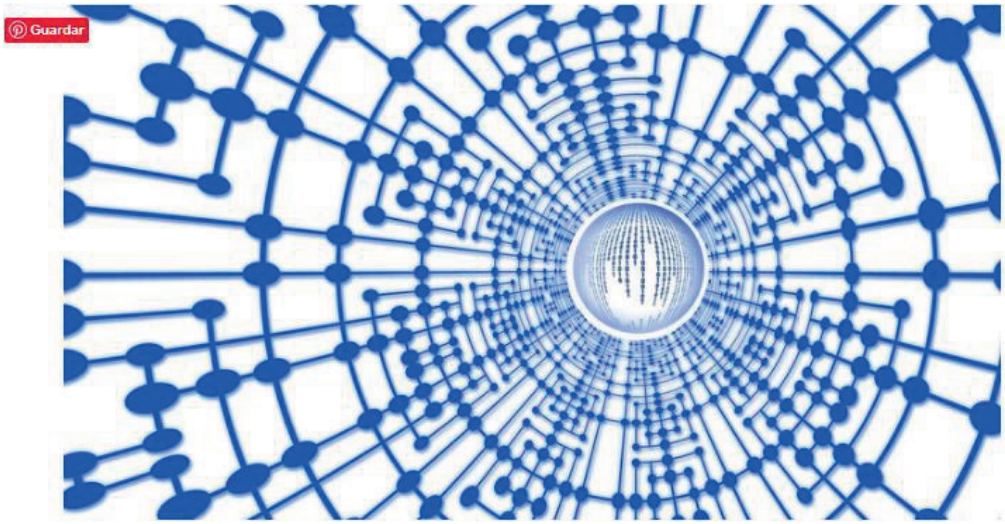
Link: https://cutt.ly/yRWsfkr



Andréia Pires · há 2 dias · 2 min para ler

# Alerta de invasores! Bancos de dados empresariais estão sob risco




Por Maria Cristina Diez, diretora comercial e de Marketing da Most Specialist Technologies

A Imperva Inc., empresa mundial de cibersegurança, revelou em setembro o que as corporações do setor de tecnologia já sabiam: quase a metade dos 27 mil bancos de dados internos analisados pela companhia ao redor do mundo está vulnerável. Nada menos que 46% delas apresentam falhas naquele que é, pelo menos na óptica administrativa, o principal ativo da empresa.

Tão grave quanto esse índice foi a identificação média de 26 falhas públicas em cada banco de dados vulnerável, em sua maioria em níveis críticos ou de alta gravidade, como descreve o relatório da Imperva. Está longe de ser motivo de comemoração, mas os bancos de dados

Link: https://cutt.ly/yRWsfkr

A realidade nua e crua é que muitas empresas mundo afora lidam com suas informações confidenciais de forma amadora. Há bancos de dados valiosos que se resumem a planilhas de Excel salvas na área de trabalho do computador, e que são acessadas diariamente. Algumas chegam a ficar simplesmente abertas. Essa exposição é um imenso outdoor convidando invasores a abrir e destruir a caixa preta da empresa. Os riscos reduzem quando esses database são alocados em nuvens, onde o nível de segurança é maior. Mas será suficiente?

A própria pesquisa da Imperva mostra que não. Um dos principais pontos de falhas dos sistemas, os chamados SPOFs na sigla em inglês, está na administração e controle dos bancos de dados. Há casos em que as fragilidades estão sem correção há pelo menos três anos. Nessas circunstâncias, 56% estão sob grave risco. Mesmo em situações em que há um firewall corporativo como barreira de proteção, a atualização permanente é essencial para manter um nível de segurança adequado.

O grande desafio hoje da TI nos procedimentos para proteção de dados é a necessidade de implementar multi-estratégias para se cercar dos malwares ou de ataques diretos de crackers, focando em soluções que vão desde a etapa de autenticação, passando pela configuração dos bancos e o uso de reforço externo para potencializar as barreiras de defesa. Em épocas anteriores, essas ações eram concentradas nos endpoints, como se fossem suficientemente eficazes na luta contra os invasores. Mas eles vêm encontrando caminhos alternativos para driblar a defesa e se infiltrar nos sistemas, como atesta o trabalho realizado pela Imperva.

A adoção de mais obstáculos é o único caminho para dificultar e desestimular as invasões. Na contramão dos números expressivos da superexposição de dados empresariais, temos exemplos positivos, como as instituições bancárias, cujos acessos aos bancos de dados estão atrelados à inteligência artificial. Pode parecer um sistema caro, pressuposição que precisa ser desmitificada. Mas o suporte de recursos de IA é o que existe de mais inovador em favor do que podemos considerar o coração da empresa. É necessário apenas usar o cérebro.

Banco de dados | tecnologia da informação | cibersegurança