CYBER SECURITY ADVISORY 2022

과학기술정보통신부

KISA 한국인터넷진흥원

AhnLab NSHC SECURITY INCA I.n.t.e.r.n.e.t ESTsecurity HAURI BITSCAN

CYBER SECURITY ADVISORY 2022

Contents

I

개요

CYBER SECURITY
ADVISORY 2022

Ⅰ 개요

한국인터넷진흥원(KISA)과 인텔리전스 네트워크사(안랩, 빛스캔, 이스트시큐리티, 하우리, 잉카인터넷, NSHC)는 국내 기업 보안담당자를 대상으로 “2021년 한 해 동안의 주요 보안 사이버 위협 대응현황”을 알아보기 위해 설문조사('21.11월)를 진행했다.

기업에서 가장 많이 발생한 사이버 위협과 주된 경로, 그리고 가장 우려되는 위협과 주력하는 보안 이슈에 대해 약 150명의 보안담당자가 응답한 결과 2022년에 주의해야 하는 사이버 보안 사항 6가지를 꼽을 수 있었다.

지속되는 랜섬웨어, 증가하는 정보유출의 피해, 피싱/악성 이메일을 통한 공격, 원격 근무 환경의 위협, 공급망 공격, 클라우드 공격이다. 이제 이러한 위협에 대해 어떻게 주의하고 대비해야 할지 알아보자.

II

우리가 주의해야 하는 보안이슈

1. 랜섬웨어
2. 악성 이메일
3. 정보 유출

II 우리가 주의해야 하는 보안이슈

1 랜섬웨어

코로나19는 지속되고 있으며, 코로나19 펜더믹과 함께 IT 환경의 급격한 성장은 인터넷 사용 대상의 확대를 기반으로 사이버 위협의 피해 범위와 규모 역시 급격하게 증가하고 있다.

특히 랜섬웨어는 전 세계적으로 기승을 부리고 있으며, 피해 또한 심각하다. 랜섬웨어에 의한 피해 규모는 2015년 3천8백억에서 2021년 23.6조 원으로 약 6,200%가 급증할 것으로 전망되며, 2031년에는 우리나라 2021년 예산 558조의 약 56%에 달하는 312조를 넘어설 것으로 전망되고 있다.

표 1 글로벌 랜섬웨어 피해금액

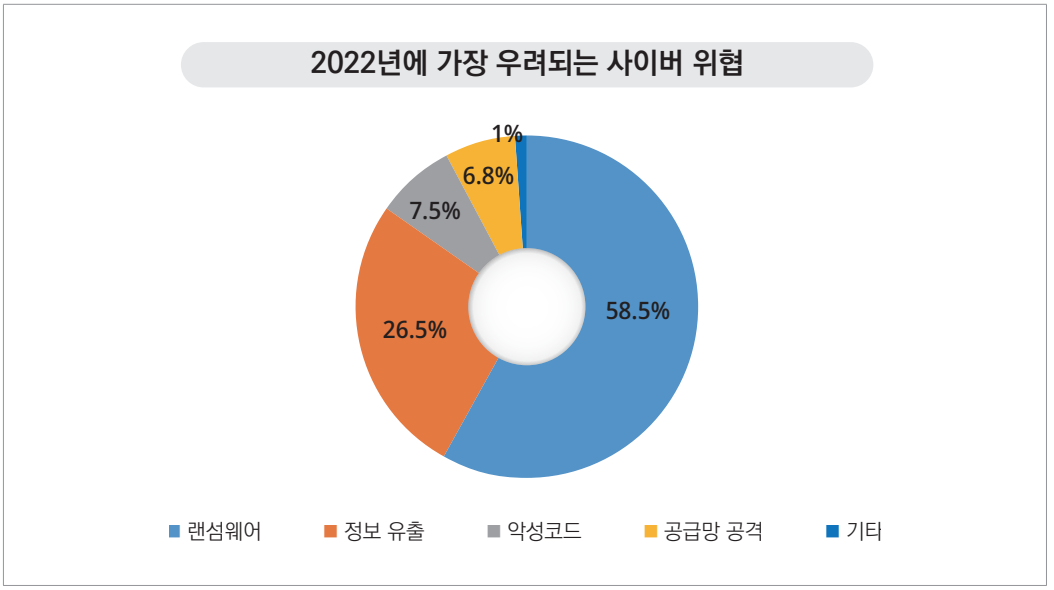
년도	2015	2021	2026	2031
피해금액	3천8백억	23조6천억	84조3천억	312조7천억

출처 : Cyber Crime Magazine 2021

공격의 범위도 의료기관, 제조사 등 다양한 산업 분야로 확대되었다. 지난 5월 미국 최대 송유관 기업 '콜로니얼 파이프라인'은 랜섬웨어로 인해 6일간 운영이 중단되었고 휘발유 값이 7년 만의 최고 수준으로 치솟았으며 해당 지역에 비상사태가 선포되는 사고가 발생하였다. 또한, 코로나19와 관련된 중요시설과 병원을 대상으로 한 랜섬웨어 공격으로 인터폴 보라색

수배서가 발부되기도 하였다. 국내에서는 성형외과 및 여성의원 등이 랜섬웨어에 감염되어 민감한 정보가 대거 유출되는 사고도 발생하였다.

이를 반영하듯 설문 결과에서도 2022년에 가장 우려되는 사이버 위협은 '랜섬웨어'로 나타났다.



