Segurança da informação digital

PEDRO JORGE FERNANDES PEREIRA

PALAVRAS-CHAVE

SEGURANÇA DA INFORMAÇÃO

INFORMAÇÃO DIGITAL

ARQUIVO DIGITAL

BIBLIOTECA DIGITAL

INTERNET

RESUMO

A segurança da informação digital constitui uma questão de grande actualidade e inegável relevância.
Seja em bibliotecas ou arquivos digitais, na banca electrónica, no *e-learning* ou em qualquer outra área, a segurança da informação digital é uma questão chave para a sobrevivência de muitas organizações.
Ao longo do presente artigo serão abordadas questões relativas à segurança física, à segurança lógica, aos principais tipos de ataques e ameaças e ainda, no final, um conjunto de sugestões (boas práticas) para reduzir o risco e promover a segurança da informação em ambiente digital.

ABSTRACT

The digital information security is getting an increasing importance and evident relevance.
Either in digital libraries or archives, the electronic banking, the e-learning or any another area, the digital information security is a key point for the survival of many organizations
This article will focus questions about the physical security, the logical security, the main types of attacks and threats and still, at the end, a few suggestions ("good practices") to reduce the risk and to promote the security of the information in a digital environment.

INTRODUÇÃO

Garantir a segurança da informação em ambiente digital constitui, cada vez mais, uma preocupação à escala mundial, seja por parte de organismos públicos, privados, universidades, empresas e até pelos cidadãos, de forma individual ou colectiva.

Na realidade, os riscos e ameaças não conhecem fronteiras de natureza geográfica, linguística, política ou qualquer outro tipo de barreiras. O que se verifica é que da mesma forma que aumenta a quantidade de informação em formato digital disponível, nomeadamente na Internet, também se verifica um aumento contínuo das ameaças e dos ataques à segurança da informação digital, levando também a um crescimento das estratégias de promoção da segurança e redução do risco.

Promover a segurança da informação digital é uma tarefa verdadeiramente multidisciplinar envolvendo, para além da Informática, outras áreas do conhecimento como o Direito, o Marketing, a Matemática, a Sociologia ou o comércio electrónico, só para dar alguns exemplos. Além disso, a variedade e diversidade de informação que se pretende proteger é muito vasta, podendo ser, por exemplo, bases de dados, fundos arquivísticos, dados pessoais altamente sigilosos, entre muitos outros.

Reforça-se, pois, a necessidade de definir, perante cada situação concreta ou até numa perspectiva mais abrangente, qual o tipo de protecção a aplicar, a respectiva arquitectura, os objectivos e, tal como foi proposto por João VALENTE (2001), a equação do trinómio custo, benefício e risco.

Fundamental é também conhecer as vulnerabilidades e fraquezas que possam existir, se são interna ou externas, quais as possíveis consequências e as melhores ferramentas e práticas a adoptar para as reduzir ou pelo menos prevenir e, caso se concretizem, ter um plano de contingência que permita uma rápida actuação e minimize as suas consequências.

SEGURANÇA FÍSICA E SEGURANÇA LÓGICA DA INFORMAÇÃO DIGITAL

Vários autores como Alberto CARNEIRO (2002) e Jack CHAMPLAIN (2003), quando abordam a segurança da informação digital fazem uma primeira distinção entre a segurança física e a segurança lógica, sendo que na presente análise vamos adoptar também esta distinção por considerarmos que é válida e adequada, além de abrangente.

>

Segurança física da informação digital

No sentido de melhor analisar a segurança física da informação digital, Alberto CARNEIRO (2002) sugere a sua subdivisão em 3 subgrupos: pessoal, equipamento e instalações.

Na segurança física referente ao **pessoal** estão as situações em que a componente humana constitui a principal fonte de atenção e de risco em situações como o erro, a falha humana, a fraude ou o roubo.

Para reforço da segurança física, na perspectiva do pessoal há que destacar particularmente questões de fundo como a **selecção e recrutamento** dos recursos humanos, a **documentação** que serve de apoio à sua actuação (manuais, normativos internos), a **formação** desses recursos humanos, a sua **sensibilização e motivação**, dar-lhes a conhecer a **política de segurança**, e o respectivo **plano de segurança**, entre outros.

