Sec-SLA: especificação e validação de métricas para acordos de níveis de serviço orientados à segurança

Rafael R. Righi, Felipe R. Pellissari, Carlos B. Westphall

[1]Programa de Pós-Graduação em Ciência da Computação – PPGCC
Laboratório de Redes e Gerência (LRG) – Universidade Federal de Santa Catarina
Caixa Postal 476 – 88040-900 Florianópolis, SC

{rrighi,rolim,westphal}@lrg.ufsc.br

Abstract. *The adoption of service level agreements (SLAs) between companies and users has had a fast increase in the area of telecommunications. The reason for that increase is mainly due to the popularization of Internet and wide use of e-commerce in many enterprises. The majority of service level agreements, so far, have been predominantly concerned with telecommunications and other related aspects of service performance. Consequently, little consideration with the security exists in these contracts. This paper contributes for feeling this gap, in aspects of specification and validation of corresponding metrics, that can be used as inputs in the elaboration of security service level agreements (Sec-SLAs), internally or among organizations.*

Resumo. *A implantação de acordos de níveis de serviço entre fornecedores e usuários tem crescido muito rápido na área de telecomunicações; isto devido principalmente à popularização das redes de computadores e dos negócios na internet. Grande parte destes contratos levam em conta somente o desempenho e características físicas dos serviços e deixam em segundo plano aspectos referentes a uma área que exige igual consideração nas organizações: a segurança computacional. Este artigo contribui para a escrita de acordos de níveis de serviço voltados à segurança (Sec-SLA) através da definição e validação de métricas para serem usadas nesses contratos e agrega valor à literatura científica da área, já que expande os conceitos existentes de Sec-SLA.*

1. Introdução

A segurança e a gerência de redes de computadores são áreas interdependentes por natureza, onde os serviços de uma área necessitam dos serviços da outra [Philip C. Hyland e Ravi Sandhu, 1998]. O desenvolvimento de acordos de níveis de serviço orientados à segurança exploram esta relação e aproximam estas duas áreas da computação, principalmente através da definição de métricas e técnicas eficientes de monitoração e controle de ativos digitais.

O aumento constante de redes de computadores é acompanhado na mesma proporção pelas preocupações com a segurança dos serviços disponibilizados aos usuários. Estas preocupações, na maioria das vezes, estão relacionadas com problemas de

vírus, incidentes de intrusão, utilização inadequada das técnicas de criptografia, adoção de controles de acesso ineficientes, entre outros.

Devido às preocupações com segurança, ao aumento da utilização da infraestrutura da internet como pilar para transações comerciais entre organizações e à importância das informações que trafegam entre as redes [Alexander Keller e Heiko Ludwig, 2003], faz-se necessária a elaboração de acordos de níveis de serviço entre as partes envolvidas que englobe, além dos tópicos usuais, conceitos de segurança computacional. Nesse contexto, o presente artigo busca concentrar esforços para encontrar métricas e parâmetros significativos para serem usados nos contratos Sec-SLA[1] e, desta forma, auxiliar os gerentes de segurança e profissionais da área que buscam aperfeiçoar a política de segurança de suas organizações.

O Sec-SLA distancia-se dos acordos de níveis de serviço convencionais quanto ao seu objetivo. O SLA habitual, chamado neste trabalho de SLA de telecomunicação, ressalta métricas como disponibilidade, vazão, largura de banda da rede e faz pouco, ou não faz, referência à segurança. No entanto, muitos princípios encontrados no Sec-SLA, como a determinação dos direitos e deveres do fornecedor e consumidor dos serviços, seguem àqueles encontrados em contratos convencionais.

Este artigo está dividido em 7 seções. A seção 2 é responsável por exibir os principais trabalhos relacionados com o tema tratado neste artigo científico. Na seção 3 são apresentados alguns aspectos teóricos sobre SLA e segurança de computadores, os quais objetivam transmitir idéias necessárias à compreensão deste documento. As seções 4 e 5, respectivamente, exibem as particularidades do Sec-SLA e as contribuições para a especificação de métricas oferecidas por este artigo. A seção 6, por sua vez, expõe os benefícios e desafios associados aos contratos que envolvem a segurança da informação. O artigo encerra na seção 7 com a conclusão, a qual reúne as principais idéias da pesquisa, além de citar os possíveis complementos sobre ela a cargo de trabalhos futuros.

