GLOBAL PERSPECTIVES & INSIGHTS

사이버 보안

파트 1: AI가 강화된 세계에서의 사이버 위협

파트 2: 사이버 회복탄력성 보장

파트 3: 새로운 제로 트러스트 경계 설정

The Institute of Internal Auditors

파트 1

AI가 강화된 세계에서의 사이버 위협

전문가 소개

안토니오 카차푸오티, CIA

안토니오 카차푸오티는 룩셈부르크에 위치한 Eurizon Capital S.A.의 내부감사 책임자이며, 이 회사는 인테사 산파올로 그룹(Intesa Sanpaolo Group)의 자산 운용사이다.

브래들리 니에지엘스키, CPA

브래들리 니에지엘스키는 Deloitte & Touche LLP의 감사 및 검증(Audit and Assurance) 파트너이며, 금융 서비스 산업의 공공 및 민간 기업을 대상으로 서비스를 제공하는 재무 혁신 및 생성형 AI 리더이다.

지난 한 해 동안 인공지능(AI)의 발전으로 인해 조직들은 이 기술이 제공하는 기회와 위협을 파악하고 따라가는 데 분주해졌다. 기업들은 온라인 정보와 거래에 거의 전적으로 의존하고 있기 때문에, 자사의 보안 활동에 대해 점점 증가하고 있는 AI가 초래할 수 있는 위협을 고려해야 한다. 악의적인 행위자들은 기업의 사이버 방어를 뚫기 위해 AI 기반 도구를 빠르게 사용하기 시작했다. 이번 글에서는 AI 주도의 세계에서 사이버 위협이 어떻게 변화했는지, 그리고 기업이 이러한 변화에 대응하여 새로운 사이버 보안 접근법을 개발하는 데 있어 내부감사가 어떻게 도움을 줄 수 있는지를 살펴본다.

사이버 범죄의 진화

강력한 사이버 방어는 항상 중요했지만, 악의적인 행위자들은 이제 AI를 활용해 조직의 방어체계를 무력화하는 능력을 더욱 정교하고 광범위하게 발전시키고 있다. "AI는 새로운 유형의 사이버 공격이라기보다는 기존 공격의 진화된 형태이다." 라고 룩셈부르크 Eurizon Capital S.A.의 내부감사 책임자인 안토니오 카차푸오티는 말한다. 또한 AI는 속도, 규모, 복잡성 및 적응성 측면에서 기존 사이버 공격보다 훨씬 고도화된 방식으로 사용되고 있으며, "바이러스처럼 시간이 지날수록 저항력을 키우기 때문에, 더 위험해진다"라고 덧붙였다.

AI는 좁은 표적형 공격에서 광범위한 파괴적 공격에 이르기까지 다양한 방식으로 악용되고 있다. 예컨대, 오늘날 많은 기업들이 이메일이나 보고서 작성을 위해 AI 생성 문서를 일상적으로 사용하지만, 악의적인 행위자들 또한 범죄 목적으로 AI 생성 문서를 사용하고 있다고 딜로이트 뉴욕의 감사 및 검증 파트너인 브래들리 니지엘스키는 말한다.

또 다른 측면에서, 피싱 공격은 보안 장벽을 뚫고 귀중한 데이터에 접근하려는 목적을 가진다. 피싱은 새로운 개념은 아니지만, FBI는 AI 기반 피싱 공격에 대해 "이 공격은 특정 수신자를 대상으로 설계된 그럴듯한 메시지를 문법과 철자까지 맞춰 제작함으로써 사기행위와 데이터 탈취의 성공 가능성을 높인다"고 경고한다.

예를 들어 자동화된 스피어 피싱은 특정 개인이나 그룹을 대상으로 하며 민감 정보를 탈취하거나 시스템 접근을 목적으로 한다. 카차푸오티는 "AI는 소셜 미디어, 커뮤니케이션 패턴, 대상에 대한 가용 데이터를 분석한 후 수신자가 민감 정보를 노출하거나 악성 링크를 클릭하도록 유도하는 메시지를 생성할 수 있다"고 설명한다. 과거에는 음성이나 외모를 통해 영상이나 전화의 진위를 판단할 수 있었지만, 지금은 특정 개인의 모습을 흉내낸 '딥페이크' 영상(개인의 시뮬레이션 영상)이나 목소리를 복제한 '보이스 해킹'으로 특정 대상을 속이고 조작할 수 있다.

