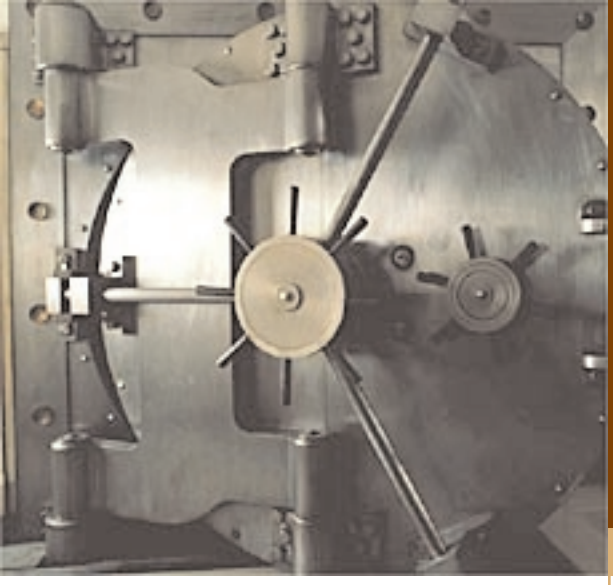


PRICEWATERHOUSECOOPERS

The Secure Solution

A monthly newsletter brought to you by the Security & Privacy Practice of PricewaterhouseCoopers

VOLUME 18, SEPTEMBER 2003

In This Issue:

This edition of *The Secure Solution*, a monthly newsletter from the Security & Privacy Practice of PricewaterhouseCoopers, includes the following: a thought leadership article on the continuing spread of email viruses; an Identity Management case study; a spotlight on a world-class Alliance Vendor; plus upcoming events covering worldwide security issues.

Each month, we will produce a newsletter providing timely, topical information about security issues. If you should have any questions about our newsletter or our Security & Privacy Practice, please contact one of our marketing professionals listed below.

Who To Contact:

James F. Kelly
Americas Marketing Leader
Global Risk Management Solutions
PricewaterhouseCoopers
415.498.5376
james.f.kelly@us.pwc.com

Kate Oliver
Marketing Director
Security and Privacy Practice
PricewaterhouseCoopers
860.241.7333
kathryn.oliver@us.pwc.com

Cutting Off The Worms' Heads: Preventing Viruses, Intrusions and Outages on Your Network

Call them worms. Call them viruses. Call them Trojan Horses. Call them malicious SPAM. Call them a form of cyberterrorism. Let's call a stop or at least put up a stronger barrier to these variant viruses that have been so prevalent this summer by having corporate IT directors step up their levels of enterprise security.

August was the worst month ever for viruses — even after more than 71,000 are known to already exist. Between Sobig.F, MS Blaster (AKA LoveSan), and Welchia (AKA Nachi), over 1.3 million computers were infected across the globe, particularly in Europe and America.[1]

And now for the really bad news… Mutations and staged releases of worms that are more insidious that anything you've yet experienced are — no doubt — being created to launch via email. Yet the majority of companies are still in a reactive mode to viruses.

So if your infrastructure doesn't yet have the proper security firewall in place to prevent further damage, infections, intrusions and downtime caused by these worms, the next waves of outbreaks will cause greater damage.

Many Firms Still Have Not Learned

Consider the facts. In his August 27 Security Pipeline article, "Sobig: Lessons Learned", editor Keith Farrell, says, "From here on we need to view each new worm or virus as a new Round One in the battle for the Net. Even as we struggle to remove the latest version, we must be prepared for the eventuality that newer and far nastier variations could be around the corner."[2]

In his August 22 Gartner Special Report entitled, "Worm Outbreak Shows Need to Keep Paying for Security", John Pescatore adds, "Many enterprises learned from those earlier attacks and reduced their exposure by shielding vulnerable Windows software or switching to more secure products… However, many firms did not learn, and many that did learn slid back and reduced the head count and other expenses required to keep Windows secure.[3]

Advice About Worms From The Security Experts

Hackers will relentlessly try to create the perfect worm. Changing your company's attitude towards email is a step in the right direction towards prevention of attacks.

