

Surrendering security

Natalie Hambly, Technology & Business magazine

August 29, 2003

URL: http://www.zdnet.com.au/insight/soa/Surrendering_security/0,39023731,20277907,00.htm



Would you put the security of your company into someone else's hands? ZDNet Australia finds out what benefits and peace of mind a managed service can provide.

Guy Stocker, technology manager at Parmalat, wanted to fully outsource management of the company's firewall. He was only spending one percent of his time looking after it, when really he thought it should be monitored around the clock, seven days a week.

Parmalat is one of the three main dairy producers in Australia. Operating in 35 locations around the country, Parmalat has the problem that its produce is perishable: Its products need to reach their end destination within days. The Australian dairy industry is moving towards an e-business model and Parmalat is using an SAP system to transact with its partners, such as Woolworths and Coles. Because of these external transactions, managing the firewall on the Internet link is critical.

"Because we are a 24x7 operation you cannot have a firewall managed one percent of that time, which I was doing, it is crazy," says Stocker.

And his concerns are valid. As security vendors always tell us, threats to company security are increasing every day and they are becoming more complex and harder to catch. Users are saying this too. AusCERT (Australian Computer Emergency Response Team) recently conducted its annual Australian Computer Crime and Security Survey. Sent out to 350 of Australia's top public companies, more than 200 CIOs responded. Their results back up what security vendors have been telling us.

Ninety-eight percent of the companies surveyed said they use antivirus, 95 percent said they use firewalls, and the results were also high for access control and physical security, yet 42 percent experienced a security incident in the last 12 months. The good news is that figure is down from 67 percent in the 2002 survey.

However companies often balk at telling anyone they have experienced a security breach. With all the talk about security, it can often seem like scaremongering, but companies are experiencing breaches and they are responding to it.

Responding to these attacks, 67 percent of CIOs reported that they are now spending more money on security. This is something that John Donovan, managing director of Symantec, is seeing as well. Donovan estimates that companies are now spending about eight percent of the IT budget on security, compared to the last year's estimate of one percent. This is a significant increase, and Donovan says it would even be as much as 12 percent for larger companies.

However throwing more money at the problem hasn't made CIOs more comfortable with their handle on security, only 11 percent said they thought their organisation was managing all computer security issues reasonably well.

Why outsource

It is probably then no wonder that more companies are leaning towards managed security services. Donovan says Symantec is seeing a big increase in the managed services side of the business, in particular the monitoring and managing of security products.

He says people generally want to farm out the areas that give them the most pain, and in security that is monitoring and management, in particular firewall management.

The survey results back this up. CIOs cited the most challenging and problematic aspects of security management as; configuration management (49 percent), keeping up to date with threats, vulnerabilities, and changes in technology (58 percent), and changing users attitudes and behaviours regarding security (59 percent).

According to Lorenzo Modesto, sales and marketing manager at security service provider Bulletproof Networks, getting rid of the patch management headache is a driver to managed security services.

"Timely security patch application is absolutely vital to maintaining security. A perfect example of this is the huge impact of worms like Nimda and Slammer. Servers affected should have been patched to an acceptable level but weren't, and in both cases the worms targeted a vulnerability for which a patch have been available for several months," says Modesto.

"At its peak we were seeing infected unmanaged servers pushing in excess of 100Mb/ps of worm traffic. The people

managing these servers were simply too busy to keep them up to date," he says.

Other reasons to outsource security are because it isn't one of the core competencies of the company, and it is too expensive to hire internal expertise.

From Stocker's point of view, keeping up to date with the latest upgrades and patches was a headache. He realised that managing security wasn't core to Parmalat's operations and also that he couldn't devote the time needed to manage the firewall and nor could he justify hiring an internal expert.

"I needed someone to manage the firewall totally because I'm not the expert and there is no way I am going to have an internal person be a specialist on it because how do you keep that person trained, and how do you keep them up to date with the latest things? We would probably spend more time reinventing the wheel," says Stocker. "If you've got a group that you can go to and that's all they do, then they have already got all the cuts and bruises, they know what not to do and what you should do to actually manage that type of infrastructure," says Stocker.

So the decision to outsource was fairly straightforward. When it came time to replace the firewall infrastructure, Stocker was referred to managed security provider Zento.

