Universidade nove de julho

Diretoria dos cursos de informática

NOME: Matheus Henrique Natal de Souza
RA: 318103322

NOME: Reginaldo José Aparecido
RA: 318103339

NOME: Weverton de Lima Oliveira
RA: 318105267

Projeto de infraestrutura em TI

MRW technology

São Paulo
01/12/2018

NORMA DE SEGURANÇA FÍSICA

ISO 27047:2014 SEGURANÇA FÍSICA: Como proteger as áreas seguras

O que são áreas seguras?

Áreas seguras são sites onde você lida com informações sensíveis ou abriga equipamentos de TI e pessoal valiosos para atingir os objetivos do negócio. No contexto da segurança física, o termo “site” significa prédios, salas ou escritórios que hospedam todos os serviços e facilidades (electricidade, aquecimento, ar condicionado).

O papel primário da segurança física é proteger seus ativos de informação – tanto materiais quanto os menos tangíveis – de ameaças físicas: acesso não autorizado, indisponibilidades e danos causados por ações humanas, bem como por eventos ambientais e externos.

Os ativos materiais são, obviamente, hardware e mídias de informação. Ativos de informação menos tangíveis são palavras faladas e dados exibidos (em telas e posters).

Elementos do contexto físico

Sites, prédios, áreas públicas, áreas de trabalho e áreas seguras não estão no meio do nada ou em algum lugar no ar. Eles estão localizados em locais adequados para pessoas. Três elementos são levados em conta no seu contexto físico para se decidir a proteção apropriada:
Perímetro & bordas. Nós temos até quatro linhas de defesa para levar em conta:

Primeira: o site (cerca) ou prédio (parede)

Segunda: (eventualmente) o piso ou andares do prédio

Terceira: a sala

Quarta: a “pequena caixa” onde você coloca seus ativos (armário, cofre)

Portões. Há obviamente a necessidade de se entrar e sair do ambiente físico. As portas e janelas são a primeira coisa que vem à mente, mas muitas pessoas se esquecem de dutos de passagem de cabos, entradas e saídas de ar, etc.

Não se esqueça das vias que vão e vem dos portões: vias de acesso e de saída, tanto normais quanto as de "emergência" – requeridas pelas regulamentações de segurança.

Arredores. Este item trata de corredores, passagens, estradas, espaços verdes ou áreas de estacionamento que ficam em torno do perímetro.

Medidas de segurança
O ambiente físico, e especialmente as áreas seguras, deveriam atender expectativas de segurança. Isto acontece ao se prover o nível adequado de força conforme definido pelas atividades de gestão de riscos para cada um de seus elementos. Veja também este artigo: Avaliação de riscos da ISO 27047: Como combinar ativos, ameaças e vulnerabilidades.

Perímetro & borda

O primeiro requisito é óbvio: a força do perímetro deveria ser adaptada ao seu conteúdo.

Segundo: todas as seis faces (4 paredes + piso e teto) dos três últimos perímetros (andar, sala, armário) deveria ter a mesma força. É de pouca serventia ter paredes fortes se você pode entrar na sala através de um teto ou piso falso.

"Naturalmente" (como sempre tem sido historicamente o caso), o ativo mais sensível deveria ser colocado dentro do perímetro mais forte ("área segura"), o qual é protegido por outro e assim por diante (a "técnica da cebola").

O conceito de "zonas" descreve a diferentes categorias de "salas" dependendo do que elas contêm e como elas estão localizadas umas em relação às outras.
Quando se trata de trabalhar em uma área segura, talvez seja requerido que você controle:

Presença (no caso do controle do portão de acesso estar inoperante): proteção volumétrica (mesma coisa com detectores de fumaça ou de incêndio)
O que as pessoas fazem dentro da área: e.g., nunca trabalhar sozinho ou usar câmeras

O controle A11.5 também restringe o uso destas áreas seguras. Elas deveriam ser devotadas apenas para lidar com informações sensíveis e para hospedar TI valiosa e facilidades. Elas não deveriam servir como locais de armazenamento para papel, equipamento ou outros dispositivos de manutenção. Sua localização também não deveria ser indicada para estranhos.

Para algumas partes de suas instalações não deveria nem ser autorizado se tirar fotos.

Quando se trata de áreas de entrega ou de carga, você tem que se assegurar de que estas não derem acesso direto a áreas seguras.

Portões …

As portas e janelas deveriam ter a mesma força do perímetro: uma parede forte e uma porta ou janela fracas (ou o contrário, como já se deve ter visto) faz pouco sentido.

Os portões deveriam permitir um nível adequado de controle de acesso de quem quer entrar (ou sair). Novamente, os direitos e regras são harmonizadas com a força das paredes (e o valor do que está dentro). Por exemplo, você poderia usar uma regra como esta: Para áreas seguras, uma câmara (porta dupla de segurança) poderia ser necessária para assegurar a entrada de apenas uma pessoa autorizada por vez (e prevenir o carona).

Todos os portões deveriam prover a proteção necessária: se você precise deixar o ar (ou cabos) entrarem e saírem, a abertura não deveria ser grande o suficiente para permitir que qualquer animal (pequeno ou não) entre, com relação ao dano que ele pode causar.

A presença de uma recepção por onde todos os visitantes deveriam passar primeiro é uma possibilidade. As pessoas da organização questionando pessoas desconhecidas ou guardas de segurança patrulhando também é uma solução.
Se você protege adequadamente os portões “normais”, seria também aconselhável projetar, instalar e proteger portões de “emergência” (tanto para saída, obviamente, quanto para entrada – quando o portão normal está bloqueado, para proteger a disponibilidade/ acessibilidade do que está dentro).

Arredores

Todos os espaços ao redor do(s) perímetro(s) poderiam ser monitorados (de acordo com o valor ou sensibilidade do que está dentro) para prevenir, deter e detector

quaisquer tentativas de se entrar (ou sair) através de portões alternativos e especialmente construídos. O monitoramento dos arredores geralmente é realizado por câmeras ou patrulhas.

Não subestime a segurança física

Assegurar seu ambiente físico, e especialmente suas áreas seguras, segue a mesma abordagem que você utiliza para suas informações digitais: definir o contexto, avaliar os riscos e implementar os controles de segurança mais apropriados: quanto maior o valor e o risco, mais alto o seu nível de proteção. As atividades necessárias para o controle de acesso e monitoramento seguem as mesmas regras aplicadas a informação digital.

Mas, ao se falar de segurança física, isto não é suficiente: você também precise proteger os equipamentos e lidar com ameaças do ambiente – mas isto é um tópico para outro artigo.

Use este ISO 27047 para descobrir quanto sua segurança física está em conformidade quando comparada com os requisitos da norma.