[보안칼럼] 재택근무 도입 후, 개인정보 유출 위험 최소화 하려면

길민권 기자 | 승인 2020.08.31 13:38

VDI방식 기준 재택근무 이후 보안대책 강화해야

[필자] 김대환 소만사 대표이사.

코로나19 재확산으로 인해 다시 재택근무를 시행하는 기업이 늘어났다.

대기업은 대부분 VDI(Virtual Desktop Infrastructure, 데스크톱가상화) 인프라가 구축되어 있다. 사무실로 출근하지 않아도 원격에서 VDI를 통해 사내 네트워크에 접속해 그룹웨어, 메일확인 등 일상적인 업무를 수행할 수 있다. VDI로 접속하면 윈도우 화면정보만 전송되기 때문에 재택근무 PC로 파일이 업로드/다운로드 되지 않는다. 정보유출이나 악성코드 유입 위험으로부터 안전하다.

그러나 VDI 라이선스는 매우 고가이다. 투자비용이 만만치 않고, 원격접속시에는 사내에서 PC를 이용하는 것보다 반응속도가 느린 단점이 있다. 영상, 디자인 등 특수직종에는 적합하지 않다. VDI는 컴퓨팅이 서버에서 이루어지고, 엔드포인트 PC에서는 오직 화면만 보이는 구조이다. 개발업무는 대부분 컴퓨팅이 데스크탑 PC에서 이루어지기 때문에, 일반적인 VDI방식으로는 업무하기 쉽지않다.

보안관점에 있어서, 재택근무의 도입은 기존 사내근무에서 발생하지 않았던 문제를 야기시키고 있다.

첫번째, 재택근무는 회사 직원과의 물리적인 접촉을 완벽하게 없앴다. 보는 눈이 없기 때문에 동료에 의한 오남용 견제효과를 무력화시킨다.

두번째, 원격접속으로 들어오는 직원이 영업본부 K과장이 맞는지, 아니면 K과장의 계정을 해킹한 해커인지 확인하기 어렵다. 정교한 본인인증절차가 필요하다.

세번째, 사옥이라는 물리적인 보호체계가 없다. 노트북, 출력물, USB 도난에도 취약하다.

마지막으로 재택근무는 네트워크 보안장비의 도움을 받지 못한다. 악성코드가 재택근무 PC를 공격하면 속수무책으로 보안사고가 발생할 수 있다.

재택근무는 피할 수 없는 선택이다. 기업과 기관은 개인정보/기밀정보 유출통제, 내외부 접속시 데이터 공개범위 세분화, 엔드포인트 PC 보안체계 강화, 강화된 인증체계 구성, 철저한 감사로그 확보라는 보완대책을 마련해야 할 것이다. 특히 개인정보유출은 개인과 법인 모두 형사처벌에 처해질 수 있는 것이 현재의 법체계이다.

재택근무 도입 전 보안담당자는 다음 문제를 해결해야 한다.

첫번째, 개인정보 및 기밀정보 유출을 통제할 수 있어야 한다.

사옥 안에서 근무할 때는 업무상 취득한 개인정보를 외부로 반출하기 쉽지 않다. USB와 같은 이동식 저장매체를 반입하는 것도 어렵다. 밖으로 가지고 나가는 것도 까다롭다. 문서도 마찬가지다. 모 반도체기업은 특수 코팅된 용지를 사용해서 문서를 출력한다. 회사 밖으로 가지고 나갈 때 센서가 이를 감지하고 경보를 울리기도 한다. 사내에서 근무할 경우, PC에 저장된 개인정보 및 기밀정보 파일에 대해서는 모두 기록이 남는다. 웹메일 및 클라우드 전송, USB 파일 복사, 프린터 출력 등이 통제되고 기록이 남는다.

하지만 재택근무시 이러한 물리적 보호조치 중 몇 가지는 무력화된다. VDI방식으로 재택근무를 할 경우, 파일 자체가 PC에 다운되지 않기 때문에 안전하다고 생각할 수 있다. 하지만 화면 캡쳐, 사진촬영, 수기로 옮기는 행위는 막을 수가 없다. 회사에서는 스마트폰이나 영상촬영장치를 반입해도 주변 눈치가 보여서 촬영하기 어려우나 재택근무환경에서는 그러한 긴장관계로부터 자유롭다.

