백서

디지털 혁신에서 제로 트러스트 액세스의 필요성

공격 표면 확장으로 CISO가 직면한 새로운 위험

종합 요약

기업에서는 사업을 가속화하고 경쟁력을 유지하기 위해 디지털 혁신(DI) 이니셔티브를 빠르게 도입하고 있습니다. 즉, 비즈니스 애플리케이션과 데이터가 회사 시설 내에서 벗어나 넓고 멀리까지 분산되어 있어 직원들이 곳곳에서 더 많은 회사 자산에 액세스하게 되었습니다. 이 때문에 기존 경계가 무너지고 내부 네트워크가 확장되는 공격면에 노출되었습니다. 이는 CISO에게 가장 큰 걱정거리입니다.

기업에서는 이러한 위협에 대응하여 "누구도, 아무 것도 신뢰하지 않는" 전략을 보안에 적용해야 합니다. 특히, CISO는 제로 트러스트 액세스(ZTA) 정책으로 네트워크를 보호함으로써, 클라우드에 있는 모든 사용자와 기기, 웹 애플리케이션을 인증해 신뢰성을 확보하고 적절한 액세스 권한을 부여해야 합니다. 제로 트러스트는 각 프로젝트의 성격이 어떻든 디지털 혁신을 보호하는 데 중요합니다.

기업 리더의 81%가 직원들이 모바일 보안에 가장 큰 위험이라고 답했습니다.[1]

네트워크 엣지의 진화

DI 이니셔티브는 규모를 막론하고 모든 기업에서 비즈니스 성장을 촉진합니다. 이런 성장에서 새로운 네트워크 엣지(프라이빗 및 퍼블릭 클라우드 인프라, 사물 인터넷(IoT), 모바일 기기, 소프트웨어 정의(SD) 지사)가 확산되는 현상이 일어납니다. 따라서 데이터, 애플리케이션, 워크플로가 기하급수적으로 증가합니다. 네트워크 안팎에서 사용자 액세스를 관리하고 여러 위치에서 다수의 기기를 상호 연결하기 위해 기업들은 이런 네트워크 엣지에 배포된 기기를 늘리고 있습니다.

이는 CISO에게 악몽과도 같을 수 있습니다. 최근 몇 년 사이에 네트워크 엣지가 폭발적으로 늘어났습니다. 기존 경계가 무너지고 공격에 취약한 개방적 환경이 형성될 정도였습니다. 사이버 위협은 더욱 만연하고 끊임없이 변화합니다. 과거에는 경계 보안이 "신뢰하지만 검증하는" 전략을 기반으로 했습니다. 하지만 네트워크에서 사용자, 기기, 애플리케이션이 지나치게 늘어난 나머지 무엇을 신뢰해야 할지 어렵게 되었습니다. 악의적 행위자는 자격 증명 유출, 멀웨어와 같은 익스플로잇을 활용해서 정상적인 계정에 액세스 권한을 얻습니다. 악의적 행위자는 침투하고 나면 횡적으로 이동할 수단을 손쉽게 알아내고, 매우 빠르게 확산되면서 평평하고 신뢰할 수 있는 내부 네트워크를 악용합니다. 침투한 악의적 행위자는 엣지 기기에 액세스한 후, 운영 중단, 데이터 유출, 금융 위기, 평판 훼손을 일으킬 만한 공격을 시작할 수 있습니다.

보안 리더는 기존의 네트워크 액세스 방식으로는 점점 늘어나는 공격을 감당할 수 없습니다. 그래서 네트워크에 있는 모든 것을 신뢰하는 전략에서 아무것도 신뢰하지 않는 전략으로 옮겨가고 있습니다. CISO는 효과적인 제로 트러스트 액세스 모델을 통해 네트워크 안팎에 있는 신뢰할 수 없는 네트워크 엣지의 취약한 영역(예: 사용자, 기기, 자산)에 대한 전략을 세웁니다.

