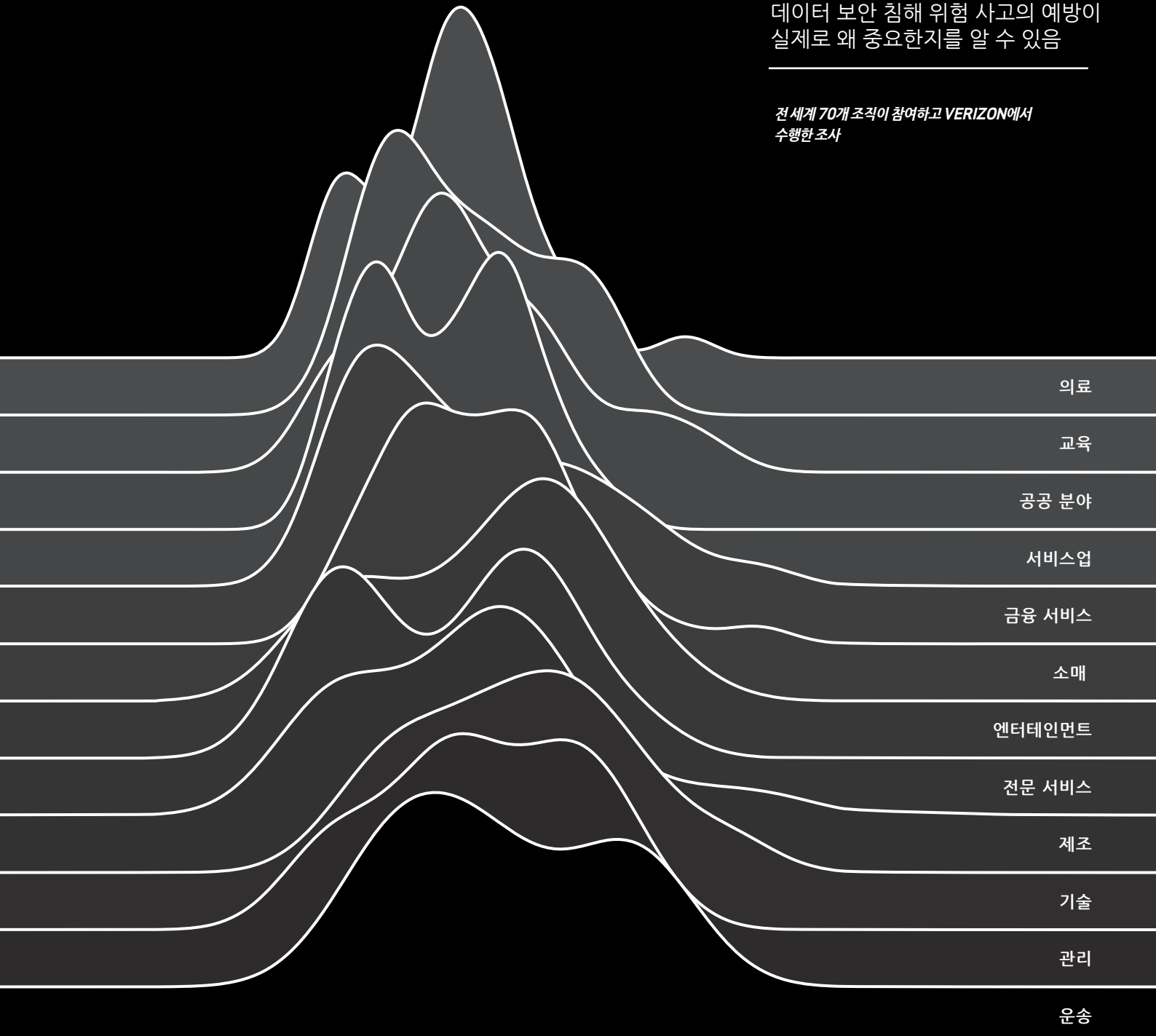
2015 데이터 보안 침해 조사 보고서

요약

4억 달러
7억 개의 레코드 손상 시 예상 손실액. 데이터 보안 침해 위험 사고의 예방이 실제로 왜 중요한지를 알 수 있음

전 세계 70개 조직이 참여하고 VERIZON에서 수행한 조사



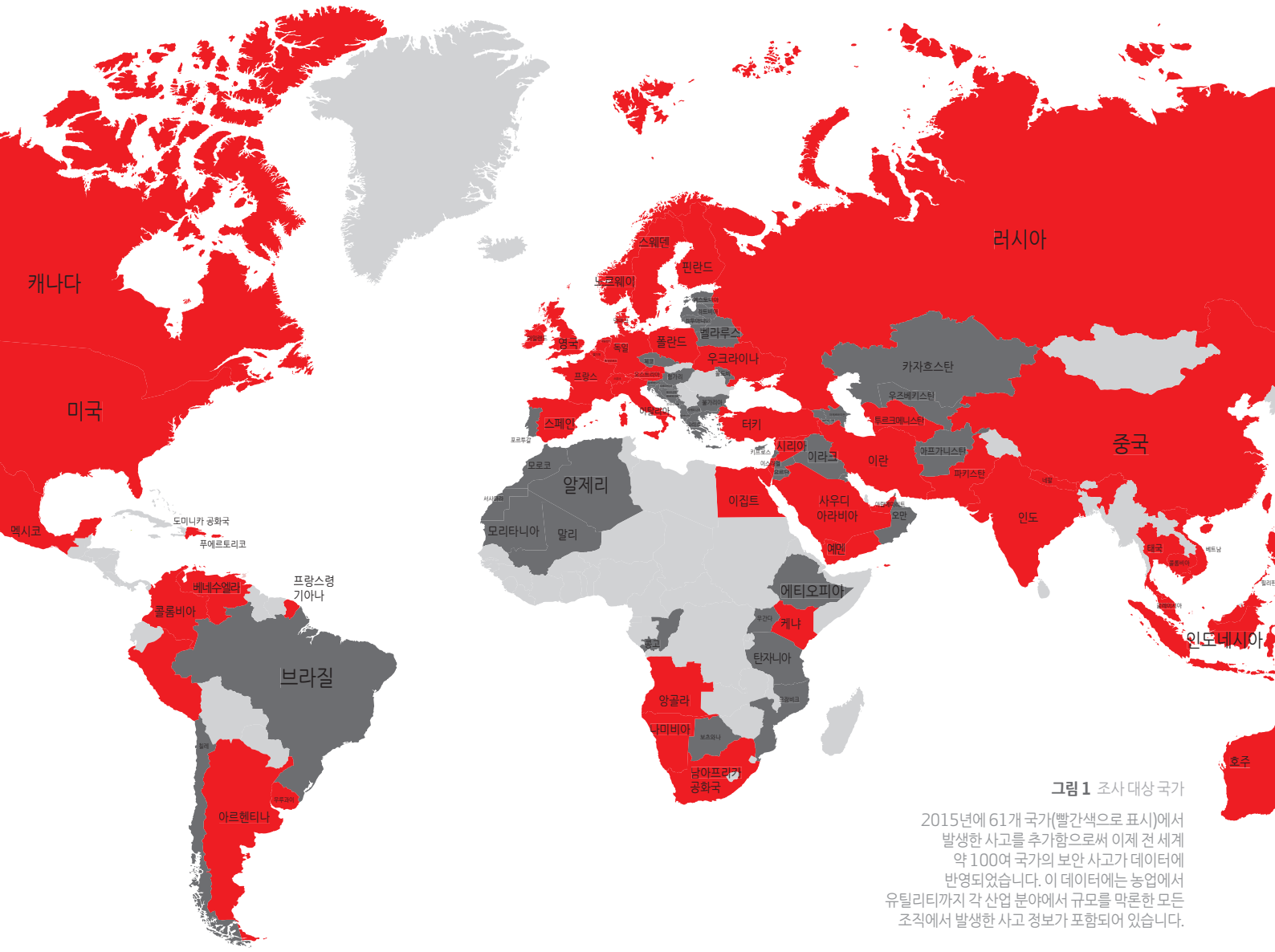


그림 1 조사 대상 국가

2015년에 61개 국가(빨간색으로 표시)에서 발생한 사고를 추가함으로써 이제 전 세계 약 100여 국가의 보안 사고가 데이터에 반영되었습니다. 이 데이터에는 농업에서 유틸리티까지 각 산업 분야에서 규모를 막론한 모든 조직에서 발생한 사고 정보가 포함되어 있습니다.

2015 DBIR

데이터 보안이 중요한 이유

데이터 보안 침해 사고로부터 조직을 보호함으로써 수천만 달러의 비용을 절감할 수 있으며, 고객 충성도와 주주의 신뢰를 유지할 수 있습니다. 데이터 보안은 IT 부서만의 일이 아닙니다. 경영진에게만 국한된 일도 아니며, 그 역할에 관계없이 모든 직원들에게도 영향을 미치는 매우 중요한 문제입니다.

공격의 동기는 매우 다양합니다. 결제 카드 데이터 또는 중요한 상업 정보를 원할 수도 있지만 단순히 비즈니스를 방해시키려는 의도로 공격할 수도 있습니다. 공격 방식 또한 갈수록 더욱 정교해지고 있으며, 피싱이나 해킹, 멀웨어를 함께 사용하는 경우도 많습니다.

그리고 공격자들은 엄청나게 빠른 속도로 몇 초 만에 방어막을 뚫고 침투할 수 있습니다. 이처럼 공격자가 시스템을 손상시키는 데는 많은 시간이 필요하지 않지만 조직이 피해 사실을 아는 데는 수개월, 심지어 수년이 걸릴 수도 있습니다.

70
데이터를 제공한 법 집행 기관 및 IT 보안 회사의 수

2,122
분석한 데이터 보안 침해 사고의 수

79,790
분류한 보안 사고의 수

Verizon 2015 데이터 보안 침해 조사 보고서 (DBIR)는 2,122건의 확인된 데이터 보안 침해 사고를 포함하여 약 80,000건의 사고에 대한 자세한 분석을 제공합니다. 이 요약에서는 그 중 몇 가지 주요 조사 결과를 소개합니다.