Fred Rica, Partner, PricewaterhouseCoopers, offered some timely advice on CNBC's Open Exchange: "If someone came to your door unannounced and rang your doorbell, you'd look through the peephole, say 'Who is it? Do I know this person?' before you open the door. Well, you have to have the same kind of consciousness and defensive posture when you're opening e-mail."

"These attacks are really nothing new," he adds. "Someone uncovered a

(see next page)

And now for the really bad news… Mutations and staged releases of worms that are more insidious that anything you've yet experienced are — no doubt — being created to launch via email. Yet the majority of companies are still in a reactive mode to viruses.

vulnerability... With the 'SoBig,' what we saw is users actually had to …click on a file attachment to make this thing spawn. Users' behaviors have to change a little bit, too. The Internet is not a safe place. All the e-mails you get are not benign. And you really have to pay attention to the subject, who the e-mail is from, and make a conscious decision: Am I going to open this thing or delete it?"[4]

Patches Aren't The Only Answer for Companies

In an interview on CNBC's Check Point, Mark Lobel, Senior Manager, PricewaterhouseCoopers, proposes a logical security approach: "Right now, when a new worm comes out, everybody's running around patching every system. That may not be the right answer for many companies. The trick is to … take the security data you have today of what systems you have, what information's on those systems, and make that data actionable… Identify the ten highest risk systems and patch them…"[5]

In a recent interview with Shane Kite, author of "Visualization Apps Key in Battle" in Securities Industry News, Andy Toner, Partner, PricewaterhouseCoopers, says: "It's taken firms too long to recognize malicious code, whether it's because of manpower resources or there's a new patch that's come out and they're not able to recognize that and apply it fast enough, or whether there's an actual new threat out there."

"The Sobig virus… and Lovesan worm… incidents have led firms to outsource security of core or critical operations to managed security services providers (MSSPs), which operate 24/7 security operations centers (SOCs)," he continues. "Because of their sole focus on security, SOC-operating providers are considered uniquely capable of identifying trends and flaws, which can lead to quicker patching."

Furthermore, Toner adds, "The recent onslaught of quick-acting computer viruses like Sobig and the Lovesan worm could provide a boost to cyber-security providers with good visualization applications… Financial services industry firms are seeking visualization tools from vendors that provide intrusion analysts with graphical representations compiled from the blinding amount of Internet and enterprise log data compiled constantly during the day to protect systems." [6]

Three Simple Ways to Prevent Worms and Email Viruses

There are some things that every computer user can do to mitigate problems caused by worms. Mark Lobel recommends a simple three-step cure for any of these viruses:

- **Step 1**: Install personal firewalls and antivirus software on every laptop computer;
- **Step 2**: Identify and test patches then use software to distribute the patch on a regular schedule or when an exploit is being used publicly; and
- **Step 3**: Scan external firewalls weekly and block vulnerable ports and services.

Consumers may have it a little easier. Mr. Rica on Next @ CNN, August 24, 2003 says, "Probably the easiest thing a home user can do is, upgrade their software to Windows XP, make sure they have what is called automatic update turned on, and whenever Microsoft issues a patch, a little icon will light up on their screen. It will say there is a new update available, and it is very easy to just click on that, download it, and make sure your machine has the most current level of protection on it." [7]

Be Proactive With An Integrated Threat Management Approach

With mutating worms and new viruses, how can an organization protect itself? John Pescatore of Gartner knows what to do. He writes, "The recent wave of vulnerabilities and worms shows that enterprises need to continue… improving processes for managing vulnerabilities, assessing threats and managing patches." [8]

To that end, IT managers need to take a proactive approach by mounting an effective defense with an enterprise-wide integrated approach to threat management. This approach can:

(see next page)

"The recent onslaught of quick-acting computer viruses like Sobig and the Lovesan worm could provide a boost to cyber-security providers with good visualisation applications… Financial services industry firms are seeking visualisation tools from vendors that provide intrusion analysts with graphical representations compiled from the blinding amount of Internet and enterprise log data compiled constantly during the day to protect systems."

