SOLVING IT TOGETHER

PRINTER SECURITY BREACHES

THE RISK IS REAL. AND IT'S GROWING.

It seems we hear of a major security breach almost on a weekly basis. Each time this occurs, it's an opportunity to learn valuable lessons about how to prevent similar losses in the future. Companies and their IT staff are becoming increasingly aware of this vulnerability.

PRINTERS USED TO SEND BOMB THREATS.

Printers and fax machines were hacked in several major universities and businesses across the United States and used to deliver bomb threats. The institutions received printed documents, faxes, and emails demanding a $25,000 ransom. Although authorities determined the messages a hoax, they struggled to determine how hackers gained network access.

MFP USED TO PENETRATE SECURE NETWORKS.

During an internal network penetration test, a security firm was able to utilise a printer's TCP/IP port to gain access to secure network segments otherwise locked out by Access Control Lists. The port was connected on the local switch that was left openly configured to be able to access all network VLANs and subnets.

Telephone: **0113 276 0210** | Email: **MPSteam@dtpgroup.co.uk** | Web: **www.dtpgroup.co.uk**

UNIVERSITY NETWORK WEAKNESSES.

An investigation into a large university found weaknesses that made its networks vulnerable. Printers accessible to anyone on the network were used to print sensitive medical documents - including organ donation logs, surgery fact sheets, prescriptions and medical records. University networks can be especially challenging to secure, since they are often open, decentralised, and permissive.

PEWDIEPIE PROPAGANDA

In a heated battle between PewDiePie and T-Series to claim the most viewers on YouTube, a PewDiePie fan exploited printers to drum up support. Nearly 50,000 internet-connected printers were accessed via open network ports which were then used to spit out flyers encouraging people to subscribe to PewDiePie. The letter also read: "Protip: Your printer is exposed to the internet. Please fix that."The prank was repeated two weeks later by different hackers, hitting more than 100,000 printers. They also implored users to secure their printers.

NORWAY PARLIAMENT

After alleged Russian interference at the Storting, Norway's Parliament building, several printers were marked with notes saying "Not to be used – very important". The event led to a security review and the understanding that unsecured printers can be used as a bridge between one network to another. New machines were bought to replace the printers after the scare.

3D PRINTERS EXPOSED ONLINE

Nearly 3,800 3D printers with an open-source OctaPrint interface had no password authentication and were available to anyone online. Attackers could easily view printer webcams and download 3D models, potentially revealing proprietary information about unreleased products. Sabotage of a competitor's 3D model is another possibility. Attackers could also modify the printer settings, reflash the device's firmware or do damage to the 3D printer itself, potentially causing a destructive fire. Searching for exposed printers is relatively easy thanks to tools like Shodan, a search engine for Internet-connected devices.

FAX MACHINE ATTACK

According to researchers at Check Point Software Technologies, cybercriminals can hack company networks and steal sensitive files by exploiting vulnerabilities in multifunction printers. The researchers took over a device by faxing malicious code disguised as an image file, then infiltrated the network the device was connected to. Millions of fax machines are still in use, especially in the medical sector. Companies should keep sensitive files in a sub-network that's separate from the network printers are connected to.

PRINTERS HACKED FOR PUBLICITY

The online training site Skillbox claimed they caused thousands of printers to print promotional flyers for a design course. Skillbox used Shodan, a search engine that finds unsecured devices connected to the Internet, then sent the print job via the printers' open 9100 port. It's just another example of why securing endpoints like printers is crucial to keeping your devices and network protected.

dtp GROUP

SOLVING IT TOGETHER