Por outro lado, há que destacar também o papel dos **utilizadores** (interno ou externos) dos sistemas que utilizam e gerem a informação digital, da importância de que se reveste apoiá-los e acompanhá-los no seu trabalho, de forma a promover também a segurança, mesmo quando estamos a referir-nos a utilizadores que podem estar a milhares de quilómetros de distância, protegidos por um monitor.

Ainda no que diz respeito ao pessoal, não pode ser esquecido o **pessoal temporário** (contratado para desempenhar funções específicas) ou contratado em regime de *outsourcing*. Este tipo de pessoal pode ter, por exemplo acesso a informação privilegiada e fazer uso da mesma de forma inadequada, constituindo um potencial risco.

Na segurança física, referente aos **equipamentos**, estamos a referir-nos ao *hardware* computacional (computadores, servidores, infra-estruturas de redes…) e outros equipamentos, como equipamento para o fornecimento de energia, sistemas de controlo de acessos físicos, sistemas de detecção e combate a incêndios, controlos de temperatura e humidade, de ventilação e de picos electromagnéticos, só para referir alguns dos mais representativos.

Por outro lado, também não podem ser descuradas as questões relativas à **manutenção** dos equipamentos e registos de todas as intervenções que venham a ocorrer e até questões aparentemente tão banais como a limpeza do equipamento podem ser um factor crítico de segurança.

Na segurança física referente às **instalações**, como o nome indica, trata-se da perspectiva de engenharia e arquitectura, nomeadamente o local onde está fisicamente instalado o "cérebro" do sistema que gere e armazena a informação digital. Para a redução do risco e reforço da segurança são fundamentais as questões relacionadas com a sua **localização**, o estado de **conservação** do edifício, os riscos de inundação, de infiltrações e de acessos indevidos, a proximidade a locais muito poluídos, zonas de tumultos ou manifestações, entre outros.

Segurança lógica da informação digital

À semelhança da segurança física, também a segurança lógica é essencial para garantir a segurança da informação digital.

Ainda que, aparentemente, menos visível a segurança lógica deve estar em permanente actualização de forma a acompanhar também a evolução dos riscos e das possíveis ameaças.

Por exemplo, um antivírus que hoje esteja actualizado daqui a 2 meses já não estará e daqui a 1 ano estará completamente ultrapassado, perdendo grande parte da sua eficácia.

Ao nível da segurança digital as possibilidades de ataque e os riscos são tantos que vários autores abordam o problema de forma diferente.

William STALLINGS (1999) adopta a perspectiva da existência de um fluxo de informação entre a fonte e do destino, existindo vários tipos de ameaças e ataques: por interrupção do fluxo de informação (ataque à disponibilidade da informação), por intercepção (ataque à confidencialidade), por modificação (ataque à integridade) e por produção (ataque à autenticidade da informação), como se pode ver na figura1.

Outros autores, como David BLACK (2002) fazem a distinção entre ataques passivos em que há intercepção (quebra de sigilo), seja por acesso ao conteúdo ou por análise de tráfego e ataques activos, seja por intercepção, modificação ou fabricação de dados.

Na prática, estas duas abordagens não são exaustivas (falta por exemplo a inclusão dos ataques do tipo DOS – *denial of service*)[1] mas referem os principais tipos de ataques e possíveis violações, seja por vírus, *spoofing*, *worms*, *hackers*, violações de privacidade, entre outros.

