방어의 경제학
THE ECONOMICS OF DEFENSE

증가하는 사이버 위협에 대비하기 위한 보안 투자 모델

JUNIPER NETWORKS

방어의 경제학:
증가하는 사이버 위협에 대비하기 위한
보안 투자 모델

주니퍼 네트웍스(Juniper Networks)가 후원하고 미국의 민간 연구소인 랜드연구소(RAND Corporation)가 진행하는 새로운 연구 주제인 “방어자의 딜레마: 사이버 보안을 위한 과정 수립”은 기업이 방어의 경제적 추진 요인동인과 장애물을 파악하는 데 도움을 주는 최초의 휴리스틱 모델(heuristic model)을 소개합니다.

사이버 공격은 모든 분야의 기업이 직면하는 가장 큰 위협으로 급부상하고 있습니다. 산업 스파이로 인한 지적재산 손실부터 빈번하게 발생하는 대규모 데이터 유출까지, 위협을 극복하고 효과적으로 관리하기 위해 기업이 해야 할 일이 많다는 것은 분명합니다. 이에 따라 기업들은 많은 시간과 에너지, 자원을 집중 투자하여 사이버 공격으로부터 오는 위협을 차단하고 있습니다.

이렇게 초점을 맞추는 것에는 타당한 이유가 있습니다. 지난해 주니퍼 네트웍스가 후원하고 RAND 연구소가 진행한 연구, “사이버 범죄 도구 및 데이터 유출 시장: 해커들의 수입원(Markets for Cybercrime Tools and Stolen Data: Hackers’ Bazaar)”에 따르면 현재 공격자들은 사상 유례없는 수준의 경제적 성숙도를 갖춘 사이버 암시장을 구축했습니다. 실제로 공격자들은 이러한 사이버 암시장을 통해, 기업 네트워크 침투 및 수익 확대에 있어 훨씬 높은 효율성을 확보하고 있습니다. 이 연구에 따르면, 공격 능력이 곧 방어 능력을 앞지를 것이라고 예측했습니다.

> 주니퍼는, 공격자에 대한 경제적 계산이 분명한 반면, 더욱 빈번하고 불분명하며 혼란스러운 환경에 직면하고 있는 기업들의 경우는 그렇지 못하다고 확신하고 있습니다.

보고서 주요 내용:

RAND의 새로운 모델은 본 요약서 및 정식 보고서를 통해 상세히 소개되고 있습니다. 이를 통해 주니퍼는 기업의 사이버 보안 비용에 영향을 주는 5대 주요 추진 요인을 파악했습니다. 각 추진 요인은 현재 기업의 사이버 보안 비용에 막대한 영향을 미치거나, 향후 그러할 것으로 예상되고 있습니다.

1. 보안 솔루션에 왕도는 없다: 모든 상황에 적용 가능한 솔루션은 없는 가운데, 기업은 최적의 투자 전략을 취하고 있지 않음
2. 많은 보안 툴에는 툴 반감기가 있으며, 그 가치가 하락 할 위험이 있음
3. 인적 자원에 투자하는 것이 장기적인 비용 절감을 가져옴
4. 기로에 선 사물 인터넷(IoT: Internet of Things)
5. 소프트웨어 취약점을 제거하면 비용을 크게 절감할 수 있음

보안 업계의 많은 종사자들은 경험을 통해 이러한 추진 요인들을 보안 프로그램의 일부로 고려해야 한다는 것을 알고 있었으며, RAND의 연구에서 처음으로 이러한 비용에 대한 추진 요인의 영향을 정량적으로 모형화했습니다.

이렇게 만들어진 새로운 모델을 통해 데이터 기반 인사이트를 제공할 수 있으며, 각 추진 요인의 중요성과 기업의 전략적이고 종합적인 보안 위험 관리 방법에 대해 이해할 수 있습니다.

방어자의 딜레마

방어자의 경제적 상황을 살펴본 RAND의 새로운 연구 조사를 통해, 최고정보보안책임자(CISO)가 보안 시스템의 안정성에 대한 확신 없이 투자를 늘리는 것은 미봉책에 불과하다는 사실을 알 수 있습니다. 더욱 심각한 사실은 CISO들은 공격자들이 방어자를 빠르게 공략하고 있다고 보고 있으며, 많은 경우 보안에 충분히 투자하고 있는지, 혹은 언제 충분히 투자했는 지 확신이 없다는 것 입니다.

이러한 현상은 많은 기업들과 보안 업계 자체가 사이버 보안을 기업이 직면하는 위험으로 올바르게 인지하지 못한다는 사실에 기인하고 있습니다. 사이버 보안 업계에서는 종종 리스크 관리에 대해 잘못 이해하는 경우가 발생하고 있습니다. 사업 결과 및 운영에 대한 리스크 보다는 위협과 취약성으로 인해 발생하는 리스크에 초점을 맞추고 있습니다. 대다수의 경우 보안에 있어 강조하는 부분을 비롯해 보안 프로그램의 가치를 입증하는 지표조차도 비즈니스적인 측면보다는 공격을 차단하는 특수 도구나 프로그램의 성능에 초점을 맞추고 있습니다.

종합 보안 프로그램은 차단된 공격의 규모를 측정하는 대신, 리스크 관리에 대한 투자 수익이나 RROI(투자에 대비 리스크 감소)를 파악하는 데 목표를 두어야 합니다. 즉, 사이버 보안 리스크의 총 비용에 가장 큰 영향을 주는 요소들과 이를 더욱 효율적으로 관리할 방법을 찾아야 합니다.

