RFP 가이드

랜섬웨어 보호

PURESTORAGE®
Uncomplicate Data Storage, Forever

목차

개요

랜섬웨어란?

랜섬웨어는 파일을 암호화하고 데이터에 대한 액세스를 복원해주는 대가로 비용을 요구하는 멀웨어(악성 코드)의 한 유형입니다. 그러나 공격자가 대가를 받고 약속을 지킨다는 보장이 없기 때문에 사이버 보안 모범 사례와 주기적인 스냅샷을 통해 랜섬웨어를 예방하는 것이 최선의 선택입니다.

랜섬웨어는 어떻게 작동할까요?

모든 악성 프로그램과 마찬가지로 랜섬웨어가 데이터에 액세스하려면 누군가 시스템이나 네트워크에 이를 다운로드해야 합니다. 랜섬웨어에 감염되는 가장 일반적인 방법은 피싱 이메일을 통해 전달되는 첨부 파일을 다운로드하는 것이지만, USB 드라이브, 손상된 앱, 감염된 웹 사이트도 공격 경로가 될 수 있습니다.

랜섬웨어가 다운로드되고 실행되면 호스트 시스템의 파일을 암호화하고 올바른 암호 해독 키 없이는 시스템을 액세스할 수 없도록 만듭니다. 일반적으로 손상된 파일 시스템의 소유자에게 파일에 다시 액세스하기 위한 대가를 지불하는 세부적인 방법이 포함된 이메일이 전송됩니다. NotPetya(영문자료) 등 보다 정교한 랜섬웨어는 사용자의 실수에 의존하지 않고 주요 시스템의 소프트웨어 취약성을 악용해 페이로드를 전달합니다.

공격이 증가하고 있을까요?

랜섬웨어 공격은 매우 흔하게 발생하고 있습니다. 이제 하루에 얼마나 많은 사이버 공격이 발생하는가가 아니라, 초당 공격 수로 측정됩니다. 과거에는 규모가 크고 잘 알려진 조직들만 랜섬웨어의 표적이 되었지만, 이제는 규모에 관계없이 모든 조직이 대비해야 합니다.

미국의 사이버 보안 연구 기업 Cybersecurity Ventures(영문자료)가 실시한 연구 조사에 따르면 2021년에는 11초마다 랜섬웨어 공격이 발생했습니다. 2031년에는 3초마다 공격이 발생하여 멀웨어로 야기되는 다운타임 비용, 복구 시간, 매출 손실 등을 포함한 총 피해 규모가 향후 5년간 해마다 15%씩 성장할 것으로 예상됩니다.

랜섬웨어 공격을 어떻게 방지할 수 있을까요?

랜섬웨어 공격을 방지하는 일반적인 방법은 다음과 같습니다.

- 알려진 결함과 취약성보다 한발 앞서 갈 수 있도록 운영 체제 및 기술 스택을 최신 상태로 유지
- 사이버 보안에 대한 투자(예: 정보 보안 교육, 네트워크 보안 감사 및 취약성 테스트)
- 관리자 권한 관리를 통해 보안 파일 및 데이터에 대한 액세스 제어
- 스냅샷 및 기타 데이터 보호 방법을 통한 잦은 파일 백업

조직의 경영이 시스템과 데이터에 크게 의존하는 시대에는, 필요한 것을 필요할 때 복구할 수 있는 능력이 필수적입니다. 시스템이 중단되고 데이터를 사용할 수 없게 될 경우 한시가 급해집니다. 재난이나 랜섬웨어가 발생했을 때 어떤 일이 일어날지를 생각하고 계획하는 것이 중요합니다.

오늘날 시장에는 다양한 랜섬웨어 솔루션이 나와 있습니다. 이러한 솔루션은 크게 세 가지 카테고리로 나뉩니다.

- **예방 및 알림:** 네트워크 및 시스템에 대한 무단 액세스를 방지합니다. 또한 멀웨어 설치를 방지하고 IT 팀에 알림을 제공할 수 있습니다.
- **근절:** 멀웨어를 격리하고 제거하는 데 도움을 줍니다. 또한 시스템과 네트워크에 대한 무단 액세스를 가능하게 하는 액세스 포인트를 닫는 데 도움이 될 수 있습니다.
- **피해 완화 및 복구:** 감염되거나 암호화된 시스템 및 데이터를 복원 및 복구합니다.

