Deloitte.

정교해진 사이버 공격의 변화 양상과 대응 전략

전 세계 3개 권역 별 20개 국가간 사이버 위협과 고려사항 비교

딜로이트 통합 연구 센터
(Deloitte Center for Integrated Research)

April, 2024

목차

리더메시지

유선희 파트너
리스크 자문본부 | Cyber

기업 조직을 겨냥한 사이버 공격은 정교해지고 빠른 속도로 확산되고 있다. 피싱, 랜섬웨어, 암호화폐 채굴 악성코드, 정교한 산업 멀웨어 등 공격 방식과 용량 그리고 속도 면에서 상당한 진화를 거듭하고 있다. 많은 기업들은 새로운 변종이 급속히 확산되면서 이에 대응하기가 점차 어려워지고 있는 상황이다.

디지털 전환(Digital Transformation)에 따른 글로벌 경제와 산업구조 변화가 불러온 부작용이라 볼 수 있다. 디지털 전환은 비즈니스 모델과 프로세스의 혁신을 가져왔지만, 사이버 범죄자들이 공격할 수 있는 범위와 기회가 확대되었기 때문이다. 이들은 주로 네트워크, 애플리케이션, 임베디드 장치, 엑세스 포인트(AP)등을 공격 대상으로 삼고 있으며, 보다 새로운 방식으로 대담한 공격을 감행하고 있다. 이들도 디지털 전환과 유사한 전환을 경험한 것이다.

현재 만연하고 있는 최신 사이버 공격은 전통적인 보안정책과 전략 및 아키텍처 그리고 개별적으로 동작하는 포인트 솔루션으로는 대응하기가 어렵다. 기업내 IT 전담 조직도 충분한 보안 기능을 제공하지 못하고 있다.

오늘날 사이버 침해 사고는 기업의 신뢰와 운영에 심각한 피해를 입힌다. 조직내 보안 이슈가 비즈니스 리더들의 최우선 과제가 되고 있는 이유이다. 이제 리더들은 최신 사이버 공격에 대처하기 위해 사업장이 위치한 지역을 고려해야 하고, 보안 인프라 수준 및 위협 요인을 식별해야 한다. 그리고 이를 대응하기 위한 적합한 보안 솔루션의 도입과 투자를 고민해야 한다.

딜로이트는 2023년 '글로벌 사이버의 미래'를 주제로 조사를 진행했다. 본 조사에는 총 20개국 소속 1,100명이 설문과 인터뷰에 참여했고, 전 세계 지역별(북미, EMEA 및 APAC)로 사이버 위협과 침해 사례를 분석해 특정 지역에 주요한 위협 요인과 우선순위를 확인했다. 딜로이트는 수집된 데이터를 기반으로 비즈니스 리더들과 보안 담당자에게 지역 맞춤화된 사이버 보안 전략 수립과 사이버 보안 취약점 해소 그리고 보안 솔루션 도입과 인프라 투자 실행과 관련한 시사점을 제공하고자 한다.

정교해진 보안 위협과 대응 전략

기업 조직을 겨냥한 사이버 공격은 정교해지고 빠른 속도로 확산되고 있다. 피싱, 랜섬웨어, 암호화폐 채굴 악성코드, 정교한 산업 멀웨어 등 공격 방식과 용량 그리고 속도 면에서 상당한 진화를 거듭하고 있다. 많은 기업들은 새로운 공격 방식 급속히 확산되면서 이에 대응하기가 점차 어려워지고 있는 상황이다

디지털 전환(Digital Transformation)에 따른 글로벌 경제와 산업구조 변화가 불러온 부작용이라 볼 수 있다. 디지털 전환은 비즈니스 모델과 프로세스의 혁신을 가져왔지만, 사이버 범죄자들이 공격할 수 있는 범위와 기회가 확대되었기 때문이다. 이들은 주로 네트워크, 애플리케이션, 임베디드 장치, 엑세스 포인트(AP)등을 공격 대상으로 삼고 있으며, 보다 새로운 방식으로 대담한 공격을 감행하고 있다. 이들도 디지털 전환과 유사한 전환을 경험한 것이다.

현재 만연하고 있는 최신 사이버 공격은 전통적인 보안정책과 전략 및 아키텍처 그리고 개별적으로 동작하는 포인트 솔루션으로는 대응하기가 어렵다. 기업내 IT 전담 조직도 충분한 보안 기능을 제공하지 못하고 있다.

오늘날 사이버 침해 사고는 기업의 신뢰와 운영에 심각한 피해를 입힌다. 조직내 보안 이슈가 비즈니스 리더들의 최우선 과제가 되고 있는 이유이다. 이제 리더들은 최신 사이버 공격에 대처하기 위해 사업장이 위치한 지역을 고려해야 하고, 보안 인프라 수준 및 위협 요인을 식별해야 한다. 그리고 이를 대응하기 위한 적합한 보안 솔루션의 도입과 투자를 고민해야 한다.

딜로이트는 2023년 '글로벌 사이버의 미래'를 주제로 조사를 진행했다. 본 조사에는 총 20개국 소속 1,100명이 설문과 인터뷰에 참여했고, 전 세계 지역별(북미, EMEA 및 APAC)로 사이버 위협과 침해 사례를 분석해 특정 지역에 주요한 위협 요인과 우선순위를 확인했다. 조사에 참여한 리더들의 의견을 수렴해 사이버 사고 패턴을 식별하고, 침해사고 영향을 최소화하는 방안을 모색했다.

딜로이트는 수집된 데이터를 기반으로 비즈니스 리더들과 보안 담당자에게 지역 맞춤화된 사이버 보안 전략 수립과 사이버 보안 취약점 해소 그리고 보안 솔루션 도입과 인프라 투자 실행과 관련한 시사점을 제공하고자 한다.

전 세계 지역별 주요국들의 사이버 위협 현황

권역별 사이버 보안 위협

이번 딜로이트 조사에 따르면, EMEA 지역에서 사이버 사고가 가장 빈번하게 발생하는 반면에 APAC 지역은 사이버 사고 발생률이 가장 낮은 것으로 나타났다. 역설적이게도 EMEA 지역은 전 세계에서 가장 강력한 보안 인프라와 개인정보보호 규정을 갖추고 있음에도 불구하고, 가장 많은 사이버 침해 사고를 경험한 것으로 나타났다.

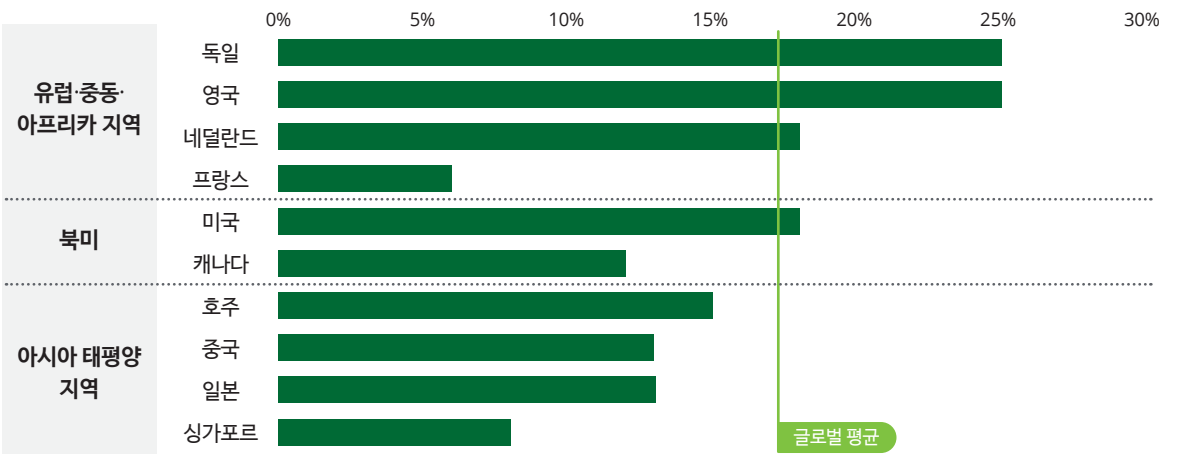
EMEA 지역에 위치한 기업들 중 20% 이상은 한 해 11건 이상의 사이버 침해 사고를 경험했으며, 독일과 영국에서 가장 많은 악성코드(Malware)감염 사고가 발생한 것으로 나타났다. 2021년 독일 연방정보기술 보안청(Bundesamt für Sicherheit in der Informations-technik, 이하 BSI) 발표에 따르면[1], '21년 2월 중 하루에 스파이웨어(Spyware), 루트킷(rootkit), 애드웨어(Adware), 크립토재킹(Cryptojacking)등 약 553,000개의 악성코드와 그 변종이 탐지되었고, 이로 인해 개인과 기업의 사이버 위협 단계가 '주의'에서 '심각' 단계로 상향 조정된 바 있다. 예외적으로 프랑스는 전체 글로벌 평균보다 낮은 발생율 보이고 있다. 이는 대부분의 프랑스 기업(97%)들은 사이버 보안과 관련된 예산을 늘리고 있고, 이 중 67%의 기업들이 SOAR[2] 기술에 투자하고 있기 때문이다.

