Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 79 (2001)

Heft: 9

Artikel: The enemy within

Autor: Cheney, John

DOI: https://doi.org/10.5169/seals-876570

ISSE

The Enemy Within

While most IT security threats are perceived to be entirely external, mounting evidence shows that malcontented or misguided employees within the firewall actually pose the more immediate commercial threat. John Cheney, managing director of managed security services company, Activis, discusses the nature of the threat and the countermeasures available to keep hackers at bay.

JOHN CHENEY

The notion that most breaches of security are external is increasingly being overturned as research shows that network managers need to apply more stringent security within the firewall. A survey from Activis, in conjunction with sister company, Integralis, illustrated the scale of the problem when it analysed 146 companies in March this year. Of the known security breaches, it determined that a significant 81% of threats were internal with an extra 13% originating from ex-employees; just 6% of the breaches were pinned on external hackers.

Where are the threats?

Whereas most security policies balance the need for openness with restricted access to important business information, internal breaches typically arise where employees are not actively prevented from gaining unauthorised access to sensitive parts of a company's management information system.

Disgruntled staff, contractors and staff with insufficient knowledge of the damage that could be inflicted pose a threat that is often overlooked by network managers. For example, simple passwords or passcodes unwittingly provided to onsite contractors or over the phone can open up many opportunities for the serious hacker or malcontented employee. Often encountering lax perimeter security, hackers can easily penetrate soft security environments and access commercially sensitive data at will.

In premeditated cases, the serious hacker can plant "time bombs" which trigger attacks within the firewall long after they've left the company, often with catastrophic results. More technically-minded hackers can even breach company security via back-door access previously set up while in employment.

Inappropriate use of the Internet is also deemed a threat as staff spending vast amounts of time surfing for bargains, downloading offensive material and using e-mail to send inappropriate material could equally compromise an IT systems performance. Although such usage may not directly lead to major security problems, staff indulgences can quickly lead to overloading network bandwidth and subsequently lowering performance, at best, and bringing down the network entirely, at worst.

Occupational Spam is another area of Internet misuse but of no less concern, as is the very real possibility of prosecutions of business under the rules of vicarious liability. This means that employers are vicariously liable for the information that their employees might send via e-mail or download from the Internet. To prevent potential lawsuits thus requires adequate policy and training.

While external and geographically remote attacks from hardcore hackers who vandalise websites, initiate denial of service attacks and commit actual theft and destruction of data (or just tampering with information) may appear less frequent, these can and do typically undermine company security which could lead to commercial ruin. And, as the results on www.attricon.org show, these are on the increase. In fact, in 2000 there were a total of 5218 known hacks whereas in the first four months of 2001, this figure was already 4200.

Monitoring is essential

Arguably, many network managers possess neither the time nor specialised skillset – but mostly the time – to run and administer 24 x 7 security monitoring. Establishing a firewall and running the security must be viewed as a process and not an event. Both time and effort must

be applied to ensure the correct level of security is introduced and continually maintained.
Equally pressing is the need for the problem to be addressed by management. Precisely because the countermeasures needed involve computer user policy and contract enforcement, internal surveillance needed requires both management action and technical competency.

Keeping risks at bay

Although technical safeguards are needed in the first instance, often involving regular and thorough system backups, reviewing user access and privileges, introducing access control systems and policing password policies, the overwhelming requirement is management recognition of the issue – before it becomes a problem.
Prevention is not just better than cure but vitally important to a company's IT system well-being. Management not only needs to appreciate that security barriers are needed but that the investment required may actually stretch their resources. Taking network managers away from running an enterprise network to police a company's security policy will not necessarily be practical or desirable. Most security needs to be completely 24 x 7 and, while crucial to the business, the justification of diverting network managers to guard against attacks isn't an easy one. The time taken to monitor both sides of firewall and implement software patches, etc requires continual maintenance and monitoring. And unless security is kept up-to-date it's unlikely that any firewall will keep pace with the next security breach, be it virus or hacker.
To conclude, companies need to realise that security is a not just about technology. In fact it is a three stage virtuous circle comprising policy, management and technology. Policy decides how the security is to be managed, what is allowed or acceptable and might include an employee Internet usage policy. The technology should be best of breed and the management needs to ensure everything is up to date in order to assess all risks all the time. [4]

