Um estudo empírico sobre o uso de métricas de segurança em ambientes reais

Rodrigo S. Miani[1], **Bruno B. Zarpelão**[2], **Leonardo S. Mendes**[3]

[1] Faculdade de Computação – Universidade Federal de Uberlândia (UFU)
Uberlândia – MG – Brazil

[2]Departamento de Computação – Universidade Estadual de Londrina (UEL)
Londrina – PR – Brazil

[3]Faculdade de Engenharia Elétrica e Computação
Universidade Estadual de Campinas (UNICAMP) Campinas – SP – Brazil

miani@facom.ufu.br, brunozarpelao@uel.br, lmendes@decom.fee.unicamp.br

Abstract. *Our work is an initial step towards understanding how theoretical security metrics are used in practice and which security issues require more attention from security practitioners. The results of the proposed survey reveals important patterns about the use of metrics in practice and highlights the value of analyzing security metrics from the point of view of characteristics such as complexity and importance.*

Resumo. *A pesquisa proposta nesse trabalho é um passo inicial para compreender como as diferentes métricas de segurança propostas na literatura são aplicadas no cotidiano das empresas e qual é a visão desses profissionais sobre os problemas que exigem maiores cuidados. Os resultados encontrados revelam alguns padrões importantes sobre o uso de métricas na prática e destaca o valor da análise de métricas de segurança sob o ponto de vista de características como complexidade e importância.*

1. Introdução

Os desafios enfrentados pelas organizações com relação ao tratamento e prevenção às ameaças de segurança são grandes e exigem muitos cuidados. Com esse intuito, diversos meios para analisar e representar a segurança de sistemas de informação são propostos. O emprego da abordagem quantitativa, em particular, é objeto de discussões dos pesquisadores da área ao longo das últimas duas décadas [Verendel 2009], [Jansen 2010].

A quantificação é um paradigma de investigação científico baseado na contagem e mensuração de observações e aplicado em diversas áreas do conhecimento humano. A partir do uso de métricas bem definidas, a quantificação permite a descrição precisa e consistente de diferentes objetos de pesquisa. A ideia de quantificação aplicada a segurança da informação envolve desde o desenvolvimento de métricas de segurança até estudos sobre impactos econômicos, avaliação de risco e modelos para medir segurança [Verendel 2009]. O emprego de métricas de segurança em cenários de TIC (Tecnologia da Informação e Comunicação), em especial, é um tópico fundamental para investigar as motivações dos ataques, avaliar a eficiência dos controles implementados e consequentemente fornecer uma visão geral sobre os problemas de segurança enfrentados pela organização.

Contudo, grande parte da literatura sobre o assunto é teórica e direcionada a sugestão de listas de métricas de segurança [Jaquith 2007], [Herrmann 2007] [Boyer and McQueen 2008], [Chew et al. 2008], [The Center for Internet Security 2010]. Poucos trabalhos analisam as métricas de segurança sob o ponto de vista prático. Esse fato aliado a escassez de estudos empíricos na área de segurança da informação [Verendel 2009], [Kotulic and Clark 2004], [Jansen 2010] reforça a necessidade de pesquisas para identificar as principais métricas usadas para avaliar o nível de segurança da informação e discutir os benefícios e a relevância de tais métricas.

O presente trabalho descreve o projeto e os resultados obtidos com a aplicação de um questionário como um primeiro passo em direção à identificação e discussão de métricas de segurança empregadas para compreender o nível de segurança da informação em uma organização. Para cumprir com esse objetivo, foram incluídas no questionário questões para identificar não somente as métricas utilizadas, mas também para avaliar os níveis de importância e complexidade percebidos pelo usuário em cada métrica. Dessa forma, é possível elucidar uma parte das estratégias utilizadas para adotar uma métrica de segurança e identificar as principais preocupações das organizações.

O restante do artigo está organizado da seguinte forma: a Seção 2 descreve os trabalhos relacionados. A Seção 3 relata a metodologia adotada para a criação da pesquisa e do questionário. A Seção 4 apresenta os principais resultados da aplicação do questionário em uma determinada população. Por fim, as conclusões e sugestões de trabalhos futuros são apresentadas na Seção 5.

2. Trabalhos relacionados

Esta seção apresenta os trabalhos relacionados sob dois pontos de vista: métricas de segurança e o uso de questionários para investigação de problemas de segurança da informação.