이러한 위협만이 AI 관련 리스크는 아니다. 카차푸오티에 따르면, AI 기반 악성코드는 대상 환경에 따라 스스로 행동을 바꾸며, 기존 보안 시스템이 이를 탐지하기 어렵게 만든다. "기본 탐지를 쉽게 우회하며, 코드 변경을 위한 다형성 기법을 사용하고 방어 조치를 분석해 이를 피할 수 있다"고 설명한다. 더 나아가, AI 기반 머신러닝 모델에 오염된 데이터를 주입해 사기 탐지 시스템에서 잘못된 예측을 유도하고 일부 사기 지표를 간과하도록 만들 수도 있다.

AI는 지능적인 데이터 탈취 기능을 통해 탈취한 데이터와 지적 자산을 실시간으로 분석하고, 그 중 가장 가치 있는 정보를 우선순위로 정하여 유출한다. 그런 다음 해당 정보를 암호화하고, 이를 해제하기 위한 몸값을 요구할 수 있다고 카차푸오티는 말한다. AI 기반 공격은 또한 합법적 사용자의 인증 정보를 침해하여 시스템 전체를 자유롭게 이동할 수 있도록 한다.

AI 기반 사이버 공격의 리스크는 그로 인해 초래될 수 있는 막대한 피해 때문에 매우 중요하다. 민감 정보가 유출되거나 악용되면 조직의 경쟁력에 심각한 타격을 줄 수 있으며, 개인정보 보호 규정을 준수하지 못한 데 따른 제재를 받을 수도 있다. 이러한 침해 사고는 고객이나 비즈니스 파트너로 하여금 해당 조직에 대한 신뢰를 잃게 만들 수 있다. 랜섬웨어 및 악성코드 공격은 조직 운영을 방해하고 중요

시스템을 중단시킬 수 있다.

이전에는 상상하기 힘들었던 일이 오늘날 현실에서 실제로 일어나고 있다. 예를 들어, CNN에 따르면 홍콩에 있는 한 다국적 기업의 직원이 영상통화에서 CFO를 흉내낸 딥페이크에 속아 무려 2,500만 달러를 송금한 사건이 발생했다.
또 다른 사례로, The Drive는 페라리 임원이 CEO의 딥페이크로부터 전화를 받은 사례를 보도했다. 이 시도는 임원이 의심을 품고 CEO만이 알 수 있는 질문을 던진 덕분에 좌절되었다. 그레이락 파트너스가 인용한 사례를 보면, 한 북한 스파이가 가짜 신원을 사용해 사이버 보안 기업에 채용된 뒤, 즉시 해당 기업의 장비에 악성코드를 설치하기도 했다.

최고의 방어

다행히도 AI는 조직이 악의적 행위자를 차단하는 데에도 활용될 수 있다. "AI를 막기 위해서는 AI를 활용해야 한다"고 카차푸오티는 말한다. 조직은 진화하는 위협에 대응하기 위해 보다 정교한 AI 기반 사이버 보안 조치를 도입해야 한다. "범죄자들이 사용하는 기술에 대해 깊이 이해하지 못한다면, 그들을 어떻게 막을 수 있겠는가?"라고 그는 묻는다. 조직은 사이버 범죄자들이 사용하는 도구와 전략을 파악하고, 이러한 지식이 사이버 보안을 강화하는 데 어떻게 도움이 되는지를 이해해야 한다.

ISACA의 보고서 "AI 기반 공격을 차단하기 위한 AI 기반 사이버 보안의 필요성(The Need for AI-powered Cybersecurity to Tackle AI-driven Attacks)"은 첨단 기술이 공격을 예방하는 데 도움이 되는 여러 방법을 제시한다:

공격 예방을 위한 방법들

- 조직 자원의 사용 방식을 분석하고, 노출된 영역을 식별하며, 자산 목록을 작성하고, 네트워크 트래픽 패턴 및 사용자 활동/행동을 파악
- 이상 징후 탐지: 예를 들어, "비정상적인 로그인, 새로운 지리적 위치나 IP 주소로부터의 접근 요청, 새로운 사용자 접근, 파일이나 기타 자료에 대한 권한 변경, 대량의 파일 추출 또는 삭제, 트래픽 급증" 등
- AI를 활용하여 의심되는 악의적 행위자를 사전에 차단하거나 로그오프 시키고, 시스템 관리자에게 해당 행위자의 활동을 경고
- 신속한 대응이 가능하도록 시스템을 지속적으로 모니터링
- 예측 분석을 통해 잠재적인 보안 위협을 예상하고 사전 예방
- 제로데이 위협, 즉 새롭고 아직 발견되지 않은 취약점을 탐지하고 예방
- 잠재적 위협에 대한 긍정오류(false positive) 발생 건수를 줄임
- 보안 평가를 자동화하여 대응 속도 향상 및 인적 오류 최소화
- 지속적인 보안을 제공하기 위해 새로운 환경과 변화에 적응할 수 있도록 확장

카차푸오티는 조직이 다양한 출처의 데이터를 통합, 분석, 상관관계 분석을 통해 더 깊은 통찰력을 얻기 위해 AI를 활용할 수 있다고 말한다. 또한 자연어 처리(Natural Language Processing, NLP)를 활용해 방대한 텍스트 데이터를 분석할 수 있다. 예를 들어, 내부감사인이 계약서를 분석해야 할 경우, NLP가 중요한 텍스트 데이터를 추출해 시스템이 이를 분석할 수 있도록 돕는다.

AI 고려사항 다루기

모든 리스크를 100% 제거할 수 없기 때문에, 니에지엘스키는 조직 전반의 다양한 영역에 걸쳐 위협을 전략적으로 평가하는 것부터 시작해야 한다고 조언한다. 여기에는 잠재적인 AI 기반 사기 벡터를 식별하고, 공격 가능성과 잠재적인 규모 및 영향을 평가하는 작업이 포함된다. 그 다음으로는 현재의 통제가 얼마나 효과적인지를 판단해야 한다고 그는 말한다.

이러한 노력의 일환으로, 니에지엘스키는 생성형 AI의 고급 추론 및 패턴 인식과 같은 새로운 기술을 활용하여 AI 기반 피싱 시도 및 딥페이크와 같은 일반적인 공격을 식별할 것을 권장한다. 일부 기업은 통화가 내부 번호에서 걸려온 것인지 외부에서 온 것인지를 확인할 수 있는 프로토콜과 기술을 사용하고 있다.

"이러한 첨단 기술은 관련 리스크를 최소화하는 데 도움이 될 수 있다"고 그는 말한다. 하지만 어떤 경우에는, 예를 들어 전화나 회의 참가자가 딥페이크인지 즉시 판단해야 하는 경우에는, 직원이 직감을 믿거나 CEO가 왜 자금 이체를 요청하는지 물어봐야 할 수 있다. 이러한 상황에서 직원들이 본인의 직감을 믿고 사내 번호로 다시 전화를 걸어 확인하거나, 해당 인물이 같은 사무실에 있다면 직접 찾아가 확인할 수 있도록 장려되어야 한다.

내부감사, 리스크 관리, IT, 사이버 보안 등 다양한 분야의 전문가로 구성된 다학제 팀은 AI의 발전을 모니터링하고, 지속적으로 리스크 관리, 보안 프로토콜, 사기 감지 시스템에 대한 업데이트를 제공할 수 있다. 니에지엘스키에 따르면, 이러한 팀은 서로 협력하여 어떤 통제가 피해를 가장 잘 예방하거나 최소화할 수 있는지를 고려해 대응 방안을 결정할 수 있다.

그는 기업들이 AI 취약성에 대해 서로의 경험을 공유하고 논의할 것을 권장하면서 "성공 사례뿐 아니라 잘못된 사례와 그로부터 어떻게 교훈을 얻었는지도 공유해야 한다. 지식 공유, 교육, 적절한 리스크 평가를 통해 AI로 인한 사기 리스크를 최소화할 수 있다."고 조언한다.

또 이러한 환경에서는 직원들에게 잠재적인 의심 활동에 대한 인식을 높이고, 침해 사고에 적절히 대응하는 행동 방침을 강화하기 위한 교육이 최우선이어야 한다고 니에지엘스키는 강조한다. 카차푸오티는 실제 상황에서 실시간으로 사이버 보안 교육을 제공하기 위해 AI 시뮬레이션을 활용할 수도 있다고 덧붙인다. AI는 사이버 훈련 중 개별 직원의 행동을 분석하고 개선점을 제시할 수 있다.

