CLOUDFLARE

새로운 보안 환경 살펴보기: 대한민국의 사이버 보안 준비 태세 설문조사

응답자 중 29%가 데이터 유출을 경험했다고 답했으며, 지난 12개월간 대한민국의 위협 환경은 여전히 불안정합니다.[1]

데이터 유출을 경험한 응답자 중 77%는 빈도가 늘어났다고 답했으며, 응답자 중 54%는 데이터 유출을 11회 이상 경험했다고 답했습니다. 중간 규모 조직에서 데이터 유출을 가장 많이 경험했으며(43%), 소매(79%), IT 및 기술(55%), 비즈니스 및 전문 서비스(45%)가 가장 많은 공격을 받은 산업들이었습니다.

응답자 중 77%가 조직 IT 예산의 10% 이상을 사이버 보안에 지출하고 있다고 답했으며, 사이버 보안의 최우선순위로 조직의 네트워크 및 데이터 보안(25%), 데이터의 안전한 저장 및 비즈니스에서의 적절한 사용(24%), 사이버 공격 방어(22%)가 꼽혔을 정도로 사이버 보안은 계속해서 IT 지출의 중요한 영역입니다.

한국이 아태지역 내 다른 국가와 비교했을 때 돋보이는 부분

	대한민국	아태지역
향후 12개월 동안 Zero Trust에 투자할 계획을 갖고 있을 가능성이 높음	51%	40%
조직에서 IT 예산의 10% 이상을 사이버 보안에 지출할 가능성이 낮음	77%	84%
규제 요건과 인증에 발맞추기 위해 주당 업무 시간의 10% 이상을 쓸 가능성이 낮음	19%	48%

사이버 보안의 최우선 순위

조직의 네트워크 및 데이터 보안 25%

데이터를 안전하게 저장 24%

사이버 공격 방어하기 22%

사이버 공격을 해결하기 위해 탐색해야 하는 솔루션이 너무 많음(44%), 인적 리소스에 대한 부담(42%), 반복적인 작업/비중요 사이버 보안 기능에 너무 많은 시간 소요(40%), 사용 중인 다른 솔루션/소프트웨어와의 통합 문제(40%) 등 여러 벤더로 인해 발생하는 어려움으로 인해 통합이 일반적으로 사용되는 전략인 것으로 나타났습니다.

웹 공격(48%), 피싱(40%), 분산 서비스 거부(DDoS) 공격(40%)이 데이터 유출을 초래한 3대 공격 벡터였으며, 개인 식별 정보(65%), 고객 데이터(62%), 사용자 액세스 자격 증명(60%)이 가장 자주 표적이 되는 자산이었습니다. 또한 응답자의 82%가 AI 때문에 데이터 유출의 정교함과 심각성이 증가하는 것에 대해 우려하고 있는 것으로 나타났습니다.

이처럼 어려운 위협 환경에도 불구하고, 복원력이 증가하고 있는 징후가 있습니다. 응답자 중 69%는 데이터 유출을 방지할 준비가 되어 있다고 생각하며, 73%는 자체 조직의 사이버 보안 태세가 "다소 성숙되었다"고 생각합니다. IT 및 기술, 리테일, 비즈니스 및 전문 서비스 조직에서 데이터 유출 방지와 관련하여 '고도로 준비되어' 있다고 가장 많이 응답했습니다.

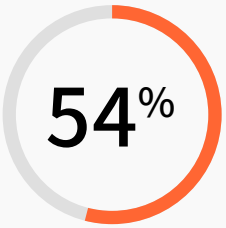
1. 데이터 유출이란 공격자가 조직의 애플리케이션, 데이터, 네트워크에 무단으로 액세스하는 사고를 말하며, 사고는 시스템 무결성을 잠재적으로 손상시킬 수 있는 행동을 말합니다.

Zero Trust 채택은 잘 진행되고 있으며, 응답자 중 33%가 자체 조직에서 현재 Zero Trust 솔루션에 투자하고 있다고 답했습니다. 또 다른 51%의 응답자는 향후 12개월 내에 Zero Trust에 투자할 계획이 있습니다. 주요 투자 동인은 VPN 대체로 인한 네트워크 속도 및 대기 시간 개선(54%), 취약한 IoT 장치로 인한 위험 감소(53%), 다단계 인증을 통한 사용자 자격 증명 도용 및 피싱의 영향 감소(52%)였습니다.

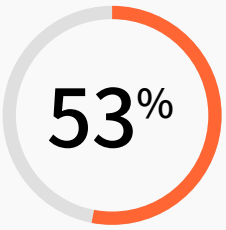
응답자들이 직면한 다른 과제로는 사이버 보안 인재 부족(35%), AI로 인한 떠오르는 위협(33%) 등이 있습니다. 응답자들은 주로 사이버 공격을 감지(44%)하고 대응(47%)하는 데 걸리는 시간을 기준으로 사이버 보안 솔루션을 평가했습니다.

