2022년 정보보호 위협분석 및 2023년 전망

- 안정적인 기업경영을 위한 23년도 사이버위협 분석, 대응방안제시 -

코로나19 상황속에서 기업들은 불가피하게 재택근무를 하게 되는 정보기술 환경의 변화를 악용한 해킹공격이 증가하였고, 디지털금융의 확장으로 편리성이 증가하는 4차 산업혁명 중흥기에 비례하여 22년 한해동안 국가사회 혼란을 야기하는 사이버공격과 랜섬웨어 및 디도스 공격등이 증가하였습니다. 이에 최근 과학기술정보통신부(장관 이종호, 이하 '과기정통부'), 한국인터넷진흥원(원장 이원태)은 사이버 위협 인텔리전스 네트워크와 함께 사이버위협에 대한 선제적 예방 및 대응체계 강화를 위해 " '22년 사이버 보안 위협 분석과 '23년 사이버 보안 위협 전망"을 발표하였습니다. 이에, 과기부 발표자료와 함께, 국가정보원과 금융보안원 등 정보보호 주요기관 등에서 선정한 23년도 사이버위협 전망, 그리고 그 시사점을 종합적으로 살펴봅니다.

1. (과기정통부) '22년 사이버보안 위협 분석과 '23년 사이버보안 위협 전망

(1) '22년 사이버 보안 위협 분석

가. 국가・사회 혼란을 야기하는 사이버 공격

22년에 해외에서는 랩서스(LAPSUS$)그룹, 친 러시아 해킹 그룹 킬넷(Killnet)등 국제 해킹그룹의 지속적 공격 시도로 국제기업 및 정부기관이 피해를 입었고, 정부나 방송사 공식 SNS 계정을 탈취 및 악용하거나 판교 데이터센터 화재의 이슈를 이용하여 피싱 등 악성메일을 배포하는 것과 같이 국민적 관심이 있는 사건 사고를 사이버공격에 즉각 활용하는 양상을 보였습니다.

나. 재택근무, 인터넷기반자원공유 전환 등 정보기술환경 변화를 악용한 공격

코로나19 이후 근무환경 변화로 관리되지 않은 사용자 기기(노트북, 태블릿 등)를 악용하여 정보유출하는 사례가 증가하고 있고, 해외에서는 인터넷기반자원공유(클라우드) 환경에서 설정오류 또는 해킹공격으로 대량의 데이터가 유출되는 사고가 증가되고 있습니다.

다. 디지털 사회를 마비시키는 금품요구악성프로그램, 분산서비스거부 공격

22년의 한국인터넷진흥원에 접수된 침해사고 신고 중 29%가 금품요구 악성 프로그램사고 (랜섬웨어) 공격이고 그중 규모분류로는 중소기업이 88.5%, 업종별로는 40.3%가 제조업에 집중되는 것과 같이 보안수준이 높지 않은 기업을 대상으로 많은 공격이 발생하였습니다. 또한 분산서비스거부공격(DDoS)공격도 증가하였는데, 주로 IoT기기가 악성코드에 감염되어 공격에 악용되었습니다.

(2) '23년 사이버 보안 위협 전망

가. 국가・산업 보안을 위협하는 국제 해킹 조직의 공격 증가

우크라이나-러시아 전쟁이 장기화됨에 따라 국가가 지원하는 해킹조직의 활동이 증가하고, 국가 기반시설 또는 국제기업을 대상으로 하는 해킹 공격이 증가할 것이며. 또한 직접적인 수익을 위한 가상자산 관련(거래소, 전자지갑, 탈 중앙화 금융 등) 해킹사고 역시 증가할 것으로 예상됩니다.

나. 재난・장애 등 민감한 사회적 현안을 악용한 사이버 공격 지속

22년도의 판교 데이터센터 화재사건을 즉시 악성코드 유포에 활용한 것과 같이 23년도에도 사회적 이슈를 악용하는 사례가 증가될 것으로 예상됩니다. 기업들은 ICT 기술을 활용하여 업무를 수행함에 따라 이메일을 통한 공격과 같이 사회공격적 기법을 통한 공격이 지속될 것으로 예상됩니다.