– Andy Toner, Partner, PricewaterhouseCoopers

- Centralise security information;
- Run the correlation programs necessary to identify the most sophisticated threats;
- Build up the necessary reporting capabilities;
- Generate actionable security data on a timely basis;
- Prevent and respond to incidents;
- Report compliance to external audiences, and
- Establish the metrics critical to benchmarking and continuous improvement.

Together, these tactical advantages can allow enterprises to demonstrate strategic improvement through:

- **Risk mitigation** to counter the rising problem of viruses as a larger number of people exploit an increasing number of vulnerabilities;
- **Cost reduction** to justify ROI by doing what is necessary before a crippling worm knocks out your network, causing millions of dollars in downtime;
- **Increased technology, process and organizational** efficiencies;
- **Adopt new regulatory compliance requirements**, such as ISO 17799 and BS 7799 security risk management frameworks; and
- **Responding to security information in a timely manner**, including the launch of a proactive patch management program.

For More Information…

To learn more about PricewaterhouseCoopers' Threat & Vulnerability Management services, contact Fred Rica, Partner, PricewaterhouseCoopers, 973.236.4052.

Sources:

[1] Carrie Kirby, "Many More Worms Will Wriggle Into Our Future", San Francisco Chronicle, September 4, 2003

[2] Keith Farrell, "Sobig: Lessons Learned", Security Pipeline, August 27, 2003, http://www.securitypipeline.com/shared/article/showArticle.jhtml?articleId=13900180

[3] John Pescatore, "A Gartner Special Report: Worm & Virus Breakout — Worm Outbreak Shows Need to Keep Paying for Security," Gartner, 22 August, 2003,

http://www4.gartner.com/research/asset_47924.jsp

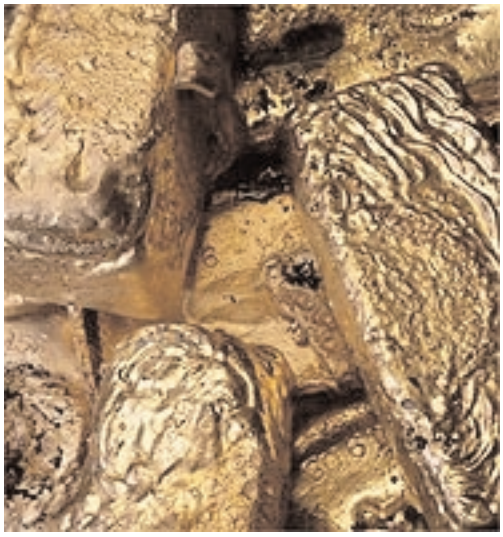
[4] Interview on CNBC Open Exchange, August 21, 2003

[5] Interview on CNBC Check Point, August 20, 2003

[6] Shane Kite, Senior Reporter, "Visualization Apps Key in Battle", Securities Industry News, August 25, 2003

[7] Interview on Next @ CNN, August 24, 2003

[8] John Pescatore, ibid, Gartner, 22 August, 2003, http://www4.gartner.com/research/asset_47924.jsp



"The end result would replace the legacy system with an integrated framework that provided secure, real-time transactional services to its employees working with high net worth customers."

Brian Jensen, Senior Manager, PricewaterhouseCoopers

Case Study: What We're Doing For a Global Financial Management Company

Description of Client's Business

The client is one of the world's leading investment banking and financial advisory companies, with offices in dozens of countries and billions of dollars in assets under management.

The Client's Challenge

"This organisation was aggressively using technology to advance its business strategies," says Brian Jensen, Senior Manager, Technology & Data Services, PricewaterhouseCoopers.

