Orange
Cyberdefense

Customer stories

Inzpire is a trusted partner of the UK MOD. They sought to combine two parts of their business and merge their network infrastructures in one.

Customer profile

Industry: Transport
Location: Lincolnshire, UK
www.inzpire.com

Solutions provided

- Dual Layer Firewalls
- Gateway Content Filtering
- Remote Working
- SIEM
- Project Management
- Implementation Consultancy
- Dedicated Account Manager
- Telephone Support

Business results

- Re-architecture of the network and security to cover two business groups
- Office move on time and to plan
- Minimal business disruption
- Retention of CESG certification
- CEO was pleased with the outcome and the IT team

Background

As an award-winning supplier of defence managed services and cutting-edge mission systems, Inzpire is a trusted partner of the UK MOD. They make the worldleading GECO family of mission systems for both airborne and land applications, Inzpire also train the British Army to fly Apache helicopters, instruct RAF pilots in cockpit skills, support UK Typhoon operations. They are experts in simulation and synthetic environments.

The challenge

The Inzpire management team decided it was time to combine its two separate groups in to larger premises and merge both of their network infrastructures. This would streamline the workflow and reduce the costs of the business creating efficiency and setting it up for the next phase of growth. With such a large, high profile project, the CEO was taking a personal interest in its success as it affected the whole of the organisation.

As well as moving the IT infrastructure to a new location and merging the two groups' networks, the business was also looking to implement new servers, IP telephony and migrate to a new operating system across its desktops and handheld devices. Another important element of the project was to reconfigure the existing IT security to protect the new secure network.

With such a task ahead the Inzpire IT team needed to work with a partner that knew their infrastructure and, more crucially, that they could trust to deliver a planned outcome. In a previous project Orange Cyberdefense had implemented key parts of the IT security infrastructure for Inzipre which included dual layer firewalls, gateway content filters, a VPN for remote working and a SIEM solution. This put Orange Cyberdefense in a position to be able work with, and advise, the IT Team at Inzpire helping to coordinate key tasks of the project.

We needed an IT security partner to help deliver a high profile project involving collaboration with other companies to set up a new secure network.

Ian Robinson,
CIS Manager

The implementation

Orange Cyberdefense and Inzpire met to discuss the project and to plan it out. Using PRINCE2 methodology Orange Cyberdefense's lead consultant worked through the security elements of the project and how it influenced the plan for the wider office move and infrastructure implementation.

Orange Cyberdefense's element of the work had an impact on the on the whole network which would not be secure until key security infrastructure was up and running. With this in mind the Orange Cyberdefense consultant enabled a temporary firewall to secure the Inzpire network and allow the other network installations to go ahead without having to wait for all of the security systems to be re-implemented. It also meant that the users could have access to critical systems quicker without the delay of waiting for the network to come back online. With a secure perimeter in place, Orange Cyberdefense's consultant helped the Inzpire team migrate the infrastructure over to the new network.

Having done previous work for Inzpire meant that the Orange Cyberdefense consultant had a wealth of knowledge around the whole network set up that could be deployed in the re-implementation. The work included, prepping the kit, cabling, racking kit and telecoms. Not worried about getting stuck in, the Orange Cyberdefense consultant was happy to put on old jeans and a T-shirt to help with the work. Once the network was back up and running the focus turned to prepping the security infrastructure and re-implementing the Dual Layer Firewalls, Gateway Content Checkers, Remote Working and the SIEM Solutions. The new IP telecoms needed to be enabled through the firewall and there was networking and security work to integrate the servers. The security element of the project also had to ensure that all the latest product versions were installed and that it was correctly locked down while still enabling the business to function correctly. As an MOD contractor Inzpire has a strict security ethos and a key element of the work was to keep support for the legacy protectively marked data as well as ensuring that the latest security practices were followed in line with the company's security policy.

The benefits

The work went smoothly and to plan with the down-time window of mid-day to mid-day achieved and the business gained a new, much larger office. The two groups of the business can now share the efficiencies of a joint work flow across a secure network that is fit for purpose.

The project went so well that the IT team received a call from their CEO to congratulate them on a job well done. He could not have been happier with the outcome.

About Orange Cyberdefense

We are Europe's largest managed security, threat detection and threat intelligence services provider. We provide integrated solutions that assess risks, detect threats, protect our customer's IT assets and respond to security incidents.