DEFENDER SUMMIT

모의 해커가 바라보는 Attack Surface

2025.05.27
발표: 양정규

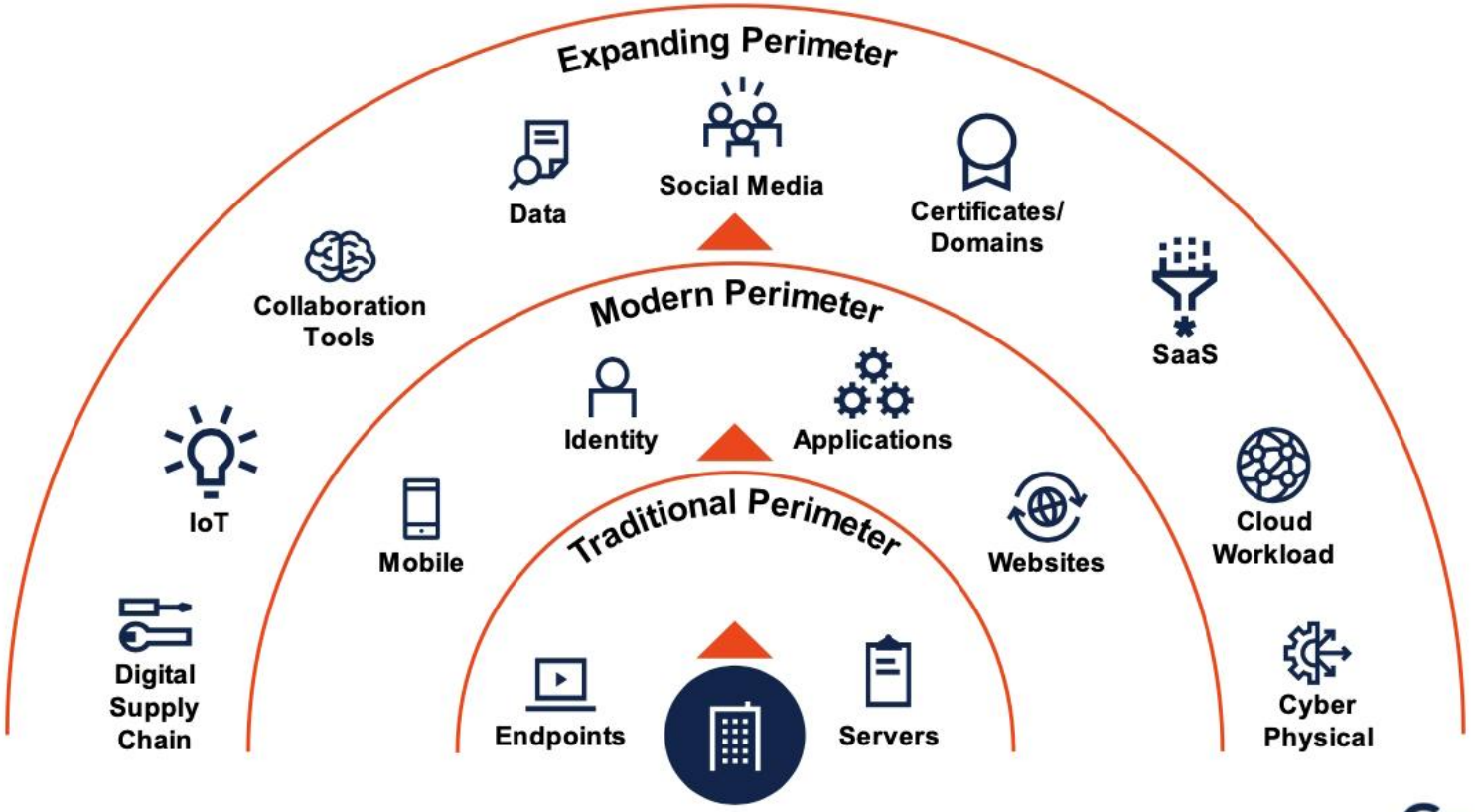
RAON SECURITY

I. Attack Surface

- 1. Attack Surface 개념
- 2. 최근 취약점 동향
- 3. 최근 공격 사례
- 4. Attack Surface 관리 중요성

1. Attack Surface 개념

Attack Surface (공격 표면)는 공격자가 시스템, 네트워크, 애플리케이션 또는 조직에 침투하거나 데이터를 탈취하기 위해 악용할 수 있는 모든 잠재적인 진입점 (entry point)들을 의미합니다.
종류로는 크게 Digital / Physical / Social Engineering Attack Surface 등이 있습니다.



출처: https://www.microcontrollertips.com

2. 최근 취약점 동향

☑ 공급망 공격 (Supply Chain Attack) 심화

- 소트프웨어 개발/배포 과정, 또는 서비스의 취약점을 이용해 다수의 하위 조직/고객에게 악성코드를 유포
- SolarWins, Kaseya, MOVEit 등 사례

☑ 제로데이 취약점 악용 증가

- 패치 발표 이전 제로데이 취약점을 해킹 그룹이나 랜섬웨어 조직이 적극적으로 구매하거나 자체 연구/발굴하여 공격에 활용
- 웹 브라우저, 운영체제, VPN/방화벽 등 보안 솔루션, 업무용 소프트웨어 등이 제로데이의 주요 타겟

☑ 클라우드 환경 악용 증가

- 클라우드 서비스 (IaaS, PaaS, SaaS)의 잘못된 설정(예: S3 버킷 공개, 취약한 IAM 정책)이나 클라우드 플랫폼 자체 취약점을 노린 공격이 지속적으로 발생
- Containter (Docker, Kubernetes) 환경의 취약점

☑ 랜섬웨어 진화

- 서비스형 랜섬웨어 (RaaS) 모델이 보편화되면서 공격 기술이 없는 이들도 쉽게 랜섬웨어 공격 감행
- 데이터 암호화, 데이터 유출 후 공개 협박 등 다중 협박으로 피해 극대화

☑ AI 기반 공격 등장 및 고도화

- AI를 이용해 더 정교한 피싱, 딥페이크를 활용한 음성/영상 조작 등 사회 공학적 공격 고도화
- AI를 활용한 취약점 분석 및 악성코드 제작

