NORMA TÉCNICA
ATI-SGR-PR/001.2:09

Norma de Segurança para Uso de Rede Sem Fio

Versão 1.0

Válida a partir da publicação da Resolução 002/2009

Palavras-chave: Segurança, Rede, Sem Fio, Ponto de Acesso.

Ati
Agência Estadual de Tecnologia da Informação

21 páginas

Sumário

Prefácio

A ATI – Agência Estadual de Tecnologia da Informação – é o órgão de coordenação e suporte técnico ao Sistema Estadual de Informática do Governo – SEIG – e que tem como atribuições propor e prover soluções integradoras de meios, métodos e competências, com uso intensivo e adequado da Tecnologia da Informação e Comunicação.

Esta Norma foi elaborada pela Unidade de Segurança da Informação – USI – da ATI com o apoio da Unidade de Data Center – UDC, redigida em conformidade com as convenções redacionais estabelecidas pela ATI e segundo os padrões nacionais e internacionais atualmente utilizados [1] [2] [3] [7].

Esta Norma é parte integrante da Política de Segurança da Informação da ATI [4], podendo vir a ser substituída ou conviver junto às demais normas de segurança futuramente elaboradas.

Esta Norma foi aprovada pela Diretoria-Executiva de Tecnologia da Informação e Comunicação da ATI (DTI) e entra em vigor na data da publicação da Resolução 006/2009.

1 Escopo

Esta Norma visa ao estabelecimento de regras de segurança para disciplinar a implantação e o uso de redes sem fio no ambiente de rede corporativo das organizações, a fim de prevenir possíveis incidentes de segurança, tais como o acesso indevido à rede e às suas funcionalidades, furto ou violação de integridade da informação e dos serviços da rede e vandalismo, este último no que se refere à destruição de dados disponíveis nos serviços da rede.

As regras estabelecidas nesta Norma estendem-se a todos os usuários dos recursos computacionais, incluindo empregados, servidores, cargos em comissão, terceirizados, estagiários, prestadores de serviços e os que, de alguma forma, fazem uso dos recursos de rede da organização.

2 Termos e definições

Para os efeitos deste documento, aplicam-se os seguintes termos e definições:

1.1

AES – *Advanced Encription Standard*

sistema de criptografia bastante complexo e capaz de prover confidencialidade e integridade dos dados. Atualmente, é o algoritmo de criptografia internacionalmente aceito e adotado como padrão para sistemas de segurança [12]

1.2

criptografia WPA2 – *Wi-Fi Protected Access 2*

recurso de criptografia para redes do tipo Wi-Fi, compatível com o padrão IEEE 802.11 (ver 1.7.1.1), que devido aos aspectos de segurança tratados tornou-se mais indicado que sua versão anterior (WPA) e que o protocolo de segurança WEP – *Wired Equivalent Privacy* – prescrito pelo padrão 802.11

1.3

DHCP – *Dynamic Host Configuration Protocol*

protocolo que oferece configuração dinâmica de terminais com concessão de endereços IP (*Internet Protocol*) de *host* e outros parâmetros de configuração para clientes de rede

1.4

Firewall

mecanismo que atua como uma barreira de proteção entre duas ou mais redes, de modo a regular, por meio de regras e a filtragem de dados, o tráfego de dados entre essas redes e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra

1.5

Firmware

software proprietário que controla diretamente o hardware do equipamento. Esse software é armazenado diretamente no *chip* de memória tais como ROM (*Read Only Memory*), *EPROM* (*Erasable and Programable ROM*) e memória flash. Alguns fabricantes de equipamentos fornecem atualizações desse tipo de software

1.6

host

ou cliente, é qualquer máquina ou computador conectado a uma rede que se beneficia de um serviço oferecido por esta

1.7

IEEE – *Institute of Electrical and Electronics Engineers*

criado em 1884, nos E.U.A., a IEEE é uma sociedade técnico-profissional internacional, dedicada ao avanço da teoria e prática da engenharia nos campos da eletricidade, eletrônica e computação [8]

1.7.1

Padrão 802

norma da IEEE que tem como objetivo definir uma padronização para redes locais, nas suas camadas 1 e 2, segundo o modelo OSI. Desse, derivam-se diversos padrões específicos para redes com cabos metálicos, óticos e sem fio. Entre os padrões derivados, designados ao meio físico sem fio destacam-se o 802.11, 802.15 e 802.16.