"Its IT team wanted to maximise its investment by standardising its varied, proprietary legacy infrastructure and consolidating existing applications to take advantage of the latest Web services tools and techniques," continues Jensen. "The end result would replace the legacy system with an integrated framework that provided secure, real-time transactional services to its employees working with high net worth customers."

Simultaneously, another challenge was to both design and deploy an abstracted Web services security layer. "This would facilitate easier management of transactional sessions, user data and application permission," says Jensen. "Our security solution had to be robust, flexible and highly scalable to support the client's financial advisors — from the opening of the financial markets through the closing."

The PricewaterhouseCoopers Solution

"We were hired to create a secure, open, standards-based technology that enabled collaboration among different business channels, based on our significant experience with Netegrity®" adds Jensen. "PwC has vast expertise with high-end, large user environments. In addition, PwC actually worked hand-in-hand with the Netegrity engineers to optimize the Transaction Minder configuration and the product."

The project team also leveraged Microsoft's .NET platform to create an extensible, abstraction layer to enable secure transaction processing between their presentation layers and legacy systems.

Overall, the security components necessary to support this integration framework included:

- A Security Application Program Interface (Microsoft® C+ development);
- A Directory Services Infrastructure (Microsoft® Active Directory, Meta Directory Server; SQL Server);
- Distributed Security Services (Netegrity® SiteMinder® and TransactionMinder™);
- Entitlements Management (existing client functionality);
- Identity Management/Provisioning (Waveset™ and existing functionality); and
- Operational Monitoring and Performance Testing.

Value propositions for the engagement included the following:

- **A proven pragmatic security approach** based on the deepest, broadest experience-base in the industry and expertise in integrating enterprise applications into a security framework;
- **An approach to leverage existing APIs and user data**
- **Creating an Open Solution** that offers a platform independent approach with plug-and-play capabilities for service components;
- **Development of a robust PwC Security Framework** to provide:
  - SOAP/SAML distributed security interfaces for integration with other applications,
  - Requests to access control solutions (SiteMinder and

"We went from zero to a fully built system in only three months. This model allows us to seamlessly integrate the client's presentation layers with their legacy systems, enabling virtually instant updates for the client's user community."

ransactionMinder),
– A viable authentication scheme with support for federated authentication mechanisms,
– Single Sign-on (SSO) authentication solution provided by SiteMinder,
– Product could enforce an end-to-end cross-authentication domain,
– Role Based user entitlements and profiles specified and exposed by a directory-based solution using LDAP and management, and
– SiteMinder/TransactionMinder for Session Management.

Benefits/Results to the Client

Project benefits included:

- Using best practices for an iterative build throughout an initial 90-day window, to better align with the client's business drivers/needs vs. a traditional six-month build and subsequent deployment;
- A standard, easy-to-use toolkit for developers and business partners;
- Secure, real-time transactional services for its employees working with high net worth customers and online trading clients;
- A reduction in redundancy and an increase in data integrity provided to all applications for a better representation of user profiles;
- The streamlining of management processes;
- One of PwC's first uses of SAML standards-based solution to facilitate the efficient transfer of user identities during the transactional processes; and
- C+ code that developed and derived a user's identity from the various backend systems – essential for deploying a role-based access control model.

"The client was thrilled with the rapid deployment of this project," concludes Jensen, "because we went from zero to a fully built system in only three months. This model allows us to seamlessly integrate the client's presentation layers with their legacy systems, enabling virtually instant updates for the client's user community. Finally, PwC was especially impressed with the client team's best practices on their side."

For More Information

To find out more about PricewaterhouseCoopers' and Netegrity's Identity Management solutions, please contact:

Brian Jensen
214-754-7304
or
Shawn Connors
646-471-7278

"We're working with PricewaterhouseCoopers' Security and Privacy Practice, a leader in Identity and Access Management solutions, to help our customers successfully implement Identity Management and manage their security risks."

