FOCO NO MERCADO DE TRABALHO

CULTURA DE SEGURANÇA

Emilio Tissato Nakamura

FORTALECIMENTO DA CULTURA DE SEGURANÇA E PRIVACIDADE

Os elementos fundamentais para o fortalecimento da cultura de segurança e privacidade são as definições da política de segurança, os treinamentos, a conscientização dos usuários e a participação ativa da alta administração.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você é o gerente de processos de segurança da empresa e deverá obter informações com seus pares, os gerentes de governança de segurança e de tecnologias de segurança. O seu papel é chave, pois a empresa depende da

definição e implementação de controles de segurança que integram os aspectos de pessoas, processos e tecnologias.

Na apresentação, o primeiro ponto tratado, sobre a cultura de segurança e privacidade da empresa, explicite que, para que ela seja forte, todos devem fazer a sua parte.

Mostre que vocês estão com um plano de treinamento e conscientização e que a política de segurança e privacidade está quase finalizada. Reforce que há o apoio, mas que o diretor de segurança da informação deve buscar a participação ativa da alta administração, que está planejada nas ações de treinamento e conscientização.

Sobre a política de segurança e privacidade, mostre que há a definição de como a empresa deve tratar os agentes externos, que consta em uma norma específica. As definições envolvem as regras para o acesso físico e lógico de fornecedores e prestadores de serviço. Um ponto importante é o uso de termos e contratos de ciência e de confidencialidade. Reforce que os trabalhos só podem ser iniciados pelos agentes externos após a assinatura dos documentos. Indique que este é um dos pontos importantes do treinamento e conscientização, já que todos os funcionários de todos os locais devem conhecer e cumprir o que está definido na política de segurança e privacidade. Você pode aplicar um questionário para validar se o treinamento em segurança foi proveitoso para os colaboradores. Para avaliar a eficácia do processo, podem ser utilizadas métricas de treinamento, como o número de colaboradores treinados e a média obtida nos questionários. Mostre otimismo com o andamento deste assunto, pois isso contribuirá efetivamente para o fortalecimento da cultura de segurança e privacidade da empresa.

Já sobre como as definições de segurança para os usuários e os administradores de sistemas, mostre uma visão de riscos que deixa claro as diferenças entre os dois acessos. No caso de senhas, por exemplo, o roubo de identidade de um usuário é crítico, porém no caso das credenciais do administrador de sistemas, os impactos são muito maiores, o que exige controles de segurança diferenciados. Cite a política de senhas definidas para os usuários e para os administradores de sistemas.

Na sua apresentação, faça um relato sobre a organização da política de segurança e privacidade. Mostre que as diretrizes gerais, como a definição das responsabilidades gerais em proteger a confidencialidade, integridade e disponibilidade das informações, estão definidas na política, enquanto os assuntos são tratados em normas especificas, como é o caso da norma de senhas. Relate que, além desta organização, o público-alvo também foi considerado, ou seja, agentes externos têm uma documentação própria e direcionada, e os usuários internos não precisam ler detalhes destinados aos agentes externos.

Sobre a segurança no desenvolvimento de sistemas, considere que a empresa segue o modelo SaaS, com a contratação de serviços. Reforce, no entanto, que análises de segurança são feitas para a definição e homologação dos fornecedores e provedores dos serviços.

Para finalizar, faça uma comparação entre os modelos de desenvolvimento de sistemas em que a equipe de desenvolvimento é da empresa e disponibilizado *on premises*, em provedor de nuvem IaaS e em provedor de nuvem PaaS.

AVANÇANDO NA PRÁTICA

EQUIPE DE DESENVOLVIMENTO PRÓPRIO E CONTRATAÇÃO DE PROVEDOR DE NUVEM

Sua empresa tem uma equipe dedicada que está desenvolvendo um sistema crítico. Ultimamente, a diretoria executiva está preocupada, pois vários ataques cibernéticos estão ocorrendo em empresas do setor, e eles solicitaram uma avaliação sobre como a segurança está sendo tratada neste desenvolvimento. A diretoria executiva também quer saber qual o modelo de contratação de nuvem foi feito, e as implicações de segurança, entre o modelo de infraestrutura como serviço (IaaS) e plataforma como serviço (PaaS).

RESOLUÇÃO

Prepare um relatório indicando o ciclo de vida de desenvolvimento seguro de *software* adotado pela empresa, incluindo elementos como os requisitos de segurança desde a concepção, e testes de segurança de análise estática (SAST) e de análise dinâmica (DAST). Além disso, apresente a modelagem da superfície de ataques e de ameaças que foi considerado, justificando as medidas de segurança que estão sendo implementadas. Mostre que, antes de o sistema ir para o ambiente de produção, estão previstos *pentests*.

Sobre o modelo de contratação de nuvem, mostre as responsabilidades de segurança envolvidos no IaaS e no PaaS. Apresente as responsabilidades de sua equipe de segurança. Por fim, faça uma matriz de responsabilidades de sua equipe e dos provedores de nuvem, justificando as razões pela escolha pelo IaaS, contando com a sua equipe capacitada a executar as atividades necessárias de segurança.