Criptografia e Segurança da Informação

Criptografia

António Santos

ISTEC

Tópicos

Segurança da Informação

A Segurança da Informação visa a proteção dos dados e informações de utilizadores ou organizações e para isso possui um conjunto de princípios, técnicas, protocolos, normas e regras que visam garantir um melhor nível de confiabilidade.

Princípios da Segurança da Informação

- Confidencialidade - Trata-se da garantia de que a informação não é disponibilizada ou divulgada a utilizadores, entidades ou processos não autorizados. Geralmente, restringindo o acesso mediante o uso de um nome de utilizador e password.
- Integridade - É a propriedade que garante a exatidão, corretude e completude da informação, ou seja, trata-se da garantia de que uma mensagem não foi alterada durante a transmissão.

Princípios da Segurança da Informação

- Autenticidade - É a garantia de que uma entidade é o que a mesma diz ser, ou seja, que os dados fornecidos são verdadeiros ou que o utilizador é o realmente o utilizador em causa.
- Disponibilidade - É a propriedade de que um sistema possa estar acessível e utilizável sob demanda de uma entidade autorizada a qualquer momento para solicitações.

Princípios da Segurança da Informação

- Não repúdio É a capacidade de comprovar a ocorrência de uma reivindicação de um evento ou ação e suas entidades originárias, quando uma mensagem é enviada, o destinatário pode provar que esta realmente foi enviada por determinada entidade ou o processo inverso. Também se tem a possibilidade de que uma pessoa não consiga negar um ato ou documento de sua autoria. Essa garantia é condição necessária para a validade jurídica de documentos e transações digitais.

Prevenção

- Proteção de hardware: impede acessos físicos não autorizados à infra-estrutura da rede, prevenindo roubos de dados, desligar de equipamentos, entre outros.
- Proteção de ficheiros e dados: proporcionada pela autenticação, controle de acesso e sistemas antivírus. Autenticação verifica a identidade do utilizador. O controle de acessos disponibiliza apenas as transações pertinentes ao utilizador e os programas antivírus garantem a proteção do sistema contra programas maliciosos.
- Proteção de perímetro: ferramentas de firewall e routers cuidam da proteção, mantendo a rede protegida contra tentativas de intrusão.

Detecção

- Alertas: sistemas de detecção de intrusões alertam os responsáveis pela segurança sobre qualquer sinal de invasão ou mudança suspeita no comportamento da rede que possa significar um padrão de ataque. Os avisos podem ser via e-mail, mensagem na consola de administração, telemovel, etc.
- Auditoria: periodicamente deve-se analisar as partes críticas do sistema a procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram; por ex: modificações no tamanho dos arquivos de passwords, utilizadores inativos, etc.

Recuperação

- Backup dos dados: manter sempre atualizados e testados os arquivos de segurança em suporte confiável e separados física e logicamente dos servidores.
- Aplicativos de Backup: ferramentas que proporcionam a recuperação rápida e confiável dos dados atualizados em caso da perda das informações originais do sistema.
- Backup do Hardware: a existência de hardware reserva, fornecimento autónomo de energia, linhas de dados redundantes, etc.

Proteção contra ataques

- Proteção da rede e da navegação na Internet
- Manutenção e atualização constante de sistemas
- Orientação dos utilizadores para identificar riscos e prevenir ataques

Rede da Empresa Protegida

Para manter a rede da empresa protegida é fundamental a utilização de uma firewall, com regras e bloqueios adequadamente configurados e atualizados.

Rede da Empresa Protegida

Existem soluções complexas com servidores de rede em Linux com firewall, proxy e outros serviços.

Rede da Empresa Protegida

- pfSense como alternativa de software livre
- Soluções conhecidas como Firewall UTM,
- Mercado: SonicWall, Fortinet, Juniper Networks, Sophos, entre outros.

Estas soluções têm como característica comum a necessidade de alto investimento em equipamentos e necessidade de manutenção constante por profissionais especializados.

Manutenção e atualização constante de sistemas

Fabricantes de sistemas e antivírus acompanham em tempo real o surgimento de novos métodos ou técnicas de ataque e sempre que identificado algo novo, rapidamente implementam correções e a proteção adequada em seus sistemas.

