
Securing NT
A sponsored
White Paper from
Windows NT & 2000
explorer
The magazine for enterprise systems managers
and
NTSecurity.net
www.ntsecurity.net

introduction

Within the following pages we present our sponsoring vendors' guides to Securing NT. We have gathered the product information from the vendors themselves and have not tested or reviewed the products. As with any important purchasing decision, we recommend that you perform a thorough course of research to determine the solution that's best for your environment. We hope that the information presented here serves as a useful starting point.

Editorial

Publisher: Jason Brown - jason@ntexplorer.com
Editor: Fiona Newbery - fiona@ntexplorer.com
Copy Editor: Andy O'Brien - andy@ntexplorer.com
Editorial Assistant: Alison Glover - alison@ntexplorer.com

UK & European Advertising

Advertising Sales: Steve Cable - steve@ntexplorer.com
Cross-platform Sales: Kathie Cutter - kathie@winntmag.com

Design & Production

Production Manager: Joanne Malpass - joanne@ntexplorer.com
Designer: Helen Owen - helen@ntexplorer.com
Printed by: Trafford Press, Manchester

This White Paper is brought to you by **Windows NT & 2000 explorer** magazine.

SUBSCRIBING TO Windows NT & 2000 explorer
Subscriptions in UK: £24 for 12 Issues, £42 for 24 Issues.
Rest of Europe: £36 for 12 Issues, £61 for 24 Issues.
To subscribe: visit our Web site www.ntexplorer.com/subscribe
or call 0161 929 2800 or email sub@ntexplorer.com with your details.
Windows NT & 2000 explorer, 6 Caspian Rd, Altrincham, Cheshire, WA14 5HH, UK.

WRITING FOR Windows NT & 2000 explorer
We welcome article submissions on topics crucial to Windows NT, Windows 2000 and BackOffice components. All articles are edited to ensure that they conform to our editorial standards of quality and objectivity. If you'd like to write for Windows NT & 2000 explorer magazine, contact Fiona Newbery, Editor, fiona@ntexplorer.com, 0161 929 2822.

ADVERTISING IN Windows NT & 2000 explorer
To receive a copy of the latest media kit with Rate Card, Editorial Calendar and subscriber profile, please contact Steve Cable, Advertising Sales Manager, steve@ntexplorer.com 0161 929 2812 or Kathie Cutter, Cross-Platform Advertising Sales, kathie@ntexplorer.com, 0161 929 2814.

Mark Joseph Edwards takes a look at the differences Windows 2000 will make to security.

Securing NT

I'm very excited about Windows 2000. And the prime reason is because of all the new security features Microsoft has built into its new operating system. As you may already know, Windows 2000 promises to deliver a far more robust security platform than we enjoy now within a Windows NT 4.0 environment.

Within the new Windows 2000 operating system, you'll find several technologies that you may not have encountered before. Those new technologies include Active Directory, X.509 Certificate support, single sign-on capabilities, Kerberos authentication, public key infrastructure (PKI,) an encrypting file system (EFS,) virtual private networking (VPN,) and more.

Each technology is designed to provide pieces of the bigger security puzzle – pieces that are obviously missing from the Windows NT 4.0 platform. Let's take a brief glance at each of these technologies to learn what they do and how they fit into the grand scheme of information security. (*A more complete version of this article is available on our Web site: www.ntexplorer.com/whitepaper.*)

Active Directory

At the core of the Windows 2000 security puzzle is Active Directory, which serves as the foundation for almost all aspects of security under Windows 2000. Active Directory provides a centralised data store for all domain security and user account information on the network, and provides redundancy and usability through replication capabilities and robust remote administration.

Under Active Directory, domain topology (or realms) can be shaped much more easily than by using Windows NT 4.0's rather flat domain modelling, and organisational units (OU) can be created in a tree-like fashion, where all resources can then be controlled within an individual organisational unit. Fine grain control of user rights can then be applied within a unit to delegate specific authority to specific users within that organisational unit.

PKI and X.509 Certificates

Windows 2000 provides support for public key infrastructure as well as X.509 certificates from any certificate issuing system that supports X.509. In a Windows 2000 network environment, network administrators define which certificate authorities (who issue certificates) are to be trusted by the network.