☑ API 보안 위협 증가

- 애플리케이션 간 통신이 API 중심으로 이루어지면서, API 자체 보안 취약점 노린 공격 증가

3. 최근 공격 사례

☑ VPN 공격 사례

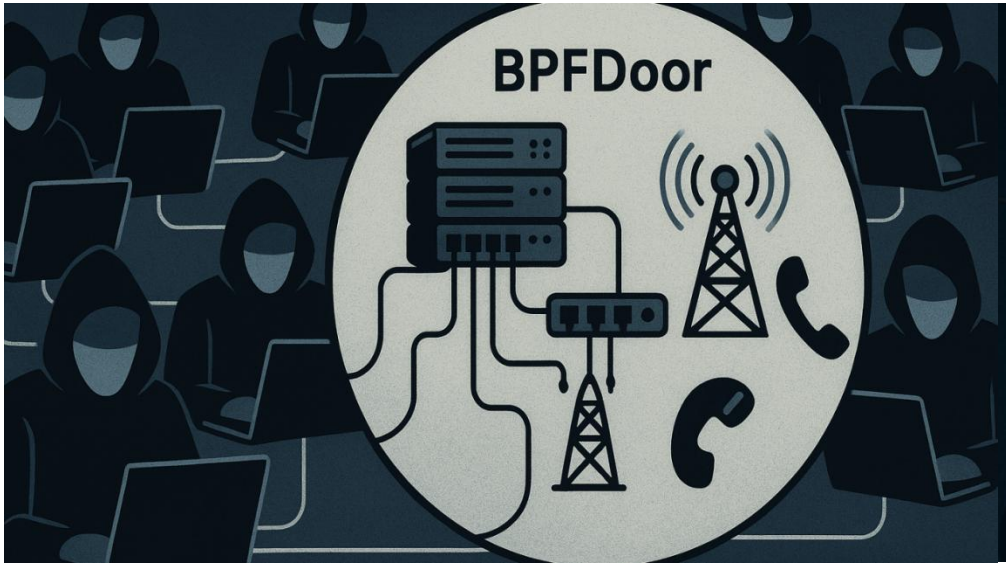
- Fortinet FortiOS SSL-VPN (CVE-2022-42475, CVE-2023-27997 등)
- Ivanti Connect Secure (CVE-2023-46805, CVE-2024-21887, CVE-2025-22457 등)
- 코로나 이후 재택 근무 증가로 VPN 사용이 증가하며 주요 공격 대상이 됨. 다수 기업, 기관에서 내부망 침투 및 데이터 유출, 랜섬웨어 감염 등에 악용됨

☑ 공급망 공격 사례

- MOVEit Transfer 대규모 데이터 유출 (CVE-2023-34362, CVE-2023-35708 등)

☑ 진화된 백도어 사례

- BPFDoor : 리눅스 백도어로 Berkeley Packet Filter 기술(커널 레벨)을 활용하여 전통적인 방화벽, IDS/IPS, 모니터링 도구로 탐지 어려움



4. Attack Surface 관리 중요성

Attack Surface를 파악해야 잠재적인 보안 위협과 취약점을 정확하게 파악하고 평가할 수 있습니다.
최근 Attack Surface가 급증하고 있어 보안 수준을 높이기 위해 Attack Surface를 관리하는 것이 매우 중요합니다.

Attack Surface의 확장

- 클라우드 솔루션 확대
- IoT 기기 증가
- OT 환경 연결성 증가
- OSINT(Open-Source INTelligence)
- Dark Web

보안 위협의 고도화/지능화

- 제로데이 취약점의 악용 증가
- 기업의 패치 속도보다 공격자의 악용 속도가 월등히 빠름
- 악성코드 은닉 기술 고도화
- 공격 기법의 지능화

원격 근무 환경 증가

- 코로나 이후 재택 근무 증가
- VPN 증가
- 갑작스러운 환경 변화에 맞는 적절한 네트워크 보안 설계 미흡
- 재택 환경이 Attack Surface로 추가

공급망 의존도 상승

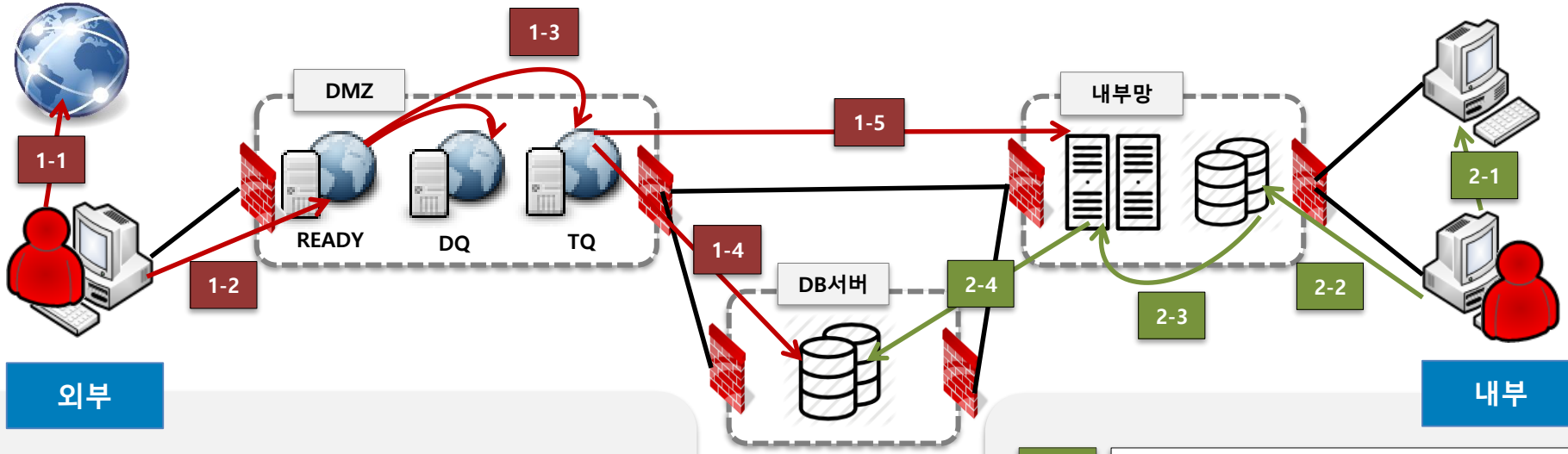
- 개발 효율성 측면
- Open Source Library 사용 증가
- Third-Party Library / Solution 사용 증가
- 높은 의존도에 비해 보안 위협 증가

II. 모의 해커 관점

- 1. 모의 해킹 Process
- 2. 외부 모의 침투
- 3. 내부 모의 침투
- 4. 중요 정보 획득
- 5. 모의 해커 관점의 Attack Surface
- 6. Real Attacker 관점의 Attack Surface

1. 모의 해킹 Process

모의 해커는 보안 강화를 위하여 실제 해커가 공격할 수 있는 외부/내부 Attack Surface를 기반으로 가상의 시나리오를 구성하고, 이를 기반으로 외부 및 내부 모의 침투를 수행합니다.