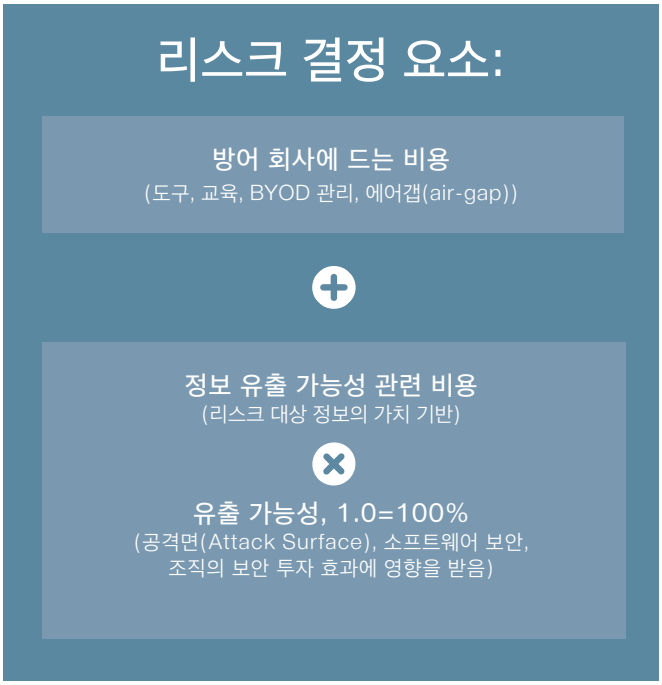
주니퍼 네트웍스는 조직의 사이버 보안 리스크 비용에 영향을 주는 주요 요소를 파악하고자, RAND의 경제 학자와 보안 전문가를 통한 연구를 실시했습니다. 또한, 본 연구를 통해 증가하는 공격 위협으로 인한 명성, 정보 및 네트워크에 대한 리스크를 더욱 효과적으로 관리하기 위해 조직이 어떠한 분야에 투자해야 하는지도 조사했습니다.

RAND는 건강 관리 지출 통제부터 국가 안보 분쟁 및 국방비 지출 처리에 이르기까지, 현재 직면하고 있는 까다로운 문제들을 극복하는 데 필요한 객관적 분석자료와 판단능력을 제공해온 경험을 가지고 있습니다. 기업의 사이버 보안 비용과 관련 현안을 검토함으로써, 보안 부서 및 담당자는 조직이 직면한 문제를 파악하고 이를 처리하기 위한 보안 제품군을 마련하는 데 있어 더욱 확실한 근거를 얻게 됩니다.

기업 보안 리스크 관련 휴리스틱 모델

RAND 연구의 초점은 보안 리스크 관리 비용과 함께 다양한 투자 결정에 영향을 주는 주요 요소를 더 잘 이해하기 위한 학습 도구를 기업에 제공하는 최초의 휴리스틱 모델(heuristic model)을 개발하는 것이었습니다. 이러한 요소의 상호 작용을 관찰함으로써, 본 모델은 사이버 보안 솔루션을 선택하는 데 필요한 다양한 시각을 형성하는 기본 틀을 제공합니다.

OCTAVE(Operationally Critical Threat, Asset and Vulnerability Evaluation), FAIR(Factor Analysis of Information Risk) 등 이미 존재하고 있는 보안 리스크 모델은 기업이 직면한 구체적 리스크와 우선적으로 보호해야 하는 정보를 평가하는 데 도움을 주고 있습니다. 반면, RAND의 모델은 사이버 보안 리스크를 관리하는 데 필요한 종합적인 비용을 체계적으로 보여주는 최초의 기본 틀입니다. 본 모델은 새로운 기술과 공격자의 활동을 소개하며 기업의 의사 결정 과정 등을 관찰해 사이버 보안 비용과 관련된 모든 상호작용 및 영향을 보여줍니다.



RAND의 모델은 리스크를 종합적으로 파악하기 위해 조직이 총 사이버 보안 비용을 최소화하는 데 사용하는 방법을 조사합니다. 여기에는 사이버 공격을 방지하기 위한 조직의 직·간접 비용은 물론, 공격으로 인한 잠재적인 손실, 공격 대상이 되는 정보의 가치와 공격 성공 가능성 등이 포함됩니다.

> RAND의 모델은 사이버 보안 리스크를 관리하는 데 필요한 종합적인 비용을 체계적으로 보여주는 최초의 기본 틀입니다

RAND의 모델은 10년 동안 조직의 비용에 영향을 준 27개 변수가 포함되어 있으며, 이를 조정함으로써 각각의 변수가 비용에 미치는 영향을 볼 수 있습니다.

일반적으로 변수는 다음과 같은 3가지 카테고리로 분류됩니다:

1. **조직적 특성: 조직의 규모, 네트워크 내 컴퓨터/디바이스의 갯수, 리스크 대상 정보의 가치.**
2. **보안 프로그램 및 투자: RAND 모델을 통해 기업은 아래 4가지 요소의 사용 여부를 결정할 수 있습니다. 각각은 비용이 발생되지만 공격으로부터 피해를 받을 가능성을 줄여 줍니다:**
   - 보안 도구 구매 및 사용 관련 직접비
   - 직원 대상으로 위협 관련 교육을 실시하기 위한 직간접비
   - 스마트 디바이스 제한과 민감한 서브네트워크의 에어갭(air-gapping)에 따른 잠재적 생산성 손실로 인한 간접비
   - 보안 프로그램을 집행하는 보안 담당자의 성실성
3. **생태계 변화:** 보안 비용은 향후 기술 생태계의 변화에 따라 달라질 수 있습니다. 예를 들어, 사물인터넷(IoT) 디바이스가 도입되면 공격면이 변화될 수도 있습니다. 또 특정 연도에 도입된 소프트웨어의 취약성을 이용한 공격과 그로 인한 비용 발생 등이 보안 비용에 영향을 미칠 수 있습니다.