2.1. Métricas de segurança

De acordo com [W. Krag Brotby 2009], métrica é um termo utilizado para denotar uma medida baseada em uma referência. Como a segurança, em seu significado mais básico, pode ser representada pela proteção contra as ameaças ou a ausência de ameaças, as métricas devem refletir o nível de segurança relativo a certo objetivo e auxiliar a tomada de decisão para tratar ou evitar ameaças. Pesquisadores do NIST [Chew et al. 2008] afirmam que a implementação de métricas de segurança pode proporcionar diversos benefícios às organizações. O processo de coleta dos dados e apresentação dos resultados permite identificar controles técnicos, operacionais ou de gestão que não estão sendo implementados ou são implementados incorretamente. Utilizando os resultados da análise das métricas, os gerentes e proprietários do sistema podem isolar os problemas, usar os dados coletados para justificar os pedidos de investimentos e assim direcionar os investimentos para as áreas que necessitam de melhorias. No entanto, a proliferação de propostas de métricas de segurança e os problemas relacionados ao uso prático das mesmas, como o uso excessivo de métricas e a avaliação da qualidade das mesmas, motivou a agência federal norte-americana de padronização e tecnologia (NIST) a desenvolver um relatório [Jansen 2010] sobre o estado da arte e possíveis áreas de pesquisa sobre o tema métricas de segurança.

O relatório mostra que, em geral, o estado atual das métricas de segurança envolve indicadores de segurança ambíguos, avaliados de modo subjetivo e que não necessariamente coincidem com os objetivos de segurança da organização. Além disso, poucos trabalhos da área mostraram a utilidade das métricas de segurança na prática. Dessa forma, Jansen [2010] afirma que os esforços em pesquisa na área de métricas de segurança devem envolver os seguintes fatores: i) determinar bons estimadores para a segurança do sistema, ii) reduzir a dependência do elemento humano nas medidas e consequentemente diminuir a subjetividade, iii) oferecer modos mais rápidos e sistemáticos para obter métricas significativas e iv) compreensão sobre os mecanismos de composição de segurança.

O presente trabalho propõe contribuições na busca de bons estimadores para a segurança do sistema, assim como na criação de métodos mais rápidos e sistemáticos para obter métricas significativas usando um questionário como ponto inicial.

2.2. Questionários como ferramenta de estudo para problemas de segurança

O uso de questionários para a investigação de problemas relacionados à segurança da informação é uma prática importante para a validação de modelos e investigação de hipóteses. Alguns trabalhos nessa área incluem: [Kajava and Savola 2005], [Sademies 2004], [Baker and Wallace 2007] e [Bayuk 2011]. Conforme mostrado em tais trabalhos, um problema comum dessa abordagem é a baixa taxa de resposta dos participantes. A sensação de insegurança gerada pela possibilidade de exposição da informação é um dos principais motivos para esse comportamento. Um meio de amenizar tal fenômeno é o uso de questionários *online* que permitem respostas anônimas.

Sademies [2004] propõe um estudo, em forma de questionário, sobre o uso de métricas de segurança em empresas finlandesas. O objetivo do trabalho é revelar como o desenvolvimento e implementação das métricas é feito nas organizações. Os resultados mostraram que métricas técnicas e métricas relacionadas à avaliação de riscos são comumente utilizadas, mas sem o uso de automação e critérios para identificar as medidas mais importantes para a organização. Outro resultado indica que a maioria das organizações não usa as métricas de segurança como um processo, mas sim em aplicações isoladas. Uma pesquisa conduzida também em empresas finlandesas [Kajava and Savola 2005] teve como objetivo identificar como a segurança da informação é medida e avaliada. Os resultados mostraram que apesar de o uso de métricas de segurança estar ainda no começo, às empresas veem com bons olhos o uso de tais técnicas. Outro importante estudo foi conduzido por Baker e Wallace [2007]. O objetivo do trabalho foi identificar como as organizações implementam controles de segurança. Foram compilados oitenta controles de segurança (uso de antivírus, *backup*, monitoração, entre outros) e os participantes indicaram quais dos controles foram implementados e também como foram implementados.

