특집 05

사이버환경에서 금융기관의 제로 트러스트 구축과 성숙도를 높이기 위한 전략

조이남 (금융정보시스템 연구회), 이무성 (㈜엠엘소프트)

목 차

1. 서 론
2. 제로 트러스트 보안 성숙도
3. 금융기관의 사이버 보안성숙도를 높이기 위한 제안
4. 금융보안 성숙도를 높이기 위한 거버넌스
5. 결 론

1. 서 론

코로나 19 이후 금융기관은 원격근무 지원을 위하여 신속하게 대응해야만 했다. 그러나 기존 외부 단말기의 물리적 통제 미흡과 안정되지 못한 네트워크 사용, 악성코드 감염에 따른 네트워크의 침해, 내부자원의 원격접근 등의 위협은 계속되었다. 이러한 위협으로부터 탈피하기 위하여 경계방어나 심층방어 접근방식을 통하여 새로운 패러다임이 도입되기 시작하였고, 최신 기술로 마이크로 서비스, 마이크로 세그멘테이션, 소프트웨어 정의 아키텍처(SDP: Soft Defined Perimeter Architecture)를 채택하기 시작하여 보안위협을 줄이려는 노력이 시작되었다. 그러나 금융기관에서 ZTA(Zero Trust Architecture)[1] 접근은 계획 단계로 아직 본격적인 구현은 시행되지 않고 있다. 이런 환경에서 필자는 ZTA의 개요와 SDP의 특성, 금융기관의 사이버 보안 성숙모델, 그리고 성숙모델을 향상시키기 위한 거버넌스에 관하여 기술하고자 한다.

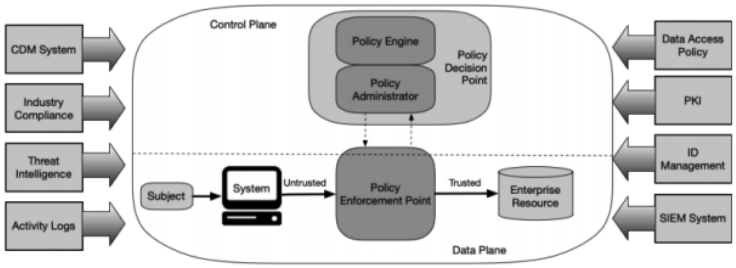
1) ZTA는 (기업 내) 존재하는 구성요소(component)의 관계, 워크플로우, 접근정책 등에 제로 트러스트(컨셉)를 적용하기 위한 사이버보안 계획' 이라고 이해할 수 있다, NIST Special Publication 800-207 Zero Trust Architecture.

2. 제로 트러스트 보안 성숙도

2.1 제로 트러스트 개요

ZT(Zero Trust) 모델은 2003년 Jericho Project가 경계형 시스템 보안 과제를 발표한 것으로, 2009년 Google Byeond Crop프로젝트가 ZT를 도입하고 2010년에 포레스트 & 리서치(Forreste & Research)가 계속 연구하였다. ZT모델에서는 "모든 네트워크 트래픽은 신뢰할 수 없다."라는 개념에 기반한다. 따라서 보안전문가는 모든 리소스를 검증하여 보호하고 엑세스 제어를 제한하여 모든 네트워크 트래픽을 검사하여 기록해야만 한다.

2019년 NIST(National Security of Standard and Technology)는 ZT의 아이디어를 ZTA의 개



출처 : NIST 특별 간행물 800-207 (제로 트러스트 아키텍처)

(그림 1) 제로 트러스트의 논리적인 구성 요소

념에 도입하고 ZTA의 개발과 구현을 원칙으로 하는 제로 트러스트 아키텍처에 관한 메뉴얼(SP 800-207)을 발행하였다. 새로운 ZT 보안 환경의 도입을 추진하려면 많은 보안비용과 5G의 광범위한 사용, 클라우드 컴퓨팅, IoT, 마이크로서비스 지향 아키텍처 등이 소요된다. 이러한 요소들은 물리적 경계 또는 소프트웨어 정의 네트워크(SDN)에 의한 소유권 경계와 사용 패턴을 재정의해야 한다[1-4].

