인터뷰

회원사무소 위협하는 랜섬웨어 공격, '한길백업'으로 해커 "꼼짝마!"

사례1. 2022년 4월, A세무사사무소 직원의 집에 있던 개인용PC를 재택근무 용도로 사용하다 랜섬웨어에 감염되었고, 그 다음날 사내 서버PC도 랜섬웨어에 감염되는 피해를 입었다. 랜섬웨어에 감염된 직원의 개인용PC와 사내 서버PC가 네트워크로 연결되어 있어서 랜섬웨어 감염 2차 피해가 발생한 것으로 추측된다. 천만다행으로 감염되지 않은 서버PC의 회계데이터를 제외한, 감염된 업무용 일반문서(엑셀, PDF, 이미지파일 등)들은 한길백업을 통해 복원했다. A세무사는 "한길백업을 몇 년에 걸쳐 이용하는 동안 데이터를 복원할 일이 없었고, 이용기간도 얼마 남지 않아 한길백업을 해지하고 직접 백업데이터를 관리하려던 찰나에 이번 일을 겪으니, 불의의 사고에 대비할 수 있는 보험처럼 사무실을 운영하는 한 계속 한길백업을 이용해야겠다" 고 말했다.

사례2. 같은 해 11월, B세무법인의 직원이 입사지원 이메일의 첨부(압축)파일을 다운로드 했다가 서버PC의 모든 파일이 랜섬웨어에 감염되었다. 랜섬웨어 감염 피해가 발생되기 며칠 전에 채용공고를 유명 취업포털사이트에 등록했기 때문에, 이메일에 첨부되어 있던 파일이 이력서가 아닌 랜섬웨어 실행파일이라고 의심하지 못했기 때문이다. 결국 랜섬웨어에 감염된 파일들은 모두 복구할 수 없어, 서버PC를 포맷할 수밖에 없었고, 안타깝게도 전날 한길백업에 백업되어 있던 회계데이터만 복원할 수 있었다. B세무법인의 C실장은 "세무사회 4월 공동구매 때마다 서버PC는 최신형 PC로 바꾸고, 백신도 유료상품으로 결제하여 사용하고 있었지만, 실제로 도움이 된 건 한길백업이었다", "다른 지점도 이러한 피해를 예방하고자 한길백업을 신청하라고 권유할 예정이다" 고 말했다.

위 사례들처럼 세무사사무소의 랜섬웨어 감염피해가 계속 발생하고 있으며, 2022년 7월에는 국내기업을 대상으로 하는 '귀신(Gwisin)' 랜섬웨어 피해가 확산되어 국내 콜택시 업체의 배차시스템과 골프장 예약시스템을 마비시킨 사례도 있었다.
랜섬웨어 공격이 갈수록 지능적이고, 공격대상도 더욱 확대됨에 따라 세무사사무소도 지속적인 관심과 주의가 요구된다. 이에 한국세무사회 전산법인 한길TIS의 권길성 대표를 만나 랜섬웨어로 인한 데이터 유실 위협으로부터 세무사사무소의 중요데이터를 안전하게 보호하는 방법을 알아보고자 한다. <편집자>


▲ 한길TIS 권길성 대표

Q. 먼저 랜섬웨어가 무엇인지 구체적으로 설명해 주세요.

A. 랜섬웨어란 컴퓨터 시스템을 마비시키거나 중요한 데이터(파일)를 암호화해 사용할 수 없게 한 뒤 이를 복구해주는 대가로 금전을 요구하는 악성코드를 말합니다. 감염된 파일을 인질로 삼아 몸값(Ransom)을 요구한다는 의미에서 랜섬웨어라는 이름이 붙었습니다. 일반적으로 알고 있는 웜, 트로이목마, 애드웨어 등의 악성코드와 유포·감염방식은 유사하지만, 백신 프로그램으로 비교적 쉽게 예방할 수 있는 일반적인 악성코드와는 다르게, 랜섬웨어는 백신 프로그램이 있어도 랜섬웨어 공격을 방어하거나 감염된 파일을 복구하는 일이 매우 어렵습니다.

Q. 랜섬웨어 감염 경로는 어떻게 되나요?

A. 신뢰할 수 없는 사이트에 접속하거나, 스팸메일의 첨부파일을 실행하거나, 불법 소프트웨어를 사용하는 등 네트워크 보안의 취약점을 통해 침투하여 감염시킵니다. 최근 랜섬웨어 공격은 이전보다 정교하고 조직화되어 많은 몸값을 받아낼 수 있는 기업이나 공공기관부터 개인용 PC까지 공격 대상이 다양해졌습니다. 실제로 국내 랜섬웨어 감염 피해가 증가하고 있고, 더욱이 세무사사무소에서도 랜섬웨어 감염피해도 발생했기 때문에 세무사 회원님들도 언제, 어디서든 랜섬웨어 공격에 당할 수 있다는 경각심을 갖고, 대비해야 합니다.

