스토리지 구성과 관리의 비결: 효과적인 사이버 복원 전략 구축 방법

01
글로벌 비즈니스가 직면하고 있는 위협

02
사이버 보안 및 리스크 관리

03
NIST 프레임워크: IBM 사이버 복원 라이프사이클의 기반

04
스토리지 인프라의 역할

05
스토리지 인프라 솔루션

06
최적의 보안 균형 유지

글로벌 비즈니스가 직면한 위협

사용자의 실수, 시스템 결함 또는 악의적인 범죄 행위 등 다양한 지점에서 발생하는 데이터 유출은 그 원인이 무엇인지와 상관없이 오늘날 비즈니스에 가장 심각하고 비용이 많이 드는 위협 중 하나입니다. 최근 Ponemon Institute의 연구에 따르면 지난 12개월 동안 전 세계적으로 발생한 데이터 유출로 인한 평균 비용은 386만 달러였습니다.[1] 데이터 유출의 영향을 받은 조직은 정상적인 비즈니스 운영이 중단될뿐만 아니라 업계 내에서 귀중한 데이터, 고객 및 명성을 잃을 위험에 직면하게 됩니다.

물론 인적 희생도 따릅니다. 세계 경제 포럼(WEF)의 2019 세계 위험 보고서에서 사이버 공격은 인간 복지의 가장 큰 위험 요소 중 하나로 평가되었습니다. WEF 설문조사에 응한 사람들 중 82%는 사이버 공격으로 인한 데이터 또는 돈의 도난 위험이 증가할 것으로 예상하고 있으며, 80%는 운영 및 인프라 중단 위험의 증가를 목격했다고 밝혔습니다.[2]

IT 조직이 만연한 보안 위협으로 인한 새로운 도전과제에 대처하기 위해서는 현재 보안에 대한 체계적인 접근 방식이 필요합니다. 선도 기업은 Safeguarded Copy와 같은 혁신적인 스토리지 기술을 채택하고 있습니다. 또한 기존의 매우 효과적인 물리적 에어 갭 (air gap) 방식을 활용하여 위협을 근절하고 비즈니스 기대치를 충족시킵니다. 이러한 접근 방식을 실행하는 열쇠는 성공적인 리스크 관리에 있습니다.

IT 조직이 만연한 보안 위협으로 인한 새로운 도전과제에 대처하기 위해서는 현재 보안에 대한 체계적인 접근 방식이 필요합니다.

사이버 보안 및 리스크 관리

조직이 혼란으로부터 스스로를 보호하거나 비용을 최소화하는 데 사용 가능한 여러 가지 방법이 있습니다. Ponemon Institute는 데이터 유출 비용을 낮추기 위한 4가지 전략을 다음과 같이 제안합니다: [1]

- 사고 대응 팀 구성
- 강력한 암호화 사용
- 비즈니스 연속성 관리 도입
- 직원 교육 개선

강력한 사이버 보안 전략을 수립하고 유지하려면, 보유하고 있는 데이터와 시스템 자산이 무엇인지, 그 가치가 어떻게 되는지, 그리고 어떤 리스크가 적용되는지 이해하기 위한 절차적 접근 방식을 활용해야 합니다. 조직의 현재와 원하는 보안 상태를 프로파일링하기 위해 리스크 관리 이론을 채택하면 발생 가능한 다양한 구현 계층을 고려할 수 있습니다. 사이버 복원 전략을 평가하고 구현하기 위해서는 강력한 프레임워크가 중요합니다.

사이버 복원 전략을 평가하고 구현하기 위해서는 강력한 프레임워크가 중요합니다.

