chapter 2

문서중앙화 솔루션, 정보보안을 위한 선택인가 필수인가

홍진영 ‖ ㈜지란지교시큐리티 사업부장

I. 서론

다양한 보안 위협에 대응하기 위한 새로운 보안 솔루션과 장비들이 시대의 유행을 따라 변화하고 있다. 문서중앙화 솔루션 역시 내외부의 보안 위협에 대응하기 위해 최근 더욱 많은 관심을 받기 시작하였고, 이러한 관심은 국내뿐 아니라 해외에서도 점차 확대되고 있다. 물론, '문서중앙화'의 개념은 국내에서만 통용되는 대명사가 되었지만, 해외에서는 ECM (Enterprise Contents Management)이나 EDMS(Electronic Document Management System)와 같은 솔루션들이 DLP(Data Loss Prevention) 솔루션과 함께 유사한 이슈로 시장의 흐름을 견인하고 있어 '문서중앙화'가 비단 국내에서만 통용되는 솔루션이라고 보기에는 어려울 것이다.

이러한 배경에는 1991년에 최초로 만들어진 사이보그(Cyborg)라는 랜섬웨어의 출현이 있으며, 이후 꾸준하게 변종이 생겨나면서 급기야 2016년에는 글로벌 주요 보안 벤더를 비롯한 국내 보안 벤더/기관에서 '랜섬웨어'를 차세대 위협으로 선정하면서 그 위험성을 경고하기 시작하였다.

* 본 내용은 홍진영 사업부장(☎ 02-2006-6996, jyhong@jiran.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

과연 랜섬웨어는 무엇일까? 랜섬웨어는 사전적인 의미를 살펴보면, ‘Ransom’이라는 ‘몸값’과 ‘Ware’라고 하는 ‘제품’의 합성어로서, 사용자 디바이스나 파일을 암호화한 뒤, 이를 인질로 몸값을 요구하는 악성 프로그램을 통칭하고 있다.

과거 랜섬웨어는 시스템을 잠금 처리하여 금전을 요구하는 ‘Locker’ 계열이 주를 이루었다면, 2013년 이후부터는 파일 자체를 암호화하여 금전을 요구하는 ‘Crypto’ 계열이 주를 이루고 있다. 강력한 암호화를 기반으로 복호화가 불가능해지면서 다양한 사이버 범죄에 활용되고 있으며, 유포 채널이 다양화되고 공격 포맷과 방법은 고도화되어 가고 있는 상황이다. 심지어 RaaS(Ransomware as a Service)라는 랜섬웨어 서비스 그룹의 등장으로 손쉽게 범죄에 이용되고 있는 추세에 있다. 실제로 2017년에 많은 언론들이 [그림 1]과 같이 감염된 PC의 화면 공개를 통해 위험성을 경고하면서, IT 지식이 없는 일반인들조차 인식할 만큼 워너크라이(Wanna Cry; 울고싶어라) 랜섬웨어는 전 세계적으로 사회적인 문제가 되었다[2]. 이는 윈도 운영체제(OS)의 취약점을 악용하여 감염된 PC와 네트워크에 연결된 모든 PC를 감염시키는 방식으로서 한동안 워너크라이의 공포에 휩싸였다. 이것이 불과 3년 전이다.

랜섬웨어는 비단 개인의 업무용 PC 자료 유실만이 문제가 아니다. 이제는 공격 타깃이 개인의 PC에 맞춰져 있기보다는, 정보의 민감도가 높은 정부기관, 의료기관, 기업 연구소 등의 PC를 대상으로 공격이 증가하는 양상을 보이면서 고액의 몸값을 요구하거나, 협상력

〈자료〉 SBS뉴스, 랜섬웨어 오늘이 고비.. “컴퓨터 켜기 전 인터넷 끊어야”. 2017. 5. 15.

