



www.panacea.co.uk



PANACEA WHITE PAPER

IT Security: A Business Investment or Overhead?

Kevin Green
Manager, Engineering Services
Panacea Ltd.

MARCH 2004

Copyright Panacea Ltd. 2003

Panacea Limited
Winton House, Winton Square,
Basingstoke, Hants, RG21 8EN

Telephone: 01256 30 50 50
Fax: 01256 30 50 30



OVERVIEW

Global communications and the flow of information from business to business is now such a fundamental part of everyday business life that many organisations can no longer function without them. Long gone are the days of reverting back to manual or paper-based systems.

When access to systems is denied, staff cannot work and organisations lose money. There are many facets to keeping systems fully functioning, most of which involve additional physical systems or duplication of systems acting as standby redundant devices ready to take up services in case of a hardware failure, but a more menacing and far more frequent threat is at hand for every organisation that is connected to the Internet, uses e-mail or employs a number of staff.

Security breaches are now a major cause of system downtime and the threats come from both internal and external sources.

Prepared by: Kevin Green
Manager, Engineering Services
Panacea Limited

Date: November 2003

AUTHOR'S PROFILE

Kevin Green has been manager of Panacea's Engineering Department for the past 13 years. During this time he has been responsible for all aspects of installation and post installation services.

In recent years, Kevin has also specialised in network infrastructure and network security, work that has been instrumental in reducing organisations communications costs while ensuring security is not compromised.

He also successfully completed a post-graduate Diploma in Management Studies and is in the final semester of completing an MBA at Portsmouth University.

CONTACT INFORMATION

Kevin Green

Manager, Engineering Services, Panacea Ltd.

Tel: 01256 305 084 [direct]

e-Mail: kgreen@panacea.co.uk

Tom Sawford

Director, Client Services, Panacea Ltd

Tel: 01256 305 190 [direct]

e-Mail: tsawford@panacea.co.uk

Head Office

Winton House, Winton Square, Basingstoke
Hants. RG21 8EN

Tel: 01256 30 50 50 [switchboard]

e-Mail: enquiries@panacea.co.uk

Contents

Security as an investment	4
Investing for the long term	6
The security policy	7
Securing the perimeter	8
- Firewalls	8
- Authentication Management	8
Checking data from trusted sources	9
- Intrusion detection systems (IDS)	9
- Anti-virus software	9
- System updates	9
Infrastructure control	10
- e-Mail content filtering	10
- Web content filtering	11
Security testing	12
- Network integrity testing	12
- Security policy testing	12
Panacea	13
Glossary of Terms	14

Security as an investment

The security of your system is like any other aspect of your business strategy it is only as good as the weakest link in the chain, and if the chain is not inspected, tested, maintained or amended then your organisation is likely to have a security risk which will remain undiscovered until it becomes the subject of a security breach.

Security can no longer be thought of as an overhead borne by the organisation, it has to be accepted as an investment in business continuity, protecting business data and intelligence, which if lost or compromised could seriously affect the business stability profitability and reputation.

The threat of the cyber-terrorism has never been more real than it is today. Worldwide malicious attacks on IT systems are in the headlines on an almost daily basis with 44% of UK businesses suffering at least one security breach in 2002, nearly twice as many as 2000*, 100 companies reported a total of 3,155 breaches between them in 2002. This phenomenon is not expected to decrease its activity either; recent reports forecast the continued growth in these malicious attacks for the foreseeable future.

Due to the nature of today's global communications access to systems on the other side of the world is as easy as accessing your systems in your home, and the activities of this breed of terrorist is costing businesses many millions of pounds every day. It is estimated that the average cost of a single sever security breach is £30,000*.

These cyber-terrorists are continually improving and honing their skills to find new ways to gain access through security devices designed to keep them out, or to code new viruses that wreak havoc throughout the business community. By the very nature of their trade, they are always one step ahead of the anti-virus software authors even if it's only by a matter of hours during which time viruses can spread across the globe many times and be circulated to hundreds or even thousands of organisations. Each organisation needs a security strategy that has been carefully formulated, implemented, maintained and regularly tested to current standards and threats, to ensure the strategy allows systems to function at optimum performance for all those authorised to access them.

