Sábado, 28 de Novembro de 2026

Guerra cibernética: Mato Grosso está preparado?

A resposta à pergunta do título é incômoda: em parte. O Estado já está na linha de fogo. O Tribunal de Justiça parou em setembro, a Secretaria de Saúde sofreu dois ataques só em 2026 e o Detran teve dados sigilosos consultados em massa.

Ao mesmo tempo, Mato Grosso tem o que a maioria dos estados brasileiros não tem: uma solução de proteção de dados estruturada com a Thales, líder mundial no setor, já funcionando na Secretaria de Educação. A ferramenta existe. O que separa o próximo órgão atacado do próximo órgão protegido é uma decisão.

Não é exagero. O mundo vive uma escalada. Em poucos dias, o FBI revelou que hackers norte-coreanos roubaram mais de US$ 400 milhões com videochamadas falsas criadas por inteligência artificial, mirando executivos, e criminosos adulteraram um único fornecedor de software para espalhar código malicioso pelos sites de 178 organizações, entre elas CNN, BBC e Zoom.

Até falhas sem ataque mostraram o tamanho da dependência digital: uma pane da Microsoft levou o presidente do STF e do CNJ, Edson Fachin, a suspender os prazos processuais em todo o país, e outra, de telecomunicações, parou todos os voos dos Estados Unidos.

No Brasil, os ataques reais se acumulam. O Porto de Santos, maior da América Latina, foi atingido por um ransomware que derrubou seus sistemas administrativos, e criminosos do exterior exigiram pagamento.

A Caixa Vida e Previdência teve copiada a base cadastral de 7,6 milhões de clientes. O Tesouro Nacional confirmou acesso indevido a 30 mil cadastros e 4 mil chaves Pix. O Serpro admitiu um ataque "sem precedentes" ao Gov.br.

O Tribunal de Justiça de Minas Gerais investiga um incidente cibernético, a Prefeitura de Belo Horizonte teve de reemitir guias de tributos e o Inep registrou tentativas de ataque durante o Enem. Segundo levantamento citado pela BBC, cada empresa brasileira sofre em média 4 mil tentativas de ataque por semana, 76% acima da média mundial.

Em Mato Grosso, o ataque já chegou.

Em setembro, o Tribunal de Justiça teve o PJe derrubado, prazos suspensos e logins e senhas criptografadas de usuários acessados, e a Polícia Federal apura se o mesmo invasor atingiu o Tribunal de Justiça da Bahia e o Senado.

A Secretaria de Saúde sofreu dois ataques em 2026: em março, com pedido de resgate, que a pasta afirma ter superado com seus mecanismos de recuperação e sem pagamento; em novembro, um novo ataque suspendeu os sistemas de todas as unidades.

No Detran, a Justiça mandou periciar 165 mil consultas automatizadas a dados sigilosos, feitas, segundo a acusação, com a credencial de um despachante. Não é o primeiro caso: em 2025, servidores foram condenados por usar logins funcionais para inserir dados falsos no sistema e regularizar veículos clonados.

Em junho, criminosos inseriram uma ordem de pagamento falsa no sistema financeiro do Estado, barrada pelas equipes técnicas antes de chegar ao banco. E a Polícia Civil já identificou tentativa de invasão do seu sistema de consultas com credenciais vazadas.

O padrão se repete: credenciais roubadas ou com uso errado, acesso a bases de dados legíveis e o órgão descobrindo o problema depois. A partir daí, há dois desfechos possíveis. No primeiro, o criminoso sai com

dados abertos, prontos para golpes, extorsão ou venda. No segundo, sai com arquivos criptografados, que sem as chaves não servem para nada.

A pergunta depois de um ataque não é só se o invasor entrou. É se o que ele levou pode ser usado.

É aqui que entra a camada que mais falta no setor público brasileiro: a proteção do próprio dado. Firewall e antivírus tentam impedir a entrada. A criptografia parte do princípio de que, um dia, alguém vai entrar. Na prática, envolve quatro frentes.

Descobrir e classificar onde estão os dados pessoais e sensíveis. Criptografar bancos de dados, arquivos e backups. Guardar as chaves em equipamentos dedicados, os HSMs, separados dos sistemas que protegem. E controlar quem pode ver o dado aberto, registrando cada acesso. Com isso, um login roubado deixa de significar acesso automático a toda a base, e um backup copiado deixa de ser um vazamento.

Criptografia não resolve tudo. Não impede que um ataque derrube sistemas, e por isso continuam indispensáveis o backup isolado e testado, a autenticação multifator e o monitoramento contínuo. Mas muda a resposta à pergunta mais grave depois de um incidente, aquela que a LGPD obriga a levar à ANPD e aos cidadãos: os dados expostos podem ser usados contra as pessoas? Com criptografia bem implantada, a resposta tende a ser não.

Mato Grosso fez o dever de casa. Há três anos, muito antes de o tema chegar às manchetes, a MTI, empresa de tecnologia da informação do Estado, foi buscar a Thales/Imperva, gigante francesa e líder mundial em segurança de dados e criptografia, e estruturou com ela uma parceria para levar essa proteção aos órgãos estaduais.

Foi um movimento pioneiro no país: enquanto a maior parte do setor público ainda trata a proteção do dado como projeto futuro, Mato Grosso já tinha o caminho técnico e os parceiros definidos.

A primeira fase do projeto foi concluída na Secretaria de Estado de Educação (Seduc), que passou a operar com criptografia em bancos de dados, sistemas e servidores de arquivos, além de descoberta e classificação de dados sensíveis e gestão centralizada de chaves. Os demais órgãos do Estado ainda não aderiram.

O portfólio da MTI reúne soluções que cobrem todo o ciclo de proteção: prevenção, com classificação de dados, criptografia e controle de acesso; detecção, com monitoramento contínuo; e resposta e mitigação de incidentes, com contenção, recuperação e continuidade dos serviços.

A preparação, porém, só protege quem a adota. Assim como fez na Seduc, a MTI apresentou a solução aos demais órgãos do Estado. O caminho técnico está pronto, o parceiro está definido e o modelo já foi testado em ambiente real.

A partir daqui, a velocidade da proteção depende de cada gestor colocar o tema no topo das suas prioridades. E o tempo joga contra: cada mês sem essa camada é mais um mês em que os dados mais sensíveis da população seguem legíveis para quem conseguir entrar.

O modelo pode ser replicado, dentro e fora do Estado, sem começar do zero. E, em segurança da informação, continuidade também é proteção: projetos interrompidos no meio do caminho, por mudança de rumo ou de prioridade, costumam deixar exatamente as brechas que os atacantes procuram.

A pergunta, então, não é se Mato Grosso tem como se proteger. Tem. É quantos órgãos ainda vão esperar o próximo ataque para usar o que já está disponível. Saúde, Detran, Fazenda e Segurança Pública guardam alguns dos dados mais sensíveis da população. Cada um que permanece sem essa camada é um risco conhecido. E risco conhecido, depois do incidente, vira a pergunta que os órgãos de controle fazem a quem decide: por que não foi feito?

O Brasil está sob ataque. Mato Grosso tem a ferramenta em mãos. Falta estendê-la a quem mais precisa, antes que a próxima manchete seja aqui.

Oscar Soares Martins é Consultor em Cibersegurança e IA