미국(18%)을 제외하면 북미와 APAC 지역에 속한 기업들은 글로벌 평균(16%)보다 낮은 사이버 사고 발생율을 보이고 있다. 싱가포르(8%), 캐나나(12%), 일본(13%), 중국(13%) 순으로 사이버 사고 발생률이 낮다. 하지만 인지된 사고 발생율이 낮다고 해서, 보안 인프라 수준이 높은 것으로 예단할 수 없다. 알려진 사고가 적다고 해서 전체 기업들이 사고를 적게 경험하는 것이 아니라는 의미이다. 기업이 보유하고 있는 사이버 위험 탐지 기능과 보안 인프라 수준이 낮아 사이버 침해 상태를 인지하지 못하고 있는 상황 일수도 있기 때문이다.

기업이 보유한 보안 인프라의 수준이나 탐지 시스템은 모든 유형의 공격에 완벽하게 대응할 수 없다. 공격이 발생했음에도 기업 내부에서 이를 감지하지 못하는 경우가 있거나, 새로운 보안 취약점이 발견되어 공격에 노출될 수도 있다.

비즈니스 리더들은 사이버 위협 요인을 지속적으로 모니터링하고, 정기적인 보안 감사를 통해 기업의 현재 상태와 취약점을 식별하고, 사이버 사고의 사전 예방과 사고 발생 시에 신속히 대응할 수 있는 계획을 마련해야 할 것이다. 현재 갖추고 있는 보안 시스템의 업그레이드와 최신 솔루션을 도입해 취약점을 보완해야할 필요성도 있다. 무엇보다도 직원들에 대한 사이버 보안 교육을 강화하여 사이버 위협에 대한 인식을 높이고, 인적요소로 인한 보안 사고를 최소화하는 것이 가장 우선되어야 할 것이다.

그림 1. 연간 지역별 사이버 사고 발생율 (상위 10개국)



국가별 사고 발생율(%) = (사이버 사고를 연 11회~16회까지 경험 했다고 응답한자 수)÷(국가별 총 응답자 수)
출처: The Deloitte Center for Integrated Research(2023), N=1,110명, 20개국

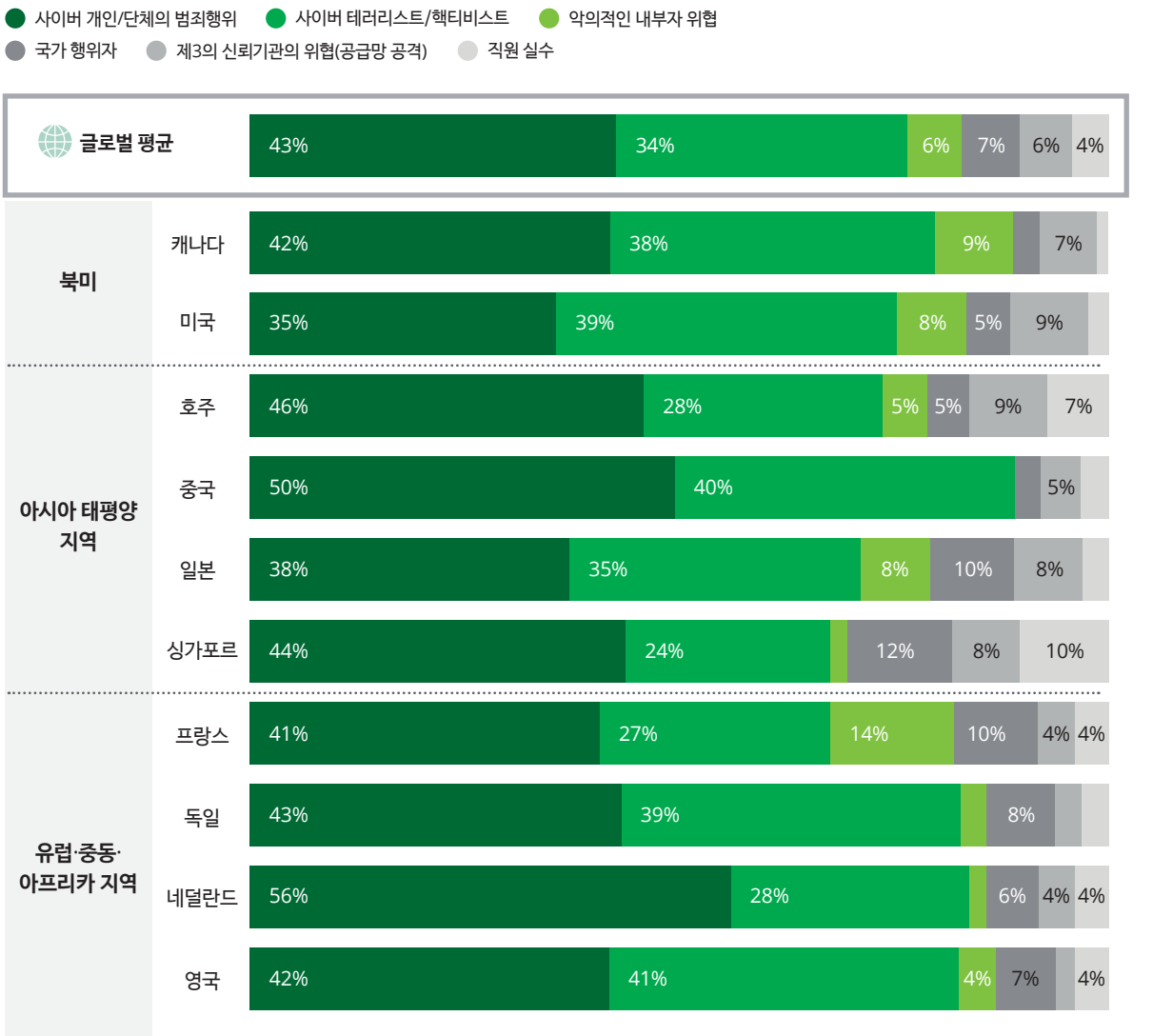
사이버 위협 행위자 유형

이번 딜로이트의 조사에서는 개인과 사이버 범죄 단체들에 의한 공격이 조사에 참여한 모든 권역과 국가들에서 가장 큰 위협으로 확인되고 있다. 그들의 공격을 가장 우려한다고 응답한 비율이 전 세계 권역(북미, EMEA 및 APAC)에서 약 40%에 육박하거나 이를 훌쩍 넘긴 수치를 보이고 있다.

국가별로 살펴보면, 네덜란드(56%)와 중국(50%)에서는 이들의 범죄 행위가 특히 높게 나타나고 있고, 영국(41%)과 중국(40%)에서는 사이버 테러리스트와 핵티비스트들의 사이버 공격 사례가 더 큰 위협으로 보고되고 있다.

전반적으로 중국에서 사이버 사고 발생율이 높게 보고되고 있는 이유는 단기간에 대규모 디지털 인프라와 전자상거래 생태계가 확대되어 사이버 범죄자들의 공격 표적이 되었고, 기업들 또한 면밀한 보안 검토 없이 신규 시스템을 빠르게 도입한 결과로 사이버 보안 취약점이 노출된 것으로 해석할 수 있다.[3]

그림 2. 기업 직면한 사이버 보안 위협 요인



출처: Deloitte Center for Integrated Research(2023), N=1,110명, 20개국

사이버 위협 행위자는 누구인가?

사이버 위협 행위자 또는 악의적인 행위자라고도 하는 위협 행위자는 디지털 디바이스나 시스템에 고의로 피해를 입히는 개인 또는 집단을 말한다. 위협 행위자는 컴퓨터 시스템, 네트워크 및 소프트웨어의 취약점을 악용하여 피싱, 랜섬웨어, 멀웨어 공격 등 다양한 사이버 공격을 지속한다.

그들은 각기 다른 동기와 기술수준, 공격 전술을 보이고 있지만, 공격의 동기와 정교함 수준에 따라 일반적으로 헥티비스트(Hacktivists), 사이버 테러리스트(Cyber terrorist), 국가 행위자(Nation states), 사이버 범죄자(Cyber criminals), 스릴추구자(Thrill-seeker) 그리고 내부 위협 행위자(Malicious employees) 등으로 구분한다.