다. 지능형 지속 공격 및 다중협박으로 무장한 금품요구악성프로그램 진화

과거 랜섬웨어는 이메일 첨부파일이나 인터넷 광고 링크등을 이용하여 사용자 PC에 감염시키고 대가를 지불하면 암호화를 풀어주는 형태 였지만, 최근엔 시스템의 취약점을 이용하거나 인증정보를 활용하여 내부 시스템에 직접 침투하여 정보탈취와 랜섬웨어 감염으로 파일 암호화, 그리고 백업 시스템과 로그 파일을 삭제하는 등의 지능형 지속 공격(APT: Advanced Persistent Threat)으로 진화 되고 있습니다. 또한 대가를 지불하면 암호화를 해제해 주던 방식에서 진화하여 사전에 수집한 내부 정보를 협박에 이용하거나 외부로 판매하는 등 다중협박 형태로 진화하고 있습니다.

라. 디지털 시대 인터넷기반자원공유 전환에 따른 위협 증가

다양한 기업과 정부 기관은 인터넷기반자원공유(클라우드)로의 전환을 서두르고 있습니다. 그에 따라 보안설정의 오류나 보안취약점을 악용한 사이버 위험은 증가될 것으로 예상됩니다. IT인프라 환경의 변화에 따른 기술적/관리적 관리방안이 체계적으로 수립되고 운영되어야 합니다.

마. 갈수록 복잡해지는 기업의 소프트웨어 공급망과 위협 증가

기업의 소프트웨어 개발 및 운영에서 오픈소스는 개발시간과 공수를 줄여주는 필수 불가결한 존재입니다. 최근 공격자들은 소스코드 공유사이트 내의 악성코드를 교묘히 삽입하는 사례가 증가되고 있습니다. 소프트웨어어의 안전한 개발과 운영을 위한 절차 마련이 필요합니다.

(3) '23년 사이버보안 대응 전략

COVID-19로 인한 비대면 근무 확산으로 기업의 보안 대상은 경계보안중심에서 개인단말기 중심 보안으로 변화 되고 있고, 제로트러스트[1] 보안이 부각됩니다. 또한 소프트웨어 개발부터 운영, 유지보수 등의 소프트웨어 공급 전단계를 관리하는 DevSecOps가 중요해 지고 있습니다. 최근 바이든 행정부에서도 사이버보안 개선에 대한 행정명령(EO14028, `21.5)를 발표하며 제로트러스트 구조를 요구하고 있고, 오픈소스의 안전한 개발 및 운영을 위한 출처를 명세하는 SBOM을 제공하도록 하는 등의 소프트웨어 공급망 보안 강화에 집중하고 있습니다. 고도화된 방어체계에서도 해킹사고 또는 오류로 기밀성, 무결성, 가용성이 저해될 수 있음으로 신속한 복구가 가능한 사이버 레질리언스[2] 대응체계를 도입할 필요가 있습니다.

---

[1] 제로트러스트(Zero Trust) : 변화하는 업무 환경의 사이버 위협에 대응하기 위해 최소 권한접근, 보안 가시성 확보등을 원칙으로하는 보안 패러다임

[2] 사이버 레질리언스(Cyber resilience) : 사이버탄력성 즉, 기존의 사이버보안을 넘어, 실패를 극복하고 지속적인 기업의 비지니시를 보장하는 차세대 방어전략

2. (금융보안원, 국가정보원, 민간정보보호전문업체) 선정 23년도 사이버위협 전망 및 키워드 비교분석

국내 정보보호 전문기관인 과학기술정보통신부, 국가정보원과 금융분야의 금융보안원에서 22년도를 사이버위협 현황을 정리하고, 23년도에 예상되는 사이버보안 이슈들을 선정하여 배포하였습니다.