2.2 금융기관의 제로 트러스트

현재 금융기관이 사용하고 있는 VPN과 게이트웨이를 통과하는 트래픽 라우팅은 비용이 높고, 효율이 떨어지며 신뢰도가 낮다. 특히 사이버 보안의 경우 기존 기반의 개념에 근거하고 있어, 제로데이 위협에는 약하다. 금융기관내의 현대화 속도와 수준차이를 감안할 때 이런 최신 아키텍처를 정보보호 방법으로 도입하고, ZT 솔루션 도입과 로드맵의 성숙도를 높여야 한다. ZT 원칙에 따른 제로 트러스트 아키텍처 성숙도 모델(ZTA-CMM)의 기본 요소와 로드맵을 수용하고 지속적으로 향상된 위험 관리와 사이버 복원력을 갖도록 해야 한다.

NIST의 제로 트러스트 원칙은 모든 데이터와 컴퓨팅 서비스는 “리소스(Resource)”이며 모든 통신은 장소에 관계없이 안정해야 한다. 또한 개별 리소스에 대한 엑세스는 세션단위로 허용하며 리소스에 대한 엑세스는 동적정책과 환경 속성에 따라 결정한다. 금융기관의 모든 IT자산은 무결성과 보안 상태를 모니터링 하고 측정하며, 접근이 허용되기 전에 동적인 자원인증과 인가가 엄격히 시행되도록 해야 한다.

2.3 제로 트러스트의 아키텍처 구성요소

제로트러스트의 구성요소는 (그림 1)과 같으며 중요한 요소로 정책 결정지점과 정책시행 지점으로 구성된다. 정책결정 지점(PDP)은 정책엔진(PE)과 정책관리자(PA)로 구성되며, 정책엔진은 접근하려는 클라이언트에 대한 액세스 권한을 부여하는 최종적인 결정을 담당한다. 정책관리자는 클라이언트와 정보자산 간의 통신경로를 설정하고 차단하는 역할을 담당하며, 클라이언트가 정보자산에 액세스하는데 사용하는 인증토큰이나 인증서의 정보를 생산한다. 이렇게 생성된 인증정보를 정책시행엔진에서 승인여부를 판단 승인되면 정책관리자는 시행 지점을 구성하며, 정책엔진에 의하여 액세스가 거부된 경우에는 정책관리자는 정책시행지점(PEP)을 구성하지 않고 연결을 종료한다.

정책시행지점(PEP)은 클라이언트와 정보자산 간의 연결을 활성화와 모니터링의 역할을 담당하며, PA와 통신하여 보안정책을 요청하거나 수신

을 하여 보안정책을 업데이트한다. 정책시행 이후에는 정보자산에 접근할 수 있는 신뢰영역이 있다. 제로 트러스트 아키텍처 구성요소에는 다양한 시스템들이 정책지점에서 활용된다. 정책 결정지점에서 활용되는 시스템으로는 CDM시스템[2], 시스템 적용분야의 규정, 내외부 식별된 취약점과 S/W 결함 정보, 시스템 활동로그, 단말기 엑세스 권한 설정, PKI[3], ID관리시스템, SIEM시스템[4] 등이다.

제로 트러스트 구현을 위한 대표적인 방법 중 하나로 소프트웨어 정의경계(Software Define Perimeter)[5]라는 방법이 있는데 OSI 네트워크 스택의 계층 1-7에서 보안을 제공하기 위하여 구현된 네트워크 보안 아키텍처이다[5].

SDP의 특징과 중심기능은 다음과 같다.

선인증 후연결, SPA에 의한 트래픽제어[6], 송수신자가 TLS프로토콜로 암호화 인증, mTLS에 의한 디바이스 검증, Dynamic Firewall, Application Binding, 동적 접속제공, 상호 핸드쉐이크 기술 등이다. 서버, 응용프로그램 데이터를 에이전트, 콘트롤러, 게이트웨이 개념으로 완벽한 스텔스 기능을 도입 운용한다[3,4,6].