Torres et al. [2009] e o seu grupo de pesquisa também propuseram um questionário para identificar fatores críticos de sucesso (*critical success factors*) que afetam a segurança da informação e as respectivas métricas para cada um dos grupos. Dentre as 40 respostas obtidas, os resultados mostraram que o comprometimento da gerência com a área de segurança e a estratégia de segurança traçada foram os fatores críticos de sucesso com as melhores avaliações. Outra investigação baseada em questionários proposta em [Alencar et al. 2013] mostra que o papel da segurança da informação em 34 empresas brasileiras estudadas ainda é simplório, focado no tratamento de *malwares* e ataques externos

não realizando atividades simples como se preocupar com a política de senhas, rotinas de backup eficientes, divulgação de segurança da informação para outros setores da organização, entre outras. O trabalho conduzido em [Machado et al. 2009] utilizou um questionário para avaliar a influência de fatores organizacionais na percepção da efetividade da segurança da informação em universidades públicas. Os pesquisadores concluíram que os fatores organizacionais identificados como mais relevantes são compatíveis com os fatores encontrados nas empresas privadas, apesar das universidades públicas terem um caráter específico de ensino, pesquisa e extensão.

É possível notar que a avaliação de métricas de segurança somente foi abordada no trabalho proposto por [Torres et al. 2009]. De modo geral, nos outros trabalhos a investigação consistia em avaliar os controles de segurança implementados (que em alguns casos são quantificados usando métricas, como mostrado em [Baker and Wallace 2007]) ou validar modelos de segurança. A principal diferenças entre o presente estudo e a análise conduzida em [Torres et al. 2009] reside no modo com que as métricas foram avaliadas pelos respondentes. Enquanto que a pesquisa realizada por Torres envolve a avaliação da aderência das métricas aos respectivos fatores críticos de sucesso, nosso objetivo consiste em identificar quais métricas são efetivamente empregadas para avaliar o nível de segurança da informação, além de propor uma análise acerca da percepção de importância e complexidade em cada uma das métricas.

3. Metodologia

Como o público alvo da investigação é a comunidade de TIC, foi utilizado um questionário anônimo e *online* com perguntas simples em que o participante levasse por volta de 15 - 20 minutos para responder toda a pesquisa. Foi usado esse estilo de questionário, pois em pesquisas ligadas a segurança da informação, o emprego de questionários longos e exigência de identificação podem desestimular a participação do público alvo [Kotulic and Clark 2004].

Baseado nos questionários propostos por [Bayuk 2011] e [Torres et al. 2009], optou-se por fornecer uma lista de métricas para ser selecionada e também avaliada pelo participante (múltipla escolha e escala de avaliação). Cinco grupos foram criados a fim de facilitar a seleção das métricas presentes no questionário. Cada um dos grupos está relacionado a um dos objetivos primários de segurança da informação em uma organização que é a proteção da informação contra usuários não autorizados [Nakamura and Geus 2007]. Os grupos são:

- Ameaças: trata dos diferentes tipos de ataques que a organização enfrenta;
- Vulnerabilidades de segurança: as vulnerabilidades de segurança representam um importante ponto de acesso para potenciais ameças;
- Como a organização lida com os ataques: a maneira com que os ataques são tratados e prevenidos;
- Alvos dos ataques: representa os possíveis alvos direcionados pelos atacantes;
- Detecção de ataques: trata dos métodos de detecção usados para encontrar ataques;

Os grupos foram baseados na classificação proposta em [Daniel E. Geer Jr and Pareek 2012], onde foram mapeadas seis importantes características usadas para avaliar o nível de segurança da informação em uma organização.

Essa classificação também serviu como base para a construção de um índice que avalia o risco percebido pelas organizações no contexto da segurança da informação [Jr. and Pareek 2012]. O trabalho, porém, não investiga como essas características são medidas, ou ainda a complexidade que envolve cada uma delas.

Após discussões com profissionais da área e da análise de diversos trabalhos [The Center for Internet Security 2010], [Chew et al. 2008], [Jaquith 2007], [Torres et al. 2009], [Boyer and McQueen 2008], [W. Krag Brotby 2009], trinta métricas foram incluídas no questionário. Outras métricas poderiam fazer parte dessa lista, porém, foram escolhidas métricas já existentes na literatura e estritamente relacionadas aos grupos definidos. Além disso, a presença de muitas métricas na pesquisa poderia aumentar o tempo de preenchimento do questionário e consequentemente diminuir o interesse dos participantes.

As três perguntas apresentadas aos participantes sobre as métricas foram as seguintes:

1. Quais métricas são utilizadas para auxiliar a compreender o nível de segurança da informação de sua organização?
2. Em uma escala de 1 a 5 (com 5 para mais importante), analise as métricas de acordo com a sua importância em avaliar o nível de segurança da informação da organização;
3. Em uma escala de 1 a 5 (com 5 para mais complexo), avalie as métricas de acordo com a complexidade de sua utilização.