Think of certificates as a more secure replacement for usernames and passwords. With a system for issuing certificates, as well as a system that guarantees certificate revocation, companies can enjoy a more secure platform for business-to-business transaction – even across the Internet.

Kerberos

Kerberos is an identity authentication protocol designed to provide scalability and single sign-on capabilities across an enterprise. Kerberos replaces the older and more vulnerable NTLM authentication protocol used in Windows NT 4.0. However, Windows 2000 will continue to support NTLM for users still founded on legacy systems.

Where NTLM is basically a private key two-party security system, Kerberos is not. Instead, Kerberos uses a three party authentication system that never requires a user to reveal sensitive information.

Under the hood Kerberos is actually very complex. However, from a 10,000-foot view, Kerberos appears rather simple but, nonetheless, it's rather ingenious and here's how it works in a nutshell. During a typical Kerberos authentication process, a client machine contacts a Kerberos-based Key Distribution Center (KDC) and requests a set of credentials that will allow it to communicate with a client-specified server. The KDC then sends the client a session key that is shared between the client and the server for which access has been requested. The KDC also sends the specified server a key containing the same shared session key that was sent to the client requesting access. Upon receipt, the specified server will then determine whether or not the session key is valid by examining several parameters, and if it is in fact valid, the server will then allow the client to connect for resource usage.

Single Sign-on

Since Windows 2000 employs both Kerberos and NTLM along with the enterprise-enabled Active Directory, the platform is capable of providing single sign-on access to just about every resource across an enterprise, as long as that resource adheres to the native security models in Windows 2000.

All of the security protocols in Windows 2000 rely on some form of user credentials, which are presented to a server upon client connection, where Windows 2000 requires the use of different credentials based on which protocol is used by the client.

Credential provisioning can be initiated in variety of ways, and you'll probably be pleased to learn that Windows 2000 provides native functionality for smart card technologies through its support of the Extensible Authentication Protocol (EAP). Smart cards can be very useful in storing encryption keys and other relevant user information, and lessen the chance of sensitive user information (such as passwords) being compromised.

Encrypting File System

Another great feature to be found within Windows 2000 is its support for a new type of file system called the Encrypting File System (EFS,) which serves to encrypt information stored on disk subsystems.

EFS is based on public key encryption technology that uses 56-bit DES and relies on Microsoft's underlying CryptoAPI architecture. Under EFS, each file is encrypted using a randomly generated user key, which remains independent of any user's main public/private key pair. And EFS encryption and decryption are performed on the fly without any need for user intervention.

EFS can encrypt individual files or entire directories, and supports access for encrypted files and directories located on remote systems. Additionally, EFS supports file import and export without the need for decryption, which means backups and restorations will work seamlessly.

Virtual Private Networking

As with Windows NT 4.0, Windows 2000 supports virtual private networks (VPNs), however, under Windows 2000 this technology is much more transparent to the end user than it is under Windows NT 4.0.

By using a helpful Network Connection Wizard, a user can quickly build a connection to any network resource using a variety of connection methods – VPNs included – by simply providing the necessary parameters.

With VPNs, Windows 2000 supports three key protocols already in wide use today: PPTP, L2TP, and IPSec. Each protocol can be used separately or in combination with an other, depending on the particular needs of your company.

Conclusion

As you can see, there are numerous types of new-found functionality within the Windows 2000 operating system. While this overview certainly does not touch on every single new bell and whistle that Microsoft has integrated into the new platform, it does provide a clear view of the main advantages that can be enjoyed by adopting it.

And while many people will certainly feel reluctant to begin a migration to the new platform, the new security features alone should serve as one of the prime motivators. With all the new security features of Windows 2000 in place on your network, you'll then be able to adopt a new level of confidence in the overall security of your enterprise network. And as we all know, that has a very direct and significant impact on the overall security of a business in general.

Take time to examine all of the new security features of Windows 2000 with a fair amount of attention towards detail. I'm certain that you'll find, as I do, that they all add up to a more secure and very inviting new Windows platform that will present a much greater challenge to any would-be intruder.

