Remote Techs

뉴쉴드 데이터 센티널로 랜섬웨어 공격으로부터 보호

지난 몇 년 동안 랜섬웨어는 사이버 보안에서 가장 큰 위협이 되었습니다. 기존의 랜섬웨어 방지는 종종 새로운 공격이나 알 수 없는 공격을 막는데 효과적이지 않았습니다. 랜섬웨어는 개인이나 기업에 치명적일 수 있습니다. 정부나 사법 기관, 의료 시스템 또는 기타 주요 기반시설 기업뿐만 아니라 컴퓨터나 네트워크에 중요한 데이터를 저장하는 사람은 누구나 위험에 처할 수 있습니다. 복구는 어려운 과정일 수 있으며 일부 피해자는 파일 복구 비용을 지불합니다. 그러나 대가를 치르더라도 파일을 복구할 수 있다는 보장은 없습니다.

Remote Techs

2006 년에 설립된 Remote Techs, Inc.는 IT 관리 서비스와 사이버 보안, 백업 및 재해 복구, 네트워크 인프라 그리고 컴퓨터 서비스에 대한 전문 지식을 제공하는 기술 솔루션 기업입니다. 이 회사는 캘리포니아에서 콜로라도, 워싱턴 주에 이르는 미국 서부 지역을 커버하고 있으며 여러 국제 고객도 보유하고 있습니다.

Remote Techs 는 건설, 운송, 제조, 재무 및 부동산 분야를 아우르는 폭넓은 고객 기반을 가지고 있습니다. 그들의 고객은 대부분 중소기업이며 보통 10-100 대의 컴퓨터를 가지고 있는데, 여기에는 비즈니스 운영에 꼭 필요한 중요 업무용 애플리케이션이 설치되어 있습니다.

Remote Techs 의 사업은 빠르게 성장하고 있습니다. 지난 몇 년 동안 Remote Techs 는 평균 약 30%의 상당한 성장을 이루었으며 현재는 1,500 개가 넘는 엔드포인트를 관리하고 있습니다.

2019 년 초 Remote Techs 의 최고운영책임자인 대린 해리스와 이야기했을 때 회사의 주요 걱정거리 중 하나는 사이버 위협

이었습니다. 그들의 고객 중 일부는 최근 랜섬웨어 공격의 영향을 받았습니다. 해리스는 솔루션을 찾아보다 뉴쉴드와 뉴쉴드 데이터 센티널 제품을 발견하게 되었습니다. "우리는 우리와 고객에 대한 공격적인 랜섬웨어 사고 후에 뉴쉴드를 알았습니다. 새로운 도구를 찾기 시작했고 그러다가 뉴쉴드 데이터 센티널을 발견했죠."

뉴쉴드 데이터 센티널에 대한 데모와 철저한 평가 이후에 해리스는 이것이 사이버 공격으로부터 고객을 보다 효과적으로 보호하고 고객의 마음의 평화를 유지시킬 수 있는 솔루션인 것을 알았습니다.

랜섬웨어의 위협과 영향

대린 해리스는 일부 고객들과 함께 랜섬웨어 위협을 직접 목격했습니다. "랜섬웨어는 기술적 관점에서 현재 사업주가 직면한 가장 큰 문제라고 주저 없이 말할 수 있어요. 랜섬웨어 도구는 점점 다양화되고 치료 및 예방 솔루션보다 빠르게 진화되고 있습니다. 랜섬웨어는 Windows 의 기본 기능을 활용해서 막대한 피해를 주죠. 이러한 기능은 관리자들이 IT 시스템을 관리하기 위해 필요한 기능이기 때문에 악성 프로그램이 이런 기능을 악용한다고 해서 우리가 할 수 있는 일은 많지 않아요. 매우 심각한 문제입니다."

사업주는 종종 랜섬웨어가 비지니스에 미치는 영향을 과소평가합니다. 다음 해리스의 설명처럼 말입니다. "고객이 랜섬웨어 위협을 보는 관점은 저와는 달라요. 나는 이것을 교육의 차이라고 생각해요. 일반 사업주는 랜섬웨어가 무엇을 하고 그 목적이 무엇인지를 이해하지 못합니다. 이러한 문제를 해결하거나 예방하는 도구를 가치 있게 평가하는 것과는 거리가 멀죠."

때때로 대화하기가 쉽지 않을 때 해리스는 이것을 자동차에 비유했습니다. "고객에게 그들이 변속기 오일을 넣는 것을 잊어버렸기 때문에 변속기가 자동차 바닥에서 떨어져 나왔다고 말하는 것과 같아요. 그리고 10 달러짜리 변속기 오일 한 병이면 5 천달러의 수리를 막았을 거라고 얘기하죠."