① 사이버 범죄자 (Cyber criminals and organized crime)

금전적 이득을 목적으로 사이버 범죄를 저지르는 개인이나 집단이다. 사이버 범죄자들이 저지르는 일반적인 범죄에는 랜섬웨어 공격과 사람들을 속여 송금을 유도하거나 신용카드 정보, 로그인 자격 증명, 지적 재산 또는 기타 개인 정보나 민감한 정보를 유출하는 피싱 사기가 있다.

② 핵티비스트(Hacktivist)

핵티비스트는 해킹 기술을 사용하여 언론의 자유를 확산하거나 인권 침해를 폭로하는 등 정치적 또는 사회적 의제를 홍보한다. 핵티비스트들은 핵티비스트들이 긍정적인 사회 변화에 영향을 미치고 있다고 생각하며 개인, 조직 또는 정부 기관을 표적으로 삼아 기밀이나 기타 민감한 정보를 폭로하는 것이 정당하다고 생각한다. 잘 알려진 핵티비스트 단체의 예로는 인터넷에서 언론의 자유를 옹호한다고 주장하는 국제 해킹 집단인 Anonymous가 있다.

③ 사이버 테러리스트(Cyber terrorist)

사이버 테러리스트는 위협하거나 폭력을 초래하는 정치적 또는 이념적 동기로 사이버 공격을 시작한다. 일부 사이버 테러리스트는 국가 행위자이기도 하며, 스스로 또는 비정부 단체를 대신하여 행동하기도 한다.

④ 국가 행위자 (Nation states)

국가와 정부는 민감한 데이터를 훔치거나 기밀 정보를 수집하거나 다른 정부의 중요 인프라를 방해할 목적으로 위협 행위자에게 자금을 지원하는 경우가 많다. 이러한 악성 활동에는 스파이 활동이나 사이버 전쟁이 포함되는 경우가 많으며 막대한 자금이 투입되는 경향이 있어 위협이 복잡하고 탐지하기가 어렵다.

⑤ 스릴 추구자(Thrill-seeker)

스릴 추구자는 말 그대로 재미를 위해 컴퓨터와 정보 시스템을 공격한다. 어떤 사람들은 민감한 정보나 데이터를 얼마나 많이 훔칠 수 있는지 확인하고 싶어 하고, 어떤 사람들은 해킹을 통해 네트워크와 컴퓨터 시스템이 어떻게 작동하는지 더 잘 이해하고자 한다. 스크립트 키드라고 불리는 한 부류의 스릴 추구자들은 고급 기술력은 부족하지만 주로 재미나 개인적인 만족을 위해 기존의 툴과 기법을 사용하여 취약한 시스템을 공격합니다. 스릴 추구자는 항상 해를 입히려는 목적을 가지고 있는 것은 아니지만, 네트워크의 사이버 보안을 방해하고 향후 사이버 공격의 문을 열어 의도하지 않은 피해를 입힐 수 있다.

⑥ 악의적 내부자 위협(Malicious employees)

대부분의 다른 행위자 유형과 달리 내부 위협 행위자는 항상 악의적인 의도를 가지고 있는 것은 아니다. 일부는 무심코 멀웨어를 설치하거나 네트워크에 액세스하는 용도로 회사에서 발급한 디바이스를 분실하고 사이버 범죄자가 획득하는 등의 인적 오류로 인해 회사에 피해를 입히기도 한다. 그러나 금전적 이득을 위해 액세스 권한을 남용하여 데이터를 훔치거나 승진에서 밀린 것에 대한 보복으로 데이터 또는 애플리케이션에 손상을 입히는 등 불만을 품은 직원과 같은 악의적인 내부자도 존재한다.

⑦ 공급망 공격, 제3의 신뢰기관의 위협(TTP, Trusted third party)

사이버 위협의 행위자 역할을 하기도 하지만 사이버 공격의 유형으로 공급망 공격을 뜻한다. 공급망 공격이란 회사의 시스템 및 데이터에 접속할 수 있는 외부 협력업체 소프트웨어 개발자나 공급업체 등을 통해 발생하는 공격이다. 특정 회사에 해커가 직접 침투하는 것이 아니라 제3자의 보안 취약점을 통해 공격하므로 '서드파티 공격'(third party attack)이라 불리기도 한다. 예컨대 한 대기업의 마케팅팀에서 외부 스타트업의 데이터 분석 도구를 사용한다고 가정하면, 해커는 보안 수준이 상대적으로 높은 대기업 대신 비교적 보안이 느슨한 스타트업을 해킹해 대기업의 내부 시스템에 우회로 침투할 수 있다는 것이다.

APAC지역 기업들은 개인과 범죄 단체들에 의한 사이버 위협 다음으로 국가 행위자와 써드파티들에 의한 사이버 공격을 가장 우려하고 있는 것으로 나타났다. 싱가포르에서는 국가행위자들의 위협(12%)을, 호주에서는 써드파티의 위협(9%)을 가장 우려하고 있는 것으로 나타났다. 각각의 경우에 전세계 평균은 5%와 3%에 불과하며 싱가포르와 호주가 나타내고 있는 수치는 세계 평균을 2배 이상의 높은 수치를 보이고 있다.

APAC 지역내에 다수의 기업들은 사이버 보안 전략을 수립하고 있으며, 자산과 리소스를 보호하기 위해 타사 보안 솔루션을 도입하고 보안 모니터링과 조기 탐지 프로세스를 가동 중이다. 위협 행위자를 완전히 막지는 못하지만 피해 범위와 영향을 최소화시키기 위한 노력인 것이다. 하지만 사이버 위협 행위자들은 사내 직원들의 실수를 침투 표적으로 삼는 경우가 많다. 이에 대응하기 위해 기업들은 사내 보안 정책 업데이트와 내부자 보안 교육을 병행하고 있다. 기업내에서 승인된 장치 외에는 사용하지 않는 것부터 비밀번호 설정 방법, 피싱 이메일의 식별과 대처 기술까지 다양한 측면을 포함하고 있다. 직원들의 보안 인식과 행동이 사이버 공격 최후의 방어선이기 때문이다.

내부자 위협은 회사 자산을 사용할 권한이 있고 합법적인 액세스가 가능한 사용자가 고의로 또는 실수로 자산을 남용한 경우에 발생한다. 내부 직원들의 보안사고를 가장 위협적으로 보고 하고 있는 국가는 프랑스(14%)로 글로벌 평균(6%)보다 높은 수치를 보이고 있다. 조사에 참여한 대부분 응답자들이 금융산업에 종사하기 때문에 나타난 결과이긴 하지만, 이는 금융 부문에서 내부자 공격에 대한 취약성이 단적으로 드러나는 순간이다.[4]

캐나다에서도 내부직원들에 의한 보안 사고율(9%) 우려가 높게 나타나지만 그 원인은 프랑스와는 전혀 다르다. 2020년 캐나다 지역 내 다수의 기업에서 정리해고가 발생했고, 이에 불만을 품은 직원이 고용주에게 손해를 입히기 위해 선택한 일탈 행위였다. 그들은 내부 기밀정보의 유출이나 악성코드 배포 등으로 보안 시스템에 치명적인 손상을 입힌 것이다.[5] 기업에 있어 그 어떤 물리적 보안과 시스템의 구축보다 내부자 보안 통제와 관리가 중요한 이유이다.

기업들은 내부자 관리와 보안 인식 교육이 상대적으로 실행이 용이하고 저렴하다는 이유로, 이를 형식적으로 운영하는 경우가 많다. 하지만 내부자들의 보안 통제와 관리는 사이버 위협에 대응하는 가장 효과적인 방법이면서 동시에 이를 등한시 했을 때 치명적인 위협이 될 수 있다는 사실을 알아야 할 것이다.