NIST 프레임워크: IBM 사이버 복원 라이프사이클의 기반

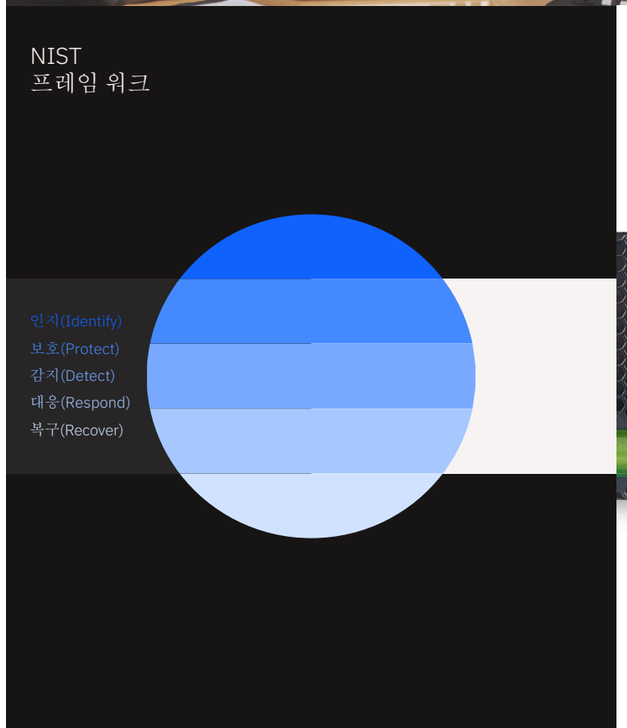
2018년, 미국의 국립 표준 기술 연구소(NIST)에서는 *'핵심 인프라의 사이버 보안 개선을 위한 프레임워크'라는 자료를 발행했습니다.* 프레임워크는 다음과 같은 세 가지 부분으로 구성됩니다. 프레임워크 코어, 프레임워크 구현 계층 및 프레임워크 프로파일.[3]

프레임워크 코어에는 일련의 사이버 보안 기능이 있습니다. 모든 조직은 다음과 같은 필수적이고 달성 가능한 조치를 취할 수 있습니다:

- **인지(Identify):** 시스템, 사람, 자산, 데이터 및 기능에 부여된 사이버 보안 위협의 리스크에 대한 조직의 이해를 촉진합니다.
- **보호(Protect):** 적절한 보호 조치를 통해 중요한 서비스가 제공되도록 보장합니다.
- **감지(Detect):** 보안 문제가 발생할 경우 즉각적으로 감지합니다.
- **대응(Respond):** 사이버 보안 사고에 대한 조치를 취합니다.
- **복구(Recover):** 사이버 보안 사고에 의해 침해된 기능 또는 서비스를 복원합니다.

이러한 기능들은 상호 작용하여 사이버 보안 리스크에 대한 조직의 관리에 더 나은 가시성을 제공합니다. 조직은 이에 대해 보다 명백히 이해함으로써, 해당 스토리지 솔루션에서 위협 요소를 없앨 수 있습니다.

이러한 기능들은 상호 작용하여 사이버 보안 리스크에 대한 조직의 관리에 더 나은 가시성을 제공합니다.



스토리지 인프라의 역할

스토리지는 오랫동안 기업 운영 측면에서 “데이터 관리자”로서의 역할을 해왔습니다. 시스템 스토리지 계층은 메인 메모리의 데이터가 저장되는 컨테이너를 제공하는 것 외에도 비정상적인 상황이 발생했을때 이를 복구할 수 있도록 도움이 되는 보호 기능을 제공했습니다. 시간이 경과함에 따라 다음과 같은 기능들의 범위가 증가하게 되었습니다.

- **백업:** 1960년대부터, 애플리케이션 사용자는 실수로 인한 삭제, 손상 또는 1차 장치 결함 등으로부터 데이터를 보호하기 위해 스토리지를 사용해 버전 별로 데이터를 저장할 수 있었습니다.
- **고가용성:** 스토리지는 지난 20여 년 동안 다중 경로 액세스, 다중 서버 액세스 및 서버 룸 내에서의 온라인 데이터 복제 등을 구현하는데 기반이 되었습니다.
- **장애 복구:** 1990년대 후반부터, 스토리지는 정전 또는 자연재해로부터 데이터를 보호하기위해 충분히 먼 원격지에 백업본을 생성하는 솔루션을 구현할 수 있게 해주었습니다.
- **신속한 온라인 데이터 복구:** 2010년대 초부터, 스토리지는 실수로 인한 데이터 삭제 또는 데이터 손상으로부터 빠른 복구를 위해 데이터의 스냅샷 백업본을 생성하는 솔루션의 기반을 제공하고 있습니다.

이와 같이 여러 위험 상황을 해결하기 위해 스토리지 시스템, 관리 소프트웨어 및 운영 프로세스에 새로운 기능이 도입되었습니다.

일반적인 스토리지 기능에서 사이버 복원 관련 기능으로 전환함에 따라 블록, 파일, 객체, 테이프, 소프트웨어 정의 스토리지 및 클라우드를 통해 제공되는 4가지 주요 기능은 다음과 같습니다.

