



Universidade Católica de Brasília

E-Learning

**MBA – Gestão de Sistemas de Informação
Segurança na Informação**

- **Professor: Ly Freitas**
- **Grupo:**
 - Ferdinan Lima**
 - Francisco Carlos Rodrigues**
 - Henrique Andrade Aragão**
 - Rael Frauzino Pereira**
 - Renata Macêdo Martins**

E-learning: O novo paradigma da educação e suas questões de segurança

O e-learning está revolucionando o sistema de ensino no mundo. Ao contrário do sistema tradicional, com o e-learning a componente presencial deixou de ser obrigatória. Basta estar em frente a um computador com acesso à Internet. Além disso, podemos escolher o tempo e o espaço para receber os ensinamentos. Através da Internet podemos aprender em qualquer país do mundo, mesmo no mais remoto. Sendo assim, podemos dizer que o E-learning é uma fonte de mudança, inovação e desenvolvimento, que visa sempre proporcionar a flexibilização dos métodos de formação procurando estar mais perto das reais necessidades das pessoas, dando-lhes respostas mais personalizadas e eficazes.

Perante uma realidade industrial em que a produção é contínua e na qual todos os tempos de formação deverão ser altamente estruturados e bem definidos, sob pena de "roubarem" excessivas horas aos postos de trabalho, sentimo-nos obrigados a preparar um trabalho que ao nosso ver apresenta respostas suficientemente flexíveis que potencializam e otimizam a aquisição do saber e competências.

Cada vez mais as empresas estão perseguindo a redução de custos sem que haja perda de competitividade. O e-learning aparece como uma forma de treinar mais pessoas, em menos tempo, com o mesmo investimento que seria feito em modo presencial. Isto acontece porque não há o deslocamento do aluno para uma sala de aula, nem passagens, nem diárias de hotel, o que acontece tradicionalmente em treinamentos na maioria das empresas.

Apesar de ser uma grande quebra de paradigma, já que trata-se de uma mudança cultural violenta no aprendizado empresarial, as empresas vão acabar induzindo e/ou obrigando seus funcionários a aprender desta forma, porque não disponibilizarão outra de aprendizado corporativo. As empresas já estão vendo isso como vantagem competitiva importante. Aquelas que conseguirem aderir primeiro a essa nova cultura, terão uma vantagem excepcional sobre seus concorrentes porque levarão bem menos tempo para transmitir conhecimento.

Já estão sendo realizados uma série de estudos e prospeções sobre a Universidade Corporativa, este tema começa a se disseminar entre as empresas, entidades governamentais e representativas de classe e instituições de ensino tradicionais do Brasil, várias já implantaram instituições com base nos princípios do e-learning e outras estão com projetos de instalação em andamento.

1. Introdução

A informação tornou-se um elemento de fundamental importância e extremamente valiosa para os negócios de hoje. Empresas e instituições em geral estão cada vez mais utilizando recursos computacionais para armazenar, produzir e distribuir informações. Assim, ao mesmo tempo em que tem aumentado a confiança das organizações em informações

providas por sistemas computacionais, infelizmente tem se observado também um aumento quase que diário no surgimento de vulnerabilidades nos diversos sistemas disponíveis no mercado.

É indiscutível o ganho que organizações terão com um crescente uso de computadores: acesso a redes de computadores, Internet e seus diversos recursos. Porém, é extremamente insensato entrar neste novo "território" tecnológico desprovido de regulamentação adequada sem entender os riscos, sem formular uma política de segurança adequada e sem definir procedimentos para proteger informações importantes de uma organização.

Decidir por onde começar a implementação de segurança em um site de e-learning ou outro qualquer pode ser um processo difícil. Por um lado, devemos primeiro entender quais são as ameaças existentes e como podemos reduzir a sua vulnerabilidade. Por outro lado, devemos ter consciência de quais são os recursos que desejamos proteger, quais são os valores destes recursos e que nível de segurança é mais adequado, dada a cultura e a filosofia proposta no site de e-learning.