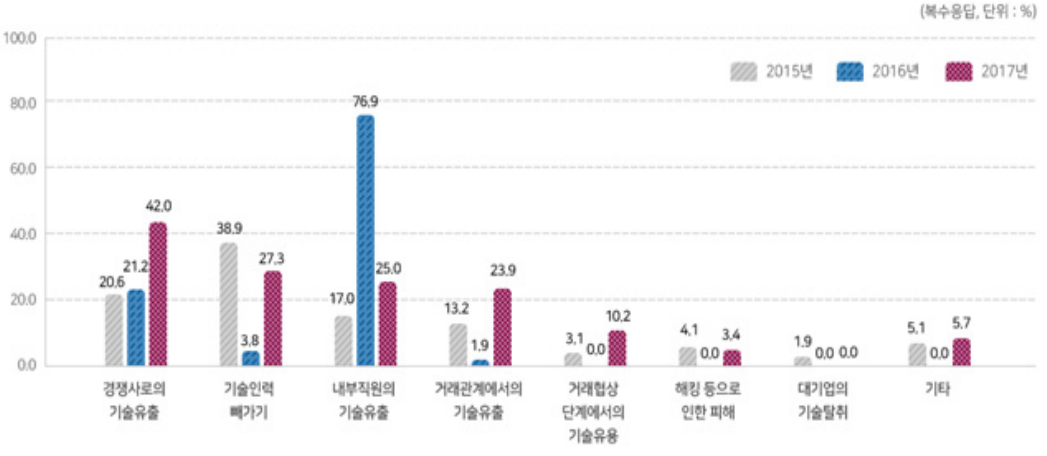
[그림 1] 랜섬웨어 감염

을 높이기 위한 전략적인 범행으로 발전하고 있기 때문에 항상 개인 PC 및 서버 보안 등에 유의해야 할 것이다. 그나마도 다행인 소식은 최근 2019년부터 랜섬웨어의 공격 빈도가 감소하고 있다는 사실이다. 하지만 언제부터 다시 급증할지 모른다. 또한, 기관과 기업 내에서 감염이 되어도 보고되지 않는 감염 사례가 있다면 또 다른 사례로 파생될 수 있다는 것을 잊지 말아야 한다.

우리는 4차 산업혁명을 맞이하면서 지식산업을 통한 경제성장을 이루고 있다. 기술 중심의 산출물을 통해 경쟁력을 확보하고 있으며, 전 산업군이 유기적으로 연결되어 협력 또는 경쟁해 나가고 있다. 이러한 산업구조 내에서는 기관과 회사 구성원의 연구 및 업무를 통해 발생하는 산출물들이 더 이상 개인의 소유가 아닌 기관과 기업의 중요한 자산이라고 할 수 있다. 그러나 안타깝게도 초반에 언급한 랜섬웨어 피해로 인해 중요 자료를 복구하지 못한 채 손실되는 것은 물론, 사용자의 과실 혹은 악위적인 행위나 보안 시스템의 부재로 인해 외부로 자료가 유출되는 사고가 발생하고 있다.

중소벤처기업부에서 발간한 '2017년 중소기업 기술보호 수준실태조사 보고서'에 의하면, [그림 2]와 같이 해킹 등 외부의 요인으로 인한 기술 유출에 비해 내부의 전·현직 임직원에 의한 기술 유출이 훨씬 심각한 것으로 나타났다[3]. 또한, 정보가 유출되는 주요 수단은 이동저장장치(USB, 외장하드, 모바일 등)와 이메일을 통한 것으로 파악되고 있다.

이제는 전 세계가 초고속 네트워크와 IOT(사물인터넷)를 기반으로 바이오 신산업과 함



〈자료〉 중소벤처기업부, 2017년도 중소기업 기술보호 수준실태조사 보고서

[그림 2] 기술 유출·탈취 유형 설문조사 결과

께 4차 산업혁명을 맞이할 준비를 하고 있는 만큼 개개인의 보안의식 고취와 체계적인 정보 보안에 관한 제도 개선을 통해 건강한 문화를 형성하고, 안전하고 효율적인 업무 환경 시스템을 구축해야 한다. 이로써 지식산업의 산출물을 안전하게 유통·관리할 수 있는 업무 프로세스를 정립해 나가야 할 것이다.

