Processo de Gestão de Vulnerabilidades de Segurança na Universidade Federal da Bahia

Gildásio Q. Júnior[1], **Rogerio Bastos**[1], **Italo Valcy S Brito**[1]

[1]Superintendência de Tecnologia da Informação
Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

{jose.gildasio,rogerio.bastos,italovalcy}@ufba.br

Resumo. *Esse artigo apresenta um relato de experiências na implantação do processo de gestão de vulnerabilidades de segurança da informação na Universidade Federal da Bahia, retratando os pontos principais de atenção na estruturação desse processo, bem como estratégias que podem ser adotadas para o sucesso na sua execução. Resultados apontam uma redução de cerca de 30% na quantidade de incidentes de segurança da organização.*

1. Introdução

A área de Segurança da Informação e Comunicações (SIC) vem ganhando importância significativa nas organizações ao longo dos últimos anos, principalmente pela consciência de que a informação é um dos principais ativos da organização. Por outro lado, o crescente indice de incidentes de segurança que atingem as organizações e os danos causados por estes incidentes evidenciam uma necessidade por ações proativas para viabilizar a proteção da SIC na organização. De acordo com a norma ABNT NBR ISO/IEC 27002 [ISO/IEC 2013], um dos controles que pode apoiar nesse sentido é o Processo de Gestão de Vulnerabilidades Técnicas.

Na UFBA, tal cenário não é diferente. Ao longo dos anos observa-se um aumento na quantidade de incidentes tratados pela Equipe de Tratamento de Incidentes de Redes (ETIR-UFBA). Embora a atuação na área de tratamento de incidentes venha se consolidando a cada ano, percebe-se a necessidade de processos de segurança que complementem essa ação reativa e, assim, reduza a quantidade de incidentes. Nesse sentido, a implantação de uma Gestão de Vulnerabilidade torna-se igualmente importante.

De acordo com [Palmaers 2013], gestão de vulnerabilidade é o processo de conhecer as fraquezas de um sistema, hardware ou software, avaliar os riscos aplicados ao negócio, para então prosseguir com o seu tratamento, seja corrigindo-a e removendo o risco, ou obtendo uma formal aceitação dos mesmos.

Diversas técnicas, ferramentas e processos são aplicados para a construção de um bom processo de gestão de vulnerabilidades. Não existe, todavia, um *framework* genérico que possa se adequar a todas as organizações [Palmaers 2013]. Especialmente no contexto de Universidades, cuja heterogeneidade dos sistemas de TI e a diversidade de perfis das pessoas são a norma, o desafio de gestão deste processo é ainda maior, principalmente para administração das expectativas de tempo e capacitação para atuação na mitigação de uma vulnerabilidade.

Este artigo apresenta um relato de experiências na implantação do processo de gestão de vulnerabilidades técnicas na UFBA, cuja estruturação foi realizada de forma simplificada e objetiva, ciente dos desafios da Universidade e observando as melhores práticas de mercado para esse tema. Nesse sentido, alguns itens vistos como imprecindíveis no processo criado para a UFBA foram: i) estruturação de uma gestão de ativos flexível; ii) alinhamento de atividades e capacitação das outras áreas para tratamento das vulnerabilidades; iii) consolidação de base de conhecimento de vulnerabilidades; e iv) definições de níveis de acordo de serviços levando em consideração criticidade da vulnerabilidade, risco ao negócio e contexto real da coordenação responsável.

O restante deste artigo está organizado da seguinte maneira. A Seção 2 apresenta o trabalho de implantação da gestão de vulnerabilidades na UFBA. A Seção 3 traz resultados preliminares e, por fim, a Seção 4 apresenta as conclusões e trabalhos futuros.

2. Trabalho Desenvolvido

Na construção desse plano de gestão de vulnerabilidades foi notável a importância de definição de três pontos: os papéis e responsabilidades do envolvidos, a definição de uma matriz para análise de risco da vulnerabilidade e de acordos de níveis de serviços com outras áreas, e, por fim, a definição de um processo para definir exatamente como a gestão de vulnerabilidades irá funcionar.

