DELL Technologies

랜섬웨어: Dell Technologies를 통한 사이버 보안 및 회복탄력성 강화

랜섬웨어란?

랜섬웨어는 몸값을 지불할 때까지 컴퓨터 시스템이나 데이터에 대한 접근을 차단하는 악성 소프트웨어(멀웨어)의 일종입니다. 가장 파괴적인 사이버 공격 유형 중 하나입니다. 전 세계 조직의 50%가 작년 한 해 동안 한 번 이상 랜섬웨어 공격을 받았으며, 랜섬웨어 공격 후 평균 다운타임은 3주에 달하여 심각한 운영 중단을 초래합니다.

증가하는 랜섬웨어 위협

랜섬웨어는 몸값을 지불할 때까지 컴퓨터 시스템이나 데이터에 대한 접근을 차단하는 악성 소프트웨어(멀웨어)의 일종입니다. 가장 파괴적인 사이버 공격 유형 중 하나입니다. 전 세계 조직의 50%가 작년 한 해 동안 한 번 이상 랜섬웨어 공격을 받았으며, 랜섬웨어 공격 후 평균 다운타임은 3주에 달하여 심각한 운영 중단을 초래합니다.

랜섬웨어의 작동 방식

랜섬웨어는 일반적으로 누군가가 악성 링크를 클릭하거나, 감염된 첨부 파일을 열거나, 손상된 웹사이트를 방문할 때 조직을 감염시킵니다. 그런 다음 시스템으로 이동하여 파일을 암호화해서 읽을 수 없게 만듭니다. 그리고 나서 랜섬웨어 프로그램은 일반적으로 암호 해독 키에 대한 대가로 결제(종종 암호화폐로)를 요구하는 메시지를 표시합니다. 몸값을 지불하지 않으면 공격자는 데이터를 삭제하거나 공개적으로 유출하겠다고 위협할 수 있습니다. 2017년에 발생한 WannaCry 공격은 랜섬웨어 공격의 대표적인 사례로, 전 세계에 빠르게 확산되어 병원, 기업, 정부 기관에 피해를 입히고 막대한 재정적 피해를 가져왔습니다. CyRiM(Cyber Risk Management)과 Lloyd's of London에 따르면 WannaCry 바이러스의 전 세계 경제적 피해는 40억~80억 달러에 달했으며, 단 며칠 만에 150개국 20만 개 이상의 시스템이 피해를 입었습니다.

피해를 입은 세계 유수 기업 중 두 곳은 서비스 중단과 복구 작업으로 3억 달러의 손실을 보고한 FedEx와 공장 여러 곳에서 생산을 일시적으로 중단해야 했던 Renault-Nissan이었습니다. 랜섬웨어 공격으로 인한 숨겨진 비용은 다음과 같은 여러 가지가 있을 수 있습니다.

- 기업의 다운타임 및 생산성 감소
- 평판 훼손
- 시스템 복구 및 패치 적용 비용
- 법률 및 규제 벌금

랜섬웨어 공격을 받으면 기업은 다음 조치를 취해야 합니다.

- 절대적으로 필요한 경우가 아니면 비용을 지불하지 마십시오. 공격자가 접근 권한을 복원할 것이라는 보장은 없습니다.
- 가능한 경우 백업에서 복원하십시오.
- 당국에 공격을 신고하십시오.
- 향후 감염을 방지하기 위해 방어 체계를 강화하십시오(예: 소프트웨어 업데이트 유지, 직원 교육, 엔드포인트 보호 사용).

Dell Technologies와 함께 랜섬웨어 공격에 대응

Dell Technologies는 랜섬웨어 위험이 피해를 입히기 전에 차단하도록 설계된 포괄적이고 미래 지향적인 툴을 조직에 제공합니다.

Dell Trusted Device를 통한 엔드포인트 보안 강화

엔드포인트는 랜섬웨어 공격의 주요 진입점인 경우가 많으므로 엔드포인트 보안은 매우 중요한 중점 영역입니다. Dell Trusted Device는 성능 저하 없이 시스템을 보호하는 하드웨어 지원 보안 기능을 통합합니다. Dell SafeBIOS 및 SafeID와 같은 솔루션은 엔드포인트 디바이스를 무단 액세스로부터 보호하고, Dell SafeData는 회사 방화벽 외부에서도 기밀 정보를 보호하기 위해 데이터를 암호화합니다. 기업은 보안 기능을 디바이스에 직접 내장함으로써 하드웨어 수준에서 보호를 보장하고 공격자가 침투해서 자리를 잡을 기회를 줄입니다.