This article has been abridged from the original which can be found at www.ntexplorer.com/whitepaper

Administration is the key

It is encouraging to note that most organisations now see the need to address system security, and as NT is becoming the most common operating environment, management is fully aware that a security strategy is required. This was certainly not the case in the past. However, many still leave security administration well down their priority list.

Get the policy right

The security of any system, but particularly NT, runs in cycles. A security specification is laid down as part of the environment rollout. This is implemented at build time and will include elements such as account settings, group membership, system and user profiles and core permissions settings. This structured approach is based on detailed analysis of requirements or some externally supplied policy. This is problem number one because there are many generic security policy definitions already available, and while some are of high quality they do not all suit specific NT requirements.

A one-shot fix

The second part of the cycle comes some time later when an auditor arrives, takes the existing policy and tests against it. Unsurprisingly he finds a number of systems/users that do not comply, a list of corrective actions is produced, the system administrator takes one look at the list and puts it on the bottom of his pile. This means that as the next audit approaches there is a desperate searching for the list, and frantic activity attempting to correct all the problems.

If any of this sounds familiar it's hardly surprising. Security is often seen as a one shot fix. If you're lucky, the organisation will have some facility to test against the defined policy on a regular basis, but very few packages can *enforce* the policy and ensure that systems stay compliant.

Security is an on-going task

NT's specific security requirements are well defined, as are the Microsoft tools required to set up the security. One of NT's problems, however, is the number of options available and the number of different tools supplied. Options mean choices, and choices mean you have to deal with the changes. The major problem areas are event log management, system policy settings, user policy settings and permissions enforcement, which normally require handling by separate tools. The security manager's requirements are for centralised information with minimal overhead on the local desktop, enforcement of the defined policy, the provision of intrusion detection and real-time security monitoring.

Comprehensive administration required

Braintree's Security CeNTre provides a dedicated NT security administration solution, rather than just an auditing tool. Within the product, security policies can be defined and target systems monitored for compliance against them. The product can then selectively correct any deviations from policy without the need for agent software. These tests can be automatically performed, thus ensuring that security levels stay set without increasing the workload on the system or security administrator.

A system administrator needs a detailed technical level report from a compliance test, whereas, say, a global security manager only needs high level compliance reports stating which machines have passed or failed. You also need the ability to handle policy exceptions thus preventing the situation where a valid non-compliant system is always reported and disregarded. Security CeNTre's focused reporting facilities ensures that security personnel receive the appropriate level of detail.

Regular monitoring is essential

Auditing of system events is always seen as an overhead, but this is mainly because there is no easy method of managing the distributed audit files. An audit trail is fairly useless unless checked regularly and can be easily analysed for unusual events or attack patterns. By collating these audit files to a central location, Security CeNTre's query tool can dramatically reduce this management overhead. Recording for later analysis is fine for most events, but critical items need to be brought to a security manager's attention as soon as possible. Security CeNTre provides automated filtering, ensuring that details of specific events or sequences of events are forwarded to a defined administrator in real-time.

Minimum impact

By bringing all of these facilities together within one dedicated solution, BrainTree's approach ensures that your security is implemented and enforced with the minimum of impact on resources. Thus, the all too common cycle of events described above can be prevented.

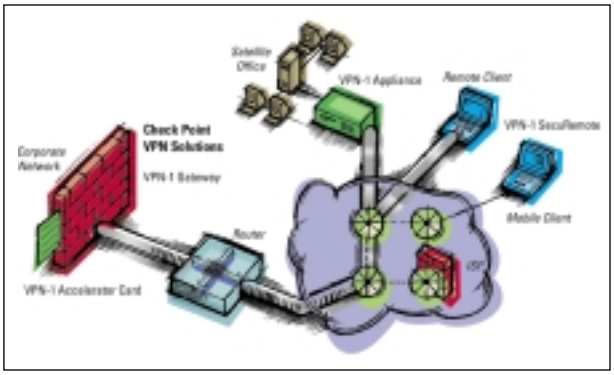
BRAINTREE™
Security Software

For further information contact BrainTree Security Software. Tel: 0161 945 1511

Mind your own business

Virtual Private Networks (VPNs) bring benefits to many organisations and are an essential component of modern business. The demand for them raises challenges that need to be faced head on by the IT industry. We need to provide solutions that match demand, functionality that matches expectation and performance levels that can cope.