네트워크에 누가 연결되었는지 알기

보안 리더는 언제나 누가 네트워크에 있는지 알아야 합니다. 그러나 취약한 비밀번호를 사용해서 네트워크에 연결하는 직원으로 인해 위험이 증가하게 됩니다. 너무나 많은 계정에 자격 증명이 필요하기 때문에 대부분 비밀번호는 지나치게 단순하고 피싱 공격과 같은 익스플로잇을 통해 쉽게 침해할 수 있습니다. 기업에서는 각 사용자가 누구이고, 회사에서 어떤 역할을 하는지 아는 것이 중요합니다. 이런 지식이 있어야 각 역할이나 직무에 필요한 리소스에 액세스할 권한을 안전하게 부여하면서도 사례별로 다른 사용자에게 추가적 액세스 권한을 제공할 수 있습니다.

사용자나 관리자 모두에게 BYOD가 인기를 끌고 있지만, 일부 CISO는 위험을 간과합니다. 공격면이 넓어지면 위협이 기존 경계의 방어를 뚫고 내부 네트워크에서 횡적으로 이동하기가 더욱 쉬워집니다. 이는 보안 침해가 매우 오랫동안 탐지되지 않는 원인 중 하나이기도 합니다. 가장 심각했던 보안 침해 사례들은 권한이 없는 사용자가 네트워크에 액세스하거나, 신뢰할 수 있는 사용자에게 액세스 권한을 부적절하게 부여한 것이 원인이 되어 일어나기도 했습니다 BYOD는 기업 내에서 보편화되고 있지만 보안 리더의 83%가 모바일 위협으로 인해 기업이 위험에 처했다고 답했습니다.[2]

기업에는 지역적으로 분산된 직원도 문제입니다. 직원들이 회사 본사, 지사 캠퍼스는 물론이고, 자택 사무실 등의 다양한 곳에서 직무를 수행하고 있습니다. 원격으로 네트워크에 액세스하는 사용자가 매우 많기 때문에 공격면이 확장될 기회가 더욱 늘어났습니다. 예를 들어, 직원은 카페, 공항, 자동차, 대중교통에서 핫스팟이나 공개 Wi-Fi를 사용해서 연결하는 경우가 많습니다.

이런 연결은 상당한 보안 위험을 발생시킵니다. 제삼자가 사용자와 회사 네트워크 사이에 오가는 모든 정보를 가로챌 수 있습니다. 공격자는 패치되지 않은 소프트웨어의 취약성을 이용하여 엔드포인트에 멀웨어를 주입합니다. 로컬 정보뿐만 아니라, 엔드포인트 기기를 통해 회사 네트워크에 액세스하는 것이 목적입니다.

이러한 문제는 대규모 원격 작업 환경에서 더욱 확대되었는데, 2020년에 COVID-19 팬데믹을 통해 모든 기업이 얻은 교훈입니다. 원격 근무 인력이 15%를 밑돌던 대부분 기업이 갑작스럽게 90% 이상 재택근무에 들어갈 수 있는 적절한 인프라와 보안 제어 역량을 갖춰야 했습니다.

이는 제로 트러스트 액세스가 중요한 이유에 포함됩니다. 기기가 수시로 네트워크에 연결되었다가 끊어지기 때문에 보안 리더는 어떤 사용자가 네트워크에 있고, 이들이 적절한 액세스 권한이 있는지 아는 것이 중요합니다. 직원의 역할이 변경되면(예: 영업부에서 운영부로 이동) 이전과는 다른 영역에 액세스해야 할 수도 있고, 보안팀에서는 매끄러운 전환을 지원해야 합니다.

최근 기업이 입은 가장 피해가 크고 성공적인 공격 대부분은 엣지 네트워크 기기가 핵심이었습니다.[3]

네트워크에 무엇이 연결되었는지 알기

보안 리더는 누가 네트워크에 있는지 알아야 할 뿐만 아니라, 항상 어떤 기기가 네트워크에 있는지도 알아야 합니다. 그러나 모바일 기기와 IoT 제품이 확산되면서 기존의 네트워크 경계가 다수의 마이크로 경계로 해체되었고 기업의 공격면이 훨씬 넓어졌습니다. 각 마이크로 경계는 각 사용자 기기와 연결되어 있기 때문에 엔드포인트가 멀웨어 감염과 지능적 익스플로잇의 중요한 표적이 되었습니다.

