MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TELECOMUNICAÇÕES

ICA 102-15

CONTROLES DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELEFONIA IP DO COMAER

2013

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

TELECOMUNICAÇÕES

ICA 102-15

CONTROLES DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELEFONIA IP DO COMAER

2013

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

PORTARIA DECEA Nº 23/DGCEA, DE 12 DE MARÇO DE 2013.

Aprova a edição da Instrução que trata dos Controles de Segurança da Informação da Rede de Telefonia IP do COMAER.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das suas atribuições que lhe confere o art. 195, inciso IV, do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1049/GC3, de 11 de novembro de 2009, e o art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 369/GC3, de 9 de junho de 2010, resolve:

Art.1º Aprovar a edição da ICA 102-15 "Controles de Segurança da Informação da Rede de Telefonia IP do COMAER", que com esta baixa.

Art. 2º Esta Instrução entra em vigor na data de sua publicação.

(a)Ten Brig Ar MARCO AURÉLIO GONÇALVES MENDES
Diretor-Geral do DECEA

(Publicado no BCA nº 061, de 01 de abril de 2013.)

SUMÁRIO

PREFÁCIO

A transmissão de voz sobre redes comutadas por pacotes IP é atualmente uma realidade na área de telecomunicações. Similarmente ao que acontece com outras tecnologias, ela apresenta riscos à segurança da informação. A Telefonia IP possui arquitetura distinta da telefonia tradicional, e estas diferenças implicam em novas vulnerabilidades associadas à segurança da informação.

O menor custo e maior flexibilidade estão entre os benefícios da adoção de uma Rede de Telefonia IP, contudo, a implantação deve ser precedida de uma análise acerca dos problemas de segurança da informação intrínsecos a esta tecnologia.

Os administradores de Rede das Organizações Militares podem, equivocadamente, supor que, devido ao fato da voz trafegar em pacotes de dados, não há a necessidade de precauções, pois a própria rede se encarregaria das proteções necessárias, entretanto esta implantação necessita de cuidados especiais.

Assim, essa Instrução do Comando da Aeronáutica orienta quanto aos cuidados que devem ser tomados pelos administradores na instalação, configuração e administração segura desta rede.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar a Norma de Segurança da Informação aplicável a Rede de Telefonia IP no COMAER.

1.2 ÂMBITO E GRAU DE SIGILO

Esta Instrução se aplica a todos as Organizações Militares do Comando da Aeronáutica, sendo considerado ostensivo o seu grau de sigilo.

1.3 ABREVIATURAS

DECEA – Departamento de Controle do Espaço Aéreo

OM – Organização Militar

SDTE – Subdepartamento Técnico do DECEA

VoIP – *Voice Over Internet Protocol*

1.4 CONCEITUAÇÃO

Os conceitos e definições estão listados no Glossário de Segurança da Informação do DECEA (MCA 7-1, de 30 de março de 2012).

Para efeito desta Norma de Segurança da Informação, entende-se por:

1.4.1 ATAQUE DO TIPO *ARP SPOOFING* OU *ARP POISONING*

É a técnica utilizada quando um *host* necessita correlacionar um endereço MAC para um IP, para tanto ele envia um *ARP request* em *broadcast.* Um atacante pode enviar *ARP replies* usando o seu próprio endereço MAC, se tornando o *default gateway*. Utilizando um ataque conhecido como *Man in the midle,* o *host* atacante forja endereços da tabela do *host* origem.

1.4.2 ATAQUE DO TIPO *CALL FRAUD (FRAUDE NAS CHAMADAS)*

É a técnica na qual o atacante utiliza a rede de telefonia ou rede VoIP indevidamente para efetuar chamadas telefônicas.

1.4.3 ATAQUE DO TIPO *CALL HIJACK (SEQUESTRO DE CHAMADAS)*

É a técnica de ataque na qual o atacante consegue simular ser um dos *user agents* da chamada. Esse tipo de ataque normalmente evolui para um ataque do tipo *man-in-the-middle*.

1.4.4 ATAQUE DO TIPO *DENIAL OF SERVICE* (DOS)

É a técnica de ataque de negação de serviço (também conhecido como ataque de DOS, um acrônimo em inglês para Denial of Service) que visa tornar os recursos de um sistema indisponíveis para seus utilizadores. Os ataques de negação de serviço são feitos geralmente de duas formas:

1.4.4.1 Forçar o sistema atacado a reinicializar ou utilizar todos os recursos (como memória ou processamento) de forma que ele não possa mais fornecer seu serviço.

1.4.4.2 Obstruir a mídia de comunicação entre os utilizadores e o sistema atacado de modo a impedir que se comuniquem adequadamente.

1.4.5 ATAQUE DO TIPO DICIONÁRIO DE AUTENTICAÇÃO *SESSION INITIATION PROTOCOL* (SIP)

É a técnica de ataque que tem como objetivo obter credenciais válidas de um usuário no sistema SIP por meio do método de força bruta. Ele envia inúmeras mensagens *REGISTER* com *userids* e senha provenientes de um arquivo de dicionário. Descoberta a senha, o atacante pode então acessar o serviço.

