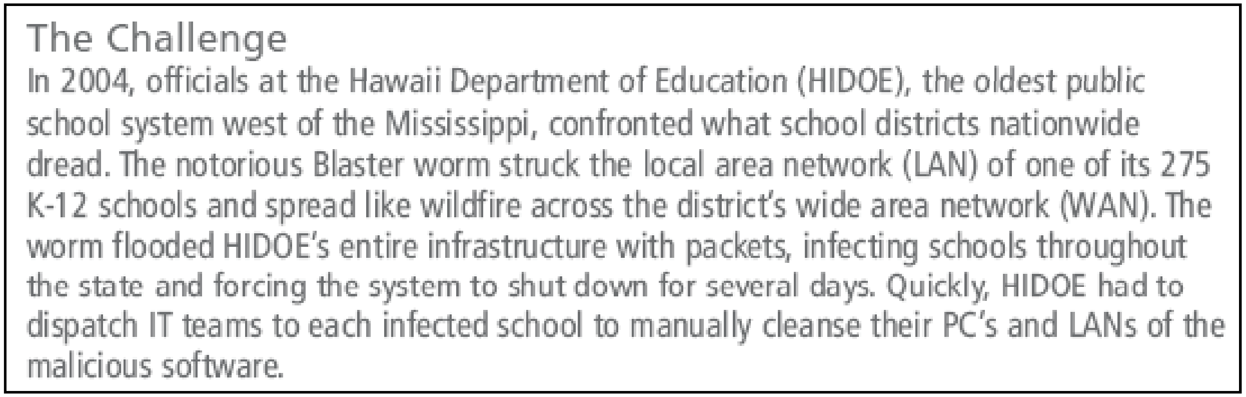
Ethical Hacking and Countermeasures

Version 6

Module LXII

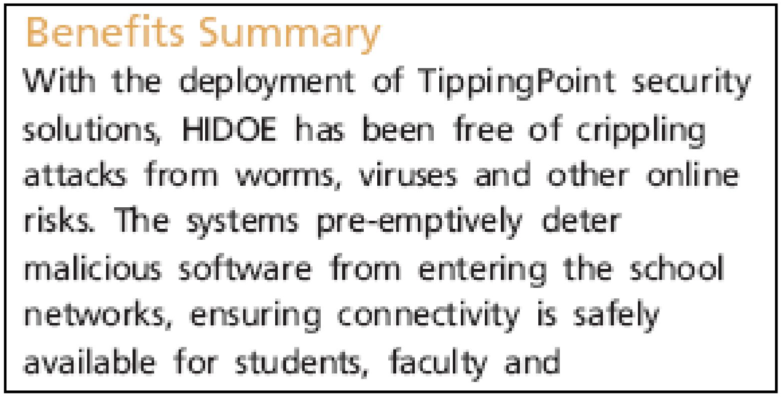
Case Studies

Hawaii Safeguards Schools Statewide Using Intrusion Protection Systems



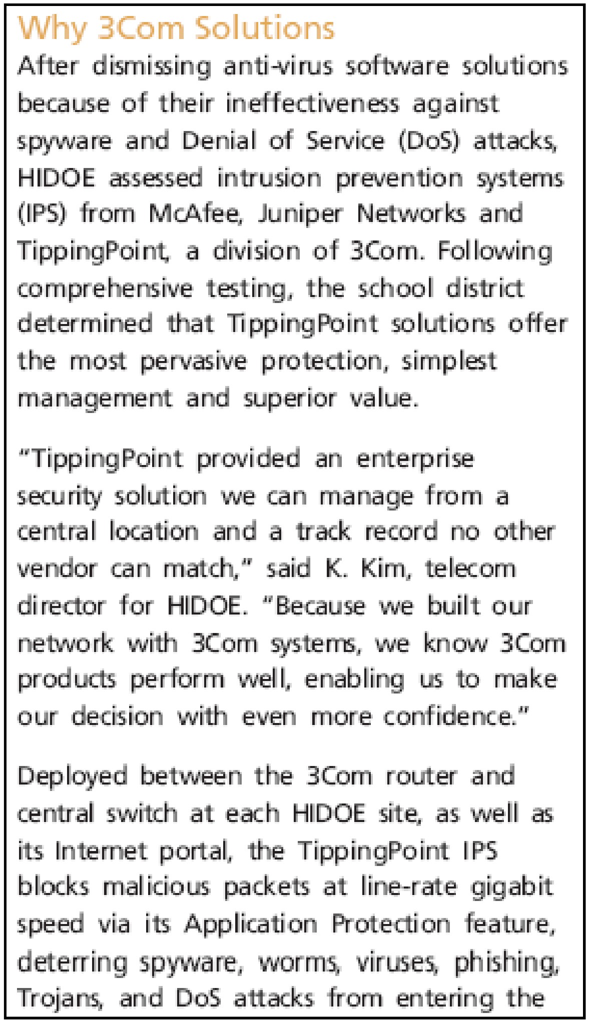
The Challenge

In 2004, officials at the Hawaii Department of Education (HIDOE), the oldest public school system west of the Mississippi, confronted what school districts nationwide dread. The notorious Blaster worm struck the local area network (LAN) of one of its 275 K-12 schools and spread like wildfire across the district's wide area network (WAN). The worm flooded HIDOE's entire infrastructure with packets, infecting schools throughout the state and forcing the system to shut down for several days. Quickly, HIDOE had to dispatch IT teams to each infected school to manually cleanse their PC's and LANs of the malicious software.



Benefits Summary

With the deployment of TippingPoint security solutions, HIDOE has been free of crippling attacks from worms, viruses and other online risks. The systems pre-emptively deter malicious software from entering the school networks, ensuring connectivity is safely available for students, faculty and



Why 3Com Solutions

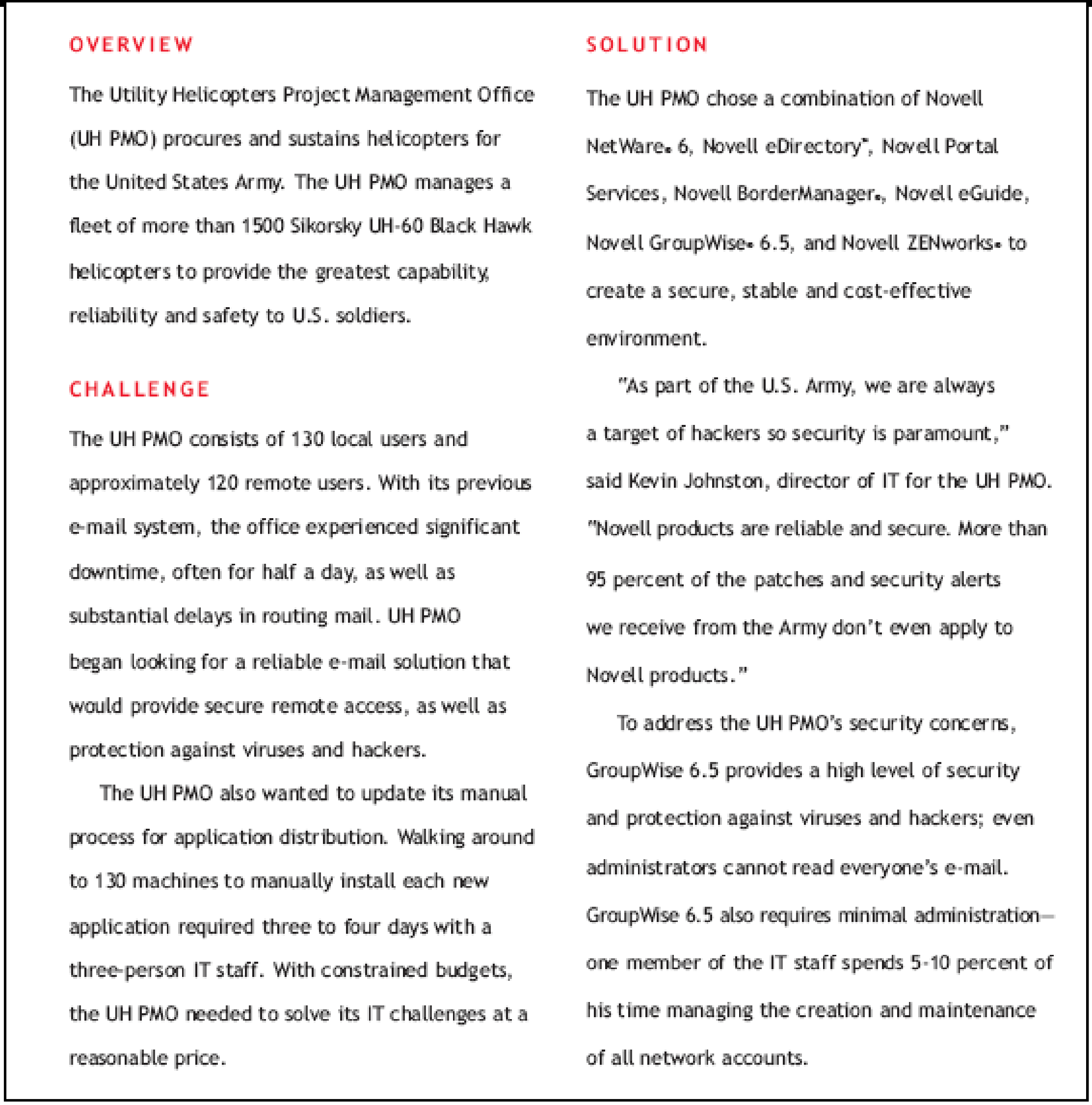
After dismissing anti-virus software solutions because of their ineffectiveness against spyware and Denial of Service (DoS) attacks, HIDOE assessed intrusion prevention systems (IPS) from McAfee, Juniper Networks and TippingPoint, a division of 3Com. Following comprehensive testing, the school district determined that TippingPoint solutions offer the most pervasive protection, simplest management and superior value.

"TippingPoint provided an enterprise security solution we can manage from a central location and a track record no other vendor can match," said K. Kim, telecom director for HIDOE. "Because we built our network with 3Com systems, we know 3Com products perform well, enabling us to make our decision with even more confidence."

Deployed between the 3Com router and central switch at each HIDOE site, as well as its Internet portal, the TippingPoint IPS blocks malicious packets at line-rate gigabit speed via its Application Protection feature, deterring spyware, worms, viruses, phishing, Trojans, and DoS attacks from entering the

Source: *http://www.tippingpoint.com*

U.S. Army Project Office Relies on Novell¨ Solutions for a High Level of Security



OVERVIEW

The Utility Helicopters Project Management Office (UH PMO) procures and sustains helicopters for the United States Army. The UH PMO manages a fleet of more than 1500 Sikorsky UH-60 Black Hawk helicopters to provide the greatest capability, reliability and safety to U.S. soldiers.

CHALLENGE

The UH PMO consists of 130 local users and approximately 120 remote users. With its previous e-mail system, the office experienced significant downtime, often for half a day, as well as substantial delays in routing mail. UH PMO began looking for a reliable e-mail solution that would provide secure remote access, as well as protection against viruses and hackers.

The UH PMO also wanted to update its manual process for application distribution. Walking around to 130 machines to manually install each new application required three to four days with a three-person IT staff. With constrained budgets, the UH PMO needed to solve its IT challenges at a reasonable price.

SOLUTION

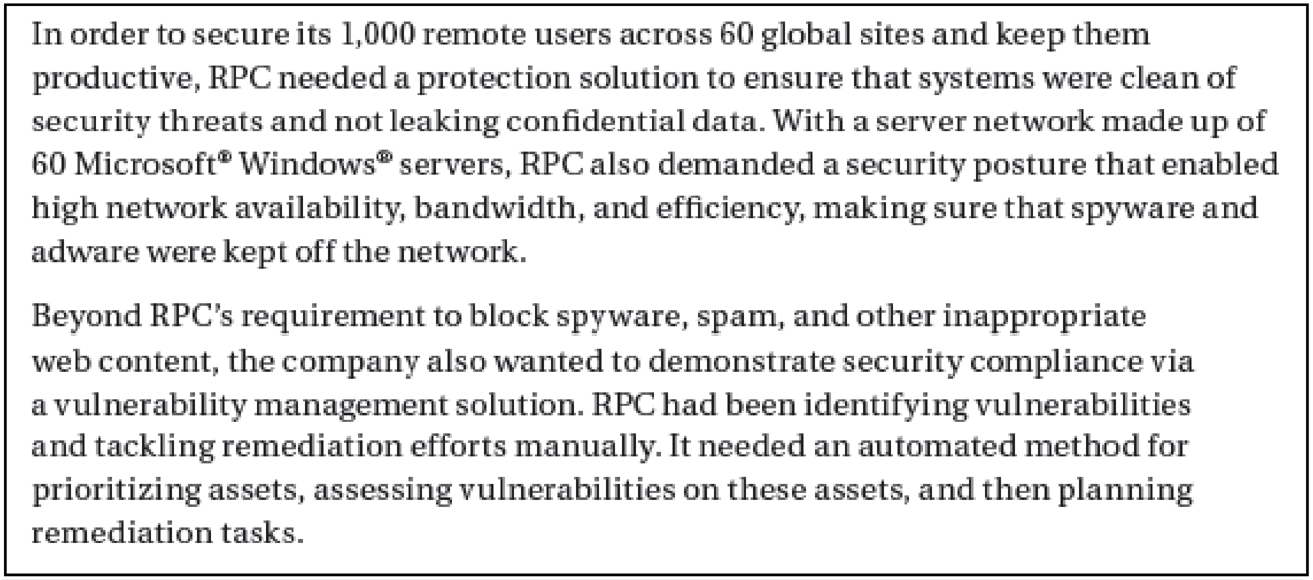
The UH PMO chose a combination of Novell NetWare® 6, Novell eDirectory™, Novell Portal Services, Novell BorderManager®, Novell eGuide, Novell GroupWise® 6.5, and Novell ZENworks® to create a secure, stable and cost-effective environment.