엔드포인트가 폭발적으로 늘어나고 공격 표면이 확장되면서 대부분 기업이 어떤 기기가 연결되는지 파악하지 못한다는 점에서 네트워크 제어에 근본적인 문제가 생겼습니다. 사실, BYOD나 IoT에는 기기 구성 표준화가 없는 것이나 마찬가지입니다. BYOD에 사용하는 모바일 기기는 네트워크를 엄청난 위험에 빠트릴 수 있습니다. 이러한 위험은 데이터 유출, 보안되지 않는 Wi-Fi, 네트워크 스푸핑, 피싱, 스파이웨어, 깨진 암호 또는 부적절한 세션 처리에서 발생할 수 있습니다. 그러나 엔드포인트 공격 표면은 IoT 기기의 폭발적 증가로 인해 가장 많이 확장됩니다.

기업에서 연결하는 "스마트" 기기가 늘어나면서 IoT 기기에 대한 사이버 공격이 기승을 부립니다. 악의적 행위자는 이러한 기기를 악용해서 분산된 서비스 거부(DDoS) 공격과 여러 가지 다양한 악의적 행위를 가합니다.

BYOD와 IoT 엔드포인트를 철저히 보호하려면 기업에서 각 기기가 어디에 있는지, 무엇을 하는지, 네트워크 토폴로지에서 다른 기기에 어떻게 연결되는지 알아야 합니다. 가시성이 부족하면 보이지 않는 위험에 취약해집니다. 보안 리더는 네트워크 엣지에서 기기를 추적할 수 있어야 합니다. 그러나 절반에 가까운 사이버 보안 전문가는 10명 중 9명이 미래의 위협에 대한 우려를 드러내면서도 IoT 기기에 대한 공격에 대응할 계획이 준비되어 있지 않다고 말했습니다.[4]

일부 기업에서는 기존의 네트워크 세그먼테이션을 사용하지만, 모든 승인된 사용자와 애플리케이션에 액세스를 제공하면서도 그 외에는 액세스를 막는 안전한 네트워크 기반 세그먼트를 정의하기가 어렵습니다. 아무리 세그먼테이션을 잘해도 네트워크 방어에 구멍(네트워크 아키텍트가 예상치 못한 액세스 시나리오)이 생기기 마련이고 악의적 행위자가 이를 익스플로잇할 수 있습니다.

게다가 검사된 기기를 신뢰할 수 있다고 가정하고 액세스 권한을 부여한다면 여전히 공격은 차단하지 못합니다. 수많은 기업이 신뢰했던 직원과 하청업체로부터 갑작스러운 공격을 받았습니다. 분실하거나 도난된 기기에서 유출된 비밀번호는 향후 네트워크를 공격하는 무기가 될 수 있습니다. 그래서 제로 트러스트 전략이 매우 중요합니다. 사이버 범죄자가 수많은 네트워크 기기를 해킹하는 데 집중하고 있으므로 보안 리더는 네트워크에 연결된 모든 기기에 대한 가시성과 탐지 능력을 향상해야 합니다.

네트워크 안팎의 자산 보호

또한, 보안 리더는 오프라인이나 다른 네트워크에서 모바일 기기 사용이 늘어나는 것에 어려움을 겪고 있습니다. 이런 기기가 회사 네트워크에 다시 로그인했을 때 멀웨어, 봇넷과 같은 보안 위협이 될 수 있습니다. 예를 들어, 많은 직원이 사적인 영역과 업무 영역에서 모두 BYOD 기기를 사용합니다. 인터넷을 탐색하고, 소셜 미디어에서 다른 사람과 교류하고, 심지어 네트워크에 로그인하지 않았을 때 개인 이메일을 받기도 합니다.

하지만 온라인 상태에서 다시 네트워크에 연결된 후, 의도치 않게 바이러스, 멀웨어, 익스플로잇 등의 여러 가지 위협에 자신의 기기와 회사 리소스를 노출할 수 있습니다.