발행기관	23년 사이버보안 위협 전망	키워드
과기정통부	국가・산업 보안을 위협하는 국제 해킹 조직의 공격 증가	국가 해킹 조직
	재난, 장애 등 민감한 사회적 현안을 악용한 사이버 공격 지속	사회공학
	지능형 지속 공격 및 다중협박으로 무장한 금품요구악성프로그램 진화	APT, 랜섬웨어
	디지털 시대 인터넷기반자원공유 전환에 따른 위협 증가	클라우드
	갈수록 복잡해지는 기업의 소프트웨어 공급망과 위협 증가	소프트웨어 공급망
금융보안원	사이버 공격 경로로 악용될 수 있는 엔데믹 취약점	새로운 공격기법
	랜섬웨어, 피싱 앱 등 사이버위협의 끝없는 진화	랜섬웨어
	오픈소스 이용 활성화와 강조되는 공급망 보안	소프트웨어 공급망
	디지털자산의 당면과제, 리스크 관리체계 마련	디지털 자산
	대세로 자리잡고 있는 클라우드와 보안 고려사항	클라우드
	인공지능 활용, 공정성, 보안성확보를 통한 이용자 보호 필수	인공지능
	디지털신원증명 활용에 따른 기대와 우려	디지털신원증명
	금융보안 규제 합리화, 전제되는 자율 보안	정부규제
	마이플랫폼 시대, 데이터 확보와 보호	데이터 보호
	금융권 채널 변화의 핵심 디지털연결	디지털 연결
국가정보원	첨단기술・안보현안 절취 목적의 사이버첩보 활동 심화	국가 해킹 조직
	사회 혼란 목적의 해킹 가능성 우려	사회공학
	공공・기업 대상 랜섬웨어 피해 확산 등 사이버 금융범죄 빈발	랜섬웨어
	용역업체・클라우드 등 민간 서비스를 악용한 공급망 해킹 지속	소프트웨어 공급망
	사이버억지 정책 회피 목적의 다양한 해킹수법 출현	새로운 공격기법
정보보호 전문기업 (이글루 코퍼레이션)	사이버 공격의 서비스화와 랜섬웨어 생태계 확장	랜섬웨어
	오픈소스 생태계로 인한 보안 위협 진화	오픈소스
	위협의 체인화, 공급망 공격 증가 추세	소프트웨어 공급망
	가상화폐의 불확실성 증가, 가상화폐 타겟팅 사이버 공격 확산	디지털 자산
	국제정세 불안, 국가 사이버 안보 위협 증가	국가 해킹 조직

23년도 사이버보안의 주된 키워드는 '국가 해킹조직', '랜섬웨어', '소프트웨어 공급망', '클라우드' 였습니다. 1) '국가 해킹 조직'은 국가가 지원하여 고도화된 기술과 대규모의 자원을 보유한 해커그룹으로써, 작게는 가상화폐 거래소나 기업의 정보유출을 수행하지만 크게는 국가 기반시설을 마비시켜 사회전체를 혼란에 이르게 하는 사이버 위협입니다. 2) '랜섬웨어'는 전통적으론 IT 시스템을 암호화하여 사용할 수 없도록 한 뒤 금전을 요구하는 공격 유형이나 최근엔 해킹 과정에서 수집한 정보를 별도로 판매하여 추가 수익을 올리거나 정보유출 사실을 미끼로 추가 금전을 요구하는 형태로 발전하고 있습니다. 3) '소프트웨어 공급망'은 소프트웨어 개발 및 활용에 있어 악의적인 사용을 제거하기 위하여 초기부터 관리되어야 하며 관련된 위협은 증가되고 있습니다. 4) '클라우드'는 대다수의 주요기업의 IT시스템이 클라우드로의 전환이 가속화되어 사용자 설정 오류, 자체보유 취약점 조치 등의 위협 증가가 예측되고 있다는 의미입니다.

3. 시사점

23년도 사이버위협 전망으로 통해 확인된 바와 같이, 멀티 디바이스를 운영하는 환경에서 개인 디바이스 측면의 보안인 제로트러스트보안과 국민의 생활과 밀접한 관계에 있는 기반시설의 중단에 신속한 복구에 중점을 둔 사이버레질리언스 대응체계의 도입 및 적용이 중요해졌습니다. 이를 위해 개별적인 대응보다는 조직화되고 체계적인 정보보호 대응을 통해서 선제적으로 대응하는 것이 필요하며, 기존에 규제기관 대응이라는 수동적 업무방식을 뛰어넘어서 사전에 정보보호 법률과 기술대응체계에 대한 취약점 점검 등을 통해 능동적인 정보보호 대응체계를 구축할 필요가 있습니다.

화우 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 제공하고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

Contacts

이근우 파트너변호사
T. (+82) 2 6003 7558
E. klee@yoonyang.com

석제범 고문
T. (+82) 2 6182 8147
E. jbseok@yoonyang.com

이광욱 파트너변호사
T. (+82) 2 6003 7535
E. kwlee@yoonyang.com

이수경 파트너변호사
T. (+82) 2 6182 8132
E. sgyi@yoonyang.com

백재환 전문위원
T. (+82) 2 6182 8366
E. jhb@yoonyang.com

지재원 연구위원
T. (+82) 2 6003 7568
E. jwji@yoonyang.com