

Securing clouds makes sense for City

Email is listed as number two on the Council's mission critical list.

The six-person IT unit for the City of Fremantle manages a network for 300 users in 10 locations across WA's port city - as well as seven websites including the Council's corporate site, an intranet and tourism and marketing sites.

The council runs a VMware environment which has brought savings but "requires state-of-the-art protection", says John Pavy, manager of information technology.

According to Pavy, Fremantle is one of the largest metropolitan retail centres outside of Perth and has long been known as "WA's other capital".

He says it's the responsibility of the local government authority to maintain and promote this character through better services along with value for ratepayers.

The council is actively improving its efficiency and effectiveness through business planning, competitive practices, benchmarking and performance management.

Within its corporate services arm, the IT business unit constantly monitors technological developments to ensure the organisation's information systems are contributing to the council's services.

However, the council's in-house messaging security software was overwhelmed by a vast volume of spam. It was receiving 10,000 emails every day and only "1800 were genuine", says Pavy.

Facing constant attack

"The in-house spam filter and anti-virus software were continually under attack, representing a huge waste of our bandwidth," says Pavy. "Because of the enormous volumes, the software would regularly lock up

and block all incoming emails, interrupting productivity and wasting IT staff time to sort the mess out."

One of the greatest risks to the City of Fremantle from malware hidden in spam and on suspect websites is damage to its network, resulting in downtime, he says.

While there has been only one successful attack in recent years, and the council's internal risk reduction strategies limited the damage to a few desktops, it proved the in-house "security solution was anything but secure".

When the council's IT team came across Software-as-a-Service (SaaS) technology, it spent a year trialing various providers to test their products' effectiveness, exploring different configurations to maximise messaging security efficiency, says Pavy.

The team chose MessageLabs' range of email security products, including Email Anti-Spam and Anti-Virus; Image Control and Content Control; Web Security Anti-Spyware Anti-Virus; and URL Filtering, all of which are hosted security services.

Once the trials were completed the council approached MessageLabs, who then passed the details to Tony Estrano, account manager at its WA-based integrator partner, L7 Solutions.



Email is critical

Glenn McTee, L7's managing director, says the deal was quickly closed and the deployment completed by Nirmal Alvares, the reseller's senior systems architect.

"Although we didn't drive the initial contact with City of Fremantle, we've worked the council before, but we've only done small pieces of work," says McTee.

He says email is listed as number two on its list of critical applications, as it comprises the majority of the council's communications.

"Having email not work properly would have a big impact for the council," says McTee. Email isn't just

The in-house spam filter and anti-virus software were continually under attack.

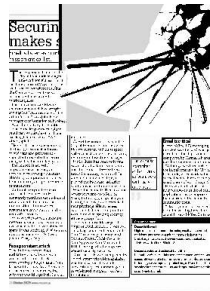
Case at a glance

Business drivers:

High proportion of Council's incoming email was spam and malicious-code attacks resulting in network downtime.
 Size of organisation: 300 network users; seven websites; 10 offices with 450 staff in total.

Business value and technical benefits:

Guaranteed clean email inboxes; safe and compliant email and web usage; network protected from downtime; no in-house labour or technology costs; improved productivity in IT and for end-users; seamless implementation, "set and forget" service; no hardware or software required.



essential to the council's business - other clients rate it as a top-three critical application, he adds.

A security cloud solution offers small to midsize organisations an alternative to products which require internal infrastructure and manpower.

"The council's previous product needed constant human intervention for the management of spam," says McTee. "This creates high overheads as staff need to be trained on how to create duplicate emails and then have it backed up."

What makes cloud security solutions attractive is there's no need for upfront capital outlay. Products such as the MessageLabs' email security is priced on a per month, per user basis.

L7 "worked out the council's previous solution would cost around \$80,000-\$100,000 - or more - to get it to work on the same level as a cloud-based email solution", he says. "That kind of expenditure makes cloud security compelling."

Pavy says his team has "more than enough" to do in meeting organisational needs and it can't afford specialised training to detect and combat Internet-level threats.

"Even if we had the time, I have to assume that whatever I imagine a Trojan, virus or bot can do, someone out there can make it happen," he says. "A hosted service significantly reduces the risk of malware arriving at our network unrecognised or sitting silent, waiting for a trigger."

That was quick

McTee says MessageLabs' product deploys quickly and has little impact on an organisation's day-to-day business, which is important for a council.

Apart from setting the controls for what type of email is allowed through, L7 tailored one or two aspects of the MessageLab's solution to suit the Council's needs.

"The solution was up and running and filtering messages within eight hours," he says. "The project took 24 hours from the time of acceptance to sign-off."

As part of its ongoing services, the integrator goes to a portal to access the council's monthly email security and filtering report. Otherwise it has very little involvement in its



The solution was up and running and filtering messages within eight hours.

Glenn McTee, managing director, L7

Gartner: Cloud security services peak in 2009.

Analyst group sees potential security cloud services

Security services provided in the cloud have the potential to provide cost savings and faster deployment compared with equivalent-capacity, premises-based equipment, but providers are yet to deliver on customer expectations, according to Gartner.

Defined by Gartner as internet-fabric-based managed security services, 'in the cloud' security services appear at the "peak of inflated expectations" on Gartner's 2009 Hype Cycle for Infrastructure Protection. Services provided may include managed firewalls, intrusion detection systems, intrusion prevention systems, antivirus services, distributed denial-of-service protection services, messaging security and Web gateways.

Gartner recommends that organisations look at using security-as-a-service providers, and bandwidth and remote connectivity service providers to consolidate premises-based equipment into cloud-based delivery options. This is especially useful for remote-office or branch-office situations that would otherwise require on-site deployment and hardware maintenance.

Ray Wagner, managing vice president at Gartner, says cloud security providers must deliver on customer expectations for the effectiveness, scalability and cost savings of performing security filtering in the cloud or as a service.

"The small or midsize business is an appealing initial market for these delivery models at lower price points, and we expect that the technology will become mainstream within two to five years," Wagner says.

email filtering, McTee claims.

Key components of the MessageLabs product include multi-layered security featuring its proprietary Sceptic engine, which captures known and unknown viruses and protects against Trojans, phishing and spyware.

The product incorporates image composition analysis which helps to identify, control and block inappropriate images contained in all email and email attachments and also features a configurable filter which allows administrators to create and enforce policies and rules controlling employee web use.

Pavy says the council receives only genuine emails, with all spam and malware infected emails blocked at the internet level and access to unsafe and non-work related websites prevented.

The IT department in local government "is a leader in collaboration with the business and the broader community, but we do so in a very dangerous environment", says Pavy.

The council's network is now protected from downtime, ensuring that its corporate websites are up and running to optimise productivity across the entire organisation, he says.

"Implementing MessageLabs' service has dramatically reduced the time and costs of managing messaging security and fixing the problems caused by spam and malware infections," says Pavy.

Not only does the malware detection capabilities minimise downtime, but its URL Filtering and Image control and content control enforces the council's acceptable use policies, says Pavy.