II. 정보보안에 대한 C-Level과 실무담당자의 고민

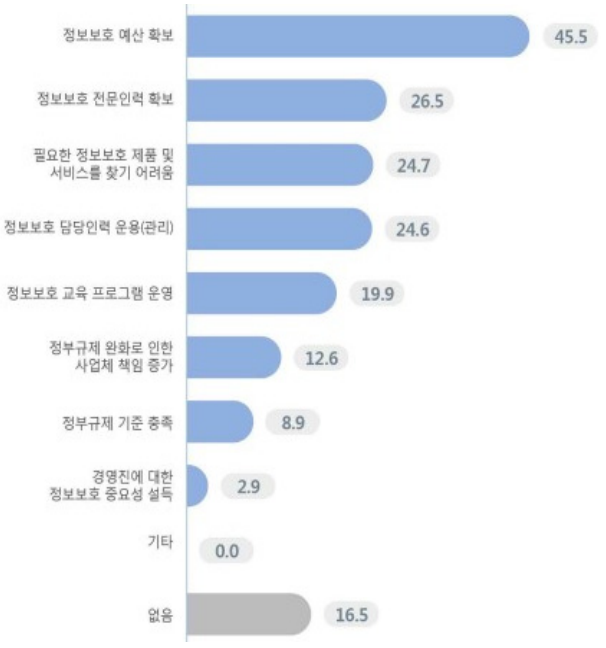
기업과 기관에서는 조직의 안정과 사업적 목표를 달성하기 위해 경영진은 많은 것들을 고민하고 해결책을 제시하기 위해 끊임없이 노력하고 있다. CEO(최고경영자)의 진두지휘 아래 COO(최고운영담당임원), CFO(재무담당임원), CIO(정보분야담당임원), CTO(기술분야담당임원) 등이 각자의 분야에서 경영의 방향과 거버넌스를 제시하고, 의사결정을 하는 과정에서 리스크가 사업에 장애가 되지 않도록 협력하는 과정은 필수적이라 할 수 있다. 또한, 시장의 다양한 요구를 반영하기 위해 새로운 C 레벨의 영역은 꾸준히 늘어가고 있다.

기업 내에는 사업을 영위하고 성장하기 위한 제품 연구 자료, 고객 정보, 사내 거버넌스를 위한 정책 등 많은 중요 문서들이 존재한다. 이러한 데이터를 보호하기 위해 법적인 제도로 CISO(최고정보보호책임자)를 의무적으로 선임하도록 하는 전자금융거래법 시행령 개정안이 금융권을 필두로 시행되었다. 이후 개인정보보호법 및 정보통신망법 등의 제정을 통해 대상 기업을 확대하여 CPO(개인정보관리책임자)를 별도로 선임하도록 했으며, 자산과 매출 규모에 따라 CISO와 CPO를 겸직하지 못하도록 하는 등 지속적으로 준수해야 할 컴플라이언스가 증가하고 있다.

거듭되는 고객의 개인 정보 유출 사고로 인해 해당 기업이 받는 이미지 타격과 법적인 책임이 무겁기 때문에 CPO는 고객의 개인정보 유출 방지를 위한 다양한 물리적/기술적 방안들을 모색해야 한다. CISO는 전반적인 정보보호 전략을 수립하고 이에 따른 관리 및 운영, 정보보호 취약점 분석, 평가 및 개선 등 정보 보안의 광범위한 부분까지 세심하게 다루어야 한다. 하지만 이러한 노력에도 불구하고, 보안의 홀은 늘 존재하며 이 홀을 틀어막다 보면 협업의 실무담당자와 이해관계가 상충되는 일이 빈번히 발생하기도 한다.

이러한 환경 내에서 전산담당자는 각각 다른 업무를 하고 있는 현업 부서들의 특수성을

고려하여 전산 시스템을 운영해야 하며, 안전한 보안 환경 내에서 효율적인 업무 프로세스를 설계해야 하는 숙명에 놓이게 되는 것이다. 정보보호 예산 확보와 전문 인력 양성에 대한 애로사항을 KISA(한국인터넷진흥원)에서 발표한 [그림 3]과 같은 '2018년도 정보보호 실태조사'에서도 확인할 수 있다[4].



