국내 스마트워크 활성화와 보안에 대한 연구

이은비, 김재훈, 김기형

아주대학교

silver1012@ajou.ac.kr, jaikim@ajou.ac.kr, kkim86@ajou.ac.kr

A study on Activation and Security of Smart Work

Eunbi Lee, Jai-Hoon Kim, Ki-Hyung Kim

Ajou University

요 약

코로나 19 영향으로 비대면(Untact) 근무 체계를 구현하기 위해 스마트워크 추진이 강화되고 있는 추세이다. 그러나 국내 기업은 가장 큰 우려 요인으로 보안 문제를 지목한다. 본 논문은 보안약점의 일반적인 심각성을 평가할 수 있는 정량적 평가 기준을 사용하여 스마트워크가 도입된 환경에서의 보안약점을 평가한다. 이를 통해 스마트워크 체제 전환 시에 발생할 수 있는 보안 약점을 최소화하여 국내 스마트워크 활성화에 도움을 줄 수 있을 것으로 기대한다.

Ⅰ. 서 론

최근 시간과 공간의 제약 없이 비대면, 온라인 방식으로 업무 수행을 가능하게 하는 스마트워크가 국내에서 주목 받고 있다. 해외는 사실 오랜 기간 동안 인구 구조 변화의 대응책으로서 스마트워크를 도입하고 널리 활용해왔다. 그러나 [그림 1]에서 보는 바와 같이 국내 스마트워크 도입율은 현저히 낮은 상황이다.

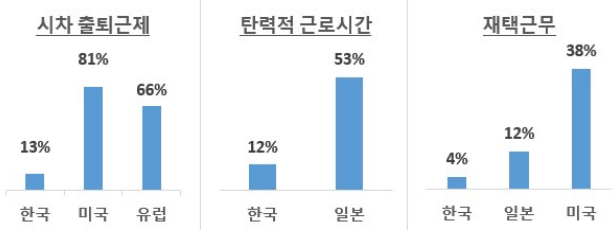

그림 1. 국내 스마트워크 도입 현황 - 해외 비교 [1,2]

Ⅱ. 본론

2.1 스마크워크에서의 클라우드 컴퓨팅 보안

클라우드 컴퓨팅 기술은 언제 어디서나 데이터를 저장, 추출, 관리 할 수 있다는 점에서 스마트워크와 밀접한 연관을 가진다. 원하는 정보에 접근이 가능하고 구성원들과 업무를 공유하고 협업 할 수 있다. 그러나 저장된 데이터가 산재되어 있다는 점이 보안 우려의 주요인으로 보인다. 클라우드 도입을 주저하는 이유에는 기밀 데이터를 회사 밖에 저장하는 것에 대한 우려 때문이라는 답변이 가장 많았다. [3]

2.1.1 정량적 보안약점 평가 시스템

클라우드 컴퓨팅은 웹에 기반한 소프트웨어 서비스이기 때문에 보안약점을 평가할 수 있는 시스템을 척도로 사용했다. 소프트웨어 보안약점은 소프트웨어의 결점으로 인하여 공격을 유발할 가능성이 있는 보안 취약점을 일컫는다. [4] 다양한 소프트웨어 보안약점 중에서 우선순위를 파악하는 것이 보안 강화에 도움될 것이라고 판단된다. [5] 따라서 본 연구는 스마트워크를 도입한 근무 환경, 스마트워크를 도입하지 않은 근무 환경을 2 가지로 나누어 보안약점을 정량적으로 평가한다.

