South African Journal
of Information Management
[DoE accredited]

Peer Reviewed Article Vol.2(1) June 2000

Intranet/Extranet security

A M Naven
anaven@worldonline.co.za

Contents

Introduction

,'… it’s natural to think that within company walls information is secure by definition.
But things aren’t that simple.'
(Benett 1996:127)

Data can be intercepted by organizations or individuals that will sell it to other parties, alter it, or use it for a variety of purposes. If the integrity and confidentiality of information cannot be protected, there is the potential that the Internet can create a great deal of damage (Ferraro, 1998:4).

This article does aims at finding an answer to the following:
What measures can an organization take to protect its confidential information assets within the computer network environment?

The answers will be discussed by means of the following issues:

- Why are security measures needed?
- What information security risks and threat agents are involved?
- What methods of protection does the information technology offer?
- Developing a security strategy and policy
- What part does trust play in the information security scenario?

For the purpose of this research an intranet was defined as a computer network, using the technologies developed for the global Internet, facilitating communication and distribution of information within an organization. An extranet is an extended intranet, based on Internet standard protocols, that allows people outside the enterprise to access the intranet via the Internet (Marchand & Davenport, 2000:349). Security is considered to be 'measures taken to guard against espionage or sabotage, crime, attack' (Merriam-Websters); 'the securing of buildings, valuables, government secrets, and the like from intrusion or theft' (Wordsmyth).

top

Why are security measures needed?

Data on an intranet is vulnerable for the following reasons:

- People in an organization are drawn from the general population, with its small but significant fraction of hackers, vandals, and opportunists. Adding to this risk is the widespread use of contract workers, who have little incentive to protect the organization's information assets.
- Not all intranets are internal. Private webs in a large organization may employ the Internet as a low-cost, wide-area network to send company data between regions.
- Even in the absence of malicious intent, an intranet without access controls is at risk of accidental erasure or overwriting of documents (Benett, 1996:128).

With the increase in cyber-terrorism and employee sabotage of company networks and IT systems, the need for tight enterprise-side network security is crucial for businesses to survive (Akesson, 2000:1). All computer networks that use the Internet infrastructure need additional protection by a secure system, for the following reasons:

- The protocols are insecure. There are absolutely no means within the protocol (e.g. DNS, ICMP, ARP etc.) to ensure that the system is talking to the right recipient on the other end.
- The operating systems are unable to protect themselves.
- Most applications lack security (Akesson, 2000:4).

What we expect from such a security system depends on what security demands there are, on how large the internal system is and how many domains are created (Akesson, 2000:3). Ensuring security on an intranet is a matter of verifying that users are who they claim to be, restricting data access where appropriate and encrypting confidential communications to prevent interception (Benett, 1996:128). Properly set up, intranet security can be an enabler, enriching the intranet with services and resources that it would not be possible to otherwise provide. Providing security increases the organization's ability to use the important collaborative aspects of an intranet (Evans, 1996:182).

top

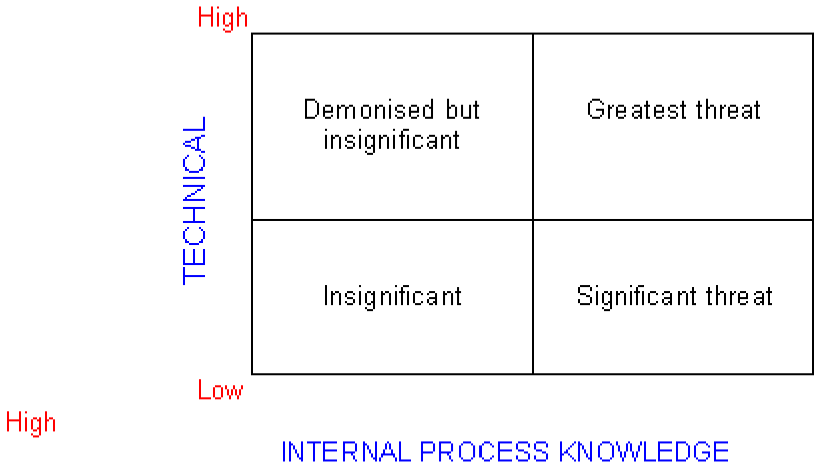
Information security risks and threat agents

Information security is at stake when:

1. There must be something of value to the organization (or which may represent a liability to the organization) if it is lost, altered, or inappropriately disclosed. This represents the risk.
2. The customer deploys layers of technology (hardware, operating systems, databases, transaction processing monitors, middleware, the applications themselves). Each is

imperfect, requiring a comprehensive set of baseline controls to describe and verify the desired security characteristics.
3. There is a person who desires to exploit the vulnerabilities in those technology layers to expose, alter, destroy or exploit the valuable and risky information (Malik, 1999:2).

