

Novas tecnologias – Sobrevivendo ao abismo

Por **André Fucs de Miranda, CISSP** <afucs@uol.com.br>

Como adotar novas tecnologias sem expor as informações e ambientes existentes em sua empresa? Como aliar flexibilidade e segurança em novos ambientes sem impor penosos atrasos em um novo serviço? Esse equilíbrio entre o tempo de implantação e o grau de risco aceitável por uma organização tem sido fonte de dores de cabeça nos últimos anos para um enorme número de gestores.

A dificuldade em definir esse equilíbrio e uma abordagem fortemente baseada em melhores práticas leva muitos security officers a serem tachados como excessivamente controladores e reativos, o que conseqüentemente leva a uma redução da importância do papel do gestor da segurança da informação.

Para reverter esse quadro, é fundamental a compreensão de como o uso de **políticas** de segurança flexíveis pode resultar em uma forma independente de lidar com mecanismos de segurança garantindo ao gestor a flexibilidade necessária para responder rapidamente a ambientes dinâmicos e tecnologias com baixo grau de maturação tecnológica.

1 Dilema ou oportunidade?

Toda nova tecnologia apresenta um potencial de risco maior ou igual que os benefícios que traz.

Uma equação simples porém assustadora, e que nos últimos séculos vêm movendo a evolução tecnológica da sociedade. Não é sem motivo que as armas de fogo antecederam o coletes e carros à prova de balas, e porquê a comunicação a distância antecedeu a criptografia. Mais do que isso, esses dois exemplos, incrivelmente pequenos frente a lista de tecnologias desenvolvidas pelo homem, ilustram perfeitamente como a tecnologia que nos provê diferenciais competitivos nos expõe a riscos antes inexistentes.

Por outro lado, novos serviços nascem da combinação adequada de inovação, estilo e tecnologia e ajudam a criar experiências que pessoas considerem úteis e válidas. Novos serviços, internos ou externos à corporação nascem portanto da necessidade das áreas de ocupar espaços antes ignorados dos elementos de uma empresa.

Diante dessas duas realidades aparentemente distintas nasce o que para muitos gestores é um dilema. A verdade é que longe disso, o cenário criado, se bem gerido, é um terreno fértil para o crescimento do Security Officer.

2 Aceitando o desafio

Talvez um dos fatos mais interessantes acerca do gerenciamento da segurança de novas tecnologias é o fato de que é fácil encontrar gestores acuados pela novidade, como se o parque tecnológico de uma empresa não costumasse conter risco totalmente ignorados. É passo fundamental do trabalho, aceitar a nova tecnologia como mais um elemento presente em uma organização, entretanto, em decorrência do estado de maturação dessa tecnologia, é apropriado tomar um posicionamento diferenciado que esse tipo de ambiente requer.

Um dos primeiros passos para isso é identificar o perfil de sua organização. Geoffrey Moore no excelente livro *Crossing the Chasm* descreve os perfis de consumidores de tecnologia e discute estratégias de como atravessar o abismo que separa consumidores visionários e pragmáticos.¹

Moore sustenta que enquanto consumidores visionários compram a tecnologia de ponta como um viabilizador de negócios, os consumidores pragmáticos compram com maior consciência e moderação, buscando referências entre seus pares mas descartando as referências de entusiastas e visionários. O autor também sustenta que para atravessar esse abismo é necessário direcionar marketing e discurso para cada perfil de consumidor, e que a atuação de forma verticalizada é fator determinante da empreitada.

Logo, se toda organização, independente de seu tamanho possui igualmente um perfil de consumo, ela deve ser encarada como consumidor interno do security office e é vital, conforme apresentado ao longo do capítulo, que a área de segurança identifique não apenas o **perfil de consumo e exposição ao risco das organizações** com que se relaciona mas que com base nisso torne-se capaz de oferecer soluções de segurança facilmente assimiladas pela organização.

Paralelamente, Clayton M. Christensen observa em *The Innovator's Dilemma* que tecnologias podem ser divididas entre **sustentadoras** e **desruptivas**. Enquanto as tecnologias sustentadoras fomentam um melhor desempenho de produtos, as denominadas tecnologias disruptivas são inovações que ainda que acrescentem novas possibilidades ao mercado ainda que apresentem uma pior performance a curto prazo dos produtos. Segundo ele “essas tecnologias costumam apresentar menor preço, simplicidade, dimensões e freqüentemente

¹ Tradução livre de Innovators, Early Adopters, Early Majority, Late Majority e Laggards

agregam maior conveniência de uso” tais como as câmeras fotográficas digitais, a telefonia móvel e redes sem fio.

Christensen argumenta ainda que ao lidar com uma tecnologia disruptiva, deve-se focar em três critérios fundamentais:

- Simplicidade, confiabilidade e conveniência;
- Flexibilidade na modificação de recursos e funcionalidades, e;
- Baixo custo final ao consumidor.

Conforme exposto no decorrer do capítulo, é justamente o custo decorrente do tempo a grande ameaça ao gestor da segurança lidando com novas tecnologias.