>

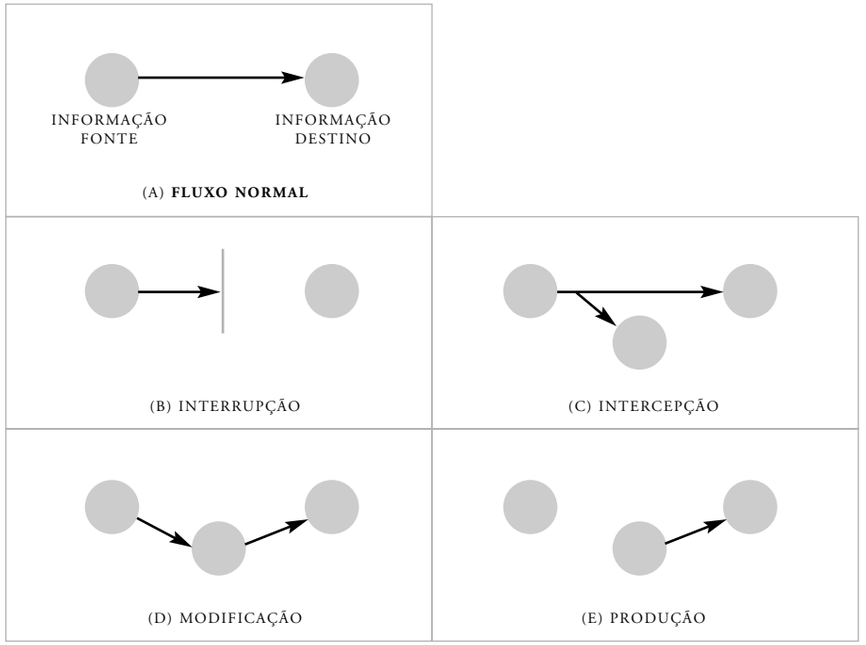

FIGURA 1 – AMEAÇAS À SEGURANÇA.

Fundamental também para a segurança lógica, para além da tipificação dos vários tipos de ataque e das melhores formas de os combater, é também uma análise, ainda que sumária, à gestão de acessos.

Uma política adequada de gestão de acessos é um elemento chave na segurança lógica. Torna-se, pois, fundamental definir os privilégios dos utilizadores ou outras estratégias de reforço da segurança como o seu pré-registo, a utilização de *firewalls* e IDS (*intrusion detection systems*)[2] que monitorizem todo o tráfego, a utilização da encriptação de dados (criptografia) e também, muito importante, a selecção de *passwords* ou palavras-chave que, tantas vezes, são subvalorizadas o que se torna ainda mais grave por existirem muitos sistemas de *password cracker* fáceis de encontrar e utilizar, tal como refere T. J. KLEVINSKI (2002) ao afirmar: «There are password crackers for almost every password-protected system available. A quick search on the Internet identifies password crackers for Windows NT, UNIX, Novell, PGP, Word, VNC, pcAnywhere, Lotus Notes, Cisco routers, WinZip, and many others.»

Mesmo tendo presente este facto, o que se verifica é que continuamos a adoptar más práticas na utilização de *passwords*, tais como:

• Escolhas demasiado óbvias como nome, apelido, morada, data de nascimento, matrícula do carro, entre outros;
• Manter os mesmos códigos durante muito tempo, a menos que o sistema nos force a mudar e, muitas vezes, ao mudar voltar a usar os mesmos códigos que anteriormente;
• Usar a mesma *password* para diferentes fins: validação no sistema, acesso à Internet, acesso à caixa de correio;
• Não combinar diferentes tipos de caracteres (maiúsculas e minúsculas, caracteres especiais, números e letras) ou, mais grave ainda, optar apenas pelo recurso a números;
• Partilhar *passwords* com outros utilizadores;
• Recorrer ao "*post-it*" ou qualquer outro sistema de registo escrito de *passwords* facilmente acessível.

São apenas alguns dos exemplos dos erros mais comuns na selecção e utilização das *passwords*.

Outro elemento fundamental em qualquer estratégia de promoção e reforço da segurança digital são as cópias de segurança, mais conhecidas por *backups*.

A realização e teste regular de *backups* pode ser o elemento de sucesso em muitas situações em que uma operação de *restore* constitui a única possibilidade de recuperação da informação.

A este respeito, Jack CHAMPLAIN (2003) destaca alguns dos principais aspectos que envolvem os *backups*, destacando nomeadamente:
• Localização física dos *backups*;
• Diferentes níveis de *backups*;
• Rotação e escolha de suportes;
• Auditorias e testes;
• Existência de um responsável pela realização de *backups*, entre outros.

O que foi dito não esgota de forma alguma o tema, mas já dá para ficar com uma perspectiva da real importância de segurança lógica.

Auditorias à segurança física e à segurança lógica

Para que a segurança física e lógica sejam verdadeiramente efectivas não chega investir em *hardware* e *software*, na formação dos recursos humanos ou actuar reactivamente perante uma situação em que a segurança da informação seja posta em risco.

