MFD SECURITY ISN'T JUST ENCRYPTION AND OVERWRITES

INSIGHTS

transcend360

Securing the office print devices (MFDs and printers) is more than just encrypted hard disks and data overwrite. I know many suppliers promote security and the risks associated with printers and MFDs but do end customers really understand the potential risks or do they just see it as a sales tactic to sell the latest most secure device?

Whenever we talk to customers about securing their print devices the starting point is not to look at the printer or MFD but to look at the main end user devices the customer has i.e. laptops, tablets and desktops. We ask the customer what they perceive as the risks and how they secure their laptops and desktops. We then move onto understanding how they secure their servers and network.

This approach gives us two important insights about the customer:

Firstly, if they are not securing these assets they are unlikely to want to secure their MFDs!

Secondly, if they are securing them, then the methods deployed to secure the MFDs should be exactly the same. The reason; because an MFD is an end user device, it can act as a server and it connects to the network. It isn't just a dumb peripheral any more.

So what areas need to be considered?

Device Identity

How do you know the device on the network is the device you thought was on the network? Many organisations deploy certificates to authenticate desktops and laptops, why should printers be different? This can also help you control MFDs being added to the network.

Device Integrity

How do you know the device is running firmware and software that is approved and tested? Malicious software on your MFDs can capture crucial information or act as a gateway to the network. You probably have policies and tools to ensure that laptops and desktops are running on approved versions of OS's and applications, why not do the same for the MFD?

Device Configuration

The biggest single risk with MFDs is that by default they are shipped with all network protocols, services and ports open, active and ready for service. You have to shut stuff down that you don't want, not open it up. Would you allow laptops and desktops to run FTP, Telnet and RSH services? Agree on and deploy a standard configuration.

Data in Transit

Data has to get to and from the MFD; this can include print jobs, configuration data, monitoring information and user information. This information is a critical asset to the organisation. If you protect it when transferring it between servers and desktops/laptops, then protect it when sending it to the MFD.

Data at Rest

Here we go; now we are looking at encryption and overwrite. If you encrypt laptop/desktop hard disks then why not do the same for your MFDs? This is one of the easiest areas to deal with, just turn encryption and overwrite on.

Access Control – authentication and authorisation

Users have to log into their laptop/desktop don't they (please say yes)? So why not the same for the MFD? Users are only authorised to perform specific functions on their laptop/desktop, for example they don't have admin rights (normally!), they can't change settings, load software etc. Controlling access to admin functions on the MFD is an absolute must, but how many organisations don't change default admin passwords (I can see a few red faces)?

Audit

Every desktop/laptop has an event/audit log; and so does every MFD. Probably like the audit log on every laptop/desktop, no one checks the audit log on the MFD! MFDs can also link into your SIEM (see Google).

Certification

How many times have organisations asked me about ISO15408 or common criteria certification and had no understanding of what they are asking for? For certification you need a benchmark and the de facto benchmark is IEEE P2600.

In summary

The key take away from this article is that organisations must treat their MFDs (and printers) as both an End User Device i.e. laptop/desktop and as a Server. Protect it in the same way, with the same approach, the same tools and the same techniques. Don't leave MFDs open as they really are a risk (and that is not just a scare story from a supplier trying to get you to buy their new devices).

About transcend360

transcend360 provide independent and unbiased consultancy specialising in Managed Print Services (MPS). We provide services that support end user customers in the definition, procurement, delivery and management of an MPS, providing support throughout the complete contract lifecycle.

www.transcend360.co.uk

info@transcend360.co.uk