3 Definindo o abismo

Se o abismo de Moore refere-se a venda e crescimento de receita, o abismo do security officer refere-se a um período onde há baixa disponibilidade de mecanismos de segurança capazes de garantir tranquilidade aos gestores.

Durante esse período, muitos gestores vêm-se acuados em decorrência da ausência de ferramentas que mapeiam e reduzem os riscos presentes na nova tecnologia. Trata-se de um momento de exposição maior a incerteza e de grande necessidade de requisitos genéricos de segurança.

O abismo pode ser visto como conseqüência direta da evolução tecnológica, baixa demanda de mecanismos de proteção, alto grau de complexidade dessas soluções e outros fatores. É interessante observar que mesmo hoje, com o aumento das preocupações a respeito da segurança da informação, a procura por mecanismos de sustentação de negócios ou ao usuário ainda é superior que a procura da segurança. Assim como no passado, primeiro inventa-se a tecnologia e só depois do surgimento dos primeiros problemas é que procura-se a solução.

4 Sobrevivendo ao abismo

No decorrer das últimas décadas, poucos mercados demonstraram-se ser mais dinâmicos e inovadores do que o de telecomunicações. Além de inovações amplamente conhecidas como as redes IP, tecnologias menos conhecidas pelo grande público tais como protocolos de sinalização e transmissão de dados transformaram profundamente esse mercado.

Esse mercado, peculiarmente pioneiro, revela porém, um abismo de anos entre a descoberta e a solução dos problemas de segurança nos protocolos de sinalização em banda. Essas vulnerabilidades, especialmente uma, conhecida como BlueBox, causaram no decorrer de 30 anos, incontáveis prejuízos as operadoras de telefonia e garantiram momentos notórios da história da informática. A técnica, apesar de ter sido tema de uma matéria da Esquire Magazine em 71, continuava a ser amplamente explorada até final dos anos 90.

Talvez por conta desse tipo de experiências, poucas organizações internacionais venham buscando tão intensamente promover a segurança da informação como a International Telecommunication Union, ou ITU cuja função principal é coordenar o sistema telefonico em âmbito global. Nos últimos 10 anos o ITU publicou mais de 25 recomendações sobre segurança da informação, sendo a mais famosa delas a recomendação X.509 que define o formato dos certificados digitais adotados no dia de hoje pela ICP Brasil, Rede do Sistema Financeiro Nacional, etc.

Porém nem todas as recomendações do ITU são tão técnicas como a X.509, duas delas chamam atenção pelo grau de abstração, a X.805 – Security Architecture for Systems providing end-to-end communications e a E.408 – Telecommunication network security requirements.

5 Entendendo a E.408

Apesar da semelhança de conteúdo, as recomendações X.805 e E.408 apresentam diferentes escopos e objetivos. Enquanto a X.805 apressa-se em definir uma arquitetura de segurança para redes, a E.408 abstrai-se ainda mais ao listar os requisitos mínimos de segurança de uma rede de telecomunicações. Ou seja, trata-se de uma recomendação de alto nível, que evita definir mecanismos e algoritmos de segurança.

Logo no início da recomendação E.408, o ITU procura definir duas grandes constantes denominadas “personagens e atores” e finalmente os “domínios de segurança”.

Segundo a recomendação, é considerado ator todo aquela pessoa (física ou jurídica) ou processo responsáveis por alguma operação no ambiente. Consequentemente, toda vez que um ator toma uma ação. Em outras palavras, uma empresa pode assumir o papel de fornecedor de soluções de telefonia, indiferentemente do fato de ser paralelamente usuário do serviço provido por seus equipamento. Segundo a publicação, são exemplos de personagens os Operadores de Telefonia, Provedores de Serviço, Usuários do Serviço, Vendedores, etc.

Já os domínios de segurança são grupos de entidades ou partes envolvidas sujeitas a uma política de segurança única ou a uma administração de segurança única. Segundo o documento, deve-se considerar a idéia de separar um ambiente em domínios de segurança para delimitar responsabilidades de gerenciamento da segurança. São considerados possíveis fatores de separação temas como distância física, limites geográficos, responsabilidades gerenciais, necessidades de disponibilidade e recuperação, etc. Uma vez definidos essas duas constantes a E.408 define uma série de objetivos de segurança e aborda a necessidade de conformidade com a legislação vigente e após expor as principais ameaças ao serviço de telecomunicações.

Só então a E.408 aborda seu tema principal, os requisitos de segurança. O documento atenta que no âmbito da recomendação, o termo requisito não denota funcionalidade mandatária a cada rede de telecomunicações mas, funcionalidades cuja obrigatoriedade ou não, dependem dos objetivos de segurança da política do operador. A Figura 1 mostra detalhadamente a relação entre os requisitos, ameaças, objetivos de demais componentes da arquitetura de segurança.

