

ORGANIZAÇÕES E SEGURANÇA INFORMÁTICA

Nuno Carvalho



Índice

Prefácio	9
Notação e Glossário	11
1.Introdução	17
2.Legislação	22
3.Política de Segurança da Empresa	36
4.Segurança Física	47
4.1.Protecções contra pessoas	48
4.2.Protecções contra incidentes (Segurança dos Ambientes)	53
5.Segurança Lógica	58
5.1.Anti Vírus	59
5.2.Firewall	62
5.3.Passwords	64
5.3.1.Windows Server	66
5.3.2.Unix	67
5.4.Controlo de Acessos	73
6.Segurança Rede	76
6.1.Proteger Activos de Rede	76
6.2.Esquemas de rede	77
6.3.Protecção dos dados na Rede	81
7.Segurança Redes sem Fios	87
8.Ataques	93
8.1.Vírus	95
8.2.Spyware	96
8.3.Spam	96
8.4.Sniffing	97
8.5.Phishing	97
8.6.Denial of Service	98
8.7.Spoofing	99
8.8.Software Exploitation	100

8.9.Data Jacking	101
9.Procedimentos/Actividades	102
9.1.Actualização dos Sistemas	102
9.2.Cópias de Segurança (Backups)	104
9.3.Auditoria	111
9.4.Registo de Eventos (Logs)	117
10.Ferramentas de Ataque e Defesa	122
10.1.Sistemas Detecção de intrusão e registos de actividades.	122
10.2.Redes	123
10.3.Vulnerabilidades	127
10.4.Redes sem fios	132
10.5.Passwords	135
10.6.Ferramentas de Backup	137
11.Bibliografia	141
12.Anexos	143
A-1. Modelo de documento de Política de Utilização da Rede	143
A-2. Legislação	149

Prefácio

A sociedade tem evoluído no sentido de uma dependência crescente das tecnologias de informação e comunicação. Um conjunto cada vez mais alargado das nossas actividades é suportado por sistemas informáticos que comunicam entre si através de tecnologias e suportes físicos diversificados, transportando quantidades crescentes de informação sobre o que fazemos, como fazemos, o que lemos e ouvimos e para onde vamos.

Nem sempre nos apercebemos do volume de informação que diariamente é recolhido em sistemas automáticos sobre o nosso quotidiano. E, sobretudo, daquilo que é possível fazer desde que se tenha acesso a essa informação.

São conhecidas muitas histórias de acesso indevido a sistemas informáticos militares, organizacionais ou bancários (e ficam por conhecer muitas mais). No entanto, não são só estes que nos devem preocupar. O acesso a informações privadas em computadores pessoais, às comunicações (móveis, fixas ou correio electrónico), a padrões de navegação na internet ou a informações contidas nos mais diversos sistemas (fisco, segurança social, ensino, portagens, etc.) pode ser muito mais danoso a nível individual, criando problemas cuja resolução nem sempre é fácil.

Apesar de tudo o que foi referido, continua-se a constatar na sociedade em geral uma grande insensibilidade para as preocupações mínimas de segurança que devem existir na utilização de qualquer sistema informático (seja essa utilização directa ou indirecta). Códigos de acesso óbvios, disponibilização fácil de informação de âmbito privado, desconhecimento e dificuldade em cumprir as mais elementares normas de segurança no acesso à internet, são algumas das principais falhas existentes.

O livro que agora é apresentado enquadra estas preocupações, abordando desde aspectos relacionados com a legislação até à enumeração de ferramentas de ataque e defesa, passando pela descrição dos principais procedimentos de segurança e dos tipos de ataques e actividades mais comuns.

A sua leitura permitirá uma maior consciencialização das dificuldades com que nos defrontamos, mas também da forma como as podemos minimizar. O leitor ficará seguramente mais familiarizado com a forma de prevenir ataques, de os saber reconhecer e de como reagir quando ocorrerem.

Embora não fugindo aos aspectos técnicos, o livro permite uma leitura agradável mesmo para os leitores menos familiarizados com as tecnologias de informação e comunicação, permitindo-lhe obter conhecimento que poderá utilizar no seu quotidiano.

*Prof. Dr. João Manuel Simões da Rocha
Presidente do Conselho Directivo do Instituto Superior de
Engenharia do Porto (ISEP)*