디지털 전환 핵심 업무로써 '보안' 지켜야

CIO는 진화하는 위협으로부터 조직을 안전하게 보호하기 위해 도구, 프로세스, 숙련된 인력이 필요하다. CIO는 감당하기 벅찬 수많은 도전 과제들과 마주하고 있다. 디지털 전환의 혁신적 업무를 수행해야 함은 물론, 고도화되고 잠재적인 피해를 유발할 수 있는 사이버 공격으로부터 조직을 보호하는 업무를 수행해야 한다. '비즈니스'와 '보안'의 요구를 모두 만족하기 위해 CIO가 반드시 고려해야 할 점을 살펴본다. 〈편집자〉

남인우 태니엄코리아 전무
inwoo.nam@tanium.com

현재 사이버 보안 위협 환경은 기술 인력과 사이버 보안 도구 포트폴리오의 조합을 기반으로 위협에 맞서 리스크를 관리하려는 CIO들에게 많은 부담이 되고 있다. 기업 내 모든 정보 기술 감독 책임자인 CIO들은 조직의 미션을 지원하고, 재무적 목표 달성을 위해 유용한 IT 가이드와 자원을 제공할 필요가 있다.

이 업무는 디지털 전환과 점점 더 깊은 인과관계가 있다. 디지털 전환은 사람마다 다르게 해석될 수 있지만, 결국 혁신적인 방식으로 디지털 기술을 적용해 신제품과 서비스를 론칭하거나, 기존 업무 프로세스를 상당한 수준으로 개선하는 것을 뜻한다.

디지털 전환은 대부분 거대하고, 분산되며, 다양한 IT 인프라로 이어지게 마련이다. 기존 대비 향상되고, 신속하며, 가치가 높은 제품과 서비스를 제공해야 하기 때문에 새로운 애플리케이션을 통해 더 많은 클라우드 서비스, 더 많은 데이터와 AI, 머신러닝의 활용은 불가피하다. 이로 인해 모바일 디바이스와 새로운 애플리케이션 아키텍처를 통해 분산된 인력으로 조직의 디지털 발자국(Digital Footprint)이 분산되며, 결국 십 년, 이십 년 전에 개발된 거대한 하나의 애플리케이션 대신, 애플리케이션 프로그래밍 인터페이스(API)와 마이크로 서비스가 활용될 가능성이 높다.

IT 공격표면과 공격 벡터의 차이 이해하기

IT 인프라가 분산되고 다양화되는 것은 공격표면 확장으로 연결된다. OWASP(Open Web Application Security Project)는 공격표면을 '공격자가 시스템에 침투해 데이터를 빼낼 수 있는 모든 다양한 지점'이라고 설명한다.

복잡한 공격표면을 보호하는 일은 어렵고, 보완적 기능을 갖춘 사이버 도구들을 요구하는 경우가 많다. 조직의 사이버 대비태세 평가는 우수한 사이버 위생(Cyber Hygiene), 사이버 보안 정책을 집행하는 효과적인 구성 관리, 사이버 도구 건전성의 지속적 모니터링으로 이뤄진다.

15년 전 대부분의 IT 시스템이 온프레미스에 위치하고, 네트워크 방화벽을 통해 보호되고 있을 때 공격표면이 지금보다 작았다. 그에 비해 오늘날의 조직은 수백 개 클라우드 서비스에 의존하고, 직원들이 원격으로 근무하고 있는 상황에서 공격표면이 상당히 커졌다. 모든 직원들의 가정용 네트워크에 연결된 디바이스는 잠재적인 공격 벡터가 될 수 있고, 이는 미션 크리티컬한 IT 리소스 침해로 이어질 수 있다.

CIO들은 이렇게 분산된 인프라의 보안 유지에 대한 책임을 맡고 있다. CIO들은 방화벽을 뚫고 들어오는 외부 위협뿐만 아니라, 솔라윈즈, 워너크라이 같이 비선형적 위협을 형성하는 애플리케이션 내의 소프트웨어 취약점에 대해서도 고려할 필요가 있다.