— Jim Hebert, General Manager for Windows Server, Microsoft

PricewaterhouseCoopers Alliance Spotlight: Microsoft

Each issue of this newsletter will feature a PricewaterhouseCoopers' strategic Alliance Vendor within our Security & Privacy Practice.

Microsoft (www.microsoft.com), founded in 1975, is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to enable people and businesses throughout the world to realise their full potential.

PricewaterhouseCoopers began working with Microsoft in 1996. PwC is now collaborating closely with Microsoft to deliver Identity and Access Management, Security and Privacy Management, as well as Wireless and VPN solutions to Global 2000 companies.

"PwC combines business understanding and security leadership with Microsoft's technology to provide enterprise-wide security solutions that deliver real benefits to multi-national organisations today," says Gary Loveland, partner, PricewaterhouseCoopers' Security & Privacy Practice. "Our work supports Microsoft's broad-based security and privacy initiatives."

How PricewaterhouseCoopers Provides Value with Microsoft

PricewaterhouseCoopers provides a full range of security and privacy services to Microsoft customers. PwC's security strategy, design, integration, assessment and other services can help companies secure their Windows infrastructures and avoid damage resulting from security or privacy compliance failures.

PwC has tailored three types of solutions to the Microsoft customer's needs:

- **Identity & Access Management** — PwC worked closely with Microsoft to develop its new Identity and Access Management Solution Accelerator, designed to guide companies through the process of planning and implementing an enterprise-wide Identity and Access Management solution. PwC's solutions for Microsoft customers in this area are:
  - **Identity & Access Management** — Development of a cost-effective approach to managing user access by selecting and deploying appropriate technologies, integrating security components and business systems and centralizing management of user access.
  - **Microsoft Active Directory** — Assistance in planning, designing, deploying and/or maintaining an Active Directory environment to create the foundation for a centralised yet flexible security repository.
  - **Microsoft Identity Integration Server (MIIS)**— Assistance in the planning and/or deployment of MIIS into an organisation to facilitate integration and maximise the investment made in this technology.

  "Identity and Access Management is critical to our enterprise customers, particularly as they move into Web services," says Jim Hebert, General Manager for Windows Server at Microsoft. "Yet managing multiple identities across a heterogeneous computing environment can be a complex technological challenge. We're working with PricewaterhouseCoopers' Security and Privacy Practice, a leader in Identity and Access Management solutions, to help our customers successfully implement Identity Management and manage their security risks."
- **Security Management** services address both the risk management and the cost containment problems associated with implementing an effective configuration and process-centric approach to security and privacy. This includes:
  - **Patch Management** — Assistance in development of effective processes, supported by the appropriate organisation and technology, to monitor, evaluate and implement software patches.

(see next page)

"PwC combines business understanding and security leadership with Microsoft's technology to provide enterprise-wide security solutions that deliver real benefits to multi-national organisations today. Our work supports Microsoft's broad-based security and privacy initiatives."

- Gary Loveland, Partner, PricewaterhouseCoopers

  - **Windows Security Assessment and Penetration Testing** — Reviews of existing or planned Windows operating systems and major Microsoft-based applications to identify configuration vulnerabilities relative to other secure deployments and recommend improvements.
  - **Windows Security Design and Implementation** — Design and help in implementation of advanced security on Windows operating systems and major Microsoft applications, aligning the configuration of the environment with other secure deployments.
  - **Security Crisis and Incident Response** — Emergency response to security incidents and assistance in preparing plans to prevent, detect and recover quickly from future incidents.
  - **Privacy Solutions** — Assistance to clients in effectively identifying, assessing and managing privacy risks by utilizing proven methodologies and leading-edge tools.