"As part of the U.S. Army, we are always a target of hackers so security is paramount," said Kevin Johnston, director of IT for the UH PMO. "Novell products are reliable and secure. More than 95 percent of the patches and security alerts we receive from the Army don't even apply to Novell products."

To address the UH PMO's security concerns, GroupWise 6.5 provides a high level of security and protection against viruses and hackers; even administrators cannot read everyone's e-mail. GroupWise 6.5 also requires minimal administration—one member of the IT staff spends 5-10 percent of his time managing the creation and maintenance of all network accounts.

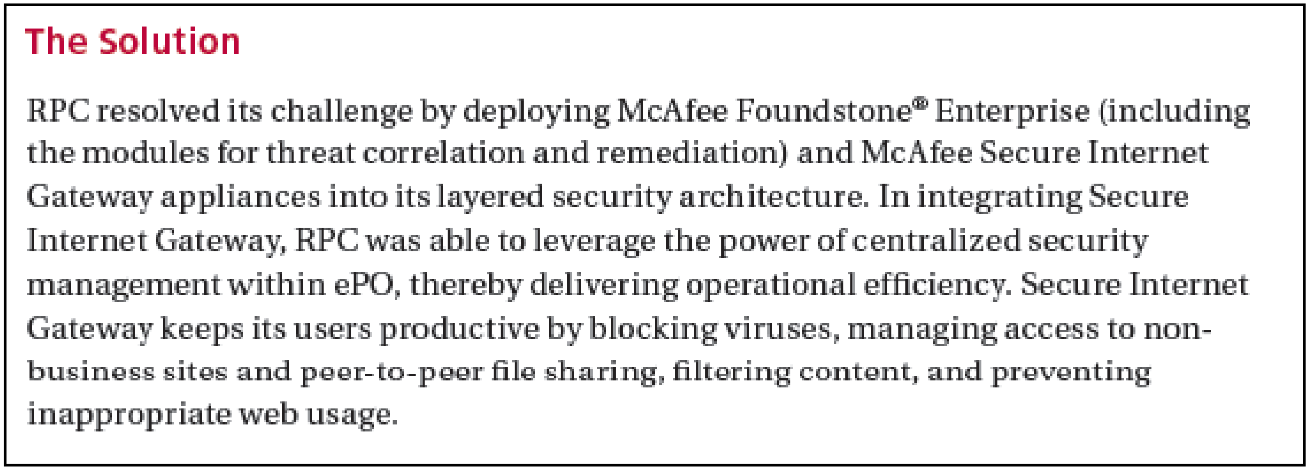
Source: *http://www.novell.com*

McAfee Gives RPC Comprehensive Visibility into its Critical Systems with Operational Efficiency



In order to secure its 1,000 remote users across 60 global sites and keep them productive, RPC needed a protection solution to ensure that systems were clean of security threats and not leaking confidential data. With a server network made up of 60 Microsoft® Windows® servers, RPC also demanded a security posture that enabled high network availability, bandwidth, and efficiency, making sure that spyware and adware were kept off the network.

Beyond RPC's requirement to block spyware, spam, and other inappropriate web content, the company also wanted to demonstrate security compliance via a vulnerability management solution. RPC had been identifying vulnerabilities and tackling remediation efforts manually. It needed an automated method for prioritizing assets, assessing vulnerabilities on these assets, and then planning remediation tasks.

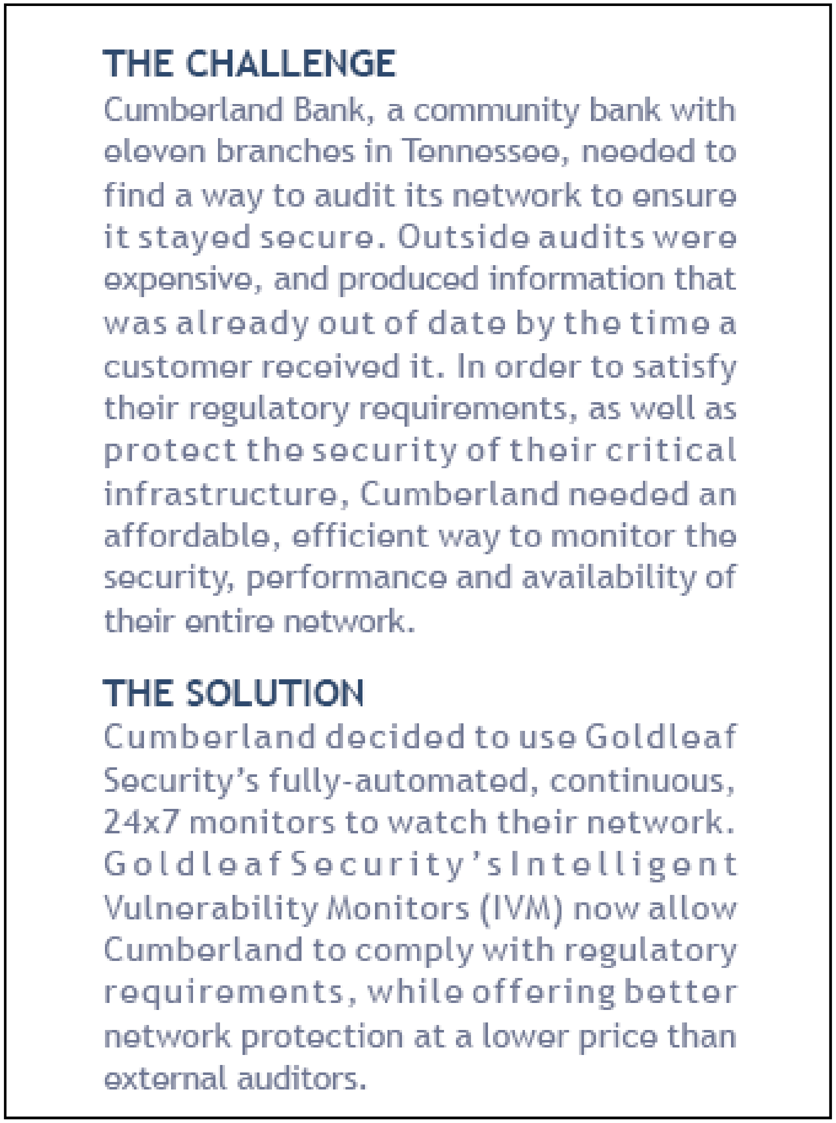


The Solution

RPC resolved its challenge by deploying McAfee Foundstone® Enterprise (including the modules for threat correlation and remediation) and McAfee Secure Internet Gateway appliances into its layered security architecture. In integrating Secure Internet Gateway, RPC was able to leverage the power of centralized security management within ePO, thereby delivering operational efficiency. Secure Internet Gateway keeps its users productive by blocking viruses, managing access to non-business sites and peer-to-peer file sharing, filtering content, and preventing inappropriate web usage.

Source: *http://i.i.com.com/*

Cumberland Bank Find Solution to Monitor the Security and Performance



THE CHALLENGE

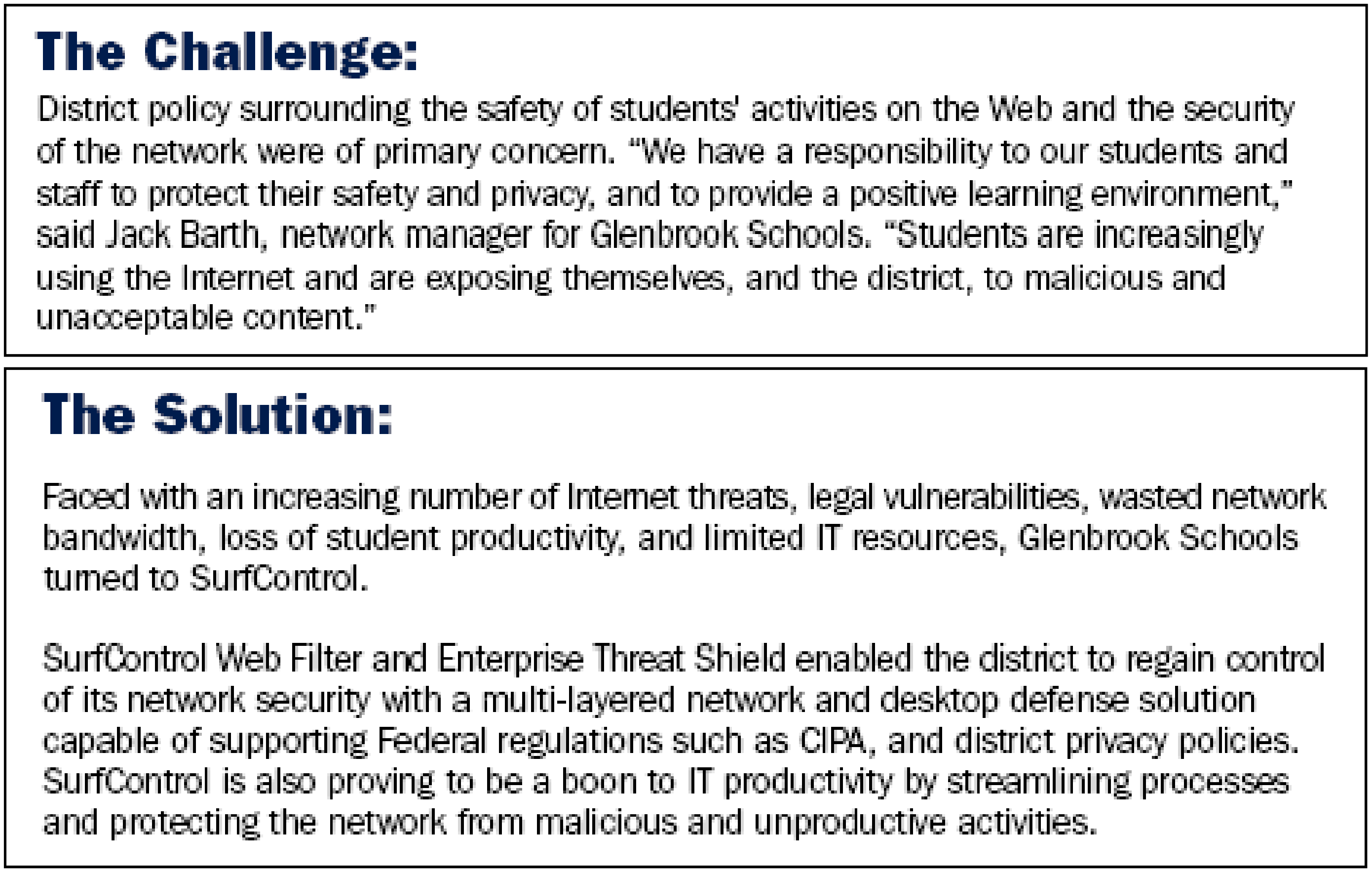
Cumberland Bank, a community bank with eleven branches in Tennessee, needed to find a way to audit its network to ensure it stayed secure. Outside audits were expensive, and produced information that was already out of date by the time a customer received it. In order to satisfy their regulatory requirements, as well as protect the security of their critical infrastructure, Cumberland needed an affordable, efficient way to monitor the security, performance and availability of their entire network.

THE SOLUTION

Cumberland decided to use Goldleaf Security's fully-automated, continuous, 24x7 monitors to watch their network. Goldleaf Security's Intelligent Vulnerability Monitors (IVM) now allow Cumberland to comply with regulatory requirements, while offering better network protection at a lower price than external auditors.

Source: *http://www.goldleaf.com/*

SurfControl Enterprise Protection Suite Protects Thousands at Glenbrook Schools Against Internet Dangers



The Challenge:

District policy surrounding the safety of students' activities on the Web and the security of the network were of primary concern. "We have a responsibility to our students and staff to protect their safety and privacy, and to provide a positive learning environment," said Jack Barth, network manager for Glenbrook Schools. "Students are increasingly using the Internet and are exposing themselves, and the district, to malicious and unacceptable content."

