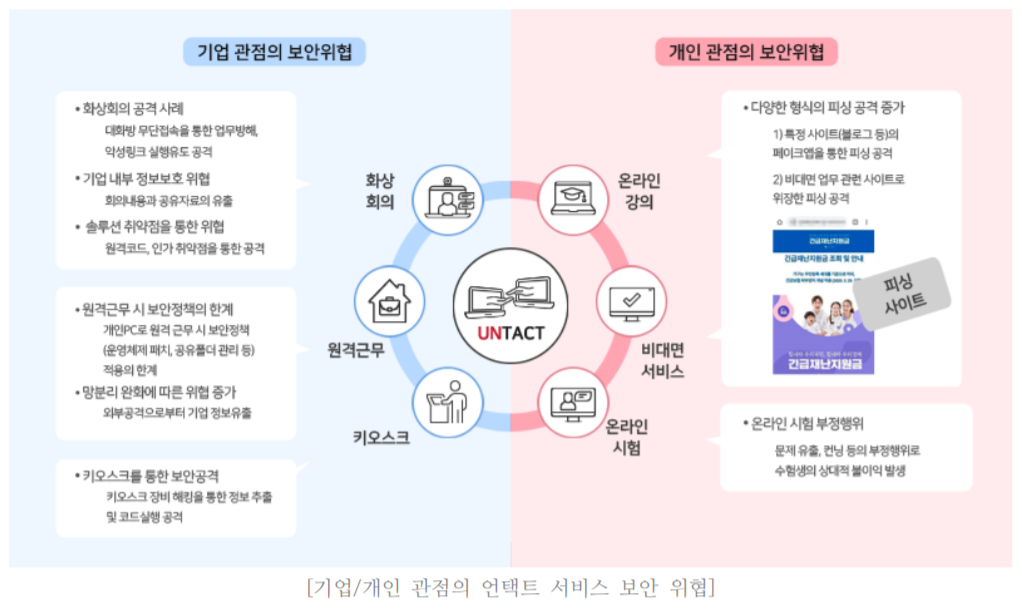
**언택트 시대 보안 방향과 웹 해킹 기법**

1989년 팀 버너스리가 웹을 개발했다. 30년이 흐른 지금 웹 즉 인터넷은 팀 버너스리가 꿈꾸던 곳이 아니다. 이제 웹은 공격자에게 돈벌이가 가능한 장소이다. 이제 인류는 물리적 환경을 뛰어넘어 웹에서 활동한다. 그리고 2020년 현재 코로나 바이러스는 인류에게 “이제 어떻게 살아갈거야?” 라는 질문을 던진다. 다행히 인류는 웹과 스마트폰을 앞세워 비대면 원격사회 전환을 가속화 하고있다. 디지털 전환은 보안담당자들에게 새로운 위협을 안겨줬다. 따라서 이 레포트는 언택트 시대에 나아가야할 웹 보안 방향과 웹 해킹 기법을 설명한다.

**1절. Untact 시대 보안 방향**

[**그림 1] 기업/개인 관점의 언택트 서비스 보안 위협**

**※출처 : SK Infosec EQST 상반기 보안이슈 보고서**

SK Infosec EQST 상반기 보안이슈 보고서의 언택트 보안위협은 [그림1]과 같다.[1]

[그림1] 핵심은 취약점 공격, 엔드포인트 위협, 내부인력의 기술 유출, 개인정보 유출이다.

결국 언택트 시대가 와 더욱 보안에 신경을 써야할 뿐, 그 본질은 같다. 그렇다면 위 3가지 보안위협을 어떻게 대비해야할까?

