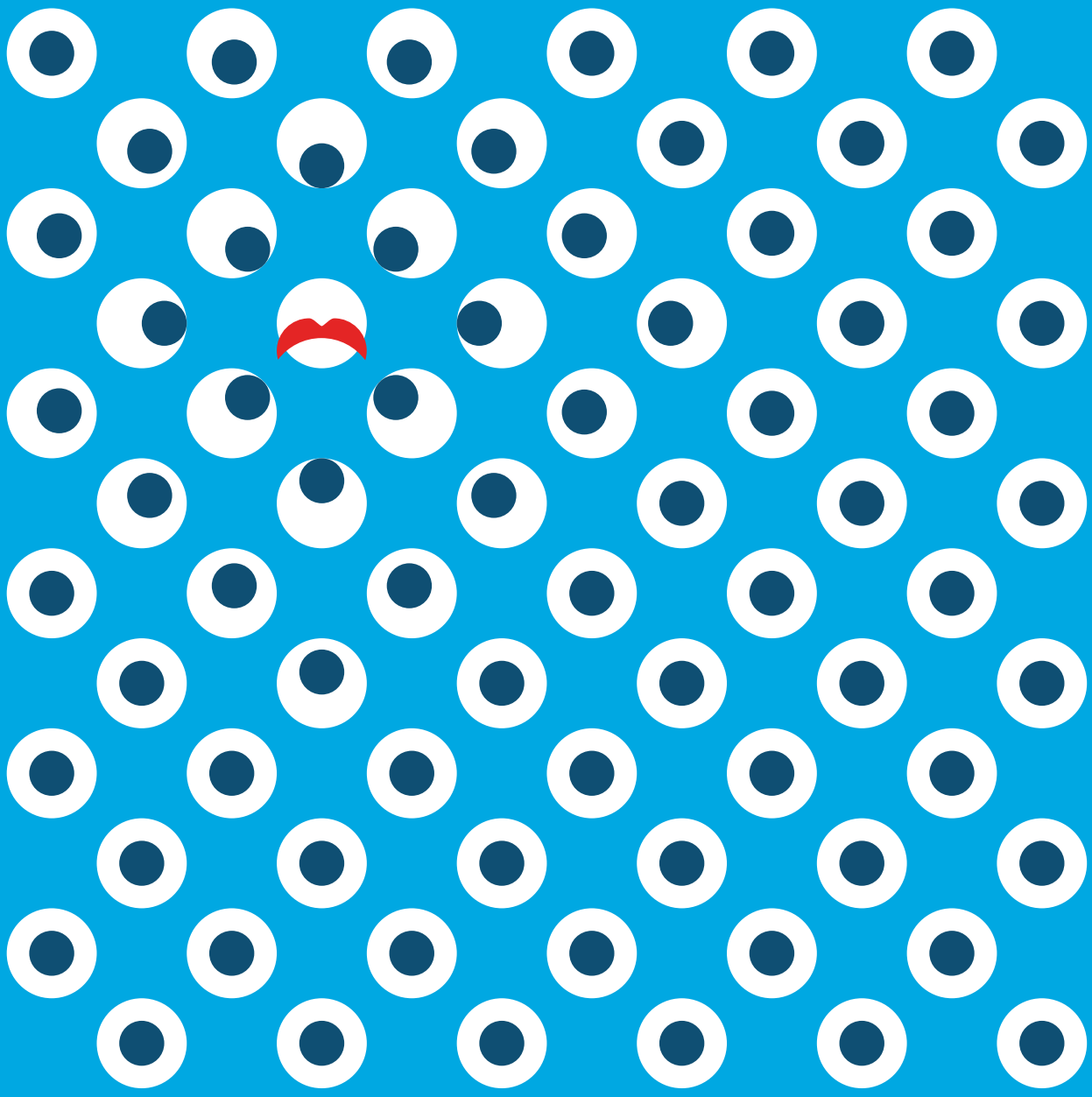

보고서 개요

보고서 개요

아시아 태평양 지역은 디지털 전환이 큰 폭으로 진행되는 흥미로운 지역입니다. 이 지역은 아주 다양한 경제의 본거지이며 미래의 연결된 도시 즉, 스마트 도시 개발을 선도하고 있습니다. 여러 국가들은 이러한 급속한 발전의 혜택을 누리고 있으며, 조직 내에서 사물 인터넷(IoT)이 보편화되면서 작업자들은 원격지에서 유연하게 작업을 하고, 더 많은 기기들이 인터넷에 연결되고 있습니다.