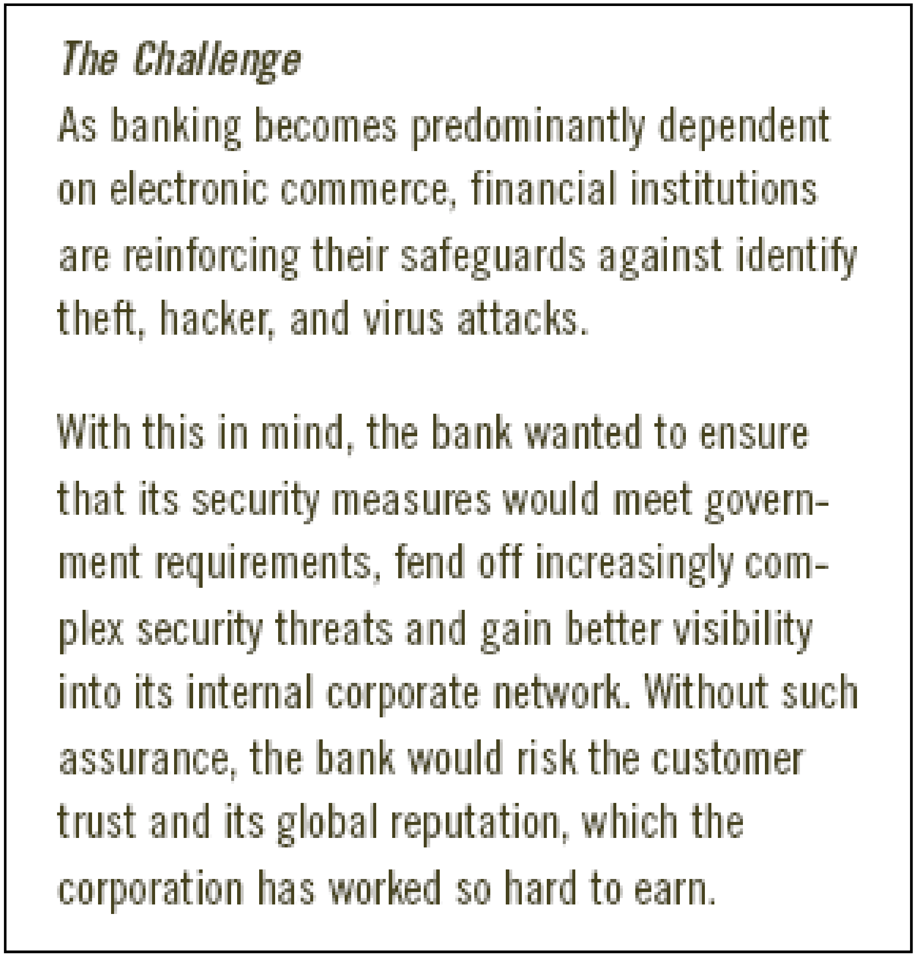
The Solution:

Faced with an increasing number of Internet threats, legal vulnerabilities, wasted network bandwidth, loss of student productivity, and limited IT resources, Glenbrook Schools turned to SurfControl.

SurfControl Web Filter and Enterprise Threat Shield enabled the district to regain control of its network security with a multi-layered network and desktop defense solution capable of supporting Federal regulations such as CIPA, and district privacy policies. SurfControl is also proving to be a boon to IT productivity by streamlining processes and protecting the network from malicious and unproductive activities.

Source: *http://www.surfcontrol.com/*

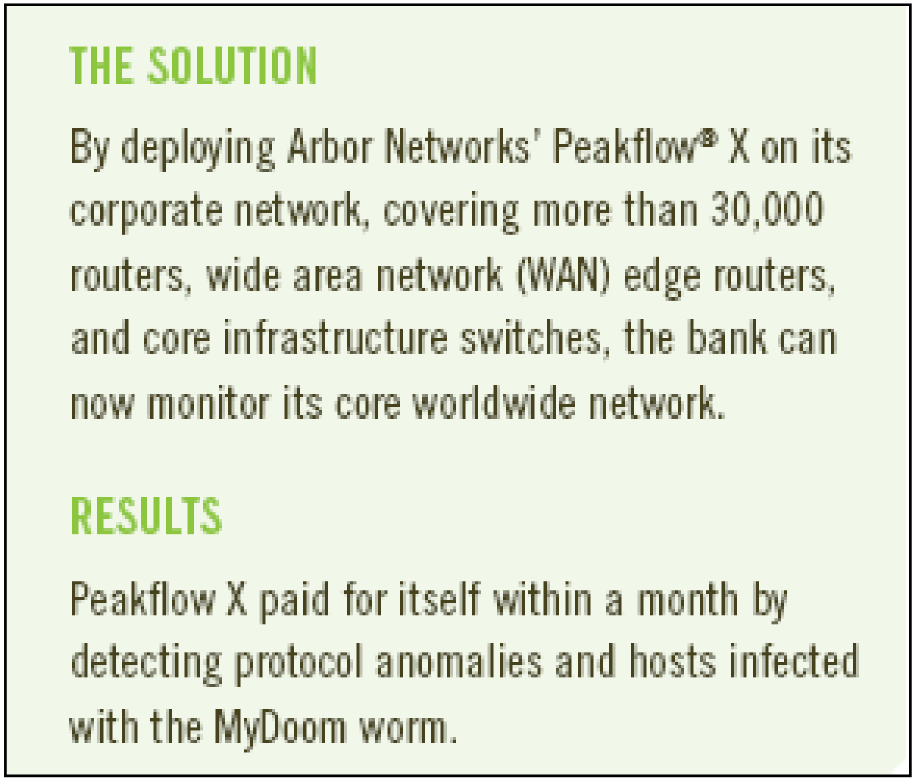
Arbor Uncovers Worm Infections Inside One of the World’s Largest Banks



The Challenge

As banking becomes predominantly dependent on electronic commerce, financial institutions are reinforcing their safeguards against identify theft, hacker, and virus attacks.

With this in mind, the bank wanted to ensure that its security measures would meet government requirements, fend off increasingly complex security threats and gain better visibility into its internal corporate network. Without such assurance, the bank would risk the customer trust and its global reputation, which the corporation has worked so hard to earn.



THE SOLUTION

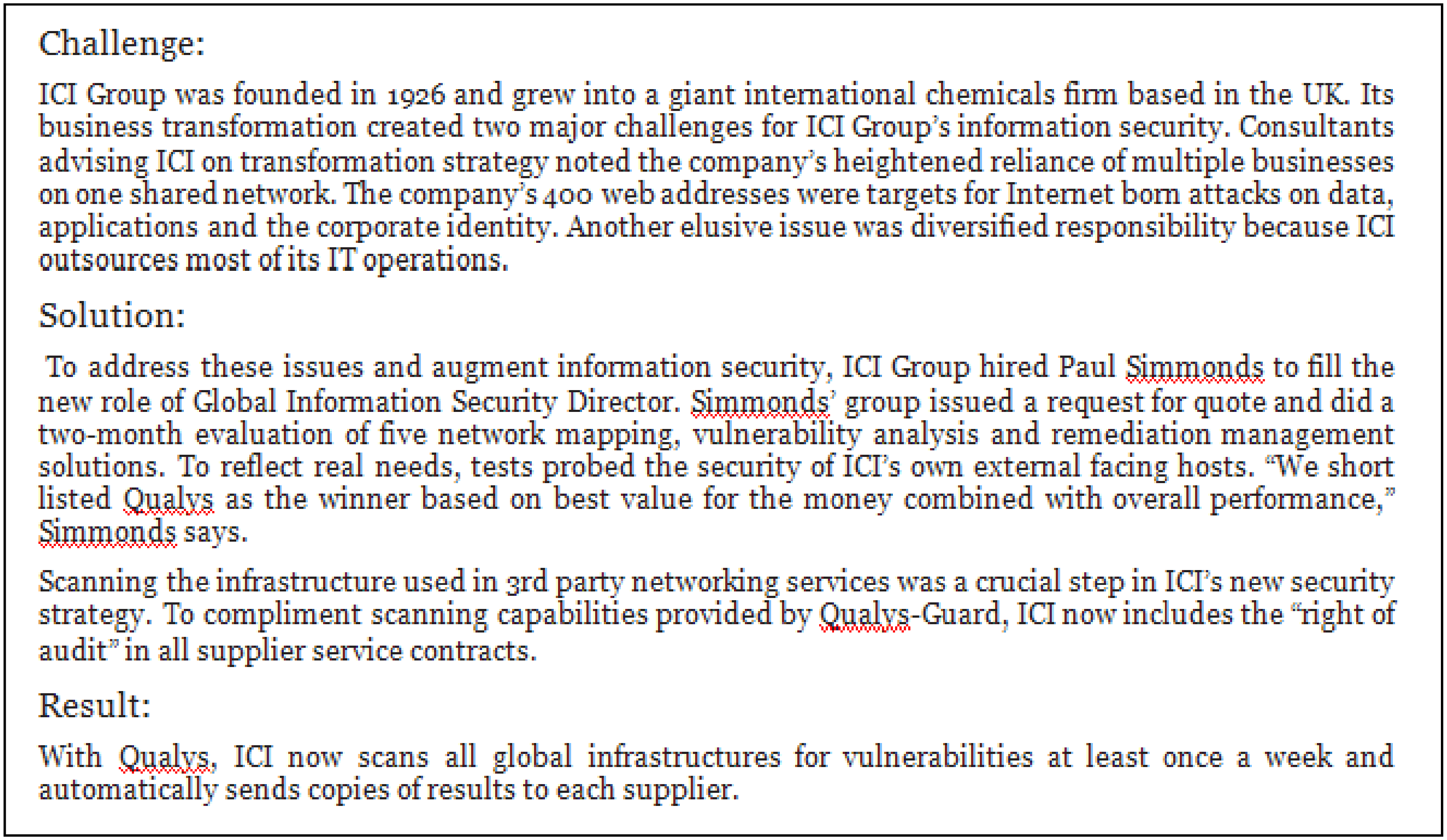
By deploying Arbor Networks' Peakflow® X on its corporate network, covering more than 30,000 routers, wide area network (WAN) edge routers, and core infrastructure switches, the bank can now monitor its core worldwide network.

RESULTS

Peakflow X paid for itself within a month by detecting protocol anomalies and hosts infected with the MyDoom worm.

Source: *http://www.arbornetworks.com/*

Imperial Chemical Industries PLC - Enforcing Security SLAs of Outsourcers



Challenge:

ICI Group was founded in 1926 and grew into a giant international chemicals firm based in the UK. Its business transformation created two major challenges for ICI Group's information security. Consultants advising ICI on transformation strategy noted the company's heightened reliance of multiple businesses on one shared network. The company's 400 web addresses were targets for Internet born attacks on data, applications and the corporate identity. Another elusive issue was diversified responsibility because ICI outsources most of its IT operations.

Solution:

To address these issues and augment information security, ICI Group hired Paul Simmonds to fill the new role of Global Information Security Director. Simmonds' group issued a request for quote and did a two-month evaluation of five network mapping, vulnerability analysis and remediation management solutions. To reflect real needs, tests probed the security of ICI's own external facing hosts. "We short listed Qualys as the winner based on best value for the money combined with overall performance," Simmonds says.

Scanning the infrastructure used in 3rd party networking services was a crucial step in ICI's new security strategy. To compliment scanning capabilities provided by Qualys-Guard, ICI now includes the "right of audit" in all supplier service contracts.

Result:

With Qualys, ICI now scans all global infrastructures for vulnerabilities at least once a week and automatically sends copies of results to each supplier.

Source: *http://www.qualys.com/*

Penetration Testing: Case Study

For obvious reasons, most users are unwilling to speak on the record of their experiences of penetration testing, but the head of one company involved in online gambling was prepared to do so.

His first experience of using an outside company to do penetration testing should have filled him with confidence. "The company did a test for us last year and found no faults at all.As far as they were concerned, we had no security worries.To be honest,that was the worst kind of report I could have had,"he says.

Unsatisfied, he followed it up this year with a second test, this time by ProCheckup (www.procheckup.com), a two-year-old privately-owned company that had been recommended to him.

ProCheckup runs a hosted service based in London where it will simulate hacker attacks on the client's systems. Rather than using the readily available open source tools favored by many companies, the ProChecknet service is built on ProCheckup's own technology, and incorporates a high level of artificial intelligence to mimic the cunning ways of a real hacker. For example, it can use polymorphic code to disguise URL strings and thereby pass unnoticed through an intrusion detection system.

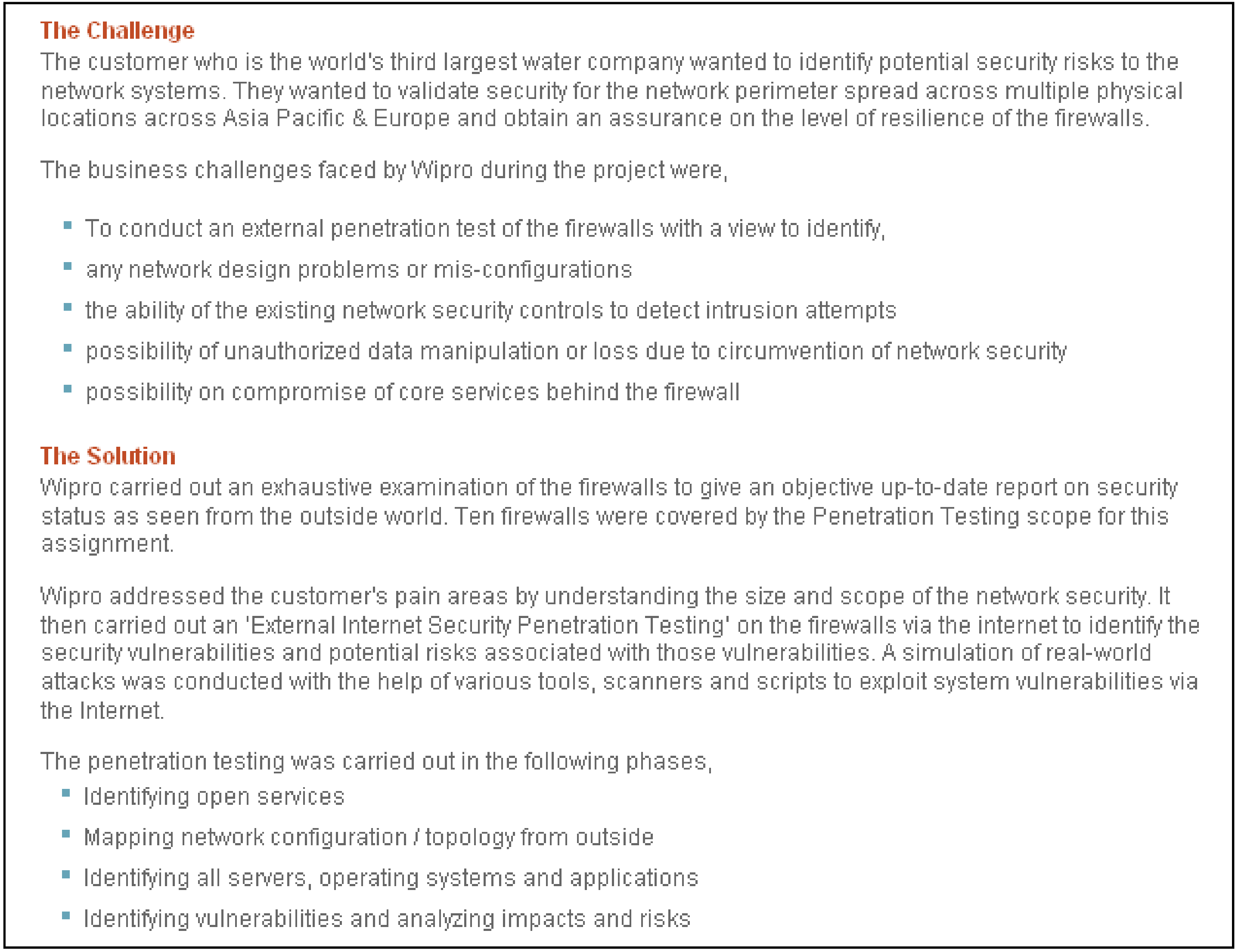
Instead of bombarding the systems with attacks in the hope that one will get through, it does an initial sweep of the systems and focuses on inflicting the kinds of attacks that are most likely to succeed.