**1. 취약점 공격**

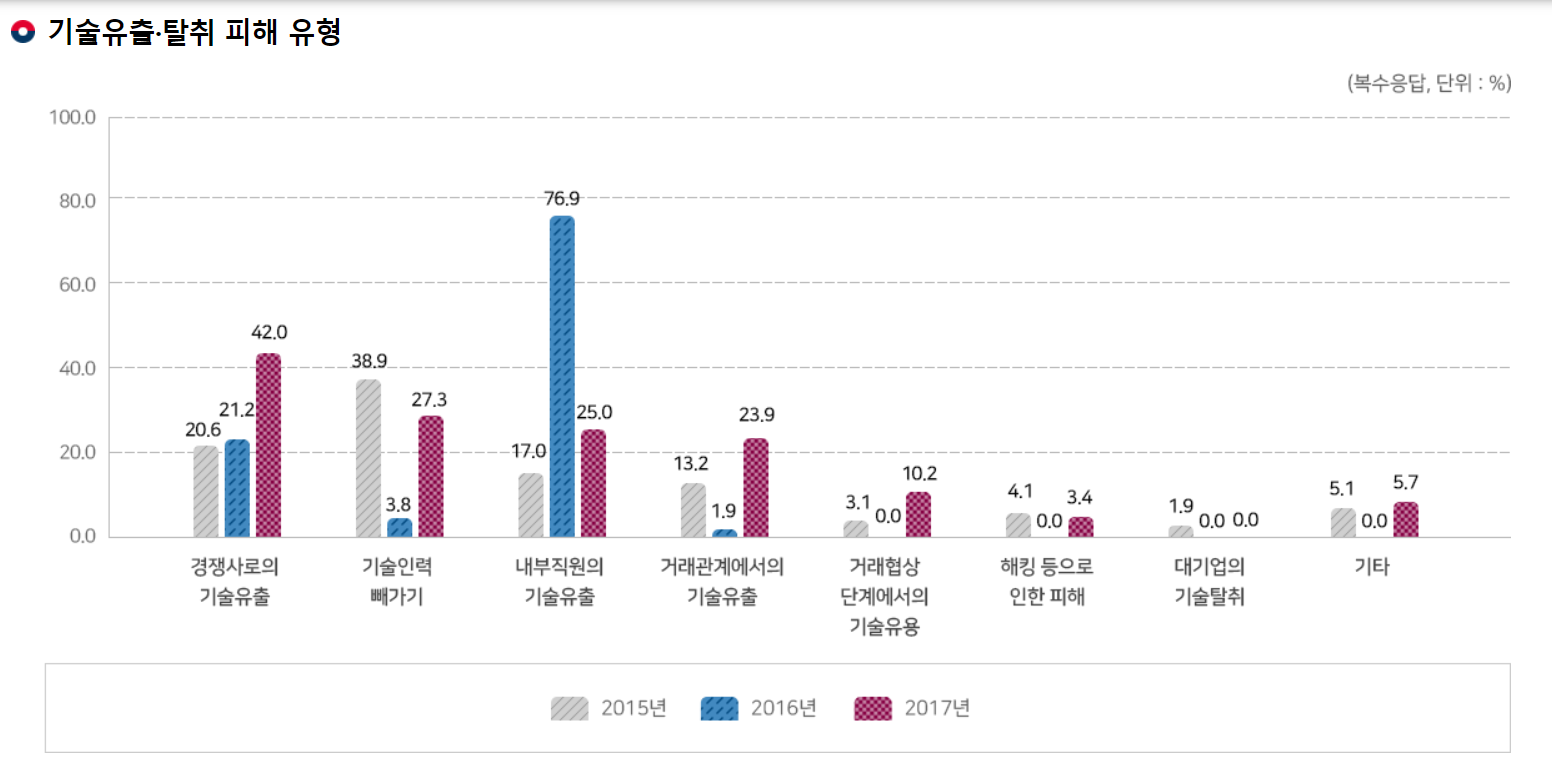
취약점이 없는 코드 즉 안전한 코드란 시큐어코딩과 좋은 개발프로세스로 만들어진 코드다. 빠른 개발 ⋅ 배포와 보안이 결합된 개발 프로세스를 DevSecOps라 한다. 하지만 아직 개발 프로세스 트렌드는 DevOps다. DevOps는 Development와 Operatios의 합성어이며, 기존 개발 업무와 관리 업무로 나눠진 두 역할 사이에서 커뮤니케이션, 협업, 통합을 강조하는 개념이다.[2] 데브옵스는 빠른 속도로 개발과 배포가 가능하다. 그러나 개발 프로세스 마지막에 보안성 평가를 해 설계 단계에서 심각한 취약점이 발견되면 처음부터 개발을 해야 될 가능성이 있다. 그리고 빠른 속도로 개발 ⋅ 배포 하다보니 보안성 평가가 제외될 때가 있다. 따라서 안전한 코드를 만들려면 DevSecOps 프로세스가 필요하다. DevSecOps는 보안을 개발과 배포 사이에 넣어 개발, 배포, 운영, 관리에 이르기까지 전 영역이 보안과 연계된 것을 의미한다.[3] 즉 보안을 보안팀 책임이 아닌 IT 부서 전체, 회사구성원 공동 책임으로 간주하는 것이다. DevSecOps는 정보보안팀, 개발팀, 운영팀 간 지속적인 협업으로 모니터링, 평가 및 분석을 진행하고 보안 결함과 취약점을 조기에 발견해 프로그램 수정에 필요한 시간을 단축시켜 재작업 비용과 보안 사고 위험을 감소시킨다. 보안팀이 DevSecOps의 자동화된 개발 주기에서 보안 기능을 수행하며, 정책도 자유롭게 설정할 수 있다. 따라서, 가급적이면 개발 초기부터 보안팀이 합류해 자동화된 어플리케이션 보안활동을 수행하여 서비스 다운이나 중요 고객정보 유출 실수를 막아야 한다.[3]

