대한민국 현황

국가 개요

CISCO

목차

아시아 태평양 지역 개요

개요

보고서 소개

최고 책임자(C-Suite)의 임무는 비즈니스의 성장과 진화를 가속화하는 것입니다. 하지만 모든 디바이스·애플리케이션·사용자·클라우드에 수시로 맹공을 퍼붓는 사이버 위협으로부터 비즈니스를 보호해야 하는 디지털 시대에 과연 최고 정보보호 책임자(CISO)는 이 같은 목표를 어떻게 실현할 수 있을까요.
정보 보안을 책임지는 기업인 Cisco는 회사의 정보보호와 비즈니스 안정성을 지키는 귀하가 최신 현황 및 정보를 통해 보다 정확한 판단과 대응에 나설 수 있도록 돕기 위해 이 보고서를 작성했습니다.

대개 CISO는 관료화된 경직성에 매몰되는 것을 경계하며 비즈니스를 지원하기를 원합니다. 그렇다면 귀하가 조금 더 개방적인 정책을 추구할 경우 어떻게 통제를 완화해야 할까요? 이는 구성원에 따라 달라질 것입니다. 따라서 CISO는 매우 심각한 위협에 대처하면서도 조직문화의 균형을 유지해야 하는 중대한 책무를 갖습니다.

아시아 태평양 지역 11 개국에 걸쳐 100~499명 규모의 조직은 물론 대기업과 공기업에 이르는 약 2000명의 보안 리더들을 대상으로 실시한 설문 조사를 통해 아래와 같이 보안 분야 의사 결정자들이 관장하는 4개 영역에서 데이터를 수집했습니다.

- **사이버보안 문화**
- **보안 경고 및 데이터 침해의 영향**
- **사이버보안 트렌드: 클라우드 및 운영 기술(OT) 위협**
- **벤더 관리에 대한 방어자의 접근법**

각 나라별 보고서에는 이러한 주제 외에도 구체적인 소개자료와 권고사항 섹션이 담겨 있습니다.

아·태 지역 요약은 △2019년 아시아 태평양 CISO 벤치마크 연구에서 도출된 8 가지 흥미로운 사실을 비롯해 △평균 경고 시정과 침해로 인한 다운타임*, 비용 등 주요 트렌드, 그리고 끝으로 보고서에서 약술한 주요 문제에 대처하기 위한 △종합 권고사항 섹션으로 구성되어 있습니다.
이와 함께 보안 환경의 단순화 방안, 이사회로부터 더 많은 투자를 확보하기 위한 전략, 보안 분야 기술격차의 해소방안 등도 소개합니다.

연구를 통해 나타난 가장 흥미로운 8가지 사실

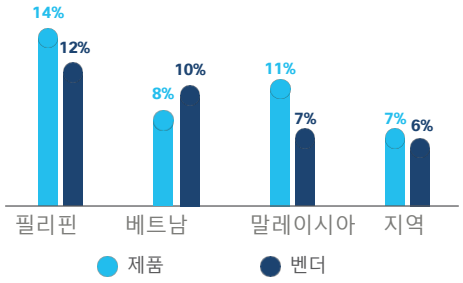
1. 자사 시스템 환경 속 벤더 및 제품에 대한 정확한 현황 파악 부재

보안 팀은 자금력이 있고 끈질긴 적을 상대하고 있으며, 사용자, 애플리케이션, 장치의 정확한 목록을 유지하는 일처럼 절대로 끝날 것 같지 않은 도전에 직면해 있습니다.

그렇기 때문에 팀이 조직을 보호하기 위해 무슨 일이 이뤄지고 있는지 아는 것은 매우 중요합니다. 그래야만 효율성을 극대화하고 헛수고를 줄일 수 있습니다.

다음은 조직 내에서 사용중인 보안 제품 또는 벤더의 수를 제대로 파악하지 못한 사례가 많은 국가들입니다. 해당 지역들이 타국에 비해 보안 환경에 대한 가시성이 낮은 데에는 다양한 원인이 있을 것입니다(조직 내 상이한 팀의 존재, 레거시 이슈 등). 그러나 정직이 최선의 정책이라는 사실을 유념해야 합니다. 당신이 "모른다는 사실"을 인정하는 것은 좋은 출발점입니다. 이를 바탕으로 문제를 해결하기 위해 노력할 수 있기 때문입니다.

도표: 사용하는 보안 제품과 벤더의 수를 모르는 상위 국가

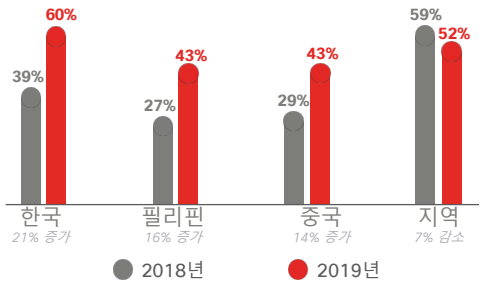


2. 사이버보안 피로 수준 2018년 대비 최대 증가

사이버보안 피로는 방어 진영이 악의적 위협이나 공격자보다 유리한 위치에 서는 것을 사실상 포기하는 것으로 정의할 수 있습니다. 이는 수신하는 보안 경고의 양에 압도된 보안팀이 사전에 효과적인 보안 전략을 수립하는 대신 끊임없이 불을 끄고 있는 것과 같습니다.

다음은 사이버보안 측면에서 힘든 한해를 보내고 피로 수준이 가장 크게 증가한 국가들입니다.

도표: 사이버보안 피로 수준 최대 증가

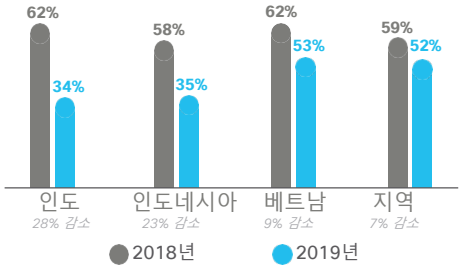


3. 사이버보안 피로 최대 감소

전반적으로 아시아 태평양의 사이버보안 피로 수준은 2018~2019년 사이에 4% 감소했습니다. 일부 큰 폭의 증가가 있었던 것을 감안할 때 이는 적지 않은 성과입니다(위 참조).

다음은 보안 분야 대응에서 가장 긍정적인 행보를 보인 국가들입니다.

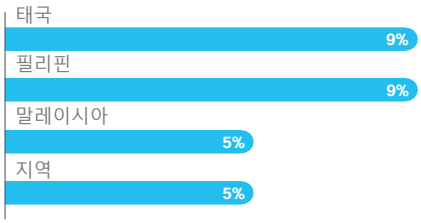
도표: 사이버보안 피로 수준 최대 감소



4. 가장 큰 다운타임 시간 경험

데이터 침해 시 목표는 가능한 신속히 운영을 정상화하고 모든 시스템에서 공격을 완전히 차단하는 것입니다. 다음은 가장 중대한 데이터 침해 후 심각한 다운타임을 경험한 조직의 비중이 높은 국가들입니다.