2.1. Papéis e Responsabilidades

A definição das pessoas e grupos que irão atuar em um processo de gestão de vulnerabilidades é extremamente importante para que se possa ter um canal limpo de comunicação a depender do tipo de vulnerabilidade e como ela deve ser tratada no contexto organizacional. Isso deve perpassar todos os níveis organizacionais, do mais operacional, os analistas responsáveis por executar as atividades, ao mais estratégico, gestores responsáveis pela tomada de decisão e aceitação dos riscos. Na construção do plano de gestão de vulnerabilidades da UFBA foram especificados os seguintes papéis e responsabilidades:

- ***Equipe de Tratamento de Incidentes de Redes (ETIR-UFBA)***: responsável por monitorar, identificar, analisar, notificar e apoiar no tratamento de vulnerabilidades de segurança da informação nos serviços e recursos de TIC no âmbito da Instituição, bem como gerar relatórios e estatísticas para acompanhamento pelas equipes técnicas envolvidas, pela alta gestão ou pelos órgãos de controle;

- ***Administrador de rede ou de sistema***: responsável por investigar e tratar as notificações de vulnerabilidades reportadas pela ETIR-UFBA, executando ações de contenção da vulnerabilidade, correção e resposta, reportando-se à ETIR-UFBA sobre ações executadas;

- ***Gestor de Configuração da STI***: responsável por monitorar mudanças ocorridas para manter a gestão de inventário de hardware e software atualizada. Na ausência do Gestor de Configuração, essa responsabilidade fica com o Gestor de Mudanças;

- ***Gestor de Mudanças da STI***: responsável por analisar as alterações no ambiente e julgar os riscos de segurança envolvidos nas mudanças;

- ***Gestor de SIC e Superintendente de TI***: acompanhar os relatórios de gestão de vulnerabilidades e escalonar o tratamento de vulnerabilidades críticas ou fora de prazo junto aos coordenadores específicos;

- ***Fabricantes e fornecedores***: responsável por corrigir vulnerabilidades em ambientes e ferramentas externas ou terceirizadas ao ambiente da UFBA, além de apoiar as equipes internas na definição de boas práticas de configuração segura ou configuração de correção de vulnerabilidades.

2.2. Matriz de Prioridade

Considerando a alta carga de trabalho a que os diversos setores já estão sujeitos, é importante definir a criticidade das vulnerabilidades identificadas a fim de que esses setores possam priorizar seu tratamento em relação às demais atividades. Nesse sentido, foi criada a matriz de prioridades conforme apresentado na Tabela 1. A partir dessa matriz, é possível avaliar quais vulnerabilidades são mais críticas e, assim, ter uma visão do impacto à organização quando do seu não tratamento.

Impacto à Organização	Score CVSS		
	Baixo	Médio	Alto
Alto	3	2	1
Médio	4	3	2
Baixo	4	4	3

Tabela 1. Matriz prioridade

Essa matriz foi criada levando em conta dois itens importantes: *score* CVSS e o impacto à organização. O CVSS, do inglês *Common Vulnerability Scoring System*[1], é um padrão criado pelo *Forum for Incident Response and Security Teams* (FIRST) para calcular a severidade de uma vulnerabilidade com base em características do ambiente.

É preciso de bastante conhecimento acerca do negócio para definir o impacto à organização que uma vulnerabilidade tem. Nesse caso, foi levado em consideração a possibilidade de ocorrência da exploração e consequências negativas para a universidade. Questões como perda de prazos legais, danos à imagem da organização, indisponibilidade de sistemas críticos para o negócio, são exemplos de consequências que devem ser avaliadas e ordenadas, contextualizando a organização.