Q. 세무사 회원의 PC가 랜섬웨어에 감염되었는지 어떻게 알 수 있나요?

A. 우선, 랜섬웨어 감염증상은 정상 파일의 확장자가 바뀌어 회계데이터가 조회되지 않거나 정상 파일이 암호화되어 엑셀, 한글, 이미지 파일 등이 실행되지 않습니다. 또한 금전을 요구하는 내용으로 바탕화면이 변경되거나, 메모장 파일(readme.txt)이 생성됩니다. 이와 같은 증상이 확인되면, 감염된 PC를 바로 종료하고 사내 네트워크로 연결된 다른 PC와의 연결을 차단해야 피해를 줄일 수 있습니다. 추가로 한국인터넷진흥원 사이버민원센터, 경찰청 사이버안전국에 신고하면 도움을 받을 수 있습니다.

Q. 랜섬웨어에 감염된 파일은 어떻게 복구할 수 있나요?

A. 한국인터넷진흥원에서 제공하는 랜섬웨어 복구프로그램을 이용하거나, 데이터복구 전문업체를 통해 복구를 시도할 수 있지만, 랜섬웨어에 감염된 파일은 복구가 불가능합니다.
그렇다고 해커(랜섬웨어 유포자)의 요구에 대응하는 것은 피해를 더 키울 수 있습니다. 해커에게 가상화폐(비트코인 등)를 송금하더라도, 데이터를 복구해준다는 보장도 없으며, 일부 데이터를 복원한 후에 추가 비용을 요구하는 등의 2차 범죄로 이어질 수 있기 때문입니다.

Q. 감염된 파일을 복구할 수 없다면, 미리 랜섬웨어 감염에 대비할 수 있는 방법은 없나요?

A. 랜섬웨어 감염에 대비할 수 있는 대표적인 4가지 방법으로 첫째, 윈도우와 같은 운영체제를 최신버전으로 유지하고 백신프로그램도 필수로 이용해야 합니다. 둘째, 보안이 취약한 웹사이트에 접속하거나 배너를 클릭하지 않습니다. 셋째, 출처가 불명확한 이메일과 첨부파일 그리고 URL링크를 실행할 때 주의해야 합니다. 넷째, 중요한 파일을 '정기적으로 백업'해야 합니다.
랜섬웨어는 보안의 취약점을 찾아내 다양한 방식으로 침투하므로 완벽하게 방어할 수 없기 때문에, 중요한 데이터를 주기적으로 미리 백업을 해놓는 것이 가장 최선의 방법인데, 직접 백업하는 것보다 자동으로 백업되는 한길백업을 이용하는 것을 추천합니다.

Q. 회원사무소에서 직접 백업하는 방식보다 한길백업을 추천하는 이유가 있을까요?

A. 한길백업이 더 편리하고, 더 안전하다는 점 때문입니다. 한길백업은 LG유플러스 IDC에 백업데이터를 이중으로 백업하여 안전하게 보관하고 있고, 한길백업의 자동백업기능을 통해 원하는 시간에 자동백업을 진행할 수 있으며, 변동된 데이터 파일만 백업하기 때문에 데이터 종류별로 복원이 가능하고, 백업시간도 짧습니다. 또한, 한길백업 담당자를 통해 백업진행 모니터링, 복원 등의 관련 서비스를 지원받을 수도 있습니다.

Q. 타 백업서비스에 비해 한길백업이 나은 점은 무엇인가요?

A. 한길백업은 뉴젠의 세무사랑Pro, 더존의 스마트A의 회계데이터뿐만 아니라 엑셀, 한글, 이미지 파일도 백업이 되고, 한국세무사회에서 추천하는 유일한 백업서비스로 2,500여 세무사 회원님들이 사용하고 있는 검증된 백업서비스입니다. 또한, 세무사 회원님들의 백업프로그램 비용 부담을 줄이고자 업체 최저가(타사 대비 50% 저렴)로 제공하고 있습니다.

Q. 더존 스마트A의 유지보수 서비스가 종료된다고 하는데, 스마트A 유지보수 서비스가 종료되어도 한길백업은 스마트A 회계데이터 파일의 백업과 복원이 가능한가요?

A. 스마트A의 유지보수 서비스가 종료되더라도, 스마트A 회계데이터 파일만 있다면 한길백업으로 백업이 가능하고, 한길백업에 보관된 스마트A 회계데이터 파일을 언제든지 복원하여 스마트A를 통해 조회할 수 있습니다.

Q. 마지막으로 세무사 회원님들께 전하고 싶은 말씀이 있습니까?

A. 잘 아시다시피 회계데이터는 수임업체의 중요한 기업정보이자 세무사사무소의 가장 핵심 자산입니다. 회계데이터 유실을 겪어본 세무사사무소 중에는 한길백업을 이용하시면서 2차, 3차 직접 백업하는 경우도 있는 것처럼 회계데이터를 보호(백업)하는 일은 아무리 강조해도 지나치지 않습니다.
랜섬웨어 감염, 서버PC 고장 등의 이유로 중요한 재산이 한순간에 사라질 수 있기에 세무사사무소에서 백업은 필수입니다. 한국세무사회 전산법인 한길TIS에서 운영 중인 한길백업을 모든 세무사님들이 가장 저렴한 비용으로 편리하게 이용하실 수 있도록 계속 노력할 것이며, 한길백업 외에 BestCMS, 세무라인, 한길팩스, 오피스몰 등 한길TIS에서 운영하고 있는 다른 서비스들도 많은 이용과 관심을 부탁드립니다. 감사합니다.