1.4.6 ATAQUE DO TIPO *DISTRIBUTED DENIAL OF SERVICE* (DDOS)

É a técnica de ataque distribuído de negação de serviço (também conhecido como DDoS, um acrônimo em inglês para *Distributed Denial of Service*). Um computador mestre (denominado "*Master*") pode ter sob seu comando uma rede de computadores ("*Zombies*" - zumbis). Neste caso, as tarefas de ataque de negação de serviço são distribuídas em uma rede de computadores que estão dominadas pelo atacante.

1.4.7 ATAQUE DO TIPO *EAVESDROPPING*

É a técnica de ataque que se baseia na violação da confidencialidade. É uma leitura não autorizada de mensagens.

1.4.8 ATAQUE DO TIPO ESCUTA DO *REAL TIME TRANSPORT PROTOCOL* (RTP)

É a técnica de ataque na qual o atacante captura o tráfego RTP de um canal de voz (hoje facilitado pelo uso da Rede Wireless), utilizando esta técnica, o atacante consegue reconstruir a conversa monitorada.

1.4.9 ATAQUE DO TIPO FALSIFICAÇÃO DE 3XX *RESPONSE CODES*

É a técnica de ataque na qual uma mensagem de redirecionamento do tipo 3xx é forjada de forma que o originador transmita a sua comunicação através de um componente de rede comprometido.

1.4.10 ATAQUE DO TIPO INSERÇÕES *TIME TRANSPORT CONTROL PROTOCOL (*RTCP)

No ataque do tipo DoS, por meio do qual o atacante pode interromper conversações em andamento, falsificando mensagens do protocolo de controle do RTP.

1.4.11 ATAQUE DO TIPO *MAN-IN-THE-MIDDLE*

1.4.11.1 É a forma de ataque na qual os dados de uma comunicação são interceptados, registrados e eventualmente alterados pelo atacante, sem que as vítimas saibam dessa intrusão.

1.4.11.2 Durante o ataque *man-in-the-middle,* a comunicação é interceptada pelo atacante e retransmitida por este de uma forma discricionária. O atacante pode decidir retransmitir entre

os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação. Como os participantes legítimos da comunicação não têm conhecimento que os dados foram adulterados, consideram estes dados como válidos, fornecendo informações e executando instruções por ordem do atacante.

1.4.12 ATAQUE DO TIPO MANIPULAÇÃO DO *CODEC* NO RTP

No ataque do tipo DoS, o atacante pode degradar a qualidade da conversação alterando a taxa de codificação para o *CODEC,* podendo implicar no consumo de maior banda de frequência.

1.4.13 ATAQUE DO TIPO MANIPULAÇÃO DOS REGISTROS

Neste ataque um *user agent* se faz passar por outro, podendo receber suas chamadas ou fazer chamadas no seu nome.

1.4.14 ATAQUE DO TIPO MANIPULAÇÕES DA FONTE DE SINCRONIZAÇÃO DO IDENTIFICADOR (SSRC) NO CABEÇALHO RTP

A reescrita do SSRC pode ser utilizada para interromper chamadas ou remover um usuário da chamada, tomando o seu lugar, ou para enviar conteúdo falso.

1.4.15 ATAQUE DO TIPO SIP BOMBING

É o ataque do tipo DoS no qual uma grande quantidade de mensagens de Telefonia IP modificadas são "injetadas" contra algum dos componente da rede SIP. Nesse caso o sistema efetua o tratamento dessas mensagens e o serviço torna-se indisponível ou com a qualidade degradada.

1.4.16 ATAQUE DO TIPO SIP-CANCEL/BYE DOS

É a técnica de ataque do tipo de DoS na qual o atacante simula uma mensagem de desconexão do tipo *CANCEL* ou *BYE* (dependendo do estado da chamada), evitando que o originador possa iniciar conversações ou interromper as sessões em andamento.

1.4.17 ATAQUE DO TIPO *SPAM OVER IP TELEPHONY* - SPIT

São as mensagens não solicitadas que chegam por meio de Voz sobre IP (VoIP) aos usuários da Rede de Telefonia IP.

1.4.18 ATAQUE DO TIPO SPOOFING

Ataque no qual uma pessoa ou programa consegue se passar por outra.

1.4.19 *CODIFICADOR - DECODIFICADOR*

Um codec, ou codificador-decodificador, converte sinais de áudio para uma forma digital compactada para transmissão e depois para um sinal de áudio descompactado para retorno. Essa conversão é a essência do VoIP.

1.4.20 *CONTENT ADDRESSABLE MEMORY TABLE* - CAM TABLE

Conteúdo endereçável de memória de tabela (CAM). É o termo que se refere à memória de conteúdo endereçável na dinâmica de um *switch ethernet*.

