법무법인(유) 화우
YOON & YANG

LEGAL UPDATE
정보보호센터
Feb. 2023

금융보안 환경 변화와 정보보호

- 금융보안 규제동향과 대응방안 -

독일의 보안개발자 블라디미르 팔란트 (Wladimir Palant)는 자신의 블로그를 통해 한국에서 사용하는 어플리케이션을 분석한 결과 다양한 보안상 문제점이 존재함을 발견하였고, 인터넷 뱅킹에서 사용하는 어플리케이션 2종에 대한 취약점을 공개함에 따라 한국 금융보안 분야에 이슈가 되고 있습니다.

현대의 금융환경은 핀테크(FinTech)의 발전으로 인한 편리함 이면에 사이버 보안 측면의 위협은 증가되고 있는데, 금융보안 분야의 사이버 위협 최신동향을 알아보고 금융분야 규제기관 동향과 기업 ESG(Environmental, Social, and Governance) 측면에서 정보보호의 중요성과 함께 현재 금융기업들의 정보보호 최신 대응현황 등을 종합적으로 설명드리겠습니다.

1. 진화하는 금융분야 사이버 위협

금융분야는 빅데이터, 블록체인, 클라우드등의 ICT기술의 발전과 COVID-19의 팬더믹이 더해져 비대면 업무 환경으로 금융보안 환경에 급격한 변화가 이루어지고 있는 가운데 디지털 발전과 사이버 보안 사이의 기술격차로 인해 은행이 민감한 데이터를 관리함에 있어 위험한 상황에 노출되고 있습니다. 글로벌 사이버 경제 리서치 기업인 Cybersecurity Ventures에 따르면 전 세계 사이버 해킹피해 규모는 2025년까지 연간 10조 5천억 달러에 이를 것으로 추정하고 있고, 금융보안원에서는 국내 소매금융 취급 은행 17곳이 17~21년 받은 사이버 공격은 109만1천606건으로 매일 598건의 사이버 공격이 발생되고 있다고 밝혔습니다.

진화하는 금융분야 사이버 위협에 대하여 금융보안원에서는 2023년도 디지털 금융의 사이버보안을 예측해 볼 수 있는 '2023년 디지털금융 및 사이버보안 이슈 전망 보고서'를 발간하였습니다. 총 10개의 항목으로 구성되어 있고, 주요 내용은 아래 표와 같습니다.

항목	주요 내용
1. **사이버 공격 경로**로 악용될 수 있는 **엔더믹 취약점**	엔더믹 취약점(Endemic Vulnerability)은 보완조치가 이루어지지 않아 장기간 악용될 가능성이 있는 취약점을 말하며 대표적인 예로는 2021년 말 알려진 Log4j가 있습니다. 취약점을 빠르게 발견하고 조치하는 절차가 중요합니다.
2. 랜섬웨어, 피싱 앱 등 **사이버 위협의 끝없는 진화**	서비스형 랜섬웨어(RaaS)의 보편화, 국가 배우 공격 그룹의 활동 증가의 사이버 위협 디지털 금융환경, 디지털 기술 등을 악용하며 진화하고 있습니다. 제로트러스트(Zero Trust)로의 보안 패러다임 전환이 대두되고 있습니다
3. **오픈소스** 이용 활성화와 강조되는 **공급망 보안**	오픈소스 사용 빈도 증가 및 복잡한 소프트웨어 구조를 기반으로 사이버 위협이 심화되고 있음으로 소프트웨어 자재명세서(SBOM)으로 안전한 오픈소스 및 소프트웨어 공급망을 관리할 필요가 있습니다.

