Auditoria de Segurança
Botium Toys

Introdução

A Botium Toys é uma empresa fictícia do curso Play It Safe: Manage Security Risks da coursera e Google, a ideia dessa auditoria é mostrar minhas capacidades e compreensões sobre as boas práticas que um analista de segurança cibernética deve aplicar.

Aqui será aplicado as habilidades aprendidas no curso sobre NIST, CIA, SPII /PII, soluções, / metodologias e identificação de problemas. O curso disponibilizou material para análise e partir dele tirarei minhas conclusões sobre o case. Os materiais são: **Botium Toys: Escopo, metas e relatório de avaliação de risco**, **Categorias de controle**, **Controles e lista de verificação de conformidade**.

Cenário

A Botium Toys é uma pequena empresa norte-americana que desenvolve e vende brinquedos. O negócio tem um único local físico. No entanto, sua presença online cresceu, atraindo clientes nos EUA e no exterior. Seu departamento de tecnologia da informação (TI) está sob crescente pressão para apoiar seu mercado on-line em todo o mundo.

O gerente do departamento de TI decidiu que uma auditoria interna de TI precisa ser realizada. Ela expressa preocupação em não ter um plano de ação solidificado para garantir a continuidade e conformidade dos negócios, à medida que o negócio cresce. Ela acredita que uma auditoria interna pode ajudar a proteger melhor a infraestrutura da empresa e ajudá-la a identificar e mitigar potenciais riscos, ameaças ou vulnerabilidades a ativos críticos. O gestor também está interessado em garantir que eles cumpram os regulamentos relacionados à aceitação de pagamentos on-line e à realização de negócios na União Europeia (UE).

O gerente de TI começa implementando o National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), estabelecendo um escopo e metas de auditoria e concluindo uma avaliação de risco. O objetivo da auditoria é fornecer uma visão geral dos riscos que a empresa pode enfrentar devido ao estado atual de sua postura de segurança. O gerente de TI quer usar os resultados da auditoria como evidência para obter aprovação para expandir seu departamento.

Mateus Breno Soares

Auditoria de Segurança
Botium Toys

Analisando as Categorias de controle

Ao acessar o arquivo para análise, **Categorias de controle**, pode-se criar uma tabela do que deve ter certa atenção e do que não precisa, conforme mostrado abaixo:

Nome do controle	Tipo de controle e seu proposito	Precisa implementar?	Prioridade
Privilégio mínimo	**Preventiva** | Reduz o risco, garantindo que fornecedores e funcionários não autorizados tenham acesso apenas aos ativos/dados de que precisam para realizar seus trabalhos.	**sim**	Alta
Planos de recuperação de desastres	**Corretivo** | Continuidade de negócios para garantir que os sistemas sejam capazes de funcionar em caso de incidente/não haja perda de produtividade/impacto nos componentes do sistema, incluindo: ambiente da sala de computadores (ar condicionado, fonte de alimentação, etc.); hardware (servidores, equipamentos dos funcionários); conectividade (rede interna, wireless); aplicativos (e-mail, dados eletrônicos); Dados e restauração.	**sim**	Alta
Políticas de senha	**Preventiva** | Estabeleça regras de força de senha para melhorar a segurança/reduzir a probabilidade de comprometimento da conta por meio de força bruta ou técnicas de ataque de dicionário.	**sim**	Alta
Políticas de controle de acesso	**Preventiva** | Aumentar a confidencialidade e a integridade dos dados.	**sim**	Alta

Auditoria de Segurança
Botium Toys

Políticas de gerenciamento de contas	**Preventiva** | Reduzir a superfície de ataque e limitar o impacto geral de funcionários descontentes / ex-funcionários.	**sim**	Alta
Separação de funções	**Preventiva** | Garantir que ninguém tenha tanto acesso que possa abusar do sistema para ganho pessoal.	**sim**	Alta
Firewall	**Preventiva** | Firewalls já estão em vigor para filtrar o tráfego indesejado/malicioso de entrar na rede interna.	**não**	Sem
Sistema de Detecção de Intrusão (IDS)	**Detectiva** | permite que a equipe de TI identifique possíveis invasões (por exemplo, tráfego anômalo) rapidamente.	**sim**	Média
Encriptação	**Impedida** | torna as informações/dados confidenciais mais seguros (por exemplo, transações de pagamento no site).	**sim**	Alta
Backups	**Corretivo** | apoia a produtividade contínua no caso de um evento; alinha-se ao plano de recuperação de desastres.	**sim**	Média
Sistema de gerenciamento de senhas	**Corretivo** | recuperação de senha, redefinição, bloqueio de notificações.	**sim**	Alta
Software antivírus (AV)	**Corretivo** | detectar e colocar em quarentena ameaças conhecidas	**sim**	Alta
Monitoramento, manutenção e intervenção manuais	**Preventiva** | necessário para que os sistemas legados identifiquem e mitiguem potenciais ameaças, riscos e vulnerabilidades	**sim**	Média

