Parâmetros para Definição do Plano de Segurança em TI

Projeto de Segurança em TI – *Definição* ISO 17799

Consiste no desenho de arquiteturas de segurança com o objetivo de introduzir mecanismos tecnológicos e procedimentos de proteção dos sistemas de TI. A metodologia a ser utilizada deve garantir numa primeira fase a análise dos requisitos de segurança críticos para o suporte ao negócio, sendo posteriormente realizado o desenho da arquitetura final e identificadas às políticas de segurança mais adequadas à operacionalização do negócio.

A arquitetura de segurança desenhada deve ser pautada pelos *padrões* da área de segurança, nomeadamente o BS-7799 ou ISO17799, visando à proteção da informação no que respeita a **privacidade** (foco: confidencialidade), **integridade** (foco: origem = destino) e **disponibilidade** (acesso).

O desenho de arquiteturas de segurança é conduzido por especialistas que avaliam quais os serviços, técnicas e mecanismos que conferem segurança aos sistemas. O desenho de arquiteturas de suporte seguro ao negócio garante a integridade, privacidade e disponibilidade da informação distribuída à colaboradores, parceiros e clientes.

O primeiro passo no processo de levantamento ou do desenho do projeto de segurança de TI é fazer o levantamento técnico e de procedimentos que atualmente já estão implementados na empresa. Deve-se mapear todo o ambiente de segurança existente, relacionando ferramentas utilizadas, processos, políticas, metodologias e os negócios a proteger.

As nove perguntas a seguir são baseadas em recomendações padrões inerentes à norma supra citada (BS7799) e não em produtos, irão auxiliar o processo de mapeamento da situação atual da empresa em relação à segurança de TI.

1. A segurança dos sistemas de TI críticos para o negócio é implementada através de mecanismos *padrão* de mercado, cobrindo todas as fases do ciclo de vida da segurança para a proteção, detecção e recuperação da informação?

2. Está sendo feita a proteção dos sistemas de TI de acordo com as necessidades e requisitos de cada negócio ou atividade de suporte ao mesmo ?

3. A configuração dos sistemas de TI é levada a cabo por Especialistas que garantem a implementação de arquiteturas de segurança de acordo com as melhores práticas de mercado, reforçando a segurança de sistemas operativos e aplicações?

4. Uma vez implementados, os mecanismos de proteção permitem a defesa dos sistemas de TI que suportam o negócio, detectando falhas de segurança em tempo real e possibilitando uma resposta imediata ao evento de um incidente?

5. Os sistemas de software e/ou hardware responsáveis pela segurança de TI da empresa contam com um procedimento periódico de atualização?

6. O serviço é executado segundo uma metodologia de trabalho, composta pelas fases de análise de requisitos, implementação e testes, sendo produzida documentação de suporte para apoio em momentos de emergência, expansão e reavaliação do plano de segurança?

7. É desenvolvido um conjunto de recomendações e orientações sobre medidas de segurança e responsabilidade dos usuários, incluindo o esclarecimento efetivo das restrições de acesso ao software e/ou hardware implementados, por forma a tornar a gestão da segurança mais eficaz?

8. A organização está em conformidade com a legislação em vigor no que respeita à escolha, tratamento e proteção da informação?

9. O projeto de Segurança de TI tem por base a instalação e configuração de:
   - Firewalls,
   - Antivírus;
   - Sistemas de detecção de intrusão;
   - Controle de acessos e segurança de conteúdos (gerenciamento de conteúdo). Web Mail; Web Page e Anti-Span.

Padrão de Segurança: ISO 17799

• INTRODUÇÃO

Os gerentes de segurança vêm a muito tempo esperando por alguém que produza um conjunto razoável de padrões de segurança de informações, reconhecido globalmente. Muitos acreditam que um código de prática, ajudaria a suportar os esforços dos gerentes de TI. Ajudaria também a influenciar decisões, aumentaria a cooperação entre os vários departamentos em nome do interesse comum pela segurança e ajudaria a tornar a segurança, uma das prioridades organizacionais.

