MAPA – Material de Avaliação Prática da Aprendizagem

Acadêmico: Marcos Vinicius de Morais	**R.A.: 201275425**
Curso: Engenharia de Software	
Disciplina: Segurança e Auditoria de Sistemas	
Valor da atividade:	**Prazo:**

Instruções para Realização da Atividade

1. Todos os campos acima deverão ser devidamente preenchidos;
2. Utilize deste formulário para a realização do MAPA;
3. Esta é uma atividade INDIVIDUAL. Caso identificado cópia de colegas, o trabalho de ambos sofrerá decréscimo de nota;
4. Utilizando este formulário, realize sua atividade, salve em seu computador, renomeie e envie em forma de anexo;
5. Formatação exigida para esta atividade: documento Word, Fonte Arial ou Times New Roman tamanho 12, Espaçamento entre linhas 1,5, texto justificado;
6. Ao utilizar quaisquer materiais de pesquisa referencie conforme as normas da ABNT;
7. Critérios de avaliação: Utilização do Template; Atendimento ao Tema; Constituição dos argumentos e organização das Ideias; Correção Gramatical e atendimento às normas ABNT;
8. Procure argumentar de forma clara e objetiva, de acordo com o conteúdo da disciplina.

Em caso de dúvidas, entre em contato com seu Professor Mediador.

Bons estudos!

Para desenvolver o seu MAPA, primeiramente leia com bastante atenção a descrição de um cenário corporativo hipotético, onde você poderia estar envolvido como Especialista em Segurança, identificando os pontos onde existem riscos aos ativos de TI.

Imagine que você foi contratado como especialista em segurança por uma empresa que atua na área de Gestão de Logística e que possui filiais em todas as unidades da federação. O principal motivo da sua contratação e direcionamento fornecido pela direção da empresa, é a avaliação e melhoria no processo de escolha dos membros do conselho diretor.

Essa grande empresa, estabeleceu um processo eletrônico para votação, utilizando um equipamento específico para isso, com um software embarcado, que possui um funcionamento *off-line*, na maior parte do tempo, mas que necessita de atualizações de *firmware* e base de dados antes do início do processo de escolha dos representantes.

A orientação passada pela presidência da empresa, é reforçar os procedimentos de segurança da informação nesse processo, objetivando aumentar a maturidade do mesmo, tanto para manter os dados seguros e íntegros como elevar o nível de disponibilidade, garantindo a continuidade dos negócios em caso de falhas pontuais na infraestrutura tecnológica.

A matriz da empresa fica em São Paulo e realiza a distribuição dos equipamentos pelo país, consolidando a leitura desses terminais em um único Data Center centralizado, onde todas as filiais se conectam via internet, diretamente e sem nenhum recurso de segurança, ao sistema principal para enviar os dados da votação. O único serviço local é uma rede cabeada que deve possuir acesso dedicado, mas por estar aberta os funcionários e clientes utilizam em seus equipamentos particulares para acesso à internet.

O Data Center que totaliza esses votos fica no térreo de um empreendimento próprio da empresa, localizado em uma região próxima ao Rio Pinheiros, onde é comum em épocas de chuva ficar bem cheio. Você também foi informado de que existe um nobreak pequeno que suporte apenas poucos minutos do Data Center funcionando, o que geralmente acarreta desligamento inesperado, causando impacto não apenas na sede, mas em todas as unidades da empresa, visto que os sistemas necessitam enviar as informações para matriz.

A empresa já sofreu questionamentos pelo setor de *compliance*, pois alguns resultados que chegaram à totalização pareceram inconsistentes, o que gerou uma desconfiança geral sobre o processo. Para completar, um equipamento particular conectado na filial de Recife, possuía uma aplicação maliciosa que se espalhou pela rede, criptografando os dados sensíveis da empresa. Houve solicitação de resgate pelo grupo Hacker para liberar as informações criptografadas, que acabou sendo pago, pois a empresa não possui sistema de backup para voltar informações nesses casos, seja local ou em nuvem.