- **분리(Isolation)** 이는 스토리지 네트워크의 다른 부분으로부터 스냅샷 또는 백업 데이터를 격리하는 정도를 말합니다. 분리는 Safeguarded Copy, 클라우드 객체 스토리지와 같은 논리적 수단 또는 물리적 에어 갭과 같은 물리적 방법을 통해 구현할 수 있습니다.
- **불변성(Immutability)**또는 위변조 방지 스토리지는 외부 또는 내부 공격자가 데이터를 변경하거나 삭제하지 못하게 만듭니다.
- **성능(Performance)** 사이버 복원 프레임워크의 핵심 기능입니다. 조직이 사이버 공격으로부터 얼마나 빨리 복구할 수 있습니까? 테이프는 백업 데이터의 격리와 불변성에 있어 매우 우수하지만 복구하는 데 몇 시간이 걸릴 수 있습니다.
- **재사용의 용이성(Ease of reuse)**또는 백업 데이터의 접근 용이성은 복구 절차를 테스트하고 백업의 유효성을 검증하며 랜섬웨어 사고 발생 시 유효한 복원 지점을 찾기 위해 데이터를 샌드박스 환경에서 복원하는데 중요한 기능입니다.

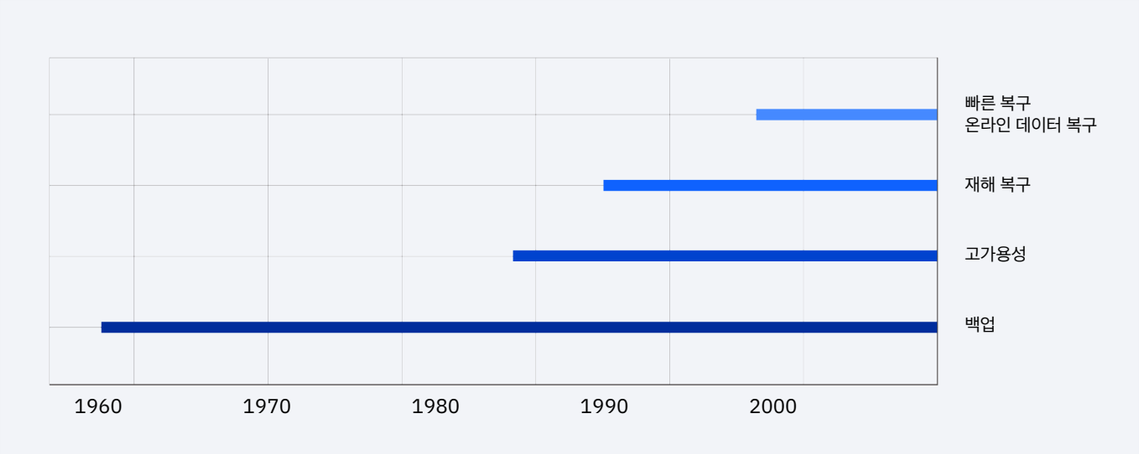


그림 1: 데이터 복구 솔루션의 변화

사이버 공격, 특히 랜섬웨어 또는 와이퍼 공격을 통한 논리적 데이터 손상(LDC) 위협은 새로운 보안 고려 사항을 제시합니다. 솔루션 제공업체는 필요한 수준의 복원력을 제공하기 위해 이미 사용하고 있는 백업 및 재해 복구 솔루션을 활용할 수도 있습니다. 하지만 새로운 위협을 해결하기 위해서는 새로운 스토리지 기능이 필요합니다.

정교한 멀웨어 공격에 직면한 경우라도 최신의 복구용 데이터 백업본을 보존하기 위해 스토리지 기능과 운영 프로세스를 결합하는 메커니즘이 필요합니다. 공격이 감지되고 대응 체계가 발동하면 보존된 최신 데이터 백업본을 사용하여 애플리케이션을 재시작하고 정상적인 서비스를 재개할 수 있습니다.

IBM® Safeguarded Copy는 변경 불가능한 특정 시점의 프로덕션 데이터 백업본 및 이중 제어 보안으로 사용자 실수, 악의적인 파괴, 멀웨어 또는 랜섬웨어 공격으로 인해 데이터가 수정되거나 삭제되는 것을 방지합니다.