**2. 엔드포인트 위협**

원격근무로 인해 기업은 개인PC 관리가 더 힘들어졌다. 유해사이트, 피싱 메일, 패치 누락, 불법 소프트웨어, USB 사용 등 다양한 위협에 노출되었다. 따라서 엔드포인트 단계가 위협에 노출 될 가능성이 매우 높아 19년도에 비해 EDR 제품이 더욱 주목받을 것이다. EDR(Endpoint Detection and Response, 엔드포인트 탐지 및 대응)솔루션은 사이버 위협을 사전에 방어할 수 없다 가정하고, 위협이 이미 기업 혹은 기관 내부에 존재한다는 관점에서 접근한다.[4] 기업과 기관은 많은 비용을 투자해 백신, 샌드박스, 방화벽, APT 솔루션 등을 구축하였지만 기존 솔루션은 알려지지 않은 위협을 탐지하기 힘들었다. 공격자들은 매우 세밀하고 지능적으로 샌드박스를 우회 공격해 보안 솔루션들을 무력화시켰다. 하지만 EDR은 엔드포인트 영역을 모니터링하여 모든 행위(파일변경, 레지스트리 변경, 네트워크 연결, 프로세스 생성 ⋅ 삭제, 윈도우 아티팩트)를 분석해 위협을 수집 ⋅ 탐지하여 실시간으로 연속적인 공격행위를 수집해 침해사고 대응이 가능하다. EDR은 엔드포인트 단계에서 발생한 모든 이벤트를 타임라인, 파일과 프로세스 평판정보 등으로 제공해 가시성과 포렌식 정보를 제공한다. 특히 EDR은 알려지지 않은 새로운 위협을 탐지한다. 따라서 엔드포인트에서 발생하는 수 많은 위협을 머신러닝, 행위분석 등으로 탐지해, 기존 APT 공격 방지 제품들이 가지고 있던 약점을 보완하였다.