Além da avaliação das métricas, foram incluídas algumas questões para ajudar a caracterizar a demografia dos participantes, como a área de atuação da organização, atividade desempenhada e o número de anos com relação à experiência na área de segurança da informação. Esse tipo de questão é importante nessa categoria de pesquisa, pois auxilia a interpretação dos resultados.

A pesquisa foi criada com o auxílio do *SurveyMonkey*, uma ferramenta que oferece uma infraestrutura completa para a criação e publicação de questionários. Porém, antes de disponibilizar a pesquisa para o público, foram feitos alguns testes na versão inicial do questionário, com a ajuda de dois profissionais da área de TIC/Segurança. Após alguns ajustes (erros ortográficos e de digitação e sugestões nas perguntas demográficas), a pesquisa foi publicada durante um mês no período entre 23/01/2013 à 23/02/2013.

Com o intuito de atingir um número representativo de respostas da comunidade de TIC, a pesquisa foi compartilhada nas seguintes listas de e-mail: administradores de rede da Unicamp, funcionários do CAIS/RNP, Sociedade Brasileira de Computação (SBC), Comissão Especial em Segurança da Informação e de Sistemas Computacionais (CESeg), analistas do CERT.br e grupos de segurança e resposta a incidentes brasileiros.

4. Resultados

Um total de 47 respostas foram obtidas ao longo do período em que a presente pesquisa foi disponibilizada na *Web*. De acordo com as respostas, a maioria dos participantes (mais de 65%) trabalha em empresas de TIC ou do ramo da educação (universidades e centros de pesquisa) e grande parte ocupam posições estritamente ligadas a resolução de problemas em segurança da informação (mais de 68% são gerentes de TIC ou analistas de

Tabela 1. Métricas utilizadas - Cinco primeiros resultados

Métrica	Resultado	Classificação
Número de ataques relacionados a Spam	23 (48,94%)	Ameaças
Número de ataques relacionados a Negação de Serviço	21 (44,68%)	Ameaças
Número de incidentes de segurança internos	21 (44,68%)	Detecção de ataques
Número de vulnerabilidades de segurança em servidores	20 (42,55%)	Vulnerabilidades
Número de incidentes de segurança externos	19 (40,43%)	Detecção de ataques

Tabela 2. Métricas utilizadas - Cinco últimos resultados

Métrica	Resultado	Classificação
Número de vulnerabilidades de segurança em recursos que estão na Nuvem	4 (8,51%)	Vulnerabilidade
Custo médio por incidente	5 (10,64%)	Como a organização lida com os ataques
Número de correções (patches) não aplicadas por período	5 (10,64%)	Como a organização lida com os ataques
Número de ataques direcionados a dispositivos móveis	5 (10,64%)	Alvos dos ataques
Número de ataques a recursos que estão na Nuvem	5 (10,64%)	Alvos dos ataques

TIC, suporte ou segurança). Além disso, os participantes possuem, em média, sete anos de experiência em segurança da informação.

4.1. Métricas com os maiores e menores índices de utilização

As Tabelas 1 e 2 apresentam os cinco primeiros e os cinco últimos resultados para a pergunta "Quais métricas são utilizadas para auxiliar a compreender o nível de segurança da informação de sua organização?". O campo "Resultado" mostra o número de participantes que escolheram tal métrica e a respectiva porcentagem do total. A classificação de cada uma das métricas é mostrado no campo "Classificação".

A Tabela 1 mostra nas primeiras posições métricas relacionadas a dois ataques clássicos: Spam e Negação de Serviço. Apesar de existir uma tendência de diminuição no número de Spams reportados [CERT.br 2013], sua incidência ainda é muito alta quando comparada com outros tipos de ataques, o que certamente influencia a presença de tal métrica entre as mais utilizadas. O Cert.br, por exemplo, reportou nos anos de 2011, 2012 e 2013 o seguintes ocorrências de Spam: 3.502.521, 1.731.842 e 811.266. Considerando ainda os anos de 2011, 2012 e 2013, a quantidade de outros tipos de problemas de segurança da informação reportados pelo Cert.br foi de 399.515, 466.029 e 264.580 o que representa uma grande diferença na relação entre Spam e outros incidentes de segurança. Ao contrário dos Spams, o volume de ataques de Negação de Serviço aumentou 32% entre 2012 e 2013, segundo relatório conduzido pela empresa norte-americana de consultoria em segurança *Prolexic* [Prolexic 2013]. No Brasil, os recentes ataques promovidos por grupos parceiros do Anonymous pode ter elevado a preocupação com esse tipo de ataque.