외부

1-1	• 대상수집 – 홈페이지, PTR레코드, 검색사이트
1-2	• 침투시도 – 인젝션, 파일 취약점, 매개변수 조작 등
1-3	• Lateral Movement – 시스템 취약점, 계정획득 등
1-4	• 개인정보 획득 – 인젝션, DB연결정보 활용 등
1-5	• 내부망 침투 가능성 – 구성도 파악 후 취약점 활용

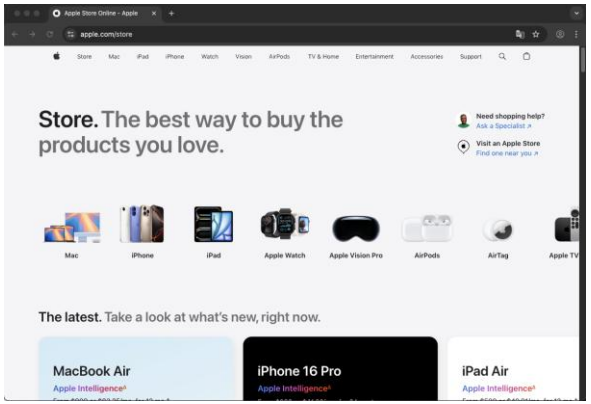
내부

2-1	• 대상수집 – 자료조사, 대역 스캔
2-2	• 침투시도 – 웹, 시스템 등 취약점
2-3	• Lateral Movement – 시스템 및 계정획득
2-4	• DB정보 – 인젝션, DB연결 정보활용 등

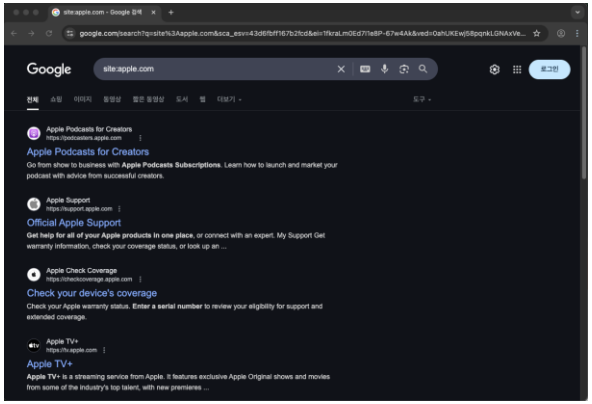
2. 외부 모의 침투 – 대상 수집

외부에서 접근 가능한 점검 대상을 확보하기 위해 포털 사이트, 검색엔진, DNS 레코드 검색을 통해 대상을 수집하고 Whois 서비스를 통해 모의 침투 대상 대역을 확인하여 점검 대상에 포함합니다.

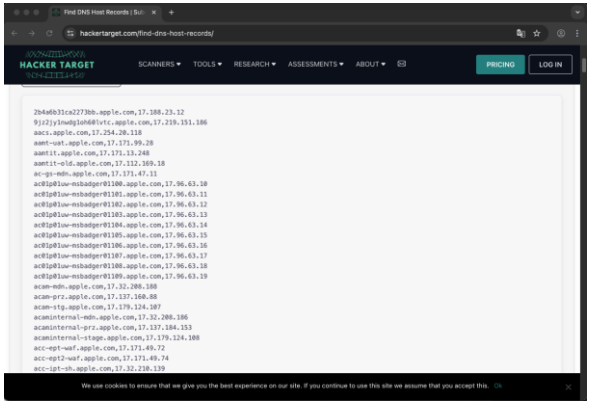
포털 홈페이지를 통한 대상 수집



검색엔진을 통한 대상 수집



DNS 레코드를 통한 대상 수집

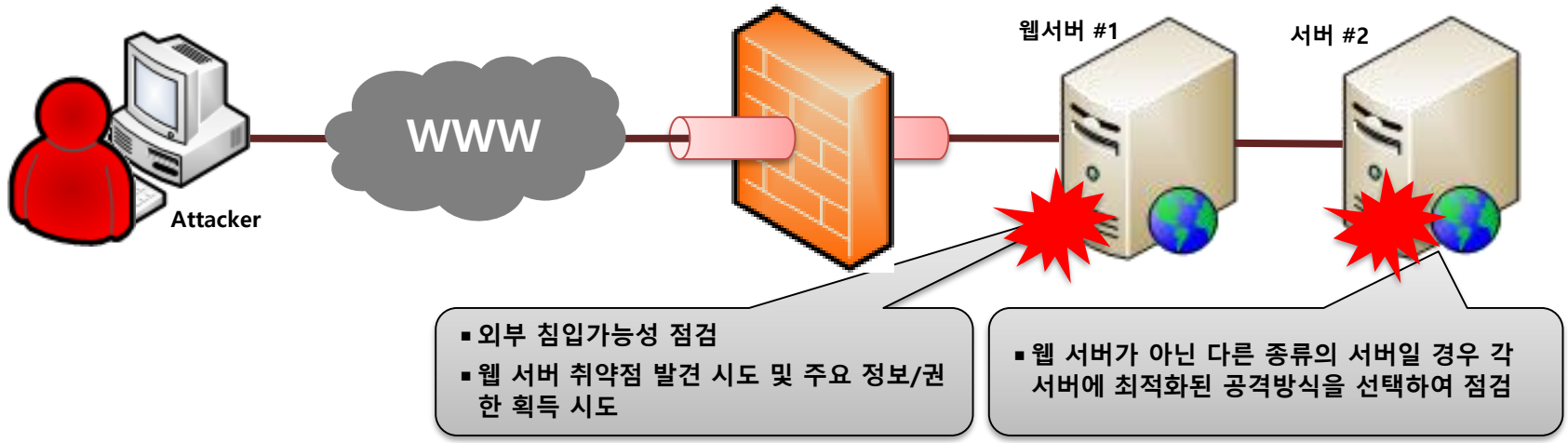


대상 IP 대역 확인

대상 자산 기반 모의해킹 대상 확보

2. 외부 모의 침투 – 침투 시도

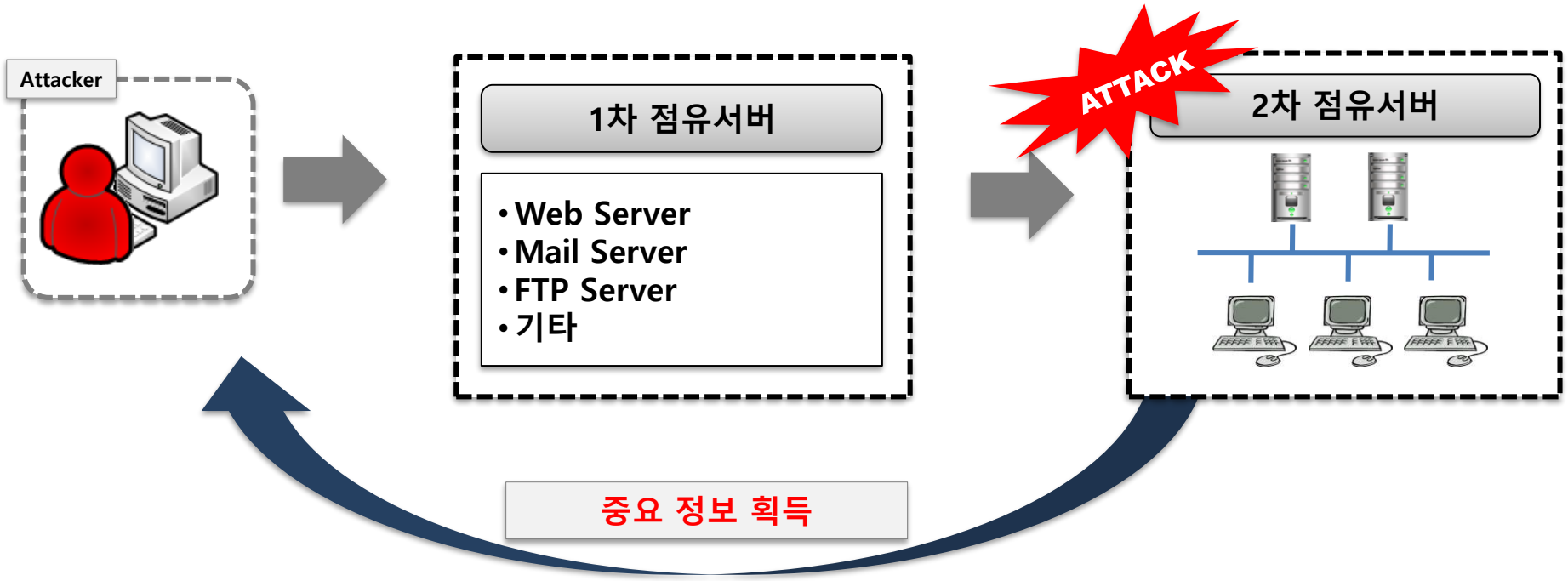
수집한 대상을 바탕으로 웹 취약점을 활용하여 침투시도를 수행하며 각 서버의 환경 및 설정에 맞는 공격을 선택하여 대상 서버의 내부 정보를 획득하거나 서버를 점유를 할 수 있는 점검을 수행합니다.



