IPS UFRGS: A implementação de bloqueios automáticos progressivos integrada ao Sistema de Registro de Estações da UFRGS

Marcos Straub, Arthur Boos, Caciano Machado, Leandro Rey, Fernando Macedo, Marcio Pohlmann

TRI - Time de Resposta a Incidentes de Segurança da
Universidade Federal do Rio Grande do Sul
Centro de Processamento de Dados
Rua Ramiro Barcelos, 2574 - Portão K – Porto Alegre – RS – Brasil

{marcos,boos,caciano,leandro,fmacedo,marcio}@cpd.ufrgs.br

Resumo. *O crescimento da rede da UFRGS nos últimos anos e o consequente aumento do número de dispositivos conectados levou os incidentes de segurança a níveis que inviabilizam o seu tratamento manual. Visando um processamento automático dos bloqueios para mitigação de incidentes de forma rápida e sem uso de um operador, foi expandida a atuação do IPS (Intrusion Prevention System) da UFRGS para agir também na rede interna, totalmente integrado ao SRE (Sistema de Registro de Estações da UFRGS). Com essa integração, consegue-se fazer um tratamento adequado, baseado nas informações providas pelo SRE. O IPS foi configurado de forma a implementar-se um sistema de bloqueios temporários e progressivos, onde os próprios usuários podem tentar resolver o problema antes do bloqueio se tornar definitivo. Este trabalho mostra como a UFRGS conseguiu que mais de 90% dos incidentes de violação da política de uso da rede (principalmente devido ao uso de programas de compartilhamento de arquivos peer-to-peer) fossem resolvidos pelos próprios usuários finais, aumentando a cultura de segurança e sem necessidade de entrar em contato com a equipe de suporte.*

1. Introdução

A UFRGS conta atualmente com mais de 14.000 computadores ativos na sua rede, que geram uma quantidade considerável de incidentes de segurança. O tratamento manual desses incidentes é uma tarefa bastante trabalhosa, o que levou o TRI (Time de Resposta a Incidentes da UFRGS) a estudar uma solução para automatizá-lo.

A solução baseia-se em um IDS (*Intrusion Detection System*), implementado com o software Snort, configurado com um conjunto de regras selecionadas pela sua frequência de "*matches*" e pela sua reputação (não ocorrência de falsos-positivos). Essa medida tornou o tratamento de incidentes muito mais ágil e menos oneroso para os operadores. O tráfego de *torrents* e outros softwares de compartilhamento de arquivos via *peer-to-peer*, não permitidos na rede da UFRGS, também foram bloqueados pelo IPS, uma vez que a utilização desse tipo de software é considerada violação da política de uso aceitável dos recursos da instituição.

Esse documento irá abordar as principais dificuldades enfrentadas pelo TRI que

motivaram a implementação do sistema. A seguir, será apresentada a solução adotada, abordando seus elementos, funcionamento e operação. Por fim, serão mostrados os resultados obtidos e algumas considerações finais.

2. O Problema

Durante os últimos anos, o número de dispositivos com acesso à Internet tem aumentado consideravelmente na rede da UFRGS. Iniciativas como a expansão das vagas da universidade e o aumento de dispositivos com capacidades de acesso à rede sem fio, tais como os *smartphones*, colaboraram para esse crescimento.

Para atender essas necessidades de acesso, o CPD da UFRGS trabalhou para tornar o gerenciamento da sua rede *wireless* mais robusto [Tonin et al. 2008]. Contudo, com a ampliação da rede da universidade, aumentou também o número de incidentes, pois nem sempre os usuários tem uma preocupação mínima com a segurança de seus recursos computacionais.

Este novo cenário exige que o tratamento de incidentes seja reformulado para atender à nova demanda, considerando que recursos para contratação de profissionais nem sempre são uma possibilidade.

2.1. O Antigo Sistema de Tratamento de Incidentes

O sistema de tratamento de incidentes anterior funcionava de maneira diferenciada para os bloqueios internos. Quando um IP da universidade era detectado no IDS, ele não era bloqueado automaticamente, ficando a cargo do TRI fazer os bloqueios. O IPS UFRGS somente funcionava para os bloqueios externos. Estes eram propagados imediatamente no *firewall*, de forma a conter ataques oriundos da Internet. A figura 1 abaixo ilustra o processo.

