RESPOSTA A IMPUGNAÇÃO APRESENTADA PELA BETHA SISTEMAS LTDA.

PROCESSO LICITATÓRIO Nº 21/2023
EDITAL DE PREGÃO Nº 07/2023

Em apertada síntese, destaca-se que a impugnação da empresa BETHA SISTEMAS LTDA. versa sobre a existência de representações no Tribunal de Contas do Estado de Santa Catarina que possuem o mesmo objeto e a mesma exigência de firewall de borda exclusivamente para a Contratante, fazendo referência aos municípios de Imbituba e Santa Rosa de Lima. Alega que a forma de hospedagem dos sistemas, o IP e o firewall direcionam o certame e restrigem a competitividade e que a resposta dada pelo seu cliente no Estudo Técnico preliminar é questionável, bem como o seu o teor.

Sem razão a impugnante.

Tem-se como desnecessário tecer maiores esclarecimentos no que se refere a semelhança do instrumento convocatório em relação a outros instrumentos publicados pelo município, pois tanto o Termo de Referência quanto o Estudo Técnico Preliminar repetem de forma exaustiva que esta Administração se baseou nas experiências e soluções adotadas por outros municípios na confecção do presente Edital.
Assim como os municípios de Imbituba e Santa Rosa de Lima, este município também foi (@22/80090494) alvo da estratégia da empresa Betha Sistemas Ltda. de utilizar-se do Tribunal de Contas do Estado de Santa Catarina para distorcer a realidade dos fatos para perpetuar-se como contratada.
Ao analisar a representação promovidas pela Impugnante e por ela mencionada em face do Município de Santa Rosa de Lima (@22/80087353) em curso e, portanto, sem decisão colegiada definitiva, observa-se que o Relator Luiz Eduardo Cherem decidiu da seguinte forma:

Quando da Decisão GAC/LEC nº 1449/2022 (fls. 1098/1103) em que concedi a medida cautelar, entendi presentes os requisitos da plausibilidade jurídica e perigo da demora, uma vez que presentes especificações que restringiriam o caráter competitivo do certame, além de haver tempo hábil para evitar prejuízo à Unidade Gestora.

Notadamente, fundamentei a plausibilidade jurídica na ausência de estudo técnico preliminar e na exigência de datacenter próprio, com supedâneo no Relatório nº 78/2022 (fls. 1085/1095) da diretoria técnica.

Sem descurar da necessária análise do mérito, o que se dará oportunamente, no âmbito destes autos, **entendo necessário revisitar-se o quesito do perigo da demora.**

Isso porque o conteúdo da peça recursal constante do @REC23/00060196 trouxe novos elementos de informação acerca do presente caso concreto, aliado à manifestação de fls. 1123/1134.

Com efeito, a Unidade Gestora esposou dificuldades na boa execução contratual pela atual detentora do contrato, a empresa Betha Sistemas Ltda., o que não estaria satisfazendo o interesse público do ente.

Malgrado se recomende que seja aberto processo administrativo sancionador próprio, a fim de se tratar dos descumprimentos contratuais, as características do presente feito permitem concluir que o ônus da demora processual não deve ser suportado pela Administração Pública do Município.

Nesse sentido é a lição de Romano Scapin:

A evidência é a segunda alternativa justificadora para expedição de provimentos provisórios no processo civil. O mesmo raciocínio desenvolvido até sua afirmação normativa serve para justificar sua utilização no processo de contas: a distribuição justa do ônus relativo ao tempo do processo deve valorizar o direito que está em evidência, antecipando, pois, a tutela a favor de quem o detém. A concepção de que a tutela estatal deve ser efetiva, tempestiva e adequada implica a necessidade de que também o processo de contas abarque técnicas que permitam essa justa distribuição.

Mais:

A técnica antecipatória, viabilizadora da utilização de provimentos provisórios no processo, não tem como objetivo, na visão de Marinoni, simplesmente resolver o problema eventualmente causado pelo perigo da tardança do provimento jurisdicional. Em verdade, ela teria por função "distribuir de forma isonômica o ônus do tempo no processo. Essa

distribuição pode ocorrer tanto em face da alegação de urgência – leia-se, de perigo de ilícito ou de perigo de dano – como em face da

necessidade de outorgar o devido valor à evidência do direito posto em juízo".

À evidência, vislumbro haver perigo da demora inverso, na medida em que a atual deficiência relatada na prestação dos serviços ocasiona danos superiores à Unidade Gestora quando comparados aos benefícios de se aguardar o desfecho deste processo.

Assim sendo, constata-se a presença de perigo da demora inverso, o que ocasiona o não preenchimento dos fundamentos necessários à manutenção da medida cautelar antes concedida, sendo sua revogação a medida de rigor, com fulcro no art. 114, § 13°, do Regimento Interno deste Tribunal de Contas:

§ 13. A medida cautelar de que trata este artigo pode ser revista por quem a tiver adotado, de ofício ou a requerimento do responsável ou interessado, sem prejuízo do disposto no §1º deste artigo.

Outrossim, não é demais frisar a importância de a Unidade Gestora proceder à devida abertura de processo administrativo sancionador, a fim de se regularizar a situação de descumprimento contratual relatada, seja cumprindo a função de se glosar valores indevidos, seja impactando na participação da contratada em futuras licitações.

No caso, analisando a defesa anexada pelo Município de Santa Rosa de Lima, é possível verificar que ela traz a tona o fato de que o sistema que atualmente utiliza, não atende as suas necessidades, apontando, inclusive, uma extensa lista de municípios que se mostram insatisfeitos que a mesma fornecedora de sistemas, a qual é a atual contratada do Município de Vargem.

