DELL Technologies

Dell Technologies와 함께 공급망 사이버 공격 방어

핵심 요약

비즈니스 운영 환경의 국제화와 상호 연결성이 점점 확장되면서, 조직이 공급망 사이버 공격으로 인한 위협도 노출되는 경우도 늘어났습니다. 이러한 교묘한 공격은 제조부터 배포, 그리고 타사 소프트웨어에 이르기까지 하드웨어 수명주기의 취약성을 악용함으로써 악의적인 행위자가 신뢰할 수 있는 애플리케이션 또는 업데이트를 통해 전체 시스템을 손상시킬 수 있도록 합니다. 이러한 인시던트는 재정적으로 큰 문제가 될 뿐만 아니라 평판을 떨어뜨리고 대규모 운영 중단 사태를 일으킬 수 있습니다.

이러한 위협의 영향은 매우 큽니다. 공급망 공격은 심각한 피해가 발생하기 전에는 탐지되지 않는 경우가 많기 때문에 사전 예방적 방어 전략이 필수적입니다. Dell Technologies는 고급 엔드포인트 보호, 사전 예방적 모니터링, 포괄적인 서버 및 데이터 보안 솔루션을 통해 기업이 공급망을 포괄적으로 보호할 수 있도록 합니다. 조직은 기술, 파트너십 및 전문 지식을 통해 회복탄력성을 강화하고 생태계에 내재된 취약성으로부터 스스로를 보호할 수 있습니다.

공급망 사이버 공격의 위협 증가

공급망 공격은 최근 몇 년 동안 크게 증가했습니다. 운영, 배송 또는 배포 중에 물리적 디바이스를 변조하거나 소프트웨어 공급업체의 약점을 발견하면 공격자는 악성 구성 요소 또는 코드를 주입하거나, 시스템을 손상시키거나, 기밀 데이터를 유출할 수 있는 수단을 얻게 됩니다. 피해자는 소규모 기업부터 글로벌 대기업까지 다양하며 심각한 재정적 손실, 고객 신뢰 훼손, 법적 후속 조치 등의 결과가 초래됩니다. Dell Technologies는 이처럼 위험이 커지고 있음을 잘 알고 있으며, 이러한 공격의 치명적인 영향을 완화하기 위한 선제적 조치를 설파합니다.

공급망 사이버 공격 이해

하드웨어 공급망 공격의 작동 방식

1. **제조 단계:** 공격자가 하드웨어 조립 중에 악성 구성 요소를 주입하여 침해된 공급업체를 활용하는 경우가 많습니다.
2. **배송 단계:** 운송 중에 디바이스를 탈취하여 유해한 펌웨어 또는 하드웨어 수정을 포함하도록 수정합니다.
3. **배포 및 활성화:** 손상된 하드웨어가 조직의 네트워크에 들어오면 공격자가 기밀 데이터에 액세스하거나 백도어 작업을 활성화합니다.

소프트웨어 공급망 공격의 작동 방식

1. **초기 침해:** 타사 소프트웨어 공급업체가 피싱, 패치되지 않은 취약성 또는 내부자 위협을 통해 침해되는 경우가 많습니다.
2. **코드 조작:** 악의적인 행위자가 배포용 소프트웨어에 멀웨어나 백도어 같은 유해한 요소를 주입합니다.

3. **최종 사용자에게 전파:** 손상된 소프트웨어를 설치하거나 업데이트하는 기업이 악성 구성 요소를 무심코 다운로드합니다.

일반적인 기법 - 하드웨어

- **펌웨어 조작:** 배포 후 활성화되는 악성 코드를 내장합니다.
- **하드웨어 이식:** 숨겨진 구성 요소를 통합하여 데이터를 모니터링하거나 유출합니다.
- **신뢰할 수 있는 공급업체 악용:** 덜 안전한 프로세스를 사용하는 타사 공급업체를 악용합니다.

일반적인 기법 - 소프트웨어

- **구성 요소 하이재킹:** 타사 라이브러리 또는 프레임워크를 악성 코드로 감염시킵니다.
- **업데이트 주입:** 익스플로잇을 포함하도록 공식 소프트웨어 업데이트를 변경합니다.
- **종속성 혼동:** 안전하지 않은 패키지 종속성에 조직이 의존하는 점을 악용합니다.