간단히 말해서, 랜섬웨어 공격으로부터 데이터를 복구하기 위한 비용은 매우 빠르고 크게 증가할 수 있습니다. Remote Techs 는 이 모든 것을 너무 잘 알고 있습니다. "일부 고객은 우리가 권장한 백업이 없고 랜섬웨어 공격 후에 대량의 데이터를 손실했으며 복구 경로도 없었어요. 그들은 6 개월 전으로 돌아가 있었어요. 재정을 다시 설계하고 은행 입출금 내역서를 확인하면서 과거 주문과 이메일을 찾으려고 노력했죠. 이러한 일을 겪은 후에 앞으로 나아간다는 것은 그들에게는 도전이었어요. 그들 중 몇몇은 지난 6~8 개월의 일을 단지 재구성하려고 2~ 3 명의 사람들을 새로 고용했어요. 매우 나쁜 상황이지요."라고 해리스가 전했습니다.

일반적으로 사용자는 훼손되거나 손실된 데이터를 복구하는 데 필요한 비용과 시간을 인지하지 못합니다. 해리스는 "잃어버린 시간, 판매 손실, 급여 손실 그리고 잃어버린 이메일을 추가하기 시작하면 총금액은 하루나 이틀만에 수십만 달러에 이르게 됩니다."라고 설명했습니다.

해결책

빠르게 진화하는 위협 행위자로 가득 찬 오늘날의 환경은 예측할 수 없습니다. 이런 환경에서 고객이 자신을 철저하게 보호할 수 있는 유일한 방법은 다층적 방어 접근법을 채택하는 것입니다. "우리는 여러 단계의 보호를 사용하며, 이것은 어떤 보안 솔루션에서든 중요한 부분입니다."라고 해리스는 말합니다. "랜섬웨어 공격에 대비하기 위해서만이 아니라, 백업 및 재해 복구 계획을 제대로 수립하는 것은 절대적으로 중요합니다. 우리는 BUDR(백업 및 재해 복구) 애플리케이션을 실행하고, 지능형 바이러스 백신 및 맬웨어 방지 시스템을 운영하고 있어요. 우리는 이제 이것을 뉴쉴드로 보완합니다. 우리가 찾은 뉴쉴드의 놀라운 특징 중의 하나는 외부 시스템에 의존하지 않고 매우 빠른 치료 도구를 모든 기계에 적용할 수 있다는 겁니다. 만약 랜섬웨어 공격이 발생하면 몇 분 내로

시스템 손상을 되돌리거나 파일의 암호를 해제할 수 있습니다. 백업, 바이러스 백신 등과 같은 다른 솔루션 없이 말이죠."

해리스는 뉴쉴드에 대해 "중요한 방어선" 이라고 평가했습니다. "사이버공격이 있거나 사용자가 실수한 경우 백업 시스템으로 돌아가서 복원하지 않고 뉴쉴드를 사용하여 신속하고 효율적으로 문제를 해결할 수 있습니다. 아주 간단하죠. 영향을 받은 시스템에 접속해서 복구하려는 데이터와 파일을 선택하고 버튼을 누르면 끝이에요."

기존의 랜섬웨어 방지는 알려진 맬웨어 및 바이러스를 탐지하고 차단할 수 있습니다. 그러나 지속적인 업데이트를 하더라도 새로운 공격이나 알 수 없는 공격을 차단하는 데는 종종 효과적이지 않습니다. 뉴쉴드 데이터 센티널은 다릅니다. 데이터가 어떻게 또는 왜 변경되었는지 관계없이 컴퓨터 시스템에 깊이 들어가서 데이터를 복구합니다. FUD(완전한 은신) 또는 제로데이 랜섬웨어조차도 뉴쉴드 데이터 센티널에 필적할 수 없습니다.

뉴쉴드 솔루션은 다양한 유형의 보호 기능을 제공합니다.

파일 및 데이터 보호 뉴쉴드 미러 쉴딩™ 기술을 활용하여 한 번의 클릭으로 원본 파일을 복구할 수 있습니다.

디스크 및 부트 보호 낫페트야(NotPetya), 배드래빗(Bad Rabbit) 및 샤문(Shamoon)과 같은 랜섬웨어 및 악성 프로그램이 부팅 프로세스의 권한을 획득하지 못하게 하여 와이퍼 맬웨어가 하드 드라이브에 있는 모든 데이터를 지우는 것을 방지합니다.

원클릭 복원 랜섬웨어 공격으로 인한 피해를 쉽게 되돌려 사용자는 기존 보안 및 스토리지 메소드가 실패한 컴퓨터와 파일에 다시 빠르게 접근할 수 있습니다.