2.4 제로 트러스트 성숙도 모델

금융기관은 제로 트러스트의 상태를 파악하기 위하여 전체 부서 직원이 참여하여 ZTA 성숙도를 체크해야 한다. 이 분석을 위하여 CISA Federal Zero Trust Strategy 의 가이드를 ZT CMM에 ID, 디바이스, 네트워크, 어플리케이션 워크로드 및 데이터로 구성된 내용을 발표하였다. 여기서 제시하는 5개의 컴퍼넌트는 금융기관에 ZTA 개발 시 적용할 수 있는 다양한 영역과 전체적인 관점을 제공한다[1,2].

CISA ZT CMM (DHS CISA)의 ZTA 성숙도 모델에서는 5개의 컴퍼넌트 내용을 Traditional, Advanced, Optional로 3 레벨로 평가하고 있다[1].

2) CDM(Constantly Diagnosis & Measures): 지속적 진단 및 대책시스템
3) PKI(Public Key Infrastructure): 공개 키 기반 구조
4) SIEM(Security Information & Event Management): 보안 정보 및 이벤트 관리
5) SDP에 대하여는 정보처리학회지 제28권 제2호를 참고한다.
6) SPA패킷에 포함된 RFC44226 기반 원타임 패스워드 “HOTP”를 기반으로 한다.

3. 금융기관의 사이버 보안 성숙도를 높이기 위한 제안

본 장에서는 제로 트러스트개념에 의한 SDP 핵심 요소와 금융거래법에 따른 사이버 환경에서 지켜야할 사항을 중심으로 금융기관 사이버 보안 성숙도를 <표 1>과 같이 제안한다.

3.1 금융기관에서 제로 트러스트 구축을 위한 고려사항

3.1.1 원격접속

금융기관에서는 원격접속을 통하여 접속하는 방식은 간접접속과 직접접속으로 구분하여 접속방식을 선택하도록 하고 있다. 직접접속은 외부단말기에서 내부망에 직접 접속하는 방식이며, 간접접속은 외부단말기에서 회사 내부의 업무용 단말기를 경유하여 내부망에 접속하는 방식이다. 외부단말기와 업무용 단말기 간 별도의 원격접속 중계서버를 통한 접속도 가능하다. 원격접속 중계서버 활용 시에는 중계서버에서 직원인증, 비인가 제어 등 추가적인 보안통제를 한다.

또한, 현재 금융기관에서 원격 근무 중 VPN을 중심으로 네트워크를 사용할때 선연결 후인증 구조로 인해 보안적인 취약점이 발생하는데 제로 트러스트의 핵심원칙 중 하나인 선인증 후연결으로