비즈니스에 미치는 영향

재정적 결과

공급망을 표적으로 삼는 공격은 법적 벌금, 시스템 복구 비용 및 고객 보상과 관련된 비용을 초래하는 경우가 많습니다. 한 글로벌 IT 관리 회사가 겪은 대규모 인시던트는 7,000만 달러를 초과하는 손실을 초래했습니다. 이 인시던트는 이러한 침해로 인한 재정적 혼란이 얼마나 큰지를 잘 보여줍니다.

운영 중단

멀웨어 침투로 인해 손상되거나 비활성화된 시스템이 가동되면 장시간 다운타임이 발생하는 경우가 많으므로 조직의 생산성이 저하되고 프로젝트 결과물이 지연됩니다.

평판에 미치는 영향

현대 비즈니스에서는 소프트웨어 파트너에 대한 신뢰가 매우 중요합니다. 조직의 소프트웨어 오퍼링과 관련된 공급망 침해는 평판을 훼손하고 고객 충성도를 떨어뜨릴 수 있습니다.

실제 사례 - 하드웨어/소프트웨어

한 글로벌 전자 제품 제조업체는 공급망에서 손상된 구성 요소를 발견했고, 이는 광범위한 시스템 장애를 야기했습니다. 이 공격으로 인해 **4,500만 달러** 이상의 복구 및 법적 비용이 발생했으며 공급업체 관계에 회복할 수 없는 피해가 발생했습니다.

SolarWinds 침해는 가장 악명 높은 소프트웨어 공급망 공격 사례 중 하나입니다. 이 회사의 Orion 제품이 손상되어 정부 기관과 Fortune 500 기업을 포함한 전 세계 여러 조직을 감염시켰습니다. 피해 추정치가 **9,000만 달러**를 초과한 이 보안 침해는 공급망 취약성이 얼마나 큰 결과를 초래할 수 있는지 잘 보여줬습니다.

공급망 공격에 대응하는 Dell Technologies의 전문 지식

Dell Technologies의 방대한 보안 솔루션 포트폴리오는 기업이 진화하는 사이버 위험에 미리 대비할 수 있도록 지원합니다.

Dell SCV(Secure Component Verification)

SCV(Secure Component Verification)는 다양한 Dell 솔루션 전반에서 하드웨어 구성 요소의 신뢰성과 무결성을 보장하도록 설계된 Dell Technologies 공급망 보안 전략의 핵심입니다. SCV는 제조 시점부터 배송 및 배포에 이르기까지 시스템 구성 요소의 암호화 검증을 제공합니다. Dell Technologies는 강력한 공급망 보안을 제공하여 공장부터 배포까지 시스템이 변조되지 않고 안전하게 보호되도록 보장합니다. 따라서 Dell Technologies 고객의 전반적인 보안, 신뢰성 및 성능이 향상됩니다.

Dell Trusted Device로 엔드포인트 보호

Dell Trusted Device는 하드웨어 및 펌웨어 수준에서 보안을 통합하여 변조 방지 시스템을 만듭니다.

- **SafeBIOS**는 부팅 시 펌웨어 무결성을 보장하여 무단 구성 변경을 방지하고, 부팅 시 펌웨어 무결성을 확인하여 손상된 시스템이 시작되는 것을 방지합니다.
- **SafeID**는 하드웨어 수준에서 인증 자격 증명을 보호하여 무단 액세스를 차단하며, 인증 키를 보호하고 무단 사용자를 차단하여 로그인 자격 증명을 보호합니다.
- **SafeData**는 기밀 비즈니스 파일에 대한 포괄적인 암호화를 지원하여 악의적인 데이터 유출 시도를 차단합니다.

CrowdStrike를 통한 사전 예방적 위협 탐지

CrowdStrike는 Dell Technologies의 기술과 통합되어 악성 소프트웨어 동작에 대한 실시간 통찰력을 제공합니다.

- **동작 위협 탐지 분석:** 하드웨어 및 펌웨어 동작을 모니터링하여 변조의 징후를 확인하고, 비정상적인 소프트웨어 활동을 탐지하여 멀웨어 배포를 방지합니다.
- **즉각적인 대응 툴:** 손상된 시스템을 AI가 격리하여 네트워크 내에서의 수평 이동을 방지합니다.
- **AI 기반 위협 문제 해결:** 위협을 적극적으로 식별하고 격리하여 엔터프라이즈 시스템 내에서의 수평 확산을 방지합니다.
- **통합 기능:** Dell Technologies와 CrowdStrike의 툴을 사용하여 하이브리드 및 멀티클라우드 환경을 포괄적으로 보호합니다.