Desde o seu lançamento pela Organização de Padrões Internacionais ISO - **I**nternational **S**tandards **O**rganization, em dezembro de 2000, o ISO 17799 se tornou o padrão de segurança mais reconhecido em todo o mundo. O ISO 17799 é definido como "um abrangente conjunto de controles formado pelas melhores práticas em segurança de informações".

- **As origens do ISO 17799**

Por mais de 100 anos, o British Standards Institute (BSi) e o International Organization for Standardization (ISO) vêm fornecendo referências globais para padrões operacionais, de fabricação e de desempenho. Uma coisa que o BSi e o ISO não tinham ainda proposto era um padrão para a segurança de informações. Finalmente em 1995, o BSi lançou seu primeiro padrão de segurança, BS 7799. O BS 7799 foi criado com a intenção de abranger assuntos de segurança relacionados ao e-commerce. Em 1995, problemas como o Y2K e EMU tornaram-se precedentes sobre todos os outros assuntos. Para piorar, o BS 7799 foi considerado inflexível e não foi adotado globalmente. O momento não era correto e questões de segurança não despertavam grande interesse naquele tempo.

Avancemos para quatro anos mais tarde. Em maio de 1999, o BSi tentou novamente, lançando a segunda versão do BS 7799, uma enorme revisão da versão anterior. Essa edição continha vários aperfeiçoamentos e melhoras desde a versão de 1995. Foi nessa época que o ISO identificou a oportunidade e começou a trabalhar na revisão do BS 7799. Em dezembro de 2000, o International Standards Organization (ISO) adotou e publicou a primeira parte do BS7799 como seu próprio padrão, chamando-o ISO 17799. Nessa mesma época, uma maneira formal de credenciamento e certificação de compatibilidade com os padrões foram adotadas. O Y2K, EMU e outras questões foram concluídas ou reduzidas no ano 2000, e a qualidade geral do padrão melhorou dramaticamente. A adoção do BS 7799 Parte 1 (o critério padrão) pelo ISO foi mais aceitável por um eleitorado internacional, e foi nessa época que um conjunto de padrões de segurança finalmente recebeu reconhecimento global.

• **Uma estrutura de recomendações**

O padrão ISO 17799 elimina a segunda parte do BS 7799, que abrange implementação. O ISO 17799, como é conhecido hoje, é uma compilação de recomendações para melhores práticas de segurança, que podem ser aplicadas por empresas, independentemente do seu porte ou setor. Ele foi criado com a intenção de ser um padrão flexível, nunca guiando seus usuários a seguir uma solução de segurança específica ao invés de outra.

As recomendações do ISO 17799 continuam neutras com relação à tecnologia e não fornecem nenhuma ajuda na avaliação ou entendimento de medidas de segurança já existentes. Por exemplo, discute a necessidade de firewalls, mas não aprofunda nos três tipos de firewalls e como devem ser usadas. Isso leva alguns opositores a dizer que o ISO 17799 é muito vago e pouco estruturado para ter seu valor realmente reconhecido.

A flexibilidade e imprecisão do ISO 17799 é intencional, pois é muito difícil criar um padrão que funcione para todos os variados ambientes de TI, e que seja capaz de crescer com a mutante paisagem tecnológica atual. Ele simplesmente fornece um conjunto de regras, em uma indústria onde elas não existiam.

• **As dez áreas de controle do ISO 17799:**

1. Política de Segurança ⇒ É necessário uma política para determinar as expectativas para segurança, o que fornece direção e suporte ao gerenciamento. A política deve também ser usada como uma base para revisões e avaliações regulares.

2. Organização da Segurança ⇒ Sugere que uma estrutura de gerenciamento seja determinada dentro da empresa, explicando quais os grupos são responsáveis por certas áreas de segurança e um processo para o gerenciamento de respostas a incidentes.