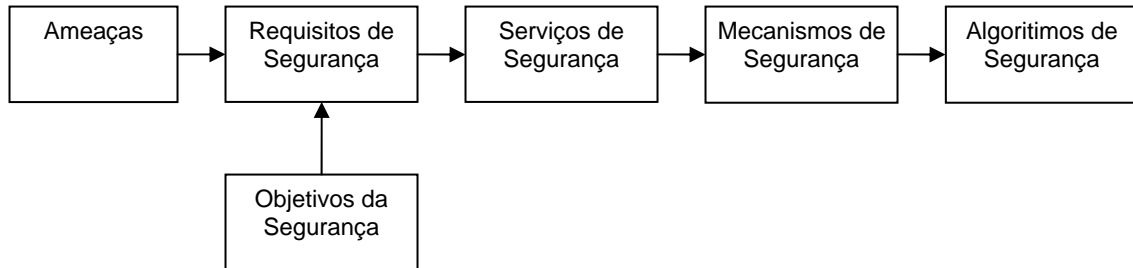


Figura 1

Atente-se também ao fato que os termos Mecanismos e Algoritmos de Segurança possuem um significado incomum à maioria. São considerados mecanismos de segurança, equipamentos ou instalações que venham a prover um serviço de segurança através do uso de um algoritmo. Ou em outras palavras, podemos considerar um sistemas de autenticação como um **mecanismo de segurança** que provê o **serviço** de controle de acesso através do uso de um **algoritmo** de critpografia e certificação digital.

Porém, a parte mais significativa do E.408 é a definição dos requisitos funcionais da segurança. Nessa parte do documento, o ITU dedica-se a mapear de forma matricial a ligação entre requisitos funcionais da segurança e as ameaças ao ambiente.

De certa forma, esse mapeamento matricial, agnóstico às tecnologias envolvida nos processos de segurança nos leva a concluir que o E.408 encara a segurança como uma tecnologia sustentadora, ou em outras palavras, independentemente das novas facilidade, custos e performance das tecnologias envolvidas elas são facilmente assimiladas pelo mercado como evoluções daquilo que já se conhecia.

6 Reaproveitando o padrão

Uma vez compreendido o padrão E.408 podemos seguir adiante a entender como podemos utilizá-lo na redução do impacto de segurança de novas tecnologias. Mas primeiro é preciso entender como os conceitos de consumo definidos por Moore e as recomendações do ITU podem trabalhar em conjunto.

Antes de mais nada, é preciso entender que as ameaças presentes em uma nova tecnologia dificilmente se diferenciam das anteriormente existentes, o que nos permite utilizar exaustivamente da abstração presente em padrões como o E.408.

Redes de Voz e sistemas de email possuem ameaças praticamente iguais, ainda que as vulnerabilidades presentes nesses ambientes sejam absolutamente diferentes.

Por outro lado, enquanto algumas empresas tem uma baixa tolerância a risco, outras preferem se expor e manter, por exemplo, um perfil de liderança tecnológica no setor. Vemos isso claramente na área de telecomunicações do mercado financeiro. Enquanto algumas instituições já estudam buscar adotar sistemas de teleconferência em suas agências, outras sequer aposentaram seus enlaces de 9600bps dentro de grandes cidades. Não se trata de taxar uma organização como ineficiente, muito pelo contrário, algumas vezes, a organização mais conservadora possui plena liderança no setor, mesmo sem fazer uso extensivo da tecnologia de ponta.

Outro exemplo do peso do perfil pode ser visto em empresas de telecomunicações cujos investimentos costumam ser orientados por tendências. Uma vez que uma grande operadora invista em uma tecnologia, as outras tendem a segui-la, adotando muitas vezes a mesma solução adotada por suas concorrentes.

Conforme vemos na Figura 2 a relação entre o perfil de consumo e exposição a risco da organização e o modelo proposto pelo E.408

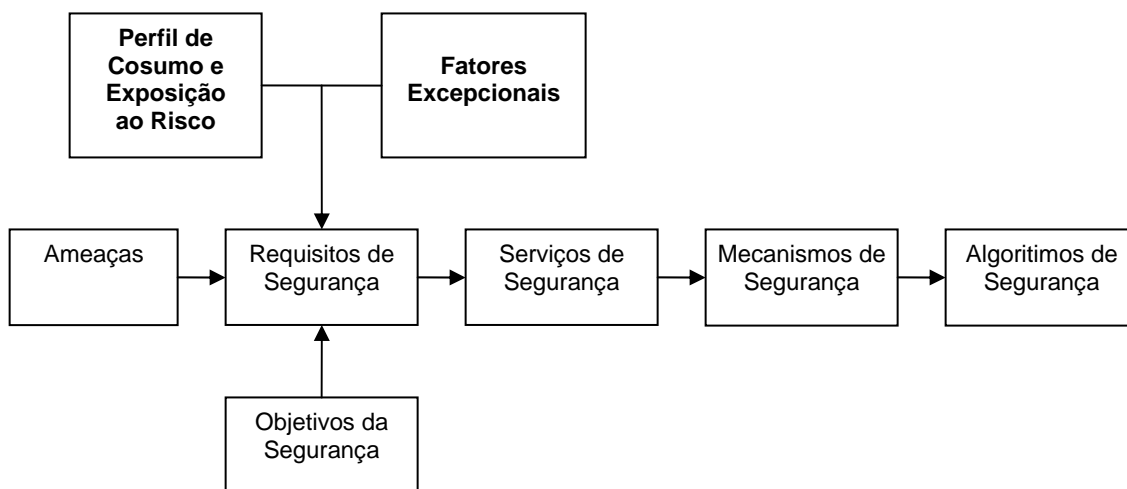


Figura 2

Essa concepção baseia-se no fato de que as mesmas ameaças costumam ser compartilhadas por tecnologias absolutamente diferentes, porém a forma de corrigi-las dependerá dentre outros, dos requisitos de segurança dessa tecnologia e do contexto de negócios em que ela está encaixada.

