New Year, New Threats

With the New Year well underway the biggest threats to cyber-security have already begun to rear their ugly heads. When combined with the cybersecurity skill shortages and the growth of development that occurs every day, 2020 is going to be in truth like every other year; rife with threats, bad actors, and general nastiness. Generally speaking, it is not something any of us are really jumping for joy about, and yet these threats are sure to give way to local security heroes & inspire technological innovations that we have yet to see. The key to success this year is to stay ahead of the threat, here are a few cybersecurity threats to keep your eyes on this new year.

> *"...2020 is going to be in truth like every other year; rife with threats, bad actors, and general nastiness."*

Mobile phishing attacks:

According to mobile threat defense company, Lookout, phishing attempts that target mobile devices are expected to become more and more common in 2020, even outpacing that of traditional email attacks. This is due to the fact that while email gateways and phishing remediation platforms tend to focus solely on on-premise but often neglect the mobile aspect. Mobile devices are also prime targets due to the nature of the device, most mobile devices due to BYOD also contain not only the corporate email account of the user, but also the user's personal email, social networking, and SMS/MMS. Long gone are the days of simply guarding the perimeter of the company, it is now time to begin enabling post-perimeter security measures to protect your company and your employees.

2FA:

With 2FA being circumvented in advanced phishing attacks, it is time to start looking to multifactor authentication which will include biometrics. This goes hand in hand with helping to defeat mobile phishing attacks.

Ransomware:

Ransomware ran rampant in 2019, and the same will happen if history tells us anything in 2020. According to IBM Security's Limor Kessem organized cyberattacks will most likely start focusing on smaller ransomware attacks rather than large scale ones, due to the ability to anonymize these smaller attacks easier. This means that while the larger companies are not safe from these attacks, smaller companies are in danger more in 2020 than they were in the past.

Deepfake Technology:

While once this technology sounded like science fiction, deepfake technology is on the rise and even has been used to swindle companies already. A deepfake is a plausible video or audio impersonation of someone, powered by artificial intelligence.

In September of 2019 the first known case of deep fake scamming, used the impersonation of a chief executive's voice, to scam the company into transferring $243,000USD to the attacker's bank account. The implications of this type of attack change the way companies will conduct business, no longer is a simple phone call enough for authorization, given mobile phishing, and now deep fakes, even video conference technology may not be enough to those who are less vigilant.

IoT Based Attacks:

The number of smart devices is on the rise, and as we have previously discussed at SecureNation, IoT devices do not always have the strongest security protocols. Expect in 2020 for there to be a rise in IoT attacks, doubling from 2019.

While these new (and old) threats may threaten all infrastructures throughout the world, hope is not lost. With vigilance, the right tools, and skills 2020 can be a year of celebration rather than that of breaches and fear. SecureNation can help by bringing a company the right tools to help defend against these threats.

> *With vigilance, the right tools, and skills 2020 can be a year of celebration rather than that of breaches and fear.*

References

https://blog.lookout.com/five-ways-security-landscape-will-shift-2020