Controle de Acesso Lógico e Físico

Prof. Alexandre Beletti Ferreira

Problema

- Com as informações armazenadas em computadores interligados com outros computadores no mundo todo surgi a necessidade de uma forte segurança de acesso lógico, ai é que vem o conceito de controle de acesso lógico. Mais primeiro teremos que entender o que são controles de acesso.

Definição

- Controle de acesso, físico e lógico, tem como objetivo proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação e divulgação não autorizada. Os sistemas computacionais, bem diferente de outros tipos de recursos, não podem ser protegidos apenas com dispositivos físicos como cadeado, correntes.

Controle de Acesso Físico

- O principal objetivo da implantação de controles de segurança física, é restringir o acesso às áreas críticas da organização, prevenindo os acessos não autorizados que podem acarretar danos a equipamentos, acessos indevidos à informação, roubos de equipamentos, entre outros.
  Os controles de acesso físico devem ser implementados em conjunto com os controles de acesso lógico. A falta de implementação desses dois controles em conjunto, seria o mesmo que restringir o acesso as informações através de senhas, mas deixar os servidores desprotegidos fisicamente, vulneráveis a roubo, por exemplo.

Localização do CPD

- A localização do CPD é um fator de grande importância, pois é ela que vai determinar as vulnerabilidades do CPD a fatores ambientais, e vulnerabilidades quanto ao acesso.
  Antes da escolha do local onde o CPD será implantado devemos observar, se o mesmo estará vulnerável aos seguintes itens: inundações; impacto de escombros; excesso de calor; excesso de poeira; excesso de umidade; excesso de radiação; magnetismo; vandalismo; exposição a gases nocivos.

Localização do CPD

- Devemos observar ainda se há proximidade de caixas d'água, materiais inflamáveis e se o CPD ficará próximo a entrada da empresa ou da fábrica.
  A proximidade do CPD à entrada da empresa ou da fábrica determina a facilidade de acesso por pessoas não autorizadas, e também o grau de dificuldade de acesso de pessoas autorizadas em dias de greve, paralizações e manifestações.

Controle de Acesso

- O acesso ao CPD deve ser restrito ao pessoal autorizado, para tanto as portas devem permanecer trancadas, e devem ser implementados controles de acesso, que registrem quem entrou no CPD, horário e permanência.
  Algumas opções de controle de acesso, são: crachas eletrônicos, dispositivos biométricos, trancas manuais usadas em conjunto com outros controles, como por exemplo lista de permanência.

Acesso de Prestadores de Serviços

- O acesso de prestadores de serviços, ou de qualquer pessoa que não esteja autorizada a acessar e permanecer no CPD, deve ser controlado e registrado, essas pessoas sempre devem estar acompanhadas de um funcionário do CPD.

Monitoramento

- O uso de câmeras de monitoramento, é importante para se monitorar o que acontece dentro e fora, próximo as entradas do CPD. Esse tipo de monitoramento é utilizado para inibir possíveis ações não autorizadas, tentativas de burla dos controles de acesso, e também é utilizado para auxiliar na detecção de responsáveis.

Cabeamento

- A estrutura do cabeamento do CPD é importante para evitar panes e problemas com a comunicação da rede da organização, portanto devem ser tomados cuidados na hora de se estruturar o cabeamento, e deve ser utilizado piso falso em todo o CPD.

Portas e Janelas

- As janelas do CPD devem estar protegidas por grades, e as portas além de estarem trancadas devem ser do tipo corta-fogo, para evitar que em caso de incêndio, o fogo se propague rapidamente.

Controles Ambientais

- Os equipamentos de informática devem estar protegidos contra fatores ambientais, como calor, umidade, poeira, fogo, etc.
  No CPD devem ser implantados os seguintes equipamentos de controle ambiental: ar condicionado; termômetros; controle de umidade; detector de fogo e fumaça; extintor de incêndio.
  A quantidade de cada equipamento varia de acordo com o tamanho da sala, porém são indispensáveis em um CPD. É recomendável que exista também um extintor de incêndio fora do CPD, próximo a porta de entrada.

No Break

- O uso de um no break é indispensável para garantir o processamento das informações em caso de interrupção no fornecimento de energia.

Backup

- O backup é um elemento fundamental na recuperação dos dados e retomada do processamento das informações. Para garantir que esse recurso esteja disponível quando necessário é recomendado que seja criado um site backup.
  Site backup é uma sala que possui as mesmas características do CPD utilizado na organização, contendo os mesmos tipos de equipamentos, com as mesmas configurações, em suma é uma cópia do atual CPD, que estará sempre disponível para assumir, se necessário, todas as operações e funções do CPD original.