Although these external threats are frequently in the headlines, and are very real, to most organisations, the threat is much closer to home. Internal breaches of security are much more common, and not just limited to individuals loading unauthorised software unauthorised and inappropriate use of e-mail and the Internet is fast becoming the major factor affecting network performance.

The speed in which Internet access is deployed to the user's desktop frequently means that access is granted without policies and procedures being put in place to ensure security of the systems. e-mail or Internet misuse by individuals within the company can leave the company liable for not protecting its whole workforce from such behaviour.

Other problems encountered are staff surfing the Internet on non-business related matters or downloading files, pictures and even music during work hours. Not only is this non-productive time costing the organisation money, it is also using up expensive bandwidth and denying its use for legitimate business related work. Only 27% of UK businesses make their staff aware of company security policies, and many organisations do not have any form of security policy at all.

The internal security threat is a very real one 48% of serious security breaches reported last year in large organisations were internal breaches.**

This is a worrying statistic as it is estimated that 98% of all organisations' intellectual property is in electronic format and that it could be only an e-mail away from being in the hands of a competitor. Systems resources and user activity needs to be monitored to ensure that not only are they suitable for the task but they are being correctly used for the business task they were designed.

An effective security strategy must cover both internal and external threats. However no amount of testing can turn a poorly designed security system into a fully secure one. If corners are cut at the design or implementation stage then the system will be prone to security breaches at every change or at worse could cause the whole system to become so inflexible that it prohibits efficient use of systems to authorised users.

Source:

** Department of trade and Industry 2002*

*** National high tech crime unit 2003*

Investing for the long term

Security in today's organisations covers a wide spectrum of procedures and products, and relates to different things for different companies from electronic communications between continents to shredding hard copies of e-mails in a local office.

Security in today's business world must be seen as a long-term investment in business continuity. To the organisation that views it as just another overhead, a breach of your network or systems is waiting somewhere just around the corner.

Any security strategy needs to address several key issues such as:

- Company wide security policy.
- How to secure the perimeter of the network.
- How to check the threat of data that's allowed to enter the network (e-mail).
- Maintaining control of the infrastructure.
- How to test the integrity of the network and the frequency of testing.

The issues raised here will be briefly explained below, the aim of this paper is to provide an introduction to network security, for a more detailed explanation of any of the following subjects please contact Kevin Green direct.

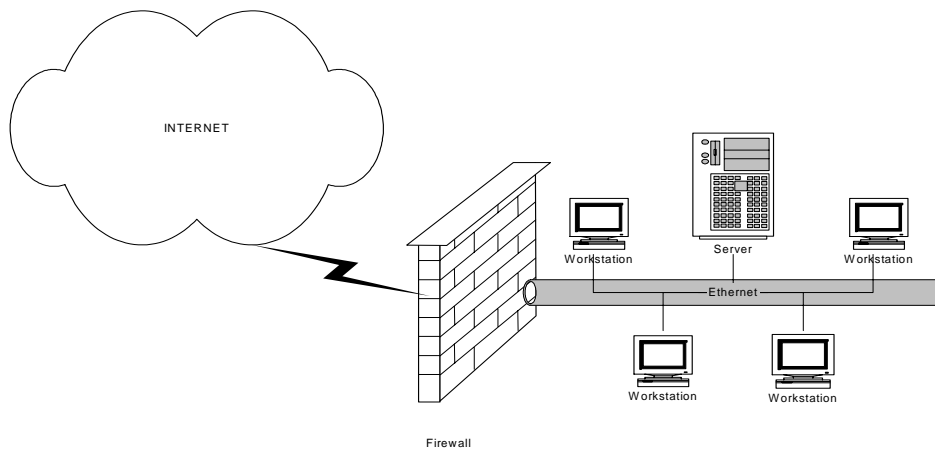
The security policy

At the heart of any security strategy is the organisations security policy outlining the organisations security plans and objectives. This policy will cover all practices that will be adopted by the whole company, detailing such activities as the use of company resources for internal and external e-mail, the acceptable access of web sites and the introduction of non authorised software onto the network, and the penalties for non-conformance.

