

# **Segurança de Redes em Ambientes Cooperativos**

**Emilio Tissato Nakamura  
Paulo Lício de Geus**

# CAPÍTULO 1

## Introdução

A necessidade de segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios.

O mundo da segurança, seja pensando em violência urbana ou em *hackers*, é peculiar. Ele é marcado pela evolução contínua, no qual novos ataques têm como resposta novas formas de proteção, que levam ao desenvolvimento de novas técnicas de ataques, de maneira que um ciclo é formado. Não é por acaso que é no elo mais fraco da corrente que os ataques acontecem. De tempos em tempos os noticiários são compostos por alguns crimes ‘da moda’, que vêm e vão. Como resposta, o policiamento é incrementado, o que resulta na inibição daquele tipo de delito. Os criminosos passam então a praticar um novo tipo de crime, que acaba virando notícia. E o ciclo assim continua. Já foi comprovada uma forte ligação entre seqüestradores e ladrões de banco, por exemplo, na qual existe uma constante migração entre as modalidades de crimes, onde o policiamento é geralmente mais falho.

Esse mesmo comportamento pode ser observado no mundo da informação, de modo que também se deve ter em mente que a segurança deve ser contínua e evolutiva. Isso ocorre porque o arsenal de defesa usado pela organização pode funcionar contra determinados tipos de ataques; porém, pode ser falho contra novas técnicas desenvolvidas para driblar esse arsenal de defesa.

Alguns fatores podem ser considerados para que a preocupação com a segurança contínua seja justificada:

- a) **Entender a natureza dos ataques é fundamental:** é preciso entender que muitos ataques são resultado da exploração de vulnerabilidades, as quais passam a existir devido a uma falha no projeto ou na implementação de um

protocolo, aplicação, serviço ou sistema, ou ainda devido a erros de configuração e administração de recursos computacionais. Isso significa que uma falha pode ser corrigida, porém novos *bugs* sempre existirão;

- b) Novas tecnologias trazem consigo novas vulnerabilidades:** é preciso ter em mente que novas vulnerabilidades surgem diariamente. Como novas tecnologias e novos sistemas são sempre criados, é razoável considerar que novas vulnerabilidades sempre existirão e, portanto, novos ataques também serão sempre criados. As redes sem fio (*wireless*), por exemplo, trazem grandes benefícios para as organizações e os usuários, porém trazem também novas vulnerabilidades que podem colocar em risco os negócios da organização;
- c) Novas formas de ataques são criadas:** a própria história mostra uma evolução constante das técnicas usadas para ataques, que estão cada vez mais sofisticadas. A mistura de diferentes técnicas, o uso de tecnologia para cobrir vestígios a cooperação entre atacantes e a criatividade são fatores que tornam a defesa mais difícil do que o habitual;
- d) Aumento da conectividade resulta em novas possibilidades de ataques:** a facilidade de acesso traz como conseqüência o aumento de novos curiosos e também da possibilidade de disfarce que podem ser usados nos ataques. Além disso, novas tecnologias, principalmente os novos protocolos de comunicação móvel, alteram o paradigma de segurança. Um cenário onde os usuários de telefones celulares são alvos de ataques e usados como porta de entrada para ataques a uma rede corporativa, por exemplo, é completamente plausível;
- e) Existência tanto de ataques direcionados quanto de ataques oportunistas:** apesar de a maioria dos ataques registrados ser oportunística, os ataques direcionados também existem em grande número. Esses ataques direcionados podem ser considerados mais perigosos, pois, existindo a intenção de atacar, a estratégia pode ser cuidadosamente pensada e estudada, e executada de modo a explorar o elo mais fraco da organização. Esses são, geralmente, os ataques que resultam em maiores prejuízos, pois não são feitos de maneira aleatória, como ocorre com os ataques oportunistas. Isso pode ser observado também pelo nível de agressividade dos ataques. Quanto mais agressivo é o ataque, maior é o nível de esforço dispensado em um ataque a um alvo específico. É interessante notar também que a agressividade de um ataque está relacionada com a severidade, ou seja, maiores perdas;
- f) A defesa é mais complexa do que o ataque:** para o *hacker*, basta que ele consiga explorar apenas um ponto de falha da organização. Caso uma determinada técnica não funcione, ele pode tentar explorar outras, até que seus objetivos

sejam atingidos. Já para as organizações, a defesa é muito mais complexa, pois exige que todos os pontos sejam defendidos. O esquecimento de um único ponto faz com que os esforços dispensados na segurança dos outros pontos sejam em vão. Isso acaba se relacionando com uma das principais falácias do mundo corporativo: a falsa sensação de segurança. É interessante notar que, quando o profissional não conhece os riscos, ele tende a achar que tudo está seguro com o ambiente. Com isso, a organização passa, na realidade, a correr riscos ainda maiores, que é o resultado da negligência. Isso acontece com os *firewalls* ou com os antivírus, por exemplo, que não podem proteger a organização contra determinados tipos de ataques.

