Keeping Your Remote Workforce Safe and Secure This Summer

We are in an increasingly mobile-first and distributed world. Remote networks and mobile users are the new reality, and they all require access to business-critical applications, which used to be located safely behind the corporate firewall. Today, users, networks and applications can – and should— exist everywhere, which puts new burdens on security teams to protect them in the same way as the traditional perimeter. With the summer travel season upon us, it is a good time to review cybersecurity best practices when it comes to remote connections to an organization's core network.

For users and security teams alike, the cardinal rule is that all traffic connecting to the network must have the same security controls and policy applied, regardless of user location. There should be no deviations or exceptions made to accommodate remote users; cybersecurity must be consistent if it's to be effective.

In the past, organizations supported various remote access strategies to enable remote users, generally backhauling traffic to the corporate network or using multiple point products. These approaches are difficult to manage, costly and inconsistent when it comes to security policy and protection. In the interest of timeliness or efficiency, employees would often bypass normal security protocols to access network resources, particularly when on vacation and trying to quickly get work done so they can get back to their R&R. An understandable behaviour in the heat of the moment, but one that could open the door for attackers to infiltrate the network.

As we know, the threat landscape continues to evolve, with new techniques and toolkits available for nearly every threat use-case, including the targeting of remote and mobile users. In an environment where infecting these users is easier, organizations need to adopt security practices that are equally easy to use, an extension of the protections they already deliver, and include a seamless user-experience that does not impede their work.

So, for IT security teams expecting a spike in remote network connections thanks to summer travel, I'd like to offer the following advice.

- If you're using separate security protection for remote networks, mobile users and your local networks, you must revaluate your strategy. You're putting a heavier burden on security and operations staff, increasing cost, and potentially opening seams in your protection that attackers can leverage.

- Consider implementing a cloud-based approach to security for remote networks and users that extends your local policies consistently. The approach should be simple for the user and provide access to all the applications they need to incentivize use.

- Personal mobile devices are a prime target for cyber attackers because they are so prevalent and can be less secure than devices issued by an employer. Make sure employees are aware that the loss or theft of a personal device, even if not used for work purposes, can provide personal data that cyber attackers can use to gain improper access to IT assets.

That said, cybersecurity cannot be the sole responsibility of the IT team; users have a role to play as well. In addition to following the cybersecurity processes your security team has put in place for remote users, here are some additional best practices to share with employees who will be travelling this summer.

- Tourists are tempting targets for thieves looking to steal smartphones, laptops and tablets. If your mobile device is stolen or even out of your possession briefly, don’t forget to notify your IT department in addition to your service provider. Many IT departments can remotely wipe sensitive corporate data from a device without effecting personal data.

- Before you travel, make sure to update your mobile devices with the latest security patches and software updates for its operating system and applications.

- Users should install password managers to keep credentials secure on their mobile devices.

- Avoid using public Wi-Fi networks or workstations in Internet cafés or hotel business centres. If you must use public Wi-Fi, be sure to log out of any SaaS applications or web sites you used and clear the browser’s cache before you end your online session. As soon as possible, change your log-in credentials for any SaaS applications or other network assets you accessed while using the public network or workstation.