POLÍTICA DE SEGURANÇA CIBERNÉTICA

DA

BRICK CAPITAL LTDA.

Em atendimento ao disposto na regulamentação em vigor, bem como em consonância com o disposto no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, a **BRICK CAPITAL LTDA.** ("Brick") mantém a presente Política de Segurança Cibernética, com o objetivo de definir regras, procedimentos e controles de segurança cibernética que sejam compatíveis com o seu porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas

A presente política deve ser sempre interpretada em conjunto com as demais políticas e normas internas da Brick, em especial no tocante à confidencialidade, à integridade e à disponibilidade dos dados e dos sistemas de informação utilizados.

Avaliação de riscos

A Brick estima que os principais riscos cibernéticos a serem considerados são:

- Infecção Ransomware: sequestro de dados, através do bloqueio de acessos a sistemas e arquivos no ambiente e exigência de um pagamento de resgate para liberação do acesso;

- Infecção Phishing: ataque cibernético mais comuns e recorrente, no qual o criminoso coloca uma "isca" na Internet para capturar usuários descuidados e, depois, roubar dados, como senhas de banco, fotos e informações pessoais;

- Colaboradores: Seja por falta de conhecimento, na maioria dos casos, ou até mesmo por ações mal-intencionadas, os colaboradores acabam sendo um dos elos mais fracos e, portanto, uma das principais causas de violações de segurança;

- Ataque de Intrusão: ataque de rede com objetivo de identificar portas abertas e vulnerabilidades no ambiente, resultando em invasão por questões financeiras, pessoais, fraudes, sabotagem ou espionagem;

- Infecção Malware: ataque efetuado através de programa malicioso hospedado no dispositivo, com objetivo de infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas.

Ações de proteção e prevenção

As ações de proteção e prevenção adotadas pela Brick são:

- Firewall Fortigate: para monitoramento e filtragem do fluxo de dados referente a comunicação ao ambiente interno Brick e externo Internet. Executa o processo de prevenção contra ataques de intrusões, verificando o tráfego na rede em busca de assinaturas de ataque, como ameaças sociais e ataques de saída, que identificam tentativas de exploração de vulnerabilidade em seu sistema operacional ou em algum programa usado no ambiente;

- Kaspersky Antivírus: instalado em todas as workstations e servidores no ambiente, com objetivo de proteção em tempo real, detecção e remoção de vírus e derivados (trojans, worms, spyware, adware, malware, ransomware, keyloggers e rootkits);

- Colaboradores: na admissão, os colaboradores assinam um compromisso de uso de hardware, software e e-mail de acordo com as políticas da empresa e periodicamente há a realização de campanhas de comunicação interna relembrando as normas de segurança de informação que devem ser observadas no dia a dia.

- Perfil de usuário: colaboradores não possuem acesso administrativo aos equipamentos, evitando a instalação de softwares ilegais e maliciosos que possam ser utilizados para vazamento de informações ou tornar o ambiente em risco. Executado periodicamente o processo de atualizações de segurança e corretivas Microsoft. Política de alteração de senha de login de rede por período.

Descrição dos mecanismos de supervisão

Para fins da supervisão dos riscos acima mencionados, a Brick desempenha as seguintes atividades:

- Firewall Fortigate: relatório diário referente as atividades analisadas de entrada e saída no ambiente, identificando tentativas de ataques de intrusão e navegação a conteúdo impróprio ao ambiente corporativo.

- SGI Tigra Consult: software de monitoramento 24x7, responsável por analisar as workstations e servidores no ambiente, alertando a equipe de tecnologia da informação quanto a eventos como base de antivírus desatualizada, serviço de firewall do Windows desativado, falha de espaço em disco e desempenho dos dispositivos.

- Console de Gerenciamento Kaspersky: console responsável pelo gerenciamento centralizado do antivírus Kaspersky no ambiente, possuindo histórico de relatórios referente a ameaças ativas, detectadas e tratadas no ambiente.

Plano de resposta a incidentes

- Integridade do Backup: responsabilidade de manter um backup diário íntegro em relação aos dados armazenados no servidor, mantendo um histórico de consulta de 29 dias anteriores.

Indicação de responsável por questões de segurança cibernética

A Diretora de *Compliance* e Risco é a responsável por questões de segurança cibernética, através da assistência de profissionais de tecnologia da informação terceirizados para a avaliação de riscos e eventuais remediações, nos termos desta política.

Revisão da política de segurança cibernética

É feita uma revisão, no mínimo, anual desta política, ou em menor periodicidade quando houver alteração na regulação referente a segurança cibernética, de modo a manter sempre atualizadas as suas disposições.

SP, 04/2024.

* * *