The approach certainly worked for our anonymous user. "They tore the system to pieces. That was purely on sniffing. We operate 24x7 so the testers could not run any exploits or denial-of-service attacks. But they did find a lot of stuff, such as directories that were visible to the outside world with read and write permissions. They were eventually able to tell every operating system we were running, all the systems, what version of software, what fixes had been applied and what had not. It was quite scary."

Importantly, he did not have to wait until the end of the test to get the bad news. Each time a serious weakness was exposed, ProCheckup alerted him and provided a fix. These were then incorporated in the final report, alongside less serious flaws.

Source: *http://www.procheckup.com/*

Security Penetration Testing



The Challenge

The customer who is the world's third largest water company wanted to identify potential security risks to the network systems. They wanted to validate security for the network perimeter spread across multiple physical locations across Asia Pacific & Europe and obtain an assurance on the level of resilience of the firewalls.

The business challenges faced by Wipro during the project were,

- To conduct an external penetration test of the firewalls with a view to identify,
- any network design problems or mis-configurations
- the ability of the existing network security controls to detect intrusion attempts
- possibility of unauthorized data manipulation or loss due to circumvention of network security
- possibility on compromise of core services behind the firewall

The Solution

Wipro carried out an exhaustive examination of the firewalls to give an objective up-to-date report on security status as seen from the outside world. Ten firewalls were covered by the Penetration Testing scope for this assignment.

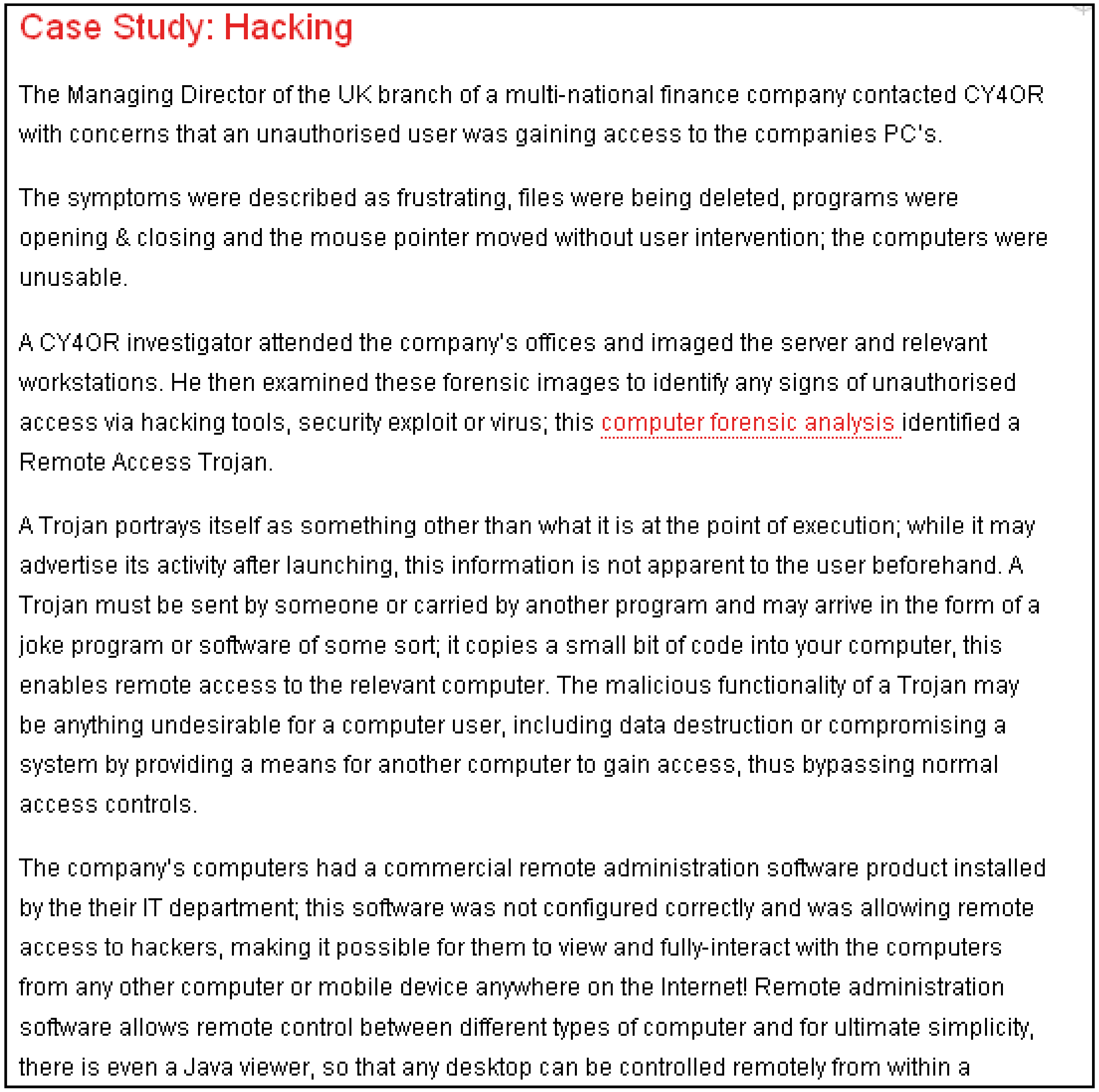
Wipro addressed the customer's pain areas by understanding the size and scope of the network security. It then carried out an 'External Internet Security Penetration Testing' on the firewalls via the internet to identify the security vulnerabilities and potential risks associated with those vulnerabilities. A simulation of real-world attacks was conducted with the help of various tools, scanners and scripts to exploit system vulnerabilities via the Internet.

The penetration testing was carried out in the following phases,

- Identifying open services
- Mapping network configuration / topology from outside
- Identifying all servers, operating systems and applications
- Identifying vulnerabilities and analyzing impacts and risks

Source: *http://wipro.com/*

Hacking Case Study



Case Study: Hacking

The Managing Director of the UK branch of a multi-national finance company contacted CY4OR with concerns that an unauthorised user was gaining access to the companies PC's.

The symptoms were described as frustrating, files were being deleted, programs were opening & closing and the mouse pointer moved without user intervention; the computers were unusable.

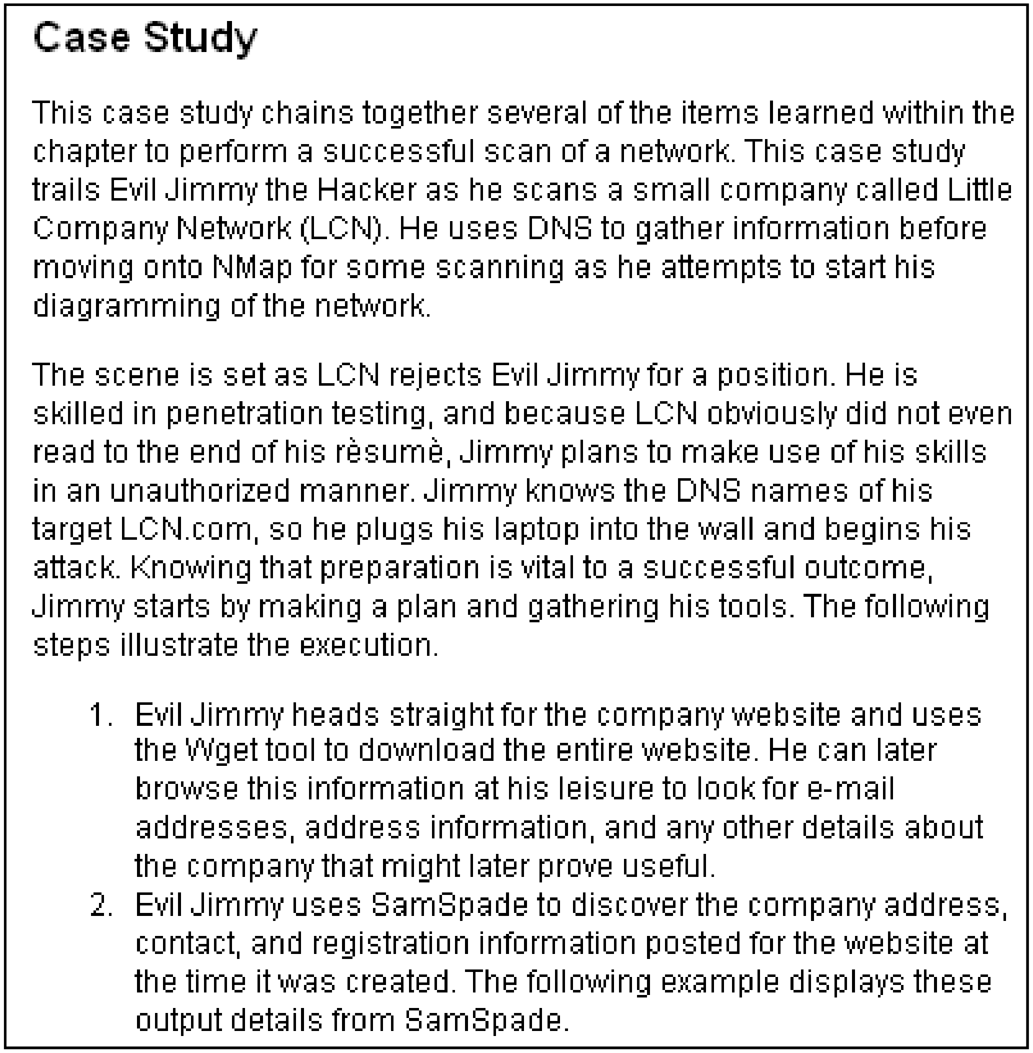
A CY4OR investigator attended the company's offices and imaged the server and relevant workstations. He then examined these forensic images to identify any signs of unauthorised access via hacking tools, security exploit or virus; this computer forensic analysis identified a Remote Access Trojan.

A Trojan portrays itself as something other than what it is at the point of execution; while it may advertise its activity after launching, this information is not apparent to the user beforehand. A Trojan must be sent by someone or carried by another program and may arrive in the form of a joke program or software of some sort; it copies a small bit of code into your computer, this enables remote access to the relevant computer. The malicious functionality of a Trojan may be anything undesirable for a computer user, including data destruction or compromising a system by providing a means for another computer to gain access, thus bypassing normal access controls.

The company's computers had a commercial remote administration software product installed by the their IT department; this software was not configured correctly and was allowing remote access to hackers, making it possible for them to view and fully-interact with the computers from any other computer or mobile device anywhere on the Internet! Remote administration software allows remote control between different types of computer and for ultimate simplicity, there is even a Java viewer, so that any desktop can be controlled remotely from within a

Source: *http://www.cy4or.co.uk/*

Evil Jimmy the Hacker as He Scans a Small Company Called Little Company Network (LCN)



Case Study

This case study chains together several of the items learned within the chapter to perform a successful scan of a network. This case study trails Evil Jimmy the Hacker as he scans a small company called Little Company Network (LCN). He uses DNS to gather information before moving onto NMap for some scanning as he attempts to start his diagramming of the network.

The scene is set as LCN rejects Evil Jimmy for a position. He is skilled in penetration testing, and because LCN obviously did not even read to the end of his rèsumè, Jimmy plans to make use of his skills in an unauthorized manner. Jimmy knows the DNS names of his target LCN.com, so he plugs his laptop into the wall and begins his attack. Knowing that preparation is vital to a successful outcome, Jimmy starts by making a plan and gathering his tools. The following steps illustrate the execution.

