스마트워크 환경에서 정보보호를 위한 보안위협 및 취약점 분석

An Analysis of Security Threats and Vulnerabilities for Information Protection in Smartwork Environment

김 희 완*
삼육대학교*

Kim, Hee-Wan*
Sahmyook Univ.*

요약

본 연구에서는 스마트워크 환경에서 정보보호를 위하여 사용자와 서비스 제공자 입장에서 정보보호 요구사항을 분석하고, 정보보호 요구사항을 바탕으로 스마트워크 도입 및 운영 관점에서의 보안 위협 및 취약점을 분석하여 대안을 찾고자 한다.

Ⅰ. 서론

정보기술의 발달로 생산성 향상을 위해 스마트워크를 도입하고 있으며 국내에서는 ICT 인프라를 바탕으로 스마트워크가 급속히 활성화 되고 있다. 스마트폰 및 태블릿 PC 등 본인의 장비를 업무에 이용하는 BYOD(Bring Your Own Device)의 확산과 전국적인 무선네트워크 서비스 보급 및 SBC(Service Base Cloud) 와 같은 클라우드 컴퓨팅 기술의 발전으로 스마트워크가 활성화 될 수 있는 환경을 제공하고 있다. 스마트워크를 추진함에 있어 많은 기업들은 업무 생산성 향상, 비용절감 등의 효율성은 향상되지만, 그에 따른 다양한 보안 위협이 존재하며 기업의 정보자산 및 서비스에 대한 문제 해결을 원하고 있는 실정이다. 따라서 스마트워크 확산을 위해 해결되어야 할 보안위협 및 취약점을 분석하여 대안을 찾고자 한다.

Ⅱ. 스마트워크

1. 스마트워크 개요

한국은 세계 최고 수준의 ICT 인프라를 바탕으로 스마트워크 분야의 경쟁력을 가지고 있지만, 면대면 접촉을 선호하는 조직문화, 보고·평가·근태 등 관리체계 문제, 그리고 정보보호에 대한 부정적인 인식 등으로 스마트워크가 확산되는데 한계점을 가지고 있다. 최근에는 공공부문 모바일 웹·앱을 제공하는 국가대표포털(m.korea.go.kr), 민원 모바일인 민원24, 행정업무를 수행하기 위한 모바일 오피스도 운영되고 있다. 민간부문에서는 삼성그룹, 코오롱그룹, GS정유 등 주요기업에서 선도적으로 모바일 오피스를 제공하고 있으며, SKT, KT, 삼성SDS 등은 기업 대상 모바일 오피스 사업 영역을 확장 중에 있다[1].

모바일오피스(Mobile Office)는 스마트폰 등의 이동형 단말기 및 무선인터넷(3G/4G/WiFi/Wibro) 등의 무선정보기술을 이용하여 언제 어디서나 기업의 데이터, 프로세스, 시스템에 접속하여 업무를 수행할 수 있는 기업 업무 환경을 의미한다[2]. 모바일오피스는 공간 제약 없이 실시간 업무처리를 가능하게 하여 현장 중심의 경영이 강화될 수 있는 특징을 가진다. 또한, 위치정보 등 모바일 기술의 특성을 활용하여 업무 프로세스 개선 및 비즈니스 모델혁신 등의 새로운 가치 창출이 가능하다[2].

2. 모바일 기반요소 기술

모바일 O/S 및 단말기는 업그레이드와 Version-Up 작업이 지속적으로 이루어지고 있으므로, 이를 검토하여 기업에 적합한 O/S와 단말기를 선정하는 작업이 필요하다[3].

모바일 서버 플랫폼은 다양한 단말 환경을 지원하여 적은 비용으로 다양한 스마트폰 환경에 적용될 수 있는 기능을 제공해야 한다. 스마트폰 플랫폼의 종류, 모바일 웹, 모바일 어플리케이션, 리치 클라이언트 등의 다양한 클라이언트 형태를 지원하고, 사용자 경험에 바탕을 둔 UI를 제공할 수 있어야 한다. 또한, 관리기능 및 보안기능을 제공함으로써 단말들의 효율적인 관리 및 제어기능을 제공하고, 단말분실 또는 해킹 등의 취약점을 해결할 수 있는 보안기능도 제공할 수 있어야 한다. 그리고 백엔드 통합 기능을 제공함으로써, 기존의 비즈니스 로직과의 연동, SNS와의 연동등과 같이 모바일 환경을 충분히 활용할 수 있는 기능을 제공하여야 한다[3].

클라이언트 플랫폼은 [표 1]과 같이 3가지 방식이 있으며 각각의 특징과 장단점을 고려해야 한다.[3].

표 1. 모바일 클라이언트 플랫폼 특징[3]

구분	특징
독립적인 Native Application	- 각 O/S에 맞도록 개별 어플리케이션을 별도로 개발하는 형태 - 성능은 우수하나 OS별로 각각 개발함으로써 비용이 높아지는 단점
통합 미들웨어를	- OS에 관계없는 범용화가 가능하나, 각각의 OS의 Version up 및 변경사항을

구분	특징
통한 단일 Application	미들웨어에 반영해야 하므로 지원기간이 늦어지거나 운영비용의 증가할 소지가 있으며 미들웨어 탑재에 따른 성능이 떨어지는 단점 발생
Hybrid client Platform	- High Performance, Medium Cost

Ⅲ. 모바일오피스 정보보호

1. 스마트워크 정보보호 요구사항

본 절에서는 모바일오피스에서의 정보보호 요구사항을 도출하였다.