Potential threat agents can be classified as depicted in Figure 1:
Figure 1 Who will be most likely to cause an information security breach (Malik, 1999:3)?



A person with low technical competency and little knowledge of basic business practices poses no real threat, except that such an individual may steal a PC for its cash value. An individual who has familiarity with internal business processes represents a significant threat. Most instances of computer crime involve insiders who abuse existing processes and avoid control measures to take money or cause damage. The technically skilled outsider is a convenient scapegoat, but in reality represents almost no threat. The skilled insider clearly represents the greatest threat, and represents the greatest challenge. Malik (1999:3) warns, 'Over time the number of skilled people will grow as computer literacy spreads, and our systems become more user friendly, fewer and fewer people will be outsiders'.

Surveys confirm Malik’s statements, indicating that internal users are responsible for most unauthorized activities. In addition, organizations that connect with business partners over private networks create a potential avenue for attack. Users on the business partner’s network may take advantage of the inter-company link to steal valuable information (Sheldon, 1996:3).

To maximize the value of intranet security, it should be allocated where, and to the extent that, it safeguards valuable data (Benett, 1996:128-129). Review the vulnerability of each of all the assets (data, documents, images and network resources people will have access to) for the following hazards:

- Exposure of sensitive material to unauthorised personnel (employees without a business need to know, temporary workers with intranet login privileges, or anyone else, if the intranet connects to the Internet.)
- Corruption or deletion of the asset. This hazard exists whenever multiple users have the ability to update shared information.
- Illegitimate or inappropriate use of shared resources. This includes files and application programs, as well as network peripherals such as printers, scanners, CD-ROM drives and modems.

Telleen (1996:2) identified three basic threat areas: storage, access and transfer. Discussions on each of these areas follow:

top

Storage protection

Storage protection refers to protection of the assets when they are not in normal use. Since intranet technology makes information location irrelevant to the logical display, one might consider storing truly sensitive content on a separately secured server with additional protection and special monitoring (Telleen, 1996:2).

top

Access control

Access security has improved dramatically over the past several years, driven largely by the Internet commerce movement. In addition to the basic password methods, systems that require physical tokens, some with challenge/response mechanisms, have become practical. Many of the servers and browsers also have the ability to create an encrypted transaction automatically before the user even provides a password, so the passwords and keys are encrypted before login. The most recent access control mechanisms are based on the ability of the Web server to tailor pages for specific users. Once a user has been authenticated, all interactions are mediated through an object layer that dynamically generates pages showing the user only the choices for which she has access privileges (Telleen, 1996:2).

Two ways of restricting access to the intranet environment are discussed in this paper. These are authentication methods and firewalls.

1. Authentication

Authentication is the process of verifying a user’s identity. Most networks, including intranets, can be set up to authenticate the user through a challenge/response dialogue, often taking the form of a username/password exchange. Authentication can either be by username and password, by the requestor’s IP address, or both. Stronger authentication is also possible with so-called 'public key' technology (encryption). Access control lists can be configured for server directories that allow or deny users access (Benett, 1996:129-130).

1.1. Restriction by user name and password:

Documents or directories are protected so that the remote user has to provide a name and password in order to get access. However, a password is only good if it’s chosen carefully. Obvious passwords can be guessed at, and WWW servers, unlike Unix login programs, don’t complain after repeated unsuccessful guesses. A determined hacker can employ a password-guessing program to break in by brute force. It is more secure to use a combination of IP address restriction and password than to use either of them alone. Another problem is that the password is vulnerable to interception as it is transmitted from browser to server. It is not encrypted in any meaningful way, so a hacker with the right hardware and software can pull it off the Internet as it passes through. In the situation where a browser sends the password each and every time it fetches a protected document, it is even easier for the hacker to intercept the transmitted data as it flows across the Internet. To avoid this, the data have to be encrypted (Stein 2000).

There are three aspects of username/password authentication:

- the username;
- the password that applies to the username; and
- what is permitted to that user when a correct username and password are supplied.

Usernames and passwords are meaningless unless a directory, directory tree, or filename is specified to which username/password access restrictions apply (Evans, 1996:189).

