Por Alexandre Sammogini

Para tanto, é necessário investir na segurança adequada para os seus dados, pois, caso isso não ocorra, a organização estará fadada a possíveis ataques cibernéticos, que possam a vir ocasionar, por exemplo, prejuízos financeiros, riscos de imagem perante o mercado, sendo que em algumas situações podem ser irreversíveis. Sendo assim, não dar a devida atenção à questão de segurança cibernética é colocar em riscos a própria empresa, seus clientes e parceiros.

Há um ditado popular que diz “é melhor prevenir do que remediar”, ou seja, é melhor mitigar um risco com ações preventivas do que ter que reparar os danos depois, procurando medidas de soluções para as suas consequências.

No sítio eletrônico do Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados (IBRASPD), uma matéria foi divulgada com os ataques cibernéticos ocorridos no período de janeiro a dezembro de 2020 e que tiveram repercussão na mídia, conforme tabela abaixo:

Fonte: https://www.ibraspd.org/incidentes

Nota-se que ao todo foram 36 (trinta e seis) empresas de diversos segmentos e portes que sofreram incidentes no exercício de 2020 e que podem ter ocorrido, inclusive, por falta de realização de “testes e desenvolvimentos” que são um dos instrumentos fundamentais para garantir que quando da implantação de um procedimento, ou seja, a sua execução, possa ocorrer de forma mais segura e correta, visando assim, evitar possíveis riscos de falha nos sistemas. Em razão disso, a atual edição do “Saiba Como” vai abordar o processo de testes e desenvolvimentos.

Confira-se na tabela abaixo e a título de exemplo, alguns comentários sobre o método desenvolvido e que deve ser implementado nas rotinas das áreas de Tecnologia da Informação pelas organizações, que é o “teste de penetração”. Esse teste, também conhecido como intrusão, visa realizar a simulação de ataques por profissionais da área direcionados para detectar possíveis fragilidades na segurança dos dados da organização e mediante o seu resultado, é possível

elaborar ou aperfeiçoar uma estratégia mais eficiente de defesa. Na prática, esses profissionais devem realizar testes nos sistemas que foram contratados pela empresa e é como se comportassem como um hacker no mundo real, permitindo assim, encontrar situações de insegurança e perigos.

Por oportuno, também existem outros tipos de testes de software que podem ser realizados de acordo com o projeto que será aplicado levando em consideração o seu grau de risco. Veja:

- Funcionais: visam validar as funções e as especificações de requisitos do próprio sistema, ou seja, é o que o sistema faz;
- Não funcionais: visam avaliar a carga, portabilidade, performance, usabilidade, dentre outros, ou seja, é como o sistema trabalha;
- Estruturais: são ligados aos componentes e integração do sistema; e
- Mudança de regressão e confirmação: visam validar se o sistema está funcionando como o esperado, suprindo a existência de alguma falha introduzida ou não coberta no início.

Por fim, como sugestões de práticas que devem ser consideradas na busca de segurança da informação dentro das organizações em relação à gestão de testes e desenvolvimentos, conforme Checklist-ISO27701 e Cys Controls – Frameworks, destaca-se:

Práticas de Desenvolvimento Seguro	Estabelecer práticas seguras de codificação apropriadas à linguagem de programação e ao ambiente de desenvolvimento que está sendo utilizado.
Simulações Periódicas de Cenário de Incidentes Para a Equipe Técnica	Planejar e conduzir rotinas de incidentes, exercícios de resposta e cenários para as áreas envolvidas na resposta a incidentes, a fim de manter a consciência e o conforto em responder às ameaças do mundo real. Os exercícios devem testar os recursos técnicos dos canais de comunicação, tomada de decisão e de resposta a incidentes, usando ferramentas e dados disponíveis.
Testes de Penetração Regulares nos Ambientes Internos e Externos da Organização	Realizar testes regulares de penetração externa e interna para identificar vulnerabilidades e vetores de ataque que podem ser usados para explorar sistemas corporativos com sucesso.
Testes de Detecção de Presença de Artefatos e Informações Não Protegidas em Sistemas	Incluir testes para a verificar a presença de informações e artefatos desprotegidos nos sistemas que podem ser úteis para invasores, incluindo diagramas de rede, arquivos de configuração, relatórios de testes de penetração mais antigos, e-mails ou documentos contendo senhas ou outras informações críticas para a operação do sistema.
Mesa de Teste Para Elementos Normalmente Não Testados na Produção	Criar um ambiente de teste que imite um ambiente de produção para testes de penetração específicos e ataques do Red Team contra elementos que normalmente não são testados na produção, como ataques contra o controle de supervisão e aquisição de dados e outros sistemas de controle e monitoria de ambiente.
Resultados dos Testes de Penetração Sejam Documentados Usando Padrões Abertos e Legíveis Por Máquina	Verificar se os resultados da equipe de Red Team são documentados utilizando padrões abertos, legíveis por máquina (por exemplo, SCAP). Criar um método de classificação e score para determinar os resultados dos exercícios da

	equipe de Red Team, para que os resultados possam ser comparados ao longo do tempo.
Informações de Contato Para Reports de Incidentes de Segurança	Reunir e manter informações sobre dados de contato de terceiros a serem usadas para relatar um incidente de segurança, como polícia, departamentos governamentais relevantes, fornecedores e parceiros do Centro de Compartilhamento e Análise de Informações (ISAC).
Informações Sobre Reports de Anomalias e Incidentes de Computador	Publicar informações para todos os colaboradores da companhia, sobre relatórios de anomalias e incidentes computacionais, na equipe de tratamento de incidentes. Essas informações devem ser incluídas nas atividades rotineiras de conscientização dos funcionários.
Ferramentas de Análise Estática e Dinâmica de Código	Aplicar ferramentas de análise estática e dinâmica de código para verificar se as práticas de codificação segura estão sendo seguidas para o software desenvolvido na organização.
Ambientes de Sistemas de Produção e Não Produção	Manter ambientes separados para sistemas de produção e não-produção. Os desenvolvedores não devem ter acesso não monitorado aos ambientes de produção.
Programa de Testes de Penetração	Estabelecer um programa para testes de penetração que inclua um escopo completo de ataques combinados, como, ataques a rede wireless, em aplicações on premises e aplicações Web.

Inicia-se um novo ano 2022 e essa Comissão deseja a todos muita esperança, paz, saúde e sabedoria, para que possamos lidar com todos os desafios que estão por vir, principalmente, aqueles relacionados a possíveis ataques cibernéticos, uma vez que a prevenção é a melhor solução. Não percam o próximo “Saiba como tornar seus processos de T.I. robustos e capazes de prevenir ataques cibernéticos – Parte IX”.

*** Comissão Regional Leste de Governança e Riscos**

Fonte: Abrapp em Foco, em 07.02.2022.