Programa de Segurança Cibernética

Versão 05
Março/2024

1. INTRODUÇÃO

Os recursos tecnológicos e a internet são indispensáveis para o funcionamento das organizações. Com eles foi possível elevar exponencialmente a capacidade de acesso, processamento e armazenamento de informações. Esses benefícios vieram acompanhados de problemas com segurança. Ataques cibernéticos se transformaram numa preocupação constante. É uma questão não só dos gestores de TI, mas de todos os profissionais de uma empresa.

O Programa de Segurança Cibernética da Biguá Capital objetiva definir responsabilidades, identificar e avaliar os riscos, estabelecer ações de prevenção, proteção, detecção e resposta aos eventuais problemas de segurança e manter esse Programa atualizado. A disseminação da cultura de segurança cibernética será sempre incentivada através de programas de treinamentos e de atualização.

O Guia de Cibersegurança da ANBIMA serviu de referência principal para a elaboração desse Programa.

2. RISCOS CIBERNÉTICOS

O crime cibernético é definido pela Organização Internacional das Comissões de Valores Mobiliários como “uma atividade nociva, executada por um grupo ou indivíduo através de computadores, sistemas de TI e / ou da internet e direcionada aos computadores, infraestrutura de TI e presença na internet de outra entidade”.

As motivações de ataques cibernéticos podem variar de fraudes, espionagem, roubo, sabotagem interna ou mesmo diversão.

Os ataques cibernéticos são realizados através de diversos métodos. Segundo a o Guia de Cibersegurança da Anbima, os mais comuns são:

- Malware – softwares que corrompem os computadores e redes, divididos em:
    - Vírus, cavalo de Tróia, spyware e ransomware.
- Engenharia social – métodos de manipulação para obter informações confidenciais, como senha, dados pessoais e número de cartão de crédito, tais como:
    - Pharming, pishing, vishing, smishing e acesso pessoal.
- Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso de botnets, o ataque vem de muitos computadores infectados utilizados para criar e manter spam ou viroses, ou inundar uma rede com mensagens resultando em uma negação de serviços.

- Invasões – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

3. AVALIAÇÃO DE RISCOS

Ativos críticos	Tipos de ameaças	Impactos	Ações de respostas	Observações
Planilhas e documentos, com destaque para os arquivos da área de investimentos e da área de back office e da área de risco e compliance	• Malware - roubo de informações	ALTO • Uso das informações para obter vantagens ilícitas • Divulgação de informações sigilosas da Venture • Risco de reputação pelo vazamento de informações	• Comunicar aos clientes e parceiros a ocorrência de um ataque cibernético • Prestar todos os esclarecimentos sobre as informações que forem divulgadas maliciosamente	• Os riscos estão associados à imagem e reputação da Biguá Capital, com pouco impacto nas áreas operacionais • Principais colaboradores têm que estar à frente das ações
Conteúdo dos discos rígidos	• Malware - vírus e ransomware	MÉDIO • Arquivos serem apagados • Impossibilidade de acesso aos arquivos	• Usar os backups de segurança localizados na Microsoft (One Drive) e no Google (Google Drive) • Providenciar computadores para a continuidade das atividades	• Os riscos estão associados às áreas operacionais Biguá Capital • Os colaboradores diretamente ligados às atividades envolvidas devem estar à frente das ações

Ativos críticos	Tipos de ameaças	Impactos	Ações de respostas	Observações
Aplicativos operacionais da área de investimentos	• Malware - vírus e ransomware	MÉDIO • Aplicativos serem apagados • Impossibilidade de acesso aos aplicativos • Uso indevido por invasão • Queda de desempenho dos computadores	• Providenciar computadores para a continuidade das atividades • Baixar versões dos aplicativos nos computadores	• Os riscos estão associados às áreas operacionais Biguá Capital • Os colaboradores diretamente ligados às atividades envolvidas devem estar à frente das ações
Site	• Ataques e invasões	BAIXO • Site ser retirado do ar • Mensagens difamatórias serem exibidas	• Retirar o site do ar até a solução dos problemas	• O site é apenas de divulgação institucional e de informações sobre os fundos, não possuindo área de clientes ou banco de dados • Os colaboradores diretamente ligados às atividades envolvidas devem estar à frente das ações

.

