서비스 개요

Cyber Recovery 서비스

Cyber Recovery 전략 개발 및 복구 프로그램 구축

주요 특징

Dell Technologies Cyber Recovery 서비스:

- 사이버 공격 후 핵심 비즈니스 기능을 복구할 수 있는 Cyber Recovery 볼트에 MVC(Minimum Viable Company) 구축
- 복구 전략 및 전사적 인시던트 대응 계획과의 통합 지점에 대한 조언
- 다양한 위협 벡터를 계획하고 복구 솔루션에 맞게 조정된 NIST Cybersecurity Framework 통합
- 복구 계획 및 절차의 개발과 테스트

비즈니스 과제

사이버 공격은 이제 일상적인 일이 되었습니다. 사이버 공격을 받으면 다운타임이 길어져 비즈니스 운영이 며칠씩, 심지어는 몇 주씩 중단될 수도 있으며, 그러면 금전적으로도 엄청난 손실이 발생하게 됩니다. 기밀 정보나 독점 데이터의 노출에 대한 우려를 넘어, 많은 사이버 공격이 데이터를 파괴하거나 데이터를 암호화해 이를 인질로 몸값을 요구하도록 설계되는 경우가 점점 늘어나고 있습니다. 최근 발생한 대다수 랜섬웨어 공격은 제조 시스템, 병원 정보 시스템, 뱅킹 시스템 및 지방 정부에 특히 큰 피해를 주었습니다. 이러한 공격은 경계에 있는 기존의 보안 제어 시스템을 우회할 수 있으므로 공격자가 몇 달 또는 경우에 따라 몇 년 동안 탐지되지 않은 상태로 최대한 많은 시스템에 영향을 미치고 비즈니스의 복구 준비를 어렵게 만듭니다. 안타깝게도 조직 외부의 해커뿐만 아니라 내부자가 연루되는 사이버 공격 수도 늘어나고 있기 때문에 모든 유형의 위협으로부터 비즈니스를 보호할 수 있는 리더십이 필요한 상황입니다. 이러한 요소로 인해 모든 업계의 비즈니스 리더들은 사이버 공격 발생 시 신속한 복구의 보장을 요구하게 되었습니다.

사이버 공격이 갈수록 지능화하고 파괴력이 커짐에 따라 기업들은 "최후의 방어선"이 될 새로운 데이터 보호 및 Cyber Recovery 활용 사례를 도입하여 심각한 사이버 공격 이후에도 비즈니스를 유지할 수 있는 방안을 고려해야 합니다.

서비스 설명

최신 접근 방식의 특징은 가장 중요한 데이터(예: 필수 애플리케이션, 데이터 및 지적 재산)의 격리된 복제본을 운영 백업 시스템에서 분리된 상태로 운영 네트워크 외부에 유지하는 것입니다. 직접적인 네트워크 연결과 다수의 롤백 시점이 제공되지 않으므로 손상되지 않은 "골드 카피(gold copy)"를 항상 복구용으로 준비할 수 있습니다.

Dell EMC PowerProtect Cyber Recovery 는 안전한 데이터 보호 볼트를 구현하는 데 도움이 되며 Dell Technologies Services 와 함께 사용할 경우 기술 및 프로세스의 도입을 가속화하여 사이버 공격으로부터 복구할 수 있는 능력에 대한 신뢰도를 높입니다. Dell Technologies 의 서비스는 자문과 구축의 두 가지 주요 영역에 중점을 두고 있습니다.

자문 단계는 데이터 보호 환경에서 Cyber Recovery 솔루션을 통합하고 최적화하기 위한 권장 사항을 중점적으로 제공합니다. 이러한 자문은 현재 상태를 분석하고 미래를 전망하여 맞춤형 Cyber Recovery 대비 전략을 수립하고 보호 및 복구에 대한 비즈니스 요구에 맞게 긴밀하게 연계하는 방식으로 이루어집니다.

자문 단계의 핵심 구성 요소는 애플리케이션에 대한 데이터를 수집하고 정상적인 비즈니스 운영의 중요성을 이해하는 데 필수적인 워크샵 및 정보 세션입니다. 이러한 고려 사항은 Cyber Recovery 볼트로 보호해야 하는 데이터에 대한 권장 사항을 도출하고, MVC(Minimum Viable Company)를 구성하는 데 도움이 됩니다. 여기서 MVC 란 핵심 기능을 먼저 재구축한 다음 비즈니스를 다시 운영하는 데 사용할 수 있는 가장 중요한 데이터와 애플리케이션의 모음입니다.

구축 단계에서는 Cyber Recovery 솔루션을 데이터 보호 환경에 통합합니다. 이 단계에서는 자문 단계를 통해 수집한 정보를 사용하여 요구 사항에 정확히 맞게 솔루션을 추가로 조정할 수 있습니다. 그리고 다음과 같은 추가 기술 및 기능을 Cyber Recovery 환경과 통합할 수도 있습니다.

- 볼트 인프라스트럭처 구축
- CyberSense 분석을 구축하여 데이터를 분석하고 침해 지표를 조기에 식별
- Cyber Recovery 볼트 요구 사항을 지원하도록 운영 백업 수정
- 추가 운영 Dell Technologies 인프라스트럭처 강화
- Cyber Recovery 볼트 및 기능을 메인프레임 환경과 통합
- 여러 플랫폼, 이기종 기술, 보존 정책 및 애플리케이션을 포함하는 Cyber Recovery 볼트 생성
- 볼트에서 복구를 실행하기 위한 자세한 운영 절차(복구 런북) 개발
- 확장된 복구 런북 및 추가 테스트 시나리오 제작 지원

기대 효과 요약

사이버 공격이 급증하면서 이제는 만약이 아닌 조직이 영향을 받는 시점의 문제가 되었습니다. 모든 비즈니스에는 사이버 인시던트 대응 및 Cyber Recovery 전략으로 충족되는 고유한 목표와 IT 요구 사항이 있습니다. Dell Technologies 컨설팅 전문가는 고객과 협력하여 심각한 사이버 공격 발생 시 고객이 비즈니스를 보호하고 복구할 수 있는 프로세스 및 절차를 개발합니다.

Dell Technologies Services 의 기능:

- 안전한 Cyber Recovery 볼트 솔루션 및 권장 사항을 통해 볼트에 MVC(Minimum Viable Company)를 구축하고 사이버 공격 발생 시 복구 지원.
- 특정 핵심 애플리케이션의 복구 기능을 보호하고 검증하여 점점 더 엄격해지는 규제 압력 등에 대응해 규정 준수 목표를 달성하도록 지원.
- 복구 전략에 맞게 조정된 NIST Cybersecurity Framework 를 인시던트 대응 준비 과정에 통합

Dell Technologies Services 에 대한 자세한 정보

Dell Technologies 전문가에게 문의

추가 리소스 보기

대화에 참여: #DellTechnologies