Porém como novas tecnologias, mesmo que de segurança, apresentam novas vulnerabilidades, o abismo **sempre** estará presente. Cabe ao gestor da segurança encontrar mecanismos disponíveis ou de fácil desenvolvimento para equilibrar os objetivos da segurança com a força do perfil da empresa e fatores excepcionais.

A publicação Risk Management Guide for Information Technology Systems do NIST - National Institute of Standards and Technology – lista dentre outras as seguintes estratégias de redução de risco:

Assumir – Consiste em aceitar a existência do risco potencial e continuar as operações ou implementar controles que reduzam o risco a um nível aceitável;

Evitar – Consiste em prevenir o risco através da eliminação de sua causa ou consequência;

Limitar – Consiste em limitar o risco através do uso de controles que minimizem o impacto da exploração de uma vulnerabilidade;

Transferir – Consiste na transferência do risco através de meios alternativos de compensação das perdas.

As estratégias apresentadas pelo NIST mostram que uma organização poderá diante de uma mesma ameaça optar por diferentes respostas e consequentemente mecanismos de proteção. Ainda nesse sentido, Moore afirma historicamente, visionários toleraram um grande nível de risco ao negócios de forma a alcançar um avanço notável na produtividade e relacionamento com os clientes. Tanto a afirmação de Moore quanto a o guia do NIST levam à conclusão de que diferentes organizações terão maior predisposição a reagir de forma compatível com seu perfil.

É possível portanto adotar, ainda que de forma simplificada o seguinte mapeamento entre estratégias e perfis:

	Visionário	Pragmático	Conservador
Característica principal	Predisposição a assumir o risco	Predisposição a limitar o risco	Predisposição a Evitar o risco
Característica Secundária	Se possível limitará o risco	Se possível irá transferir o risco	Se possível irá transferir o risco

Tabela 1

Como mostra a Tabela 1 ao considerar uma nova tecnologia, security officer e a organização devem além de medir o risco, avaliar também, as características das soluções disponíveis até mesmo ao ponto de adotar soluções intermediárias, capazes de promover a adoção da nova tecnologia com um grau mínimo de controles. O conceito torna-se mais claro ao observarmos o seguinte exemplo.

Considere que essa é a lista de vulnerabilidades básicas apresentadas pelas famílias de rede sem fio baseadas no padrão IEEE 802.11.

Ameaça / Tecnologia	WLAN
<i>Spoofing</i>	X
Interceptação	X (sniffing)
Acesso não autorizado	X
Repúdio	X
Denial of Service	X

Tabela 2

Essas ameaças deram origem a pelo menos dois formatos de segurança amplamente aceitos, o primeiro conhecido como WEP – Wired Equivalent Privacy e um segundo denominado WPA2² - Wi-Fi Protected Access.

WLAN	
Ameaça	Solução WEP
<i>Spoofing</i>	N/A
Interceptação	Criptografia
Acesso não autorizado	Criptografia
Repúdio	N/A
Denial of Service	N/A

WLAN	
Ameaça	Solução WPA2
<i>Spoofing</i>	Assinaturas digitais
Interceptação	Criptografia
Acesso não autorizado	Autenticação forte
Repúdio	Assinaturas digitais
Denial of Service	N/A

Tabela 3

Conforme observa-se na Tabela 3 nota-se claramente que apesar de promoverem segurança para uma mesma tecnologia, WEP e WPA2 apresentam um nível distinto de proteção. Isso entretanto não significa que redes sem fio só se tornaram seguras após a padronização do WPA2. Com base na Tabela 4, observa-se que bem antes do WPA2 ter sido padronizado, soluções paleativas baseadas em uso de VPN IPsec ofereciam nível de segurança semelhante ao das soluções atuais.

WLAN	
Ameaça	Solução WEP+Ipsec
<i>Spoofing</i>	Assinaturas Digitais
Interceptação	Criptografia
Acesso não autorizado	Autenticação forte
Repúdio	Assinaturas digitais
Denial of Service	N/A

WLAN	
Ameaça	Solução WPA2
<i>Spoofing</i>	Assinaturas digitais
Interceptação	Criptografia
Acesso não autorizado	Autenticação forte
Repúdio	Assinaturas digitais
Denial of Service	N/A

Tabela 4

Ou seja, enquanto soluções integradas como o WPA2 tendem a apresentar custo operacional inferior, a adoção de tecnologias paleativas, oferece respostas mais rápidas, muitas viabilizando tanto um nível aceitável de risco quanto o avanço significativo que os visionários de Moore buscam.