**g) Aumento dos crimes digitais:** o que não pode ser subestimado são os indícios de que os crimes digitais estão se tornando cada vez mais organizados. As comunidades criminosas contam, atualmente, com o respaldo da própria internet, que permite que limites geográficos sejam transpostos, oferecendo possibilidades de novos tipos de ataques. Além disso, a legislação para crimes digitais ainda está na fase da infância em muitos países, o que acaba dificultando uma ação mais severa para a inibição dos crimes.

Dentre os fatos que demonstram o aumento da importância da segurança, pode-se destacar a rápida disseminação de vírus e *worms*, que são cada vez mais sofisticados. Utilizando técnicas que incluem a engenharia social, canais seguros de comunicação, exploração de vulnerabilidades e arquitetura distribuída, os ataques visam a contaminação e a disseminação rápida, além do uso das vítimas como origem de novos ataques. A evolução dos ataques aponta para o uso de técnicas ainda mais sofisticadas, como o uso de códigos polimórficos para a criação de vírus, *worms*, *backdoor* ou *exploits*, para dificultar sua detecção. Além disso, ferramentas que implementam mecanismos que dificultam a adoção da forense computacional também já estão sendo desenvolvidos. Os canais ocultos ou cobertos (*covert channels*) tendem a ser usados para os ataques, nos quais os controles são enviados por túneis criados com o uso de HTTPS ou o SSH, por exemplo. O uso de ‘pontes’ de ataques e mecanismos do TCP/IP para dificultar a detecção e investigação igualmente tende a ser cada vez mais utilizado. Ataques a infra-estruturas envolvendo roteamento ou DNS, por exemplo, também podem ser realizados.

Alguns incidentes mostram que os prejuízos com a falta de segurança podem ser grandes. O roubo de 5,6 milhões de números de cartões de crédito da Visa e da MasterCard de uma administradora de cartões americana, em fevereiro de 2003 [JT 03], por exemplo, pode sugerir grandes problemas e inconvenientes para as vítimas. No Brasil, o roubo de mais de 152 mil senhas de acesso de grandes provedores de acesso, em março de 2003, resultou em quebra de privacidade e, em muitos casos,

perdas bem maiores [REV 03]. No âmbito mundial, variações de *worms* como o Klez ainda continuam na ativa, mesmo passado mais de um ano desde seu surgimento. A primeira versão do Klez surgiu em novembro de 2001 e a versão mais perigosa, em maio de 2002; em março de 2003, o Klez era o *worm* mais ativo do mês [MES 03]. Em junho de 2002, um incidente de segurança envolvendo usuários de cinco dos maiores bancos e administradores de cartões de crédito do Brasil resultou em prejuízos calculados em R\$ 100 mil [TER 02], mostrando que incidentes envolvendo instituições financeiras estão se tornando cada vez mais comuns, seja no Brasil ou em outros países.

Outros incidentes notórios podem ser lembrados, como o que envolveu o *worm* Nimda, em setembro de 2001. Um alto grau de evolução pôde ser observado no Nimda, que foi capaz de atacar tanto sistemas *web* quanto sistemas de e-mail. Antes do aparecimento do Nimda, um outro *worm*, o Code Red (e sua variação Code Red II), vinha, e ainda vem, causando grandes prejuízos, não somente às organizações que sofreram o ataque, mas à internet como um todo. Causando lentidão na rede, o Code Red resultou em prejuízos estimados em 2,6 bilhões de dólares nos Estados Unidos, em julho e agosto de 2001. Outro notório evento foi a exploração em larga escala de ferramentas para ataques coordenados e distribuídos, que afetaram e causaram grandes prejuízos, durante 2000, a *sites* como Amazon Books, Yahoo, CNN, eBay, UOL e ZipMail. Somaram-se ainda ataques a *sites* de comércio eletrônico, notadamente o roubo de informações sobre clientes da CDNow, até mesmo dos números de cartões de crédito. Casos de ‘pichações’ de *sites* Web também são um fato corriqueiro, demonstrando a rápida popularização dos ataques a sistemas de computadores.