CrowdStrike를 통한 사전 예방적 탐지

조직이 실시간으로 위협을 탐지하고 대응할 수 있는 적절한 툴을 사용한다면 랜섬웨어 공격이 불가피한 것은 아닙니다. Dell의 솔루션 포트폴리오의 일부로 제공되는 CrowdStrike는 AI 및 행동 분석 기반의 차세대 엔드포인트 보호 플랫폼을 제공합니다. 이 기술은 의심스러운 활동이 공격으로 발전하기 전에 이를 식별하고 무력화합니다. CrowdStrike는 Dell 인프라스트럭처와 완벽하게 통합되어 IT 팀이 전체 환경에 대한 가시성을 유지하여 즉각적이고 효과적인 위협 대응을 제공할 수 있도록 지원합니다.

Dell PowerProtect를 통한 포괄적인 데이터 보호

Dell PowerProtect 솔루션은 랜섬웨어 회복탄력성의 근간입니다. 이러한 고급 데이터 보호 툴은 엔터프라이즈 데이터를 내부 및 외부 위협으로부터 보호하도록 설계되었습니다. 변경 불가능한 백업과 같은 기능은 랜섬웨어에 의해 데이터가 변경, 삭제 또는 암호화될 수 없도록 보장하여 지능형 공격에도 안정적인 안전망을 제공합니다. 예를 들어 Dell PowerProtect Cyber Recovery 볼트는 에어 갭 기술을 사용하여 중요 데이터를 네트워크에서 격리함으로써 가장 정교한 침해 상황에서도 데이터가 손상되지 않도록 보장합니다. 자동화된 이상 징후 탐지 및 지능형 워크플로를 통해 조직은 악의적인 활동을 조기에 탐지하고 랜섬웨어 확산 전에 대응할 수 있습니다.

Dell PowerSwitch 네트워킹 및 SmartFabric OS를 통한 고급 네트워크 보안 및 마이크로 세분화

인프라스트럭처 전반에 걸쳐 고급 네트워크 세분화, 엄격한 액세스 제어, 실시간 트래픽 분석을 제공하여 제로데이 공격에 대한 방어를 강화합니다.

Dell Data Protection Services를 통한 대규모 복구

Dell Technologies는 랜섬웨어 대비 상태에 있어 예방이 중요하지만, 복구 또한 매우 중요하다는 것을 잘 알고 있습니다. Dell Data Protection Services는 자동화된 백업 및 복구 솔루션뿐만 아니라 전문가 주도 컨설팅을 제공하여 기업이 신속하게 복구하고 다운타임을 최소화할 수 있도록 지원합니다. 원격 데이터 복구 및 인시던트 대응과 같은 서비스는 조직이 위기 상황에서 필요한 지원을 받을 수 있도록 보장합니다. 이 포괄적인 접근 방식은 데이터 무결성을 유지하고 복구 시간을 단축하여 운영 중단을 방지합니다.

이는 악의적인 내부자 위협에 대응하는 Dell 솔루션 포트폴리오의 몇 가지 예에 불과합니다.

파트너십을 통한 강점

Dell의 협력적인 접근 방식은 Dell만의 기술을 넘어 보호 범위를 확장합니다. CrowdStrike 및 Secureworks와 같은 선도적인 사이버 보안 기업과의 파트너십을 통해 Dell은 가능한 모든 공격 벡터를 해결하는 통합 솔루션 생태계를 제공합니다. 이러한 솔루션을 함께 사용하면 포괄적인 보안 적용 범위가 제공되므로 기업은 고유한 위험 프로파일에 맞춤화된 다중 계층 방어 체계를 구축할 수 있습니다.

Dell을 선택해야 하는 이유

Dell Technologies는 단순한 기술 공급업체가 아니라 랜섬웨어와의 전쟁에서 신뢰할 수 있는 파트너입니다. Dell Technologies는 혁신, 전문성, 그리고 기업 역량 강화를 위한 헌신을 결합하여 조직에 진화하는 위협에 맞서는 데 필요한 툴과 확신을 제공합니다. 엔드포인트 보안, 중요 데이터 보호 또는 신속한 복구 지원 등 어떤 용도로든 Dell Technologies의 제품과 서비스는 운영 연속성과 안심할 수 있는 환경을 보장합니다.