랜섬웨어는 여전히 커지고 있는 우려 사항입니다. 응답자 중 36%가 랜섬웨어를 우려했고, 웹 애플리케이션이나 서버의 패치되지 않은 취약점에 대한 공격자의 악용(52%)이 가장 일반적인 침입 수단이었습니다.

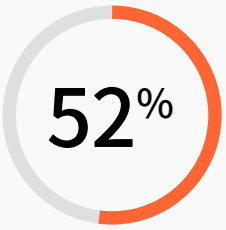
Zero Trust의 핵심 투자 동인



VPN 대체로 인한 네트워크 속도 및 대기 시간 개선



취약한 IoT 장치로 인한 위험 감소



다단계 인증을 통해 사용자 자격 증명 도용 및 피싱의 영향을 줄임

규제 및 규정 준수에 이용되는 리소스

응답자 조직의 27%에서 규제 및 규제 준수 요건을 해결하기 위해 IT 예산의 5% 이상을 지출하고 있습니다

한국 응답자의 19%가 업계의 규제 요건과 인증에 발맞추기 위해 주당 근무 시간의 10% 이상을 근무한다고 답했습니다

조직에서 지난 2년 이내에 랜섬웨어 공격을 경험한 응답자 중 33%는 자신의 조직에서는 랜섬을 지급했다고 답했지만, 38%는 공개적으로 랜섬을 지급하지 않겠다고 다짐했습니다. 랜섬을 지급하게 된 주요 요인은 고객의 압박(57%)이었습니다. 그러나 응답자들은 자체 조직이 직원 교육(53%), 2단계 인증(81%), 맬웨어 방지 소프트웨어(66%)의 배포를 통한 랜섬웨어 위협을 완화하는 것과 관련하여 적어도 "다소 성숙되었다"고 생각했습니다.

규제 및 규제 준수도 올해의 연구에서 중요한 주제로 떠올랐습니다. 응답자의 27%가 속한 조직의 경우 IT 예산의 5% 이상을 규제 및 규제 준수 요건을 해결하는 데 지출하고 있습니다. 응답자 중 19%는 업계 규제 요건 및 인증에 발맞추기 위해 주당 근무 시간의 10% 이상을 업무에 할애하고 있다고 답했습니다. 그러나 규제 및 규제 준수에 대한 이러한 투자는 조직의 기본 개인정보 보호 및/또는 보안 수준 향상(50%), 조직의 평판 및 브랜드 개선(44%), 조직의 기술 및 데이터 무결성 향상(44%) 등 조직에 긍정적인 영향을 미쳤습니다.

권장 사항

이러한 연구 결과를 염두에 두고 내년에 CISO가 수행해야 할 6가지 사항을 권장합니다.

복잡성을 줄이기 위한 솔루션 간소화

Cloudflare에서는 작년 보고서에서 SASE를 통해 보안 아키텍처를 간소화할 것을 제안했습니다. 올해에도 그 제안은 여전히 유지되며, 솔루션과 IT 벤더가 많다고 해서 위험이 감소하지는 않으리라는 증거가 분명합니다. 조직에서는 배포되는 솔루션의 수를 최소화하고 솔루션을 구매하는 IT 공급업체들을 통합하기 위해 더 신중한 접근 방식을 고려해야 합니다.

연결 사슬에서 가장 약한 고리를 강화

글로벌화되고 상호 연결된 오늘날의 환경에서 모든 조직에서는 소프트웨어 공급망에 의존합니다. 애플리케이션은 오픈 소스 코드를 기반으로 구축되었고, API, 타사 통합도 증가하는 모두 공격면의 일부입니다. 이와 같은 공격면의 확장 때문에 새로운 파트너를 온보딩한다는 것이 도구 자체가 아닌 전체 개발 생태계를 신뢰하기로 선택하는 것을 의미하게 되는 것입니다. 경계 기반 보안 모델로부터 아무도 신뢰하지 않고 공격자가 이미 네트워크 내에 있다고 가정하고 ID 및 컨텍스트를 기반으로 사용자, 장치, 워크로드를 평가하는 Zero Trust 모델로 이동하면 공급망 침해와 관련된 위험을 줄일 수 있습니다. 설계 원칙에 따라 안전하게 보호하는 데 전념하는 파트너를 찾으세요.

랜섬웨어 공격자의 영향력을 제한하고 요구 사항에 대한 계획을 세우세요

랜섬웨어 공격이 증가하고 있으므로 CISO 및 이사회에서는 대비 계획을 마련해야 합니다. 이 연구의 증거를 살펴보면, 랜섬을 지급한 조직에서는 거의 모든 경우 자체 행동을 후회했기 때문에 그 계획에 랜섬 지급이 포함되어서는 안 됩니다. Cloudflare에서는 Zero Trust 역량을 활용하여 유출 발생 시 내부망 이동을 최소화하는 전략을 권장합니다. 또한 강력한 복원 프로그램이 있으면 공격자의 요구로 인한 영향력이 줄어듭니다. 보증은 가장 중요한 시스템과 데이터의 효율성과 완전성을 보장할 수 있는지 테스트를 거친 정기적인 데이터 백업에서 시작됩니다. 정기적인 재해 복구 테스트를 하는 것은 미흡한 부분을 파악하고 운영을 복구하고 영향을 줄이는 역량을 구축하는 데 아주 중요합니다.