새롭게 부상하고 있는 공격 기회

모빌리티가 발달하고 사물 인터넷(IoT)이 점점 더 많이 사용되면서 데이터와 시스템에 대한 공격 가능성이 증가할까요?

6개월 동안 모든 무선 장치에서의 악성 활동을 살펴본 결과, 모든 유형의 멀웨어 공격이 매우 낮은 빈도로 나타났으며 대부분은 단순 자원 낭비 유형으로 그 영향이나 감염률이 심각한 것은 아니었습니다.

M2M(사물 지능 통신: Machine to Machine) 장치에 관련된 보안 사고는 많지 않았습니다. 그렇다고 해서 방어막을 계획할 때 이 분야를 무시해도 되는 것은 아니며, 강력한 액세스 제어 및 중요한 데이터에 대한 암호화가 필요합니다.

여전히 위협적인 구식 기법

피싱은 여전히 인기 있는 공격 기법으로 이제는 멀웨어의 설치까지 가능한 수준으로 진화되었습니다. 조사 결과 이러한 공격의 효과가 점점 더 커지고 있으며, 23%의 수신자가 피싱 메시지를 열어보고, 11%가 첨부 파일을 여는 것으로 나타났습니다. 더 큰 문제는 평균 82초 만에 첫 번째 클릭이 발생한다는 사실입니다.

조사한 20,000개 조직에서 차단된 멀웨어 이벤트의 수는 약 1억 7천만 개에 달하며, 그 중 70-90%는 여러 조직에 걸쳐 발생한 것이 아니라 한 조직 내에서만 나타난 것이었습니다. 그러나 이들은 특정 대상을 목표로 개발된 멀웨어가 아니었습니다. 물론 그러한 멀웨어도 있었지만 매번 공격할 때마다 코드가 조금씩 변조된 멀웨어가 대부분이었습니다. 이렇게 변조된 멀웨어는 기존 바이러스 백신 제품이 찾고 있는 서명을 우회하므로 악성 코드가 침투하여 시스템을 손상시킬 수 있습니다.

계속 남아 있는 기존의 취약점

2014년에 발생한 보안 공격의 약 97%가 10개의 취약점을, 나머지 3%의 공격이 기타 7,000,000개의 취약점을 악용한 것으로 확인되었습니다. 대부분의 공격이 수개월 또는 수년 전에 패치가 제공된 알려진 취약점을 여전히 악용하고 있는 것입니다. 2014년에 확인된 취약점 중에는 2007년에 발견된 취약점도 있었습니다.