2. Trabalhos Relacionados

Embora exista uma vasta literatura que investiga a integração entre gerência de redes e segurança, a elaboração de acordos de níveis de serviço voltados à segurança e a definição de métricas para serem usadas nesses contratos são áreas novas e em expansão. Entre os pioneiros nessa área está o trabalho desenvolvido por [Ronda R. Henning, 2000], o qual relaciona os conceitos de SLA e segurança em ambientes empresariais colocando ênfase no processo de implantação do acordo e nos custos envolvidos nessa operação.

O presente artigo expande as pesquisas realizadas por [Ronda R. Henning, 2000] e especifica, através de uma metodologia (ver seção 5), métricas de segurança eficazes para serem utilizadas em contratos do tipo Sec-SLA. Com relação à classificação da relevância das métricas de segurança, etapa importante para reconhecer quais métricas merecem maior destaque no acordo, este trabalho buscou apoio nos estudos efetuados por [Michael E. Whitman, 2003], os quais associam as principais ameaças às redes de computadores com os mecanismos de proteção conhecidos.

A monitoração das métricas, embora fundamentais em todo processo de gerência,

[1] *Security-Service Level Agreements*

não são o ponto preponderante dessa pesquisa. No entanto, algumas das métricas de segurança apresentadas para o Sec-SLA (essencialmente aquelas relacionadas com os vírus e SPAMs) foram monitoradas; tarefa que auxiliou na atribuição dos níveis de serviço a cada métrica do contrato. Nessa etapa do trabalho as idéias contidas nos artigos escritos por [Guilherme Rhoden e Edison Lopes Melo e Carlos Westphall, 2002] e [Luciano P. Gaspary e Leonardo L. Fagundes, 2003] foram fundamentais, pois orientaram como utilizar os protocolos de gerência na análise de problemas de segurança.

Por final, observa-se que o Sec-SLA pode ser discutido como um contrato derivado dos SLAs convencionais. Os trabalhos que abordam os acordos de níveis de serviço para área de telecomunicações ([SLA Management Team, 2001] e outros) contribuíram para que a pesquisa contenha, além da descrição e validação de métricas de segurança, aspectos como benefícios e desafios vinculados aos acordos Sec-SLA.

3. Aspectos Teóricos

O Sec-SLA está associado à área de segurança computacional e aos acordos de níveis de serviço. Visto isso, percebe-se a necessidade de haver, antes da sua definição e da especificação das métricas, uma contextualização sobre as idéias fundamentais que circundam estes dois ítens relacionados ao Sec-SLA. Não é, no entanto, pretensão deste documento englobar toda a problemática que envolve as questões de segurança, mas como mencionado anteriormente, o objetivo é construir a base para o entendimento dos aspectos que compõem o Sec-SLA.

3.1. Acordos de Níveis de Serviço

O SLA é descrito como uma declaração de expectativas e obrigações que existem no relacionamento de negócio entre duas organizações: o provedor do serviço e seu consumidor [SLA Management Team, 2001, Avrahan Left e James Rayfield, 2003]. Esta declaração, muitas vezes chamada de contrato, especifica os níveis de qualidade de serviço[2] que o fornecedor se compromete em disponibilizar, além de cláusulas legais, como as conseqüências para cada parte se houver descumprimento de deveres.

O consumidor do serviço utiliza o SLA para verificar se ele está atualmente recebendo o serviço dentro dos níveis acertados no contrato [A. Keller e G. Kar e H. Ludwig e A. Dan, 2002]. No entanto, para isso acontecer é necessário que ele possua ferramentas para realizar as medições e que os níveis do serviço escritos no contrato estejam claros. Geralmente, as aplicações para monitoração e controle do SLA fazem uso de protocolos de gerência de redes, como o SNMP [Philip C. Hyland e Ravi Sandhu, 1998], e disponibilizam gráficos e relatórios de métricas. Assim, o consumidor percebe o comportamento do serviço contratado.

Segundo [Nathan J. Muller, 1999], existe um número mínimo de componentes que devem fazer parte do SLA (ver Tabela 1). Entre os integrantes destacam-se a especificação dos serviços oferecidos e os níveis de qualidade para cada um deles, respectivamente os ítens “serviços” e “parâmetros” da Tabela 1. O contrato deverá selecionar um nível de serviço que contemple os anseios dos usuários e as possibilidades do fornecedor.

[2]QoS - *Quality of service* [Jean Pierre Courtiat, 2001, Amitava Dutta-Roy, 2000].

