

Workshop ANBIMA: Resposta a Incidentes Cibernéticos

Resumo

Texto elaborado pelo consultor Nicholas Miller (Aedile Consulting)

No dia 22/3, a ANBIMA realizou um exercício teórico de resposta a incidentes de segurança cibernética na sede da associação, em São Paulo. O workshop faz parte de um abrangente esforço da ANBIMA para aumentar o conhecimento e aplicação da segurança cibernética entre seus associados.

A segurança cibernética é um tema ímpar que afeta organizações de todos os portes, em todos os setores, e exige uma estratégia planejada em toda a organização para combater incidentes. Os participantes receberam informações sobre controles técnicos e de governança e supervisão necessários a serem conduzidos pela empresa para garantir que o risco cibernético seja bem gerenciado.

No geral, minhas impressões sobre o workshop e sobre os participantes foram que estes entenderam o risco que os incidentes cibernéticos representam para suas organizações e que estavam tomando medidas proativas para melhorar sua postura em relação à segurança cibernética. Cabe destacar que houve muito debate entre os participantes sobre a importância de uma abordagem conjunta entre TI, Compliance e outras áreas da empresa. Uma abordagem de segurança cibernética desse tipo em toda a organização tem uma chance muito maior de sucesso do que uma que é delegada apenas como um 'problema de TI'.

O workshop foi elaborado com base nos resultados da pesquisa de segurança cibernética enviada aos associados em 2017. A atividade foi desenvolvida especificamente para gestores de recursos, com foco em melhorias na compreensão e na resiliência contra ameaças cibernéticas comuns em pequenas organizações.

Os três cenários teóricos cobriram ameaças cibernéticas comuns que todas as organizações provavelmente enfrentarão de forma contínua. Cada cenário teórico explorou como o ataque avança e como consegue ser bem-sucedido e mostrou como o processo de resposta a incidentes pode ser conduzido.

Os dois primeiros cenários cobriram um ataque de ransomware e malware que se espalharam automaticamente pela rede. O cenário final analisa a resposta a incidentes quando serviços em nuvem são alvo de ataque. Nesse cenário, exploramos os benefícios e riscos dos serviços em

nuvem, o modelo de responsabilidade compartilhada em nuvem e a importância de proteger os dados nela contidos.

Próximos Passos

O workshop foi um exercício valioso para explorar como os ataques cibernéticos podem ocorrer e fornecer uma estrutura para o processo de resposta a incidentes. Cada cenário de ataque cibernético também mostrou como os controles básicos podem ser extremamente eficazes na prevenção e limitação de ataques cibernéticos. O conhecimento desses controles básicos pode ser usado como um exercício de benchmarking eficaz, e os participantes também receberam uma série de sugestões de workshops que poderiam ser realizados em suas próprias organizações.

Esses workshops ajudarão as organizações a entender melhor seus atuais níveis de risco cibernético contra ameaças comuns, fornecer tarefas práticas de resposta a incidentes e ajudar a melhorar a comunicação entre os departamentos da empresa no caso de um incidente.

É altamente recomendável que todas as organizações reservem tempo para realizar esses workshops e garantir que seus resultados sejam apresentados às estruturas de governança de segurança cibernética dentro de suas organizações.