1.4.21 FONTE DE SINCRONIZAÇÃO DO IDENTIFICADOR *SYNCHRONIZATION SOURCE* (SSRC)

O SSRC identifica a fonte de sincronização. Este identificador é escolhido aleatoriamente, com a intenção de ser único entre todas as fontes de uma mesma sessão. A lista de CSRC identifica as fontes (SSRC) que contribuíram para a obtenção dos dados contidos no pacote que contém esses identificadores. O número de identificadores é dado no campo CC.

1.4.22 IP *SECURITY* (IPSEC)

A plataforma IPSec foi desenvolvida para prover serviços de segurança de alta qualidade, baseados em criptografia, para a camada de rede e/ou para as camadas superiores. O conjunto de serviços oferecidos inclui controle de acesso, integridade não orientada à conexão, autenticação da origem dos dados e confidencialidade (criptografia).

1.4.23 MULTICAST

Comunicação na qual um quadro é enviado para um grupo específico de dispositivos ou clientes. Os clientes da transmissão *multicast* devem ser membros de um grupo *multicast* lógico para receber as informações.

1.4.24 *NEWORK ASSERTED IDENTITY*

O *Nework Asserted Identity* é um mecanismo específico para a troca de identidade entre elementos de rede que já possuam relacionamento confiável utilizando algum outro mecanismo ou política de segurança. A utilidade desse tipo de mecanismo é, por exemplo, permitir que um usuário, depois de autenticado, realize chamadas anônimas sem que para isso a rede perca a possibilidade de rastrear a chamada realizada, preservando assim a privacidade do originador.

1.4.25 PROTOCOLO TELNET

É o protocolo de rede utilizado na Internet ou redes locais para proporcionar uma facilidade de comunicação bidirecional interativa baseada em texto usando uma conexão terminal virtual. Este protocolo permite acesso remoto a qualquer máquina em uma rede, mas é mais inseguro, pois os dados utilizados para o acesso remoto não são criptografados.

1.4.26 *PUBLIC SWITCHED TELEPHONE NETWORK - PSTN*

Sigla em inglês para o termo RTPC que significa Rede de Telefonia Pública Comutada.

1.4.27 *QUALITY OF SERVICE - QoS*

Designa a capacidade de fornecer um serviço conforme os requisitos de tempos de resposta e de banda concorrida. Aplicado às redes de comutação de pacotes (redes

baseadas na utilização de switchs) o QoS designa a aptidão de garantir um nível aceitável de perda de pacotes.

1.4.28 *REAL TIME TRANSPORT PROTOCOL* - RTP

É o protocolo padrão associado ao gerenciamento da transmissão em tempo real de multimídia de dados sobre qualquer transmissão unicast ou multicast na rede.

1.4.29 *SESSION INITIATION PROTOCOL* - SIP

É o protocolo de controle referente à camada de aplicações do Modelo de Referência OSI (*Open System Interconnection*), que é usado para iniciar, modificar ou terminar sessões ou chamadas multimídia entre usuários. Dentre suas funcionalidades destacam-se a localização de usuários, o estabelecimento de chamadas, o suporte a *unicast* ou *multicast,* administração na participação de chamadas (transferências, conferência, entre outros).

1.4.30 *SECURE REAL-TIME PROCOTOL - SRTP*

É o protocolo de segurança que oferece confidencialidade, autenticidade, integridade e proteção contra replays que são retransmissão fraudulenta dos pacotes RTP (*Real Time Transport Protocol*). Fornece ainda criptografia e previne ataques de monitoramento do protocolo RTP.

1.4.31 TELEFONE IP

Aparelho telefônico que se diferencia de um aparelho telefônico convencional por possuir todo o conjunto de hardware e software que o capacita a realizar chamadas de voz sobre IP. Diferentemente de um terminal convencional, o telefone IP se conecta diretamente à rede local (LAN) e implementa os protocolos necessários para efetuar a comunicação.

1.4.32 TELEFONIA IP

1.4.32.1 É a tecnologia que permite a transmissão de voz, em tempo real, sobre uma rede de dados que utiliza o protocolo IP.

1.4.32.2 O objetivo da telefonia em redes IP é prover uma forma alternativa aos sistemas tradicionais, mantendo, no mínimo, as mesmas funcionalidades e qualidade similar, e aproveitando a sinergia da rede para o transporte de voz e dados.

1.4.33 *TIME TRANSPORT CONTROL PROTOCOL (RTCP)*

Protocolo que se baseia no envio periódico de pacotes de controle a todos os participantes da conexão (chamada), usando o mesmo mecanismo de distribuição dos pacotes de mídia (Voz). Desta forma, com um controle mínimo, é realizada a transmissão de dados em tempo real usando o suporte dos pacotes UDP da rede IP.

1.4.34 *TOTAL COST OF OWNERSHIP - TCO*

É a estimativa financeira projetada para consumidores e gerentes de empresas a avaliar os custos diretos e indiretos relacionados à aquisição de todo o investimento

necessário, tal como softwares e hardwares, além do gasto inerente de tais produtos para mantê-los em funcionamento.

