Pensamento Autônomo

Longitude
A Financial Times Company

Segurança e risco de TI: a automação inteligente reduz a sobrecarga

ARTIGO

ORACLE

Sumário

Introdução

A solução para a questão da segurança

A automação é a chave para a segurança

A autonomia é o futuro da segurança de dados

ORACLE

Introdução

É hora de pensar de forma diferente sobre a segurança de TI.

O Fórum Econômico Mundial reconhece a crescente ameaça à cibersegurança e a classifica, junto com as condições climáticas extremas e os desastres naturais, como um dos cinco principais riscos atualmente enfrentados no mundo, com "grande incidência de fraude e roubo de dados" em quinto lugar na lista e "ciberataques em larga escala" em quarto. Além disso, a Cybersecurity Ventures considera o crime cibernético como a maior ameaça para todas as empresas do mundo e prevê que, até 2021, isso gerará um custo de US$ 6 trilhões ao ano, o dobro do custo em 2015.

"Existem vários vetores de ameaça, internos e externos", diz Greg Jensen, diretor sênior de segurança em nuvem da Oracle. "E é impossível lidar manualmente com todas essas ameaças."

É impossível também contratar e treinar pessoal suficiente para lidar com essas vulnerabilidades crescentes de segurança. De acordo com a Enterprise Strategy Group, mais da metade dos tomadores de decisões de TI e de negócios relatam uma escassez problemática de qualificação em segurança hoje.

Uma pesquisa da Oracle contribui para essa conclusão, citando a falta de capacitação e de pessoal qualificado como o segundo maior desafio da cibersegurança. E a previsão é de que essa lacuna de conhecimento piore ainda mais. Até 2021, a Cybersecurity Ventures prevê que serão abertos mais de 3,5 milhões de empregos em cibersegurança.

> *"Existem vários vetores de ameaça, internos e externos."*
>
> **Greg Jensen, diretor sênior de segurança em nuvem da Oracle**

ORACLE

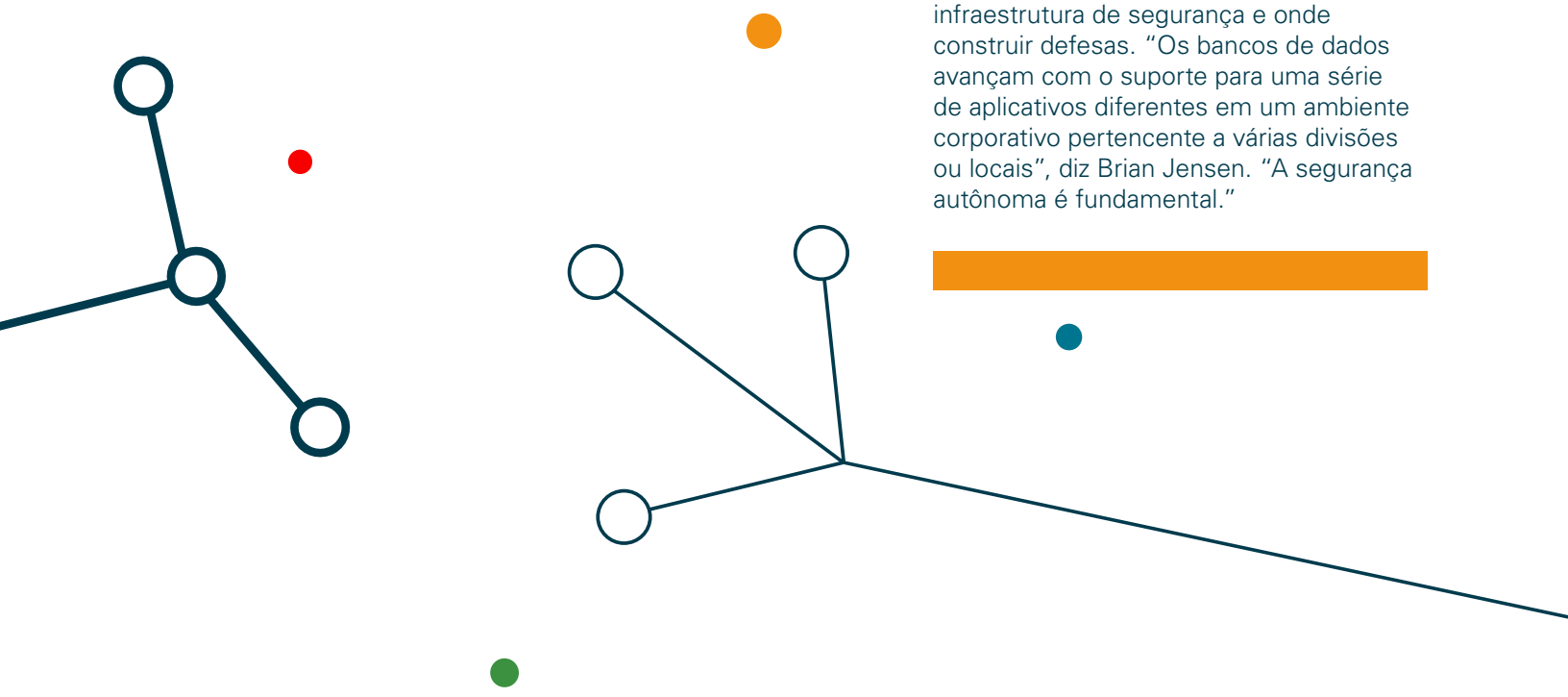
> *"Com o avanço de bancos de dados com suporte para uma série de aplicativos diferentes em um ambiente corporativo pertencente a várias divisões ou locais, a segurança autônoma é fundamental."*
>
> **Brian Jensen, líder de consultoria de vendas de risco de aplicativos da KPMG**

