Arquitetura da INTRAER
- Uma Questão de Segurança

Cap.-Av. Daniel Santos Coimbra

1 - Introdução

Em 1997, num esforço combinado da DEPV e da antiga DIRINFE, o então Ministério da Aeronáutica deu início à implantação de uma grande rede de computadores, interligando todas as suas organizações através do sistema TELESAT da EMBRATEL. Essa grande rede de computadores do Comando da Aeronáutica, que utilizava todas as tecnologias existentes na INTERNET, foi denominada INTRAER, ou seja, a INTRANET da Aeronáutica.

Ao mesmo tempo que facilitava a comunicação, essa rede trazia também em seu bojo problemas de segurança de dados. Com o intuito de resolver esses problemas, a DIRINFE propôs a aprovação da NSMA 7-13, "Segurança de Dados no MAER", o que ocorreu em 1999. Esse documento sugeria que cada comandante devesse, após verificar as vulnerabilidades existentes em sua rede, elaborar planos de segurança local, o que não foi suficiente para resolver o problema.

A privatização da EMBRATEL contribuiu para o agravamento do quadro de falta de segurança, fazendo com que os Estados Unidos tivessem um acesso potencial à INTRAER, através do satélite.

Todos esses fatos expõem a Aeronáutica de tal forma que o possível prejuízo torna-se incalculável. Com efeito, pode-se imaginar o que aconteceria se um planejamento estratégico do EMAER ou um relatório de auditoria da SEFA parasse em mãos erradas. Portanto, isso acarreta uma necessidade de aperfeiçoamento da INTRAER.

Para compreensão total do assunto, torna-se necessário entender a arquitetura atual da rede de comunicação de dados e suas restrições no aspecto de segurança.

2 - A Arquitetura da INTRAER

A INTRAER faz uso do protocolo eletrônico de comunicação de rede conhecido como TCP/IP, o mesmo utilizado na INTERNET. Esse protocolo oferece uma gama muito variada de serviços, ou seja, possibilita que vários tipos de aplicações façam uso da rede, como, por exemplo, banco de dados, vídeo-conferência e correio eletrônico, entre outros.

Esse protocolo também viabiliza a comunicação através de pacotes, de maneira que as informações são fracionadas, sendo transmitidas em partes e enviadas uma de cada vez. Uma maneira fácil de entender essa tecnologia de pacotes é imaginar que uma pessoa deseja enviar uma carta que contenha vários parágrafos. Ao invés de enviá-la de uma única vez, ela separaria os parágrafos, colocando um em cada envelope.

Neste caso, é fácil perceber que o destinatário deve receber todas as correspondências, que teriam um número seqüencial, colocando os parágrafos de forma ordenada, de modo a restaurar o conteúdo original.

Ao se fazer esse paralelo, verifica-se que, da mesma forma que os envelopes, os pacotes teriam o endereço do remetente, do destinatário e um número seqüencial. Essa tecnologia de rede trabalha também com camadas de rede, que podem ser definidas na forma de um pacote inserido em outro pacote. De volta ao exemplo dos envelopes, pode-se imaginar que o remetente serve na EAOAR, o destinatário no CCA-BR e toda a comunicação segue via malote. A pessoa entregaria a correspondência no protocolo da EAOAR, que envia para o protocolo da UNIFA. Lá ela é colocada dentro de um outro envelope para o GAP-BR, que ao receber e abrir o mesmo, constata a existência de uma correspondência para um militar do CCA-BR.

Até agora foi considerado o plano lógico, ou seja, a parte afeta aos programas ou aplicativos. Ao avaliar o plano físico, depara-se com a existência de computadores que possuem placas de rede. Nela são encaixados cabos que vão até portas, receptáculos de um *hub* (dispositivo utilizado para conectar os equipamentos que compõem uma rede), os quais são interligados através de um *switch*.

Todo esse emaranhado de computadores, *hub* e *switch* compõem uma rede. Para viabilizar a comunicação entre dois ou mais destes grupos de equipamentos, é necessária a utilização de roteadores.

Valendo-se novamente do exemplo da carta, o roteador seria a agência do correio responsável por separar as cartas por localidade, despachando-as nos seus respectivos vôos.

No mundo da telefonia, constata-se hoje em dia que a comunicação entre cidades distantes é realizada, principalmente, através de satélites. Esse fato também ocorre ao se conectar duas redes que se encontrem na mesma situação.