이 가이드에서는 랜섬웨어 피해 완화 및 복구에 중점을 둡니다.

데이터 보호만으로는 충분하지 않습니다

오늘날 대부분의 조직은 백업 및 복구 또는 데이터 보호 솔루션을 사용하고 있지만 그것만으로는 충분하지 않을 수 있습니다. 얼마 전까지는 감염되거나 암호화된 파일 및 시스템에 대한 백업을 간단히 복원하고 평소처럼 업무를 재개할 수 있었습니다.

그러나 해커들이 이에 대비해 전술을 바꿨습니다. 이제 해커는 공격을 시작하기 몇 주 또는 몇 달 전에 환경에 침투합니다. 해커는 암호화 공격을 시작하기 전에 백업 및 아카이브를 먼저 손상시키고 파괴합니다. 그래야 시스템 복호화를 위해 대가를 지불할 가능성이 높아지기 때문입니다.

가장 중요한 데이터와 애플리케이션을 복구할 수 있다는 것은 가장 좋은 보험입니다.

귀사의 랜섬웨어 피해 완화 및 복구 계획과 솔루션을 평가해야 하는 이유는 무엇일까요?

- 랜섬웨어에 대한 우려가 현재와 가까운 미래의 가장 큰 이유입니다. 백업은 보호되어야 합니다.
- 비용이 많이 드는 다운타임을 방지하기 위해 데이터와 애플리케이션을 신속하게 복원할 수 있어야 합니다. 최근 복구 이벤트가 계획대로 진행되지 않았다면, 신속한 조치가 필요합니다. (예: 데이터베이스 복구가 너무 오래 걸림) 랜섬웨어 문제로 인해 더 빠른 복구가 필요해졌습니다.
- 많은 조직들이 기존 백업 제품에 대한 불만을 토로하고 있습니다. 랜섬웨어 솔루션의 필요성과 결합하면, 지금이 새로운 백업 솔루션을 도입하고 소프트웨어와 스토리지를 포함한 전체 환경을 바꿀 수 있는 절호의 기회입니다.

조직에 중요한 사항 파악하기

다양한 솔루션을 검토하기 전에 자체 평가를 수행하여 어떤 데이터가 비즈니스에 중요한지, 얼마나 많은 데이터가 중요한지, 어떤 애플리케이션이 조직에 가장 중요한지, 중단 후 복구를 위해 조직이 어떤 서비스 수준 계약(SLA)을 설정했는지 파악해야 합니다.

재해 발생 후 주요 목표는 비즈니스에 중요한 데이터와 애플리케이션을 먼저 복원하여 비즈니스를 신속하게 재개할 수 있도록 하는 것입니다. 중요하지 않은 데이터와 시스템에는 비즈니스에 중요한 항목과 다른 SLA가 마련되어야 합니다.

랜섬웨어 솔루션

많은 공급업체가 포괄적인 솔루션을 만들기 위해 다양한 기능 세트와 툴을 함께 결합하지만, 이것이 최선의 전략이 아닐 수 있습니다. 예방(발생 전 공격 방지), 근절(랜섬웨어가 시작되거나 확산된 후 공격을 중지하고 환경에서 제거), 피해 완화 또는 복구(공격 후 복원 및 복구) 분야에서 차별화된 솔루션을 제공하는 공급업체를 찾아야 합니다.

귀사의 IT 담당자가 쉽게 이해하고 운영하여 조직의 SLA를 충족하는 데 도움을 줄 수 있는 솔루션을 찾아야 합니다. 솔루션을 선택했으면 계획을 세우고 단계와 절차를 문서화하고 실천해야 합니다.

