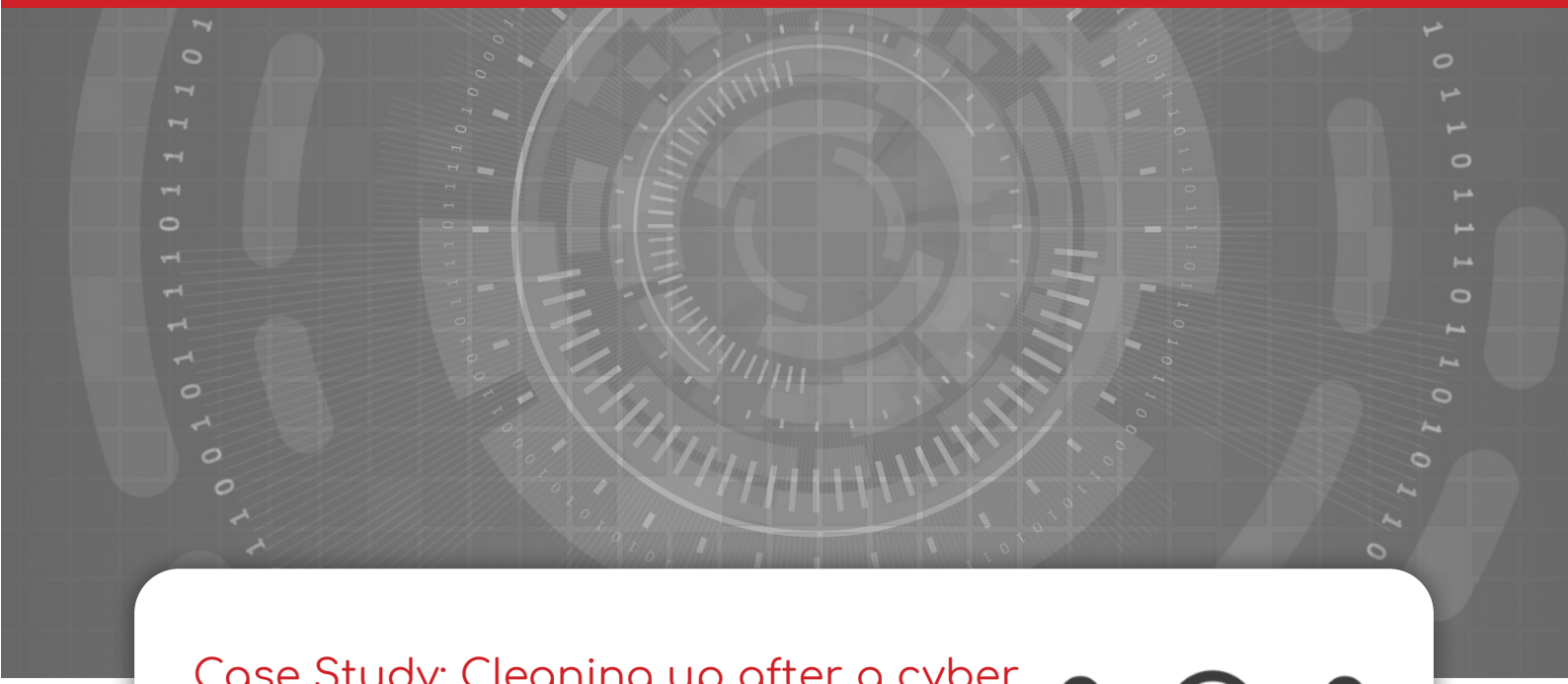
making work flow



Case Study: Cleaning up after a cyber attack: Food Production Company

An established fresh food organisation with production facilities located worldwide. Its business model relies on a robust IT infrastructure to ensure it operates efficiently and meets customer demand with fresh produce.

Case Summary

Name: Cleaning up after a cyber attack
Food Production Company
Sector: Food production

Overview

Our client suffered a serious cyberattack that resulted in network intrusion across all its sites.

Solution

- ASL Technology

Benefits

- Clean up the aftermath and rebuild their network with security as a priority
- We address the security skills gap for many of our clients, providing expertise in cyber security across the entire network

Overview

Our client suffered a serious cyberattack that resulted in network intrusion across all its sites. The perpetrators used Emotet – one of the most common and pervasive malware threats for business today – in tandem with Trickbot ransomware.

The malware fools users into infecting endpoints through phishing emails. Emotet's ability to infect networks in different ways means that it has remained a 'top 10' cyberattack for many months.

The attack forced our client to disconnect all its network devices which had huge impact on its business operations – loss of profit and damage to its brand reputation. Food orders are processed electronically, and deliveries are scheduled automatically via an integrated system.

The unexpected network shut down affected the delivery schedule and staff were required to work additional hours to manage unhappy customers. The severity of the cyberattack also rendered many of its UK PCs irreparable, causing our client additional unplanned cost.

Solution

When our client alerted us to the attack, the first step was to isolate the complete network in order to contain the problem. Every device was disconnected, including PCs, servers, routers, and of course printers.

We then tested each device for malware in isolation and only reconnected each device to the network once we were sure it was safe. Working with the suppliers of our client's printers and multi-function devices (MFDs) to confirm that these devices were free from malware, we devised a cyber defence strategy that minimised the risk from future cyber threats.

ASL recommended use of an isolated printer VLAN to create a secure printing infrastructure that would help protect the corporate network against future attacks. Configuring the network in this way prevents print devices from having any direct access to the internet or any other network device.

While implementing these network changes, other security measures were put in place. For example, the 'secure release' feature ensures that print jobs are only released when the user is next to the printer. This approach ensures confidential documents are only picked up by the people who printed them and eliminates the waste that results from jobs printed but never collected.

Using process called 'host hardening', we carefully configured the settings on each MFD.

The entire clean-up operation, including the introduction of extra security measures and reconfiguring all their machines took just one week across all UK sites. Our client's network infrastructure is now configured as securely as possible and downtime of their business operations was minimised.

Benefits

Realising that your business has suffered a cyberattack is a stressful experience. We worked with our client's IT team to minimise the consequences of the attack, clean up the aftermath and rebuild their network with security as a priority.

While 55% of firms experienced a cyberattack in 2019, just like our client, the reality is that most businesses admit that they are underprepared for breaches. Only half of businesses think that they can defend themselves against cyberattacks[1]. Meanwhile, cyberattacks cost firms millions each year.

As securing networks from cyber threats becomes more complex, it can be difficult to find people with the relevant skills and up-to-date knowledge to put robust security measures in place. We address the security skills gap for many of our clients, providing expertise in cyber security across the entire network – including the issues around printer security.

Source 1: https://www.bbc.co.uk/news/business-48017943

ASL
making work flow

Head Office
Technology House
20 Trafalgar Way
Bar Hill
Cambridge
CB23 8SQ