1회 1주차 본문 → suns_min1025

Q.[정보보안] 랜섬웨어 대응을 위한 다양한 방안이 발표되었다. 다음에 대해 설명하시오.

A. 가) 랜섬웨어 특징

대상의 변화	개인 PC에서 높은 몸값을 지불할 능력이 되는 대기업, 사회기반시설, 생활필수 산업으로 표적이 옮겨지고 있음
공격기법의 고도화	피싱 이메일, 감염된 웹사이트에서 원격 데스크톱, 알려진 소프트웨어 취약점을 악용하는 등 공격 방식이 다른 사이버 위협과 융합되고 있음
서비스형 랜섬웨어 (RaaS)의 활성화	랜섬웨어가 전문 조직에 의해 제작되어 판매되면서 전문지식이 없는 공격자도 비용만 지불하면 랜섬웨어 공격을 할 수 있도록 서비스형으로 진화되었음
랜섬웨어의 가상화폐	가상화폐 등장으로 기존의 금융 시스템을 거치지 않더라도 금전 거래가 가능하고 익명성까지 보장하고 있어 랜섬웨어의 좋은 플랫폼 역할을 하게 됨

- 주요전파경로

구분	악성코드 경유 홈페이지 방문	이메일, SNS	시스템, NW, SW보안 취약점
감염경로	악성코드 설치된 홈페이지 접속시 악성코드 감염	이메일 - 첨부파일 실행 SNS - 링크 등을 통한 악성코드 실행·감염	취약점을 이용한 침투, 악성코드 설치
원인	OS 보안패치 미적용, SW 취약점 방치 등	이용자 보안인식 미비, 실수 등	운영·관리 체계 미비, 이용자 교육부족 등

나) 백업 유형 및 백업 정책 수정 방안

구분	백업 방법
TAPE 백업	각 시스템의 데이터를 백업 TAPE에 복제할 수 있음, 외부 저장소가 필요하다는 지속 소산보관이 용이
Cloud 백업	외부 영역에 데이터를 백업하는 방식, 외부 소산 관리가 용이하며, 보안서비스를 제공받을 수 있는 장점이 있음
NAS 백업	NAS백업 기술의 고도화로 자체 Cloud 백업 구성 및 별도 백업 기능 보유
USB 외장디스크	별도의 백업 소프트웨어 없이 사용자가 직접 백업 계획을 수립하고 수동 백업 수행

백업정책은 백업 대상에 따라 시스템 백업, 데이터 백업, 환경설정 백업 등으로 목적에 따라 다양한 방식이 있으며, 외부의 영향으로부터 백업 데이터의 안전성 확보를 위해 다중 백업을 실시하더라도 최근 악성적 목적의 랜섬웨어로부터 중요 데이터를 안전하게 보호하기 위해서는 소산백업 이후 네트워크를 분리하여 보관해야한다.

다) 랜섬웨어 예방 강화 전략

- 모든 소프트웨어에 최신 패치 및 업데이트 적용
- 가능한 2단계 인증 및 암호화 사용
- 효과적인 백업 및 재해복구 대책 마련
- 직원에게 최신 사이버 위협과 이를 방지하기 위한 방법을 교육
- 사이버 보안 정책의 모범 사례를 거버넌스 구현

전과정으로 조직 내에서 랜섬웨어를 대응하기 위한 방안은 기본적인 사이버 보안 정책을 잘 따르는 것이다. 또한 랜섬웨어 사고를 인지하면 신고도 매우 중요하다. 최근 경찰청에서 랜드크립 랜섬웨어 유포자를 검거한 사례처럼 사고 발생 시 관련 기관에 적극적으로 신고하여 유사피해를 막아야 한다.

1월 1주차 논문 → suns_min1025

Q. [금융논문] 디지털 금융이 금융환경에 미치는 영향과 발전방안

A. 코로나19 확산 이후 대면서비스가 위축되면서 코로나 이전부터 진행되던 투자환경과 함께 금융의 디지털 혁신이 가속화되었다. 특히 금융부분에서 모든 뱅킹, 암호자산 등 산재되어 있던 새로운 금융서비스가 등장하고 아마존, 구글 등 비금융 빅테크 기업이 제공하는 결제, 송금 등 금융서비스도 점차 확대되었다. 이에 본고는 디지털 금융이 금융환경에 미치는 영향과 발전방안에 대하여 알아보고자 한다.
최근의 금융혁신은 비금융 IT 회사가 지급결제·송금, 자금중개, 금융투자 등의 금융서비스 제공을 확대하면서 금융회사와 핀테크 또는 경쟁하는 협력의 금융산업 구조가 변화되었다.

· 비금융 IT 회사 (핀테크 기업, 빅테크 기업)

핀테크 기업은 금융회사와 협업하여 기존에 제공되던 금융서비스에 자신의 디지털 전환 선기술을 접목하는 방식으로 고객에게 금융회사보다 편리하고 간편한 금융서비스를 제공하고 있다. 핀테크 기업은 지급결제·송금, 대출, 자산관리, 보험 등의 서비스를 대상으로 경쟁력 있는 불야이 특화시킨 영업모델 형태를 보유하고 있다. 서비스 제공이 증가함에 따라 금융회사의 기능이 분야별로 대체되면서 오픈 뱅킹 시스템 도입, 핀테크 투자 급증 등 불확실한 현상이 가속되고 있다.
빅테크 기업은 전자상거래 플랫폼을 보유하여 고객 데이터를 빅데이터, AI 등의 기술로 활용해 분석한 후 고객맞춤형 금융상품을 판매하는 방식으로 금융서비스를 제공하고 있다. 전자 상거래 플랫폼의 일부로 지급결제서비스를 제공하게 시작해 대출, MMF 등 자산관리서비스, 보험상품 판매 등 영업 범위를 확대하여 금융거래 디지털 플랫폼 형태로 전환하였다.
기존 플랫폼에 기반한 네트워크 효과를 통해 금융서비스 제공이 비교적 확대되면서 운영 등 금융회사에 대한 잠재적 위협요인으로 부상되었다.

· 금융회사 (은행, 증권사, 보험사)

금융회사는 핀테크 기업과 제휴를 확대하는 한편 IT 기업의 금융서비스에 대응한 경쟁력을 제고하기 위해 자사 금융서비스에 디지털 전환 선기술을 융합하기 시작했다. 기존 은행과 달리 비대면 디지털 채널만 운용하여 금융서비스를 저렴하게 제공하는 인터넷전문은행 (네오뱅크)을 설립하기 시작했다.
증권사의 경우 알고리즘 매매 비중이 높아지고 자동화된 고객 자산 운용·자문 서비스인 로보어드바이저 시장규모도 확대하였다.
보험사의 경우 신상품 개발에 새로운 데이터 획득 및 분석 기술을 도입함으로써 기존의 사각지대 였던 영역까지 확장하였다.
디지털 금융은 금융회사와 금융소비자는 물론 중앙은행, 감독당국 등에 미치는 영향이 크다. 금융서비스의 효율성 제고, 금융시스템의 복원력 향상 등 긍정적인 효과와 함께 새로운 금융서비스가 기존 시장을 대체하는 과정에서 다양한 리스크도 증가될 것이다. 중앙은행의 경우 금융서비스의 플랫폼화, 달러화 등이 야기할 수 있는 통화신용정책의 유효성 및 파급경로 변화에 대한 연구를 확대할 필요가 있다. 금융당국의 경우 비금융회사의 금융 제공 확대, AI 기술 적용 확대 등에 따른 감독 사각지대 발생으로 금융소비자 보호가 저해되지 않도록 데이터보안 등 유의해야한다.