Ainda na Tabela 1 as métricas ligadas ao número de incidentes de segurança também apareceram entre as mais utilizadas. Esse resultado era de certa forma já esperado, pois, apesar de fornecerem uma visão restrita sobre as ataques realizados contra a organização (somente ataques com sucesso são contabilizados), tais métricas são frequentemente citadas na literatura como indicadores relevantes para avaliar o nível de segurança. O número de incidentes de segurança internos, em especial, chama a atenção. Ataques efetuados dentro da organização, em geral, podem causar muitos problemas e são difí-

Tabela 3. Comparação entre as métricas utilizadas em cada grupo

	Média	Desvio padrão	Agrupamento para o teste de Tukey (*)
Ameaças	2,66	2,17	A
Detecção de ataques	1,83	1,479	A B
Vulnerabilidades	1,234	1,605	B
Como a organização lida com os ataques	1,043	1,197	B
Alvos dos ataques	1,021	1,26	B
$p < 0,0001$			

ceis de mitigar [Nakamura and Geus 2007]. Porém, estudos como [Richardson 2011] e [Verizon 2012], apontam uma queda no número desses ataques. Os resultados encontrados na pesquisa proposta mostram que apesar da tendência de diminuição, os ataques internos ainda preocupam os profissionais de segurança.

Fora do grupo dos cinco primeiros (Tabela 2) pode-se destacar os resultados para a segurança dos dispositivos móveis e recursos alocados na nuvem. Esses dois tipos de recursos são razoavelmente novos do ponto de vista tecnológico, ou seja, a frequência de ataques em tais recursos pode ainda não ser a suficiente para chamar a atenção dos profissionais de segurança. Ou ainda, os recursos de segurança existentes não dão o suporte necessário para tais áreas, dificultando a detecção e tratamento desses ataques. A segurança da computação em nuvem, por exemplo, é um tópico de pesquisa atual e com diversos problemas de pesquisa em aberto [Kaufman 2009] assim como trabalhos recentes revelam as dificuldades enfrentadas pelos profissionais de segurança com os funcionários levando seus próprios dispositivos móveis para os domínios da empresa [Thomson 2012]. Apesar de aparecer em diversas listas de recomendação de métricas de segurança, o custo médio por incidente é utilizado por somente 10,64% dos participantes. O uso de tal métrica está diretamente ligado à habilidade da organização em estimar os custos ligados aos incidentes de segurança. Os resultados sugerem uma ausência de políticas voltadas para lidar com os efeitos econômicos causados pelos problemas de segurança da informação.

4.2. Uso das métricas por grupo

Os resultados presentes nas Tabelas 1 e 2 também mostraram que dentre as cinco métricas mais utilizadas, duas pertencem ao grupo Ameaças e duas pertencem ao grupo Detecção de Ataques e que dentre as cinco métricas menos utilizadas, duas pertencem ao grupo Como a organização lida com o ataques e duas ao grupo Alvos dos ataques. Essa análise revela uma possível tendência acerca do modo com que as métricas são utilizadas. No intuito de identificar as diferenças entre cada um dos grupos foi utilizado um procedimento estatístico conhecido como Análise de Variância (ANOVA). Para cada participante da pesquisa, foram identificadas as métricas selecionadas como "utilizadas" e os respectivos grupos para cada uma delas. A Tabela 3 mostra os resultados dos testes ANOVA para as diferenças entre cada um dos grupos.

O valor p encontrado mostra que a hipótese nula H_0 (não há evidência de diferença significativa entre as populações) deve ser descartada. Assim, existem diferenças significativas entre pelo menos duas médias da população estudada. Para identificar os grupos que causam diferenças aplicamos o teste de Tukey em nossa amostra. A coluna "Agrupamento para o teste de Tukey" mostra a informação de agrupamento do teste. Nesse caso, médias que não compartilham letras possuem diferenças significativas. Portanto,

foi possível encontrar diferenças significativas entre a variável "Ameaças" e as variáveis "Vulnerabilidades", "Como a organização lida com os ataques" e "Alvos dos ataques".

O resultado encontrado sugere uma preferência pelo uso de métricas ligadas à contagem de tipos específicos de ataques. Essa descoberta revela que apesar da segurança ser uma atividade complexa e depender de diversos fatores, os ataques sofridos pela organização desempenham um papel importante para a percepção do nível de segurança da informação. Tais métricas funcionam como uma valiosa fonte de informação inicial, mas, quando usadas isoladamente podem levar a problemas de interpretação. Um aumento no número de ataques, por exemplo, pode representar que a organização está mais vulnerável aos ataques assim como também pode indicar que mais recursos (tempo, funcionários e tecnologia) foram alocados para a detecção de incidentes. É importante que outras métricas sejam usadas em conjunto com as métricas do grupo "Ameaças" para melhorar a compreensão do cenário de ataques.