**3. 내부인력의 기술유출**

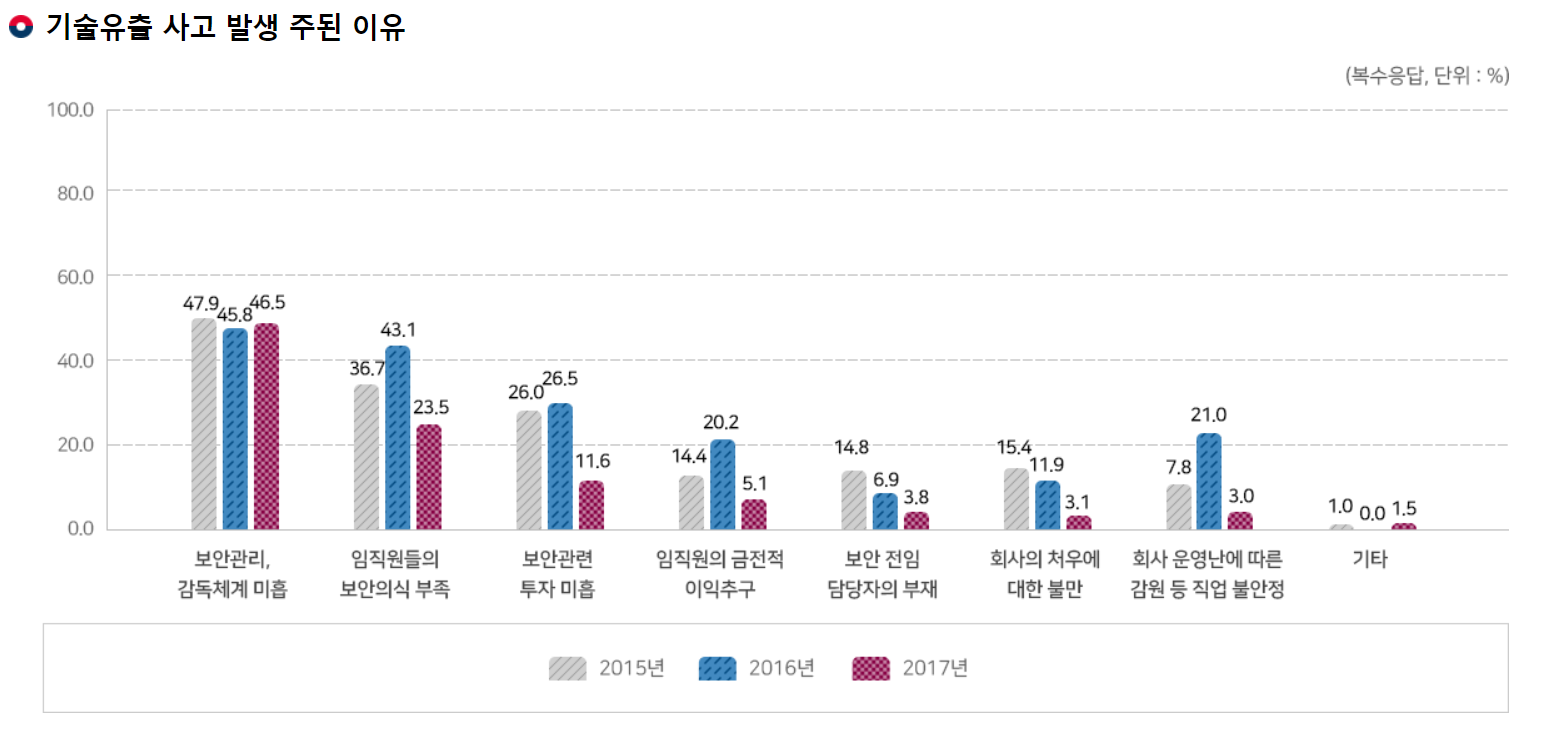
화상회의 솔루션 취약점으로 회의내용과 자료가 유출될 수 있다. 그리고 내부인력에 의한 기술 유출 역시 조심해야한다. 이직을 준비하는 직원은 회사 보안 정책에 벗어나 있으므로 기술 유출을 시도할 가능성이 있다. 중소벤처기업부가 발간한 2017년 중소기업 기술보호역량수준 실태조사에 따르면 기술유출 피해유형 1위는 내부직원의 기술유출이다.

****

**[그림2] 기술유출 탈취 피해 유형**

**※출처 2017년 중소기업 기술보호역량수준 실태조사**

그리고 기술유출 사고 발생 주된 이유는 보안관리, 감독체계 미흡과 임직원 보안의식 부족이 주된 이유로 나타났다. 원격근무로 직원들은 기업 보안정책에서 벗어나 있고 보안관리체계와 보안의식이 부족한 중소기업은 더욱 보안위협에 대비해야 한다.