1.4.35 *TRANSPORT LAYER SECURITY - TLS*

É o protocolo de rede que utiliza criptografia, que proporciona segurança de comunicação na Internet para serviços como *email* (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados.

1.4.36 *UNICAST*

A transmissão *unicast* é quando um determinado terminal "A" envia a informação apenas para o terminal "B".

1.4.37 VIRTUAL LAN - VLAN

É uma rede comutada, logicamente segmentada por funções ou aplicações, sem considerar a localização física dos usuários.

1.5 DOCUMENTOS DE REFERÊNCIA

a) DCA 7-2 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO DECEA, de 2010;

b) PCA 7-11 – PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO DO DECEA, de 2010;

c) NSCA 7-13 – SEGURANÇA DE SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO NO COMANDO DA AERONÁUTICA, de 2006; e

2 RESPONSABILIDADES

2.1 SUBDEPARTAMENTO TÉCNICO DO DECEA

2.1.1 Estabelecer normas, padrões e metodologias relativas à segurança da informação, que estejam em conformidade com a legislação brasileira e com os padrões aceitos internacionalmente.

2.1.2 Estabelecer normas, padrões e metodologias que regulem o emprego de controles de segurança da informação em Rede de Telefonia IP.

2.1.3 Estabelecer planejamento de auditoria de segurança da informação para verificar a implantação das diretrizes desta Instrução do Comando da Aeronáutica nas Organizações Militares Subordinadas ao COMAER.

2.2 AOS GESTORES DE SISTEMA DE TELEFONIA VOIP

2.2.1 Administrar a Rede de Telefonia IP em conformidade com as boas práticas de segurança da informação presentes nesta Norma.

2.2.2 Apoiar na instalação, configuração e administração da Rede de Telefonia IP em sua Organização Militar.

2.3 AOS MANTENEDORES DE SISTEMA DE TELEFONIA VOIP

2.3.1 Elaborar os procedimentos de segurança da informação e instrução de segurança da informação de acordo com esta Instrução do Comando da Aeronáutica.

2.3.2 Implantar os controles de segurança da informação em sua Organização Militar, conforme recomendado nesta Instrução, em conjunto com o proprietário dos ativos da Rede de Telefonia IP.

3 VISÃO GERAL DOS PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELEFONIA IP

3.1 Os princípios de segurança da informação para a Rede de Telefonia IP estão descritos abaixo:

a) confidencialidade: garantir uma comunicação de voz sobre IP que não possa ser acessada por pessoas não autorizadas;

b) integridade: detectar quaisquer alterações intencionais ou não aos dados que trafegam na rede; e

c) disponibilidade: garantir que os dispositivos e os indivíduos possam acessar uma Rede de Telefonia IP e seus recursos, sempre que necessário.

3.2 Os princípios de segurança da informação para a Rede de Telefonia IP e para as redes cabeadas ou sem fio são os mesmos.

3.3 Os ataques a Rede de Telefonia IP podem ser divididos em três categorias segundo o tipo principal de impacto: de disponibilidade, de integridade e de confidencialidade.

3.4 Os ataques à disponibilidade podem causar a interrupção das comunicações pela indisponibilidade ou degradação do serviço. Dentro dessa categoria incluem-se ataques do tipo DoS e DDoS.

3.5 Os ataques à integridade tentam comprometer os serviços Telefonia IP através da alteração do conteúdo da conversação. Dentro dessa categoria são incluídos o MITM, *Call Hijack, Spoofing e o Call Fraud.*

3.6 Alguns exemplos de ataque à confidencialidade consistem no monitoramento (*eavesdropping*), podendo expor informações confidenciais de determinado negócio, operação ou pessoa física, e passível de evolução para ataques contra a integridade.

3.7 Os principais ataques que podem apresentar óbices para o perfeito funcionamento de uma Rede de Telefonia IP estão descritas abaixo e as suas conceituações definidas no item 1.4 deste documento:

a) ataque de dicionário de autenticação SIP;

b) ataque de *Call Hijack*;

c) ataque de SIP *Bombing;*

d) ataque de SIP-*Cancel/Bye DoS;*

e) ataque de manipulação dos registros;

f) ataque de falsificação de 3xx *Response Codes*;

g) ataque de escuta do RTP;

h) ataque de manipulações do SSRC no RTP;

i) ataque de manipulação do *CODEC* no RTP;

j) ataque de inserções RTCP; e

k) ataque de *Call Fraud.*

4 REDE DE TELEFONIA IP

4.1 O tipo de Rede de Telefonia IP utilizada no COMAER se baseia em tecnologia que permite a transmissão de voz, em tempo real, sobre uma rede de dados que utiliza o protocolo IP.