2.3. Fluxograma do Processo

Todo o fluxo de atividades na gestão de vulnerabilidades planejado para a UFBA pode ser entendido passando por três grandes fases. A primeira consiste em ter o conhecimento da vulnerabilidade. Isso pode ser feito de diversas formas, por exemplo, fazendo auditorias nos sistemas ou monitorando listas de e-mail e *newsletter* de fornecedores e comunidades. Após receber as vulnerabilidades é preciso executar um filtro de aplicabilidade, fazendo uma checagem se a vulnerabilidade pode atingir algum ativo de fato da organização. Esta primeira validação consiste de um casamento simples entre a lista de

[1]https://www.first.org/cvss/ (último acesso 23/04/2018)

ativos da organização e os alertas de vulnerabilidades identificados. Não obstante, deve-se ter uma preocupação especial para não expôr ferramentas ou versões de software da organização, o que culminaria em novos riscos de segurança.

A partir desse primeiro filtro inicial, um analista irá validar se o ambiente está realmente exposto por tal vulnerabilidade. Muitas vulnerabilidades dependem de condições de exploração complexa, requerem configurações específicas do ativo ou ainda não estão presentes no cenário da organização (e.g., devido a desativação de uma função ou aplicação de um *patch*). Portanto, sempre que possível, é importanta validar e documentar as etapas de teste ou não teste do ativo, registrando na base de conhecimento. Ao identificar a brecha de segurança, deve-se prosseguir com a classificação da vulnerabilidade, conforme Seção 2.2. O próximo passo é produzir uma notificação formal da vulnerabilidade e enviá-la aos responsáveis pelo ativo.

Após notificar os responsáveis, inicia-se a última grande fase: acompanhamento da vulnerabilidade. Nessa fase, a equipe da ETIR-UFBA, em contato com os responsáveis pelo ativo, verifica e, se preciso, auxilia no tratamento da vulnerabilidade alertada. Ainda nessa fase, pode-se realizar a validação da correção aplicada, confirmando a mitigação do risco. Todos esses passos podem ser vistos de maneira estruturada em Figura 1.

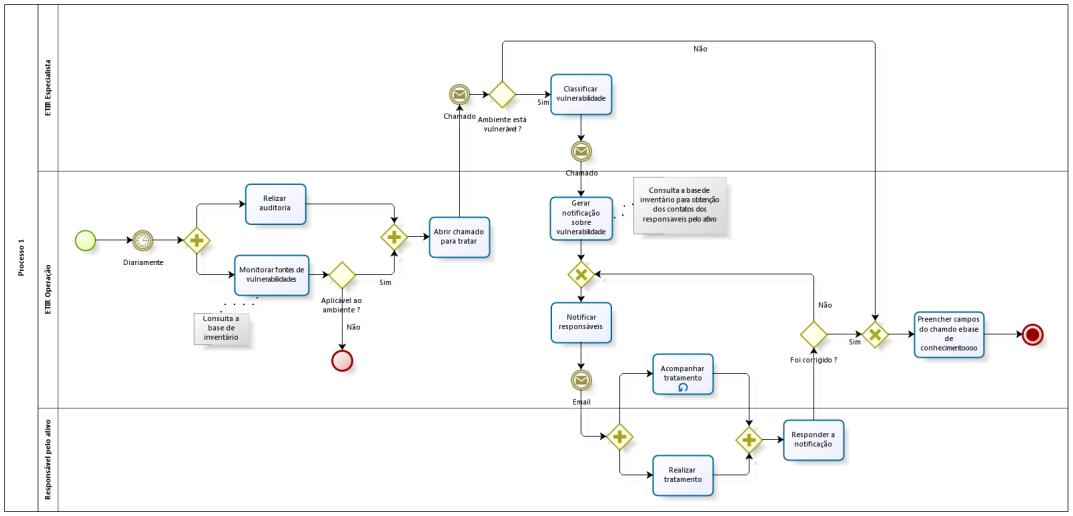

Figura 1. Fluxograma do plano de gestão de vulnerabilidades da UFBA

3. Resultados

Desde a aplicação desse plano de gestão de vulnerabilidades, iniciada no segundo semestre de 2017, houve uma redução na quantidade de incidentes de segurança, como mostra a Figura 2. O gráfico em questão apresenta um resultado importante, tendo em vista que observa-se uma redução na ordem de 30% da quantidade de incidentes a partir do tratamento provativo das vulnerabilidades que seriam possivelmente exploradas.