출시

Remote Techs 는 시간을 두고 뉴쉴드 데이터 센티널을 모든 관리 엔드포인트에게 출시할 계획을 가지고 있습니다. Remote Tech 는 기존 주요 고객과 이미 해당 프로세스를 시작했으며 신규 고객에게는 고급 보안 제공의 일환으로 뉴쉴드 솔루션을 제안할 것입니다.

"우리는 사업주, 회계 담당자, 우수 영업 사원 등과 같은 거의 모든 핵심 인력에게 뉴쉴드를 배포하고 있습니다. 이러한 사용자의 컴퓨터에는 매우 민감한 데이터가 있기 때문에 보호해야 합니다. 우리는 카세야를 사용하여 소프트웨어를 배포하고 설치합니다. 뉴쉴드를 설치할 사용자와 시스템을 선택하고 패키지를 내립니다. 할 수 있는 가장 간단한 설치죠." 라고 해리스는 말합니다.

그에 따르면 이 솔루션은 고객층으로부터 호평을 받고 있습니다. "고객은 마음의 평화를 원합니다. 고객은 빠른 치료 옵션을 좋아하죠. 이것은 표준 계층 방어의 일부가 되어가고 있습니다. 뉴쉴드 같은 치료 중점적이며 빠른 복구 기능을 가진 여러 제품을 갖추고 위협 방지에 초점을 둔 다른 제품도 배치해야 합니다. 하나의 제품으로 당신이 필요한 모든 작업을 수행하기를 바라는 것은 더 이상 가능하지 않아요."

Remote Techs 의 혜택

뉴쉴드 데이터 센티널을 엔드포인트에 배포한 후 Remote Techs 는 어떠한 사이버 공격에도 중요한 데이터를 보호할 수 있는 안정적인 솔루션을 고객에게 제공할 수 있게 되었습니다. 구체적인 이점은 다음과 같습니다.

- **백업 솔루션 없이 보호된 시스템에서 데이터를 매우 빠르게 복구할 수 있는 능력**

Remote Techs 는 뉴쉴드 데이터 센티널을 첫번째 방어선으로 사용하여 백업 복원이나 다른 재해 복구 솔루션을 트리거할 필요 없이 모든 유형의 데이터를 로컬에서 매우 신속하게 복구할 수 있습니다.

- **마음의 평화**

뉴쉴드 데이터 센티널을 이용하면 사용자는 데이터의 안전성에 대해 걱정할 필요가 없습니다. 중요한 데이터는 항상 보호됩니다.

- **파일 및 데이터 보호, 디스크 및 부트 보호 그리고 원클릭 복원**
- **언제 어디서든 보호**

데이터를 복구하기 위해 보호된 시스템이 온라인 상태이거나 네트워크에 연결되어 있지 않아도 됩니다. 모든 랜섬웨어 공격으로부터 데이터는 항상 보호되며 오프라인 또는 온라인에서 복구할 수 있습니다.

- **카세야 같은 표준 RMM 소프트웨어와 설치 통합**
- **사용 및 배포의 용이성**

뉴쉴드 데이터 센티널에는 다양한 기능이 있습니다. 해리스가 가장 좋아하는 기능은 무엇일까요? "우리와 고객에게 주된 혜택은 마음의 평화입니다. 이것은 어떤 종류의 공격에도, 심지어 사용자의 잘못된 결정에 대해서도 훌륭한 치료 도구가 됩니다. 뉴쉴드만이 복잡하지 않으면서 매우 빠르게 할 수 있는 일들이 있습니다. 다른 애플리케이션으로는 할 수 없죠."

해리스는 다음도 덧붙였습니다. "내년 또는 18 개월 안에 우리 환경의 모든 기기에 보급되어 있을 겁니다. 이것이 우리의 목표입니다."

뉴쉴드

서울시 영등포구 국제금융로 6 길 33 | (070) 4352-7333 | www.neushield.co.kr

NeuShield, Inc. 는 관리형 서비스 공급자(MSP) 및 IT 관리자에게 비즈니스에 영향을 줄 수 있는 랜섬웨어 및 기타 위협으로부터 모든 PC 와 서버를 전체적으로 보호하는 완벽한 솔루션을 제공합니다. 수상 경력에 빛나는 뉴쉴드의 미러 쉴딩™ 기술을 사용하면 백업이나 롤백에 의존하지 않고 사이버 위협으로 인한 모든 유형의 손상, 삭제 또는 암호화로부터 데이터를 즉시 복구할 수 있습니다. 당신의 데이터는 다시는 인질이 되지 않을 것입니다. 뉴쉴드에 대한 자세한 내용을 보려면 **http://www.neushield.co.kr** 을 방문해 주세요.

서울시 영등포구 국제금융로 6 길 33 | (070) 4352-7333 | www.neushield.co.kr