내부감사의 기여

카차푸오티는 내부감사는 조직의 노력이 AI 관련 도전 과제에 부합하도록 지원할 수 있으며, 여기에는 AI의 잠재력을 활용하는 동시에 리스크를 완화하는 것이 포함된다고 말했다. 또 그는 "내부감사는 포괄적인 리스크 평가를 수행하고, AI 시스템을 보안, 윤리 및 컴플라이언스 관점에서 감사하며, 안전한 혁신을 지원해야 한다"며, "내부감사는 AI 위협에 대처할 수 있을 정도로 강력한 사이버 전략을 수립하는 데 기여할 수 있다."고 덧붙였다.

또한, 카차푸오티는 내부감사는 일반적으로 핵심적인 방어선이지만, AI에 관련해서는 위험 관리에 있어 보다 역동적인 접근을 취함으로써 공격선의 역할도 수행해야 한다고 말한다. 그는 "리스크가 닥치기를 기다릴 이유가 어디 있는가? 정면으로 맞서 공격할 수 있다면 말이다"라고 묻는다. 이는 조직이 적절한 거버넌스 통제와 지속적인 개선을 보장하면서 기회를 극대화할 수 있도록 새로운 기술을 선도적으로 활용하는 것을 의미한다.

> "AI는 결코 내부감사인을 대체하지는 않겠지만, 강력한 조력자가 될 수 있다."
>
> - 안토니오 카차푸오티, CIA

내부감사 부서 내에서도 "AI는 결코 내부감사인을 대체하지는 않지만, 강력한 조력자가 될 수 있다"고 카차푸오티는 말한다.

그는 내부감사가 AI를 활용하여 다음과 같은 이점을 얻을 수 있다고 설명한다:

- 방대한 양의 데이터를 분석하고 테스트에서의 표본을 전체 모집단에 근접한 수준으로 확대한다.
- 테스트 절차를 자동화하고 주요 통제를 모니터링하여 반복적인 업무를 수행함으로써 내부감사 전문가가 보다 고차원의 업무에 집중할 수 있도록 한다.
- AI 알고리즘을 활용하여 정기적인 감사에 의존하는 대신 데이터를 지속적으로 모니터링함으로써 비정상적인 활동을 보다 신속하게 식별하고 대응할 수 있도록 한다.
- 예측 분석을 활용하여 향후 결과를 예측하고, 보다 정보에 기반한 의사결정과 권고를 가능하게 한다
- 작업 문서를 신속하게 요약하여 내부감사인이 최종 보고서를 작성할 때 활용할 수 있도록 한다.

AI는 모든 통제 기능 전반에 걸쳐 감사 발견사항을 보다 일관되고 효율적으로 관리할 수 있게 해준다. 카차푸오티는 "매우 규모가 큰 기업의 경우, 여러 기능에서 수행되는 수많은 감사업무를 고려해야 한다"고 말한다. AI는 내부감사인이 데이터를 통합된 방식으로 수집할 수 있도록 하여 중복을 방지하게 해준다.

AI 기반 사이버 위협: 주요 사실들

- 보안 전문가의 97%가 AI로 인한 사이버 보안 사고가 발생할 것에 대해 우려하고 있으며, AI는 번아웃(소진 현상)을 유발하고 있다.
- 75%의 보안 전문가가 지난 1년 동안 AI 기반 사이버 위협 증가로 인해 사이버 보안 전략을 변경해야 했다.
- 73%의 보안팀이 '사전 예방' 역량에 더 집중하길 원하고 있다.
- 61%의 조직이 지난 1년 동안 딥페이크 사건의 증가를 경험했다.
- 이들 공격의 75%는 CEO나 C-레벨 임원을 사칭하는 형태였다.