Uma experiência recente da ETIR-UFBA nesse contexto foi o conhecimento de uma vulnerabilidade gravíssima em um software de conteúdo bastante utilizado e difundido na universidade. Assim identificada a vulnerabilidade e o impacto que sua exploração causaria à infraestrutura, executou-se o processo de forma ágil e sistematizada, resultando na mitigação em tempo recorde e com efetividade desejada.

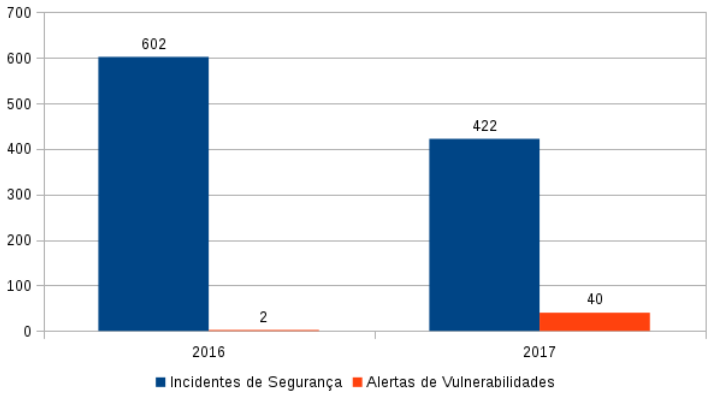

Figura 2. Quantidade de incidentes de segurança e vulnerabilidades de conhecimento da ETIR-UFBA em 2016 e 2017

Outro ponto importante é a credibilidade que um processo bem estabelecimento de gestão de vulnerabilidades agrega à equipe de segurança. Uma vez que uma notificação é realizada e acompanhada pela equipe, a alta gestão tem à mão insumos para efetivamente tomar decisões sobre a priorização das ações das equipes, bem como as próprias equipes responsáveis pelo ativo recebem demandas para realização de manutenções planejadas de correção. Mesmo em caso de aceitação do risco, a decisão é tomada de forma consciente.

4. Conclusões e Trabalhos Futuros

A estruturação de um plano efetivo de segurança da informação na organização passa não pelo tratamento dos incidentes de segurança, mas também da execução proativa de medidas evitem ou reduzam sua ocorrência. Este artigo apresentou a estruturação do Processo de Gestão de Vulnerabilidades na UFBA, como um mecanismo efetivo para auxiliar o time de segurança e trazer grandes resultados positivos. A partir da adoção desse processo, foi possível constatar uma redução de cerca de 30% na quantidade de incidentes, cujos dados poderiam comprometer o negócio e a imagem da organização.

Infelizmente não há solução geral para todos os cenários e contextos. Portanto, a organização deve estar atenta que a gestão de vulnerabilidades não é apenas a instalação de uma ferramenta ou a contratação de uma consultoria, mas sim a execução e gestão de um processo que, a partir do ciclo PDCA, evolui e consolida-se em todas as equipes.

Como trabalhos futuros, espera-se consolidar os indicadores da gestão de vulnerabilidades, para apoio na tomada de decisão da alta gestão e para auxílio, por exemplo, na contratação de produtos ou priorização de projetos na área de SIC. Além disso, já está em andamento a incorporação da gestão de vulnerabilidades junto ao processo de desenvolvimento de software da UFBA, agregando análise de segurança desde as fases de levantamento de requisitos.

Referências

ISO/IEC (2013). ISO 27002: 2013. *Information Technology-Security Techniques-Code of Practice for Information Security Management. ISO*.

Palmaers, T. (2013). Implementing a vulnerability management process. *SANS Institute Reading Room*. `http://goo.gl/pSdpN3`.