랜섬웨어 공격은 금전 탈취를 주목적으로 하고 있으며, 공격 시 확보한 정보의 유출을 볼모로 한 협박 등 기존의 사이버 공격과는 다른 특징을 보인다. 공격자는 랜섬 비용이 지불이 되지 않는 경우 서비스를 마비시키거나 다크웹을 통해 정보를 유출하는 등 다양한 방법을 결합하고 있다. 이러한 영향으로 랜섬웨어는 2022년도 가장 큰 위협일 것이다. 그러면 어떻게 대비해야 할까? 랜섬웨어는 한번 감염되면 복구가 매우 어렵기 때문에 주기적인 백업을 통해 데이터 복원력을 확보하는 것이 최선의 대비책이다.

랜섬웨어 대비를 위한 백업 대책

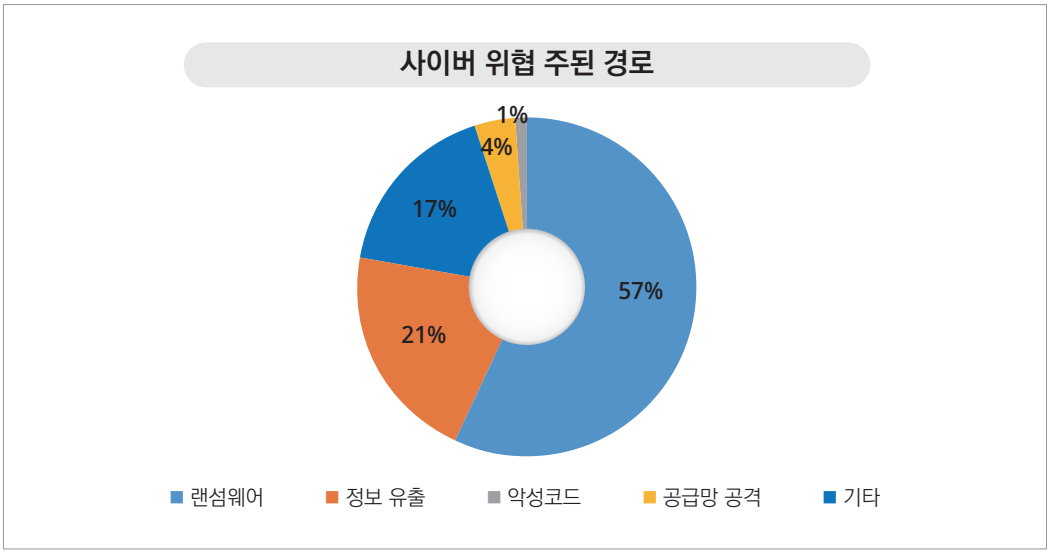
- **안전한 백업 및 재해복구정책 수립**
  - 백업 대상별 백업 기간, 담당자 설정 및 관리
  - 데이터 중요성을 검토하여 RTO, RPO 수립
- **주기적인 백업(주간, 일간)과 백업데이터의 유효성 점검**
  - 월간은 전체 백업, 일 또는 주간 백업은 증분백업 등 주기적인 백업 수행
  - 기업 규모에 맞는 백업 전략을 수립하여 백업
    ※ 대기업 : 직접 백업, 네트워크 백업, SAN 백업, 디스크 복제, Cloud 백업
    ※ 중소기업 : TAPE 백업, Cloud 백업, NAS 백업, 외장 디스크 백업
- **정기적인 백신 점검 및 프로그램(SW) 보안 업데이트 수행**
  - 백업 시스템 백신 설치 및 주기적인 보안 업데이트 수행
  - 백신 담당자 권한 설정 및 외부 인터넷 차단 또는 망분리
  - 백업담당자 및 운영자 PC 대상으로 악성코드 감염, 백신 업데이트 등 보안성 점검
- **별도의 매체에 정기적으로 데이터 백업 후 인터넷과 분리하여 보관**
  - 백업 저장 매체에 대한 물리적인 접근통제 및 권한 설정 필요
- **랜섬웨어 비상 대응을 위한 백업 테스트 및 모의훈련/교육 실시**
  - 백업 테스트를 통한 백업 및 복원의 정기적 적정성 확인
  - 다양한 환경에서 연 1회 이상 테스트를 진행함으로 데이터 무결성, 시스템 가용성 유지

TIP

- **침해사고(랜섬웨어, 해킹 등) 신고***
  * 보호나라-상담 및 신고 페이지
  * 랜섬웨어 전용 페이지(KISA stop 랜섬웨어)-https://boho.or.kr/ransom
  * 전화 신고-(국번없이) 118
  - 원스톱 경찰 신고, 피해 대응·복구 지원, 재발 방지 기술지원
- **랜섬웨어 대응을 위한 안전한 정보시스템 백업 가이드*('21.11)**
  * 보호나라-https://boho.or.kr/data/guideView.do?bulletin_writing_sequence=36327
  - 백업 정책, 백업 시스템 구축 및 방식, 고려사항 등이 기술되어 있음
- **Special Report - Ransomware 보고서*('21.9)**
  * 보호나라-https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=36211
- **최근 기업 대상 랜섬웨어 사고사례 및 대응방안*('20.11)**
  * 보호나라-https://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=35798

2 악성 이메일

사이버 공격의 시작점은 어디일까? 공격자는 개인의 PC나 기업 시스템에 침투하기 위해 다양한 방법을 시도한다. 특히, 이메일은 특별한 경로를 거치지 않고도 사용자에게 쉽게 접근할 수 있어 해킹 공격의 주요 통로로 활용되고 있다. 트렌드마이크로(Trend Micro) 조사에 따르면 지난해 피싱 공격을 차단한 사례가 전년 대비 19% 증가했으며, 스팸을 통해 전송되는 피싱 위협을 탐지한 수가 41% 늘어났다. 설문조사 결과에서도 사이버 위협의 주된 경로로 '이메일'이 가장 높은 비율로 나타났다.



