TLP:WHITE

비대면 서비스 개발·운영 환경
주요 보안 취약 사례별 대응방안

인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

과학기술정보통신부

KISA 한국인터넷진흥원

CONTENTS

집　　필 : 사이버방역단 방역점검팀
김대완 선임, 고은혜 선임
배승권 팀장

감　　수 : 신대규 본부장, 서정훈 단장

KISC KrCERT/CC KOREA INTERNET SECURITY CENTER
인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

제1장
개요

Ⅰ. 개요

1. 배경

원격교육, 화상회의, 비대면 진료 등 ICT 기반의 다양한 비대면 서비스가 일상화되고, 제조, 유통 등 전통산업 분야의 디지털 전환이 가속화되면서 디지털 역량이 국가 경쟁력을 결정짓는 핵심요소로 강조되고 있다.

산업 전반에 비대면 확산 및 디지털 전환이 가속화됨에 따라 새로운 사이버 보안 위협도 빠르게 증가하고 있다. 특히, 클라우드, 빅데이터, AI 등을 활용한 비대면 업무 환경 도입 및 디지털 전환 과정에서 관련 시스템과 서비스의 보안 취약점을 노린 공격도 증가할 것으로 예상된다.

기업의 전산시스템이 폐쇄형 시스템에서 원격근무 지원을 위한 개방형 분산 시스템으로 변화하고, 원격근무, 화상회의 등 비대면 서비스, IoT 적용 확대 등 네트워크 연결 접점이 증가하면서 침해사고에 대한 위협도 함께 증가하고 있다.

기업에서는 이러한 사이버 보안 위협 및 해킹 공격으로부터 피해를 입지 않도록 철저한 대비가 필요하다. 하지만 일부 기업의 경우, 인력과 예산 부족 등의 이유로 비대면 도입 및 디지털 전환 준비가 미흡한 상황이며, 정보보호 활동에도 어려움을 겪고 있는 실정이다.

이에 한국인터넷진흥원은 안전한 디지털 이용 환경을 조성하고 국민들이 비대면 서비스를 안심하고 이용할 수 있도록 원격교육, 화상회의 등 비대면 서비스를 개발·운영하는 중소기업의 인프라(시스템, 네트워크 등)를 대상으로 보안 취약점을 점검하고 기업이 해당 취약점을 조치할 수 있도록 지원하였다.

본 매뉴얼는 비대면 서비스 개발·운영 환경에 대한 보안 취약점 점검 결과를 바탕으로 발견된 주요 취약 사례에 대한 위험성을 알리고 취약점을 보완하기 위한 고려사항과 대응 방안을 제시하고 있으며, 더 나아가 침해사고 예방 및 이용자 피해를 최소화하고자 한다.

2. 매뉴얼 목적 및 구성

목적	- 비대면 서비스의 안전한 개발·운영 환경 구축 - 비대면 서비스 개발·운영 기업의 침해사고 예방 및 서비스 이용자의 피해 최소화
대상	- 비대면 서비스 개발자 및 운영자(IT, 보안)
범위	- 본 매뉴얼에서 제시하는 내용은 서비스 개발·운영 환경의 보안 강화를 위한 일부 방안을 포함하고 있음 · 취약점 대응을 위한 상세 방안 등은 기업별 서비스 운영 방식 및 운영 환경을 검토하고, 응용하여 적용해야 함
구성	Ⅰ. 개요 1. 배경 2. 매뉴얼 목적 및 구성 Ⅱ. 주요 보안 취약 사례 및 대응 방안 1. 네트워크 보안 2. 유·무선 공유기 보안 3. 클라우드 보안 4. 서버 보안 5. 데이터베이스 보안 6. 업무용 PC 보안 Ⅲ. 시사점

제2장

주요 보안 취약 사례 및 대응 방안

Ⅱ. 주요 취약 사례 및 대응 방안

한국인터넷진흥원에서는 비대면 서비스를 개발·운영하는 기업을 대상으로 보안 취약점 점검을 진행하며 네트워크, 유·무선 공유기, 클라우드, 서버, 데이터베이스, 업무용 PC로 분야를 나누어 보안수준을 진단하였다. 각 분야별 발견된 주요 보안 취약 사례와 함께 보안 강화를 위한 대응 방안을 알아보고자 한다.

1. 네트워크 보안

서비스 개발·운영 환경에서 접근통제가 미흡한 경우, 비공개 파일 다운로드나 비공개 페이지(관리자 페이지, 서버 자원 관리 페이지 등)의 외부 노출이 발생할 수 있다. 이런 비인가 접근은 악성코드 삽입이나 개인정보 유출 등의 침해사고로 이어질 수 있어 주의가 필요하다.

이와 같은 침해사고를 예방하고 네트워크 보안을 강화하기 위해서는 개발·운영 환경에 필요한 접근을 식별하고 통제해야 한다.

네트워크 보안 분야에서는 네트워크 구성 및 접근제어 항목을 중점적으로 점검하였다. 점검 결과 주요 시스템의 분리 운영 미흡(53.1%)과 네트워크 영역 간 접근통제 미흡(90.9%) 등의 취약 사례를 확인하였다.

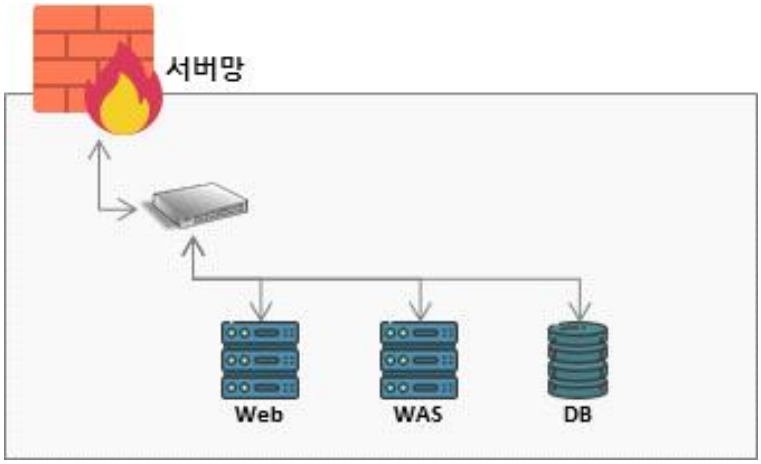
1 독립 서버 운영

Web서비스와 DB와 같은 중요 서비스를 하나의 서버에서 운영하는 경우, 특정 서비스의 장애 및 공격으로 인한 서버 중단이 다른 서비스까지 영향을 미치게 될 수 있다. 또한 외부 노출이 불필요한 서비스가 외부에 노출될 수 있는데, 특히 Web, WAS, DB를 동일 서버에서 운영하는 경우에는 DB의 중요 정보가 유출될 수 있다.

위와 같은 피해를 방지하기 위해 서버는 목적 및 서비스에 따라 분리하여 운영해야 한다. 일반적으로 서버는 아래와 같이 분리하여 구성하며, 기업에서 운영 중인 서비스의 특성에 따라 서버를 다양하게 분리 운영할 수 있다.

분류	대상
Web 서버	- 사용자 직접 접속이 필요한 Web 서비스 등
WAS 서버	- 동적인 데이터를 처리하는 서비스 등
DB 서버	- 데이터를 저장하는 DB 서비스 등
기타 서버	- 기타 주요 목적이 다른 서비스 등

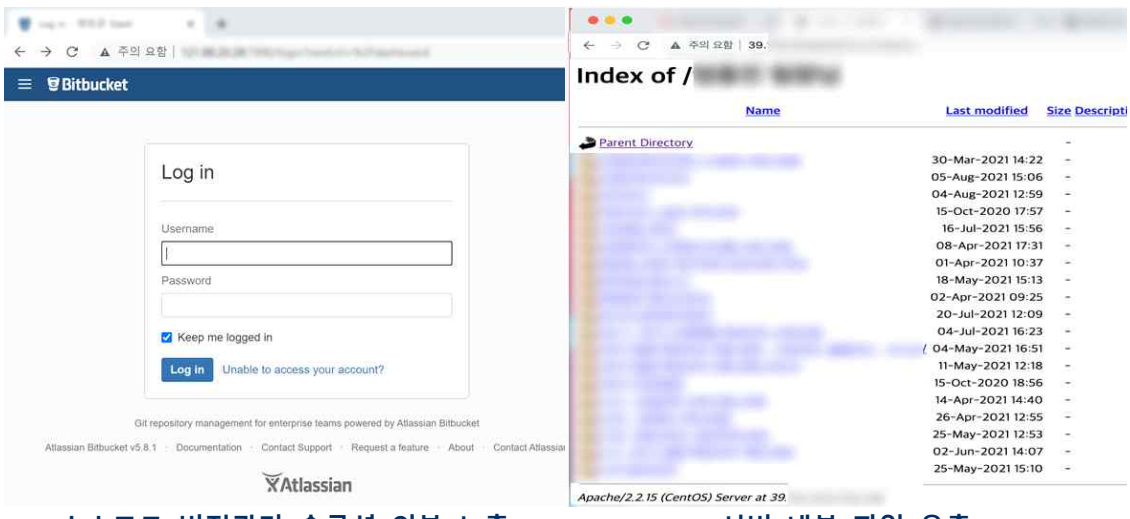
<그림 1-1> 서버 분리 운영 예시(On-premise)



2 네트워크 영역 분리 운영

대외 서비스를 제공하는 서버와 외부 노출이 불필요한 서버를 네트워크 영역을 분리없이 같은 네트워크에서 운영하는 취약 사례도 확인하였다. 네트워크 영역 분리가 미흡한 경우, 내부 서버가 외부에 노출될 수 있으며 이로 인해 소스코드나 인증정보와 같은 중요정보가 유출될 수 있으므로 주의가 필요하다.

<그림 1-2> 내부 서비스의 외부 노출 사례



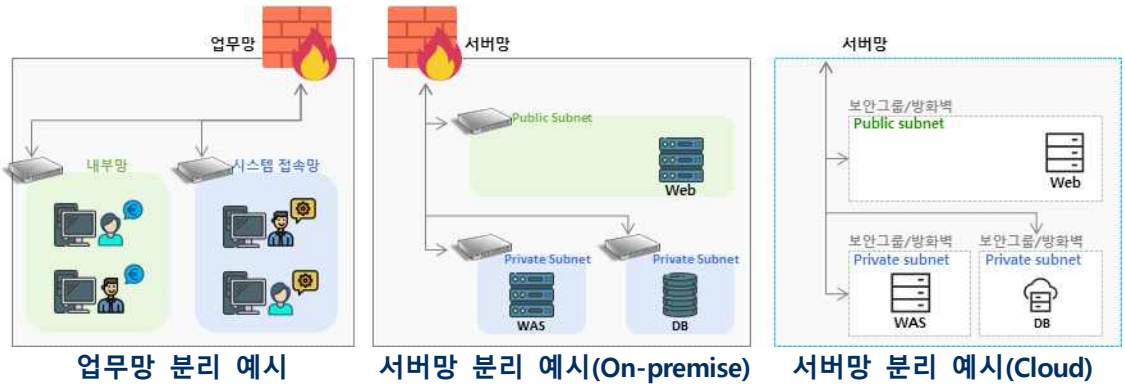
소스코드 버전관리 솔루션 외부 노출 서버 내부 파일 유출

네트워크를 분리하면 악성코드가 감염되었을 때, 다른 네트워크로 피해가 확산되는 것을 방지할 수 있다. 네트워크를 분리할 때에는 업무 목적에 따라 업무망, 시스템 운영망(서버망 등)으로 분리할 수 있다.