1.2. **Restriction by IP address, subnet or domain:**

Servers are using the TCP/IP hostname or numerical network address of customer workstations as access criteria. Servers look up hostnames using these addresses and the Domain Name Service. Rules can be set up based on either of these, making a considerable amount of fine-tuning possible (Evans, 1996:196). Individual documents or whole directories are protected in such a way that only browsers connecting from certain IP (Internet) addresses, IP subnets, or domains can access them. This method provides secure restriction against casual nosiness but not against a determined hacker. To be safe, IP address restriction must be combined with something that checks the identity of the user, such as a check for user name and password. It can be made much safer by running the server behind a firewall machine that is capable of detecting and rejecting attempts at spoofing IP addresses. Such detection works best for intercepting packets from the outside world that claim to be from trusted machines on the internal network. However, if a browser is set to use a proxy server to fetch documents, then the server will only know about the IP address of the proxy, not the real user’s. This means that if the proxy is in a trusted domain, anyone can use that proxy to access the organization’s intranet/extranet site (Stein, 2000).

Restriction by host or domain name has the same risks as restriction by IP address, but also suffers from the risk of 'DNS spoofing', an attack in which the server is temporarily fooled into thinking that a trusted host name belongs to an alien IP address. To lessen that risk, some servers can be configured to do an extra DNS lookup for each client. After translating the IP address of the incoming request to a host name, the server uses the DNS to translate from the host name back to the IP address. If the two addresses don’t match, the access is forbidden (Stein, 2000).

1.3. **Encryption using public key cryptography:**

Both the request for the document and the document itself are encrypted in such a way that the text cannot be read by anyone but the intended recipient. Public key cryptography can also be used for reliable user verification (Stein, 2000). A more detailed discussion on encryption methods follows later on in the article.

2. **Firewalls**

If the organization is also connected to the Internet, it should be ensured that the intranet is not generally accessible to the outside world. It’s a fact of Internet life that there are people who want to break into other people’s networks via the Internet. Reasons vary from innocent curiosity to malicious cracking to business and international espionage. The fact that IP addresses can be easily spoofed makes it essential to add a firewall as a protection mechanism (Evans, 1996:207).

Many companies and organizations base their security around a firewall. A firewall is a device that sits between a private, trusted internal network and the outside, public, untrusted Internet, providing secure access and communications between these two networks. Its purpose is to limit access into and out of the organization’s network based on the organization’s access policy. Firewalls permit desired services coming from the outside, such as Internet e-mail, to pass and to allow access to the WWW from inside the protected networks. The idea is to allow some services to pass and to deny others. Since a firewall is at least partly in the public eye, it can act as a storefront for the organization – a place to make brochure information about products and services available to the browsing public. Some firewalls can double as web servers (Evans, 1996:207; Benett, 1996:134). The safest firewall would block all traffic, but that defeats the purpose of making the connection, so selected traffic needs to be strictly controlled in a secure way (Sheldon, 1996:2).

The typical use of a firewall product in a network is to isolate corporate assets from each other and from the outside world in a secure and manageable manner. Multiple firewall devices can be installed to keep wily hackers out of the organization's networks. Any device that controls network traffic for security reasons can be called a firewall, and in fact the term 'firewall' is used in a generic way. Sheldon (1996:4-7) describes different strategies in the use of firewalls for protecting network resources:

2.1. **Packet filtering:**

Packets are first checked and then either dropped or allowed to enter based on various rules and specified criteria. Often called screening routers, they work in the lower layers of the network protocol stack. The router connects two networks and performs packet filtering to control traffic between the networks. They provide filtering based on information related to the hare-wired address of a computer, its IP address (network layer) and types of connections (transport layer). Administrators program the device with a set of rules that define how packet filtering is done. Those rules may be difficult to implement and error-prone, which could potentially open up holes in the network barricades.

2.2. **Proxy server gateways:**

A proxy server is a component of a firewall that controls how internal users access the outside world (the Internet) and how Internet users access the internal network. Application-level proxy servers provide a high level of protection. In some cases, the proxy blocks all outside connections and only allows users to access the Internet. In other cases, both inbound and outbound traffic are allowed under strictly controlled conditions (Sheldon, 1996:2).

A proxy server gateway acts as an agent for a user who needs to access a system on the other side of the firewall. They operate at the upper levels of the protocol stack and provide proxy services on external networks for internal clients and perform advanced monitoring and traffic control by looking at certain information inside packets. The proxy service changes the IP address of the client packets to essentially hide the internal client to the Internet, and then it acts as a proxy agent for the client on the Internet. Using proxies reduces the threat from hackers who monitor network traffic to pick up information about computers on internal networks. The proxy hides the addresses of all internal computers. There are two types of proxy servers:

- Circuit-level gateway: This type provides a controlled network connection between internal and external systems. A virtual 'circuit' exists between the internal client and the proxy server. Internet requests go through this circuit to the proxy server, and the proxy server delivers those requests to the Internet after changing the IP address. External users only see the IP address of the proxy server. While traffic is allowed through, external systems never see the internal systems. This type of connection is often used to connect 'trusted' internal users to the Internet.
- Application-level gateway: Provides all the basic proxy features and also provides extensive packet analysis. When packets from the outside arrive at the gateway, they are examined and evaluated to determine if the security policy allows the packet to

enter into the internal network. Not only does the server evaluate IP addresses, it also looks at the data in the packets to stop hackers from hiding information in the packets.