도표: 5일 이상 다운타임*을 경험한 조직의 비중



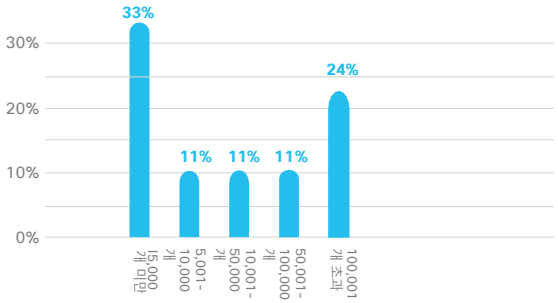
(참고: 각국 보고서에 다운타임 개선과 효과적인 사이버 대응계획 수립을 위한 권고사항이 제시됨.)

5. 일일 보안경고에 대한 실제 조사 횟수 증가

아시아 태평양 지역의 보안 실무자들은 전 세계 다른 지역에 비해 더 자주 보안 경고를 수신합니다.

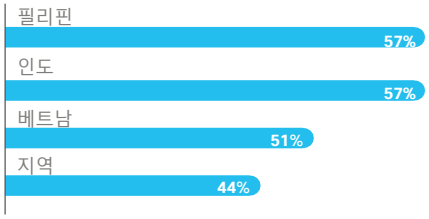
전 세계 응답자 중 49%가 하루에 5,000개 미만의 경고를 수신한다고 보고한 반면(일부 국가는 하루에 500,000개 이상의 경고 수신) 아시아 태평양 지역의 수치는 33%에 그쳤습니다(다만 지난해 평균치인 25%에 비해 크게 개선된 수치임).
대부분의 국가는 매일 5,000개를 훨씬 웃도는 경고를 수신합니다.

도표: 수신한 경고의 지역 평균:



늘 그렇듯 문제는 경고 수신 후 얼마나 대응조사가 이뤄졌느냐에 있습니다. 아태 지역에서 조사가 이뤄진 경고의 비중은 44% 입니다(지난해 대비 12% 감소). 다음은 수신 경고 대비 조사비중이 높은 국가들입니다.

도표: 조사한 경고의 퍼센트가 가장 높은 국가들



6. 유효한 경고에 대한 높은 시정 비중

조사보다 적법한 보안 사건을 완전히 해결하는 것이 더 중요합니다. 아시아 태평양 지역의 평균 시정 수준은 글로벌 평균(43%)보다 낮은 38% 입니다.

2019년에는 조사 중 발견된 적법한 경고의 수가 크게 줄었습니다. 이는 실제 사건이 없다는 점에서 방어자에게는 희소식인 반면 오탐지율이 증가하고 있음을 의미하며, 조사 수준이 감소하는 잠재적 원인이 될 수 있습니다.

다음은 시정 실적이 가장 높은 국가들입니다 (필리핀이 조사와 시정에서 모두 정상에 랭크됨):

도표: 시정된 경고의 비중이 가장 높은 국가들

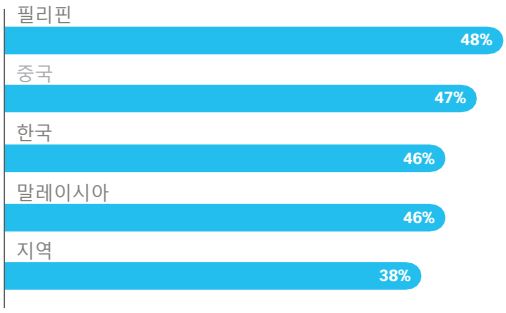
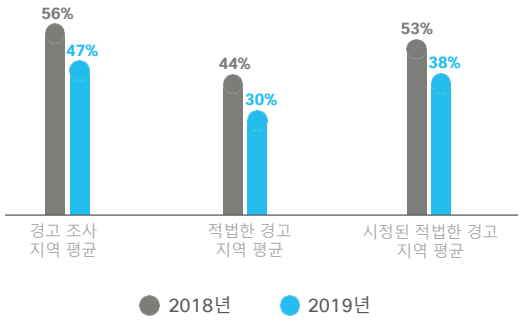


도표: 조사·적법·시정된 보안 경고의 아태 지역 평균 비중 (2018·2019년)

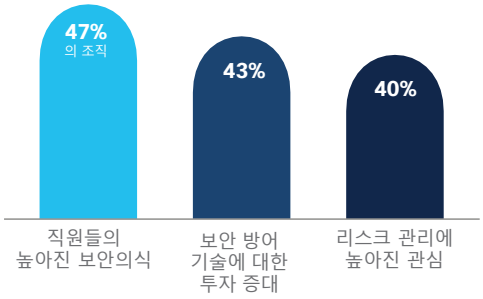


7. 침해사고 후 가장 많이 개선된 영역

아시아 태평양 지역 내 조직들은 지난해 침해사고를 경험한 뒤 상당한 개선을 보였습니다. 가장 뛰어난 성과는 직원들의 높아진 보안의식입니다. 보안 전문팀에 대한 투자와 역량 격차 해소라는 숙제를 안고 있는 아태 지역이라는 점을 감안할 때 상당한 의미가 있습니다. 그 결과 조직들은 일반 직원들의 협조 속에 피싱 및 이메일 스푸핑 공격 시도를 더 효과적으로 방어할 수 있을 것입니다.

또 한 가지 주목할 점은 전세계적으로 가장 크게 개선된(34%) CISO의 고용입니다. 하지만 아태 지역에서 이 같은 전략을 선택한 조직은 24%에 불과합니다. 전략적 역할에 대한 투자보다는 일반 직원이나 보안 도구를 활용한 접근법을 선호하는 경향을 보였습니다. 이는 예산 배정에 영향을 미칠 수 있으며, 이에 대해서는 지역 트렌드 섹션에서 살펴보겠습니다.

도표: 침해사건 후 개선이 이뤄진 3대 영역



8. 가장 다양한 이종 보안벤더를 관리하는 국가

2019년 보고서에 나타난 것처럼, 아시아 태평양 지역의 조직들이 사이버보안과 관련하여 직면하고 있는 문제들(상당한 양의 경고와 다운타임 시간 등)은 주로 멀티 벤더 환경에서 통합의 부재에서 비롯된 것으로 보입니다.

보안 벤더는 제품을 판매하는 것보다 비즈니스를 보호하는 데 관심을 가져야 합니다.

가장 좋은 방법은 보안이 하나의 팀으로 작동하는 것입니다. 실시간으로 소통하고, 서로 배우며, 일심동체가 되어 대응하는 팀이 필요합니다. 엔드포인트 보안은 네트워크 및 클라우드 보안과 연계되어야 하며, ID와 액세스를 관리하는 MFA를 확보해야 합니다. 또한, 플랫폼 접근방식을 통해서만 비즈니스를 보호할 수 있습니다.

이 같은 조건이 충족될 때 더 쉽고 효과적인 보안이 구현될 것입니다.

다음은 멀티 벤더 환경에서 일하는 것이 가장 어렵다고 응답한 국가들입니다. 평균적으로 가장 많은 벤더를 상대하는 국가들과 이 접근법이 더 어렵다고 하는 국가들(변화와 통합의 필요성 시사) 사이에는 상관관계가 있습니다.