3. Classificação e Controle do Patrimônio ⇒ Exige um inventário do patrimônio de informações da empresa e, com esse conhecimento, garante que o nível e o escopo de proteção apropriado seja aplicado.

4. Segurança dos Funcionários ⇒ Indica a necessidade de educar e informar os funcionários atuais ou potenciais sobre a expectativa da empresa para com eles, com relação a assuntos confidenciais e de segurança, e como sua função na segurança se enquadra na operação geral da empresa. Tenha um plano de relatórios de incidentes.

5. Segurança Física e Ambiental ⇒ Aborda a necessidade de proteger áreas seguras, equipamentos de segurança e controles gerais.

6. Gerenciamento de Operações e Comunicações ⇒ Os objetivos dessa seção incluem:

1. Garantir instalações para a operação correta e segura do processamento de informações;
2. Minimizar o risco de falhas dos sistemas;
3. Proteger a integridade do software e/ou das informações;
4. Manter a integridade e disponibilidade do processamento de informações e comunicações;
5. Garantir a proteção das informações em redes e da infra-estrutura de suporte;
6. Evitar danos ao patrimônio e interrupções nas atividades da empresa;
7. Prevenir perdas, modificações ou uso inadequado das informações trocadas entre empresas.

7. Controle de Acesso ⇒ Identifica a importância da monitoração e controle do acesso a recursos da rede e de aplicativos, para proteger contra abusos internos e intrusões externas.

8. Manutenção e Desenvolvimento de Sistemas ⇒ Reforça que com todos os esforços de TI, tudo deve ser implementado e mantido com a segurança em mente, usando os controles de segurança em todas as etapas do processo.

9. Gerenciamento da Continuidade dos Negócios ⇒ Recomenda que as empresas se preparem com maneiras de neutralizar as interrupções às atividades comerciais, e protejam os processos comerciais cruciais, no evento de uma falha ou desastre.

10. Compatibilidade ⇒ Instrui as empresas a observar como a sua compatibilidade com o ISO 17799 se integra ou não com outros requisitos legais como o European Union's Directive on Privacy (Diretivas da União Européia sobre Privacidade), Health Insurance Portability and Accountability Act (Decreto de Responsabilidade e Portabilidade de Seguro de Saúde, HIPAA) e o Gramm-Leach-Bliley Act (GLBA). Essa seção exige também uma revisão da política de segurança e compatibilidade técnica, além de considerações a serem feitas com relação ao sistema do processo de auditoria, para garantir que cada empresa se beneficie o máximo possível.

- **Benefícios do ISO 17799**

Uma empresa com o certificado ISO 17799 pode fazer mais negócios do que aquelas sem certificação. Se um cliente em potencial estiver escolhendo entre dois serviços diferentes, e a segurança for uma preocupação, eles geralmente selecionarão a opção certificada. Além disso, uma empresa certificada oferecerá:

- Segurança corporativa aprimorada
- Planejamento e Gerenciamento de segurança mais efetivo
- Parcerias e e-commerce mais seguros

- Confiança aprimorada do cliente
- Auditorias de segurança mais seguras e precisas
- Redução de responsabilidades legais

• **Status do ISO 17799**

O ISO está atualmente revisando o 17799 para torná-lo mais aceitável pelo seu público global. O ISO 17799 determinou o primeiro padrão e suas recomendações principais e idéias serão criadas e expandidas de acordo com as necessidades futuras. Até então o ISO 17799 é o padrão a ser seguido.

Se a sua empresa não possui um programa de proteção de informações, o ISO 1779 pode fornecer as diretrizes para a criação de um. Mesmo que você não queira se tornar certificado, o ISO 17799 pode servir como um guia para a criação da postura de segurança da sua empresa. Você pode pensar nesse padrão como uma boa diretriz de segurança a ser usada pela sua empresa. Porém, você poderá descobrir que os benefícios da certificação podem ser muito abrangentes.

• **Fontes de Pesquisa:**

- "*Building Effective Security Policies*"
- "*Up to Standard: BS7799 and Your Enterprise*"