악성 이메일을 이용한 공격은 목적과 형태가 다양하다. 단순히 첨부 파일이나 링크를 통해 악성코드를 유포하는 것부터 시작해 특정 서비스를 사칭하여 사용자의 계정을 탈취하기도 한다. 특히 사회적 이슈를 이용해 수신자가 의심 없이 열어보도록 하는 방식도 많이 쓰이고 있다. 국내는 외교·안보·국방·통일 분야 종사자를 대상으로 대북·북미 관계를 분석한 보고서, 전문가 토론회, 전문가 대상 설문조사 등의 내용으로 위장한 스피어피싱이 자주 발견되어 주의가 필요하다.

최근 공격자는 메일 수신자를 정확하게 지정해 보내는 치밀함도 보인다. 검색엔진을 통해 검색되는 담당자 메일주소, 회사 사이트에 공개된 메일 주소, SNS 등을 통해 수집하거나

이전에 유출된 개인정보 등을 통해 타깃 기업의 담당자에게 그 사람의 업무와 맞는 메일을 보낸다. 인사 담당자에게 이력서를, 구매 담당자에게 견적서를 보내는 등 업무와 관련된 내용으로 위장하여 메일을 발송한다. 또한, 업무 관련 내용을 위장하기 위해 공문이나 문서 양식, 폰트, 자주 사용하는 문체 등을 그대로 따라 하는 등 정교함도 보인다. 첨부 문서는 악성 매크로, 자바스크립트 등을 삽입해 해당 문서를 일정 부분 이상 읽어 내려가면 악성코드가 활성화되도록 한다. 따라서 문서를 열었을 때 악성 여부를 검사하는 백신 프로그램 등 PC 보안 솔루션을 우회할 수 있다. 이처럼 공격이 정교해지면서 피해도 크게 증가하고 있다. 이러한 악성 메일에 대비하기 위해서 어떠한 것을 주의해야 하는지 알아보자.

피싱, 악성 이메일을 통한 위협 주의사항

- **포털사 공지로 위장한 피싱 공격 주의**

  ※ 주요 포털사 고객센터를 사칭한 악성 이메일 기승

  – 공식 안내 메일인지 발신지 확인이 중요

  ex) 국내 N 포털사의 경우 공지 메일의 경우 별도의 초록색 아이콘을 제목에 넣어두고 있어 육안으로 확인 가능

- **의심스러운 메일 수신 시 발신자 진위 확인**

- **출처가 불분명한 악성 링크 및 첨부파일 클릭 주의**

  ※ 특정 기관을 사칭하거나 사회 이슈로 위장한 메일 주의

  ※ 사용자를 속여 ID, PW를 입력하도록 유도하는 메일 주의

- **매크로 및 암호 설정이 된 악성 문서 주의**

  – 암호가 설정된 경우 발신자에게 직접 연락해 사실 여부 확인

  ※ 악성 문서 파일에 암호를 설정해 보안 탐지 회피 및 공격 진행

  – 매크로(콘텐츠 사용) 허용 유도 시 주의 필요

  ※ 오피스 매크로 기능을 악용한 공격이 증가

- **백신 프로그램 설치 및 최신 버전 유지**

TIP

- **민간분야 사이버 위기대응 모의훈련***

  * 보호나라-https://www.boho.or.kr/webprotect/cyberSimulationTraining.do

  - 사이버공격 예방 및 피해 최소화를 위해 실전형 모의훈련(해킹메일, 디도스 공격, 모의침투) 지원

    ※ (해킹메일) 기업 임직원 대상으로 사회공학적 해킹메일을 발송하여 기업 탐지·대응 체계 제고

- **피싱 및 스미싱 상담 및 신고 서비스***

  * 보호나라-https://www.boho.or.kr/consult/phishing.do

- **피싱 및 악성메일 카드뉴스***

  * 보호나라-https://www.boho.or.kr/cyber/preventPhishing.do

- **2020년 4분기 사이버 위협 동향보고서*('21.1)**

  * 보호나라-https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35866

  - (가이드) Q&A로 알아보는 해킹메일

- **TTPs#4 피싱타깃 정찰과 공격 자원 분석*('20.12)**

  * 보호나라-https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35846

- **스피어피싱 공격 타깃별 피해 시나리오 분석*('20.11)**

  * 보호나라-https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35793

- **피싱 메일 공격 사례 분석 및 대응 방안*('20.8)**

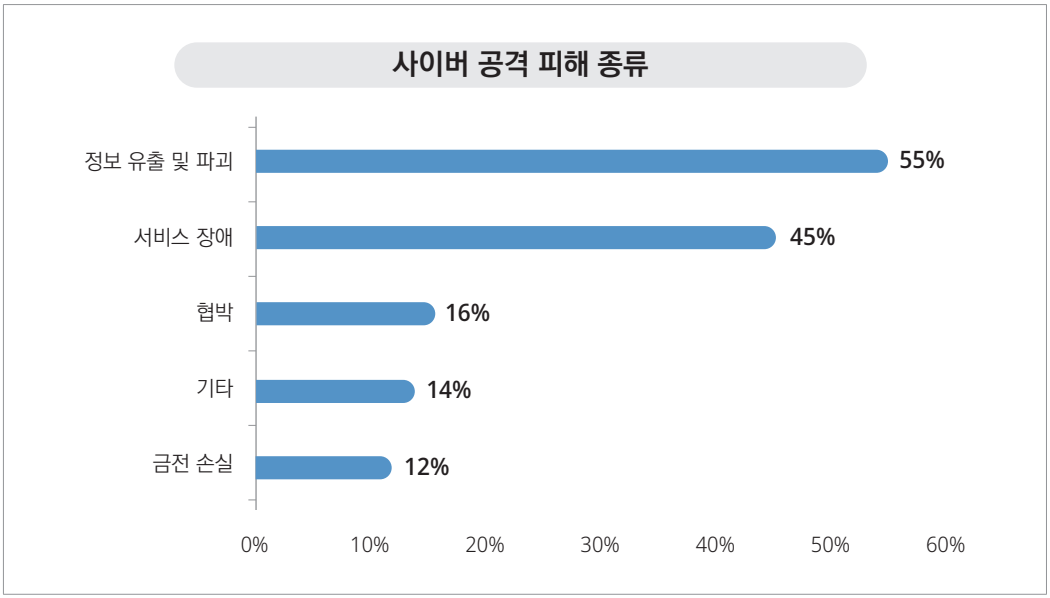
  * 보호나라-https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35560