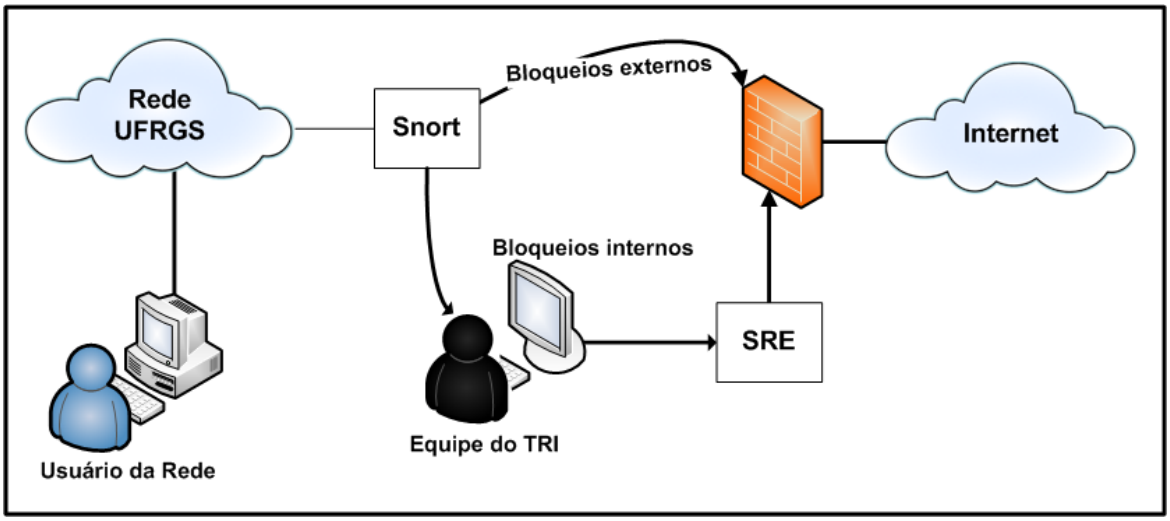

Figura 1. Sistema antigo de tratamento de incidentes

Quando ocorriam eventos de segurança relacionados a IPs internos, era

necessário que a equipe do TRI fizesse uma triagem. O analista utilizava uma série de recursos auxiliares como, por exemplo, os *flows* e o *prewikka* (interface de visualização de alertas), para coletar evidências e verificar a criticidade do ataque informado pelo IDS.

Depois de avaliado, o incidente era registrado no SRE (*Sistema de Registro de Estações)* [Machado et al. 2009] com todas as informações obtidas no processo de triagem (tipo de incidente, horário, comentários, etc). Assim que o bloqueio era efetuado, o usuário da rede era alertado através do redirecionamento das suas requisições HTTP para uma página com informações do bloqueio. Essa página continha informações obtidas do SRE, como por exemplo, o ramal da equipe de suporte específica. Essa equipe tem a responsabilidade de auxiliar o usuário a resolver o problema e efetuar o desbloqueio. Essas ligações acabam sendo um problema para alguns usuários que não se sentem à vontade para entrar em contato com o suporte e acabam adiando esse contato. Como cada um desses incidentes demanda que o usuário entre em contato, acaba causando uma grande carga no atendimento.

O maior problema dessa forma de tratamento de incidentes é o grande tempo de resposta. Como a contenção para IPs internos era feita exclusivamente de forma manual, muitas vezes os incidentes não eram tratados com a agilidade necessária, o que aumentava a probabilidade de outros computadores serem afetados pelo *malware*.

