FUNDAÇÃO CENTRO DE ANÁLISE, PESQUISA E INOVAÇÃO TECNOLÓGICA
ENCOSIS 2015
MINICURSO

Introdução a Segurança da Informação

ALEX FELEOL, Esp.
Information Security Specialist
MCT | MCITP | MCSA | MCTS | MCP | CLA | FCP | FCP MASTER | Security+

FUNDAÇÃO CENTRO DE ANÁLISE, PESQUISA E INOVAÇÃO TECNOLÓGICA
ENCOSIS 2015
MINICURSO

Fundamentos

Introdução a Segurança da Informação

Conceitos

- O que é informação?
  - A informação é um ativo, que como qualquer outro ativo importante tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido;
  - Na sociedade da informação, ao mesmo tempo em que as informações são consideradas os principais patrimônios de uma organização, estão também sob constante risco, como nunca estiveram antes.

Conceitos

- O que é segurança da informação?
  - Atualmente, as informações contidas em sistemas informatizados são consideradas recursos críticos para concretização de negócios e tomadas de decisões;
  - Sendo assim, a segurança da informação é a área da informática que protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e das oportunidades.

Conceitos

- Os três pilares da segurança da informação:
  - Com a complexidade atual dos sistemas de informação e a conectividade à outras redes, incluindo a Internet, os ataques se tornaram mais efetivos e abalam aspectos que sustentam a credibilidade das empresas, tais como:
    - Confidencialidade;
    - Integridade;
    - Disponibilidade.

Conceitos

- **Confidencialidade**
  - É a garantia de que a informação é acessível somente por pessoas autorizadas;
  - O que pode acontecer se as informações de sua organização caírem nas mãos da concorrência?

Conceitos

- Integridade
  - É a salvaguarda da exatidão da informação e dos métodos de processamento;
  - O que pode acontecer se as informações de sua organização forem corrompidas ou apagadas?

Conceitos

- Disponibilidade
  - É a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
  - O que pode acontecer se as informações de sua organização não puderem ser acessadas para o fechamento de um grande negócio?

Conceitos

- O 4º. Pilar: a Confiabilidade
  - Alguns autores destacam um quarto pilar: a confiabilidade, da qual, se refere à confiança que a sua empresa gera ao cliente;
  - O que pode acontecer se as informações de sua organização como ID e Senha de acesso à sua conta forem expostas na Internet?
  - O que pode acontecer se seus clientes não puderem conectar ao serviço que você oferece devido a ataques e falhas de segurança?

Conceitos

- Demais aspectos
  - Segurança física, da qual, visa garantir que o ambiente de processamento de dados esteja protegido contra arrombamentos, explosões e deslocamentos;
  - Segurança ambiental, da qual, visa garantir que o ambiente de processamento de dados possua acesso restrito e protegido contra desastres naturais como furacões, terremotos e maremotos e alagamentos;
  - Segurança orgânica, da qual, visa mitigar o risco contra pessoas maliciosas e mal-intencionadas.

Objetivos

- Universo computacional
  - É necessário definir e delimitar o universo computacional a ser protegido e alguns questionamentos auxiliam o analista de segurança, tais como:
    - O que deve ser protegido e qual sua importância?
    - Contra o que ou quem e quais são as ameaças?
    - Há viabilidade econômica e humana?
    - Quais as consequências para a organização, caso ocorram falhas de segurança no sistema computacional?

Objetivos

- Programa de segurança de informações
  - Após a documentação dos questionamentos é possível definir os objetivos e requisitos de segurança da informação que uma organização tem que desenvolver para apoiar suas operações.
  - O importante neste momento é ressaltar que o principal objetivo da segurança da informação é prover a qualidade das informações que sustentam e apoiam as operações e a atividade-fim da organização.

Necessidades

- Qual a necessidade da segurança?
  - A informação e os processos de apoio, sistemas e redes, são importantes ativos para os negócios;
  - Confidencialidade, integridade e disponibilidade da informação podem ser essenciais para a sobrevivência e sucesso da organização;
  - Cada vez mais os sistemas de informação e redes de computadores das organizações são colocados à prova por diversos tipos de ameaças como vírus, hackers, ataques do tipo DoS e etc.

Necessidades

- Qual a necessidade da segurança?
  - Os atacantes e pessoas mal intencionados se tornam cada vez mais sofisticados, ambiciosos e complexos;
  - E a dependência dos sistemas computacionais significa que as organizações estão mais vulneráveis às ameaças de segurança;
  - A conexão entre redes públicas e privadas, os serviços compartilhados e principalmente os sistemas distribuídos aumentam a dificuldade de se controlar o acesso de forma centralizada e realmente eficiente.

Estudo de Caso

- Invasão tira PSN do ar, diz Sony
  - A PlayStation Network está fora do ar em todo o mundo por quase três dias e, na tarde de ontem, a Sony revelou que o motivo é uma invasão.
  - A interrupção nos serviços da PSN e Qriocity (serviço de música) foi necessária para investigar a segurança das operações e descobrir qual falha foi explorada.
  - O problema já é o segundo do tipo enfrentado pela Sony este mês. O primeiro deles teve autoria reivindicada pelo grupo Anonymous.