도표: 멀티 벤더 환경에서 일하는 것이 가장 어렵다고 응답한 조직의 비중이 가장 높은 국가들

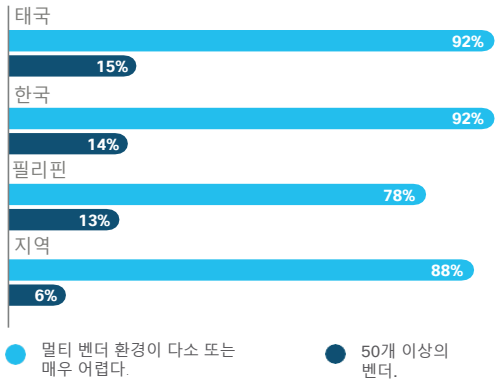
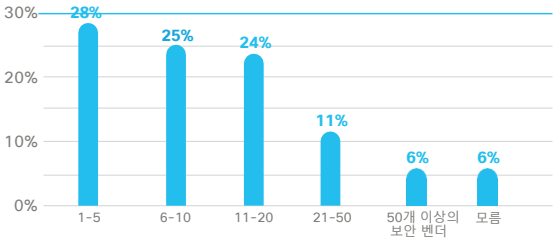


도표: 지역 평균 비율



아시아 태평양 지역 주요 트렌드

1. 클라우드

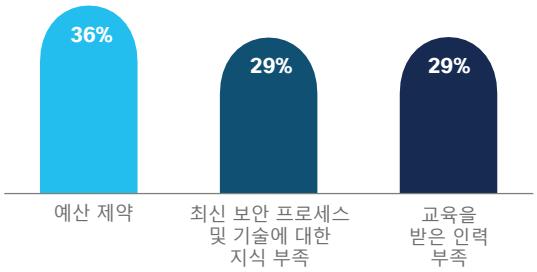
아시아 태평양 국가들은 온-프레미스보다 클라우드에 인프라를 호스팅하는 비율이 더 높은 경향이 있습니다. 아태 지역에서 80~100%의 클라우드 호스팅 비율을 보이는 곳은 16%에 달해 전세계 평균치(9%)보다 높습니다.

조직들이 클라우드 기술을 받아들이는 주된 이유를 묻는 질문에, '사용의 편리성'(52%)이 가장 많은 응답을 보이며 1위에 꼽혔고, '더 나은 데이터 보안'(50%)이 근소한 차이로 뒤를 이었습니다.

2. 고급 보안기술 채택시 최대 걸림돌

사이버보안 활동을 강화하는 데 가장 큰 장애물이 무엇인지 물었습니다. 흥미롭게도 3대 걸림돌로 꼽힌 요인들은 조금씩 악순환의 고리로 연결되어 있습니다. 예를 들어, 최신 도구에 필요한 예산을 확보하기 위해서는 이를 구현할 수 있는 지식, 기술, 그리고 인적자원이 필요합니다. 각 요인들은 아태 지역의 핵심 이슈들로 서로를 규정하는 측면이 있습니다.

도표: 고급 보안기술 채택시 최대 걸림돌



3. 운영 기술(OT) 공격

OT 네트워크는 제조, 유틸리티, 방어 등의 인프라와 조명, 엘리베이터, 냉/난방 시스템 등 주요 시설 운영에 필요한 건물 인프라를 지원합니다. OT 시스템은 이러한 운영의 안전을 모니터링하고 보장합니다. 예컨대, OT 네트워크는 스위치를 모니터링하고 특정 값을 초과하면 중단하도록 할 수 있습니다. OT 시스템은 극히 중요한 인프라를 제어하지만, 역설적으로 노후한 소프트웨어와 하드웨어에서 실행되는 경우가 종종 있습니다. 이 때문에 패치가 힘들고 악의적인 공격에 매우 취약합니다.

NotPetya(일명 Nyetya)는 우크라이나에서 널리 사용되는 회계 소프트웨어인 M.E.Doc의 업데이트를 통해 처음 알려진 멀웨어입니다.
처음에는 기업의 IT 네트워크를 감염시키는 소프트웨어 익스플로잇(취약성 공격)이었지만, 걷잡을 수 없이 확산되면서 기업의 OT 네트워크를 파괴하기 시작했습니다.
NotPetya와 같은 류의 사이버공격이 더욱 우려스러운 것은 OT 네트워크가 중요한 기업 데이터를 수용하는 기업 IT 네트워크와 연결되는 사례가 늘고 있다는 점입니다.

우리는 조직들이 OT공격을 경험한 적이 있는지, 그리고 OT 공격이 향후 더 거세질 것으로 예상하는 지에 대해 물었습니다.

아시아 태평양 조직의 25%는 OT 공격을 경험한 적이 있고, 73%는 이듬해에 증가 추세를 보일 것으로 예상했습니다. 나머지는 사이버공격이 OT가 아닌 IT에 집중될 것으로 내다봤습니다.

이는 OT에 공격이 집중될 것으로 판단한 조직이 50%에 불과했던 지난해에 비춰볼 때 큰 변화입니다.

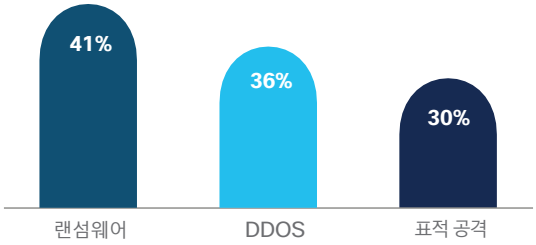
이와 대조적으로 다른 지역에서는 21%의 조직이 OT 공격을 경험한 적이 있다고 응답했고, 64%는 그 다음해에 OT 공격이 증가할 것으로 전망했습니다. 36%는 OT 공격이 증가하는 추세가 아니라고 판단했습니다.

이는 보안 업계가 얼마나 사후 대응적인지를 다시금 일깨워 줍니다. 우리는 공격을 받은 뒤에야 문제를 심각하게 받아들이는 경향이 있습니다. 아시아 태평양 지역의 조직들은 이미 많은 OT 공격을 경험했기 때문에 OT 공격이 증가할 것으로 예상하는 비율도 더 높습니다.

4. 3대 보안 위험

응답자들에게 3대 보안 위험을 물은 결과 물어보았으며, 랜섬웨어(41%), DDOS(36%), 표적 공격(피싱, 이메일 스푸핑 등 · 30%) 등의 순으로 나타났습니다.

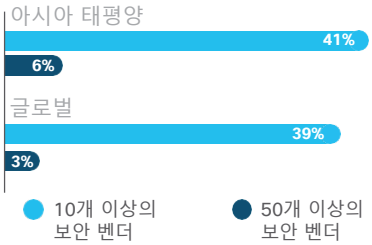
도표: 3대 보안 위험



5. 멀티 벤더 환경 관리

아시아 태평양 지역의 조직들은 다른 글로벌 국가들에 비해 기업마다 조금씩 더 많은 벤더를 관리하고 있습니다. 41%는 10개 이상의 벤더를 관리하고(글로벌 39%), 6%는 50개 이상의 벤더를 관리하고 있습니다(글로벌 3%).

도표: 보안 환경에서 10개 또는 50개 이상의 벤더를 관리하는 조직의 비중(아시아 태평양 및 글로벌)



멀티 벤더 환경을 관리하는 것이 얼마나 힘든지 묻는 질문에 아시아 태평양 국가들이 더 어려움을 겪는 것으로 나타났습니다. 응답자의 83%가 '다소 또는 매우 힘들다'고 답해 다른 지역(79%)보다 높은 수치를 보였습니다. 많은 수의 벤더와 이에 대한 관리 부담 사이에 직접적인 상관관계가 있는 것으로 보입니다.