IBM Redpaper *DS8000® Safeguarded Copy* 는 보존용 백업본을 생성하기 위해 필요한 세 가지 새로운 기능을 다음과 같이 정리합니다:

- **백업 단위화(Granularity):** 데이터 손상 사고 시 데이터 손실을 최소화하기 위해 여러 버전의 보존용 백업본을 만들 수 있어야 합니다.
- **분리(Isolation):** 문제가 생긴 호스트 시스템으로 인해 보존용 백업본이 손상될 수 없도록 사용 중인 프로덕션 데이터와 분리해야 합니다. (이는 “에어 갭”으로도 알려져 있습니다.)
- **불변성(Immutability):** 보존용 백업본이 조작되지 못하도록 보호되어야 합니다.[4]

IDC는 '사이버 복원 프레임워크 활성화를 위한 5가지 핵심 기술' 백서에서 자동화 및 오케스트레이션과 규제준수 점검 보고 및 보증이라는 두 가지 고려 사항을 추가했습니다.[3] LDC 공격 복원력에만 적용되는 것은 아니지만, 권장 실행 목록에 포함하기에 적합합니다.

스토리지 인프라 솔루션

성공적인 스토리지 솔루션은 LDC 공격이나 실수로 인한 데이터 손상이 발생했을 때 복원력 있는 IT 운영이 가능하게 해주는 매우 다양한 기능을 제공합니다. 포괄적 솔루션은 스토리지 기능, 네트워크 구성, 관리 제어 및 물리 보안 기능을 결합하고 있습니다.

스냅샷, WORM(Write Once, Read Many) 미디어를 사용하여 보호된 백업, 테이프 에어 갭 보호 및 클라우드 오브젝트 스토리지 등 현재 사용 가능한 주요 사이버 복원 솔루션과 기술 중 일부를 살펴보겠습니다.

전통적인 스냅샷 기반 백업 및 복구

스냅샷은 기존 백업 요구 사항을 해결하기 위한 최고의 비용 효율적인 방법 중 하나가 되었습니다. 공간 효율적인 읽기 전용 데이터 백업본은 이전의 데이터 버전을 신속하게 복원하는 데 사용 가능한 비용 효과적인 복원 지점을 제공합니다. 실수로 인한 삭제나 데이터 손상으로부터 복구하기 위해 스냅샷을 활용하는 추세가 점점 더 늘고 있습니다.

보호된 스냅샷

스냅샷을 보호하는 최상의 방법은 무엇입니까? 하나의 접근 방식은 프로덕션 시스템의 스토리지 볼륨을 동일한 유형의 보조 스토리지 시스템으로 복제하는 것입니다. 그런 다음, 주기적 스냅샷을 보조 어레이의 복구 백업본으로 사용할 수 있습니다. 복제 및 스냅샷 기능은 소프트웨어를 통해 자동화해야 합니다. 백업 전용 스토리지 시스템은 애플리케이션 서버에 직접 연결해서는 안되며, 백업할 데이터를 받는 포트만이 이 스토리지 시스템의 유일한 데이터 연결 통로이어야 합니다.

LDC 멀웨어 공격이나 복구 조치 테스트의 경우, 이 백업용 스토리지 시스템에 저장된 데이터 백업본을 프로덕션 스토리지 시스템으로 다시 이동할 수 있는 복구용 백업본의 소스로 사용해야 합니다. 백업 전용 스토리지 시스템을 사용하면 프로덕션과 보호 백업본 사이에 논리적인 에어 갭이 생깁니다. 시스템 간의 물리적인 분리는 구현 설계의 문제입니다. 백업 전용 스토리지 시스템을 동일한 데이터 센터내에 혹은 가까운 거리에 설치하면 백업 성능이 향상되고 네트워크 비용을 절감할 수 있습니다. 또한 백업 전용 스토리지 시스템이 DR에 사용되는 원격 시설에 설치될 수도 있습니다.

WORM 미디어로 보호된 백업
백업 및 아카이브 소프트웨어 시스템은 전체 데이터 백업본을 관리형 스토리지 공간에 저장한 후에 변경된 데이터만 저장하여 백업 버전을 유지 및 관리할 수 있도록 해줍니다. 복구용 백업본을 보호하는 데 WORM 미디어가 유용할 수 있습니다. 테이프 카트리지는 WORM 미디어로 테이프 드라이브에 의해 덮어 쓰기가 비활성화된 복구용 백업본을 생성하는 데 사용됩니다. 한번 WORM 카트리지로 설정되면 애플리케이션이나 관리 서버의 어떤 멀웨어라도 백업본을 파괴할 수 없습니다.

공간 효율적인 스냅샷과 달리 테이프에 생성되는 전체 백업본은 데이터를 백업하는 데 시간이 걸립니다. 복원 속도는 스냅샷으로 수행할 수 있는 속도보다 훨씬 느립니다. 각 비즈니스의 요구에 맞게 설계 요소를 개별적으로 정의해야 하겠지만 오프라인 미디어에 데이터를 보존하는 백업으로 보강된 스냅샷 기반 복구 솔루션을 사용하여 완벽한 방어망을 구축하는 것이 바람직합니다.