>

Fundamental é também uma actuação preventiva, sendo aqui fundamental o papel das auditorias à segurança, tal como defende John KRAMER (2003).

Na realidade, quer a segurança física, quer a lógica dos sistemas devem ser regularmente testadas e postas à prova, de preferência por auditores exteriores à organização. Para verificar os níveis de segurança podem, por exemplo, ser feitos testes de penetração (muito comum em *websites*), *restore* de *backups*, tentativas de intrusão, verificação do estado de conservação dos edifícios, simulação de acidentes, testes aos antivírus e *firewalls*, entre outros.

Toda a política de segurança deve estar sintetizada num plano de segurança, que sistematiza a política de segurança da organização, ajudando os auditores a analisarem as medidas adoptadas, apontando as principais falhas e medidas para as ultrapassar e, por outro lado, servindo como instrumento de trabalho para toda a organização.

O RISCO COMO FACTOR DE DECISÃO

João VALENTE (2001) apresenta uma proposta de criar um trinómio custo, benefício e risco em qualquer sistema de informação não restringindo a análise ao binómio custo/benefício, o que faz todo o sentido, particularmente na informação em ambiente digital.

Na realidade, na concepção e implementação de qualquer sistema, do mais simples ao mais complexo, convém ter presentes os riscos associados e não apenas os custos e os benefícios que se espera vir a obter com a sua implementação. Ou seja, aquando do cálculo do ROI (*return of investment*)[3], deve já estar previsto que o risco pode afectar seriamente o retorno face ao investimento, podendo comprometer toda a estratégia desenvolvida.

Por exemplo, se dada organização implementar um sistema em que a componente digital da informação tenha um peso elevado deve prever já que existem riscos que podem alterar completamente os benefícios esperados, seja por vírus, intrusão por correio electrónico, recusa de serviço (*denial of service*), perda de dados confidencias ou qualquer outro motivo.

A DIMENSÃO LEGAL E NORMATIVA

Para além de todas as potenciais ameaças e riscos, a procura de soluções capazes de dar resposta, para além das limitações do ponto de vista humano, tecnológico ou até económico, pode esbarrar também em limitações de carácter mais jurídico e legal.

Na realidade, o que se verifica é que ao se tratar de uma área ainda muito nova e em constante mutação, nem sempre tem sido possível acompanhar juridicamente todas as situações com a rapidez desejável, existindo situações de verdadeiros "vazios legais".

As situações, hipotéticas e possíveis, são muito diversificadas e vão desde as cópias ilegais de *software* (por *download*, duplicação ou qualquer outro processo), à questão dos DRM (*digital rights management*)[4], passando por muitos outros casos como o direito à informação versus o direito à privacidade, a definição de regras para o comércio electrónico, o estabelecimento de penalidades para os *hackers* e *crackers*…

Justifica-se, pois, uma análise, ainda que sumária, à realidade portuguesa.

Portugal, enquanto membro da União Europeia tem também transposto várias normas comunitárias para a sua própria legislação, além de várias iniciativas nacionais:

• O primeiro exemplo é já de 1990 e consistiu numa resolução do Conselho de Ministros (n.º 5/90, de 28 de Fevereiro) que aprovou as "Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática", mais conhecidas por **SEGNAC 4**.

• Seguiu-se em 1991 a Lei n.º 109/91, de 17 de Agosto (**Lei da Criminalidade Informática**), que categoriza e pune os crimes informáticos, definindo seis categorias. Apesar de desactualizada continua ainda em vigor, sendo as categorias:
· Falsidade informática;
· Dano relativo a dados ou programas informáticos;
· Sabotagem informática;
· Acesso ilegítimo;
· Intercepção ilegítima;
· Reprodução ilegítima de programa protegido.

• A Lei n.º 114/91, de 3 de Setembro, inicia o processo de **licenciamento de *software***, sendo retomada pelo Código de Direitos de Autor e Direitos Conexos, o Regime de Protecção Jurídica dos Programas de Computador (DL n.º 252/94, de 20 de Outubro), o DL n.º 122/2000, de 4 de Julho, referente à Protecção Jurídica das Bases de Dados e o papel da ASSOFT (Associação Portuguesa de Software).