6. 평균 경고 시정

아시아 태평양 지역 국가들은 전 세계에 비해 경고 조사(44% vs 글로벌 51%), 적법한 경고 시정(38% vs 글로벌 43%) 등 부문에서 뒤처집니다.
이는 지난해 아·태 지역에서 적법한 경고 시정이 53% 였던 것에 비하면 크게 감소한 수치입니다.

7. 다운타임 및 비용

다운타임*은 특히 올해 아시아 태평양 국가에서 많이 발생한 문제입니다. 전 세계적으로 볼 때 심각한 침해가 발생한 후 24시간 이상 다운타임을 경험한 조직은 평균 4%입니다.

아시아 태평양 지역의 경우는 23%입니다. 이 지역의 조직 중 13%가 48시간 이상 다운되었고 5%는 정상 업무가 재개될 때까지 5일이 소요됐습니다.

이는 9%의 조직이 24시간 이상 다운타임을 겪었던 2018년에 비해 급격히 증가한 것입니다.
23%라는 수치는 일부 국가가 한해 동안 엄청난 침해를 받았다는 것을 의미합니다.

이 같은 통계는 결국 침해에 따른 비용이 이 지역에서 더 높다는 것을 의미합니다(비용에는 조사 비용, 수익 손실, 고객 손실, 기회 손실, 직접비 등이 포함됨). 전 세계적으로 33%의 조직이 가장 심각한 침해가 발생한 후 $100,000 미만을 지불했습니다. 아시아 태평양의 경우 24%만이 $100,000 미만 그룹에 속합니다.

중간의 비용구간을 살펴 보면, 다른 지역에서 33%의 조직이 가장 심각한 침해가 발생한 후 $1,000,000 이상을 지불했습니다. 아시아 태평양 지역에서는 이 수치가 37%였습니다.

매우 심각한 침해($5,000,000 이상) 구간의 경우, 이러한 비용을 지불한 사례가 전세계적으로 8%에 불과하지만 APJC 조직은 상대적으로 높은 12%에 달했습니다. 이 구간에서의 높은 수치는 올해 이 지역에서 더 심각한 침해사고를 겪었을 가능성을 방증합니다.

주요 연구 결과에 기초한 7가지 권고사항

1. 단순성 구현

아시아 태평양 지역 국가들이 멀티 벤더 환경에서 겪고 있다고 밝힌 문제들에 대해서는 제로 트러스트(Zero Trust) 접근법을 고려하는 것이 적절할 수 있습니다.

이 접근법은 다음 세 가지 주요 영역에 주목하여 보안을 단순화합니다.

작업 인력(Workforce)
자격 증명 도용, 피싱 및 기타 ID 기반 공격등으로부터 사용자와 장치를 보호합니다.

작업 부하(Workload)
멀티 클라우드 환경을 관리하고 네트워크간 수평 이동을 억제합니다.

작업 공간(Workplace)
사용자와 장치에 대한 정보를 얻고, 위협을 파악하고, 네트워크에서 이뤄지는 모든 연결에 대한 통제력을 유지합니다.

제로 트러스트는 작업 공간을 보호하기 위해 사용자 ID의 신뢰 수준, 그리고 조직에서 업무 수행시 접근권을 정의하는 일에서 시작됩니다.
장치 점검과 사용자 인증 이후 중요한 요소는 어떤 애플리케이션과 경로를 통해 접근해야 하는지, 그리고 어떤 행위가 경계를 넘어선 것인 지 등에 대한 통제와 관리입니다.

제로 트러스트 접근법의 골자는 사용자가 각자의 임무와 관련되고 승인된 영역에만 접근할 수 있도록 제한하는 것입니다. 이 모든 일이 최종 사용자에게 미치는 영향을 최소화하면서 이뤄져야 합니다. 이용시 보안 통제의 영역에서 어려움을 느끼면 이는 곧 기피현상으로 이어집니다.
민첩하고 유연한 접근법의 매력은 장소를 가리지 않고(클라우드, 로컬 데이터 센터 또는 제3자 애플리케이션 등 어디에서 실행되든) 새로운 애플리케이션을 추가할 수 있다는 데 있습니다. 문이 어디에 있든 정책에 따라 중앙에서 열고 닫을 수 있습니다.

2. 기존 보안 도구의 간소화와 복잡성 관리

수많은 조직이 비호환성이 만연한 산업에서 개별 솔루션을 선택할 수밖에 없었습니다. 서로 이가 맞지 않는 제품들을 짜깁기하면서 끝없이 쳇바퀴를 돌리는 격이었습니다. 여기에 수많은 다른 문제(새로운 규정, 이사회의 지시, 예산, 보안 부서의 회전문 인사)가 가중됩니다. 고된 행군은 결코 끝나지 않습니다.

플랫폼은 '단순한 아이디어'가 근간이 되어야 합니다. 보안 솔루션은 하나의 팀으로 작동하도록 설계해야 합니다. 서로 배워야 합니다. 일체화돼 듣고 반응해야 합니다. 이 같은 환경이 구현돼야 보다 체계적이고 효과적인 보안이 가능합니다.

무엇보다 중요한 것은 모든 것을 교체하기 전에 '보유한 것을 활용'하고 모든 역량과자산이 풀어야 할 문제에 투입되도록 해야한다는 점입니다. Cisco는 고객을 보다 효과적으로 보호할 수 있도록 서드파티와의 통합에도 주력하고 있습니다. 불순한 의도의 세력들이 서로 협력하고 연계돼 있는 것처럼 우리도 하나의 산업으로서 똑같은 방식을 추구할 필요가 있습니다. 그렇지 않으면 우리는 언제까지나 해커들의 손과 규칙에 휘둘리게 될 것입니다.

3. 사이버보안 피로 수준 완화

전반적으로 아시아 태평양 지역에서 사이버보안 피로를 겪는 조직은 평균 52%에 달했습니다. 이는 지난해 대비 4% 감소한 수치입니다. 전반적으로 더 나아졌지만, 지난해에 비해 16% 감소한 글로벌 수준(30%)에 비하면 개선 폭은 미미합니다.

한국, 필리핀, 중국 등 일부 국가에서는 피로 수준이 오히려 크게 높아졌습니다.

과도한 피로는 보안 산업에서 상당히 심각한 문제가 될 수 있습니다. 사이버보안 피로를 해소하기 위한 몇 가지 방안을 제시합니다.

1. 교육
조직들은 벤더와 인증 기관이 제공하는 사이버보안 강좌를 활용하여 사내 역량을 강화하고 소속 팀들에게 앞서간다는 자신감을 심어줄 수 있습니다. 현재 Cisco Learning Network는 네트워크가 공격을 받았을 때 긴급 대응 임무를 수행하는 담당자들을 대상으로 새로운 Cisco 사이버보안 전문가 인증을 제공합니다. GIAC(Global Information Assurance Certification)은 보안 전문가가 비인가 접근 또는 네트워크 기반 공격 뒤 남겨진 증거물과 활동을 추출 및 분석하는 새로운 Network Forensic Analyst 인증을 제공합니다.