Mesmo que existissem profissionais suficientes com treinamento em segurança, essa não seria a solução para as crescentes ameaças cada vez mais comuns e complexas. "Não conseguimos fazer isso apenas com o fator humano", diz Greg Jensen. "Não podemos capacitar ou contratar um número suficiente de pessoas para sair desse problema."

De um lado, há um cenário de ameaça crescente; de outro, há a evolução da infraestrutura interna de TI das organizações. No passado, os ativos e os sistemas de TI ficavam em um único local, protegidos por fortalezas, como um castelo cercado por muralhas.

"Qualquer coisa dentro da muralha do castelo era protegida pela mesma infraestrutura", diz Brian Jensen, líder de consultoria de vendas de risco de aplicativos Oracle da KPMG. "Agora não há nenhum castelo — cada aplicativo e banco de dados associado tem que ser independente e se proteger por conta própria."

A automação inteligente está mudando a forma como pensamos sobre a infraestrutura de segurança e onde construir defesas. "Os bancos de dados avançam com o suporte para uma série de aplicativos diferentes em um ambiente corporativo pertencente a várias divisões ou locais", diz Brian Jensen. "A segurança autônoma é fundamental."



ORACLE

A solução para a questão da segurança

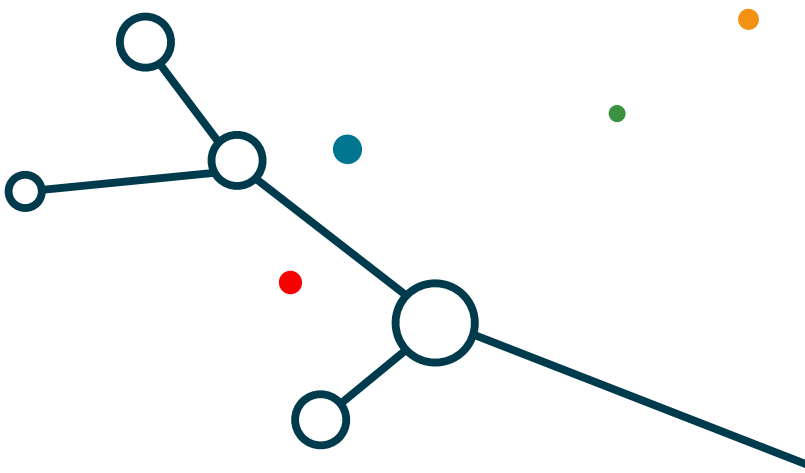
Existem vários desafios para a proteção dos dados e aplicativos das organizações, e não menos importante é o grande número de eventos relacionados à segurança. "As organizações enfrentam 3,2 bilhões de eventos por mês", diz Greg Jensen. "Atualmente, dos 3,2 bilhões, em média apenas 31 são ameaças reais à segurança." É muito tumulto para se lidar, e analisar tantos registros é humanamente impossível.