John Cheney, *Managing Director of ACTIVIS, UK, (www.activis.com) who are exhibiting at ISSE 2001 – Information Security Solutions Europe, from 26–28 September 2001 at QEII Conference Centre, London. This article has been written as part of a series for ISSE 2001.*

Zusammenfassung

Der Feind von innen

Wenn auch davon ausgegangen wird, dass die meisten Sicherheitsbedrohungen von aussen kommen, so gibt es doch immer mehr Hinweise darauf, dass unzufriedene oder fehlgeleitete Mitarbeiter innerhalb der Firewall eine direktere Geschäftsbedrohung darstellen. John Cheney, Leitender Direktor bei Activis, einem Unternehmen im Bereich von Managed Security Services, erläutert die Art der Bedrohung und die Gegenmassnahmen, mit der Hacker in Schach gehalten werden können. Die Vorstellung, dass die meisten Sicherheitsverletzungen externer Art sind, wird zunehmend durch Forschungen widerlegt, aus denen sich schliessen lässt, dass Netzwerk-Manager strengere Sicherheitsvorkehrungen innerhalb der Firewall einsetzen müssen. Die Unternehmen müssen sich darüber klar werden, dass es bei der Sicherheit nicht nur um Technologie geht. Es handelt sich vielmehr um die drei Bestandteile Richtlinien, Management und Technologie. Durch die Richtlinien wird festgelegt, wie die Sicherheit verwaltet wird, und was erlaubt oder akzeptabel ist. Dazu können Richtlinien über die Internet-Nutzung durch Mitarbeiter gehören. Die Technologie sollte die höchste Qualität haben, und das Management muss sicherstellen, dass alles Up-to-Date ist, damit jederzeit alle Risiken abgeschätzt werden können.

Aibo liest E-Mails

Der Roboterhund Aibo von Sony hat im letzten Jahr einigen Wirbel verursacht. Wem das Batterie-verbrauchende «Haustier» zu wenig intelligent war, dem kann jetzt geholfen werden: Das Unternehmen hat eine Software herausgebracht, mit dessen Hilfe Aibo E-Mails lesen und Webseiten verarbeiten kann. Da er die (japanische) Sprache beherrscht, kann er dem Besitzer künftig die eingehende elektronische Post vorlesen.

Sony Corporation
6-7-35 Kitashinagawa
Shinagawa-ku
Tokyo 141. Japan
Tel. +81-3-3448 2111

Routinewartung am Auto – ein Milliardengeschäft

Aus dem letzten Jahresbericht der amerikanischen Motor & Equipment Manufacturers Association (MEMA) geht hervor, dass in den USA für Standard-Wartungsarbeiten rund um das Auto viel Geld ausgegeben wird. Zu solchen Routinearbeiten gehören Zündungseinstellung, Ölwechsel, der Austausch von Scheinwerferlampen und Rücklichtern, Luftfilteraustausch oder der Ersatz von Batterien. Dafür haben die Amerikaner 1999 die Summe von 23 Mia. US-$ auf den Tisch gelegt – in der Werkstatt wohlgemerkt, nicht im Do-it-yourself-Verfahren.

MEMA
P.O. Box 12255
Research Triangle Park
NC 27709, USA

Echte E-Mail auf dem Handy

SMS (Short Message Service) mit ihrem sehr begrenzten Textvorrat sind eher ein Notbehelf für «echtes» E-Mail auf dem Mobilfunkgerät. NTT DoCoMo als Marktführer in Japan will jetzt seine 23 Millionen I-mode-Nutzer auf das gemeinsam von DoCoMo und AOL betriebene E-Mail-Festnetz aufschalten: Mit dem neuen «AOLi»-Service will DoCoMo einen Fuss in das japanische AOL-Geschäft bekommen.

NTT DoCoMo, Inc.
11-1, Nagatacho 2-chome
Chiyoda-ku
Tokyo 100-6150, Japan
Tel. +81-3-5156 1366