PODCAST EPISODE: CYBERSECURITY THREATS YOU MUST BE AWARE OF IN THE HYBRID WORKPLACE

TJ: Hi, I'm TJ. In this episode, we'll be focusing on the issue of cybersecurity in the emerging hybrid work environment, the kind of threats you should be aware of during the transition, and some best practices to safeguard your enterprise's future.

<Guest Intro, Welcome and Thanks you's>

TJ: A major consequence of the COVID-19 pandemic is the altered debate around remote working. The pandemic demystified the remote working model which resulted in many organizations looking for a hybrid model that combines remote working as well as the occasional trip to the office.

The pandemic also played a key role in forcing businesses to migrate their business applications and infrastructure to the cloud for building digital resilience within the enterprise. While technology adoption has been a boon, data touchpoints are now more spread out than before. This has unintentionally increased possibilities of cyberattacks and misuse of security gaps by hackers.

This shift to work from home and hybrid work poses certain security risks for both employees and the organizations. According to you, **is remote working one of the greater cyber security challenges facing our IT leaders today?**

Guest: Absolutely, the hybrid workplace offers a great challenge for IT leaders who will now have to simultaneously manage and mitigate network security risks that occur both in and out of the office. At the same time, they must provide a seamless experience that enables employees to work from anywhere. Businesses should look into investing in security solutions that provide greater visibility into employee behaviors and reduce complexity. They must educate employees about threats to prevent security incidents before they happen.

TJ: You mention educating employees for the purpose of threat prevention. How important of a role you think will be played by the workforce in this new age of workplace cyber security?

Guest: ESET, a global leader in cybersecurity research, from earlier this year found that 80% of global businesses are confident their home-working employees have the knowledge and technology needed to handle cyber threats. However, in the same study, three-quarters (73%) admitted they are likely to be impacted by a cybersecurity incident, and half said they'd already been breached in the past. This kind of disconnect does not make for coherent cybersecurity planning and as you know, threats often thrive in the absence of strategic decision making and preparation.

TJ: Yes, couldn't have said it any better myself.

Guest: Ask any cybersecurity professional and they'll probably tell you that the weakest link in the corporate security chain is the employee. That's why we saw phishing campaigns repurposed en masse during the early days of the pandemic to lure users desperate for the latest news about the crisis. In April 2020, Google claimed to be blocking over 240 million COVID-themed spam messages each day, and 18 million malware and phishing emails.

Home workers are more exposed because they may be distracted by housemates or family members, and therefore more likely to mistakenly click on malicious links. Contacting IT support or even getting a colleague to sanity-check a suspicious email is much harder when working remotely, while personal laptops and home networks may also offer fewer protections from malware. There are considerable things to worry about when it comes to employee habits in the realm of cybersecurity in this time of remote working.

TJ: Clearly that's a sign of impending trouble if not addressed in time. But it's not just the employees, it seems the cyber threats itself are also evolving with the advent of remote and hybrid working.

Guest: That is correct. The security threat landscape is becoming more dynamic– a recent McAfee Labs COVID-19 threat report noted that threats targeting cloud services have increased by 630%. Organizations must cope with the fact that the employees need to access and communicate data beyond the periphery of the usual security firewalls. As I just mentioned, most of the rise in the attacks were from phishing campaigns. Specifically, along with an increase in ransomware, attacks deployed via phishing emails, the rise in vishing (voice spear phishing) attacks was also noticed. An interesting point to note, the 2020 Verizon Business Data Breach Investigations Report identified that 22% of all breaches were caused by human error and ignorance. More often than not, we seem to be going back to human considerations and much as the technical ones in this security narrative.

TJ: So, there are obviously a few potential problems an organization needs to keep in mind. What are some of the major threats, you believe, an enterprise needs to plan for while actually transitioning to a hybrid workplace?

Guest: During this remote or hybrid transition, some companies may face operational risks of not being able to support a large number of simultaneous Virtual Proxy Network (VPN) connections to their infrastructure and services. This can result in inconvenience for employees who require access to resources. This may even cause further strain on IT teams, if they're not prepared for this. Bumping up the number of simultaneous VPN connections to accommodate all remote employees should be first on the security best practices list.

Some organizations have a policy for centrally managing and deploying software and security updates to end points. Delivering them all at once to VPN-connected employees could create bandwidth congestion and affect inbound and outbound traffic. Gradual rollout procedures must be devised for deploying those updates.

There is a risk of improperly implementing access and authentication policies, which will result in employees accessing unauthorized resources. There is the possibility of sensitive data ending up in shadow IT– solutions or devices that are not approved by companies and are difficult for IT teams to track and manage, let alone ensure the security firewalls. This is a consequence of bad employee habits developing in the work-from-home time period. Many remote workers are likely to be accessing company servers or cloud accounts over public networks and the use of domestic IoT devices such as printers, cameras and TVs using default settings, creating further vulnerabilities.

TJ: With these numerous threats in mind, how can organizations address the cyber security issues arising out of the transition?

Guest: The most dangerous threats are not the ones that have been previously detected, but the ones that are yet to be discovered. Hybrid working still needs further deciphering and therefore, an evolving strategy around its various aspects, including security. Businesses should break down barriers, whether institutional or resource-wise, that hinder possible advantages of utilizing the latest in cyber threat protection; these advancements include technologies such as big data and predictive AI.

Organizations must consider security solutions that provide advanced web security protection across end points and technologies preventing exploitation of network vulnerabilities. Strong anti-phishing

and network-attack defence technologies that can accurately detect and block such threats from preying on employees are a must.

Most importantly, we must acknowledge that it's going to be increasingly difficult to keep a check on remotely-working staff behaviour. It's inevitable that employees are enabled to meet the challenges of their new environment and act as the first line of defence. The good news is that, while securing the new hybrid workplace will be challenging, there are best practices that can guide CIOs. The **Zero Trust model** is gaining in popularity as a way to manage the complexity of on-premises and remote, cloud-based workers and systems. Led by internal deployments at Google, Microsoft and other tech pioneers, it's based around the premise that the old notion of corporate perimeter security is now defunct.

TJ: I think we should elaborate a little bit on this 'Zero Trust' concept.

Guest: Today, devices and users within the corporate network are no longer to be blindly trusted. Instead, they must be dynamically and continuously authenticated, with access restricted according to "least privilege" principles and network segmentation put in place to further limit potentially malicious activity. Adopting a zero-trust approach assumes the possibilities of attacks from inside and outside the organization. This requires any attempt to access data or internal infrastructure with unsanctioned tools to be treated as a network security risk and be authenticated. By reducing the amount of data; each employee can access and keep information on a need-to-know basis; hence the likelihood of phishing attacks is lowered.

It will require multiple technologies to work effectively, from multi-factor authentication (MFA) and end-to-end encryption, to network detection and response, micro-segmentation and more.

TJ: There is a lot to digest from all that we've discussed with regards to the changing landscape of enterprise cybersecurity. I believe our listeners will really appreciate everything that you've told us in this episode. It was a pleasure to have you and hopefully the future will see improved business practices in terms of protecting the employees and their data from potential cyber threats.

Guest: Thank you.