4.2 Dentre outros benefícios, as redes de Telefonia IP auxiliam na diminuição de custos de telefonia, principalmente nas chamadas de longa distância. Porém, a maioria das Organizações Militares já possui uma infraestrutura de telefonia legada. Assim, para integrar as redes, de forma transparente, é utilizado um *Gateway* conectado entre a rede de Telefonia IP e a rede de telefonia convencional.

4.3 Quando o usuário utiliza um Telefone IP para comunicação com um telefone convencional, sua voz é digitalizada, transmitida através da rede de dados até o seu PABX IP que envia a chamada para o *Gateway* VoIP, esse decodificará os pacotes IP em voz e transmitirá através de uma linha convencional até o telefone de destino. O oposto é realizado quando um número convencional liga para um telefone IP.

4.4 A figura 01 ilustra a arquitetura típica de uma Rede de Telefonia IP.

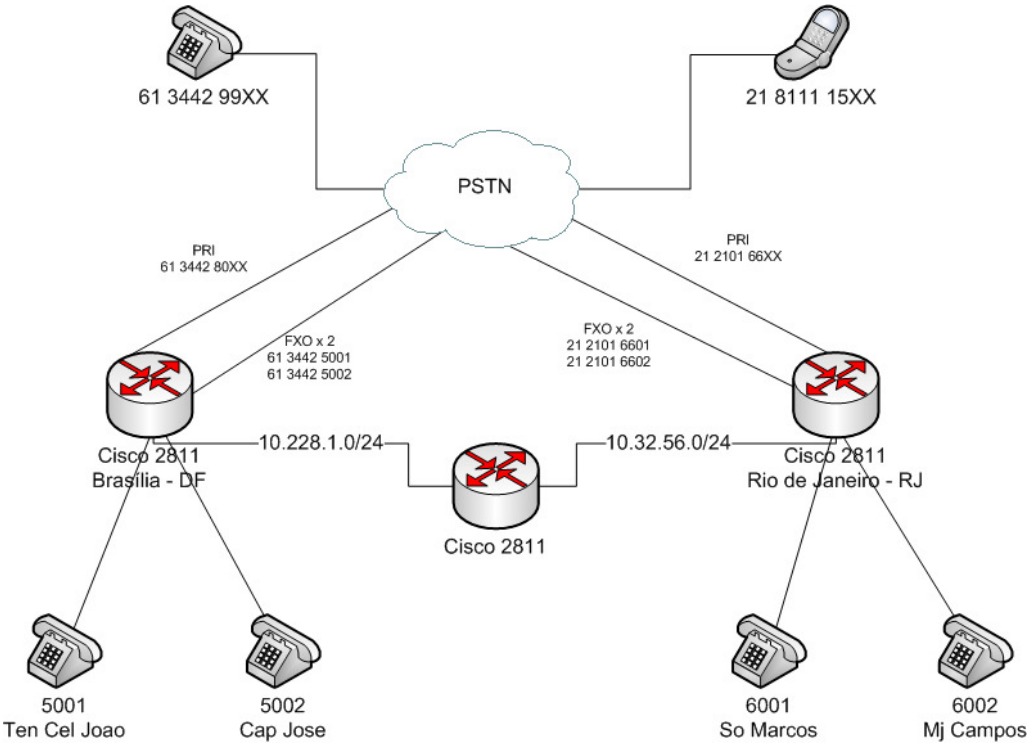

Figura 01 - Arquitetura Típica de uma Rede de Telefonia IP.

5 PROCEDIMENTO DE SEGURANÇA DA INFORMAÇÃO PARA USO DA REDE DE TELEFONIA IP

O COMAER e suas Organizações Militares Subordinadas devem mitigar os riscos para a utilização de Rede de Telefonia IP mediante a aplicação de controles de segurança da informação. A seguir, serão apresentadas as recomendações de segurança no correto emprego de uma Rede de Telefonia IP. Estes itens estão agrupados em categorias para facilitar a compreensão.

5.1 PADRONIZAÇÃO DE SISTEMAS OPERACIONAIS

5.1.1 As Organizações Militares devem padronizar os sistemas operacionais e aplicações utilizadas na Rede de Telefonia IP. Embora normalmente exista a necessidade de utilização de sistemas heterogêneos nos ambientes de Tecnologia da Informação atuais, deve-se buscar o máximo de padronização possível em relação ao uso de marcas, modelos e fabricantes de equipamentos, e de sistemas operacionais instalados na Rede de Telefonia IP. Isto facilita bastante a administração da Telefonia IP, reduzindo o Total *Cost of Ownership* e possibilitando uma gestão mais eficiente da segurança da informação.

5.2 ARQUITETURA DA REDE

5.2.1 Os dispositivos de Telefonia IP devem ser separados por meio do uso de VLANs, ou seja, redes lógicas distintas para dados e voz, permitindo a aplicação de controles de acesso que identifiquem os protocolos e serviços autorizados a trafegar. O equipamento de rede não deve ser utilizado como uma ponte *(bridge*) que conecta diretamente a Rede de Telefonia IP e a rede interna. Caso contrário, se o equipamento de rede for comprometido por um atacante, toda a rede, inclusive a rede interna, estará vulnerável, podendo causar o acesso indevido as informações classificadas e aos recursos computacionais.