여전히 계속되고 있는 익숙한 패턴

작년, Verizon은 발생 가능한 대부분의 문제를 포함하는 9가지 사고 패턴을 발표했습니다. 올해 역시 전체 사고의 96%가 이 패턴에 포함되었습니다. 그나마 다행스러운 점은 대부분의 조직이 직면하는 보안 위협은 대부분 이 패턴 중 3개의 패턴에 포함될 가능성이 높다는 사실입니다. Verizon의 9가지 사고 분류 패턴을 사용하면 우선 순위에 따라 효과적으로 방법을 강구하여 강력한 방어 토대를 구축할 수 있습니다.

비용 증가

데이터 보안 예산을 정당성을 설명하고 그 가치를 입증할 수 있도록 보안 침해 사고의 비용을 산출해 줄 것을 요청하는 조직이 많습니다. 올해, DBIR에서는 최초로 데이터 보호에 실패할 경우 기업에서 지불해야 할 비용을 산출해 보았습니다.

기존의 다른 모델은 보안 침해 사고로 인한 비용을 지나치게 단순화하는 경향이 있습니다. Verizon은 실제 사이버 배상책임 보험에 청구된 데이터를 사용하여 손상된 레코드의 수가 증가함에 따른 비용의 불확실성을 해소한 더욱 강력한 모델을 개발했습니다.

이 모델을 사용하여 추정한 1,000개 레코드에 대한 보안 침해 사고의 평균 손실액은 52,000달러 - 87,000달러(레코드당 52달러 - 87달러)였으며, 1,000만 개의 레코드에 발생한 보안 침해 사고의 평균 손실액은 210만 달러 - 520만 달러(레코드당 0.21 - 0.52달러)로 나타났습니다.

23%

작년, 23%의 수신자가 피싱 메시지를 열어보고 11%가 첨부 파일을 클릭한 것으로 나타났습니다.

96%

작년 DBIR에서는 지난 10년간 발생한 사고의 92%를 9가지 패턴으로 분류할 수 있다고 보고했습니다. 지난 12개월 간 보안 위협 환경에는 많은 변화가 있었지만 여전히 대부분의 사고(96%)가 이 9가지 패턴에 해당되는 것으로 나타나고 있습니다.

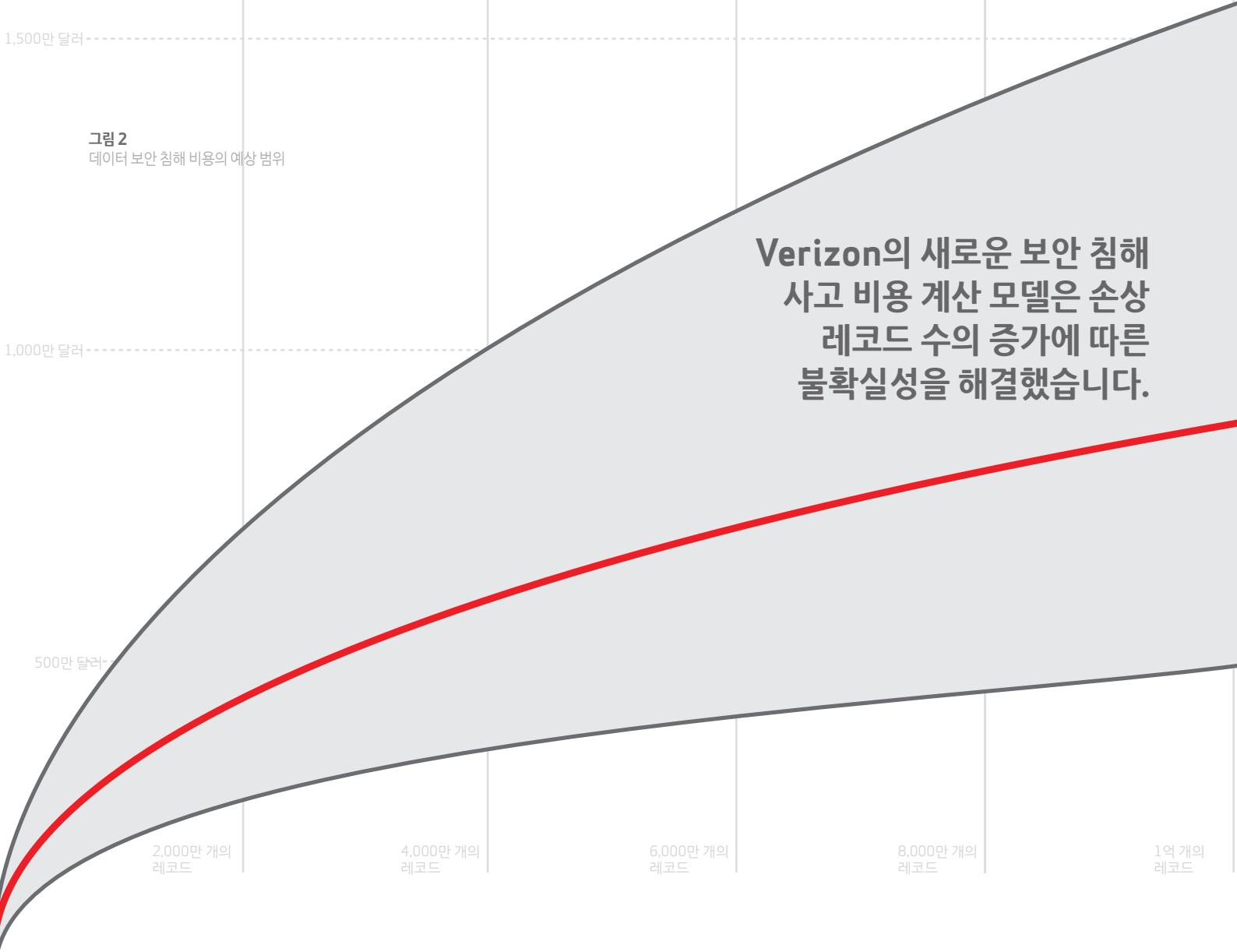


그림 2
데이터 보안 침해 비용의 예상 범위

Verizon의 새로운 보안 침해 사고 비용 계산 모델은 손상 레코드 수의 증가에 따른 불확실성을 해결했습니다.

보안 침해 사고의 비용

데이터 보안 침해 사고의 비용은 얼마나 될까요? 이제 데이터 보호에 실패할 경우 지불해야 할 비용을 더욱 합리적으로 평가할 수 있습니다.