- **TTPs#2 스피어 피싱으로 정보를 수집하는 공격망 구성 방식 분석*('20.6)**

  * 보호나라-https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35471

3 정보 유출

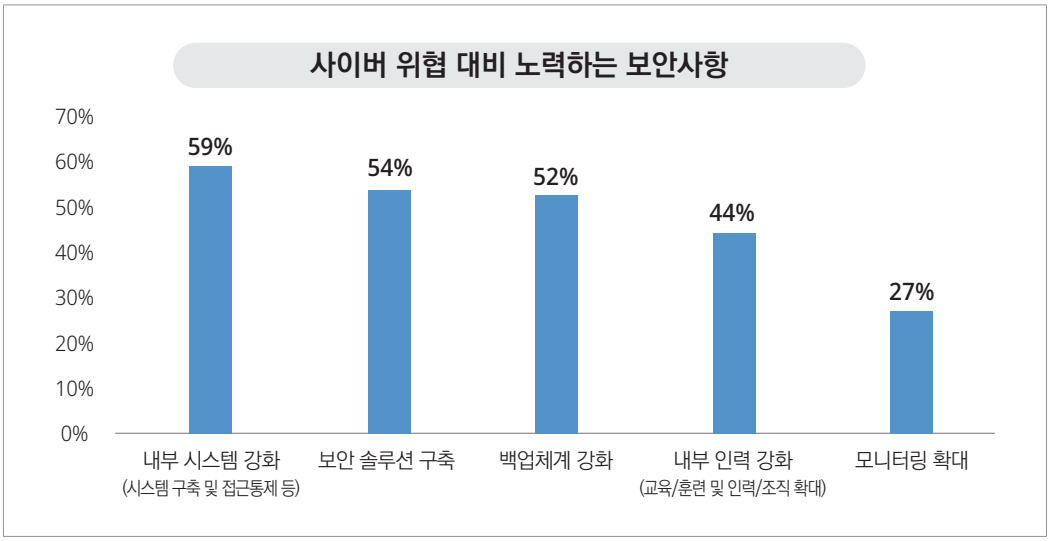
사이버 공격의 시작점이 악성 메일이라면 마지막 단계는 무엇일까? 공격자는 금전과 정보획득 등 여러 가지를 목표로 할 것이다. 가장 많이 발생하는 피해는 무엇일까? 사이버 공격 피해 종류에 대해 설문조사 결과 '정보 유출 및 파괴'가 가장 높게 나타났다.



최근 월패드 해킹 사고로 사생활이 무방비로 노출되어 충격을 주었다. 약 700여 개 아파트 단지의 월패드가 해킹되어 촬영된 영상이 무더기로 유출됐기 때문이다. 특히, 다크웹에 해당 영상들이 불법 유통되고 있어 더욱 문제가 되고 있다. 지난 3월에는 국내 H사의 내부 자료가 다크웹에 유출되어 이슈가 되었다. 이뿐만 아니라 국내 기업의 시스템 계정, 지식 자산 등의 정보가 다크웹을 통해 유출·판매되는 사고가 증가하고 있다. 다크웹의 문제는 익명성으로 추적이 어렵다는 것이며, 공격자는 판매를 위해 정보의 일부만 샘플로 공개하고 있어 수사의 진행도 어렵다. 더욱이 유출된 정보를 악용하여 또 다른 공격을 진행하고 있어 피해가 점점 커지고 있다. 따라서 사전에 대비하는 것이 중요하다.

그러면 어떻게 대비하여야 할까? 국내 기업들을 대상으로 사이버 위협에 대비하기 위해 어떠한 노력을 하고 있는지 알아보았다. 설문조사 결과, '내부시스템 강화', '보안 솔루션

구축'이 높은 비율로 나타났다. 가장 중점을 두고 있는 보안 사항에서 정보 유출에 대비하려면 체크해야 할 포인트가 무엇인지 알아보자.