5.2.2 As conexões da rede com outras redes externas devem ser protegidas por *firewalls*. Se a Rede de Telefonia IP for conectada diretamente a outras redes internas ou com a Internet, sem a instalação de um *firewall*, estará sendo criada uma vulnerabilidade passível de exploração, podendo causar o acesso indevido aos serviços e informações internas por parte de usuários não autorizados, principalmente se existir uma conexão, não monitorada, com a Internet.

5.3 CRIPTOGRAFIA E AUTENTICAÇÃO

5.3.1 É mandatória a implantação de um *banner* de advertência para *login* na interface de administração da Rede de Telefonia IP. A exibição de uma mensagem de advertência no processo de *logon* na interface de administração visa informar que o equipamento em questão pertence à Organização Militar e é de uso restrito para usuários autorizados, e que os acessos eventualmente são monitorados.

5.3.2 Deve ser implantado mecanismo para ocultação do esquema de endereçamento IP utilizado na rede interna. O conhecimento da arquitetura e dos endereços IP utilizados pelos equipamentos da rede interna (servidores, estações, etc.) facilita o planejamento de ataques. Por este motivo, é fortemente recomendável a inserção de mecanismos que permitam ocultar estas informações de usuários não autorizados, evitando que as redes possam ser mapeadas remotamente por algum atacante.

5.3.3 O protocolo 802.1X deve ser implementado na Rede de Telefonia IP para autenticação de dispositivos na referida Rede.

5.3.4 As Organizações Militares também devem implementar o protocolo *Newtork Asserted Identity* para autenticação dos usuários que utilizam a Rede de Telefonia IP. O *Newtork Asserted Identity* é um mecanismo específico para a troca de identidade entre elementos de rede que já possuam relacionamento confiável, utilizando outro mecanismo ou política de segurança da informação.

5.4 AUDITORIA E MONITORAMENTO

5.4.1 A opção de envio de *logs* dos aplicativos usados na Rede de Telefonia IP deve ser habilitada e configurada de forma a registrar os eventos relevantes de segurança da informação. Os *logs* ajudam a identificar potenciais problemas de *software* e *hardware* e permitem identificar tentativas de acesso não autorizado e outros eventos relevantes, fornecendo ainda evidências no caso de um incidente de segurança da informação.

5.4.2 As Organizações Militares devem proteger os registros de auditoria *(logs*) gerados pela Rede de Telefonia IP contra acessos indevidos. Embora normalmente a auditoria seja limitada em funcionalidade, recomenda-se que estes documentos sejam protegidos contra acessos indevidos, visando preservar a sua integridade.

5.4.3 As Organizações Militares devem verificar periodicamente os registros de *logs* gerados pela Rede de Telefonia IP. Embora necessário, o simples processo de registro dos eventos relevantes para a segurança da informação relacionados ao funcionamento e utilização da rede não é suficiente. Para que os eventos de segurança da informação possam ser efetivamente rastreados, é importante que os registros sejam periodicamente analisados.

5.4.4 As Organizações Militares devem implementar um sistema de monitoramento de tráfego na Rede de Telefonia IP. Sistemas de monitoramento do uso da banda permitem um melhor acompanhamento da utilização do *link* de comunicação e consequentemente possibilitam melhor planejamento de capacidade, evitando o consumo excessivo da banda por serviços não essenciais. Além disso, a monitoração constante do tráfego permite detectar incidentes de segurança da informação.

5.5 CONFIGURAÇÕES DE SISTEMAS E APLICAÇÕES

5.5.1 As Organizações Militares devem configurar os equipamentos da Rede de Telefonia IP com parâmetros diferentes da configuração *default* do fabricante. Estão disponíveis na Internet informações sobre a configuração *default* de diversos tipos de equipamentos para Rede Telefonia IP e que poderão ser utilizados para acesso indevido, caso não sejam alterados pelos administradores do referido serviço.

5.5.2 O serviço *telnet* deve ser desabilitado na administração da Rede de Telefonia IP, pois transmite os dados no modo de texto claro, ou seja, sem criptografia.

5.5.3 O Protocolo de Transporte Seguro em Tempo Real (SRTP) deve ser implementado na Rede de Telefonia IP, uma vez que fornece criptografia e proteção *replay* para os dados RTP, tanto *unicast* e *multicast* de aplicações.

5.5.4 Deve ser implantado controle de acesso à rede lógica (porta segura). Ex: controle por endereço MAC. Assim, a implementação de controle de porta segura evita que um possível atacante possa transmitir *frames* com diferente endereço MAC de origem, com o objetivo de exaurir a *CAM table* do switch, fazendo com que este passe a operar identicamente a um *hub*. Deve ser implementado um mecanismos de QoS nos meios de comunicação de Telefonia IP.