〈표 1〉 금융기관 사이버 보안 성숙도 표

	초기단계	발전단계 (초기단계에 추가)	고급단계 (초기 및 발전단계에 추가)
아이디 인증	선인증 후접속, ID, 비밀번호, 생체인증, OTP사용, 전화인증, 일정한 회수이상 인증 불가시 취소, 접속차단 해제에 본인 확인 절차 마련, 원격접속 시 직원과 접속서버에 대한인증, 미인가 리소스 취소,SPA사용에의한 접속자보호	비밀번호 주기적 교환, 한 리소스의 인가를 타 리소스에 자동허가 불가, 자산관리시스템 사용자 인증	자료처리 중간에 간헐적아이디 체크(일정시간 간격(10분, 30분 등) 또는 일정한 자료처리 후(1000건, 1만 건 등)에 아이디(또는 OTP) 체크
디바이스 인증	핀번호, 디바이스 인증번호 체크, 한 디바이스 허가를 다른 디바이스 허가에 사용 여부, 외부단말기의 업무용 단말기 보안 설정 여부, 디바이스 운영체제 유무, 내용년수 지난 운영체제 사용 여부, 데이터 송신 기능 유무 체크, 사용자 디바이스의 상태와 소프트웨어 버전 체크, 미인가 S/W차단 여부, 외부단말기에 USB 등 외부자료 보관 장치 사용금지, 원격 근무자가 외부단말기의 보안설정 변경 불허, 단말기 도난방지대책 마련	현사용자 디바이스의 이전사용 기록 관리 여부, 최소접근과 접근 가시성체크, 리소스 패치여부 체크, 개인소유 디바이스 리소스 관리를 회사용 디바이스와 동일하게 관리	사용자 디바이스의 위치, 사용시간 프로세스 요구사항의 실시간 수집, 동적 체크, 사용자 디바이스의 행위관찰, 분석, 사용패턴 비정상 행위 식별 기능 체크
네트워크 (통신)	내외부 통신소스의 인증여부, 무결성, 암호기술에 의한 기밀보장 여부, 액세스 요청 시 보안체크, 허가된 포트만 외부기관과 연결	내부 접근자 자동 인증차단, 부정사용자 차단, 네트워크 방화벽 설치, 상호 핸드쉐이크 기술로 중간자 공격방어	통신에 관한 정보 실시간 수집, 수집데이터 정보 분석, 정보정책 반영 실시간 처리
응용 프로그램, 워크로드	응용프로그램 횡적이동 금지(application binding) 및 모니터링, 마이크로 세그멘테이션, 모든 응용서비스 리소스관리, 접근권한 및 작업권한 세션별로 진행, 업무수행에 필요한 최소권한 부여, 허가 권한을 유효기간 동안 사용, 오픈소스 사용 시 취약점 점검	트랜잭션 시행 시 계속적인 모니터링, 정상적인 업무처리를 위하여 리소스 패치처리, 중앙집중 점검, 외부명령 개입금지	시뮬레이션 프로그램으로 애플리케이션 모니터링, 실시간 프로그램 감시, 자료처리결과 체크(체크 포인트 실행)
데이터	보안처리 입력 데이터, 자료처리 중 데이터, 자료처리 후 데이터 암호화, 데이터 처리 후 백업처리, 데이터처리 후 무결성 체크	데이터처리 일정 구간마다 체크포인트 가동, 백업데이터 실시간 보관, 일부데이터 암호화	실시간 자료처리 점검, 실시간 백업처데이터 생성 보관, 전 데이터 암호화, 데이터 3중 실시간 보관
거버넌스	보안 인력, 예산 반영, 정보보호 조직관리 여부, CISO 임명과 조직 구성, 사고발생 시 복구계획, 보안연수 시행 체크, 불시 사고 복구연습 시행	법규 준수 여부 체크, 점검결과 보고 받음, 규정위반자 처벌, 전 직원교육 시행, 이해관계자에 정보보호 홍보, 정보보호위원회 업무 보고 받음	취약자산 별도관리, SIEM 내용 체크 후 주요 사항 개선, 거버넌스 문화 창조

만 바꾸어도 큰변화가 일어난다. 또한 SPA에의한 연결자를 확인하는 절차를 도입하면 서버가 스텔스되어 성숙도가 더욱 높아지고, 응용프로그램 레벨에서 마이크로 세그멘테이션이 가능하도록 하면 횡적이동이 불가하게 되어 보안성숙도는 발전단계로 높아질 수 있다.

3.1.2 단말/사용자 보안

가. 단말기 인증

외부단말기에 백신프로그램을 설치하고 실시간 탐지해야 하며, 정기적으로 업데이트하고, 정보유출 되지 않도록 실시간 검사를 실행한다. 또

한 기술지원이 종료된 운영체제(예: Window7)를 사용해서는 안 되며, 보안패치는 필수 사항이다. 외부단말기에는 로그인, 비밀번호 및 화면보호기를 설정하고 일정시간(예 10분)동안 업무처리를 하지 않으면 화면 잠근 장치가 작동되어야 한다. 정보유출 방지를 위하여 화면 캡처방지, 개인정보 등 중요정보 마스킹처리, 내부 전산자료 출력금지, 출력물 내 워터마킹 적용이 되어야 한다[7].

SDP 필수사항인 선접속 후인증을 위하여 콘트롤러, 에이전트, 게이트웨이 기능을 갖는 소프트웨어와 디바이스의 설치가 필요하고, 디바이스와, 사용자인 멀티인증으로 이들 기능을 이용하여 외부침투 해킹을 방지해야 한다[3-5].

나. ID인증과 디바이스 인증

ID에는 개인ID, 비밀번호, OTP기기, 전화인증, 바이오인증과 실시간 디바이스와 사용자 인증이 필요하다. 디바이스는 사용하지 않을 때 OFF하며, 일정한 회수이상 인증실패 시 접속을 차단하고, 차단해지를 위하여 직접 점포에 방문하여 신고한다. 성숙도 지표에서 강조하는 ID의 주기적 교체와 자료처리 중간에도 ID를 실시간으로 확인하는 기능이 추가되고, 디바이스 부문에서도 접근 가시성을 갖도록 하면 성숙도가 높아진다.