>

• Com a Lei n.º 67/98, de 26 de Outubro (e respectiva Declaração Rectificativa n.º 22/98, de 20 de Novembro), foi transposta a directiva comunitária que regulamenta a maneira como devem ser mantidos e transmitidos os dados pessoais, protegendo os cidadãos, nomeadamente nas situações das empresas/entidades que possuem bases de dados com informação sobre as pessoas, sendo conhecida como **Lei da Protecção dos Dados Pessoais**.

• A Lei n.º 68/98, de 26 de Outubro, cria a **Comissão Nacional de Protecção de Dados** (CNPD) com poderes muito vastos, que vão desde a aplicação de coimas, à emissão de pareceres incidindo a sua actividade particularmente sobre a protecção dos dados pessoais.

• Com o Decreto-Lei n.º 290-D/99, de 2 de Agosto, depois retomado no Decreto-Lei n.º 62/2003, de 3 de Abril, que vem dar cumprimento à Directiva Comunitária 1999/93/CE, **equiparando o documento electrónico ao documento em papel**, graças à «assinatura digital certificada por uma entidade credenciada». Em Portugal, essa entidade é o Instituto das Tecnologias da Informação na Justiça, assistido pelo Conselho Técnico de Credenciação, criado pelo Decreto-Lei n.º 234/2000, de 25 de Setembro.

• Com a Resolução do Conselho de Ministros n.º 94/99, de 25 de Agosto, foi criada a Iniciativa Nacional para o **Comércio Electrónico**, surgindo diplomas posteriores de enquadramento, caso do Decreto-lei n.º 375/99, de 18 de Setembro, que equipara a factura electrónica à do papel (retomado pelo Decreto Regulamentar n.º 16/2000, de 2 de Outubro).

• A 23 de Novembro de 2001, Portugal é também um dos países signatários da **Convenção sobre o Cibercrime**[5], assinada em Budapeste cujo objectivo é, basicamente, a harmonização de legislação relativa a crimes informáticos, incluindo questões relacionadas com conteúdos ilegais como a pornografia ou a possibilidade de extradição, entre os países signatários, de criminosos que tenham efectuado estes crimes, sendo assim favorecida a cooperação entre os vários países.

• De destacar também o Decreto-lei n.º 7/2004, de 7 de Janeiro, que faz a transposição da Directiva Comunitária 2000/31/CE, de 8 de Junho, intitulada "**Directiva sobre o Comércio Electrónico**" que vem introduzir um conjunto de pontos referentes a contratos electrónicos, resolução de litígios entre os vários Estados, colaboração judicial e, muito importante, introduz o conceito, no seu artigo 7.º, de opção negativa, ou seja *out-put* para comunicações de carácter comercial ou outras não solicitadas, vulgarmente conhecidas por ***spam***, verdadeiro flagelo do correio electrónico.

• A **Norma ISO/IEC 17799**[6] é relativa à segurança da informação e procura contribuir para a segurança das organizações, dos seus colaboradores, instalações e, sobretudo, dos seus sistemas de informação, sendo o seu título "Tecnologias da Informação – Código de prática para a gestão da segurança da informação".

Trata-se de um documento composto por dez capítulos, em que cada um analisa com rigor e pormenor uma questão relacionada com a gestão da segurança da informação, incluindo medidas e sugestões para a obtenção de um nível de segurança óptimo. Quanto aos capítulos são:

1. Política de Segurança;
2. Segurança Organizacional;
3. Controlo e Classificação de Bens;
4. Segurança Pessoal;
5. Segurança Física e Ambiental;
6. Gestão de Comunicações e Operações;
7. Controlo de Acessos;
8. Desenvolvimento e Manutenção de Sistemas;
9. Gestão da Continuidade do Negócio;
10. Conformidade.

Pode dizer-se, sem exagero, que se trata de um documento de consulta obrigatória, dada a sua abrangência e profundidade.

O SEGURO ELECTRÓNICO

É um dado adquirido que dificilmente se consegue um sistema completamente seguro, como afirma Wilson OLIVEIRA (2001):

«O único sistema totalmente seguro é aquele que não possui nenhuma forma de acesso externo, está trancado num sala totalmente lacrada e da qual uma única pessoa possui a chave. E esta pessoa morreu o ano passado.»