Realmente seriam muitos desafios de segurança e continuidade para um Especialista em Segurança, não é mesmo? Assim, para entregar essa atividade MAPA, você precisa descrever:

1 - Quais riscos você identifica no cenário apresentado dessa empresa? Cite ao menos 5 (cinco) riscos, explicando o porque eles são riscos para o negócio.

Risco 1: Durante o processo de envio dos dados ao Data Center, existem vulnerabilidades que comprometem a integridade e confidencialidade dos dados de votação. A inexistência de recursos de segurança durante a transmissão dos dados de votação possibilita possíveis ataques hacker que possam manipular os dados enviados pelas filiais que encontram-se espalhadas por todo país e se conectam diretamente ao Data Center, estabelecido em São Paulo.

Inclusive, a empresa já sofreu questionamentos do setor de *compliance*, pois alguns resultados pareciam inconsistentes.

De fato, a falta de segurança na transmissão de dados confidenciais pode comprometer o resultado final da votação, tendo em vista que esses dados podem ser manipulados em um possível ataque hacker, ou pode causar desconfiança simplesmente pelo fato de não haver segurança e confidencialidade durante a transmissão dos dados.

Risco 2: A empresa possui um único serviço local, sendo uma rede cabeada para o acesso à internet. Entretanto, clientes e funcionários utilizam dessa rede aberta, acessando-a de seus dispositivos particulares. Dispositivos pessoais não possuem a mesma política de segurança que uma organização exige, podendo ser hospedeiros de diversos tipos de vírus. Uma vez que um dispositivo infectado se conecta a mesma rede do Data Center, podem ocorrer ataques que comprometam a integridade e confidencialidade dos dados, como também a disponibilidade dos serviços oferecidos pelo Data center, comprometendo os pilares da segurança da informação.

Neste sentido, ocorreu um fato na filial de Recife, quando um equipamento particular infectado, foi conectado na rede da empresa. Este equipamento possuía uma aplicação maliciosa, a qual se espalhou pela rede e criptografou dados sensíveis da empresa, como um típico ataque *Ransomware*. Assim, a empresa teve diversos prejuízos, sendo financeiros, morais e nos dados armazenados.

Risco 3: A estrutura física do Data Center está estabelecida no térreo, em uma região próxima a um rio, que, em época de chuvas é habitual ficar cheio. Ocorre que, este rio fica predisposto a extrapolar o seu limite em caso de uma quantidade excessiva de chuvas, podendo vir a causar alagamentos e enchentes. Devido a isso, o Data Center fica vulnerável a sofrer algum ataque oriundo de desastre natural, caso uma enchente atinja o local onde está localizada a estrutura do Data Center.

Risco 4: O nobreak é um equipamento muito importante em uma estrutura de T.I. Em uma rede de energia elétrica é comum acontecer oscilações e quedas, e a interrupção repentina de energia pode comprometer o bom funcionamento de equipamentos de T.I. Devido a isso, as empresas devem se precaver a fim de evitar que esse tipo de falha cause danos aos seus equipamentos e consequentemente à rotina da organização.

Sendo assim, o nobreak torna-se fundamental para evitar que esse tipo de transtorno aconteça, pois a sua função é utilizar da energia armazenada em baterias quando o fornecimento de energia elétrica for interrompido. Entretanto, deve ser realizado um levantamento de consumo dos equipamentos da empresa para definir a capacidade de energia necessária para garantir o funcionamento dos equipamentos pelo tempo necessário.

Visto que a empresa possui um *nobreak* pequeno com autonomia de poucos minutos, a disponibilidade dos recursos fica comprometida, pois caso falte energia no Data Center na data da votação, o desligamento do sistema principal causará danos em todas as filiais da empresa que não conseguirão enviar seus dados de votações. Outro risco detectado no processo atual, é uma possível

falha nos equipamentos, tendo em vista que a interrupção repentina de energia, pode corromper o sistema operacional ou causar falhas no hardware dos equipamentos de T.I. do Data Center.