웹 서비스 침해 가능성 점검	• 공격자가 외부네트워크에서 인젝션, 파일 업로드, 파일 다운로드, 매개변수 조작 등에 대한 공격을 시도하여 침해 가능성이 존재하는지 점검
서버 유형에 맞는 공격 방식 선택	▪ 일반적인 웹 환경이 아닌 Framework 사용한 서버일 경우 해당 서버에 맞는 점검을 선택 ▪ 웹 서버가 아닌 외부에 오픈된 Admin, FTP, File Manager 서버에 대한 적절한 진단방식을 선택

2. 외부 모의 침투 – Lateral Movement

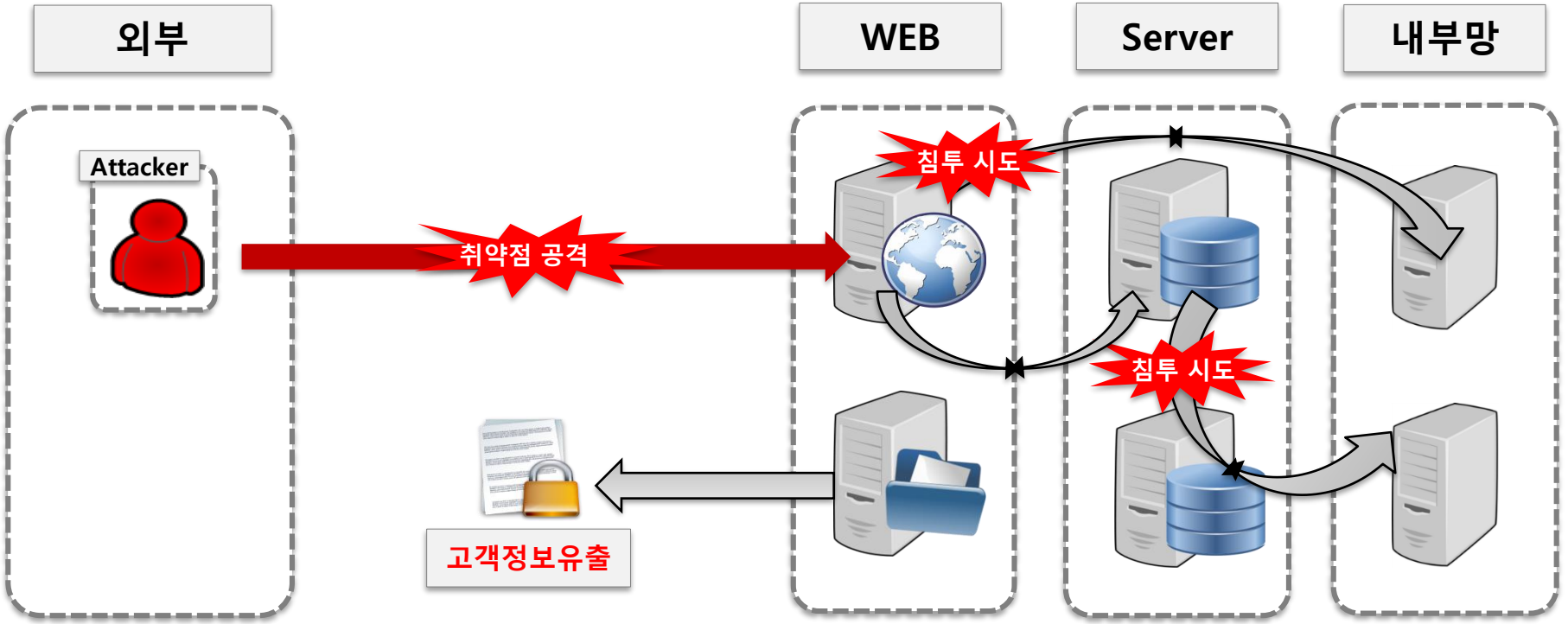
외부 공개 서버에 침입한 후 구간에서 내부 중요 서버로 침투 가능성, 방화벽 룰 설정 오류 및 관대한 정책 존재 여부 점검합니다.



주변 서버권한 획득	• 공격자가 1차 점유서버를 획득한 상황을 가정하고 2차로 점유 가능한 서버가 있는지 확인한 뒤에 개인정보, DB 접속정보, 회사 자산 정보등 중요 정보 획득을 시도합니다.

2. 외부 모의 침투 – 내부망 침투

취약점을 이용하여 점유한 서버를 활용하여 내부망 침투 가능성을 진단합니다. 이는 네트워크 분석을 통하여 구성도를 파악하고 방화벽 설정오류 및 기타 정상 포트를 악용하여 시도를 수행합니다.



내부망 침투 시도

- 웹 및 시스템 취약점을 활용하여 접근 권한이 많은 서버 점유 시도
- 방화벽 설정 오류 및 기타 정상 포트를 악용하여 내부망 침투 가능성 진단

2. 외부 모의 침투 – 내부망 침투

내부 직원의 PC에 악성코드가 침입하였을 경우 망 분리 솔루션, 개인정보 보호 솔루션 등 보안 솔루션의 취약점을 통해 중요 정보 유출이 가능한 지 점검합니다.