다. 네트워크 사용

인증을 받은 장비와 사용자는 일부 또는 전부 암호화가 된 데이터를 전송한다. 데이터의 전송을 일정 시간이나 일정 데이터처리 후에는 전송된 데이터 수량, 금액과 송수신자를 확인해야 한다. 네트워크 방화벽으로 DDoS 공격을 방어하고, 상호 핸드쉐이크 기술과 mTLS, IKE로 상호인증 암호 프로토콜로 중간자 공격을 불허한다.

라. 응용 업무처리

사용 OS의 취약점 점검, 공개소프트의 취약점 점검, 처리업무의 Segment 적용과 Binding, 중앙집중식 점검, 외부명령 적합도 검사, Application flow 체크, 마이크로 세그멘테이션에 의한 횡적이동 금지 등 제반 사항을 점검하고 이행하도록 해야 한다. 점검 빈도는 수시, 또는 계속 실시간 체크도 가능하게 해야 한다.

마. 데이터

초기 일부 데이터 또는 전 데이터 암호화 보관, 백업데이터 배치 또는 온라인 실시간 작성하고, 데이터 보관은 3중으로 클라우드센터와 백업센터에 보관한다. 이상의 필수사항 외에 개인방화벽 설정, 외부단말기 도난방지 조치, 운영체제 계정, 권한 제한을 권고하며, 외부로부터의 악의적인 네트워크 접근차단을 위한 방화벽을 설치한다. 단말기 도난방지를 위하여 잠근 장치를 통하여 도난에 대비하고 일정시간 근무자가 자리를 떠날때 PC를 종료처리 한다.

모바일 기기 보안통제를 위하여 내용 년수가 지난 운영체제 사용을 금지하며, 모바일 기기에 잠금을 설정하고 잠금 설정을 해지 시에는 안전한 인증방법, 바이오 인증, PIN번호 인증을 사용 한다. 모바일 기기의 불법적 네트워크 접속을 차단하기 위하여 NFC, 핫스팟 등 기능은 사용하지 않도록 한다.

간접접속 방식 중 원격접속 시 단말기 간 파일 전송은 차단하고, 임의로 차단설정을 변경하지 못하도록 하며, 외부단말기는 화면 출력에 필요한 포트만 접속을 허용하고 그 외의 접속은 차단한다. 또한 외부단말기에는 업무자료는 저장이 안 되도록 하고, 취약한 원격 접속 프로그램을 사용 금지하며, 사용 중인 원격프로그램에 신규 취약점이

발견되면 즉시 보안 패치를 적용한다.

VDI의 가상업무용 단말기는 업무수행 후 초기화 조치하여 업무자료의 외부 유출을 방지한다. 개인 단말기를 업무에 사용할 경우 보안통제를 해야 한다. 원격근무자가 외부단말기의 보안설정을 임의 변경하지 못하도록 하며 USB 등 외부 저장장치에 읽기, 쓰기 기능을 차단한다. 외부 단말기에서 민감한 업무자료를 처리할 경우 외부 단말기 내 가상머신 환경을 구성하고 가상머신 디스크를 암호화 조치해야 한다. 업무자료를 내부 서버로 전송할 경우 자료의 무결성을 검증해야 한다. 최소한의 IP 및 포트로만 연결을 허용하고, 접속한 내부시스템의 정보는 1년 이상 기록, 보관한다.

3.1.3 통신회선

원격접속 시 통신회선은 전용회선과 동등한 보안수준을 갖춘 가상 사설망(IPSec VPN)을 의무적으로 구축, 운영한다. 이 경우 전송데이터의 기밀성 및 무결성 보장, 클라이언트 및 서버 인증, 중간자 공격, 재생공격을 예방해야 한다. 통신장비에 안전한 알고리즘을 사용하고, 내부망 접속 시 인터넷 접속차단 등의 조치를 의무적으로 적용하며, 원격접속 후 일정시간 업무처리가 없으면 네트워크 연결을 차단해야 한다. 원격근무자에 대하여는 보안서약서를 받고, 공공장소에서의 원격접속을 금지한다.