주니퍼는 본 모델이 CISO가 조직을 보호하고 더 넓은 시각으로 사이버 보안 제품군을 선택하는 데 다양한 결정을 내릴 수 있게 돕는 체계적인 출발점이 될 수 있다고 생각합니다.

> 이 모델은 CISO가 조직을 보호하고 더 넓은 시각으로 사이버 보안 제품군을 선택하는 데 있어 다양한 결정을 내릴 수 있게 돕는 체계적인 출발점 입니다.

주니퍼는 기업들이 다양한 변수를 조직에 적용할 수 있게 하는 양방향 해석 모델을 마련했습니다. 이를 통해 사용자는 비용에 가장 큰 영향을 주는 주요 변수를 파악하고, 기업이 실행 시 고려해야 하는 보안 투자의 적절한 조합을 결정할 수 있습니다.

각 기업마다 직면하고 있는 니즈와 문제점이 다르기 때문에 RAND 모델은 진단보다 방향성을 제시해주고 있습니다. 그러나 본 모델은 조직 내에서 더 많은 지원을 확보해야 하는 보안 전문가에게는 강력한 출발점이자 근거가 될 수 있습니다.

모델을 총체적으로 파악하고자 하는 기업 및 정책 입안자를 위해 RAND 정식 모델의 방법론이 정식 보고서에 부록으로 제공됩니다.

사이버 보안 리스크 관리를 위한 경제적 고려 사항

본 모델은 사이버 공격 비용과 조직의 보안 지출 사이의 역학 관계를 나타냅니다.

비용은 다음의 모든 요소를 고려해 결정됩니다:

사이버 공격으로 인한 손실 + 사용자 교육 직접비 + 도구 구매 및 사용 관련 직접비 + BYOD/스마트 기기 사용 제한에 따른 간접비 + 민감한 서브네트워크 에어갭(air-gap)으로 인한 간접비

사이버 공격으로 인한 손실

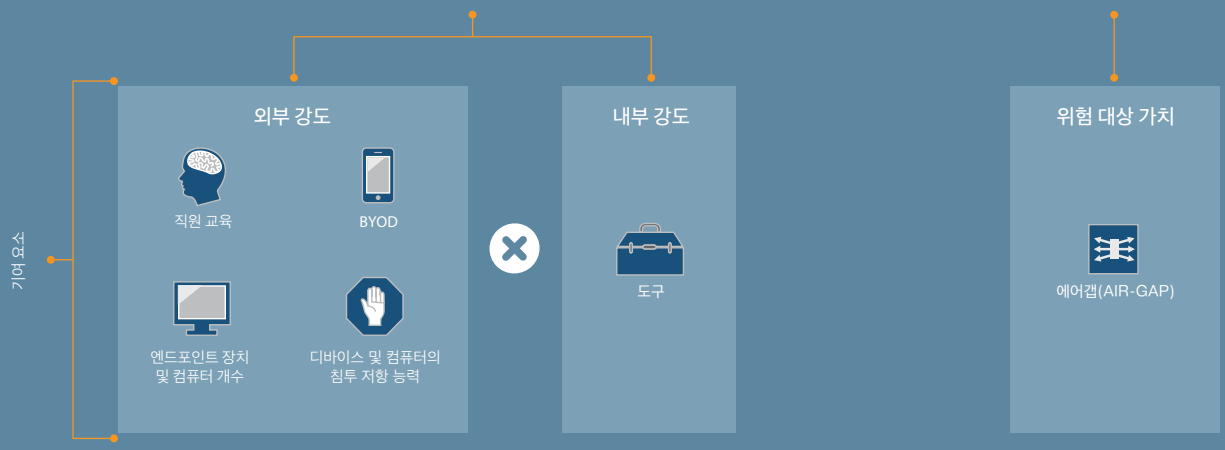
공격 가능성

모델에서 해당 연도에 조직이 공격에 의해 피해를 입을 가능성은 조직의 외부 강도와 내부 강도의 결과에 따릅니다.

×

공격 영향

공격의 영향은 공격자가 권한을 확보한 정보의 가치에 따라 결정됩니다.



시간에 따른 변화:

- 컴퓨터 및 디바이스의 개수 및 취약성
- 사이버 공격과 관련된 손실의 변화
- 새로운 사이버 보안 도구 도입
- 대응 방법의 출현에 따라 일부 도구의 효과 감소

2015년을 0년차로 가정해 해당 연도에 대한 계산을 진행했으며 향후 10년에 대해 각 연도별 반복 계산을 실시했습니다.