1.1 사용자 입장에서의 정보보호 요구사항

1) (사용자인증) 서비스를 등록한 본인 이외에는 인증을 통과할 수 없어야 함
2) (단말인증) 서비스를 등록한 단말 이외에는 서비스를 사용할 수 없어야 함
3) (가용성) 사용자는 언제, 어디서나 서비스를 사용할 수 있어야 함
4) (무결성) 애플리케이션 및 콘텐츠의 무결성을 보장해야 함
5) (접근제어) 전송되거나 서버에 저장되는 데이터는 데이터와 특성에 따라 보호되어야 함
6) (자료백업) 클라우드 스토리지에 저장된 자료의 손실을 막기 위해 백업 기능을 제공해야 함
7) (내용 프라이버시) 제3자는 사용자가 사용하는 서비스 및 콘텐츠의 내용을 알 수 없어야 함
8) (AP 인증) AP에 대한 안전성 분석 기능을 제공해야 함
9) (자료저장 제어) 자료의 유출을 막기 위해 허가된 스토리지 외에는 저장되지 않아야 함
10) (자료공유 제어) 서비스를 사용할 수 있는 사용자들 간의 자료 공유가 제한되어야 함
11) (사용 제어) 서비스를 사용하는 본인 이외에 다른 사람들이 서비스 내용을 볼 수 없어야 함
12) (위치 프라이버시) 사용자가 휴대 단말을 이용하여 서비스를 받을 경우 제3자는 사용자의 위치를 추적할 수 없어야 함

1.2 서비스 제공자 입장에서 정보보호 요구사항

1) (서비스보안) 사용자가 사용하는 서비스가 다양한 공격으로부터 원치 않은 피해를 방지할 수 있어야 함
2) (단말보안) 사용자가 사용하는 단말기가 다양한 공격으로부터 원치 않은 피해를 방지할 수 있어야 함
3) (서버보안) 서버가 다양한 공격으로부터 원치 않은 피해를 방지할 수 있어야 함
4) (부정사용방지) 인가되지 않은 사용자가 서비스를 이용할 수 없어야 함

2. 스마트워크 보안 위협 및 취약점

스마트워크 정보보호 요구사항을 바탕으로 스마트워크 도입 및 운영 관점에서의 보안 위협 및 취약점을 도출하였다.

표 2. 스마트워크 구조별 보안 위협 및 취약점[4]

분류	내용
공통부분의 보안 위협 및 취약점	
사용자	정보를 유출 하고자 하는 악의적인 직원
	기업 정보를 가진 직원의 퇴사
서비스	업무 서비스의 보안 취약점
	계정도용으로 인한 비허가자의 업무 서비스 사용
무선	보안이 설정되지 않은 AP와의 무선랜 연결
	블루투스, 와이파이 다이렉트와 같은 직원간의 직접적인 정보교환
네트워크	네트워크 구간에서의 패킷 스니핑
	스위치, 라우터 등 네트워크 장비 해킹
사내망	휴대단말을 경유한 내부 서버 해킹
	클라우드 컴퓨팅의 보안 취약점
모바일오피스 보안 위협 및 취약점	
사용자	직원의 부주의한 업무 수행
단말	업무 단말의 분실.도난
	가족, 친척 등 지인의 업무 단말 사용
	업무 단말의 정보 백업, 동기화
	업무 단말의 판매.양도
	업무 단말 운영체제의 보안 취약점
	비허가 단말에서 업무 애플리케이션 사용

스마트워크 환경에서는 다양한 보안위협이 존재하고 있으며 이러한, 보안위협은 전혀 막을 수 없는 위협들이 아니라 사용자나 기업(기관)의 측면에서 관리한다면, 보다 안전한 스마트워크 환경을 구축할 수 있을 것이다. 국내외 기업(기관)에게 스마트워크 도입을 촉진하고, 스마트워크 환경 구축을 활발하게 하기 위해서는 스마트워크에 대한 보안 대책을 마련하여 스마트워크 환경에서 발생할 수 있는 보안 사고를 최소화하고 미연에 방지할 수 있도록 하여야 한다.

Ⅳ. 결론

스마트워크를 통해 근무 위치와 무관하게 원격 협업 환경을 구성하고 보다 유연한 근무 환경 기반 형성이 가능하여 업무 효율성 향상 등 많은 이점을 기대할 수 있다[1][9].

하지만, 스마트워크 환경은 많은 보안 취약점을 갖고 있으며, 따라서 안전한 스마트워크 환경을 구축하기 위해 신뢰성이 높고 체계적인 위험관리를 통해 보안위협과 취약점 분석을 통하여 적절한 정보보호 대책을 마련하였는지를 점검할 필요가 있다.

■ 참 고 문 헌 ■

[1] 한국정보화진흥원, “국가정보화백서”, 한국정보화진흥원, 2011.
[2] 한기준, 김동수, 김희완, “스마트워크 기반의 정보보호 감리 모형”, 디지털정책연구, 제11권, 제2호, pp.229-239, 2014.
[3] 방송통신위원회, “기업을 위한 스마트워크 도입 운영 가이드 북”, 방송통신위원회, 2011.
[4] 한국인터넷진흥원, “스마트워크 도입을 위한 정보보호 수립 기준 연구”, 한국인터넷진흥원, 2011.