How To Secure Your Hybrid Work Environment

As organisations move away from full remote working environments, we are all preparing for the next big shift – hybrid work. With the introduction of permanent hybrid work environments, where some users are operating remotely and others are in offices, organisations will be faced with new security challenges. Security has never been more important, as we operate in the most complex cybersecurity landscape we’ve ever seen. Tech giants like Microsoft are urging organisations to adopt a Zero Trust approach, where a network can check automatically for abnormal behaviour, such as a user logging into an account one day on a different type of machine, or a connection coming from an unexpected location. As many IT professionals know, these changes open up the opportunity for risks. As employers adopt this new change to a hybrid work environment, there are some critical security considerations your organisation needs to explore.

**Adopting a Zero Trust Strategy**

In the new hybrid world where identity and device management is critical, adopting a Zero Trust strategy is no longer an option, but is a business imperative. With Zero Trust, you assume breach and provide the least privileged access necessary, supporting the maintenance of security amid the IT complexities that come with hybrid work environment. Considering how complex hybrid working can be, the adoption of a Zero Trust strategy won’t happen overnight, and so it’s important to map out your path to Zero Trust, manage your progress and most importantly encourage your users to embrace the new measures that will be introduced as part of Zero Trust security.

**Start With Identity**

Through recent attacks, a clear theme has emerged – that identity will be central to attacks of the future. Weak passwords and phishing are entry points for the majority of attacks, and are most times the easiest areas of our security set-up to improve. The introduction of simple tools like Multi Factor Authentication (MFA), can significantly improve your security posture. MFA not only protects your individual devices but the entire network. If you are already a Microsoft customer, with Azure or Microsoft 365, you can activate MFA across your IT estate at no additional cost. Implementing MFA, for organisations of all shapes and sizes, can be seamless once you prepare your users through an MFA adoption plan.

**Grant Least Privileged Access**

The concept of least privileged access is not a new one, but is something that we rarely see implemented effectively, as in the past organisations have favoured convenience over security posture. Least Privileged Access ensures that users only what access to applications, systems and data that are required for them to fulfil their roles. Now, with the introduction hybrid work environments, organisations are faced with new challenges in protecting their data, with the growth of personal device use and remote working. This new normal has presented us with enormous cybersecurity risks and challenges, but least privileged access can offer a piece of mind by preventing any weaknesses from being exploited.

**Device Management Is More Important Than Ever Before**

The arrival of COVID-19 has resulted in an increase of individuals using their own devices for work, and now in a hybrid work environment, companies need to restructure their Bring Your Own Device (BYOD) practices and policies. Many organisations are considering treating all devices as if they are mobile, whether they are intended to be used in the office or not, which will result in them having to process all devices through solutions like mobile device management and MFA. Additionally, it will be critical that organisations ensure any personal or BYOD devices are kept up-to-date with security and operating system updates, the same way on-premise devices are.

**Make Security Everyone’s Job**

The way we work has changed, and so too have the security risks that we are faced with. With people working from home, faced with new risks and challenges, organisations must prioritise security training for all users to avoid the now popular phishing and social-engineering attacks. Topical phishing messages on vaccine updates or COVID Corporate Guidelines are increasing and proving to be successful, so it is important that your users are trained and prepared to better protect your organisation.

**What’s Next**

COVID-19 has changed the way we live and work, presenting new challenges in cybersecurity for organisations around the world. At Nostra, it is our job to help people and organisations to feel safe and protect their businesses from any cyber criminals looking to take advantage on the shift to hybrid working. If you are interested in discussing how Nostra can help safeguard your organisation from even the most sophisticated threats, please contact our expert team at <https://nostra.ie/contact/>