Log4J 취약점과 오늘날의 공격표면

오늘날 애플리케이션에는 수백 혹은 수천 개의 소프트웨어

컴포넌트와 서비스가 포함돼 있으며, 하나의 취약점만 있어도 전체 애플리케이션과 애플리케이션을 실행하는 조직의 보안이 위태로워질 수 있다. 새롭게 등장하는 위협에 적응할 수 있는 기능이 있는 도구를 갖추면 시간을 절약하고, 위험을 줄이며, 조직의 사이버 대비태세를 향상시키게 된다.

예를 들어 널리 사용되는 여러 버전의 오픈소스 로그 유틸리티는 버그가 포함돼 있으며, 이로 인해 공격자들은 로거(Logger)의 자바 네이밍(Java Naming)과 디렉토리 인터페이스(Directory Interface)에 스트링을 포함시켜 권한이 없는 사용자가 높은 권한이 필요한 애플리케이션에서 코드 실행을 허용할 수 있다. 이렇게 크리티컬한 취약점을 악용한 공격은 랜섬웨어 확산, 데이터 탈취, 시스템 차단 등에 사용될 수 있는 것이다.

NIST 중요도(Criticality) 평가에서 10점 만점에 10점을 받은 Log4j 취약점은 가장 흔하게 사용되는 자바 컴포넌트 리포지토리의 약 4%를 비롯해 웹과 애플리케이션 소프트웨어에서 핵심 컴포넌트로 자주 발견된다. Log4j 소프트웨어 아티팩트는 업계 대표 상용 애플리케이션은 물론 내부적으로 개발한 사내용 애플리케이션에서도 발견된다.

Log4j 취약점은 이제 조직의 공격표면에 포함된다고 할 수 있다. Log4j 취약점을 통해 공격자들은 기업용 네트워크에 코인 채굴 소프트웨어를 설치하고, 새로운 형태의 랜섬웨어 공격을 감행하며, 벨기에 국방부를 침투할 수 있다.

Log4j는 CIO들이 직면하고 있는 다음과 같은 주요 도전과제를 다시 한번 상기시킨다. 광범위하고 복잡한 IT 인프라를 선택, 배포, 관리하면서, 동시에 위협이 아무리 복잡하고 새롭더라도 공격표면에 있는 모든 위협의 식별, 완화, 사이버 대비태세 관리, 리스크 경감, 고정된 예산으로 비용 유지 등을 처리해야 한다.

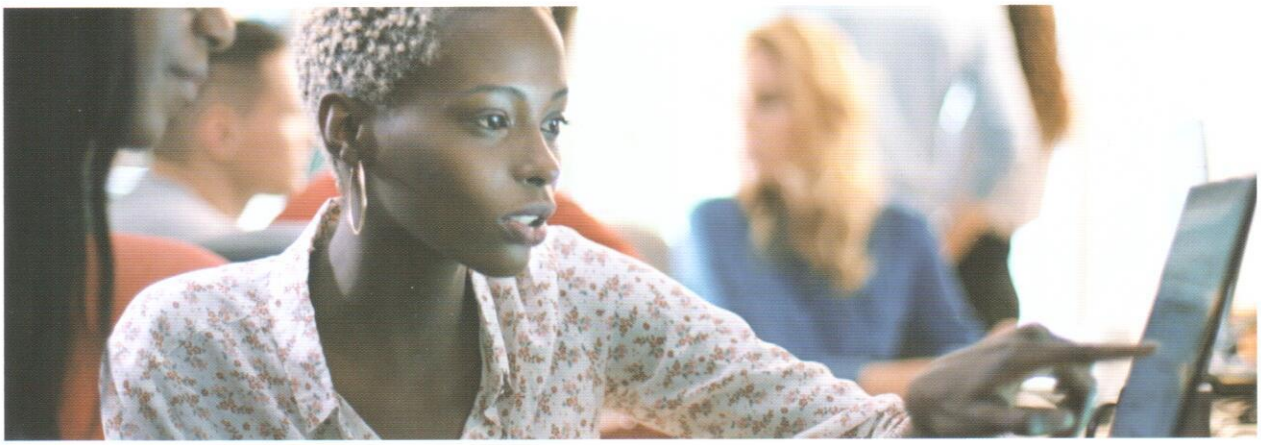
공격표면은 현재 어떤 상태인지와 무관하게 지속적으로 변화된 모습을 나타낸다. 2015년에는 기업 데이터의 30%가 클라우드에 저장돼 있었고, 2020년까지 그 비율은 50%였다. 자료에 따르면 애플리케이션, 서비스, 데이터의 클라우드 마이그레이션은 계속될 것으로 전망된다. 이러한 클라우드 마이그레이션과 더불어 기타 디지털 전환 노력은 복잡성을 높이고, 공격표면 확대를 가중시킬 것이다.