이로 인해 성장과 발전으로 향하는 진입로가 활짝 열린 반면, 기업과 개인을 대상으로 하는 심각한 사이버 보안 위협과 위험도 동시에 발생했습니다. 공격의 수법은 갈수록 정교해지고 첨단 기술을 이용해서 조직을 침해하고 있습니다.

2017년 유례 없는 사이버 공격이 발생했지만, 아직 사이버 보안 대응은 탄탄한 디지털 인프라를 기반으로 하는 것이 아니라, 사후 대응 수준에 머무는 경우가 많습니다. 예를 들어 아시아 태평양 지역의 기업들은 매 분마다 6회의 위협을 받고 있지만 경보의 50%만 조사됩니다.

아시아 태평양 지역 11개 국가의 2,000여 명의 응답자들로부터 보안 실태를 조사 연구한 <시스코 2018 아시아 태평양 보안 역량 벤치마크 보고서> (독립적인 제3자 연구소에서 실시) 는 이 지역의 보안 현황에 관한 통찰을 제공합니다. 동북 아시아의 중국, 한국, 일본, 동남 아시아 지역의 싱가포르, 태국, 말레이시아, 베트남, 필리핀, 인도네시아 그리고 호주와 인도가 포함되었습니다.*

이 보고서에서 시스코는 사이버 보안 사고로 인한 잠재적인 경제적 손실과 방어자들이 해결해야 할 문제와 극복해야 할 도전 과제가 많다는 점을 강조합니다. 시스코의 연구와 통찰은 오늘날 급속도로 진화하는 정교한 사이버 보안 위협에 조직이 효과적으로 대응할 수 있도록 지원하는 것을 목표로 합니다.
이 보고서의 주요 분석 결과는 다음과 같습니다.

1. 사이버 침해

아시아 태평양 지역의 기업들은 매일 10,000건에 달하는 위협을 받고 있습니다. 즉, 매 분마다 6회의 위협을 받는다는 의미입니다. 응답자의 69%는 매일 5,000회 이상의 위협을 받는다고 답변했습니다. 그러나 전체 경보 횟수의 50%만 조사되고 있다고 밝혀졌습니다.

2. 부족한 보안 대응 역량

조사에서 2,000여 명의 응답자를 대상으로 그들이 보유한 디지털 보안 인프라에 관해 질문했습니다. 응답자의 9%는 조직에 사이버 보안 전담 전문가가 없다고 답변했고, 13%는 조직에 사이버 보안을 직접 책임지는 임원이 없다고 답변했습니다.

응답자 중 42%만 경영진이 사이버 보안에 우선 순위를 두고 있다고 답변했고, 44%만이 조직 내의 보안 역할 및 책임에 관해 명확한 명령 체계가 있어야 한다는 데 적극 동의했습니다.

3. 경제적 손실 및 평판 하락

사이버 공격은 기업의 재무적 손실과 평판 실추 등 광범위한 파급효과를 가져옵니다. 동남 아시아 지역의 경우, 전체 사이버 공격의 51%가 1백만 달러 이상의 경제적 손실을 초래했습니다. 10% 에 가까운 응답자는 사이버 공격으로 인한 비용이 5백만 달러 이상이라고 답했습니다. 응답자의 33%는 보안 침해로 인한 비용이 1백만~5백만 달러에 달한다고 응답했습니다.

4. 다각화된 공격

사이버 공격의 형태 또한 변화하고 있습니다. 공격자는 이제 IT 인프라 공격에만 마무르지 않고, 일상적인 사업 기능과 실행에 영향을 미치는 운영기술(OT)을 겨냥하고 있습니다.
조직의 30%는 이미 이와 유사한 사이버 공격을 경험한 반면, 50%는 이러한 추세를 기정 사실로 예상한다고 답했습니다. 이에 덧붙여, 아시아 태평양 지역 응답자의 41%는 운영 인프라가 공격을 받을 경우, 자신들의 업무가 영향을 받을 것이라고 답했습니다.