Ainda é possível verificar que as questões apontadas como direcionantes e restritivas pela impugnante foram por elas atendidas no pregão presencial 30/2020 promovido pelo Município de Ipumirim.

No mesmo sentido, na Representação 22/80007694 há um relato dramático do Município de Imbituba informando as dificuldades enfrentadas pelo município na sua relação com a contratada.

Ora, o Município de Vargem já havia promovido licitação com objeto idêntico no Pregão Presencial 37/2022 que foi Representado pela empresa impugnante sob a alegação de que não foi realizado Estudo Técnico Preliminar, o qual, ainda que exigível na Nova Lei de Licitações, não é exigida pela Lei nº 10.520/2002, a qual regia o anterior e o atual certame.

Ainda assim, o Município se empenhou a realizar Estudo Técnico preliminar tendo como norte a busca de soluções adotadas por outros municípios, dentre eles, Catanduvas.

Ainda **assim, não satisfeita, a empresa impugnante não contradiz nenhuma das respostas dadas pelo Município, alegando que "*o questionário contem respostas questionáveis e que evidentemente destoam da realidade*", mas não afirma quais dessas respostas estariam erradas!**

Portanto, tem-se como temerária a tentativa da impugnante de buscar desqualificar o Estudo Técnico Preliminar e as respostas dadas pelos municípios, uma vez que as respostas coadunam com a realidade dos fatos. Trata-se, assim, da falácia do ataque ao argumentador – também conhecida pelo seu nome em latim *argumentum ad hominem* – em que para se fugir do debate, ataca-se a pessoa do argumentador, não o argumento, o que não será reverberado e dispensa maiores ilações por esta Administração que julga improcedente a impugnação nesse sentido.
Em relação aos requisitos relativos a hospedagem do sistema, destaca-se que a Advocacia Geral da União assevera em suas notas explicativas referente aos modelos de contratações por ela disponibilizado que:

> Nota Explicativa 2: Caso o objeto do contrato envolva, ainda que indiretamente, o acesso ou o **tratamento de dados pessoais**, é **possível que a Administração estabeleça modelagem contratual por meio da qual seja imposto ao Contratado o dever de disponibilizar à Administração a possibilidade de acesso direto a esses dados, o que deve se dar com todas as cautelas cabíveis em relação ao tema.**
> **Vale lembrar que eventual requerimento administrativo do titular dos dados será direcionado à Administração, sendo certo que comandos oriundos de Autoridade Regulatória ou do Poder Judiciário serão igualmente direcionados à Administração, inclusive com risco de responsabilização objetiva.** Por isso, em situações em que for justificável, fica a recomendação para que a Administração crie condições para que possa atender tempestivamente o requerimento do titular dos dados ou eventual comando regulatório ou judicial. Tudo isso para que a Administração tenha condições de atender o requerimento ou comando tempestivamente, sem depender exclusivamente do Contratado para tanto.
> **O tema deve ser avaliado pela Administração com base nos riscos da contratação em relação aos dados pessoais eventualmente envolvidos**.

Portanto, a Administração é responsável pelos dados armazenados nos sistemas de gestão pública por ela contratados, razão pela qual tem-se como inafastável a necessidade de se estabelecer em edital requisitos de segurança das informações.

A justificativa para um detalhamento de uma infraestrutura relacionada ao datacenter encontra robusto amparo na Lei Geral de Proteção de Dados, nas palavras da doutrina especializada:

> Pois bem. A diretriz geral estabelecida pelo artigo 23 da LGPD, com efeito, demonstra atenção do legislador para o atual (e real) contexto sociopolítico, em que a Administração Pública precisa, de ordinário, se organizar em torno de sistemas eficientes de gestão de dados. Com efeito, a **informatização dos dados, mais do que um imperativo da eficiência administrativa e da governança pública, configura providência verdadeiramente essencial à própria viabilização estratégica da função executiva, haja vista o gigantesco volume de dados e informações que precisam ser diariamente processados pelo poder público, pelos mais diversos motivos: desde cruzamento de informações constantes de declarações do imposto de renda até a manutenção de prontuários de pacientes em uma unidade básica de saúde**.
> Sem dúvidas, portanto, esses "***sistemas governamentais são alimentados por dados pessoais e sensíveis, relacionados à saúde, a educação, a previdência, ao imposto de renda, a assistência social, a informação bancária, dentre tantas outras informações pessoais que estão em poder da Administração Pública***" [3].
> Ocorre que, como acertadamente reconhece Danilo Doneda, o tratamento de dados pessoais — sobretudo por meio de processos automatizados — é uma atividade de risco, que "***se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais***" [4].
> Daí a se cogitar, também no contexto do tratamento de dados pessoais pelo poder público — e talvez com ainda maior razão —, a observância do já mencionado princípio da responsabilização (artigo 6º, X): como observam Bruno Feigelson et al., o artigo 31 da LGPD evidencia a aplicação deste princípio à órbita pública, prevendo "*a aplicação de medidas cabíveis pela ANPD na hipótese de ser verificada qualquer infração ao disposto na LGPD durante o tratamento de dados por órgãos públicos*" [5].
> [...]

