Cybersecurity Challenges and Solutions during Covid Pandemic

Big Data Trunk

Introduction

While the rest of the world was fighting a battle against the dreadful coronavirus, there were some people who were celebrating at that time. Yes you read it right, as many businesses had come online to keep up the work flow it opened many doors for cyber criminals to make billions of dollars.

Work from Home was a blessing in disguise for both employees and employers, but at the same time many of them became victims of cybercrimes.

In February 2020 Amazon web services had experienced and mitigated 2.3Tbps DDoS attack, which had a pocket forwarding rate of 293.1Mpps and request rate per second of 694,201. It was one of the largest DDoS attacks in history.

In July 2020 Twitter was breached by a group of 3 attackers, who took over twitter accounts of famous people like Barack Obama, Elon musk, and Jeff Bezos. These attackers used these stolen accounts to post about bitcoin scams and earned more than $10,000.

Since the Covid 19 pandemic, cyber security has become like a game of famous Disney characters Tom and Jerry between cyber attackers and defenders. No matter how smartly defenders create the solution for identifying and blocking the various techniques, the cyber attackers will come with stronger techniques.

Businesses are facing Cyber Security challenges while using the following devices/services:

Using personal devices

Many small and medium-scale industries allow employees to use their own laptops for professional work. While working from personal devices and with home WI-FI, users are more prone to cyber-attacks, as these devices might not use antivirus or anti-malware scans regularly. Moreover, the home working environment doesn't have sophisticated enterprise-level cyber threat detection and prevention measures.

Using cell phones

Cell phones today are as smart as computers and laptops, that's why many people prefer to work on mobile. Problem with using mobile phones for work is that many people may have installed malicious apps unknowingly, so when they use their phones to save their work related data, it's dreadful for the organization's cyber security they are working for.

Using various video conferencing apps

During pandemic video conferencing was an effective way of connecting with peers and also for joining online courses. But have you ever thought that using these apps costs your personal information! Hackers steal your name, email address and password by attacking these video conference apps.

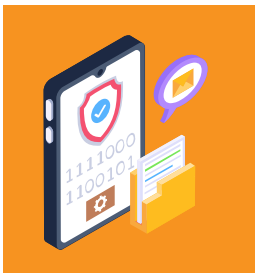
They also use credential stuffing techniques where hackers used the previously stolen names and passwords to gain access to other accounts.

Through various apps and websites

During Covid 19 many daily wage earners lost their source of daily income and were in a pathetic situation. Hackers took advantage of even this situation and made fake websites and solicited donations through email links.

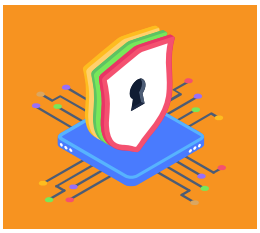
At that time people were so anxious that they used to check the count of infected people and areas every now and then on apps and websites. These apps and websites were also laden with virus and identity theft malware

Solution



Antivirus Protection

While allowing employees to work on their personal device, employers should confirm with the antivirus protection in their devices. If their devices are not equipped with this protection then, they should provide their employees license for antivirus and malware detection software.

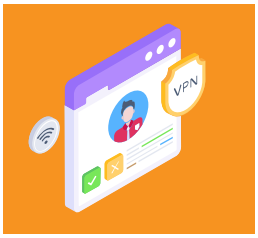


Cyber security awareness

Staff should be educated about the best practices and procedures to follow while sending important email or other content to private email addresses.

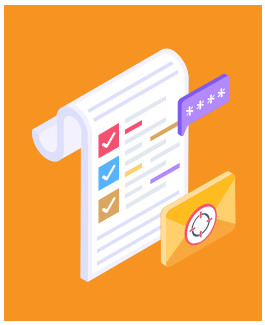
Phishing awareness

Employees should be alert and attentive while receiving emails and should check the authenticity of the mail address of the sender.



Use VPN and secured home network

Using virtual private networks can add another layer of protection to your internet while working from home. You should also have a strong Wi-Fi password and you should change it frequently.



Frequent reviews and identification of weak spots

Companies should keep on checking whether existing controls are robust enough, and should be prepared with solutions for the latest kind of cyber-attack. Along with reviews, companies should also run tests to identify loopholes in the system and work to mend it as soon as possible.

Apply new technology

Cloud based services and platforms are effective and easy to deploy and adopt. They help companies to increase the depth and breadth of their protection rapidly. Security edge, cloud based data leakage prevention and threat protection controls can help safeguard an organization’s critical assets.

Risk management

Business should apply Governance, Risk and Compliance (GRC) solutions for improved risk solutions. It provides a detailed view of a company's risk exposure and helps link together the various risk disciplines.

Prepare for attacks

In this high risk time companies should carry out cyber crisis simulation process to prepare their response to cyber-attacks

Conclusion

Cybercrime is a huge threat for businesses that are trying hard to survive in this testing time of Covid pandemic . But with the right measures and timely actions companies can conquer these hurdles.

Big Data Trunk

Learn more about Big Data Trunk Courses & Training

www.bigdatatrunk.com

training@bigdatatrunk.com

+1-415-484-6702