² O WPA2 é assim denominado por ser uma padronização internacional derivante de uma padrão conhecido como WPA que serviu como solução intermediária entre o WEP e o WPA2.

Se considerarmos a cronologia a seguir, vemos claramente que as redes WiFi permaneceram o mesmo nível de segurança por cerca de dois anos após padrão WEP ter sido publicamente reconhecido como inseguro.

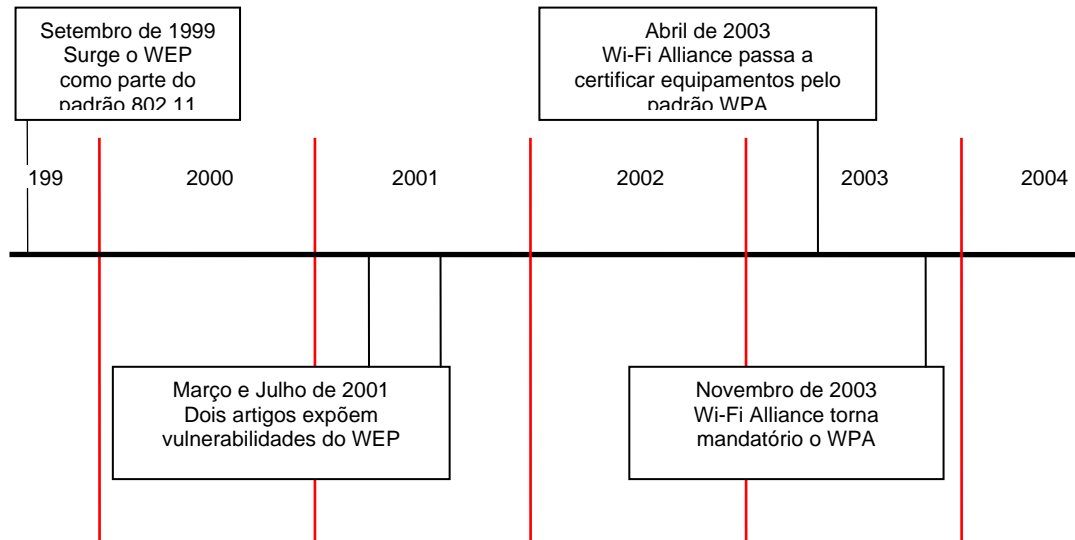


Figura 3

Entretanto a adoção das redes sem fio prosseguiu. De acordo com o IDC, somente em 2002 cerca de 10 milhões de interfaces wireless haviam sido vendidos no mundo.³

A verdade é que aplicações que necessitavam de mobilidade em instituições indispostas a elevar de forma drástica o seu grau existente de risco, adotaram técnicas de limitação fazendo uso de mecanismos de segurança como o IPsec, um mecanismo padronizado de criptografia de redes de dados publicado ainda em 1998 pelo IETF.

Ainda assim o que teria levado inúmeros gestores de segurança a rotularem como inseguras as redes sem fio? Conservadorismo, excesso de zelo e pouca flexibilidade são, sem dúvida alguma, parte da resposta. O fato é que analisadas friamente, sem o fator passional que uma nova tecnologia traz, as redes sem fio e redes convencionais possuem as mesmas ameaças ainda que as vulnerabilidades referentes a cada tecnologia sejam distintas. Ainda que sejam encaradas como tecnologias disruptivas por gestores de segurança, as redes sem fio são essencialmente suportantes ao negócio.

³ Worldwide Wireless LAN Equipment 2004-2008 Forecast - Abner Germanow, IDC #31377 June 2004

De fato, a lista de vulnerabilidades apresentada na Tabela 2 representa as vulnerabilidades de praticamente todas as redes de transmissão de dados, sejam elas baseadas em tecnologias sem fio ou não.

Para atravessar o abismo da segurança em novas tecnologias, é necessário absorver esses novos conceitos e ao mesmo tempo focar nas ameaças e não apenas nas vulnerabilidades da nova tecnologia.

7 Controles baseados em Classes Funcionais

Uma estratégia muito interessante recomendada pelo ITU e adotada por algumas organizações é a adoção de Classes Funcionais onde define-se os serviços de segurança mínimos a uma determinada classe.

Utilizando o modelo proposto pelo E.408, é possível definir a seguinte série de classes funcionais baseadas no perfil da organização. O conceito é simples, considerando-se que dificilmente o Security Office terá força suficiente para inviabilizar a adoção de uma nova tecnologia crítica ao negócio de sua organização, os gestores devem focar em uma abordagem construtiva à adoção da tecnologia.

O uso de classes oferece ao gestor grande flexibilidade, visto que ele pode diferenciar tanto critérios de negócio como o perfil dos clientes internos, e agrupá-los de forma a oferecer soluções individualizadas.