2. 수동 프로세스의 자동화
이는 멀웨어의 침투가 확산되는 것을 막기 위해 부질없는 숨바꼭질을 계속할 필요가 없다는 것을 의미합니다. 예를 들어, 네트워크 보안 장치는 감염된 컴퓨터를 탐지하고 자동으로 네트워크에서 격리시켜 추가적인 피해를 차단할 수 있습니다.

3. 제로 트러스트 접근법을 통한 오케스트레이션(위 참조)

4. 소프트웨어의 최신 상태 유지
패치되지 않았거나 오래된 소프트웨어는 악의적인 공격자에게 매력적인 공격 지점을 노출하고 보안 팀의 부담을 가중합니다.

4. 다운타임을 줄이는 사이버 대응 계획 수립

침해에 따른 다운타임과 비용을 줄이기 위해서는 이해하기 쉬운 사이버 대응 계획을 수립하고 정기적으로 테스트하는 것이 중요합니다.

다음은 계획 수립시 고려해야 할 몇 가지 팁입니다.

- 업무 지정 – 누가 무엇을 하는가? 분석, 팀/고객/동료들과의 의사소통, 원격 근무 도입 등이 포함된 역할과 책임에 대한 규정이 필요합니다.
- 리더 선정 – 비즈니스와 보안 전략을 이해하고 있는 사람.
- 계획은 최신 위협을 수용할 수 있는 유연성을 지녀야 합니다.
- 원격지에서 복제돼야 할 네트워크의 핵심 컴포넌트를 선정합니다.
- 핵심 팀원의 부재에 대비한 백업 계획을 수립합니다.

기업의 데이터가 인터넷에 노출되면 비즈니스에 어떤 피해가 발생할 지 자문해 보십시오. 다운타임과 평판의 손상에 그칠까요, 아니면 더 큰 비용을 초래할까요.

5. 이사회에서 더 많은 예산을 배정받는 방법

우선 주목할 점은 아시아 태평양 지역은 CISO를 고용하려는 의향이 다른 지역 국가들에 비해 적다는 것입니다. 침해 발생 후 글로벌 수준에서 최고의 개선책은 CISO의 고용이었습니다. 아시아 태평양 지역에서 CISO 고용은 글로벌 평균과 10%의 차이를 보일 뿐만 아니라 가장 적게 선택된 방안 중 하나로 꼽힙니다. 전략적 차원에서 C-Suite(최고 책임자)의 지원이 없으면 보안예산 배정에 차질이 빚어질 수 있습니다.

두번째는 사이버 보안 보고서에 대한 이사회의 불만족입니다. 연구에 따르면 이사회의 약 ¼은 사이버보안과 관련된 보고 수준에 불만을 느끼고 있는 것으로 나타났습니다. 벤치마킹의 부재, 특정 비즈니스가 직면한 위험요인의 불명확성, 보고서의 복잡성과 난해함 등이 이유로 꼽힙니다.

사이버보안에 대한 지원 확대를 요구할 때 가장 유념해야 할 점은 문제를 단순화해 요구사항을 명확히 해야 한다는 것입니다. 개선이 필요한 사항을 명확히 꿰뚫고 있지 못하면 사이버 범죄자들에게 엄청나게 유리한 고지를 내어 줄 뿐 아니라 이사회에서 투자의 당위성을 설득할 수 없습니다.

올바른 사이버보안은 실제로 강력한 경쟁력 우위를 부여합니다. 이제 더 이상 "아무 일도" 일어나지 않도록 하는 것이 목표가 아닙니다. 대신 보안은 기업의 차별화된 경쟁력이 되고 있습니다. "우리는 안전하기 때문에 그 일을 할 수 있습니다." "우리는 안전하기 때문에 클라우드로 확장할 수 있습니다."

다음은 이사회에서 더 많은 예산을 배정받기 위한 방안들입니다.

1 비즈니스와 관련된 사이버 보안의 위험 요인을 구체적으로 명시합니다. 회사가 무미건조한 이력서를 좋아하지 않는 것처럼 이사회도 관련성이 떨어지는 안건 검토를 반기지 않습니다. 당신에게 위험은 무엇을 뜻합니까? 귀사는 성수기에 위험이 따르는 소매업체입니까? 직원들이 섀도우(비승인) IT를 사용할 가능성이 높습니까?

2 동종업계 다른 기업들과 비교하여 벤치마킹하는 것이 중요합니다. 이사회는 전후 맥락에 주목합니다. 위험의 감소 또는 회피는 모든 기업이 원하는 목표입니다.

3 더 좋은 방법은 데이터 침해에 따른 잠재적 비용을 화폐 가치로 환산하는 것입니다. 여기에 관련 법률과 제재에 따른 벌금을 추가하는 것도 잊지 마십시오.

4 사이버 공격의 시나리오(예: 엔드포인트에 대한 랜섬웨어 공격)를 예로 듭니다. 현재의 보안 체계에서 어떻게 공격에 대응하는 지, 그리고 또 어떻게 보안 층위를 구성해 보다 효과적으로 피해를 최소화하는 지 등에 대해 설명합니다. 얼마나 신속하게 대응할 수 있는가? 위협을 인지한 시점은 언제인가? 개선방안은 무엇인가? 그리고 또 멀웨어 제거에 필요한 잠재적 다운타임/비용을 화폐 가치로 제시합니다.

또한 중대한 침해를 계기로 이사회와 논의의 기회를 가질 수 있습니다. 그러한 침해가 어떻게 조직에서 발생할 수 있는지 설명합니다. 그리고 그 취약성의 해결방안을 보여 주세요.

6. 올바른 역량 확보

업계의 분석에 따르면 내년에만 전 세계적으로 200만 명의 사이버보안 전문가가 부족할 것으로 예상됩니다. 이 문제가 해소되지 않으면 2021년에는 그 수치가 350만 명에 이를 수도 있습니다. 보안 위협이 나날이 다양해지면서 여러 분야의 글로벌 사이버보안 인력을 확보할 필요성이 커지고 있습니다.

다음은 지역 전반에 걸쳐 보안 역량을 강화하기 위해 고려할 수 있는 사항들입니다:

1 새로운 인력 확보를 위한 노력이 필요합니다. Cisco Australia는 여성의 사이버보안 분야 합류를 장려하기 위해 호주 전역의 여자 대학생들을 Cisco 멘토(여성 및 남성)와 연결하는 6개월짜리 MentorMe 프로그램을 시작했습니다. 이는 보안분야 종사자로서 우리가 해야 할 역할입니다! 멘토 프로그램은 사이버보안의 다양한 실무 분야에 새로운 인력 유입을 이끌어 낼 수 있는 방법 중 하나입니다.

2 보안 관련 논의가 이사회로 넘어가면 CISO와 그 팀들은 사이버보안 데이터를 분석하는 데이터 사이언스 스킬, 그리고 신뢰 (회사 평판)와 위험 (비용)을 관리하는 비즈니스 스킬이 필요합니다. 새로운 CISO는 전문 기술용어가 아닌 평이한 언어로 소통해야 합니다.