**[그림3] 기술유출 탈취 피해 유형**

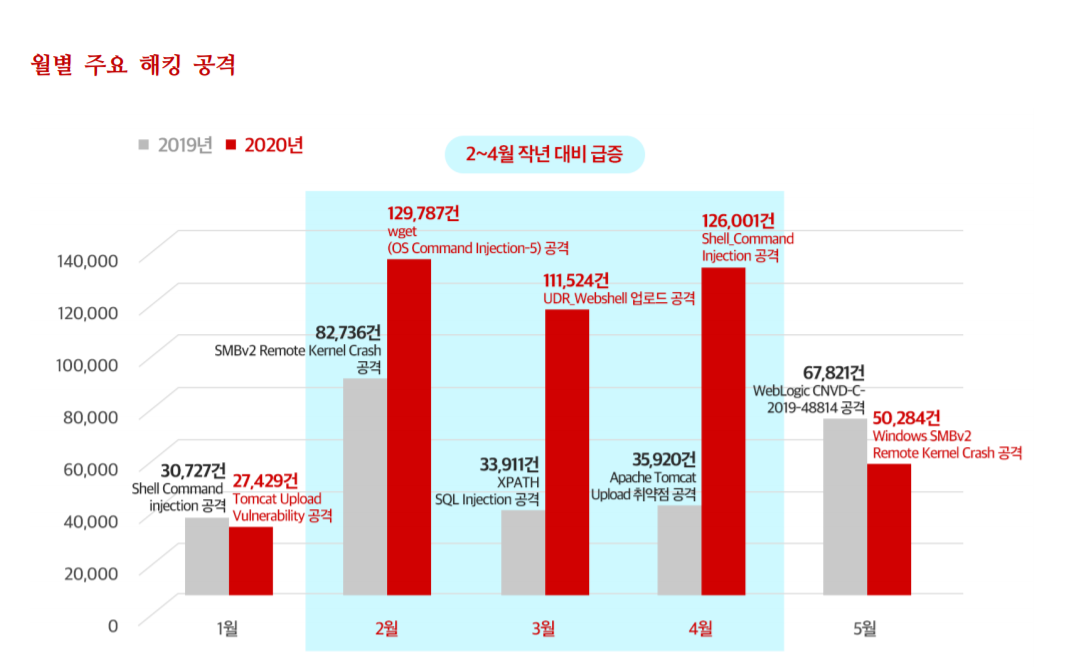
**※출처 2017년 중소기업 기술보호역량수준 실태조사**

**4. 개인정보 유출**

코로나 이슈에 따른 재난 지원금 등 매우 세밀하고 지능화된 피싱메일, 문자에 따른 악성코드 감염을 조심해야 한다. 그리고 기업 내부망에 구축된 보안솔루션 제약을 받지 않아 음란 사이트, 불법 도박 사이트, 불법 만화 공유 사이트 등 유해사이트 접근이 자유로워 악성코드 감염을 조심해야 한다. 개인 노트북이 아닌 업무용 노트북을 사용해 원격근무를 하는 기업이 많아 감염 시 업무용 노트북에 저장되어 있는 직원과 고객사 개인정보 심지어 기업 내부정보가 유출될 수 있다.

**2절. 웹 해킹 기법**

SK Infosec EQST 상반기 보안이슈 보고서에 따르면 2020년 상반기 월별 주요 해킹 공격은 Command Injection 공격과 WebShell 업로드 공격이다. 따라서 WebShell 공격에 사용되는 파일 업로드 취약점을 설명한다.



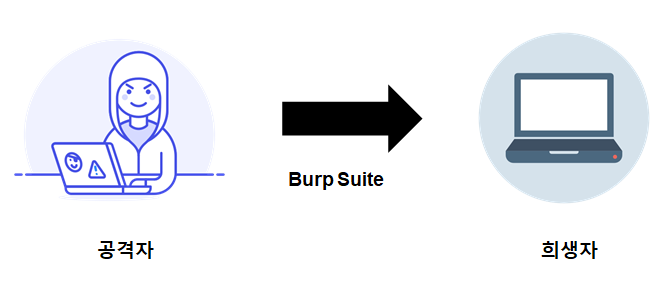
**[그림4] 월별 주요 해킹 공격**

**※출처 : SK Infosec EQST 상반기 보안이슈 보고서**

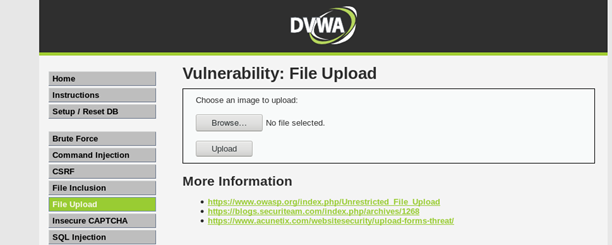
**1. File Upload 취약점**

파일 업로드 취약점은 OWASP TOP 10에 꾸준히 올라오는 취약점이다. 파일 업로드 기능을 악용한 공격으로서 업로드 시 확장자 제한을 하지 않거나 웹서버 취약점으로 발생한다. 악성파일 즉 웹쉘파일을 업로드 해 서버 루트 권한을 획득해 명령을 실행할 수 있다.