This policy also forms the framework of what decisions need to be taken in the event of a security breach and guidelines of how to recover from such an event and any emergency procedures to be activated to prevent further breaches.

The security policy should be considered as a living document that requires frequent testing and updating.

Securing the perimeter



Firewalls

A firewall is a fundamental device in connecting any network to the Internet. It analyses the traffic being passed through it to ensure that only authorised traffic or traffic from trusted destinations gets through to the 'secure' side of the firewall.

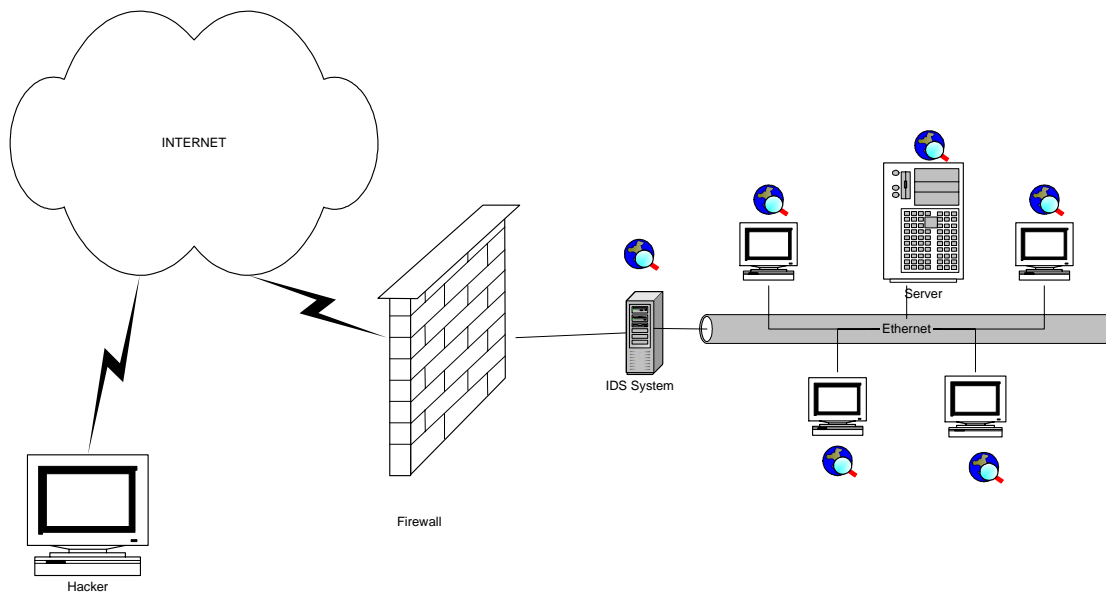
Other functions that many firewalls have incorporated are virtual private networks (VPN) this feature allows encrypted traffic to pass from a remote office or user to gain access through the firewall thereby using a low cost Internet connection as a transport medium over possibly many thousands of miles, and with reduced costs of Internet access an inexpensive way for home workers to gain secure network access.

Authentication Management

In most organisations server authentication is achieved by the use of user name and password only. Passwords are notoriously simple to either guess or overcome using software designed to crack simple codes. Most people use passwords easily remembered (family or pets names) and therefore are easily cracked.

Authentication management tools can provide an additional level of authentication security for remote users by producing a random generated number which is in used in conjunction with a user pin number, the codes only have a window of opportunity lasting in the region of sixty seconds after which time another random number is generated making authentication almost hack proof.

Checking data from trusted sources



Intrusion detection systems (IDS)

As the name suggests these products sit within the secured area analysing all data entering the citadel as well as data being transferred within this area. These products ensure traffic passing around the network is not only valid traffic but that it also has no malicious intent. Modern IDS are capable of not only detecting attempted intrusions and reporting breaches or attempted breaches, they can also automatically plug any holes that have allowed the breach to occur.