또한 아래 예시처럼 업무망과 서버망 내에서도 업무의 중요도 및 특성을 고려하여 네트워크를 다양한 방식으로 구성할 수 있다.

분류		용도
업무망/사내망	시스템 접속망	- 서비스 개발·운영 환경에 접속할 수 있는 네트워크
	내부망	- 사내 업무 네트워크
	외부망	- 외부 인터넷에 접속할 수 있는 네트워크
서버망	DMZ/Public Zone	- 외부 접근이 필요한 서버를 운영하는 네트워크
	내부망/Private Zone	- 외부 접근이 불필요한 서버를 운영하는 네트워크

<그림 1-3> 네트워크 영역 분리 예시



업무망 분리 예시 서버망 분리 예시(On-premise) 서버망 분리 예시(Cloud)

제시한 예시 이외에도 기업별로 위험분석을 통해 수립한 네트워크 관리 정책에 따라 보다 세부적으로 네트워크 영역을 분리하여 운영할 필요가 있다.

3 네트워크 접근통제

특히 네트워크 영역 간 접근통제가 미흡한 사례가 다수 기업에서 확인되었는데, 아래는 발견된 접근통제 미흡 사례 중 일부(예시)이다.

① 위탁업체 작업, 외근 작업 등의 임시 정책 등록 및 사용 후 미삭제

출발지	목적지	포트번호	허용/거부	비고
1.1.1.1	DB서버	TCP/3306	Allow	DB(임시)

② 네트워크 변경에 따른 신규 정책 추가 후, 기존 정책 미삭제

출발지	목적지	포트번호	허용/거부	비고
2.2.2.2	Web서버	TCP/22	Allow	원격접속
3.3.3.3	Web서버	TCP/22	Allow	원격접속(과거)

③ 모든 대상으로부터 모든 서버, 서비스 접근 허용

출발지	목적지	포트번호	허용/거부	비고
Any	Any	Any	Allow	-

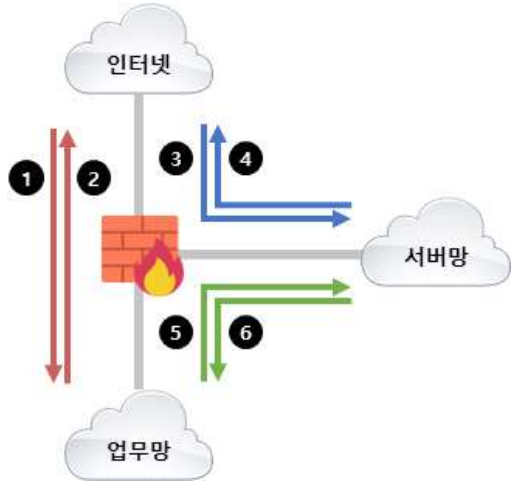
위 사례 ①, ②처럼 네트워크 접근통제 정책이 관리되지 않아 미사용 정책이 삭제되지 않고 남아있는 경우가 많았다. 특히 사례 ③은 불특정 사용자로부터 네트워크의 서버 및 데이터베이스 등에 대한 모든 접근이 허용된 상태이다. 이렇게 모두 허용 정책이 적용된 경우, 서버 내부 정보가 유출되거나 무작위 대입 공격(Brute Force Attack)으로 인해 서버 제어권이 탈취될 수 있다.

<그림 1-4> 접근통제 미흡으로 인한 접근시도 사례

네트워크 접근통제를 위해서는 해당 네트워크에 접속이 필요한 사용자 혹은 시스템과 관련 서비스의 파악이 선행되어야 한다. 방화벽 정책을 설정하게 되면, 방화벽은 출발지, 목적지, 포트 정보를 통해 접근을 식별하고, 식별된 접근은 정책에 따라 접근통제 한다.

아래는 업무망 및 서버망에 일반적으로 필요한 접근제어 정책이다. 업무 형태에 따라 필요한 접근제어가 다를 수 있다.

<그림 1-5> 네트워크 접근제어 정책 예시



구분	접근제어 정책
① 인터넷→업무망	전체 차단
② 업무망→인터넷	전체 허용(내부직원 인터넷사용) 유해사이트 차단
③ 인터넷→서버망	웹 서비스 관련 접근 허용
④ 서버망→인터넷	전체 차단 필요 IP, Port만 허용
⑤ 업무망→서버망	필요 IP, Port만 허용
⑥ 서버망→업무망	필요 IP, Port만 허용

아래는 일반적인 서비스 운영 상황에서의 서버망 내부 방화벽 정책 예시이다. 기업에서 운영하는 서비스의 특성에 따라 필요한 방화벽 정책이 다를 수 있으므로, 하단의 방화벽 정책은 단순 참고용으로만 활용하고, 기업 내부적으로 충분한 검증 후 적용해야 한다.

정책번호	출발지	목적지	포트번호	허용/거부	비고
6	사무실	DB서버	TCP/3306	Allow	DB
5	사무실	Web서버, WAS, DB서버	TCP/22	Allow	SSH
4	WAS	DB서버	TCP/3306	Allow	DB
3	Web서버	WAS	TCP/8009	Allow	서비스
2	Any	Web서버	TCP/80,443	Allow	HTTP,HTTPS
1	Any	Any	Any	Deny	-

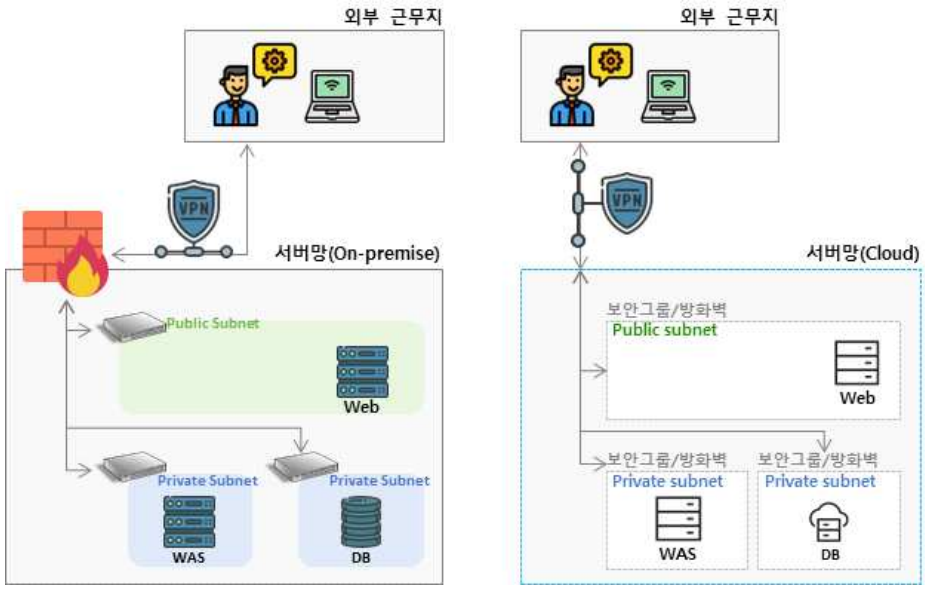
① 식별되지 않은 모든 접근 거부(Deny)
② Web서버는 대외서비스 제공을 위해 모든 대상으로부터 Web 서비스 포트(HTTP, HTTPS) 접근 허용
③ WAS는 Web서버로부터 요청을 받아 처리 후, 다시 Web서버로 전달하기 위해 서비스 포트 접근 허용
④ DB서버는 WAS에서의 DB 조회 등의 작업을 위한 접근 허용
⑤⑥ 시스템 유지보수나 DB 직접 접속을 위해 관리자(운영, 개발 등)의 서버 접속 허용

4 통신 채널 보안

추가로, 최근 원격근무가 증가하여 회사 사무공간이 아닌 외부에서의 서버 접속 및 관리가 필요한 경우가 많다. 가정에서 사용하는 개인 네트워크 혹은 카페, 공항 등에서 사용하는 공용 네트워크는 보안이 충분하지 않기 때문에, 해당 네트워크를 사용하는 모든 디바이스는 보안 위협에 노출되어있다. 이렇게 외부 네트워크를 이용해 서버에 접속해야 하는 경우, VPN(Virtual Private Network) 접속 및 암호화 통신 적용을 통한 보안 강화가 필요하다.

On-premise 환경에서의 경우 대부분의 방화벽에서 제공하는 Client to Site 방식의 SSL VPN 기능을 활성화하여 VPN을 구성할 수 있다. 클라우드 환경에서도 VPN, Client VPN 기능을 적용할 수 있다.

<그림 1-6> VPN을 통한 시스템 접속



VPN 접속 예시(On-premise) VPN 접속 예시(Cloud)

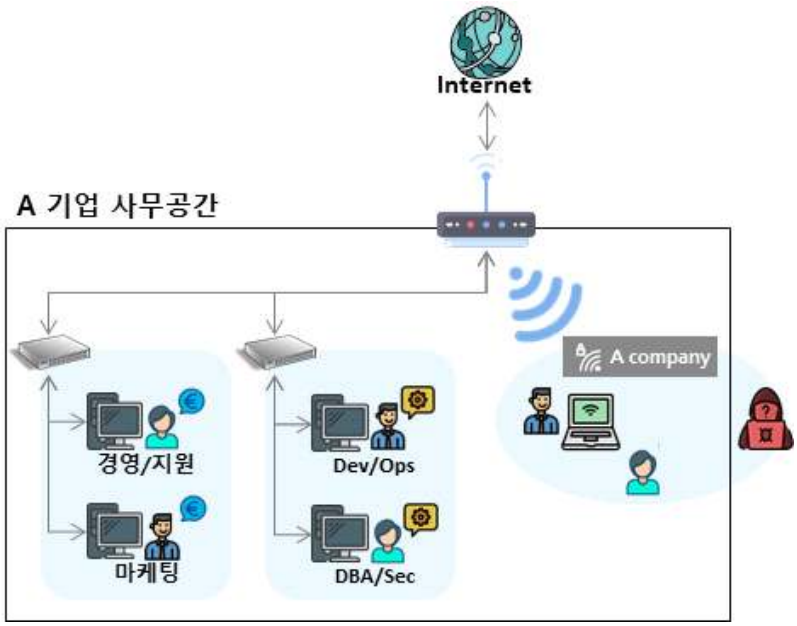
2. 유·무선 공유기 보안

대부분의 기업이 회의실에서의 노트북 사용, 공유 오피스 근무 등으로 무선 네트워크를 이용*하고 있다. 특히, 소규모 기업일수록 비용 등의 문제로 별도 네트워크 회선을 구축하지 않고 공유기를 이용하는 등 무선랜 의존도가 높게 나타났다.

* 비대면 서비스 개발·운영 환경 점검 대상 기업 중 98%가 업무망 내 무선랜 운영

무선 공유기는 간편하게 설치가 가능하며 네트워크 접속의 편의성을 증가 시켜주지만, 동시에 네트워크로의 접점이 늘어나기 때문에 보안 위협도 증가하게 된다. 무선랜의 가장 큰 취약점은 물리적으로 사무실 내부에 침입하지 않더라도 외부에서 사내 네트워크에 침투할 수 있다는 점이다. 무선랜은 비콘(beacon)이라는 무선신호를 발생시키며, 이 신호 때문에 건물 상·하층 및 공용 복도에서 사내 네트워크에 대한 식별 및 접속시도가 가능하다.