정보 유출 대비를 위한 검토사항

- **안전한 문서 보안 정책 수립**
  - 기업, 기관, 개인 등의 중요데이터 및 기밀문서의 정보 보호 및 열람 제한
  - DRM 솔루션 등을 통한 문서 암호화 및 반출 시 열람 불가
  - 문서 중앙화 솔루션 등을 활용하여 문서 이력 기록 및 버전 관리
- **비인가 단말기 통제**
  - 매체제어 솔루션 등을 통해 인가되지 않은 이동형 저장장치 및 단말기 통제
    * USB, PC, SD카드, 외장하드, 스마트폰, 프린터 등
- **데이터베이스 계정 관리 및 접근 통제**

  ※ DB 취약점을 통해 고객정보에 접근 또는 유출 주의
  - 데이터베이스 관리자 및 직무별 접근 통제
  - 사용하지 않는 계정, 기본 계정 등 삭제 및 주기적 검토 수행
  - 데이터베이스의 별도의 네트워크 영역으로 구분
  - 데이터베이스 접근을 허용하는 IP, 포트(Port), 응용 프로그램 통제
- **백신 프로그램 설치 및 최신 버전 유지**
  - 실시간 감시 기능 활성화로 감염 예방 및 악성코드 유입 차단

  ※ 원격근무 증가로 개인 단말기 정보 유출형 악성코드 감염 피해 증가

TIP

- **개인정보침해 신고센터***

  * https://privacy.kisa.or.kr/

  – 개인 및 공공기관, 사업자의 개인정보 관련 침해 신고 및 상담 지원

- **e프라이버시 클린서비스***

  * https://www.eprivacy.go.kr/

  – 인터넷 이용자의 본인확인 내역(주민등록번호, 아이핀, 휴대폰 등) 통합 조회 및 웹사이트 회원 탈퇴, 개인정보(열람, 처리정지 등) 지원

- **월패드 등 홈네트워크 기기 관리·이용자 보안수칙*('21.11)**

  * 보호나라-https://www.boho.or.kr/img/wallpad.png

- **사물인터넷 소형 스마트 홈가전 보안 가이드(이용자용)*('21.11)**

  * 보호나라-https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=24924

  – [2장] 스마트 홈·가전 보안 위협 및 대응방안 – 2.1 정보 유출

- **가명정보 처리 가이드라인*('21.10)**

  * https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000843428&fileSn=0

- **개인정보 유출 대응 매뉴얼*('20.12)**

  * https://www.kisa.or.kr/public/laws/laws3.jsp

- **시설별 개인정보보호 가이드라인*('20.12)**

  * https://www.kisa.or.kr/public/laws/laws3.jsp

  – 사회복지시설, 의료기관, 약국, 학원·교습 편

III

우리가 강화해야 하는 보안사항

1. 원격 근무
2. 공급망 공격
3. 클라우드 보안

Ⅲ 우리가 강화해야 하는 보안사항

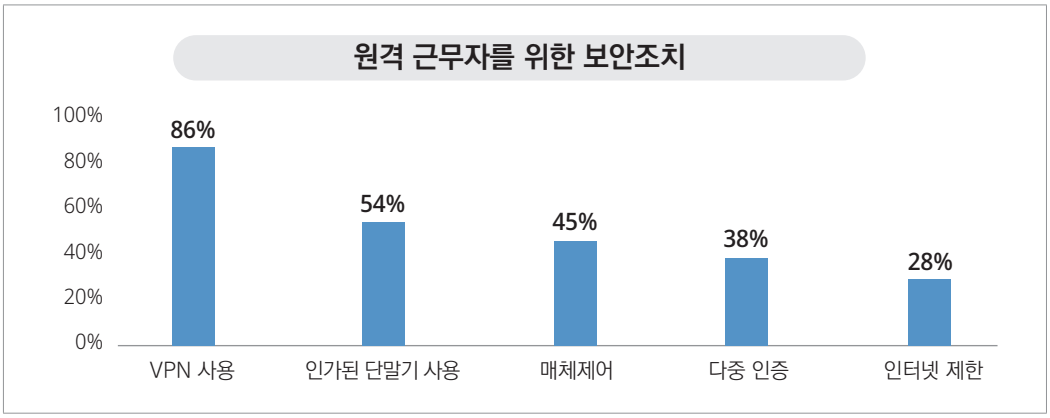
1 원격 근무

코로나19로 인하여 우리의 근무 환경은 변화되었다. 원격 근무가 활성화되었으며, 화상회의는 훨씬 친숙해졌다. 글로벌 리서치 기관 가트너(Gartner)에 따르면 코로나19 장기화로 인해 지난해 원격 근무는 전년 대비 41%나 높아졌으며, 2024년에는 전 세계 기업의 74%가 완전히 원격 근무로 전환될 것으로 전망했다. 대한상공회의소 조사에서도 코로나19로 비대면 원격 근무를 시행한 기업이 이전 대비 4배 이상 증가했다고 한다.

이러한 변화는 보안 위협 또한 증가시켰다. '2021 탈레스 글로벌 데이터 위협 보고서(2021 Thales Global Data Threat Report)'에 따르면, 약 47%의 기업이 지난 1년 동안 사이버 공격의 볼륨(또는 규모) 및 범위와 심각성이 증가했으며, 1년 이상 원격 근무 환경이 조성되고 있음에도 불구하고, 82%의 기업이 원격 근무 보안 위협에 대해 여전히 우려하고 있는 것으로 나타났다. 더욱이 46%의 기업이 자사의 보안 인프라가 코로나19로 야기된 위협에 대응할 준비가 되어 있지 않다고 밝혔다.

국내도 마찬가지다. 대부분의 기업은 방역을 위해 계획에 없던 원격 업무 인프라를 급히 구축했다. 때문에 원격 근무 장기화를 고려하지 않고, 기업 내부망에 원격 접속 수단을 연계하는 간단한 대응에 그친 곳들이 많다. VPN(가상사설망)이 대표적이다. 설문조사 결과,

원격 근무자를 위한 보안 조치로 'VPN 사용'은 86%로 높게 나타났지만 '매체제어', '인터넷 제한', '다중 인증'은 현저하게 낮았다.