4.3. Relação entre a percepção de importância e complexidade na escolha das métricas

Diferentemente de trabalhos anteriores [Jaquith 2007], [Herrmann 2007] [Boyer and McQueen 2008], [Chew et al. 2008], [The Center for Internet Security 2010] em que métricas de segurança são sugeridas sem nenhuma justificativa prática, esse trabalho busca identificar métricas que são empregadas na práticas e divulgá-las para a comunidade de segurança. Contudo, um problema comum no processo de seleção e implantação de métricas é conhecido como uso excessivo de métricas [W. Krag Brotby 2009], ou seja, a organização pode gastar recursos implementando muitas métricas e não usá-las de fato. Portanto, para diminuir o impacto do uso excessivo de métricas, ao invés de simplesmente listar as métricas com o maior índice de utilização iremos refiná-las usando dois atributos: as avaliações de importância e complexidade. Dessa forma os seguintes conjuntos de métricas serão investigados:

- Conjunto 1 - Métricas que estão entre as mais utilizadas e que são importantes e simples;
- Conjunto 2 - Métricas que estão entre as mais utilizadas e que são importantes e complexas;
- Conjunto 3 - Métricas que não estão entre as mais utilizadas, não figuram entre as mais importantes e são complexas;
- Conjunto 4 - Métricas que não estão entre as mais utilizadas, não figuram entre as mais importantes e são simples.

Os conjuntos 1 e 2 apresentam não somente as métricas com alto índice de utilização, mas também com boa avaliação no quesito importância e com diferentes níveis de complexidade. Tais grupos funcionam como critérios para facilitar a seleção das métricas. Já os conjuntos 3 e 4 apresentam as métricas com pequeno índice de utilização, baixa avaliação no quesito importância e com diferentes níveis de complexidade. Esses conjuntos funcionam como um crivo para o possível descarte de métricas.

Os conjuntos foram construídos da seguinte forma: agrupamento das métricas de acordo com o a) número de respostas para a pergunta 1 (quais métricas são utilizadas), b) avaliações médias obtidas com a pergunta 2 (avaliação da importância) e c) avaliações médias obtidas com a pergunta 3 (avaliação da complexidade). Por exemplo, considere

Tabela 4. Conjunto 1 - Métricas que estão entre as mais utilizadas, importantes e simples

Métrica	Grupo
Número de incidentes de segurança internos reportados/detectados	Detecção de ataques
Número de ataques relacionados a estrutura física da organização	Ameaças
Número de ataques relacionados a Phishing	Ameaças
Número de ataques relacionados a Malwares	Ameaças

Tabela 5. Conjunto 2 - Métricas que estão entre as mais utilizadas, importantes e complexas

Métrica	Grupo
Número de vulnerabilidades de segurança em servidores	Vulnerabilidades
Número de vulnerabilidades de segurança em equipamentos de rede	Vulnerabilidades
Número de incidentes críticos (severos) reportados/detectados	Detecção dos ataques
Número de incidentes de segurança externos reportados/detectados	Detecção de ataques
Número de ataques relacionados a exploração de vulnerabilidades de segurança	Ameaças
Número de ataques relacionados a Negação de Serviço	Ameaças
Tempo médio para se recuperar de um incidente	Como a organização lida com os ataques
Número de ataques direcionados a servidores	Alvos dos ataques

que uma determinada métrica A foi citada como utilizada por 4 participantes e cada um dos participantes atribuiu as notas (3,4,3,5) e (1,2,2,3) para importância e complexidade. Dessa forma temos o valor 4 para a utilização, 3,75 para o valor médio de importância e 2 para complexidade. O próximo passo consistiu em separar os valores abaixo e acima da média para cada métrica. Para encontrar os componentes do conjunto 1 selecionamos os valores acima da média para utilização, acima da média para importância e abaixo da média para complexidade. O conjunto 1 é dado pela intersecção entre eles. Os conjuntos 2, 3 e 4 são obtidos de maneira análoga.

É importante ressaltar que a presente classificação reflete as preferências da população investigada. O objetivo desse trabalho é fornecer insumos iniciais para a discussão da relevância das diversas métricas de segurança propostas na literatura, visto a ausência de referências sobre o tema. O agrupamento proposto atinge os alvos primários do artigo, mas também instiga a replicação dos resultados para novas métricas e diferentes amostras populacionais.

