SailPoint

공격자 경제 분석: 서드파티 위험의 역할

사이버 복원력이 서드파티 액세스를 보호하기 위해 아이덴티티 우선 전략을 요구하는 이유

$9.5조

2024년 사이버 범죄 관련 예상 비용[1]

사이버 범죄의 규모를 국가 GDP와 비교하면, 미국과 중국에 이어 세계 3위에 해당합니다.

이는 전 세계 주요 불법 약물 밀매를 모두 합한 것보다 수익성이 더 큽니다.

63%

비직원에게 제공되는 액세스를 파악하고 있지 못하는 기업의 비율[2]

54%

부적절한 액세스 권한을 보유한 비직원으로 인해 보안 문제를 겪은 기업의 비율[3]

59%

서드파티로 인한 데이터 침해를 경험한 기업의 비율[4]

공격 사슬의 시작 지점

위협 행위자들은 다음 방식으로 인증 정보를 도용하므로 액세스 관리에는 한계가 있습니다.

- 크레덴셜 스터핑
- 키 로깅 멀웨어
- 피싱
- 소셜 엔지니어링

내부 공격자

외부 공격자

사이버 공격으로 인해 상당한 피해를 입은 기업의 **41%**가 공격이 서드파티에서 시작되었다고 말했습니다.[6]

도급업체 | **공급망 파트너** | **공급업체** | **계열사**

점점 더 많은 회사에서 서드파티 비직원을 활용하여 업무를 처리하고 있습니다.

이들 비직원은 직원은 아님에도 불구하고 기업의 가장 중요한 자산에 액세스할 수 있습니다.

기업의 **97%**가 서드파티 비직원에게 액세스를 제공합니다.[5]

앱 | 데이터 | DevOps | IaaS/PaaS | 온프레미스 | SaaS

권한을 보유한 계정

위협 행위자는 서드파티 보안 프로토콜의 격차, 낮은 수준의 보안 교육, 덜 엄격하게 통제되고 모니터링되는 액세스 권한을 이용해 비직원을 표적으로 삼습니다.

단 **13%**의 기업만이 서드파티의 보안 위험을 지속적으로 모니터링합니다.[7]

데이터 유출 | **랜섬웨어** | **서비스 장애**

$429만

서드파티 데이터 유출의 평균 비용[8]

absa

서드파티 보안을 보장하는 것은 기업의 확장된 네트워크를 보호하는 데 가장 중요합니다. SailPoint에서 Absa Bank를 지원한 방식은 다음과 같습니다.

12,000

보안 아이덴티티 권한을 부여받은 비직원 수

15

더 빠른 서드파티 액세스를 위한 온보딩 단축 일수

$300

온보딩한 비직원 아이덴티티 당 절감 금액

자세한 내용

SailPoint

1. eSentire
2. Imprivata
3. SailPoint
4. RiskRecon
5. SailPoint
6. World Economic Forum
7. Panorays
8. IBM