1. Evil Jimmy heads straight for the company website and uses the Wget tool to download the entire website. He can later browse this information at his leisure to look for e-mail addresses, address information, and any other details about the company that might later prove useful.
2. Evil Jimmy uses SamSpade to discover the company address, contact, and registration information posted for the website at the time it was created. The following example displays these output details from SamSpade.

Source: *http://www.ciscopress.com/*

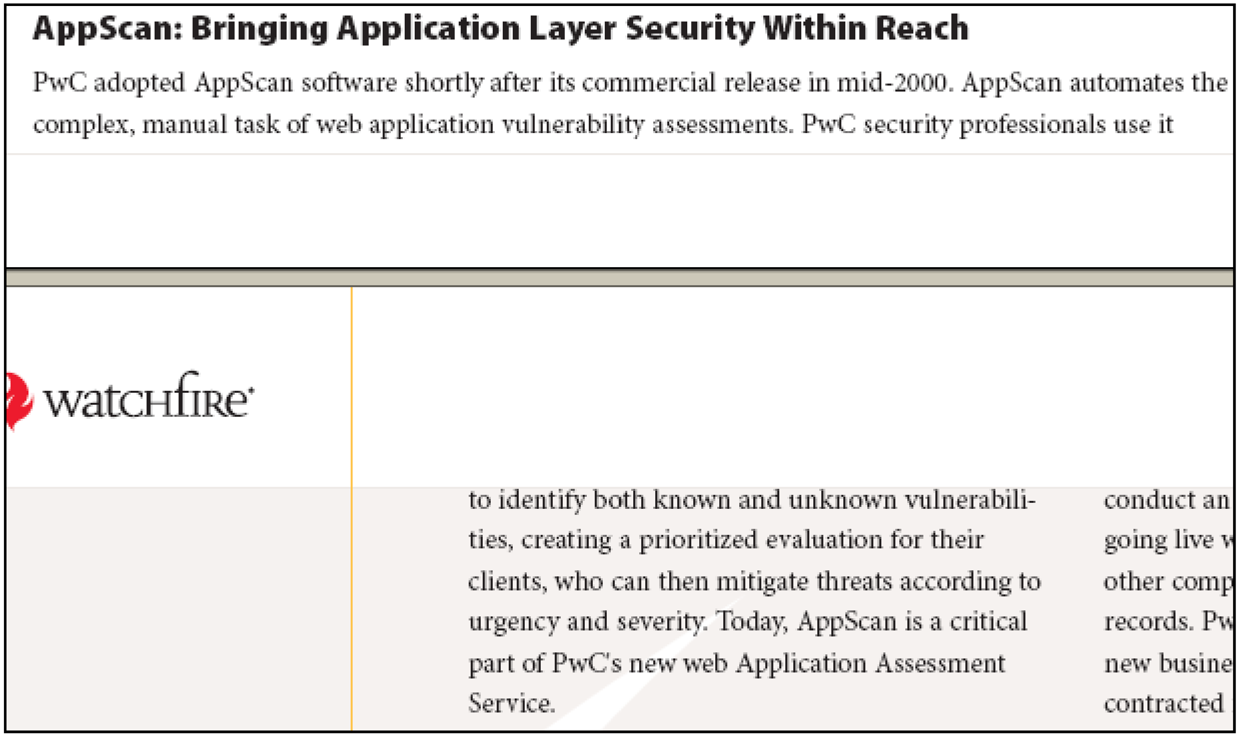
PwC Integrates AppScan into Threat and Vulnerability Practice Enabling Rapid Application Security

THE CHALLENGE

PwC had growing demand from its clients to expand their risk assessment practice into web application vulnerability assessments and wanted an automated solution that would enable them to deliver its service efficiently.

THE BENEFIT

AppScan enables quick, accurate, flexible and efficient web application vulnerability assessments. Rapid and thorough assessment facilitates comprehensive application fixes, cost-effectively keeping businesses and information assets safe.



AppScan: Bringing Application Layer Security Within Reach

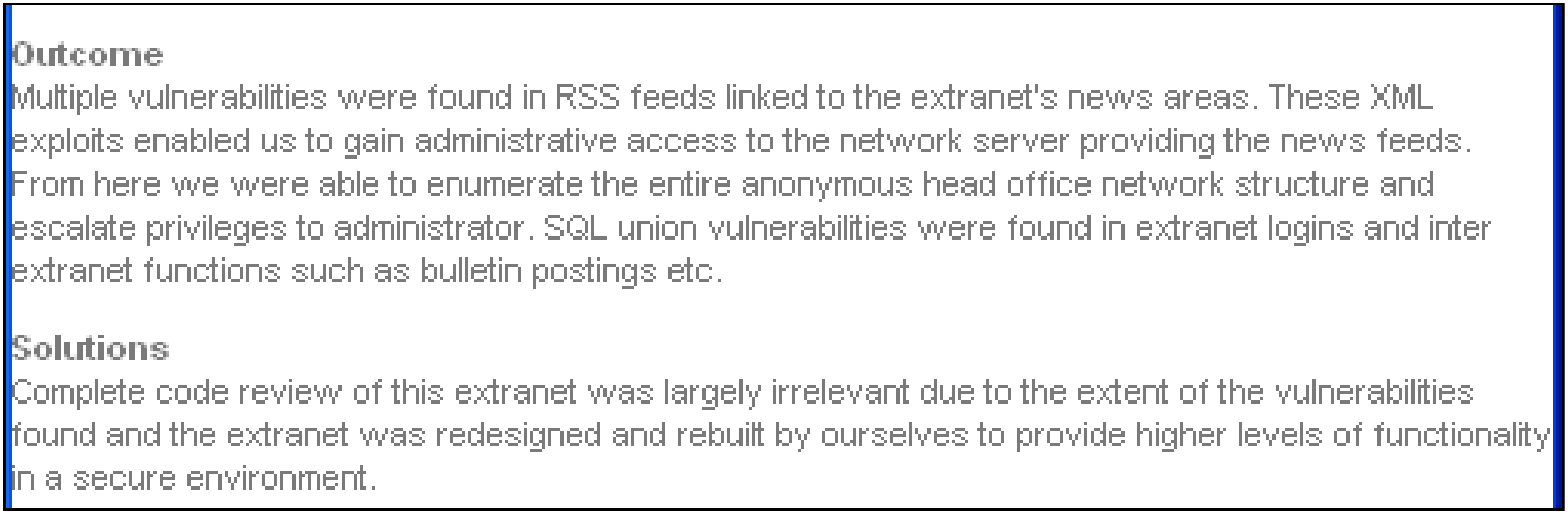
PwC adopted AppScan software shortly after its commercial release in mid-2000. AppScan automates the complex, manual task of web application vulnerability assessments. PwC security professionals use it

to identify both known and unknown vulnerabilities, creating a prioritized evaluation for their clients, who can then mitigate threats according to urgency and severity. Today, AppScan is a critical part of PwC's new web Application Assessment Service.

conduct an
going live w
other comp
records. Pw
new busine
contracted

Source: *http://www.watchfire.com/*

Case Study for RSS



Outcome

Multiple vulnerabilities were found in RSS feeds linked to the extranet's news areas. These XML exploits enabled us to gain administrative access to the network server providing the news feeds. From here we were able to enumerate the entire anonymous head office network structure and escalate privileges to administrator. SQL union vulnerabilities were found in extranet logins and inter extranet functions such as bulletin postings etc.

Solutions

Complete code review of this extranet was largely irrelevant due to the extent of the vulnerabilities found and the extranet was redesigned and rebuilt by ourselves to provide higher levels of functionality in a secure environment.

Source: *http://www.encription.co.uk/*

IT Consulting Firm Improves E-Mail Filtering, Increases Productivity With New Solution

Situation

Headquartered in Unterschleißheim, Germany, infoWAN Datenkommunikation GmbH is an IT solution provider that offers consulting, training, software development, and sales and distribution services for German businesses with complex IT infrastructures.

The company is a Microsoft® Gold Certified Partner and specializes in helping its customers deploy solutions based on Microsoft software, including the Active Directory® service, the Windows Server® 2003 operating system, Microsoft Exchange Server, Microsoft Forefront™ Security for Exchange Server, Microsoft Internet Security and Acceleration Server, Microsoft Office Communications Server, and the System Center family of products. "Our customers range from very small start-up companies to global enterprises with more than 100,000 employees, in many diverse industries," says Lars Riehn, Chief Executive Officer, infoWAN.

As with many organizations today, e-mail viruses and unsolicited e-mail are major concerns for infoWAN. In fact, on an average day, an infoWAN employee might receive more than 100 spam messages. "In the past, that number has been even higher for some of our sales staff," says Riehn. This spam includes e-mails promoting everything from online pharmacies to illegitimate stock recommendations and money-laundering job schemes. Recently, a wave of e-mails pretending to contain invoices and order confirmations, each containing some sort of malware, has swept over Germany. Some of those e-mails appeared to come from official German investigators (Bundeskriminalamt), informing recipients that they have been caught downloading illegal music files from the internet. "As you might imagine, we have all spent a lot of time trying to monitor these messages and clean up e-mail inboxes each day," adds Riehn. "Productivity has suffered as a result."

Solution

In late 2006, infoWAN deployed Microsoft Exchange Server 2007 as part of the Microsoft Rapid Deployment Program for the technology. At the same time, infoWAN was invited by the Microsoft Exchange Hosted Services team to implement an antispam and antivirus solution. Exchange Hosted Services, which requires no upfront capital investment, removes incoming e-mail threats before they reach the corporate firewall.

In particular, infoWAN decided to use the Exchange Hosted Filtering service, an extension of Exchange Server 2007 that operates over the Internet and provides organizations with hosted filtering for active spam and virus protection. The solution routes all incoming and outgoing e-mail messages through a Microsoft global data center network, where edge-blocking technology looks at the connections delivering incoming messages and blocks those sent from illegitimate senders.

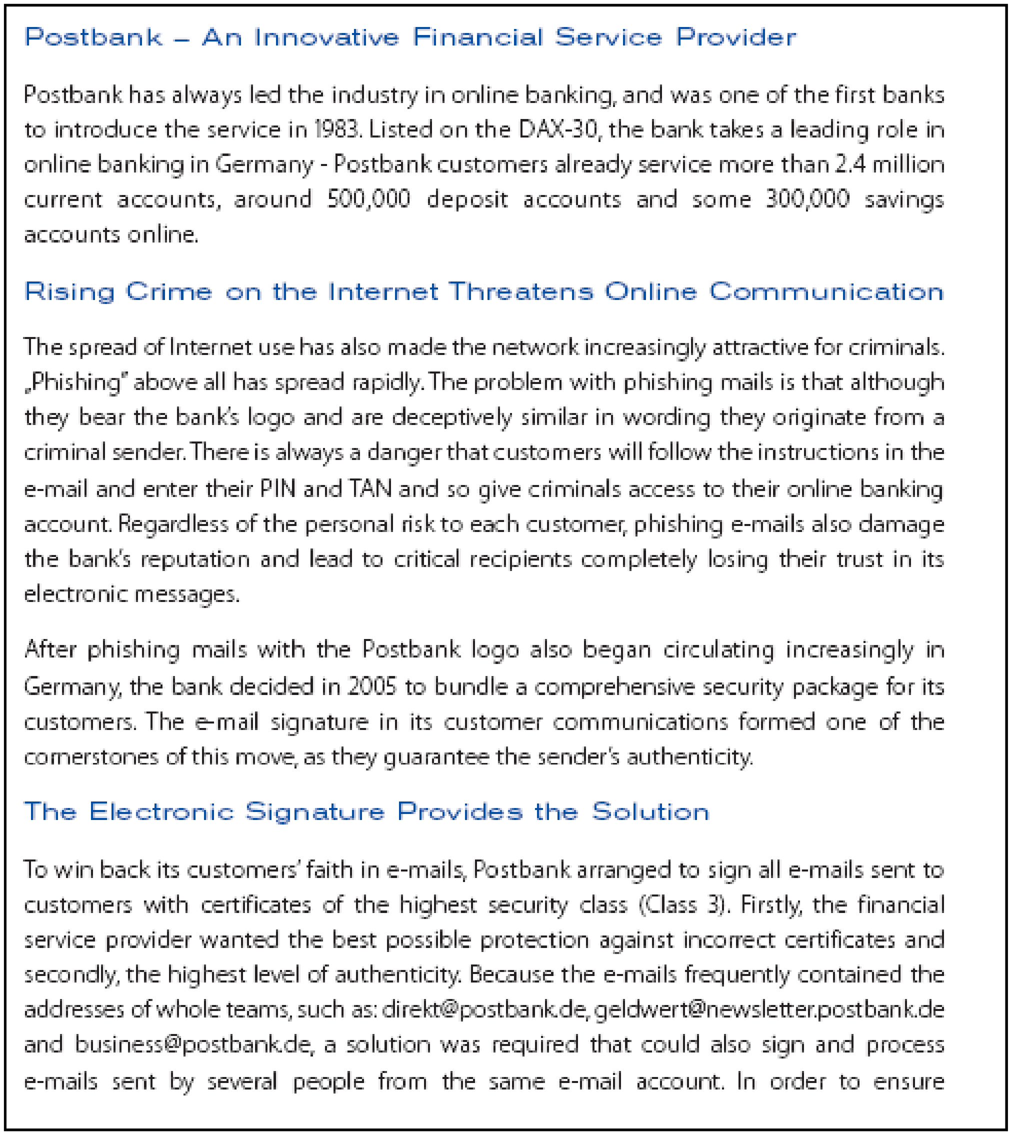
In early 2007, infoWAN began using both the e-mail queuing and the virus and spam filtering functions of the Exchange Hosted Filtering service. To coincide with its newly deployed Exchange Server 2007 environment, infoWAN also decided to use Microsoft Forefront Security for Exchange Server for antivirus protection. In addition, the company is making use of new edge server roles in Exchange Server 2007 that have enhanced security elements. "We wanted to use all the Exchange Server security features in addition to Exchange Hosted Services, to receive another level of protection," says Riehn.