0년차 ——— 10년차

JUNIPER NETWORKS

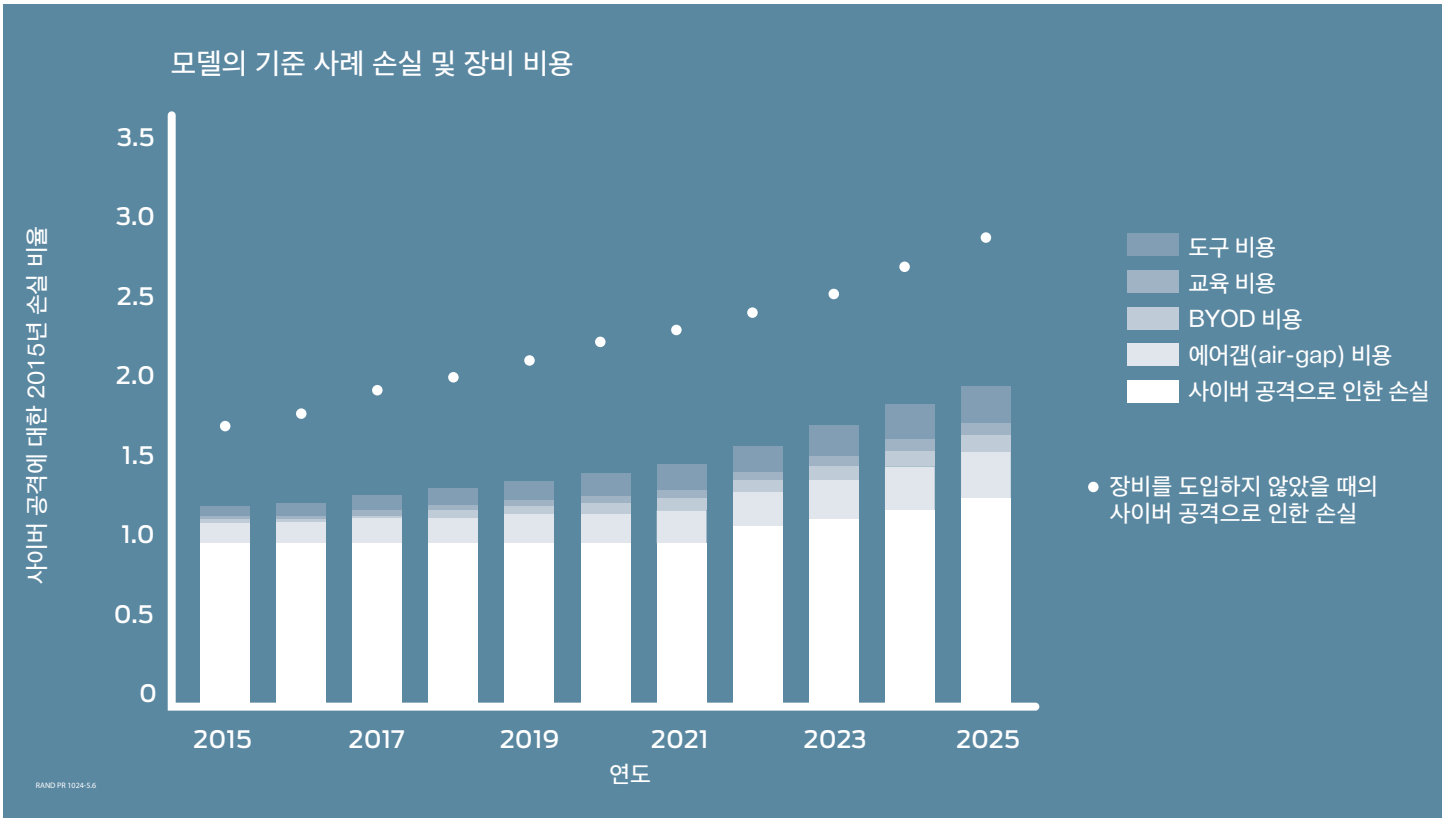
휴리스틱 모델을 통해 살펴보는 보안 과정

모델의 작동 원리보다 더 중요한 것은 모델이 제공하는 인사이트입니다. RAND의 보고서는 본 모델을 사용하여 기준선 사례를 상세히 설명하며, 전사적 비용과 함께 모델이 적용된 10년 동안의 비용 변화를 검토합니다.

RAND의 모델은 향후 10년 동안 모든 기업의 사이버 보안 리스크 관리 비용이 38% 증가할 것으로 전망합니다.

> 향후 10년 동안 모든 기업의 사이버 보안 리스크 관리 비용이 38% 증가할 것입니다.

흥미로운 점은 대부분의 비용 증가 원인은 사이버 공격으로 인한 손실 증가가 아니었습니다. 오히려 기업의 잠재적인 손실 관리에 있어 도구 및 교육 투자, 개인 장비 사용(BYOD)/스마트 디바이스 제한 및 네트워크 에어갭(air-gap)과 같은 보안 프로그램의 비용 증가가 그 원인으로 작용했습니다. 그러나 이 비용에 투자하지 않았을 때 발생할 수 있는 손실이 더욱 크고 증가 속도도 빠르기 때문에, 궁극적으로 보안에 투자는 비용 효과적입니다. 아래 차트에서 점선은 기업이 네트워크 보호에 투자하지 않았을 때의 손실을 보여줍니다.



최고정보보안책임자(CISO)를 위한 주요 비용 요소

RAND의 모델은 기업에게 가치있는 인사이트도 제공합니다. 주니퍼는 기업이 보안 태세를 발전시켜 나갈 때 고려해야 할 5가지 비용 요소를 RAND 모델이 확인했다고 봅니다. 이러한 요소들은 보안 분야의 많은 사람들에게 경험적으로 사실이라고 알려져 있지만, RAND 모델이 이들의 강력한 경제적 영향력의 중요성을 확인해줍니다.