A implantação do serviço de QoS na Rede de Telefonia IP melhora a qualidade do serviço, garantindo, assim, prioridade, reserva de banda e menor atraso para os pacotes de voz.

5.5.5 Deve ser implementado mecanismo de validação de pacotes ARP (*Dynamic Arp Inspection, Arp Validation* e outros) na Rede de Telefonia IP. A implementação de mecanismo de validação de pacotes ARP evita ataques do tipo *ARP Spoofing* ou ARP *Poisoning*. Este ataque consiste no encaminhamento de uma resposta falsa à requisição ARP original ou via *Gratuitous* ARP, permitindo ao atacante atuar no meio da comunicação (*Man-in-the-Middle*) para monitorar o tráfego de rede.

5.5.6 Devem ser implementados os protocolos HTTPS/IPSEC/SSH na administração da Rede de Telefonia IP. Os protocolos de segurança HTTPS/IPSEC/SSH permitem acesso seguro à interface de gerência dos dispositivos Telefonia IP.

5.6 CONFIGURAÇÃO DO SISTEMA OPERACIONAL DO SERVIDOR VOIP

5.6.1 Os registros da auditoria ("*logs*") gerados pelos ativos da rede de Telefonia IP devem ser protegidos contra acessos indevidos. A análise crítica dos registros da auditoria permite detectar eventos relevantes para a segurança da informação e são alvos preferenciais de "atacantes" que tentam apagar evidências de suas ações sobre o sistema. Por este motivo, os "*logs*" do sistema precisam ser mantidos em local seguro, protegidos contra leituras e modificações não autorizadas.

5.6.2 A auditoria do sistema operacional deve ser habilitada e configurada de forma a registrar os eventos relevantes para a segurança da informação. Com o "*log*" do sistema desabilitado, não será possível rastrear eventos relevantes para a segurança da informação, tais como tentativas de acesso não autorizado, erros operacionais, problemas relacionados ao *hardware* ou ao *software*, etc, de forma a identificar os respectivos agentes causadores. Estes problemas eventualmente poderão comprometer o sistema, caso não sejam detectados e tratados.

5.6.3 Uma mensagem de advertência deve ser exibida para os usuários durante o "*login*" no sistema operacional. A exibição de uma mensagem de advertência durante o "*login*" tem como propósito explicitar que o sistema em questão pertence à empresa e é de uso restrito para usuários autorizados, e que os acessos estarão sendo gravados em "*Logs*". Do ponto de vista legal, é recomendável explicitar que o uso do sistema ou serviço é restrito e que o acesso indevido poderá ter implicações legais.

5.6.4 Os serviços desnecessários devem ser desabilitados no sistema operacional. A experiência demonstra que muitos ataques exploram vulnerabilidades em serviços que os usuários tipicamente não utilizam. Cada serviço instalado expõe o sistema ao risco de ser comprometido através da exploração de falhas que ainda não foram sequer divulgadas. Também é provável que estes serviços não estejam atualizados por não haver documentação nem procedimentos formais que indiquem sua existência, aumentando ainda mais os riscos de comprometimento do sistema. Além disso, podem ocorrer impactos sobre performance do serviço ou equipamento. Por estes motivos, recomenda-se que todos os serviços desnecessários para o bom funcionamento do sistema sejam desabilitados.

5.7 POLÍTICA DE SENHA FORTE

5.7.1 As Organizações Militares devem substituir as senhas padrão fornecidas pelo fabricante para acesso administrador da Rede de Telefonia IP por outras de política forte, ou seja,

alteradas regularmente até 120 dias com no mínimo 10 caracteres, entre eles: letras maiúsculas e minúsculas, números e caracteres especiais. Os dados dos parâmetros *default* de vários modelos de equipamento da Rede de Telefonia IP, incluindo o acesso administrativo, estão disponíveis na Internet. De posse da senha de administração, um atacante pode obter controle total sobre a rede, com o risco de acesso indevido a informações classificadas, fraude ou indisponibilidade dos serviços.

5.8 ATUALIZAÇÃO

5.8.1 As Organizações Militares devem adquirir produtos que podem ser atualizados facilmente em *software* ou *firmware*.

5.8.2 Os administradores de rede devem verificar regularmente com fornecedores para identificar novos *patches*, *upgrades*, ou atualizações e aplicá-las conforme necessário.

5.8.3 As Organizações Militares devem testar os *patches* e atualizações de software regularmente. Estes também devem ser testados antes da sua implementação para garantir que eles funcionem corretamente.

5.9 TRATAMENTO DE INCIDENTES NA REDE DE TELEFONIA IP

5.9.1 As Organizações Militares devem elaborar um procedimento de segurança da informação de resposta a incidente para a Rede de Telefonia IP. No caso de algum ataque local ou remoto ser bem sucedido e ocasionar o comprometimento de sistemas de informação internos deverá ser reportado para o CTIR.AER.