Item	Descrição
Descrição do ambiente	Contém informações que descrevem por que existe a necessidade de criação do SLA e quais vantagens ele irá trazer
Partes	Identifica quais as partes que realizam o acordo
Serviços	Responsável por exibir as peculiaridades do serviço
Parâmetros	Especifica em quais níveis os usuários ou clientes podem esperar a prestação do serviço
Disponibilidade	Apresenta a porcentagem mínima de tempo que o serviço acordado deve manter-se operacional
Limitações	Coloca as possíveis limitações do serviço em momentos críticos que independem de quem o oferece
Compensações	Caso o acordo proferido for quebrado, este item menciona as conseqüências para cada parte
Medições	Como o serviço disponibilizado é monitorado e avaliado

Tabela 1: Principais componentes de um SLA [Nathan J. Muller, 1999]

Um SLA não é um acordo estático; ele possui um ciclo de vida e três fases distintas [Dinesh Verma, 1999]. A primeira chama-se "fase de criação" e envolve a elaboração do contrato e suas características. A segunda fase denomina-se "fase de operação" e é aquela onde o SLA entra em funcionamento e o cliente pode sugerir reparos no contrato. Quando a assinatura de determinado serviço chega ao fim e possivelmente vários ciclos de vida já se passaram, chega a "fase de remoção". Nela todas as informações de configuração relacionadas ao serviço são removidas; neste momento o SLA deixa de existir.

Figura 1: Exemplo de SLA entre duas organizações

Grande parte dos acordos de níveis de serviço são efetivados entre companhias diferentes, onde uma delas presta serviço à outra [Andre Van Der Walt, 2003]. A Figura 1 apresenta esse modelo e mostra duas filiais de uma mesma organização que se interligam através do uso de serviços de uma segunda organização. Embora este esquema seja o mais encontrado, contratos de SLA implementados dentro de uma mesma companhia ou organização também possuem significado e relevância, principalmente no âmbito deste artigo. O SLA construído dentro da própria companhia é comumente escrito pelo departamento de IT[3] (1^a parte) para os membros da organização (2^a parte) e descreve as obrigações deste departamento para com a organização, como os usuários irão acessar os recursos da companhia e quais os níveis de qualidade que estes podem esperar dos serviços [Nathan J. Muller, 1999].

3.2. Segurança Computacional

A segurança de sistemas (computadores e informações) está entre as áreas da computação com maior proeminência, devido especialmente à importância dela no cotidiano das pes-

[3] *Information Tecnology*

soas e negócios empresariais [William Stallings, 2003]. A segurança se importa com a proteção dos ativos digitais armazenados em computadores e redes de processamento de dados [H. Venter e J. Eloff, 2003].

Pode-se afirmar que um computador é seguro se ele está livre de vulnerabilidades e preocupações a respeito de ameaças. A segurança computacional, neste sentido, é a disciplina que nos ajuda a ficar despreocupados com os computadores, sendo assim possível reconhecer a palavra "seguro" como um atributo de um sistema ou objeto [Carl E. Landwehr, 2001].

Para indicar um sistema como sendo seguro, ele deve manter três propriedades básicas: confidencialidade, integridade e disponibilidade [Carl E. Landwehr, 2001]. A confidencialidade é a propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização. Analogamente, a integridade pode ser descrita como a condição na qual recursos são protegidos contra modificações sem prévia autorização. Por fim, a disponibilidade é responsável por garantir que a informação estará acessível para usuários legítimos quando estes requiserem.

Para assegurar que os sistemas implantem as propriedades citadas anteriormente e sejam ditos seguros, existe a necessidade de adoção de mecanismos de segurança. Os mecanismos de segurança são os responsáveis efetivos pela garantia das propriedades e política de segurança. A Tabela 2, conforme escrito por [Gunther Pernul, 1995], agrega os mais notáveis mecanismos de proteção.

Mecanismo	**Definição**
Criptografia	Transforma dados em algo ininteligível para o inimigo, isto é, esconde o seu conteúdo semântico.
Autenticação	Verifica se uma entidade é quem afirma ser
Autorização	Processo de determinar que tipo de atividades são permitidas
Auditoria	Exame dos registros e das atividades do sistema para avaliar sobre sua confiabilidade

Tabela 2: Principais mecanismos de segurança

A política de segurança relaciona as propriedades e mecanismos de segurança a um domínio, além de definir o escopo e as características de cada serviço que se pretende proteger [Joaquim Quinteiro Uchoa, 2001]. Ela determina regras que, quando seguidas corretamente, diminuem os riscos de incidentes de segurança à organização. Não existe como garantir a totalidade da segurança de um sistema; o que se busca é alcançar patamares admissíveis para o problema. Conforme [Carl E. Landwehr, 2001], uma organização sem uma política de segurança pode ser comparada com uma sociedade sem leis.