Shameful business

Stocker says he is very happy with Zento's service so far, and he was lucky to be referred to a good provider. Unfortunately finding a trustworthy security provider can be a bit hit and miss.

Kim Valois, director of global information security services at CSC, says there are a few security practices that she doesn't respect. She says there are some security practitioners who are "overlooking or omitting things or who border on negligent".

Valois says she ran across one such company that performed a security assessment for a client. After the assessment, this service provider gave a list of all of the security vulnerabilities the company was open to, however what it didn't provide was a complete risk assessment that includes how likely it would be that any of those risks would actually occur.

"Putting risks into perspective is critical to creating a pragmatic plan behind it. Otherwise it is just scaremongering. I think it's our obligation to put things in perspective, and that's important. People don't want to throw money away at a ghost," says Valois.

Arthur Argyropoulos of Zento says there are only around three managed security service providers at the moment that truly do managed IT security.

"I think it's very early days in the management of IT security. People claim 24x7 support but really they just have guys with pagers that get woken up at 3am," he says. "If [customers] meet the guys at the low end, they will have a low respect for what a managed service can provide."

Of course detecting the good from the bad isn't always easy. The best way to find a good (or bad) provider will be to ask around and find out what the experience has been for your colleagues in the industry.

However there are some basic service levels that you can check. First of all, check if they provide a true 24x7 service. Also ask for references and look for a provider that has built up relationships with its customers. And shop around.

One IT manager who was looking to fully outsource his company's security approached around 15 service providers. That might seem like a high number, but sorting out the good from the bad wasn't too difficult. Firstly some providers didn't even get back to him. Of those that did respond, he conducted interviews with them all and found that some were totally sales focused while others were technically focused. Also, only a few of the providers were willing to give quotes, and of those few, some weren't willing to break down the costs to show how much each service would cost.

CSC's Valois says you should look for providers that are straight with you and who don't try to push up budgets.

To get an idea of what a managed security provider can offer, Modesto says a typical service offering includes service configuration, ongoing and proactive patch management, ongoing monitoring, proactive response and troubleshooting within an agreed response window, and alerts of other operating system vulnerabilities when they spring up that may affect another part of the customer's network.

Service guarantees

And these services should all be set out in the service level agreement. (SLA). When it comes to the SLAs however, things tend to get tricky. Be aware that outsourcing security management does not mean that your company is now guaranteed 100 percent safety. Further, if a breach occurs and it costs your company millions, don't expect the provider to be responsible for that.

A security service provider cannot guarantee you will not be attacked, but it can guarantee certain service levels, for example, how long it should take to respond to an attack, how quickly the problem is resolved, how quickly to warn you

of a breach or vulnerability, and various reporting levels.

Stocker can tell you all about contract woes; his road to outsourcing security has not been without difficulty. Firstly, when discussing the service with Zento, it ended up being too expensive. So it took some renegotiation of the service, and Stocker decided that Parmalat would actually own the CheckPoint firewall which brought the price down.

He was ready to sign the contract, but it first had to be checked with Parmalat's lawyers, due to company policy. Then the trouble started. The lawyers came back and said Parmalat's insurance company would not be happy with the contract, because it would mean handing company risk over to Zento who would not actually be liable. If a security breach occurred and Parmalat incurred financial losses, Parmalat would be turning to its insurer. The insurer would then be turning to the security service provider, Zento, who under contract wasn't liable for the damage.

The contract was discussed with Parmalat's lawyers and Zento's lawyers for three months, trying to find agreement. According to Stocker, eventually Zento said it could move no further because it would be putting itself at risk, so Stocker and Zento had to come up with another plan.

"We sold him a CheckPoint firewall in high-availability mode and at the time we were talking managed security, but the company policy would not let a third party manage it, so Guy bought the technology and we created a derivative of our services," says Argyropoulos.

"So he manages the firewall and manages the risk, and we provide the monitoring 24x7, a secure Web portal, monthly reports, the alert and escalation procedures, and the technical expertise. He manages the updates to the firewall, the maintenance, and he puts in the policy in the firewall."

It means that Stocker no longer has to keep up to date with the latest patches, and he doesn't have to spend his time trying to be up with the latest technology, but if anything needs to be changed, the decision has to go through Stocker first.