One of the problems with proxies is that they must evaluate a lot of information in a lot of packets. In addition, a separate proxy needs to be installed for each application (FTP; HTTP; SMTP). This affects performance and costs. A new class of firewall product has emerged that uses stateful inspection techniques.

2.3. **Stateful inspection techniques:**

Instead of examining the contents of each packet, the bit patterns of the packets are compared to packets that are already known to be trusted. While stateful inspection provides speed and transparency, one of its biggest disadvantages is that inside packets make their way to the outside network, thus exposing the internal IP addresses to potential hackers. Some firewall vendors use stateful inspection and proxies together for added security.

2.4 **Virtual Private Network (VPN):**

This is an extension of standard firewall capabilities to permit authenticated, encrypted communications between sites over the Internet. Using a VPN, users at a remote site can access sensitive data at another site in a secure fashion over the Internet, making it possible to extend the availability of the intranet to remote company sites without having to set up a private network. All the data that flows on the public Internet backbones is encrypted before it leaves the local network, then decrypted when it arrives at the other end of the connection.

A firewall is not a stand-alone device. It needs to be managed and monitored on a regular basis. Action needs to be taken in the event of an attack. It is also only one part of the defence. If attackers do get inside, they should be kept from looting the systems by implementing security measures at each domain and server (Sheldon, 1996:5).

Once in place, a firewall requires constant observation. Security policies and procedures must be put into place. No firewall can protect against inadequate or mismanaged policies. A weakness in the policy or the inability to enforce the policy will weaken any protection provided by even the best firewalls. Security policies must be outlined in advance so administrators and users know what type of activities are allowed on the network. Sheldon (1996:7-8) identified some issues that the policy statement should address, namely: internal and external access; remote user access; virus protection and avoidance; encryption requirements; program usage; as well as the following considerations:

- Network traffic to and from outside networks such as the Internet must pass through the firewall.
- Do not run any services on the firewall except those specifically required to be provided by firewall services.
- Do not allow any passwords or internal addresses to cross the firewall.
- Evaluate what kind of traffic to be allowed from the external side of the network. Electronic mail is the usual requirement.
- If users are accessing the Web with Web browsers, implement Web client-server security protocols and encryption techniques.

However, a firewall offers only a perimeter protection. A part of the solution is to partition the internal network into secure domains and use secure gateways to control accesses between them. The internal security domains must have strong external protection and only authenticated users have access to the servers within. External traffic to the domain should be encrypted to prevent password sniffing and packet modification (Akesson, 2000:1-3).

Firewalls can be extremely effective at keeping 'outsiders' out. Allowing remote users to access intranet resources is one of the trickiest security problems to be faced. A partial solution is to employ secure Web servers inside the organization. The firewall is configured to allow public key encrypted packets. However, even though the risk from packet sniffers is reduced, an interceptor could gain access by playing back the encrypted packets. Two approaches have become standard to get around this problem:

- The user generates sequences of one-time passwords prior to leaving the organization. Every time the user logs in remotely, he uses the next password in the sequence. Playback of intercepted passwords is unsuccessful.
- Challenge/response calculators or tokens are portable calculators that encrypt a random message from the firewall each time the user attempts to log in. The encryption method is unique for each calculator and known by the firewall. Thus, the only person who could generate the correct encrypted 'response' to the firewall is the user with the right calculator. No passwords are necessary; the user’s name and possession of the token authenticate him (Benett, 1996:135-136)

top

Protecting information in transit

Valuables in transit make attractive targets for thieves. The same is true in the virtual world. Unless a closed, secured network is used, information can always be hijacked in transit. And, even in a closed network, the information can be hijacked without extraordinary precautions. The major way to protect it is to encrypt the transmission or the information on the page (Telleen, 1996:2).

In addition to encryption techniques, some organizations have developed methods for strategically breaking content into anonymous chunks for transmission and presentation. This can be done at two levels. Since the user generally knows what they accessed, a page with sensitive information may be designed without any identifying contextual information on it. The second level is at the packet level. When information is sent over the intranet, the content is broken into small packets, and the packets are reassembled at their destination. The information can be divided in such a way that no single packet contains enough data to derive the sensitive information. On a busy, diverse intranet, finding enough of the right packets to reconstruct the message is like finding a needle in a haystack. If each packet is encrypted with a different key, the task becomes almost impossible (Telleen, 1996:3).