공격의 증폭 및 강도를 부채질하는 AI에 대비하기

공격자들은 AI를 이용할 것이며, CISO는 AI 방어 전략을 마련해야 합니다. 사이버 보안 리더는 단순히 문제를 아웃소싱하는 것을 경계해야 하지만, 인재 모델, 거버넌스 프레임워크, 규제 준수 요건, 사용량 모니터링 등을 검토할 필요는 분명히 있습니다. 지금 취할 수 있는 주요 조치는 타사 벤더의 AI 모델에서 사용되는 데이터를 이해하고 귀사의 요건에 부합하도록 타사 벤더와의 계약 조건을 검토하는 것입니다. 귀사의 현재 보안 도구는 늘어나는 AI 공격에 어떻게 대응하나요? 많은 Cloudflare 제품은 Cloudflare의 방대한 전역 네트워크를 활용하여 새로운 위협에 선제적으로 대응합니다.

자본에서 운영 비용으로 투자를 전환하세요

대부분의 경우 예산에 압박을 받고 있으며 사이버 보안 리더는 훌륭한 재정 관리자가 되어야 합니다. 기존 팀원의 숙련도를 높여 미래 상황에 맞춰 복잡성을 줄이고 프로세스를 간소화해 보세요. 역할을 재편하여 효과를 극대화하는 동시에 지연 시간을 줄일 수 있는 기회를 살펴보세요. 일부 기능을 MSP에 아웃소싱하여 자본 비용에서 운영 비용으로 투자를 전환하는 것도 고려해 볼 가치가 있습니다.

더 많은 정밀 조사에 익숙해지시기 바랍니다

사이버 보안 리더들은 내외부적으로 강화되는 조사를 받고 있으며, 이에 따라 이미 상당한 압박이 더 가중되고 있습니다. 이러한 정밀 조사는 계속될 것이며 CISO는 변화하는 규제(현지 또는 국제)를 준수하고 이사회 구성원의 요구를 충족할 기회를 부지런히 모색해야 합니다. 감사 약속을 협상하여 범위와 타임라인을 명확하게 하여 고객에게 가치를 더 많이 제공하지 못하고 위험을 줄이지도 못하는 작업을 줄이세요.

클라우드 연결성으로 이동하세요

Cloudflare에서는 회사의 직원, 애플리케이션, 네트워크를 연결하고 보호하는 클라우드 연결성이라는 새로운 서비스 범주를 제공하여 어디에서든 보안을 제공하는 데 중요한 역할을 합니다. 애플리케이션, API 및 네트워크 보안, Zero Trust, 글로벌 위협 인텔리전스 등 Cloudflare의 광범위한 보안 포트폴리오를 통해 조직에서는 사이버 공격에 대비하여 디지털 인프라를 강화할 수 있습니다. 조직에서는 온라인 데이터 및 지적 재산의 보안을 보장하고 브랜드의 무결성을 보호할 수 있습니다.

이러한 보안 서비스는 Cloudflare의 프로그래밍 가능한 전역 클라우드 네트워크 서비스 플랫폼을 기반으로 구축되며 전 세계 인터넷 트래픽의 상당 부분을 연결하고 보호하며 하루 평균 1,820억 건의 위협을 차단합니다. 이 전역 클라우드 네트워크는 다운타임의 위험을 최소화하고 네트워크 중단 및 인프라 장애에 대한 이중화와 복원력을 제공하여 높은 가용성을 보장합니다.

Cloudflare의 모든 솔루션 제품군에 대해 자세히 알아보고 영업 담당자에게 데모 또는 POC를 요청하시려면 **cloudflare.com/ko-kr/**을 방문해 주세요. 기존의 보안 상태를 평가한 후 직원, 애플리케이션, 장치, 네트워크, 데이터 부문의 사이버 보안 강화를 위한 실행 계획을 마련하도록 Cloudflare에서 지원합니다.

대한민국을 포함한 아태지역 전체 보고서를 읽으시려면 QR 코드 스캔하시기 바랍니다.

* **새로운 보안 환경 탐색하기: 아시아 태평양 지역의 사이버 보안 준비 태세 설문조사**에는 아시아 태평양, 일본, 중국의 보안 시장에 대한 조사 결과가 실려 있습니다. 이 연구는 대한민국을 포함한 14개 시장의 사이버 보안 관련 의사 결정권자 및 전문가 3,844명을 대상으로 수행되었습니다.