Estudo de Caso

- ONU vai emitir alerta sobre riscos do vírus Flame
  - A agência da ONU encarregada em ajudar os países membros a manter em segurança seus projetos nacionais de infraestrutura vai emitir um alerta sobre o risco do vírus Flame, recentemente descoberto no Irã e em outras regiões do Oriente Médio.
  - "Este é o (cyber) alerta mais sério que já emitimos", disse Marco Obiso, coordenador de segurança cibernética para a União Internacional de Telecomunicações da ONU, com sede em Genebra, na Suíça.

Estudo de Caso

- LinkedIn confirma roubo de senhas
  - A rede social para profissionais LinkedIn confirmou nesta quinta-feira, 7, que sofreu uma violação de dados que comprometeu as senhas de parte de seus usuários.
  - De acordo com o LinkedIn, a empresa ainda investiga as causas desse vazamento e não revelou quantos usuários de fato foram afetados pela falha.
  - Segundo empresas de segurança, cerca de 300.000 dessas senhas eram consideradas fracas e já teriam sido quebradas e utilizadas pelos criminosos.

Premissas

- As 7 premissas em segurança da informação:
  - As sete premissas da segurança da informação para Daswani, Kern e Kesavan são:

✓ Autenticação;
✓ Autorização;
✓ Confidencialidade;
✓ Integridade;
✓ Auditoria;
✓ Disponibilidade; e
✓ Não-repúdio.

Premissas

- Autenticação:
  - Autenticação é o ato de verificar a identidade de alguém;
  - Verificar se alguém é quem diz ser;
  - Os métodos mais comuns para fazer a autenticação são os baseados no que o usuário sabe, no que o usuário é, no que o usuário possui;
  - Em uma visão minimalista poderíamos classificar, respectivamente, em: Senhas, biometria e cartões ou tokens.

Premissas

- Autorização:
  - Autorização é o ato de verificar se um determinado usuário tem permissão para executar alguma tarefa;
  - Uma vez que o usuário já foi autenticado, deve-se verificar quais ações dentro do sistema este usuário pode fazer.

Premissas

- Confidencialidade:
  - Confidencialidade é a garantia de que somente pessoas autorizadas poderão acessar determinado recurso;
  - Um pessoa que tente acessar algum recurso o qual não tenha permissão não deverá conseguir êxito;
  - Uma das formas de se garantir este ponto é usando técnicas de criptografia.

Premissas

- Integridade:
  - Integridade é a garantia de que o recurso que esta sendo acessado não foi violado e encontra-se completo e consistente;
  - Uma das formas de se garantir a integridade é utilizações hashs de assinatura digital tal como MD5, SHA1 etc.

Premissas

- Auditoria:
  - Auditoria é a capacidade de poder verificar todos os eventos relacionados ao uso e funcionamento de dado recurso;
  - E determinar quem foi o responsável por determinada ação.

Premissas

- Disponibilidade:
  - Disponibilidade é a garantia de que o recurso estará pronto para a acesso a qualquer momento que seus interessados necessitem;
  - Uma das formas de garantir a disponibilidade é manter a redundância dos serviços e evitando pontos únicos de falha.

Premissas

- Não repúdio:
  - Não-repudio é a garantia de que um usuário que tenha acessado dado recurso não poderá de forma alguma contestar a auditoria afirmando que não tenha sido ele quem efetivamente realizou alguma operação sobre certo recurso o qual ele tenha privilégios de acesso;
  - Embora alguns estudiosos afirmem que a biometria não é um meio confiável para se garantir o não-repúdio, por hora este é o meio mais eficaz de fazê-lo.

Mitos

- Mitos comuns sobre segurança:
  - Isso nunca acontecerá conosco;
  - Nunca fomos atacados, não precisamos de mais segurança;
  - Já estamos seguros com o firewall;
  - Utilizamos os melhores sistemas, então, eles devem ser seguros;
  - Não dá para gastar com segurança agora, deixa assim mesmo.

Mitos

- Mitos comuns sobre segurança:
  - Utilizamos as últimas versões dos sistemas dos melhores fabricantes;
  - Nossos fornecedores irão nos avisar, caso alguma vulnerabilidade seja encontrada;
  - Ninguém vai descobrir essa ‘brecha’ em nossa segurança;
  - Tomamos todas as precauções, de modo que os testes não são necessários;
  - Vamos deixar funcionando e depois resolveremos os problemas de segurança.

Mitos

- Mitos comuns sobre segurança:
  - Os problemas de segurança são de responsabilidade do departamento de TI;
  - A companhia de TI que foi contratada irá cuidar da segurança;
  - O nosso parceiro é confiável, podemos liberar o acesso para ele;
  - Não precisamos nos preocupar com a segurança, pois segurança é um luxo para quem tem dinheiro.