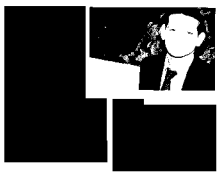
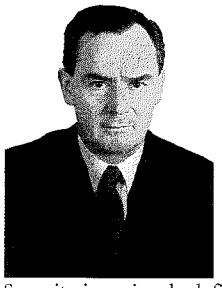
Publication: Irish Computer
Date: Tuesday, November 16, 2004
Page: 20
Extract: 1 of 6
Circulation: 10.237
Author:
Headline: SECURITY IS AGELESS



SECURITY IS AGELESS

NAPIER WILLIAMS LOOKS AT THE REASONS FOR TAKING A TOP-LEVEL HOLISTIC APPROACH TO THE IMPORTANCE OF ORGANISATIONAL SECURITY.



Colm Murphy, technical director with Espion.

Security is variously defined as the quality or state of being secure and freedom from danger, fear or anxiety. It is also the provision of protection involving measures taken to guard against espionage, sabotage, crime, attack and escape according to Merriam Webster's Colligate Dictionary.

The above has been chosen as the starting point to underline the importance of taking a top-level holistic approach to the importance of organisational security. In today's environment it is highly unlikely that any organisation can be free "from danger, fear or anxiety" but an organisation can certainly improve its prospects despite all the threats. In this article we look at some of the protective measures that can be put in place. The bottom line is that the breaches of and enforcement of security is mainly about people. Colm Murphy, technical director with Espion, said that when conducting penetration tests only about 60 per cent of the tests achieve penetration but when social engineering tests are conducted involving soliciting information from employees about 90 per cent are successful proving yet again that the weakest link is people.

There is an old maxim in management to the effect that if you cannot measure something you cannot control or manage it. Thus the starting point is to identify what is of value to the organisation, what needs to be protected and to establish the value of these assets. Mark Smith and Philip Sloan, security architects with HP, explained that risk assessment is used to identify key assets and the controls that are in place. Gareth Price, security solutions designer with EsatBT, said that the company is a significant player in the consultancy, design and support areas. In the security area the company provides risk assessment, compliance and regulation assessment, technical design and solutions and performance appraisal. Division of responsibilities another old accounting practice usually implemented for security reasons should still have its place in the modern organisation.

Publication: Irish Computer
Date: Tuesday, November 16, 2004
Page: 20
Extract: 2 of 6
Circulation: 10.237
Author:
Headline: SECURITY IS AGELESS

Employees should work on a need-to-know basis with sensible divisional boundaries.

TECHNICAL

In technical terms networks should be segmented. Checkpoint market a product called InterSpect, an internal security gateway that is designed to stop the spread of worms in an organisation by segmenting the network for different departments. InterSpect intelligently inspects internal traffic to identify and block unauthorised or malicious behaviour as well as specific attacks. It uses sophisticated security segmentation to prevent unauthorised access between network zones and quarantines computers generating suspicious activity.

Establishing the policies and rules around security is a non-trivial exercise that requires the involvement of top-level management. These are the people that should understand what is of value to the organisation and will in any event have to carry the can for security breaches a task that is becoming more onerous under recent legislation and pending legislation not to mention industry regulations. Senior management, in many cases, do not appreciate how dependent their organisations have become on the IT infrastructure and the extent to which IT has become interwoven with business processes.

Gerry Carroll, Entrysys's director of channel and marketing, said that there is a broad level of understanding of risks but there is little understanding of how dependent organisations are on IT. This disconnect was also underlined in a recent survey conducted in EMEA on behalf of BMC Software where 52 per cent of IT decision makers believed that business and IT strategies are not in harmony.

Once the policies have been established rules can be formulated to help ensure that the policies become practice. An essential part of this process is persuading employees to "buy-in". As Emmet Rafferty, CEO of Topsec, stated organisations should have clearly spelled out policies that members sign-up to that are backed-up by a sensible level of administration. This involves training and in many cases a significant cultural shift to accept that security is not an optional extra but rather a key part of daily activity that does not necessarily end when leaving the place of employment. We are living in an era of rapid change thus there will be changes in the relative importance of the assets being protected, in the nature of the threats, and in the tools and methods that are available to challenge these threats. Systems must be reviewed on a regular basis preferable by an outside agency. HP's Smith and Sloan indicated that typically these reviews should be annual.

Publication: Irish Computer
Date: Tuesday, November 16, 2004
Page: 20
Extract: 3 of 6
Circulation: 10.237
Author:
Headline: SECURITY IS AGELESS

I.T. STUFF

One of the common threads that ran through many of the interviews conducted for this article is the need for a multi-tiered approach to protection. The high fortress wall and moat approach of yesteryear is no longer adequate as the sophistication of threats escalates and the sources of threats come from many different directions including internal and external. The need to react more quickly has been adequately underlined by the world wide success of such worms as Blaster that could in many cases have been avoided by keeping patches up to date.

Real-time reaction using IDP (intrusion detection protection) has become an imperative for many organisations. The breath of threats has lead to the development of many different solutions that have to be purchased, implemented and managed. This increasing management overhead is unsustainable especially in smaller organisations and it comes as no surprise to see the recent emergence of appliances that bundle a number of protective features.

Just like the proliferation in the variety of threats the number of threat combatants keeps growing. Anti-virus has long been a given and most systems are now automatically updated preferable on a daily basis. Hugh Marron, business development manager with IPOtions recommends that organisations should deploy two different anti-virus protection programs covering the flow of data in both directions.

