

Parte 7 - Componentes dos Sistemas de Segurança de Dados

Políticas de Segurança

Políticas de Segurança são compostas por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para uma determinada empresa recebam a proteção conveniente, de modo a garantir três itens básicos, a saber:

- Confidencialidade
- Integridade
- Disponibilidade

Uma política de segurança da informação tem como propósito, fornecer orientação e apoio às ações de gestão de segurança. Esta política deve levar em consideração três blocos principais:

- Diretrizes (Camada Estratégica)

As Diretrizes devem expressar a importância que a empresa dá para a informação, o comprometimento da mesma para com a segurança da Informação.

- Normas (Camada Tática)

As normas detalham situações, ambientes e processos específicos que detalham e fornecem orientação para o uso adequado da informação, exemplos de normas descrevem a forma de fornecimento e alteração de senhas, ou o uso da Internet por funcionários.

- Procedimentos e Instruções (Camada operacional)

Podem ser o detalhamento de cada ação associada a cada situação para o uso das informações. Um exemplo deste componente pode estar associado aos passos necessários para o uso de codificação de arquivos ou o uso de informações confidenciais.

Para a elaboração de uma política de segurança é essencial a definição do escopo da política de segurança e a identificação de contra quem a informação está sendo protegida.

O Escopo de uma política pode compreender alguns serviços, departamentos ou processos específicos do negócio da empresa. Após esta definição poderá ser considerado os elementos básicos: Hardware, Software, Dados e Documentação.

Para a identificação das ameaças poderá ser levado em consideração aspectos, tais como: Acesso não autorizados; Revelação não autorizada de Informações e Erros de Sistemas e de usuários.

O sucesso de uma política de segurança está associado à sua divulgação e cobrança de cumprimento, uma forma de divulgação pode ser através da própria Intranet da empresa, vide na fig. 1 ao lado um exemplo de divulgação.

Também a questão de determinação de responsabilidades deve estar presente através da nomeação de um representante de cada departamento. Finalmente, os processos de negócio devem prever rotinas de auditoria e o devido gerenciamento da segurança da informação.

Cartilha de Segurança para Internet 3.1

Parte III: Incidentes de Segurança e Uso Abusivo da Rede

[Anterior](#) [Início](#) [Próximo](#) [Versão para impressão](#)

Esta parte da Cartilha aborda tópicos relativos a incidentes de segurança, política de uso aceitável, registros de eventos e sistemas de alertas relativos ao processo de identificação e notificação de incidentes de segurança.

Sumário

1. Incidentes de Segurança e Abusos

- 1.1. O que é incidente de segurança?
- 1.2. O que é política de segurança?
- 1.3. O que é política de uso aceitável (AUP)?
- 1.4. O que pode ser considerado uso abusivo da rede?

2. Registros de Eventos (logs)

- 2.1. O que são logs?
- 2.2. O que é um sistema de detecção de intrusão (IDS)?
- 2.3. Que tipo de atividade pode ocasionar a geração de um log?
- 2.4. O que é um falso positivo?
- 2.5. Que tipo de informação está presente em um log?


Figura 1 - Cartilha de Segurança

A manutenção de uma política de segurança da informação requer a) Aceitação desta mesma política por parte dos usuários; b) Testes da Política e c) Revisão periódica destas políticas.

A aceitação dos usuários deve ser através de um documento elaborado de forma clara e objetiva que resume os principais pontos da política, assim como as responsabilidades e direitos dos usuários e da organização, vide modelo utilizado pela PRODERJ na figura 1 abaixo.

Por ultimo deve ficar claro que uma política de segurança é dinâmica, e assim devem sofrer mudanças periódicas de modo a garantir atualizações que ocorrem com o tempo envolvendo processos empresariais e mudanças tecnológicas.

Figura 2 - Modelo de Termo de Responsabilidade



TERMO INDIVIDUAL DE RESPONSABILIDADE

Pelo presente instrumento, eu, _____
matrícula/identidade nº _____, perante o Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ, na qualidade de usuário dos recursos de processamento da informação do PRODERJ, declaro estar ciente e concordar com a **Política de Segurança da Informação** composta por suas Diretrizes Gerais, Normas, Procedimentos e Instruções, que estão disponíveis na INTRANET, seção Política de Segurança (<http://intranet>) .

Declaro, também, estar ciente de que os acessos por mim realizados à internet, bem como o conteúdo das mensagens enviadas através do Correio Eletrônico corporativo são monitorados automaticamente.

Declaro, ainda, estar ciente das minhas responsabilidades descritas nas normas da Política de Segurança da Informação e que, a não observância desses preceitos, implicará na aplicação das sanções previstas nas Diretrizes Gerais desta Política.