Mateus Breno Soares

Auditoria de Segurança
Botium Toys

Cofre controlado pelo tempo	**Impedida** | reduzir a superfície de ataque/impacto de ameaças físicas.	**sim**	Baixo
Iluminação adequada	**Impedida** | limitar lugares "escondidos" para dissuadir ameaças.	**sim**	Baixo
Circuito fechado de televisão (CFTV) de vigilância	**Preventiva** / **Detectiva** | pode reduzir o risco de certos eventos; pode ser usado após o evento para investigação.	**sim**	Média
Armários de bloqueio (para engrenagens de rede)	**Preventiva** | aumentar a integridade impedindo que pessoas/indivíduos não autorizados acessem / modifiquem fisicamente o equipamento da infraestrutura de rede.	**sim**	Média
Sinalização indicando alarme do prestador de serviços	**Impedida** | faz com que a probabilidade de um ataque bem-sucedido pareça baixa.	**sim**	Baixa
Fechaduras	**Preventiva** | ativos físicos e digitais são mais seguros	**sim**	Alta
Detecção e prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.)	**Detectiva** / **Preventiva** | detectar incêndio no local físico da loja de brinquedos para evitar danos ao estoque, servidores, etc.	**sim**	Média

Mateus Breno Soares

Auditoria de Segurança
Botium Toys

Conformidade

Segundo o **EUR-Lex**, o Regulamento Geral sobre a Proteção de Dados (RGPD) protege os indivíduos sempre que os seus dados forem objeto de tratamento pelo setor privado e pela maior parte do setor público. O tratamento de dados pelas autoridades competentes para efeitos de aplicação da lei está sujeito à Diretiva sobre a Proteção de Dados na Aplicação da Lei.

A **IBM** aponta também a NIST CSF, e que as funções fornecem uma visão geral dos protocolos de segurança de melhores práticas. As funções não devem ser etapas processuais, mas devem ser executadas "simultaneamente e continuamente para formar uma cultura operacional que aborde o risco dinâmico de segurança cibernética". Categorias e subcategorias fornecem planos de ação mais concretos para departamentos ou processos específicos dentro de uma organização.

Segundo o **PagBrasi**l, o PCI DSS é composto por um conjunto de requerimentos e procedimentos de segurança cujo objetivo é proteger as informações pessoais dos titulares de cartão e, portanto, reduzir o risco de roubo de dados de cartão ou fraude.

Por fim, a **SafeWay**, menciona o SOC 1 tem como foco avaliar os controles que afetam as demonstrações financeiras dos clientes, como os relacionados a folha de pagamento e processamento de pagamentos. E o SOC 2 busca avaliar os controles internos de forma mais abrangente, com ênfase na segurança da informação. Os Trust Services Criteria incluem segurança, disponibilidade, integridade do processamento, confidencialidade e privacidade.

Mateus Breno Soares

Auditoria de Segurança
Botium Toys

Soluções

Umas das primeiras coisas a serem feitas é aplicar a RGPD na empresa, para que exista o controle e segurança dos dados de cada colaborador e também para os clientes. Além de deixá-los seguros, essa aplicação releva a reputação da empresa positivamente no mercado.

Para que isso funcione efetivamente é importante seguir as metodologias de segurança da NIST CSF, caso aplicada, pode-se ter mais camadas de segurança dentro da Botium Toys.

Outra boa sugestão é a aplicação o PCI DSS para melhorar a segurança das transações, tanto cliente/empresa quanto empresa/mercado, esse procedimento garante a privacidade dos dados relacionados ao financeiro e segurança nas transações de pagamentos dos clientes.

Por último, aplicar as áreas de SOC 1 e 2 dentro da companhia faz com que esteja mais preparada a incidentes de segurança, pois, dessa forma pode-se prever ou até mesmo se preparar para em caso de invasões.

Mateus Breno Soares

Auditoria de Segurança
Botium Toys

Conclusão

Ao aplicar essas soluções dentro das análises feitas nos documentos propostos, fica mais fácil lidar, se preparar e evitar incidentes, e dando esse primeiro passo de segurança, a reputação da Botium Toys pode melhorar na visão de mercado, pois assegurará aos clientes e investidores a preocupação com a segurança de todos.

Mateus Breno Soares