$254

100개 레코드에 대한 보안 침해 사고의 레코드당 예상 비용은 254달러입니다.

9 ¢

1억 개 레코드에 대한 보안 침해 사고의 경우 그 수치는 0.09달러로 하락합니다. 물론 총 비용은 크게 증가합니다.

Verizon은 데이터 보안 침해 사고가 발생한 약 200건의 사이버 배상책임 보험 청구 사례를 분석한 결과, 데이터 보안 침해 사고로 인한 금전적 손실의 규모를 더욱 정확하게 파악할 수 있었습니다.

평균의 오류를 해결하는 모델

다른 분석 기관에서 사용한 모델에 따라 먼저 레코드당 평균 비용을 계산해 본 결과, 설문 조사 데이터를 바탕으로 산출된 예상 금액보다 상당히 적은 0.58달러로 나타났습니다. 그러나 실제 사례에서 소요된 비용과 비교해 보면 이 예상의 정확성에 많은 의구심이 생길 수 밖에 없습니다.

보안 침해 사고의 비용은 선형적 모델을 따르지 않습니다. 실제로는 레코드당 비용이 손실된 레코드의 수와 반비례합니다. 따라서 평균을 사용할 경우 레코드의 수가 증가할수록 평균값과의 차이도 크게 증가합니다. 그리고 Verizon은 10만 개 이상의 레코드가 손상된 사고를 포함하여 광범위한 사고를 다룰 수 있는 모델을 만들기를 원했습니다.

따라서 단순히 평균을 사용하는 대신, 레코드 수에 따른 실제 비용의 변화를 모델링했습니다. Verizon은 이 방법이 훨씬 더 신뢰할 수 있는 지표를 제공할 것이라 믿습니다.

그리고 Verizon의 모델은 모든 조직에서 발생하는 보안 침해 사고의 비용을 예측하는데 적용할 수 있습니다.

회사의 규모는 보안 침해 사고의 비용에 영향을 주지 않습니다.

대기업에서 보고하는 손실액이 엄청난 이유는 이러한 사고에 연관된 레코드의 수가 훨씬 더 많기 때문입니다. 조직의 규모에 관계없이 유사한 수의 레코드가 손상된 보안 침해 사고는 그 손실액도 유사한 수준인 것으로 나타났습니다.

최고의 모델 제공

100개의 레코드가 손상된 보안 침해 사고의 예상 비용은 25,445달러(레코드당 254달러)로 계산된 반면, 1억 개 레코드가 손상된 경우 약 900만 달러로 비용이 증가했습니다(레코드당 0.09달러). 그러나 물론 보안 침해 사고의 실제 비용은 손상된 레코드의 수 외, 여러 가지 요인에 따라 달라질 수 있습니다.

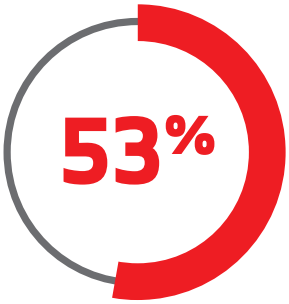
가장 중요한 요인 중 하나는 결제 카드 정보, 의료 레코드 등과 같은 손상된 데이터의 유형입니다. 보안 침해 사고의 예상 비용을 정확하게 예측하기 위해서는 한 가지 수치만이 아니라 여러 가지 요인을 고려해야 합니다.

아래 표는 예상 금액과 관련하여 평균 및 단일 이벤트에 대해 95% 신뢰 구간으로 계산된 최소 금액과 최대 금액을 보여줍니다. 예상 손실액 양 옆의 열(왼쪽 차트에 표시됨)은 같은 수의 레코드가 손상된 여러 사고의 평균값이며, 바깥쪽 열에는 개별 사고에 대한 수치가 반영되어 있습니다.

따라서 예를 들어 Verizon의 모델에서 1,000개의 레코드에 대한 보안 침해 사고의 손실액은 3,000달러부터 150만 달러에 이릅니다. 여러 가지 특이한 사례까지 포함시킨 결과 그 수치가 매우 광범위합니다. 반면 같은 1,000개 레코드의 보안 침해 사고에 대해 평균 비용을 살펴보면 52,000달러 - 87,000달러 정도의 금액임을 알 수 있습니다.

이러한 비용의 의미

보안 침해 사고가 발생하면 비즈니스를 보호하는 데 필요한 노력과 리소스에 대한 비용보다 훨씬 더 많은 비용을 지불하게 됩니다. 이 모델을 사용하여 각 조직에 일어날 수 있는 데이터 보안 침해 사고의 손실액 규모를 참고할 수 있기를 바랍니다.



Verizon의 분석 결과, 보안 침해 사고의 비용에서 차이가 생기는 원인의 53%는 손상된 레코드의 수로 설명할 수 있습니다. 나머지 47%의 비용 차이는 보안 대비 상태 등의 몇 가지 요인에 따라 달라질 수 있습니다.

그림 3 보안 침해 사고 비용 분석

레코드의 수	예측(최소)	평균(최소)	예상 손실액	평균(최대)	예측(최대)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