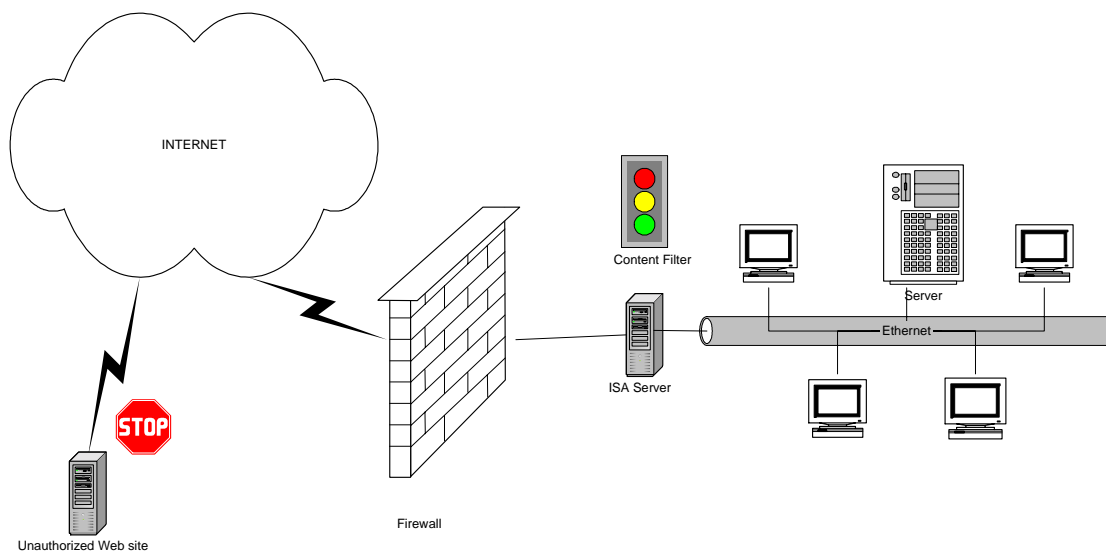
Anti-virus software

This is so widely used in today's systems that it hardly needs any introduction, however there are still systems in the business community that do not update the latest anti-virus automatically or are not the latest versions available. Keeping up to date with these programmes not only gives you the best chance of detecting virus's as soon as they become known, but the latest software also includes additional features to further protect networks.

System updates

Operating system updates are mostly available free to licensed users but are widely dismissed by systems managers as not being relevant. However, malicious attacks are now targeting vulnerabilities within operating systems to gain access to systems or to deny legitimate users access to their systems.

Infrastructure control



e-Mail content filtering

These products ensure the security of the organisation by checking all e-mails within an organisation this ensures bandwidth is not wasted by staff sending internal spam (junk e-mail) such as jokes, pictures or MP3 file formats around the organisation. These products can also prevent unwanted spam e-mails from entering the system. This not only benefits the organisation in terms of reduced time wasted opening and reading them but it also prevents valuable system storage being wasted.

Organisations also have a legal requirement to ensure that all staff work in an environment free from harassment or discrimination, as e-mail is now a widely used in all communications its content must also comply to these legal standards.

Illegal or offensive content may include:

- Pornographic images downloaded off the Web
- e-Mail jokes (either sent or received)
- Pornographic or racially offensive e-mail attachments
- Rumours or gossip regarding a fellow employee
- Unauthorised release of personal employee information
- e-Mail discussions that result in employee harassment or discrimination

All e-mail can be filtered and its content searched for potentially offensive words or phrases by comparing e-mails against separate dictionaries of offensive or derogatory words or phrases. This not only protects your organisation against offensive or discriminatory e-mails it can also protect the organisation from loss of confidential material which could be e-mailed to outside agencies, again by subjecting all e-mails to a set of filter rules and dictionaries confidential material can be kept within the organisation.