출처: GenAI in Cybersecurity: Friend or Foe? Voice of SECOPS, 제5판, 2024년

리스크를 완화하고 그로부터 가치를 창출하기 위해, 니에지엘스키는 내부감사인이 기술 발전에 대한 지식을 지속적으로 업데이트할 것을 권장한다. 그는 "매일 새로운 것이 등장한다"고 말한다. 내부감사인은 잠재적 리스크에 대한 대응을 '사후적'이기보다는 '선제적'으로 식별하는 데 집중해야 한다. 그는, 세계가 새로운 기술을 활용하려는 가운데, 내부감사인은 조직의 건전성을 보호하기 위해 새로운 규제 및 윤리 기준에 대한 거버넌스와 컴플라이언스에도 집중해야 한다고 말한다.

"내부감사인은 악의적인 행위자의 입장에서 생각해야 한다"고 니에지엘스키는 말한다. "악의적인 행위자가 조직에 어떻게 침투할지를 묻기보다는, 자신이 조직에 대해 알고 있는 정보를 바탕으로 악의적인 행위자라면 무엇을 할지 자문해보아야 한다. 조직을 정량적 관점뿐만 아니라 정성적 관점에서도 고려해야 한다."

카차푸오티는 내부감사인이 혼자 모든 것을 감당하려 해서는 안 된다고 말하며, 통제 기능, 컴플라이언스, 리스크 관리, 외부 감사인, 규제기관 등 모든 검증 제공자 및 이해관계자들과의 협업을 통해 리스크를 예방하고 완화해야 한다고 권고한다. 그는 "AI 도구와 사이버보안 전문가 간의 협업, 그리고 강력한 거버넌스 프레임워크는 이러한 환경을 헤쳐 나가고 새롭게 등장하는 리스크에 대응하기 위해 필수적이다"라고 강조한다.

파트 2

사이버 회복탄력성 보장

전문가 소개

DC 창(Chang), CPA, CDPSE, CISSP, CRISC, CISA

DC 창은 텍사스주 댈러스에 위치한 유나이티드 항공에서 디지털 기술 및 사이버 보안 부문의 감사 이사(Audit Director)이다.

마이클 에콜스, CISSP

마이클 에콜스는 워싱턴 D.C.에 본사를 둔 Max Cybersecurity LLC의 최고경영자(CEO)이다.

저스틴 헤들리, CPA, CISSP, CISA, CRISC

저스틴 헤들리는 앨라배마주 버밍햄에 위치한 Warren Averett의 리스크 자문 및 보증 서비스 그룹에서 시니어 매니저로 재직 중이다.

조직들이 사이버 공격을 방지하기 위한 적절한 도구를 확보하려고 노력하고 있음에도, 어떤 형태로든 침해나 침입을 겪게 될 가능성은 거의 확실하다. 이런 현실을 감안할 때, 기업은 사이버 공격에 빠르게 대응하고 회복하는 능력에도 집중해야 한다. 이 섹션에서는 공격에 대한 회복탄력성을 이해하고 이를 내재화하는 방법, 그리고 조직의 대응력을 강화하는 데 있어 내부감사의 역할을 설명한다.

회복을 위한 준비

Max Cybersecurity LLC의 CEO인 마이클 에콜스에 따르면, 최상의 사이버 회복탄력성은 단순한 사후 대응이 아니다. 회복탄력성은 계획, 프로세스, 분석, 교육, 핵심 서비스, 관리 등으로 구성된 연속적인 실행 체계이며, 이를 통해 조직은 공격 이후에도 운영을 유지하거나 복구할 수 있다. 다만, 이 모든 것은 문제가 발생하기 전에 미리 갖추어져야 한다.

예를 들어 에콜스는 한 로펌 고객과 협업한 경험을 공유한다. 해당 로펌은 웹사이트를 통해 모든 의뢰를 받는 구조였는데, 며칠간 의뢰가 전혀 없다는 사실을 뒤늦게 인지했고, 그제야 해킹 피해를 당했음을 알아챘다. 그는 "해당 로펌은 웹사이트 의뢰 감소에 대한 모니터링과 이상 징후에 대한 알림 시스템을 사전에 갖췄어야 한다"고 말한다.

식별해야 할 문제들 — 웹 트래픽 감소와 같은 — 은 기업마다 다르며, 하나 이상일 가능성이 높다. 에콜스는 많은 경우, 조직은 전력 공급에 영향을 미칠 수 있는 사고에 대비하고자 할 것이며, 이를 위해 본사와 독립된 발전기를 배치해 공격의 영향을 받지 않도록 준비하는 조치를 취할 수 있다고 말한다.