Visionário	Pragmático	Conservador
<i>Ênfase na disponibilização da tecnologia</i>	<i>Ênfase na limitação de riscos</i>	<i>Ênfático em evitar o risco</i>
<ul style="list-style-type: none"> • Autenticação • Controle de acesso na camada de aplicação • Alarmes e auditoria 	<ul style="list-style-type: none"> • Autenticação • Controle de acesso sobre a conexão • Alarmes e auditoria • Autenticação da origem de dados • Controle de Integridade da conexão 	<ul style="list-style-type: none"> • Autenticação • Controle de acesso sobre a conexão • Alarmes e auditoria • Autenticação da origem de dados • Controle de Integridade da conexão • Confidencialidade da conexão;
Opcionais: <ul style="list-style-type: none"> • Controle de acesso sobre a conexão 	Opcionais: <ul style="list-style-type: none"> • Confidencialidade da conexão 	Opcionais: <ul style="list-style-type: none"> • Transparência ao usuário

Tabela 5

Ou utilizando novamente a tecnologia de redes sem fio IEEE 802.11 pode-se ver como as classes funcionais podem ser atreladas a requisitos de negócio:

WLAN		
Hot spots	Corporativa perimetral	Corporativa de larga escala
Ênfase na disponibilidade da tecnologia	Ênfase na limitação de riscos	Ênfático em evitar o risco
<ul style="list-style-type: none"> • Autenticação junto ao access point é realizada através de interface WWW; • Alarmes e auditoria são disponíveis 	<ul style="list-style-type: none"> • Assume-se a rede sem fio como área insegura, requerendo mecanismo adicional de segurança; • Autenticação e controle de acesso e integridade da conexão assim como a autenticação da origem de dados são providos por cliente IPsec 	<ul style="list-style-type: none"> • WPA/WPA2
<ul style="list-style-type: none"> • WEP pode ser usado como provedor de privacidade mínima. Cabe ao usuário do hot spot utilizar mecanismo adicional de segurança se desejar. 	<ul style="list-style-type: none"> • Uso da funcionalidade de criptografia de dados do Ipsec⁴ 	

Tabela 6

A Tabela 6 mostra que considerando os fatores excepcionais e de perfil de tolerância ao risco, diferentes organização puderam ou não aplicar a mesma tecnologia sem compromisso a seus negócios. Curiosamente hoje, mesmo após o WPA2 estar disponível no mercado, raríssimos são os casos de HOT Spots que o consideram necessário. Não se trata apenas de ignorar o problema, lançando-o sobre as costas do usuário, o fato é que esse modelo de negócios tolera uma exposição maior às ameaças presentes na nova tecnologia enquanto a organização necessita disponibilizar a tecnologia para garantir sua sobrevivência.

Outro fato interessante a se aprender do modelo de segurança adotado em HOT spots é que esses pontos fazem uso de mecanismos de autenticação integrados à camada de aplicação. A tabela abaixo, é parte da norma ISO 7498-2 que normatizou ainda em 1989 uma série de serviços de segurança e as camadas do modelo OSI ao qual deveriam se aplicar:⁵

⁴ Apesar de redes IPsec sem criptografia não serem comuns, o protocolo trata separadamente a autenticação de origem e a criptografia do conteúdo de dados;

⁵ Note que o TCP/IP baseia-se no mesmo princípio de camadas do modelo OSI, entretanto, a separação e número de camadas não são idênticos. Por ser mais flexível foi adotado nesse texto o modelo OSI.

! A norma ISO 7498-2 não reconhecia originalmente sistemas de autenticação e controle de acesso na 2ª camada. Entretanto essa funcionalidade foi incorporada por tecnologias posteriores ao padrão.

Service	Layer						
	1	2	3	4	5	6	7
Peer Entity Authentication	•	!	Y	Y	•	•	Y
Data Origin Authentication	•	•	Y	Y	•	•	Y
Access Control Service	•	!	Y	Y	•	•	Y
Connection Confidentiality	Y	Y	Y	Y	•	•	Y
Connectionless Confidentiality	•	Y	Y	Y	•	•	Y
Selective Field Confidentiality	•	•	•	•	•	•	Y
Traffic Flow Confidentiality	Y	•	Y	•	•	•	Y
Connection Integrity with Recovery	•	•	•	Y	•	•	Y
Connection Integrity without Recovery	•	•	Y	Y	•	•	Y
Selective Field Connection Integrity	•	•	•	•	•	•	Y
Connectionless Integrity	•	•	Y	Y	•	•	Y
Selective Field Connectionless Integrity	•	•	•	•	•	•	Y
Non-repudiation, Origin	•	•	•	•	•	•	Y
Non-repudiation, Delivery	•	•	•	•	•	•	Y

Tabela 7

Note portanto que desde as especificações básicas do modelo OSI a camada de aplicação possui grande responsabilidade acerca da segurança do processo de comunicação. Aplicações como ssh e https são exemplos atuais da aplicação desse conceito onde ao invés de definir mecanismos de segurança nas camadas inferiores, os desenvolvedores dessas tecnologias atacaram o problema no nível mais alto do modelo OSI.

Observa-se portanto que o modelo de segurança aplicado por hotspots remonta ao ano de 1989, mais de 10 anos antes do lançamento da tecnologia de redes sem fio na qual se baseiam atualmente.