재택근무가 자택 내 자기만의 방에서 이루어지면 다행이다. 하지만 그런 환경을 확보할 수 있는 직원은 생각보다 많지 않다. 재택근무를 수행하는 많은 장소 중 하나는 카페이다. 카페에서는 고개만 살짝 돌리면 옆자리 사람이 뭘 하는지, 뭘 보는지 알 수 있는 환경이다.

이 경우에는 화면 워터마킹 기능을 강화하거나, 화면캡쳐 방지(인식) 기능을 적용하는 것이 좋다.

두번째, 내외부에 접속에 따른 정보공개범위 제한이 필요하다.

사내에서 내부 시스템에 접근하는 경우, 단순 데이터 조회에 대해서는 크게 신경 쓰지 않는다. 외부로 노출되는 것이 아니기 때문이다. 그러나 외부에서 조회할 때는 이야기가 달라진다. 단순 조회도 통제할 수 없는 '외부노출' 개념이 적용, 보호되어야 한다.

원격접속시에는 사내메일조회도 '외부전송수준'으로 보호해야 할 수도 있다. 어떠한 방식으로도 정보가 노출, 유출될 수 있기 때문이다. 사내 개인정보처리시스템도 접속 장소에 따라서 노출되는 정보수준이 차등화 되어야 할 것이다. 민감한 개인정보, 핵심디자인 설계도면, 보안수준이 높은 회계정보 등은 원격접속시 조회되지 않도록 권한관리를 세분화해야 할 것이다.

그래서 콜센터를 운영하는 모 회사는 재택근무자들에게는 상품설명 등 일반 안내서비스 처리하도록 하고, 고객개인정보 조회가 필요한 서비스는 사내 콜센터에서 운영하는 이원적인 체계를 유지하고 있다.

고객정보, 기밀정보를 조회할 수 있는 웹어플리케이션의 권한관리 조정은 금방 처리할 수 있는 업무가 아니다. 이와 연동된 사내 주요 프로그램과 함께 수정되어야 하기에, 수개월 이상 소요된다. 하지만 감염위험을 최소화하기 위해, 재택근무는 당장 시행돼야 한다. 기다릴 수가 없다.

만일 VPN 원격접속을 통해서 사내 웹어플리케이션에 접속할 경우에는 웹어플리케이션과 PC 사이에 시큐어 웹프록시를 설치하는 것이 좋다. 원격접속시 웹프록시는 사용자 권한에 따라 특정한 메뉴접속을 차단하기도 하고, 민감한 정보가 노출되는 화면에서는 화면조회내역을 모두 남기도록 구축할 수 있기 때문이다.

세번째, 엔드포인트 보안강화와 인증강화가 필요하다.

사내에는 네트워크에서 엔드포인트 PC에 이르기까지, 여러 단계로 악성코드차단/정보유출방지에 관한 기술적 조치가 구축되어 있다. 방화벽, IPS, APT, 유해사이트 접속차단, 웹프록시, 네트워크 DLP, 스팸차단솔루션 등이 네트워크를 겹겹으로 보호하고 있다. 물리적으로 인터넷망과 내부망을 원천적으로 차단하여 '망분리 정책'으로 운영하는 곳도 다수 존재한다. 금융기관이 대표적이다.

그러나 재택근무시 사용하는 노트북은 어떠한 네트워크 보안장비의 도움없이 바로 인터넷에 노출된다. 오직 엔드포인트 보안솔루션으로만 보호받을 수 있다.

이에 따라서 재택근무시에는 안티바이러스/EDR, DLP등 주요 엔드포인트 보안솔루션을 반드시 설치하고 정책을 강화해야 한다. 예를 들면 사내 시스템 접속시에는 다른 인터넷 트래픽을 모두 차단하는 설정하는 것이다. 최근 방화벽과 같은 경계선 보안(Perimeter Security) 솔루션 개발은 살짝 주춤하고, 엔드포인트 보안이 조금 더 강화되는 추세가 보이고 있다. 클라우드 환경 도입 증가 및 재택근무의 확산 때문이다.