이 가이드에서는 공격 후 복구에 중점을 둡니다. 무엇을 복구할 수 있는지, 어떻게, 어떤 기간 내에 복구해야 하는지 랜섬웨어 피해 완화 솔루션을 선택할 때 토론을 거쳐야 합니다. 이는 중요한 주제로, 규모에 관계없이 모든 조직이 신중하게 고려할 필요가 있습니다.

데이터 보호 솔루션 통합

백업은 자연 재해, 인재, 데이터 손상, 우발적인 삭제 등 일반적인 시나리오로부터 중요한 데이터를 보호해줍니다. 그러나 랜섬웨어 공격은 디스크나 테이프 등의 레거시 아키텍처에 구축된 기존 데이터 보호 인프라에 예상치 못했던 큰 부담을 줄 수 있습니다.

먼저, 복구 SLA를 충족하는 데 이미 어려움을 겪고 있다면, 랜섬웨어 공격으로 인해 계획되지 않은 추가적인 다운타임이 발생해 상황이 악화될 수 있습니다. 다음으로 백업 시스템과 데이터가 손상되어 데이터 복구를 고려하기도 전에 백업 솔루션을 다시 설치하고 재구성해야만 할 수 있습니다. Enterprise Strategy Group (ESG)에 따르면, 87%의 조직은 데이터 백업 복사본이 랜섬웨어 공격에 감염되거나 손상될 것을 우려하고 있습니다.

복구 전략

공격으로부터 복구하는 동안 고려해야 하는 두 가지 중요한 사항이 있습니다. 백업에 사용할 수 있는 유효하고 사용 가능한 데이터 복사본이 공격으로부터 안전한가? 그리고 가능한 가장 빠른 복구 방식은 무엇인가? 공격 발생 후 데이터 손상 피해를 완화하는 가장 좋은 방법은 감염된 시스템 및 데이터의 백업을 복원하는 것입니다. 복구 계획을 세울 때, 랜섬웨어 공격 피해 완화의 핵심은 안정성과 복구 속도입니다.

첫째, 데이터를 백업해야 하고, 의도적이고 악의적인 삭제로부터 백업을 보호해야 합니다. 이를 위해서는 백업이 저장되는 시스템이 간단하고 안정적이어서 지속적으로 유지 관리를 할 필요가 없을 뿐만 아니라 불변성을 갖추어야 합니다. 여기서 불변성(immutability)은 오브젝트가 생성된 후 변경이나 삭제되는 것을 방지하는 시스템의 기능을 의미합니다. 이뮤터블 플러스(Immutable Plus)는 관리자의 크리덴셜이 손상된 경우에도 백업의 변경을 방지하는 기능입니다.

둘째, 백업 시스템도 신속하게 복원할 수 있어야 합니다. 심각한 영향을 피할 수 있을 정도로 빠르게 백업을 복원할 수 없다면, 이러한 백업이 존재할 이유가 없습니다. 랜섬웨어 공격 시 백업 시스템이 조직적 또는 재정적으로 큰 영향을 받지 않도록 신속하게 복원할 수 있나요? 데이터센터의 많은 부분이 관여하는 복원을 지원할 수 있나요? 스토리지와 네트워크가 대규모 복구를 처리할 수 있나요?

조직의 SLA가 몇 시간 또는 며칠 단위로 측정되는 경우 인프라가 SLA 목표를 달성할 수 있는지 확인하기 위해, 대규모 공격으로부터 복구하는 데 시간이 얼마나 걸리는지 계산해봐야 합니다.

고려해야 할 사항:

- 대규모 데이터를 마지막으로 복원한 것이 언제인가요?
- 얼마나 걸렸나요?
- 복구를 위한 SLA는 무엇인가요?
- 어디에서 인프라의 병목 현상이 나타나나요?
- 솔루션으로 SLA 목표를 달성할 수 있나요?

훌륭한 제안 요청서(RFP)는 다양한 솔루션과 벤더 간에 공평한 경쟁의 장을 만들어 비교 및 선택을 더 쉽게 만듭니다. RFP를 작성할 때 직면하는 일반적인 과제는 귀사의 요구사항과 공급업체의 제품을 일치시키려면 어떤 질문을 해야 할지 아는 것입니다.