Rio de Janeiro, ____ de _____ de ____.

(Assinatura)

Tipos de Ataques a sistemas computacionais

O vandalismo eletrônico é tema atualmente cada vez mais preocupante, são frequentes as notícias de invasões a banco de dados de empresas, desconfiguração de websites, roubos de senhas e desvios de recursos de clientes de bancos, bloqueios de acessos a computadores entre outras formas de ataques a sistemas informatizados. Abaixo, na figura 3, exemplo de e-mail falso utilizado por hackers para extrair dados confidenciais de usuários Internet Banking.

Sabe-se também que alguns dos problemas para a redução destes delitos ou mesmo a punição das pessoas envolvidas é a dificuldade de identificação dos autores destes atos além da fragilidade dos sistemas e dos controles organizacionais e principalmente do desconhecimento ou falta de interesse por parte dos usuários em adotarem medidas de segurança, algumas extremamente simples tais como o uso de antivírus ou outras ferramentas mais sofisticadas como a instalação de antispyswares ou sistemas de firewalls que exigem configurações especiais para atingirem o seu objetivo.

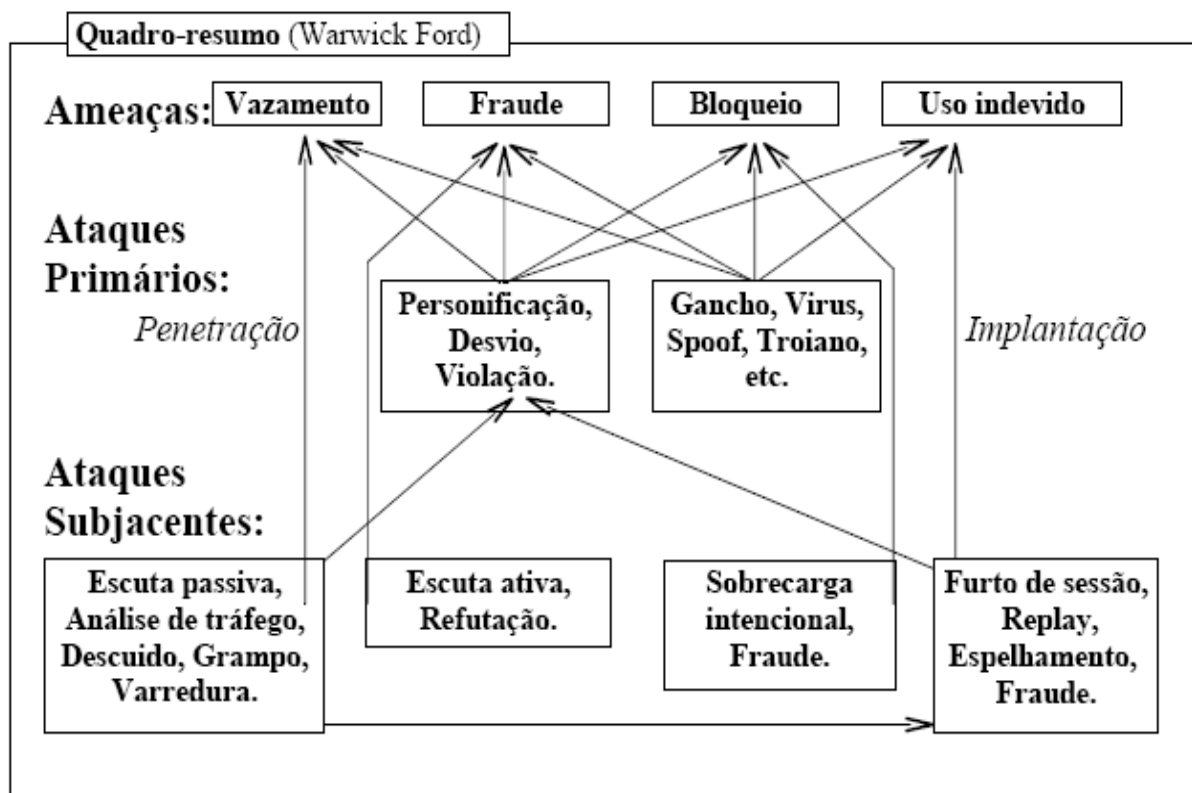
Segundo o especialista Warwick Ford ataques a sistemas informatizados podem ser classificados da seguinte forma:

- Ameaças Básicas: tais como vazamentos, fraudes, bloqueios e uso indevido de informações
- Ataques Primários por penetração: uso indevido de privilégios, exploração de falhas ou Ataques primários por implantação: infecções, cavalos de tróia, backdoor.
- Ataques Subjacentes: Escutas passivas, descuido, grampo, varredura



Fig. 3 - Email Falso

Abaixo, na figura 4, Quadro-Resumo detalhado elaborado por Warwick Ford detalhando Ameaças e Ataques



Protocolos Criptográficos

A criptografia termo originado do Grego *kryptós* "escondido", e *gráphein*, "escrita" é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário - detentor da "chave secreta" - o que a torna difícil de ser lida por alguém não autorizado.

