Predictions in Cyber

Bradley Harper

Cookeville, TN

[brharper42@tntech.edu](mailto:brharper42@tntech.edu)

The year 2020 was heavily controlled by COVID-19 driving the majority of the available workforce to move online. Due in-part to the rapid shift to an online presence, many did not take the proper precautions in doing such. Some sought only to be able to continue to be employed while others took a malicious approach to the situation. According to [1], “a recent report from PwC found that cyber security is more business critical than ever before”. [1] continues by stating that PwC found, “that 96% of executives have shifted their cyber security strategy due to Covid-19 and 40% of executives say they are accelerating digitisation. Around 55% of enterprise executives plan to increase their cyber security budgets in 2021 and 51% are adding full-time cyber staff in 2021. PwC found that most executives are planning to ramp up their cybersecurity spending in 2021 despite the majority of them, 64%, expecting business revenues to decline”. The pandemic has led to a spike in cybersecurity needs in such a short period of time. Contrary to what would be expected though, PwC also expects that a quarter of organizations actually intend to slash their cyber budgets in the year 2021. With the age of electronics on the rise, it is unlikely this would be a good idea for those organizations as cybercrime morphs and changes often. Moving forward, many are expecting to continue to work remotely significantly more than they used to. In doing so, security teams will need to remain vigilant in the near future for the unknowing nature of those partaking in such remote connections. Another prediction would be that of a Zero Trust policy which would make “access to networks, applications and data be as limited as possible, so expect zero trust capabilities to begin to show up in every kind of access product”. This would make a dent in the case of stolen credentials and reduce the need for VPNs. Unfortunately Zero Trust policies can be thought of like a pirate ship riddled with cannon holes. Weaknesses will still be taken advantage of and then water will sink the ship along with the crew. The next prediction deals with the cloud and its misconfigurations stating, “the explosion in remote work led to acceleration in digital business transformation and application migrations to the cloud”. [1] continues by mentioning “along with that rush will come the inevitable cloud bucket misconfigurations and security breaches”. The company CompariTech estimated approximately six percent of Google Cloud buckets are at risk due to misconfiguration. 2021 should also expect a storm of ransomware as it continues to grow each year. “Sophos predicts that the big ransomware families will become ‘more evasive and nation-state-like in sophistication,’ targeting larger companies with multimillion-dollar ransom demands, and ransomware-as-a-service will continue to let smaller players wreak havoc with everyone else,” says [1]. Some of the names that should be expected are Ryuk, RagnarLocker, Netwalker, REvil, Egregor/Maze, Dharma and Buer Loader. Although a name or a threat may be heard and reported in the news, the ones that cause the most damage are the ones that everyone already knows about. Commodity Malware will grow with things such as loaders and botnets which can harm more than might appear.

Works Cited

[1] Cyber Security In 2021 2020 digital transformation Predictions Coronavirues covid-19 Trends. [Online]. Available: https://www.cybersecurityintelligence.com/blog/cyber-security-in-2021---predictions-and-trends-5386.html. [Accessed: 28-Jan-2021].