Todos esses princípios foram observados no planejamento da arquitetura da INTRAER, fazendo com que ela apresentasse a disposição a seguir (Fig. 1).

Pode-se verificar que todos os equipamentos enumerados até agora, e que

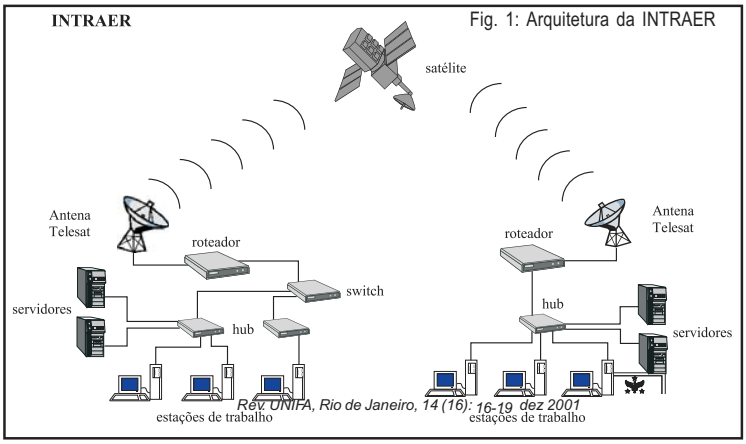

Fig. 1: Arquitetura da INTRAER

constam da arquitetura atual da INTRAER, não contemplam aspectos de segurança, tornando vulneráveis os dados transmitidos e manipulados, advindo uma necessidade de protegê-los. Porém, qual a real necessidade de proteção e segurança dessas informações?

3 - Necessidade de Segurança

Para garantir a segurança de uma informação, é necessário que as medidas adotadas preservem a: * confidencialidade - certeza de que só é acessada por quem tiver autorização; * disponibilidade - está disponível no momento em que se necessita da mesma; * integridade - não é modificada; e * autenticidade - a comprovação de quem enviou realmente é quem diz ser.

Para que esses aspectos sejam preservados, faz-se necessária uma análise de segurança do local a ser protegido, levando-se em consideração uma série de fatores, como, por exemplo, o tipo dos dados, as pessoas envolvidas, as documentações e os locais físicos, dentre outros.

As medidas a serem adotadas sempre estão diretamente ligadas com a importância do bem a ser protegido, ou seja, são utilizados recursos que justifiquem o valor da informação.

Essa análise não é trivial, o que provavelmente acarreta a solicitação de assessoria de uma organização qualificada, que deve se preocupar, principalmente, em identificar as áreas mais sensíveis, de forma a particionar e compartimentar a rede em níveis de segurança.

Outro aspecto importante a ser considerado é o meio de comunicação e suas características. No caso da transmissão via satélite, verifica-se que os dados podem ser coletados por outros países, gerando uma necessidade de proteção.

4 - A Arquitetura Proposta

O isolamento das redes é possível através de *firewall*, de *proxy* (servidor HTTP especial que tipicamente roda em em uma máquina firewall) ou de ambos. O tipo de equipamento a ser utilizado é função da necessidade de segurança.

Contudo, uma vulnerabilidade permanece, pois os referidos equipamentos funcionam como isoladores da rede, isto é, porteiros. Eles não garantem que um atacante situado dentro da rede seja impedido de agir, nem que os dados autorizados a passar permaneçam protegidos.

Dessa forma, faz-se necessária a utilização de um equipamento de criptografia, responsável por tornar uma mensagem ininteligível, para quem não está autorizado a acessá-la, e um de assinatura digital, que garante a identificação dos usuários de forma segura.

Com esses equipamentos já citados, pode-se garantir confidencialidade, disponibilidade, integridade e autenticidade dos dados veiculados na INTRAER.

Existe uma máxima em segurança de informática que retrata a impossibilidade de se garantir que um dado esteja 100% seguro. Isso não seria diferente para qualquer solução adotada pelo COMAER. As medidas a serem tomadas visariam dificultar ao máximo a invasão ou o comprometimento da informação.

O equipamento que exigirá um cuidado triplicado será o dispositivo criptográfico, que deverá ser de fabricação nacional, com um algoritmo de criptografia desenvolvido pelo CEPESC (Centro de Pesquisas e de Desenvolvimento para a Segurança das Comunicações).