4. Sec-SLA: SLA para Segurança

O Sec-SLA exibe os cuidados ou deveres relacionados à segurança que o fornecedor do serviço deve tomar. Por exemplo, a Figura 1 mostra uma organização que utiliza os serviços de telecomunicações para conectar suas duas regiões de abrangência. Neste SLA os principais aspectos são a disponibilidade do canal de comunicação, a vazão média que

será entregue, a taxa de erros máxima e a identificação de possíveis picos de congestionamento. A diferença deste modelo para o Sec-SLA é percebida nos enfoques; o Sec-SLA, para este mesmo ambiente, estaria preocupado com métricas relacionadas à criptografia ou não do canal de comunicação, o suporte à integridade da informação que trafega na rede pública, registros de transporte de mensagens no canal, entre outras.

O acordo de níveis de serviço para área de segurança não anula a necessidade de criação de um SLA de telecomunicações e semelhantes. Recomenda-se a utilização de contratos separados quando as métricas abrangerem mais de um setor específico, pois esta atitude gera maior organização e facilidades para a administração dos SLA's. Além disso, como os alvos dos contratos são diferentes, é inviável unir mais de um tópico em um único contrato.

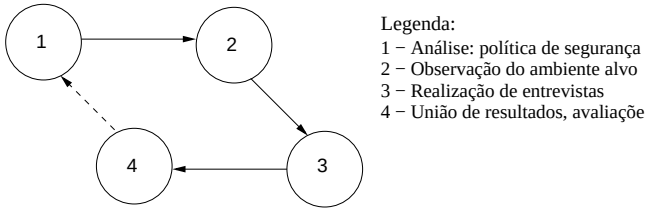

Figura 2: Etapas para elaboração de um Sec-SLA

O Sec-SLA pode ser inserido dentro do contexto de uma única empresa[4] ou entre organizações. Em ambas circunstâncias, [Ronda R. Henning, 2000] recomenda quatro passos a serem seguidos no desenvolvimento de um Sec-SLA: análise da política de segurança, observação da infraestrutura alvo do contrato, entrevistas com todos os envolvidos no acordo, união dos resultados e avaliação do processo (ver Figura 2). A análise da política de segurança é importante para delimitar as métricas de segurança vigentes para o SLA. A verificação do ambiente onde será implantado o contrato objetiva encontrar quais mecanismos de segurança precisarão ser instalados. Já a apreciação dos resultados visa compreender se o SLA está apto para tornar-se operacional.

O acordo de níveis de serviço para segurança não substitui os mecanismos de segurança. Sua utilização deve ser comparada com a aquisição de um seguro, pois ele define os níveis relativos de conforto que a organização tem em relação à proteção da informação.

5. Métricas de Segurança para o Sec-SLA

Definir as métricas de segurança que comporão o Sec-SLA é a principal atividade executada no processo de elaboração do contrato. Esta tarefa não é simples, visto que organizações diferentes possuem necessidades diferentes quanto à segurança computacional.

Nesse sentido, este artigo busca contribuir para a expansão dos acordos de níveis de serviço para segurança através da definição e validação de métricas para nortear a construção do contrato. As métricas encontradas se enquadram melhor em um cenário de

[4]Também chamado de *intracompany* [Nathan J. Muller, 1999].

SLA dentro da própria organização, onde os usuários e o departamento de tecnologia da informação são as partes envolvidas.

Antes de exibir as métricas para o Sec-SLA é indispensável apresentar a metodologia como elas foram alcançadas. As métricas especificadas advém de pesquisas feitas na rede de computadores do departamento de Informática e Estatística da Universidade Federal de Santa Catarina (INE-UFSC) no esforço de produzir um acordo de níveis de serviço relacionado a segurança entre a administração/gerência da rede e seus usuários (alunos da graduação, pós-graduação e professores). Foram realizados os passos propostos por [Ronda R. Henning, 2000] demonstrados na Figura 2 e as entrevistas com os usuários - aproximadamente 1500 - aconteceram sob a forma de questionário[5]. Aliado às informações recolhidas junto aos usuários, foram definidos parâmetros iniciais para as métricas alcançadas.

