랜섬웨어로부터 백업 데이터센터 보호 전략

기업 최후의 보루인 Backup Data를 랜섬웨어로부터 지키는 현실적인 방안

2017년 6월 랜섬웨어 공격으로 엄청난 피해가 발생했습니다. 이번 공격은 의도적으로 여러 기업에 호스팅 서비스를 제공하는 회사를 대상으로 이뤄진 공격이어서 피해가 더욱 확산되었습니다. 특히, 해커들은 매우 치밀하게도 이 회사의 백업 데이터까지 랜섬웨어를 감염시켜 복구가 원천적으로 불가능하게 만들었습니다. 이를 계기로 한국의 호스팅 회사를 상대로 해커들의 공격은 더 많이 발생할 것이라는 어두운 전망도 나오고 있습니다.

이제 랜섬웨어 공격은 결코 남의 일이 아니며, 우리 코 앞의 현실입니다. **과거 랜섬웨어에 대항하는 기업의 최후 방어선은 [로컬 및 내트워크를 통한 엄격한 백업 정책수립과 백업관리]**이라고 생각되어져 왔으나, **백업 서버가 공격된 시점에서는 이에 대응하는 다른 전략이 요구**되어집니다. 기업 최후의 보루인 백업본을 어떻게 하면 지켜낼 수 있을까요? 이제 랜섬웨어로부터 **백업 데이터를 지켜낼 수 있는 전략**들을 소개합니다.

전략은 크게 4가지입니다. **백업본의 소산, 시스템 접근 제한, 접근이 어려운 백업시스템, 안전한 스토리지**의 구성이라면 랜섬웨어로부터 안전하게 백업시스템과 백업센터를 보호할 수 있습니다. 이 전략 중의 몇가지는 귀사의 시스템에서도 큰 비용 없이 적용하실수 있습니다. 그 이유를 하나하나 살펴보겠습니다.

- **백업본 소산:** 이번 피해의 가장 큰 원인 중의 하나는 원본 서버와 백업본이 저장된 서버가 같은 네트워크 상에 운영되어 있기 때문입니다. 랜섬웨어는 강한 전파성이 있어서, 최소한의 1개 이상의 백업본은 네트워크의 외부나 클라우드 상에 저장되어야 합니다. 이런 규칙을 백업의 Golden Rule이라고 하는데, 소산된 백업본이 재난발생 시 최후 방어선으로 활용할 수 있기 때문입니다.

- **시스템 접근 제한:** 백업서버 운영 시, 다소 불편하더라도 원격접속이 불가능하게 차단하고, 필요시 접속하더라도 이를 최소화해야 합니다. 백업 서버의 치명적인 장애복구 혹은 점검을 위해 Shell 접근이 필요할 경우는 SSH 접근 옵션을 활성화한 뒤 원격으로 접속하거나, 실제 물리 서버에 Console을 연결운영하는것이 가장 안전합니다.

- **접근이 어려운 백업시스템**: 백업시스템이 범용적이고 알려진 시스템일수록 랜섬웨어 공격에 취약할 수 밖에 없습니다. 일반적인 OS와 표준규격의 프로토콜을 이용하는 시스템에 비해서, 백업시스템이 독자적인 OS를 사용하고, 백업원본서버,백업서버,스토리지 간의 통신이 독자적인 전송프로토콜을 사용하게되면 랜섬웨어로부터 상대적으로 안전합니다.

- **안전한 스토리지:** 램섬웨어가 시스템에 로딩이되면 해당 시스템과 접근 가능한 모든 화일을 감염시킵니다. 백업시스템과 스토리지시스템에 데이터가 저장되려라도 감염된 화일이 파일이 실행될 수 없도록 저장되는 구조라면 백업 및 스토리지 시스템 내에서도 전파의 위협이 사라집니다.

이 중에서 귀사에서 미비되어 있는 부분이 있다면, 바로 적용하십시요. 작은 관심과 실행이 랜섬웨어로부터 귀사의 백업본을 보다 더 안전하게 만들 수 있습니다.

램섬웨어에 대한 최선의 해결책은 안전한 백업체계!

램섬웨어에 철저한 백업체계 구축만이 유일한 대응방안입니다.

- **지금 백업을 시작하세요!**
  중소기업의 40%는 정기적인 백업을 하지 않는다고 합니다. 백업의 시작이 예방의 첫걸음입니다.
- **PC의 백업계획을 수립하세요.**
  대부분 기업의 60%는 데이터를 PC나 노트북에 저장한다고합니다. 중요한 데이타가 PC에 저장되어 있는경우많습니다. 회사 내 PC레벨에서도 백업계획을 수립하세요.
- **백업을 여러 곳에 소산하세요.**
  백업시스템도 공격받을 수 있습니다. 네트워크 내부가 아닌 외부에 백업을 저장해 최후의 방서선으로 활용하세요

위와 같이 랜섬웨어에 대한 대응전략은 복잡하거나 어렵지 않습니다. 작은 관심으로도 귀사의 시스템을 안전하게 보호할 수 있습니다.