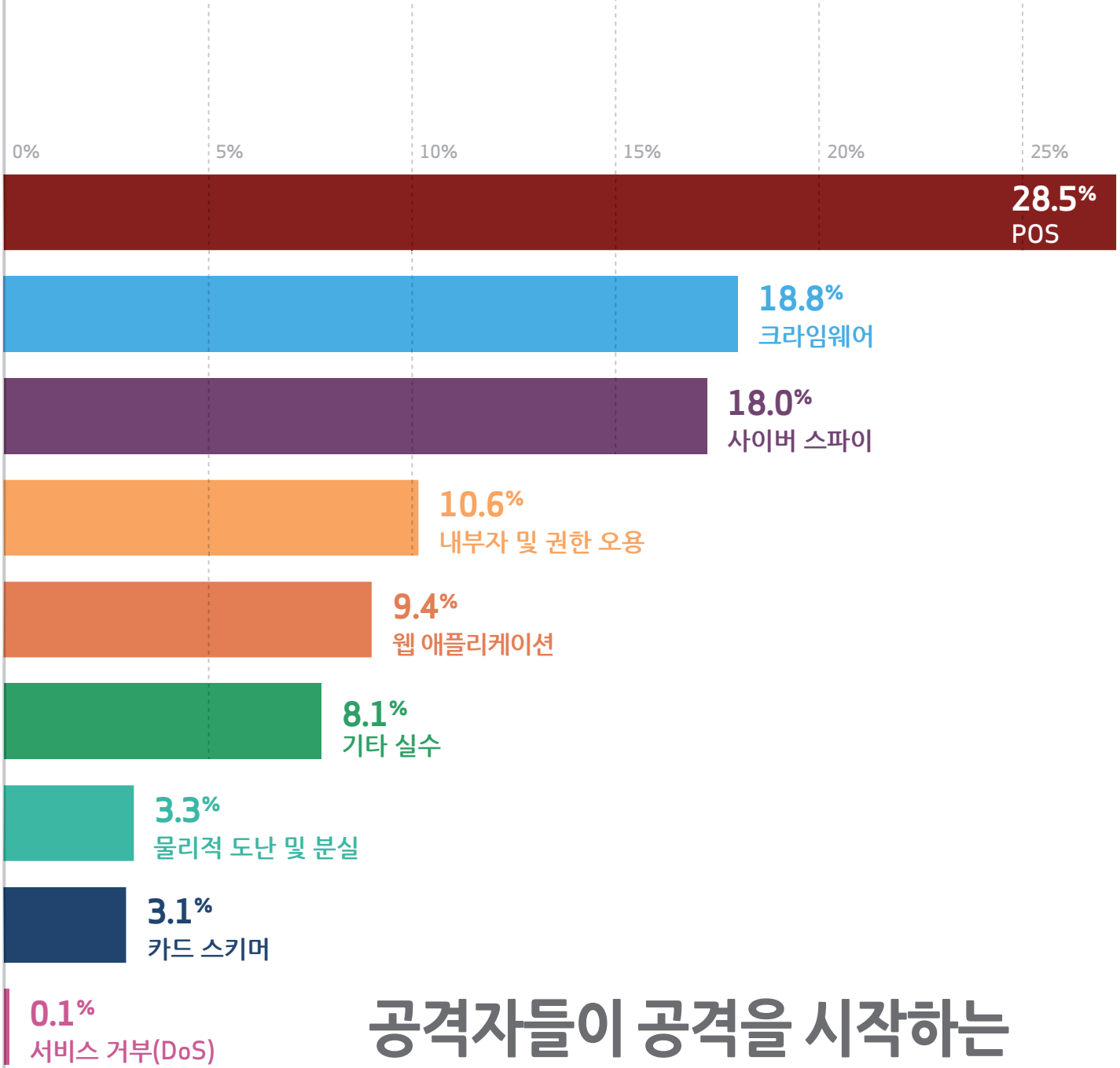


그림 4
사고 분류 패턴별 보안 침해 사고의 빈도

공격자들이 공격을 시작하는 방법

작년, Verizon은 각 기업에서 발생할 수 있는 대부분의 보안 침해 사고에 해당하는 9가지 사고 패턴을 분류했습니다. 올해의 데이터 세트에서도 96%의 보안 침해 사고가 이 패턴에 포함되는 것으로 나타났습니다. 그리고 조직이 직면하는 대부분의 보안 위협은 그 중 3가지 패턴에만 해당될 가능성이 높습니다.

지금까지 Verizon에서 조사한 대부분의 사고는 위 9가지 패턴에 포함됩니다.

데이터에 대한 보안 위협은 갈수록 복잡하고 광범위해지고 있습니다. 그러나 Verizon은 통계 방법을 사용하여 유사한 사고와 보안 침해를 분류함으로써 가장 큰 위협을 식별하고 보안 조사를 시작할 우선 순위를 정하는 데 도움이 되는 프레임워크를 만들었습니다.

데이터 손상이 확인되지 않은 사고를 포함한 모든 사고를 검토한 결과 잘못된 수신자에게 이메일을 전송하거나 기밀 정보를 안전하게 폐기하지 않거나 지위를 이용하여 기밀 데이터를 수집하는 등, 주요 3개 패턴의 공통 분모가 사람임을 알 수 있었습니다.

확인된 데이터 보안 침해 사고(위 그림 4 참조)를 보면 기업이 기존 방어 체제에서 가장 취약한 공격 패턴이 무엇인지 알 수 있습니다. 바로 POS(Point-of-Sale) 사고, 크라임웨어, 사이버 스파이입니다.