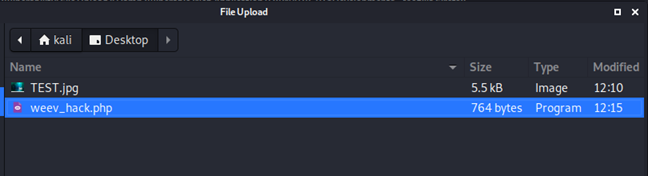
환경 구성은 공격자(Kali Linux) -> 웹 프록시 도구(Burp suite) -> 희생자(DVWA)로 설정하며 공격자가 Burp suite 도구를 이용해 웹쉘 파일을 업로드 해 권한을 획득하는 실습을 진행한다.

****

DVWA는 OWASP TOP 10을 기반으로 취약하게 구성한 웹 환경이다. 레벨은 Medium 단계로 웹쉘 파일을 업로드하겠다.

****

**[그림5] 파일 업로드 페이지 화면**

****

**[그림6] 파일 업로드**

업로드 결과 JPEG 또는 PNG 파일만 업로드가 가능하다. 따라서 Burp suite로 패킷을 변조해 보안설정을 우회하겠다.

****

**[그림7] 파일 업로드 결과**

Burp suite로 패킷을 캡쳐하였다. HTTP header Content-Type 확인 결과 application/x-php를 사용한다. Content-Type은 HTTP header 세부사항 중 하나로서 브라우저가 서버에 보내는 데이터 타입을 나타낸다. Content-Type을 image/png로 변조해 패킷을 전송하겠다.

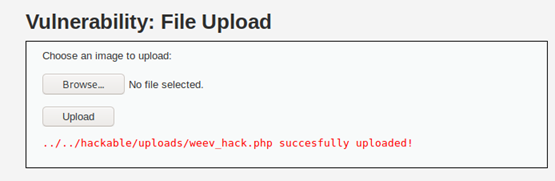
****

**[그림8] Content-Type 확인**

****

**[그림9] Content-Type 변조**

업로드 결과 웹쉘 파일이 성공적으로 업로드되었다.

****

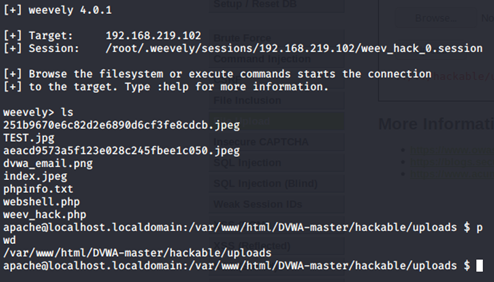
**[그림10] 업로드 성공**

공격에 사용된 웹쉘은 Kali-Linux에서 제공하는 weevley웹쉘 생성 도구로 생성하였다. 이 웹쉘은 공격자 PC에서 원격으로 웹쉘을 실행해 권한을 획득할 수 있다. Kali-Linux에서 웹쉘을 실행하겠다.

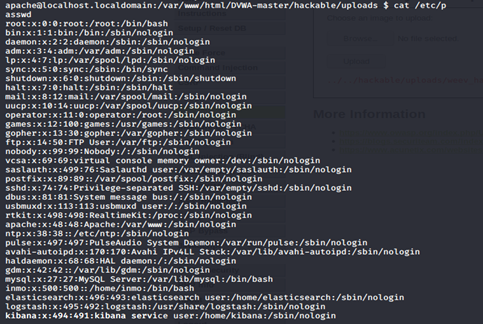
****

**[그림11] 웹쉘 실행**

실행 결과 서버 권한을 획득하였다. ls, pwd 명령어 실행 뿐만 아니라 passwd 디렉토리에 접근해 서버에 존재하는 계정을 확인할 수 있다. 이렇듯 파일업로드 취약점은 서버권한 획득을 가능하게 하는 치명적인 취약점이다.