2.1.2 보안 약점의 정량적 평가를 위한 기반 연구

CWSS(Common Weakness Scoring System)는 소프트웨어 보안약점의 중요도를 정량적으로 평가하는 체계이다. [그림 2]는 해당 시스템이 제시하는 16 개의 평가 척도가 기본 발견 심각성, 공격 측면의 심각성, 환경적 심각성 3 개의 그룹으로 분류됨을 보여준다. 그리고 그룹 항목별 점수를 산출식에 적용하면 보안약점 점수를 0 에서 100 사이의 점수가 도출된다. [6]

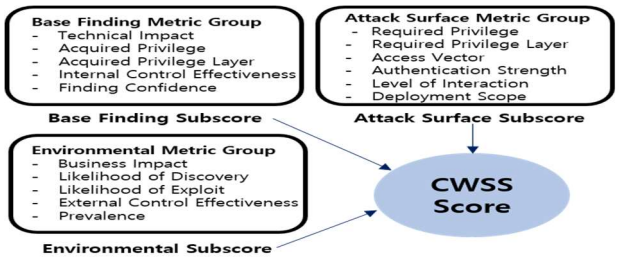

그림 2. Common Weakness Scoring System (CWSS) Scoring [6]

2.2 평가 척도 별 점수와 근거

16 개의 평가 척도는 특정 소프트웨어에서의 특정한 보안약점을 평가하는데 사용된다. 따라서 스마트워크 도입 환경에서 보안약점의 일반적인 중요도 평가에 적합하다고 판단되는 6 개 척도를 선정하여 평가 항목으로 사용하였다.

1) 기술적 영향: 데이터 침해는 클라우드 보안 협회에서 2 년 연속 가장 큰 위협요인으로 선정한 문제이다[7]. 스마트워크를 미도입한 환경에서도 데이터 유출에 따른 피해 심각성이 클 것으로 예상되지만 스마트워크를 도입한 환경보다는 피해 심각성이 적을 것으로 판단된다. 클라우드의 가상화 기반 취약점으로 인해 악성코드 감염 및 전파, 디도스 공격 등의 관련 피해가 일어나기에 좀 더 쉬운 환경이기 때문이다. [8]

2) 필요 권한: 최근 CSA(Cloud Security Alliance)는 엑세스 권한 보호를 위해 ID, 크리덴셜, 엑세스, 키 관리의 중요성을 강조하고 있다[7]. 클라우드 솔루션을 도입하는 기업이 많아지고 개인정보 보호 의식이 강화되어 원격근무 솔루션의 보안 기능 및 인증이 강화되고 있는 추세이다[9]. 스마트워크가 도입되지 않은 근무 환경에서도 보안 침해를 위한 시스템에 접근하기 위해서 부분적인 관리자 권한을 필요로 한다고 판단하여 동일한 등급의 같은 점수를 부여했다.

3)상호작용 정도: 클라우드 보안 사고 사례 중, 직원 계정을 해킹하여 회원 정보를 유출하고 스팸메일을 발송한 사례, 소프트웨어 취약점을 해킹하여 데이터를 손실 시킨 사례를 확인할 수 있다. [10] 이를 통해 피공격자가 평소 업무 시에 하는 일반적 행동들을 수행해야 해당 보안약점에 대한 공격이 가능하다고 판단했다. 스마트워크 미도입 환경에서는 클라우드 보안 사고 발생 확률이 적으며 어느 정도 의심이 될만한 작업을 수행해야 공격이 가능해질 것으로 예상된다.

4)발견 가능성: 사물인터넷 및 빅데이터의 확산으로 전보다 많은 기업이 주요 정보를 클라우드에 보관하고 있다. 따라서 클라우드 보안 약점을 발견하고 침해하는데 성공하면 얻는 이득이 클 것으로 예상된다. [11] 그러나 클라우드 시스템의 복잡성이라는 특성 때문에 취약점 발견에 성공하기 위해서는 높은 기술을 요구될 것으로 판단된다. 스마트워크를 도입하지 않은 환경에서는 클라우드를 매개로 타인과 데이터를 공유할 확률이 적으며 성공에 따른 이익도 많지 않아 해커의 공격 타겟이 되기 쉽지않을 것으로 예상된다.