4. PROGRAMA DE SEGURANÇA CIBERNÉTICA

4.1 RESPONSABILIDADES

As questões estratégicas da área de TI e de segurança da informação e cibernética são de responsabilidade do Comitê Executivo e terá o suporte técnico do diretor de Risco e Compliance. Este comandará a implantação das decisões do Comitê Executivo.

O Programa de Segurança Cibernética da Biguá Capital será de responsabilidade do Diretor de Risco e Compliance. Em função da avaliação de impactos de eventuais ataques cibernéticos, o Comitê Executivo poderá comandar as ações de respostas.

O suporte terceirizado de informática é parte importante desse Programa, tendo participação na auditoria preventiva e nas ações corretivas.

4.2 CONTROLE E CONSCIENTIZAÇÃO DOS USUÁRIOS

Os colaboradores da Biguá Capital são o elo mais delicado em um programa de segurança cibernética. A efetividade do programa depende não somente dos equipamentos e soluções de segurança, mas também da conscientização dos colaboradores da instituição quanto à importância das práticas de segurança.

- Regras de definição de senha
    - Os acessos aos computadores deverão ter senha de acesso com o mínimo de 6 dígitos, necessariamente contendo maiúscula, minúscula, números e caracteres especiais.
    - As senhas de acessos às plataformas ou aos sites devem seguir, quando possível, a recomendação acima.
    - A senha terá que ser trocada anualmente.

- Utilização de dispositivos, softwares, sites e mídias sociais
    - Somente serão permitidos softwares, licenciados ou com direito de uso, necessários para a execução de tarefas relativas à Biguá Capital.
    - São vetados acessos a sites com conteúdo alheio às atividades desempenhadas por cada sócio ou que sejam indicados como não seguros pelo monitoramento do software McAfee WebAdvisor.
    - A utilização de dispositivos móveis, como HD portátil e pen drive só serão permitidos após aprovação da área de Risco e Compliance e deverão ser verificados pelo antivírus antes de serem utilizados.

- Treinamento periódico
    - O treinamento terá como objetivo que os colaboradores se habituem às rotinas e controles como, por exemplo, as restrições à utilização da internet, de acesso aos e-mails pessoais e

mídias sociais. Parte dos ataques cibernéticos pode ser originada internamente caso um sócio utilize dispositivos, aplicativos, sites e mídias sociais não autorizadas pela instituição.
- O treinamento deve incentivar que executivos e colaboradores adotem boas práticas, por exemplo, na definição das suas senhas e se tornem sensíveis às possíveis ameaças, por exemplo, no caso de phishing.
- Todos os colaboradores receberão treinamento periódico sobre segurança cibernética.
- Os novos colaboradores receberão treinamento sobre os procedimentos de segurança adotados na empresa.

4.3 CONTROLES TECNOLÓGICOS

Como forma de proteção de ameaças cibernéticas, a Biguá Capital possui uma estrutura de tecnologia com os seguintes componentes:

- Triplo sistema de armazenamento de dados, sendo um no HD e dois backups na nuvem, sendo um na Microsoft e outro no Google.
- Os logins e as senhas de acesso aos sites e softwares de uso corporativo são arquivadas no software KeePass, protegida com senha criptografada de conhecimento exclusivo do diretor de Risco e Compliance e de um membro da Equipe de Compliance.
  Os logins e senhas de acesso às plataformas operacionais e à extranet do administrador dos fundos geridos são de conhecimento apenas dos usuários autorizados e do diretor de Risco e Compliance e também serão arquivadas no KeePass.
  Os logins e senhas de acesso aos computadores são definidas pelos usuários e serão arquivadas no KeePass.

- A Biguá Capital mantém atualizado um inventário dos hardwares e softwares. A atualização se dará sempre que houver entrada ou saída itens e será auditado no fim de cada ano.