〈자료〉 한국인터넷진흥원, 2018년도 정보보호 실태조사 보고서

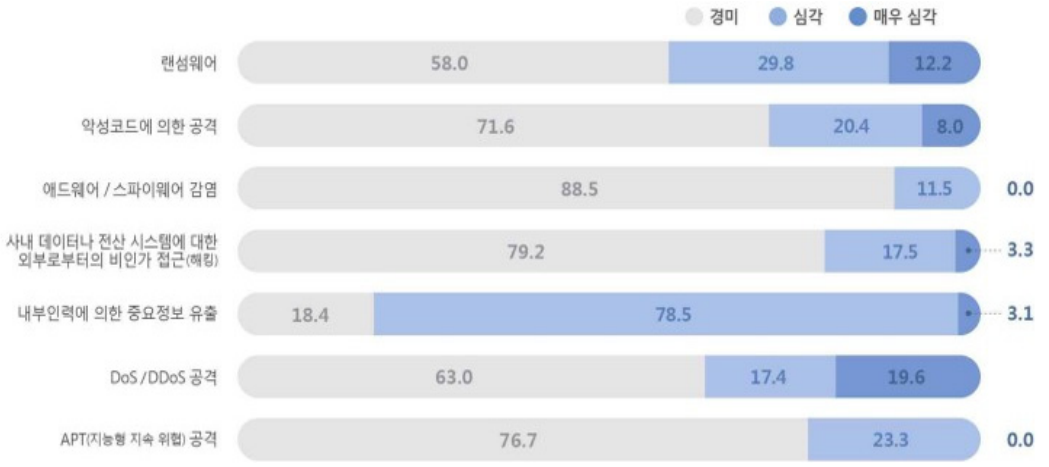
[그림 3] 정보보호 애로사항 설문조사 결과(%, 복수응답)

글로벌 경기 침체 속에서 넉넉한 예산을 투자하기 어려운 상황일지라도 보안 사고로 인한 손실과 기업의 이미지 실추는 미리 투자하는 금액에 비해 치러야 할 희생이 훨씬 크기 때문에 전산 실무담당자는 현실성 있는 투자 예산을 편성하고, C 레벨에서 적극적으로 검토해야 할 필요가 있을 것이다. 또한, 정보 보안 회사에서는 더욱 안정된 제품 개발과 운영할 수 있는 인력 양성 및 교육 프로그램을 꾸준히 개발해 나가야 할 것이다.

III. 데이터 자산 보호의 필요성

일반적으로 사무직 근로자는 오전에 출근해서 PC에 전원을 켜고, 이메일을 확인하며 오늘의 업무 현황을 파악한 후 하루의 일과를 시작한다. 각자의 업무에 따라 연구 결과서, 영업 정보, 고객 정보, 인사 정보 등 다양한 형태의 데이터를 신규 생성하고 개인 PC에 카테고리별로 정리해 나간다. 그리고 이 데이터들을 팀 혹은 협력 부서들과 이메일 또는 메신저 등을 통해 공유하고 협업하는 것이 일반적인 업무환경이다.

그러나 [그림 4]와 같이 침해 사고를 경험한 업체를 대상으로 진행한 설문조사 결과 중 유형별 심각성 정도에 대해 살펴보면, 서두에 언급되었던 랜섬웨어/악성코드에 의한



〈자료〉 한국인터넷진흥원, 2018년도 정보보호 실태조사 보고서

[그림 4] 침해사고 유형별 심각성 정도 설문조사 결과(단위: %)

공격의 심각성과 함께 내부 인력에 의한 중요 정보 유출에 대한 우려가 눈에 띄게 부각되고 있는 것이 현실이다[5].

이 조사 결과를 통해 업무의 결과물인 데이터에 대한 관리가 얼마나 중요한지를 알 수 있다. 이제는 랜섬웨어 공격에 대한 대책과 함께 내부 인력에 의한 중요 정보 유출을 방지하기 위한 보안의식 고취는 물론, 사전에 사고를 방지할 수 있는 시스템적인 방안에 대해서도 고민할 필요가 있는 것이다.