United Airlines의 디지털 기술 및 사이버 보안 감사 이사인 DC 창(Chang)에 따르면, 다가올 일에 대비하기 위해서는 현재의 사이버 보안 환경을 맥락 속에서 이해해야 한다. 20년 전에는 대부분의 조직이 자체 데이터 센터를 보유하고 있었고, 사이버 보안은 어느 정도 물리적인 문과 창문 뒤에 서버를 두고 잠그는 것으로 관리되었다. 그러나 오늘날 데이터는 가상 환경에 저장되며, 이는 전 세계의 악의적 행위자들에게 취약할 수 있다.

"디지털 환경에서는 우리가 관리해야 할 창과 문이 수천, 수만 개에 이르며, 이들은 매일 추가되고 제거되고 있다"고 창(Chang)은 말한다. 조직은 위기 상황에서 필요한 회복탄력성을 개발하기 위해 디지털 가속화의 속도와 범위에 대해 인식할 필요가 있다.

사이버 회복탄력성이란
"사이버 자원을 사용하는
또는 사이버 자원에 의해
가능해진 시스템이, 악조건,
스트레스, 공격, 손상 등의
상황을 예측, 견디고, 복구하며,
적응할 수 있는 능력을
의미한다."

- 미국 국립표준기술연구소(NIST)

거버넌스와 문화

Warren Averett의 리스크 자문 및 검증 서비스 그룹의 수석 관리자 저스틴 헤들리에 따르면, 거버넌스는 사이버 회복탄력성 구축에 있어 핵심적인 역할을 한다. 그는 "우리는 직원들이 보안에 취약한 비밀번호를 사용하거나 의심스러운 링크를 클릭하기 때문에 직원이 약점이라는 말을 계속 듣는데, 리더들이 참여하지 않는다면 직원들에게 자신의 역할을 다하길 기대할 수 없다"고 말한다.

여러 측면에서 사이버 보안은 단순한 기술 문제가 아니라 조직 문화의 문제이다. 에콜스는 "조직 구성원 90%의 사고방식을 바꾸더라도, 단 한 사람이 이메일의 링크를 클릭하면 회사 전체가 위태로워질 수 있다"고 말한다. 사이버 보안에 대한 인식이 높은 조직 문화는 조직의 기대 수준을 명확히 하고, 소비자와 비즈니스 파트너에게 신뢰를 제공한다. 그는 "은행은 이해관계자의 신뢰에 의존하기 때문에 사이버 회복탄력성을 가장 먼저 구축한 그룹 중 하나였다"고 설명한다.

헤들리는 리더들이 단순히 분기별로 사이버 보안 팁을 담은 이메일을 발송하거나 기초적인 연례 보안 교육을 제공하는 수준을 넘어서, 사이버 보안 문화를 조성할 것을 권장한다. 그의 조직에서는 직원들에게 자체적으로 가짜 피싱 이메일을 발송하고, 해당 이메일 내 의심스러운 링크를 클릭한 직원들에게 추가 교육을 제공하는 방법을 사용한다. 그는 "사이버 거버넌스가 실제로 어떻게 작동하는지를 보여주어야 한다. 단지 이론으로 끝나서는 안 된다"라고 강조한다.

규제의 영향

최종 확정된 규정인 **「사이버보안 리스크 관리, 전략, 거버넌스 및 사고 공개 (Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure)」**에 따라 미국 증권거래위원회(SEC)는 상장기업에게 중대한 사이버보안 사고를 공개하고, 사이버 리스크를 어떻게 평가, 식별 및 관리하는지를 주기적으로 공시하도록 요구함으로써 조직에 대한 기대치를 높였다. 창(Chang)은 이 규정이 "전 세계 모든 조직이 반드시 고려해야 할 본질적인 사안"을 부각한다고 말한다.

헤들리는 이 규정이 다른 여러 요건들과 더불어, 조직으로 하여금 사이버 보안 실무가 실제로 운영되고 있음을 보장하도록 강제한다고 말한다. 그는 IT 기능이 종종 고립된 구조에서 운영되며, 리더들은 그 작동 방식을 완전히 이해하지 못한 채 묵시적으로 신뢰하는 경우가 많다고 지적한다. 그는 "이러한 방식은 변화해야 한다"고 강조하며, 조직 전반에 걸쳐 내부 데이터와 고객 데이터를 어떻게 다루고 사이버 문제에 어떻게 대응할지에 대한 공통된 이해가 필요하다고 덧붙인다.