<그림 2-1> 업무환경에서의 무선 공유기 운영 예시



유·무선 공유기 보안 분야에서는 초기 인증 정보 설정, 최신 펌웨어 업데이트, 무선 네트워크 보호대책 등을 점검하였다. 점검 결과 다수의 기업에서 무선 네트워크 환경을 사용하고 있지만 보호대책 적용은 미흡(95.2%)한 것으로 확인되었다.

1 무선랜 관리

업무망에서 무선랜을 운영하는 경우, 방화벽 우회 및 업무망으로의 직접 침입 등의 수단이 될 수 있다. 따라서 무선랜은 업무 목적이 아닌 회의실, 게스트 제공 등을 목적으로만 활용하고, 업무망과 분리하여 별도 운영하는 것을 권고한다. 업무에 무선랜 이용이 필요한 경우, 다음 사항들에 대해서 충분히 고려하고 이용정책을 수립한 뒤 도입하여야 한다.

무선랜 운영 보안정책(예)

① 무선랜 용도 정의
② 무선랜을 통한 접근 가능 네트워크 범위 정의
③ 취약하지 않은 암호 사용 및 주기적인 암호 변경
④ 관리자 지정 및 주기적 보안 점검
⑤ 주기적인 로그 점검
⑥ 기타 (무선랜 사용시간 제한 등)

[참고] 알기쉬운 공중 무선랜 보안 안내서, KISA

무선랜을 도입할 때에는 관리자 페이지 초기 인증정보 변경, 불필요한 서비스 비활성화, 최신 펌웨어 업데이트, 보안 설정 적용 등을 해야 한다.

2 SSID 알림 설정

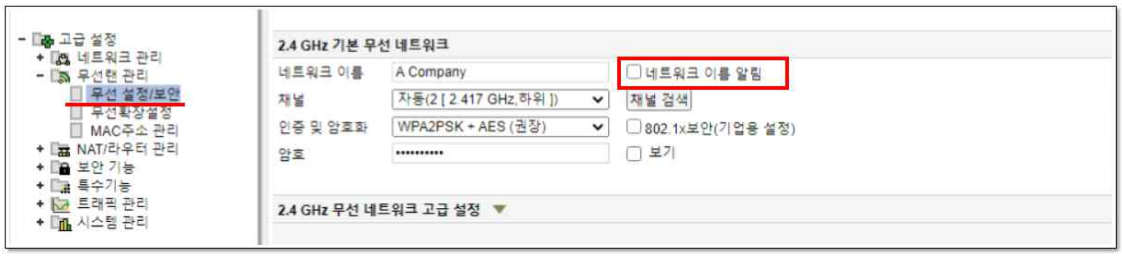
네트워크 이름 알림 기능을 사용하게 되면, 비인가자가 SSID*를 보고 특정 기업의 무선 네트워크임을 쉽게 식별할 수 있다.

* SSID(Service Set IDentifier) : 무선 장치간에 구분하기 위한 문자열 식별자

이를 방지하기 위해 무선랜의 SSID를 주변에 알리지 않도록 "네트워크 이름 알림 기능" 해제 또는 "SSID 숨김"을 설정하고 사용하여야 한다.

· SSID 알림 기능 해제 방법

<그림 2-2> 무선랜 SSID 알림 기능 해제 설정 화면



① 무선랜 관리페이지 접속
② 고급 설정 > 무선랜 관리 > 무선 설정/보안 열기
③ '네트워크 이름 알림' 체크 해제

* 공유기 모델에 따라 기능 설정 방법이 다를 수 있음

3 무선랜 인증 절차 – 패스워드

무선랜에 패스워드를 적용하였지만 관리 편의성을 위해 단순 반복 문자열과 같이 쉽게 유추가 가능한 패스워드를 사용하는 사례가 확인되었다.

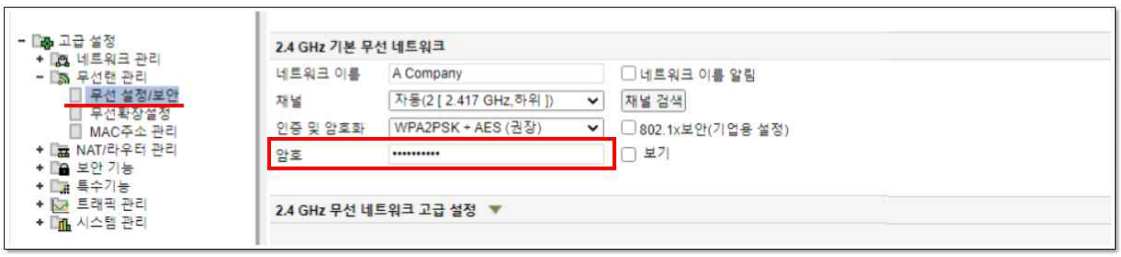
<그림 2-3> 무선랜 인증 관리 미흡 사례

취약한 패스워드 사용 외부인 접견구역 무선랜 사용

패스워드는 비인가자의 침입으로부터 네트워크를 보호할 최소한의 보안 설정 중 하나로 패스워드가 설정된 경우 비인가자는 네트워크에 바로 침입할 수 없다. 인가된 사용자만이 무선 네트워크에 접속할 수 있도록 패스워드를 설정하여 인증절차를 추가하여야 한다.

· 패스워드 설정 방법

<그림 2-4> 무선랜 암호 설정 화면



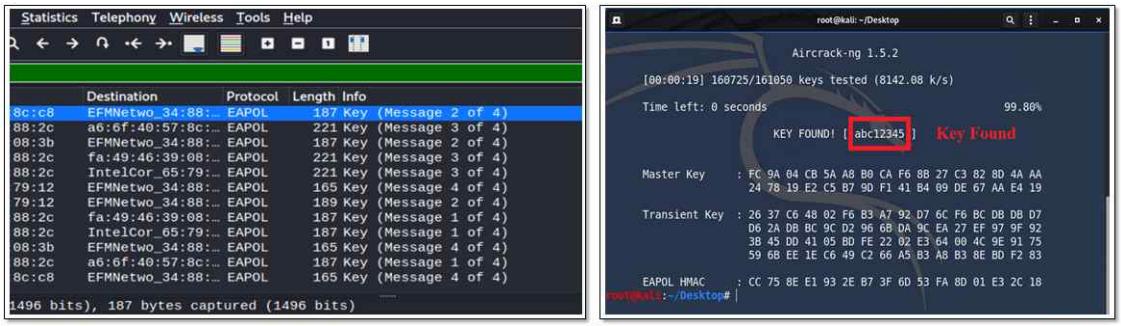
① 무선랜 관리페이지 접속
② 고급 설정 > 무선랜 관리 > 무선 설정/보안 열기
③ 암호 설정

* 공유기 모델에 따라 기능 설정 방법이 다를 수 있음

4 무선랜 인증 절차 – MAC 주소 인증

비인가자는 패스워드가 설정된 무선랜에 대하여 인증 정보 탈취, 사전 공격(Dictionary Attack) 등을 통해 네트워크 접속 시도를 할 수 있다.

<그림 2-5> 무선랜 인증정보 탈취 및 크랙 예시



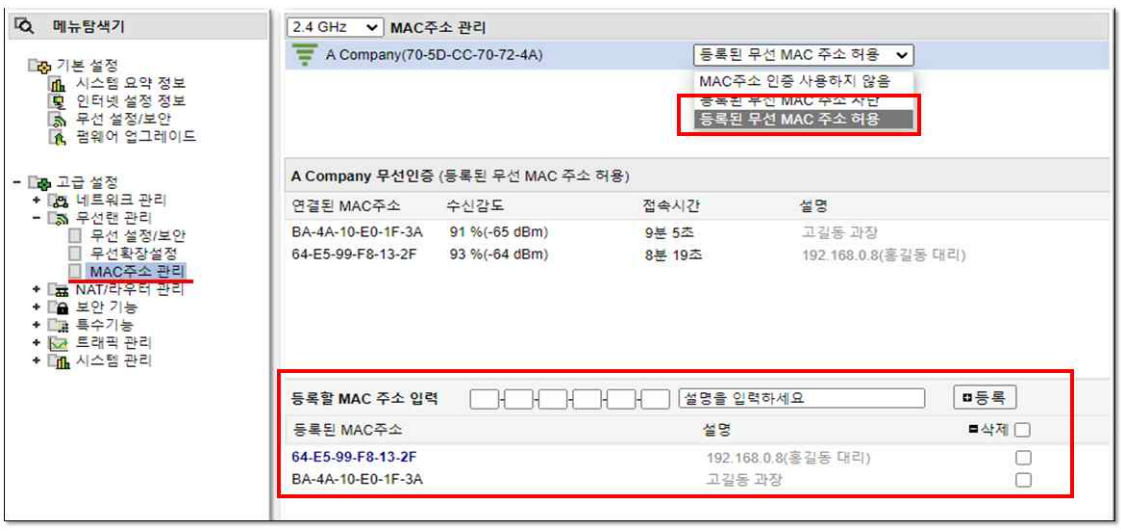
이렇게 인증정보를 탈취하여 무선랜에 접근하는 경우, 디바이스 인증과정을 추가하여 비인가자의 네트워크 접속을 차단할 수 있다. 디바이스 인증은 접속 디바이스의 MAC* 주소로 인가된 디바이스인지 확인하기 때문에 등록되지 않은 MAC 주소를 가진 디바이스의 접속을 차단한다.

* MAC(Media Access Control Address) : 네트워크상에서 기기 구분을 위해 사용되는 네트워크 카드의 물리적 주소

디바이스 MAC 주소 인증을 설정할 때 허용할 MAC 주소를 등록하지 않고 기능을 활성화하면 모든 기기들의 접속이 불가능해질 수 있다. 따라서 MAC 주소 인증 설정을 적용하기 전에 무선랜 접속할 디바이스를 식별하고, MAC 주소를 등록하여야 한다.

· 디바이스 인증 설정 방법

<그림 2-6> 무선랜 연결 시 디바이스 인증 설정 화면



① 무선랜 관리페이지 접속
② 고급 설정 > 무선랜 관리 > MAC 주소 관리 열기
③ 디바이스의 MAC 주소 입력 및 등록
④ '등록된 무선 MAC 주소 허용' 설정

* 공유기 모델에 따라 기능 설정 방법이 다를 수 있음

3. 클라우드 보안

On-Premise, IDC, 클라우드 등 비대면 서비스 개발·운영을 위한 다양한 환경이 있지만, 최근에는 물리적 공간, 비용을 포함한 초기 투자비용 절감 등을 목적으로 기업 규모와 상관없이 다수의 기업에서 클라우드 환경을 도입*하고 있다.

* 비대면 서비스 개발·운영 환경 점검 대상 기업 중 63%가 클라우드 환경 이용

클라우드 서비스는 관리 콘솔을 통해 서버를 쉽게 확장하거나 관리할 수 있게 도와준다. 하지만 클라우드 관리 콘솔에서 서비스 개발·운영 환경 전체에 대한 직접 제어가 가능하기 때문에 각별한 주의가 필요하다.

