

# Revista REDES - Agosto2002

Luis Farinha

18 de Novembro de 2002

## Conteúdo

1	Introdução	2
2	Na senda da plataforma .NET	2
3	Assinatura com impressão digital	4
4	Segurança e 10 Gigabit em destaque	4
5	802.11 ganha terreno	4
6	802.1x, o protocolo do futuro?	4
7	IPCablecom persegue banda larga.	5
8	Bibliografia	5

# 1 Introdução

Um dos problemas que nos dá mais dores de cabeça nos dias de hoje é a questão da segurança dos nossos dados. Erradamente muitos dos gestores continuam a considerar este ponto como apenas mais uma despesa. Que métodos aplicar? Que software adquirir? Estas são apenas algumas entre muitas perguntas que se colocam quando já é tarde de mais e dados já foram perdidos de maneira irreversível. Numa altura em que qualquer empresa anseia estar na linha da frente, a protecção do seu sistema de informação é tão vital como garantir bons serviços. Isto leva-nos ao facto que a segurança é um dos investimentos mais importantes numa rede, quer esta seja pública ou empresarial. Não ter um sistema de segurança adequado pode sair muito mais caro a uma empresa, fazendo com que perca muito mais do que o que aplicaria para proteger a sua informação mais confidencial e estratégica para o seu negócio. Isto permite-lhe também ter um sistema de informação operacional vinte e quatro horas por dia e acessível a partir de qualquer ponto do mundo, dando uma imagem inovadora e dinâmica da sua empresa.

Encarar a segurança como apenas uma protecção contra ataques vindos do exterior é um modo errado de encarar o problema. Esta envolve muito mais aspectos tais como regras para o controlo de acessos, condições de funcionamento dos equipamentos, partilha de informação assim como a disponibilização da mesma para o exterior, enquadrando-se esta numa política adequada à empresa. Existem imensos aspectos inerentes a este tema, isto é, a segurança passa por tudo o que possa afectar a saúde dos dados da nossa empresa tal como a integridade do sistema.

Uma política de segurança demasiado rígida pode também ser uma má abordagem. O equilíbrio entre um sistema eficaz e suficientemente seguro é difícil mas essencial. Devido ao facto deste problema ter muitas abordagens, conseguir uma boa política de segurança é sempre diferente de empresa para empresa e deve ser proporcional aos riscos que envolve a sua área assim como a capacidade de investimento nesta área que a empresa suporte. Aqui também é importante conseguir um bom balanço entre as necessidades da empresa e as suas capacidades financeiras, não descuidando do facto que é muito importante ter os seus dados assegurados.

## 2 Na senda da plataforma .NET

Nos nossos dias a criação de novo software está tão desenvolvida que nem damos por vezes pelos novos produtos que são lançados para o mercado. Não é certamente o que acontece com os novos produtos Microsoft da gama **.NET**. Tendo a segurança como bandeira, estes novos produtos apregoam ser mais fiáveis, mais rápidos e seguros. Um bom exemplo disso é a nova ferramenta *Visual J# .NET* lançada para substituir o *Visual J++*. Com este passo a Microsoft pretende abandonar a linguagem Java para transitar para o

**XML**. Como linguagem o **XML** trabalha de modo a identificar estruturas em documentos e interpreta-las, podendo ser definido de um grosso modo como o avanço do *HTML*. Avançando com este processo a Microsoft espera conseguir melhorar a compatibilidade entre este software e o já existente. O *Visual Studio .NET* faz também a integração de linguagens como a **ASP.NET** e da **ADO.NET**. Quanto à **ASP.NET** é capaz de nos proporcionar aplicações do estilo *HTML*, usando um processo de construção muito mais facilitado, e poupando muito tempo na sua elaboração. Ao contrário do clássico *ASP*, o **.NET** é capaz de suportar linguagens como *VB.NET*, *C#* e *JScript.NET* mantendo a interoperabilidade com todos os principais WEB Browsers. Por outro lado a **ADO.NET** é uma evolução do Microsoft Active Data Objects (ADO) que através da linguagem *XML* consegue garantir a transferencia de dados para qualquer aplicação em qualquer plataforma.

O aperecimento desta nova linguagem (*J#*) que vem alargar mais um pouco a gama de linguagens de programação da Microsoft, e o facto de ser uma linguagem criada pratriamente de raiz deve-se ao facto de existir conflitos com a Sun Microsystems. Com este contratempo a reutilização de código em *JAVA* é quase nula.