1. 보안 솔루션에 왕도는 없다: 모든 상황에 맞는 솔루션은 없으며, 기업은 최적의 투자 전략을 취하고 있지 않음

RAND의 연구는 많은 기업들이 최적의 경제적 전략을 사용하여 투자를 하는 방향으로 가지 않을 것으로 보고 있습니다. 최적의 보안 도구 개수, 직원 교육, 개인용 디바이스 제한, 인터넷에서 분리해야 할 네트워크 결정 등은 회사마다 크게 다릅니다.

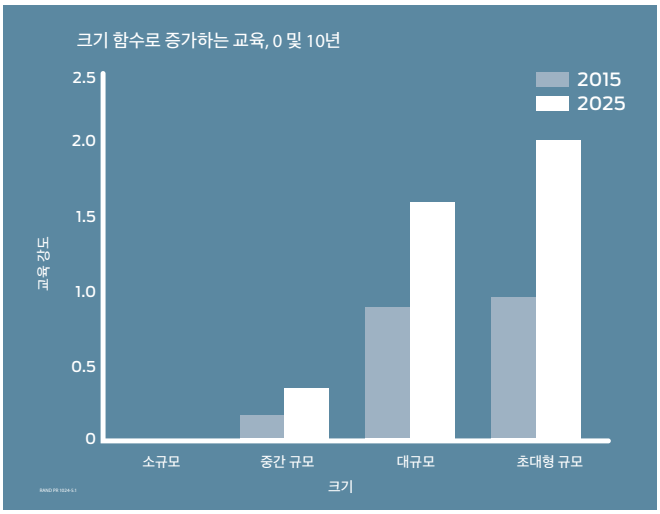
중소기업

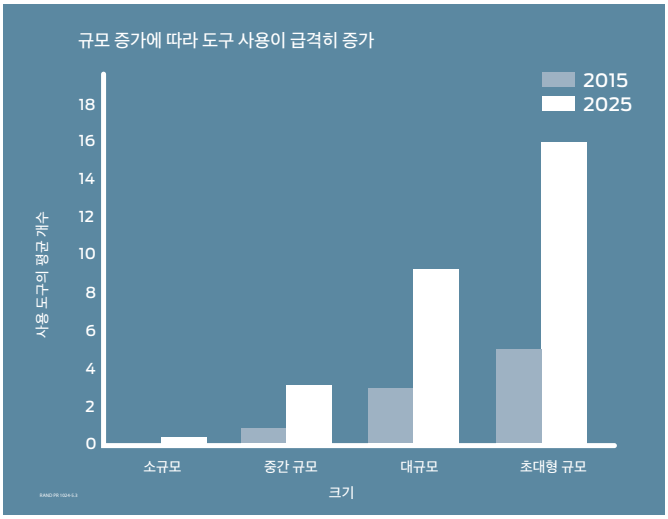
중소기업은 복합 보안 교육 및 고급 보안 기술에 많은 투자를 하지 않으면서 기본 도구와 정책만으로 가장 많은 혜택을 보고 있습니다. 중소기업의 공격면은 더욱 작고 정교한 공격을 받을 가능성이 적기 때문에, 높은 가격의 보안 제품에 과도하게 투자하면 정보 유출과 그로 인한 잠재적인 손실 가능성과 비교해 비용 추가가 불균형적으로 이루어질 수 밖에 없게 됩니다. 중소기업의 경우, 기본 도구와 방침이 잘 구축되어 있으면 네트워크를 보호하고 네트워크 상에서 개인 장비의 사용을 제한하여 효과적으로 보안을 유지할 수 있습니다.

대형 조직 및 민감한 정보 보유 조직

반면 대형 조직이나 방산업체, 또는 엄청난 양의 지적재산을 가진 조직 등 매우 민감한 정보를 가진 조직은 정책과 도구에 포괄적으로 투자해야 합니다. 첨단 공격의 대상이 되거나, 매일 대량 공격을 받고 특정한 유형의 침입을 받을 가능성이 훨씬 크기 때문입니다. 대대적으로 투자를 하지 않으면 사고로 인해 막대한 손실이 발생할 수 있습니다.

더불어 대기업은 보안 투자로부터 오는 '규모의 경제' 이점을 누릴 수 있습니다. 예를 들어, 직원 수가 증가함에 따라 1인당 고급 보안 교육의 비용 효과가 증가합니다.





기본 보안 인식 교육과 상용 도구가 마련되어 있다고 가정.

2. 많은 보안 툴에는 반감기가 있고 가치 하락의 위험이 있음

기업이 직면한 가장 까다로운 문제 중 하나는 공격자가 방어 수단을 피하기 위해 사용하는 대응공격(countermeasure)입니다. 공격자는 새로운 보안 기술에 대한 대응공격을 꾸준히 개발하기 때문에 이러한 도구의 상대적인 효과가 시간이 지나면서 제한되고 기업은 방어를 위한 새로운 기술에 투자해야 합니다.

샌드박싱(sandboxing) 또는 안티 바이러스와 같은 감지 시스템을 예로 들수 있습니다. 이러한 공격은 최초로 배포되었을 때의 대응이 매우 중요하고 대형 조직의 보안 활동에 있어 필수적인 부분이지만, 이러한 유형의 방어는 대응공격에 취약합니다. 따라서 지속적인 재평가가 필요하며 새로운 솔루션을 배치하여 공격자에 대한 방어 효과를 유지해야 합니다. 대응조치가 또 다른 대응공격을 낳는 적대적 역학이 사이버 증강의 근본 원인입니다.

이러한 공격자의 패턴으로 인해 기업이 유사한 수준의 보안을 유지하기 위해 보안에 투자해야 하는 비용이 증가합니다. 또한 이로 인해 회사의 전체적인 운영 비용도 증가하여 보안 팀이 관리해야 하는 보안 기술이 크게 증가하게 됩니다.

