TANIUM

전 세계가 재택근무를 도입하면서

분산된 업무 환경으로 전환됨에 따라 사이버 공격 증가

핵심 요약

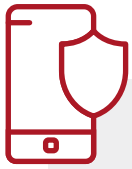
COVID-19는 이전에 겪었던 일과 전혀 다른 성격의 충격적인 사건이다.
경제 위기와 보건 위기가 복합된 COVID-19는 단순히 직접적인 재무적 영향뿐만 아니라
운영 구조 측면에서 많은 기업들에게 광범위한 영향을 끼쳤다.
전세계 기업들은 직원들에게 철저한 재택근무 명령을 내리고, 전례 없는 규모의 분산 근무를
실시하며 정부 지시에 대응했다. 일부에서는 팬데믹이 물러간 이후에도 직원 다섯 명 중
최대 두 명은 계속하여 원격 근무할 것이라 예상했다.

바이러스 발병 전, IT 선도기업들은 이미 여러 도전 과제에 대한 우려를 나타내고 있었다.
엔드포인트 가시성 갭(Visibility Gap)은 예상치 않게 발생되며, 응답자의 71%는
매주 확인되지 않은 IT자산이 발견된 적 있다고 대답했다.
주요 도전 과제로 무질서한 도구 확산(Tool Sprawl), 섀도우 IT(Shadow IT), 단절된 IT 팀 및
레거시 기술 등이 꼽혔다. 대부분(53%)의 IT 최고 담당자들은 가시성 갭(Visibility Gap)으로 인해
사이버 공격에 노출될 수 있을 뿐 아니라 브랜드 이미지에 악영향을 끼치고, 컴플라이언스
미준수로 인한 과징금 및 고객 이탈 등의 부정적인 영향을 유발할 수 있다는 우려를 표했다.

태니엄은 이번 위기로 인해 이러한 도전과제가 얼마나 심화됐으며, 조직들이 앞으로 다가올
어려움에 얼마나 대비하고 있는지 파악하기 위해 이번 국제 연구를 의뢰했다.

본 보고서는 미국, 영국, 프랑스 독일의 1천4명의 CXO(CEO, CIO, CTO)와 Vice President를
대상으로 한 인터뷰를 기반으로 작성됐다. 인터뷰 대상의 조직은 모두 글로벌 COVID-19
팬데믹 기간 동안 분산 근무 체제로 전환했으며, 직원의 규모는 1천명 이상이다.

확인된 사항



CXO 및 Vice Presidents는 원격 근무 보안 과제로 어려움을 겪고 있다

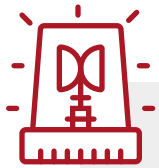
COVID-19 팬데믹 기간에 이들의 85%는 분산 근무 전환 준비가 잘 되었다 느꼈지만[1] 98퍼센트는 그 이후 원격 근무 보안 과제에 직면했다고 대답했다.
2019년 같은 시기 대비, 응답자의74%는 분산 근무 전환을 위해 IT 지출을 늘렸음에도 불구하고
이와 같은 결과가 나타났다고 말했다.

보안 문제 해결을 미루는 기업들

개인 디바이스에 패치를 배포하는데 어려움을 겪고, 이로 인해 조직이 위험에 노출됐다고 대답한 응답자는
43%였으며, 93%는 분산 근무 전환을 지원하기 위해 다른 보안 과제를 우선순위에서 뒤로 미루거나 취소했다고 답했다.
이런 업무로는 식별 및 접근 관리(IAM)와 보안 전략 업무 등이 포함된다.

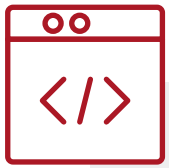
COVID-19로 인해 노출된 기업 보안 공백

공격의 빈도가 잦아졌다고 보고한 응답자는 90%였다.
신규 장비의 가시성 확보, VPN 요건으로 인한 IT 수용 능력의 한계,
화상 회의로 인한 보안 위험 증가가 3대 보안 과제였다.



이것이 뉴노멀 (New Normal)

대부분(85%)의 응답자는 팬데믹의 부정적인 영향을 조직에서 몇 달간 체감하게 될 것이라고 예상했다.
실제로, 과반(50%)의 응답자는 컴플라이언스 규제(26%), 사이버 보안 위험 관리(25%),
사이버 위험과 직원 프라이버시의 균형(19%) 등의 다양한 이유로
자택에서 성공적으로 IT를 이행하는데 장기적인 어려움을 겪을 것이라고 말했다.



새로운 현실에서 가시성(Visibility) 및 통제(Control)가 가장 중요

응답자의 절반은(48%) 직원들이 현장으로 업무를 복귀할 때
IT 자산의 가시성을 강화하는 엔드포인트 관리에 투자할 계획이라고 밝혔으며,
패치 관리 절차를 강화할 계획이라고 답한 응답자는 47%에 해당한다.