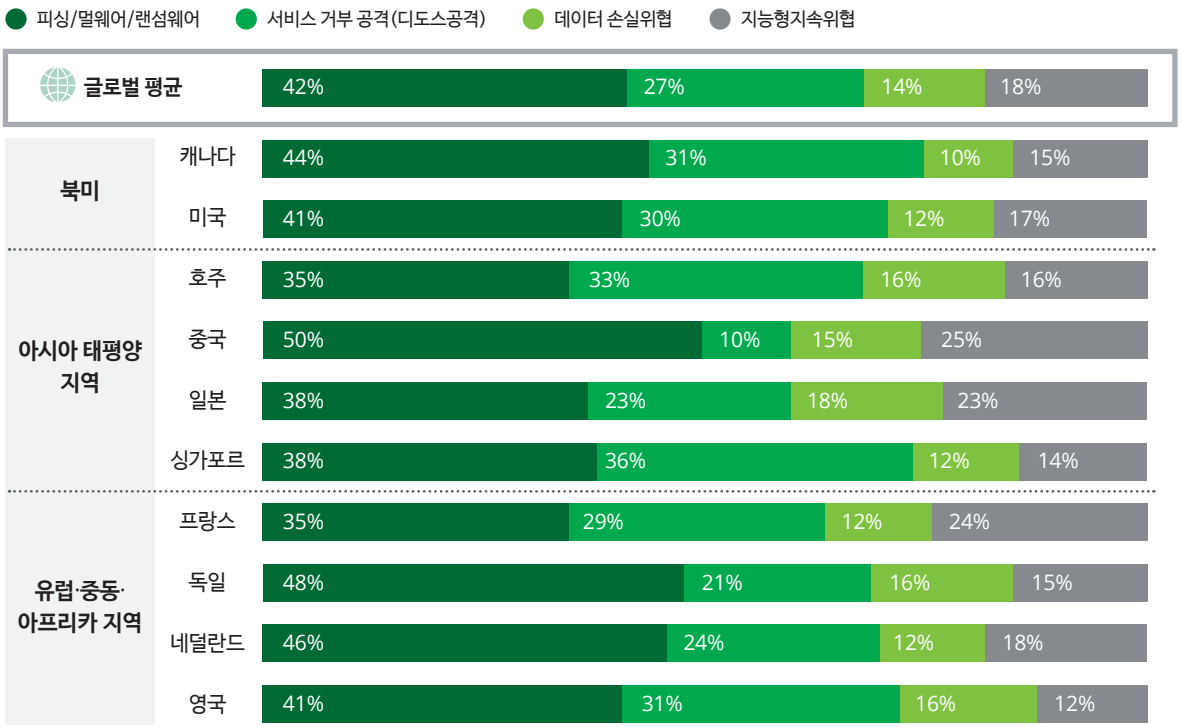
사이버 위협 행위자들의 전술

전 세계에서 발생하는 대부분의 사이버 공격은 '피싱', '멀웨어'(악성 소프트웨어) 그리고 '랜섬웨어' 방식이다. 이러한 방식은 중국(50%)과 독일(48%)에서 가장 위협적인 사이버 공격으로 여겨지고 있다. 중국과 독일이 경험한 사이버 사고들과 2023년 3월 보고된 랜섬웨어 증가율(60%)[6] 과 무관하지 않다. 중국과 독일내 기업들은 자사에 적합한 보안 교육 프로그램 개발과 실행에 집중해야 하며, 악성 코드 등의 사이버 공격을 효과적으로 탐지할 수 있는 소프트웨어 도입에 투자해야 한다. 다음으로 디도스 공격(DDoS, 분산 서비스 거부 공격)은 특정 서버(컴퓨터)나 네트워크 장비를 대상으로 많은 데이터를 발생시켜 장애를 일으키는 방식이다. 디도스 공격은 목표 시스템의 리소스를 사기성 트래픽으로 가득 채우고, 결국 시스템을 압도하여 합법적인 요청을 방해하고 시스템 수행능력을 저하시킨다. 이러한 공격은 전세계 모든 지역에서 널리 퍼진 것으로 보고되고 있다. 이번 딜로이트의 조사에서도 싱가포르(36%)와 호주(33%)에서 가장 높은 우려를 나타냈다.

DDoS 공격으로부터 시스템을 보호하기 위해서는 일반적으로 네트워크 트래픽을 스크러빙 센터로 라우팅하거나, 부하 분산 장치를 사용하여 공격 트래픽을 재분배하는 등 악성 트래픽 흐름을 우회 시키는 방법을 채택하고 있다. 하지만 그전에 기업들은 공격에 노출되는 지점을 최소화하고, 대량 트랙픽을 처리할 수 있도록 충분히 확장된 네트워크를 보유해야 할 것이다. 최근 기업들은 DDoS공격에 대한 방어 체계를 강화하기 위해 웹 애플리케이션 방화벽(WAF), 콘텐츠 전송 네트워크(CDN), 보안 정보 및 이벤트 관리 솔루션(SIEM) 또는 엔드포인트 탐지 및 대응(EDR), 네트워크 탐지 및 대응(NDR), 확장 탐지 및 대응(XDR) 등의 기술을 도입하고 있다. 이와 같은 DDoS 방어 솔루션들은 AI를 사용하여 네트워크 인프라에서 비정상적인 트래픽 패턴을 실시간으로 모니터링하고, 공격으로 탐지 시 자동으로 대응할 수 있는 기능(예: 의심스러운 네트워크 연결 종료)을 제공하고 있기 때문이다. 그러나 무엇보다도 간과하지 말아야 할 것은 비 정상적인 트래픽 패턴을 구분할 수 있는 숙련된 인력을 네트워크 관리 업무에 배치하는 것이다.[7]

DDoS공격과 더불어 지능형 지속 공격(APTs) 역시 높은 우려를 보이고 있는 사이버 공격 유형이다. 프랑스(24%)는 글로벌 평균(6%)보다 3배 이상 높은 우려를 나타냈고, 일본(23%)은 다른 국가들보다 5% 포인트 이상 높은 위협의 대상으로 보고하고 있다.

그림 3. 국가별 사이버 공격 유형



출처: Deloitte Center for Integrated Research(2023), N=1,110명, 20개국

사이버 공격 유형

사이버 범죄자들은 여러 가지 정교한 툴과 기술을 사용해 엔터프라이즈 IT 시스템, 개인용 컴퓨터 및 기타 대상에 대한 사이버 공격을 시작한다. 일반적인 사이버 공격의 유형은 다음과 같다.

① 피싱(Phishing)

피싱 공격은 사람들이 공유해서는 안 되는 정보를 공유하거나, 다운로드해서는 안 되는 소프트웨어를 다운로드하거나, 범죄자들에게 돈을 보내는 등 하지 말아야 할 일들을 하도록 유도하는 것을 말한다. 가장 기본적인 피싱은 가짜 이메일이나 문자 메시지를 사용하여 사용자의 로그인 정보를 훔치거나, 민감한 데이터를 유출하거나, 멀웨어를 유포하는 것이다. 피싱 메시지는 합법적인 발신자가 보낸 것처럼 보이도록 설계되는 경우가 많다. 이러한 메시지는 일반적으로 피해자가 악성 웹사이트로 연결되는 하이퍼링크를 클릭하거나 멀웨어를 담고 있는 이메일 첨부 파일을 열도록 유도한다.

② 멀웨어(Malware)

멀웨어는 시스템을 감염시켜 작동 불능 상태로 만들 수 있는 악성 소프트웨어이다. 멀웨어는 데이터를 파괴하거나, 정보를 훔치거나, 운영 체제의 실행 기능에 중요한 파일을 지울 수도 있다.

③ 랜섬웨어(Ramsom ware)

랜섬웨어는 강력한 암호화를 사용하여 데이터 또는 시스템을 인질로 잡는 정교한 멀웨어입니다. 사이버 범죄자는 시스템을 풀어주고 기능을 복원하는 대가로 금전을 요구한다.

④ 서비스 거부 공격(Denial-of-service attacks)

해커가 멀웨어나 서비스 거부 공격(Denial-of-service attacks)을 사용하여 시스템 또는 서버 충돌을 일으킬 수 있다. 이로 인해 발생하는 다운타임은 심각한 서비스 중단과 금전적 손실로 이어질 수 있으며, 데이터 침해 비용 보고서에 따르면, 데이터 침해로 인해 발생하는 비즈니스 손실은 평균 142만 달러에 달한다.

⑤ 데이터 손실위협(Data -loss- related threats)

사용중 데이터(사용 중 데이터: RAM, 캐시 메모리, CPU 레지스터 안의 활성 데이터), 이동 중 데이터(안전한 내부 또는 공개 인터넷 등의 네트워크를 통해 전송되는 데이터), 보관 중 데이터(데이터베이스, 파일시스템, 일종의 백업 스토리지 인프라에 저장된 데이터)의 유출과 손실을 초래하는 사이버 공격을 말한다.

⑥ 지능형 지속 공격(Advanced persistent threats, APTs)

네트워크에 은밀하게 잠복해 있는 사이버 위협, 대부분의 멀웨어는 빠르게 피해를 입히는 공격을 실행하지만, APTs는 이와 달리 보다 전략적이고 은밀한 접근 방식을 취한다. 공격자는 트로이 목마 또는 피싱과 같은 기존 멀웨어를 통해 침입한 다음, 비밀리에 이동하여 네트워크 전체에 공격 소프트웨어를 심으면서 자신의 흔적을 숨긴다. 이렇게 기반을 마련하면 원하던 목표를 달성할 수 있으며, 대부분의 경우 목표는 몇 개월 또는 몇 년에 걸쳐 지속적으로 꾸준히 데이터를 누출한다.