A criptografia é utilizada por meio de chaves, que nada mais são do que funções matemáticas que embaralham ou encriptam a mensagem. Assim, só o receptor da mensagem pode ler a informação com facilidade, pode ajuda a imputar responsabilidade, prover acuracidade e privacidade, pode prevenir fraudes em comércio eletrônico e garantir a validade de transações financeiras.

Desta forma a criptografia utilizada de forma apropriada protege o anonimato e fornece provas de identidade de pessoas. Pode impedir vândalos de alterarem páginas na internet e concorrentes obterem de forma fácil o acesso a documentos confidenciais. Com o comércio eletrônico sendo transferido para as redes de computadores via internet, a criptografia torna-se cada vez mais obrigatória para a segurança dos negócios.

Os esquemas criptográficos são classificados em:

- Simétricos: quando a chave de cifragem e de decifragem é a mesma. Portanto os dois lados envolvidos na comunicação precisam ter conhecimento da chave secreta. E a transferência dessa chave deve ser feita de uma forma segura, para evitar sua interceptação. Esse esquema tem como principal vantagem a performance. Um exemplo de algoritmo usando esse esquema é o DES - Data Encryption Standard, desenvolvido na década de 70 pela IBM.

- Assimétricos: quando existe um par de chaves uma privada e outra pública, onde uma mensagem cifrada por uma das chaves só pode ser decifrada pelo seu par. Nesse caso o dono do par de chaves, por exemplo Bob, deixa sua chave pública disponível para todos e guarda seguramente sua chave privada. Quando alguém quiser enviar uma mensagem para Bob deve cifrá-la com a chave pública de Bob. E assim só Bob terá a chave privada necessária para decifrar tal mensagem. Esse esquema permite também conferir a autoria de uma mensagem. Por esta característica este esquema é também conhecido por assinatura digital. A principal vantagem do esquema assimétrico é o uso do par de chaves privada e pública que elimina a necessidade da transmissão da chave secreta. Um exemplo de algoritmo usando esse esquema é o RSA - desenvolvido por Rivest, Shamir and Adleman no início da década de 80.

- Um terceiro esquema é um sistema híbrido, onde o esquema simétrico e assimétrico são usados em conjunto. Nele a chave simétrica usada para cifrar a mensagem é cifrada com a chave pública do receptor da mensagem gerando o envelope digital. Esse esquema garante uma melhor performance, por utilizar o esquema simétrico, que é mais rápido, e um meio seguro de transmissão da chave através do esquema assimétrico.

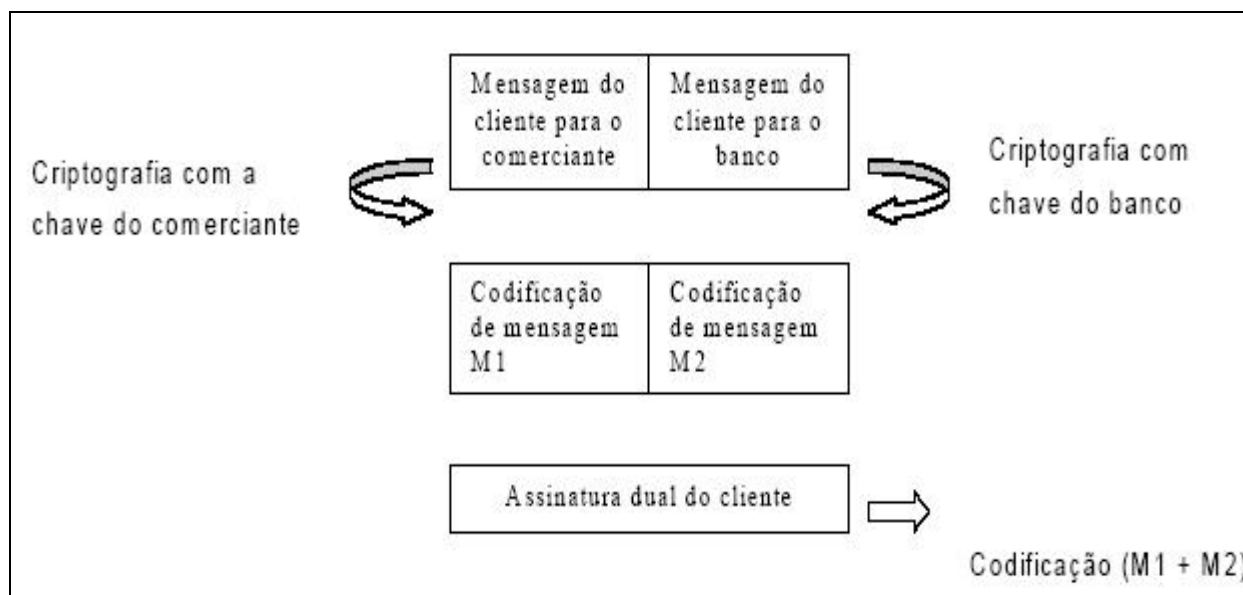
Em redes fechadas, é possível utilizar uma única chave para encriptar e desincriptar a mensagem, pois não há o risco de esta chave ser interceptada. Era a técnica de que se utilizava, a título de exemplo, o sistema bancário décadas atrás, quando da remessa de ordens de pagamento. Já numa rede aberta, como a Internet, um sistema com uma única chave não seria seguro, pois no momento em que a chave fosse transmitida para que o receptor pudesse decriptar o documento, haveria a possibilidade de esta chave ser interceptada, comprometendo a segurança dos dados.