1.7.1.1

Padrão 802.11

utilizado para conexões sem fio para empresas e residências, doutrinariamente classificado como redes do tipo WLAN (*Wireless Local Area Network*) e comumente chamado de rede Wi-Fi. O padrão IEEE 802.11 [9] também subdivide-se em padrões que especificam características técnicas da transmissão por ondas de rádio. Os destaques são: 802.11a, 802.11b, 802.11g e 802.11n.

1.7.1.2

Padrão 802.15

utilizado para dispositivos que possuem conexão de curta distância, geralmente utilizadas por dispositivos pessoais e com pouco volume de tráfego. Destaca-se a tecnologia conhecida como bluetooth. Esse padrão é doutrinariamente classificado como redes do tipo WPAN (*Wireless Personal Area Network*).

1.7.1.3

Padrão 802.16

doutrinariamente classificado como redes do tipo WMAN (*Wireless Metropolitan Area Network*), são utilizados para conexões sem fio de longa distância, geralmente abrangendo áreas como metrópoles. Um exemplo é a rede chamada WiMax.

1.8

Log

termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de *log* pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais

1.9

Ponto de Acesso

do inglês Access Point ou simplesmente AP. É um equipamento que realiza a interconexão entre todos os dispositivos que fazem parte de uma rede sem fio.

Em geral se conecta a uma rede cabeada servindo de ponto de acesso para uma outra rede, como por exemplo, a Internet

1.10

Proxy

servidor que atende a requisições repassando os dados a outros servidores ou requisitantes. Dentre suas inúmeras funções, no quesito segurança, o *proxy* é usado como filtro de conteúdo, impedindo o acesso a conteúdo proibido pela política de segurança da organização

1.11

SSID – *Service Set Identifier*

identificador de uma rede sem fio. Normalmente usado no momento da conexão, no qual o cliente localiza as redes sem fio disponíveis e escolhe a que ele quer realizar a conexão por meio do SSID

1.12

VLAN – *Virtual LAN*

termo em inglês para Redes Locais Virtuais. É uma rede logicamente independente criada a partir de uma segmentação lógica da rede local

1.13

VPN – *Virtual Private Network*

termo em inglês para Rede Particular Virtual. É uma rede de comunicação privada construída sobre uma rede pública, por exemplo, a Internet. VPN's consideradas seguras utilizam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a

privacidade das comunicações requeridas. Quando adequadamente implementados, esses protocolos podem assegurar comunicações seguras em redes consideradas inseguras.

3 Normas

3.1 Disposições Gerais

As normas abaixo relacionadas trazem como premissa básica o conceito de que tudo o que não for permitido e/ou liberado é considerado violação à Política de Segurança da Informação da ATI [4].

Salienta-se que, em virtude de ser a segurança da informação um processo contínuo e de estar a ATI em pleno processo de elaboração e implantação de sua Política de Segurança da Informação, novas normas e possíveis alterações de versão estarão sendo implementadas. Neste último caso, revogando-se, automaticamente, a norma anterior, devendo, portanto, todos os que fazem uso dos recursos computacionais da ATI, em especial àqueles que fazem uso da rede local sem fio, manterem-se atualizados e obedientes às normas em vigor que serão disponibilizadas pela ATI para fins de conhecimento.

Ressalta-se que, primordialmente, todos os que necessitem de acesso aos recursos de rede da ATI, deverão, como requisito básico, ter assinado o “Termo de Responsabilidade” [5], comprometendo-se à estrita observância e obediência às condições e requisitos básicos para o acesso aos recursos computacionais da ATI, cujo descumprimento incorrerá nas penalidades cabíveis de acordo com a infração cometida e penalidades previstas em legislação competente.