클라우드 분야에서는 클라우드 계정 관리 및 권한 검토, 콘솔 접근제어 등을 점검하였다. 점검 결과 관리자 계정 관리 및 권한 검토 취약(90.9%) 사례가 다수 기업에서 확인되었다.

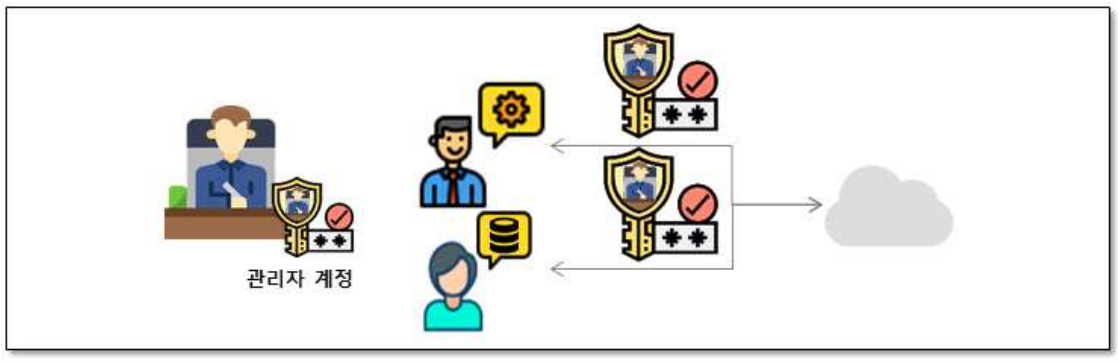
* 주요 취약 사례 및 대응 방안은 다수의 기업에서 사용 중인 AWS를 예시로 작성하였다.

1 계정 관리

클라우드 관리 콘솔의 계정 관리에서는 사용자 계정 없이 관리자 계정만 사용하거나 사용자 계정을 공용으로 사용하는 등의 계정 관리 미흡 사례가 확인되었다.

계정은 사용자를 식별하기 위한 정보로 공용으로 사용하는 경우, 침해사고가 발생했을 때 원인 분석이 어려울 수 있다. 특히, 클라우드 관리 콘솔의 관리자 계정은 최고 관리자 권한을 가지고 있기 때문에 계정 정보가 유출되는 경우 클라우드 인프라에 대한 제어권이 탈취될 수 있다.

<그림 3-1> 관리자 계정 공유 사용



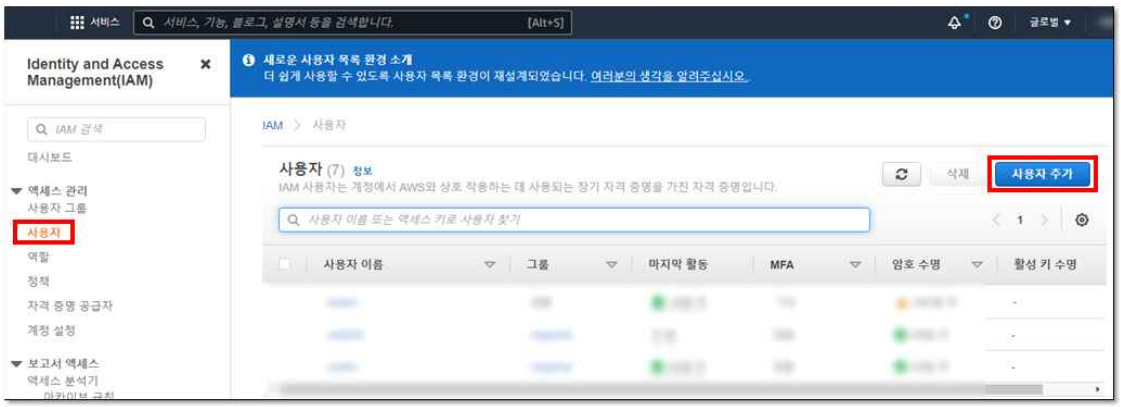
클라우드 관리 콘솔은 일반적으로 관리자 계정(루트 사용자, Main Account 등) 이외에 별도로 사용자 계정(IAM, Sub Account 등)을 생성할 수 있다. 관리자 계정은 클라우드 서비스에 가입할 때 사용한 계정으로 최고 관리자 권한을 가지고 있으며, 사용자 계정은 계정마다 역할 및 업무에 따라 권한을 부여하여 사용할 수 있다.

관리자 계정은 클라우드 인프라 내 모든 리소스에 대해 권한을 가지고 있기 때문에, 인증 정보를 공유하여 공용으로 사용하지 않고 최소한으로만 사용하여야 한다. 따라서 클라우드 관리 콘솔에 접속이 필요한 사용자를 식별하고, 각 사용자에게 개별 계정을 발급하고 관리하여야 한다.

· 사용자 계정 생성 방법

사용자 계정은 관리자 계정으로 로그인하고 사용자 계정 관련 메뉴에 접속하여 사용자 계정을 생성하고 관리할 수 있다.

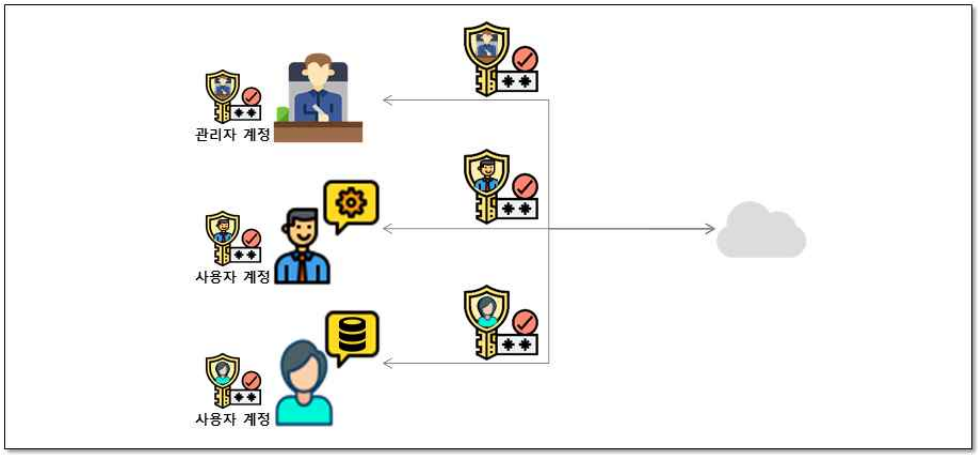
<그림 3-2> 사용자 계정 추가 화면



① 클라우드 관리자 콘솔에 관리자 계정으로 로그인
② 서비스 검색창에 사용자 계정 관련 서비스명("IAM", "Sub Account" 등) 검색 및 이동
③ 사용자 추가

* 클라우드 서비스에 따라 설정 방법이 다를 수 있음

<그림 3-3> 관리자, 사용자 계정 분리



2 계정 권한 관리

클라우드 관리 콘솔에 접속하는 사용자마다 개별 사용자 계정을 생성하였지만, 모든 사용자 계정에 관리자 권한을 부여한 사례도 확인하였다.

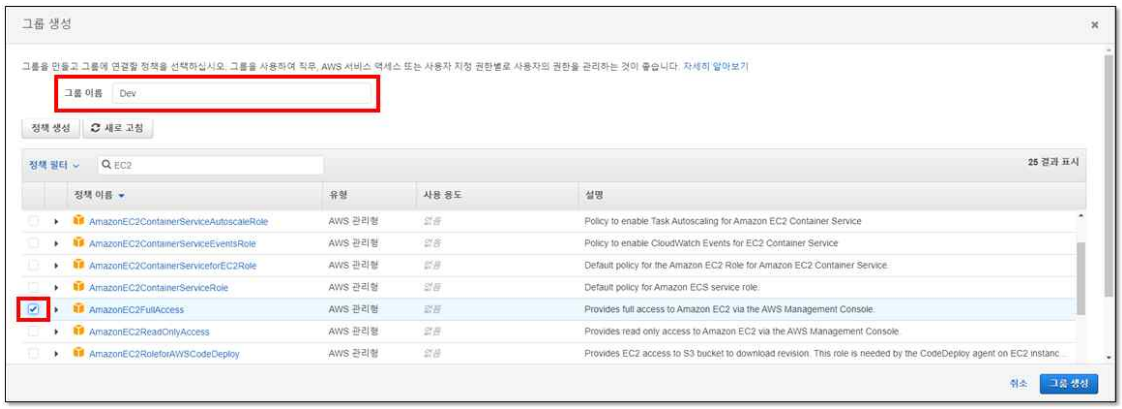
클라우드 관리 콘솔의 사용자 계정에는 계정마다 역할 및 권한을 부여할 수 있다. 사용자의 직무(개발, 운영 등)에 따라 필요한 최소한의 권한만을 부여해야 한다.

<그림 3-4> 사용자 계정에 권한 부여

사용자 계정에 과도한 권한 부여 사용자 계정에 직무관련 권한 부여

· 사용자 계정 역할 및 권한 부여 방법

<그림 3-5> 사용자 계정 권한 추가 및 정책 설정 화면

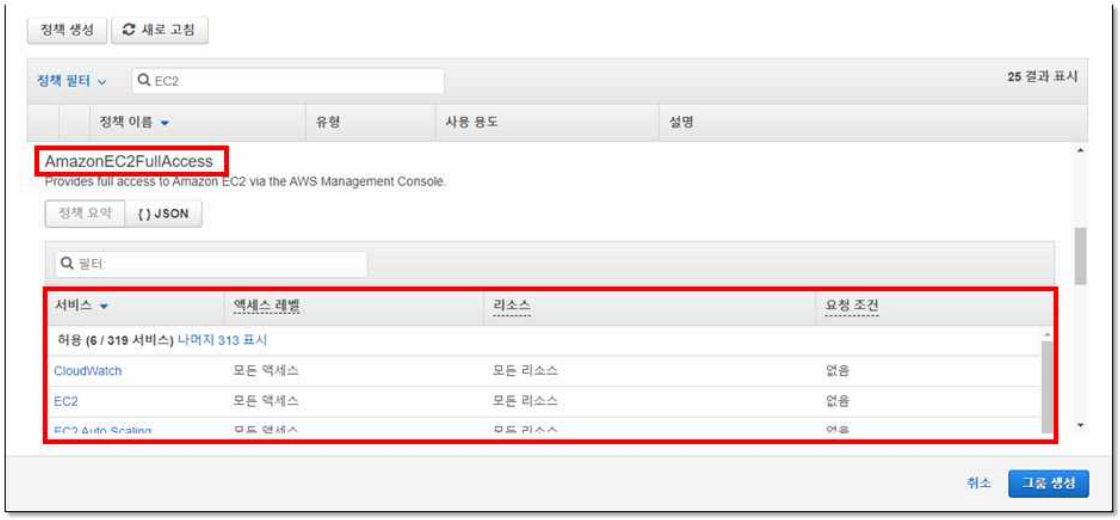


① 클라우드 관리자 콘솔 로그인
② 사용자 계정 권한 설정 페이지로 이동
③ 권한 그룹 생성 및 그룹에 사용자 추가
④ 정책 추가

* 클라우드 서비스에 따라 설정 방법이 다를 수 있음

클라우드 서비스에는 미리 정의된 다양한 정책이 존재하며, 각 정책에는 여러 권한이 포함되어있다. 미리 정의되어있는 정책 이외에 기업에서 필요한 세밀한 정책이 필요한 경우 [정책 생성] 버튼을 통해 수동으로 정책을 생성할 수 있다.