Sem dúvida, o modelo proposto pela ISO 7498-2 é por demais tecnicista, porém, ao assimilar o foco dessa norma na abstração por camadas, percebe-se que o alvo final não é a tecnologia em si mas a potencialização do uso de analogias.

Um fator interessante do modelo de negócios de hotspots é o fato de que as únicas informações que precisam ser protegidas ao trafegar na rede sem fio são aquelas relativas ao método de pagamento do serviço e autenticação, ou seja, requisitos não muito diferentes dos demais sites de comércio eletrônico. Por outro lado, empresas ansiosas por oferecer a tecnologia de redes sem fio, optaram por considerar suas redes sem fio ambientes não confiáveis, requerindo o uso de VPNs idênticas àquelas utilizadas por seus usuários remotos.

O uso de analogias ou comparação entre tecnologias pode prover inúmeras respostas ao gestor que busca aliar velocidade de assimilação da tecnologia e o nível de segurança exigido pela empresa.

Assim como observa Clayton Christensen, são organizações capazes de se adaptar às limitações de uma tecnologia que tendem a fomentar a evolução dessa tecnologia e justamente por isso não é de se espantar que as soluções adotadas pelo WPA2 sejam de fato similares às soluções intermediárias baseadas em IPsec ou SSL.

8 Limitação do risco

Conforme foi exposto anteriormente, existe mais de uma forma de limitar o risco ao qual uma nova tecnologia nos expõe e cada empresa possui uma tendência a optar por determinado mecanismo. Dentre as formas mais comuns podemos citar a segmentação e controle perimetral, assim como a sobreposição de camadas, cujos mais simples exemplos são respectivamente o uso de firewalls e VPNs.

Voltando-se ao passado recente, observa-se que uma vez ameaçadas por um ambiente tão descontrolado como a Internet as empresas decidiram construir muralhas ao redor de sua infra-estrutura, ao mesmo tempo em que adotavam as VPNs como mecanismo facilitador de negócios, permitindo acesso remoto e seguro a colaboradores e parceiros de negócios.

Porém, como exposto logo no início desse capítulo, **toda nova tecnologia apresenta um potencial de risco maior ou igual que os benefícios que traz** e novamente *firewalls* e VPNs apresentam um fenômeno interessante no que tange a segurança.

Hoje, quando *firewalls* e *VPNs* encontram-se perfeitamente integrados como um só produto a realidade encontrada pelos primeiros usuários de VPNs assemelha-se mais a um desenho rupestre do que do desenho de uma rede de dados.

Os primeiros firewalls ofereciam primariamente controle de acesso com base em pacotes, sem conceitos como controle de sessão e conteúdo. Já VPNs buscavam oferecer aos dados trafegando em uma rede insegura um nível de privacidade semelhante ao encontrado em uma rede privada. Porém, esses objetivos e distintos levaram a um novo problema. Como controlar o acesso de usuários através de VPN sendo que ele encontra-se criptografado? E como garantir que esse acesso criptografado não fosse usado para um eventual ataque?

Já em dezembro de 1998 pesquisadores publicavam na lista *bugtraq*⁶ o impacto causado pela disponibilização do software do provedor America Online aos usuários de um ambiente. O programa criava um tunel entre o micro do usuário e a AOL o qual não era sujeito às políticas de controle de acesso impostas através do firewall.

⁶ AOL client uses IP tunneling, Jenik, A. , 21 Dez 1998 <http://seclists.org/lists/bugtraq/1998/Dec/0101.html>

Foi através do resultado dessas pesquisas que tornou-se evidente a necessidade de integração entre *firewalls* e *VPNs*, assim como mecanismos que impedissem que o usuário de uma VPN não pudesse acessar simultaneamente sites públicos e a VPN da empresa.

Outro exemplo, dessa vez vindo do mercado financeiro é a indisponibilidade dos sistemas auto atendimento presenciais durante a noite. Diante das ameaças que a presente situação da segurança pública oferece ao usuários dos sistemas de auto-atendimento, organizações adaptaram-se ao risco e interromperam o funcionamento dos sistemas em lugares não vigiados após as 22 horas, além é claro, de limitar os danos ao impor limites de saque de dinheiro após esse mesmo horário.

Conclui-se portanto que a limitação de risco é obtida através do confinamento, monitoramento do novo ambiente, impondo limites entre a nova tecnologia e o ambiente já estabelecido. Esses limites podem ser meramente tecnológicos ou aplicados ao negócio tais como os limites diários de transações em um sistema de Internet Banking.

9 Assunção do risco

Considerando-se a certitude da existência do risco mas também o desconhecimento de ameaças ou disponibilidade de mecanismos que protejam o novo ambiente e até mesmo a ignorância parcial acerca dos riscos, há uma estratégia amplamente adotada por organizações vanguardistas que consiste em assumir o risco ao mesmo tempo em que promove a evolução do nível de segurança do novo ambiente. É possível observar o uso prático dessa estratégia no mercado financeiro brasileiro. Apesar de notadamente limitados no que tange a segurança, os sistemas de automação e pagamentos baseados em cartões magnéticos continuam sendo amplamente usados, ainda que tanto ameaças quanto tecnologias capazes de corrigi-las existam. Como a substituição repentina de cartões magnéticos por smart cards traria custos operacionais elevados as instituições financeiras optaram por assumir o risco ao mesmo tempo em que encontram meios paleativos de combater o risco.