많은 규제가 그러하듯, "궁극적으로는 투명성이 핵심이 될 것"이라며 "중대한 침해 사고가 발생했을 때, 기업은 그 사고에 어떻게 대응할 것인지에 대한 명확한 프로세스를 갖추고 있어야 한다." 라고 에콜스는 말한다.

- 68%의 침해 사고는 사회공학적 공격에 속아 넘어가거나 실수를 저지르는 등 악의적이지 않은 인간적 요인에 의해 발생하였다.
- 사용자가 피싱 이메일에 속아 넘어가는 데 걸리는 시간의 중간값은 60초 미만이다.
- 침해 사고의 15%는 제3자 또는 공급업체와 관련이 있으며, 여기에는 소프트웨어 공급망, 호스팅 파트너 인프라, 또는 데이터 관리인도 포함된다.

출처: Verizon Business 2024 데이터 유출 조사 보고서

AI의 도입 추가

인공지능(AI)은 사이버 문제를 예방하고, 공격 이후 회복탄력성을 강화하는 데 있어 매우 유용한 도구가 될 수 있다. 저스틴 헤들리는, 차세대 방화벽이나 지점 보호 시스템(point protection systems)과 같은 기술은 데이터 트래픽을 분석하고 조사해야 할 이상 징후를 찾아내는 과정을 보다 용이하게 만든다고 설명한다. 그는 "최근 몇 년간 AI의 활용은 게임 체인저가 되었으며, 앞으로도 기업들이 공격을 탐지하고 대응하는 능력을 향상시키는 데 도움을 줄 것"이라고 말한다.

AI는 동시에 조직을 겨냥한 무기로 사용될 수도 있다. 마이클 에콜스는 "만약 간과해 온 취약점이 있다면, AI는 해커들이 이를 찾아내는 데 도움을 줄 것"이라고 경고한다.

헤일리에 따르면 조직은 새로운 도구를 통해 얻을 수 있는 효율성 증대와 보안 및 개인정보 보호의 필요성 사이에서 균형을 유지해야 한다. 새로운 기술은 반복적인 작업을 제거하는 데 도움이 되지만, 이러한 작업에는 종종 민감 정보를 프로그램에 입력하는 과정이 포함된다. 그는 "사람들이 해당 기술을 완전히 이해하지 못한다는 점을 악의적 행위자들이 알고 있기 때문에, 이러한 기술을 겨냥한 공격이 계속 발생하고 있다"고 지적하는데, 이로 인해 프로그램에 포함된 민감 정보가가 특히 취약해질 수 있다.

회복탄력성을 구축하기 위해 조직은 지속적으로 진화하는 기술에 대해 구성원을 교육하고, 기술 사용이 조직의 리스크 수용 수준에 부합하는지 확인해야 한다. 헤들리는 "기업이 최고의 기술과 역량을 보유하고 있더라도, 사용자가 생성형 AI(GenAI) 도구를 통해 의도치 않게, 혹은 때로는 의도적으로 데이터를 외부로 유출할 수 있다"고 말한다.

에콜스는 조직이 전통적인 사이버 공격 방식 또한 간과하지 않도록 주의해야 한다고 말한다. 그는 많은 사이버 문제들이 새로운 기술보다는 잘못된 설정, 정립된 절차의 미준수와 같은 기존의 문제들에서 기인한다고 지적한다. 또한 많은 침해 사고가 이미 알려졌지만 아직 해결되지 않은 취약점이나 설치되지 않은 패치(paches)와 관련되어 있다고 말한다. 이러한 이유로 최종 사용자를 대상으로 한 기존 위협 및 신종 위협에 대한 교육이 특히 중요하다. 그는 "감사인은 표면만 보지 말고 그 이면을 들여다보며, 무관심으로 인해 발생한 숨겨진 취약점을 찾아내기 위해 고객에게 올바른 질문을 던져야 한다"고 강조한다.