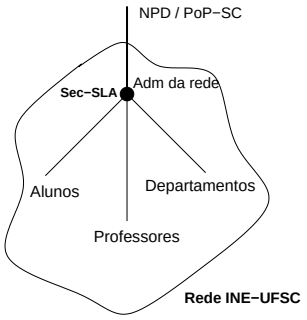

Figura 3: Ambiente de rede onde a metodologia de pesquisa foi aplicada

As métricas de segurança que receberam maior distinção pelos usuários foram o número de vírus não detectados e de mensagens indesejadas recebidas (observe a Figura 4). Essas informações foram confirmadas pelos responsáveis pela rede em estudo e vêm ao encontro dos relatórios publicados por [SANS Institute, 2003], os quais indicam uma tendência de retomada de proliferação de vírus e vermes pela internet, principalmente a partir de 2001.

A Tabela 3 exibe as métricas para o Sec-SLA, juntamente com uma breve descrição de cada uma delas. Ambientes diferentes nem sempre exigem as mesmas métricas e parâmetros. Uma determinada organização poder considerar um bom parâmetro para a métrica número de vírus não detectados o valor “dois vírus por ano”, enquanto que para outras este valor pode ser inadmissível. Constata-se então, que o Sec-SLA exige um estudo particular do ambiente onde o mesmo será posto em prática.

A Tabela 4 apresenta alguns parâmetros para as métricas definidas, especificamente para o ambiente de rede em estudo (ver Figura 3). Nessa tabela as colunas indicam os níveis de serviço e as linhas referenciam cada uma das métricas. Os parâmetros, muitas vezes chamados de SLS[6] [Janusz Gozdecki e Andrezej Jajszczyk, 2003], relacionam os níveis e as métricas e indicam as qualidades esperadas para cada nível do contrato.

Com o objetivo de verificar se os parâmetros iniciais propostos realmente se enquadram no acordo Sec-SLA foram realizadas medições das métricas mais relevantes de

[5] As informações relacionadas ao questionário utilizado na especificação das métricas e ao processo de monitoração estão dispostas em `http://www.lrg.ufsc.br/~rrighi/sec-sla.html`.

[6] *Service Level Specification.*

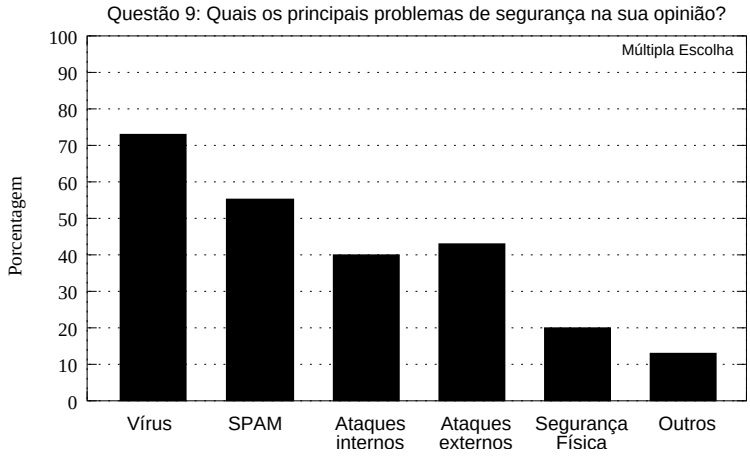

Figura 4: Gráfico das respostas à questão 9 do questionário

acordo com os usuários - número de vírus e de mensagens indesejadas. Com relação ao número de vírus, levando em conta a preocupação dos usuários, foi tomado como parâmetro inicial o valor "0 vírus por ano". Como em um período de 5 meses não foram registrados notificações de recebimento de vírus pelo correio eletrônico, pode-se concluir que o parâmetro inicial tem fundamento.

