



SoftScan and Keyfort Restore Order to Law Firm's Email

Email has become by far the most popular medium for criminals to undermine an organisation's information security. A successful attack can jeopardise not just data integrity but also the integrity of the company itself. To ensure comprehensive protection, organisations need to scan both inbound and outbound email.

Andrew and Andrew is a prominent law firm based in Portsmouth and operating throughout the South East. It is one of the first two firms in Hampshire to gain professionally recognised accreditations for its systems of work and practice management standards under the Investors in People and Law Society's Lexcel Schemes.

Andrew and Andrew uses email extensively to communicate throughout its business and uses SoftScan, a hosted email security service, to protect against email borne threats. SoftScan provides protection against viruses (known and unknown), spam and other email threats including phishing and joe-jobbing, in addition to offering policy filtering. It is totally configurable, allowing the administrator to tailor the system to personal preferences, company policies or local legislation.

Sally Power, practice manager of Andrew and Andrew comments, "Being a law firm makes us all too aware of the legal implications of staff viewing explicit material unnecessarily or the devastation that a computer virus infection can bring. We scan both inbound and outbound email because we need to ensure that not only are we protected from attacks coming in, but should anything go wrong we need to be certain that our servers aren't distributing malicious emails either."

Avoid the dangers of not checking outbound email

There are two main dangers to allowing outbound email to leave unchecked via company servers. The first is irrespective of how comprehensively inbound email has been scanned, a virus can still enter a network via another source such as a laptop, flash memory card or cd-rom. If it is not caught, within seconds email servers could be an unwitting accomplice to infecting another company's server. The second danger is that if a machine has been compromised within the organisation, it could be surreptitiously sending out spam. This is not only potentially harmful to the company's reputation, but also using vital resources such as bandwidth.



Increasingly, spam is distributed via botnets, a network of PCs known as zombie computers that have been infected with a Trojan that puts them at the disposal of the botmaster. The botnets are then rented out for a variety of uses including denial of service attacks and spamming. The Trojan also normally gives the botmaster a backdoor into the machine that can be used to update aspects of the malicious software or even download confidential company information.

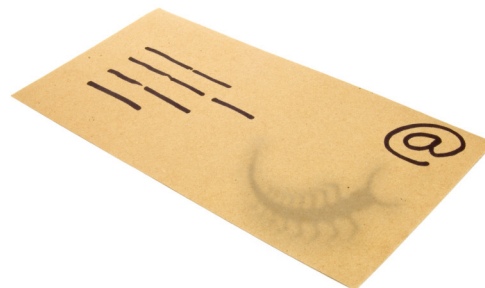
"We chose to use SoftScan on the recommendation of Keyfort who look after our networks for us," continues Sally Power. "We find SoftScan very easy to use and far more effective at stopping spam than our previous solution. It allows us to concentrate on our work without having to worry about email protection. In particular with SoftScan we don't have to worry about unknown viruses as SoftScan's own scanner Paranoid picks up anything it thinks is suspicious."

Keyfort, implement and manage secure networks used for data, voice and video. Based in Bournemouth, Keyfort has customers throughout the private and public sector. Understanding Andrew and Andrew requirements, Keyfort suggested SoftScan's hosted service as it offered a number of benefits including no hardware or software to manage and update. In addition, SoftScan's Paranoid scanner would offer Andrew and Andrew unparalleled protection against email threats not yet identified by traditional anti-virus scanners.

Stop unknown viruses in email

Paranoid adds the extra level of scanning capabilities required to detect suspicious email content from entering an organisation's network, learning and adapting with every email it scans.

Paranoid's Virus Probability Analysis (VPA) developed exclusively for SoftScan by anti-virus experts, calculates the probability of harmful content within an email. Once the email has passed through the normal anti-virus filters, VPA carries out a series of steps that includes analysing both the email message and any attachments in greater detail.



It looks at a variety of characteristics that may identify the message as suspicious including the binary code of any attachment, the binary type used and what's inside the binary. VPA also investigates the email message itself looking at specific characteristics, where it came from and a series of other distinguishable features. If the malware writer has deliberately forged the email or binary in an attempt to avoid detection, then VPA switches tactics too and re-analyses the message using a different set of rules.

"With SoftScan we really feel that we have email threats covered and our inboxes are no longer filled with spam. Keyfort's suggestion has relieved us from the burden of managing email security effectively and the overall integrity and reliability of our email system has improved. Overall the service we receive from SoftScan is a significant improvement on our previous supplier and I would recommend anyone to take a look at the service they offer."