Tabela 6. Conjunto 3 - Métricas que não estão entre as mais utilizadas, não figuram entre as mais importantes e são complexas

Métrica	Grupo
Número de ataques relacionados a Engenharia Social	Ameaças
Número de ataques relacionados a Botnets	Ameaças
Número de ataques a recursos que estão na nuvem	Ameaças
Custo médio por incidente	Como a organização lida com os ataques
Tempo médio entre incidentes	Como a organização lida com os ataques
Número de vulnerabilidades de segurança em dispositivos móveis	Vulnerabilidades
Número de vulnerabilidades de segurança em recursos que estão na nuvem	Vulnerabilidades
Número de ataques direcionados a dispositivos móveis	Alvos dos ataques

Tabela 7. Conjunto 4 - Métricas que não estão entre as mais utilizadas, não figuram entre as mais importantes e são simples

Métrica	Grupo
Porcentagem de tentativas de intrusão bloqueadas	Detecção dos ataques
Porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários	Detecção dos ataques
Número de correções (patches) aplicadas por período	Como a organização lida com os ataques
Número de correções (patches) não aplicadas por período	Como a organização lida com os ataques

As Tabelas 4, 5, 6 e 7 mostram as métricas presentes em cada um dos conjuntos. Somente quatro métricas fazem parte do conjunto 1 que lista não somente as mais importantes e utilizadas como também as mais simples. Não é surpresa a presença de métricas ligadas a vírus e códigos maliciosos (*Malwares* e *Phishing*), já que tais ameaças representam riscos de segurança óbvios e persistentes para as organizações. A presença da métrica que trata sobre incidentes de segurança internos entre as mais utilizadas e importantes corrobora estudos recentes sobre a relevância em combater os *insiders* na organização [Alencar et al. 2013], [Pfleeger et al. 2010]. É sabido também que as estratégias para mitigação das ameaças internas são complexas e envolvem questões de tecnologia, processo e pessoal. Os resultados obtidos em nossa pesquisa mostram que o problema ainda reside na mitigação de tais ameaças e não na detecção das mesmas. No conjunto 2 chama a atenção as métricas sobre vulnerabilidades de segurança, não pelo uso ou pela importância mas devido a complexidade. É possível afirmar que no domínio da segurança da informação, vulnerabilidades representam uma das fontes de dados mais extensas [Verendel 2009] [Miani 2013]. Além disso, uma variedade de softwares para verificação de vulnerabilidades (*vulnerabilities scanners*) pode ser encontrada, alguns, inclusive sob a licença GPL (*OpenVAS*). O resultado encontrado indica dificuldades na coleta de informação sobre vulnerabilidades de segurança ou ainda no manuseio de tais softwares.

O conjunto 3, apresentado na Tabela 6, apresenta uma importante diferença entre três métricas que são citadas com frequência na literatura: tempo médio para se recuperar de um incidente, custo médio por incidente e tempo médio entre incidentes. Enquanto que o tempo médio para se recuperar de um incidente situou-se no conjunto 2, as outras duas métricas posicionaram-se no conjunto 3 em que não são utilizadas, não figuram entre as mais importantes e são complexas. Outra descoberta envolve as métricas sobre dispositivos móveis e recursos disponíveis na nuvem. Conforme discutido anteriormente, esse resultado reside no fato de que a segurança em computação em nuvem ainda é uma área em desenvolvimento, assim como lidar com proliferação dos dispositivos móveis. Por fim, o conjunto 4 representa as métricas que não estão entre as mais utilizadas, não figuram entre as mais importantes e são simples. O presente conjunto apresenta um contraste entre encontrar vulnerabilidades de segurança e corrigí-las. A correção, por meio da instalação de patches, é uma prática essencial em segurança já que impede futuros problemas relacionados a tal vulnerabilidade. Porém, a contabilização dos patches aplicados, apesar de simplicidade, não representou importância na avaliação do nível de segurança da organização.