Manutenção e atualização constante de sistemas

Hardware bem configurado, routers sem portas disponiveis, uso de portas não padrão para comunicações, etc.

Orientação dos utilizadores para identificar riscos e prevenir ataque

Orientar os utilizadores a identificarem possíveis ameaças e evitarem ações que possam permitir a entrada de algum vírus. Antes de qualquer medida a ser implementada, comece por orientar os colaboradores da organização sobre os riscos e prejuízos, formas de ataque e o que fazer para evitar incidentes.

Orientação dos utilizadores para identificar riscos e prevenir ataque

Os criminosos procuram explorar a falta de conhecimento e curiosidade dos utilizadores, enviando mensagens falsas por e-mail, com assuntos populares ou fazerem-se passar por pessoas conhecidas e confiáveis, induzindo os utilizadores a clicarem em links contidos no conteúdo das mensagens, que direcionam para sites nocivos - Phishing.

Orientação dos utilizadores para identificar riscos e prevenir ataque

- Os utilizadores devem evitar o uso das redes sociais e/ou aceder a websites que não sejam de uso profissional por forma a evitar a criação de falhas de acesso.
- Não devem ter previlégios para instalar software, pois estes são muitas vezes seduzidos por certo tipo de software que pode vir infetado.

Catastrofes Naturais

- Ambientais - tremores de terra, incêndios, inundações, queda de raios, tempestades magnéticos, etc.;
- Politicas - ataques terroristas, motins, etc.;

Catastrofes Fisicas

- Politicas - ataques terroristas, motins, etc.;
- Materiais - degradação irreparavel, perda ou roubo de equipamentos computacionais, como discos magnéticos, computadores portáteis, etc.

Falhas Previsiveis dos Sistemas

- Quebra no fornecimento de energia elétrica ou falha na fonte de alimentação de um equipamento.
- Bloqueio na execução de aplicações ou sistemas operativos.
- Falhas temporárias de conectividade em troços de redes.

Defesas Contra Atividades não Autorizadas

- Acesso a informação - todos os tipos de acesso a informações reservadas ou confidenciais, logo, não explicitamente tornadas públicas, guardadas em sistemas computacionais ou em trânsito na rede.
- Alteração de informação - incluem-se todas as atividades que, de forma camuflada ou explicita, alterem ou eliminem informação pertencentes a terceiros sem autorização, guardada em sistemas computacionais ou em transito em redes.

Defesas Contra Atividades não Autorizadas

- Utilização exagerada ou abusiva de recursos computacionais - os recursos computacionais podem ser de diversos tipos: tempo de processamento, memoria primária ou secundária, tempo e material de impressão, ocupação de redes de comunicação, etc.
- Impedimento de prestação de serviço de DoS (Denial of Service) - o impedimento de prestação de serviço é um caso extremo de uso excessivo ou abusivo de recursos computacionais. E é extremo porque o objetivo primeiro da atividade ilícita é impedir que terceiros tenham acesso aos recursos afetados sem qualquer usufruto próprio dos mesmos.

Princípios de Prevenção e Proteção

As formas de proteção da informação devem ser definidas a partir da análise das possíveis ameaças e riscos que a rede está submetida, com a finalidade de manter sua confidencialidade, disponibilidade e integridade, e também para atender aos objetivos de gestão traçados pela alta direção.

Sistemas de Detecção de Intrusões

- Baseados em host (Host-based Intrusion Detection Systems - HIDS)
- Baseados em rede (Network-based Intrusion Detection Systems - NIDS).

Detecção de Anomalias

Uma anomalia é definida como algo diferente, anormal, peculiar ou que não seja facilmente classificado. Apesar desse conceito se aplicar a praticamente tudo, estamos interessados em como se aplica à segurança de computadores. Neste contexto, uma anomalia pode ser definida como ações ou dados que não sejam considerados normais por um determinado sistema, utilizador ou rede.

Tipos de Anomalias

- Anomalias em Padrões de Tráfego: Os sistemas que procuram por anomalias em padrões de tráfego da rede são considerados sistemas de anomalias no padrão de tráfego.
- Anomalias em Padrões de Protocolos: Os sistemas que procuram por anomalias em padrões protocolos são considerados sistemas de anomalias de protocolos.