5)침해 가능성: 클라우드 업무 환경에서 단말기 플랫폼 종류는 다양하고 각 단말이 가진 보안 위협도 다르다[10]. 클라우드는 저장된 데이터의 정확한 위치를 파악하기가 어렵고 다수의 사용자가 자원을 사용할 수 있는 '공유자원'의 특성을 가진다. [11] 즉, 침해가 다양한 곳에서 다수의 원인으로 일어날 것으로 예상된다. 스마트워크를 도입하지 않은 환경은 다른 사용자와 클라우드를 통해서 파일을 공유하지 않으므로 취약점 발견 및 침해 성공 확률 모두 낮을 것으로 예상된다.

6)출현도: 클라우드 보안 사고 사례 분석을 통해 데이터 보호 책임의 주체가 사용자에게 옮겨가고 있음을 알 수 있다. CSA (Cloud Security Alliance)에서 최근에 발표한 2019 년 클라우드 보안 위협요소는 보안 사고 문제의 대부분이 기술적 문제보다 기술 외적인 문제가 많음을 보여준다[7]. 스마트워크를 도입하지 않은 환경에서는 취약점이 실제로 출현하는 정도가 적으며 보안약점이 정기적으로 발견되는 수준이라고 판단된다.

평가 척도별 점수를 CWSS (Common Weakness Scoring System)에서 제시한 계산식은 하기와 같다. [6]

보안약점 중요도 점수 = 기본 발견 심각성 × 공격 측면의 심각성 × 환경적 심각성

기본 발견 심각성 = [(10 × 기술적 영향 + 5 × (획득한 권한 + 획득한 권한 계층) + 5 × 발견 신뢰도) * 내부 통제 효과] × 4.0

공격 측면의 심각성 = [20 × (필요 권한 + 필요 권한 계층 + 접근 벡터) + 20 × 배포 범위 + 15 × 상호작용정도 + 5 × 인증 강도] / 100.0

환경적 심각성 = [(10 × 사업적 영향 + 3 × 발견 가능성 + 4 × 침해 가능성 + 3 × 출현도) × 외부 통제 효과] / 20.0

※ 선정한 6 가지 척도를 제외한 나머지 척도에 대해서는 제외(Not Applicable)의 점수인 1.0 을 부여하였다. 반영되지 않은 평가 척도는 평가 등급 중 제외(Not Applicable)로 평가되어 점수가 적용되기 때문에 CWSS(Common Weakness Scoring System) 에서 제시된 점수 산출식을 그대로 사용하였다. [6]

2.3 중요도 점수에 대한 평가와 비교

표 1. 스마트워크를 도입한 환경에서의 보안 약점 중요도 점수

평가 항목	평가결과		평가 근거
기술적 영향	C	1.0	TI 항목 / 점수 Modify data (2/1/0) / 2 Read data (2/1/0) / 2 DoS: unreliable execution (2/1/0) / 1 DoS: resource consumption (2/1/0) / 1 Execute unauthorized code or commands (4/2/0) / 2 Gain privileges / assume identity (2/1/0) / 1 Bypass protection mechanism (2/1/0) / 1 Hide activities (2/1/0) / 1 합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N) / 11
필요 권한	P	0.6	전체적인 관리자 권한은 필요하지 않으나 부분적인 관리자 권한을 필요로 함
상호작용 정도	T	0.9	피공격자의 일반적인 행동이 수행되어야 침해가 가능함
발견 가능성	M	0.6	공격자가 보안 약점 발견을 위해 소스코드 접근 혹은 역공학을 수행해야함
침해 가능성	D	0.6	해당 보안 약점으로 인한 침해 가능성이 다양하게 일어날 경우
출현정도	W	1.0	해당 보안약점이 매우 종종 발견되는 경우이나 일반적으로 광범위하게 퍼져 있지는 않음
전체 점수	**77.8**		