5.10 AÇÕES DE CONTINUIDADE DE NEGÓCIOS

5.10.1 As Organizações Militares devem elaborar um plano de contingência em caso de perda de acesso administrativo a Rede de Telefonia IP. Se a senha do equipamento for perdida ou esquecida e não puder ser recuperada, várias funções restritas ao administrador ficarão indisponíveis.

5.10.2 As Organizações Militares devem executar um procedimento de segurança da informação de cópias de segurança periódico para os arquivos de configuração da Rede de Telefonia IP. Uma cópia de segurança do arquivo de configuração deve ser gerada após cada alteração relevante. A existência de uma cópia ("*backup*") deste arquivo ajuda a reduzir o tempo de indisponibilidade quando da ocorrência de eventos que requeiram a sua reinstalação ou reconfiguração, como por exemplo, falhas inesperadas de software ou hardware. O armazenamento de cópias de segurança atualizadas também permite que seja realizado um histórico das alterações efetuadas.

5.11 AVALIAÇÕES DE SEGURANÇA DA REDE DE TELEFONIA IP

5.11.1 As Organizações Militares devem executar procedimento de segurança da informação para mapeamento de portas e serviços não autorizados. A existência destas dentro de uma rede permite ataques a sistemas desconhecidos pelos administradores, ou indicam máquinas que foram invadidas e que tiveram serviços adicionais instalados. O mapeamento periódico dessas portas e serviços é importante para que o administrador da rede conheça, de maneira pró-ativa, quais serviços não autorizados estão em uso na rede e possa desabilitá-los antes que eventos de segurança da informação possam ocorrer, ou então, para identificar máquinas que já foram comprometidas.

5.11.2 As Organizações Militares devem executar periodicamente procedimento de segurança da informação para identificação de vulnerabilidades. Atualmente, é frequente a criação de programas com código maliciosos e a descoberta de novas falhas em sistemas de informação. A capacidade de operação estável depende diretamente da atualização dos *patches* que eliminam ou minimizam essas vulnerabilidades, e das configurações dos sistemas de informação que restringem o acesso e tornam o sistema mais seguro.

5.12 INVENTÁRIO DE ATIVOS DE INFORMAÇÃO

5.12.1 As Organizações Militares devem elaborar um inventário dos equipamentos da Rede de Telefonia IP. É necessário ter controle de quais equipamentos são utilizados em suas instalações (estações, servidores, sistemas, etc.) para assegurar que as proteções estão sendo implementadas e ter gerência patrimonial sobre seus ativos de informação.

5.12.2 O inventário de ativos de informação da Rede de Telefonia IP deve conter os seguintes requisitos: descrição, proprietário e custodiante do ativo, localização lógica e física, critérios de segurança da informação, números de ramal, usuários e etc.

5.13 DOCUMENTAÇÃO

5.13.1 As Organizações Militares devem documentar os procedimentos de instalação e configuração dos ativos da Rede de Telefonia IP. A existência de uma documentação da instalação, configuração e manutenção destes equipamentos auxilia a evitar erros de operação, permite a verificação de conformidade da configuração em relação a políticas, e também facilita a recuperação do sistema em caso de falhas de *software* ou *hardware*.

5.13.2 As Organizações Militares devem documentar a arquitetura da Rede de Telefonia IP. A existência desta ajuda a evitar erros de operação, permite a verificação de conformidade da configuração em relação a políticas e também torna possível uma reconfiguração mais rápida do ambiente, reduzindo o tempo de indisponibilidade (*downtime*) no caso de necessidade de reinstalação dos sistemas.

5.13.3 As Organizações Militares devem manter atualizada a documentação da arquitetura da Rede de Telefonia IP. Expansões da rede, redistribuição de equipamentos, mudanças de endereçamento e outras alterações geralmente são feitos sem a devida atualização dos documentos da rede de Telefonia IP. Uma documentação desatualizada provoca erros, retrabalhos e, na ocorrência de incidentes de segurança da informação, pode aumentar o tempo de indisponibilidade dos serviços afetados.

6 DISPOSIÇÕES FINAIS

6.1 A Norma de Segurança da Informação apresentada nesta Instrução é de caráter geral e será revisada, periodicamente, a cada vinte e quatro meses.

6.2 Esta Norma de Segurança da Informação contém boas práticas de segurança da informação para Rede de Telefonia IP de forma genérica. Como os procedimentos de configuração variam com relação à marca e modelo, para obter informações sobre os detalhes da implementação é necessário consultar a documentação fornecida pelo fabricante.

6.3 As Organizações Militares nas quais a Rede de Telefonia IP já está em operação tem o prazo de até vinte e quatro meses, após a publicação desta ICA, para se adequar às diretrizes contidas nesta Norma. Após esse prazo, caso a Organização Militar não tenha feito a devida adequação, o acesso a Rede de Telefonia IP deve ser cessado imediatamente.

6.4 Casos não previstos nesta Instrução deverão ser levados à apreciação do Exmo. Sr. Chefe do Subdepartamento Técnico do DECEA.