1. **Encryption**

Data encryption is the solution to problems like packet sniffing and session hijacking (Sheldon, 1996:5). Modern encryption is achieved with algorithms/mathematical formula that use a 'key' to encrypt and decrypt messages by turning text or other data into digital gibberish and then by restoring it to its original form (Froomkin & Branson, 1998:2).

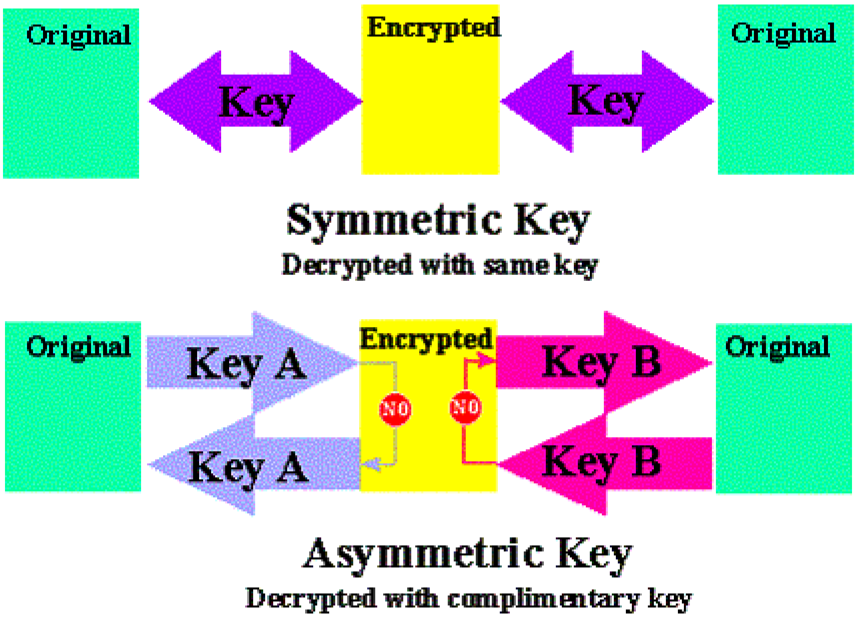
Benett (1996:131) describes encryption as the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. In a multi-user setting, encryption allows secure communication over an insecure channel. He says that encryption works by encoding the text of a message with a key, which is just a very long number. Typical keys are 40, 64, 80 or 128 digits long, with the longer keys affording stronger encryption. A key’s strength refers to the amount of computation required to crack it.

A person who needs to send a message to a recipient encrypts the message with the recipient's public key. The message can only be read by decrypting it with the recipient's private key. This way, anyone can send a secure message, but only the intended party can read it. A digital certificate is needed to set up a server capable of secure communications. Certificates confirm that the person holding a public key is who he claims to be. In this sense, certificates are the ultimate in user authentication, and digital signatures based on private keys offer the highest level of trust (Benett, 1996:132).

Encryption is perhaps the single most important technology for network security and it has uses beyond protecting information in transit. Many encryption algorithms can be used with other algorithms to ensure the integrity of the electronic content, that is, to ensure that someone has not changed information in contracts or other legal documents after the parties have reached agreement. Some encryption approaches require special hardware, some use tokens (disks or smart cards) and others are strictly software (Telleen, 1996:3).

Telleen (1996:3) distinguishes two types of keys in use today. The first is called a symmetric key, because the same string of characters is used both to encrypt the information and to return the information to normal form. The second is called an asymmetric key, because the string of characters used to encrypt the information will not return it to normal form. A different string of characters is required to decrypt the information. Figure 2 explains these two processes in a visual format.

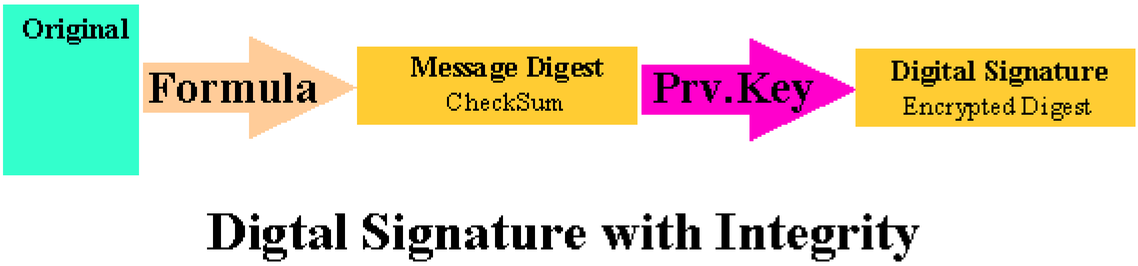
Figure 2 Symmetric and asymmetric encryption keys (Telleen, 1996:3)