이 프로세스에 도움이 되도록, 퓨어스토리지는 랜섬웨어 피해 완화 및 복구를 위해 RFP 프로세스에 추가할 수 있는 일련의 기준을 마련했습니다. 이러한 기준은 입증된 랜섬웨어 아키텍처를 통한 실제 경험을 기반으로 합니다. 이러한 질문은 스토리지 시스템을 검토하는 데 도움이 될 수 있습니다.

공급업체의 응답을 사용해 현재 및 미래의 요구사항을 공급업체의 주장 및 기능과 비교해 평가해야 합니다. 이 가이드가 모든 것을 포함하지는 않지만 랜섬웨어 피해 완화 솔루션의 주요 요구사항을 파악하는 데 도움이 될 것입니다.

RFP 질문 예시

섹션 1: 데이터 보호 솔루션

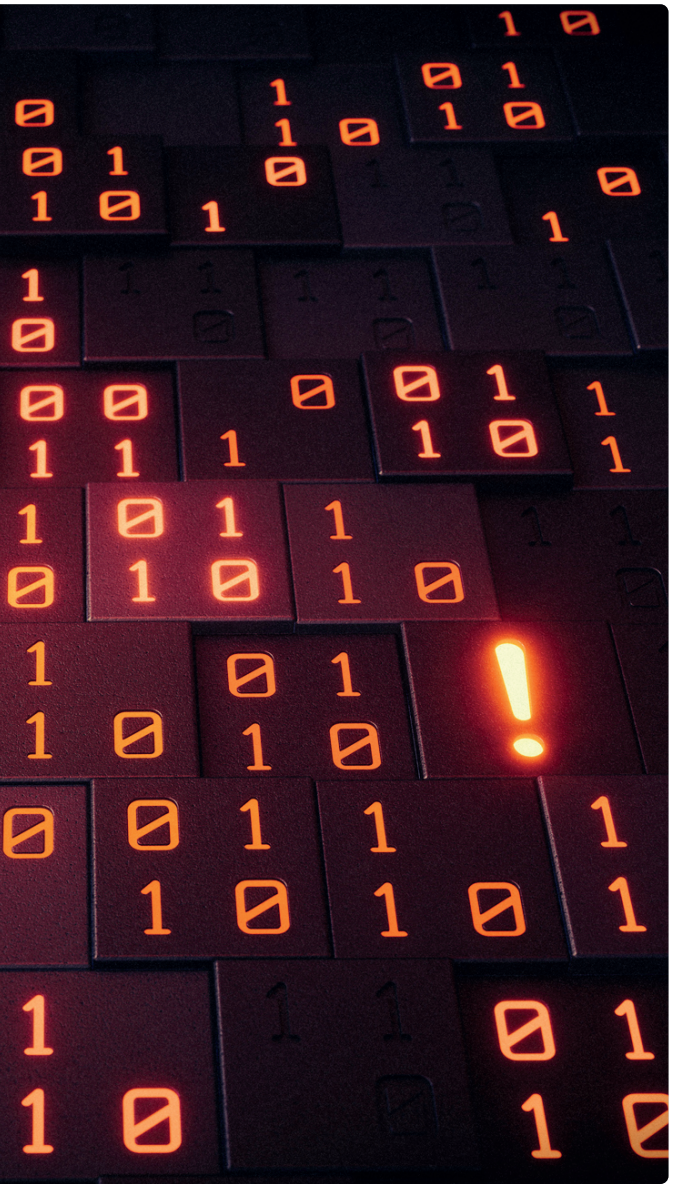
시스템의 데이터 보호 기능을 설명해주세요.