****

**[그림12] 권한획득 및 명령어 실행**

****

**[그림13] 권한획득 및 명령어 실행**

**3절. 결론**

웹쉘 공격에 사용되는 파일 업로드 취약점은 OWASP TOP 10이 공개될 때 마다 늘 포함되며 서버권한 획득이 가능해 매우 치명적인 취약점이다. 기술이 발전되고 개발속도가 빨라지지만 OWASP TOP 10 절반은 기존에 포함되었던 취약점이다. 기존 취약점이 계속 존재하는 건 개발프로세스 문제이다. 점점 치밀해지는 APT 공격에 대응하기 위해 많은 보안솔루션이 출시되지만 여전히 기업 내부에는 보안솔루션이 탐지하지 못하는 허점이 존재한다. 심지어 웹 환경은 스마트폰, 자율주행차, 스마트시티, 홈 등 모든 사회와 산업 환경을 연결 지어 더 많은 위협에 노출될 것이다. 언택트 시대는 원격근무로 발생하는 또 다른 위협을 발생시킬 것이다. 따라서 기존 취약점과 사회변화로 인해 발생하는 신규 취약점을 줄여나가야 한다. 완벽할 순 없다만 노출되는 위협 수를 줄여야 한다. 그 방안이 DevSecOps, Endpoint 보안이다. 특히 DevSecOps를 단순히 개발프로세스에 보안성 평가를 넣는 것에 그치는 것이 아니라 보안을 보안팀만의 업무가 아니라 개발,운영팀 등 회사구성원 모두가 함께 책임져야한다. 그리고 데이터 중요도에 따라 기밀자료 데이터와 일반 데이터를 나누는 해외와 달리 국내는 내부 업무망과 인터넷이 연결된 외부망을 나누고 있어 원격근무로 회사 외부에서 별도 망연계 제품을 사용해 내부 업무망에 접속하는 상황이다.[5] 외부에서 내부접근이 필수인 언택트 시대에 이러한 보안체계는 위험하다. 망연계 제품에 심각한 취약점이 있다면 해커는 내부 업무망에 쉽게 접근 가능하다. 최근 업무환경은 코로나로 인한 원격근무 외에도 탄력근무제, 디지털 노마드 프리랜서, 외주업체 등과 같이 기업 내부가 아닌 외부에서 업무를 보는 인력이 늘어나고 있다. 따라서 내부, 외부로만 나누는 망분리에서 벗어나 데이터 중요도에 따라 기밀, 일반 데이터를 나누고 접근 권한을 세밀하게 나눠야 한다. 그러나 적절한 접근권한을 가진 직원이 기밀데이터를 유출할 가능성이 있다. 따라서 기밀 데이터 접근 시 정보보안팀에서 접근 이유를 확인해야 한다. 기밀 데이터에는 DLP를 적용하고 기술 유출 시 즉각 대응이 가능하도록 대응 매뉴얼을 구축해야 한다.[6] 그러나 DLP를 적용하더라도 원격근무자가 기밀 데이터를 스마트폰으로 촬영할 수 있으므로 기밀 데이터에 포렌식 워터마크를 적용하여 기술유출을 대비해야 한다. 언택트 시대는 내부, 외부 경계를 무너뜨렸다. 이제 기업과 보안담당자는 제로트러스트 관점으로 보안을 바라봐야 한다. 제로트러스트란 기관 내, 외부를 막론하고 적절한 인증 절차 없이는 그 누구도 신뢰해서는 안 되며, 시스템에 접속하고자 하는 모든 것에 접속권한를 부여하기 전 신원 확인 과정을 거쳐야 한다는 것이다.[7] 그리고 기업 전 구성원이 보안을 경영 활동과 업무에 제약을 주는 것이 아니라 경영과 업무에 꼭 필요하다 생각하는 의지가 중요하다. 좋은 개발프로세스, 다양한 보안솔루션을 구매하더라도 회사구성원 보안의식이 낮다면 끊임없이 위협에 노출됨을 명심해야 한다.

**참고문헌**

**[1] SK Infosec EQST 2020년 상반기 보안이슈 보고서**

**[2]** [**https://blog.lgcns.com/1755**](https://blog.lgcns.com/1755)

**[3]** [**https://blog.lgcns.com/2086**](https://blog.lgcns.com/2086)

**[4]** [**http://blog.naver.com/skinfosec2000/221479897959**](http://blog.naver.com/skinfosec2000/221479897959)

**[5]** [**https://www.sedaily.com/NewsVIew/1Z41SGGLZX**](https://www.sedaily.com/NewsVIew/1Z41SGGLZX)

**[6] https://www.somansa.com/introduce/newsevent/global\_edr\_dlp\_trend/**

**[7]** [**http://www.ciokorea.com/news/37013**](http://www.ciokorea.com/news/37013)