공격자는 이러한 상황을 놓치지 않는다. 원격 접속 권한만 획득하면 기업 내부망의 각종 보안 솔루션을 우회하기 수월하다는 점을 공략하는 것이다. 최근 한국원자력연구원과 한국항공우주산업(KAI) 등 국가주요시설을 대상으로 VPN 취약점을 악용한 공격이 발생하여 이슈가 되었다. 보안기업 어베스트(Avast)에서는 원격 근무에 이용되는 직원의 VPN 계정 정보와 보안 취약점을 악용해 기업 내부망에 침투하여 특정 소프트웨어 제품 변조를 시도하는 사고가 발생하였다. 이는 기업 네트워크 경계가 집까지 확장되어 보다 주의 깊은 보안 조치가 필요하다는 점을 시사하고 있다.

원격 근무 위협에 대비하여 고려할 보안사항

기업

- **안전한 단말기 보안 정책 수립**
  - 업무용 단말기 반·출입 시 보안 점검 수행 및 이력 관리
  - 지급이 가능한 경우 보안 제품을 설치한 업무용 단말기 제공
- **안전한 네트워크 정책 수립**
  - 원격 근무자 일정 시간 부재 시 네트워크 차단
  - VPN 사용 등 안전한 네트워크 사용
    ※ VPN 미보유 기업의 경우 사내망 접속 최소화 및 백신 설치, 수시 점검 정책 수립
  - 원격 근무자의 사내 네트워크 접속 현황 관리 및 우회 접속 집중 모니터링 시행

• **중요 문서 등 데이터 보안 정책 수립**
  - 데이터 외부 전송 시 관리자의 승인 절차 수립
  - DRM 설정 등 암호화를 통해 데이터 유출 방지
  - 원격 근무자의 작업 파일 반입 시 악성코드 감염 여부 등 검사
  - 중요 데이터 주기적인 백업 및 관리

• **원격 근무자 대상 보안 인식 제고**
  - 사용 소프트웨어 최신 업데이트 권고
  - 공유기 패스워드 설정, 웹사이트 이용 자제 등 보안 교육 시행

• **원격 근무 사용자 계정 및 접근 권한 관리**
  - 원격 근무자의 비밀번호 설정 강화 및 접근 권한 최소화 방안 마련
  - 원격 근무 시스템 접근 시 OTP 등 다중 인증 적용

근무자

• **운영체제 및 소프트웨어 최신 업데이트**

※ 최근 발생하는 랜섬웨어 등 지능형 위협은 운영체제나 소프트웨어의 취약점을 이용함에 따라 운영체제를 포함한 모든 소프트웨어를 항상 최신의 상태로 유지하는 것이 중요

• **백신 프로그램 설치 및 최신 업데이트**
  - 백신 프로그램 자동 업데이트 및 실시간 검사 설정

• **불필요한 웹 사이트 이용 자제**
  - 업무상 꼭 필요한 경우를 제외하고 웹사이트 접속 및 사용을 자제

• **파일 다운로드 및 실행 주의**
  - 불분명한 출처 링크 클릭 및 파일 다운로드 주의
  - 공식적인 경로의 소프트웨어만 다운로드 및 설치

• **안전한 네트워크 사용**
  - 가정용 무선 네트워크 보안 설정 및 최신 업데이트
  - 개인 영업장(카페, 식당 등)에 설치된 사설 네트워크 사용 자제
  - 내부(사내) 네트워크 접속 시 VPN 사용 등 기업 보안 정책 준수

• **단말기 패스워드 및 보안 설정**
  - CMOS, OS 등 패스워드 설정 및 자동 로그인 제한
  - 화면보호기 설정

• **중요 문서는 별도의 저장장치에 주기적으로 백업**
  - 인가된 저장장치(외장하드, USB 등)를 이용하여 중요 문서 별도 저장
    ※ USB 저장장치 사용시, USB 자동실행 방지 및 자동 검사 설정
  - 상용 클라우드 이용 금지 등 데이터 복사 및 유출에 대한 대응책 적용

TIP

- **내 PC 돌보미***

  * 보호나라-https://www.boho.or.kr/webprotect/pcSecCheck.do

  - 사이버 위협에 즉각적으로 대응이 어려운 개인 PC 이용자를 위해 원격 보안점검 지원

- **비대면 서비스 취약점 점검***

  * 보호나라-https://www.boho.or.kr/webprotect/untactcon.do

  - 중소기업의 보안 강화를 위해 서비스(홈페이지·모바일앱) 및 기업 인프라 대상 보안 취약점 점검 지원

- **비대면 업무환경 도입·운영을 위한 보안 가이드*('20.6)**

  * 보호나라-https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=35467

- **원격수업 대비 지켜야 할 실천수칙*('20.4)**

  * 보호나라-https://www.boho.or.kr/cyber/protectionPractices.do

- **재택·원격근무 정보보호 6대 실천 수칙*('20.3)**

  * 보호나라-https://www.boho.or.kr/data/guideView.do?bulletin_writing_sequence=35319

2 공급망 공격

솔라윈즈(Solar Winds), 카세야(Kaseya) 등 최근 공급망 공격이 증가함에 따라 피해 또한 커지고 있다. 솔라윈즈 사태의 경우 악성 업데이트를 내려받은 고객사는 약 3만 3,000개며, 이 가운데 1만 8,000여 개 기업이 실제 피해를 당했을 것으로 추정된다. 공급망 공격은 보안 수준이 높은 정부 기관 또는 금융기관을 직접 공격하는 방법 대신, 공격 대상 기업들이 사용하고 있는 솔루션 공급자 또는 파트너사를 통한 우회 침투방안을 선택하고 있다. 따라서 파급력이 크고 대규모 피해를 발생시킨다. 아수스(ASUS) 소프트웨어 업데이트 시스템 해킹(2019), 솔라윈즈(Solar Winds) 공급망 공격 사태(2020), MS 익스체인지 서버 취약점(2021) 등이 대표적인 서드파티 소프트웨어를 통한 공격 사례이다.

