SHIN&KIM
법무법인(유) 세종

2025년 사이버위협 전망 및 대응 필요성

2024.12.27

과학기술정보통신부와 한국인터넷진흥원은 2024년 12월 18일 AI 활성화에 따른 부작용 중 하나인 사이버 위협에 대해 기업이 선제적으로 예방하고 대응 체계를 강화할 수 있도록 「2025년 사이버 위협 전망」을 발표하였습니다. 해당 보고서는 점차 지능화, 고도화되고 있는 사이버 위협에 체계적으로 대응하기 위해 2024년 발생한 사이버 위협 사례를 선정·분석하고, 2025년에 발생할 수 있는 주요 사이버 위협을 전망하였습니다.

2024년 사이버 위협 사례	① 사이버 사기(쓰레기 편지, 금융 사기, 큐알사기 등)로 인한 국민 피해
	② 소프트웨어 공급망 공격 등 복합적인 공격 전술 사용
	③금품요구 악성 프로그램(랜섬웨어) 공격기법 고도화
2025년 사이버 위협 전망	① 공격자의 생성형 인공지능 활용 본격화
	② 디지털 융복합 체계에 대한 사이버 위협 증가
	③ 국제 환경 변화에 따른 사이버 위협 증가
	④ 무차별 (분산 서비스 거부)디도스 공격 증가

1. 2025년 사이버 위협 전망

(1) 공격자의 생성형 인공지능 활용 본격화

- 특정 소프트웨어와 경로를 통해서만 접근 가능한 네트워크인 다크웹에서 FruadGPT(사기), WormGPT(악성코드 생성) 등 사이버 범죄에 특화된 악성 생성형 인공지능이 본격적으로 활용될 수 있음
- 공격자는 ChatGPT 등 검증된 서비스를 활용한 스피어 피싱(spear phishing)* 메일을 작성하거나 공격 도구(취약점 탐색, 침투 등)를 개발할 수 있음

  * 특정 개인 또는 그룹을 대상으로 메일을 보내 가짜 사이트로 유도하여 악성 코드를 설치하게 하거나 ID/패스워드를 입력하도록 하여 네트워크에 침입하는 피싱 공격으로, 공격자는 의도한 대상을 조사하고 피해자가 믿을 만한 구실을 제공하기 때문에 피해 발생 가능성이 더 높음

- 온라인에 공개된 동영상, 사진 등을 활용하여 딥페이크(deepfake) 영상을 제작하고 피해자를 협박하거나 사회적 여론을 조작하는

등 개인적 피해, 사회적 갈등을 야기할 가능성이 우려됨

* 인공지능 기술로 영상, 이미지 등을 조작하여 사실처럼 보이게 만드는 합성 기술

(2) 디지털 융복합 체계에 대한 사이버 위협 증가

- ICT 발전으로 스마트 팜, 자율주행차, 스마트 빌딩, 스마트 교통 시스템 등 산업 전반에 걸쳐 디지털 전환이 가속화되고 있는 가운데, 5G 등 이동통신망 기반의 융합 제품 및 서비스에 대한 보안 위협이 증가할 것으로 예상됨
- 이용자의 일상생활과 다양한 산업 분야에 보급된 사물인터넷(IoT) 기기 중 보안이 취약한 기기를 탐색하여 악성코드를 감염시키고 이를 봇넷(botnet)*으로 활용하는 등 디도스(DDoS, 분산서비스거부) 공격**과 같은 사이버 공격에 악용할 우려가 있음

  * 2024년 9월 중국 해킹그룹 플랙스 타이푼이 전 세계 26만대 IoT 장비로 구성된 봇넷을 운영하고 있는 것이 적발된 바 있음

  ** 악성코드에 감염된 단말기를 통해 대규모 트래픽을 발생시켜 기업에서 운영 중인 서버의 자원이나 네트워크 대역폭을 고갈시키는 전통적인 사이버 공격 방식

(3) 국제 환경 변화에 따른 사이버 위협 증가 가능성

- 글로벌 이슈, 전쟁, 정치적 갈등이 심화될 경우 특정 국가나 단체를 겨냥한 핵티비스트(hacktivist: hacking + activist)의 사이버 공격 활동이 심화될 수 있음 특히 미국의 (친)가상자산 정책으로 비트코인 가치 변동성이 확대됨에 따라 가상자산 사업자 및 이용자, 거래소, 블록체인 기업 등에 대해 공격이 집중될 것으로 보임
- 양자 기술, 인공지능 등 신흥 기술이 국가 경쟁력을 결정 짓는 핵심 요소로 부상함에 따라 원천 기술 보호의 중요성이 강조되고 있는 가운데, 원천 기술을 절취하기 위해 보안이 취약한 협력사 등 기업들을 대상으로 한 사이버 공격이 증가할 것으로 예상됨