Web content filtering

These products can allow, limit or deny access to either some or all web sites, for either some or all members of staff; they are also capable of producing reports of staff, the sites visited and the frequency of web surfing. By using these products, it's easy to demonstrate how productivity can be maintained or increased as it reduces the amount of time staff spend surfing the web on non-business related sites.

In organisations where this technology has been deployed using statistics gathered before filtering was enabled and multiplying by the average hourly rate of pay, it was shown that the ROI is a matter of months in the majority of cases. The flexibility of these filter products can also allow for staff to surf freely to suitable sites (i.e. news sites) at certain times of the day or at anytime outside of normal work hours. Another business benefit of these systems is that the downloading of music and pictures etc can be prohibited ensuring that expensive bandwidth that the organisation is paying for is only being used for business purposes.

Security testing

Network integrity testing

Network vulnerability testing is achieved by subjecting the network to a series of controlled intrusion attacks from a friendly site that then reports on its ability to break into the network. These tests are designed to use all known methods hackers use to gain access so need repeating periodically to ensure the latest methods are used.

Security policy testing

As previously mentioned, the security policy is at the heart of any security strategy and must be considered a living document that grows and evolves with the organisation, it must also be considered unique, as it would be a dangerous assumption that there could be 'one size to fit all'. As with any policy it needs periodic testing to ensure its completeness and relevance to an ever-changing environment.

Please note that in all cases recommendations can only be made after a review of your specific requirements.

For more details on security procedures, products and services including compliance, contact Panacea on 01256 30 50 50 or e-mail enquiries@panacea.co.uk.

Panacea

At Panacea Ltd, the security division looks upon security as comprising four distinct areas that combine to create a comprehensive secure network strategy tailored to the needs of the customer.

The areas are:

Confidentiality

The aim here is to ensure all company confidential data is kept within the organisation.

Accessibility

To ensure that all trusted personnel have unhindered, uninterrupted access to the systems for which they are authorised.

Legal

The security policy of the organisation and its practical implementation has to comply with legal requirements of privacy and decency.

Measurable

Any security strategy must be capable of being tested and checked for compliance at regular intervals, and remedial work carried out to ensure the integrity of the system.

CALM

The security strategy methodology Panacea consultants follow for every customer, whatever their size or requirement is the CALM approach. It is designed to cover all requirements using a combination of the mentioned products and strategies depending upon the customers situation and current needs.

Glossary of terms

Common Terms used in security technologies

Anti-virus

A software program designed to identify and remove a known or potential computer virus

Authentication

The process of determining the identity of a user that is attempting to access a network. Authentication occurs through challenge/response time-based code sequences or other techniques.

Authorisation

The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorised to have access to a specific service.

Content blocking

The ability to block network traffic based on actual packet content.

Content filtering, scanning or screening

The ability to review the actual information that an end user sees when using a specific Internet application. For example, the content of e-mail.

DMZ (de-militarized zone)

A network added between a protected network and an external network in order to provide an additional layer of security. Sometimes called a perimeter network.

Filter

A filter is a program or section of code that is designed to examine each input or output request for certain qualifying criteria and then process or forward it accordingly. .

Firewall

A firewall is a program that protects the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet will want a firewall to prevent outsiders from accessing its own private data resources.

Hacker

Hacker is a term used by some to mean "a clever programmer" and by others, especially journalists or their editors, to mean "someone who tries to break into computer systems."

Intrusion detection

Detection of break-ins or attempts by reviewing logs or other information available on a network.

Malicious Code

Malicious code is any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system. Traditional examples of malicious code include viruses, worms, Trojan Horses, and attack scripts, while more modern examples include Java attack applets and dangerous ActiveX controls.

Monitoring

A view of individual user activity on a network, generally in real time. Provides administrators with the ability to view the content of user utilised applications.

Network Service Access Policy

A high level, issue specific policy which defines those services that will be allowed or explicitly denied from a restricted network, the way in which these services will be used, and the conditions for exceptions to the policy.

Packet Filters

Packet filters keep out certain data packets based on their source and destination addresses and service type. Filters can be used to block connections from or to specific hosts, networks or ports. Packet filters are simple and fast but make decisions based on limited amounts of information.