- **Wireless and VPN Security** — These services address the design and implementation of a well designed remote access or wireless infrastructure in order to improve security and lower administrative costs. They include:
  - **Wireless and VPN** — Provide services to help customers identify the appropriate strategy, design and implementation of wireless and Virtual Private Network (VPN) technologies, ensuring that effective security controls are in place.
  - **Internet Security and Acceleration Server** — Provide services to enable a client to identify the appropriate strategy, design and implementation of perimeter protection devices. Provide detailed guidance to ensure that host operating systems are aligned with other secure deployments.

To learn more…

Please visit http://www.pwc.com/microsoft.

Microsoft Contact:
Richard Harris
1.510.531.6709

PricewaterhouseCoopers Contact:
Gary Loveland
1.949.437.5380

Don't miss these important security events.

Mark Your Calendars! Upcoming Conferences, Seminars and Webinars

Join PricewaterhouseCoopers and our Alliance Vendors at these important upcoming security conferences and events.

SECURITY CONFERENCES

Sarbanes-Oxley Compliance for Customers of SAP Software

Sponsored by: Wellesley Information Services (WIS)
Date: November 3-5, 2003
Location: Marriott Crystal Gateway, Arlington, VA (Washington, D.C.)
This conference is the definitive place to learn precisely how to bring your organization into compliance with the Sarbanes-Oxley Act. Highlights include:

- 60 in-depth sessions
- 5 comprehensive tracks
- Keynote address by Congressman Michael Oxley
- Industry forums
- Pre-conference "Jumpstart" session
- Ask-the-expert meetings
- Case studies
- Plus, special events and networking opportunities

Register online at: http://www.socompliance.com/

UPCOMING WEBCASTS

To be announced…

ARCHIVED SARBANES-OXLEY WEBINARS

Microsoft Executive Circle Presents: How does Identity Management Support Sarbanex-Oxley Compliance?

Presented by: Steve Wilkens, Director, PricewaterhouseCoopers LLP; Ashley Arbuckle, CISSP Manager, Security & Privacy Practice, PricewaterhouseCoopers LLP; and Sandeep Sinha, Lead Product Manager, Microsoft Corporation
This event was held live on August 13, 2003.
URL for viewing: www.microsoft.com/usa/webcasts/ondemand/2141.asp

PricewaterhouseCoopers On Demand Webcasts

Rebroadcast of Two-part Webcast: "Sarbanes-Oxley: Leveraging Your SAP Environment to Enhance Financial Controls"

Part One - March 20, 2003
Part Two - April 3, 2003
URL for viewing: www.pwc.com/extweb/ncevents.nsf/DocID/C9A3A9AA9241A2AB85256CE50062EB08

ARCHIVED IDENTITY MANAGEMENT WEBINARS

The Power of Roles in Identity Management, Featuring Merrill Lynch – September 18, 2003

Join PricewaterhouseCoopers, Netegrity and special guest Merrill Lynch for a practical discussion on role-based Identity and Access Management. We'll share best practices, strategies, and a client example presented by Dean Mazboudi, Vice President — Data & Technology Architecture from Merrill Lynch.
URL for viewing: http://members.netegrity.com/Event.cfm?Id=473&campaction=60

Microsoft Executive Circle Presents: Identity Management in the HealthCare Industry – July 22, 2003

URL for viewing: www.microsoft.com/usa/webcasts/ondemand/2089.asp

(see next page)

Join us at these upcoming industry events.

Microsoft Executive Circle Presents: Planning for Identity and Access Management Solution – June 17, 2003

URL for viewing: www.microsoft.com/usa/webcasts/ondemand/1987.asp

Netegrity On Demand Webcasts

Best Practices for Migrating from SiteMinder v4.x to v5.5 - July 31, 2003

URL for viewing: www.netegrity.com/events/events.cfm?page=eventsarchived

Real-World Identity and Access Management Deployment Experiences - An Interactive Panel Discussion - June 19, 2003

URL for viewing: www.netegrity.com/events/events.cfm?page=eventsarchived

WANT TO KNOW MORE?

Please contact Bryan Welch, Global Risk Management Solutions, at bryan.r.welch@us.pwc.com, 415.498.7991.