Após o usuário entrar em contato e providenciar a solução, era necessário monitorar se o incidente havia sido realmente resolvido. O usuário envia um relatório do antivírus para atestar a remoção do *malware*, mas esses nem sempre correspondem ao evento detectado pelo IDS. Nesses casos, o computador poderia ser desbloqueado pela equipe de suporte, mas como o problema não foi realmente resolvido, o incidente acabaria sendo reaberto. Em alguns casos, um usuário mal intencionado pode mentir sobre a solução do incidente, o que aumenta a dificuldade para resolvê-lo.

Outro tipo de incidente que necessita de uma resposta rápida é o uso de softwares de compartilhamento de arquivos do tipo *peer-to-peer*. O uso desse tipo de software acaba sendo usado predominantemente para fazer o download de arquivos protegidos por direitos autorais, o que é inadmissível na rede da universidade.

Devido aos problemas listados, tornou-se necessário que o IPS UFRGS fosse ativado também na rede interna e reformulado, para que os bloqueios automáticos não causassem uma grande carga no atendimento de suporte. Para atender a essas necessidades, foi desenvolvida uma nova modalidade de bloqueio interno: o bloqueio temporário.

3. Arquitetura do IPS com Bloqueios Temporários e Definitivos

O sistema de IPS é utilizado na proteção da rede da UFRGS, efetuando bloqueios de forma automática. Atua no *firewall* de borda da rede, e está integrado aos sensores IDS, instalados em pontos chave da rede interna. Baseado nos alertas recebidos, esse sistema efetua bloqueios de forma automática, podendo esses serem realizados em caráter definitivo ou temporário, cuja duração é pré-configurada em função do tipo de alerta recebido.

Até o final do ano passado, o IPS processava apenas incidentes com origem

em redes externas. A partir de janeiro deste ano, o processo foi expandido para efetuar bloqueios em computadores internos, inicialmente devido a violações de política de uso adequado da rede, mais especificamente a utilização de software de compartilhamento de arquivos via *peer-to-peer* e, mais recentemente, por *malware*.

No novo sistema, o funcionário do TRI deve se preocupar em fazer a alimentação das regras que serão automatizadas, ao invés de fazer somente a triagem dos incidentes (figura 2). Assim que o IPS tiver informações suficientes, ele poderá interagir diretamente no SRE e no *firewall,* para efetuar os bloqueios de segurança.

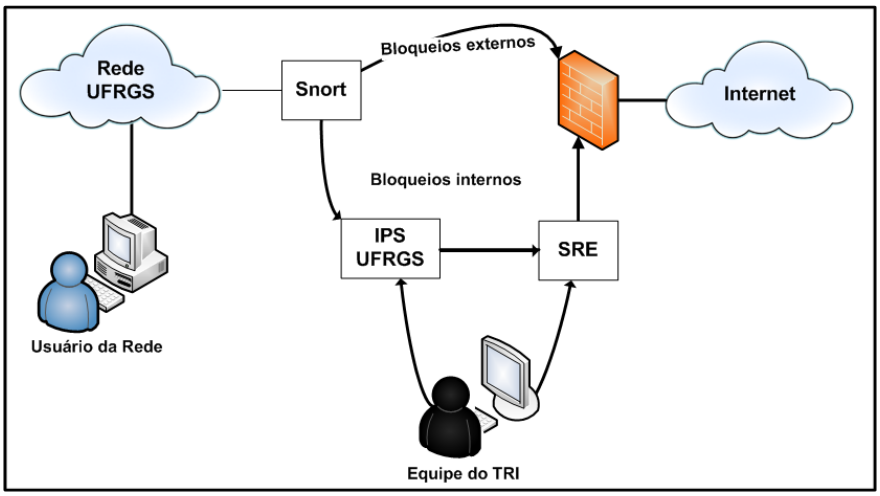

Figura 2. Sistema de bloqueios automáticos integrado ao SRE

O IPS da UFRGS é baseado no software SnortSAM, que é constituído pelos módulos cliente (*plug-in*) e servidor (agente). O cliente foi incorporado ao software Barnyard2, que recebe os alertas oriundos do Snort e envia as diretivas de bloqueio para o agente, na estação de gerência, de acordo com parâmetros pré-estabelecidos. O agente, após receber essas diretivas, prepara e envia os comandos adequados para o *firewall*. O próprio agente gerencia automaticamente os desbloqueios, quando o tempo de bloqueio expira.