PAP (Password Authentication Procedure)

A procedure used to validate a connection request. After the link is established, the requestor sends a password and an id to the server. The server either validates the request and sends back an acknowledgement, terminates the connection, or offers the requestor another chance.

Password-based Attacks

An attack where repetitive attempts are made to duplicate a valid log-in and/or password sequence.

Platform Attack

An attack that is focused on vulnerabilities in the operating system hosting the firewall.

Protocol Attacks

A protocol attack is when the characteristics of network services are exploited by the attacker. Examples include the creation of infinite protocol loops which result in denial of services (e.g., echo packets under IP), the use of information packets under the Network News Transfer Protocol to map out a remote site, and use of the Source Quench protocol element to reduce traffic rates through select network paths.

Proxy

An agent that acts on behalf of a user, typically accepting a connection from a user and completing a connection on behalf of the user with a remote host or service.

Proxy Server

A proxy server is one that acts on behalf of one or more other servers, usually for screening, firewall, caching, or a combination of these purposes. Gateway is often used as a synonym for 'proxy server.' Typically, a proxy server is used within a company or enterprise to gather all Internet requests, forward them out to Internet servers, and then receive the responses and in turn forward them to the original requestor within the company.

RAS (Remote Access Services)

A feature built into Windows NT that enables users to log into an NT-based LAN using a modem, X.25 connection or WAN link. RAS works with several major network protocols, including TCP/IP, IPX, and NetBEUI.

Replay Prevention

To provide protection against replay attacks in which a message is stored and re-used later, replacing or repeating the original.

Signatures

Viruses employ signatures by which they identify themselves to themselves and thereby avoid corrupting their own code. Standard viruses, including most macro viruses, use character-based signatures. More complex viruses, such as polymorphic viruses, use algorithmic signatures.

Smart Card

About the size of a credit card, a smart card is a plastic card with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically "recharged" for additional use. Currently used to establish your identity when logging on to an Internet access provider.

SMTP (Simple Mail Transport Protocol)

The standard protocol used for Internet e-mail messages.

SNMP (Simple Network Management Protocol)

The protocol governing network management and the monitoring of network devices and their functions.

Spoofing

The term for establishing a connection with a forged sender address. This normally involves exploiting a trust relationship that exists between source and destination addresses/systems.

S/WAN (Secure Wide Area Network)

An initiative to promote the deployment of Internet based Virtual Private Networks (VPN)

TCP/IP (Transmission Control Protocol/Internet Protocol)

The standard family of protocols for communicating with Internet devices.

Trojan horse

A software entity that appears to do something quite normal but which, in fact, contains a trapdoor or attack program.

URL Blocking

The tracking and denying of user access to undesirable web sites based on predefined site content.

User Administration

User Administration is a process aimed at creating users efficiently, controlling what they can do, limiting the damage they can cause, and monitoring their activities on a system or network.

ULA (User Level Authentication)

User Level Authentication refers to the ability to track the usage of a VPN connection to a given individual, on a specific machine, during a specific time period, by the assignment of a unique username. It also implies the restriction of patron use of the VPN in an anonymous manner.

Virus

A virus is a piece of programming code inserted into other programming to cause some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programming from other sites or be present on a diskette. The source of the file you're downloading or of a diskette you've received are often unaware of the virus. The virus lies dormant until circumstances cause its code to be executed by the computer. Some viruses are playful in intent and effect and some can be quite harmful, erasing data or causing your hard disk to require reformatting.

Virus Scanner

A program that searches files for possible viruses, including e-mail and attachments.

VPN (Virtual Private Networking)

A VPN is a technology that overlays communications networks with a management and security layer. Though VPN technology, network managers can set up secure relationships while still enjoying the low cost of a public network such as the Internet.

Web Attack

Any attack from the outside aimed at Web server vulnerabilities.

Worm

A type of virus that disables a computer by creating a large number of copies of itself within the computer's memory, forcing out other programs. Worm viruses are generally constructed to also copy themselves to other linked computers.