Asymmetric keys have some very pragmatic uses. One of the keys can be made public while the other is held in private. This way if someone wants to send an encrypted message, the message can be encrypted using the receiver's public key knowing that only the receiver can decrypt it. The other use of asymmetric keys is for digital signatures. A message encrypted with a private key can only be decrypted with the public version of the same key. Since each private key belongs to a specific person, this acts as a digital signature (Telleen, 1996:4)

In reality digital signatures involve a more complex process that provides even more protection from tampering than physical signatures. This involves integrity techniques that are used to ensure that the information received is the same as the information that was sent. This is important for several reasons. First, an error in transmission may have altered or dropped an important piece of information. Second, someone may have maliciously altered the information even though they could not decrypt it. Like encryption, a mathematical formula is involved. In this case it takes the entire set of information and reduces it to a unique numeric sequence. If one bit in the information changes, the resulting sequence will not be the same. The unique sequence, called an integrity check sum, is created and sent with the message. On the other end, a new check sum is calculated and compared to the original. If they match, the message is guaranteed to be the same as sent. The check sum is also called a message digest. A digital signature is used by encrypting only the message digest (or check sum) of the document if the information itself is not sensitive. If the decrypted message digest matches that of the current document, it ensures that the person whose public key decrypted the document 'signed' it, and it ensures that the document being looked at has not been altered since it was signed. This is why even when an entire document is encrypted the digital signature still includes the message digest. It ensures the document has not been altered after the signature (Telleen, 1996:4-5). Telleen (1996:5) explains the process as depicted in Figure 3:

Figure 3 The use of encryption as a digital signature to indicate message integrity (Telleen, 1996:5)



2. **Certification**

A word often mentioned alongside encryption is 'certification'. In transactions where something of value will change hands one would like to certify that the person or company on the other side is who they say they are. This is the problem certification attempts to solve. Electronic certification uses multiple digital signatures to certify the authenticity of the parties. The originating party might provide a certificate with their information on it. Part of that certificate is a digital signature and certificate of the authorizing reference. The digital signature of the reference is based on the check sum of the public information including their certificate, thus assuring that none of the public information has been altered. The reference's public key ensures that they really 'signed' the certificate, their digital signature ensures the integrity of the information and their certificate contains a reference certifying that they really are who they say they are. Where certificates are used today most do not involve more that three levels of certificates (Telleen, 1996:5).

3. **Packet screening**

Packet screening is primarily used for information entering an intranet from outside. This is software that looks inside each packet received before it is allowed inside the firewall. The packet is screened for information patterns that look like viruses or attempts to break security barriers. Suspicious packets are logged and kept from entering the intranet. (Telleen, 1996:6).

top

Developing a security strategy and policy

The issues of strategies and policies have been mentioned throughout the discussion. It has been said that 'no firewall can protect against inadequate or mismanaged policies' (Sheldon, 1996:7) and 'a security solution is only as good as the weakest link' (Malik, 1999:5).

1. **The security policy**

The most important, time consuming and contentious activity in implementing a security policy will be determining what information needs to be protected. No amount of technology can help with this process, because the factors are individual perceptions and comfort levels. The security policy sets the processes and ground rules for determining how information gets put into or taken out of restriction categories. Decisions on specific information will be made by the individuals who own the information (Telleen, 1996:8).

The first step is to document an intranet security policy. This document should consist of two parts: a goals statement and a responsibility statement.

- The goals should indicate where the enterprise stands on the balance of value versus cost, business requirements versus risk, openness versus gate keeping and what constitutes the optimum balance for the enterprise. Does the policy allow access to everything unless specifically identified for denial, or does it deny access to everything unless specifically identified for access. These will have very different effects and impacts on the culture, productivity and innovation of the organization.
- The responsibility section provides a clear statement of how security will be administered within the enterprise including:
    - who (what organization and position) is responsible for maintaining and monitoring the corporate intranet security strategy and policy
    - who reviews and approves that strategy and policy
    - a description of how this function and strategy fit with other security organizations in the enterprise, and what is expected of each organization.

The second step in creating an intranet security policy is creating a written process that describes how responsibility for intranet security will be delegated, implemented and enforced. This includes a management section and an individual employee section.