RAND 모델에 따르면 시간이 지나면서 이러한 대응공격을 처리하는 기술의 효과가 향후 10년 동안 65% 감소할 것으로 예상됩니다. 따라서 모델이 작동한 첫 해와 마지막 해에 지출한 금액과 비교했을 때, 보안 툴에 기업이 지출해야 할 전체 비용은 조직의 전체 보안 비용과 비례하여 16.2% 증가합니다. 이러한 수치가 적어 보일 수도 있지만, 도구가 기업의 최대 단일 보안 비용이라는 점을 고려하면 증가 금액은 매우 크다 할 수 있습니다.

그렇다면 기업은 어떻게 투자에 집중해야 할까요? RAND는 특정 유형의 보안 도구는 대응공격에 취약하지 않다는 사실을 발견했습니다. 보안 및 패치 관리 개선에 중심을 둔 기술 및 보안 기능, 자동화 및 기업 네트워크에서의 정책 실행 개선은 공격자가 회피하려는 도구 유형이 아니기 때문에 이 범주에 속합니다.

결국 대부분의 기업은 두 범주에 속하는 도구를 결합하여 시스템을 보호해야 합니다. 하지만 주니퍼는 기업이 이러한 역학이 존재한다는 것을 이해하고, 새로운 투자를 평가할 때 그러한 사실을 염두에 두는 것이 가장 중요하다고 생각합니다.

대응공격에 취약

- 이상 감지
- 시그니처 감지
- 샌드박싱 맬웨어(Sandboxing malware)
- 역 해킹(Hack-backs)
- 피싱 방지 교육

대응공격에 덜 취약

- 방화벽 정책 실행 및 자동화
- 다중 요소 인증
- 자동화 패치 관리 및 패치 버전 모니터링
- 서브네트워크 고립
- 네트워크 액세스 관리

3. 인적 자원의 중요성: 기업의 인적 자원에 투자가 장기적인 비용 절감을 가져옴

RAND의 모델이 제안하는 요소 중 시간이 지나면서 보안 비용을 크게 줄일 수 있는 방법은 보안 담당자 육성 및 교육에 대한 투자입니다. 새로운 도구에 대한 투자가 중요한 만큼, 잘 조직되고 지식을 갖춘 보안 팀 구성도 그에 못지 않게 중요합니다. 본 모델에서는, 최고의 도구도 올바른 관리가 이루어지지 않으면 효과가 없다는 점을 고려하고 있습니다.

RAND 모델에 따르면 성실성이 낮은 조직에 비해 성실성이 높은 기업, 즉 보안 프로그램을 관리하는 데 있어 가장 효과적인 조직을 갖춘 기업은, 본 모델이 작동하는 첫 해에 사이버 보안 비용을 19%, 10년 차에는 28%까지 절감할 수 있습니다.

주니퍼는 오늘날 지식이 풍부한 보안 전문가가 부족한 것이 사실이며, 이를 보강함으로써 얻을 수 있는 잠재적 비용 절감 효과가 매우 크다고 생각합니다. 기업은 보안팀 교육 및 확장에 적극적으로 투자해야 합니다. 신규 채용이 불가능하다면, 전문 보안 기능을 외부 전문가에게 위탁하는 것도 방법입니다. RAND의 보고서는 관리 서비스(managed services)를 활용하면 다음과 같은 이점이 있다고 설명합니다:

> 많은 방어자들은 다양한 고객에게 제공할 수 있는 특정 서비스 중에서도, 일부 중요 방어 기능을 전문가에게 위탁하고 있습니다. 예를 들어, 많은 대형 조직이 자체 네트워크 침투 시험을 실시하지 않는데, 이는 해당 분야가 매우 전문화되어 있어 유지를 위한 최고 수준의 역량을 갖춘 직원을 채용하기가 어렵기 때문입니다.[1]

2015

성실성 레벨	공격 비용에서의 차이
매우 낮음	13% 증가
낮음	10% 증가
중간 규모	중립적
높음	중립적
매우 높음	6% 감소

2025

성실성 레벨	공격 비용에서의 차이
매우 낮음	18% 증가
낮음	13% 증가
중간 규모	중립적
높음	6% 감소
매우 높음	10% 감소

[1] "방어자의 딜레마: 사이버 보안을 향한 과정 수립," RAND Corporation, 2015년, Martin Libicki, Lillian Ablon 및 Timothy Webb.

4. 기로에 선 사물인터넷(IoT: Internet of Things)

IzoT에 관심이 높아지고 있습니다. 그러나 한 가지 분명한 것은 가까운 미래에 전보다 많은 디바이스가 기업 네트워크에 연결되리라는 것 입니다. RAND에 따르면 IoT는 보안 비용 전반에 걸쳐 영향을 미칠 것입니다. 하지만 그 영향이 긍정적인지, 혹은 부정적인지는 확실치 않습니다. 오늘날 많은 조직이 기로에 서 있다는 주니퍼의 생각은 이러한 상황에 기인합니다.

기업이 스마트하고 정교하게 보안 기술 및 기기를 관리하여 IoT의 보안 시사점을 적절히 처리할 수 있다면 네트워크 기기의 개수가 전통적인 PC의 수를 넘어서는 과정에서도 장기적으로 비용 절감을 이끌어 낼 수 있습니다. 반면에 IoT가 초기 PC 시대와 비슷한 길을 걷는다면 수많은 보안 문제가 발생하고 기업의 보안 비용은 급격히 상승할 것입니다.