Ademais, o acesso à Internet e/ou corporativo por meio de rede sem fio na ATI,

implica na devida subordinação às demais normas que compõem a política de segurança da ATI, pelo usuário.

Neste momento, são abordados apenas os aspectos de segurança do padrão 802.11 (ver 1.7.1.1), embora o padrão IEEE 802 (ver 1.7.1) defina também outros padrões específicos (ver 1.7.1.2 e 1.7.1.3).

A utilização de redes sem fio permite mobilidade e independência de infraestrutura cabeada, sobretudo para os pontos clientes (ver 1.6). Entretanto, faz-se necessário o uso de recursos de segurança de forma a garantir não apenas a restrição de acesso à infraestrutura, mas também, os demais requisitos de segurança da informação: confidencialidade, autenticidade, integridade e disponibilidade, especialmente quando se trata de acesso aos recursos corporativos.

3.2 Ambiente corporativo

A implementação de uma rede sem fio corporativa no ambiente da organização deverá atender aos seguintes requisitos de segurança:

a) a solução de rede sem fio corporativa deverá seguir os padrões de mercado recomendados (ver 1.7) e estar de acordo com as normas estabelecidas neste documento, devendo para tanto, existir um projeto elaborado por uma equipe técnica especializada, que deverá estudar também as peculiaridades do ambiente, o raio de cobertura do sinal de rádio, a velocidade da conexão, a especificação dos equipamentos e seus recursos de segurança e demais itens necessários à implantação da solução;

b) os pontos de acesso (ver 1.9) deverão ser conectados aos ativos de rede da rede local atendendo ao raio de cobertura da solução, porém, sob uma VLAN (ver 1.12) específica para este fim, com faixa de endereços IP's inválidos e distintos aos da rede local corporativa, de forma a evitar que os recursos corporativos estejam sob riscos de segurança;

c) os pontos de acesso deverão estar dispostos em locais físicos que não permitam ou, ao menos, intimidem ou desestimulem a manipulação feita por terceiros não autorizados. Para uma melhor proteção do equipamento, recipientes poderão ser utilizados ou adaptados para esses dispositivos, de forma que não comprometam a eficiência da transmissão de dados por ondas de rádio;

d) cada ponto de acesso deverá ter seu *firmware* (ver 1.5) sempre atualizado, de maneira a evitar invasões por brechas no seu sistema de configuração;

e) os pontos de acesso deverão ser configurados com criptografia forte de acordo com o padrão AES (ver 1.1) mais seguro e atual do mercado, que implementa a autenticação 802.11 (ver 1.7.1.1);

f) para fazer uso dos recursos da rede sem fio corporativa, os usuários deverão configurar seus respectivos dispositivos sem fio para usar a criptografia padrão AES (ver 1.1), conforme a alínea e) desta seção;

g) o controle de acesso à Internet e/ou corporativo por meio da rede sem fio da organização deverá ser subordinado a um *firewall* (ver 1.4). Este, por sua vez, interligará a rede sem fio à rede local, se houver, e ao servidor *proxy* (ver 1.10);

h) deverá estar habilitado, de forma integrada ao serviço de diretório ou a

algum sistema de autenticação de usuário, um serviço de autenticação remota, que permitirá o acesso à base única de usuários por qualquer etapa de autenticação, seja do ponto de acesso (ver 1.9), de uma VPN (ver 1.13) ou do domínio, sendo este último opcional;

i) os usuários ao se conectarem à rede sem fio, conforme a alínea f) desta seção, a princípio, apenas terão acesso à Internet por meio do serviço *proxy*, permanecendo, dessa forma, isolados da rede corporativa e dos recursos disponibilizados por esta. A autenticação será realizada a partir de uma base única de usuários, conforme explícito na alínea h) desta seção;

