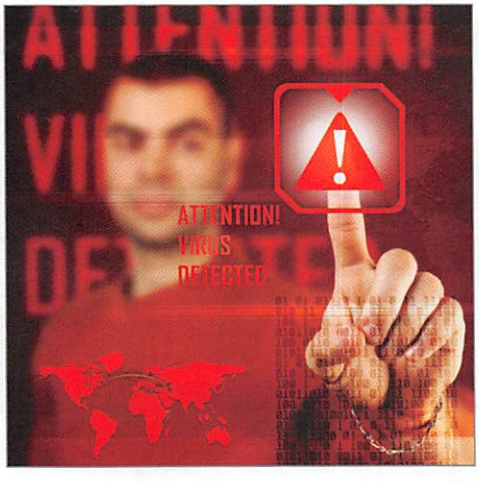
Firewalls can give a false sense of security to companies that don't have the resources to shore up their systems with more than that.

By George Baldonado

While firewalls are an important step in protecting a business's network, it's not without its flaws, and the best hackers know that. The recent Juniper hacks highlights this situation on a very public, grand scale, and underlines that most companies, corporations, and agencies don't even know that it's happening to them.

The Juniper Attack

"As evidenced by the recent attack on the Juniper products, armies of cyber hackers from all over the world are targeting the world's cyber infrastructure, military, data, intellectual property, innovations, our ideas and even our identity information. At their disposal are thousands of foreign computer 'bots' that churn out thousands of hack attempts per millisecond looking to gain a foothold anywhere they can. Sooner or later the targeted network will fold or open up. Once it folds, either the network or application will crash, or worse, the data will be compromised. This affects all companies and agencies that use, store, or access sensitive information."



says George Baldonado, president and CEO of Oasis Technology.

"Additionally, the millions of cyber hack attempts also congest the company's network bandwidth until the bandwidth is so full of hack attempts that normal business cannot be transacted," adds Baldonado. "While companies have installed a general firewall, most firewalls cannot withstand or control a barrage of attempts that number in the millions per hour. Unfortunately, most companies do not even know that this is happening" says Baldonado.

Many times companies don't think they'll get hacked because they're not big enough. Your size doesn't matter when it comes to hackers. This is an urban legend. What hackers do is look for any weak IP. This is an IP that has vulnerabilities – and hackers don't care who owns the IP address. All they care about is that they can get into the network. Many times, these hackers are like miners. Once they find a gold nugget (a weak IP address), they sell these IP addresses to big time hackers who use this information to obtain as much information from your computers as quietly as possible. It is important to note that they do not alert you because then they can come back over and over again to obtain more and more information. Once they get in, the sky's the limit.

How Do They Get Your IP?

Your last question is probably "Well then, how DO they get my IP addresses?" The answer is simple.They start out numerically from 0.0.0.1 and continue up until they find a weak IP address. While it is true that many IP addresses are not "public addresses", the hackers already know that. They just program their computers to begin at the first IP address and continue on until 255.255.255.255. At this time, mathematically, there are only about 4.2 billion combinations for the entire world, minus about a billion for "nonpublic addresses". So the hackers just let their many computers do all the work while they just wait for their computers to spit out lists of weak IP addresses. The hackers only care about weak IP addresses – they don't particularly care who you are.

Open Doors

Lastly, by design, firewalls present a logical 'door' that is intended to stop the hackers.

However, hackers have become so advanced that the firewall 'door' is not an impediment for them – rather, it's a target for them to attack and hack.

Unlike firewalls, there's technology (like Oasis Technology's Titan's architecture) that doesn't present any "door", and is invisible to the hackers. The Titan device is a stealth mode product that connects to the front of your network and stops the silent, multi-pronged cyber hacking attempts, DDOS, Heartbleed, Poodle, etc., from even getting to any firewall's 'door' and cannot be detected in the process.

"Firewalls still play an important part in what they do and are needed. But as the Juniper examples shows us, it can't be the end-all for protection," says Baldonado. ■

George Baldonado is the president and CEO of Oasis Technology. Oasis Technology is a leading provider of products and consulting services for information technology, security and network systems, serving all industries. For more information about Oasis Technology or Titan, www.oasistechnology.com.