O segundo desafio de segurança é o acompanhamento dos patches. Só a Microsoft libera dezenas de patches todos os meses. Se levarmos em conta os patches de todos os outros fornecedores, não é nenhuma surpresa que os profissionais de TI tenham dificuldades para acompanhar. Não é apenas o volume de patches que causa atrasos na atualização dos sistemas; as empresas têm várias razões diferentes para não implantar patches de segurança, inclusive o fato de que muitas delas possuem centenas e até mesmo milhares de bancos de dados. A execução de um patch pode demorar milhares de horas, muitas vezes exigindo um tempo de inatividade ou a interrupção dos negócios.

"Há questões operacionais válidas pelas quais, às vezes, as organizações não aplicam um patch tão rápido quanto deveriam quando descobrem uma vulnerabilidade para a qual há um patch disponível", afirma Doug Cahill, analista sênior e diretor de grupo da Enterprise Strategy Group. "Às vezes, a aplicação de um patch requer a reinicialização do sistema, que pode afetar um SLA [acordo de nível de serviço]; outras vezes, a empresa ainda não suporta a nova versão para a qual o sistema operacional será atualizado pelo patch, ou o patch pode afetar o desempenho do sistema, e isso afetaria o tempo de resposta do SLA."

A computação em nuvem é o terceiro desafio com o qual as organizações estão lidando. O próprio elemento do modelo em nuvem que traz valor aos usuários — o fato de ser remoto e distribuído — causa problemas administrativos que afetam a segurança. "A TI tornou-se cada vez mais descentralizada", diz Cahill. "As unidades de negócios estão tomando suas próprias decisões de TI, incluindo o desenvolvimento e a entrega de seus próprios aplicativos."

Isso significa que há pouca ou nenhuma supervisão de segurança para esses aplicativos em nuvem, e as organizações podem não saber quais aplicativos estão sendo executados e onde estão todos os seus dados confidenciais. Isso é um grande problema. Quase todos os entrevistados (93%) no Relatório de Ameaças à Nuvem da Oracle e KPMG afirmam que lidam com o uso de aplicativos em nuvem por invasores. Além disso, um quarto deles cita o uso não autorizado de serviços em nuvem como seu maior desafio de cibersegurança hoje.



ORACLE

A automação é a chave para a segurança

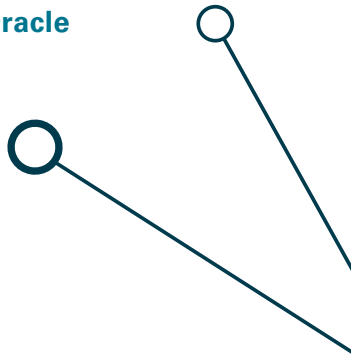
As organizações podem implantar usuários, aplicativos, dispositivos e infraestrutura com uma rapidez nunca vista antes. Ao longo de toda essa atividade, os profissionais de segurança têm dois objetivos principais: remover os processos manuais propensos a erros e detectar e responder em tempo real às ameaças emergentes. A automação inteligente permite que eles façam as duas coisas.

A detecção automatizada identifica vulnerabilidades e ameaças em tempo real, permitindo uma resposta rápida para reduzir os ataques cibernéticos internos e externos. "Os CISOs medem o tempo médio de detecção e o tempo médio de resposta", diz Greg Jensen, da Oracle. "O machine learning e a inteligência artificial reduzem os falsos positivos e os falsos negativos e encontram as ameaças reais, além de reduzir o tempo médio de resposta."

A automação inteligente também gerencia os patches de segurança, economizando tempo e recursos humanos. Isso é fundamental para reduzir vulnerabilidades de dia zero antes que elas sejam exploradas. Como reconhecem o valor da aplicação de patches, a maioria dos entrevistados no Relatório de Ameaças à Nuvem da Oracle e KPMG disse que implementou (43%) ou pretende implementar (46%) o gerenciamento automatizado de patches nos próximos dois anos.