사이버 공격이 비즈니스에 미치는 영향

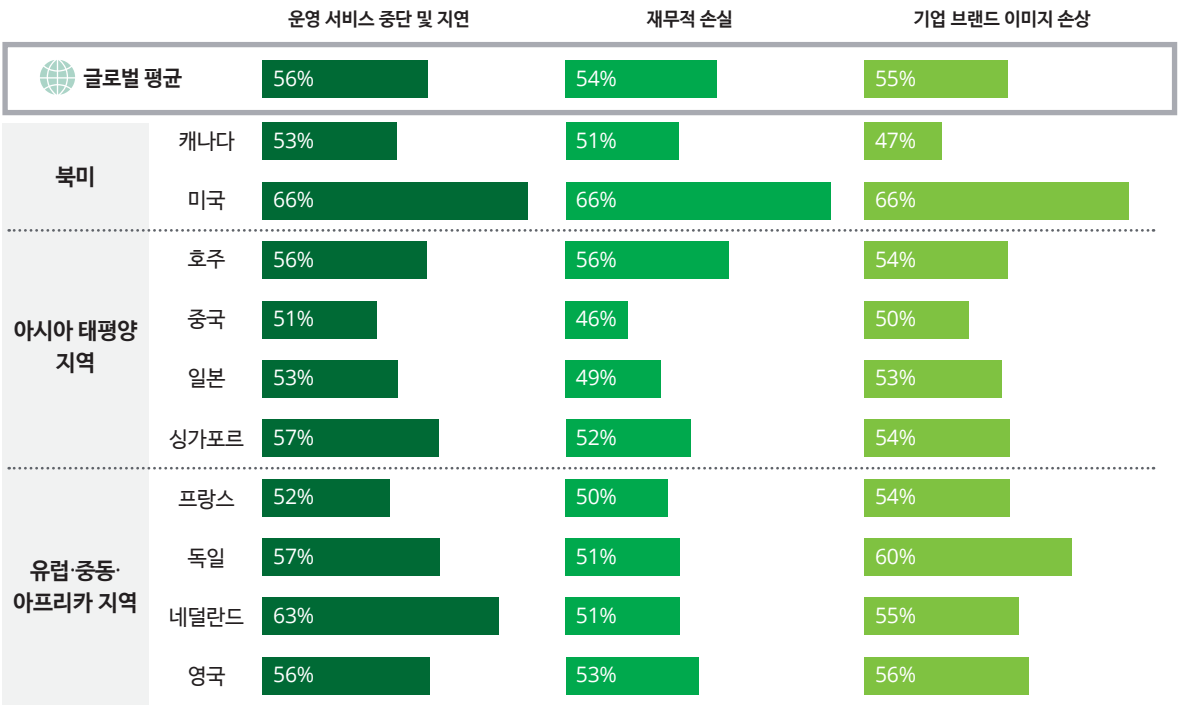
사이버 공격이 기업에 잠재적 위협이 될 수 있고, 모든 프로세스와 운영에 심각한 손실을 초래할 수 있다는 것은 전 세계적으로 공통된 인식이다. 딜로이트의 조사 결과에서도 기업에 대한 사이버 위협은 운영 서비스 중단 또는 지연 발생(56%), 기업의 이미지 손상(55%) 및 재무적 손실(54%) 순으로 높게 나타났다.

미주 지역에서는 미국의 사이버 위협 우려 수준(66%)이 운영, 재무, 브랜드 이미지의 전 부문에서 글로벌 평균을 상회하는 것으로 나타났으며, 유럽 지역에서는 글로벌 평균과 비슷한 수준을 보이고 있지만, 네덜란드는 운영 영역(63%)에서, 독일은 기업 브랜드 이미지(60%) 영역에서 높은 우려를 나타내고 있다. 그리고 추가 분석 결과 조사에 참여한 유럽 지역 기업 중 74%는 사이버 공격으로 '수익손실'과 'IP도난' 을 한 번 이상 경험한 것으로 나타났다.

사이버 공격은 기업의 다차원적인 손실 규모를 넘어 국가의 안보까지 위협할 수 있다 한다. 국가의 주요 인프라 시설과 IT(정보통신)시스템을 일거에 멈출 수 있는 파괴력이 있기 때문이다. 국가 핵심 기반시설에 대한 최악의 사이버 공격으로 2021년 5월에 발생한 '콜로니얼 파이프라인' 랜섬웨어 피해 사건이 실례다. 미 남동부 일대 석유의 45% 이상을 점유하는 송유관업체 콜로니얼의 파이프라인이 러시아 해킹 집단인 '다크사이드'(DarkSide)의 랜섬웨어 공격을 받아 일주일 가까이 멈춰섰다. 이 여파로 7년만에 유가가 최고치를 기록하는 등 미국과 전세계 경제에도 적잖은 충격을 줬다. 독일에서도 2022년 10월, 독일 안할트-비터펠트에서 발생한 랜섬웨어 사건[8]으로 인해 지역 당국은 재난 상태를 선포하고 200일 이상 대민 서비스를 중단 한바 있었다. 이는 독일 최초의 "사이버 재앙"으로 기록되고 있다.

사이버 공격이 축적되면 국가 전체의 경제적, 사회적, 정치적 안정에 영향을 미칠 수 있다. 사이버 공격에 대한 적절한 대응은 기업 뿐 아니라 국가 차원에서도 중요한 과제로 인식되어야 하는 이유이다.

그림 4. 사이버 침해 영역과 손실 정도 (N=1,100명)



출처: Deloitte Center for Integrated Research(2023), N=1,110명, 20개국

사이버 위협 대응 전략

이번 딜로이트의 조사 결과는 기업의 사이버 전략 수립과 목표 설정에 필요한 정보이며, 위협 인텔리전트[9]로써 가치가 있다. 그러나 다수의 기업들은 사이버 공격에 대비한 전략 수립과 실행에 어려움을 겪고 있다. 현재 기업들은 그들이 위치한 지역에서 빈번한 발생하는 사이버 공격 유형을 파악하지 못하고 있고, 이에 대한 회복력 또한 갖추고 있지 않기 때문이다. 기업들은 그들이 위치한 지역과 사이버 대응 수준을 고려한 사이버 전략 수립이 필요하다. 그리고 이러한 전략 방향 하에 역량 평가와 자원 재조정이 이뤄져야 하고, 사이버 투자에 대한 효과성을 확신한 상태에서 과감한 투자가 집행되어야 할 것이다.

딜로이트는 사이버 대응 전략 방향을 다음과 같이 제시했다. 먼저 상시적인 위협 탐지와 사이버 사고 대응 계획 수립에 집중해야 한다. 멀웨어 위협과 APTs 공격이 우려가 높은 국가에서는 네트워크 탐지 및 침입 모니터링으로 알 수 없는 IP와 네트워크 트래픽 급증, 기타 정교한 공격 징후를 탐색에 필요한 솔루션 도입이 필요하고, 이를 통해 잠재적 피해를 최소화해야 한다.

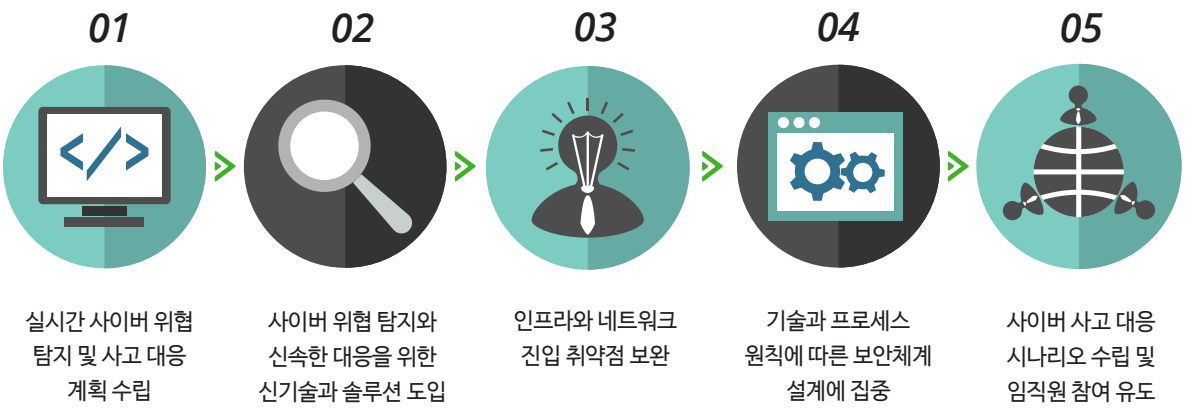
둘째, 사이버 위협 탐지와 신속한 대응을 위한 신기술과 솔루션 도입이 필요하다. 대규모 데이터로부터 사이버 사고 징후를 조기에 식별하고 예방할 수 있는 인공지능 기술 도입이 요구된다.

셋째, 인프라와 네트워크 진입 취약점을 식별하고 보완해야 한다. 네트워크 라우터를 비롯한 인터넷 연결 지점은 공격자의 표적이 되기 쉽다. 지속적인 인프라 유지 보수와 관련 부서 간 협업과 역량 개발이 필수적이다.