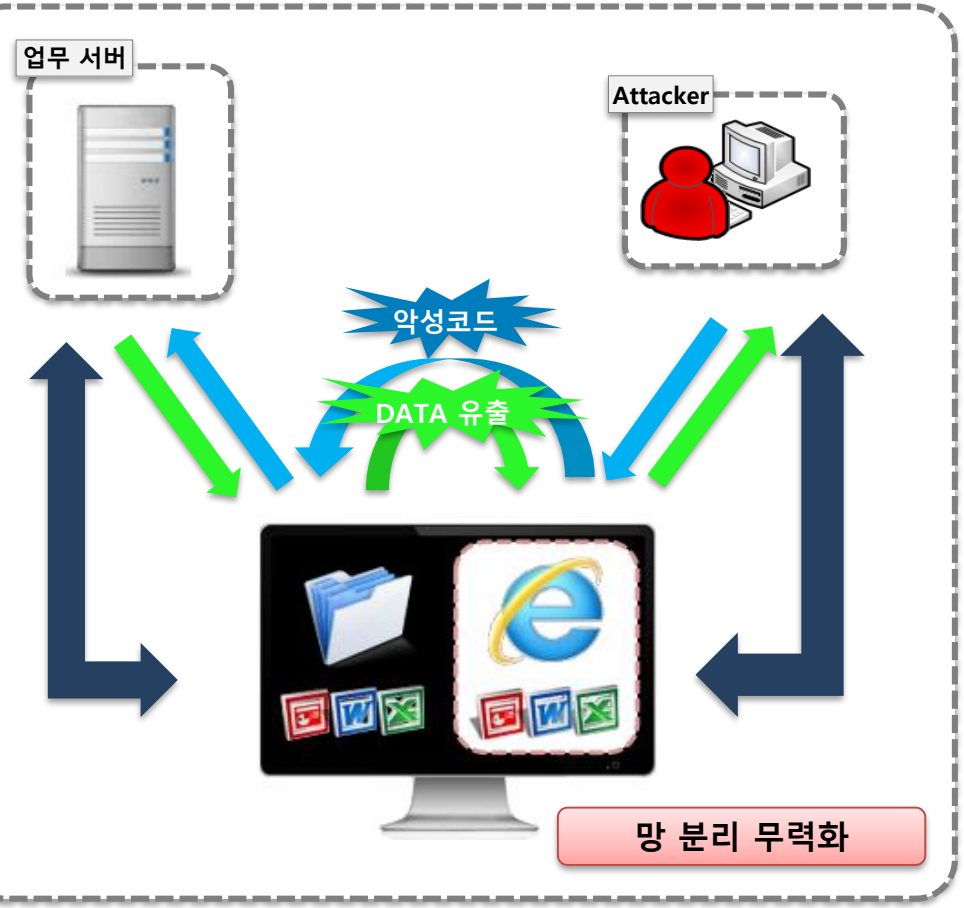
1 악성코드 감염

- 업무 망 PC가 웹, USB, Mail 등을 통해 악성코드에 감염된 상태로 가정
- 감염된 PC를 통해 내부 데이터 유출 가능성 점검

2 업무 / 인터넷 접점 취약점

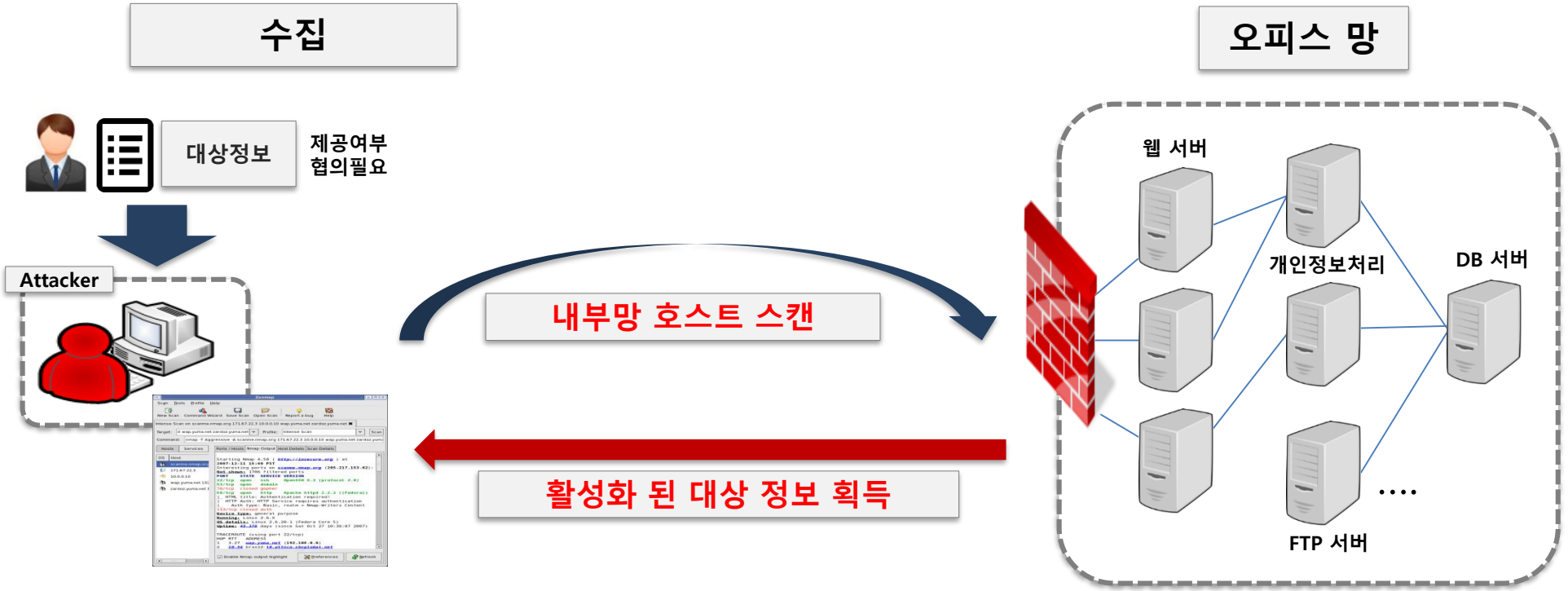
- 업무 망 보안 UPDATE 서버를 통한 자료 유출 가능성 점검
- 업무 / 인터넷 자료교환 시스템 취약점 통한 자료 유출 가능성 점검