최근 전 세계를 강타한 Log4j 취약점은 대부분 서버에 사용되고 있기 때문에 공격 파급 영향력이 매우 크다. 더구나 Log4j 사용 식별이 쉽지 않아 보안 업데이트 등을 통한 정상화까지 상당 기간이 소요될 것으로 예상된다. 여기에 공격자는 봇넷, 랜섬웨어, 크립토마이너 등 다양한 방법으로 악용하고 있어 글로벌 디지털 인프라를 흔드는 치명적인 위협으로 성장하고 있다. 이처럼 Java, WebLogic 등 널리 이용되는 소프트웨어의 취약점을 이용한 공격은 앞으로 한층 더 고도화 될 것으로 보인다. 앞으로 공격자들은 소프트웨어 취약점을 이용한 공급망 공격을 이어갈 것이며, 공격의 초기 진입점으로 이용할 것으로 보인다. 따라서 공급망 공격에 주의하기 위해서는 기업(기관)과 소프트웨어 개발 업체의 2가지 관점에서 보안 점검 사항 도출이 필요하다.

공급망 공격에 대비하기 위한 보안 점검 사항

소프트웨어 활용 기업(기관)

- **소프트웨어 실행 권한 최소화**
  - 소프트웨어 실행 권한 검토 및 필요 권한만 할당
- **안전한 계정 사용 및 관리**
  - 업데이트 파일 업로드 및 파일 동기화 소프트웨어의 불필요한 계정 삭제 및 안전한 패스워드 사용
- **업데이트 무결성 검증**
  - 실행 파일, 비실행 파일, 업데이트 정책 파일 등 업데이트 관련하여 무결성 검증
- **업데이트 서버 URL, IP 대역 및 포트(Port) 변조 확인**
  - 특정 주소만 활용하는지 확인 후 해당 네트워크 주소에서만 배포되도록 설정
- **시스템 이상징후 탐지 등 대응 프로세스 수립**
  - 사고 발생 시 신속한 대응을 위한 비상 연락망 구축
- **백신 프로그램 최신 업데이트**

소프트웨어 개발 업체

- **시큐어 코딩을 활용한 안전한 개발**
  - 소프트웨어 개발 주기 전체에서 시큐어 코딩을 활용하여 발생 가능한 취약점 제거
- **시스템 망 분리 및 접근통제**
  - 개발 시스템 망 분리 및 불필요한 포트(Port) 차단
  - 작업을 수행하는 시스템은 지정된 관리자 외 접근 차단
- **별도의 인증서 관리 시스템 사용**
  - 코드 서명 작업을 수행하는 시스템 및 인증서 관리 시스템은 일반 업무 PC와 혼용 금지
- **안전한 코드 서명 절차 수립 및 운영**
  - 인증서 사용 로그 기록 및 관리자 승인 절차 수립
- **배포 및 업데이트 파일 코드 서명**
  - 소프트웨어와 관련된 설정 및 설치 파일 등 모든 파일에 전자 서명 적용 및 확인
- **안전한 배포를 위한 SSL 등 암호화 적용**
  - 안전한 패키지화를 통하여 파일 배포 및 안전한 단말기에서 언팩하여 사용
  - 안전한 통신채널을 사용하여 소프트웨어 전달
- **취약점 관리 및 주기적인 업데이트 수행**
  - 배포한 소프트웨어에서 발견된 취약점 관리 및 패치 프로세스 운영

TIP

- **중소기업 SW 보안약점 진단***

  * 보호나라-https://krcert.or.kr/webprotect/securityWeakness.do

  - 기업이 보유한 SW의 소스코드 내 보안약점을 진단 및 제거 지원(출장형, 내방형)

- **SW 개발보안 교육***

  * https://academy.kisa.or.kr/main.kisa

- **보안 취약점 신고포상제(개방형 취약점 분석 플랫폼)***

  * 보호나라-https://www.boho.or.kr/consult/software/vulnerability.do

- **보안 취약점 신고포상제를 통해 알아본 놓치기 쉬운 취약점 사례별 대응방안*('21.2.)**

  * 보호나라-https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35907

- **모바일 딥링크(Deeplink) 취약점 관련 보안 조치 가이드*('21.5)**

  * 보호나라-https://www.boho.or.kr/data/guideView.do?bulletin_writing_sequence=35434

- **공급망 공격 사례 분석 및 대응 방안*('19.7)**

  * 보호나라-https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35089

3 클라우드 보안

디지털 전환이 가속화되어 클라우드 이용이 급속도로 확대되었다. 제조, 금융, 자동차, 의료, 통신 등의 산업계 전반에서 클라우드 전환이 발 빠르게 일어나고 있다. 글로벌 리서치 기관 가트너(Gartner)에 따르면 전 세계 클라우드 매출은 21년 4,080억 달러에서 22년에는 4,740억 달러로 증가할 것으로 전망된다.

그러나 보안에 대한 충분한 고려 없이 클라우드가 도입됨에 따라 기업들이 관련 보안 사고를 겪는 경우도 많아졌다. 클라우드 엔지니어링 전문가 대상 설문조사*에서는 36%의 기업이 지난 1년 사이 심각한 클라우드 데이터 유출이나 침해를 경험했다고 답했다. 최근 아마존(Amazon) AWS가 다운되어 트위치(Twitch), 줌(Zoom) 등을 포함한 수많은 온라인 서비스가 영향을 입었다. 국내에서는 야놀자, 스타일쉐어, 집꾸미기, 스퀘어랩, 샤넬코리아 등의 기업이 클라우드를 사용하다 개인정보 유출되는 사고를 겪었다.** 클라우드 관리자 접근 권한을 충분히 제한하지 않거나, 보안 취약점을 방치함에 따라 개인정보가 대량 유출되는 사고가 발생한 것이다. 이렇게 서비스 오류, 관리적 문제 등으로 클라우드 사고는 빈번하게 발생하고 있다.