Outro exemplo onde gestores optaram por assumir os riscos encontra-se justamente em sistemas de voz sobre IP, que no momento em que esse livro é escrito é uma das tecnologias em grande ascensão no mercado mundial. Os diversos desenvolvedores de sistemas de voz sobre IP costumam definir um grupo comum de ameaças a esse tipo de ambientes. O CableLabs, responsável pelo desenvolvimento do padrão Voice over PacketCable, que padroniza a voz sobre IP em redes de TV a Cabo lista dentre outras as seguintes ameaças:

- Roubo de Serviços e clonagem
- Interceptação;
- Manipulação de protocolo;

- Interrupção de serviços;

Basicamente, a lista de ameaças é quase igual à de uma operadora de telefonia móvel. O padrão de segurança em ambientes PacketCable é bastante detalhado e lista entre outros mecanismos a adoção de IPSec como proteção contra interceptação de sinais. Curiosamente, diversas das operadoras de TV a cabo que decidiram oferecer serviços de voz a seus clientes optam por não fazer uso do IPSec. A razão é simples, o uso desse mecanismo encarece a solução à medida em que requer maior capacidade de processamento e tráfego de dados dos dispositivos envolvidos, reduzindo significativamente a escalabilidade da solução, o que pode em muitos casos inviabilizar o início das operações.

O fato é que ainda que já sejam conhecidas ferramentas e ataques capazes de realizar escutas de conversas telefônicas em voz sobre IP, a privacidade oferecida por uma rede de voz sobre PacketCable é equivalente àquela oferecida por uma rede de voz convencional, o que acaba reduzindo significativamente a importância dos mecanismos de privacidade das conversas.

Portanto, ao contrário do que creem muitos gestores de segurança a assunção do risco pode ser uma estratégia eficaz e aceitável na adoção de novas tecnologias, desde que devidamente avaliado o contexto de negócio. Gerenciar riscos existentes, desenvolvendo processos que garantam a evolução e adoção dos recursos de segurança é perfeitamente aceitável desde que realizado de forma consciente

10 Transferência do risco

Ao contrário do que a maioria acredita a limitação e assunção não são as formas mais populares de reação ao risco. A forma mais comum entre os controles de risco é a transferência do risco, cujo maior exemplo são os seguros utilizados no dia a dia de milhares de pessoas e empresas. Porém a contratação de seguro não é a única saída para aqueles que desejam transferir o risco existente em uma nova tecnologia, na verdade, vem do comércio eletrônico uma das políticas mais conhecidas acerca dessa estratégia.

Durante o nascimento do comércio eletrônico sites e operadoras possuíam prioridades distintas. Enquanto as lojas eletrônicas precisavam vender para viabilizar suas atividades e o negócio que ali se iniciava, operadores de cartão de crédito, cujo negócio já estava plenamente estabelecido não viam necessidade de prover mecanismos de segurança flexíveis. Às vistas da operadora, a compra em um site não diferia significativamente das compras realizadas por telefone e portanto nada mais natural do que adotar as mesmas medidas utilizadas por empresas especializadas em venda por telefone, entre elas, onerar o vendedor pelos custos de transações fraudulentas.

Ao agir dessa forma, as operadoras simplesmente transferiram o risco que a nova tecnologia apresentava aos comerciantes, obrigando-os a adotar mecanismos que evitassem as fraudes. Esses mecanismos muitas vezes não eram tão inovadores quanto a tecnologia da qual faziam uso, controles mais rígido sobre logística e entrega de encomendas são tão críticos para esses sites quanto firewalls, criptografia e equipamentos redundantes.

Curiosamente, a transferência de responsabilidades permitiu às bandeiras de cartão de crédito viabilizar as transações eletrônicas ainda que o padrão SET de pagamentos eletrônicos desenvolvido em conjunto por MasterCard e VISA nunca tenha sido amplamente utilizado.

10 Indo além

Uma vez comentadas a assunção, limitação e transferência do risco, o que dizer da prevenção ou eliminação do risco? Acredito que há pouco a se dizer sobre isso quando se fala em novas tecnologias, ou mesmo que se trata de ingenuidade considerar que essa opção é viável nos dias de hoje. A competitividade acentua o grau de exposição ao risco nas empresas e security officers são cada vez mais pressionados a produzir soluções inovadoras ou até mesmo reutilizar conceitos. Reutilize conceitos e seja criativo e flexível. O mercado e sua empresa agradecem.

Sobre o Autor:

André Fucs de Miranda é Certified Information Systems Security Professional com cerca de uma década de atuação no mercado internacional de segurança da informação. Participou de alguns dos mais importantes projetos de VoIP do Oriente Médio, e em sua carreira registra passagem em empresas como Lucent Technologies, Unibanco e CFSEC Security Architects.