망 분리 취약점 점검



3. 내부 모의 침투 – 대상 수집

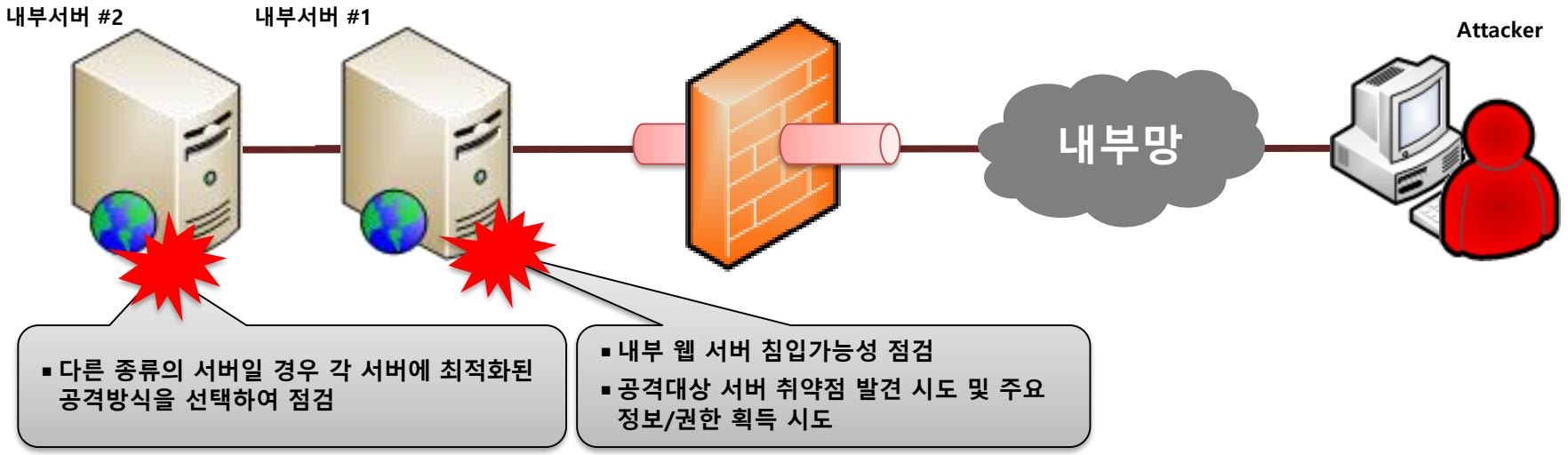
담당자와 협의 후 대상정보를 받거나 그렇지 않을 경우 오피스 망을 대상으로 네트워크 스캔을 진행하여 진단 대상을 확보합니다. 확보 된 대상은 담당자 승인 후 점검을 수행합니다.



대상수집	• 점검대상 리스트 대상 • 네트워크 스캔 후 점검 대상 정보를 획득 한 뒤 담당자 승인 후 점검 수행

3. 내부 모의 침투 – 침투 시도

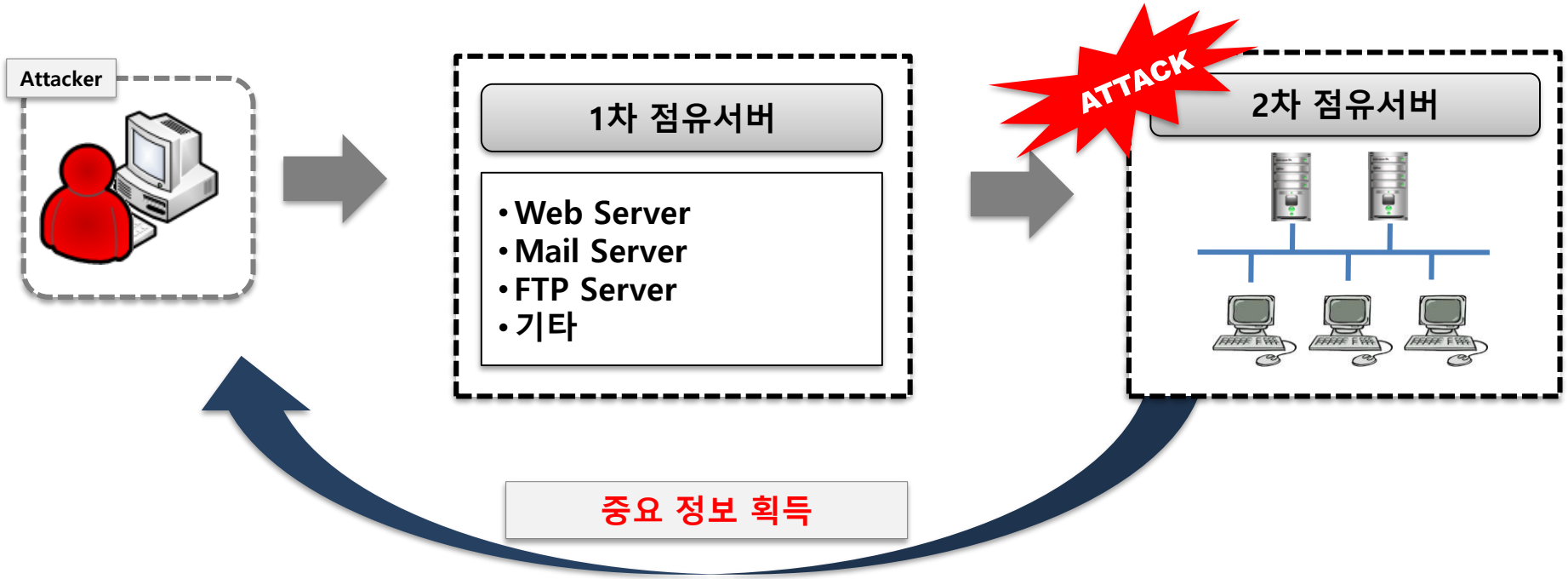
수집한 대상을 바탕으로 웹 취약점을 활용하여 침투시도를 수행하며 각 서버의 환경 및 설정에 맞는 공격을 선택하여 대상 서버의 내부 정보를 획득하거나 서버를 점유를 할 수 있는 점검을 수행합니다.



내부 웹 서비스 침해 가능성 점검	• 공격자가 내부네트워크에서 인젝션, 파일 업로드, 파일 다운로드, 매개변수 조작 등에 대한 공격을 시도하여 침해 가능성이 존재하는지 점검
서버 유형에 맞는 공격 방식 선택	▪ 일반적인 웹 환경이 아닌 Framework 사용한 서버일 경우 해당 서버에 맞는 점검을 선택 ▪ 웹 서버가 아닌 내부에 오픈된 Admin, FTP, File Manager 서버에 대한 적절한 진단방식을 선택

3. 내부 모의 침투 - Lateral Movement

내부망 서버에 침입한 후 구간에서 기타 주변 서버에 대한 침투 가능성, 방화벽 룰 설정 오류 및 관대한 정책 존재 여부 점검합니다.