<그림 3-6> 정책 세부정보 확인 화면

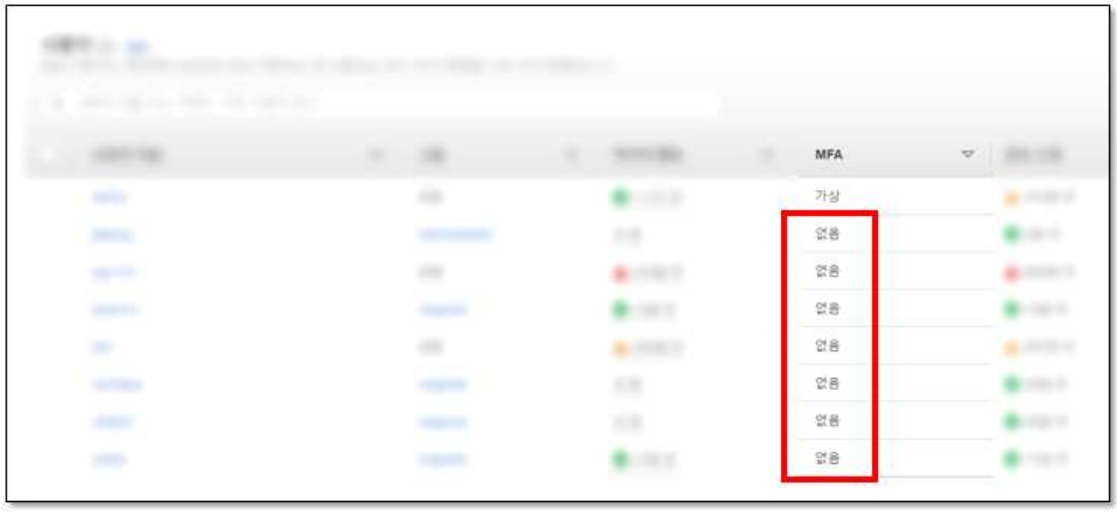


검토 페이지에서 설정된 세부 정보 및 권한 요약 사항 검토 후 사용자 만들기 버튼을 통해 사용자 계정 분리 및 최소 권한 부여가 가능하다.

3 강화된 인증 절차

다수의 기업에서 클라우드 관리 콘솔 로그인 시, 아이디, 패스워드로만 인증하는 것을 확인하였다.

<그림 3-7> 사용자 계정 MFA 적용 미흡 사례



강화된 인증 절차(MFA*)를 적용하면 아이디, 패스워드를 통한 인증뿐만 아니라 인증 절차가 추가되기 때문에 계정 정보 유출로 인한 피해를 예방할 수 있다.

* MFA(Multi Factor Authentication) : 다중 보안 인증기능

· **MFA 설정 방법**

사용자 계정으로 클라우드 관리 콘솔에 로그인 후 계정 설정에서 MFA를 설정할 수 있다.

<그림 3-8> 사용자 계정 MFA 설정 화면

① 클라우드 관리자 콘솔 로그인
② 계정 > 보안 자격 증명 관련 페이지로 이동
③ 멀티 팩터 인증(MFA) 메뉴에서 적용 가능한 MFA 방법(MFA 디바이스 관리) 선택

* 클라우드 서비스에 따라 설정 방법이 다를 수 있음

위와 같이 사용자 계정에서 MFA를 설정하는 방법도 있지만, IAM 정책을 통해 MFA를 강제화하도록 설정할 수도 있다.

4. 서버 보안

온라인으로 서비스를 제공하는 서버가 취약한 경우, 랜섬웨어에 감염되어 서비스 제공 불가로 손실이 발생하거나 서비스 메인 페이지를 변경하는 디페이스 공격으로 회사 브랜드 가치가 실추되는 등 다양한 피해가 발생할 수 있다. 서버 취약점은 다양한 피해와 직결될 수 있으므로 서버 보안 관리에 주의를 기울여야한다.

<그림 4-1> 디페이스 피해 예시

서비스의 정상적인 운영을 위해서는 웹페이지, 어플리케이션 자체에 대한 보안이나, 3rd party 보안도 중요하지만, 비대면 서비스 개발·운영 환경 취약점 점검에서는 서비스 운영을 위한 서버 보안에 집중하여 점검을 진행하였다.

서버 보안 분야에서는 계정, 세션, 권한, 로그 관리 등의 항목을 점검하였다. 점검 결과 안전한 인증 및 세션관리 미흡(97.8%), 관리자 계정 최소 사용 및 권한 검토 미흡(85.7%) 등의 취약 사례가 다수 기업에서 확인되었다.

* 주요 취약 사례 및 대응 방안은 다수의 기업에서 사용 중인 CentOS를 예시로 작성하였다.

1 서버 접속 계정 관리

계정 관리 항목에서 다수의 사용자가 계정을 공유하여 사용하거나 퇴사자의 계정이 남아 있는 등 여러 취약 사례를 확인할 수 있었다.

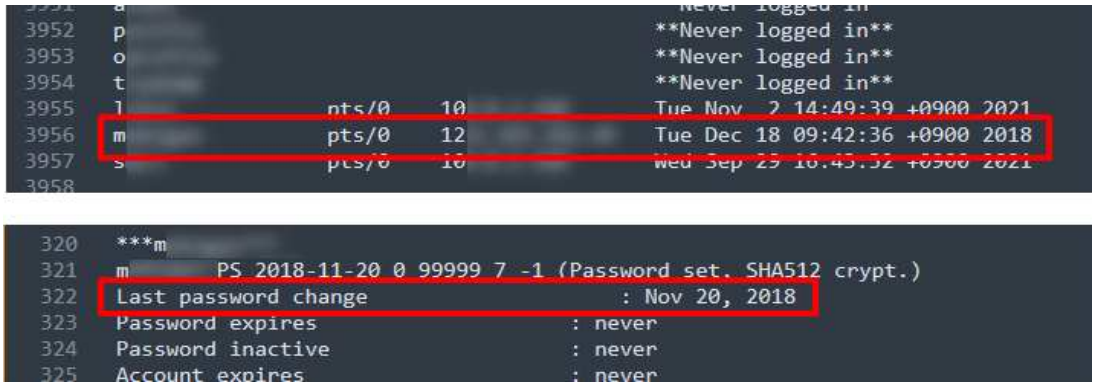
하나의 계정을 여러 명의 사용자가 공유하여 사용하면 패스워드와 같은 인증정보를 주기적으로 변경하기 어렵기 때문에 관리가 누락될 수 있으며, 퇴사자나 직무가 변경된 직원과 같이

서버 접속이 불필요한 비인가자도 서버에 접속할 수 있게 된다. 또한 계정을 공유하여 사용하면 장애나 침해사고 발생 시, 원인분석 및 책임추적성 확보가 어렵다.

서버 계정은 서버에서 운영할 주요 서비스와 관련 업무 담당자를 식별한 뒤 생성 및 관리하여야 한다. 서비스 운영을 위한 계정과 사용자가 접속하는 계정은 분리하여 발급하여야 하며, 사용자별 개별 계정을 생성하여 사용해야 한다.

또한 개별 계정을 생성하였지만, 퇴사 또는 직무변경에 대한 사용자 권한 회수가 정상적으로 이루어지지 않은 사례도 다수 확인하였다. 이 경우 불필요한 사용자 계정이 방치되어 주기적인 패스워드 변경과 같은 관리가 어렵다. 비인가자는 방치된 계정에 대한 무작위 대입 공격 후, 서버에 무단침입하거나 제어권을 탈취할 수 있다.

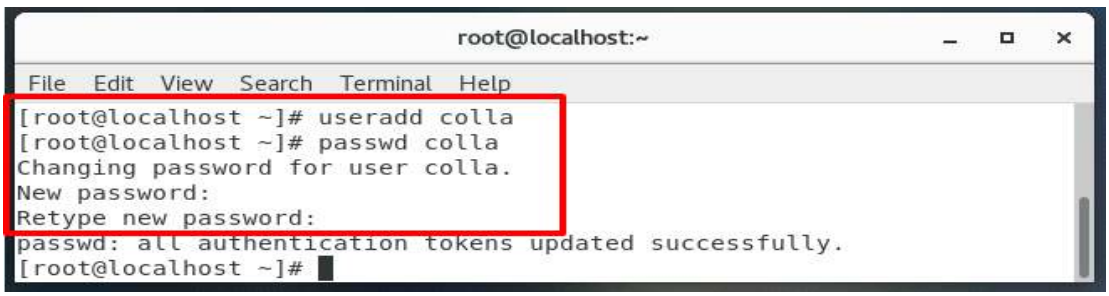
<그림 4-3> 퇴사자 계정 방치 사례



· 서버 계정 생성 방법

서버 계정은 아래 명령어를 참고하여 생성할 수 있으며, 계정에 대한 패스워드 설정을 통해 주기적으로 패스워드를 변경하도록 할 수 있다.

<그림 4-2> 서버 계정 생성 예시



useradd [계정명] : 사용자 추가 명령어
-d : 사용자의 홈 디렉터리 위치를 지정하며, 기본값은 /home
-g [그룹명] : 새로운 사용자의 그룹을 지정
-u [UserID] : 새로운 사용자의 ID 값을 지정

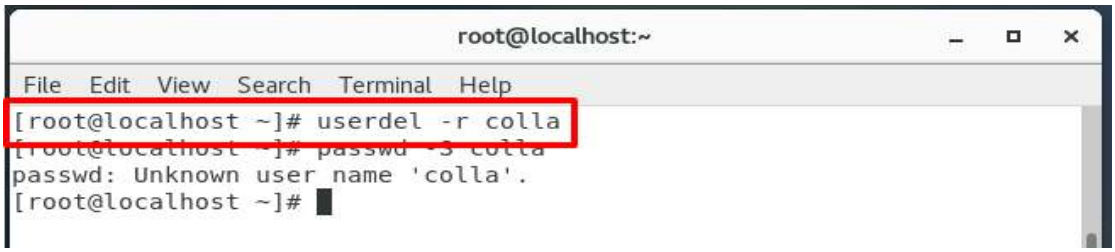
passwd [계정명] : 사용자 패스워드 설정 명령어
-d, --delete : 사용자의 패스워드를 삭제한다.
-e, --expire : 강제적으로 사용자의 패스워드를 만료시킨다.
-x, --maxdays MAX_DAYS : 패스워드 사용 최대 유효기간(MAX_DAYS) 설정
-S, --status : 사용자의 패스워드 관련 설정 정보를 출력

* 운영체제에 따라 설정 방법이 다를 수 있음

· **서버 계정 삭제 방법**

퇴사나 직무변경으로 서버 접속이 불필요한 사용자가 생기는 경우, 아래 명령어를 활용하여 계정을 삭제하는 등의 조치를 취하여 비인가자가 서버에 접속할 수 없도록 하여야 한다.