IV. 데이터의 안전하고 효율적인 관리 방안

전통적으로 국내에서는 중요 문서나 도면 파일 등이 다양한 경로를 통해 외부로 유출되는 사고에 대비하기 위해 DRM(Digital Right Management), DLP 등에 의존해 오고 있다. 또한, 랜섬웨어에 대응하기 위한 가장 최선의 방법은 백업이라고 업계에서는 이야기해 왔다.

하지만 DRM, DLP의 경우 각 분야의 업무 특성을 모두 반영하기에는 어려움이 있었으며, 랜섬웨어를 방지하기 위해 개인의 PC를 주기적으로 백업하는 방식에 대한 한계를 느끼게 되었다. 이에 따라 보안 측면의 차단에 중점을 두기보다는 안전한 환경에서 효율적

인 문서 유통을 위한 방안에 대한 관심이 커지고 있다.

문서는 생성/저장/유통/파기의 라이프 사이클이 존재하며, 이에 따라 문서에 대한 가시성을 확보해야 하기에 '문서중앙화'라는 개념이 주목받기 시작했다.

문서중앙화란 말 그대로 업무 중 생성되는 모든 문서들을 중앙 서버에 저장하고 활용하는 환경을 의미한다. 조직 내에 산재되어 있는 지식 자산들을 중앙 관리를 통해 내·외부 위협으로부터 보호하고, 동시에 효율적인 협업 환경을 구축하는 것을 목표로 한다. 국내에서의 문서중앙화 솔루션은 기본적으로 개인 PC에서의 매체 제어를 통해 로컬 드라이브나 USB 등에 문서가 저장되는 것을 원천 차단하고, 중앙 스토리지에 저장할 수 있도록 한다. 또한, 업무의 생산성 향상을 위한 다양한 기능과 보안정책들을 제공하고 있다.

문서중앙화 시장 초기인 2010년 초반에는 외산 EDMS나 ECM이 문서중앙화의 개념으로 국내에 진입했다. 하지만, 커스텀 이슈나 업무의 특수성 등으로 인해 정착하지 못하고 현재는 대부분 국내 업체의 문서중앙화 솔루션들이 주류를 이루고 있다. [표 1]의 주요 기능은 국내의 문서중앙화 솔루션이 기본적으로 제공하고 있는 기능들로서 대부분의 국산 솔루션들의 기술력이 상향 평준화되고 있는 상황이다[6]. 다만, 각 솔루션 벤더들은 '보안에 방점을 두느냐? 사용자의 편의성에 방점을 두느냐?'와 같은 출발점에 따라 솔루션의

[표 1] 문서중앙화의 주요 기본 기능

구분	기능	기능상세
매체 제어	로컬저장 금지	로컬 PC에 파일 저장 금지
	USB 및 외장하드 저장 제어	외부 HW 매체를 통한 유출 금지
	메일/메신저 파일첨부 제어	미결재 파일 반출 금지
사용자 기능	윈도 탐색기 기반 UI	기존 로컬 환경과 동일한 탐색기 환경
	개인함/공유함	개인파일 관리 및 공유폴더 구분 제공
	파일 로그 조회	개인 파일에 대한 이력조회 및 형상관리
	결재 기능	문서반출을 위한 결재 기능
	로컬 보안폴더	CAD 및 대용량 파일 관리를 위한 영역 제공
	오프라인 모드	네트워크 단절 시 파일 생성 기능 및 업로드
관리자 기능	파일 관리	모든 파일 목록 및 로그 조회
	사용자 관리	조직도 연동을 통한 유연한 사용자 관리
	중간관리자 설정	관리기능별 관리 권한 분할

〈자료〉 ㈜지란지교시큐리티 문서중앙화 표준제안서 참조

성격이 미묘하게 다른 모습을 보이고 있다. 하지만, 보안과 편의성 어느 하나 포기해서는 안 된다는 것이 필자의 소신이다.

