Metropolitan Networks Case Study – The Chartered Institute of Environmental Health

From congested to clean - how to rescue a compromised network

Chartered Institute of Environmental Health

Metropolitan Networks identified and resolved problems that were overwhelming the network at the Chartered Institute of Environmental Health. The viruses and attacks that were propagating on the network had reached a point where they were almost impossible to contain.

"To say we are pleased with the result may be a bit of an understatement. Metropolitan Networks has put us back in control of our network and rescued us from a potential crisis."
Sean Mohammed, IT Manager, Chartered Institute of Environmental Health.

The Chartered Institute of Environmental Health (CIEH) is an independent professional body and registered charity representing those who work in environmental health and related disciplines. Their primary function is the promotion of knowledge and understanding of environmental health issues.

A drain on the network

Despite having two Cisco Pix firewalls and antivirus protection on both the server and each of the 120 desktop computers, The CIEH found its network was plagued with viruses, its two 2 mbps WAN connections were heavily overloaded, and work was grinding to a halt. Sean explains: *"A large proportion of the ICT departments resources were being consumed by this problem. It was leaving us with little time or money to implement any of the new projects we had planned to undertake."*

The Institute has had a long relationship with the technicians at Metropolitan Networks and valued their security expertise, so when it was recommended they trial a PacketLogic from Netintact, never before seen in the UK, the CIEH had enough faith in Metropolitan Networks to give it a try.

Insight

"The PacketLogic was a godsend. It was like a blind man being given his sight. We could see instantly all traffic on our network. We could inspect our network to see which machines were using up our bandwidth, and which applications they were using to do it. It also allowed us to identify irregularities in our bandwidth usage and so see where viruses had propagated."

The PacketLogic not only allowed the CIEH to inspect how their bandwidth was being used, and identify problems, but also offered a solution to those problems. As an application layer firewall it was able to block non-essential bandwidth consuming applications such as instant messaging and file sharing. It was able to divide and assign bandwidth for different activities and reserve a premium for the most mission critical.

An important part of preventing future attacks was identifying where the original attacks had come from in the first place. It was found user intervention on AV software, public webmail accounts which bypass AV scanning from the email server, and 3rd party devices such as USB memory sticks all had their part to play in introducing and propagating viruses.

Again the CIEH looked to Metropolitan Networks to remedy this problem, which was quite a straight forward and inexpensive one:

1. Place a small Fortigate on the network edge to offer AV protection, for all company e-mail, http, SMTP, imap, pop, and ftp traffic.
2. Educate staff on the importance of using local AV software, and keeping it up to date.
3. Use the PacketLogic to block potentially compromising applications such as file sharing.

An outstanding success

The initial small Fortigate was so impressive that the CIEH quickly decided to replace their two Cisco Pix firewalls with two Fortigate 300 Unified Threat Management solutions to offer not just firewall and anti-virus protection, but also intrusion detection/ prevention, anti-spam, anti-spyware, and IPSec VPN usage.

These days the CIEH benefit from a secure, robust network. The daily problems Sean faced are a thing of the past.

"I would be first to admit our network was unmanaged. We were overwhelmed with problems and didn't know where to start. The PacketLogic enabled us to identify and eradicate the problems on our network, and the Fortigate gives us the protection from future attacks.

"It isn't everyday you get a satisfying answer to such a complex problem, We feel indebted to Metropolitan Networks for the way they were able to secure, protect and give us the tools to manage our network. Their experience, expertise, and wisdom have made my life a lot easier."

Metropolitan Networks, TMS House, Cray Avenue, Orpington, Kent. BR5 3QB
Tel: +44 (0)870 777 4951 Fax: +44 (0)870 777 4954
www.metropolitannetworks.co.uk