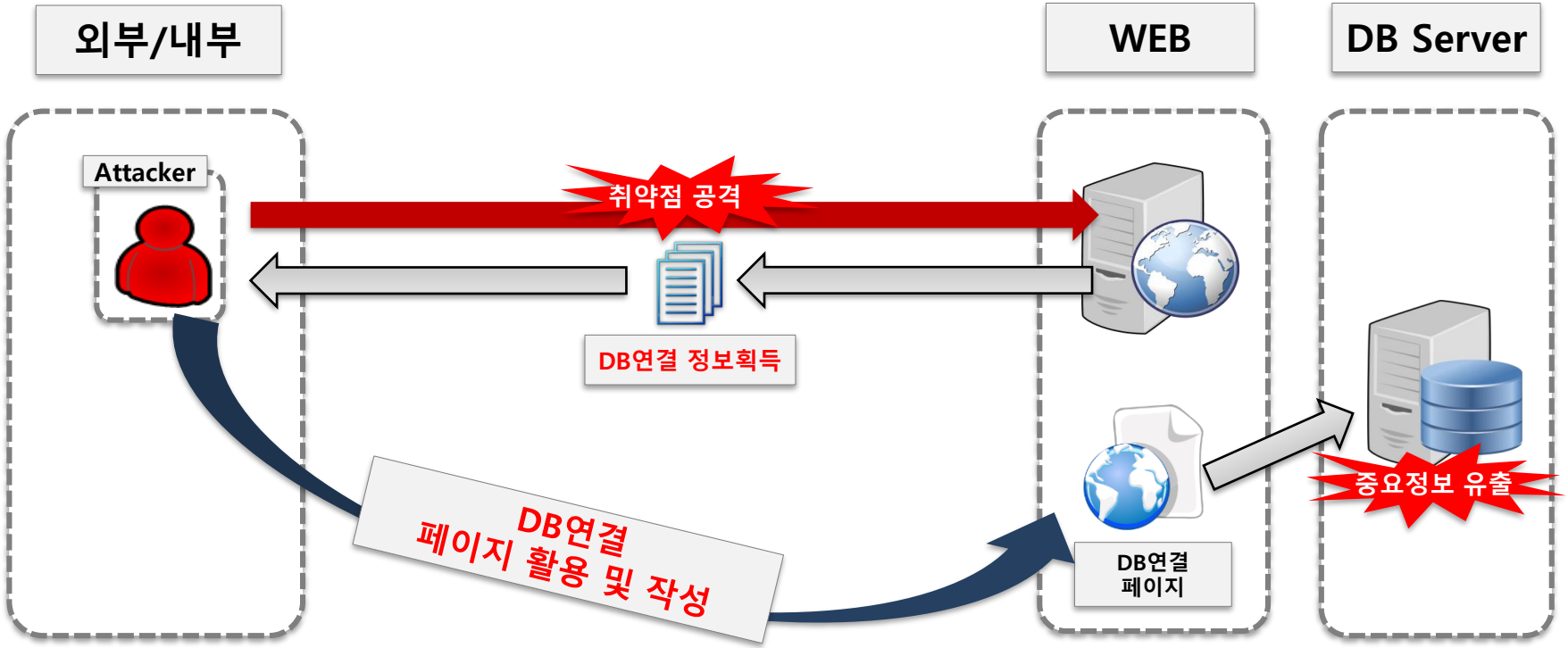


주변 서버권한 획득

- 공격자가 1차 점유서버를 획득한 상황을 가정하고 2차로 점유 가능한 서버가 있는지 확인한 뒤에 개인정보, DB 접속정보, 회사 자산 정보등 중요 정보 획득을 시도합니다.

4. 중요정보 획득

취약점을 이용하여 Web Application 소스 분석 후 DB 연결 정보를 획득하여 기존에 있는 페이지를 활용하여 DB에 연결하거나 기존의 페이지가 없을 경우 DB 연결 페이지를 작성하여 개인정보 노출 가능성을 점검합니다.



DB연결을 통한 개인정보 획득 시도

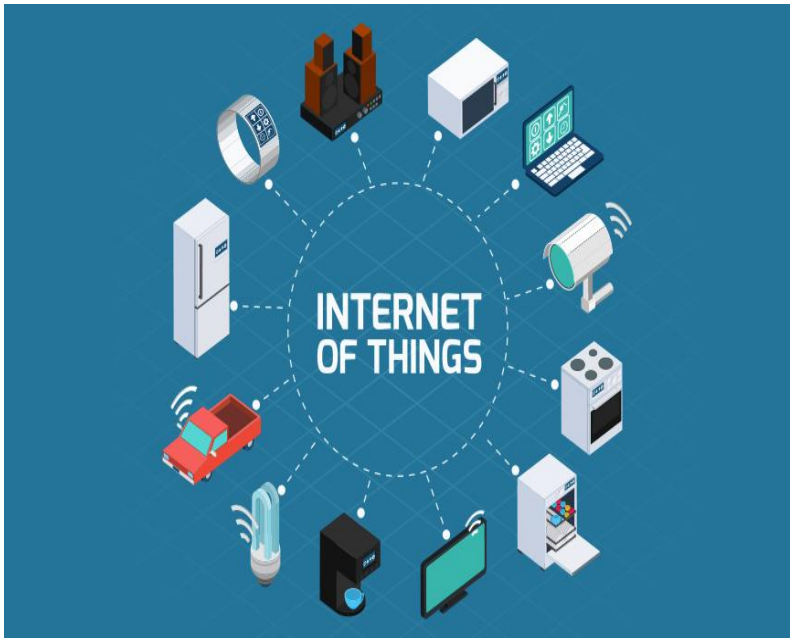
- DB연결 페이지의 SQL 인젝션 취약점을 활용한 중요정보 유출 시도
- 해당 서버를 점유한 경우 DB접속 이용하여 DB연결 페이지를 작성하고 중요정보 유출 시도

5. 모의 해커 관점의 Attack Surface

모의 해커가 대상을 바라보는 시각

- Mobile

- IoT



6. Real Attacker 관점의 Attack Surface

Real Attacker는 모의 해커와 다른 시각으로 바라 봅니다.
모의 해커와는 다르게 시간의 제한이 없으며 동원되는 방법도 더 다양하게 선택할 수 있습니다.

Target	• 최종 목적은 중요 정보나 금전적 이익을 얻을 수 있는 대상 • 그러나 그 대상으로 접근하기 위해 오히려 보안이 허술한 대상을 먼저 Targeting 할 수 있음 • IoT, Printer 등 동일 네트워크 상 취약하고 은닉하기 좋은 Target 공략
Attack Surface 증가	• 모의 해커와 다르게 Social Engineering 기법도 사용 • 대상 기업에 국한되지 않고 Third-Party, Open Source, 보안솔루션 등 Attack Surface 증가
획득 경로 다양성	• 제로데이 취약점 및 악성코드 등을 구매 • 다크웹 등을 통한 다양한 정보 및 해킹 도구 획득
지속성	• 모의 해커는 계약된 기간에 국한 • 목적을 이루기 위해 지속적으로 Attack Surface 공격 수행
은닉	• 공격 성공 후 지속적인 정보 유출을 위해 은닉 • 은닉 후 새로운 Attack Surface 모니터링 및 공격