Benefits

The Exchange Hosted Filtering Service provided infoWAN with an easy-to-deploy antispam and antivirus solution that is simple to manage. infoWAN now has much stronger e-mail filtering and queuing capabilities, and employees are more productive because they

Source: *http://download.microsoft.com/*

Postbank Signs Customer E-mails With Team Certificates From TC TrustCenter, To Protect its Customers Against Phishing



Postbank – An Innovative Financial Service Provider

Postbank has always led the industry in online banking, and was one of the first banks to introduce the service in 1983. Listed on the DAX-30, the bank takes a leading role in online banking in Germany - Postbank customers already service more than 2.4 million current accounts, around 500,000 deposit accounts and some 300,000 savings accounts online.

Rising Crime on the Internet Threatens Online Communication

The spread of Internet use has also made the network increasingly attractive for criminals. „Phishing" above all has spread rapidly. The problem with phishing mails is that although they bear the bank's logo and are deceptively similar in wording they originate from a criminal sender. There is always a danger that customers will follow the instructions in the e-mail and enter their PIN and TAN and so give criminals access to their online banking account. Regardless of the personal risk to each customer, phishing e-mails also damage the bank's reputation and lead to critical recipients completely losing their trust in its electronic messages.

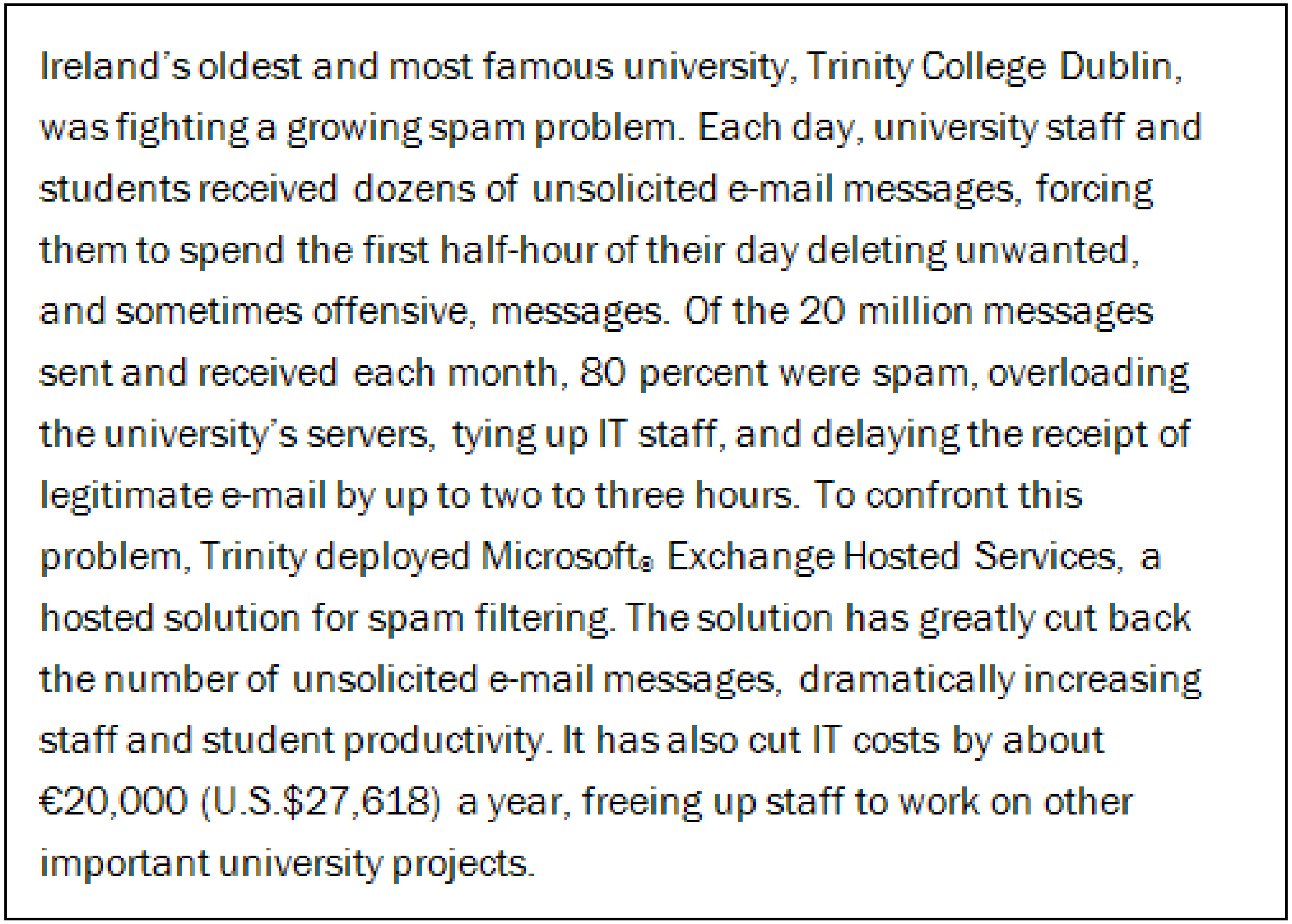
After phishing mails with the Postbank logo also began circulating increasingly in Germany, the bank decided in 2005 to bundle a comprehensive security package for its customers. The e-mail signature in its customer communications formed one of the cornerstones of this move, as they guarantee the sender's authenticity.

The Electronic Signature Provides the Solution

To win back its customers' faith in e-mails, Postbank arranged to sign all e-mails sent to customers with certificates of the highest security class (Class 3). Firstly, the financial service provider wanted the best possible protection against incorrect certificates and secondly, the highest level of authenticity. Because the e-mails frequently contained the addresses of whole teams, such as: direkt@postbank.de, geldwert@newsletter.postbank.de and business@postbank.de, a solution was required that could also sign and process e-mails sent by several people from the same e-mail account. In order to ensure

Source: *http://www.trustcenter.de/*

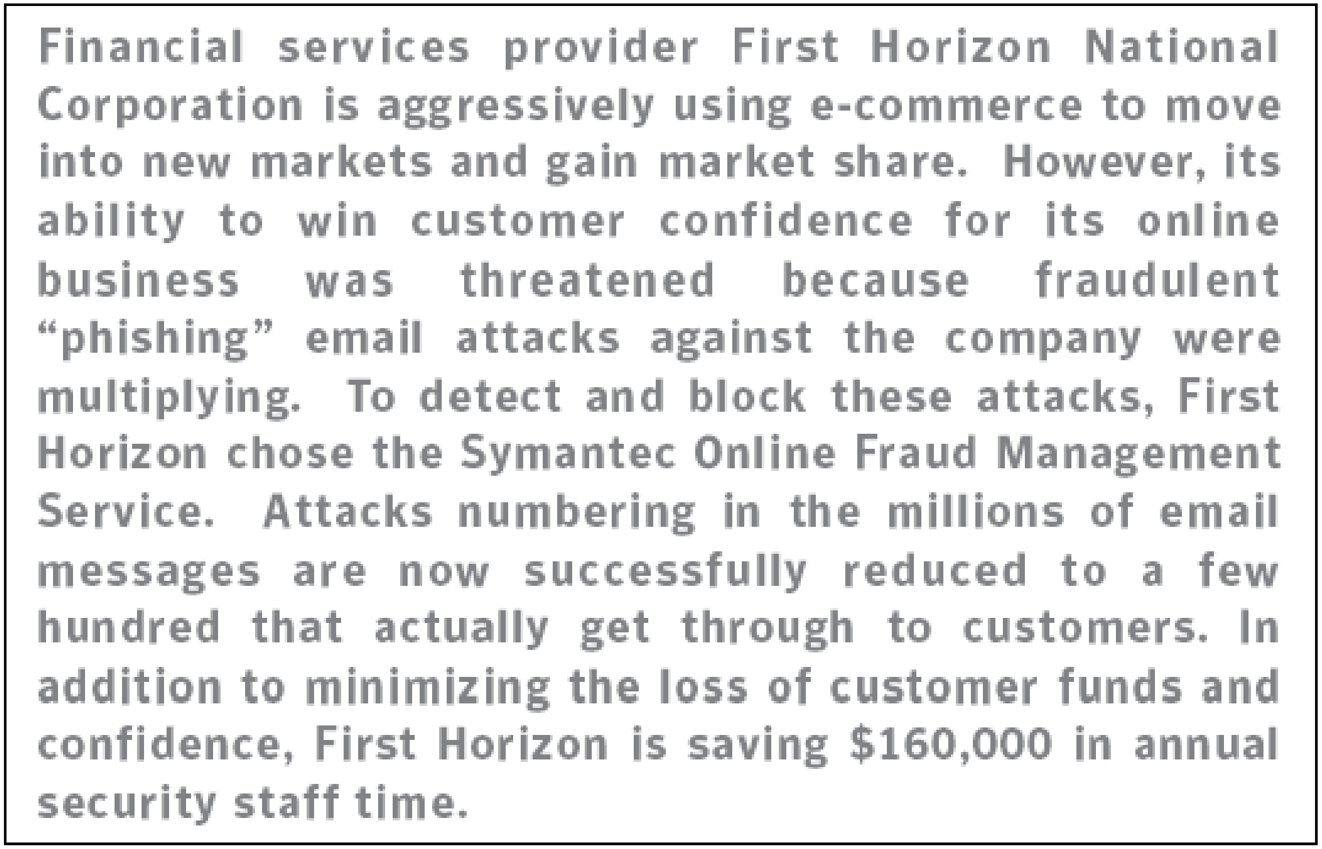
University Limits Spam, Reduces IT Costs With E-Mail Filtering Service



Ireland's oldest and most famous university, Trinity College Dublin, was fighting a growing spam problem. Each day, university staff and students received dozens of unsolicited e-mail messages, forcing them to spend the first half-hour of their day deleting unwanted, and sometimes offensive, messages. Of the 20 million messages sent and received each month, 80 percent were spam, overloading the university's servers, tying up IT staff, and delaying the receipt of legitimate e-mail by up to two to three hours. To confront this problem, Trinity deployed Microsoft® Exchange Hosted Services, a hosted solution for spam filtering. The solution has greatly cut back the number of unsolicited e-mail messages, dramatically increasing staff and student productivity. It has also cut IT costs by about €20,000 (U.S.$27,618) a year, freeing up staff to work on other important university projects.

Source: *http://download.microsoft.com/*

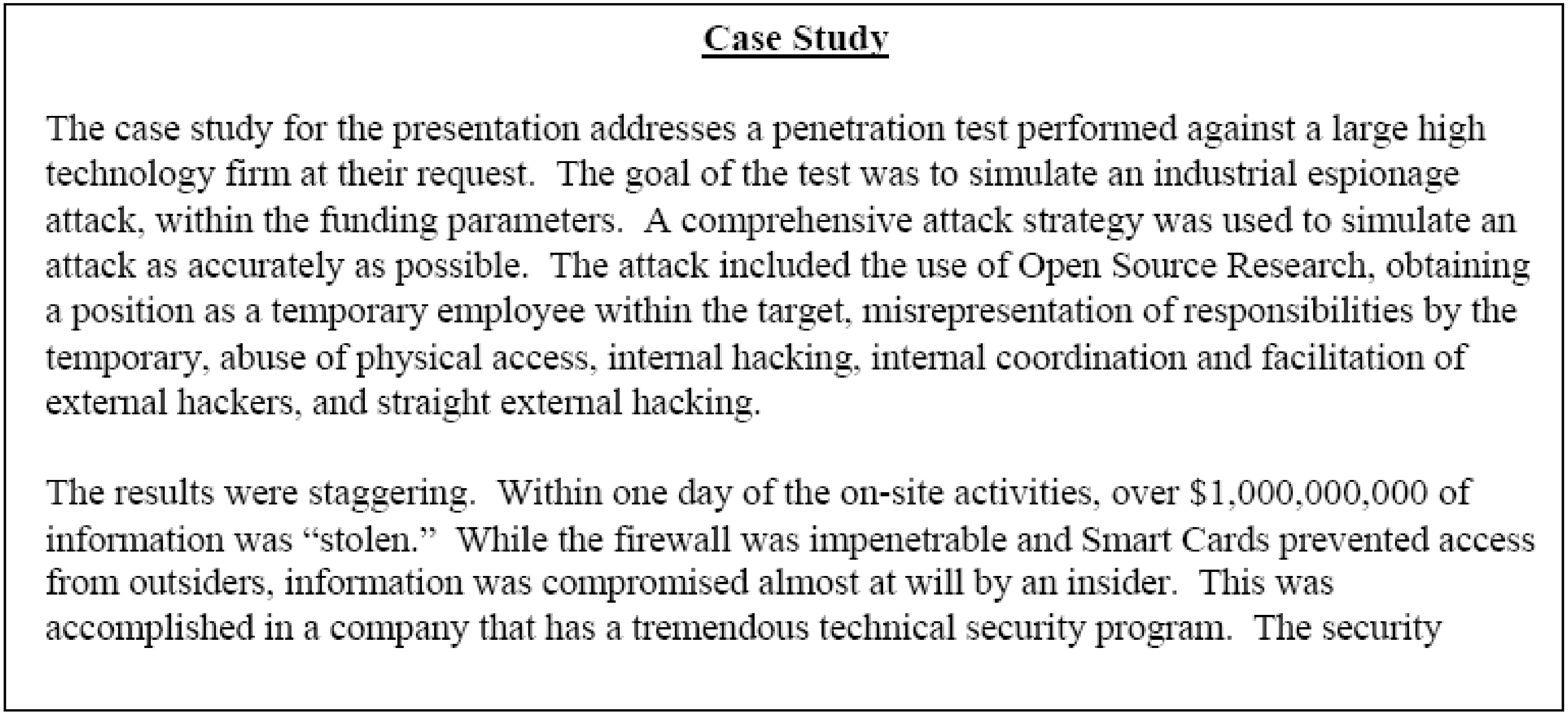
Hooking "Phishing" Emails Before They Reach Customers with Online Fraud Management Service



Financial services provider First Horizon National Corporation is aggressively using e-commerce to move into new markets and gain market share. However, its ability to win customer confidence for its online business was threatened because fraudulent "phishing" email attacks against the company were multiplying. To detect and block these attacks, First Horizon chose the Symantec Online Fraud Management Service. Attacks numbering in the millions of email messages are now successfully reduced to a few hundred that actually get through to customers. In addition to minimizing the loss of customer funds and confidence, First Horizon is saving $160,000 in annual security staff time.