Porém, também não podemos ser derrotistas. Há que apostar em estratégias que reduzam o risco, surgindo aqui uma nova área de negócio: o seguro electrónico.

Trata-se de uma área que ainda agora está a dar os primeiros passos em Portugal, mas em países como os Estados Unidos já está estabilizada e dividida em classes

>

mais ou menos próximas, como *Network Risk Insurance*, *Hacker Insurance*, *Cyber Risk Insurance*, *E-Business Insurance*.

Na prática, o recurso ao seguro electrónico, mediante acordos entre os clientes e as companhias de seguros, pode representar uma importante estratégia de reforço de segurança da informação digital, com implicações tremendas no negócio e envolvendo quantias astronómicas, como refere Jim CARROL (2003): «Hacker insurance is expected to explode from $100 million sideshow into a $2.5 billion behemoth by 2005.»

Ou seja, as probabilidades de sofrer um ataque ou uma situação em que a segurança da informação digital seja comprometida são de tal forma elevadas que a transferência do risco, mediante o pagamento de uma apólice, se justifica facilmente.

A título meramente informativo o CSI (The Computer Security Institute)[7] num levantamento baseado nas respostas de 503 grandes entidades dos Estados Unidos (envolvendo agências governamentais, empresas financeiras, hospitais e universidades) concluiu no seu "2002 Computer Crime Survey" que:
• 90% dos que responderam ao inquérito tinham detectado situações em que a segurança da informação foi posta em causa;
• 80% afirmaram que essas situações representaram perdas financeiras;
• 223 dos que responderam ao inquérito quantificaram as suas perdas, sendo o valor final estimado em 455.848.000 dólares.

BOAS PRÁTICAS PARA PROMOVER A SEGURANÇA DA INFORMAÇÃO EM AMBIENTE DIGITAL

Nesta última parte do artigo, provavelmente a mais importante, vão ser apresentadas boas práticas capazes de, por um lado, reduzir os riscos e ameaças e, por outro, reforçar a segurança.

Dado o elevado número e diversidade de possíveis ataques e ameaças, torna-se necessária uma resposta que assente muito na prevenção e não apenas no combate. Além disso, nessa estratégia de prevenção, os recursos humanos são um elemento chave e qualquer plano de segurança ou proposta de boas práticas terá que ter isso em linha de conta.

Assim, com o objectivo de apresentar um conjunto de boas práticas, podem ser criados grupos que sintetizem as boas práticas.

Vamos considerar a criação de 5 grupos principais com possível exemplo para um plano de segurança:
• O correio electrónico;
• Antivírus;
• *Passwords*;
• A Internet/intranet;
• *Backups*.

O **correio electrónico** está chegar a um ponto que, apesar de todas as suas vantagens e potencialidades começa já ser questionada a sua validade, tal como afirma Jim RAPOZA (2002): «Namely, given the constant progression of spam, viruses and other problems, e-mail is quickly approaching the point where the rewards of using it no longer out weight the risks.»

Assim, para minimizar os riscos a utilização do *mail* deve ter regras claras para todos os seus utilizadores, podendo estas ser mais ou menos restritivas consoante os perfis que sejam definidos, por exemplo, no local de trabalho não autorizar o *mail* para fins lúdicos, para participação em correntes de *mail*, não permitir receber ou enviar ficheiros anexos, entre outros. Ou seja, esta poderosa ferramenta é também muitas vezes o elo mais fraco na cadeia de segurança, sendo necessário apostar em *hardware* e *software* (*firewalls*, sistemas de IDS, sistemas *anti-spam*…) adequados sob pena de os riscos se tornarem superiores aos benefícios.

Também os **antivírus** são uma ferramenta essencial e a sua utilização é uma boa prática fundamental. A sua utilização e actualização regular é crucial, mais ainda quando se está ligado ao exterior, nomeadamente à Internet, seja para utilização do correio electrónico, para partilha de ficheiros, pesquisa de informação, para *downloads* ou qualquer outro motivo.

O risco está sempre presente. Afinal de contas todos os dias surgem novas vírus aos quais há ainda a acrescentar os *worms*, os *trojan horses*, entre outros.

Assim, a utilização dos antivírus tem que ser regular, sendo comum serem os próprios sistemas que efectuam as actualizações e testes regulares.

