Date: 2/21/2021

To: CISO for the ITN 295 Gateways to Dark Web

From: Afeefah Manzoor

Subject: Cyber Security Summit- San Diego

The focus of the Cyber Security Summit that was hosted in San Diego was the how our security has been compromised by being thrusted home to work from the pandemic without much of a security plan put in place and how much vulnerable we have become.

Since everyone has been thrusted home to work over remote from the COVID-19 pandemic, many companies are facing many security issues and an increase in not being able to thwart attacks. Over the past year, companies have noticed that there has been an increase in social engineering attacks and ransomware attacks by sixty-four percent. Personal identifying information also has seen to be taken over and sold on the dark web as increased 429% since March 2020, when everyone has been pushed to work from home on less secure networks and security practices, such as a 234% increase of users connecting to public and unsecure networks. In the San Diego area alone, the FBI alone deals with more than ten cases a week.

We are living in a post-compromised society where an unauthorized user will inevitably be in a network. The real question we must look at is how we can mitigate this unauthorized. The main issue for security professional is to figure out what exactly is malicious traffic since all traffic, including malicious traffic is encrypted, the question remains is how do security professionals figure this out. Many unauthorized users are in the network before any malicious activity is done, and in the instance of a ransomware attack, the unauthorized user will steal the information to extort if the ransom is not paid or sometimes even if the ransom is paid, this is known ad double extortion. Some other faults that have occurred due to nearly the whole workforce to being forced to work from home to help combat the pandemic are that security patches are taking much longer to be deployed, forty days longer.

Security professionals have figured out several ways to workout the issues that have arised from working from home. The first thing that can be done is to monitor all end-points. Another way that security will change with the new normal that has occurred, has caused legacy tools to miss novel threats by asking the wrong questions, but this can be fixed is by using AI (Artificial Intelligence) to understand the companies’ online immune system and what it means to be apart of this ecosystem. The use of AI will help security professionals since AI in-itself learns the environment and will understand what is normal and can easily flag anything that looks out of place, much easier than it being done manually. Some other recommendations include establishing a Remote Workforce Agreement. With this agreement, it will go over privacy rights, and lets employers be transparent with their employees to let them know what the monitoring software does. Other things that can be done to help create a security team is to establish a monitoring, detections and response program, to develop and implement response Service Level Agreements that are tailor specifically to high level assets, aim to for less than ten-percent false positives, as well as perform at least two cyber exercises per year- one being a tactile exercise and the other an executive, table-top exercise.

Overall the San Diego Cyber Security Summit covered how vulnerable companies and users are by being thrusted into working remote without much preparations and ways security professionals have tried to overcome these challenges.