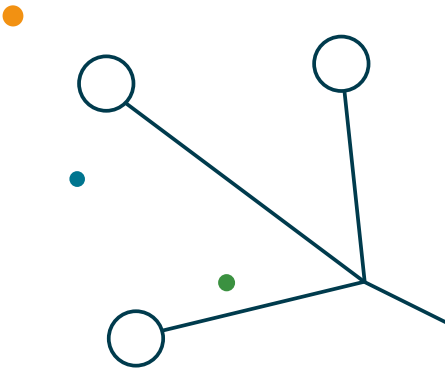
"O machine learning e a inteligência artificial reduzem os falsos positivos e os falsos negativos e encontram as ameaças reais, além de reduzir o tempo médio de resposta."

Greg Jensen, diretor sênior de segurança em nuvem da Oracle



ORACLE

A autonomia é o futuro da segurança de dados



Sempre haverá novas ameaças à segurança — à medida que TI evolui, os maus atores procuram explorar vulnerabilidades e riscos. Para fazer o acompanhamento, a tecnologia autônoma deve ser uma parte fundamental do manual de segurança das organizações. Essa é a única maneira de reduzir a sobrecarga operacional de corrigir vulnerabilidades conhecidas e diminuir o tempo para identificar e atenuar explorações conhecidas e desconhecidas.

"Vivemos em uma economia dominada por aplicativos, em que interagimos com eles tanto na vida pessoal como na profissional todos os dias", diz Cahill, da ESG. "Isso cria uma superfície de ataque que cresce continuamente — novas vulnerabilidades estão sendo introduzidas o tempo todo. As organizações precisam estar em um ciclo de repetição infinita para descobrir os riscos antes que eles possam ser explorados. A segurança autônoma ajuda a fechar essa janela de exposição."

À medida que as unidades de negócios tomam suas próprias decisões de TI e fazem seus próprios aplicativos e entregas, aumenta a descentralização de TI dentro da empresa. É por esse motivo que o futuro de TI são os aplicativos, que devem trabalhar todos juntos, mesmo quando sua infraestrutura subjacente for diferente e eles não forem necessariamente protegidos pelos mesmos mecanismos.

Para proteger a empresa e seus ativos de forma eficaz, a equipe de segurança deve ser composta pelos tomadores de decisões e os provedores internos — um conselho que orienta a direção de TI dentro da organização. Isso implica o uso da automação inteligente para proteger os ativos, onde quer que eles sejam implantados.

"Os aspectos positivos associados a esse novo mundo automatizado são incríveis", diz Brian Jensen, da KPMG. "Nossa economia empresarial nos EUA será muito mais eficiente por causa disso. No entanto, temos que gerenciar o risco de forma intencional, observar a realidade do risco e tomar as medidas adequadas para atenuá-lo. Não podemos esquecer que estamos aqui para capacitar e proteger."

> *"Os aspectos positivos associados a esse novo mundo automatizado são incríveis."*
>
> **Brian Jensen, líder de consultoria de vendas de vendas de risco de aplicativos da KPMG**

ORACLE

Entrevistados

Greg Jensen, diretor sênior de segurança em nuvem da Oracle

Doug Cahill, analista sênior e diretor de grupo da Enterprise Strategy Group

Brian Jensen, líder de consultoria de vendas de risco de aplicativos da KPMG

Fontes

Relatório de Ameaças à Nuvem Oracle/KPMG 2019

Relatório de Trabalhos de Cibersegurança 2018-2021,
Cybersecurity Ventures

Esses são os maiores riscos enfrentados no mundo em 2019,
Fórum Econômico Mundial

Pesquisa de Intenções de Gastos em Tecnologia 2019,
Enterprise Strategy Group

Relatório Anual Oficial de Crimes Cibernéticos 2019,
Cybersecurity Ventures

Experimente a Oracle Cloud gratuitamente

cloud.oracle.com/tryit

Longitude
A Financial Times Company

ORACLE