만약 변화가 보안 속도를 앞지를 경우, 조직이 치명적인 피해를 입게 될 것이다. 이는 조직이 랜섬웨어 공격, 데이터 탈취, 기업용 이메일 침해(BEC) 공격 등으로 인한 피해와 운영 지장이 발생할 수 있다. 기업은 랜섬으로 수천만 달러를 지불하게 될 것이며, 만일 공격으로 인해 소비자의 기밀 데이터가 유출됐다면 미국 연방거래위원회(FTC)에 수천만 달러의 과징금을 내야 할 수도 있다.

따라서 CIO들은 변화를 추진하면서, 동시에 지속적으로 진화하는 공격표면에 적응해 기업의 IT 인프라를 보호하는 균형잡기에도 노력을 기울어야 한다. 하지만 이는 결코 쉬운 일이 아니다.

전체 시스템에 대한 실시간 가시성 확보

공격표면에 보안 기능을 적용하기 위해서는 끊임없이 변



화하는 특성을 세밀하게 감안해야 한다. CIO는 눈에 보이지 않는 위협을 방어할 수는 없기 때문에 취약점을 이해하고, 위협 완화를 위해 월간 또는 주간 보고에 의존할 수밖에 없다. 공격표면 관리를 위해서는 실시간 데이터에 접근해 위협 속도에 맞춰 탐지에서 대응으로 전환하는 능력이 필요하다.

취약점은 침해된 엔드포인트가 네트워크에 연결되는 순간 또는 오래된 소프트웨어의 컴포넌트가 백업에서 다시 설치되는 순간 나타날 수 있다. 사이버 대비태세는 현재의 소프트웨어 및 승인된 소프트웨어를 고려해야 한다.

엔드포인트와 네트워크를 모니터링하기 위한 도구는 최대한 실시간 인텔리전스 제공과 조사가 뒷받침돼야 한다. 시스템이 침해당한 사실이 2주 뒤에 발견된다면, 공격자들이 너무 유리한 고지를 점령하게 되는 상황이다. 그 시점이면 랜섬웨어는 이미 데이터센터와 여러 지역으로 확산됐을 수도 있고, 핵심 데이터를 발견해 탈취를 끝마쳤을 수도 있다.

학습·사용 용이성 보장해야

CIO는 핵심적인 사이버 기능을 제공하면서, 동시에 가장 학습 부담이 적은 도구를 선택해야 한다. 새로운 팀에서 신규 애플리케이션이나 서비스에 반드시 보안을 적용해야 한다면 이들에게 과도하게 복잡하지 않은 도구를 제공할 것을 강력히 권장한다. 팀원들은 복잡하거나 거추장스러운 도구를 어떻게 관리할지 신경 쓰는 대신, 본연의 업무에 집중해야 하기 때문이다.

인재와 기술은 새롭게 등장하는 위협에 대해 조직의 대응 행동을 가속화할 수 있는 핵심 요소다. 사이버 위협 환경은 점점 더 변동성을 보이거나, 불확실하거나, 복잡하거나 또는 불분명해지기 때문에, 이런 민첩성은 더욱 더 그렇다.

앞서 언급한 것처럼, 정교하고 치명적인 행동이라도 때를 놓친다면, 아무런 행동을 취하지 않는 것과 같은 결과를 낳게 된다. 효과적인 사이버 역량 도입에서 속도는 필수적인 요소다.

