Uso de Captive Portal
nas Casas do Estudante da UFRGS

Fernando D. F. Macedo, Caciano dos S. Machado, Marcio Pohlmann,

Leandro F. Rey, Marcos S. Nascimento, Arthur B. Júnior

Centro de Processamento de Dados - Universidade Federal do Rio Grande do Sul

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

1. Introdução

A UFRGS possui três Casas do Estudante que servem de alojamento estudantil. Em cada uma das Casas, CEU, CEUFRGS e CEFAV, existe uma Comissão de Informática, responsável pelos recursos computacionais. Todavia, nessas redes não existia um controle automatizado na atribuição dos endereços IP e na identificação de usuários, o que acabava dificultando o tratamento dos incidentes de rede e de segurança. A seguir, apresentaremos a motivação para a implantação do sistema de *Captive Portal* para as Casas do Estudante, como o sistema funciona e a nossa experiência com a implantação.

2. O Captive Portal nas Casas do Estudante

Antes da implantação do sistema, o gerenciamento dos endereços IP nas redes das Casas do Estudante era realizado pelas Comissões de Informática, compostas e definidas pelos próprios moradores. Porém, o controle manual dos endereços era trabalhoso e complexo, e o bloqueio por casos de *malware* e violação da política de uso da rede levavam os usuários a atribuir endereços IP arbitrários aos seus dispositivos quando não conseguiam contatar a comissão responsável. Muitas vezes, esses endereços já estavam sendo utilizados por outros usuários, gerando conflitos de IP. Além disso, os usuários, ao terem os seus IPs bloqueados, trocavam de endereço para algum IP sem incidente ativo, o que dificultava muito o tratamento desses incidentes.

As redes das Casas dos Estudantes diferem das outras redes da Universidade, pois há uso constante durante as 24 horas do dia. Devido a essa peculiaridade, as redes das casas foram as primeiras a adotar os mecanismos de bloqueios automáticos e temporários [Straub et al. 2012] desenvolvidos pela equipe de segurança. Esse sistema permite que os usuários possam resolver os incidentes de baixa severidade sem a intervenção da equipe, que está disponível apenas em horário comercial. Posteriormente, esse mecanismo foi estendido para toda a rede institucional.

As principais ferramentas que compõem o sistema de *Captive Portal* implantado são: Coova Chilli (*software* de autenticação à rede e serviço de DHCP); Apache (servidor *Web* com a página de autenticação); Freeradius (responsável pela autenticação do usuário). Para fazer o seu acesso à rede, o usuário é redirecionado pelo *Captive*

Portal para uma página *Web* de autenticação. A autenticação é realizada através das credenciais institucionais do usuário da UFRGS ou através de um tíquete de acesso. Os tíquetes de acesso são credenciais temporárias concedidas a usuários sem vínculo com a Universidade e solucionam os casos de estudantes que permanecem na Casa após a sua formatura, além de vestibulandos e intercambistas.

Com a implantação do sistema, não é mais possível utilizar a rede de forma anônima, pois é necessário o uso das suas credenciais para acesso à rede. Dessa forma, a ocorrência de incidentes de segurança ativos foi reduzida. Um dispositivo bloqueado, mesmo que mude o seu endereço IP, ficará com tráfego limitado à rede local, além de incentivar a autonomia dos usuários para resolução dos incidentes.

A solução levou, naturalmente, a uma limitação na largura de banda das redes que anteriormente não existia. Inicialmente, ela foi limitada a 1 Mbps para cada usuário, posteriormente sendo aumentada para 2 Mbps, fato que foi questionado pelos moradores. Observamos, entretanto, que o uso médio por usuário é de até 250 Kbps e portanto que a limitação teria impacto mínimo, o que foi compreendido pelos moradores. O número máximo de usuários observado foi de 212 usuários, com 161 usuários autenticados.

3. Considerações Finais

A implantação do *Captive Portal* nas redes das Casas do Estudante da UFRGS aumentou a segurança, organização e administração dessas redes. A implantação forneceu a experiência necessária para a adoção dos bloqueios automáticos e temporários em toda a rede da UFRGS. Verificou-se que eles ajudam os usuários de maneira eficaz a solucionar incidentes de segurança, além de incentivar a conformidade com as políticas institucionais de uso da rede de dados. A cooperação das Comissões de Informática das Casas do Estudante da UFRGS foi fundamental para o sucesso do projeto.

Referências

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

Straub, M., Boos, A., Machado, C., Rey, L., Macedo, F., Pohlmann, M. (2012) **IPS UFRGS: A implementação de bloqueios automáticos progressivos integrada ao Sistema de Registro de Estações da UFRGS.** 1º Fórum Brasileiro de CSIRTs - São Paulo - SP.