<그림 4-4> 서버 계정 삭제 예시



userdel [계정명] : 사용자 추가 명령어
-r : 사용자 ID 및 홈 디렉터리까지 함께 삭제

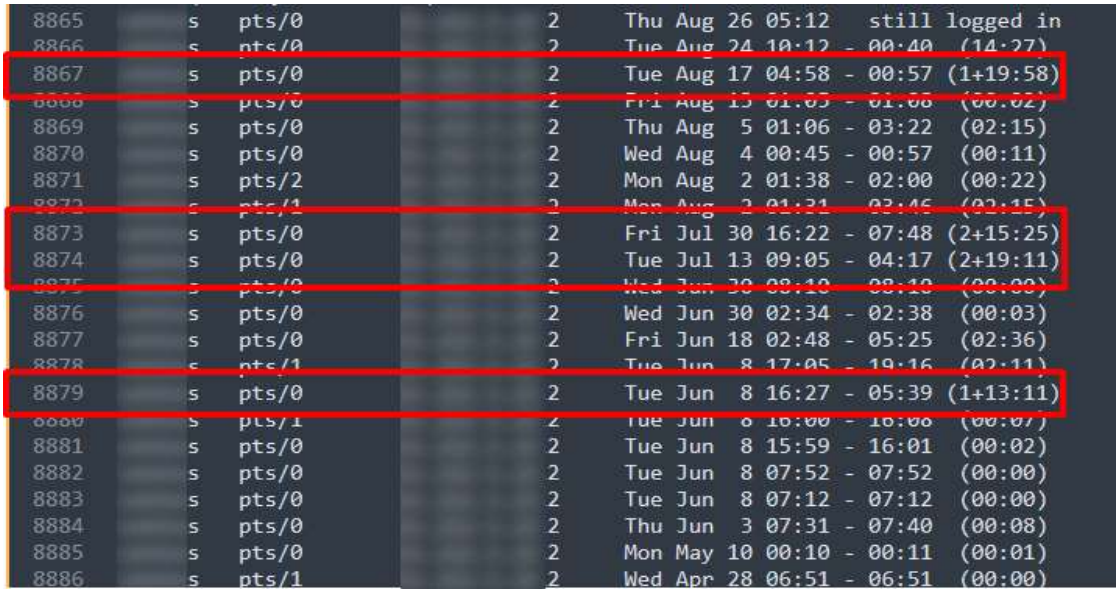
* 운영체제에 따라 설정 방법이 다를 수 있음

2 인증 및 세션 관리

서비스 개발, 테스트, 유지보수 등을 목적으로 클라우드, IDC에 위치한 서버에 접속하기 위해서는 원격 터미널 서비스 사용이 필요하다. 하지만 다수의 기업에서 세션 타임아웃을 설정하지 않는 등 보안 설정을 적용하지 않고 사용하는 것을 확인하였다.

SSH 서비스를 기본 설정 값으로 사용하는 경우, 세션 타임아웃이 무제한으로 설정되어 세션을 종료하지 않으면 세션이 끊어지지 않고 유지된다. 따라서 원격 터미널 서비스에 접속한 뒤 자리를 이석하거나 퇴근하는 등 오랜 시간 사용하지 않더라도 세션이 유지되기 때문에, 비인가자에 의한 물리적 접근 및 세션 탈취에 취약할 수 있다.

<그림 4-5> 장기간 세션 유지 사례



원격 터미널 서비스를 통한 서버 접속은 효율성을 증대시키는 만큼 공격자도 취약점을 악용해 서버에 쉽게 접속할 수 있도록 한다. 이런 공격을 방지하기 위해 원격 터미널 서비스의 보안 설정을 통해 보안을 강화하고 사용하여야 한다.

· SSH 서비스 보안 설정 방법

일반적으로 원격 터미널 서비스의 보안 강화를 위해서 아래와 같이 SSH 설정파일 (/etc/ssh/sshd_config)*을 활용한다.

* 운영체제에 따라서 설정파일 위치가 다를 수 있음

<그림 4-6> /etc/ssh/sshd_config 설정

```
15 # semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
16
17 Port 30223
18 #AddressFamily any
19 #ListenAddress 0.0.0.0
20 #ListenAddress ::
21
22 HostKey /etc/ssh/ssh_host_rsa_key
23 #HostKey /etc/ssh/ssh_host_dsa_key
24 HostKey /etc/ssh/ssh_host_ecdsa_key
25 HostKey /etc/ssh/ssh_host_ed25519_key
26
27 # Ciphers and keying
28 #RekeyLimit default none
29
30 # Logging
31 #SyslogFacility AUTH
32 SyslogFacility AUTHPRIV
33 #LogLevel INFO
34
35 # Authentication:
36
37 #LoginGraceTime 2m
38 PermitRootLogin no
39 #StrictModes yes
40 MaxAuthTries 3
41 #MaxSessions 10
42 #PubkeyAuthentication yes
```

```
109 #PermitUserEnvironment no
110 #Compression delayed
111 ClientAliveInterval 600
112 ClientAliveCountMax 3
113 #ShowPatchLevel no
114 #UseDNS yes
115 #PidFile /var/run/sshd.pid
116 #MaxStartups 10:30:100
117 #PermitTunnel no
118 #ChrootDirectory none
119 #VersionAddendum none
```

① 기본 서비스 포트인 22번의 직접 노출을 피하기 위하여 임의 포트번호로 변경 사용
② 최고 권한계정인 root 계정의 직접적 사용을 제한하기 위한 원격 로그인 차단
③ 비인가자의 무작위 대입 공격을 대비하여 로그인 인증 실패 시 시도 제한 횟수 설정
④ 원격 접속 사용자가 자리 이석 시 장시간 세션 대기 상태 유지로 인한 외부 위협을 방지하기 위한 세션타임아웃 설정
- ClientAliveInterval 600 // 클라이언트의 연결 확인 간격 시간(초)
- ClientAliveCountMax 3 // 클라이언트의 응답 부재 시 확인 횟수(회)

※ ClientAliveInterval(600초) X ClientAliveCountMax(3회) = 30분

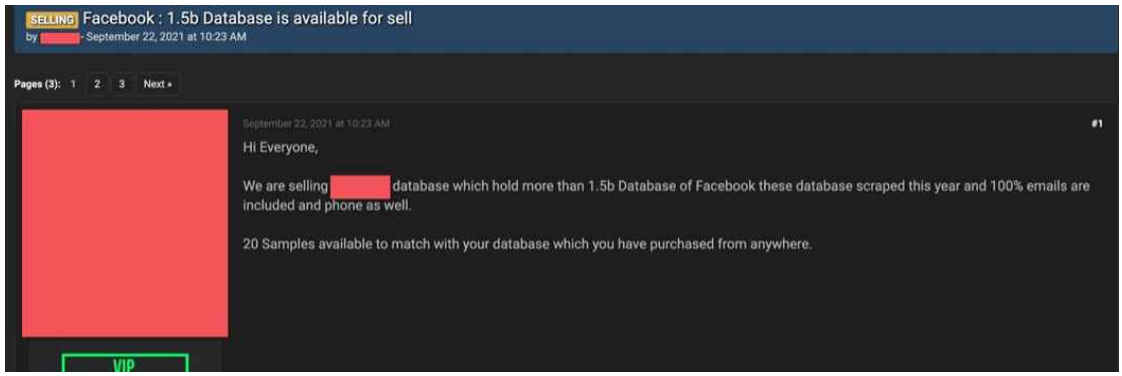
* 운영체제에 따라 설정 방법이 다를 수 있음

5. 데이터베이스 보안

데이터베이스는 온라인 서비스를 제공하기 위한 필수 구성요소 중 하나로, 수집하거나 생성한 데이터를 효율적으로 관리 및 저장하기 위해 사용한다. 주로 판매 상품이나 서비스 정보, 결제 정보를 관리하거나 이름, 연락처와 같은 이용자 개인정보 등을 관리하는 용도로 사용한다.

이용자의 개인정보가 유출되면 보이스 피싱과 같은 2차 피해나 개인 사생활 노출 등의 피해가 발생 할 수 있으므로 데이터베이스 보안은 다른 분야보다 특히 더 중요하다. 또한 개인정보를 취급하는 경우, 법적 요구사항을 준수하여야 하므로 관련 법령의 개정 및 동향도 주기적으로 확인하여야 한다.

<그림 5-1> 유출된 데이터베이스 판매 사례



데이터베이스 분야에서는 계정 관리, 접근제어, 백업, 로그 관리 등을 점검하였다. 점검 결과 로그 관리 미흡(92.2%), 계정 관리 미흡(68.9%) 등의 취약 사례가 다수의 기업에서 확인되었다.

* 주요 취약 사례 및 대응 방안은 다수의 기업에서 사용 중인 MySQL을 예시로 작성하였다.

1 데이터베이스 로그 기록 및 감사

다수의 기업에서 데이터베이스 로그가 서버 자원을 많이 사용하여 서비스에 영향을 미칠 수 있다는 이유로 로그 기능을 OFF 하거나, 로그 보관 비용 문제로 로그를 별도 보관하지 않는 사례가 확인되었다.

<그림 5-2> 데이터베이스 로깅 설정 미흡 사례

```
mysql> show variables like '%log';
+---------------------------------+-------+
| Variable_name                   | Value |
+---------------------------------+-------+
| back_log                        | 80    |
| general_log                     | OFF   |
| innodb_api_enable_binlog        | OFF   |
| innodb_locks_unsafe_for_binlog  | OFF   |
| log_statements_unsafe_for_binlog | ON    |
| log_syslog                      | OFF   |
| relay_log                       |       |
| slow_query_log                  | OFF   |
| sync_binlog                     | 1     |
| sync_relay_log                  | 10000 |
+---------------------------------+-------+
10 rows in set (0.01 sec)
```

데이터베이스 로그는 데이터베이스에 접속하거나 실행된 쿼리 등을 기록하여, 추후 책임 추적을 가능하게 하는 중요한 역할을 한다. 데이터베이스 로그를 남기지 않는다면, 데이터 삭제 등의 비정상적인 동작에 대한 원인 분석이 어려우며, 데이터가 유출되었을 때 접근 경로 등을 분석하기 어렵다. 이처럼 침해사고와 장애에 대한 정확한 원인 분석을 위해 데이터베이스 로그 기록은 서비스 운영에 필수적으로 요구된다.

데이터베이스 로그는 Error Log, General Log, Slow Query Log, Audit Log 등이 존재하며, 가장 많이 사용되는 General Log와 Slow Query Log의 설정 방법은 아래와 같다.

· General Log 설정 방법

General Log는 데이터베이스에 클라이언트가 접속하거나 수행된 SQL Query 등 데이터베이스 전반적인 사항에 대한 기록이다.

데이터베이스 설정파일(/etc/my.cnf)*에서 아래와 같이 로그 기록 기능을 활성화하고 서비스를 재시작하면 General Log 기록을 남길 수 있다.

* 데이터베이스 설치 환경에 따라서 설정파일 위치가 다를 수 있음

<그림 5-3> General Log 설정 방법

```
[root@localhost mysql]# vi /etc/my.cnf
#log_output = 'TABLE' or 'FILE' or 'TABLE,FILE'
log_output='TABLE'

#general_log
general_log=1
#general_log_file=[dir]
[root@localhost mysql]# service mysqld restart
```

log_output='TABLE'
- log 기록 형태 TABLE 형태로 지정한다.
  * TABLE 형태, FILE 형태, 혹은 TABLE,FILE 형태 모두 설정 가능하다.

general_log = 1;
- general log 기록 기능을 활성화 한다.