- Os principais softwares utilizados nos computadores da Venture são atualizados automaticamente sempre que são liberadas as novas versões. São eles o Microsoft 365, Teams, Power BI, McAfee PC Security, Skype e a plataforma operacional Fast Trade.

- Para a prevenção de ameaças utilizamos o McAfee PC Security que dispõe de firewall, antivírus com varredura diária em todos os computadores e atualização automática de novas versões.
  É possível a emissão de relatórios mensais de todos os equipamentos cadastrados, verificando as detecções realizadas em cada um e eventuais faltas de atualizações de versões. Nesse caso a atualização será imediata e será averiguado o motivo dessa falha, com ação de correção para evitar que ocorra novamente.

4.4 PLANO DE RESPOSTA A INCIDENTES

A Biguá Capital elaborou uma lista de ativos críticos, considerando o tipo de ataque, seus impactos, as ações de respostas necessárias e a eventual participação dos executivos chaves.

O objetivo é ser capaz de reagir tempestivamente em caso de incidentes. Os principais componentes são:

- Procedimentos de detecção e investigação para a identificação, correção do problema e acionamento dos colaboradores-chaves e contatos externos:
    - Quanto mais cedo um ataque cibernético é percebido, mas efetivas podem ser as ações de resposta. A detecção dependerá do tipo de ataque, podendo ser mais visível, caso de ataques que afetem o desempenho dos equipamentos. Na eventualidade de roubo de informações sigilosas, a detecção poderá ser mais demorada.
      O McAfee PC Security atua on line em todos os computadores e está configurado para eliminar as ameaças e avisar sobre esses eventos. Como mencionado acima, possibilita a emissão de relatórios gerenciais sobre o status dos computadores.
      Na tabela de Avaliação de Risco, item 3 acima, há uma seleção de ações de respostas imediatas a serem executadas e os grupos de responsabilidades que irão comandar.
      Casos não previstos serão analisados pela área de Risco e Compliance com o suporte especializado para a adoção das respostas adequadas no menor prazo possível.

- Plano de comunicação:
    - A comunicação de ataques cibernéticos será definida em função do tipo de ataque. Casos que possam ter repercussões para os clientes e parceiros da Biguá Capital terão o comando do Comitê Executivo que ficará responsável com a comunicação externa. Sendo necessário, os órgãos reguladores e autorreguladores também serão envolvidos.
      Já os casos com efeitos estritamente internos terão o comando da área de Risco e Compliance e a comunicação será interna, envolvendo todos os colaboradores.

- Plano de continuidade dos negócios e processos de recuperação:
    - A Biguá Capital tem elaborado um Plano de Contingência e de Continuidade dos Negócios com o mapeamento das contingências que podem afetar as operações diárias e as soluções para cada tipo de evento.
      No caso específico de ataques cibernéticos, as ações de respostas estão listadas na tabela de Avaliação de Risco, já citada acima. Ações adicionais poderão ser definidas, caso necessárias.
      Os ataques podem impossibilitar o uso dos equipamentos, momentaneamente ou de forma definitiva. Nesses casos, serão alugados equipamentos semelhantes até o conserto dos originais ou a aquisição de novos.
      Todos os dados e arquivos da Biguá Capital tem backups diários com dupla redundância na nuvem. Caso haja perda de dados nos equipamentos, os backups serão recuperados e instalados nos equipamentos.
      Os softwares e plataformas podem ser baixados pelos sites dos produtores.
      É utilizado um sistema de webmails, através da Gmail. Todos as mensagens ficam guardadas nos servidores do webmail e podem ser acessadas nos equipamentos substitutos.
      Dessa forma a Venture poderá recuperar suas operações diárias sem muita demora.

5. REVISÃO

Esse Programa foi elaborado considerando a estrutura pessoal e a infraestrutura de hardware e de software atualizada na edição desta versão da Política. As mudanças dessas condições poderão levar à revisão parcial ou completa do Programa.