5. 이해당사자의 철저한 감시 강화

사이버 보안 사고는 조직에게 재무적인 손실을 유발 할 뿐만 아니라, 조직이 고객이나 이해당사자의 신뢰를 얻는 역량도 약화시키고 있습니다, 응답자의 72%는 고객의 개인정보 보호에 대한 우려가 커지면 매출 주기가 길어진다고 답했습니다. 응답자의 거의 절반은 매출 주기가 한 달 이상 지연된다고 답했습니다.

경영진들은 내년에 투자자, 보험회사, 규제기관, 비즈니스 파트너, 경영진, 감시단체, 이익집단, 언론 및 직원 등과 같은 이해당사자의 감시가 더욱 철저해질 것으로 생각하고 있습니다.

*일본, 중국, 인도, 호주 응답자는 2017년에 인터뷰를 마쳤습니다. 싱가포르, 인도네시아, 태국은 2018년 6월, 이 연구의 마지막 단계에 인터뷰를 진행했습니다.

방어자를 위한 권장사항

조직이 불가피하게 사이버 공격을 당할 경우, 방어자는 준비가 되어 있으며, 또 얼마나 신속하게 회복할 수 있을까요?
준비가 되어 있다고 하더라도, 방어자는 전략적인 보안 개선책을 만들고, 모범 사례의 공통점들을 수용한다면, 새롭게 등장하는 사이버 위험에 노출을 줄이고, 공격자의 진행 속도를 둔화시키며, 사이버 위협 환경에 관한 가시성을 높일 수 있습니다.

방어자는 다음 사항을 고려해야 합니다.

- 클라우드 보안 플랫폼처럼 확장 가능한 최전방 방어 도구 구축
- 애플리케이션, 시스템 및 기기 패치에 관한 기업의 정책 및 관행 준수 여부 확인
- 침해 발생 노출을 최소화하는 네트워크 세그멘테이션 실행
- 차세대 엔드포인트 프로세스 모니터링 도구 채택
- 적시에 정확한 보안 위협 정보에 관한 데이터 및 프로세스에 접근하여, 이 데이터를 보안 모니터링과 이벤팅에 통합
- 보다 더 심층적인 고급 도구 활용
- 보안 대응 절차의 검토 및 실행
- 데이터 백업 빈도 제고 및 복원 절차 테스트 진행 – 모든 것이 급변하고 네트워크 기반의 랜섬웨어 웜, 파괴적인 사이버 무기가 만연한 세상에서 더욱 중요
- 공급망에 대한 공격의 위험을 줄이는 데 도움이 되는 보안 기술의 효율성을 제3자 테스트로 진행 검토
- 마이크로 서비스, 클라우드 서비스 및 애플리케이션 관리 시스템에 대한 보안 검사 실시
- 보안 시스템 검토 및 SSL 분석 (가능하면 SSL 복호화 포함) 사용 검토

방어자는 기계학습 기능이나 인공지능 기능이 포함된 고급 보안 기술을 채택하는 것을 고려해야 합니다. 암호화된 웹 트래픽 내부에 악성 프로그램으로 해당 통신을 숨기거나, 악의적인 내부자가 기업 클라우드 시스템을 통해 중요한 데이터를 내보낼 경우, 보안 팀에게는 이러한 악의적 행위를 은폐하는 암호화 기능 사용을 예방하고 탐지할 수 있는 효율적인 도구가 필요합니다.

보고서에 관하여

시스코 2018 아태지역 보안 역량 벤치마크 보고서에는 공격에 대한 조직과 사용자의 방어를 돕도록 고안된 당사의 최신 보안 산업 선진화가 들어있습니다. 당사는 상대방이 저지선을 뚫고 탐지를 피하는 기술과 전략도 검토합니다. 이 보고서는 Cisco 2018 보안 성능 벤치마크 연구의 핵심 사항을 강조하고, 기업의 경계태세와 공격에 대해 방어하는 준비 의식을 검토합니다.