넷째 도입 예정인 새로운 시스템/기술과 프로세스 원칙에 따른 보안 체계 설계가 필요하다. 클라우드 도입은 기업에게 사이버 사고 대응 역량과 회복력을 갖추는 데 중요한 요소이다. 클라우드 마이그레이션 단계부터 데이터를 '컨테이너'화하고 피드백 루프가 안전하게 활성화된 상태가 되도록 보안 체계를 설계해야 한다.

마지막으로 사이버 사고 대응 시나리오를 수립하고 사이버 보안교육과 프로그램 실행 시 임직원들의 적극적인 참여를 유도해야 한다. 소셜 엔지니어링 방식의 피싱 공격은 직원들의 부주의와 인식 부족 때문에 빈번히 발생하고 있다. 피싱 교육에 투자하는 시간과 비용을 늘릴수록 임직원들의 사이버 위협 인지 수준을 향상시킬 수 있을 것이다.

그림 5. 사이버 전략 방향 및 우선 실행 사항

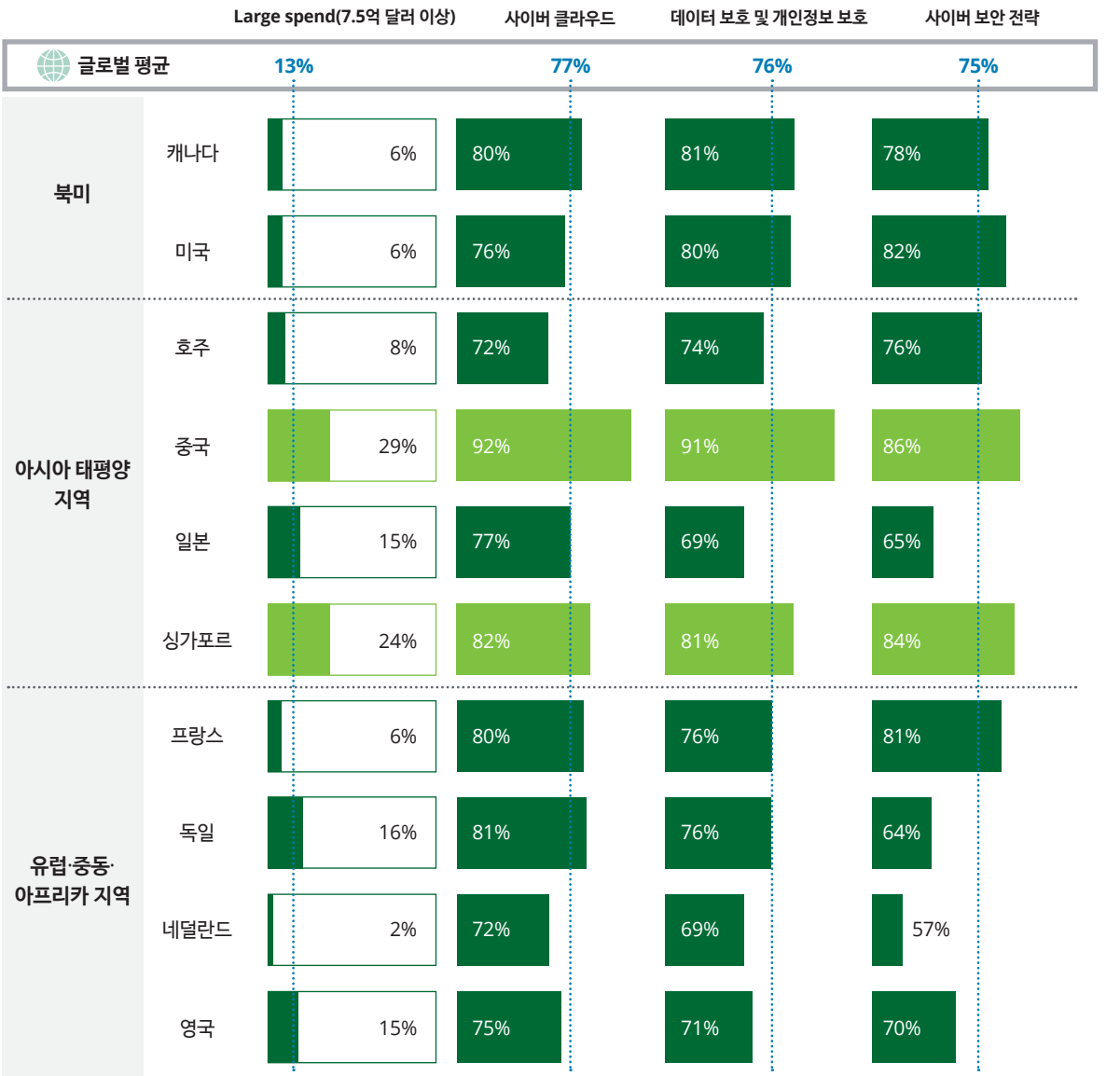


사이버 투자 우선 순위 : 전략, 클라우드, 데이터 및 개인정보보호

전 세계 다수의 기업들의 사이버 투자 방향은 사이버 보안 전략, 사이버 클라우드, 데이터 보호 및 개인정보 보호 분야에 집중되고 있다. 그리고 조사 참여 기업 중 약 13%가 사이버 보안 분야에 연간 약 7.5억 달러 이상(약 9천억 원)의 대규모 투자를 실행하고 있는 것으로 나타났다.

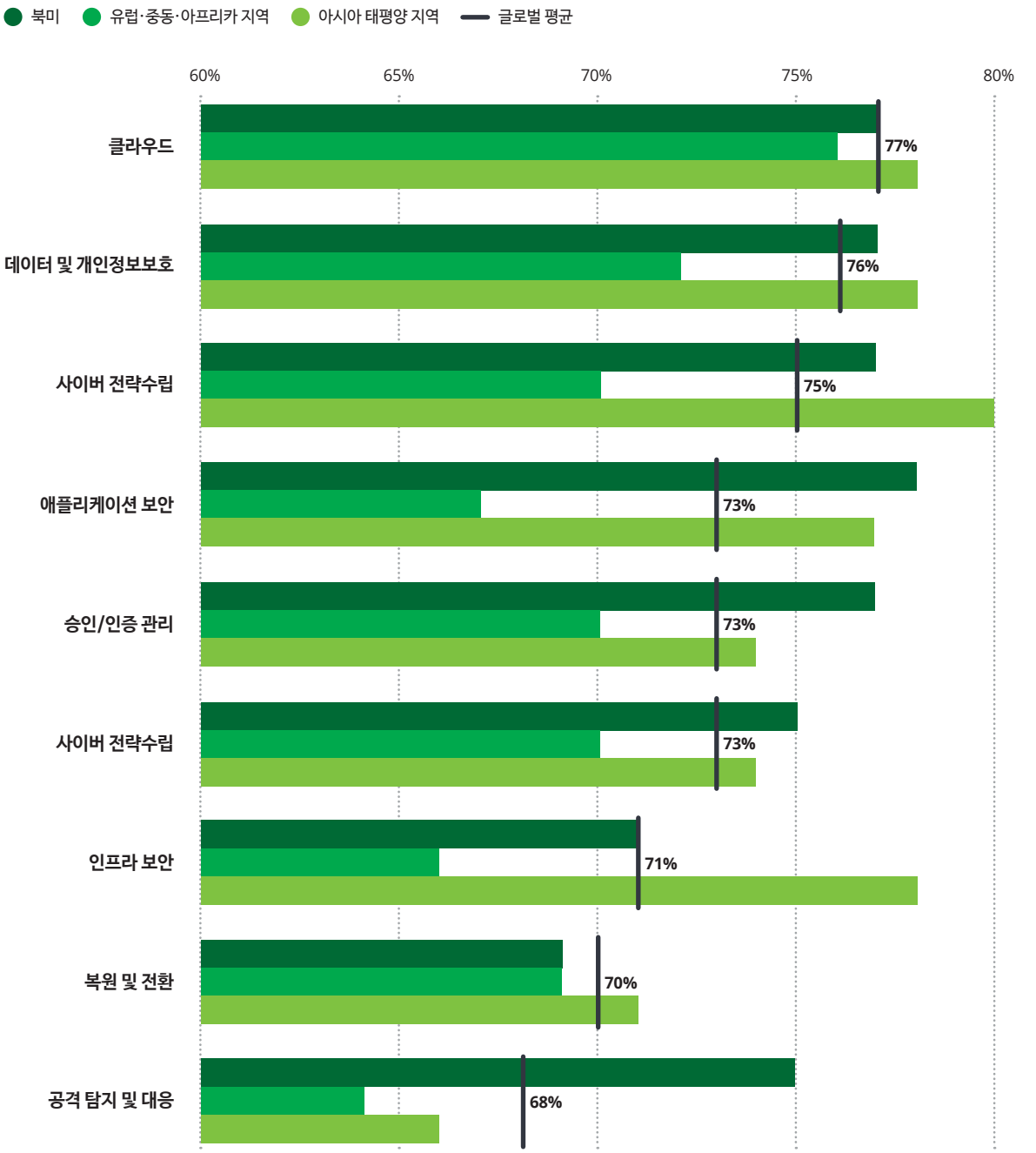
독일(16%)과 영국(15%)제외한 미주와 유럽 지역에 대부분의 국가들에서 대규모 사이버 투자를 실행하는 기업은 10% 미만이지만, APAC 지역에 중국(29%)과 싱가포르(24%)는 글로벌 평균(13%)보다 10%포인트 이상 높은 수치를 보이고 있다. 그리고 이들이 집중하고 있는 주요한 투자 영역은 사이버 클라우드 구축(77%)과 데이터 및 개인정보보호(76%), 사이버 전략(75%)인 것으로 나타났다. 이 결과는 조사에 참여한 기업 전체를 대상으로 도출한 결과와 크게 다르지 않다.