Os equipamentos de segurança já enumerados viabilizam a elaboração de uma proposta de arquitetura de rede mais segura. A figura 2 mostra uma arquitetura geral, no entanto, deve-se observar que estão sendo tratados casos distintos de necessidade de segurança.

Nesta proposta, toda organização conta com um *firewall* na entrada da rede, o qual é responsável por garantir a rede como um

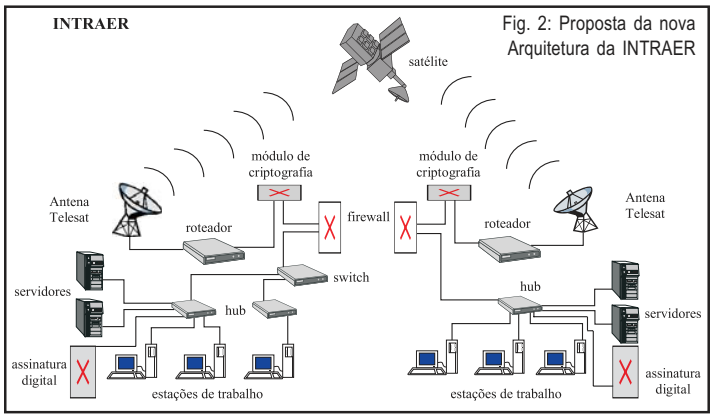

Fig. 2: Proposta da nova Arquitetura da INTRAER

todo. A criptografia é aplicada a todos os dados transmitidos pelo satélite.

O acesso aos recursos da rede só está disponível através da autenticação no equipamento de assinatura digital. Ao ativar um sistema de registro que grave todas as ações dos usuários, é possível verificar quem tenta executar uma ação espúria.

A idéia consiste em separar redes com necessidades de segurança diferentes. Essa situação também será válida para computadores de uma mesma organização que requeiram tratamento diferenciado.

Esse segundo nível de segurança, por localidade, é muito importante, visto que, além de criar mais uma barreira, protege as informações de qualquer ataque de origem interna.

Dessa forma, nos locais onde a necessidade de segurança for baixa, é utilizado um *proxy*, onde a necessidade for média, é utilizado um *firewall,* e onde a necessidade for alta, são utilizados um *firewall* e um *proxy* com conexão dedicada. Essa última proposta permite que todo acesso à rede crítica passe do *firewall* para o *proxy*, retornando para o *firewall*.

O grande segredo e complicação de toda essa proposta é a configuração dos equipamentos, com as respectivas regras, o que foge totalmente do escopo desse trabalho, que só propõe a analisar a arquitetura da rede.

Esta proposta eleva o nível da segurança dos dados que trafegam na INTRAER, tornando a rede mais confiável para o trâmite de informações, sejam elas sigilosas ou não.

5 - Conclusão

Este trabalho teve como escopo propor o aperfeiçoamento da arquitetura da INTRAER, de modo a garantir a segurança dos dados e informações transitados em seu meio.

Essa mudança na arquitetura é necessária, visto que atualmente a grande rede do COMAER não conta com nenhum dispositivo de segurança capaz de evitar a ação de pessoas mal intencionadas.

A necessidade de segurança é uma realidade, principalmente com a interligação de redes e a automatização e informatização dos processos. A guerra moderna tende a ser trabalhada nos pilares da segurança de dados, explorando suas falhas, como afirmou o General S. Bogdanov, Chefe de Estado-Maior para Assuntos Operacionais e Estratégicos da Rússia, fazendo referência à Guerra do Golfo:

"O Iraque perdeu a guerra mesmo antes dela começar. Essa foi uma guerra de inteligência, guerra eletrônica, comando, controle e contra-inteligência. As tropas iraquianas ficaram cegas e surdas. A guerra moderna pode ser vencida pela informática, e isso agora é vital." (DENNING, 1999, p. 7)

REFERÊNCIAS

1. BRASIL. Decreto nº 3505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 2000.
2. DENNING, Dorothy. Information Warfare and Security. United States of America: Addison Wesley, 1999. 522p.
3. MINISTÉRIO DA AERONÁUTICA. Comando-Geral de Apoio. NSMA 7-13. Segurança de Dados no Ministério da Aeronáutica. Brasília, 1999.
4. SIYAN, Karanjit et HARE, Chris. Internet Firewalls and Network Security. Indianapolis, USA: New Riders Publishing, 1995. 420p.