Source: *http://eval.veritas.com/*

Corporate Espionage: Case Study



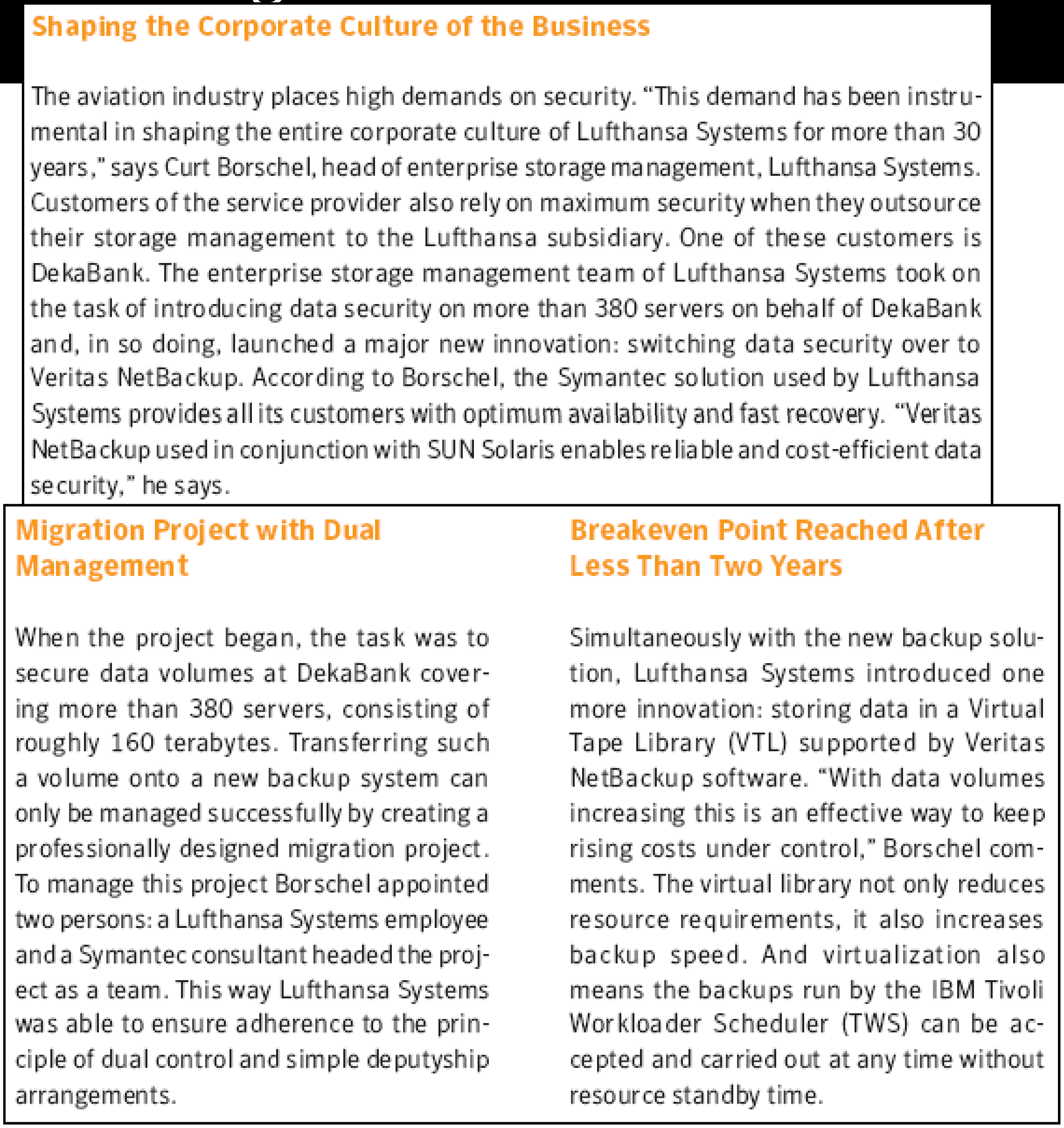
Case Study

The case study for the presentation addresses a penetration test performed against a large high technology firm at their request. The goal of the test was to simulate an industrial espionage attack, within the funding parameters. A comprehensive attack strategy was used to simulate an attack as accurately as possible. The attack included the use of Open Source Research, obtaining a position as a temporary employee within the target, misrepresentation of responsibilities by the temporary, abuse of physical access, internal hacking, internal coordination and facilitation of external hackers, and straight external hacking.

The results were staggering. Within one day of the on-site activities, over $1,000,000,000 of information was "stolen." While the firewall was impenetrable and Smart Cards prevented access from outsiders, information was compromised almost at will by an insider. This was accomplished in a company that has a tremendous technical security program. The security

Source: *http://csrc.nist.gov/*

Making Data Security a Top Priority for Leading IT Provider to the Airline Industry



Shaping the Corporate Culture of the Business

The aviation industry places high demands on security. “This demand has been instrumental in shaping the entire corporate culture of Lufthansa Systems for more than 30 years,” says Curt Borschel, head of enterprise storage management, Lufthansa Systems. Customers of the service provider also rely on maximum security when they outsource their storage management to the Lufthansa subsidiary. One of these customers is DekaBank. The enterprise storage management team of Lufthansa Systems took on the task of introducing data security on more than 380 servers on behalf of DekaBank and, in so doing, launched a major new innovation: switching data security over to Veritas NetBackup. According to Borschel, the Symantec solution used by Lufthansa Systems provides all its customers with optimum availability and fast recovery. “Veritas NetBackup used in conjunction with SUN Solaris enables reliable and cost-efficient data security,” he says.

Migration Project with Dual Management

When the project began, the task was to secure data volumes at DekaBank covering more than 380 servers, consisting of roughly 160 terabytes. Transferring such a volume onto a new backup system can only be managed successfully by creating a professionally designed migration project. To manage this project Borschel appointed two persons: a Lufthansa Systems employee and a Symantec consultant headed the project as a team. This way Lufthansa Systems was able to ensure adherence to the principle of dual control and simple deputyship arrangements.

Breakeven Point Reached After Less Than Two Years

Simultaneously with the new backup solution, Lufthansa Systems introduced one more innovation: storing data in a Virtual Tape Library (VTL) supported by Veritas NetBackup software. “With data volumes increasing this is an effective way to keep rising costs under control,” Borschel comments. The virtual library not only reduces resource requirements, it also increases backup speed. And virtualization also means the backups run by the IBM Tivoli Workloader Scheduler (TWS) can be accepted and carried out at any time without resource standby time.

Source: *http://eval.veritas.com/*

Eliminating Spam In Its Tracks with Multi-Layered Solutions from Symantec

The Challenge

Established in 1960, SEGA Corporation is a worldwide leader in interactive both inside and outside the home, encompassing consumer business, amusement machine sales, and amusement center operations. The company develops, publishes and distributes interactive entertainment software products for a variety of hardware platforms including PC, wireless devices, and those manufactured by Nintendo, Microsoft and Sony Computer Entertainment Inc. SEGA Corporation has 34 domestic and 28 overseas offices, and about 3,500 employees.

Spam was becoming an increasingly urgent problem for SEGA. With all domestic email environments integrated in one data center, all SEGA's Internet mail goes through one gateway. With a flow rate of about 3,000 emails an hour, SEGA IT staff discovered that about 70 percent of all mail received was spam. "SEGA's operations cannot work properly without email," says Mr. Takamitsu Shoji, Team Manager, Information Systems Department, SEGA Corporation. "So increasing spam posed a potential threat to the entire company."

The Solution

SEGA's IT team evaluated different anti-spam solutions from December 2005 to June 2006, testing six different products by renting one from each company and connecting it to the gateway for two weeks. Though the team evaluated each software solution with many factors in mind, detection error rate was particularly important—since the company planned to automatically delete spam, false positives would be unacceptable. Symantec™ Mail Security 8160 and 8260 models combined had the best detection error rate of all the solutions tested.

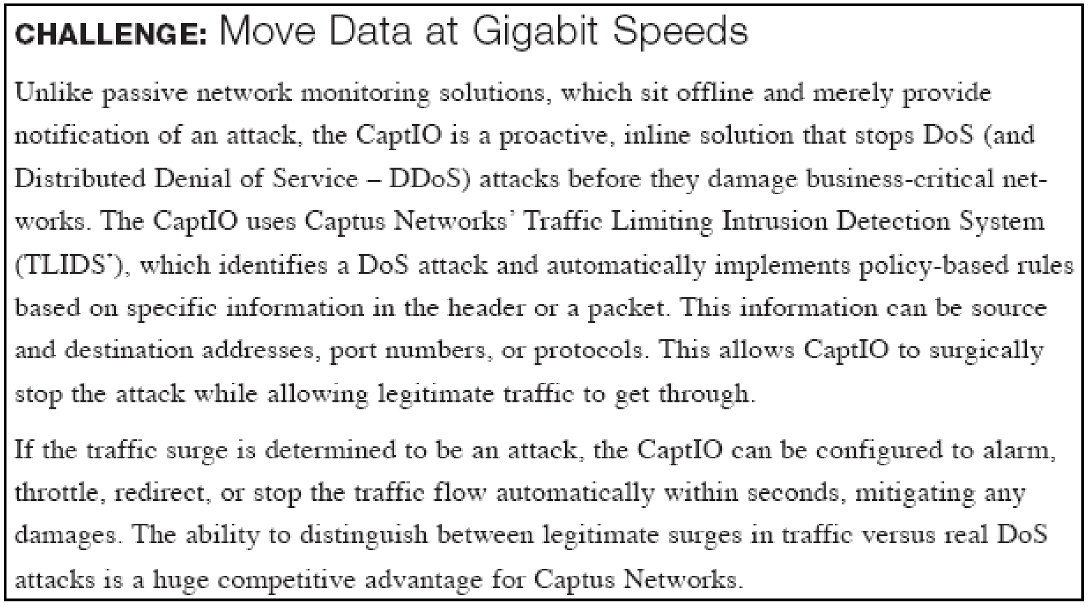
The Results

Since deployment, the multi-layered Mail Security continues to work with 0 false positives, and over 92 percent of English and non-English spam is deleted before it ever reaches users' inboxes. "End users from each department commented that they receive fewer spam," Mr. Shoji says.

Mail Security's accuracy allows SEGA to take this measure without fear of accidentally deleting vital information. Mr. Urai says, "With almost no chance of detection error, it allows us to deal with spam before it ever reaches users, preventing the loss of business efficiency."

Source: *http://eval.veritas.com/mktginfo/*

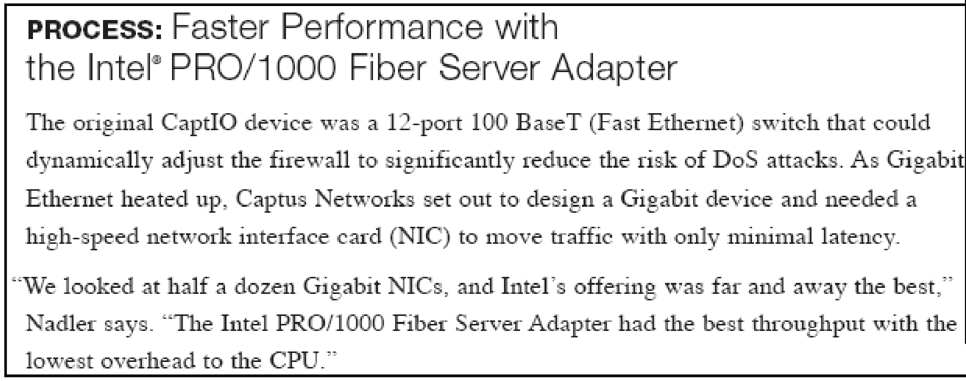
Captus Networks Helps Prevent Denial of Service Attacks with Intel® Network Adapters for Multi-gigabit Scalability



CHALLENGE: Move Data at Gigabit Speeds

Unlike passive network monitoring solutions, which sit offline and merely provide notification of an attack, the CaptIO is a proactive, inline solution that stops DoS (and Distributed Denial of Service – DDoS) attacks before they damage business-critical networks. The CaptIO uses Captus Networks' Traffic Limiting Intrusion Detection System (TLIDS®), which identifies a DoS attack and automatically implements policy-based rules based on specific information in the header or a packet. This information can be source and destination addresses, port numbers, or protocols. This allows CaptIO to surgically stop the attack while allowing legitimate traffic to get through.