(4) 무차별 디도스(DDoS) 공격 증가 예상

- 정치적 이념 등 다양한 목적을 가진 핵티비스트의 무차별적인 디도스(DDoS) 공격으로 서비스 중단이 빈번하게 발생하여 기업의 신뢰도 하락이나 재정적 피해가 더욱 심각해질 것으로 예상됨 다크웹에서 서비스형 디도스(DDoS-as-a-Service) 도구가 판매되는 등 기술적 지식이 부족한 일반 사람도 디도스(DDoS) 공격을 시도할 수 있는 환경이 조성됨에 따라 사이버 공격으로 인한 피해는 정부 공공 및 민간 기업을 가리지 않고 지속 증가할 것으로 보임

  * 비용을 지불하면 누구나 구축된 인프라를 통해 디도스(DDoS) 공격을 실행할 수 있는 서비스

2. 시사점

- 데이터 활용을 전제로 한 생성형 인공지능이 또 다른 측면에서는 사이버 보안에 최대 위협으로 작용할 것이 우려되는 가운데 미래에는 사이버 위협이 사전 예측이 어려운 형태로 발전하여 개인 및 기업 등에 심각한 피해를 야기할 것으로 전망됩니다.
- 이에 생성형 인공지능을 이미 도입하였거나 도입하고자 하는 기업은 안전한 생성형 인공지능 사용을 위해 기술 도입 단계에서부터 데이터 보안을 내재화하고 생성형 인공지능이 사용되는 전 단계를 포괄하는 상시 모니터링 체계를 구축하여 지속적으로 점검할 필요가 있습니다.
- 잠재적인 사이버 위협으로부터 기업이 보유하고 있는 중요 시스템 및 데이터를 효과적으로 보호하기 위해서는 전사 차원에서 사이버 보안 사고를 사전, 사후적으로 관리하는 조직의 능력(사이버 회복탄력성, Cyber Resilience)을 강화하는 것이 필요합니다. 이를 위해서는 데이터 처리 전 단계에 걸쳐 데이터 처리 흐름(flow)을 파악하기 위해 지속적으로 모니터링하고, 기업 특성에 맞는 보안 조치, 업계 표준 및 내부 규정 등을 정비해 두어야 할 것입니다.

About Shin & Kim’s ICT Group 개인정보데이터팀, AI센터

법무법인(유) 세종은 개인정보 보호 및 데이터 시큐리티 분야에 차별화된 전문성과 인적 네트워크(윤종인 전 개인정보보호위원회 위원장, 최재유 전 과학기술정보통신부 차관, 최광희 전 한국인터넷진흥원 실장 등)를 보유하고 있으며, 기업들을 위하여 개인정보보호법과

GDPR을 비롯한 국내외 개인정보 규제 자문, 개인정보 유출사건 대응, 개인정보 컴플라이언스 체계 수립, 데이터 보안 체계 구축 등 개인정보보호에 관한 전문적인 자문을 제공하고 있습니다. 이에 더해 개인정보 보호법 제2차 개정 및 하위법령 제정, 관련 제도개선에 있어 법무법인(유한) 세종 ICT그룹은 TMT, AI 및 사이버 보안 분야의 규제 및 비즈니스 리스크 최소화를 위해 전문적, 체계적으로 대응해 오고 있으며, 가명정보, 데이터 활용, ICT 산업 전반에 대한 규제 동향 파악 및 대관, 입법컨설팅, 규제영향력 분석과 기업의 전략 수립 등에 대한 전반적인 법률자문을 제공하고 있으므로, 보다 전문적인 내용이나 궁금하신 사항이 있으면 언제든지 연락 주시기 바랍니다.

관련구성원

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

장준영
변호사

02-316-4985
jyojang@shinkim.com

노진홍
변호사

02-316-1639
jhnoh@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

허민도
변호사

02-316-1987
mdhur@shinkim.com

최선웅
변호사

02-316-7951
swchoi@shinkim.com

최광희
고문

02-316-4651
khchoi@shinkim.com