Backup

- O site backup deve estar localizado fora da empresa, pois se a sua ativação for decorrência de um desastre, ele não será afetado. Nele devem conter os últimos backups feitos, mantendo as informações atualizadas.
  Independente do uso do site backup, as fitas de backup devem ser armazenadas em local externo a organização em cofres anti-chamas, deve ser mantida ainda uma cópia do backup atual no CPD em cofre apropriado, para a rápida recuperação dos dados.

Metodologia de Backup

- O backup dos sistemas críticos devem estar preferencialmente separados
  dos outros backups para facilitar a sua restauração.
  Os cuidados tomados com essas fitas, devem ser os mesmos utilizados na
  política de backup utilizada pela organização, sendo observados os seguintes itens:
  -local onde serão armazenadas as fitas de backup;
  -uso de cofres;
  -controle da ordem cronológica de baixa dos backups;
  -controle da vida útil das fitas de backup;
  -simulações periódicas da restauração dos backups.

Controle de Acesso Lógico

- Controle de acesso lógico são medidas e procedimentos com o objetivo de proteger as informações contra acesso não autorizado feito por pessoas ou programas. Este controle pode ser encarado de duas maneiras diferentes, através do controle ao recurso compartilhado ou do usuário que deverá ter certos privilégios.

Controle de Acesso Lógico

- A proteção de recursos computacionais baseia-se nas necessidades de acesso de cada usuário, quanto a identificação e autenticação do usuários normalmente são feitas através de uma ID (identificação) e senha.

Segurança Lógica - Autenticação

- Autenticação é a capacidade de garantir que um usuário é de fato quem ele diz ser. É uma das funções de segurança mais importantes que um sistema operacional deve fornecer. Os mecanismos de autenticação podem ser divididos em quatro categorias:

Algo que você sabe

- O mecanismo mais utilizado é o onipresente, mas relativamente inseguro, par formado pelo nome do usuário e sua senha, assim como números PIN usados para acesso a Banco 24 Horas e combinações de cofres.

Algo que você tem

- Chaves de carro, cartões de banco 24 horas, e outros dispositivos físicos são mecanismos de autenticação que exigem a posse física de um dispositivo sem igual identificar um usuário.

Algo que você é

- Impressões digitais, análise de retina e reconhecimento de voz são exemplos de mecanismos biométricos que podem ser usados para fornecer um nível bem alto de autenticação.

Algum lugar onde você está

- Endereços de adaptador de rede, caller-ID, e sistema baseado em Posicionamento Global via Satélite provêem informação de autenticação baseada na localização do usuário.

- Sistemas de autenticação forte geralmente requerem simultaneamente o uso de pelo menos dois destes mecanismos. Por exemplo, o acesso à sua conta bancária em um banco 24 horas requer tanto a posse física do cartão 24 horas como o conhecimento do PIN. A confidencialidade da informação usada para autenticar os usuários é extremamente importante. Se você escrever o número do PIN no cartão 24 horas, a autenticação forte está perdida. Semelhantemente, se a informação de nome e senha do usuário trafegar abertamente através da rede, é impossível obter-se uma autenticação confiável.

Senhas

- Senha de acesso é o método mais utilizado, pelas empresas para a autenticação de usuários. Porém para garantir o seu uso adequado, deve ser definida uma política de senhas, em que sejam criadas regras para a criação, troca e uso das mesmas. As regras definidas devem ser divulgadas a todos os funcionários e colaboradores da organização.

SmartCards

- Na autenticação com Smart Cards é utilizada a combinação de um cartão com uma senha.
  Smart card é um tipo de cartão plástico semelhante a um cartão de crédito com um ou mais microchips embutidos, capaz de armazenar e processar dados. Um smart card pode ser programado para desempenhar inúmeras funções.
  É utilizado tanto para controle de acesso lógico como para controle de acesso físico.

Biometria

- Este tipo de tecnologia utiliza a análise de características humanas, como impressões digitais, retina, rosto e de padrões de voz e de assinatura.
  A vantagem sobre as outras tecnologias de autenticação é que o usuário é identificado por características únicas, pessoais e intransferíveis, dispensando o uso de senhas, cartões ou crachás.
  É utilizado tanto para controle de acesso físico como para controle de acesso lógico.

One-time password

- Esta tecnologia consiste em fornecer uma senha de acesso diferente a cada determinado intervalo de tempo (1 minuto, 30 segundos, etc.), permitindo que o usuário se conecte naquele instante.
  As tecnologias de one-time password tornam sem efeito a ação de sniffers, já que a cada conexão uma nova senha deve ser informada, permitindo que seja utilizado um canal inseguro.
  Para a geração das senhas são utilizados tokens no formato de cartões, chaveiros ou aparelhos semelhantes a calculadoras.

Bibliografia

- SCUA – Segurança da Informação

http://www.scua.com.br/site/seguranca/