- The management section contains a description of responsibilities at each organizational and management level. Another important part of this section is the security objectives and how they will be monitored. Where appropriate, standards may be provided that help the manager make decisions consistent with the corporate goals and policies. Standards and security classifications can be particularly useful in helping managers determine when they need to classify (or should not classify) a specific type of information.
- A very clear statement of employee responsibilities, expectations and sanctions is required for an effective security implementation. However, the statement is not sufficient if employees are not aware of its existence. A well-defined employee communication program should follow the statement. The programme must address not only the initial introduction of expected responsibilities to each employee; it also must include an ongoing awareness and refresher programme. This can be done in conjunction with other security awareness programmes and with other Internet standards programmes.

The final required part of an intranet security policy is the definition of an audit program to monitor and manage compliance and risk. The important point here is that the security policy should explicitly call for regular audits, both internally and by independent auditors, and define how they will happen and who in the enterprise will be apprised of the results. A program of continuous logging, analysis and monitoring of activity for suspicious patterns is critical for servers with sensitive information (and this includes the firewall that protects the intranet). A program of active intrusion testing, looking for vulnerabilities, is also a good idea (Telleen, 1996:8).

2. **The security strategy**

Telleen (1996:6) warns that security strategies should not be based on current or future products or technology. They need to be based on the functional needs and risks of the organization. The toughest part of developing a security strategy is determining what needs to be secured, and from whom. Security is not free. Every time the security level is tightened, the organization pays in terms of increased complexity of access, increased response time and reduced communication. Security is a balance of value, risk and practicality.

An effective information security strategy includes a balanced emphasis on many factors:

1. Soundness of design
   The strength of the basic technologies VENDOR FOCUS
2. Robustness of functionality (features)
   The robustness of specific security technologies
3. Operability (performance; scalability; integration)
   The operation of the technologies in conformance
   with the desired level of control
4. Acceptability (cost; productivity; appearance)
   The acceptability of those controls with the
   affected personnel USER FOCUS
5. Sustainability (administration; maintenance; support)
   The continuing burden of technology and platform support
   and maintenance as the application environment evolves.

Malik (1999:5) is of opinion that too often excessive focus is placed on the first two points, being driven by vendor emphasis who are generally not concerned with issues of operability, acceptability or sustainability.

top

Trust

According to Ferraro (1998:1-2), it is not possible to separate the issues of technology, security, and trust. While firewalls are keeping Internet intruders out, internal users might be looting the organization's systems. Separate departments, workgroups, divisions, or business partners might have to be set up, using the same firewall technology, and encryption might have to be implemented throughout the organization. Firewalls also do not protect against leaks, such as users connecting to the outside with a desktop modem. In addition, if some new threat comes along, the firewall might not be able to protect against it. Viruses and misuse of security devices are also a threat (Sheldon, 1996:5).

All the security precautions in the world can't protect any intranet from overall poor security practices. Poor user choices of passwords always lead the list of computer and network security risks. Users with privileged access should not leave their workstations unattended without any sort of active screen or office door lock, as anyone can sit down and browse the files and directories that are supposed to have limited access. While customers are being educated about such everyday security matters, a potential security breach like this can be harmful to the whole security effort (Evans, 1996:186;196)

The bottom line is that the organization needs to trust its employees, because information security violation can occur in a perfectly secure intranet/Internet communication action involving people who have authorised access to privileged information.

top

Conclusion

Telleen (1996:6) identifies three kinds of activities that organizations attempt to stop:

- Unauthorized access to information
- Unauthorized changes to information
- Malicious destruction of information or processes (including introducing viruses)

The processes discussed in this article supplies methods for dealing with all three. While point products continue to improve, integration and staffing challenges will severely impede customers’ ability to achieve adequate enterprise security during the next five years. Secure, distributed implementations are rare for three major reasons:

- Today’s client operating systems lack basic security functions, such as system integrity, identification and authentication, and audit
- Most network infrastructures do not support privacy, authentication or access control.
- The physical security of the system is impossible to guarantee because of the sheer number of components and their wide geographic dispersion.

Regardless of the technology used, any of these factors will serve as the 'weakest link' in the trust model (Malik 1999:14).

However, the real problem seems to be that insiders are involved in most of the significant information security breaches (Malik, 1999:3). Therefore the toughest issues around security are not technical, but organizational and strategic (Telleen, 1996:1). Before deploying any information tool, senior managers should consider the following: Assuming that an employee observes someone doing something on the computer that might be inappropriate:

- Would the employee know if the action was right or wrong?
- Would the employee choose to report the wrong action?
- Would the employee know how to report the wrong action?

Further more:

- Does the enterprise teach awareness of security issues?
- Does it have a culture that supports security?
- Are there management mechanisms in place to reinforce that culture? (Malik, 1999:1).

The vast majority of data leaks in break-ins result from human error or carelessness. Closing that risk is a matter of policy, education and enforcement (Benett, 1996:134).

top

References

Akesson, L. 2000. Is a firewall secure enough? Intranet Design Magazine. March 2000. [Online] Available WWW: http://idm.internet.com/articles/200003/se_03_29_00a.html.