Realizando um esforço adicional para provar a segurança proporcionada pelos seus novos produtos, a Microsoft não se evitou os custos, relaizando uma serie de teste com ferramentas de intrusão, assim como a revisão de linhas de código. A **PKI** (Public Key Infrastructure) é um dos realces feitos na área de gestão de segurança. A **PKI** pertence a um grupo de mecanismos utilizados para garantir que uma comunicação, ou troca de dados seja segura, e que seja vista apenas por quem queremos. A **PKI** é muito utilizada para a encriptação de documentos.

Embora o software seja uma enorme vantagem, pequenas ideias para tornar uma rede segura, tais como colocar a nossa informação mais preciosa em locais de difícil acesso, ou menos sugestivos para quem queira invadir a rede ou a máquina em questão. Outras práticas mais usuais passam pelas carismáticas *firewalls* que são um dos vários obstáculos aos intrusos, impedindo acessos para ou do exterior se assim forem configuradas. A sua localização esta dependente de vários aspectos entre os quais estão as necessidades da empresa e a eventual disponibilidade que deseja oferecer.

Detectar um intruso pode ser difícil, apesar de todos os métodos que existem. Pode-se tentar começando por vigiar processos, assim como certos acessos feitos, vigiando os portos.

Continuando no tema de encriptação pode-se recorrer ao protocolo IPsec, utilizado nas redes IP recorrendo aos vários serviços de encriptação.

### 3 Assinatura com impressão digital

Disponibilizando 20Kb para o armazenamento de impressões ou certificados digitais, assim como para chaves de encriptação, a Rainbow Technologies mostra assim a sua chave de identificação biométrica para a autenticação dos trabalhos de uma empresa. Compatível com as normas **PKI** e **VPN**, esta chave gera as chaves de encriptação necessárias, sendo completamente autónoma de qualquer base de dados, ela guarda na memória todos os certificados, utilizadores e as respectivas impressões digitais. Para reconhecer as impressões digitais a chave oferece entre 12 a 70 critérios de discriminação.

### 4 Segurança e 10 Gigabit em destaque

O mais recente passo da evolução em termos de redes e a ultra veloz Ethernet a 10Gb. Graças as novas capacidades dos PC's que são cada vez mais exigentes em recursos, esta nova tecnologia é uma boa nova para quem pretende ter uma LAN. Várias companhias estão a apresentar produtos que suportem esta categoria. Com o seu fascinante desempenho torna-se uma escolha obrigatória, quer para os consumidores, quer para os fornecedores de *hardware*. E como tal, novas questões surgem, quer em termos de segurança, quer em termos de compatibilidade. Para isso a IEEE 802.3 criou as respectivas normas, e continua a actualizá-las de modo a corrigir os problemas que todas as tecnologias possuem no seu início.

### 5 802.11 ganha terreno

Cada vez mais utilizadas, as redes se fios são uma solução viável nos nossos dias. Isso faz com que haja uma necessidade maior de segurança. É então que este tipo de redes recuperou do atraso em relação às suas oponentes com as recentemente finalizadas normas 802.11a e 802.11b. Este passo foi essencial pois estas normas são viradas para gestão de serviços prestados pelas Wireless.

Um dos problemas destas redes, trata-se do débito, pois estão mais sujeitas a erros de transmissão, e por consequência, são mais susceptíveis a retransmissão de dados. São estes tipos de problemas que as normas 802.11 esperam resolver, entre outros, como a segurança.

### 6 802.1x, o protocolo do futuro?

Inicialmente proposta para resolver os problemas de segurança nas LAN de cabo, este protocolo de autenticação foi rapidamente adoptado pelas WLAN. Um dos seus principais objectivos é criar alternativas as vias de autenticação existentes(endereço MAC e IP).

Devido à sua funcionalidade várias marcas já adaptaram os seus produtos ao 802.1x.

## 7 IPCablecom persegue banda larga.

Melhorar serviços e aumentar a segurança são necessidades das mais básicas nas redes actuais. Como este papel não pode ser só do hardware, apesar de este ser cada vez mais fiável, normas como a **IPCablecom** são sempre bem vindas.

Responsável, entre outras coisas, pelo encaminhamento de serviços, interface com a rede telefonica, segurança e outros.

## 8 Bibliografia

Usei no trabalho as seguintes referências:

Revista Redes - Agosto2002 n.º 88

<http://www.microsoft.com/net>

<http://www.xml.com>

<http://csrc.nist.gov/pki/>

<http://www.microsoft.com/technet/security/pkitech.asp>

<http://www.microsoft.com/windows2000/technologies/security/default.asp>