표 2. 스마트워크를 도입하지 않은 환경에서의 보안 약점 중요도 점수

평가 항목	평가결과		평가 근거
기술적 영향	H	0.9	TI 항목 / 점수 Modify data (2/1/0) / 1 Read data (2/1/0) / 1 DoS: unreliable execution (2/1/0) / 0 DoS: resource consumption (2/1/0) / 0 Execute unauthorized code or commands (4/2/0) / 2 Gain privileges / assume identity (2/1/0) / 1 Bypass protection mechanism (2/1/0) / 0 Hide activities (2/1/0) / 0 합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N) / 5
필요 권한	P	0.6	전체적인 관리자 권한은 필요하지 않으나 부분적인 관리자 권한을 필요로 함
상호작용 정도	M	0.8	피공격자가 어느 정도 의심이 될만한 작업을 수행해야 해당 보안 약점에 대한 공격이 가능함
발견 가능성	L	0.2	공격자가 보안 약점을 발견하기 위해서 고도로 전문화된 기술과 함께 많은 시간량을 투자하여 소스코드에 접근해야함
침해 가능성	M	0.6	공격자가 해당 보안 약점을 공격할 확률은 높으나 성공을 위해 다수의 시도를 필요로 함
출현정도	C	0.8	해당 보안약점이 정기적으로 발견되는 경우
전체 점수	**65.8**		

[표 1]과 [표 2]의 비교를 통해 스마트워크를 도입한 환경이 그렇지 않은 근무 환경보다 12 점 높은 보안 약점을 가지고 있음을 알 수 있었다. 이는 기술적 피해 영향, 상호작용 정도, 공격자의 보안 약점 발견 및 침해 가능성, 취약점 발생 사례 측면에서 보안 취약점을 줄이기 위해 노력해야한다는 점을 보여준다.

Ⅲ. 결론

포스트 코로나를 대비하여 점차 많은 기업들이 온프레미스(On-premise) 환경의 인프라를 클라우드 환경을 전환할 것으로 예상된다. 근무 형태의 디지털 전환이 안정적으로 이루어질 수 있도록 클라우드 보안 강화 연구 또한 지속적으로 이루어 져야할 것이다.

ACKNOWLEDGMENT

이 논문은 2018 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업과(NRF-2018R1D1A1B07040573) 2020 년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (P0008703, 2020 년 산업전문인력역량강화사업).

참 고 문 헌

[1] 고용노동부. 일·가정 양립 실태조사. 세종: 고용노동부 여성고용정책과, 2016

[2] 대한상공회의소. 2016. "기업의 유연근무제 도입 실태 조사". http://www.korcham.net/nCham/Service/Economy/appl/KcciReportDetail.asp?SEQ_NO_C010=2012093085 0&CHAM_CD=B001

[3] IDG Korea. 무엇이 클라우드 도입을 주저하게 하나. 서울: IDG Korea, 2015

[4] 행정안전부 · 한국인터넷진흥원, 전자정부 SW 개발 · 운영자를 위한 소프트웨어. 세종: 행정안전부, 2019

[5] 안준선, 방지호, 이은영. "소프트웨어 보안약점의 중요도에 대한 정량 평가 기준 연구." 정보보호학회논문지 22, no.6(2012): 1407-1415

[6] CWE (Common Weakness Enumeration). 2014. "Common Weakness Scoring System". http://cwe.mitre.org/cwss/

[7] CSA (Cloud Security Alliance). "Top Threats to Cloud Computing: Egregious Eleven.", 2019

[8]정성재, 배유미, "클라우드 보안 위협요소와 기술 동향 분석." 보안공학연구논문지 10 , No.2(2013): 199-211

[9] 소프트웨어정책연구소. 원격근무 솔루션 기술·시장 동향 및 시사점. 성남: 소프트웨어정책연구소, 2020

[10] 정부 3.0 추진위원회, 정부 3.0 클라우드 인프라 및 서비스 기획연구, 서울: 정부 3.0 추진위원회, 2014

[11]소프트웨어정책연구소. 클라우드 보안의 핵심이슈와 대응책. 성남: 소프트웨어정책연구소, 2017