[1] "매우 잘 준비되었음"과 "충분히 준비되었음" 응답 합산

생각 보다 어려운 현실

대부분(85%)의 CXO와 Vice President들은 원격 근무 전환에 대비가 잘 되어 있다고 생각했다.
심지어 74%의 응답자는2019년 동기 대비 분산 근무 전환을 위해 IT 지출을 늘렸다고 응답하였고,
이중 38%는 IT 지출액이 51%이상 증가했다고 말했다.
하지만, 다수는 사이버 보안 위기의 영향을 과소평가했으며,
98%는 COVID-19로 인한 분산 근무 모델로 전환 하면서 보안 과제에 직면했다고 대답했다.

기업 및 조직이 방심했던 핵심 영역 중 하나는 패치 문제였다.
88%의 응답자는 패치 적용에서 어려움을 겪었다고 응답하였다.
실제로 43%의 응답자는 원격 근무 직원의 개인 디바이스에 패치를 적용하는데 어려움을 겪었으며,
이로 인해 조직이 위험에 노출된 것으로 나타났다. 또한 45%는 스캔 및 패치는 가능했지만,
수많은 장치의 보안문제가 해결되고 패치가 잘 적용 되었는지는 추적할 수 없었다고 호소했다.

보류된 보안 문제들

일부 사례에서 보안 영향은 매우 심각하게 나타났으며,
잠재적으로 기업 및 조직에 심각한 위험으로 추가 노출시킬 수 있다.

CXO 및 Vice President들 가운데 네 명 중 하나(26%)는 팬데믹이 시작된 이후 패치 또는
취약성 스캔 등의 취약성 관리에 우선순위가 낮아졌다고 대답했다.
응답자들은 이 기간 동안 엔드포인트에 대한 가시성 부족 및 VPN 업무 과중으로 인해
취약성 관리에 대한 우선순위를 낮췄다.
이러한 결정은 마이크로소프트가 가장 큰 규모의 패치를 포함한,
매월 두번째 화요일 정기 패치(Patch Tuesday) 업데이트를 배포한 기간과 겹친다.
이 기간 동안 VPN과 기타 원격 근무 툴에서 취약점을 노리는 사이버 범죄에 쉽게 노출 된다고
다수의 보고서는 경고했다.

응답자 93%는 원격근무 전환에 대응하기 위해 보안 우선순위를 취소하거나 보류해야 했다고 말했다.
보류 혹은 취소로 인해 타격을 입은 업무로 가장 빈번하게 언급된 영역은
식별 및 접근 관리(IAM) (39%), 보안 전략 업무(40%)였다.

COVID-19로 노출된 기업 보안 공백

이와 동시에 기업 및 조직은 보안 태세에서 공백을 노리는
기회주의적 사이버 범죄자와 국가간의 사이버 공격이 급증하는 경험을 했다.
90%는 팬데믹으로 인하여 사이버 공격 빈도 증가 현상을 관찰했으며,
평소 대비 위협이 30% 늘어났다고 보고했다.
가장 일반적인 공격은 데이터 노출(38%)이었으며,
업무 이메일 침해 또는 허위 트랜잭션(37%)과 피싱 공격(35%)이 뒤를 이었다.

분산 근무로 전환하는 과정에서 CXO와 Vice President들에게 가장 큰 3대 보안 위기는
다음과 같다고 응답하였다.

- **네트워크 상의 개인용 컴퓨팅 장치 식별(27%)**
  - 가시성 갭(gap)의 문제가 다시 한 번 확인되었다.
  응답자 중 45%는 on-site 보안 위험을 줄이기 위해 기업 네트워크 상에 개인 디바이스를
  접근 할 수 없게 함으로써 향후 조직이 정상 업무로 돌아 갈 것 있을 것이라고 답하였다.

- **VPN 요건으로 인한 IT 수용능력 초과(22%)**
  - 잘못된 VPN 구성은 패치 문제를 유발할 수 있으며, 이러한 잘못된
  트래픽 라우팅으로 인해 직원들에 대한 보안 컨트롤이 불가능 할 수 있다.

- **화상 회의로 인한 보안 위험 증가 (20%)**
  - 서둘러 도입한 화상회의 툴이 기업용으로는 적합하지 않을 수 있다.
  팬데믹이 한창이던 시점에 널리 이용된 한 플랫폼에서
  두 가지 중요한 결함이 발견됐다.

CXO들과 Vice President들은 보안 문제를 분산 근무 및 관련된 디지털 트렌스포메이션을
대응함에 있어 예산, 이사회의 지지 및 인력/전문성 확보 보다 더 중요한 과제로 평가하고 있다.
장기적으로 보았을 때, 가까운 미래에 대부분의 사무 업무가 원격으로 이루어질 것이라
가정 했을 때, 만약 보안 문제를 제대로 관리하지 않는다면 조직의 재정 및 브랜드 이미지에
주요한 위험요소가 될 수 있다.

[2] 응답자들이 답한 공격은 다음과 같다 :
데이터 노출, 비즈니스 이메일 침해/허위 트랜잭션, 피싱, 디도스 공격, 패스워드 침해, 랜섬 공격, 기타 멀웨어 공격

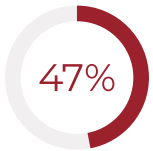
미래 예측

대부분(85%)의 CXO와 Vice President들은 팬데믹의 부정적인 영향 속에서 운용 시 발생하는
부정적인 영향이 최소 3개월 이상 지속될 것으로 보고 있으며,
응답자 중 셋 중 한 명(33%)은 6개월에서 12개월간 유지될 것으로 전망했다.
따라서, 기업 및 조직이 원격 업무 도전과제를 시급히 해결하는 것이 점점 더 중요해지고 있다.