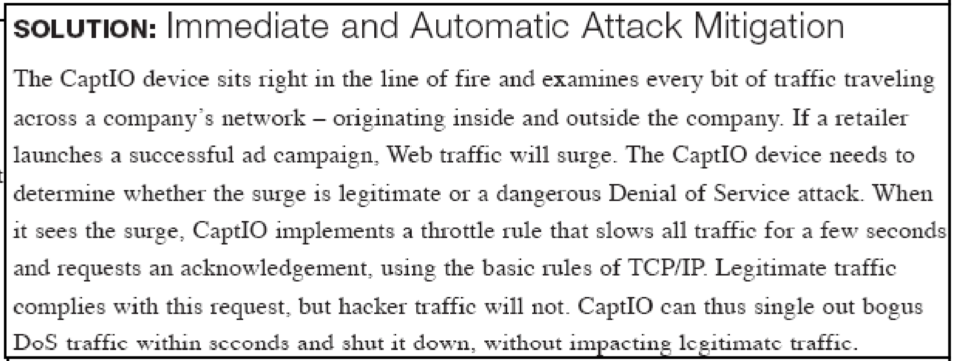
If the traffic surge is determined to be an attack, the CaptIO can be configured to alarm, throttle, redirect, or stop the traffic flow automatically within seconds, mitigating any damages. The ability to distinguish between legitimate surges in traffic versus real DoS attacks is a huge competitive advantage for Captus Networks.



PROCESS: Faster Performance with the Intel® PRO/1000 Fiber Server Adapter

The original CaptIO device was a 12-port 100 BaseT (Fast Ethernet) switch that could dynamically adjust the firewall to significantly reduce the risk of DoS attacks. As Gigabit Ethernet heated up, Captus Networks set out to design a Gigabit device and needed a high-speed network interface card (NIC) to move traffic with only minimal latency.

"We looked at half a dozen Gigabit NICs, and Intel's offering was far and away the best," Nadler says. "The Intel PRO/1000 Fiber Server Adapter had the best throughput with the lowest overhead to the CPU."

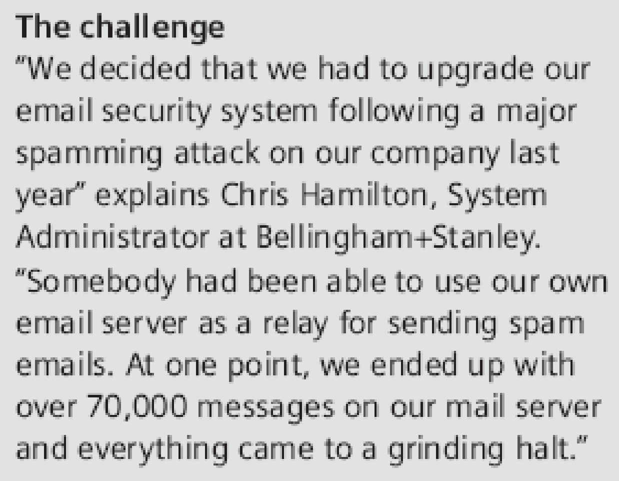


SOLUTION: Immediate and Automatic Attack Mitigation

The CaptIO device sits right in the line of fire and examines every bit of traffic traveling across a company's network – originating inside and outside the company. If a retailer launches a successful ad campaign, Web traffic will surge. The CaptIO device needs to determine whether the surge is legitimate or a dangerous Denial of Service attack. When it sees the surge, CaptIO implements a throttle rule that slows all traffic for a few seconds and requests an acknowledgement, using the basic rules of TCP/IP. Legitimate traffic complies with this request, but hacker traffic will not. CaptIO can thus single out bogus DoS traffic within seconds and shut it down, without impacting legitimate traffic.

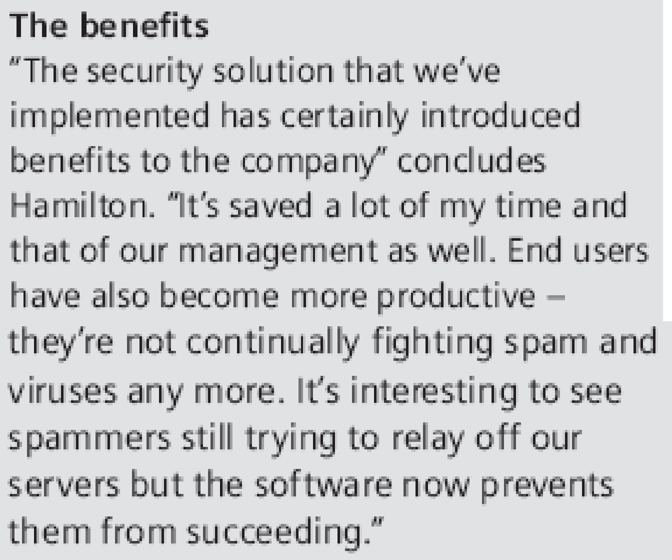
Source: *http://www.intel.com/network/*

Bellingham+Stanley Implement Integrated Solution For Web And Email Security



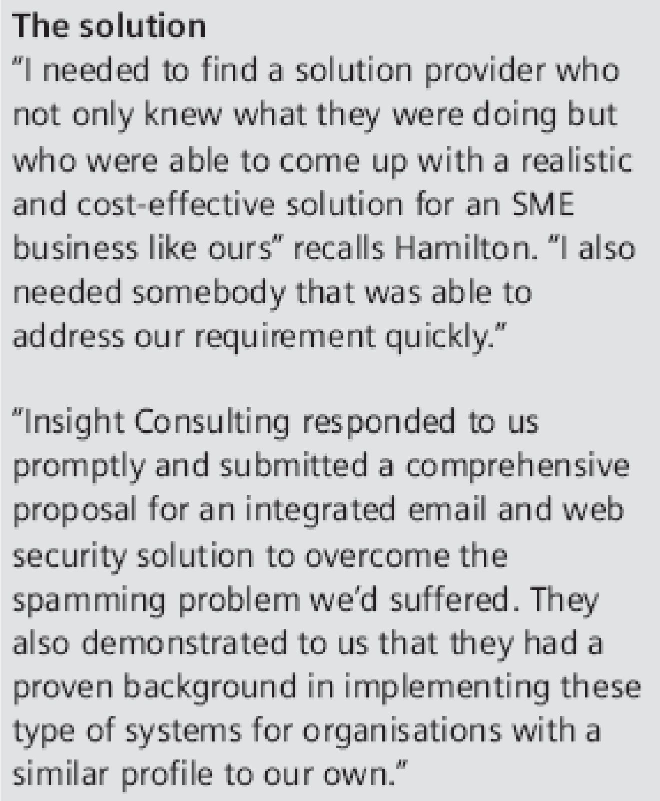
The challenge

"We decided that we had to upgrade our email security system following a major spamming attack on our company last year" explains Chris Hamilton, System Administrator at Bellingham+Stanley. "Somebody had been able to use our own email server as a relay for sending spam emails. At one point, we ended up with over 70,000 messages on our mail server and everything came to a grinding halt."



The benefits

"The security solution that we've implemented has certainly introduced benefits to the company" concludes Hamilton. "It's saved a lot of my time and that of our management as well. End users have also become more productive – they're not continually fighting spam and viruses any more. It's interesting to see spammers still trying to relay off our servers but the software now prevents them from succeeding."



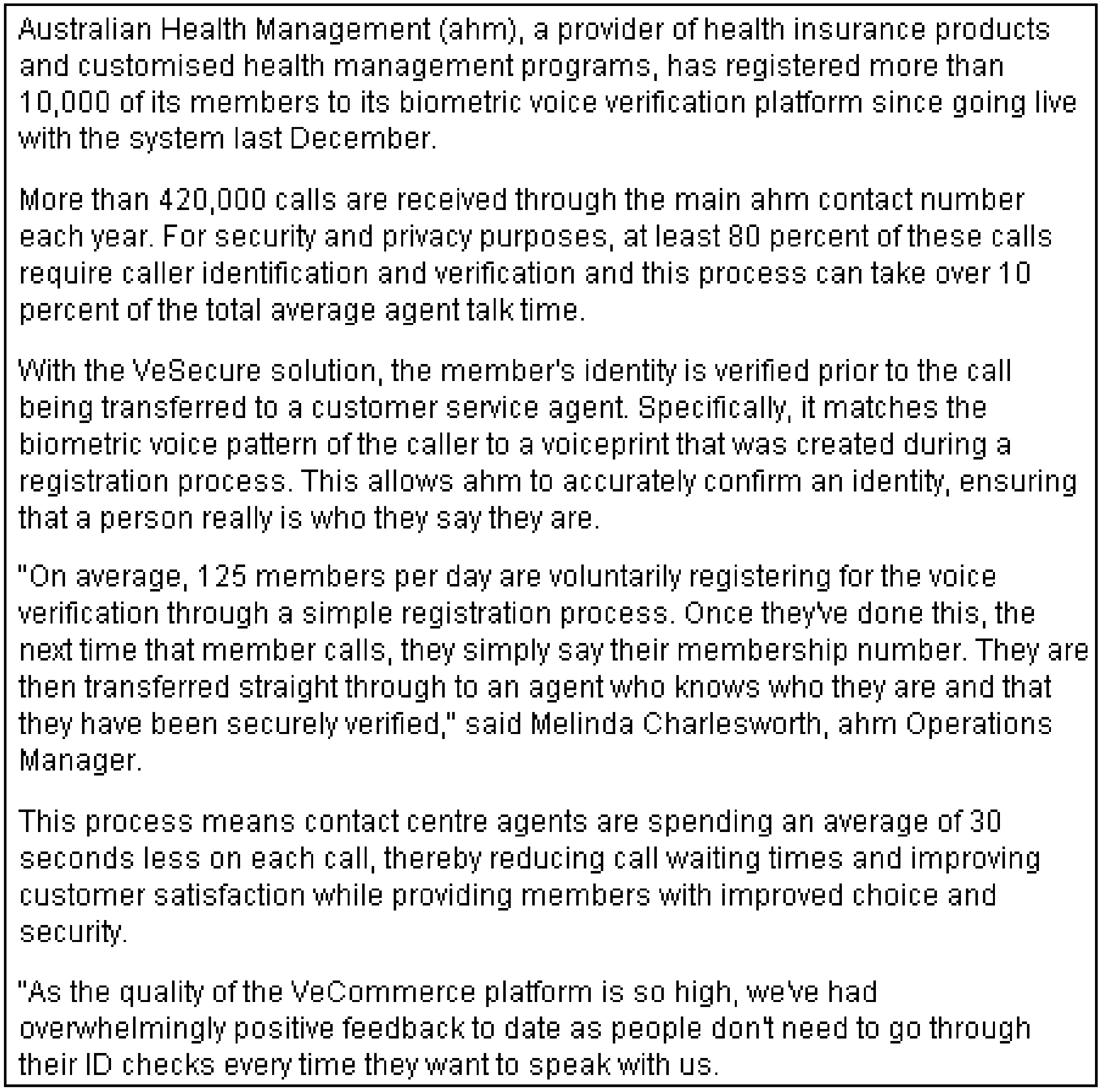
The solution

"I needed to find a solution provider who not only knew what they were doing but who were able to come up with a realistic and cost-effective solution for an SME business like ours" recalls Hamilton. "I also needed somebody that was able to address our requirement quickly."

"Insight Consulting responded to us promptly and submitted a comprehensive proposal for an integrated email and web security solution to overcome the spamming problem we'd suffered. They also demonstrated to us that they had a proven background in implementing these type of systems for organisations with a similar profile to our own."

Source: *http://www.insight.co.uk/files/*

Australian Company Implements World’s Largest Biometric Voice ID System



Australian Health Management (ahm), a provider of health insurance products and customised health management programs, has registered more than 10,000 of its members to its biometric voice verification platform since going live with the system last December.

More than 420,000 calls are received through the main ahm contact number each year. For security and privacy purposes, at least 80 percent of these calls require caller identification and verification and this process can take over 10 percent of the total average agent talk time.

With the VeSecure solution, the member's identity is verified prior to the call being transferred to a customer service agent. Specifically, it matches the biometric voice pattern of the caller to a voiceprint that was created during a registration process. This allows ahm to accurately confirm an identity, ensuring that a person really is who they say they are.

"On average, 125 members per day are voluntarily registering for the voice verification through a simple registration process. Once they've done this, the next time that member calls, they simply say their membership number. They are then transferred straight through to an agent who knows who they are and that they have been securely verified," said Melinda Charlesworth, ahm Operations Manager.

This process means contact centre agents are spending an average of 30 seconds less on each call, thereby reducing call waiting times and improving customer satisfaction while providing members with improved choice and security.

"As the quality of the VeCommerce platform is so high, we've had overwhelmingly positive feedback to date as people don't need to go through their ID checks every time they want to speak with us.

Source: *http://www.searchsecurity.com.au/*

Summary

This module has drawn various cases of information theft and security around the world

It draws a picture of various practical applications that many companies have adopted to enhance security of their assets