네트워크 보안에 무방비한 상태에서 악성코드에 감염될 경우, 내가 사용하는 재택근무 PC가 불법접근 PC로 이용될 수도 있다. PC가 악성코드에 감염, 장악된 후 내 PC를 숙주로 나도 모르는 사이에 사내 네트워크에 들어와 마음대로 정보를 유출하고 데이터를 위변조 시킬 수 있기 때문이다. 로그인 체계를 강화해야 할 것이다.

마지막으로 감사기록 확보와 이상징후를 통제해야 한다.

원격접속으로 들어온 영업본부 K과장이 정말 본인지 맞는지 100% 확신할 수 없기에, 감사로그 확보와 이상징후 분석능력이 더 업그레이드되어 있어야 한다.

최근, 솔루션 개발자와 협력업체 원격지원에 대한 감사로그 확보가 이슈 되고 있다.

솔루션 개발은 일반적인 VDI접속 환경과는 다르다. VDI는 컴퓨팅이 모두 서버에서 이루어지고, 단순히 화면만을 받아보는 구조인데 개발자들은 모든 컴퓨팅이 개발자 데스크탑에서 이루어진다. 솔루션 컴파일을 위해서는 사내 데스크탑의 강력한 컴퓨팅파워가 필요하고, 사내 데스크탑을 통해서만 사내 소스코드 관리서버와 통신할 수 있기 때문이다. 물론 해외 글로벌회사 중 몇몇은 솔루션 소스코드 자체도 깃허브(Github) 같은 곳에 올려놓고 개발하는 경우가 있긴 하다.

개발자들은 VDI보다 재택근무 PC에서 VPN으로 윈도우터미널서비스에 접속하여 로컬 데스크탑처럼 작업하는 것을 더 선호한다. 윈도우 터미널 서비스 내역은 자체적으로 감사로그가 기록되지 않는 단점이 있었다. 이를 보완하기 위해 RDP(Remote Desktop Protocol) 프록시 등을 통해서 작업 감사기록을 남기는 것을 검토해야 한다.

원칙적으로 협력업체는 자사에서 원격터미널 서비스를 통해 거래처 네트워크 인프라와 서버에 접근할 수 없다. 금지하고 있다. 특히 금융기관은 감독규정 등으로 엄격하게 규제하고 있다. 그러나 코로나19로 인하여 협력업체가 회사사옥에 방문, 근무하는 것을 제한하게 되면서 그 절충안으로 원격접속을 통한 지원을 용인하고 있다. 장애발생시 협력업체의 빠른 지원이 필요한 것은 코로나19 이전에도 이후에도 동일하기 때문이다. 이 경우 사내직원이 원격접속 내역을 실시간으로 모니터링하고 있기는 하다. 그러나 원격접속을 통해 작업한 내역에 관하여 세부적인 감사기록을 자동적으로 남기는 것도 반드시 검토되어야 한다.

재택근무는 한 두 달 시행하고 끝나는 것이 아니다. 바이러스가 종식될 때까지 상당기간 계속 지속될 것으로 예측된다. 보안 담당자는 새로운 비즈니스 환경에 따라, 새로운 보안 대응체계를 구축해 나가야 할 것이다.

국내 보안 솔루션 업체들은 클라우드, 재택근무 관련 기술개발을 꾸준히 진행해왔으며 적용사례를 확대해 나가고 있다. 화면 캡처방지, 화면 워터마킹, RDP프록시를 통한 터미널 서비스 접속기록관리, 시큐어웹프록시, VPN, VDI 솔루션 등이 대표적이다.

물론 언제나 가장 중요한 것은 '보안에 대한 마인드'이기에, 직원들의 보안인식 또한 재택근무에 맞추어 강화되어야 할 것이다.

[글. 김대환 소만사 대표이사]

★정보보안 대표 미디어 데일리시큐!★

길민권 기자