Quanto às ***passwords***, são também um elemento chave da segurança.

Ao nível das boas práticas são toda aquelas que vão para além das escolhas lógicas e óbvias, da não combinação de maiúsculas e minúsculas e caracteres especiais, da utilização de uma mesma *password* com diferentes fins, da sua partilha, da utilização de códigos já usados anteriormente ou da sua não mudança regular.

>

Convém ter presente que a *password* é uma forma de autenticação e validação e como tal deve ser única e intransmissível.

Ou seja, a escolha e utilização das *passwords* são também um elemento chave da segurança na segurança da informação digital além de garantirem que cada indivíduo é único e não se confunde com os demais.

Convém também ter presente que a **Internet e a *intranet*** são distintas, mesmo que a apresentação seja comum.

A *intranet* pode ser considerada como é uma infra-estrutura baseada nos padrões e tecnologias da Internet, mas em que os limites estão definidos, seja em redes públicas ou privadas, permitindo também a comunicação entre locais diferentes, mas ao contrário da Internet numa escala mais fechada e com regras definidas, podendo ou não ter acessos para o exterior. Não existindo acesso ao exterior, naturalmente que os riscos são menores, mas também se perdem muitas das potencialidades que a Internet possui.

Na prática, os próprios utilizadores devem ter presente essa distinção de modo a reduzir o risco e a reforçar a segurança, sendo que, por exemplo, parte da informação disponível na *intranet* pode estar também na Internet, mas não a totalidade dessa informação.

Também os ***backups*** já foram referidos anteriormente, mas merecem uma nova referência dada a sua importância e valor sendo muitas vezes a única solução para salvaguardar a recuperar a informação que, por qualquer razão, como vírus, erro humano, falha técnica, catástrofe natural ou outra estaria irremediavelmente condenada.

E mesmo nos sistemas de pequeno porte ou até nos computadores de uso pessoal, portáteis ou não, a realização de *backups* deve ser regular, mais ainda nos dias de hoje em que os suportes de *backup* têm custos reduzidos e a operação de *restore*, se necessário, é bastante simples.

Porém, não basta fazer *backups* regulares. Há que proceder a testes e verificações permanentes.

CONCLUSÃO

O presente artigo não deve ser visto como um trabalho encerrado. O objectivo é exactamente o oposto, sendo que o que se pretende é que sirva de alerta para os riscos existentes e não apenas para as potencialidades que a informação digital veio trazer.

É um trabalho exploratório e que não tem outra ambição que a de mostrar que a segurança da informação em ambiente digital está em permanente risco e que cada um de nós, individualmente ou em grupo, pode fazer alguma coisa para diminuir os riscos e reforçar a segurança.

NOTAS

[1] http://www.cert.org/tech_tips/denial_of_service.html

[2] http://www.cerias.purdue.edu/about/history/coast_resources/intrusion_detection/

[3] http://intrack.com/intranet/ireturn.shtml

[4] http://www.dlib.org/dlib/june01/iannella/06iannella.html

[5] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[6] http://www.iso-17799.com/

[7] http://www.gocsi.com/

BIBLIOGRAFIA

ARMS, William – *Digital Libraries*. Massachusetts: MIT Press, 2000.

ASSOCIAÇÃO PORTUGUESA DE SEGURADORAS – *Estudo: Seguro Electrónico*. Lisboa: APS, 2002.

BAHAN, Chad. *The Disaster Recovery Plan*. [Consult. 30 Nov. 2004]. Disponível em – http://www.sans.org/rr/papers/index.php?id=1164

BLACK, David. *ISCSI: Active and Passive attacks*. [Consult. 25 Nov. 2004]. Disponível em http://www.pdl.cmu.edu/mailinglists/ips/mail/msg09840.html

CAMPOS, Fernanda – "Informação Digital: um novo património a preservar". *Cadernos BAD*, 2002 (2). BAD: Lisboa.

CARNEIRO, Alberto – *Introdução à Segurança dos Sistemas de informação*. Lisboa: FCA Editores, 2002.

CARROL, Jim – *Understanding Network Risk Insurance. A customized Workshop*: USA, 2003.

CHAMPLAIN, Jack – *Auditing Information Systems*, 2.d ed. New Jersey: Jon Wiley & Sons, 2003.