* 데이터베이스에 따라 설정 방법이 다를 수 있음

General Log가 설정되었는지는 아래와 같이 확인할 수 있다.

<그림 5-4> General Log 설정 확인 및 Log 예

```
mysql> show variables where Variable_name in ('version','general_log','general_log_file');
+------------------+-------------------------------+
| Variable_name    | Value                         |
+------------------+-------------------------------+
| general_log      | ON                            |
| general_log_file | /var/lib/mysql/localhost.log  |
| version          | 5.7.37                        |
+------------------+-------------------------------+
3 rows in set (0.00 sec)
mysql> select * from general_log;
+----------------------------+----------------------------+-----------+-----------+--------------+-------------------
| event_time                 | user_host                  | thread_id | server_id | command_type | argument
+----------------------------+----------------------------+-----------+-----------+--------------+-------------------
| 2022-04-18 21:35:46.846396 | root[root] @ localhost [] |         6 |         0 | Query        | set global log_out
| 2022-04-18 21:36:00.526570 | root[root] @ localhost [] |         6 |         0 | Query        | set global general_
| 2022-04-18 21:36:26.854882 | root[root] @ localhost [] |         6 |         0 | Query        | show variables whe
| 2022-04-18 21:37:22.735004 | root[root] @ localhost [] |         6 |         0 | Query        | select * from gene
| 2022-04-18 22:06:27.990474 | root[root] @ localhost [] |         6 |         0 | Query        | set global slow_qu
```

· Slow Query Log 설정 방법

Slow Query Log는 일정 시간 내에 수행되지 못한 쿼리에 대한 기록이다. 예를 들어 서비스를 테스트 및 운영하면서 일반적으로 쿼리가 3초 이내에 수행되는 경우, 3초 이상 소요되는 일반적이지 않은 쿼리에 대해서 기록할 수 있다.

데이터베이스 설정파일(/etc/my.cnf)*에서 아래와 같이 로그 기록 기능을 활성화하고 서비스를 재시작하면 Slow Query Log를 남길 수 있다. long_query_time은 임계 시간을 설정할 수 있는 값으로, 운영 환경의 프로세서, 메모리 사양 등에 따라 편차가 존재할 수 있으므로 평균 소요시간 등을 테스트하고 임계치를 설정하여야 한다.

* 데이터베이스 설치 환경에 따라서 설정파일 위치가 다를 수 있음

<그림 5-5> Slow Query Log 설정 방법

```
[root@localhost mysql]# vi /etc/my.cnf
#slow_query_log
slow_query_log=1
long_query_time=3
[root@localhost mysql]# service mysqld restart
```

slow_query_log = 1;
- slow query log 기록 기능을 활성화 한다.

long_query_time = 3;
- slow query log 기록 임계 시간을 설정한다.

* 데이터베이스에 따라 설정 방법이 다를 수 있음

Slow Query Log가 설정되었는지는 아래와 같이 확인할 수 있다.

<그림 5-6> Slow Query Log 설정 확인 및 Log 예

```
mysql> select * from slow_log;
+----------------------------+----------------------------+----------------+----------------+-----------+------
| start_time                 | user_host                  | query_time     | lock_time      | rows_sent | rows_
+----------------------------+----------------------------+----------------+----------------+-----------+------
| 2022-04-18 23:19:14.572325 | root[root] @ localhost [] | 00:00:25.854583 | 00:00:00.004902 |        86 |
+----------------------------+----------------------------+----------------+----------------+-----------+------
1 row in set (0.00 sec)
```

로그는 일정 기간동안 누적 보관이 필요하기 때문에 저장소 공간이 많이 필요할 수 있다. 따라서 설정 초기에는 주기적으로 저장소 상태를 확인하여, 백업 계획을 수립하고 이행하여야 한다.

2 데이터베이스 계정 관리

취약점 점검 결과, 서비스용 계정과 DBA가 사용하는 계정이 동일하거나 테스트용 임시 계정, 퇴사자 계정 등 미사용 계정이 방치된 사례도 확인되었다. 서비스, DBA가 동일한 계정을 사용하는 경우 장애 등의 원인 분석이 어려울 수 있으며, 다수의 사용자가 공용 계정을 사용하면 패스워드를 공유하게 되어 인증정보 유출 등의 위협이 증가하게 된다.

<그림 5-7> 데이터베이스 계정 접근제어 미흡 사례

```
mysql> select Host, User, authentication_string from user;
+-----------+---------------+------
| Host      | User          | authe
+-----------+---------------+------
| localhost | root          | *9547
| localhost | mysql.session | *THIS
| localhost | mysql.sys     | *THIS
| %         | dba           | *299C
+-----------+---------------+------
4 rows in set (0.00 sec)
```

따라서 공용 계정을 사용하지 않도록 접속이 필요한 사용자들은 개별 계정을 사용하도록 하고, 미사용 계정은 즉시 삭제할 수 있도록 계정을 관리해야 한다.

· 데이터베이스 사용자 계정 추가 방법

아래의 명령어를 통해 사용자 개별 계정 발급이 가능하며, 계정 정보 유출 시 비인가자의 접근을 차단하기 위하여 접근 가능 IP를 계정별로 지정할 수 있다.

<그림 5-8> 데이터베이스 사용자 추가

```
mysql> create user 'jack'@'192.168.32.129' identified by 'NewAccount57!@';
Query OK, 0 rows affected (0.00 sec)

mysql> select Host, User from user;
+----------------+---------------+
| Host           | User          |
+----------------+---------------+
| %              | dba           |
| %              | dev           |
| %              | vuln          |
| 192.168.32.129 | jack          |
| localhost      | mysql.session |
| localhost      | mysql.sys     |
| localhost      | root          |
+----------------+---------------+
7 rows in set (0.00 sec)
```

create user '[사용자 계정]'@'[허용IP]' identified by '[계정 패스워드]';
(예) create user 'jack'@'%' identified by 'NewAccount57!@';
(예) create user 'jack'@'192.168.32.129' identified by 'NewAccount57!@';

* 데이터베이스에 따라 설정 방법이 다를 수 있음

사용자 계정에 허용 IP를 지정하는 경우, 데이터베이스 접속 시 IP를 확인하고 접근을 허용하므로 주요 업무 장소인 사무실 IP 등으로 지정하여 계정 보안을 강화할 수 있다.

<그림 5-9> host 지정 계정의 데이터베이스 접근 시도 실패, 성공 로그기록

```
| 2022-04-19 00:28:42.809794 | [jack] @ localhost []              |      19 |        0 | Connect
jack@localhost on  using Socket
| 2022-04-19 00:28:42.809883 | [jack] @ localhost []              |      19 |        0 | Connect
Access denied for user 'jack'@'localhost' (using password: YES)
| 2022-04-19 00:28:59.302814 | [jack] @  [192.168.32.129]         |      20 |        0 | Connect
jack@192.168.32.129 on  using SSL/TLS
```

· 데이터베이스 사용자 계정 삭제 방법

먼저 불필요한 계정이 있는지 확인하기 위해서, 데이터베이스 사용자 계정 목록을 조회하여, 사용자 계정을 식별한다.

<그림 5-10> 데이터베이스 사용자 계정 목록 확인

```
mysql> select Host, User from user;
+-----------+---------------+
| Host      | User          |
+-----------+---------------+
| %         | dba           |
| %         | dev           |
| %         | gildong       |
| %         | vuln          |
| localhost | mysql.session |
| localhost | mysql.sys     |
| localhost | root          |
+-----------+---------------+
7 rows in set (0.00 sec)
```

select host, user, authentication_string from user;

* 데이터베이스에 따라 설정 방법이 다를 수 있음

확인한 사용자 계정 목록 중 미사용 계정이 접속이 가능한 상태로 방치되어있는 경우 비인가자의 접속으로 인한 데이터 유출 및 피해가 발생할 수 있으므로 아래와 같이 미사용 계정을 삭제하여 접근권한을 회수하여야 한다.

<그림 5-11> 데이터베이스 사용자 삭제

```
mysql> drop user gildong@'%';
Query OK, 0 rows affected (0.00 sec)

mysql> select Host, User from user;
+-----------+------------------+
| Host      | User             |
+-----------+------------------+
| %         | dba              |
| %         | dev              |
| %         | vuln             |
| localhost | mysql.session    |
| localhost | mysql.sys        |
| localhost | root             |
+-----------+------------------+
6 rows in set (0.00 sec)
```

```
drop user gildong@'%;
```

* 데이터베이스에 따라 설정 방법이 다를 수 있음

추가로 예기치 않은 침해사고와 장애가 발생했을 때, 빠른 서비스의 정상화를 위하여 주기적으로 데이터베이스를 백업해야 한다.

6. 업무용 PC 보안

사용자의 업무에 따라 업무용으로 사용하는 PC를 통해 계약서나 고객정보, 서비스 소스코드 등의 중요 정보에 접근하거나 서비스 운영 시스템에 접속하기도 한다. 이런 중요 업무를 수행하는 PC의 경우, 개인 용도로 사용하는 PC보다 더 높은 수준의 보안 관리가 필요하다.

특히 최근에는 원격근무가 증가하며, 사무실 이외에도 카페, 공유 오피스, 집 등 공간의 제약 없이 근무하거나, 이동이 편리한 노트북을 업무용으로 사용하는 기업들이 증가하고 있다. 이렇게 공공장소를 포함하여 외부에서 업무를 수행하게 되는 경우, 업무용 PC의 분실과 비인가자의 접근 등의 보안 위협에 노출될 수 있기 때문에 사용자의 주의가 필요하다.

업무용 PC 분야에서는 인증 관리, 서비스 관리, 보안 업데이트 및 악성코드 탐지 활동 등을 점검하였다. 점검 결과 인증 관리 미흡(87%) 사례가 다수 기업에서 확인되었다.

1 패스워드 관리

다수의 기업에서 업무용 PC의 패스워드를 장기간 변경하지 않은 사례가 많이 확인되었다. 패스워드의 장기 미변경은 원격데스크톱(RDP), 공유폴더 등 원격 연결 또는 OS 권한 탈취를 위한 무차별 대입공격에 노출될 수 있다. 심지어 일부 사용자는 업무용 PC를 패스워드와 같은 별도의 인증 절차 없이 사용하여, 비인가자도 업무용 PC에 접근이 가능한 상태로 사용하는 것을 확인하였다.

<그림 6-1> 업무용 PC 패스워드 미설정 사례

패스워드의 주기적 변경 설정의 경우, Windows 운영체제의 로컬 보안 정책 기능을 활용하여 적용할 수 있다. 이 기능을 활용하면 일정 기간 이후 패스워드를 변경하게 하거나, 패스워드 복잡성 만족 여부 검증을 통해 강력한 패스워드를 사용하도록 설정할 수 있다. 보안 정책 설정 방법은 아래와 같으며, 전체 사용자 계정에 대한 암호 정책 설정과 개별 사용자 계정에 대한 암호 정책 설정 두 가지 모두 적용하여야 한다.