3.1. Sistema de Detecção e Geração de Alertas

A estrutura de sensores é distribuída e totalmente baseada em software livre. Atualmente, são processados apenas os alertas enviados por sensores utilizando o Snort. Os demais sensores, como os do nosso sistema de *honeypots*, ainda precisam de uma maior integração ao IPS, para que seus alertas possam ser devidamente processados.

O processamento dos alertas relacionados a computadores internos começa com a escolha cuidadosa dos alertas que deverão gerar bloqueios. O identificador do alerta (SID) é então configurado, especificando-se o tempo de bloqueio e se o IP a ser considerado é o de origem ou destino. Esses parâmetros é que vão fazer com que o Barnyard2 determine quais alertas devem gerar bloqueio, qual o IP a ser bloqueado e por quanto tempo.

Além dos alertas, é preciso fazer uma seleção criteriosa das redes que ficarão

submetidas ao IPS. Para isso, pode ser empregado o uso de *whitelists* de modo a impedir que a rede do *datacenter*, ou um servidor, sejam bloqueados, por exemplo.

3.2. Modalidades de Bloqueio e as Métricas de Progressividade

No novo sistema existem duas modalidades de bloqueio: os temporários, que são automaticamente desbloqueados quando o tempo expira e os definitivos, que só podem ser desbloqueados depois do usuário entrar em contato com a equipe de suporte a incidentes de segurança.

A rigor, todos os bloqueios passaram a ser temporários. Depois que um determinado incidente ultrapassa um certo número de reincidências, o bloqueio torna-se definitivo. Esse tipo de medida é necessária, pois o usuário poderá necessitar de auxílio para a resolução do problema ou ele não está dando a atenção necessária ao problema. Nesses casos, dependendo do caráter e frequencia dos bloqueios, estes progridem de temporários para definitivos.

Para definir a progressividade, o IPS UFRGS precisa que algumas métricas sejam cadastradas. Para cada alerta passível de gerar um bloqueio (SID), são estabelecidos o tempo de duração do bloqueio, o número de vezes que esses bloqueios temporários podem acontecer antes de se tornarem definitivos e a janela de tempo na qual serão buscados os incidentes anteriores. Por exemplo, um usuário pode ser bloqueado temporariamente por três vezes de quinze minutos cada, durante um mês. Se ele exceder esse limite, o bloqueio será transformado em definitivo.

3.3 SRE UFRGS e o Registro de Incidentes

O Sistema de Registro de Estações da UFRGS foi desenvolvido para facilitar as tarefas de gerência dos dispositivos que ingressam na rede da Universidade [Machado et al. 2010]. O SRE mantém não só as bases de dados com os registros dos equipamentos na rede, mas também uma base com os dados de incidentes de segurança.

Durante a fase em que o bloqueio é temporário, o incidente é registrado, mas não é criado um *ticket* de acompanhamento. Somente são inseridas no banco de dados de incidentes do SRE informações como hora, tipo de incidente, IP e MAC, para que o IPS UFRGS tenha informações necessárias para verificar se é preciso efetuar a progressividade no bloqueio. Além do bloqueio no firewall, quando o usuário tenta navegar na Internet é feito o redirecionamento para uma página informativa, onde são mostrados os motivos do bloqueio e o tempo que ainda falta para o IP ser liberado (figura 3). Quando o usuário for bloqueado definitivamente, é criado também um *ticket* do incidente e encaminhado à equipe de suporte para ser tratado. A página informativa que é mostrada ao usuário, descrita anteriormente, é modificada, de modo a conter informações mais específicas e orientações de como proceder para resolver o problema.

A página de bloqueio é um elemento de grande importância na abordagem utilizada. Se as informações contidas nela forem suficientes para que o usuário consiga entender o problema e tratar o incidente sem muitas dificuldades, será bem menos provável que um bloqueio chegue a ser definitivo. A página precisa deixar claro quando um bloqueio é temporário e quais as medidas que ele precisará tomar para resolvê-lo o mais rápido possível. No entanto, preencher a página com informações muito técnicas irá frustrar o usuário mais leigo. Portanto, é preciso fazer um acompanhamento para

verificar a eficiência das informações contidas para se ter a menor taxa de bloqueios definitivos possível.