VPN configurations fall into three categories: Intranet VPNs, for secure communications between, and amongst, internal corporate departments and branch offices; Remote Access VPNs, between a corporation and remote or mobile employees; and Extranet VPNs, between a company and its strategic partners, customers and suppliers. The technological requirement for each of these is different, presenting varying demands for encryption, authentication, traffic control, availability and access.



VPNs are usually a mix of these systems serving multiple constituencies, remote sites, mobile users and an increasing diversity of business partners and customers. The expectation is that a VPN will increase sales, cut costs, accelerate development, and strengthen relationships. It is recognised, however, that security of information is vital and that the Internet as a communication medium jeopardises the privacy of data and users.

The IT industry has to meet these expectations, enabling business to reap the benefits of the technology whilst also allaying security fears. A successful VPN implementation requires open systems; the continuing security of the data passing over it demands control and management. These are the challenges we face.

The VPN market is populated with incomplete solutions, focusing either on one type of VPN or one aspect of the problem. Most VPN vendors offer products that only provide authentication or encryption, inadequate for mission-critical VPNs as they do not provide basic access control. Most vendors sell their VPN products as yet one more networking device which customers must manage separately and somehow integrate into their overall security policy. Most leave the Quality of Service and reliability aspects to service providers, rather than giving users the tools they need to put performance predictability in their own hands.

This piecemeal approach leads to real security threats. Because the VPNs are not integrated into an organisation's enterprise security policy, they provide limited manageability, scalability and interoperability. Furthermore, these solutions invariably lead to access performance restrictions by virtue of their inefficiency within a poorly co-ordinated system.

There are, however, a few fully integrated VPN solutions that do face the challenges. These solutions are comprehensive and integrated packages. They are based around firewalls utilising Stateful Inspection™ to reach the highest possible degree of protection. Their architecture achieves consistent performance, enables scalability, and allows the support of new and custom applications much more quickly than any alternative.

Add centralised management to these firewalls so that a single, enterprise-wide security policy can be distributed and controlled, and most of the security and management challenges are overcome. But for the kind of VPNs that business expects, they are, by themselves, not enough.

Within remote user VPNs the key element is authentication and continuing management, especially as the members change frequently. As authentication technology progresses, the ideal solution needs to be scalable and extensible whilst remaining capable of incorporating technological innovations easily.

The Private in VPN must mean exactly that. Business needs to protect its information at all levels and at all times. Due to differing implementations and variations in encryption schemes, the ideal VPN solution must pass traffic at the strongest encryption level possible between any two points.

VPNs lead to significant increases in traffic and higher loads on central processing power. The VPN solutions we offer need to provide the means to manage server loads, direct traffic intelligently to ensure mission-critical applications get high priority, and supplement processor power by taking away the high loading encryption tasks and dedicating optimised circuitry and processing chips to the task.

It is only when all these requirements are met that we begin to offer what the market expects and is demanding. The business benefits of flexibility and cost reductions may be negated if the solutions we provide are lacking in any one of the critical areas. Only with an integrated VPN solution that combines security, traffic control and enterprise management can we and our customers realise the benefits of secure, reliable and manageable business communications – this is the challenge of Virtual Private Networking; some of us are beginning to meet it.

CHECK POINT™
Software Technologies Ltd.

For further information contact Check Point Software Technologies UK. Tel: 01223 713600

Flexible firewall fortifications

The Windows NT operating system is configured, by default, primarily for flexibility rather than security. Therefore, Windows NT has some known and, more importantly, as yet undetected security weaknesses.

With the release of CyberGuard Firewall for Windows NT, CyberGuard concentrated on improving the overall security of the Windows NT operating system while maintaining flexibility. This was accomplished through SecureGuard for Windows NT, CyberGuard's product that functions as a wrapper around the Windows NT operating system, providing additional security.