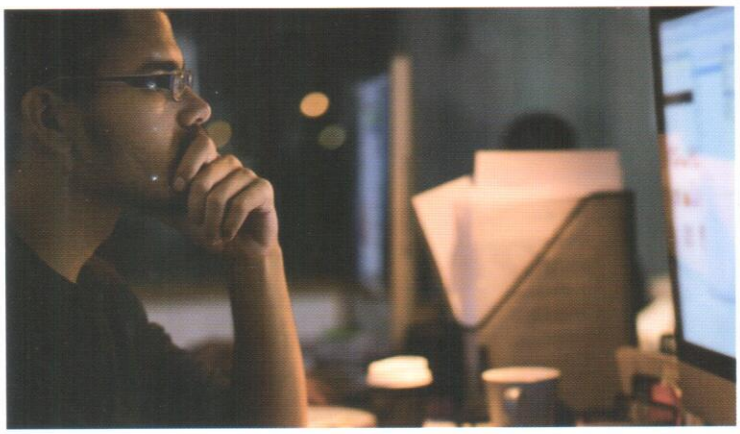
추가 고려사항으로는 CIO들이 새로운 위협에 대응하면서, 보안팀과 운용팀이 더욱 수월하게 협력할 수 있도록 만드는 도구를 선택해야 한다는 것이다. 소스 코드에서 나타나는 심각한 취약성은 분명 Log4j가 마지막은 아닐 것이다. 보안팀과 운용팀은 어떤 보안 위협에 대해서라도 가장 신속하게 대응할 수 있는 방향전환 도구가 필요하다.

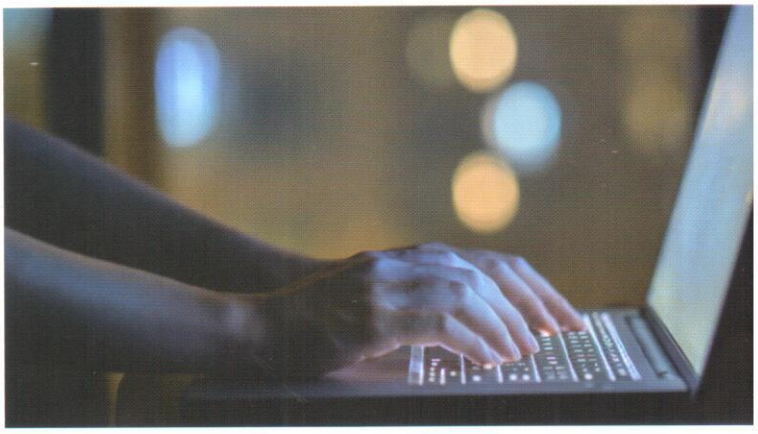
포괄적인 커버리지 지원·중앙화 및 자동화 필수

포괄적 커버리지를 위해서는 가장 광범위하게 엔드포인트 및 기타 IT 자산을 아우르는 도구를 선택해야 한다. 안타깝게도, 대부분의 취약점 평가와 엔드포인트 관리 시스템은 상당한 비중으로 엔드포인트를 누락하며, 많은 경우 최대 20%까지 누락 비중이 나타난다.

IT 담당부서에서 엔드포인트를 확인할 수 없다면 침해 지표 모니터링 또는 발견이 불가능하며, 자동 패치 일정에 포함시킬 수도 없다.

이로 인해 사이버 위생은 취약해지고, 엔드포인트 구성에 어긋남이 발생되며, 필요한 지점이나 시점에 오류가 발생하





는 불건전한 상태로 이어진다. 엔드포인트 가시성은 복잡한 공격표면 관리를 위한 효과적 접근방식에 있어서 밑거름 역할을 한다.

공격표면에는 조직의 네트워크에 연결돼 있는 모든 엔드포인트와 시스템이 포함된다. 때문에 CIO들은 반드시 일부가 아닌 전체적인 공격표면을 볼 수 있도록 시스템을 구축해야 한다.

CIO들은 가능한 상호 운용성이 있는 도구를 선정해, 위협 감지와 패치 관리 등 서로 다른 컴퓨터 보안 기능 영역에서도 업무 자동화가 가능하고, 데이터를 가시적으로 확인, 접근, 이해할 수 있도록 만들어야 한다.