- 솔루션의 구성 요소를 설명해주세요.
- 어떤 데이터 보호 애플리케이션과 통합할 수 있나요?
- 역할 기반 액세스 제어(RBAC)를 제공하나요?
- 재해복구 복사본을 어떻게 보호하나요?
- 솔루션이 복제되나요?
- 솔루션이 온-프레미스, 하이브리드 또는 클라우드 기반인가요?
- 어떤 구매 모델을 제공하나요?
- 어떤 업그레이드 또는 보상 판매 프로그램을 제공하나요?
- 솔루션에 어떤 보고 기능이 포함되어 있나요?
- 솔루션에는 어떤 인증이 포함되어 있나요?
- 귀하의 솔루션은 어떤 규정을 준수하나요?
- 귀사의 솔루션은 어떤 프로토콜을 지원하나요?
- 솔루션에 특정 하드웨어가 필요한가요?
- 업데이트는 어떻게 설치되나요?
- 삭제, 랜섬웨어 및 의도적인 삭제로부터 어떻게 보호를 하나요?
- 어떤 서드파티 랜섬웨어 탐지 공급업체와 통합할 수 있나요?
- 귀사의 솔루션은 제로 데이 공격으로부터 복구하기 위한 오케스트레이션을 제공하나요?
- 귀사의 솔루션은 멀웨어, 우발적인 삭제, 데이터 손상, 기술 장애, 또는 사이트 장애로부터 데이터를 보호하는 기능에 스냅샷, 클론 및 복제 기능을 제공할 수 있나요?
- 귀사의 솔루션은 백업 불변성을 제공하나요?
- 스냅샷 생성, 데이터 복제 및 멀웨어 관리를 위해 제공되는 옵션을 설명해주세요.
- 솔루션을 차별화하는 추가 보안 기능을 설명해주세요.

섹션 2: 백업

시스템의 백업 기능을 설명해주세요.

- 솔루션이 어떻게 랜섬웨어 공격으로부터 조직을 보호하는지 설명해주세요.
- 어떤 워크로드를 보호할 수 있나요?
- 어떤 유형의 시스템을 백업할 수 있나요?
- 전체, 증분 또는 차등 백업을 사용하나요?
- 중복 제거를 사용하나요? 어떤 유형이 사용되나요?
- 데이터는 어떻게 백업되나요?
- 복구 가능성을 어떻게 보장하나요?
- 백업 또는 스냅샷은 얼마나 자주 실행되나요?
- 귀사의 솔루션은 변경 불가능한 백업을 생성할 수 있나요?
- 불변성을 어떻게 보장하나요?
- 귀사의 솔루션은 자동 복구 기능을 제공하나요?
- 변경할 수 없는 백업 또는 스냅샷을 제공하나요?
- 변경할 수 없는 백업 또는 스냅샷은 어떤 프로세스를 통해 생성되나요?
- 변경할 수 없는 스냅샷이 IT 환경 내부에 있나요, 아니면 외부에 있나요?
- 귀사의 솔루션은 백업 테스트를 제공하나요?
- 귀사의 솔루션은 데이터 백업을 계층화하나요?
- 변조 또는 삭제로부터 백업을 어떻게 보호하나요?



섹션 3: 복구

솔루션의 복구 역량을 설명해주세요.

- 솔루션이 제공할 수 있는 복구 시간 목표(RTO)는 무엇인가요?
- 귀사의 솔루션은 자동화된 페일오버를 제공하나요?
- 귀하의 솔루션은 즉각적인 복구를 제공하나요?
- 변경할 수 없는 스냅샷 또는 백업은 어떻게 복구되나요?
- 중복 제거는 복구 시간에 어떤 영향을 주나요?
- 데이터는 어떻게 복원되나요?
- 변경할 수 없는 복사본을 어떻게 복구하나요?
- 예상되는 복원 속도는 얼마나 되나요?
- 24시간 동안 얼마나 많은 데이터를 복원할 수 있나요?
- 어떤 수준의 복원 세분성이 제공되나요? (파일, 특정 시점, 증분, 차등 등)
- 클라우드 기반 스토리지에 어떻게 페일오버를 하나요?
- 클라우드 기반 스토리지의 경우 데이터를 온프레미스로 다시 마이그레이션하는 데 이그레스 요금이 발생하나요?

섹션 4: 인프라

솔루션의 인프라에 대해 설명해주세요.

- 대규모 복원을 수행하려면 솔루션에 어떤 유형의 스토리지가 필요합니까? 필요한 네트워크 속도는 얼마나 되나요?
- 백업은 어디에 저장되나요? 백업이 클라우드에 저장될 수 있나요?
- 필요한 스토리지 용량은 얼마나 되나요?
- 변경할 수 없는 백업에는 어느 정도의 스토리지 용량이 필요한가요?