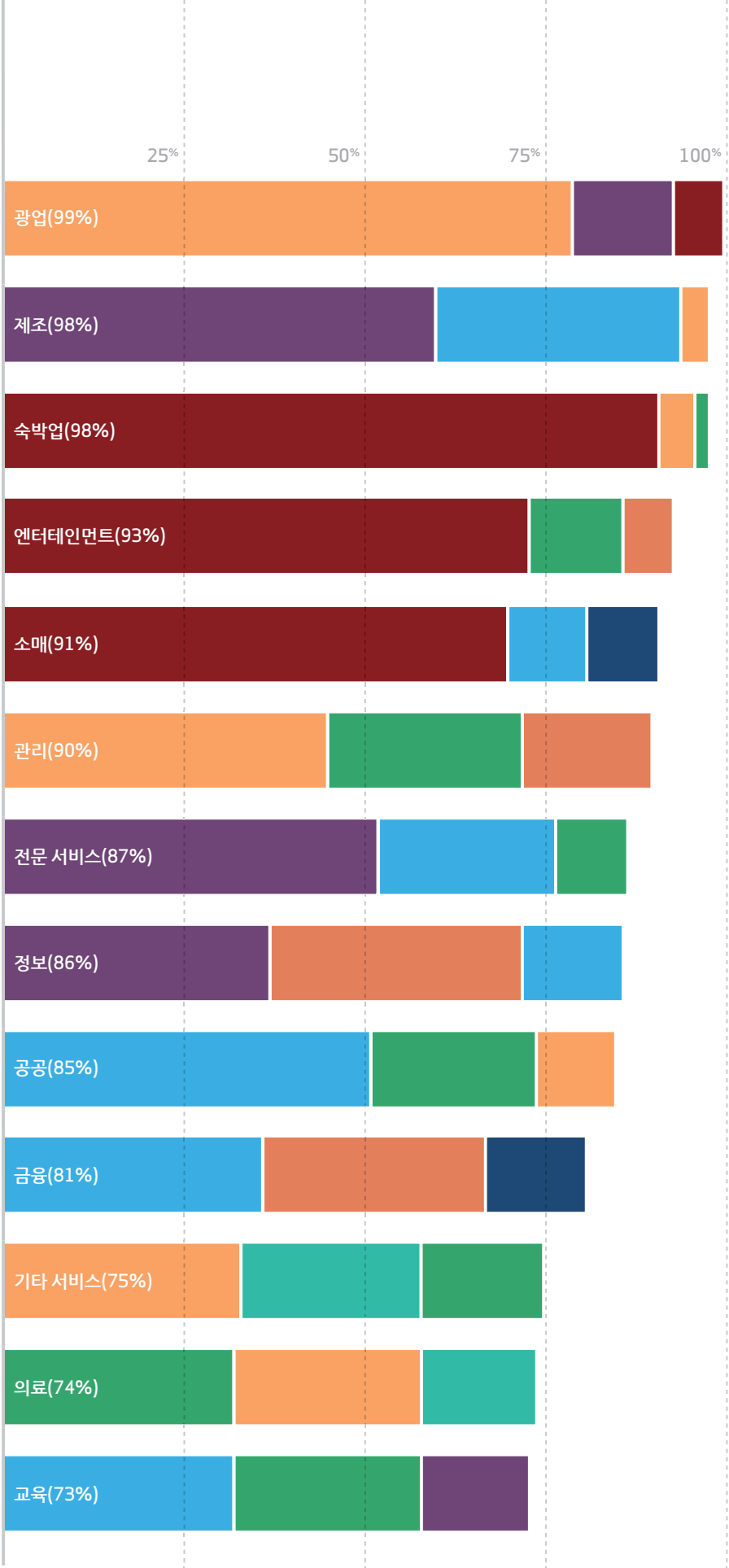


그림 5 데이터 유출, 산업별 주요 3가지 패턴

각 산업별 3가지 주요 패턴

각 산업마다 처한 보안 위협의 성격도 다릅니다. 각 산업에서 직면하고 있는 주요 보안 위협을 이해하면 적절한 방어막을 구축하는 데 도움이 될 것입니다.

그나마 다행스러운 점은 대부분의 산업에서 발생한 보안 침해 중 3/4 이상이 9가지 패턴 중 3가지 패턴에 해당된다는 사실입니다(왼쪽 그림 5 참조).

평균적으로 각 산업에서 보안 침해 사고의 83%가 이 3가지 패턴에 포함됩니다.

또한 각 부문에서 운영 모델이 유사한 다른 조직을 살펴봄으로써 어디에 노력을 집중해야 할 지 알 수 있습니다. 2015 DBIR에서는 산업 프로파일링에 대한 심화 탐구를 통해 각 산업의 하위 부문 간 보안 위협 프로필의 유사성을 확인할 수 있었습니다.

- 크라임웨어
- 사이버 스파이
- 서비스 거부 공격
- 내부자 및 권한 오용
- 기타 실수
- 결제 카드 스키머
- 물리적 도난 및 분실
- POS 침입
- 웹 애플리케이션 공격

9가지 패턴

작년에 Verizon에서 분류한 9가지 사고 패턴을 통해 더 쉽게 보안 위협 환경을 이해할 수 있으며, 회사의 전략에 집중하여 더욱 효과적으로 보안 투자의 우선 순위를 정할 수 있습니다.

POS 침입

공격자가 결제 데이터를 캡처하기 위해 POS 애플리케이션을 실행하는 컴퓨터와 서버를 손상시키는 공격입니다.

가장 많이 발생하는 산업: 숙박, 엔터테인먼트, 소매

소규모 보안 침해에서는 공격자가 단순히 암호를 추측하거나 브루트포스 무차별 대입 공격 방식을 사용하는 경우가 많지만, 대규모 보안 침해 사고에서는 보조 시스템을 공격하여 POS 시스템에 대한 액세스를 확보할 수 있습니다. 2014년에 발생한 여러 건의 사고에서는 POS 서비스 업체가 공격의 시발점이 되었습니다. 기본 자격 증명에 의존하는 것에서 이제는 직원을 대상으로 하는 직접 소셜 엔지니어링을 통해 습득한 로그인 정보를 사용하는 것으로 그 추세가 바뀌고 있습니다.

예방법 PCI DSS 규정 준수는 POS 시스템 보호를 위한 가장 기본적인 수단입니다. 2015 PCI 규정 준수 보고서에서 기업의 준수율이 가장 낮은 항목은 취약점 검사 및 테스트인 것으로 나타났습니다.

크라임웨어

멀웨어를 사용하여 시스템을 손상시키는 모든 공격을 포함하는 광범위한 카테고리입니다. 전형적인 기회 유형의 공격으로 금전적 이익이 주요 동기입니다.

가장 많이 발생하는 산업: 공공, 정보, 소매

올해에만 공격 기법 중 하나로 피싱을 사용한 사고가 수백 건 발생했습니다. 그리고 거래 기밀이 손상된 여러 사례에서 기본적인 멀웨어만으로도 기업 데이터가 위험해 질 수 있음이 입증되었습니다.

예방법 바이러스 백신과 브라우저 패치를 적용하여 공격을 차단하고, 2단계 인증을 사용하여 손상을 최소화합니다. 감지된 악성 프로그램에서 수행하려고 한 작업을 통해 우선적으로 리소스를 투입해야 할 분야를 파악합니다.

사이버 스파이

특정 국가의 정부와 관련된 인물이 조직에 침투하여 주로 명확한 대상에 대한 피싱 공격을 통해 지적 자산을 훔치는 행위를 말합니다.

가장 많이 발생하는 산업: 제조, 공공, 전문 서비스

올해에는 사이버 스파이 관련 데이터 보안 침해 사고가 내부자 오용 또는 웹 애플리케이션 공격보다 더 많이 발생했습니다. 사이버 스파이는 일반적으로 피싱 캠페인이 포함되며, 이 캠페인을 통해 정교한 멀웨어를 침투시킵니다.

예방법 즉시 패치를 적용하고 바이러스 백신 소프트웨어를 최신 버전으로 업데이트합니다. 사고 대응 및 대책을 수립하기 위한 기본 토대로 시스템, 네트워크 및 애플리케이션 활동을 기록합니다.

내부자 및 권한 오용

주로 내부자의 오용이 여기에 해당되지만 외부자(공모를 통해) 및 파트너(허가된 권한을 사용)도 가능합니다.