회복탄력적인 미래 건설

랜섬웨어 공격은 끊임없이 진화하고 있지만, Dell Technologies와 함께라면 기업은 한발 앞서 나갈 수 있습니다. 첨단 하드웨어, 소프트웨어 및 서비스를 활용하여 조직은 회복탄력성, 적응력, 신뢰성을 갖춘 사이버 보안 프레임워크를 구축할 수 있습니다. 랜섬웨어에 맞서는 Dell Technologies의 포괄적인 솔루션으로 지금 바로 데이터를 보호하고 운영을 보호하며 비즈니스의 미래에 대비하십시오.

비즈니스의 회복탄력성을 확보하려면 현재 위협 환경을 이해하고 새로운 위협에 대한 최신 정보를 파악하는 것이 중요합니다. Dell Technologies의 사이버 보안 전문가들은 새로운 공격 벡터(이를 뭐라고 부를까요?)를 지속적으로 모니터링하고 제품 및 서비스의 잠재적 취약성을 사전 예방적으로 해결하기 위해 노력합니다. 이를 통해 끊임없이 진화하는 랜섬웨어 위협에 맞서 최신 보호 기능을 제공할 수 있습니다.

기업은 최신 정보를 파악하는 것 외에도 다층적인 보안 접근 방식을 도입해야 합니다. 즉, 방화벽, 멀웨어 방지 소프트웨어, 침입 탐지 시스템, 데이터 백업과 같은 다양한 보안 조치를 구축해야 합니다. 방어 전략을 다각화하면 어떠한 공격의 영향도 최소화할 수 있고, 랜섬웨어 시도가 성공하더라도 비즈니스 운영을 유지할 수 있습니다.

보안 조치를 정기적으로 테스트하고 업데이트하는 것(시스템 패치 적용 및 정책 업데이트)도 중요합니다. 해커들은 기존 보안 조치를 우회하는 새로운 방법을 끊임없이 찾고 있으므로, 기업은 정기적으로 방어 체계를 테스트하고 필요에 따라 업데이트하여 앞서 나가는 것이 매우 중요합니다. 여기에는 정기적인 취약성 진단, 침투 테스트 및 패치 관리가 포함됩니다.

랜섬웨어로부터 비즈니스를 보호하는 또 다른 주요 측면은 직원들에게 사이버 보안 모범 사례를 교육하는 것입니다. 많은 랜섬웨어 공격은 피싱 이메일이나 악성 링크와 같은 소셜 엔지니어링 전술을 통해 시작됩니다. 직원들에게 이러한 위협을 발견하고 피하는 방법을 교육함으로써 공격 성공 가능성을 크게 줄일 수 있습니다.

또한 재해 복구 계획을 수립하면 랜섬웨어 공격의 영향을 크게 완화할 수 있습니다. 이 계획에는 중요한 데이터 및 시스템의 정규 백업과 공격 대응 및 복구를 위한 명확한 절차가 포함되어야 합니다.

이러한 사전 예방적 조치 외에 강력한 인시던트 대응 계획을 수립하는 것도 중요합니다. 여기에는 랜섬웨어 공격 처리를 위한 명확하게 정의된 역할과 책임뿐만 아니라 이해 관계자에게 알리고 피해를 완화하기 위한 통신 프로토콜이 포함됩니다.

마지막으로, 랜섬웨어 공격의 최신 동향과 발전 상황에 대한 정보를 지속적으로 파악하면 잠재적 위협보다 한발 앞서 대응하는 데 도움이 됩니다. 업계 보고서와 보안 전문가의 업데이트를 정기적으로 검토함으로써 비즈니스를 보호하기 위한 새로운 보안 조치를 사전 예방적으로 구현할 수 있습니다.

어떤 기업도 랜섬웨어 공격으로부터 자유로울 수는 없지만, 적절한 전략과 툴을 갖추면 이러한 공격의 위험과 영향을 최소화할 수 있습니다. 사이버 보안에 대한 사전 예방적 접근 방식을 취하면 비즈니스를 보호할 뿐만 아니라 고객 및 이해 관계자와의 신뢰를 구축할 수 있습니다.

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