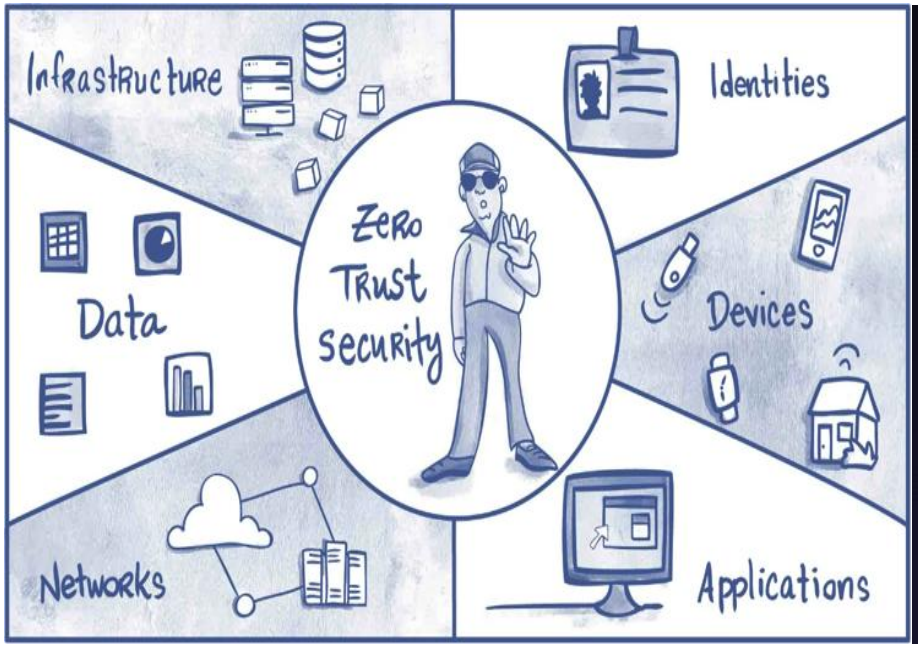
III. 대응 전략

- 1. Zero Trust
- 2. Attack Surface Management
- 3. 취약점 패치 및 관리
- 4. 결론

1. Zero Trust

절대 신뢰하지 말고 항상 검증하라 (Never Trust, Always Verify)

1. Resources : 모든 데이터, 컴퓨팅 서비스는 자원으로 보호 대상
2. Communication : 모든 통신은 내부망/외부망 관계없이 동일한 보안 요구 충족 필요
3. Per-session Access : 개별 엔터프라이즈 리소스에 대한 접근은 세션 별로 검증하여 부여
4. Dynamic Policy : 액세스는 클라이언트 ID, 애플리케이션/서비스 및 요청 자산의 동적 정책에 따라 결정, 모든 단말기에 설치된 소프트웨어 버전, 네트워크 위치, 요청 시간 및 날짜, 이전에 관찰한 행동처럼 상세한 정보에 기반
5. Monitoring : 기업은 모든 소유 자산 및 관련 자산의 무결성과 보안 상태를 계속 모니터링, 측정
6. Authentication And Authorization : 모든 인증 및 권한 승인은 동적이며 액서스 허용 전 철저히 적용
7. Continuous Improvement : 기업은 자산, 네트워크 인프라, 현재 통신 상태에 대한 가능한 많은 정보 수집 & 점검



2. Attack Surface Management

기업의 디지털 자산을 지속적으로 감시하는 Attack Surface Management 수행 필요

1. 공개된 자산 탐색 : 도메인, IP, 클라우드 인프라, 외부 시스템 등을 자동으로 스캔
2. 취약점 분석 : 알려진 보안 취약점, Misconfiguration, 공개 Credential 식별, 모의 해킹
3. 리스크 평가 및 대응 : 위험도가 높은 자산을 우선순위로 설정, 보안 조치
4. 지속적인 모니터링 : 새로운 취약점 및 위협 요소 발생 시 즉시 경고

3. 취약점 패치 및 관리

보안 솔루션과 병행해야 할 대응 전략은 취약점을 패치하고 관리하는 것입니다.
취약점은 대상에 따라 패치 방법 및 관리 방법이 다를 수 있습니다. 이와 같은 조치를 지속적으로 수행해야 합니다.

기업 자체 개발 솔루션	• SAST/DAST/SCA 등을 활용하여 개발 초기 단계부터 정적/동적 분석을 수행하여 수정 • Secure Coding 준수, DevSecOps 문화 조성 • 패치 적용 후 충분한 우회 가능성 테스트 및 QA
Third-Party 솔루션	• 벤더가 제공하는 보안 패치 신속히 적용, 패치 관리 시스템 활용, 사전 검증 • 정확한 Third-Party 솔루션 인벤토리 관리 (버전 정보 포함) • 패치 불가능/지연 시 해당 솔루션의 네트워크 접근 제한, 기능 제한 등 보안 통제 적용
보안 솔루션	• 장애 발생 시 보안 공백이 발생하므로 소프트웨어 패치, 시그니처, 엔진 업데이트 등 업데이트 • 보안 점검을 주기적으로 수행하도록 벤더에 권고 • 이력 관리 및 단계적 패치 적용
IoT 기기	• 종류가 매우 다양하고, 제조사별 관리 방식이 상이하여 패치 어려움 • 자동 업데이트 및 정기적인 펌웨어 업데이트 수행 • 네트워크 세분화를 통해 중요 시스템과 격리 필요
Cloud 환경	• CSP와 사용자 간의 책임 범위가 다름 • 운영 중인 서비스가 기업 자체 개발일 경우 위의 패치 및 관리 방법 수행 • IaaS, PaaS, SaaS 별 책임 범위 확인하여 조치

4. 결론

100%의 보안은 존재하지 않습니다.
그러나, 사전 예방과 모니터링, 빠른 대응을 통해 침해 사고를 예방하고 피해를 최소화 할 수는 있습니다.

보안 주체	대응 전략 및 방안
개발자	▶ 주요 취약점을 이해하고 설계단계부터 Secure Coding을 하도록 합니다. ▶ 보안 담당자의 요구에 따라 발견된 취약점을 빠르게 패치합니다. ▶ 사용하는 프레임워크, 라이브러리, 개발 도구 등의 보안 취약점을 주기적으로 확인하고 최신 버전으로 업그레이드 합니다. ▶ API 를 안전하게 사용합니다. Key 노출 등은 최소화합니다.
기업의 정보보호 담당자	▶ 기업/기관의 모든 Attack Surface를 파악하고 관리합니다. (중요도 불문) ▶ 주기적인 모의 해킹, 취약점 점검 등을 통해 위험 평가를 실시하고 대책을 적용합니다. ▶ 통합 보안 관제(SIEM/SOAR)를 수행하여 위협을 탐지하고 초기 대응 시간을 단축합니다.
컨설팅/보안솔루션 기업	▶ 최신 해킹 기법, 보안 트렌드를 연구하고 숙지하여 실제 공격자의 공격을 방어할 수 있도록 합니다. ▶ 보안솔루션에 대해 주기적으로 모의 해킹을 실시하고 공급망의 무결성을 수시로 확인합니다. ▶ 보안 인식 제고를 위해 노력하고 침해사고 발생 시 신속 대응합니다.

고객의 정보보호를 위한
최고의 파트너가 되겠습니다.

RAON SECURITY

(주)라온시큐리티
[TEL] 02-862-9890 [FAX] 02-862-9891
[URL] http://www.raonsecurity.com
서울 금천구 가산디지털1로 131 BYC하이시티 B동 903호