4. **디지털자산**의 당면과제, **리스크 관리체계** 마련	디지털 자산의 가치 상승에 따라 거래소, 전자지갑등 대한 사이버 공격이 급증하고 있습니다. 관련 사업자 자체적으로 위험평가, 비즈니스 연속성 계획수립 등 리스크 관리를 수행해야할 필요가 있습니다.
5. 대세로 자리잡은 **클라우드**와 **보안 고려사항**	클라우드는 금융권 핵심 인프라로 자리잡고 있지만 보안사고가 지속적으로 발생되고 있습니다. CSPM(Cloud Security Posture Management)등의 통합 모니터링 및 관리 기능이 강조되고 있습니다
6. **인공지능 활용**, 공정성, 보안성 확보를 통한 **이용자 보호 필수**	금융권내 다양한 분야에서 AI가 활용되고 있으나 편향된 데이터를 학습하거나, 부족한 학습데이터로 인해 신뢰성에 문제가 발생할 수 있습니다. 데이터 결합 후 재사용, 공동 AI 데이터셋 구축과 AI 기술로 인한 차별을 방지하는 규제가 필요합니다.
7. **디지털 신원증명** 활용에 따른 기대와 우려	코로나 19 이후 인터넷 뱅킹등 금융거래에 분산신원증명(DID:Decentralized IDentifier)과 같은 비대면 신원증명 방식이 활용되고 있으나 개인정보 유출, 해킹, 신원도용의 문제, 새로운 인증 방식에 따른 보안 위협이 발생등의 우려가 존재합니다.
8. 금융보안 **규제 합리화,** 전제되는 **자율 보안**	금융권의 빅데이터, 인공지능, 오픈 API, 클라우드 활용등 ICT 기술을 활용한 디지털 전환을 추진중이나 기존 규제로 인해 어려움이 존재한다는 의견이 제기되고 있습니다. 금융규제 샌드박스 운영을 통해 규제 합리화를 기대하고 있습니다.
9. **마이플랫폼** 시대, **데이터** 확보와 보호	개인별 맞춤형 금융/생활 서비스를 제공하는 마이플랫폼(My Platform)시대는 양질의 개인정보가 대량으로 집중/융합됨으로 데이터 확보 경쟁 및 독과점 이슈가 발생될 가능성이 있습니다. 금융 소비자 권리 보장과 개인정보 이용 원칙에 기반한 정보보호활동이 필요합니다.
10. 금융권 **채널** 변화의 핵심 **디지털 연결**	고객 스스로 디지털 기기를 이용하여 업무를 볼 수 있는 무인(혁신)점포가 등장하였으나, 혁신 점포내 돌발 상황으로 인한 서비스 지연, 셀프 서비스 기기대상 사이버 위협, 디지털 연결에 따른 리스크 전이 등 발생 가능한 보안 위협 검토 및 대응방안 마련이 필요합니다.

<출처: 금융보안원2023년 디지털금융 및 사이버보안 이슈 전망 보고서 주요내용>

2. 금융보안 분야 정책 및 규제 동향

23년 금융보안분야 규제는 전자금융, 데이터, 디지털자산, 온라인 플랫폼, 정보통신 서비스 등의 분야에서 다양한법령 및 제도 변화가 예상됩니다.

가장 주의 깊게 지켜봐야하는 제도 변화는 금융위원회에서 지난 22년 12월 발표한 '금융보안규제 선진화 방안'입니다. 주요 내용은 CISO의 권한을 확대하고 금융회사 자체적으로 보안리스크를 분석하여 대응하는 '자율보안체계'로의 전환을 추진하는 '△ 보안거버넌스 개선', 금융회사의 안전성 확보의무사항의 세부사항은 규제가 아닌 가이드 형태로 전환하는 등의 사후 책임을 강화하는 '△ 보안규제를 정비', 보안규정 위반여부를 감독중심에서 자율보안체계의 검증 중심과 보안 거버넌스 구축을 위한 컨설팅 기능을 강화하는 '△ 관리/감독 선진화'입니다. 그 중 가장 핵심은 '자율보안체계 로의 전환' 입니다. '자율보안체계로의 전환' 은 '뉴욕주 금융사이버보안 규정(23 NYCRR 500)', '유럽은행감독청(EBA) 내부 거버넌스 가이드라인' 그리고 '유럽연합 PSD2의 전문인배상책임보험 최저보상한도 산출기준' 등의 컴플라이언스와 NIST RMF(Risk Management Framework)기반의 보안 체계 적용으로 금융사 자체적으로 보안리스크를 분석/판단하고 리스크에 비례한 보안체계를 수립하는 것을 필요로 합니다. 따라서 '자율보안체계로의 전환"은 자연스럽게 금융 정보보호 분야의 다양한 변화 및 투자 확대를 동반할 것입니다.

다음으로 23년도에는 연구·개발 분야에 대한 망분리 규제 완화 등 전자금융감독규정 개정안이 시행됨에 따라 금융 분야의 오픈소스 활용이 보다 확대될 것으로 예상됩니다. 그에 따라 금융보안원에서는 '오픈소스 소프트웨어 활용관리 안내서'를 배포하였습니다. 주요 내용으로는 '오픈소스 소개', '오픈소스 보안성 관리', '오픈소스 세부 관리 절차', '자가점검 체크리스트 등'입니다. 해당 안내서는 비규제 성격으로 금융회사의 자율보안체계 강화 및 안전한 오픈소스 활용에 도움이 될 것으로 기대 됩니다.

마지막으로 금융분아 정보통신 서비스를 위하여 '데이터센터 안전성 확보 관련' 개정 법률이 시행 예정입니다. '데이터센터 안전성 확보' 관련 법률은 판교 데이터센터 화재로 인한 금융 서비스 제공 안정성을 제고하기 위한 법안들로 방송통신서비스 긴급복구를 위한 정보체계의 구성과 물리적/기술적 보호조치를 추가하는 '방송통신 발전 기본법', 부가통신사업자에게 서비스 안정수단 확보 이행 관련 자료를 과학기술정보통신부장관에게 제출하게 하는 '전기통신사업법', 집적정보통신시설, 정보통신서비스 제공에 대한 사전점검, 사고 발생후 신고를 과학기술정보통신부장관에게 하도록 하는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'입니다. 언급된 법령은 정보통신 서비스의 안정성에 도움이 될 것으로 기대됩니다.