유용한 자료

퓨어스토리지 랜섬웨어 솔루션 소개

퓨어스토리지는 올플래시 데이터센터부터 가장 현대적인 데이터 보호 솔루션과 에버그린(Evergreen) 구독 모델에 이르기까지 항상 혁신을 선도해 왔습니다.

퓨어스토리지는 모든 것을 유연하게 소비할 수 있는 서비스로 제공하며 클라우드의 경제성을 제공합니다. 간단한 클라우드 이동성은 데이터 서비스를 클라우드로 원활하게 확장할 수 있도록 합니다.

퓨어스토리지는 간단한 설정, 손쉬운 운영, 광범위한 통합을 제공합니다.

그러나 퓨어스토리지를 차별화해주는 요소는 고객과 파트너를 위한 프리미엄 지원입니다.

ESG에 따르면, 79%의 조직은 지난 12개월 동안 최소 한 번 이상의 랜섬웨어 공격 시도를 경험했습니다. 더 놀라운 사실은, 공격을 받은 조직의 86%는 대가를 지불했음에도 모든 데이터를 복구하지는 못했다는 것입니다. 이제 대비를 해야 합니다. 취약점을 파악하고 퓨어스토리지가 어떻게 도울 수 있는지 알아보세요. 랜섬웨어에 대적할 준비가 되셨나요?

백업은 재해, 데이터 손상 또는 실수로 인한 삭제 같은 일반적인 시나리오로부터 중요한 데이터를 보호합니다. 그러나 랜섬웨어는 기존 데이터 보호 인프라에 더 큰 부담을 줄 수 있습니다. 퓨어스토리지의 플래시블레이드(FlashBlade//S)와 플래시어레이(FlashArray)에서 사용 가능한 세이프모드(SafeMode) 스냅샷은 랜섬웨어 공격으로부터 데이터 백업을 보호할 수 있도록 불변성을 제공합니다.

랜섬웨어로부터 백업 보호: 세이프모드 스냅샷은 안전한 복사본을 생성하여 백업 데이터와 메타데이터를 보호합니다.

랜섬웨어는 관리자 크리덴셜이 있어도 세이프모드 스냅샷을 삭제, 수정 또는 암호화할 수 없습니다. 예측할 수 없는 세상에서 연중무휴 24시간 지원을 받을 수 있습니다.

올플래시 스토리지의 간단함을 갖춘 스냅샷: 스냅샷 일정 수립과 보존은 완전하게 맞춤화 가능하며, 쉽게 배포할 수 있습니다. 중단 없이 확장 및 업그레이드할 수 있습니다. 또한 백업 소프트웨어를 변경할 필요가 없습니다. 그냥 설정만 해두면 됩니다.

비즈니스 속도에 맞춰 복구 가속화: 기존의 재해 복구 솔루션은 느립니다. 플래시블레이드는 운영 및 테스트/개발 워크로드를 위한 페타바이트 규모의 데이터 복구 성능을 통해 복구 지점 및 복구 시간 목표를 달성합니다.

다중 프로토콜 지원: 네이티브 서버 메시지 블록(SMB) 지원을 추가하면 백업이 더 빠르고 효율적으로 수행됩니다. SMB 지원은 윈도우 애플리케이션에 높은 성능을 제공하고 더 폭넓은 비즈니스 요구사항 및 사용 사례를 지원합니다.

더 알아보기

- 랜섬웨어 보호에 대해 자세히 알아보세요.
- 세이프모드로 랜섬웨어의 영향을 완화하는 방법을 알아보세요.
- 뉴올리언스 시(영문자료)와 COCC(영문자료)가 퓨어스토리지와 함께 랜섬웨어로 인한 피해를 어떻게 예방하고 있는지 알아보세요.

purestorage.com/kr

02-6001-3330

PURESTORAGE®
Uncomplicate Data Storage, Forever

PS2089-02 01/2023