Porém, os ataques que vêm causando os maiores problemas para as organizações são aqueles que acontecem a partir da sua própria rede, ou seja, os ataques internos. Somado a isso, está o fato de as conexões entre as redes das organizações alcançarem níveis de integração cada vez maiores. Os ambientes cooperativos, formados a partir de conexões entre organizações e filiais, fornecedores, parceiros comerciais, distribuidores, vendedores ou usuários móveis, resultam na necessidade de um novo tipo de abordagem quanto à segurança. Em oposição à idéia inicial, quando o objetivo era proteger a rede da organização isolando-a das redes públicas, nos ambientes cooperativos o objetivo é justamente o contrário: disponibilizar cada vez mais serviços e permitir a comunicação entre sistemas de diferentes organizações, de forma segura. A complexidade aumenta, pois agora a proteção deve ocorrer não somente contra os ataques vindos da rede pública, mas também contra aqueles que podem ser considerados internos, originados a partir de qualquer ponto do ambiente cooperativo.

É interessante observar que o crescimento da importância e até mesmo da dependência do papel da tecnologia nos negócios, somado ao aumento da facilidade de acesso e ao avanço das técnicas usadas para ataques e fraudes eletrônicos, resultam no aumento do número de incidentes de segurança, o que faz com que as organizações devam ser protegidas da melhor maneira possível. Afinal de contas, é o próprio negócio, em forma de bits e bytes, que está em jogo.

Assim, entender os problemas e as formas de resolvê-los torna-se imprescindível, principalmente porque não se pode proteger contra riscos que não se conhece. Este livro tem como principal objetivo apresentar os conceitos, as técnicas e as tecnologias de segurança que podem ser usados na proteção dos valores computacionais internos das organizações. Para isso, a formação de um ambiente cooperativo e as motivações para a implementação de uma segurança coerente serão discutidas. Os motivos que levam à adoção de determinada tecnologia também serão discutidos, bem como a integração das diversas tecnologias existentes, que é, de fato, o grande desafio das organizações.

## Estrutura básica

O livro é dividido em três partes: a Parte I, composta pelos capítulos 2, 3, 4 e 5, faz a ambientação dos problemas que devem ser enfrentados pelas organizações; a Parte II, formada pelos capítulos de 6 a 11, apresenta as técnicas, conceitos e tecnologias que podem ser utilizadas na luta contra os problemas de segurança vistos na Parte I. Já a Parte III (capítulos 12 e 13) apresenta o modelo de segurança proposto pelos autores, no qual os recursos apresentados na Parte II são aplicados no ambiente cooperativo.

O Capítulo 2 faz a apresentação de um ambiente cooperativo e as necessidades de segurança são demonstradas no Capítulo 3. Os riscos que rondam as organizações, representados pelas técnicas de ataque mais utilizadas, são discutidos no Capítulo 4. O Capítulo 5 trata das redes sem fio, que possuem uma importância cada vez maior na vida das pessoas, porém trazem consigo novos riscos.

A política de segurança, os *firewalls*, os sistemas de detecção de intrusão, a criptografia, as redes privadas virtuais e a autenticação dos usuários são discutidos, respectivamente, nos capítulos 6, 7, 8, 9, 10 e 11. Já o Capítulo 12 discute as configurações que podem fazer parte de um ambiente cooperativo, enquanto o Capítulo 13 discute os aspectos de segurança envolvidos nesse tipo de ambiente e o modelo de gestão de segurança proposto. Ele é composto pela arquitetura do *firewall* cooperativo, o modo de minimizar a complexidade das regras de filtragem e o modelo hierárquico de defesa. Este último é destinado a facilitar a compreensão

dos problemas de segurança inerentes a esse tipo de ambiente, resultando assim em menos erros na definição da estratégia de segurança da organização. Ainda no Capítulo 13, o Modelo de Teias tem como objetivo auxiliar no gerenciamento da complexidade da segurança. O Capítulo 14 traz a conclusão do livro.

A seguir, o leitor encontrará um resumo mais detalhado de cada capítulo.