보안에 중점을 두는 경우, 현업에서 업무의 흐름이 어디선가 정체 현상이 발생하게 된다. 반면, 사용자의 편의성에만 포커스를 맞추다 보면 보안의 홀이 어딘가에 존재하게 되어 일부 사용자들과 외부의 해커들이 이를 인지하게 될 경우에 치명적인 보안 사고가 발생하게 된다.

문서중앙화 검토 시 가장 궁금해 하는 사항이 “어느 시점부터 문서를 중앙화할 것인가”이다. 대부분의 솔루션들은 초기에 에이전트를 설치하면 매체 제어 기능이 활성화되어 로컬에 있는 모든 문서 파일들은 읽기 전용으로 속성이 변경되고, 이 파일들은 USB나 외장 하드를 통해 복사하지 못하도록 통제를 받게 된다. 본인이 업무적으로 사용할 파일들을 중앙 서버에 업로드한 이후에 파일 편집 등 정상적으로 사용할 수 있게 되며, 이후 신규로 생성되는 모든 파일들은 중앙 서버에만 저장된다. 만약, 회사의 정책에 따라 PC의 모든 파일을 강제 중앙화해야 한다면, 파일을 강제적으로 서버에 업로드할 수 있는 기능들도 제공되고 있다. 하지만 이 경우 개인적인 파일이나 업무에 불필요한 파일 등으로 인해 스토리지 용량 부담과 네트워크 부하 등이 발생하므로 신중한 결정이 필요하다.

에이전트 설치 및 파일 업로드 이후에는 윈도 탐색기에서 PC 환경과 동일하게 사용이 가능하기 때문에 사용자들은 이질감 없이 업무를 볼 수 있다. 또 문서중앙화 솔루션들은 화이트리스트 기반의 애플리케이션 제어를 하고 있어 인가되지 않은 애플리케이션은 중앙 서버의 파일에 접근하지 못하여 랜섬웨어를 원천적으로 차단하기 때문에 사용자들의 불안감을 불식시킬 수 있다. 일부 제품들은 랜섬웨어 방어를 위해 네트워크 드라이브 방식이 아닌 전용 탐색기 기반으로 제공하는 경우도 있다. 이 경우에는 안전성을 높일 수 있는 반면, 기존의 PC 업무 환경과는 상당 부분에서 차이가 있어 사용자에 따라 불편함을 느낄 수 있다.

기존 PC 업무 환경에서는 부서 동료나 타 부서와 협업을 위해 메신저나 이메일로 문서를 공유하고, 그 결과를 또다시 동일한 매체를 통해 주고 받는 과정에서 중복문서들이 기하급수적으로 생산된다. 또 이 문서들의 이력 관리를 위해 많은 리소스를 투자해야 한다. 이와 같은 비효율적인 업무 프로세스를 가지고 있다면 문서중앙화의 공유함을 통해 사용자 및 부서별 권한 설정으로 안전하게 유통/공유하고, 문서의 형상관리 기능을 활용

하여 효율적인 업무 협업 환경 구성을 기대해 볼 수 있다.

특히, 제조업의 경우 CAD나 그래픽 툴을 사용한 도면 설계나, 이미지 작업이 많은 업무 환경으로 네트워크로 파일을 액세스하여 편집하고 저장함에 있어 불가피하게 딜레이가 발생할 수밖에 없다. 문서중앙화는 로컬에 보안 드라이브를 생성하여 특정 보안 영역에 다운로드하여 편집하고, 스케줄링에 의해 이후 파일을 중앙 서버에 업로드될 수 있도록 제공하고 있어 불편함을 최소화한다. 동시에 보안장치를 통해 파일의 외부 유출이나 화면 캡처를 방지한다. 네트워크 단절 시에는 로컬 영역에 사용자가 저장할 수 있는 '템프 드라이브(Temp Drive)'를 활용하여 신규 문서를 생성하고, 네트워크 연결 시 중앙 서버에 강제 중앙화할 수 있는 등의 다양한 돌발 변수에 대한 대응이 가능하다.