Benett, G. 1996. Secure Web servers on an intranet. In: Introducing intranets. Indianapolis: Que. p.127-136

December, J. 1996. Units of analysis for Internet communication. Journal of Computer Mediated Communication v1(4):1-22 March 1996. [Online].http://www.ascusc.org/jcmc/vol1/issue4/december.html

Evans, T.. 1996. Intranet security. In: Building an Intranet. Indianapolis: Sams.net. pp181-209.

Ferraro, A. 1998. Electronic commerce: The issues and challenges to creating trust and a positive image in consumer sales on the World Wide Web. FirstMonday. Issue 3 1998. [Online] Available WWW: http://www.firstmonday.dk/issues/issue3_6/ferraro/index.html.

Froomkin, D. & Branson, A. 1998. Deciphering encryption. Washingtonpost.com Encryption Special Report 8 May 1998. [Online] Available WWW: http://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm.

Malik, B. 1999. Information security scenario: Are you feeling secure? In: The future of IT: Planning for the business focussed IT organization beyond the Millennium. (Cape Town: 2 August 1999) Conference presented by Gartner Group IT Management Advisory Services.

Marchand, D.A. & Davenport, T.H. (eds). 2000. Mastering information management. London: Prentice Hall.

Matisse, E. 2000. Glossary of Internet Terms. [Online] Available WWW: http://www.matisse.net/files/glossary.html.

Merriam-Webster Online Dictionary. 2000. [Online] Available WWW:http://www.mw.com.

Sheldon, T. 1996. General firewall white paper. Windows NT Security Handbook McGraw-Hill. November 1996 [Online] Available WWW: http://www.ntreseach.com/firewall.htm.

Simmonds, M.D. 1999. Search Engine Terms: as suggested by members of the I-Search Digest [Online] Available WWW: http://cadenza.org/search_engine_terms/srchsz.htm.

Stein, L. 2000. The World Wide Web Security FAQ: Protecting confidential documents at your site. 24 March 2000. [Online] Available WWW: http://www.w3.org/Security/Faq/wwwsf3.html
Telleen, S.L. 1996.

Security and availability. Intranet Organization Chapter 5 1996. [Online] Available WWW: http://www.iorg.com/intranetorg/chpt5.html

Wordsmyth Dictionary 2000 [Online] Available WWW: http://www.wordsmyth.net

top

APPENDIX 1: Glossary of terms

The following terms are used in this discussion, but not explicitly defined:

Application A piece of software designed to meet a specific purpose (Marchand & Davenport, 2000:349)

Browser A Client program (software) that is used to look at various kinds of Internet resources (Matisse, 2000)

Domain A range of IP addresses, corresponding to a particular network on the Internet. (Benett, 1996:9)

Gateway The technical meaning is a hardware or software set-up that translates between two dissimilar protocols. Another, sloppier meaning of gateway is to describe any mechanism for providing access to another system. (Matisse, 2000)

Hacker An expert at programming and solving problems with a computer; A person who illegally gains access to and sometimes tampers with information in a computer system (Merriam-Webster, 2000)

IP address The location of all computers on the Internet is uniquely specified by a set of four numbers separated by periods, e.g. 159.74.20.254. IP addresses can be assigned a mnemonic – Fully Qualified Domain Name (FQDN) (Benett, 1996:9)

Operating system Software that controls the operation of a computer and directs the processing of programs (as by assigning storage space in memory and controlling input and output functions) (Merriam-Webster, 2000)

Packets Protocols break a message into bundles of data before sending it. Each packet contains information about who sent it and where it is going, in addition to user data. (Benett, 1996:156)

Protocol The language that one computer uses to communicate with another (Marchand & Davenport, 2000:350), e.g.:
FTP – File Transfer Protocol
HTTP – HyperText Transport Protocol
SMTP – Simple Mail Transport Protocol
TCP/IP – Transmission Control Protocol/Internet Protocol (This is the suite of protocols that defines the Internet)

Server A computer and its associated hardware and software applications that act as a repository for information files or software programs (December, 1996:5)
A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running (Matisse, 2000)

Spoofing The alteration or creation of a document with intent to deceive an electronic catalogue or filing system. Also known as spamdexing or spamming. (Simmonds, 1999)

Disclaimer

Articles published in SAJIM are the opinions of the authors and do not necessarily reflect the opinion of the Editor, Board, Publisher, Webmaster or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special, incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user’s use of the Website.

ISSN 1560-683

Published by InterWord Communications for the Centre for Research in Web-based Applications,
Rand Afrikaans University