

# Desvendando a economia dos invasores cibernéticos: o risco oferecido por terceiros

Por que a resiliência cibernética exige uma estratégia que priorize a identidade ao garantir o acesso de terceiros.

US\$ **9,5**  
TRILHÕES

Custos previstos associados ao cibercrime em 2024<sup>1</sup>

Se fosse medido como um país, o cibercrime ficaria em terceiro lugar, atrás dos EUA e da China

Mais lucrativo do que o comércio global de todas as principais drogas ilícitas juntas

**63%**

das organizações não têm visibilidade do acesso concedido a não-funcionários<sup>2</sup>

**54%**

das organizações já enfrentaram algum problema de segurança devido a um não-funcionário com direitos de acesso inadequados.<sup>3</sup>

**59%**

das organizações já tiveram uma violação de dados causada por terceiros.<sup>4</sup>

## A cadeia de ataques começa aqui

O gerenciamento de acesso não é suficiente porque os autores das ameaças roubam credenciais por meio de:

- ▶ Preenchimento de credenciais
- ▶ Malware de registro de digitação
- ▶ Phishing
- ▶ Engenharia social



**Invasor interno**



**Invasor externo**

41% das organizações que sofreram um impacto material de um ataque cibernético disseram que ele se originou de terceiros.<sup>6</sup>

Prestadores de serviço

Parceiros da cadeia de suprimentos

Fornecedores

Afiliações

Cada vez mais empresas utilizam não-funcionários de terceiros em suas atividades.

Apesar de não serem funcionários efetivos, esses trabalhadores têm acesso aos ativos mais valiosos da sua organização.

97% das organizações fornecem acesso a não-funcionários de terceiros.<sup>5</sup>



Apps

001011  
110010  
010101

Dados



DevOps



IaaS/PaaS



No local



SaaS

Contas privilegiadas

Autores de ameaças têm como alvo não-funcionários devido a falhas nos protocolos de segurança de empresas terceirizadas, níveis mais baixos de treinamento nessa área e permissões de acesso que são controladas e monitoradas com menos rigor.

Apenas 13% das organizações monitoram continuamente o risco de segurança de seus terceiros.<sup>7</sup>

Violação de dados

Ransomware

Interrupção do serviço

**US\$ 4,29 milhões**

custo médio de uma violação de dados causada por terceiros.<sup>8</sup>



Garantir a segurança de terceiros é fundamental para proteger toda a rede de alcance de sua organização. Veja como ajudamos o Absa Bank.

**12.000**

não-funcionários capacitados com identidades seguras.

**15**

dias a menos no tempo de integração para garantir acesso mais rápido a terceiros.

**US\$300**

economia por identidade integrada de não-funcionário.

[Leia a história](#)