"We've gone to a halfway arrangement... I get them to do the updates, I get them to do the patch updates, but I do that on a per hour basis, so if there is a new service pack to go in or a new upgrade, I employ their services to do that," explains Stocker. "They can't make changes to the firewall infrastructure; they can't make changes to the rule, and they can't do policy updates."

For Zento, its deal with Parmalat was a first; no other customer had broken down the service like that before. Argyropoulos says Zento saw the opportunity for that type of service and now offers a suite of managed services. He sees the managed security service growing faster than the outsourcing environment, and is now providing a service like the one provided for Parmalat, for three other companies

As for Stocker, he is very happy with the service he receives from Zento, but he says his preferred option is still to fully outsource.

"If I didn't have the legal obligations of the contract I would do it tomorrow," he says.

Who's out there

Following are some managed security service providers we came across when researching for this article. There are so many that we couldn't include them all, but this list should get you started.

AT&T

AT&T offers a range of security services, including managed premise-based firewall services (Nokia, Checkpoint); Security consulting; network scanning services (vulnerability and virus); and managed intrusion detection.

Bulletproof Networks

Bulletproof Networks specialises in providing Internet security including gateway and router management, managed, shared and dedicated hosting, monitoring and reporting services.

Dimension Data

Dimension Data's motto for its security services is protect, detect, respond. Services include planning of policy and procedures, framework production, architecture design and implementation, identity management, remote access, VPN, training courses, managed services, operational services, and vulnerability, threat, and risk assessment.

Equant

Equant works with customers to examine security policies, define the requirements, then tailor the gateway. Equant configures all hardware and software gateway appliances, provides ongoing monitoring and maintenance, and monitors every aspect of the gateway to ensure optimal performance. It offers real-time analysis of firewall log files and monthly traffic analysis reports, and security policy support.

LogicaCMG

LogicaCMG designs, builds and operates security solutions for Australian companies. LogicaCMG offers a broad range of security solutions. Services include Internet gateway hosting, penetration testing network and applications, vulnerability assessments, threat and risk assessments, and business continuity planning.

Logical

Logical offers round-the-clock network security management. Linked with its WAN/LAN and server management, Logical offers full infrastructure protection including security review, vulnerability assessments, monitoring and management of systems, incidents, configurations, software, documentation, and restoration, teamed with the ability to link content filtering, intrusion protection, and virus management.

Macquarie Corporate Telecommunications

Macquarie Corporate offers a comprehensive range of managed security solutions designed to meet the needs of corporate and government organisations. Services include DSD Accredited Gateway Solutions, antivirus, spam/URL/content filtering, and independent professional services including audits, vulnerability assessments, risk and threat assessments, and health checks.

MailGuard

MailGuard is a managed anti-virus and content filtering email management service. MailGuard utilises and supported by Sophos Anti-Virus, Norton Anti-Virus (Symantec) & McAfee (NAI) on a 24x7 basis. Services include: anti-virus and content filtering, spam management, alert and control, with statistics and information accessible from an Internet browser.

TPI

TPI is a global outsourcing advisory firm that manages virtually 100 percent of the large outsourcing deals in Australia. It provides outsourcing strategy, in addition to managing the transaction and the post deal relationship management.

TruSecure

TruSecure offers fully integrated, enterprise risk management services providing proactive risk reduction with real-time security management, monitoring, and response.

Zento

Zento manages firewalls, intrusion detection and prevention systems, and anti-virus solutions from a single platform. False positives are removed and real alerts are managed within SLA parameters. Zento's technical staff have accreditations in the technologies the company supports, including CheckPoint, NetScreen, Cisco, Trend Micro, and Computer Associates.

90East

90East is a leading supplier of managed security services operating secure perimeters, secure hosting and VPN's connecting all tiers of government and any commercial entities transacting with government. 90East operates certified security solutions, combining best of breed products, hardware and software, from its ASIO and Defence Signals Directorate certified Secure Operations Centres. The result is a solution suite enabling organisations and individuals to communicate and conduct business over the Internet.

Copyright © 2005 CNET Networks, Inc. All Rights Reserved.

ZDNET is a registered service mark of CNET Networks, Inc. ZDNET Logo is a service mark of CNET NETWORKS, Inc.