Westminster eForum
eCrime, cyber-threats and protecting critical infrastructure

Protecting Critical Network Infrastructure at Distributed Sites

Robert Waldie, Opengear

Much of the discussion around eCrime and cyber security has focused on securing servers and desktops from the operating system up through to the application layer. Lurking beneath at the network layer lies three acute vulnerabilities to critical network hardware – denial-of-service and breach of availability, targeted exploits to compromise integrity, and internal cyber sabotage by network administrators.

A cyber security audit and incident response plan should address these vulnerabilities by implementing a best practice solution that includes:

- Infrastructure monitoring for intrusion and incident detection
- Consolidated infrastructure management access with comprehensive logging for administration audit trail and forensic analysis
- Secure out-of-band control with run book automation for incident recovery and remediation

These recommendations hold not just for critical network infrastructure at centralised high density installs, such as ISPs and data centres (where they are more likely to be implemented already), but also for network infrastructure at distributed sites.

The adoption of cloud services has delivered enormous benefits, particularly for SME, enterprise branch offices, home workers and members of the distributed workforce. Uneconomical back office servers that were underutilised and expensive to maintain have been virtualised with Software- & Infrastructure-as-a-Service, providing billing, CRM, collaboration and teleconferencing systems from the cloud.

However, physical network edge infrastructure is still required to tether distributed workers to the cloud and the systems they rely upon for day-to-day operations. When this infrastructure is unavailable, businesses cannot service their customers – short-term financial losses may run in to tens of thousands of pounds per hour in lost revenues and lost productivity, as well as longer-term damage to reputation.

Consequently, the cost of network downtime has risen dramatically. Distributed sites are less likely to have the bandwidth or redundant network

infrastructure to absorb a sustained distributed-denial-of-service attack, making them soft targets for increasingly targeted and financially motivated attacks. While incidents such as the Amazon EC2 outage has drawn focus to the risks at the cloud hub, the spokes of the organisation are also vulnerable.

The total primary cost of network outage is the cost of downtime factored with the mean-time-to-recovery. Distributed sites will often have little or no local network administrator staff to respond to an incident, and with the network connection saturated or offline, remote managed service provider or corporate IT administrators are hamstrung. With no remote access to the management ports of critical network infrastructure, a site visit becomes necessary and the time-to-recovery becomes hours or days.

To address this, a secondary out-of-band network connection should be provisioned at each distributed site – be it old fashioned dial-up, or secure VPN over a secondary wired or cellular broadband link – dedicated to provide authenticated, encrypted and auditable out-of-band access directly to the management ports of critical network infrastructure. Network-enabled management ports should be physically segregated onto a separate management network, to remain accessible regardless of state of the production network.

Run book automation implements the workflow that administrators use to detect and respond to an incident or outage, as a series of automatically triggered programs or scripts. Run book automation can effectively install a virtual network administrator at each distributed site, not just to optimise MTTR with automatic recovery scripts, but also to mitigate human error and cyber sabotage.

Finally, as evidenced recently by the Stuxnet worm, malware has expanded beyond the traditional hunting ground of desktop and server operating systems. The Psyb0t worm targets the embedded operating systems of the network infrastructure itself, previously considered too obscure to be truly vulnerable. Alarmingly, this means network infrastructure inside the perimeter such as managed switches and Voice-over-IP systems are now a potential vector for man-in-the-middle attacks, eavesdropping and data theft. This threat is still emerging, but underscores the importance of continually monitoring network infrastructure at the operating firmware level.

Biography

Robert Waldie manages business development for Opengear in the UK and Europe, and provides network management solutions architecture and technical training for Opengear's partners and customers. His background is in embedded systems development of infrastructure management and network security appliances.