3.1.4 원격근무 규정

전자금융감독 규정 시행세칙 제 2조의 2(망분리 적용 예외).

규정 제15조 제1항 제3호에서 금융감독원장의 확인을 받은 경우는 다음과 같다.

(1) 내부통신망에 연결된 단말기가 업무상 필수적으로 외부기관과 연결해야하는 경우, 다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다.

(2) 규정 12조의 보안대책을 적용한 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 외부망으로 부터 내부업무용 시스템으로 원격접속 할 수 있다. 금융감독원 시행 세칙에 보안장비중 “원격근무시 VPN 등”이라고 되어있는 부문이 있는데 여기에 “VPN과 제로 트러스트 기술을 반영”한다면 금융기관들이 보안장비를 도입할 때 제로 트러스트의 기능을 도입하여 보안성숙도가 크게 개선될 수 있다.

위에서 제시한 내용들을 성실히 수행하면 제로 트러스트의 성숙도를 높이는데 기여 할 수 있다.

4. 금융보안 성숙도를 높이기 위한 거버넌스

4.1 거버넌스의 개요

최근 들어 금융 IT 환경 변화와 국내외 보안사고가 계속하여 발생하고 있어 효과적인 관리가 필요하게 되었다. 국내 금융권의 보안수준은 전자금융거래법, 전자금융 감독규정 등에 최소한의 법규준수 활동에 머물러 있어 보안성숙도를 높여야 할 필요성이 높아졌다.

우리나라 금융기관에서도 최고 경영층을 중심으로 톱다운 방식의 강력한 보안을 강화하여, 보안 사고 발생 시 신속한 복원력이 향상되어 이용자 보호와 금융회사의 피해가 최소화 되도록 하고 있다[7-9].

4.2 금융보안 성숙도를 높이기 거버넌스

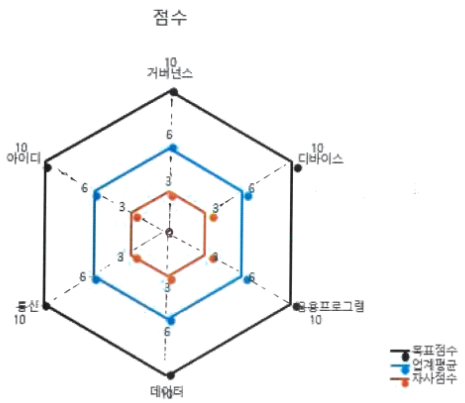
금융보안부문이 기술적 관점에서 관리, 제도화 단계에서 발전하여 정보보호 거버넌스로 진입하면서, 금융회사의 자율성 제고를 위하여 필요한 조치를 법률로 정하였다.

가. 금융회사 최고경영자의 보안업무(전자금융 감독규정, 2014. 1. 1.)
나. 정보보호최고책임자 지정 요구(전자금융거래법, 2012. 5. 15.)
다. 양벌규정 책임주위 원칙반영 (전자금융거래법, 2012. 5. 15.)

4.3 정보보호 성숙도 지표

금융기관의 정보보호 활동 수준을 파악 할 수 있는 방법으로 '정보보호 성숙도 지표'와 '정보보호 활동스코어 표'를 만들 수 있는데 여기 제시한 <표 1>과 (그림 2)은 목표로 한 금융기관의 제로 트러스트의 성숙도를 높이는데 큰 역할을 할 수 있다.

위의 지표는 정보보호 활동에 대한 가시적 자료로 성과 지표를 만드는데 참고가 될 것이며, 조직문화를 유도하거나 이사회, 투자자, 금융당국 등 이해관계자에게 정보보호 거버넌스 활동 및 주요 성과를 홍보하는데도 도움이 된다.



(그림 2) 정보보호 활동 스코어 표

5. 결 론

앞 장에서 여러 가지로 보안강화를 위한 방법론을 설명하였지만 DHS CISA에서 제공하는 모델 5개 분야인 Identity, Device, Network/ Enviroment, Application Workload, Data에서 단계적으로 성숙도를 높여 나가는 방법을 참고하여, 필자가 만든 정보보호 활동 스코어 <표 1>를 이용하면 도움이 될 것이다.