5. Conclusão

O presente trabalho propôs uma pesquisa para avaliar como as métricas presentes na literatura são empregadas nas organizações. Foi possível notar a preocupação dos participantes com duas ameaças específicas (Spam e Negação de serviço) e com as vulnerabilidades de segurança encontradas em servidores. Também foram encontradas diferenças significativas entre as métricas pertencentes aos grupos "Ameaças" e os grupos "Vulnerabilidades", "Como a organização lida com os ataques" e "Alvos dos ataques". Tal diferença reforça a tese de que os ataques disparados contra a organização desempenham um papel fundamental na percepção do nível de segurança da informação, ainda que inúmeros fatores possam ter contribuído para a realização de tal ataque. Além disso, as métricas foram classificadas sob a ótica das avaliações de importância e complexidade, fornecendo um novo critério para que profissionais e pesquisadores da área possam aperfeiçoar o entendimento do árduo processo de seleção e implementação de métricas. Apesar dos resultados manisfestarem a preferência da população investigada, não encontramos na literatura referências que adotam esse ponto de vista. Acredita-se, portanto, que este trabalho possa servir como um ponto inicial para explorar os benefícios e os problemas do emprego de métricas em segurança da informação. Trabalhos futuros incluem o estudo da qualidade da implementação das métricas, investigação da relação entre o uso de métricas e a ocorrência de incidentes de segurança e as variações acerca do uso de métricas em organizações de setores e tamanhos diferentes.

Agradecimentos

À FAPESP e a Universidade Federal de Uberlândia pelo apoio financeiro e institucional e aos profissionais da área de TIC que participaram desta pesquisa.

Referências

Alencar, G., Queiroz, A., and Queiroz, R. J. (2013). Insiders: Um Fator Ativo na Segurança da Informação. In *IX Simpósio Brasileiro de Sistemas de Informação (SBSI 2013)*, p. 61–72.

Baker, W. and Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, 5(1):36–44.

Bayuk, J. L. (2011). *Measuring Systems Security: An Initial Security Theoretical Construct Framework*. PhD thesis, Stevens Institute of Technology.

Boyer, W. and McQueen, M. (2008). Ideal based cyber security technical metrics for control systems. In *Critical Information Infrastructures Security*, p. 246–260.

CERT.br (2013). Estatísticas dos Incidentes Reportados ao CERT.br.

Chew, E., Swanson, M., Stine, K., and Bartol, N. (2008). SP 800-55 Rev. 1. Performance Measurement Guide for Information Security. Technical Report July, National Institute of Standards and Technology (NIST).

Daniel E. Geer Jr and Pareek, M. (2012). ICS Update. *IEEE Security & Privacy Magazine*, 10(June):93–95.

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*. Auerbach Publications.

Jansen, W. (2010). Directions in security metrics research. Technical report, National Institute of Standards and Technology (NIST).

Jaquith, A. (2007). *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley Professional.

Jr., D. E. G. and Pareek, M. (2012). Index of Cyber Security.

Kajava, J. and Savola, R. (2005). Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes. In *Proceedings of the European University Information Systems (EUNIS)*.

Kaufman, L. (2009). Data security in the world of cloud computing. *IEEE Security & Privacy*, p. 61–64.

Kotulic, A. G. and Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, 41(5):597–607.

Machado, C., Cabral, L., Santos, J., and Motta, G. (2009). Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico. In *V Simpósio Brasileiro de Sistemas de Informação (SBSI 2009)*, p. 97–108.

Miani, R. S. (2013). *Um estudo sobre métricas e quantificação em segurança da informação*. PhD thesis, University of Campinas (UNICAMP).

Nakamura, E. T. and Geus, P. L. (2007). *Segurança de Redes em Ambientes Cooperativos*. Editora Novatec.

Pfleeger, S., Predd, J., Hunker, J., and Bulford, C. (2010). Insiders Behaving Badly: Addressing Bad Actors and Their Actions. *IEEE Transactions on Information Forensics and Security*, 5(1):169–179.

Prolexic (2013). Global DDoS Attack Report. Technical report.

Richardson, R. (2011). Computer Crime and Security Survey. Technical report, Computer Security Institute.

Sademies, A. (2004). *Process Approach to Information Security Metrics in Finnish Industry and State Institutions*. PhD thesis, University of Oulu.

The Center for Internet Security (2010). The CIS Security Metrics. Technical Report 28, The Center for Internet Security.

Thomson, G. (2012). BYOD: enabling the chaos. *Network Security*, 2012(2):5–8.

Torres, J., Sarriegi, J., Hernantes, J., and Lauge, A. (2009). Steering Security through Measurement. *Trust, Privacy and Security in Digital Business*, p. 95–104.

Verendel, V. (2009). Quantified security is a weak hypothesis. In *Proceedings of the 2009 workshop on New security paradigms workshop - NSPW '09*, p. 37–49.

Verizon (2012). 2012 Data Breach Investigations Report. Technical report, Verizon.

W. Krag Brotby (2009). *Information security management metrics: a definitive guide to effective security monitoring and measurement*. Auerbach Publications.