디지털 금융 관련 사항은 아래 뉴스레터를 참고하시길 바랍니다.
* 디지털 금융 법령/제도 변화 관련 참고(2022. 12 뉴스레터) ☞ 2023년 디지털금융 법령·제도 변화

3. 기업ESG와 금융 정보보호

정보보안은 ESG 관점에서도 금융업계의 주요 이슈입니다. 지난해 개정한 한국ESG기준원의 평가 기준이 되는 ESG 모범규준에서도 정보보호 영역에서 정보보안 거버넌스 구축, 개인정보 수집 및 활용, 개인정보 보호 활동 공개와 정보 주체 권리 보장에 관한 내용을 담았고, 해외 ESG 공시 기준에서도 정보보안 관련 정보를 중요하게 보고 있습니다. 특히, 지속가능성회계기준위원회(SASB)에서는 고객 개인 정보와 데이터 보안과 같은 보안 이슈를 중요한 지표로 언급하고 있는데, 이는 정보 보안 사고나 관리 수준이 기업 재무성과에 영향을 미칠 수 있기에 투자자들이 살펴봐야 할 '리스크 데이터'라는 것을 의미합니다.

실제 메타 플랫폼스는 2016년부터 2021년 사이 3차례 발생한 개인정보 유출로 인해 MSCI의 ESG 평가에서 최하등급 전 단계인 B등급을 받았고, 2019년에는 개인정보 유출 논란과 프라이버시 보호 노력에 대한 불확실성을 이유로 S&P ESG 지수에서 퇴출당하기도 했습니다. ESG 평가기관 관계자는 데일리임팩트에 "IT업계에 못지 않게 금융에서도 고객 자산, 부채 등 민감한 신용 정보를 다루기에 정보 보안은 중요한 ESG 이슈"이며 "사고 발생 시 평가 감점 요인이 될 수 있기에 정보보호 책임자 선임 및 정보 보안 리스크 관리 체계 구축을 위해 노력할 필요가 있다"고 설명하고 있습니다.

4. 마치며

이복현 금융감독원장은 22년말 금융 정보보호 관련 컨퍼런스에서 "기존의 금융 보안 안전망으로는 더 이상 안심할 수 없다"며 "정보보호최고책임자(CISO)를 포함한 경영진이 자체적으로 정보보호 진단을 시행하고, 취약요인을 개선하는 등 사이버 보안 위협에 대한 대응 역량을 강화해야 한다"고 말했습니다. 실제 금융권에서 사이버 공격은 빈번히 일어나고 있고, 금융보안원 발표에 따르면, 국내 소매금융 취급은행 17곳이 2017년~2021년 받은 사이버 공격은 109만1606건으로, 일 평균 598건이 발생하는 셈인데, 발생 건수 또한 매년 증가하고 있습니다.

특히, 스마트뱅킹이 보편화 됨에 따라 각 은행들은 각자의 방식으로 대응책을 마련하고 있습니다. △신한은행은 기존 정보보호활동과 더불어 임직원의 업무용 PC를 악성코드 감염으로부터 대응하기 위한 제로트러스트(ZeroTrust) 기반의 솔루션을 도입하고, 재택근무자에 대한 정보보안을 강화하기 위한 수단으로 안면인식 보안 시스템을 적용하였습니다. △우리은행은 금융보안원과 함께 보안 취약점을 찾기 위해 버그바운티(Bug Bounty)를 수행하여 잠재적 취약점을 선제적으로 발견하며 클라우드 국제 표준 보안 인증인 ISO 27017을 취득하는 등의 보안을 강화하고자 노력하고 있습니다. △NH농협은 사이버 보안위협에 대응하고자 인공지능기반의 보안관제 체계 구축과 더불어 보안 업무 자동화 체계인 SOAR(Security Orchestration, Automation & Response)시스템을 도입하여 업무 효율성을 재고 하고 있습니다.

이처럼 금융사들이 제로트러스트(ZeroTrust), 버그바운티(Bug Bounty) 등의 다양한 노력을 기울이고 있지만 절차적, 기술적 취약점은 꾸준히 발견되고 있습니다. 디지털금융의 발전으로 사이버 공격 발생 횟수의 증가, 공격 대상의 다각화, 공격 기법의 고도화로 체계적이고 종합적인 보안대책이 중요하며, 그에 맞는 합리적인 규제와 법과 기술이 융합된 종합적인 대응전략이 필요합니다.

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

김용태 고문
T. (+82) 2 6003 7043
E. kimyt@yoonyang.com

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

주민석 파트너변호사
T. (+82) 2 6003 7521
E. msjoo@yoonyang.com

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

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