Identity 부문에서는 패스워드와 멀티인증, 지속적인 검증, 실시간 체크 등으로 개선해 나가고, Device 부문에서는 디바이스 상시 검증과 실시간으로 검증, 체크하면 된다. 네트워크 환경에서는 대규모 세그멘테이션과 내부와 외부의 트래픽 암호화 위협보호 기반으로 전 트래픽이 암호화될 필요가 있다. 그리고 Application Workload에서는 로컬인증에 의한 엑세스, 중앙집중식 인증기반 엑세스, 지속적인 접근허가, 어플리케이션 워크플로우의 통합운영이 필요하며, 데이터부문은 전 데이터를 암호화하는 것을 목적으로 동적지원을 해야 한다.

이러한 목표는 성숙도 레벨을 높일 수 있으나, 실제로 실행하는 업무를 단계별로 개선해 나가는 것이 중요하며 장비의 성능 확보와 보안 관련 예산 확보가 더 중요하다.

보안성 강화를 종합하여 언급한다면, 대상 네트워크 정보가 노출되지 않도록 서버 등 스텔스 기능을 갖도록 하고, 최소한의 인증과정(SPA: Single Packet Authorization)으로 DDoS공격을 방지한다. Dynamic Firewall로 사전에 허용된 대상만 접속가능하게 하며, IPsec Tunnel로 보안을 강화한다. 그리고 지정된 Application만 서비스 연결이 가능하게 한다.

이 모두를 단계적으로 시행하고 전사가 협조 체제로 가는 거버넌스를 도입하여, 평소에 전체직원의 정보보호 노력이 계속되어야 보안 성숙도를 높일 수 있다.

참 고 문 헌

[1] CSA, Toward a Zero Trust Architevture, 2021.

[2] NIST, SpecialPublication800-207, ZeroTrust Architecture, 2020.

[3] CSA, SDP Architecture Guide, 2022.

[4] CSA, Soware-Defined Perimeter(SDP) Specification v. 2.0, 2022.

[5] 조이남, 박완성, 최우봉, 한동우, 이무성, “클라우드 컴퓨팅 변화에 따른 제로 트러스트 네트워크 구현을 위한 보안시스템”, 정보처리학회지, 제 28호, 제 2권, pp. 59-67, 2021년.

[6] 박승규, “Cloud IoT 시스템의 보안을 위한 소프트웨어정의 경계기반의 접근제어 시스템 개발”, The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 21, No. 2, pp.15-26, 2021.

[7] 금융보안원, 금융회사 재택근무 보안안내서, 2020년 12월.

[8] `금융보안원, 거버넌스 가이드(ver. 3.0), 2019년.

[9] 금융보안원, 디지털 금융 및 사이버 보안 이슈 전망, 2022년

저 자 약 력

조 이 남

이메일 : choleenam75@naver.com

- 1965년 서울대학교 수학교육과 (학사)
- 1970년 성균관대학교 경제개발대학원 EDPS전공 (석사)
- 1987년 건국대학교 산업대학원 전산학 (석사)
- 1993년 홍익대학교 대학원 전산학 (박사)
- 1971년~2001년 금융결제원 / 전무이사
- 1977년~2022년 한국정보과학회 / 부회장
- 1984년~2022년 한국IT 전문가협회 / 회장
- 1991년~2022년 한국정보처리학회 /회장
- 1997년~2022년 금융정보시스템 연구회 /회장 (현 명예회장)
- 관심분야 : 금융결제제도, 금융보안

이 무 성

이메일 : musso@mlsoft.com

- 1983년 국내최초 한글워드프로세서 명필 개발 (KIST공동)
- 1995년 미디어랜드 (현 엠엘소프트) 설립 / 대표이사
- 1997년 TCO!Stream, IT자산관리 개발
- 2007년 TCO!secuNAC, 네트워크 접근통제 개발
- 2013년 TGATE(NAC) 개발
- 2014년 대한항공 NAC개발, 금감원 IMP 구축
- 2015년 농협중앙회, 신한은행, 수협, 기업은행 등 NAC 구축
- 2019년~2022년 TGATE(SDP) 개발 및 보급