## **Parte I – Conceitos básicos de segurança**

### **Capítulo 1 – Introdução**

### **Capítulo 2 – O ambiente cooperativo**

Este capítulo mostra a dependência cada vez maior da informática e das telecomunicações para o sucesso das organizações, o que faz com que um novo ambiente de extrema importância surja no âmbito computacional: o ambiente cooperativo. Como consequência, diversos novos problemas passam a ocorrer nesse ambiente, principalmente com relação à segurança dos seus recursos. As triangulações, nas quais uma organização A acessa as informações de C, por intermédio de sua comunicação com a organização B, é apenas um desses problemas que devem ser tratados. A complexidade de conexões e a heterogeneidade do ambiente também devem ser consideradas.

### **Capítulo 3 – A necessidade de segurança**

Neste capítulo, cujo enfoque é a natureza da segurança, discutem-se questões sobre investimentos em segurança e os seus mitos. Faz-se também uma análise sobre a influência das medidas de segurança nas funcionalidades dos sistemas e na produtividade dos usuários. A segurança é necessária, porém sua estratégia de implementação deve ser bem definida, medindo-se custos e benefícios, pois a segurança total não é possível. A análise dos riscos possui um papel fundamental nesse contexto.

### **Capítulo 4 – Os riscos que rondam as organizações**

Este capítulo apresenta os riscos a que as organizações estão sujeitas. Os possíveis atacantes e os métodos, técnicas e ferramentas utilizados por eles são apresentados, mostrando que as preocupações com a segurança devem ser tratadas com a máxima atenção e cuidado, para que a continuidade dos negócios das organizações não seja

afetada. É contra esses riscos que as organizações têm de lutar, principalmente através das técnicas, tecnologias e conceitos a serem discutidos na Parte II deste livro. Os riscos envolvem aspectos humanos, explorados pela engenharia social, e aspectos técnicos. Detalhes de alguns dos ataques mais conhecidos podem ser encontrados neste capítulo, incluindo análises de ferramentas de DDoS e de *worms* como o Nimda, o Code Red, o Klez, o Sapphire e o Deloder. Com o objetivo de ilustrar os passos utilizados pelos atacantes, os ataques foram agrupados em categorias que incluem a obtenção de informações sobre os sistemas-alvo, passando por técnicas que incluem negação de serviço (*Denial of Service – DoS*), ataques ativos, ataques coordenados e ataques às aplicações e aos protocolos.

## Capítulo 5 – Novas funcionalidades e riscos: redes sem fio

O uso de redes sem fio (*wireless*) vem aumentando substancialmente, resultando em um impacto significativo na vida das pessoas. Seja em distâncias mais longas (telefones celulares), em distâncias médias (*Wireless LAN*, WLAN) ou em curtas distâncias (Bluetooth), as redes sem fio facilitam o dia-a-dia das pessoas; no entanto, trazem consigo novos riscos. Elas apresentam diferenças essenciais se comparadas às redes com fio, de modo que protocolos de segurança foram definidos para a proteção dos acessos sem fio, principalmente para a autenticação e proteção no nível de enlace. Este capítulo discute os aspectos de segurança existentes nas redes sem fio, em particular no padrão IEEE 802.11 e Bluetooth.

## Parte II – Técnicas e tecnologias disponíveis para defesa

### Capítulo 6 – Política de segurança

O objetivo deste capítulo é demonstrar a importância da política de segurança, discutindo pontos como seu planejamento, seus elementos, os pontos a serem tratados e os maiores obstáculos a serem vencidos, principalmente em sua implementação. Alguns pontos específicos que devem ser tratados pela política também são exemplificados, como os casos da política de senhas, do *firewall* e do acesso remoto. A discussão estende-se até a política de segurança em ambientes cooperativos, que possuem suas particularidades. Os bolsões de segurança característicos dos ambientes cooperativos são uma dessas particularidades.

### Capítulo 7 – Firewall

Este capítulo trata de um dos principais componentes de um sistema de segurança, o *firewall*, e tem como objetivo discutir a definição do termo *firewall*, que vem so-

frendo modificações com o tempo, além de discutir a evolução que vem ocorrendo nesse importante componente de segurança. Os conceitos técnicos envolvidos, fundamentais para a escolha do melhor tipo de *firewall* para cada organização, são apresentados detalhadamente. As arquiteturas de um *firewall*, que influem substancialmente no nível de segurança, também são discutidas. Por fim, conclui-se que o *firewall* não pode ser a única linha de defesa para garantir a segurança de uma organização.