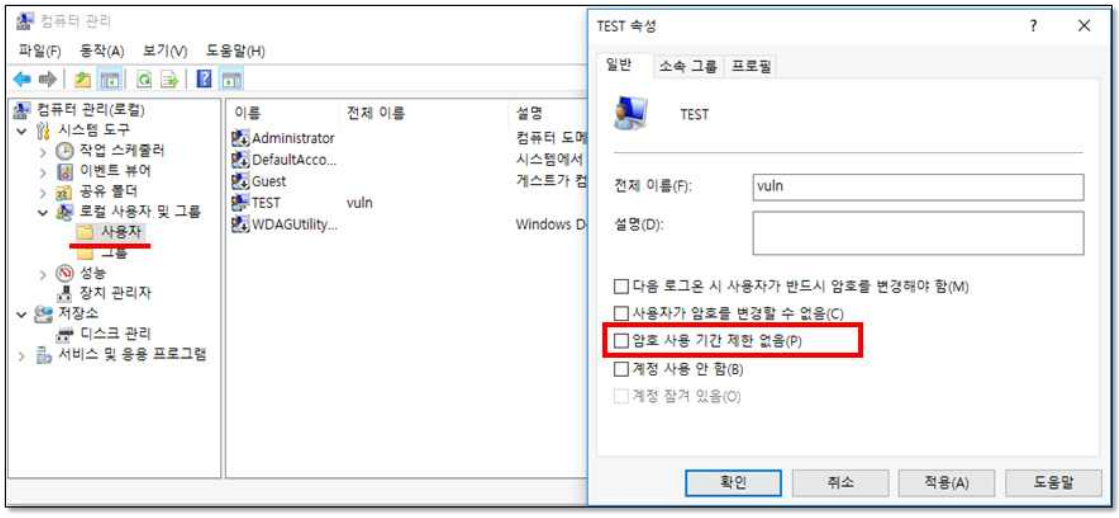
· 암호 정책 설정 방법 - 전체 사용자 계정

<그림 6-2> 암호 정책 설정 화면 – 전체 사용자 계정

① 그룹 정책 관리 콘솔* 열기
* 실행 창(Win+'R')에서 "gpedit.msc" 입력 후 열기
② 컴퓨터 구성 > Windows 설정 > 보안 설정 > 계정 정책 > 암호 정책 열기
③ 암호 정책(최대 암호 사용 기간 등) 설정하기

· 암호 정책 설정 방법 - 개별 사용자 계정

<그림 6-3> 암호 정책 설정 화면 – 개별 사용자 계정



① 컴퓨터 관리 콘솔* 열기
* 실행 창(Win+'R')에서 "compmgmt.msc" 열기
② 시스템 도구 > 로컬 사용자 및 그룹 > 사용자 열기
③ 계정 선택 및 속성 열기
④ '암호 사용 기간 제한 없음' 체크 해제

2 불필요 서비스 관리

또한 업무용 PC에서 업무 목적 이외의 메신저, 원격제어, 파일공유 서비스 등의 불필요한 서비스를 사용하는 사례를 다수 확인하였다. 특히 서비스를 개발·운영하거나 혹은 중요 자료를 취급하는 PC의 경우, 정보유출 및 악성코드 감염으로 인한 피해가 크기 때문에 더욱 주의가 필요하다.

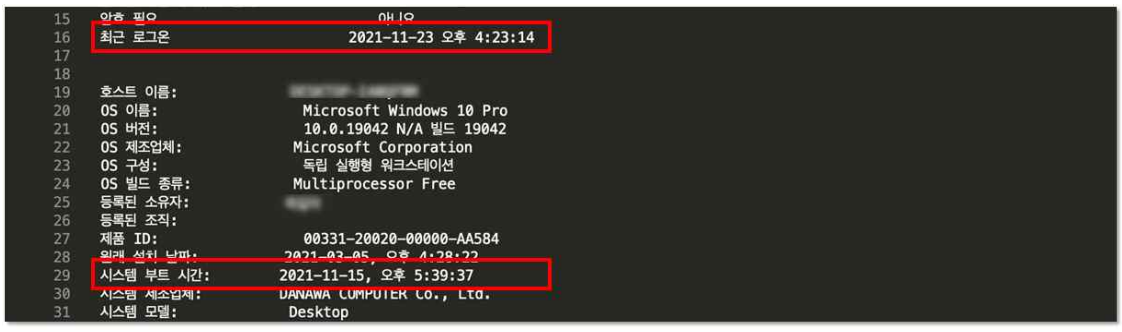
<그림 6-4> 업무 목적 외 불필요 서비스 사용 사례

3 업무용 PC 관리

점검 항목 이외에도 업무용 PC 관리가 미흡한 사례가 확인되었다. 업무용 PC를 장기간 종료하지 않고 사용하는 사례가 있었는데, 이 경우 취약점에 대한 보안패치를 포함한 업데이트가 정상적으로 이루어지지 않게 된다.

또한, 업무용 PC를 사용하거나 관리하는 사람이 없는 업무 시간 이후에도 켜진 상태로 방치하는 경우, 해당 PC의 취약점을 악용한 공격이 발생할 수 있다. 공격당한 업무용 PC를 통해 사내 네트워크에 침투하는 경우, 다른 업무용 PC 혹은 파일서버까지 악성코드에 감염될 수 있다. 특히 시스템 관리자의 업무용 PC인 경우, 인증서 탈취, 주요 시스템 접속 권한 탈취로 전체 인프라에 대한 위협이 발생할 수 있다.

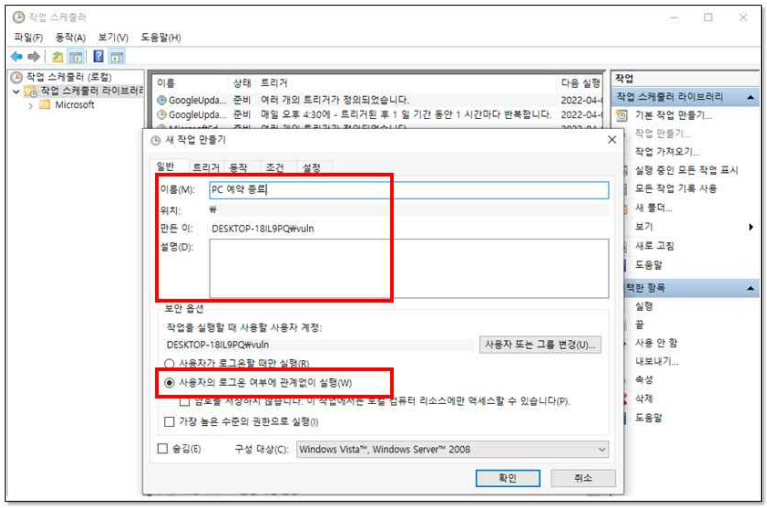
<그림 6-5> 업무용 PC 장기 미종료 사용 사례



업무용 PC가 켜진 상태로 방치되지 않도록 Windows 운영체제에서 기본으로 제공하는 기능을 활용하여 자동 종료되도록 설정할 수 있다.

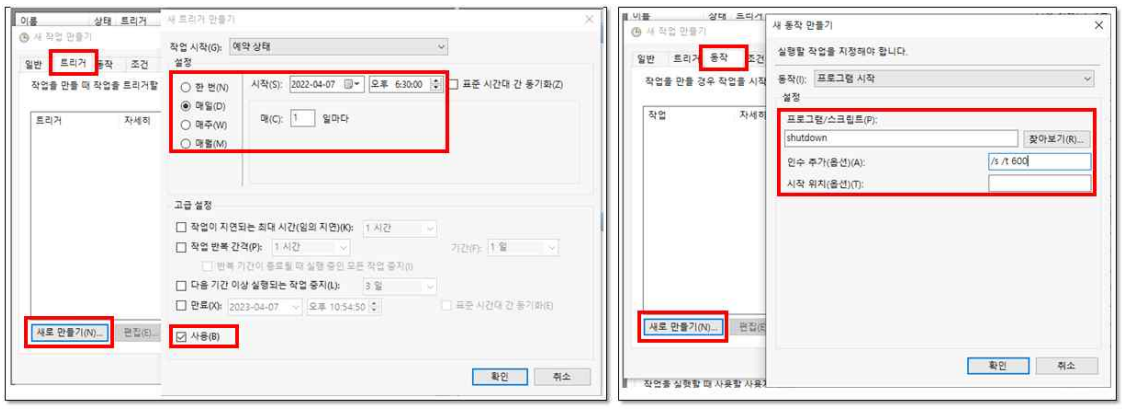
· PC 예약 종료 작업 스케줄러 생성 방법

<그림 6-6> PC 예약 종료 작업 스케줄러 생성 화면(1)



① 작업 스케줄러* 열기
  * 실행 창(Win+'R')에서 "taskschd.msc" 열기
② 작업 스케줄러 라이브러리에서 작업 만들기
③ 작업의 일반 정보 입력 및 '사용자의 로그온 여부와 관계없이 실행' 옵션 선택

<그림 6-7> PC 예약 종료 작업 스케줄러 생성 화면(2)



④ 트리거 탭에서 새 트리거 만들기
⑤ 작업 시작 시간 설정 및 하단의 '사용' 체크
⑥ 동작 탭에서 새 동작 만들기
⑦ 동작할 프로그램/스크립트 및 인수 등 입력

잔업 등으로 인해 늦은 시간 PC 사용 중 자동 종료로 인해 작업 내용이 손실 될 수 있으므로 PC 미사용 시간을 고려하여 지정하여야 한다.

이외에도, 보안 프로그램 실행, 불필요한 파일 삭제 등 업무용 PC에 대한 주기적인 작업이 필요한 경우 작업 스케줄러를 활용하여 효율적으로 관리할 수 있다.

제3장
시사점

Ⅲ. 시사점

본 매뉴얼의 보안 취약 사례는 지난해 한국인터넷진흥원에서 비대면 서비스를 개발·운영하는 기업을 대상으로 진행한 보안 취약점 점검 결과를 기반으로 작성하였으며, 최소한의 보안 조치사항을 포함하고 있다.

디지털 전환 시대를 맞이하여 매년 새로운 보안 위협과 사이버 공격이 발생하고 있으며, 기업 내에서도 신규 자산 도입 및 네트워크 구성 변경 등 환경 변화에 따른 보안 위협도 발생하고 있다. 이에 각 기업에서는 본 매뉴얼을 참고하는 것 이외에도 시스템 운영 환경과 보안 관리 수준을 면밀히 살펴보고 보안 취약점을 점검하고 조치하는 것이 필요하다.

기업에서 보유한 서버, 데이터베이스 등 중요 자산을 식별하고 위협 요소를 분석 한 뒤, 위협 요소를 해결하기 위한 대응방안을 강구하는 활동을 지속적으로 반복하며 위험 관리하여야 한다. 특히, 식별 및 관리되지 않아 방치된 자산은 취약점 공격 및 해킹 공격의 주요 접점이 될 수 있다.

지속적인 위험 관리를 위해서는 보안 전담 인력 및 예산 투자가 이루어져야 하나 중소·영세 기업에서는 단기간 내에 추진하기 어렵기 때문에 중장기 계획을 수립할 필요가 있다. 다만, 취약 사례 중 일부는 단기간 조치할 수 있는 항목도 존재하므로 보안에 조금만 관심을 가져도 대응이 가능하다.

보안 사고로 인하여 이용자 정보유출로 기업 이미지의 심각한 피해가 발생하거나, 랜섬웨어와 같은 악성코드 감염으로 서비스가 중단되는 등 여러 리스크가 있으므로 보안을 고려한 경영 관리가 필요하다.

이제는 보안은 선택이 아닌 필수 사항임을 인식하여야 한다.