Other Windows NT firewall vendors attempt to enhance Windows NT security by simply patching known holes, recommending that certain capabilities be disabled, and automatically terminating suspicious processes. This approach has serious implications. Every time a new Windows NT security issue is identified, firewall administrators must go through the disruptive and time-consuming task of bringing down the firewall and obtaining and installing patch updates to the firewall software. Recommendations force firewall administrators to spend time educating themselves about the consequences of disabling tunable features and functions in Windows NT. Not all firewall administrators will invest their time this way and oversights can become significant when many features and functions are involved. Automatic termination of suspicious processes requires comparing each process against an enterprise-defined list of acceptable processes. Managing this administrator-maintained list can significantly add to firewall installation time.

Security Hardening

CyberGuard offers SecureGuard for Windows NT, the strongest possible protection against both known and unknown holes and attacks on Windows NT. This approach provides numerous important benefits. SecureGuard for Windows NT is specific enough to address known gaps in Windows NT security. It is also general enough to protect against Windows NT security problems that have not yet been identified. Without SecureGuard for Windows NT, enterprises are vulnerable to these unknown security holes, that most professional hackers typically attack and successfully penetrate. By default, SecureGuard for Windows NT automatically disables risky features and functions in Windows NT. For flexibility in those rare instances when corporate security policy warrants a security override, these tunable parameters can be explicitly enabled. Because Trojan-horse-supporting capabilities are disabled by default, there is no need to terminate suspicious processes, and no chance of inadvertently curtailing useful processes.

Most Windows NT firewall vendors provide recommendations to firewall administrators for installing their products in a Windows NT environment. This passive approach places responsibility for basic firewall security in the hands of the Windows system administrator or security manager. CyberGuard believes fundamental firewall security should be provided by the default behavior of the firewall, not merely through a recommendation. As part of SecureGuard for Windows NT, CyberGuard provides default security hardening measures. The system administrator must explicitly re-enable any disabled capabilities if the corporate security policy permits or requires them. Due to its convenient "check-box implementation", this aspect of SecureGuard for Windows NT reduces the likelihood of a configuration mistake or oversight that could create a large security hole.

Watchdog Services

The watchdog services of some firewall vendors terminate questionable processes. The effort of identifying these processes can range from irritating to impossible. In contrast, the environment hardening performed by SecureGuard for Windows NT cleanses the Windows NT environment so that rogue processes cannot be created and, therefore, do not need to be terminated. Disallowing rogue processes to be created provides significantly more security than monitoring and attempting to terminate such programs.

The watchdog service ensures the fault tolerance of the CyberGuard Firewall for Windows NT and provides a single point of control for its custodial processes.

Packet Interceptor

The packet interceptor anticipates and prevents the exploitation of security holes in Windows NT. It guarantees the interception of data packets before they reach user level, ensures the automatic and dynamic generation of pseudo drivers for each network I/O device, and prohibits the bypassing of the packet interceptor when a new interface is created. Additionally, the packet interceptor improves performance by not propagating denied packets up the IP stack.

TCP/IP protocol and MAC (media access control) adapter drivers are adjacent layers in the Windows NT operating system's networking stack. CyberGuard inserts several drivers between these two layers.

The SecureGuard technology described above and used by CyberGuard Firewall for Windows NT takes a proactive, secure approach to protecting the firewall from potential Windows NT vulnerabilities. It is an important development in providing a Secure NT-based firewall solution.

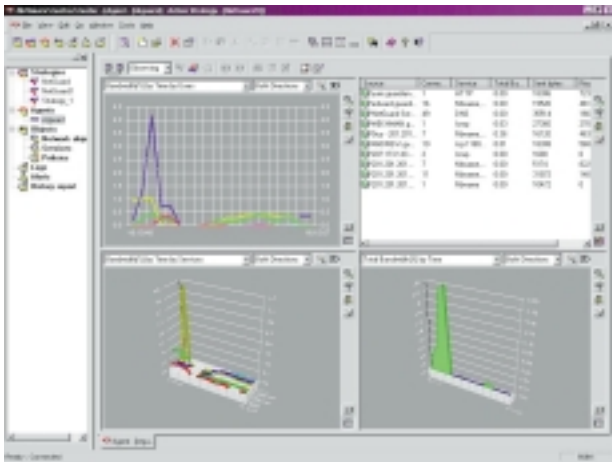
CYBERGUARD CORPORATION

For further information contact CyberGuard Europe Ltd. Tel: 01276 683713

Guarding Internet bandwidth

The Internet is a curious and wonderful place – shot through with all the quarks and sparks of humanity. When accessed from home, Internet surfers zoom exclusively down their phone line, across their ISP's (Internet Service Provider) backbone and out into the vastness of the Internet. Pretty exciting.