j) o acesso aos recursos corporativos da organização exigirá aos usuários, além da autenticação na rede sem fio, uma nova autenticação, dessa vez no serviço de VPN (ver 1.13), de acordo com seu enquadramento na política de acesso aos recursos da rede corporativa da organização, se houver;

k) o identificador da rede sem fio (SSID, ver 1.11) deverá ser diverso ao padrão de fábrica, portanto, deve ser substituído por outro a ser definido pela equipe técnica responsável. O recurso de publicação do SSID deverá estar habilitado para que a rede sem fio possa ser automaticamente detectada;

l) o serviço de DHCP (ver 1.3) da rede sem fio deverá estar habilitado e configurado com uma faixa de endereços IP's inválidos e distintos da rede corporativa da organização, conforme já definido na alínea b);

m) a senha de administração dos pontos de acesso integrantes da rede sem fio deverá ser diversa ao padrão de fábrica e, portanto, deverá ser

substituída por outra a ser definida pela equipe técnica responsável, conforme as recomendações de uso e formação de senhas [6]. Esta senha deve ser a mesma para todos os pontos de acesso integrantes da solução, de forma a facilitar sua administração pela equipe técnica responsável;

n) o sistema de *log* (ver 1.8) dos pontos de acesso integrantes da rede sem fio deverá ser ativado e configurado pela equipe técnica responsável a fim de viabilizar auditorias e detecção de problemas;

o) o acesso à rede sem fio deverá estar subordinado ao cadastramento prévio do usuário no serviço de diretório da rede ou outra solução que dê provimento a uma base única de usuários (ver alínea h)). ;

3.3 Ambiente não-corporativo

Consideram-se dispositivos sem fio, destinados ao uso não-corporativo, aqueles que estão dispostos fora da infraestrutura da rede local corporativa da organização.

Embora a existência desses ambientes ofereçam menos risco à estrutura corporativa de rede local, a sua utilização equivocada, no que diz respeito aos aspectos de segurança, pode implicar em risco de segurança considerável à organização.

Dessa forma, faz-se necessário o cumprimento dos seguintes requisitos de segurança:

a) a utilização de redes sem fio pelos técnicos da organização para fins de estudo e/ou domínio da tecnologia deverá ser feita de forma independente de qualquer infraestrutura de rede da organização, de forma que não exista

conexão simultânea destes com a rede local, a fim de se evitar riscos de segurança aos recursos corporativos. Além disso, os técnicos envolvidos deverão dedicar cuidados com a segurança local dos *hosts* (ver 1.6) envolvidos para que não venham a representar riscos de segurança aos recursos corporativos ao serem posteriormente conectados à rede local;

b) A Unidade de Segurança da Informação – USI, por intermédio da Gerência de Relacionamento do Governo – GRG – da ATI, deverá ser contatada para prover orientações e recomendações quanto as melhores práticas nos aspectos de segurança sobre o uso de redes locais sem fio.

4 Verificação de Conformidade

Para garantir o cumprimento das regras anteriormente mencionadas, a organização deverá utilizar os seguintes meios:

a) adoção de soluções de segurança tais como: *firewall*, serviço de autenticação, VPN, *proxy*, além da própria criptografia integrante da solução de rede sem fio;

b) a Unidade de Segurança da Informação – USI – da ATI ou setor responsável em se tratando das demais organizações, reserva-se ao direito de auditar os relatórios do acesso à Internet de cada usuário, bem como, realizar auditoria nas configurações e *logs* dos equipamentos integrantes dos ambientes de redes sem fio da organização, a fim de garantir conformidade às normas de segurança ora estabelecidas.

5 Penalidades

5.1 Disposições Gerais

O não cumprimento das normas estabelecidas neste documento (Norma de Segurança para Uso de Rede Sem Fio), seja isolada ou cumulativamente, poderá implicar, de acordo com a infração cometida, em punições conforme descritas nas seções a seguir.