'연합' 형태의 접근방식을 도입하고, 상호 호환이 매끄러운 여러 도구를 사용하면 간소화된 보안업무 절차 구축은 더욱 손쉬워진다. 자동화 역시 수월해진다. 공동 플랫폼 내에서 방향 전환 기능은 보안 운영 센터(SOC) 애널리스트들에게 매우 중요하다.

왜냐하면 인시던트를 조사하고 위협을 완화하기 위해 하나의 도구 모음에서 다른 도구 모음으로 전환하는 시간도 쉽게 허비되지 않기 때문이다.

전문성 있는 인재와 팀 구성

성공적인 위협 완화 전략에 도구만 포함돼 있는 것은 아니다. CIO들은 탐지에서 대응, 복구까지 전환 속도가 더욱 짧아지고 있는 촘촘한 사이클 내에서 업무 완수를 위해 지식, 기술, 능력(KSA)을 갖춘 사고력 있는 인재가 필요하다. 변화하는 공격표면으로부터 최선을 다해 조직을 보호하기 위한 이러한 접근방식은 기능과 프로세스를 동기화해 조직의 프로세스를 강화시키기 위한 도구의 기능을 활용한다.

예를 들어, 조직은 레드팀을 활용해 진화하는 IT 인프라의 모든 부분에 대한 침투 테스트를 실시함으로써, 공격자보다 한 발 먼저 새로운 취약점을 발견할 수 있다. 이러한 활동의 결과로 공격표면에 대한 하드닝(Hardening)을 수행함과 동시에, 조직적 학습 프로세스에도 정보를 제공할 수 있다. 이러한 반복 훈련(Sets and Reps)은 사이버 인력의 KSA 대비 태세를 향상시키는 귀중한 학습 기회가 된다.

디지털 전환 프로젝트 설계 및 계획 단계에서 보안 및 애플리케이션 개발 팀에 보안 분야 전문가를 합류시킨다면 보안을 사후에 덧붙이기보다는 신제품과 서비스에 처음부터 포함시킬 수 있다.

제로 트러스트 접근법으로 공격표면 줄여

CIO들은 공격표면 접근을 줄이고, 공격자의 손쉬운 네트워크 이동을 차단하기 위해 제로 트러스트(Zero Trust) 전략을 도입해야 한다. 제로 트러스트 모델에서는 그 어떤 사용자, 프로세스 혹은 디바이스도 어떤 형태의 조사 없이 무엇도 신뢰하지 않는다.

다시 말해 디바이스 컴플라이언스 조사, 사용자의 역할, 성공적 인증이 없이는 네트워크 서비스 또는 리소스에 대한 접근권한이 부여되지 않는다는 의미다. 실질적으로 조직의 미션을 기반으로 허가된 사용자, 디바이스, 프로세스를 제외하고 모두 그리고 모든 접근이 거부된다.

불필요한 포트, IP주소, 프로토콜을 차단함으로써, IT 조직들은 공격표면의 규모를 줄이는 한편, 공격자가 침투해 네트워크 전반으로 내부 확산 공격, 가치 있는 데이터 탐색, 또는 랜섬웨어 확산을 더 어렵게 만들 수 있다.

CIO들은 디지털 전환 이니셔티브에 대해 기본적으로 제로 트러스트 보안 전략을 활용해 공격표면을 줄이고, 신규 IT 서비스와 인프라가 회복력을 갖추며, 디지털 사업 운영이 가능하도록 대비할 수 있다.

디지털 전환은 결코 끝나지 않았다. 생존과 번영을 꿈꾸는 조직은 반드시 혁신하고, 새로운 제품과 서비스를 출시하며, 기존의 것은 최적화해야만 한다. 그 결과, 모든 조직의 공격표면은 지속적으로 바뀌며, 무한하게 확장될 가능성이 높다.

이러한 변화와 공격자들의 진화하는 위협을 따라잡기 위해 CIO들은 도구, 프로세스, 숙련된 인력이 필요하며, 이를 통해 조직의 IT 인프라에 항상 높은 수준의 보안을 유지할 수 있다.