강력한 테이프 에어 갭 보호
“에어 갭”은 멀웨어 감염, 시스템 결함 또는 사용자 실수로 인해 발생할 수 있는 데이터 손상을 방지하기 위해 물리적이거나 가상적인 시스템 또는 네트워크 분리를 의미합니다. 에어 갭의 기본적인 개념은 분리된 백업 전용 스토리지 시스템을 주기적으로 온라인으로 가져와 최신 변경 사항을 백업하고 다시 오프라인으로 유지하는 것입니다. 백업본 생성에 스냅샷 방식을 도입하면 손상된 애플리케이션을 신속하게 복원할 수 있습니다.

하지만 백업된 데이터를 완벽하게 보호하는 것에는 몇 가지 제약이 따릅니다. 보호된 백업본에 대한 네트워크 또는 소프트웨어 액세스를 제공하지 않는 가장 완벽한 보호 접근 방식은 테이프 라이브러리를 사용하여 구현할 수 있습니다. 테이프의 기본적인 오프라인 특성은 실제 물리적인 에어 갭을 제공하며 사이버 범죄를 근절하는 가장 안전한 보호 옵션 중 하나를 제공합니다.

에어 갭 기법, WORM 및 기타 보안 기능의 활용 등 테이프를 통한 데이터 보호의 보다 자세한 정보는 '현대적이고 강력한 데이터 보호를 제공하는 IBM 테이프 솔루션' 솔루션 보고서를 참고하십시오.

클라우드 오브젝트 스토리지로 데이터 보호
클라우드 오브젝트 스토리지는 데이터를 저장하고 보호하는 데 지속 가능하고 안전하며 비용 효과적인 방법입니다. 정책 정의를 통해 기본, 최소 및 최대 보존 기간에 대한 유연성을 확보할 수 있습니다. 이러한 보존 기간과 추가적인 법적 보유 기간은 데이터가 클라우드에 저장될 때 단일 객체나 다중 객체 단위로 적용할 수 있습니다. 이것은 보존 기간과 모든 법적 보유 기간이 만료될 때까지는 해당 데이터 객체를 삭제할 수 없다는 의미입니다.

최적의 보안 균형 유지

데이터에 대한 액세스를 차단하거나 데이터를 손상시키는 사이버 공격은 줄지 않고 있습니다. 사실, 더욱 정교해 지고 있습니다. 그렇기 때문에 조직이 사용하는 기술과 데이터 보호 원칙 사이에서 적절한 균형을 유지하는 것이 효과적인 보안 전략을 구축하는 데 필수적인 요소입니다. 성공적인 공격의 피해를 복구하는 절차도 잘 설계된 보안 체계의 중요한 부분입니다.

두 가지 경우 모두에서, 일련의 위협으로부터 시스템을 보호하는데 핵심 보안 기능을 갖춘 여러 스토리지 솔루션이 중요한 역할을 수행합니다. 그러나 현재의 위협 환경과 보호해야 할 정보를 제대로 이해하지 못하면 적절한 균형을 맞추는 것이 매우 어려울 수 있습니다.

기업들은 포괄적인 스토리지 전략을 구축하는 데 도움이 되는 NIST 프레임워크나 리스크 관리 규정과 같은 접근 방식을 활용할 수 있습니다. 증가하는 보안 위협에 대응하기 위한 사이버 복원 솔루션을 구현하는데 스냅샷, 테이프 에어 갭 보호 및 클라우드 오브젝트 스토리지와 같은 기술을 사용할 수 있습니다.

피해를 입지 않도록 미리 준비하십시오. 잘 조율된 사이버 복원 전략 구현에 대해 보다 자세히 알아보려면 다음 웹 사이트를 방문하십시오. https://www.ibm.com/kr-ko/it-infrastructure/storage/mainframe.

참고 자료

1. “2018 Cost of a Data Breach Study: Global Overview.” Ponemon Institute, July 2018.
2. “Global Risks Report 2019, 14th Edition.” World Economic Forum, Geneva, Switzerland, 2019.
3. Phil Goodwin and Sean Pike, “Five key technologies for enabling a cyber resilience framework.” IDC, July 2018.
4. Bert Dufrasne, Francesco Anderloni, Roger Eriksson, and Lisa Martinez. “IBM FlashSystem A9000 and A9000R Business Continuity Solutions, A draft IBM Redpaper publication.” IBM Corp., November 2018.