> **Inequivocamente, o regime jurídico estabelecido pela LGPD investe o controlador e o operador da condição de garantidores da não ocorrência de danos em virtude do tratamento de dados pessoais. Deve-se lembrar, neste sentido, que eventual omissão da Administração Pública na adoção de cautelas e demais procedimentos de segurança (por imposição expressa dos princípios da segurança e da prevenção) no tratamento de dados pessoais, tendo em vista a sua posição de controladora ou operadora, jamais consistirá em omissão genérica, mas, sim, em omissão específica, a atrair o regime geral da responsabilidade civil objetiva prevista no artigo 37, §6º, da Constituição Federal — em consonância com a jurisprudência pacífica do Supremo Tribunal Federal** (AI 852.237 AgR,
>
> relator min. Celso de Mello, 2ª Turma, julgado em 25/6/2013). (PEREIRA. Flávio Henrique Unes, ALVIM, Rafael da Silva. O Regime de responsabilidade do Estado na Lei Geral de Proteção de Dados. https://www.conjur.com.br/2020-nov-22/pereira-alvim-regime-responsabilidade-estado-lgpd). (grifo nosso).

Diante disso, o Tribunal de Contas da União decidiu da seguinte forma em relação ao tema:

> LEVANTAMENTO SOBRE A GOVERNANÇA E GESTÃO DE SEGURANÇA DA INFORMAÇÃO E DE **SEGURANÇA CIBERNÉTICA NA ADMINISTRAÇÃO PÚBLICA FEDERAL**. PANORAMA GERAL. **PRINCIPAIS RISCOS E VULNERABILIDADES**. GRANDES TRANSFORMAÇÕES DIGITAIS. DILIGÊNCIA. CIÊNCIA.
> [...]
> 285. Em julho de 2017, o GSI/PR publicou o documento "**Requisitos Mínimos de Segurança da Informação aos Órgãos da Administração Pública Federal**"[endnoteRef:52] (peça 42, p. 1062-1073) , com "**a finalidade de elevar e aprimorar a segurança da informação** no âmbito da [APF], sendo constituídos por uma coletânea dos principais procedimentos extraídos dos normativos exarados pelo [DSIC/GSI/PR], com alguns complementos e atualizações", influenciado "em substantiva proporção pela crescente incidência de ataques cibernéticos, e por constantes ameaças à segurança da informação, que p**assaram a requerer dos gestores do tema atenção, dedicação e estudo muito maiores e abrangentes**" (peça 42, p. 1063) . [52:]
> 286. Para o escopo deste levantamento, relevam as "Orientações Gerenciais" e as "Orientações Técnicas" (itens 2.1 e 2.2) . Dentre as primeiras, destacam-se: institucionalizar e revisar periodicamente política

> de SegInfo, PCA, política de backup e PCN; constituir formalmente CGSI; nomear gestor de SegInfo; constituir ETIR; mapear e inventariar os ativos de informação; realizar gestão dos riscos de SegInfo; **e fortalecer internamente a cultura de SegInfo** (peça 42, p. 1063-1065) .
> 287. Dentre as últimas, frisam-se: **usar protocolo HTTPS; manter desenvolvedores atualizados; estabelecer política de senhas; não utilizar senhas padrão; nunca armazenar usuários, senhas ou chaves criptográficas no código fonte; validar entradas de dados; implementar logs; conceder acessos mínimos aos usuários; tratar mensagens de erro de bancos de dados e servidores web; não armazenar dados de produção em ambientes de teste e de homologação; realizar testes de intrusão; eliminar vulnerabilidades reportadas; segregar ambientes e redes com firewall (manter regras por meio de processo formal) ; não usar portas de comunicação inseguras (e.g. telnet e FTP) ; monitorar validade de certificados digitais; preferir soluções com criptografia** (e.g. SFTP e Secure Socket Shell - SSH) [peça 42, p. 1065-1068].

Portanto, considerando que o objeto engloba dois tipos de serviços diferentes (software x datacenter) mas que um complementa o outro, entende-se que deve haver especificações de datacenter devidamente apropriadas a garantir requisitos mínimos de segurança para a contratação, o que não causa nenhum prejuízo a competitividade, pois a própria representante já foi vencedora de certames com exigências semelhantes.

São quase que diárias as informações advindas da imprensa a respeito de invasões a banco de dados de sistemas municipais. Recentemente, noticiou-se no Estado do Paraná que malfeitores tiveram acesso aos bancos de dados de aproximadamente 200 municípios clientes da empresa Elotech Gestão Pública Ltda no mês de dezembro de 2022: https://palmeira.pr.gov.br/comunicado-sistemas-utilizados-pelo-municipio-estao-indisponiveis/.

No caso, a solução adotada pela empresa foi:

> "A Elotech também comunicou à CMC que, como processo de mitigação, contratará serviços de testes de invasão (Pentest) e que já adquiriu um **novo Firewall de alta segurança**. Foi feito Boletim de Ocorrência e as investigações estão sob responsabilidade da Polícia Civil do Paraná."