URI System
T: 1588-4855
E: master@urisystem.co.kr

Acronis

Acronis Storage 2.0
랜섬웨어에 강한 Software Defined Storage

Acronis Storage 2.0

소프트웨어 정의 스토리지는 스토리지 소프트웨어가 실행 기반인 하드웨어에 의해 정의되지 않으며 하드웨어에서 분리되어 시장에서 공급되는 모든 업계 표준 하드웨어에서 실행될 수 있는 소프트웨어 기반 스토리지입니다.

볼륨 확장 시, 기존의 비싼 하드웨어를 증설해야했던 HW 기반 스토리지와는 달리 상대적으로 저렴한 비용으로 고성능 스토리지를 구축할 수 있는 것이 큰 장점입니다.

Acronis Storage 2.0은 Software Defined Storage 분야를 선두하는 제품으로 다음과 같은 장점을 가지고 있습니다.

- ❖ Easy: 단 14번 클릭으로 5분안에 설치되고 WEB-GUI로 운영이 편리함
- ❖ Fast: SSD caching으로 고성능을 제공하며, Ceph보다 5배 빠른 성능을 제공
- ❖ Safe: Erasure Coding, Acronis Cloud RAID, Acronis Notary with Blockchain 등 데이타 보호를 위한 최신 보안 기술이 적용됨
- ❖ Efficient: 기존의 하드웨어로 스토리지 구성이 가능하며 대규모의 확장도 중단없이 가능
- ❖ Optimized for Backup: Acronis Backup cloud를 바로 시작할 수 있어서 안정적인 데이터 보호를 설치 즉시 시작할 수 있음.

URI System
T: 1588-4855
E: master@urisystem.co.kr

랜섬웨어에 대한 최선의 해결책은 안전한 백업체계를 구축하는 것입니다. 그러나 24시간이 모자르는 IT 관리자 입장에서는 백업본을 외부에 저장하는 체계 구축, 시스템 접근 관리, 접근이 어려운 백업시스템 구축, 안전한 스토리지 구축하는 것은 실행하기 쉽지 않은 일입니다. 최적의 솔루션을 각기 확인하고 운영해야하기 때문입니다.

Acronis Storage2.0은 Software Defined Storage로서 표준 하드웨어라면 어디에도 설치와 운영이 가능한 소프트웨어 스토리지 입니다. 특히, 스토리지 뿐만 아니라 안전한 백업 서비스인 Acronis Backup Cloud가 포함되어 있어서, 랜섬웨어 대응 백업 시스템을 구축하는 분들께 적합합니다. 이 제품은 랜섬웨어를 해결하기 위해 만들어진 것은 아닙니다. 다만, 스토리지에서 갖는 특징과 기능들이 랜섬웨어 대응에 적합한 형상을 가지고 있습니다. 이제 그 특징들을 살펴보겠습니다.

- 3-2-1 백업 운영: Acronis Storage 2.0은 백업본을 손쉽게 저장/관리할 수 있습니다. 3개의 백업본을 2개 이상의 미디어로, 1개는 자동적으로 클라우드에 저장 가능하여, 최후의 방어선을 손쉽게 상시 유지할 수 있습니다.
- 시스템 접근제한: 관리자는 WEB-GUI를 통해 운영/관리하나, 치명적 장애 혹은 점검을 위해서는 반듯이 Shell로 접근해야 합니다.이를 위해서는 ssh접근 옵션을 활성화(Default:비활성화)하여 접속하거나, 물리서버에 직접 연결해야 하기 때문에 해커가 접근하기 어렵습니다.
- Unique OS & Protocol: 이미 노출된 Windows, CentOS, Fedora 등에 비하여, 자체 개발된 OS에서 운영되어 취약점의 외부 노출이 최소화되어 있습니다. 또한, 범용 프로토콜이 아닌 자체 프로토콜을 사용하여 데이터를 전송하기 때문에 취약점이 오픈되지 않았으며, 이를 통한 액세스도 불가능합니다.즉, Acronis Backup Agent를 통한 백업 전송 외에는 다른 파일을 업로드할 방법이 원천 차단되어 안전합니다.
- 안전한 데이터 저장: Acronis Storage는 Acronis Backup 데이터만 저장할 수 있으며, Erasure-coding 기법으로 분산저장됩니다. 즉, 스토리지 내에서 실행이 불가능해 전파의 위협이 없습니다.

Acronis Storage 2.0은 이외에도 Acronis Cloud RAID, Acronis Notary™ with blockchain 등의 최신 보안 기술로 데이터를 안전하게 보호합니다.

랜섬웨어! 체계적인 준비만이 유일한 해결책입니다. Acronis는 고객사의 준비를 돕기위해 노력합니다.

|Acronis Storage 2.0 구성도|