## Capítulo 8 – Sistema de detecção de intrusão

O sistema de detecção de intrusão (*Intrusion Detection Systems* – IDS) constitui um componente de segurança essencial em um ambiente cooperativo. Neste capítulo serão discutidos os objetivos dos sistemas de detecção de intrusão e os tipos de sistemas que podem ser usados para a proteção do ambiente. Os tipos de IDS e as metodologias de detecção utilizadas serão discutidos, bem como as limitações de cada abordagem. Sua localização na rede da organização influi diretamente nos resultados da detecção, de forma que ela é discutida no capítulo. Os sistemas que visam não apenas a detecção, mas também a prevenção dos ataques – sistemas de prevenção de intrusão (*Intrusion Prevention System* – IPS) – também são apresentados neste capítulo.

## Capítulo 9 – A criptografia e a PKI

A criptografia é uma ciência que possui importância fundamental para a segurança, ao servir de base para diversas tecnologias e protocolos, tais como a *Secure Socket Layer* (SSL) e o *IP Security* (IPSec). Suas propriedades – sigilo, integridade, autenticação e não-repúdio – garantem o armazenamento, as comunicações e as transações seguras, essenciais no mundo atual. Este capítulo discute o papel da criptografia e os aspectos relacionados à sua segurança. A infra-estrutura de chaves públicas (*Public Key Infrastructure* – PKI), baseada na criptografia assimétrica, vem ganhando uma importância cada vez maior, principalmente nos ambientes cooperativos, e também será discutida neste capítulo.

## Capítulo 10 – Redes privadas virtuais

As redes privadas virtuais (*Virtual Private Network* – VPN) possuem grande importância para as organizações, principalmente no seu aspecto econômico, ao permitir que as conexões físicas dedicadas de longa distância sejam substituídas pelas suas correspondentes a redes públicas, normalmente de curta distância. As VPNs permitem também a substituição das estruturas de conexões remotas, que podem ser

eliminadas em função da utilização dos clientes e provedores VPN. Porém, essas vantagens requerem uma série de considerações com relação à segurança, pois as informações das organizações passam a trafegar por meio de uma rede pública. A criptografia associada a VPNs não é suficiente: este capítulo visa discutir a VPN e as implicações de segurança envolvidas, além dos principais protocolos disponíveis (L2TP, PPTP, IPSec) para a comunicação entre as organizações por intermédio de túneis virtuais.

## Capítulo 11 – Autenticação

A autenticação é essencial para a segurança dos sistemas, ao validar a identificação dos usuários, concedendo-lhes a autorização para o acesso aos recursos. A autenticação pode ser realizada com base em alguma coisa que o usuário sabe, em alguma coisa que o usuário tem ou em alguma coisa que o usuário é, como será visto neste capítulo. O capítulo mostra também os pontos importantes a serem considerados no controle de acesso, que tem como base a autenticação dos usuários, e discute as vantagens e desvantagens do *Single Sign-On* (SSO), que tenta resolver um dos maiores problemas relacionados à autenticação – o mau uso das senhas.

## Parte III – Modelo de segurança para um ambiente cooperativo

### Capítulo 12 – As configurações de um ambiente cooperativo

Este capítulo apresenta os diversos cenários que representam as redes das organizações, cuja evolução (aumento dos números de conexões) leva à formação de ambientes cooperativos. Será visto que a complexidade aumenta a cada nova conexão, o que exige uma análise profunda das implicações envolvidas e das tecnologias necessárias que serão utilizadas na arquitetura de segurança da organização. Este capítulo analisa as diversas configurações de componentes importantes para a segurança da organização, como o *firewall*, a *Virtual Private Network* (VPN), o *Intrusion Detection System* (IDS) e a *Public Key Infrastructure* (PKI), de acordo com as necessidades que vão surgindo com a evolução das conexões. As discussões deste capítulo culminam com a arquitetura do *firewall* cooperativo, que é conceituado no Capítulo 13.

## Capítulo 13 – O modelo de segurança para ambientes cooperativos

Este capítulo tem como objetivo apresentar um modelo de segurança para o ambiente cooperativo. Os aspectos envolvidos com o ambiente cooperativo são discutidos, e em seguida são demonstradas as dificuldades existentes na definição e implementação das regras de filtragem. A seguir, será apresentada uma abordagem para a manipulação da complexidade das regras de filtragem utilizando-se o *iptables*. A arquitetura do *firewall* cooperativo também é apresentada, culminando na definição de cinco níveis hierárquicos de defesa, que visam minimizar a complexidade e tornar mais simples a administração da segurança em um ambiente cooperativo. Uma discussão sobre o gerenciamento da complexidade da segurança também é realizada, com a apresentação do Modelo de Teias.

## Capítulo 14 – Conclusão