Risco 5: Um item primordial em se tratando de segurança da informação é o *backup*. Todo sistema que tenha a capacidade de armazenar dados, deve possuir *backups*. Até mesmo arquivos, documentos, ou planilhas utilizadas na organização devem estar dentro de uma rotina de *backup*.

Manipulamos os dados rotineiramente e o mesmo arquivo sempre está alocado no mesmo lugar, íntegro e atualizado. Muitas vezes, não pensamos que problemas podem ocorrer e que esses dados precisarão ser recuperados.

No caso da empresa citada nesta atividade não foi diferente. Visto que não existe rotinas de backup para os dados do Data Center, existe uma vulnerabilidade que compromete a disponibilidade e integridade dos dados, pois assim como aconteceu, um ataque hacker que criptografa os dados e posteriormente cobra um alto valor pelo resgate, pode ser resolvido mais facilmente quando se tem um backup íntegro. Assim como um sistema corrompido por desligamentos inesperados, pode ser reestabelecido em menor tempo e menor custo quando se tem o backup dos dados armazenados.

Vale ressaltar que esses backups podem ser realizados utilizando outros dispositivos alocados em diferentes regiões, como também podem ser armazenados em nuvem, a depender da necessidade da empresa.

Outro fator importante é que a empresa em questão, não possui um equipamento sobressalente como backup, a fim de reestabelecer os serviços no caso de falha no hardware do equipamento principal. Sendo assim, os serviços oferecidos pelo Data Center ficariam indisponíveis por tempo indeterminado, até que seja realizada a manutenção no hardware defeituoso, comprometendo todo o processo de votação em andamento.

2 - Para cada risco identificado descreva uma ou mais ações para eliminar, mitigar ou terceirizar o risco.

Risco 1: Para que o envio dos dados de votação seja realizado de forma segura, devem ser utilizados recursos de segurança como a criptografia dos dados, utilizando assinaturas digitais que garantem a autenticidade dos dados. Também pode ser utilizado uma VPN - Rede Privada Virtual, que cria uma conexão protegida e privada, garantindo segurança entre as partes, utilizando uma rota privada mesmo acessando uma rede pública.

Risco 2: Politicas de segurança devem ser implementadas nessa rede, a fim de garantir a sua integridade e confidencialidade, sendo dois pilares importantes na segurança da informação. Com base nisso, somente dispositivos autorizados devem estar conectados à rede em questão. Dispositivos particulares de clientes, funcionários ou desconhecidos devem ter o acesso negado. Além disso, devem ser implementados firewalls que permitam somente os serviços necessários para o envio de dados das filiais ao Data Center.

Risco 3: Dada a importância de um Data Center, diversos critérios devem ser analisados para a sua construção. Inclusive a região onde será montada a sua estrutura física. Por estar próximo a uma área com risco de enchentes e inundações, deve ser feito uma análise de risco, avaliando os possíveis impactos caso esse risco se concretize. Se possível, deve ser realizada a realocação desse Data Center para um andar superior, ou para uma região onde tenha maior segurança e menor risco de desastres naturais.

Risco 4: O nobreak que sustenta o Data Center, em casos de falta de energia elétrica, tem uma baixa capacidade de armazenamento, sustentando os equipamentos por pouco tempo. Para solucionar esse problema, deve ser realizado um levantamento do consumo de cada equipamento, levando em consideração a necessidade de mantê-lo estabilizado caso falte energia, dada a sua importância. Ademais, deve ser adquirido novos nobreaks com capacidade de armazenamento adequada ao consumo do Data Center. Dada a importância e necessidade de garantir todos os pilares da segurança da informação, investir em geradores de energia se torna um fator primordial, tendo em vista que nobreaks tem a função de garantir a autonomia do Data Center durante o acionamento dos motores e a transição da rede de energia elétrica comum para a rede elétrica gerada pelo gerador da organização.