Em um processo de integração de procedimentos de segurança em um e-learning, é importante que se tenha claro quais são os objetivos e qual a importância destes novos procedimentos e das novas tecnologias a serem introduzidas. É importante fazer um levantamento das necessidades, problemas e requerimentos e acima de tudo convencer a gerência e ao público freqüente no site da importância deste processo.

2. Itens a considerar

Procuraremos dar uma visão geral não técnica de alguns aspectos relevantes de segurança que devem ser levados em consideração por gerentes de sistemas de informação e executivos que tomam decisões que afetam a infra-estrutura de segurança. A seguir, tem-se alguns itens que devem ser considerados.

1. Como justificar investimentos em infra-estruturas para segurança?
2. O que uma política de segurança deve conter?
3. Que deve ser considerado em um programa de treinamento em segurança?
4. Quais são os problemas comuns de segurança encontrados nos sites?

Como justificar investimentos com infra-estruturas para segurança?

- Fazer uma análise de riscos para identificar os recursos que se deseja proteger e para determinar os seus valores.

Estes recursos podem ser classificados nas seguintes categorias:

- Físico: computadores, equipamentos de rede, mídia de armazenamento, etc.
- Intelectual: código de programa e documentação, informações de servidores WWW, informações de banco de dados, projetos;

- Valores não palpáveis: reputação da empresa, privacidade de usuários, informações confidenciais, moral de empregados;
- Serviços computacionais: alocação de CPU, discos, suporte técnico.
- Identificar valores de bens físicos é uma tarefa fácil, basta levantar o valor de reposição de um novo. A parte difícil é determinar que propriedade intelectual significativa sua organização possui e quais bens não palpáveis são recursos-chave.
 - Demonstrar que as tentativas de ataques são numerosas demais para serem ignoradas
 - Instalar programas para monitorar o tráfego na rede e registrar as tentativas de ataques;
 - Utilizar algumas ferramentas para obter o máximo de informação que você puder sobre as vulnerabilidades da rede.
 - Discutir os impactos potenciais na reputação e lucros em caso de um ataque de negação de serviço. Que prejuízo teria se o site de e-learning ficasse fora de operação horas ou até mesmo dias?
 - Fornecer informações de ataques ocorridos na Internet, as empresas que foram atacadas e os danos sofridos.

O que uma política de segurança deve conter?

- Um dos elementos mais cruciais de uma infra-estrutura é a definição de uma política de segurança que atenda às necessidades do site de e-learning. Esta política deve servir como instrumento de comunicação e deve conter:
 - Explicações
 - É importante que a política seja explícita e clara sobre o por quê das decisões que foram tomadas. A maioria das pessoas não segue regras a menos que entenda por que são importantes.
 - Responsabilidades
- Uma política de segurança define expectativas e responsabilidades entre o site e seus usuários. Todos devem saber o que se espera de cada um. Não crie uma política baseada no que os usuários necessitam saber para manter o site seguro ou somente no que os administradores precisam fazer. Todos devem ser considerados.
 - Use uma linguagem comum

- Escreva um texto claro, preciso, em uma linguagem de fácil entendimento e direto ao assunto. Não seja muito formal.
- Faça cumprir a autoridade.

A política deverá especificar quem vai decidir e aplicar os tipos de penalidades disponíveis.

Que deve ser considerado em um programa de treinamento em segurança?

- Fornecer treinamento com regularidade para a equipe;
- Manter a equipe de suporte informada das atuais tendências em incidentes de segurança em computadores;
- Revisar seus procedimentos de treinamento regularmente e assegurar-se que continuam atualizados e relevantes para o seu ambiente.

Quais são os problemas comuns de segurança encontrados nos sites

- Recursos insuficientes do site

Os problemas mais comuns em segurança estão relacionados a organizações que não dedicam recursos suficientes para implementar níveis adequados de segurança. Apesar deste problema não ser mais tão freqüente, ainda hoje escutamos queixas de administradores de sistemas de que em suas organizações a segurança não é tida como um tema de grande relevância.