Figura 3. Tela informativa de bloqueio temporário

4. Resultados Alcançados

Ao estender a atuação do IPS à rede interna da universidade, a expectativa inicial era agilizar a contenção de determinados tipos de incidentes e reduzir o trabalho no processo. Foi necessário um certo tempo de testes e ajustes, até que se pudesse chegar a um conjunto aceitável de regras, que permitisse efetuar bloqueios de forma confiável e com uma taxa mínima de falsos positivos.

Os falsos positivos foram tratados com muito cuidado na implementação do trabalho. Eventos como esses, por menos frequentes que sejam, afetam muito na credibilidade do IPS. Com isso em mente, a equipe TRI foi bastante criteriosa ao incluir novas assinaturas no sistema, garantindo assim uma taxa de falsos positivos bem próxima de zero.

A página de bloqueio foi um dos elementos do sistema que sofreu a maior quantidade de ajustes. Primeiramente, a página mostrava a data e horário que o computador seria desbloqueado. No entanto, muitos usuários acabavam ligando para o TRI, pois não haviam percebido que a data de desbloqueio era apenas poucos minutos no futuro. Desse modo, foi adicionado à data um contador de minutos (ou horas), tornando a informação do momento de desbloqueio mais clara e assim diminuindo o número de usuários confusos. Outra mudança importante foi não deixar a informação do ramal para contato em evidência. Os usuários acabam vendo o ramal e ligando sem mesmo ler as informações que lhe eram apresentadas..

Outro ponto importante são os ajustes nas métricas de bloqueio definitivo. Se for

concedido pouco tempo de bloqueio temporário ao usuário, ele acabará ligando, pois não conseguiu resolver em tempo. Se for dado tempo demais, pode dar margem para o usuário negligenciar o incidente. Portanto, é necessário sempre avaliar o tempo de resposta dos usuários na resolução dos eventos sempre que for ativada uma nova assinatura. Alguns eventos podem levar mais tempo para ser solucionados do que outros. São esses ajustes, juntamente com as informações da página de bloqueio, que irão garantir a eficiência do sistema.

Desde a ativação do IPS, em termos proporcionais, o número reduzido de bloqueios que progrediram à fase definitivos foi caindo rapidamente. Além dos ajustes nos tempos de bloqueio, esse decréscimo mostra um grande envolvimento do usuário final na solução dos problemas (figura 4).