Porém, o quadro da falta da segurança é ainda mais alarmante, em junho de 2022 (ou seja: antes dos incidentes de segurança ocorrido nos 200 Municípios clientes da Elotech Gestão Pública Ltda), a jornalista Fernanda Campagnucci escreveu para o blog "Um Dado a Mais", um estudo sobre o panorama da falta de segurança dos municípios no âmbito nacional, e, que sustenta que **mais de 300 municípios já haviam sido atacados,**

nos últimos 3 anos, somando-se aos ataques ocorridos no Paraná, pode-se chegar, seguramente, a mais de 500 Municípios afetados:

Municípios à deriva: sem segurança digital, mais de 300 foram atacados em 3 anos

por Fernanda Campagnucci - em Tecnologia & Sociedade - 28 de junho de 2022

Cidades de todos os portes são afetadas e casos têm algo preocupante em comum: não há qualquer transparência sobre a extensão dos danos, nem menção a planos de resposta a incidentes ou aviso aos titulares de dados sobre a exposição

Em pelo menos 310 cidades brasileiras, a população enfrentou dias de serviços interrompidos, teve seus dados pessoais expostos ou mesmo impostos desviados dos cofres públicos por causa de ataques cibernéticos, de 2019 até hoje. Na falta de um levantamento oficial sobre o assunto,

coletei os dados de maneira inédita a partir de informações precárias publicadas em veículos locais ou em notas públicas das próprias prefeituras. É a ponta de um iceberg: muitos mais podem ter sido alvo de ataques sem que os casos fossem noticiados.

Casos de invasão digital a órgãos públicos ganharam grande destaque na imprensa nos últimos tempos, sobretudo na esfera federal. Mas, sem ter a mesma capacidade de se defender e sem políticas consistentes de governança de dados, os municípios se tornam vítimas silenciosas dessa epidemia de ataques, que cresce rapidamente no Brasil.

O investimento necessário, mas com frequência adiado, acaba se traduzindo em prejuízos difíceis de quantificar. Há prefeituras em que os cidadãos ficaram até duas semanas sem acesso a qualquer serviço público — mesmo aulas remotas, instituídas na pandemia, tiveram de ser suspensas. Em diversos outros, funcionários e fornecedores ficaram dias sem receber pagamentos.

Há, ainda, casos de equipes que fizeram mutirões para refazer processos e relançar informações em sistemas — o que é muito grave do ponto de vista de integridade pública, pois dá margem a erros e alteração indevida de dados históricos. A vulnerabilidade atinge também os computadores de secretarias de finanças, permitindo ataques sempre suspeitos a contas bancárias e desvio de recursos.

Categorizei os ataques identificados em cinco tipos:

(1) Ransomware, que envolve o "sequestro" de dados com uso de criptografia e mediante solicitação de pagamento;

(2) 'Pichação', também chamado pelo termo técnico em inglês defacement, em que sites são alterados ou mensagens de cunho político são postadas;

(3) Desvio de recursos, quando, por causa da infecção de máquinas com vírus, contas bancárias são afetadas;

(4) Sem informações sobre o método, quando as notícias são tão superficiais que não permitem identificar o tipo de ataque e

(5) DDoS, ou ataques distribuídos de negação de serviços, quando o excesso de requisições a um site acaba por derrubá-lo.

Municípios de todos os portes estão sujeitos aos ataques: dos maiores e mais ricos, como capitais e cidades com alto desenvolvimento socioeconômico, aos pequenos, em que o desvio de recursos chegou a representar dois meses inteiros de arrecadação (é o caso de Imbuia-SC, com cerca de 6 mil habitantes).

O que todos parecem ter em comum: não há qualquer transparência sobre a extensão dos danos, nem a quais dados foram afetados, especialmente os de natureza pessoal e sensível. Tampouco há qualquer menção à existência de um Plano de Resposta a Incidentes, como previsto na Lei Geral de Proteção de Dados (LGPD), ou de aviso aos titulares de dados sobre a exposição. Finalmente, em nenhum dos casos há informação

sobre eventual notificação do ocorrido à Autoridade Nacional de Proteção de Dados (ANPD).

Quase 30 casos foram classificados como "sem informação sobre o método", pois as notas oficiais ou notícias a respeito das ocorrências eram tão lacônicas que não permitiam compreender o que de fato aconteceu. Da mesma forma, pouco se sabe sobre os resultados de investigações ou conclusões e medidas tomadas depois que os casos foram noticiados.

Desvio de R$ 14,5 milhões

Entre os ataques, o tipo mais curioso é o que envolve desvio de recursos. Identifiquei pelo menos dez que, somados, representaram R$ 14,5 milhões a menos nos cofres dos municípios. Em diversas das notícias, a polícia civil de diferentes estados diz trabalhar com a hipótese de vulnerabilidades

nos computadores ou na rede das prefeituras — em Campinas (SP), por exemplo, R$ 7,4 milhões foram desviados da conta em que recebe o Imposto Predial e Territorial Urbano (IPTU) e não é utilizada para fazer nenhum tipo de pagamento.

Em Virgolândia (MG), a origem da invasão que desviou R$ 152 mil de quatro contas da prefeitura em maio de 2021 teria sido um arquivo infectado enviado a uma funcionária do Tesouro Municipal, que acreditava estar abrindo uma nota fiscal. Um mês depois, em Jaboticatubas (MG), R$ 2,9 milhões de reais desapareceram das contas da prefeitura em menos de uma hora, desviados em 42 transferências.

Nem sempre as instituições bancárias ressarcem os municípios — enquanto Campinas (SP) conseguiu acordo com o Banco do Brasil para devolução, a prefeitura de Matelândia (PR), com cerca de 18 mil habitantes, precisou ir à Justiça demandar o ressarcimento dos quase R$ 500 mil desviados de suas contas.

Apesar da semelhança de métodos e coincidência de datas, as notícias esparsas das diferentes localidades não dão a entender que haja alguma investigação nacional a respeito dos grupos envolvidos.

Uma moderna queima de arquivos?

