**1. 제로 트러스트 네트워크**
데이터 보안에 대한 기존의 접근 방식은 뚫을 수 없는 벽을 쌓는 것이었지만, 여기에는 치명적인 결함이 있다는 인식이 커지고 있다. 네트워크가 여러 클라우드 공급업체, 분산된 물리적 위치 및 인력 등으로 방어 경계를 유지하는 것은 매우 어렵거나 불가능하다.

그래서 제로 트러스트(Zero trust)라는 새로운 사고 방식을 가져야 할 때가 됐다.

사이버 범죄자와 악의적인 사용자는 취약한 고리를 이용해 네트워크에 액세스한 다음, 측면 이동을 통해 심각한 피해를 가한다. 데이터에 액세스하려는 모든 장치 또는 사람에 대한 엄격한 ID 확인이 필요하다. 어떤 요청도 맹목적으로 믿어서는 안된다.

다소 급진적으로 보일 수 있는 제로 트러스트는 보안 프로세스를 다시 생각하고 여러 기술을 채택해야 한다. 하지만 지금까지 해결이 불가능하다고 증명된 문제를 처리할 수 있는 전체적인 전략을 제공한다.

**2. 차세대 프라이버시, 보안 및 규정 준수**
데이터 개인정보보호 및 보안에 대한 기대가 바뀌고 있다. 사람들은 자신의 개인정보가 노출되는 것을 두려워하고 기업이 보유하고 있는 소중한 데이터를 한층 더 보호하기를 기대하고 있다. 데이터 유출 비용은 단순히 정리하는 데 소요되는 비용이 아니며 적용될 수 있는 벌금과 벌칙은 물론, 평판 훼손까지 포함한다.

규정 준수(compliance) 요구사항을 충족하지 못하면 책임있는 회사로서의 지위가 위험하다. 내부 위험뿐만 아니라 파트너 및 모든 서드파티를 포함한 전체 비즈니스에서 적절한 평가를 수행하는 것이 중요하다. 일반 대중과 규제 당국 모두 사이버보안 사고 발생시 인내심이나 관용이 크게 감소한 것으로 나타났다.

규정 준수를 보장하기 위해 기업은 사전 예방 조치를 취하고 일정에 따라 들어오는 모든 규정을 미리 살펴야 한다. 규제에 직면한 상황에 대응해 급하게 일회용 밴드를 붙이는 것보다 광범위한 보안 전략을 구현하고 향후를 대비한 탄탄한 기반을 구축하는 것이 좋다.

**3. 새로운 위협 모니터링 및 탐지**
대부분의 기업은 잠재적 위협을 탐지하기 위해 실시간 모니터링 및 스캔의 필요성을 이해하고 있다. 알려진 취약점을 검사하고 이를 완화하기 위해 움직이는 것은 퍼즐의 일부일뿐이다. 악의적인 페이로드가 릴리스되는 성공적인 공격과 보안 시스템이 이를 탐지하는 순간 사이의 간격을 줄이는 것이 중요하다. 그러나 위협이 익숙하지 않는 경우, 위협을 탐지하는 데 몇 시간 이상 걸리기도 한다.

새로운 위협이 끊임없이 진화하고 있으므로 모니터링 및 탐지 기술은 진화해야 한다. 업체는 더 나은 위협 인텔리전스를 개발해야 하며, 이를 최대한 활용할 수 있는 방법에 대해 생각해 볼 필요가 있다. 위협 인텔리전스의 효과를 얻기 위해서는 자동화 및 전문 지식과 함께 회사의 위험 감수성을 깊이 이해해야 한다.

**4. 피싱 공격 및 원격 브라우저 격리**
사람들은 종종 쉽게 조작되며 사이버 범죄자들은 네트워크 액세스 권한을 획득하기 위해 소셜 엔지니어링을 활용한다. 피싱, 그리고 스미싱과 같은 변형 공격은 일반적이다. 피싱 공격은 이제 악성코드보다 보안 전문가들에게 더 큰 관심사가 됐다. 잠재적인 공격은 엄청나게 다양하고 정교하다. 사이버 범죄자들은 액세스 및 도구를 판매하고 효과가 있는 새로운 전략을 개발, 공유한다.

보안 인식 교육이 권장되지만, 위협을 무효화하는 것만으로는 충분하지 않다. 가상화 및 컨테이너 기술을 통한 원격 브라우저 격리(Remote browser isolation)는 중요한 데이터 및 인프라에서 웹 브라우징과 같은 고위험 행동을 분리하는 좋은 방법이 될 수 있다. 대부분의 악성코드는 직원이 잘못된 링크를 클릭하거나 잘못된 웹 사이트를 방문해 다운로드된다. 이 모든 것을 막는 것은 불가능할 수도 있지만, 원격 브라우저 격리는 이런 행동이 비즈니스에 큰 피해를 주는 것을 막을 수 있다.

**5. 클라우드 보안**
다양한 산업군에서 모든 규모의 기업은 클라우드에 점점 더 많은 데이터를 저장하고 있다. 클라우드 서비스는 확장성과 비용 효율성을 제공하지만 회사 서비스와 데이터가 여러 위치에 분산될 수 있다는 것을 의미한다. 대부분의 기업은 비즈니스 가치를 제공하는 레거시 애플리케이션에 의존하면서 민첩하고 새로운 서비스와 제품을 개발할 수 있는 하이브리드 클라우드 인프라를 보유하고 있다.

문제는 클라우드 채택으로 잠재적 공격 영역이 증가하고 서드파티가 보유한 데이터에 대해 보안 책임이 있다는 것이다. 관리해야 할 상당한 위험이 있다. 클라우드 서비스는 매력적인 공격 대상이기 때문에 기업은 클라우드 보안을 위한 베스트 프랙티스를 적용하는 것이 필수적이다.