COLE, Eric – *Hackers Beware: defending your network form the Wiley Hacker*. USA: New Riders Publishing, 2001.

ELLIS, Juanita; SPEED, Timothy – *The Internet Security Guidebook: from Planning to Deployment*. USA: Academic Press 2001.

KLEVINSKY, T. J.; LALIBERTE, Scott; GUPTA, Ajay – *Hack I.T.: Security Through Penetration Testing*. Indianapolis: Addison Wesley, 2002.

KRAMER, John – *The CISA® Prep Guide: Mastering the Certified Information Systems Auditor Exam*. Indianapolis: Wiley Publishing, 2003.

MARQUES, Ana Margarida; ANJOS, Mafalda; VAZ, Sónia Queiroz – *101 Perguntas e Respostas sobre o Direito da Internet e da Informática*. V. Famalicão: Centro Atlântico Editora, 2002.

MCCLURE, Stuart; SHAH, Saumil; SHAH, Shreeraj – *Web Hacking: Attacks and Defense*. Boston: Addison Wesley, 2002.

OLIVEIRA, Wilson – *Segurança da Informação: Técnicas e Soluções*. Porto: Centro Atlântico Editora, 2001.

OLIVEIRA, Wilson – *Técnicas para Hackers – Soluções para Segurança*. 2.ª ed. Porto: Centro Atlântico Editora, 2003.

OPPLIGER, Rolf – *Internet and Intranet Security*. Norwood: Artech House Publishers, 1998.

PEREIRA, Joel Timóteo Ramos – *Direito da Internet e Comércio Electrónico*. Lisboa: Sociedade Editora, 2001.

RAPOZA, Jim. E-mail Risks are Taking a Toll on the Rewards. October 2002. [Consult. 22 Nov. 2004]. Disponível em: http://www.eweek.com/article2/0,3959,660001,00.asp

RHEE, Man Young – *Internet Security: Cryptographic Principles, Algorithms and Protocols*. England: Wiley & Sons, 2003.

ROSS, Keith; KUROSE, James – *Computer Networking: a top-down approach featuring the Internet*, 2. ed. USA: Pearson Education, 2003.

SCHETINA, Erik; GREEN, Ken; CARLSON, Jacob – *Aprenda a desenvolver e construir Sites Seguros*. Rio de Janeiro: Editora Campus, 2002:.

SCHIFFMAN, Mike – *Hacker's challenge: test your incident response skills using 20 scenarios*. USA: McGraw-Hill, 2001.

SCHNEIER, Bruce – *Secrets and lies: Digital Security in a Networked World*. New York: John Wiley and Sons, 2000.

SHINDER, Debra L. – *Scene of the Cybercrime: Computer Forensics Handbook*. Rockland: Syngress Publishing, 2002.

SILVA, Pedro Tavares *et al* – *Segurança dos Sistemas de informação: Gestão Estratégica da Segurança Empresarial*. Lisboa: Centro Atlântico, 2003.

SPEED, Tim; ELLIS, Juanita – *Internet Security: A Jumpstart for Systems Administrators and IT Managers*. Burlington: Elsevier Science, 2003.

STALLINGS, Williams – *Cryptography and Network Security: Principles and Pratice*, 2. ed. New Jersey: Prentice Hall, 1999.

STEFANEK, George – *Information Security Best Practices: 205 basic rules*. USA: Butterworth--Heinemann, 2002.

TANENBAUM, Andrew – *Computer Networks*, 4 ed. New Jersey: Prentice Hall, 2003.

TOIGO, J. William – *Disaster Recovery Planning*. 2 ed. New Jersey: Prentice Hall, 2000.

TRIMER, Don – "Tape-free backup/Recovery: Requirements and Advantages". *Infostor*, Março 2002.

VALENTE, João – "Segurança nos Sistemas de informação". *Dirigir* n. º 13. Lisboa: IEFP, 2001.

VARAJÃO, José Eduardo – *A Arquitectura da Gestão de Sistemas de Informação*. Lisboa: FCA Editores, 2002.

VARLEJS, Jana (ed.) – *Safeguarding Electronic Information: law and order on the Internet and other computer security quandries*. Jefferson: Rutgers Graduate School of Library and Information Library Studies, 1996.