No meio de tantos ataques, é de se questionar se algumas invasões não podem estar sendo forjadas para desvio de recursos ou "queima de arquivos" — o que seria outro problema sério de integridade pública. Um caso assim foi denunciado em Santa Catarina. A Prefeitura de Biguaçu (SC), que ficou cerca de 40 dias com sistemas indisponíveis alegando ter sido vítima de ransomware no final de 2020, está sendo investigada pela Polícia Civil do estado por suposta falsa comunicação de crime, segundo o portal local ND Mais.

Em Mateus Leme (MG), em setembro de 2020, um ataque também foi colocado em dúvida. Foram duas etapas: primeiro, listas de documentos pessoais de munícipes inscritos na dívida ativa começaram a circular na internet. Depois que a prefeitura disse que estava investigando os responsáveis, novo ataque foi feito, desta vez de ransomware, o que levou

a administração a suspeitar que o objetivo era apagar rastros do primeiro vazamento — algo não confirmado.

Ativismo anticiência e pró-Bolsonaro

Os ataques de defacement foram bastante comuns durante a pandemia. Longe de apenas chamarem a atenção, também impactaram serviços e não há clareza sobre até que ponto chegaram a expor dados pessoais. Na maior parte das vezes esse tipo de ataque explora vulnerabilidades apenas no código do front-end das páginas, mas algumas notícias falam em "senhas fracas" de administradores que teriam sido comprometidas.

O mais expressivo deles atingiu de uma só vez 245 prefeituras catarinenses (o que representa 83% de todo o estado), em dezembro de 2021. Essas cidades tinham sites e serviços hospedados nos servidores da Federação Catarinense de Municípios. Os criminosos escreveram mensagens políticas contra medidas de proteção da Covid-19 e em apoio à reeleição de Bolsonaro.

Em outros ataques aqui categorizados como "sem informação sobre o método", não há mais detalhes sobre o tipo de invasão, mas também tiveram como alvo os sites e sistemas de secretarias de saúde, em protesto contra medidas sanitárias de combate à pandemia e contra as campanhas de vacinação.

Apagando incêndio, sem prevenir novos

Sem o foco na prevenção e em governança de dados, as prefeituras parecem estar apagando incêndio. No final de 2019, duas prefeituras chegaram a decretar estado de emergência após os ataques — medida administrativa que permite dispensar ritos de licitação, por exemplo. É o caso de Barrinha (SP) que, com a folha de pagamentos "sequestrada", pagou mil servidores manualmente. Em Itacarambi (MG), depois de ter esgotado as possibilidades de recuperação dos dados, o município "fechou" a prefeitura por 15 dias, suspendendo serviços financeiros, tributários, emissões de notas fiscais e de gestão de recursos humanos, entre outros.

Algumas chegam a contratar serviços para descriptografar arquivos após ataques de ransomware — não há detalhes sobre o sucesso dessas medidas. O diário oficial da Prefeitura de Alto Taquari (MT), por exemplo, traz a informação de que a administração contratou, por dispensa de licitação, empresa para essa finalidade, por R$ 23,7 mil.

A implementação da LGPD pode ser encarada como oportunidade para estabelecer estruturas de governança que se articulem à política de serviços digitais e de transparência, com mapeamento de dados e de riscos a que estão sujeitos. O investimento nessa infraestrutura precisa ser transparente. As prefeituras também precisam ficar atentas às consultorias oportunistas que prometem "adequar" as cidades à LGPD, sem promover de fato uma estrutura permanente que dê conta de proteger os dados dos cidadãos.

Rua Benjamin Margotti, 289 - Vargem - SC | CEP: 89638-000
prefeitura@vargem.sc.gov.br - Fone (49) 3549-0068 | 3549-0018

Abaixo, listo todos os ataques identificados em notícias locais e notas oficiais de municípios afetados, em prefeituras ou câmaras municipais. Não entraram no escopo notícias sobre roubo de credenciais de redes sociais oficiais.

RANSOMWARE

Envolve o "sequestro" de dados com uso de criptografia e mediante solicitação de pagamento.

Prefeitura de Alegre (ES), junho de 2022: ataque de ransomware deixou sistemas indisponíveis.
Prefeitura de Rio Bom (PR), abril de 2022: cidade suspendeu atendimento ao público após ataque de ransomware, que afetou maior parte dos sistemas da gestão municipal; prefeito diz ter conseguido restabelecer graças à existência de backup.
Prefeitura de Pontes e Lacerda (MT), janeiro de 2022: ataque de ransomware bloqueou bancos de dados e impediu atendimento ao público.
Prefeitura de Taboão da Serra (SP), agosto de 2021: ataque de ransomware tirou todos os sistemas da prefeitura do ar e provocou o fechamento da Atende – Central de Atendimento ao Cidadão. Servidor principal e o de backup foram afetados.
Prefeitura de Bandeirantes (MS), julho de 2021: ataque de ransomware comprometeu "dados e arquivos", mas gestão alegou que sua prestadora de serviço realiza backup e faria a restauração.
Prefeitura de Eldorado (SP), abril de 2021: ataque de ransomware bloqueou "todos os dados" da prefeitura e levou uma semana até que a prefeitura voltasse perto da "normalidade". Pagamento de funcionários atrasou por dias.
Prefeitura de Nova Venécia (ES), novembro de 2020: ataque de ransomware bloqueou o acesso aos sistemas administrativo, contábil e financeiro do município.
Prefeitura de Tupã (SP), outubro de 2020: ataque de ransomware atingiu todos os sistemas da Prefeitura – dos tributos aos serviços, passando por educação e saúde. O último backup datava de quase um mês atrás, e por isso a prefeitura disse que seria necessário "uma grande força tarefa conjunta para o relançamento desses dados".
Prefeitura de Candiota (RS), outubro de 2020: ataque de ransomware deixou os sistemas da cidade indisponíveis durante dias, até que pudesse backup fosse restabelecido.
Prefeitura de Mateus Leme (MG), setembro de 2020: o ataque aconteceu em duas etapas: primeiro, listas de documentos pessoais de munícipes

