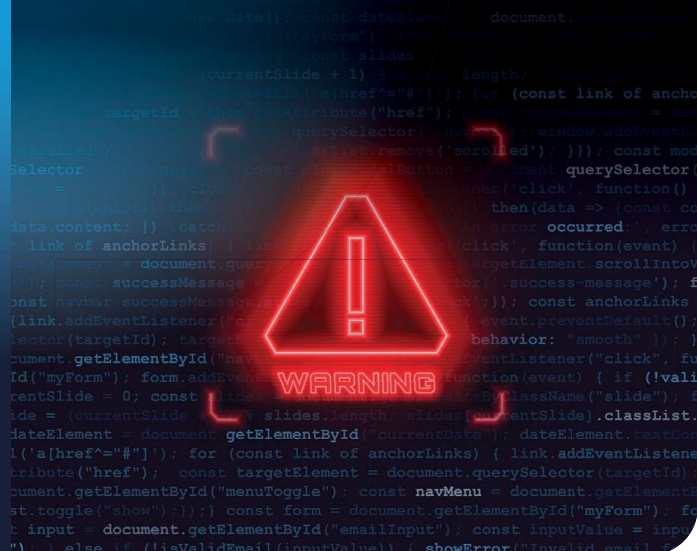


A Violação da Oracle Cloud Revelou uma Verdade Dura: A Infraestrutura de Nuvem Pública é uma Superfície de Ataque de IA Crescente para Cibercriminosos



Resumo

No início de 2025, um threat actor identificado como **Rose87168** reivindicou a responsabilidade por uma grande violação da **Oracle Cloud Infrastructure (OCI)**, alegando ter comprometido mais de **6 milhões de registros** em aproximadamente **140.000 inquilinos (tenants)**. Embora a Oracle não tenha confirmado oficialmente o incidente, pesquisadores acreditam que o atacante explorou uma **vulnerabilidade de dia zero (zero-day)** ou uma **configuração inadequada na camada de autenticação OAuth2**, obtendo acesso não autorizado a informações altamente sensíveis, como credenciais de **Single Sign-On (SSO)**, senhas **LDAP**, chaves **OAuth** e dados específicos de cada inquilino.

Este incidente vai além de um evento isolado de segurança—é um **alerta urgente** para todas as organizações que dependem de plataformas de nuvem pública para hospedar seus dados **críticos** ou de **alto valor**. Ele expõe um risco sistêmico na arquitetura compartilhada dessas plataformas: mesmo quando as organizações seguem as melhores práticas—como políticas rigorosas de **IAM (Identity and Access Management)**, acesso de **privilegio mínimo** e monitoramento contínuo—elas permanecem vulneráveis **se o provedor de nuvem cometer um único erro arquitetural ou operacional**.

As vulnerabilidades de dia zero são, por definição, **imunes à diligência do provedor**. Pior ainda, os **ataques entre inquilinos (cross-tenant)**, nos quais uma violação em um inquilino se propaga para outros, podem ocorrer quando o plano de controle (control plane) da nuvem é comprometido. Embora raros, incidentes como o da Oracle ilustram que **ameaças potencializadas pela IA** são cada vez mais capazes de identificar e explorar tais vulnerabilidades em escala.

Este documento analisa **como e por que, em nosso mundo de IA, a nuvem pública tornou-se o principal vetor de ataque para cibercriminosos**, como violações entre inquilinos podem acontecer mesmo com controles internos robustos, e **por que dados críticos ou de alto valor devem ser isolados de ambientes de nuvem pública** para mitigar esses riscos emergentes.

O Manual do Cibercrime com IA: Por Que a Nuvem Pública é o Campo Ideal

O surgimento da inteligência artificial (IA) no cibercrime aumentou drasticamente a frequência, a sofisticação e o sucesso dos ataques a ambientes de nuvem pública. Essas plataformas — embora ofereçam escala e conveniência — também representam os alvos centralizados de maior valor para agentes de ameaça. As ferramentas de IA agora permitem que os atacantes:

- *Escaneiem rapidamente vulnerabilidades (como falhas de dia zero),*
- *Criem iscas de phishing altamente direcionadas,*
- *Automatizem tentativas de intrusão, e*
- *Ataquem operações de nuvem para facilitar a contaminação entre inquilinos (cross-tenant).*

O resultado é que a infraestrutura de nuvem pública está mais exposta do que nunca.