이와 같은 문서중앙화가 기본적으로 갖추어야 할 기능 외에도 [표 2]와 같이 사용자의 요구 사항과 업무의 편의성, 컴플라이언스를 준수하기 위한 다양한 보안 기능들이 진화하고 있다. 개인정보보호법 제4장 29조에 의하면 "개인정보처리자는 개인정보가 분실·도난 유출·위조·변조 또는 훼손되지 아니하도록 내부 관리 계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 해야 한다"라고 명시되어 있다.

[표 2] 진화해 가는 특화 기능

구분	기능	기능상세
보안기능	문서 필터	개인정보 파일 및 민감 문구 검출 및 제어
	암호화	저장되는 파일 암호화 및 통신구간 암호화
	원격접속 및 출력물 제어	PC 원격차단 및 출력물(워터마크 등) 보안
편의기능	검색 기능	파일명, 본문검색, 상세검색
	태그/메모 기능	문서 속성에 태그/메모 Flag

〈자료〉 ㈜지란지교시큐리티 문서중앙화 표준제안서 참조

문서중앙화는 중앙 서버에 저장되는 파일 중에 개인 정보가 포함된 문서들이 저장될 경우에 별도의 격리 조치나 열람 권한 설정 등 다양한 사후 처리를 통해 컴플라이언스 준수를 용이하도록 한다. 또한, 본문 검색, 태그/메모에 대한 플래그 표시 기능 등 추후 파일의 검색을 용이하게 하기 위한 다양한 아이디어들이 적용되면서 국내 문서중앙화 솔루션이 제공하는 사용자 편의 기능은 갈수록 개선되고 있다.

V. 업무형태 변화에 대응(재택근무)

지난해 12월에 시작한 코로나19 감염병이 전세계적으로 확산 되며 세계보건기구(WHO)에서는 2020년 3월 11일에 팬데믹 선포에 까지 이르렀다. 국내뿐만 아니라 전 세계적으로 국가 비상사태를 맞으며 추가적인 감염병 확산을 막기 위해 안간힘을 쓰고 있다. 국내에서도 2월부터 사회적 거리두기 캠페인의 일환으로 재택근무를 독려하며 많은 기업들이 전사적으로 재택근무를 시행했다. 하지만 사전에 재택근무에 대한 매뉴얼 및 시스템이 갖춰져 있지 않은 기업들은 갑작스러운 상황에 어려움을 겪어야 했다.

문서중앙화 솔루션은 모든 업무 문서가 중앙의 서버에 저장되어 있기 때문에 이와 같은 상황에서 “재택근무 모드”로 전환하여 자택의 개인 PC에 Agent 설치만으로 사내의 동일한 보안 정책 내에서 바로 업무를 진행하고, 각자 자택에서 근무하고 있는 동료들과의 원활한 협업 환경을 구성할 수 있다. 재택근무가 종료되어 사무실로 출근하여도 재택 시 생성되었던 문서들을 그대로 활용할 수 있어 업무의 영속성을 보장 할 수 있게 한다.

많은 경제 전문가들은 이번 코로나19를 계기로 업무의 형태가 다양한 모습으로 변화를 이룰 것으로 예측하고 있다. 급변하는 업무 환경에 유연하게 대응하기 위한 우리의 노력과 준비가 필요한 시점이다.

VI. 신기술과의 융합

서두에 언급되었던 랜섬웨어나 악성코드를 유입시키기 위해 기존의 보안 환경을 무력화하고 사회공학(Social Engineering)과 보안 솔루션을 우회하는 기술을 결합한 문서 기반의 공격 기법들이 갈수록 지능화되고 있다. 이와 같은 문서 기반의 공격은 MS오피스, 한글(HWP), PDF 등 응용 소프트웨어에서 제공하는 액티브 콘텐츠(Macro, JavaScript, OLE 객체 등)를 이용하여 교묘하게 악성코드를 배포하기 때문에 일반적인 보안 위협보다 대응하기 어려운 게 사실이다. 이에, 기존 보안 솔루션을 보완할 수 있는 차세대 멀웨어 대응기술로 CDR(Content Disarm & Reconstruction; 콘텐츠 악성코드 무해화) 기술이 주목받기 시작했다.