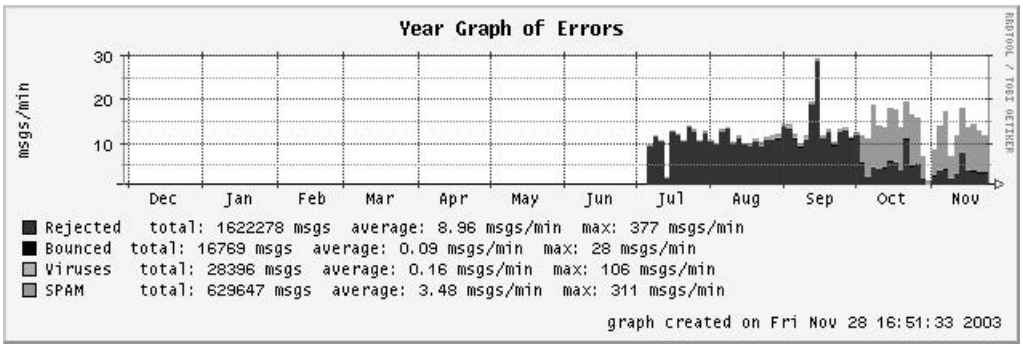

Figura 5: Medição de erros no correio eletrônico da rede INE-UFSC

Com relação a SPAM, o parâmetro inicial precisou ser modificado visto que o número de mensagens indesejadas recebidas por cada usuário foi superior ao valor "5 mensagens por mês". No questionário, o qual foi aplicado antes da implantação do programa anti-spam[7], os usuários apontaram o recebimento de aproximadamente 108 SPAM's por mês e, como mostra a Figura 5, a média de SPAM's detectados é de 100 mensagens por mês (total de mensagens por mês dividido pelo número de usuários). Portanto, a métrica número de mensagens indesejadas da Tabela 4 foi alterada para o valor "10 mensagens por mês". Os parâmetros para as demais métricas especificadas foram definidos através de interações com os administradores da rede e observação das necessidades do ambiente em estudo.

O processo de validação das métricas busca verificar se elas são adequadas e legítimas para o uso em um Sec-SLA no ambiente de rede alvo do artigo. O questionário preenchido pelos usuários da rede de computadores é um dos responsáveis pela

[7]O programa anti-spam chama-se SpamAssassin e entrou em operação no mês de julho de 2003.

ID	Métrica	Descrição
1	Número de vírus não detectados	Identifica o número de programas maliciosos que o usuário pode receber em determinado período. Relacionado com a integridade das informações.
2	Número de mensagens indesejadas recebidas (SPAM)	Define quantas mensagens indesejadas o usuário pode receber em seu correio eletrônico
3	Treinamento de usuários	Informa a periodicidade com que os usuários participarão de treinamentos e palestras
4	Controle físico	Técnica utilizada para garantir a integridade física dos equipamentos e ativos digitais
5	Política de backup	Mostra a freqüência dos backups, o meio de armazenamento e o tempo que eles são guardados
6	Registro de eventos	Define qual a política adotada para arquivar os logs gerados pelos sistemas da organização
7	Número de invasões	Calcula o número de invasões ao sistema vindas de dentro ou de fora da organização
8	Gerência de senha	Apresenta a freqüência com que os usuários devem modificar sua senha e a quantidade de letras e números que ela deve conter
9	Tempo de reparo	Informa o tempo que o departamento de IT leva para deixar o sistema operacional em caso de pane
10	Plano de contingência	Exibe o plano que será executado em caso de uma atividade anormal inesperada acontecer no sistema

Tabela 3: Métricas para utilização no Sec-SLA

tarefa de validação, pois as métricas que ele aponta refletem a pretensão dos entrevistados quanto aos serviços de segurança. Outra técnica usada para perceber a importância de uma métrica foi verificar quais as maiores reivindicações e queixas dos usuários junto aos administradores da rede INE-UFSC. Aliado a essas técnicas, as informações disponibilizadas por [Michael E. Whitman, 2003] foram fundamentais no momento da validação (veja a seção 2). Assim, pode-se observar se as preocupações com a segurança retratam as métricas atingidas.

O monitoramento do contrato, como apresentado na seção 3.1, é muito importante para usuários e provedores dos serviços. No Sec-SLA, observa-se que o monitoramento das métricas e parâmetros é complexo, pois o paradigma agente-gerente, normalmente usado na verificação de outros tipos de SLA, não enquadra-se facilmente a todas questões de segurança. Entretanto, trabalhos científicos como [Luciano P. Gaspary e Leonardo L. Fagundes, 2003] têm utilizado agentes RMON avançados com sucesso na monitoração de intrusos e ataques de segurança.