* Fugue and Sonatype, State of Cloud Security 2021

** 출처: it.chosun, '잇단 고객사 정보유출 사고에 AWS 책임론 급부상', 2021.11.1

앞으로 클라우드 환경을 노린 공격은 점차 고도화되고 증가할 것으로 예상된다. 실제로 지난 9월 IBM에 따르면 클라우드에서 배포된 애플리케이션에서 발견된 취약점 수는 지난 5년 새 150% 급증했으며, 심각도도 보다 심화됐다. 설문조사 결과에서도 내년에 주목할 보안 이슈로 '클라우드 보안'이 높게 나타났다.

클라우드 보안을 위한 권고사항

- **안전한 사용자 패스워드 관리 절차 수립**
  - 숫자, 영문자, 특수문자 등 조합하고 주기적인 변경 필요
  - 이용자 패스워드 분실, 도난 시 안전한 재발급 절차(본인인증 등) 수립
- **안전한 계정 사용 및 관리**
  - 클라우드 접속 시 다중 인증 사용
  - 로그인 성공 또는 실패에 따른 모니터링 및 계정 잠금 사용
  - 자동 로그인 설정 제한 필요
- **업무의 정상화, 연속성 확보를 위한 백업 정책 수립**
  - 주기적인 백업을 통해 데이터 손실 최소화
- **데이터 유출 방지를 위한 보안 정책 수립**
  - 데이터 공유 방법에 대한 표준 및 가이드 마련
  - 클라우드에 데이터 저장 시 암호화 사용
  - 데이터의 중요도, 민감도에 따른 데이터 액세스 권한 차등 부여
- **클라우드 서비스 위협 점검 및 주기적인 검토 수행**
  - 클라우드 서비스에 대한 위협 점검 목록 작성 및 관리
  - 위협 점검 목록을 기반으로 지속적으로 위협 식별, 평가, 완화 필요

TIP

- **클라우드 서비스 보안인증제***

  * https://isms.kisa.or.kr/main/csap/intro

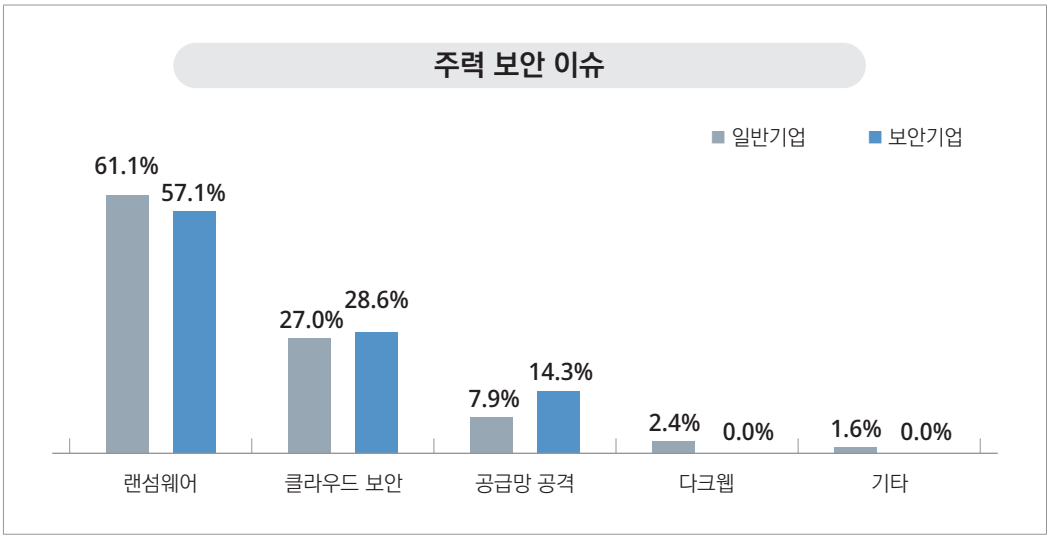
  - 정보보호 기준 준수 여부를 평가·인증하여 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 지원
- **민간분야 주요정보통신기반시설 클라우드 이용 가이드라인*('21.4)**

  * 보호나라-https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=36035
- **클라우드 취약점 점검 가이드*('20.12)**

  * https://isms.kisa.or.kr/main/csap/notice
- **클라우드 정보보호 안내서*('17)**

  * https://isms.kisa.or.kr/main/csap/notice

- **AWS 보안 가이드***
  * https://aws.amazon.com/ko/blogs/korea/improving-security-architecture-controls-for-wfh/
  * https://aws.amazon.com/ko/compliance/solutions-guide/
- **Azure 보안 가이드***
  * https://docs.microsoft.com/ko-kr/azure/security/fundamentals/
- **Docker 보안 가이드***
  * https://docs.docker.com/engine/security/
- **Google 클라우드 보안 가이드***
  * https://cloud.google.com/security?hl=ko
- **네이버 클라우드 보안 가이드***
  * https://www.ncloud.com/api/support/download/5/97
- **KT 클라우드 보안 가이드***
  * https://cloud.kt.com/solution/security/



CYBER SECURITY ADVISORY 2022

과학기술정보통신부

KISA 한국인터넷진흥원

AhnLab NSHC SECURITY INCA I.n.t.e.r.n.e.t ESTsecurity HAURI BITSCAN