From Ashes To Armor: Fortify Fire Services Against Cyber Threats

We have witnessed a significant digital transformation for emergency response services, as seen in other public sector services. An increasing resilience in digital technologies brings many benefits, particularly about enhanced efficiency and coordination – critical objectives for providing effective fire services.

However, as fire departments collectively adopt interconnected systems, cloud-based and smart technologies to enhance their services, the cyber threat landscape grows exponentially, exposing them to evolving cyber security challenges and new threats to make the need for ensuring their cyber security robust paramount.

Ransomware Threats

While systems in the public sector have been upgraded and updated since the infamous WannaCry ransomware that caused major disruption to the NHS in 2017, the threat of ransomware is still real. In 2021, Qakbot made its way through various email chains and was a precursor to ransomware. There were instances where this malware made its way to employees of fire services but was luckily thwarted by better response techniques and lessons learned from WannaCry. However, it is clearly evident that regular security awareness training is required to better deal with other potential cyber risks, such as not giving out work email addresses unnecessarily, using best practices passwords and educating staff on malicious email campaigns.

Multi-Layered Defence

While many fire services, such as the London Fire Commission, have already adopted multi-layered defence strategies, ranging from anti-viruses and malware scanning to strategies for implementing regular system patches, such approaches tend to be bespoke. There is no one-size-fits-all solution that can be implemented to serve organisations which have different business objectives.

It is important to not only procure robust cyber-defence systems, but also ensure that the capabilities within such a system aligns with business objectives while also providing robustness to new, evolving attacks from external sources that can disrupt key front-line activities of fire services.

Proactive Response

As first responders, organisations in the fire services should prioritise efficiency and proactive behaviours when responding to emergencies. The same should be applied to cyber security. Every day, multiple security events can occur on your networks that may impact your assets. In a single month, there could be up to hundreds of thousands of these events, of which only a few thousand may be alarms that should be analysed and tens of these alarms that need to be thoroughly investigated. It is important that signs of potential attacks can be identified and prevented in real-time, to prevent and mitigate any impact on critical services.

Service/Offering	Introductory	Foundations	Intermediate	Advanced
NCSC Guidelines	●	●	●	●
Standards Compliance Review	●	●	●	●
Gap Analysis	●	●	●	●
Security Improvement Planning	●	●	●	●
Security Awareness & Training	●	●	●	●
Procedure & Policy Review	●	●	●	●
Network Configuration Review	●	●	●	●
Risk Review	●	●	●	●
IT/OT Asset Discovery	●	●	●	●
Firewall Security Checkup	●	●	●	●
Framework Review (Cyber	●	●	●	●
Information Security Management	●	●	●	●
Authentication Review		●	●	●
Business Continuity Planning		●	●	●
Disaster Recovery Planning		●	●	●
Incident Response Planning		●	●	●
Identity & Access Management		●	●	●
Threat Assessment		●	●	●
Penetration Testing		●	●	●
Internal/External Audit		●	●	●
Threat Intelligence			●	●
Vulnerability Management			●	●
CISO as a Service			●	●
Third-Party Risk Management			●	●
IT/OT Consultancy			●	●
MXDR & Endpoint Management				●
Red Teaming				●
Breach Attack Simulation (BAS)				●
SIEM & SOC Advisory Services				●

To find out more or to speak to an expert contact us today.
www.sapphire.net / 0845 5827001