- Suporte ou autoridade insuficiente

Nem sempre a equipe de suporte tem apoio de sua gerência ou autoridade para adotar medidas de segurança apropriadas. Sem este apoio e autoridade, a equipe não pode implementar controles de segurança satisfatórios e fazer com que as políticas de segurança sejam cumpridas. Este é um ponto crucial para que uma política de segurança seja bem sucedida.

- Sistemas com problemas de segurança

Ainda hoje máquinas/sistemas continuam sendo vendidos com configurações default trazendo sérias vulnerabilidades. Sistemas operacionais (alguns mais que outros) devem ter sua configuração default muito bem revista após sua instalação para remoção de possíveis furos de segurança.

- Patches não aplicados

Em alguns sites não existe uma preocupação com instalação de patches (pacotes de correção de furos de segurança do próprio sistema) divulgados pelos fabricantes em suas máquinas. O tempo entre a divulgação da vulnerabilidade e a liberação do patch é

considerável, neste intervalo a sua rede pode ficar desprotegida, a menos que você contorne o problema desabilitando o serviço, removendo e/ou alterando permissões, ou restringindo acesso à máquina. Deve-se estar atento aos anúncios de vulnerabilidades divulgados na Internet.

- Senhas reutilizadas não criptografadas

Alguns sites ainda utilizam sistema de autenticação sem criptografia em acessos remotos e ainda com senhas reutilizadas. Em uma conexão via Telnet ou rlogin, por exemplo, senhas passam às claras pela rede, portanto facilitando a vida de quem estiver monitorando a rede. Algumas soluções são sugeridas para atacar este problema, como: senhas não reutilizáveis. Algumas soluções para autenticação remota com criptografia podem ser utilizadas como uso dos pacotes: Kerberos e SSH (Secure Shell).

- Acesso aberto à rede

Acesso às máquinas internas sem restrições ou sem monitoramento do tráfego da rede é um outro problema crítico e ainda comumente encontrado. Se você decide não utilizar um firewall para filtrar o tráfego entre a Internet e sua rede interna, existem outras alternativas livremente disponíveis na Internet que permitem esta filtragem de pacotes. Estas ferramentas pelo menos irão reduzir os seus riscos.

- Contas de usuários criadas sem critérios segurança

Alguns sites criam contas com senhas default e muitas vezes estas senhas nunca são trocadas pelos usuários. Devem ser utilizados procedimentos que definam métodos para criação de contas. O mesmo se aplica para permissões de diretórios, arquivos de configuração do ambiente, assim como algoritmos que serão utilizados para gerar a senha inicial do usuário.

- Monitoramento e expiração de contas ineficientes

Muitos sites não têm uma política definida e quando a têm muitas vezes não é seguida. Contas de usuários que deixam a empresa às vezes permanecem sem serem removidas. Estas contas podem ser descobertas por intrusos ou usuários locais mal intencionados.

- Sistemas novos mal configurados

Algumas máquinas são instaladas na rede sem nenhuma preocupação com segurança. Se a rede não tem firewall ou nenhum outro controle de acesso, pelo menos um padrão mínimo de segurança deveria ser implementado.

3. Conclusões

Gostaríamos de enfatizar que segurança é uma questão à qual se deve dar alta prioridade. Apresentamos uma metodologia revolucionária de ensino e alguns itens que se deve ter em mente ao se planejar mecanismos de segurança. Também é bom salientar que o único sistema de computação totalmente seguro é aquele que nunca foi ligado na corrente elétrica. Deve ser selecionado um nível de segurança que se considere apropriado avaliando o impacto financeiro e em sua reputação no caso de um possível ataque bem sucedido ao seu site. Esperamos ter ajudado e incentivo na busca de uma infra-estrutura apropriada de e-learning e de segurança.