Firewalls have long been seen as an essential defence and while their name may seem to suggest the obvious in realty they are little understood by the non-technical. Windows XP has a firewall that is set on by default with Service Pack 2 but as Espion's Murphy explained this does not support packet inspection and does not have any anti virus or intelligence built-in. Content filtering has come to the fore with the apparent ever-increasing volume of spam e-mail. There are many anti-spam products and service providers. Topsec have a service called Blockmale that provides an e-mail scanning service and many service providers offer similar facilities.

IDS (intrusion detection systems) have been round for many years providing information "after the fact" about unauthorised or unusual activity on the network. These systems are not designed to stop malevolent activity and it comes as little surprise to find that IDP systems coming to the fore as they provide active protection by blocking the malevolent activity. Both IDS and IDP can lead to false positives by unintentionally reporting or blocking valid network activity.

Putting many of these security tools together we have appliances like Espion's Fortinet that supports six security features including firewall and VPN, content management, URL filtering, QoS, file blocking and anti virus scanning. Outsourcing is used in many IT areas including the security arena where usually only parts of the security function are outsourced. Topsec provide extensive communication services from monitoring centres and has added IT services to monitor servers, IDS and firewalls.

Publication: Irish Computer
Date: Tuesday, November 16, 2004
Page: 20
Extract: 4 of 6
Circulation: 10.237
Author:
Headline: SECURITY IS AGELESS

BOUNDARIES

Wireless LANs do not have to be any less secure than wired LANs providing secure installation procedures and sensible practices are followed. According to Conrad Simpson, managing director of Celare, the rules and policies for a wired network should be established before implementing a wireless network with its additional risks. Devices that connect to a network should were practical be pre-identified using fixed IP addresses and MAC (media access control) identification. While MAC spoofing can fool authentication systems the more barriers that are deployed against potential intruders the less likely they are to gain access. Wireless devices that are not being used with wireless LANs should be reconfigured to ensure that they do act as passive devices that can be easily hijacked to gain access into the corporate network. Peer-to-peer wireless connections should be avoided, as they are seldom secure.

Mobile users with laptops and other devices do not have to be seen as a security nightmare providing they are properly managed. Conventional wisdom says that they should connect into the corporate network using secure VPN (virtual private network) and encryption. Combine this with strong authentication requiring at least two features such as password and some biometric measure or something like Happy Meal from CryptoCard that generates a one-time password. The latter has become quite affordable costing $499 for a five-user system (www.cryptocard.com).

As Espion's Murphy said, laptop users must not be allowed "to have two arms to the internet", in other words users should only be allowed to log on to the internet through the corporate internet connection to avoid the possibility of foreign agents taking over some of the laptop functions. A key requirement is keeping anti virus, patches and other security software up to date. Part of the log-on authentication should check and if necessary perform the required updates. Personal firewalls should be maintained on all notebooks and all sensitive data should only be stored in an encrypted format.

While some may argue that you can never have too much insurance the reality is governed by cost. In the case of IT security it is a ques-

Publication: Irish Computer
Date: Tuesday, November 16, 2004
Page: 20
Extract: 5 of 6
Circulation: 10.237
Author:
Headline: SECURITY IS AGELESS

Emmet Rafferty, CEO of Topsec.

Hugh Marron, director of IPOptions.

tion of balancing the risk against the cost of security. The risks vary from industry to industry with banking and finance at the higher end of the scale. According to Simpson, MD of Celare, the normal expenditure on security measures appears to be about three to four per cent of the IT budget but in the case of financial organisations this can be as high as eight per cent. These percentages are expected to grow with many organisations likely to pay out six to eight per cent. Gartner have published figures that indicate that the cost of the security element in a new web based project should be in the range of 12 to 15 per cent.

WRAP-UP

The nature of security threats is altering with the increasing role of organised crime. One of the emerging trends thrown up by Espion's Honeynet Project is the increasing incidence of security hacks by organised criminals. The medium, of exchange that shifted from barter to money hundreds of years ago is now shifting to electronic impulses that are much more difficult to track due to their invisibility. New legislation and industry regulations are mandating organisations to put the necessary procedures in place to ensure that the risks are minimised.

Like most human endeavours there will always be people seeking shortcuts to riches. IT security will be an ongoing problem although the methods of attack will change and organisations will have to adopt new tools to protect their infrastructure. Reaction times to new threats will be shortened and possible solutions like predictive technologies will probably come into play while more sophisticated analysis of internet activity will help to pinpoint potential sources and methods of attack. The underlying lesson is that human participation will continue to play a key role in ensuring damage limitation while IT tools will continue to grow in sophistication to combat these threats.

Publication: Irish Computer
Date: Tuesday, November 16, 2004
Page: 20
Extract: 6 of 6
Circulation: 10.237
Author:
Headline: SECURITY IS AGELESS

CONTACTS:		
Cable & Wireless	www.cw.ie	01 404 0333
Celara	www.celare.com	01 633 1506
CheckPoint	www.checkpoint.com	+44 1276 713 600
Cisco	www.cisco.com	01 819 2700
Computer Associates	www.ca.com	01 478 0800
Complete Network Technology	www.complete.ie	01 885 5400
Enterasys Networks	www.enterasys.com	087 907 8811
EsatBT	www.esatbt.com	1800 924 924
Espion	www.espion.ie	01 663 6326
IPOptions	www.ipoptions.com	01 824 3772
Hewlett Packard	www.hp.com	01 615 8200
Microsoft	www.ms.com/spam	01 671 6255
NetScreen	www.netscreen.com	+44 8700 750 000
Novell	www.novell.com	01 605 8000
Renaissance	http://www.renaissance.ie	01 280 9410
Rits	www.ritsgroup.com	01 642 0500
Software Security	www.softwaresecurity.ie	051 851 625
Topsec	www.topsectechnology.com	01 466 0686