Security Begins at Home
By Mike Sheward

As I glance around my living room, I can't help but notice the number of devices in my field of vision that have an IP address. I see a couple of laptops, a smart TV, my DVR, a games console, security camera system and a couple of smartphones. That'll be 8 IP connected devices without turning my head a single degree.

I consider my set up to be fairly typical; I can guarantee that there are plenty of homes out there with so many more devices floating about the place.

The rapid growth of the number of IP connected devices has pushed technologies that only a few years ago resided exclusively in the realm of the office IT department.

Consumers can take home the power of packet filtering firewalls, access control lists, port forwarding, advanced routing and wireless encryption – all for about 70 quid.

However, as we can all attest, having all of these tools in the box and knowing exactly what they can do are two very different things. Anyone who has given a child a toy on Christmas day that requires some sort of construction, or installation of randomly shaped, impossible to find batteries, will know that the finer details are frequently glazed over in favour of getting the thing working as fast as possible.

The same is true of home IT and networking equipment. Get it operational, so that everyone at home can use it, and then go back to relaxing.

It used to be the case that what happens at home stays at home. However, in today's world, the home is an extension of the workplace. The work computer goes from the home network, to the work network and back again. Often, the work computer will stay in the office, and only the 'work' will go backwards and forwards. Documents and spreadsheets sent out of the relative safety of the corporate email system, to personal email addresses where the contents can be harvested for sidebar advert material, and other much worse things.

The lines between home and work are blurred. If your company loses data as a result of a breach originating in an employees home network or equipment, it is still your organisations data. It is your organisation that will feel the pain.

Now, you can't very well go around and knock on all your employees' front doors and say 'Hi, I need to sweep your network, it's basically an extension of the office'. Some may not like this; it may be considered an invasion of privacy.

What you can do as a business, is offer basic security advice to employees that will reduce the risk a home breach becoming an office breach.

Provide Wireless Security Advice

The single biggest weakness in home networks is poorly configured wireless encryption. It takes about 10 minutes to remind employees of the need to ensure they are running WPA2 encryption with a complex password.

Provide Antivirus Software

An increasingly common strategy is to offer antivirus software for free or at a reduced cost to employees for home use. That way you can guarantee they aren't going to fall for a fake AV scam, and they are running something half decent.

Host a Mobile Device Security Drop In

It takes about 5 minutes to look at someone's mobile device and determine if it is appropriately protected with a passcode and automatic lockout. A drop in session once a month for employees will help build relationships between the IT/security team and the employee and is a non-intrusive way to help enforce mobile device policies are personal devices.

Encourage Secure Use of Social Networks

Content spread over social networks can either be mildly embarrassing or down right destructive. Provide advice to employees on how to restrict access to social networking profiles, and encourage them to pass on the lessons to their immediate families. Little Timmy's relentless installation of apps on a machine Dad uses to manage payroll is a situation we'd all like to avoid.

Make Consumer Device Security News Accessible

Not everyone knows where to look for security news, and to be honest; most people outside of the 'biz' will never visit a security news site. The occasional cyber security story may go mainstream if the impact is big enough. As an organisation, you should do what you can to inform employees of security problems with consumer devices, which may impact them.

A good example of this is advising employees when a bug is discovered in a consumer grade router that requires a firmware upgrade to fix.

Conclusion

These ideas are designed to be powerful enough to have a positive impact on security at home, which will spill over into the work environment. While at the same time being lightweight enough to maintain with little overhead or intrusion into an employees private space.

And for those who say that they do not permit employees to work at home – if someone needs to work, they will work, and they will use the tools they have available to complete that work. If that means grabbing the nearest computer to send an email, or work on a document, chances are they'll do it. It's human nature to want to get the task done with the least resistance.

Talk to your employees; ask them how they use home technologies to do work, and build controls and programs that help them understand the responsibility of ensuring that information security begins at home.