POLÍTICA DE SEGURANÇA CIBERNÉTICA

DG ADMINISTRADORA DE CARTEIRAS DE VALORES MOBILIÁRIOS LTDA

INTRODUÇÃO

A Política de Segurança Cibernética (“PSC”) da DG ADMINISTRADORA DE CARTEIRAS DE VALORES MOBILIÁRIOS LTDA (“DG”), tem por objetivo mitigar ao máximo os riscos de ataques cibernéticos, visto que os serviços financeiros têm uma grande interface com os clientes e assim grande vulnerabilidade aos ataques cibernéticos.

De acordo com recomendações da própria ANBIMA a DG adota processos e controles com 5 medidas e funções bem definidas;

IDENTIFICAÇÃO/AVALIAÇÃO DE RISCOS (risk assessment)

A DG foi constituída para Gestão de Carteiras de Fundos especificamente de uma mesma família, mesmo núcleo familiar, fato esse que nos proporciona maior assertividade nas ações contra possíveis ataques cibernéticos pois conhecemos bem nossos stakeholders e suas atividades.

O primeiro processo definido pelo Compliance da DG é a identificação dos riscos internos e externos, os ativos de hardware e software e processos que precisam de proteção.

Durante essa avaliação inicial buscamos identificar os processos e ativos relevantes usados para seu correto funcionamento através da criação de regras para a classificação das informações geradas pela DG, permitindo com isso a implementação de processos para o devido manuseio, armazenamento, transporte e descarte quando necessário.

As vulnerabilidades dos ativos em questão serão avaliadas, identificando assim possíveis ameaças e o grau de exposição dos ativos a elas.

O Comitê de Compliance da DG é responsável pela gestão da segurança cibernética, com representação e governança apropriada, agindo livremente na instituição para desenvolver e executar ações de prevenção e proteção periodicamente e extraordinariamente quando houverem suspeitas de ataques cibernéticos

AÇÕES DE PREVENÇÃO E PROTEÇÃO

Em seguida entram em prática medidas com objetivo de mitigar e minimizar os riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de novos controles.

A implementação desses controles passa pela identificação, autenticação e autorização dos usuários, ou sistemas, aos ativos da DG.

A DG estabelece regras para definição de senhas de acesso a dispositivos corporativo descritas de forma abrangente no Manual de Segurança das Informações.

A DG limita os acessos internos, uma vez concedidos, a apenas recursos relevantes para o desempenho das atividades. A concessão de acesso é implementada de forma a ser revogada rapidamente quando necessário.

Os eventos de login e alteração de senhas são passíveis de auditoria e rastreáveis.

A DG, ao incluir novos equipamentos e sistemas em produção, garantir que sejam feitas configurações seguras dos recursos. Procuramos sempre realizar testes em ambientes de homologação e de prova de conceito antes do envio à produção.

A DG possui restrição ao acesso físico, às áreas com informações críticas/sensíveis.

A DG implementa segurança de borda, nas redes de computadores, por meio de firewalls e outros mecanismos de filtros de pacotes.

A DG dispõe de recursos anti-malware em todas estações e servidores de rede, como antivírus e firewalls pessoais.

A DG estabelece processos internos a fim de manter segregação de serviços, restringindo-se o tráfego de dados apenas entre os equipamentos relevantes e necessários às atividades em questão.

A política de Segurança das Informação da DG proíbe em seus processos a instalação e execução de software e aplicações não autorizadas por meio de controles de execução de processos

Como regra geral, A DG possui mecanismos de monitoramento de todas as ações de proteção implementadas para garantir o bom funcionamento e efetividade dessas normas e procedimentos estabelecidos. Mantendo assim inventários atualizados de hardware e software, bem como a verificação com frequência para identificar elementos estranhos à instituição.

A DG mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando sempre que forem disponibilizadas as devidas atualizações, monitorando diariamente as rotinas de backup, executando testes regulares de restauração dos dados.

Periodicamente também realizamos testes de invasão externa e phishing bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa na estrutura.

MONITORAMENTO E TESTES

Com objetivo de detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados pela DG, são realizados periodicamente testes no plano de resposta a incidentes, simulando os cenários especificados durante sua criação e desenvolvimento.

Através do uso de ferramentas de centralização e análise de logs a DG analisa regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

PLANO DE RESPOSTA

A DG desenvolveu um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa para essas situações. O plano é sempre discutido amplamente pelo comitê de Compliance da DG, definindo papéis e responsabilidades dentro do plano de ação, prevendo acionamento dos colaboradores-chaves e contatos externos relevantes quando necessário.

O plano de resposta da DG considera os cenários de ameaças previstos na avaliação de risco, utilizando critérios para classificação dos incidentes, por severidade. Abrangendo também questões de segurança e controles de acesso inclusive nas instalações de contingência.

RECICLAGEM E REVISÃO

A DG mantém o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos, processos e reavaliando os riscos residuais, implementações de proteção, planos de resposta a incidentes e monitoramento dos ambientes.

O Compliance Officer deve manter-se atualizado e informado sobre novas vulnerabilidades e ameaças que possam alterar a exposição da instituição aos riscos avaliados originalmente.

A DG busca promover e disseminar a cultura de segurança com a criação de canais de comunicação internos utilizados para divulgar o programa de segurança cibernética, assim como conscientizar sobre os riscos e as práticas de segurança, dar treinamentos e repassar novas orientações.