inscritos na dívida ativa começaram a circular na internet; depois que a prefeitura disse que estava investigando os responsáveis, novo ataque foi feito, desta vez de ransomware, o que levou a administração a suspeitar que o objetivo era apagar rastros do primeiro vazamento.
Prefeitura do Rio de Janeiro (RJ), junho de 2020: ataque de ransomware tornou sistemas de diversas unidades de saúde indisponíveis, no auge da pandemia de Covid-19, prejudicando o trabalho dos médicos e o atendimento a pacientes.
Prefeitura de Jerônimo Monteiro (ES), maio de 2020: ataque de ransomware bloqueou acesso a sistemas administrativo, contábil e financeiro da administração municipal.

Prefeitura de Venda Nova do Imigrante (ES), maio de 2020: ataque bloqueou arquivos da administração municipal e suspendeu serviços por dias, inclusive emissão de alvará e pagamentos.
Prefeitura de Birigui (SP), janeiro de 2020: ataque de ransomware paralisou serviços, mas administração diz que detectou e agiu rapidamente para restabelecer dados e sistemas.
Prefeitura de Barrinha (SP), outubro de 2019: ataque de ransomware fez prefeitura pagar mil servidores manualmente e chegou a decretar estado de emergência.
Prefeitura de Itacarambi (MG), novembro de 2019: após ataque de ransomware e esgotar as possibilidades de recuperação dos dados, o município chegou a decretar estado de emergência que "fechou" a prefeitura por 15 dias, suspendendo serviços financeiros, tributários, emissões de notas fiscais e de gestão de recursos humanos, entre outros.
Prefeitura de Ponta Grossa (PR), setembro de 2019: ataque teve acesso a informações pessoais (inclusive foram utilizadas para ameaçar prefeito, expondo dados seus e de parentes) e foi feita exigência de pagamento. Não fica claro se é ransomware com dados criptografados ou se a ameaça de extorsão é para não divulgar dados que invasores teriam obtido no ataque.
Prefeitura de Alto Taquari (MT), fevereiro de 2019: não há informações sobre o ataque, mas o diário oficial traz a informação de que a Prefeitura contratou, por dispensa de licitação, empresa para "descriptografia" de arquivos após ataque de ransoware, por R$ 23,7 mil.

'PICHAÇÃO' (defacement)

Também chamado pelo termo técnico em inglês defacement, em que sites são alterados ou mensagens de cunho político são postadas.

Prefeitura de Imperatriz (MA), março de 2022: mensagem de protesto contra o aumento de preços dos combustíveis foi deixada no site da prefeitura, que afirmou que os bancos de dados não foram comprometidos.
Prefeitura de Florianópolis (SC), fevereiro de 2022: grupo tirou site do ar e deixou mensagem reivindicando o ataque e alterando textos da página principal da prefeitura.
Prefeitura de Juazeiro do Norte (CE), dezembro de 2021: site foi alterado com mensagem contra o isolamento social para enfrentamento da Covid-19; administração esclareceu que apenas front-end foi afetado, sem comprometimento de dados.
Prefeitura de Brumadinho (MG), dezembro de 2021: sofreu ataque com mensagem de protesto sobre a tragédia causada pela Vale, retirando o site do ar por algumas horas.
Prefeitura de Manaus (AM), dezembro de 2021: pelo menos 12 sites da prefeitura saíram do ar; responsável deixou mensagem na página, mas prefeitura não deu detalhes sobre o comprometimento de bases de dados.
245 prefeituras catarinenses, dezembro de 2021: esse ataque afetou em uma só tacada 245 cidades (83% de todo o estado) que tinham sites e serviços hospedados nos servidores da Federação Catarinense de Municípios; os criminosos escreveram mensagens políticas contra medidas de proteção da Covid-19 e em apoio à reeleição de Bolsonaro.
Prefeitura de Barcarena (PA), outubro de 2021: coletivo publicou mensagem contra a administração da cidade, que expulsou moradores de uma comunidade quilombola na região.

Prefeitura de Fama (MG), agosto de 2021: neste ataque, o nome de Bolsonaro foi publicado no lugar do vice-prefeito e o do prefeito, alterado para "hacker sincero".
Prefeitura de Belo Horizonte (MG), junho de 2021: invasão comprometeu sistema de fiscalização da Prefeitura e interrompeu trabalho dos fiscais; mensagem exibida nas telas dos computadores da prefeitura atacava o prefeito e as medidas de combate à pandemia.
Prefeitura de Serra Negra (SP), junho de 2021: ataque publicou mensagens ofensivas no site da prefeitura.
Câmara Municipal de Santa Cruz do Sul (RS), abril de 2021: ataque de grupo tirou site do ar e deixou mensagens provocativas para administradores do sistema.
Prefeitura de Mato Rico (PR), dezembro de 2020: ataque retirou sites da prefeitura do ar por pelo menos 24 horas.
Prefeitura de Praia Grande (SP), fevereiro de 2021: ataque postou, no site oficial da cidade, uma fotografia do ator David Hasselhoff, famoso pelo seriado S.OS. Malibu.
Prefeitura de Caraguatatuba (SP), maio de 2020: página oficial da cidade amanheceu com a foto de Bolsonaro, usando máscara com dizeres anticorrupção e alusivos às eleições de 2022. Grupo que assumiu a autoria divulga em redes sociais ataques semelhantes a outros órgãos públicos.