In the office, the story is a little different. Maybe the company's network is permanently connected to an ISP and the Internet via a 'leased line' connection. Or maybe the company is connected to the Internet via an ISDN line that instantly dials the Internet when a connection is required.



Let's imagine a scenario. A company has set up a Web site for your potential customers to visit on the internal network. This afternoon an unscrupulous member of that company's IT department has decided to email Doom III (a 15 MB computer game) to a friend out over the Internet. It will take the company's email server well over an hour to pass this file to the relevant email server out in the Internet.

The problem is, that whilst this transfer is happening – the company's Internet connection will be saturated, just at the very the moment when a potential customer wants to visit the company Web site to view products and make a big purchase. The potential customer gives up after two minutes, because the company Web site seems so slow – those Web pages that could have been winging their way swiftly to the potential customers' Web browser, are now having to squeeze past the DoomIII email on an overloaded, unmanaged Internet connection. This means lost business.

The need for Bandwidth Security, particularly for e-commerce applications, has lead to the birth of a surprising new product for managing Internet connections, Guardian - The NetGuard Control Centre. Guardian incorporates a firewall to protect your network from unwanted visitors and, of course, IPsec VPNs, but Guardian also features an Internet bandwidth management tool. This simple bandwidth management tool allows an IT Manager to allocate and guarantee Internet bandwidth to users, user groups, Web servers, email servers and e-commerce applications. This means that critical applications no longer ever need to get 'burned'. 'Bandwidth' is a generic IT term used to describe the speed and flow of any total network or single network connection. In this case bandwidth refers to the speed and flow of an Internet connection.

This means that the business that could have been lost earlier because of Doom III can now be protected by assigning a guaranteed portion of the Internet connection to the Web server. Let's say we have a 64Kbps leased line – you may assign 40% of that to your Web traffic, increasing to 100% if no other use is being made of the connection. Key members of staff who have access to Web browsing the Internet may be guaranteed 30%, again, rising to 100% if no other Internet traffic is active. This leaves 20% for the mail server, except when all else is quiet, when it could also claim the full 100%.

The firewall part of the Guardian Firewall for Windows NT/2000 operates before the bandwidth management. A firewall allows and denies certain traffic to come and go between your company's network and the Internet. A typical simple firewall strategy would deny all traffic unless specifically permitted. Your strategy would probably allow email packets into your network, provided they were destined only for your email server. You would also allow Web browsing packets, provided the destination address was only your Web server. Outbound traffic (from your network to the Internet) might allow everyone to have free access to the Web – although with Guardian it is easy to have a significant group of users only permitted to browse the Web before 9.00am, between 12:00 - 2:00, and after 5:30pm.

Guardian also allows IT Managers to monitor Internet usage both historically and in real-time of both Internet and IPsec VPN sessions (to other firewalls and mobile/home users).

If a particular user seems to be responsible for a large proportion of Internet usage – then a user-activity report can be generated showing which Web sites were visited, for how long, and using up how much bandwidth. In real-time, if a user is caught browsing www.playboy.com – then this connection can be suspended there and then. The Guardian History Database is stored in ODBC format, this can be analysed using MS Access or MS Excel.

GUARDIAN

For further information contact NetGuard UK Ltd. Tel: 01628 533433

Countering the lure of Internet seduction

Properly managed, the Internet can be a valuable information resource for your company. Without controls however, it can reduce employee productivity, interfere with network bandwidth and even lead to litigation and impair your company's reputation.

"The Internet can be a seductive place," says Steve Purdham, President of surfCONTROL, based in Congleton, Cheshire and Scotts Valley, California. "When your employees spend work time surfing the Web for their personal interests, it can dig right in to your firm's bottom line. It is fair to say that most people using Internet technology don't intentionally 'time waste', but this easy access to high value personal information can be seductive, especially to task-orientated workers who often have boring, repetitive jobs. It is also clear that this type of casual surfing could mean a severe loss of productivity to a business."