Cibercriminosos com IA estão mirando cada vez mais as plataformas de nuvem pública porque elas combinam quatro qualidades atrativas:

| Fator | Por que atrai os atacantes |
|-------------------------------------|---|
| Superfície de Ataque Massiva | As plataformas, sempre ativas e voltadas para a internet, apresentam inúmeros pontos de entrada prontos para exploração, como APIs configuradas incorretamente, portas abertas e serviços de metadados expostos. Ferramentas de IA podem escanear, analisar e atacar milhares desses ambientes simultaneamente, automatizando a descoberta e a exploração de brechas em escala. |
| Concentração de dados de alto valor | As nuvens públicas hospedam bilhões de registros de alto valor dos setores jurídico, financeiro e de saúde governamentais e de infraestrutura crítica. Os clientes estão dispostos a pagar os resgates mais altos e mais rápidos por dados de alto valor. |
| Infraestrutura Multi-inquilino | As nuvens públicas compartilham o mesmo hardware, as mesmas plataformas de virtualização e as mesmas ferramentas de gerenciamento consoles em vários inquilinos. Uma infraestrutura compartilhada significa que os atacantes podem explorar configurações incorretas, falhas em APIs ou vulnerabilidades de dia zero no hipervisor para se mover lateralmente entre contas especialmente na presença de uma falha no plano de controle. |
| Alto ROI para os atacantes | Uma vez dentro da infraestrutura de um provedor de nuvem, os atacantes obtêm acesso a quantidades massivas de dados entre centenas ou milhares de vítimas simultaneamente — maximizando o potencial de lucro. Para ransomware, roubo de dados ou revenda de credenciais. Um único ataque bem-sucedido pode sustentar uma operação cibercriminal por meses. |

Como a IA Está Atacando a Nuvem Pública

A IA acelerou dramaticamente a forma como os cibercriminosos descobrem e exploram vulnerabilidades e evitam detecção na nuvem pública. As vulnerabilidades mais perigosas são as de dia zero (zero-day). Trata-se de uma falha em software ou hardware que é desconhecida pelo fabricante no momento em que é explorada. Por não haver correção (patch) ou defesa disponível, ela permite que os atacantes:

- Explorar sistemas antes mesmo de sua detecção.
- Direcionar planos de controle, APIs ou hipervisores para obter acesso privilegiado.
- Obter acesso entre inquilinos (cross-tenant), manipular, criptografar ou excluir dados em um ambiente de nuvem.

No caso da violação da Oracle, acredita-se que uma vulnerabilidade de dia zero no protocolo OAuth2 permitiu acesso não autenticado entre serviços — supostamente comprometendo milhões de registros em 140.000 inquilinos.

Técnicas Conduzidas por IA para Violar a Nuvem:

Independentemente de ser implantado com **Proxmox VE**, **Scale Computing**, **VMware** ou **Hyper-V**, o **Nexsan Unity** oferece a mesma experiência segura e de alto desempenho em armazenamento:

- **Análise de Código Automatizada:** Varredura do código-fonte em busca de falhas previamente desconhecidas e sem correção disponível (zero-day). A IA aprende padrões que indicam fraquezas na lógica, no tratamento de entradas (input handling) e no gerenciamento de memória, aplicando esse conhecimento para escanear novas bases de código na velocidade da máquina.
- **Fuzzing Generativo com IA:** "Fuzzing" é o processo de enviar entradas malformadas ou inesperadas a um software para provocar uma falha (crash) ou comportamento anômalo. Este processo pode encontrar bugs que podem se tornar vulnerabilidades de dia zero (zero-days). A IA aumenta massivamente a eficiência e a taxa de sucesso na descoberta de bugs exploráveis.
- **Reconhecimento Automatizado:** Dois alvos principais: Varredura de buckets S3 abertos, chaves de acesso configuradas incorretamente ou funções do IAM (Identity and Access Management) com permissões excessivas, tanto no provedor de nuvem quanto nos ambientes dos inquilinos. Varredura de vulnerabilidades conhecidas que a equipe de nuvem ou um inquilino não corrigiu com os patches de segurança.
- **Monitoramento de Lançamentos de Patches e Diffs de Código:** Ao analisar patches e alterações de código "antes/depois", a IA pode fazer engenharia reversa de vulnerabilidades — e criar exploits armazenados antes que os patches sejam totalmente implantados ("ataques de N-day"). Isso torna os ataques de N-day (contra falhas recém-divulgadas) mais perigosos: a IA pode transformá-los em exploits funcionais em poucas horas.
- **Phishing Sofisticado:** A IA cria páginas de login convincentes e imita a comunicação de executivos para roubar credenciais.
- **Evacuação Adaptativa:** Malware conduzido por IA altera sua assinatura e comportamento em tempo real para evitar detecção.

O Problema Central: A Nuvem Pressupõe Confiança no Provedor

A segurança da nuvem pública repousa sobre o modelo de responsabilidade compartilhada:

- Você protege as suas cargas de trabalho (workloads)
- O provedor protege a infraestrutura.

Porém, quando a infraestrutura do provedor é o vetor de ataque — como suspeito na violação da Oracle — **o modelo entra em colapso**.

Não importa o quão bem uma organização proteja seu IAM, sua criptografia e sua segurança de rede, ela permanece exposta se a camada de identidade, o plano de controle ou o hipervisor do provedor de nuvem forem violados.

Isso não é teórico. A violação da Oracle se junta a uma lista crescente de grandes incidentes relacionados à nuvem — evidenciando que a confiança nas camadas invisíveis de um provedor pode se tornar um ponto único de falha catastrófica..



Uma Divisão Estratégica: O que Pertence na Nuvem — e o que Não Pertence

A melhor maneira de reduzir o risco corporativo frente a cibercriminosos é decidir quais dados colocar na nuvem pública e quais dados manter em seu data center local (on-premise). É importante observar que, claro, mesmo os dados em seu data center privado estão sujeitos a um ciberataque. No entanto, **sua capacidade de controlar os vetores de ataque está 100% em suas mãos**.

As plataformas de nuvem pública são ideais para:

- Hospedagem de sites
- Ambientes de desenvolvimento
- Plataformas de colaboração
- Projetos analíticos de curto prazo
- Dados não sensíveis ou publicamente disponíveis

Essas cargas de trabalho se beneficiam da escalabilidade e da eficiência de custos da nuvem. No entanto, **elas não exigem integridade de dados à prova de falhas, imutabilidade ou trilhas de auditoria de nível jurídico**.

Dados de Alto Valor, No Entanto, Exigem Mais:

| Atributos de Dados de Alto Valor | Por que a Nuvem Pública é Insuficiente |
|--|--|
| Requisitos Regulatórios ou Legais | Os provedores de nuvem pública podem não oferecer armazenamento WORM certificado, criptografia ou sistema de registros em blockchain |
| Propriedade Intelectual Sensível (PI/IP) ou Dados Pessoais (PII) | A infraestrutura compartilhada aumenta o risco de exposição não autorizada. |
| Retenção e Descarte de Longo Prazo | A nuvem pública carece de exclusão criptográfica verdadeira e de backup com air-gap, e pode não oferecer imposição robusta de políticas de retenção. |
| Requisito de Cadeia de Custódia | As vulnerabilidades no plano de controle quebram a integridade da evidência digital. Sem capacidade de saber se um arquivo foi acessado, mas não alterado. |

Melhores Práticas: Protegendo Dados de Alto

Valor Fora da Nuvem Pública

As organizações precisam seguir todas as melhores práticas para proteger todos os seus dados e sua empresa contra cibercriminosos. Essas práticas incluem detecção e resposta em endpoints (EDR), software antimalware, firewalls e a manutenção de patches de software atualizados. Além destas, as organizações que gerenciam dados críticos, sensíveis ou regulamentados (Dados de Alto Valor) devem adotar a seguinte estratégia:

- **Mova os Dados de Alto Valor para Armazenamento com Air-Gap e Imutável.** Utilize soluções on-premise ou híbridas, como o Nexsan Assureon, que impõem a imutabilidade de arquivos, air-gap e registros de auditoria baseados em blockchain.
- **Imponha a Retenção com Verificação de Tempo de Terceiros.** Utilize uma solução de armazenamento que integre, aceite e imponha regras de retenção em nível de arquivo na camada de armazenamento, diretamente de seu sistema de gerenciamento de documentos. Previna a falsificação de arquivos (archive spoofing) utilizando autoridades de tempo independentes de terceiros para validação de timestamp e controles de descarte de dados.
- **Adote uma Arquitetura de Confiança Zero (Zero Trust Architecture).** As nuvens públicas raramente implementam uma segmentação de rede verdadeira na camada de armazenamento. O Assureon oferece uma superfície de ataque com zero executáveis, isolada da sua rede corporativa.
- **Empregue Criptografia de Arquivo Único.** Em vez de criptografar volumes inteiros, utilize chaves únicas por arquivo para máxima privacidade e para permitir a exclusão criptográfica (crítico para o GDPR e mandatos de descarte de dados).
- **Imutabilidade, Versionamento e Restauração Rápida.** Quando o versionamento de arquivos é adicionado ao armazenamento imutável, o arquivo criptografado por ransomware não consegue sobrescrever o arquivo original. Isso permite uma recuperação completa de um ataque de ransomware através da restauração da versão original. No Assureon, isso pode ser feito pela restauração instantânea de atalhos virtuais para os arquivos originais.

Assureon High Value Data

Solução de alta segurança e propósito específico, projetada para proteger evidências digitais em um mundo impulsionado pela IA.



Palavra Final: A Oracle é um Caso de Estudo — Não uma Exceção

O incidente da Oracle Cloud é um lembrete contundente de que o elo mais fraco na nuvem pode não ser você — pode ser o provedor. Contudo, o fato de uma violação ter ocorrido demonstra que mesmo os provedores de nuvem maiores e mais maduros são vulneráveis a falhas de dia zero (zero-day) e a brechas no plano de controle, o que pode resultar na exposição de dados entre inquilinos — um risco particularmente perigoso em um ambiente multi-inquilino, onde os atacantes podem "pular" do ambiente de um cliente para o de outro. **Quando** — e não **se** — isso acontecer, o erro deles se torna a sua crise.

A nuvem continua sendo uma ferramenta poderosa — mas apenas para as cargas de trabalho adequadas. Sua arquitetura, se não for complementada com imutabilidade, air-gapping e controle de acesso granular, deixa as organizações vulneráveis a ransomware, roubo de dados e falhas de conformidade.

É hora das empresas reavaliarem quais dados realmente pertencem à nuvem — e quais dados precisam de proteção em nível de fortaleza. Quando se trata de proteger os ativos digitais mais críticos da sua organização, **o lugar mais seguro está fora do raio de explosão.**

Se a sua organização está armazenando dados de alto valor — jurídicos, regulamentados, probatórios ou insubstituíveis — **em plataformas de nuvem pública**, elimine o risco compartilhado que você pode não conseguir controlar ou conter. Faça isso **transferindo esses Dados de Alto Valor para um appliance de armazenamento seguro de dados Assureon.**

SOBRE NEXSAN

Nexsan® é um líder global em capacitar seus clientes a armazenar, proteger e gerenciar dados com segurança. Fundada em 1999, a Nexsan conquistou a reputação de oferecer o armazenamento mais confiável, seguro e econômico, mantendo sempre a agilidade para entregar continuamente soluções de armazenamento e gerenciamento de dados desenvolvidas sob medida, que atendem aos requisitos complexos e em constante mudança de TI, negócios e orçamento. A tecnologia patenteadada da Nexsan é ideal para uma variedade de casos de uso, incluindo backup e recuperação, distribuição e streaming de conteúdo, dados de laboratório científico, virtualização, dados probatórios, vigilância por vídeo digital, conformidade regulatória e registros de saúde. Para mais informações, visit www.nexsan.com.