다행히 이러한 과제를 신속히 해결할 계획을 갖고 있다. 70%의 CXO와 Vice President들은
컴플라이언스 요건을 준수하고(26%), 사이버 위험을 관리하며(25%), 직원의 프라이버시와
사이버 위험의 균형을 유지하여(19%) 원격 근무에 있어 사이버보안을 최우선순위로 삼겠다고 밝혔다.

거의 모든 응답자(96%)는 직원들이 사무실로 복귀할 때
위험을 줄이기 위한 변화를 시행할 계획이라고 대답했다.
이들은 다음과 같은 분야에 중점적으로 투자해 실행할 예정이다.

**IT 자산 관리의 가시성(Visibility) 확대를 위한
엔드포인트 관리(48%)**



**패치 관리
프로세스 개선(47%)**

**IT 분산을 위한
클라우드 컴퓨팅(45%)**

**VPN 의존도를 줄이기 위한
제로 트러스트(zero trust) 모델(38%)**

새로운 현실에서 가시성(Visibility) 및 통제(Control)가 가장 중요

오늘날 IT 및 비즈니스 리더들은 자신이 처한 상황에 대해 잘 인지하고 있다.
대부분의 조직은 2020년 초 그들 앞에 놓인 도전 과제를 잘 해결 하였다.
하지만, 직원 생산성을 지원하는 것 만으로는 충분치 않다.
어디에서나 일하는(Work-From-Anywhere) 새로운 시대에서
지속적인 사이버 위험 완화에 관심과 신경을 충분히 쏟지 않는다면,
조직들은 심각한 재무적 타격과 이미지 손상을 입게 될 수 있다.

많은 CXO와 Vice President들은 이러한 도전 과제들을 초기에 과소평가했을 수도 있다.
하지만 이제 이들은 패치, VPN, 엔드포인트 가시성 등 IT 보안 및 운용상
어디에서 문제가 가장 두드러지는지 파악하고 있다.
또한 대규모 원격 근무 지원은 많은 이들에게 뉴노멀이 될 것임을 의미한다는 사실도 주지하고 있다.

마지막으로, 많은 기업 및 조직들은 잠재적 패치 되지 않은 취약점에 대응하고,
크게 확대된 기업 공격(Attack Surface) 전반의 위험을 완화해야 한다.
이를 위한 최선의 방법은IT 엔드포인트 가시성 및 온프레미스(On-Premise)와
클라우드 환경을 통제 및 개선하는 것이다. 이를 통해 보다 생산적이고 유연한 업무 방식,
분산화된 클라우드 컴퓨팅 모델 및 보안에 대한 보다
신속한 제로 트러스트(Zero Trust) 접근방식을 추진할 수 있을 것이다. 뿐만 아니라,
조직들이 미루었던 보안 프로젝트들을 다시 원 궤도로 돌려놓을 수 있다는 의미이기도 하다.

이는 현재 직면한 글로벌 위기 속에서, 통합 엔드포인트 관리 및 보안을 중심에 두고
비즈니스를 지원하여 IT를 강화하겠다는 새로운 결단의 전화위복 될 수 있다.

이번 연구는 2020년 5월 29일부터 2020년 6월 6일까지 미국, 영국, 프랑스, 독일의 직원 1천명 이상의 기업의
CXO와 Vice Presidents(CEO, CIO, CTO) 1천4명을 대상으로 태니엄(Tanium)을 대신해
영국의 조사전문 업체 센서스와이드(Censuswide)가 설문조사를 통해 수행했다.
센서스와이드는 ESOMAR (European Society for Opinion and Marketing Research, 유럽 마케팅 리서치 협회)의
원칙을 기반으로 하는 시장조사협회(Market Research Society)를 따르며, 해당 협회 회원을 채용하고 있다.

TANIUM

Tanium은 세계에서 가장 높은 보안 수준의 IT환경을 위한 통합 엔드포인트 관리 및 보안 플랫폼을 제공합니다.
매우 빠른 속도, 가시성 및 규모를 제공하는 당사는 Fortune 100대 기업 절반, 상위 소매업체 및 금융기관 그리고 미정보기관/ 육/해/공 해병대를 지원하고 있으며,
이들 조직은 Tanium을 활용하여 신속한 비즈니스 결정을 내리고 효율적으로 운영하며 보안 위험을 줄이고 있습니다.
Tanium은 최근 Forbes 선정 "2019년 최고의 100대 클라우드 컴퓨팅 민간 기업"에서 7위,
FORTUNE 선정 미국 "최고의 100대 중소기업 직장" 10위, 영국 최고 직장 18위를 차지했습니다.
지금 www.tanium.com을 방문하거나 LinkedIn 및 Twitter에서 팔로우하세요.

tanium.com

@Tanium

info@tanium.com