Devido a expansão dos negócios eletrônicos empresas e pesquisadores vem desenvolvendo mecanismos para tornar seguros os processos de pagamentos via e-commerce. Muitos sistemas de pagamentos e criptografias foram criados ou estão sendo adaptados com este objetivo tais como CyberCash, Electronic Cheque, First Virtual Accounts, PGP, etc. Cada sistema apresenta vantagens, mas dificilmente conseguem atender de forma simultânea todos os requisitos necessários para garantir a segurança do processo como um todo para o comércio eletrônico.

O padrão SET, criado em 1996 por um consórcio de empresas, formado pela Visa, MasterCard, Netscape, IBM, Microsoft, GTE, SAIC, Terisa Systems e Verisign, para garantir a transmissão segura de informações pessoais e financeiras em redes públicas. Essa segurança é garantida com o uso de esquemas de criptografia durante as atividades de autorização, autenticação e identificação da compra e venda eletrônica oferecendo um alto grau de segurança para as transações eletrônicas, utilizando o esquema híbrido de criptografia, utiliza o algoritmo RSA no esquema assimétrico e o DES no simétrico. Em uma transação do SET, há informações que são particulares entre o consumidor e o comerciante (como os itens pedidos) e também entre o consumidor e o banco (como o número da conta). O SET permite que ambos os tipos de informação digital sejam incluídos numa única transação, por meio de uma estrutura criptográfica chamada assinatura dual. Uma mensagem de requisição de compra dos SET consiste em dois campos, um para o comerciante e outro para seu banco. O campo do comerciante é criptografado com a chave pública do comerciante; o do banco, com a chave pública do banco.

O padrão SET não fornece o número do cartão de crédito do consumidor, mas o banco pode, por opção, fornecer o número ao comerciante quando este envia a confirmação. Além desses blocos criptografados, a requisição de compra contém codificações de mensagem de cada um dos campos, e uma assinatura. A assinatura é obtida concatenando-se as duas codificações, fazendo a codificação das duas codificações de mensagem, e assinando a codificação de mensagem resultante. A figura 4 abaixo mostra como isto é feito. A assinatura dual permite que o comerciante e o banco validem sua assinatura em sua parte da requisição de compra, sem precisar decifrar o campo da outra parte.

Figura 4 - Requisição de Compra no Padrão SET



Por último, cabe ressaltar que o protocolo SET, assim como o HTTP, é um protocolo de comunicação para Internet, porém seu uso é exclusivo para transações comerciais.

Referências Bibliográficas

- BANCO BRADESCO. Bradesco Segurança. Disponível em <www.bradescoseguranca.com.br> Acesso 15 fev. 2009
- CARVALHO, Luciano Gonçalves de. Segurança de Redes. São Paulo: Ed. Ciência Moderna, 2005
- CERT.BR Cartilha de Segurança para Internet. Disponível em <<http://cartilha.cert.br/>> Acesso em 21 fev. 2009
- PRODERJ. Diretrizes Gerais de Segurança da Informação. Disponível em <www.proderj.rj.gov.br/politica_seguranca.asp>. Acesso em 20 fev. 2009
- SILVA, Francisco José. Segurança na Web, Ensaios e Ciência, vol. 4, nr. 001, Abril 2000
- TORRES, Maria Flávia Cunha de Figueiredo. Tecnologias da Infra-estrutura de Informação em Ambientes Colaborativos de Ensino Comércio Eletrônico, disponível em <<http://www.dca.fee.unicamp.br>>