Prefeitura de Foz do Iguaçu (PR), fevereiro de 2020: página oficial da cidade foi invadida e imagem com dados do prefeito foi publicada; nota da prefeitura diz que causa foi a senha de um usuário, considerada fraca.

DESVIO DE RECURSOS

Por causa da infecção de máquinas com vírus, contas bancárias são afetadas.

Câmara Municipal de Cachoeiro de Itapemirim (ES), fevereiro de 2022: cerca de R$ 200 mil foram desviados — e estornados pela Caixa Econômica Federal.
Prefeitura de Euclides da Cunha Paulista (SP), dezembro de 2021: mais de R$ 500 mil foram desviados das contas dos setores de convênio da educação, da saúde e do Tesouro Municipal.
Prefeitura de Matelândia (PR), dezembro de 2021: valores que ultrapassam R$ 410 mil foram retirados de várias contas da cidade e instituições bancárias se negaram a estornar; prefeitura cobra na justiça.
Prefeitura de Jauru (MT), agosto de 2021: R$ 370 mil foram desviados de contas da cidade, sem mais explicações sobre o método.
Prefeitura de Santa Cruz do Xingu (MT), julho de 2021: seis transferências atribuídas a hackers desviaram, no total, R$ 113 mil das contas da prefeitura.
Prefeitura de Jaboticatubas (MG), junho de 2021: R$ 2,9 milhões de reais desapareceram das contas da cidade em menos de 1 hora, que foram desviados em 42 transferências.
Prefeitura de Campinas (SP), junho de 2021: ataque causou desvio de R$ 7,4 milhões da conta que a prefeitura usa para receber pagamentos do IPTU; polícia trabalha com a hipótese de ataque a computadores da Secretaria de Finanças.
Prefeitura de Virgolândia (MG), maio de 2021: invasores retiraram R$ 152 mil dos cofres municipais depois que um arquivo infectado por vírus foi aberto por uma servidora que trabalha no Tesouro, acreditando se tratar de uma nota fiscal; gestão diz que conseguiu recuperar a soma.

Prefeitura de Piratini (RS), abril de 2021: invasores fizeram 12 transações nas contas da Prefeitura no valor de mais de R$ 500 mil.
Santa Rosa de Lima (SC), abril de 2021: invasores retiraram recursos de quatro contas da cidade, somando R$ 300 mil. Valor foi recuperado.
Prefeitura de Imbuia (SC), março de 2021: ataque desviou quase R$ 2 milhões por meio de Pix, um tipo de transação que sequer era adotado pela gestão. O valor representa dois meses de toda a arrecadação do município, que tem pouco mais de 6 mil habitantes.

SEM INFORMAÇÕES SOBRE MÉTODO

As notícias são tão superficiais que não permitem identificar o tipo de ataque.

Prefeitura de Curitiba (PR), março de 2022: ataque cibernético "travou" o sistema de transporte público da cidade, como recargas de bilhete; quase 60% das linhas urbanas têm pagamento exclusivo por cartão de transporte.
Prefeitura de São Sebastião do Caí (RS), fevereiro de 2022: ataque impediu o pagamento de servidores municipais — servidores da Secretaria da Fazenda trabalharam durante todo o período de carnaval para refazer os cálculos da folha, após perda de dados. Já havia ocorrido em 2019, e a prefeitura alegou ter tomado medidas como instalar "antivírus".
Prefeitura de Limeira do Oeste (MG), janeiro de 2022: a cidade levou 13 dias para recuperar as informações e refazer processos, atrasando pagamento dos funcionários.
Prefeitura de Teresina (PI), dezembro de 2021: sistemas da Prefeitura e de diversas instituições públicas saíram do ar depois de o governo do Estado ter tornado os domínios e subdomínios pi.gov.br indisponíveis como "medida preventiva" a ataques.
Prefeitura de Campo Grande (MS), dezembro de 2021: também retirou site do ar como "medida preventiva" por ataque ao Ministério da Saúde, alegando que município não foi afetado.
Prefeitura de Caicó (RN), dezembro de 2021: página da Prefeitura saiu do ar após ataque, mas gestão afirmou que dados não foram comprometidos
Prefeitura de Cáceres (MT), dezembro de 2021: sistema da Secretaria Municipal da Fazenda ficou fora do ar e impediu emissão de notas fiscais; não há informação sobre origem e motivos, mas a administração diz que está trabalhando para restabelecer e recuperar o banco de dados"
Prefeitura de Ribeirão Pires (SP), outubro de 2021: ataque levou cidade a suspender todos os atendimentos.
Prefeitura de Vitória (ES), outubro de 2021: mais de cem serviços da cidade saíram do ar e ficaram quase uma semana indisponíveis, incluindo pagamento de impostos; alunos foram orientados a não acessar sistema de ensino a distância.
Prefeitura de Macaé (RJ), junho de 2021: segundo administração da cidade, "servidores importantes foram infectados e muitos dados acabaram corrompidos, deixando a maioria dos sistemas internos indisponíveis", depois de um computador da rede ter sido infectado por malware.
Prefeitura de Águas Lindas de Goiás (GO), junho de 2021: site foi retirado do ar e serviços foram suspensos após ataque.
Prefeitura de Cassilândia (MS), maio de 2021: ataque provocou perda de dados e derrubou sistema de cobrança da prefeitura e do departamento de gestão de água, mas administração disse ter backup. Segundo a gestão, isso já vinha sendo prevenido desde que, em 2014, dados de 8 meses de trabalho foram perdidos.
Prefeitura de Campo Limpo Paulista (SP), março de 2021: ataque inseriu mensagem com nome do grupo que teria sido responsável pela invasão;