6. Benefícios e Dificuldades do Sec-SLA

A maior vantagem derivada da implantação do Sec-SLA é a cultura de cuidados com segurança que a organização adquire. O processo de criação desse acordo necessita a

ID	Métrica	Nível 0 (máx)	Nível 1	Nível 2 (mín)
1	Número de vírus	0 vírus/ano	2 vírus/ano	5 vírus/ano
2	Número de mensagens indesejadas (SPAM)	10 msg/mês	50 msg/mês	100 msg/mês
3	Treinamento	2 vezes/ano	1 vez/ano	nenhum
4	Controle físico	uso de sala cofre mais o guarda 24h	guarda 24h	mínimo
5	Política de backup	1 vez/semana	1 vez/mês	1 vez/semestre
6	Registro de eventos	log distribuído e protegido	sem gerência de logs	sem gerência de logs
7	Número de invasões	inadmissível	1 invasão/ano	2 invasões/ano
8	Gerência de senha	troca todos os meses - c/ números e letras	sem trocas	sem trocas
9	Tempo de reparo	máx. 1h	máx. 2h	máx. 4h
10	Plano de contingência	existente e testado	existente	não existente

Tabela 4: Exemplo de parâmetros e níveis para o Sec-SLA

definição de uma política de segurança e o engajamento de administradores e usuários dos serviços da rede no combate às questões de segurança. Este comprometimento é importante, pois para uma política de segurança tornar-se eficiente é preciso, além de um documento escrito, costumes e hábitos condizentes com a causa por parte de todos os envolvidos.

A utilização plena do Sec-SLA assegura aos usuários que os responsáveis pelos serviços de rede estarão atentos às vulnerabilidades de segurança e às regras do contrato, já que uma falha de segurança resultará em uma compensação aos usuários prejudicados. Da mesma forma, os gerentes e administradores terão a garantia de uso pelos usuários de senhas fortes e permissões corretas em seus documentos, pois estes também terão obrigações a cumprir. Essas relações somente são possíveis nos contratos porque os termos e cláusulas são escritos totalmente de maneira formal [Jacques Bouman e Jos Trienekens, 1999].

Entre as dificuldades existentes na elaboração do Sec-SLA estão a qualificação dos parâmetros de segurança para as métricas do contrato e o custo do processo. Os serviços de segurança historicamente não têm sido quantificados em termos concretos [Ronda R. Henning, 2000], o que complica a construção de parâmetros qualificados. Soma-se a isso, as diferentes concepções de segurança presentes na literatura e meios de comunicação. Com relação ao custo, para passar por todas as etapas de criação do acordo, treinar usuários e gerenciar o ciclo de vida do Sec-SLA, é requerido gastos excessivos. As organizações de pequeno porte devem planejar com cuidado as despesas referentes ao Sec-SLA para não perceberem tardiamente que a relação custo$\times$benefício não alcançou os índices almejados.

7. Conclusão

Este artigo especifica métricas que colaboram qualitativamente para escrita de acordos de níveis de serviço relacionados à segurança entre diferentes companhias ou departa-

mentos de uma mesma organização. Aliado às métricas, agrega-se mais informações aos conceitos de Sec-SLA, proporcionando enriquecimento da literatura da área.

Reforça-se, como em seções passadas, que o Sec-SLA pode coexistir com outros tipos de acordos normalmente. Sugere-se que não haja mistura de métricas de diferentes áreas em um mesmo contrato; SLA's específicos possuem maior clareza de objetivo e probabilidade de serem bem sucedidos.

Com relação ao questionário distribuído entre os usuários da rede INE-UFSC, o qual foi vital na elaboração das métricas para o Sec-SLA, detectou-se que as maiores preocupações dos usuários são o recebimento de vírus e mensagens indesejadas pelo correio eletrônico pessoal. Diante disso, recomenda-se que futuros contratos Sec-SLA, sabendo destas informações, concentrem esforços especiais nestas duas importantes métricas.

O encontro de parâmetros para as métricas especificadas, uma das preocupações do trabalho, possibilitou a definição de um Sec-SLA para a rede em estudo. As medições, realizadas principalmente sob as métricas destacadas pelos usuários, e a interação com os administradores da rede INE-UFSC foram os principais elementos nesse processo.

O artigo apresentou a utilização do Sec-SLA principalmente em ambientes internos às organizações, onde uma das partes do contrato eram os usuários e a outra a gerência e administração da rede de computadores. O uso do Sec-SLA não se restringe a este cenário. Observa-se como tendência futura a adoção desses tipos de contratos entre empresas que tercerizam os serviços de segurança, por exemplo, entre uma organização que utiliza um *firewall* ou um programa anti-vírus de outra. Neste contexto, o emprego de acordos formais são críticos e um Sec-SLA é fundamental.