그림 6. 주요 10개국 사이버 투자 규모 및 집중 분야



출처: Deloitte Center for Integrated Research(2023), N=1,110명, 20개국

그림 7. 참여국들의 사이버 투자 집중 분야



출처: Deloitte Center for Integrated Research(2023), N=1,110명, 20개국

APAC 지역은 9개 투자 집중 분야 중에서 8개 부문이 글로벌 평균 보다 높지만, 유럽지역은 대부분 글로벌 평균 보다 낮은 수치를 보이고 있다. 투자 규모가 클수록 사이버 공격 발생 빈도가 낮게 난 것으로(그림1 참조), 사이버 투자의 효과성이 어느정도 입증된 것으로 봐야 할 것이다. 전 세계 기업들은 정교해진 사이버 위협에 직면해 있기 때문에 위치한 지역에 따른 위협 인텔리전스 개발과 관리가 필요하다. 이는 실질적인 사이버 전략 수립과 투자 실행에 필수적인 정보가 되며, 사전에 위협 식별과 사이버 공격시 재무적 위험과 손실을 최소화하는 최후의 보루가 된다.

사이버 위협 대응을 위한 제언

기업은 사이버 전략 실행과 보안 시스템 구축으로 사이버 공격에 대응할 수 있다. 하지만 시스템 의존방식에는 한계가 있다. 기술, 프로세스, 인적자원 요소가 적절히 조합될 때 중요한 시스템과 민감 정보가 보호되고, 기업의 사이버 보안이 실현되는 것이다.

사이버 공격 예방

많은 기업들은 위협 관리 전략을 수립하고 자산과 리소스를 파악하고 보호하고 있다. 그리고 사이버 위협 관리에는 다음과 같은 정책 및 보안 솔루션이 포함될 수 있다.

먼저 최소 권한 액세스, 다중 인증, 강력한 비밀번호 정책을 포함한 ID 및 액세스 관리(IAM) 플랫폼과 운영 정책이 필요하다. 이 정책 실행 시 인증된 인원만 리소스에 액세스할 수 있다. 회사에서는 재택 근무자가 보안되지 않은 Wi-Fi를 통해 중요한 리소스에 액세스할 때 VPN(가상 사설망)을 사용하도록 요구할 수도 있다.

둘째, 종합 데이터 보안 플랫폼 및 DLP(Data Loss Prevention) 툴은 중요한 데이터를 암호화하고 액세스 및 사용량을 모니터링하며 의심스러운 활동이 감지될 때 경고를 표시할 수 있다. 또한 정기적으로 데이터 백업을 수행하면 침해가 발생했을 때 피해를 최소화할 수 있다.

셋째, 방화벽은 위협 행위자가 애초에 네트워크에 침입할 수 없도록 차단하는 데 도움된다. 그리고 방화벽은 명령 및 제어 서버와 통신을 시도하는 멀웨어와 같이 네트워크 외부로 유출되는 악성 트래픽도 차단할 수 있다.

넷째, 사용자에게 보안 인식 교육을 제공하면 사용자가 피싱 및 기타 소셜 엔지니어링 공격과 같은 가장 일반적인 사이버 공격 벡터를 파악하고 피할 수 있을 것이다.

다섯째, 패치 관리 일정 및 정기적인 침투 테스트를 포함한 취약점 관리 정책은 해커가 취약점을 악용하기 전에 미리 파악하고 차단할 수 있을 것이다.

여섯째, 공격 표면 관리(ASM) 툴은 잠재적으로 취약한 자산을 사이버 공격자가 발견하기 전에 파악하고 카탈로그화, 수정할 수 있다.

마지막으로 통합 엔드포인트 관리(UEM) 툴을 사용하면 노트북, 데스크톱, 모바일 디바이스 등 기업 네트워크의 모든 엔드포인트에 대한 보안 정책과 제어를 적용할 수 있다.

사이버 공격 탐지

시이버 공격 시도를 완전히 방지하는 것은 불가능하므로 기업은 지속적인 보안 모니터링 및 조기 탐지 프로세스와 솔루션 도입으로 진행 중인 사이버 공격을 식별하고 플래그를 지정할 수도 있다.

먼저 보안 정보 및 이벤트 관리(SIEM) 시스템은 침입 탐지 시스템(IDS), 엔드포인트 탐지 및 대응 시스템(EDR) 및 기타 보안 솔루션을 비롯한 다양한 내부 사이버 보안 툴의 경보를 중앙 집중화하고 추적할 수 있다.

둘째, 위협 인텔리전스 플랫폼은 보안 경고가 강화되어 보안팀이 직면할 수 있는 사이버 보안 위협 유형을 이해하는 데 도움되며, 바이러스 백신 소프트웨어는 컴퓨터 시스템에서 악성 프로그램을 정기적으로 검사하고 발견된 멀웨어를 자동으로 제거할 수 있다.

마지막으로 사전 예방적 위협 헌팅 프로세스는 지능형 지속 공격(APTs)과 같이 네트워크에 은밀하게 잠복해 있는 사이버 위협을 추적할 수 있다.

사이버 공격에 대한 대응

기업은 진행 중인 사이버 공격 및 기타 사이버 보안 이벤트에 적절히 대응하기 위한 조치를 취할 수도 있어야 한다. 먼저 인시던트 대응 계획이 필요하다. 다양한 종류의 사이버 공격을 차단하고 제거하며 영향을 받는 시스템을 복원하고 근본 원인을 분석하여 향후 공격을 방지할 수 있으며, 사이버 공격으로 인한 전반적인 비용을 절감할 수도 있다.

둘째, 보안 오케스트레이션, 자동화 및 대응(SOAR) 솔루션을 사용하면 보안팀이 반자동 또는 완전 자동화된 플레이북을 통해 서로 다른 보안 툴을 조정하여 사이버 공격에 실시간으로 대응할 수 있다.

마지막으로 확장 탐지 및 대응(XDR) 솔루션은 사용자, 엔드포인트, 이메일, 애플리케이션, 네트워크, 클라우드 워크로드 및 데이터 등 모든 보안 계층에 걸쳐 보안 툴과 운영을 통합할 수 있다. 그리고 XDR은 사전 예방적 위협 헌팅을 비롯해 복잡한 사이버 공격 예방, 탐지, 조사 및 대응 프로세스를 자동화하는 데 도움이 된다.

결과적으로 사이버 공격에 대응하기 위해서는 먼저, 기술(솔루션, 프로그램 등)요소, 프로세스 요소(전략과 거버넌스, 정책, 절차, 프레임워크 등)를 살펴보고, 전체적인 사이버 공격자들의 침투 공백이 있는지 확인해야 한다.

둘째는 인적 자원 요소로 내외부 임직원들의 예방적 보안 수단과 태세를 확인해야 한다. 데이터와 시스템, 환경, 그리고 무엇보다 비즈니스를 보호하기 위한 조치가 마련되어 있는지를 확인하는 것이다.

셋째는지속적으로 환경을 파악하고, 시스템 내에서 일어나는 활동을 로깅하기 위한 적절한 도구를 갖고 있는지, 정상적인 범위를 벗어나는 활동을 분석하기 위한 적절한 분석 방법을 확보했는지를 확인이 필요하다.

마지막은 대처할 준비가 되었는지, 회복력이 있는지 여부다. 사고에 대처하기 위한 프로세스가 마련되어 있는지, 이러한 프로세스와 계획을 사전에 테스트했는지, 경영진을 포함하여 이를 전파할 대상이 누구인지 알고 있는지가 중요하다.