Risco 5: Deve ser criada uma rotina de backup para armazenamento seguro das informações da empresa. Esse backup deve ser realizado copiando os dados do Data Center atual, para outro dispositivo que esteja em uma região diferente, de preferência distante do local onde está situado o Data Center. Pode ser avaliada a possibilidade de que seja feito o backup em nuvem, desde que seja uma plataforma confiável que garanta além de outros pilares, a confidencialidade que é fundamental no processo de votação. Além do backup dos dados, outro fator importante, é garantir um backup caso haja uma falha de hardware. Devem ser preparados, equipamentos que fiquem disponíveis caso algum hardware apresente falhas.. Caso isso aconteça, basta restaurar o backup de dados no dispositivo reserva, até que seja realizada a manutenção no Data Center principal, sem que o processo de votação tenha sua integridade, disponibilidade e confidencialidade comprometidas.

3 - Partindo do princípio de que você, Especialista em Segurança, poderá contribuir com melhorias na Política de Segurança da Informação, descreva ao menos 3 (três) itens que você vai sugerir e explique por qual razão elas são importantes e os efeitos positivos que você pretende com elas.

1 – Conscientizar a equipe é importante para garantir que todos os colaboradores estejam comprometidos com o processo. Muitos ataques são realizados explorando a falta de conhecimento e maturidade de colaboradores, que acabam contribuindo inconscientemente com o sucesso do atacante.

Investir em treinamentos é importante para que a equipe esteja alinhada tecnicamente, elevando o conhecimento dos colaboradores e promovendo a integração entre eles, garantindo maior retorno nos resultados esperados.

O treinamento eleva o conhecimento técnico da equipe, promovendo a sensibilização e o comprometimento com a política de segurança da empresa. E isso trará resultados significativos garantindo que a equipe trabalhe com o mesmo propósito, elevando o nível de maturidade, eficiência e eficácia na aplicação das políticas de segurança da informação.

2 – Partindo do princípio em que a empresa já sofreu com ataques do tipo Ransomware, inclusive foi necessário ceder ao pagamento do resgate exigido. Sugiro criarmos uma política de backup, a fim de garantir a integridade dos dados da empresa. Considerando que todo sistema está sujeito a sofrer algum tipo de ataque, mesmo que se tenha uma politica de segurança robusta, deve ser implementado rotinas de backup regularmente, armazenando cópias fiéis de seus dados em um ambiente seguro, fisicamente distante da localidade do Data Center, como também em um ambiente seguro em nuvem. Essa prática garante que, em caso de um novo ataque, ou falha em algum equipamento no Data Center, esse backup esteja íntegro e pronto para ser reestabelecido sem que a empresa sofra danos que comprometam a confiabilidade no processo de votação.

Auditorias devem ser realizadas com frequência, a fim de acompanhar o período adequado da realização de cópias, como também a segurança no armazenamento das mesmas, além de realizar testes de integridade, recuperando os dados em um ambiente de testes, garantindo assim a eficácia do processo.

3 – Investir na infraestrutura do Data Center garante a disponibilidade de seus serviços sempre que necessário. Para isso, deve ser criado uma espécie de check-list, a fim de acompanhar e testar periodicamente o funcionamento dos equipamentos, como também a segurança do ambiente em que encontram suas instalações. As atualizações da base de dados e firmware, devem ser realizadas frequentemente, corrigindo as falhas e vulnerabilidades antes que sejam exploradas por ataques maliciosos.

Além das informações apresentadas, utilize os conhecimentos adquiridos no livro da disciplina, aulas conceituais e ao vivo. Fique à vontade para explorar o cenário em todas as suas possibilidades.