3 보안 전문기술, 인텔리전스 및 혁신적인 신기술에 지속적으로 투자하는 보안 관리 서비스 공급자(MSSP)와 보안 파트너를 이용하는 것을 고려합니다. 이는 역동적으로 변하는 보안위협 환경에 뒤처지지 않는 방법이기도 합니다.

4 기존 인력의 재교육입니다. 2020년 도쿄 올림픽을 지원할 인력교육과 차세대 사이버보안 전문가 육성을 위한 노력의 일환으로, 일본 지역 Cisco 팀은 Cybersecurity Talent 이니셔티브 프로그램을 도입했습니다. Cisco Net Academy Net Academy Net Academy 커리큘럼과 현장 교육 기회를 결합한 이 프로그램은 일본 내 여성 엔지니어링 인력의 확대 및 양성을 위해 힘을 쏟고 있습니다. 이 모델은 현지의 전업 재교육에도 적용되고 있습니다.

부족은 심각해 보이고 여전히 풀어야 할 숙제도 많습니다. 하지만 희망을 가질 만한 이유가 있습니다. 우리가 5년 전에 Cisco Net Academy Cisco Net Academy Cisco Net Academy에서 사이버보안 코스를 개설한 이래 50만명에 가까운 학생들이 교육을 이수했고, 그 중 32%가 지난 1년새 괄목할 만한 관심을 보였습니다. 실제로 FY17 –FY18 회계연도에만 사이버보안 코스에 참가한 학생 수가 238% 238% 증가했습니다 .

7. 직원들의 보안 인식 고취

우리는 종종 보안 측면 에서 가장 취약한 고리는 "사람 "이라는 말을 듣습니다. 이 말이 사실일 수도 있지만, 과장된 묘사일 수도 있습니다. 우리는 매일같이 업무를 수행하고 목표달성을 위해 애쓰는 동안에도 사이버 범죄자들은 손쉽게 우리를 겨누고 있습니다. 아무런 의심 없이 악성 링크나 첨부 파일 클릭을 유도하는 악당들의 수법은 날로 교묘해지고 있습니다. 이제 우리에게 필요한 것은 사람간 상호작용에 파고드는 악당들의 위협과 그 유형에 대한 보다 심도 깊은 이해입니다.

표적 공격은 아시아 태평양 지역 조직들이 꼽은 3대 위험 중 하나입니다. 다음은 피싱과 이메일 스푸핑 등 직원들이 매일 수신하는 공격에 대처하는 방법입니다.

- 긴급한 요구를 경계하세요. 예를 들어, 당신이 어떤 이익을 얻거나 어떤 일을 예방하기 위해 당장 뭔가를 해야 한다고 재촉하는 경우 주의가 필요합니다.
- 지나치게 후한 할인 혜택, 모르는 사람이 보내거나 기대하지 않던 이메일/첨부 파일을 조심하십시오.
- 링크를 클릭하기 전 한 번 더 살펴보십시오. 의심스러워 보이면 대개 문제가 있는 것입니다!
- 직원들이 피싱 공격에 어떻게 반응하는지 평가하는 모의 연습을 수행한 뒤 교육절차를 실행하세요. Duo Security가 제공하는 무료 피싱 평가 도구 Duo Insight는 취약한 사용자와 장치를 수분 내로 찾아내 즉시 보호해줍니다.
- 발신자의 주소를 확인하십시오. 틀린 철자가 있는 지 확인하세요.
- 정책을 강화하십시오. 송금 시 항상 전화를 걸어 확인하십시오. (그냥 반송하지 마십시오. 사기꾼도 그렇게 할 수 있습니다!)
- 이메일 주소에 귀하의 수신 도메인이 포함된 발신자(Mail-From) 및 “friendly from”(From) 헤더가 있는 메시지는 모두 필터링하십시오.

참고:

1. * 다운타임: 가용한 글로벌 데이터 세트는 “24시간”을 초과하는 수준의 세부 정보를 제공하지 않으며 4%의 수치에는 며칠까지 연장되는 데이터가 포함될 수 있습니다.
2. "글로벌(Global)”은 2019년 2월에 발표된 설문조사에 해당합니다. 여기에는 전 세계 18개국이 포함되며, 이 가운데 4개국(호주, 인도, 일본, 중국)이 아시아 태평양 지역에 속합니다. 지역 데이터는 2019년 7월에 이러한 수치에 대한 응답으로 수집되었으며 “글로벌” 수치에 포함되지 않습니다.

대한민국 개요

서론

한국 보고서에서는 두 가지 사실이 주목을 끕니다. 첫째, 사이버 피로를 경험하고 있는 조직의 수가 현저하게 증가했다는 점입니다. 이는 보안위협에 대한 조직의 우위를 잠재적으로 포기한 것과 같습니다. 둘째, 매일 100,000건 이상의 보안 경고가 확인되는 대규모 조직 에서 수신되는 경고의 수가 지난해 3배 이상 증가했습니다.

이는 통합이 되지 않은 멀티 벤더/멀티 프로덕트 환경 때문일 수 있습니다(무려 92% 의 조직이 미흡한 통합에 대처하기 위해 고심중입니다). 이는 한국이 더 긴 다운타임과 더 큰 비용을 지불하고 있음을 의미합니다. 힘겨운 투쟁의 정서가 한국 보안 팀들 사이에 널리 퍼져 있습니다.

긍정적인 측면에서 보면, 매일 막대한 양의 경고를 수신하는 불리한 조건에도 불구하고 한국은 적법한 경고를 조사하고 시정할 수 있다는 점에서 엄청난 발전을 이뤘습니다.

한국의 사이버보안 문화

고급 보안 기술의 채택을 가로막는 장애 요인을 살펴보면, 한국은 고위 간부급이 사이버보안을 우선 과제로 여기지 않는 점을 지적한 비중이 다른 지역에 비해 두드러집니다.

한국에서는 20%의 조직이 이를 중요한 장애 요인으로 꼽았습니다. 이는 가장 많이 언급된 이유는 아니지만, 전 세계 다른 지역과 비교할 때 가장 상반되는 현상 중 하나입니다. 불행히도 한국은 인도네시아와 더불어 보안의 중요성에 대한 인식 제고에 더 많은 노력이 필요한 국가입니다.

표: 조직 내 최신 보안 프로세스 및 기술 채택시 가장 큰 장애 요인

	한국	지역	글로벌
예산 제약	34%	35%	35%
우선순위의 경합	19%	22%	26%
교육을 받은 인력 부족	24%	29%	24%
최신 보안 프로세스 및 기술에 대한 지식 부족	32%	33%	22%
레거시 시스템의 호환성 문제	23%	29%	27%
인증 요구사항	15%	20%	24%
조직 문화/사이버보안에 대한 태도	26%	27%	21%
시장에서 입증되기 전까지 구입을 꺼림	12%	18%	20%
현재의 업무가 너무 과중하여 새로운 책임을 맡을 수 없음	8%	23%	22%
조직이 높은 가치의 공격 표적이 아님	13%	16%	16%
보안이 고위 간부급의 우선 과제가 아님	20%	15%	13%

또 한 가지 주목할 점은 한국에서는 최신 보안 프로세스 및 기술에 대한 지식의 부족이 다른 국가에 비해 훨씬 큰 장애 요인이라는 사실입니다. 이는 결국 보안 교육 예산에 대한 경영진의 지원 부족으로 이어질 수 있습니다.

