POLÍTICA DE SEGURANÇA CIBERNÉTICA

08-02-2019

SUMÁRIO

I. INTRODUÇÃO 3
II. RISK ASSESSMENT 3
III. AÇÕES DE PREVENÇÃO E PROTEÇÃO 3
IV. MONITORAMENTO E TESTES 5
V. PLANO DE RESPOSTA A INCIDENTES 5
VI. RECICLAGEM E REVISÃO 6
VII. VIGÊNCIA 6

I. INTRODUÇÃO

A fim de garantir a segurança das informações em seu poder, a TRX adota a presente política de segurança cibernética ("Política"), tendo por base cinco principais pilares, quais sejam: (i) *risk assessment*; (ii) ações de prevenção e proteção; (iii) monitoramento e testes; (iv) planos de resposta; (v) reciclagem, treinamentos e revisão periódica.

O responsável por tratar e resolver questões relacionadas à segurança cibernética dentro da TRX é o Sr. Vitor Caetanel Nogueira ("DdC", ou "área responsável", quando em conjunto com os Colaboradores de sua equipe).

II. RISK ASSESSMENT

De acordo com o Guia Anbima de Segurança Cibernética, os principais ataques aos quais as instituições estão expostas são os seguintes:

(a) Malware;
(b) Engenharia social;
(c) Pharming;
(d) Phishing;
(e) Cishing;
(f) Smishing;
(g) Acesso pessoal;
(h) Ataques de DDoS e botnets; e
(i) Invasões.

Para proteger os equipamentos da TRX, a sua rede, assim como as informações armazenadas eletronicamente contra os riscos listados acima e outros, a TRX definiu em documento apartado todos os ativos relevantes à instituição (*v.g.* documentos confidenciais, dados pessoais dos investidores, etc).

A definição de ativos sujeitos à risco cibernético, assim como a localização do armazenamento da informação digital e grau do risco ("Inventário") será atualizada periodicamente, a exclusivo critério da área responsável.

A TRX mapeia os principais riscos aos quais cada item do Inventário está exposto, classificando-os de acordo com o seu valor monetário e o seu nível de importância para as atividades da TRX.

III. AÇÕES DE PREVENÇÃO E PROTEÇÃO

A TRX adota por princípio o fato de que um ataque cibernético é sempre iminente. Assim, a TRX segue rigorosamente alguns princípios básicos para prevenir ataques do gênero.

- Segregação de acessos

Conforme já especificado em outras políticas internas, a TRX segrega os acessos aos sistemas conforme a necessidade de cada área e/ou Colaborador, bem como adota regras mínimas na definição de senhas de acesso a dispositivos corporativos.

Os acessos são concedidos com autorização da área responsável, sob responsabilidade do DdC. É realizada uma revisão nos acessos concedidos sempre que alguém muda de função dentro da TRX.

Dados sensíveis e/ou estratégicos também são armazenados em diretórios de acesso restrito dentro da rede, permitindo apenas que colaboradores que farão efetivamente uso das informações para desempenhar seus trabalhos tenham o acesso correspondente.

- Logins rastreáveis e auditáveis

Todos os eventos de login e alterações de senhas devem permanecer auditáveis e rastreáveis.

- Prevenção no acesso remoto

A TRX adota os mais elevados padrões de segurança quando necessária a realização de acessos remotos.

- Instalação de novos equipamentos

A TRX deverá garantir que a configuração e instalação de novos equipamentos e sistemas seja realizada somente por pessoas autorizadas e de forma segura. Devem ser realizados testes de homologação e de prova de conceito antes do envio do produto à ambiente de produção.

- Contratação de terceiros

Na contratação de terceiros que poderão ter acesso à base de dados ou informações sensíveis da TRX, clientes ou stakeholders, a TRX deverá solicitar evidências de que o terceiro possui política específica de segurança das informações (ou afins), devendo a TRX se certificar (inclusive contratualmente) de que (i) os dados sejam sempre que possível anonimizados antes do envio; e (ii) os dados sejam prontamente deletados após a prestação do serviço ou assim que solicitado pela TRX.