RAND의 모델은 IoT가 도입되면서 후자와 같은 상황이 일어날 경우 사이버 공격으로 인해 기업이 입게 될 손실이 10년 동안 30% 증가할 것으로 예측했습니다.

대부분의 기업이 직접적으로 IoT의 영향을 받기까지 앞으로 수년의 기간이 더 남아 있지만, 주니퍼는 지금부터 기업이 이러한 디바이스를 보안 프로그램과 네트워크에 어떻게 포함시킬 것인지 심사숙고해야 한다고 생각합니다. 기업은 이러한 새로운 디바이스 및 연결장치로 인해 증가할 대역폭을 감당할 수 있는 보안 인프라 성능을 갖추어야 합니다.

더불어 기업은 기업 환경에 도입되는 이러한 새로운 디바이스를 관리하기 위해 어떠한 보안 컨트롤 장치를 마련해야 하는 지 결정해야 합니다. 기업들은 현재의 BYOD 관리 방법과 유사하게 가까운 미래에 네트워크에 도입될 새로운 IoT 연결장치를 제공하고 관리할 적절한 솔루션을 갖추어야 합니다. 이러한 과제에는 적절한 권한 관리 기능을 수립 및 실행하여, 새로운 디바이스가 공격면을 증가시키지 않게 하는 것 입니다. 뿐만 아니라, 직장에서 직원용 IoT 디바이스 사용에 대해 기업의 명확한 정책을 수립하는 것도 필요합니다.

5. 소프트웨어 취약점을 제거하면 비용을 크게 절감할 수 있음

RAND가 파악한 바에 따르면, 비용에 막대한 영향을 주는 부분 중 하나는 기업이 사용하는 소프트웨어와 애플리케이션에서 악용 가능한 취약성 빈도입니다. 기업에서는 기본 시스템과 소프트웨어가 안전하지 않기 때문에 방어 조치에 투자해야 하는 경우가 종종 발생합니다. 안타깝게도 이러한 특정 지표는 CISO가 통제할 수 없으며, 코드를 작성하는 소프트웨어 제작 업체의 능력에 따라 좌우됩니다.

RAND의 모델에 따르면 소프트웨어 취약성 빈도가 반으로 줄면 기업의 전체적인 사이버 보안 비용이 25% 감소합니다.

그러나 소프트웨어 취약성이 앞으로는 더 적게 발생할지 여부는 확실치 않습니다. 만일 네트워크 및 소프트웨어 기술이 정적인 상태로 남는다면 방어자가 결국은 우위를 차지하게 될 것이지만, 혁신은 정보 기술 분야의 생명입니다.

RAND의 연구에 따르면 IoT의 도입에 따라 장치가 확산되고 이전 버전의 코드를 바탕으로 한 소프트웨어 생태계의 복잡성이 증가하면서 새로운 취약성 빈도가 증가할 수 있습니다.

다행히 소프트웨어 품질 개선을 위한 많은 작업이 진행되고 있습니다. 예를 들어 제품을 배송하기 전, 개발자가 취약성을 파악하는 데 도움을 주는 무료 도구가 개발되어 있으며, 이러한 도구를 사용하는 소프트웨어 제작 업체가 증가함에 따라 제품에서 발견된 취약성은 점차 감소할 것입니다.

주니퍼는 기업이 자체적으로 사용하는 소프트웨어를 검사하고, 소프트웨어 제공자에게 더 우수한 보안 테스트 및 패치를 요구해야 한다고 생각합니다. 기업이 불량 보안 프로그램을 사용하는 것은, 소프트웨어 제작 업체로 하여금 취약성이 적고 더욱 우수한 제품을 만들게 하는 강력한 자극이 될 것입니다.

기업 및 업계가 나아갈 길

그렇다면 사이버 위협이 증가하는 시대에 기업이 리스크에 대한 보안 투자 관리를 위해 할 수 있는 것은 무엇일까요?

보안 포트폴리오를 사업 분야와 마찬가지로 관리

기업은 하나의 사업분야와 마찬가지로 더 우수한 보안 관리 방법을 찾아야 합니다. 즉, 다양한 결정의 장단점을 정량화해야 합니다. 주니퍼는 RAND 모델을 통해 보안 태세 및 지출을 평가할 때 기업이 고려해야 할 여러 실행 가능한 인사이트를 제공한다고 생각합니다.

결국 CISO는 더 우수한 지표를 확보하여 RROI를 결정하기 위해 노력해야 합니다. 한마디로 기업은 주식 포트폴리오를 관리하듯 프로그램의 수명 주기 및 효과를 지속적으로 평가해야 합니다. 주니퍼의 양방향 모델 해석과 RAND의 정식 모델 및 방법론은 이러한 상황에서 기업의 고유하고 다양한 필요를 충족시키 가장 효과적인 도구를 결정하는 데 유용합니다.

대응공격을 염두에 둔 보안 도구 평가

RAND의 연구 결과에 따르면 "체계적인 방어에서 조직은 보안 수단에 대한 대응 방법이 만들어질 가능성을 염두에 두고 투자를 결정해야 합니다. 즉, 기업은 대응 방법이 만들어질 가능성이 적은 보안 수단을 설치해야 합니다."