한국의 조직들에게 사이버보안 피로를 겪고 있는지 물었습니다.

한국의 사이버 보안피로 비율은 전 세계 평균을 크게 웃돕니다(한국 60% : 글로벌 30%).
이는 최신 프로세스를 효과적으로 활용할 수 없다는 좌절감에서 비롯된 것으로 보입니다.
더욱 주목해야 할 점은 사이버 피로를 겪고 있다고 응답한 조직의 비율(60%)이 2018년(39%)에 비해 급격히 상승했다는 것입니다. 한국의 조직들에게 지난 12개월은 쉽지 않았을 것이 분명합니다.

보안 경고와 데이터 침해의 영향

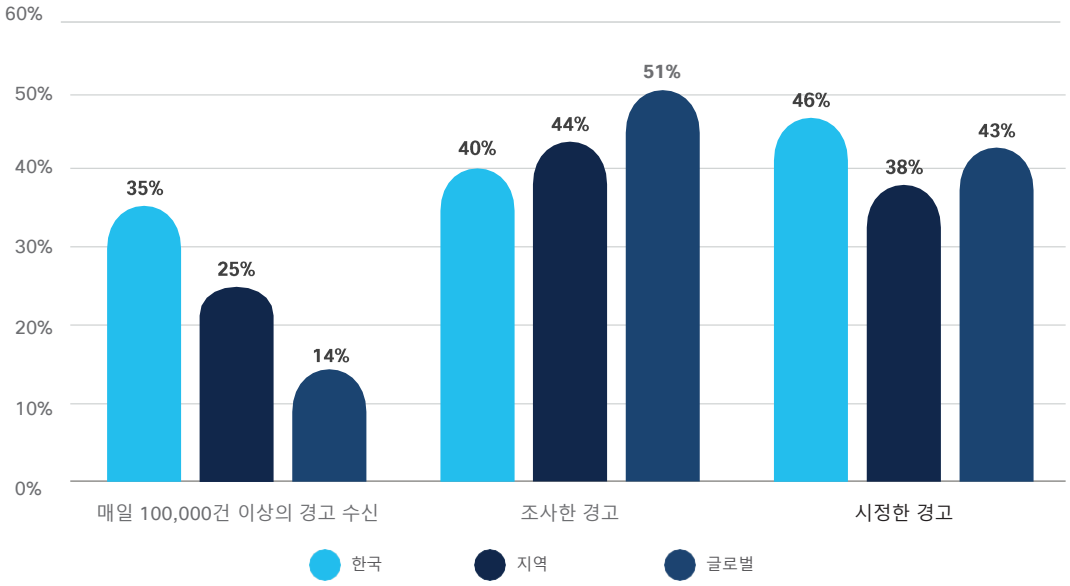
한국은 전체적으로 수신되는 평균 보안 경고량의 2배 이상을 수신합니다. 매일 100,000건 이상의 경고를 수신하는 조직이 35%에 달해 전 세계 평균인 14%와 대조를 이룹니다. 2018년에는 해당 수치가 11%에 불과했습니다. 이는 2019년 사이버 피로가 급격히 상승한 또 한 가지 이유일 수 있습니다.

평균적으로 한국의 조직들은 수신된 모든 경고의 40%를 조사할 수 있습니다. 경고의 양이 급격히 상승한 점을 감안할 때 이는 긍정적으로 볼 대목입니다. 2018년에는 수신 경고량이 더 적었음에도 30%만 조사할 수 있었습니다. 따라서, 보안 경고의 인한 엄청난 도전에도 지난해 한국은 더 많은 사건을 조사하는 놀라운 진보를 이뤘습니다.

적법한 경고의 비중은 글로벌 평균을 약간 밑돕니다. 이는 경고가 적법하지 않은 것으로 간주되기 전 상당량의 오인 판정을 조사하고 있음을 뜻합니다.

한국은 적법한 경고를 성공적으로 시정한 비율이 46%로 글로벌 평균인 43%를 웃돕니다. 매일 평균 이상의 경고를 수신하므로 역시 긍정적인 측면입니다. 시정한 경고의 비율도 2018년 40%에 비해 향상되었습니다.

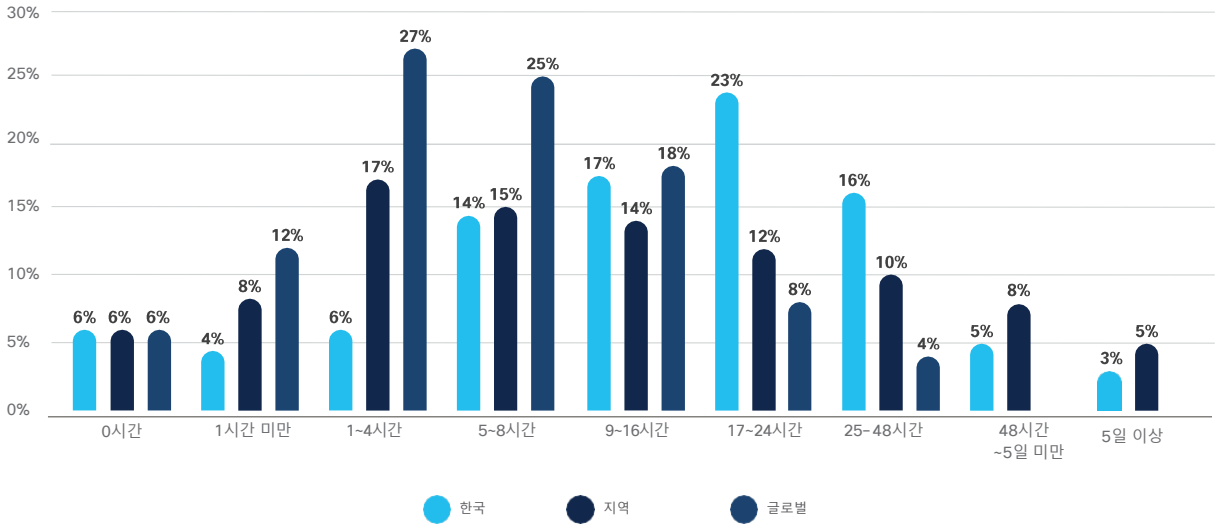
도표: 수신, 조사, 시정된 경고



침해 발생 후 이뤄진 개선 측면에서 볼 때 가장 많이 선택된 개선 사항은 피싱 및 이메일 스푸핑 등의 공격이 네트워크에 침투하기 전 무력화를 위해 직원들의 보안 의식 교육을 강화한 것입니다.

조직이 경험한 가장 심각한 침해가 무엇이고 그로 인해 시스템이 얼마나 오랫동안 다운되었는지에 대해서도 물었습니다. 아·태 지역에서는 다운타임이 다른 국가보다 훨씬 큰 문제이기 때문에, 한국의 조직들에게는 상당히 껄끄러운 결과 일 수 있습니다. 8%의 조직이 48시간 이상 다운타임을 경험하고, 2/3가량(64%)은 심각한 침해 후 9시간 이상 시스템 가동을 중단해야 했습니다.