Com relação a trabalhos futuros, vê-se a necessidade de aperfeiçoamento na monitoração de métricas e qualidades de serviço relacionadas com a segurança computacional. Apesar de existirem alguns trabalhos na área (ver seção 5), pesquisas que integram as métricas em um mesmo ambiente de monitoração são boas propostas para trabalhos futuros.

Referências

A. Keller e G. Kar e H. Ludwig e A. Dan (2002). Managing Dynamic Services: A Contract Based Approach to a Conceptual Architecture. *In: Proceedings of Network Operations and Management*, pages 513–528. Florence, Italy.

Alexander Keller e Heiko Ludwig (2003). The WSLA Framework: Specifying and Monitoring Service Level Agreements for Web Services. *Journal of Network and Systems Management*, 11(1):57–81.

Amitava Dutta-Roy (2000). The Cost of Quality in Internet Style Networks. *IEEE Spectrum*, 37(9):57–62.

Andre Van Der Walt (2003). Managed Security Services - who needs it ? *Computer Fraud and Security*, 2003(8):15–17.

Avrahan Left e James Rayfield (2003). Service Level Agreements and Commercial Grids. *IEEE Internet Computing*, 7(4):44–50.

Carl E. Landwehr (2001). Computer security. *International Journal of Information Security*, 1(1):3–13.

Dinesh Verma (1999). *Supporting Service Level Agreements on IP Networks*. New Riders, Indianapolis, US. ISBN: 1-57870-146-5.

Guilherme Rhoden e Edison Lopes Melo e Carlos Westphall (2002). Detecção de intrusões em backbones de redes de computadores através da análise de comportamento com SNMP. *In: 20 Simpósio Brasileiro de Redes de Computadores. Workshop em Segurança de Sistemas Computacionais.*, pages 9–16. Búzios, Brasil.

Gunther Pernul (1995). Information Systems Security: Scope, State-of-the-art, and Evaluation of Techniques. *International Journal of Information Management*, 15(3):239–255.

H. Venter e J. Eloff (2003). A taxonomy for information security technologies. *Computers & Security*, 22(4):299–307.

Jacques Bouman e Jos Trienekens (1999). Specification of Service Level Agreements, Clarifying Concepts on the Basis of Practical Research. *In: Proceedings of Software Technology and Engineering Practice - STEP*, pages 169–178.

Janusz Gozdecki e Andrezej Jajszczyk (2003). Quality of Service Terminology in IP Networks. *Communications Magazine IEEE*, 41(3):153–159.

Jean Pierre Courtiat (2001). Qualidade de Serviço no Mundo IP. Minicurso - Simpósio Brasileiro de Redes de Computadores (SBRC). Florianópolis, Brasil.

Joaquim Quinteiro Uchoa (2001). Políticas de Segurança e Políticas de Uso. Simpósio de Segurança em Informática (SSI). São José dos Campos, Brasil.

Luciano P. Gaspary e Leonardo L. Fagundes (2003). Avanços Rumo à Integração de Tecnologias de Gerenciamento de Redes e Segurança. Minicurso da Escola Regional de Redes de Computadores - ERRC. PUCRS, Porto Alegre, Brasil.

Michael E. Whitman (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, 46(8):91–95.

Nathan J. Muller (1999). Managing Service Level Agreements. *International Journal of Network Management*, 9(3):155–166.

Philip C. Hyland e Ravi Sandhu (1998). Management of Network Security Applications. *In: Proceedings of 21st NIST-NCSC National Information Systems Security Conferense*, pages 154–168. Virginia, US.

Ronda R. Henning (2000). Security Service Level Agreements: Quantifiable Security for the Enterprise? *In: Proceedings of the workshop on New security paradigms*, pages 54–60. ISBN:1-58113-149-6.

SANS Institute (2003). The Twenty Most Critical Internet Security Vulnerabilities. Acesso via internet. Disponível em: http://www.sans.org/top20/.

SLA Management Team (2001). SLA Management Handbook. *TeleManagement Forum*. Public Evaluation, Version 1.5 GB 917.

William Stallings (2003). *Crytography and Network Security*, page 44. Prentice Hall, New Jersey, United States, 3th edition. ISBN: 0-13-091429-0.