문서중앙화는 신규 생성되는 문서뿐 아니라, 외부에서 유입되는 모든 파일들을 중앙에

〈자료〉 ㈜지란지교시큐리티 신기술융합사업부 제공

[그림 5] CDR(콘텐츠 악성코드 무해화) 과정

저장하기 때문에, 유입 경로가 이메일, 인터넷, USB 등 어디가 되었든 간에 중앙 서버에 저장이 되는 시점에서 [그림 5]와 같이 무해화 과정을 거치게 되면 중앙 서버에는 항상 무결한 파일들만 존재하여 한 단계 더 안전한 업무환경을 제공할 수 있게 된다.

향후 AI에 대한 연구 개발이 더욱 활발히 진행되어 문서보안 영역에 적용될 수 있다면 중앙 서버에 저장되어 있는 방대한 양의 데이터를 러닝머신의 학습을 통해 해당 조직에 적합한 “전사 표준 분류체계”를 자동화하고, 데이터 자산에 대한 위협을 사전에 감지하여 조치할 수 있는 시스템으로도 성장할 수 있을 것이라 기대한다.

VII. 결론

문서중앙화를 검토하는 과정에서 중도에 도입이 중단되거나 망설이는 경우를 종종 경험하게 된다. 가장 큰 이유 중 한 가지는 현업의 담당자들과의 충분한 이해와 협의가 부족하기 때문에 발생한다. 개인의 자산으로 인식되어 온 데이터를 회사의 자산으로 여기는 시각의 변화가 필요한 시점이다.

때문에 문서중앙화 도입 검토 시 반드시 목적을 분명히 하고, 이에 따라 조직과 업무의 성격에 맞는 정책 검토가 선행되어야 한다. 문서중앙화 솔루션에는 매체 제어를 통해 초기 도입 시 강제 업로드할 것인지 혹은 사용자가 업무에 필요한 문서만을 업로드할 것인지부터 로컬 저장 금지의 범위, 외부 반출 문서의 범위 및 결재 워크플로우, 개인 정보 및 기밀문서의 범위 등 조직별 특성에 맞게 범위를 설정하고 충분한 설득과 이해관계를 형성해야 한다.

문서중앙화 솔루션은 한번 도입하게 되면 회사의 자산을 중앙에서 관리하기 때문에 제품을 선정함에 있어 신중함을 거듭해야 할 것이다. 우리가 설정한 목적에 부합하는 제품인지, 사용자의 편의성과 보안 측면에서 적절하게 잘 조합이 되었는지를 판단해야 한다. 또한, 장애 발생 시 업무가 중단될 수 있기 때문에 지속적인 유지 보수를 위한 개발사의 신속하고 유연한 기술 지원 역량과 사업의 영속성 또한 아주 중요한 항목이다.

과거에는 데이터 자산의 중앙화의 필요성에 대한 인식이 높지 않았다. 또 솔루션의 안정성 및 개발사의 영세함 등으로 인해 문서중앙화 시장의 확대가 어려웠다. 하지만 기술의 발전에 따라 보이지 않는 내외부 위협에 대응하기 위한 업계와 정부의 노력이 지속되고 있으며, 이에 따라 데이터 자산의 중앙화에 대한 관심도 높아지고 있다. 올바른 정책과 내부 협의를 통해 적합한 시스템을 도입하여 기업 내 중요 자산인 데이터를 안전하게 보호해야 할 것이다.

[참고문헌]

[1] ITWorld, “지난 5년간 규모가 컸던 랜섬웨어 공격 6종”, 2019. 12. 27.
[2] SBS뉴스, “랜섬웨어 오늘이 고비..‘컴퓨터 켜기 전 인터넷 끊어야”, 2017. 5. 15.
[3] 중소벤처기업부, “2017년도 중소기업 기술보호 수준실태조사 보고서”, 2018. 1, 10.
[4] 한국인터넷진흥원, “2018년도 정보보호 실태조사 보고서”, 2019, p.47.
[5] 한국인터넷진흥원, “2018년도 정보보호 실태조사 보고서”, 2019, p.88.
[6] 데이터넷, “문서중앙화에 대한 편견과 오해”, 2017. 11. 9.