With the Internet well along the road to becoming a 'must-have' business tool, it's incumbent on any company to ensure that the inadvertent, or misguided actions of a few people do not negatively impact the performance of the rest.

"Increasingly, companies have to worry about employees sending inappropriate emails which can be used to show the employer tolerated a hostile work environment," says Chris Christiansen, an analyst at International Data Corporation (IDC) in Framingham, Massachussetts. Christiansen commends surfCONTROL because of its positive slant. "I like the fact that it contains both a positive and a negative list of sites. So it doesn't merely stop employees from visiting certain sites, it also encourages them to visit others."

According to IDC, surfCONTROL is the No. 1 vendor in the market. "The rapid growth of this market reflects business concern with the seriousness of uncontrolled Internet access," says Christiansen.

In addressing this concern, companies need to manage Internet and email usage in order to:

- Protect employee productivity by eliminating the opportunity for idle exploration of Web sites
- Preserve security by preventing employees from visiting 'undesirable neighbourhoods'
- Conserve network bandwidth so it is reserved for legitimate business uses

- Maintain the company's reputation and reduce the threat of litigation, by preventing an unwarranted association between the company and an offensive URL

Solutions can take many forms: from the simple, but draconian, measure of not allowing corporate connection to the Internet at all, through to total open Internet access to all information, at all times, by all personnel. In a real business environment, neither of these extremes is the answer. The core of any solution will be the Internet acceptable use policy of the organisation. Simply: *who can do what, when and how* with the Internet resource so as to maximise the business benefit. This will create an environment which, on the one hand delivers all the benefits of Internet access to the corporation, yet on the other keeps non-business usage to an acceptable level. Any individual implementation of an acceptable use policy must also recognise that it cannot create unrealistic administrative loads or take such a myopic view of the Internet that the business value is diminished.

JSB's surfCONTROL, the corporate Internet filtering software, will help you to monitor and control employee use of the Internet to ensure that your Internet access is business access.

surfCONTROL gives you the tools to understand Internet use, along with the rules that allow you to implement your acceptable use policy. "Using the built-in reports, forward looking companies can do much more than block access to selected sites." says Jack Attwell, President of Trellis Network Services in Princeton, New Jersey, who uses surfCONTROL to help solve hostile workplace issues. "The cost of lost productivity could be huge, because you never know who's doing what on the Internet. The unlikeliest people sometimes cause the largest problems. Now with surfCONTROL we can warn individuals who are contravening our Internet use policy and take corrective action, thereby protecting the company."

To find out if your company is suffering from Internet seduction, download the free no-obligation, 30-day trial today from www.surfCONTROL.com

For further information contact surfCONTROL. Tel: 01260 296250

Inside job

The ability to communicate with people thousands of miles away, or to conduct trade at the touch of a button, has revolutionised the way we live our lives and conduct our business. However, this commercial advantage can prove to be a security risk if organisational and technological issues are not properly addressed. Organisations can find themselves open to attack from hackers using the Internet — the very medium that they themselves are using to identify new business opportunities. But where do you start in order to avoid this?

Initially, a risk assessment should be performed on your network. From this assessment weaknesses can be identified and a security policy can be established and implemented.

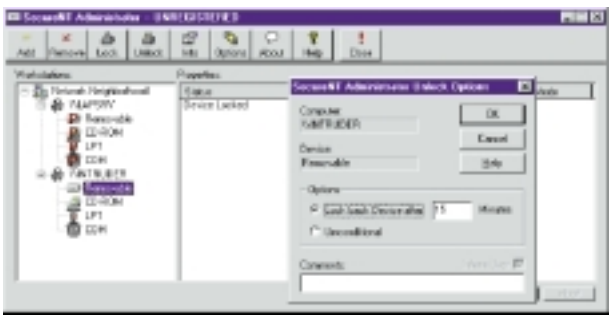
Once a policy has been identified, the next step is to examine the possible tools for the job. The first weapon to be deployed is the Internet firewall which defines who, from the outside, has access to your network. A popular misconception of a firewall is that it is used to prevent access to your network resource. A firewall, in fact, together with associated log and reporting tools, should be used to allow secure and authorised access to a network depending on the policy your organisation has decided to implement.

