IBM 보안 서비스 사이버 보안 인텔리전스 지수

IBM의 전 세계 보안 운영 환경을 기반으로 사이버 보안 공격 및 보안 사고 데이터 분석

보고서 소개

IBM 매니지드 보안 서비스는 130여 개국, 3,700여 곳의 고객을 위해 연중무휴 24시간 제공되며, 매일 수백억 건의 이벤트를 모니터링합니다.

이러한 글로벌 운영 기반을 토대로 IBM 분석가들은 방대한 데이터를 활용할 수 있고, 최신 보안 위협과 사이버 보안 위협 환경을 종합적으로 파악할 수 있습니다.

이 보고서는 2012년 10월 1일 ~ 2012년 12월 31일의 데이터를 토대로 작성되었습니다. 이는 보안 사고에 대한 사전 모니터링과 관리, 사후 대응과 포렌식(Forensic) 분석 과정에서 수집된 데이터입니다.

본 데이터와 분석에서는 악의적 의도가 아니라 내부자의 실수에 의한 데이터 유출과 일상적으로 탐지되는 악성 코드 또는 스팸은 제외했습니다.

보안 인텔리전스 그 이상

보안 인텔리전스는 효과적인 사이버 보안 전략의 필수적인 부분입니다. 광범위한 보안 모니터링을 통해 최고 정보 보안 책임자(CISO)는 통찰력을 얻고, 최신 보안 공격을 파악할 수 있습니다. 또한 공격의 출처를 파악하고 이를 차단하거나 줄일 방법을 제안할 수도 있습니다.

보안 위협을 분석하는 것은 매우 중요한 일이지만, 이것이 다는 아닙니다. 이 보고서는 보안 공격 중 몇 건이 보안 사고로 진행되었는지, 어떤 조치가 이를 막을 수 있었을 것인지, 이러한 흐름이 업종별로는 어떻게 달라지는지를 조명합니다.

사이버 보안 공격 발생률

보안 공격은 정보 시스템 자원 또는 정보 자체를 수집, 중단, 거부, 저하, 파괴하려는 온갖 종류의 악의적 활동을 의미합니다.[1]

1년	1주	1일
1조 3740만	260만	38만

가장 공격을 많이 받는 업종

사이버 보안 공격 발생률은 업종에 따라 크게 달라지며, 공격 빈도가 가장 높은 5개 업종들 간에도 상당한 차이가 있습니다.[1]

업종	주 평균 공격 건수
의료 및 사회 보장 서비스	1,010만
운송	980만
접객	550만
금융 및 보험	360만
제조	260만

공격 범주

공격은 다양한 형태를 띠며, 공격 유형은 업종에 따라 달라집니다.[1]

공격 유형	빈도
악성 코드	33%
지속적인 탐색/스캔	28%
무단 액세스	15%
로우앤슬로우(Low–and–slow) 공격	12%
액세스 또는 신임 정보 악용 공격	11%
서비스 거부(DoS)	2%

공격자 범주

고의성 없는 실행자는 사이버 보안 공격의 배후 중에서 가장 소규모이지만, 이들에 의해 매주 약 50.9건의 의도치 않은 데이터 유출 사고가 일어나고 있습니다.[1]

공격자	빈도
외부자	44%
알 수 없음	24%
악의적 의도를 지닌 내부자	23%
고의성 없는 실행자	9%

공격자의 동기

대응이 취해진 후 IBM 비상 대응(Emergency Response) 컨설턴트들이 확신하거나 추정한 공격의 동기는 다음과 같습니다.[1]

동기	빈도
우발적	49%
산업 스파이, 금융 범죄, 테러 행위, 도용	23%
고용주/일자리에 대한 불만	15%
사회적 운동, 시민 불복종	7%
기타	6%

사이버 보안 사고 발생률

IT 보안 사고란 사이버 공격이 성공적으로 표적을 무너뜨린 경우를 의미합니다. 사고 발생률은 관찰 대상 데이터에서 사이버 공격 100만 건당 성공한 사고의 비율로 계산됩니다.

1.07건의 사고/
100만 번의 공격[1]

보안 사고당 평균 비용 예상치

비용이란 보안 사고를 해결하기 위해 비상 대응 서비스를 수행하는 데 드는 평균적인 비용을 의미합니다. 이 수치에는 시스템 가동 중단, 고객사 직원의 업무 시간, 평판 관련 리스크, 회사의 브랜드 가치 실추 등이 포함되지 않습니다.

사고 유형	평균적인 대응 비용[2]
봇넷 활동	$120,000
네트워크 손상	$92,156
맬웨어 감염	$61,875
이메일 손상	$33,000
데이터 유출	$23,062

보안 사고가 발생한 이유[3]

보안 사고의 잠재적 원인 중 80%는 일반 사용자의 실수 및 시스템 관리 부실과 관련이 있습니다.

이유	빈도
잘못 구성된 시스템/애플리케이션	42%
최종 사용자 오류	31%
미확인	17%
취약 코드	6%
타겟공격, 취약성 이용	6%

업종의 성숙도 지수

보안 성숙도 지수는 관찰 대상인 업종 범주의 사이버 보안 사고 발생률을 평가한 것입니다. 보안이 성숙한 업종은 사고 발생률이 훨씬 낮습니다. 다음은 공격 100만 건당 사고의 비율입니다.[1]

성숙도 가장 높음		성숙도 가장 낮음	
업종	**공격 100만 건당 사고 수**	**업종**	**공격 100만 건당 사고 수**
부동산	0.14	건설	4.49
운송	0.28	교육	1.97
접객	0.42	공익 산업	1.91
금융 및 보험	0.45	광업, 석유 및 가스	1.80
의료 및 사회 보장 서비스	0.57	역외 활동	1.70

추가 정보

사이버 보안 위협으로부터 귀사를 보호하고 귀사의 IT 보안을 강화하는 데 IBM이 어떤 도움을 줄 수 있는지 알아보십시오. IBM 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 다음 웹 사이트에서 알아보실 수 있습니다.

ibm.com/services/security

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
March 2013

[1]IBM 사이버 보안 인텔리전스 & 대응 팀(IBM Cyber Security Intelligence & Response Team)이 2012년에, 특히 2012년 10월 1일 ~ 12월 31일에 중점적으로 수집한 고객 모니터링 및 컨설팅 데이터와 그 분석에 기초합니다. IBM 매니지드 보안 서비스는 130여 개국, 3,700여 곳의 고객을 위해 연중무휴 24시간 제공되며, 매일 수백억 건의 이벤트를 모니터링합니다. 이 데이터와 분석에서는 악의적 의도가 없는 내부자의 실수에 의한 데이터 유출과 일상적으로 탐지되는 악성 코드 또는 스팸은 제외했습니다.

[2]사고당 평균 비용은 IBM 비상 대응 서비스(Emergency Response Service, ERS)에 소요된 평균 시간을 사고별로 분류한 것에 기초하며, 2012년의 IBM ERS 프로젝트 비용 내역을 토대로 합니다.

[3]데이터와 분석은 IBM X-Force 트렌드 및 리스크 보고서(Trend & Risk Report)에 기초합니다.

Please Recycle