Insper

Cybersegurança em nuvem

Prof. Dr. Rodolfo Avelino

Caso ABC Place

Fundada em 2012, a ABC PLACE consolidou-se como um nome proeminente no comércio eletrônico nacional, conquistando um espaço sólido e reconhecido no mercado. Com mais de 100 colaboradores em sua sede, que abriga também o centro de distribuição, a empresa tem utilizado a plataforma de vendas baseada no sistema WooCommerce desde sua criação.

A estrutura técnica foi inicialmente instalada e configurada por um ex-funcionário, responsável pelo desenvolvimento do sistema de gestão da empresa. Dois anos atrás, a equipe de TI começou a ser formada, embora sua atuação tenha se concentrado principalmente nas demandas internas do escritório.

Neste momento, a ABC PLACE está em processo de migração de sua plataforma de vendas para o ambiente cloud computing. A diretoria enfatizou a importância vital dessa migração, porém, a equipe diretiva está apreensiva e temerosa de que riscos cibernéticos possam se materializar, afetando negativamente a estratégia e o negócio da empresa. Incidentes passados minaram a confiança dos diretores na equipe de TI.

Diante dessa falta de confiança, o presidente da empresa solicitou uma compreensão aprofundada dos riscos cibernéticos atuais e seu potencial impacto na migração. Como primeira etapa desse processo de gestão de riscos, a equipe resgatou um levantamento das principais ameaças relacionadas a riscos cibernéticos em empresas do mesmo segmento, realizado há dois anos, para verificar se tais ameaças estão presentes na ABC PLACE.

Insper

Segue abaixo a tabela com as ameaças cibernéticas identificadas em empresas semelhantes na época:

Ameaça	Descrição
Insider	Hacking interno
Malwares	Ransomware e outros tipos de códigos maliciosos que possam comprometer os recursos do ambiente computacional.
Denial of service	DOS ou DDOS
Injeção de código	SQLi ou qualquer outro tipo de ataque que possa executar comandos por meio de chamadas web.
Informação comprometida	Tentativa ou sucesso na destruição, corrupção ou divulgação de informações sensíveis corporativas ou de propriedade intelectual.
Eavesdropping	Ataque utilizado por invasores para “roubar” senhas, CPF, dados de cartões de crédito, conversas sigilosas, logins dos usuários.

Insper

Durante entrevistas com a equipe de TI, foram identificados os seguintes pontos:

1. **Boas práticas de segurança:** A empresa não adota boas práticas de segurança. Dispositivos de rede e servidores mantêm configurações padrão, sem políticas de "hardening".
2. **Gestão de usuários:** A equipe de TI utiliza os usuários 'administrator' e ‘root’ para acesso aos servidores.
3. **Gestão de vulnerabilidades:** Não há uma política de gestão de vulnerabilidades nem análise do estado da rede.
4. **Acesso inseguro:** Acesso aos servidores não é realizado por meio de VPN.
5. **Filtro de pacotes e conexões web:** Ausência de política de firewall e detecção maliciosa de conexões web.
6. **Aplicação e SGBD em mesmo servidor:** A plataforma de vendas e seu banco de dados compartilham o mesmo servidor.
7. **Monitoramento de segurança:** Falta de ferramentas para monitorar os recursos computacionais da plataforma de vendas.

Esses pontos destacam áreas críticas que necessitam de atenção e ação imediata para mitigar os riscos cibernéticos na empresa.

Insper

Tarefa:

Você deverá identificar, pesquisar nos materiais disponibilizados no Blackboard e na Internet os riscos cibernéticos e:

1 – Descrever as ameaças e vulnerabilidades existentes;

2 – Descrever os riscos e demonstrar o impacto dos mesmos na cadeia de valor da empresa;

3 – Descrever quais planos de ação podem ser criados para mitigar os riscos;

4 – Criar uma apresentação executiva para demonstrar o cenário atual de riscos para o presidente e comitê executivo da empresa. A apresentação deverá demonstrar os riscos atuais e impactos ao negócio por prioridade, responsáveis pelo risco e ações de curto prazo para mitigar os riscos identificados. A data da apresentação está prevista para o dia 9 de dezembro.

Dicas

Durante a Análise dos Riscos em grupo:

- **Busque detalhar cada vulnerabilidade:** Explore e exemplifique como cada ponto identificado pode ser explorado por invasores e como isso pode impactar a empresa.
- **Consequências potenciais:** Destaque as possíveis consequências para a empresa, desde perda de dados até danos financeiros e reputacionais.

Insper

Plano de Ação / Mitigação:

- **Recomendações claras:** Sugira ações específicas para mitigar cada vulnerabilidade. Isso pode incluir implementação de boas práticas de segurança, investimento em ferramentas, treinamento de equipe, entre outros.
- **Priorização de ações:** Sugira uma hierarquia para implementar essas soluções, identificando aquelas de alta prioridade e impacto imediato.

Atualização de Tecnologias e Práticas:

- **Ênfase na necessidade de atualização:** Aponte a importância de atualizar as tecnologias, separar a aplicação e o banco de dados, implementar firewalls e sistemas de detecção de intrusos.
- **Educação e Conscientização:** Sugira programas de treinamento para a equipe de TI e funcionários sobre práticas de segurança.