가장 많이 발생하는 산업: 공공, 의료, 금융

올해 발생한 대부분의 보안 침해 사고는 최종 사용자와 관련되어 있지만(그림 6 참조) 임원부터 말단 사원까지 사내 직원 누구나 잠재적 범죄자가 될 수 있습니다. 40%의 사고는 금전적 이익이 그 동기였지만 허가되지 않은 해결 방법을 사용하는 직원들에 의해서도 손상이 발생했습니다.

예방법 첫 단계는 어떤 데이터가 어디에 보관되어 있으며 누가 액세스하는지를 파악하는 것입니다. 그런 다음 추가 감사와 사기 탐지 프로세스가 필요한 분야를 찾습니다. 퇴사한 직원의 장치를 검사하여 회사의 방어 체계에서 보완해야 할 약점을 찾을 수 있습니다.

그림 6
내부자 오용의 가해자

웹 애플리케이션 공격

웹 애플리케이션(예: 컨텐츠 관리 시스템(CMS) 또는 전자상거래 플랫폼)에서 훔친 자격 증명 또는 취약점을 사용합니다.

가장 많이 발생하는 산업: 정보, 금융, 공공

2014년에 발생한 거의 모든 웹 애플리케이션 공격은 기회 유형이었으며 공격하기 쉬운 대상을 목표로 했습니다. 대부분의 공격은 일반적으로 고객의 장치에서 훔친 자격 증명(그림 7 참조)를 사용합니다.

예방법 로드 밸런싱 장치, 웹 애플리케이션 및 데이터베이스 거래 로그를 검토하여 악성 활동을 식별합니다. 2단계 인증을 사용하고 로그인 시도 실패가 반복되는 계정을 잠급니다.

기타 실수

보안을 손상시키는 모든 실수를 말합니다.

가장 많이 발생하는 산업: 공공, 정보, 의료

대부분의 사고에는 항상 직원들이 연루되어 있습니다. 실수 사고에서 가장 많이 나타나는 3가지 주요 요인으로는 의도하지 않은 수신자에게 중요한 정보 전송(30%), 비공개 데이터를 공개 웹 서버에 게시(17%), 개인 및 의료 데이터의 안전하지 않은 폐기(12%)가 있습니다.

예방법 데이터를 보호하기 위해서는 사용자의 중요한 정보 전송을 차단하는 데이터 손실 방지(DLP) 소프트웨어를 구현하는 것이 좋습니다. 데이터 보안과 중요한 자료의 폐기 방법에 대한 직원 재교육 또한 필요합니다.

물리적 도난 및 분실

노트북, USB 드라이브, 인쇄된 용지 및 기타 정보 자산의 분실, 주로 사무실과 차량에서 발생합니다.

가장 많이 발생하는 산업: 공공, 의료, 금융

2014년에 발생한 거의 모든 도난 사고는 기회 유형의 공격이었으며, 55%는 작업 공간 내에서, 22%는 차량에서 발생했습니다.

예방법 이 범주의 사고 중 15%는 분실 사실을 알아채는 데 수일이 걸립니다. 장치를 암호화하여 저장된 데이터를 보호하고, 정기적으로 백업을 실시하여 중요한 데이터의 분실을 방지하고 다운타임을 줄입니다.

결제 카드 스키머

결제 카드의 데이터를 읽기 위해 ATM, 주유 펌프 또는 POS 단말기에 물리적인 "스키머"를 설치합니다.

가장 많이 발생하는 산업: 금융, 소매

공격자들은 이제 얇고 투명한 카드 스키머를 카드 판독기 슬롯 내부에 장착하여 사용합니다.

예방법 결제 터미널을 모니터링하고 직원들을 교육하여 스키머 및 의심스러운 동작을 식별합니다.

DoS(서비스 거부) 공격

비즈니스의 정상적인 운영을 중단시킬 목적으로 악성 트래픽을 과도하게 발생시키는 "봇넷"을 사용합니다.

가장 많이 발생하는 산업: 공공, 소매, 금융

분산 DoS 공격의 수는 2014년에 2배로 증가했으며, 점점 더 많은 공격자들이 인터넷 자체의 인프라를 사용하여 공격을 증폭시키고 있습니다.

예방법 서비스의 위치, 구성 방식을 파악합니다. 알려진 봇넷 서버의 액세스를 차단하고 시스템에 패치를 적용합니다. 방어 계획을 세울 수 있도록 정기적으로 훈련을 실시합니다. 또한 손상된 서비스를 복구하기 위한 기술을 추가해야 합니다.

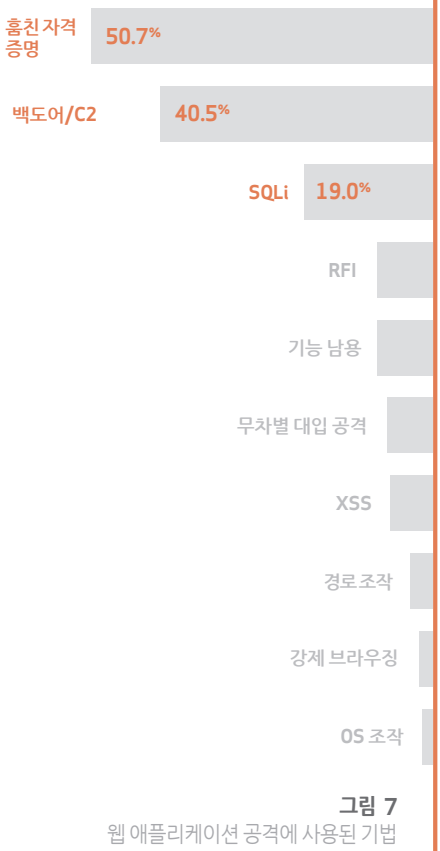


그림 7
웹 애플리케이션 공격에 사용된 기법

새롭게 부상하고 있는 보안 위협

올해의 DBIR에서는 CEO와 CIO가 우려하고 있는 몇 가지 새로운 잠재적 위험에 대해서도 살펴보았습니다. 특히, 스마트폰과 태블릿 사용의 증가, 실제 구현으로 빠르게 전환하고 있는 사물 인터넷(IoT)으로 인한 위험에 대해 살펴보았습니다.

0.03%

지난 6개월 동안 Verizon 네트워크를 사용한 수천만 대의 스마트폰과 태블릿에서 악성 활동을 조사한 결과, 연간 0.03% 미만의 장치만 감염된 것으로 확인되었습니다.