사이버 보안은 한 번 점검하고 문제를 해결하는 식으로 끝나는 과업이 아니다. 매일 확인하고 점검하여, 기업 전사 차원으로 보안 의식을 내재화시켜야 할 것이다. 단순히 기업 내부 자산과 시스템을 조직을 안전하게 보호하는 것이 아니라, 기업 경쟁력을 뒷받침하는 사업적 기능으로 강화해 나가야 할 것이다.

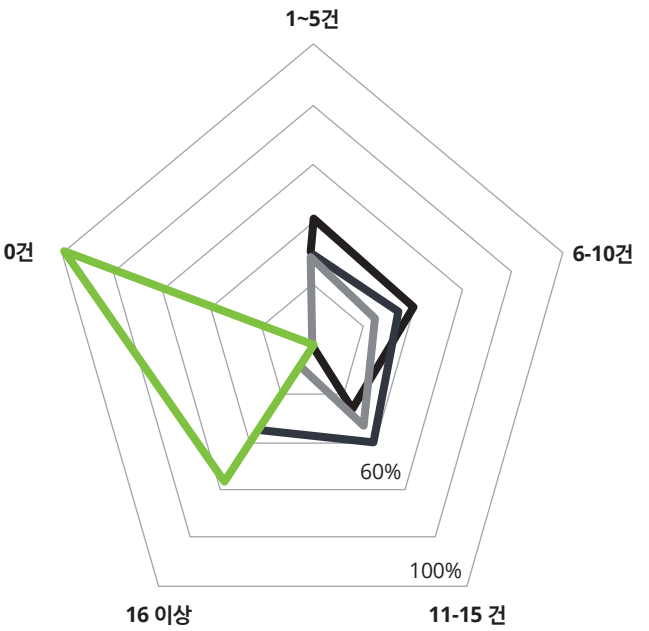
참고

조사 방법론

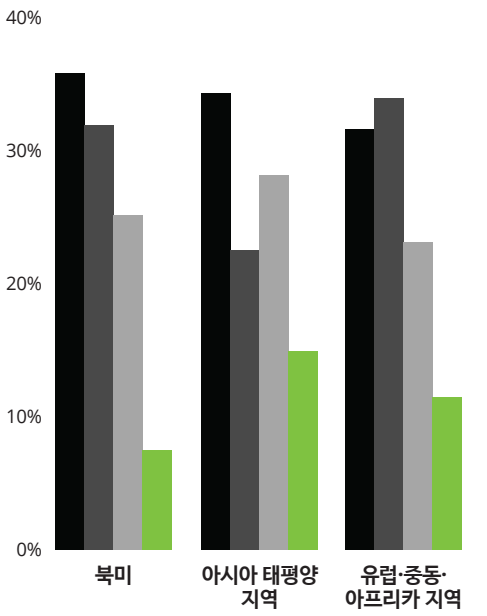
이번 조사는 미주, 유럽-중동-아프리카, 아시아태평양 3개 지역의 사이버 보안 위협 동향과 차이점을 파악하는 것을 목표로 한다. 2022년 9월부터 10월까지 진행된 설문조사에서 1,110건의 응답을 분석했다.

호주, 캐나다, 중국, 프랑스, 독일, 일본, 네덜란드, 싱가포르, 영국, 미국 등 10개 국가를 대상으로 각 국가별 총 응답자 수(40명 이상)와 합리적으로 대표성이 있는 것으로 간주되는 산업별 응답을 분석에 포함시켰다. 이 분석에 나타난 4개의 사이버 사고 프로필 또는 클러스터는 설문조사에서 위협, 행위자, 도구 및 기술, 부정적인 결과의 수에 대한 동일한 4개의 설문조사 질문을 기반으로 한다. 이러한 질문은 요인 분석을 통해 검증된 클러스터를 사용하여 계층적 클러스터 분석에 입력되었으며, 그 결과 도출된 클러스터는 전체 설문조사에서 조사되어 사고와 관련된 사이버 지출 프로필에 대한 추가 인사이트를 제공하고 있다.

작년 사이버 사고 발행 건수
(네 가지 침해 프로파일 클러스터 기준)



지역별 침해 그룹



1: 낮은 사이버 사고, 높은 비용
2: 중간 수준의 사이버 사고, 가장 높은 비용
3: 가장 낮은 사이버 사고, 중간수준의 비용
4:가장 높은 사이버 사고, 가장 낮은 비용

주석

1. DW, “German cybersecurity office issues dire threat warning”, October 21, 2021.
2. SOAR(Security Orchestration, Automation and Response)는 보안 인력들이 보안 오케이스트레이션((Security Orchestration), 자동화(Automation) 및 IT 보안사고 대응(Response)을 지원하는 소루션으로 이를 통해 보안팀은 프로세스를 간소화 하고 사고 대응 프로세스를 가속화 할 수 있다.
3. Barry van Wyk, “China’s cyber crime problem is growing”, The China Project, August 23, 2022.
4. Doug Bonderud, “Why Financial Services Companies Are More Prone to Insider Threats, and What They Can do About It,” BizTech Magazine, September 21, 2021.
5. Staff, “41% of Canadian businesses have laid off staff due to coronavirus: Stats Can,” Benefits Canada, May 1, 2020 ; Tim Keary, “How mass layoffs can create new risks for corporate security,” Venture Beat, April 14, 2023.
6. Vikki Davies, “Cyber insurer reports 60% spike in ransomware in March 2023,” Cyber Magazine, May 18, 2023
7. Amazon Web Services, “What is a DDoS Attack? - Protection and mitigation techniques using managed Distributed Denial of Service (DDoS) protection service, Web Access Firewall (WAF), and Content Delivery Network (CDN)” accessed August 4, 2023.
8. Alexander Martin, “German cyber agency warns threat situation is ‘higherthan ever,” The Record, October 25, 2022.
9. 위협 인텔리전스는 위협 행위자의 동기, 대상, 공격 방식을 이해하기 위해 수집, 처리, 분석되는 데이터를 말한다.

참고문헌

- Deloitte, Cybersecurity threats and Incidents differ by region – How 20 countries and three global regions compare across key threat considerations
- Deloitte, Deloitte Cyber Threat Trends – 2022 Deloitte Global Cyber threat intelligence threat assessment

RISK Advisory [Cyber]

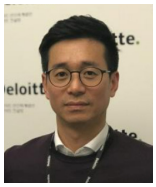
딜로이트 Cyber 서비스는 고객이 복잡한 사이버 위협으로부터 조직의 정보자산을 보호하고 조직의 전략적 성장, 혁신 및 성과 목표를 이룰 수 있도록 지원합니다.

정보보안 전략 수립 및 마스터플랜 수립 / 정보보안 관리체계 고도화 / TPCRM (Third Party Cyber Risk Management) / 정보보안 인증 지원 및 상시 보안 자문: ISMS-P, PCI-DSS, ISO 27001, SOC(System and Organization Controls), Webtrust 등 / 개인정보보호 자문 / 전자서명인증평가 / EVA (External Vulnerability Assessment): 취약점 점검 및 모의해킹 / GDPR (General Data Protection Regulation) 대응 / 침해사고대응 모의훈련 컨설팅 / 사이버 침해사고 분석 및 대응

Contact Point

서영수 파트너
리스크 자문본부 I Cyber
Tel: 02 6676 1929
Email: youngseo@deloitte.com

유선희 파트너
리스크 자문본부 I Cyber
Tel: 02 6676 2956
Email: sunhyou@deloitte.com



이상훈 이사
리스크 자문본부 I Cyber
Tel: 02 6676 2937
Email: sanghunlee@deloitte.com

조성규 이사
리스크 자문본부 I Cyber
Tel: 02 6676 2978
Email: sungkcho@deloitte.com

한호규 이사
리스크 자문본부 I Cyber
Tel: 02 6676 1922
Email: hhahn@deloitte.com

신진환 이사
리스크 자문본부 I Cyber
Tel: 02 6676 4675
Email: jinshin@deloitte.com

이재웅 이사
리스크 자문본부 I Cyber
Tel: 02 6676 2918
Email: jaewoonlee@deloitte.com

김유철 이사
리스크 자문본부 I Cyber
Tel: 02 6676 3076
Email: yuckim@deloitte.com

김용환 이사
리스크 자문본부 I Cyber
Tel: 02 6676 2099
Email: yonghwkim@deloitte.com

앱스토어, 구글플레이/카카오톡에서 '딜로이트 인사이트'를 검색해보세요.
더욱 다양한 소식을 만나보실 수 있습니다.

Deloitte. Insights

성장전략본부 리더
손재호 Partner
jaehoson@deloitte.com

딜로이트 인사이트 리더
정동섭 Partner
dongjeong@deloitte.com

연구원
배순한 Director
soobae@deloitte.com

디자이너
박근령 Senior Consultant
keunrpark@deloitte.com

Contact us
krinsightsend@deloitte.com