Dell Technologies의 서버 및 스토리지 솔루션을 통해 보안 강화

Dell PowerEdge 서버 제품군은 고급 보호 기능을 통합하여 미션 크리티컬 소프트웨어 플랫폼을 보호합니다. Dell PowerStore와 같은 스토리지 시스템은 업계 최고 수준의 암호화 기능을 애플리케이션 및 데이터에 제공합니다.

- **보안 서버 펌웨어:** 하드웨어 수준에서의 무단 변경을 모니터링하고 차단합니다.
- **격리된 네트워크 모니터링:** 공급망 변조를 나타내는 이상 징후를 탐지합니다.
- **변경 불가능한 백업:** 기본 스토리지가 손상된 경우에도 복구 시점을 보호합니다.
- **복구 볼트:** 환경이 격리되어 있어 손상된 시스템에서 시작된 계단식 장애가 차단됩니다.

위험을 완화하기 위한 다계층 접근 방식

Dell Technologies는 기술, 인력 관행, 업데이트된 프로세스를 결합한 포괄적인 전략을 채택할 것을 기업에 권장합니다.

전략적 단계

- **공급망 가시성 향상:** 모든 공급업체가 엄격한 보안 표준을 준수하고 모든 단계에서 하드웨어를 인증하도록 요구합니다.
- **고급 암호화 구현:** 고급 프로토콜을 사용하여 모든 수준에서 데이터를 보호하여 손상된 하드웨어에서도 접근성을 제한합니다.
- **제로 트러스트 정책 도입:** 어떠한 디바이스, 애플리케이션 또는 사용자도 검증 없이 자동으로 신뢰를 얻을 수 없습니다.
- **보안 코딩 표준:** 소프트웨어 파트너와 협력하여 플러그인, API 및 통합에 대한 엄격한 지침을 적용합니다.
- **정기적인 활동 및 감사 모니터링:** 가시성 감사를 자주 수행함으로써 타사 서비스 전반의 무결성을 보장합니다.
- **정기 테스트 수행:** 침투 테스트 및 펌웨어 평가를 배포하여 디바이스 무결성을 지속적으로 검증합니다.
- **직원 교육:** 의심스러운 동작을 수행하는 구성 요소 또는 패키지를 눈치챌 수 있도록 팀을 교육합니다.

Dell Professional Services가 비즈니스 회복탄력성을 보장하는 방법

Dell Professional Services는 강력한 공급망 방어 체계를 구현할 수 있도록 기업을 안내합니다. 숙련된 사이버 보안 전문가로 구성된 팀이 조직의 고유한 요구 사항에 맞춘 평가, 교육 및 위협 대응 전략을 제공합니다.

- **구현 지침:** 공급업체 환경 전반에 걸쳐 제로 트러스트 관행 및 감사를 받은 공급업체 관행을 전략적으로 조율합니다.
- **인시던트 대응:** 악의적인 인시던트 발생 후에 기업이 신속하게 복구할 수 있도록 합니다.

Dell Technologies와 함께하는 미래 지향적인 엔터프라이즈 시스템

공급망 사이버 공격은 최신 위협의 교묘함을 잘 보여줍니다. 기업은 보안 침해를 방지할 뿐만 아니라 인시던트 발생 시 신속한 복구를 보장하는 보호 기능을 필요로 합니다. Dell Technologies와 파트너십을 맺으면 첨단 툴, 전략적 전문 지식, 신뢰할 수 있는 협업 네트워크를 이용할 수 있습니다.

다음 단계 진행

Dell Technologies가 제시하는 모범 사례를 구현하여 기밀 자산을 보호하고 운영 신뢰성을 간소화하십시오. 엔터프라이즈 시스템의 수명 연장을 준비하면서 지금 바로 맞춤형 컨설팅을 받으십시오.

Dell Technologies과 함께하면 공급망 사이버 보안을 강화하면서 신뢰성, 적응성 및 혁신을 달성할 수 있습니다. 오늘의 노력은 내일의 성공을 보장합니다.

더 안전하고 미래는 Dell Technologies와 함께 시작됩니다. Dell Technologies를 통해 가장 중요한 것을 보호하십시오.

Dell.com/SecuritySolutions에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.

Dell 솔루션에 대한
자세한 정보

Dell Technologies
전문가에게 문의

추가 리소스 보기

#HashTag로
대화에 참여하기

DELL Technologies