이에 따라 주니퍼는 기업의 네트워크 보안에 있어 중앙 집중식 관리 및 분산 실행 플랫폼을 통해 보안 작업을 자동화하는 도구에 우선적으로 투자해야 한다고 생각합니다. 자동화(Automation)는 주니퍼의 핵심 분야이며, 고객에게 자동화 도구에 대한 투자를 추천하는 여러 가지 이유가 있습니다:

- 자동화가 내장된 도구는 대응공격에 덜 취약하여 시간에 따른 효과 감소가 적고, 더욱 오랜 기간 가치를 유지합니다
- 자동화는 과도한 업무에 노출되는 IT 팀의 운영 수요를 줄여 조직의 여타 보안 비용을 줄일 수 있습니다
- 자동화로 보안 담당자가 시스템 구성 및 시험에 투입하는 시간을 절감할 수 있으며, 이를 통해 정교한 공격의 빈도를 줄이고 새로운 방어 기능을 추가하는 등 더욱 중요한 작업에 집중할 수 있습니다
- 마지막으로 중앙 집중식 시스템을 갖추면 관리 및 실행이 용이해져 기타 보안 투자의 장점을 증가시키는 데 도움이 될 수 있습니다. 예를 들어 위협 감지 피드의 자동화 및 중앙 관리를 통해 위협 정보에 대한 다양한 소스를 네트워크 상의 실행 포인트로 연계하는 작업을 신속히 처리할 수 있습니다

자동화 관련 주니퍼의 작업 및 투자에 대한 자세한 정보는 여기를 참고하십시오.

산업 전반에 걸친 조치 필요

CISO만으로는 보안을 체계적으로 발전시킬 수 없습니다. 주니퍼는 현재 역학 관계를 바꾸고 방어자에게 유리한 상황을 만들기 위해, 보안 업계 전반과 정부가 중요한 역할을 수행해야 한다고 생각합니다.

차세대 교육

공격자보다 앞서 나가기 위해서는 차세대 개발자들이 혁신적인 기술을 더욱 안전하게 만들수 있도록 교육해야 합니다. RAND의 보고서도 "안전한 코드 작성은 컴퓨터 공학 전공자의 정규 과정이 아닙니다. 이들은 장치를 개발하고 제작할 차세대 엔지니어입니다"라고 언급하며 이러한 주장을 지지하고 있습니다.

차세대 개발자를 교육하여 본질적으로 더욱 안전한 소프트웨어를 개발한다면 보안 위험 및 기업의 전체적인 보안 비용을 줄일 수 있습니다.

학생 대상 보안 교육은 앞으로 보안 전문가가 증가하여 더욱 효과적으로 업무를 수행하게 된다는 의미도 있습니다. 지금이라도 기반을 다진다면 향후 보안 업계가 직면할 숙련된 전문가 부족 현상을 극복할 수 있을 것입니다. 더불어 해킹 윤리에 대해 배움으로써 검은 유혹을 받을 수 있는 많은 미래 해커들이 보안 기술을 올바른 곳에 사용하도록 유도할 수 있을 것입니다.

대응공격을 염두에 두고 기술 개발

한편 주니퍼와 같은 보안 혁신 기업들은 공격자의 대응공격을 극복할 수 있도록 설계된 보안 기술을 꾸준히 개발하고 네트워크의 가시성 및 통제수단을 개선해 나가야 합니다. 공격자와 방어자 사이의 공방은 끊임없이 계속되겠지만 이러한 현실을 극복하기 위한 노력이 새로운 기술에 대한 공격자의 공략 속도를 늦출 수 있을 것입니다.

본 보고서 및 모델은 사이버 보안 위험을 이해하기 위한 최종 버전이 아닙니다. 이제 보안 업계가 어떻게 위험을 이해하고 있는지에 대한 토론이 시작이어야 합니다. 주니퍼 네트웍스와 RAND 연구소가 함께 하는 작업이 향후 이러한 논의를 진행하고 촉진하는 데 도움이 되기를 바랍니다.

랜드연구소(RAND Corporation)의 정식 보고서를 비롯한 작년 보고서 및 보충 자료는 이곳에서 찾을 수 있습니다.

보고서 소개

"방어자의 딜레마: 사이버 보안을 위한 과정 수립(The Defender's Dilemma: Charting a Course Toward Cybersecurity)," RAND Corporation 보안 전문가, Martin Libicki, Lillian Ablon 및 Timothy Webb가 저술. 2013년 10월부터 2014년 8월까지 현재 및 향후 위협 환경에 대해 CISO와 진행한 심층 인터뷰를 바탕으로 합니다. 본 연구는 주니퍼의 후원을 받아 RAND가 진행한 2부작 시리즈의 첫 번째 보고서와 "사이버 범죄 도구 및 데이터 유출 시장: 해커들의 수입원(Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar)"를 바탕으로 하며, 이 보고서는 공격자의 경제적 추진 요인과 이들이 활동을 확장하기 위해 구축한 정교한 지하 암시장을 다룹니다.

본사 및 영업 본부

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
전화: 888.JUNIPER (888.586.4737) 또는
+1.408.745.2000
팩스: +1.408.745.2100
www.juniper.net

APAC 및 EMEA 본부

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
네덜란드 암스테르담
전화: +31.0.207.125.700
팩스: +31.0.207.125.701

JUNIPER NETWORKS

Juniper Networks(NYSE: JNPR)는 라우팅, 스위칭 및 보안 분야에서 혁신을 제공합니다. 소프트웨어, 실리콘 및 시스템에서 Juniper Networks의 혁신은 네트워킹 경험과 경제를 변화시킵니다. 추가 정보는 Juniper Networks(www.juniper.net)를 방문하거나 Twitter와 Facebook에서 Juniper와 연결하십시오.