Once access has been allowed through the firewall, screening and intrusion measures should be put into place. These come in the form of virus-scanning products that check for anomalies in email attachments, scan for viruses at both the workstation and server level and provide protection from (for example) Java and ActiveX applets. Intrusion detection performs the task of checking to see if any unauthorised presence has managed to come into the network through the 'back door'.

The internal threat

Once you have secured your organisation from the outside, and ensured that nobody unauthorised can enter your network, you might be entitled to believe that your resource was safe from attack. However, 90% of IT security breaches are internal and more than 45% are carried out by disgruntled employees (IDC White Paper Delivering the value of IT: Security as a stratetic priority).

So how do you control what individual employees do with your time, money and resources? The most practical way to improve internal security is to restrict user access to individual peripherals such as CD-ROMs, floppy drives, COM ports and local hard drives on their workstations. The answer lies in the form of centrally managed, transparent I/O port control software that gives you total control over who has access to what and when and for how long, strengthening that weak link and at the same time adding flexibility to your security policy.



Unlocking the floppy unit using SecureNT Admin

Solutions from W32

Two security packages from W32 that offer this level of internal security management are SecureNT and SecureEXE.

SecureNT is a powerful desktop security administrator which allows system administrators to implement strict security policies by controlling end-user access to I/O devices such as the floppy drive, CD-ROM, LPT and COM ports. SecureNT is ideal for heterogeneous corporate networks involving several different Windows operating systems, because it can bring NT-level security to Win95/98 desktops. It thus offers the same level of security as diskless PCs or hardware locks, but is cheaper, more flexible and can be remotely operated by authorised SecureNT administrators. It is highly secure, as it is tightly integrated into the Windows OS software and cannot be bypassed by end-users. The Metropolitan Police recently took advantage of SecureNT's features to secure all 6,000 of its desktop PCs through W32.

SecureEXE is a package (to be released shortly) that allows security managers and system administrators to control which programme a user is authorised to run. It will intercept and deny all requests for execution for all programs (and DLLs) that are not authorised. This means that Trojans such as Back Orifice and NetBus as well as computer viruses cannot be installed or run. SecureEXE thoroughly examines each executable you want to authorise and calculates a number of unique identifiers. This makes it impossible to bypass SecureEXE – if the executable is not recognised then it will not be authorised – and to be recognised it has to be identical to the one you have authorised. SecureEXE also has the advantage of taking up very little of a system administrator's time, unlike some tools packages.

Both of these packages offer the kind of security that can enable businesses to take full advantage of the Internet's major business benefits while minimising the risks it can also present. A manager can thus have the peace of mind that comes with security while retaining the competitive edge.

For further information contact W32. Tel: 0181 371 8377

Directory of Sponsors

BrainTree Security Software
Parkway House
Palatine Road
Northenden
Manchester
M22 4DB
Tel: 0161 9451511
Fax: 0161 9452150
www.braintree.co.uk

Check Point
Suite 5B, Enterprise House
Vision Park
Histon
Cambridge
CB4 9ZR
Tel: 01223 713600
Fax: 01223 236847
www.checkpoint.com

CyberGuard Europe Ltd
Riverside Way
Watchmoor Park
Camberley
Surrey
GU15 3YD
Tel: 01276 683713
Fax: 01276 678733
www.cyberguard.com
email: info@cyberguard.co.uk

NetGuard UK Ltd
Thamesbourne Lodge
Station Road
Bourne End
SL8 5QH
Tel: 01628 533433
Fax: 01628 532252
www.netguard.co.uk

surfCONTROL is distributed in the UK by Peapod
The Harlequin Centre
Southall Lane
Southall
Middlesex
UB2 5NH
Tel: 0181 606 9990
Fax: 0181 574 9294
www.surfcontrol.com

W32
Carradine House
237 Regents Park Road
Finchley
London
N3 3LF
Tel: 0181 371 8377
Fax: 0181 346 9177
www.warehouse32.co.uk

In association with

NTSecurity.net
www.ntsecurity.net