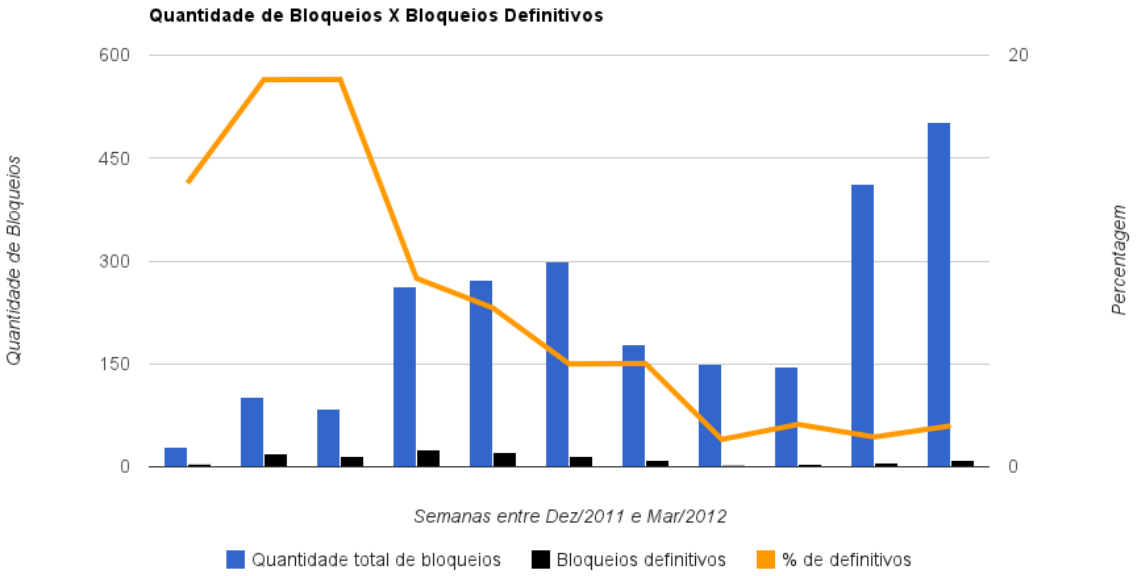

Figura 4. Bloqueios efetuados pelo IPS UFRGS

Além disso, apesar do aumento na quantidade de incidentes no início do semestre, houve um aumento ínfimo na taxa de bloqueios definitivos (figura 4). Isso sugere que o sistema de bloqueios temporários, ao proporcionar uma participação ativa do usuário na solução do problema, teve também um impacto positivo na questão da sua conscientização em termos de segurança da informação e das políticas de uso vigentes.

Outro aspecto resultante desse processo é que ele permite que o próprio usuário saiba quase que de imediato se as suas ações efetivamente resolveram o problema, reduzindo a necessidade de monitoração e, consequentemente, a carga de trabalho da equipe de segurança.

Um problema que IPS UFRGS tem enfrentado é o uso de NAT nas unidades. Apesar de desaconselhado pelo CPD, existem diversos setores e muitas bases *wireless* com essa configuração. O NAT inviabiliza a identificação do causador do incidente e todos os usuários que estejam atrás de um desses equipamentos acabam prejudicados, quando é feito o bloqueio. Nesses casos, o TRI precisa avaliar o impacto que esses

bloqueios terão e auxiliar os gerentes de rede das unidades a considerar iniciativas para remover o NAT.

5. Considerações Finais

É relativamente fácil implementar um sistema de IPS, atuando na borda da rede e efetuando bloqueios de IPs externos. Desafio maior e bem diferente, é fazer o IPS atuar na rede interna, onde o impacto resultante de um bloqueio indevido a um servidor ou onde um elevado número de falsos positivos pode rapidamente inviabilizar essa solução. Desde a seleção e testes de novas regras que irão gerar os bloqueios, até a criteriosa elaboração das *whitelists*, onde estarão os IPs dos servidores e dos equipamentos críticos da infraestrutura de rede, são necessários cuidados e planejamento adequados. Particularidades da rede, tais como utilização de NAT, já mencionado, também devem ser levados em conta.

Apesar de se ter obtido resultados bastante satisfatórios com o IPS atuando na rede interna da UFRGS, ainda há muito por fazer. Os bloqueios atualmente são efetuados apenas no firewall de borda, bem longe do ideal, que seria garantir que o equipamento bloqueado seja isolado da rede local. O IPS é apenas mais uma linha de defesa, em termos de segurança da informação. É necessário também efetuar ações que reduzam efetivamente os incidentes de segurança, tais como, por exemplo, investimentos em treinamento de usuários.

Referências

Machado, C., Soares, D., Rey, L., Ziulkoski, L., Tonin, R., Marchezan, C., Postal, E., Horowitz, E. (2009). **Implantação do Sistema de Registro de Estações da UFRGS.** III Workshop de Tecnologia da Informação das IFES, Belém - PA.

Tonin, R., Machado, C., Postal, E., Rey, L., Ziulkoski, L. (2008). **Sistema de Gerenciamento de Redes Wireless da UFRGS.** II Workshop de Tecnologia da Informacao das IFES, Gramado - RS.

Ceron, J., Rey, L, Boos, A., Machado, C., Macedo, F., Bringhenti, F., Pohlmann, M. (2010) **Sistema de Registro de Estações da UFRGS como Ferramenta de Segurança.** IV Workshop de TI das IFES, Rio de Janeiro - RJ.