5.2 Comunicação de descumprimento

a) será encaminhada, por e-mail, uma notificação ao responsável informando sobre o descumprimento da norma, com a indicação precisa da violação praticada e, em caso de reincidência, será enviada uma cópia para o superior imediato.

5.3 Advertência ou Suspensão

a) a pena de advertência ou suspensão será aplicada nos casos legais e após regular apreciação, por meio de processo administrativo disciplinar.

5.4 Demissão por justa causa

a) a pena de demissão por justa causa será aplicada nos casos legais e após regular apreciação, por meio de processo administrativo disciplinar;

b) aos funcionários enquadrados no regime de trabalho CLT (Consolidação das Leis do Trabalho), ditos “empregados”, a pena de demissão por justa causa será aplicada nas hipóteses previstas no art. 482, Parágrafo único,

da Consolidação das Leis do Trabalho, Decreto-lei nº 5.452, de 1º de maio de 1943;

c) aos funcionários enquadrados no regime de trabalho ESTATUTÁRIO, ditos “servidores públicos”, a pena de demissão será aplicada nas hipóteses previstas no art. 204, da Lei 6.123, de 20 de julho de 1968, do Estatuto dos Funcionários Públicos do Estado de Pernambuco, e nas hipóteses das penas pelo cometimento de crime contra a administração pública previstas no Decreto-Lei n° 2.848, de 7 de dezembro de 1940, do Código Penal;

d) aos funcionários sob cargo em comissão, a pena de exoneração será aplicada com base no art. 37, inciso II, da Constituição Federal, nas hipóteses previstas no art. 204, da Lei 6.123, de 20 de julho de 1968, do Estatuto dos Funcionários Públicos do Estado de Pernambuco, e nas hipóteses das penas pelo cometimento de crime contra a administração pública previstas no Decreto-Lei n° 2.848, de 7 de dezembro de 1940, do Código Penal;

e) aos funcionários terceirizados e prestadores de serviço, será solicitado à empresa prestadora da respectiva mão-de-obra, o afastamento definitivo do funcionário, podendo a organização solicitar a substituição deste ou até mesmo, rescindir o contrato de prestação de serviço, conforme cláusulas contratuais pré-estabelecidas.

6 Bibliografia

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBRISO/IEC27001, Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos, mar. de 2006.

[2] ABNT. NBRISO/IEC27002, Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação, ago. de 2005.

[3] ABNT. NBRISO/IEC27005, Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação, jul. de 2006.

[4] ATI – Agência Estadual de Tecnologia da Informação. Política de Segurança da Informação. Versão 1.0 – Recife, 2008. Disponível em: <www.ati.pe.gov.br>. Acesso em: 20 de jan. de 2009.

[5] ATI. Termo de Responsabilidade – Recife, 2008. Disponível em: <www.ati.pe.gov.br>. Acesso em: 20 de jan. de 2009.

[6] ATI. Recomendações de Uso e Formação de Senhas. Recife, 2008. Disponível em: <http://www2.ati.pe.gov.br/web/siteati/recomendacoes2>. Acesso em: 16 de jan. de 2009.

[7] ATI. Norma para elaboração, estruturação e redação de normas técnicas para o SEIG. Versão 1.0 – Recife, 2009. Disponível em: <www.ati.pe.gov.br>. Acesso em: 12 de jan. De 2009.

[8] IEEE. Disponível em: <http://www.ieee.org/portal/site>. Acesso em 20 de jan. de 2009.

[9] IEEE. Padrão 802. Disponível em: <http://grouper.ieee.org/groups/802>. Acesso em 20 de jan. de 2009.

[10] Wi-Fi Alliance. Disponível em: <http://www.wi-fi.org/>. Acesso em 20 de jan. De 2009.

[11] COULOURIS, George; Dollimore, Jean e Kindberg, Tim. Sistemas Distribuídos: conceitos e projeto. Tradução João Tordelho. - 4ª ed. - Porto Alegre: Editora Bookman, 2007.

[12] DAEMEN, Joan; Steve Borg e Vincent Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag, 2002.