Recomendação de Segurança 004/2012 - CGTI/VPGDI

Em 18 de Dezembro de 2012

Para: Gestores de TI das unidades da Fiocruz
Assunto: Segurança em Redes Wireless

Visando a implementação de ações de segurança da informação com o objetivo de reduzir riscos operacionais em relação ao acesso ou recuperação indevida das informações trafegadas por meio de redes sem fio, faz-se necessário implementar mecanismos que garantam a autenticidade, confidencialidade e a integridade dos dados trafegados. Vale ressaltar que no *War Driving* não se executa qualquer atividade intrusiva e todas as atividades realizadas estão em conformidade com a legislação em vigor.

Sendo assim, com base nas boas práticas de mercado, o Serviço de Segurança da Informação e Comunicações recomenda que:

1) **Segmentação a rede**: segmentar a rede de forma que a rede corporativa utilizada pelos equipamentos dos funcionários não seja a mesma acessada por terceiros (alunos, visitantes, etc.).
2) **Proteção física:** alguns Access Points (AP) possuem uma opção de *reset* físico que faz com que todas as configurações de fábrica sejam recarregadas. Nesses casos, é muito importante que o AP fique em um local com acesso físico controlado.
3) **Autenticação dos AP**: alterar a senha administrativa dos equipamentos, para uma senha segura, com base em uma senha forte (letras, números e caracteres especiais).
4) **Atualização de Firmware**: manter atualizado o firmware dos equipamentos, mantendo-os livres de falhas conhecidas.
5) **Modos de configuração**: a maioria dos AP permite vários meios de configuração: HTTP, SNMP, SSH, Telnet, etc. Sempre que possível, é importante desabilitar os que não forem necessários e optar por um modo de configuração que não seja pela própria rede *wireless*, mas sim pela rede cabeada ou ainda via conexão serial. Isso minimiza as chances de que a sessão de configuração com o AP seja capturada por algum cliente *wireless*.

6) ***Broadcast* de SSID:** sempre que possível, desabilite o *broadcast* de SSID pelo AP. Embora seja uma medida simples, pode dificultar o uso de alguns programas populares de mapeamento de redes *wireless*.

7) **Filtragem por endereço MAC:** alguns AP possuem o recurso de filtragem de clientes *wireless* por endereço MAC. Embora endereços MAC possam ser forjados e muitas vezes não seja prático manter uma lista de endereços MAC dos clientes autorizados (e em alguns casos inviável, como em conferências), deve ser considerado sempre que possível, mantendo assim um cadastro dos hosts e dos seus respectivos MAC *address*.

8) **Autenticação e criptografia**: recomendamos que não utilizem WEP (Wired Equivalent Privacy), devido facilidade de ataques conhecidos a este protocolo. E aconselhamos que utilizem WPA2 (*Wi-Fi Protected Access*) com autenticação 802.1X - 802.11i. Se houver dispositivos clientes ou pontos de acesso incapazes de suportar o WPA2, procure realizar atualizações de firmware ou se possível substitua esses equipamentos. O modo de chave pré-partilhada (PSK ou *Pre- Shared Key*) do WPA ou do WPA2 não é seguro para ambientes empresariais. Pois quando se usa este modo, a mesma chave tem de ser inserida em cada dispositivo cliente. Utilizando o modo EAP (*Extensible Authentication Protocol*) do WPA e do WPA2 utiliza-se autenticação 802.1X em vez de chaves PSK, assim há a possibilidade de dar a cada usuário ou cliente as suas próprias credenciais de login: nome de usuário e senha e/ou um certificado digital, sendo possível integrar esta autenticação a uma base de usuários existente como no caso de uma rede que utiliza servidores de domínio *Active Directory* utilizando serviços nativos que permitam a autenticação utilizando RADIUS aos APs.

Atenciosamente,

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações