PREFEITURA MUNICIPAL DE ARAÇOIABA DA SERRA

Av.Luane Milanda de Oliveira, 600-Jardim Salete, CEP 18.190-000 Estado de São Paulo.

CNPJ.: 46.634.069.0001-78

Fone (015) 3281-7000

ATENÇÃO

Destinado as pessoas físicas titulares de dados armazenados junto à Prefeitura.

A Prefeitura Municipal de Araçoiaba da Serra informa que sofreu um ataque cibernético (incidente de segurança da informação) do tipo Ransomware (conhecido como sequestro de dados) que atingiu aproximadamente 70% da base de dados de pessoas físicas. A Prefeitura iniciou imediatamente o processo de verificação interna e comunicou o ocorrido às autoridades competentes.

A Prefeitura Municipal de Araçoiaba da serra segue rigorosos padrões de segurança da informação, baseados nas melhores práticas de mercado e tem trabalhado continuamente para mitigar os danos e evitar a reincidência desse tipo de incidente.

Leia o Documento Completo e ter todas as informações

1. Resumo e data de ocorrência do incidente;

No dia 08 de setembro de 2024, a Prefeitura Municipal de Araçoiaba da Serra sofreu um ataque cibernético do tipo Ransomware (conhecido como sequestro de dados). Os invasores criptografaram uma parte significativa dos sistemas e alegam ter obtido cópias de arquivos dos servidores da empresa, entre esses arquivos estão os bancos de dados. Durante o ataque, os criminosos deixaram um manifesto informando que, caso o resgate não fosse pago, eles publicariam os dados supostamente copiados em plataformas públicas ou vendê-los a terceiros. No entanto, não há confirmação precisa se houve cópia de arquivos.

2. Descrição dos dados pessoais afetados;

Os dados pessoais supostamente copiados estavam armazenados em bancos de dados, e não em arquivos abertos, estando protegidos pelas configurações de segurança da linguagem de banco de dados. Entre os bancos de dados comprometidos estão o de tributos, que contém informações pessoais dos contribuintes, como nome, endereço e documentos pessoais, e o banco de dados de educação, que também armazena dados pessoais, incluindo nome do aluno, nome dos pais, documentos pessoais, RA e endereço.

3. Riscos e consequências aos titulares de dados;

Quando ocorre um ataque de Ransomware com risco de vazamento de dados, os titulares dos dados pessoais ficam expostos a uma série de riscos e consequências, que podem ser graves. Aqui estão os principais:

a) Roubo de Identidade

- Risco: Informações pessoais como nome, CPF, RG, endereços, números de telefone podem ser usadas para fraudes e roubo de identidade.
- Consequência: Os criminosos podem abrir contas bancárias, solicitar empréstimos, ou realizar compras em nome dos titulares dos dados, causando prejuízos financeiros e danos à reputação.

b) Exposição de Dados Sensíveis

- Risco: Informações confidenciais, como dados fiscais e educacionais, podem ser expostas publicamente ou vendidas a terceiros mal-intencionados.
- Consequência: Titulares podem sofrer discriminação, estigmatização ou constrangimento, especialmente se dados comportamento estiverem envolvidos.

c) Abuso de Dados Pessoais

- Risco: Informações pessoais vazadas podem ser usadas para extorsão, chantagem ou manipulação psicológica.

- Consequência: Indivíduos podem ser coagidos ou intimidados com a ameaça de divulgação de informações sensíveis ou comprometedoras, o que pode afetar a vida pessoal e profissional das vítimas.

d) Phishing e Ataques de Engenharia Social

- Risco: Após um vazamento, criminosos podem usar os dados obtidos para realizar ataques de phishing mais sofisticados e personalizados, com o objetivo de enganar as vítimas.
- Consequência: As vítimas podem ser induzidas a fornecer mais informações confidenciais, clicar em links maliciosos ou baixar malware, agravando ainda mais o prejuízo.

e) Danos à Privacidade

- Risco: A exposição de dados pessoais, especialmente os mais sensíveis, pode causar uma invasão severa da privacidade dos titulares.
- Consequência: A confiança em instituições que armazenam os dados pode ser permanentemente abalada, e os titulares podem sofrer angústia psicológica devido à violação de sua privacidade.

f) Impacto Psicológico

- Risco: O sentimento de vulnerabilidade e a perda de controle sobre informações pessoais podem causar estresse, ansiedade e traumas psicológicos.
- Consequência: O impacto emocional de saber que dados privados podem estar circulando entre criminosos pode afetar o bem-estar mental das vítimas.

Medidas de Mitigação para os Titulares:

- Monitoramento de crédito: Serviços de proteção e monitoramento de crédito podem ser oferecidos às vítimas.
- Alteração de senhas e credenciais: Recomenda-se a troca imediata de senhas e a adoção de autenticação em dois fatores.
- Alertas de segurança: Configuração de alertas para atividades incomuns nas contas pessoais, como transações bancárias.
- Orientação sobre fraudes: Educação sobre como reconhecer e evitar tentativas de phishing e golpes.

4. Medidas tomadas e recomendadas para mitigar seus efeitos, se cabíveis;

a) Resposta imediata ao incidente

- Identificação do alcance do vazamento: Não há evidências que confirmem que os dados foram realmente copiados, tampouco há evidências de publicação.
- Contenção do incidente: Foram isolados todos os sistemas afetados para evitar a disseminação do vazamento.
- Notificação das autoridades: Foi realizada a notificação provisória à ANPD.

b) Fortalecimento da segurança

- Auditoria dos sistemas de segurança: Foi realizada uma análise completa do ambiente computacional desta municipalidade para identificar as vulnerabilidades que permitiram o vazamento e está sendo traçado um plano de ação para implementar medidas de segurança adicionais.
- Aprimoramento da criptografia: Está sendo projetado que os dados sensíveis dos bancos de dados estejam devidamente criptografados, tanto em trânsito quanto em repouso.
- Revisar políticas de acesso: Está sendo analisada as permissões de acesso aos dados sensíveis para que apenas usuários autorizados tenham acesso.
- Monitoramento contínuo: Está sendo estudada a implementação de ferramentas adicionais de monitoramento que possam detectar e identificar novos ataques.

c) Apoio aos indivíduos afetados

- Oferecer suporte: Forneça orientações sobre medidas que os afetados devem tomar, como trocar senhas e monitorar transações financeiras.
- Proteção contra fraude: Em casos de vazamento de dados financeiros ou documentos pessoais, considere oferecer serviços de monitoramento de crédito ou proteção contra fraude.

d) Reforço da conformidade legal

- Cumprir as normas de privacidade: As ações tomadas estão em conformidade com a lei de proteção de dados, LGPD, ou outras legislações aplicáveis.
- Documentação e relatórios: Está sendo documentado todas as medidas adotadas para mitigar o vazamento e prevenir novos incidentes.
- Estão sendo implantadas medidas de segurança para prevenção a longo prazo
- Treinamento contínuo de funcionários: Será implantada uma rotina de treinamentos aos funcionários sobre segurança da informação, com objetivo de mitigar ameaças futuras.
- Realizar testes de invasão: Está sendo desenvolvida uma rotina regular para avaliação das defesas de segurança através de simulações de ataque pode ajudar a identificar pontos fracos.
- Essas ações visam não apenas mitigar os efeitos de um vazamento, mas também prevenir futuros incidentes, garantindo que os dados pessoais estejam mais protegidos.

5. Dados de contato do controlador para obtenção de informações adicionais sobre o incidente.

E-mail.: lgpd@aracoiaba.sp.gov.br

Telefone: 15-32817000