도표: 데이터 침해 후 다운타임*



클라우드 트렌드

클라우드에 호스팅하는 IT 인프라 비율 측면에서 한국의 조직들은 전 세계 평균과 상당히 일치합니다. 대부분 절반 가량의 인프라를 호스팅하고 나머지 절반은 온 프레미스로 운영합니다.

클라우드를 선택한 이유를 묻는 질문에 한국 기업들이 가장 많이 언급한 이유는 클라우드 기술이 온 프레미스보다 사용하기 쉽다는 점이었고 클라우드가 제공하는 확장성이 그 뒤를 이었습니다.

표: 기업들이 클라우드로 IT 인프라를 호스팅하는 이유

	한국	지역	글로벌
CapEx보다 OpEx 선호	30%	33%	26%
내부 IT 인력 부족	30%	22%	25%
클라우드가 더 강력한 데이터 보안 제공	35%	50%	50%
확장성	37%	43%	40%
규제 준수 요구사항	27%	29%	27%
외부인과의 협업 용이	32%	52%	37%
사용의 편리성	39%	19%	51%
비즈니스에 핵심적이지 않아 아웃소싱 선호	24%	40%	18%
기타	0%	-	1%

한국의 조직들은 다른 국가에 비해 운영 기술(OT)에 대한 공격이 늘어날 가능성에 회의적입니다. 38%의 조직은 다음해에 이런 일이 발생할 것이라고 믿지 않았습니다. 이와 대조적으로 베트남과 태국은 “믿는다”는 비율이 훨씬 더 높았습니다. 이 국가들은 이미 더 높은 비중의 OT 공격을 경험했다는 점에 주목해야 합니다. 이 같은 사실은 다시 한번 보안 산업의 사후 대응적 성격을 보여줍니다. 일부 조직은 너무 늦게 공격에 관심을 보이는 경향이 있습니다.

방어자의 접근법

한국 조직의 56%는 보안 환경에서 10개 이상의 벤더를 이용합니다. 이는 아·태 지역에서 가장 높은 비율 중 하나입니다. 불행히도 멀티 벤더 접근법은 적지 않은 문제점을 노출하고 있습니다. 무려 92%의 조직이 이러한 유형의 환경에서 경고를 조정(오케스트레이션)하는 데 어려움을 겪고 있다고 응답했습니다.

이 같은 애로가 사이버 피로에 영향을 미치는 것은 물론입니다. 권고사항 섹션에서 멀티 벤더 환경에서 통합의 중요성에 대해 살펴 보겠습니다.

권고사항

사이버보안과 관련해 한국의 조직들이 직면하는 수많은 문제들(경고 수, 과도한 다운타임 시간 등)은 주로 멀티 벤더 환경에서 통합이 제대로 이뤄지지 않은 데 따른 것으로 보입니다. 보안 벤더는 제품을 판매하는 것보다 비즈니스 보호에 관심을 가져야 합니다.

가장 좋은 방법은 보안이 하나의 팀으로 작동하는 것입니다. 실시간으로 소통하고, 서로 배우며, 일체화돼 유기적으로 대응하는 팀이 필요합니다. 엔드포인트 보안은 네트워크 보안 및 클라우드 보안과 연계되어야 하며, ID와 액세스를 관리하는 MFA를 확보해야 합니다. 그리고 플랫폼 접근방식을 통해서만 비즈니스를 보호할 수 있습니다. 이러한 요건이 충족되면 보안은 더 쉽고 효과적으로 이뤄집니다.

한국이 안고 있는 또 다른 문제점은 경영진의 지원 부족입니다. 다음은 이사회 수준에서 보안 문제에 대한 인식을 제고하는 4가지 방안입니다.

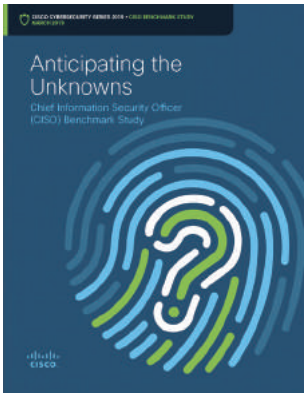
- 비즈니스와 관련된 사이버 보안의 위험 요인을 구체적으로 명시합니다. 회사가 무미건조한 이력서를 좋아하지 않는 것처럼 이사회도 관련성이 떨어지는 안건 검토를 반기지 않습니다. 않습니다. 당신에게 위험은 무엇을 의미합니까? 성수기에 위험이 따르는 소매업체입니까? 직원들이 섀도우(비승인) IT를 사용할 가능성이 높습니까?
- 동종업계 다른 기업들과 비교하여 벤치마킹하는 것이 중요합니다. 이사회는 전후 맥락에 주목합니다. 위험의 감소 또는 회피는 모든 기업이 원하는 목표입니다.
- 더 좋은 방법은 데이터 침해에 따른 잠재적 비용을 화폐 가치로 환산하는것입니다. 여기에 관련 법률과 제재에 따른 벌금을 추가하는 것도 잊지 마십시오.
- 사이버 공격의 시나리오(예 : 엔드포인트에 대한 랜섬웨어 공격)를 예로 듭니다. 현재의 보안 체계에서 어떻게 공격에 대응하는 지, 그리고 또 어떻게 보안 층위를 구성해 보다 효과적으로 피해를 최소화하는 지 등에 대해 설명합니다. 얼마나 신속하게 대응할 수 있는가? 위협을 인지한 시점은 언제인가? 개선 방안은 무엇인가? 그리고 또 멀웨어 제거에 필요한 잠재적 다운타임 비용을 화폐 가치로 제시합니다.

Cisco 사이버보안 시리즈

Cisco는 지난 10년 동안 글로벌 사이버보안의 현황에 관심을 가진 보안 전문가들을 위해 다양한 보안 및 위협 인텔리전스 정보를 발표했습니다. 이러한 종합 보고서들은 위협의 동향, 그리고 조직에 미치는 영향에 대한 상세한 설명과 데이터 침해로 인한 피해방지를 위한 모범 사례를 제공합니다.

새로운 방식으로 사고의 리더십을 추구하는 Cisco 사이버보안 시리즈는 일련의 리서치 기반 데이터 중심 보고서를 발행하고 있습니다. Cisco는 여러 분야에 관심을 지닌 보안 전문가들을 위해 다양한 보고서를 포함하며 발행물을 확대해 왔습니다.
보안 산업의 혁신가 및 위협 연구자들의 깊고 넓은 전문지식이 망라된 2019년 보고서 시리즈에는 데이터 프라이버시 벤치마크 연구, 위협 보고서, CISO 벤치마크 연구 등을 담고 있으며, 올 한해 계속 출간될 예정입니다.

자세한 정보와 보고서의 모든 아카이브 사본을 보려면 다음 사이트를 방문하십시오:
www.cisco.com/go/securityreports



시스코 시스템즈 코리아 Cisco Systems Korea Ltd.
서울특별시 강남구 영동대로 517 아셈타워 5층 (우)06164 5F
ASEM Tower, 517, Yeongdong-daero, Gangnam-gu, Seoul, Korea

Cisco는 전 세계에 200개 이상의 지사를 두고 있습니다. 주소, 전화 번호, 팩스 번호는 Cisco 웹사이트 www.cisco.com/go/offices에 나와 있습니다.

2019년 12월 발행 CISO_01_0319_r1