TECHNATIVE

wavex
EXPERIENCE EXCELLENCE

The Role of IT in Remote Working

on SEPTEMBER 25, 2017 ◦ ENTERPRISE

Remote working used to be limited to simply taking your documents in a briefcase home with you to review in the evening, writes Gavin Russell, CEO of Wavex

As communication infrastructure has improved (with the amount of homes with superfast broadband connections topping 10.8 million last year), workers now desire an almost identical experience at home to working in the office.

This year is thought to be something of a tipping point when it comes to remote working, with more than half of businesses in the UK now offering remote working policies. It is a trend that is likely to continue too, as the same research by the Work Foundation at Lancaster University, predicts that by 2020 some 70 percent of organisations will have followed suit.

The popularity from both a business and worker perspective is not hard to see. For businesses, allowing home working can reduce bricks and mortar expenditure considerably, as less office space is required. From a worker's point of view, they're able to save money by reducing their commute, and able to work in a comfortable environment with less distractions.

Proceed with caution

However, it's not simply a case of allowing any employee with a laptop, internet connection and desire to work in their pyjamas the option to work from home. You need to proceed with caution. Before this option is offered, there needs to be a certain amount of technology investment undertaken to ensure that they, and your business, are safe from the latest wave of cyber security threats.

To do this needs a range of technologies working seamlessly together to provide secure access while not impacting end user experience. The best form of authentication is currently two factor; which your users will be used to from when they bank online. It ensures that access is only provided when a user meets two separate authentication criteria, often a password and a unique, temporary code provided to their mobile handset via SMS.

Once your employee is connected, the data between their device (which could be anything from a traditional PC to a tablet or mobile phone) and your organisation's servers must be encrypted. As older cryptography techniques have become easier to hack, connections should now be secured using IPSEC with DES or 3DES. This means should a hacker be able to intercept your data, it should be unintelligible.

While simple passwords to crack – such as 123456 or password1 – are never recommended, the advice around passwords has somewhat evolved. The National Institute of Standards and Technology now recommends focusing on usability and practicality as opposed to an overly complex password that your staff will only have to write down in order to remember it!

Accessing data

The technologies used by remote workers to access the information they need to undertake their day-to-day operations from home has needed to evolve. Simply allowing your staff to access the file repositories on your network from home as they would in the office, could leave you open to being infected should their laptop or home PC be carrying a virus. It is just not practical to rely on the IT department to secure the myriad of bring your own device (BYoD) personal end-points that remote workers use, therefore, other solutions have become necessary.

Many organisations have started providing specific remote desktop solutions via the cloud. These send a live snapshot of your office desktop to a remote device. If a user clicks or types, these interactions are reflected on the server. This means no applications need to be installed on the remote device and it provides a barrier for viruses to traverse from the remote workers device back into the corporate network. However, if the user is offline or their connection drops it means they can't work.

The third, and often better, solution is to provide access to all files via a web server through a browser. This will generally use the SSL (Secure Sockets Layer) protocol to establish an encrypted link. Because so many devices now support web browsing, this provides many more ways to work remotely.

The new 9-to-5

With the advancements of technology and the push for the ability to work remotely coming from both sides, the traditional work and life balance is becoming increasingly blended. Work emails can be sent straight to mobile devices, work can be completed anywhere thanks to laptops, and the days of a simple 9-to-5 existence are but a distant memory.

Seeking the right balance between usability and security remains a great challenge though. Mobile Device Management (MDM) technology has become a critical way for IT departments to manage all the additional endpoints brought on by the remote working trend, and provides a means to instruct devices to delete any sensitive data should the device be compromised.

Link to the original article:
https://www.technative.io/the-role-of-it-in-remote-working/