5억

2020년까지 50억 개의 기업 IoT 장치와 함께 수십억 개의 소비자 IoT 장치가 사용될 것입니다.

출처: Verizon State of the Market: The Internet of Things 2015

과장된 모바일 보안 위협

모바일 기술에 의존하고 있는 기업이 증가하고 있으며, 스마트폰과 태블릿, 특히 조직의 제어가 이루어지지 않고 있는 이러한 기기는 해커의 다음 공격 대상이 될 것이라는 우려가 확산되고 있습니다. 이러한 우려를 해결하기 위해 Verizon은 최초로 모바일 멀웨어와 관련 보안 위협에 대해 분석했습니다.

모바일 플랫폼은 취약할 수 있지만 Verizon의 사고, 보안 침해 및 무선 네트워크 데이터를 살펴보면 아직은 공격자들이 선호하는 공격 대상이 아님을 확인할 수 있었습니다. 무선 네트워크 상의 모바일 장치에서 발생한 악성 활동을 분석한 결과 모바일 멀웨어의 발생 빈도는 매우 낮으며, 애드웨어와 기타 단순 자원 낭비 등, 대부분은 감염되어도 중대한 영향을 미치지 않는 것으로 나타났습니다. 업무를 마비시킬 중대한 멀웨어가 발생한 장치의 수는 연간 0.03% 미만에 불과했습니다.

회사 네트워크를 손상시킬 가능성이 높은 것으로 알려진 기법에 우선적으로 리소스를 투자하는 것이 좋으며, 이러한 기법은 Verizon의 9가지 사고 패턴을 통해 손쉽게 확인할 수 있습니다. 모바일 보안 면에서는 장치의 사용 방식을 파악하고 제어해야 합니다. 이를 통해 의심스러운 활동을 인식하여 보안 위협 환경의 변화에 신속히 대응할 수 있습니다.

안전하지 않은 사물 인터넷

모든 M2M(Machine to Machine) 장치가 인터넷을 지원하거나 중요한 정보를 전송하지는 않지만 IoT가 IT 환경에서 증가하고 있는 것은 사실입니다. 따라서 새로운 지능적 장치 전략를 시작할 때는 보안을 중요하게 고려해야 합니다.

2014년에 알려진 사고 중에서 M2M 장치(예: 연결된 차량 및 스마트 시티)가 연루된 보안 사고나 이를 통한 데이터 유출 사고는 아직 많지 않지만 그렇다고 안심할 수는 없습니다. 보고에 의하면 연결된 장치가 다른 시스템을 손상시키기 위한 진입 지점으로 사용되고 있으며, 서비스 거부 공격을 위한 봇넷에 IoT 장치를 함께 사용하고 있다고 합니다.

따라서 IoT 환경을 구축하려는 경우 보안 위협 모델링 분석을 수행하여 가장 발생 가능성이 높은 공격과 그 동기, M2M 서비스가 가장 취약한 분야를 파악하는 것이 좋습니다.

IoT 애플리케이션 내의 데이터를 안전하게 보호하기 위해서는 다음과 같은 조치를 취해야 합니다.

- 반드시 필요한 데이터만 수집
- 강력한 동의 및 액세스 제어 구현
- 암호화 및 익명화된 형태로 데이터 전송
- 데이터 분리(동향 분석을 수행할 경우 예외)

결론: 행동해야 할 때

그림 8 사고 관련 기간 분석

보안 사고를 발각하는 데 걸리는 기간이 길어질수록 공격자는 더 오랫동안 피해를 입힐 수 있습니다. 56%의 사고에서 조직이 보안 침해 공격 발생 사실을 파악하는 데 수시간 이상이 소요되며, 25%는 수일 이상이 소요됩니다. 그리고 이러한 "감지의 격차"는 더 커지고 있습니다.

60%의 사고에서 공격자는 몇 분 내로 조직을 손상시킬 수 있습니다.

주요 보안 침해 공격의 원인을 살펴보면 약 25%가 인터넷으로 액세스 가능한 웹 서비스에 대한 다단계 인증 및 패치 적용으로 방지할 수 있었던 것으로 나타났습니다. Verizon에서 식별한 관리/제어 미비 문제의 40%가 사이버 보안 주요 보안 제어의 "쉽고 간단한 예방 조치" 카테고리에 속하는 것으로 확인되었습니다.

2015 DBIR에서는 자세한 정보와 권고 사항을 제공하고 있으며, 그 중 7가지 공통 주제는 다음과 같습니다.

- **항상 경계해야 합니다.** 조직의 보안 침해 사실에 대해 경찰이나 고객이 먼저 알게 되는 경우가 많습니다. 로그 파일과 변경 관리 시스템을 통해 조기에 위험 신호를 파악할 수 있습니다.
- **첫 번째 방어막은 사람입니다.** 직원에게 보안의 중요성, 공격 신호를 감지하는 방법, 의심스러운 사항 발생 시 대응 조치 등에 대해 교육합니다.
- **"필요할 경우"에 한해 데이터를 제공합니다.** 업무 수행에 반드시 필요한 시스템 직원으로 액세스를 제한합니다. 그리고 직원의 역할이 바뀌거나 퇴직 시 액세스 권한을 해지하는 프로세스를 마련해야 합니다.
- **즉시 패치를 적용합니다.** 잘 구성된 IT 환경, 최신 버전으로 업데이트된 바이러스 백신 소프트웨어만으로도 많은 공격을 예방할 수 있습니다.
- **중요한 데이터는 암호화합니다.** 중요한 데이터의 도난을 방지할 수는 없지만 훔친 데이터를 범죄에 악용하기 어렵게 만들 수는 있습니다.
- **2단계 인증을 사용합니다.** 암호의 도난 위험을 줄일 수는 없어도 분실 또는 도난 당한 자격 증명으로 인한 피해를 줄일 수는 있습니다.
- **물리적 보안도 중요합니다.** 데이터 도난이 항상 온라인에서만 일어나는 것은 아닙니다. 범죄자들은 컴퓨터나 결제 단말기를 변조하거나 인쇄물 상자를 훔치기도 합니다.

Verizon 데이터 보안 침해 조사 보고서는 조직에 대한 보안 위협을 이해하고 이에 대한 방어를 개선하는 데 도움이 됩니다. 자세한 내용을 알아보려면 다음 사이트에서 전체 보고서를 다운로드하십시오. verizonenterprise.com/DBIR/2015.

verizonenterprise.com/kr