No contrato a ser celebrado com terceiros prestadores de serviços, a TRX deve se pautar pelos princípios aqui estabelecidos, dentro dos quais se incluem as seguintes recomendações: (i) cláusulas de proibição de compartilhamento de senha entre os funcionários do terceiro

contratado; (ii) cláusulas de proibição de compartilhamento de códigos fonte na internet, quando couber; (iii) cláusulas de confidencialidade, quando couber.

- *Firewall*, antivírus e *internet*

A TRX conta com firewall e antivírus com a finalidade de evitar ou mitigar riscos cibernéticos.

- Uso do correio eletrônico ("e-mail")

O usuário do endereço de e-mail deve adotar precauções e ser diligente em relação aos usuários destinatários da mensagem, além de se atentar para o nível de sigilo das informações contidas na mensagem, e os links e arquivos de terceiros externos à TRX, ainda que conhecidos.

- Back-up das informações

O backup é realizado semanalmente.

- *Downloads*

Observadas as disposições da Política de Segurança da Informação, *downloads* poderão ser realizados, desde que ligados à atividade profissional do usuário. O DdC e área responsável poderão, a seu exclusivo critério e em conjunto com o TI, decidir por bloquear previamente determinados tipos de *downloads*.

IV. MONITORAMENTO E TESTES

A TRX deve assegurar o funcionamento contínuo e correto dos mecanismos de controle descritos acima.

A TRX mantém inventários de *hardware* e *software*, verificando-os periodicamente para identificar elementos estranhos à instituição. A área responsável deve diligenciar para manter os sistemas operacionais e os *softwares* atualizados.

O DdC é responsável ainda por monitorar as rotinas de backup, executando testes regulares de restauração dos dados.

Ademais, sempre que possível a TRX deverá realizar *pentests* (testes de invasão), assim como análises de vulnerabilidades, contratando terceiros especializados, se necessário.

V. PLANO DE RESPOSTA A INCIDENTES

A TRX conta com plano de resposta aos incidentes ("Plano") que leva em conta os cenários de ameaças previstos durante a realização do *risk assessment*. O Plano deve ser de conhecimento apenas dos responsáveis pela segurança cibernética, além dos diretores e dos sócios, e deverá levar em consideração os cenários de ameaças previstos no *risk assessment*.

Em caso de ataque cibernético, a TRX, por meio de sua área responsável, deve diligenciar para tratar o ataque e permitir a continuidade dos negócios.

O eventual vazamento de informações para fins maliciosos é tratado pela imediata troca de criptografia dos arquivos e estudo para análise se o vazamento foi de causa interna (colaborador tirando dados da empresa) ou externa (arquivos obtidos através de invasão de *hacker*).

Caso qualquer funcionário detecte uma suspeita de ataque cibernético, deverá prontamente comunicar aos responsáveis por esta Política, para que estes entrem em contato com o DdC e este tome as medidas que entender necessárias.

As documentações relacionadas ao gerenciamento dos incidentes deverão ser arquivadas com a área responsável da TRX.

VI. RECICLAGEM E REVISÃO

Esta Política será revisada em periodicidade mínima de um ano, ou sempre que houver alteração na regulação referente a segurança cibernética.

Sem embargo, a TRX deverá garantir que o *risk assessment*, as implementações de proteção, o plano de resposta a incidentes e o respectivo monitoramento estejam sempre atualizados.

A área responsável da TRX deve promover a cultura de cibersegurança junto aos Colaboradores da instituição. É fundamental, apenas para citar um exemplo, que os Colaboradores tenham especial atenção ao clicar em links recebidos ainda que provenientes de um remetente aparentemente conhecido.

Para atingir a melhor cultura em cibersegurança, a TRX poderá promover cursos, arcar com custos de eventos sobre o tema, como também investir na formação de seus profissionais, a seu exclusivo critério.

VII. VIGÊNCIA

Esta Política revoga todas as versões anteriores e passa a vigorar na data de sua aprovação pela Diretoria. Eventual incompatibilidade entre as versões anteriores e a versão atual, se existirem, serão tratadas pelo DdC.