대부분 기업이 네트워크를 오가는 엔드포인트 수를 파악하지 못한 상태에서 기기를 개인적 용도와 업무 용도로 모두 사용하는 행태가 벌어지고 있습니다. 최근 Ponemon Institute 보고서에서 기업의 63%가 네트워크에 연결되지 않은 엔드포인트를 모니터링할 수 없다고 답했고, 절반 이상이 엔드포인트 기기의 규정 준수 상태를 확인할 수 없다고 답했습니다.[5] 네트워크에 연결된 기기가 너무 많아 모든 엔드포인트를 모니터링하기 어렵습니다. 따라서 CISO와 보안팀은 이로 인한 상당한 위험을 관리하는 데 어려움을 겪고 있습니다.

모든 기기를 지속적으로 식별, 분할 및 모니터링하는 ZTA 프레임워크로 옮긴다면 위험이 크고 평평한 네트워크를 바꾸어, 내부 리소스를 안전하게 보호하면서도 데이터, 애플리케이션, 지적 재산까지 보호할 수 있습니다. 이 전략은 경계 중심적 보안 전략과 관련된 위험을 낮출 뿐만 아니라, 네트워크에 연결되지 않은 기기에 대한 가시성과 제어를 강화하고 전체 네트워크와 보안 관리를 단순화합니다.

기업의 63%가 회사 네트워크를 떠난 엔드포인트 기기를 모니터링하지 못하고, 53%가 멀웨어에 감염된 엔드포인트가 최근 12개월 사이에 증가했다고 답했습니다.[6]

결론: 제로 트러스트 액세스 전략의 필요성

DI 이니셔티브는 비즈니스 성과를 개선합니다. 다른 한편으로는 DI 이니셔티브로 인해 기업의 공격 표면이 확장, 변경되면서 사이버 위협이 악용할 수 있는 새로운 공격 벡터가 생기기 때문에 CISO와 팀원, 리소스에 부담을 가중합니다. 악의적 행위자는 더욱 지능적이고 발전되었고 기존의 경계 보안 전략만으로는 부족합니다. 위협의 성격과 지능적 수준에 따라 달라지겠지만, 기업에는 보안 인프라에서 위협의 모든 측면을 감시할 수 있는 단일 지점이 존재하지 않습니다. CISO는 제로 트러스트 액세스를 활용하면 네트워크에 연결되는 사용자와 기기에 집중하고, 이들의 ID를 확인하여 적절한 액세스 권한과 신뢰를 부여할 수 있습니다.

공격 표면이 늘어나는 가장 큰 이유 중 하나는 네트워크에 연결되는 IoT와 스마트 기기가 확산되고 있기 때문입니다. 보안 리더는 네트워크에 액세스하는 기기가 넘쳐나고 있어서 완전한 가시성을 갖추지 못한 경우가 많고 CISO는 사각지대에서 피해가 발생한다는 것을 힘겹게 교훈으로 얻었습니다. 기업에서 모든 엔드포인트 기기를 철저히 보호하려면 네트워크 전체에 제로 트러스트 액세스 정책을 적용해야 합니다. 각 기기가 어디에 있고, 무엇을 하고, 네트워크에서 다른 기기와 어떻게 연결되는지 파악하면서도 위협이 될 만한 비정상적인 동작을 지속적 모니터링으로 탐지해야 합니다.

[1] "Mobile Security Index 2019," Verizon, 2019.

[2] 상게서.

[3] Neil Jenkins and Natasha Cohen, "Living on the Edge," Cyber Threat Alliance, 2019년 4월 30일.

[4] "Only 47% of cybersecurity pros are prepared to deal with attacks on their IoT devices," Help Net Security, 2019년 11월 8일.

[5] "The Cost of Insecure Endpoints," Ponemon Institute, 2020.

[6] 상게서.

FORTINET®

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 **전화:** 080-559-8989 **Email:** kr-callcenter@fortinet.com

wp-securing-digital-innovation
696181-A-0-KR