Getty Images

SECURITY > ENDPOINT PROTECTION

5G Adoption Should Change How Organizations Approach Security

With 5G adoption, businesses will be able to power more IoT devices and perform tasks more quickly, but there will be security ramifications.

Karen D. Schwartz | Feb 08, 2020

Last year, all four wireless carriers began offering 5G, and people couldn't be happier. While some may have to wait until devices and infrastructure fully catch

communication that are up to 20 times faster than 4G LTE. 5G can reach speeds of 20GB per second, while 4G LTE maxes out at 1GB per second. While this is a nice-to-have in many situations, businesses are looking forward to 5G adoption to power more Internet of Things (IoT) devices and enable their employees to perform tasks very quickly.

"This is the first time we've had this type of functionality all at once," said Dmitry Kurbatov, chief technology officer at Positive Technologies, a security solutions provider. "LTE provided huge bandwidth, but the modems used for LTE consumed too much power to be used for more powerful IoT devices. The same is true of 2G: It provided great covering for the network and was accessible everywhere, but the connection speed wasn't good enough for a satisfactory experience."

With the increased spectrum and ability to segment networks, enterprises are likely to start using 5G more and more. Not only will it provide opportunities for coverage that WiFi may not have provided, but it could potentially replace WiFi or Bluetooth in some situations.

While all of this sounds great, it's important to stop and consider the security ramifications. Done right, 5G can actually be the most secure cellular technology to date. 5G encrypts more data, and because it's based on software and runs in the cloud, it's easier to monitor.

But it's not that simple. There is a greater risk of attacks on both IoT and mobile devices, simply because there will be so many more of them. With such fast speeds, employees are likely to choose 5G for their mobile devices instead of WiFi, and employers will use 5G for their IoT sensors.

With 5G adoption, it becomes much easier for organizations to expand their use of

CTO for Global Service Providers at Palo Alto Networks.

The same challenges will occur with mobile devices. Employees will begin bypassing the company network to connect to services and applications in the cloud simply because it's so fast and efficient.

"There is a good chance that an employee might never connect to the WiFi network, especially when they are using cloud services that don't reside behind a firewall, like Office 365," said Russ Mohr, engineering director at MobileIron. "So you have employees connecting on devices through 5G networks to services the company doesn't own anymore. That really limits a company's visibility as to what's happening on those 5G networks and with the service they are consuming."

It comes down to an erosion of the corporate perimeter. And if companies aren't aware of all devices connecting to the 5G network or what they are accessing, how can they protect those devices and their company's data?

Protecting Your Company's Data in a 5G World

The proliferation of devices and a lack of visibility are only part of the problem. In addition, there are many more small cells in 5G networks. That's because 5G has such high frequency and high bandwidth, which requires a lot of small cells. And more small cells increases the possibility of more rogue cellphone towers built by hackers. With a fake small cell tower, for example, a hacker could launch a man-in-the-middle or denial-of-service attack, find a user's location or hijack a device to steal data or run up a bill.

Another problem is a general lack of security in 5G hardware. While Huawei is a famous example—experts have discovered that the company's 5G hardware is

the U.S. for now, for example, it's being used throughout Europe because it's less expensive. That should cause concern for any company whose employees travel overseas."

Addressing 5G Security Issues Head-On

While the security challenges with 5G adoption are very real, there are steps you can take to help make your company's data and devices more secure.

The first step is making sure you know exactly what devices are connected to 5G at all times. That means being able to discover, identify and profile devices. Once you know what's connected, it's important to understand the known vulnerabilities of those particular devices, so you can adapt your security posture to accommodate them.

"When you're adding more devices that aren't managed the way old devices were, you need to have the visibility to understand them, profile them and understand their risks," Stevens explained. "Once you know that something has a new vulnerability, you can change your network security posture to protect you even before you are patched."

One way to do that is by using software that profiles devices on the network and has connections to information about known vulnerabilities to both the devices and the network. The software could then inform the company about current risks, which allows the company to adapt its security posture to accommodate the risk.

Another important step is to continually monitor your network for the unexpected. For example, if your IoT devices suddenly start behaving differently, it may be a sign of a security breach. Continually monitoring the network is the way to catch

allowing access to someone who has the right user ID and password, look at the specific device being used and apply a policy engine to that device to make sure it's trustworthy.

By examining a specific device and applying a policy engine, an organization can determine whether a mobile or IoT device has been rooted, jailbroken or tampered with in any way. It can also determine if it has the right certificate chain of trust, if it is running acceptable apps, whether it contains malware or whether there is an active attack happening on the device at that moment.

Zero trust is more important in the era of 5G than ever.

"You actually need to be able to trust whatever is connected to the network because you can't trust the network—because you don't own the network. Maybe a hacker owns that small cell or Deutsche Telekom owns it and there is Huawei equipment behind it," Mohr said. "So, you have to be sure the device is safe before we allow it to connect, and you need to do that every time. You might trust a device today but it might be hacked tomorrow, so it requires a continuous approach to security."

It comes down to this: While 5G is really just a more advanced evolution of 4G, it introduces new risks, and those risk must be addressed.

"I worry about enterprises making sure they adapt how they are thinking about security because this enabling technology is allowing them to do things they couldn't do before, and the biggest risk they face is that they don't think about it that way," said Stevens. "They just think they are adding more things and it will be fine. That's not a safe assumption. 5G will enable really interesting developments, but enterprises really need to pay attention to it and think about how they characterize their risk and adapt. If they don't think of it as something different and

0 COMMENTS

RELATED

Menlo Releases Sandboxed Approach to Data Loss Prevention

FEB 25, 2020

F5 Continues to Shape Its Future with New App Security Products

FEB 24, 2020

SPONSORED CONTENT

Ovum Report: Qualys Readies its Next-Gen Vulnerability Management Offering

FEB 18, 2020

VMware Pushes 'Intrinsic Security' at VMworld 2019 Europe

NOV 08, 2019