Prefeitura de Itabirito (MG), fevereiro de 2021: serviços ficaram indisponíveis após tentativa de ataque, que não foi explicado na nota divulgada pela cidade.
Prefeitura de Saquarema (RJ), fevereiro de 2021: ataque deixou sistemas da cidade fora do ar e administração afirmou que nenhum dado dos contribuintes foi vazado.
Prefeitura de Balneário Camboriú (SC), janeiro de 2021: invasão parou sistemas da prefeitura por dias, atrasando pagamento de funcionários e fornecedores. Segundo portal da região, não havia backup — e, logo após o episódio, gestão decidiu gastar R$ 1,3 milhão em soluções para salvaguardar arquivos. A administração chegou a dizer que ataque ocorreu devido à falta de atualização de computadores que utilizam Windows 10.
Prefeitura de Volta Redonda (RJ), maio de 2020: site oficial fica mais de um dia fora do ar por tentativa de invasão.
Prefeitura de Umuarama (PR), julho de 2019: prefeitura disse ter sido alvo de ataque que suspendeu o atendimento de serviços por diversos dias.Ou ataques distribuídos de negação de serviços, quando o excesso de requisições a um site acaba por derrubá-lo

Prefeitura de Cuiabá (MT), março de 2021: prefeito registrou boletim de ocorrência após alegar que o site de vacinação da cidade teria sofrido ataque que causou sobrecarga nos agendamentos.
Prefeitura de Boituva (SP), abril de 2021: sistemas de cadastro para vacinação saíram do ar após ataque de 200 mil requisições por segundo.
Prefeitura de Divinópolis (MG), fevereiro de 2021: sistema de cadastro de vacina para profissionais da saúde sofreu ataque com excesso de requisições e ficou fora do ar.
Prefeitura de Chapecó (SC), janeiro de 2021: informações são escassas mas, pela descrição, o caso se assemelha a ataque de negação de serviços, que provocou lentidão e instabilidade no site oficial da cidade.
(http://umdadoamais.com/municipios-a-deriva-sem-seguranca-digital-mais-de-300-foram-atacados-em-3-anos/#comments)

Portanto, cabe ao Município especificar requisitos de segurança relativo ao data center, uma vez que cabe a ele a escolha de uma solução que considere seguro, seguindo parâmetros universais.
Conforme dito anteriormente, a responsabilidade das informações armazenadas no banco de dados é da administração, a qual responde objetivamente pelos danos que o acesso não autorizado pode ocasionar a terceiros, por força do artigo 37, §6º, da Constituição Federal.

Nesse sentido, segue o entendimento do Tribunal de Contas do Estado de Santa Catarina:

> REPRESENTAÇÃO. EMPRESA ESTATAL. LICITAÇÃO. CONTRATAÇÃO DE PRESTAÇÃO DE SERVIÇOS ESPECIALIZADOS DE DATA CENTER E LICENCIAMENTO DO SOFTWARE VMWARE. QUESTIONAMENTO SOBRE EXIGÊNCIAS DO EDITAL IRREGULARIDADES NÃO CONFIRMADAS. IMPROCEDÊNCIA. ARQUIVAMENTO. Não confirmadas as alegações de omissões e irregularidades no edital de procedimento licitatório eletrônico, mormente ante as justificativas apresentadas pela Unidade Gestora para as opções adotadas na elaboração das regras do certame, **com intuito de promover a contratação na forma que melhor atenda às necessidades da entidade, é o caso de considerar improcedente a representação**. (TCE-SC, Acórdão 1351, 17/10/2022).

Um firewall exclusivo permite controlar o tráfego que entra e sai do sistema e definir regras de segurança que bloqueiam o tráfego mal-intencionado, evitando o acesso de invasores, roubo de informações confidenciais e interrupções no sistema. Ademais, é comum que empresas que fornecem serviços de software em nuvem ofereçam um firewall exclusivo para proteger seus sistemas contra ataques cibernéticos, o que significa que não há evidência de que a exigência de um *firewall* exclusivo dificulte a participação de qualquer empresa.

Além disso, um firewall exclusivo pode auxiliar na identificação de padrões de tráfego suspeitos e alertar as equipes de segurança da informação para que possam tomar medidas adicionais para proteger o sistema. Também é possível integrá-lo a outras ferramentas de segurança, como sistemas de detecção de intrusão, para fortalecer a defesa contra ameaças.

Portanto, repete-se que a responsabilidade das informações armazenadas no banco de dados é da administração, a qual responde objetivamente pelos danos que o acesso não autorizado pode ocasionar a terceiros, por força do artigo 37, §6º, da Constituição Federal, razão pela qual é improcedente a impugnação.

DECISÃO

Diante o exposto, julga-se improcedente a impugnação.

Vargem, 03 de Maio de 2023

Danielly Cavalli

Danielly Cavalli
Secretária de Administração e Finanças