> 이해관계자, 특히 조직의 이사회와 최고경영진은 사이버 사고 대응 및 복구 통제가 잘 설계되고 효과적이며 효율적으로 구현되었는지를 확인하기 위해 독립적이고 객관적이며 전문적인 검증 서비스를 신뢰한다. 내부감사 기능은 이러한 서비스를 국제내부감사표준(Standards)에 부합하게 제공하고, 특히 조직의 정보기술 및 정보보안 기능에서 명시적으로 사용하는 일반적으로 인정된 통제 프레임워크를 참조함으로써 조직에 가치를 더한다."
>
> *출처: 글로벌 기술 감사 가이드(Global Technology Audit Guide): 사이버 사고 대응 및 복구 감사, 제2판, 글로벌 실무 가이드(Global Practice Guide), 내부감사인협회(The Institute of Internal Auditors), 2024년*

내부감사가 회복탄력성 향상에 기여할 수 있는 방법

에콜스는 이러한 환경 속에서 내부감사는 감사 결과를 조직의 회복탄력성을 강화하고 사이버보안 취약점을 식별하는 방향으로 구조화하여, 고객이 허술한 사이버보안이 초래할 수 있는 잠재적 결과를 이해하도록 도와야 한다고 말한다. 고객들은은 최악의 상황이 자신들에게 일어나지 않을 것이라고 가정할 수 있지만, 내부감사인은 이러한 불신을 잠시 유보하고 상상하기 어려운 상황까지 고려할 수 있어야 한다. 예를 들어, 에콜스는 한 고객이 소셜미디어 계정에 기업 이메일 주소 사용을 금지하는 모범 사례를 가지고 있었지만, 이를 공식 정책으로 문서화하지는 않았던 사례를 언급한다. 이 접근 방식의 오류는 작년 말 MGM이 심각한 데이터 침해 사고를 겪으면서 명확

해졌다. 해당 침해에 대한 조사 결과에 따르면, 한 직원이 소셜미디어 플랫폼에 업무용 이메일을 사용하고 있었고, 해커는 링크드인(LinkedIn)에서 해당 직원의 정보를 찾아내 MGM의 IT 헬프데스크에 전화를 건 다음 그 직원을 사칭했다. 이를 통해 해커는 시스템 접근에 필요한 자격 증명을 획득하고 MGM의 시스템에 악성 코드를 심을 수 있었다. 에콜스는 "모범 사례는 많은 사람들의 경험에서 도출된 것이며, 가능하다면 공식 정책으로 제정되어야 한다"고 강조한다.

내부감사인은 또한 감사에서의 컴플라이언스 측면이 사이버 회복탄력성 구축을 위한 첫걸음에 불과하다는 점을 이해해야 한다. 에콜스는 "컴플라이언스는 곧 보안인 것은 아니다"라고 말한다. 내부감사인은 자신이 발견한 사항을 고객 조직의 보안 강화를 위한 심도 있는 인사이트로 전환하는 데 집중해야 하며, 고객 팀이 아직 인식하지 못했거나 답을 찾지 못한 질문을 제기해야 한다.

에콜스는 "이 질문에 대한 답을 구하고자 하지 않거나 답을 찾지 않는 행위 자체가 하나의 취약점을 초래할 수 있다는 점을 고객에게 명확히 설명할 수 있어야 한다"고 강조한다.

투명성은 매우 중요하다. 내부감사인은 감사 범위와 계획된 테스트 절차, 그리고 발생한 문제에 대해 명확히 해야 한다. 헤들리는 "특히 IT 리스크와 관련된 경우에는 조기에 자주 소통하는 것이 중요하다"고 강조하며, 내부감사인이 성급하게 판단을 내리기보다는 고객 팀의 사고 과정을 열린 자세로 듣고 협업을 장려할 것을 권고한다.

헤들리는 IT 팀이 다양한 사업 부문의 요구를 충족시키느라 종종 과중한 업무에 시달리며, 애플리케이션 운영 유지부터 일상적인 하드웨어 문제 처리까지 모든 책임을 지는 경우가 많다고 설명한다. 이로 인해 사이버보안은 항상 최우선 순위가 아닐 수 있다. 내부감사인은 이러한 어려움에 대한 인식을 제고하고, 각 팀들이 이를 해결할 수 있도록 교육함으로써 감사를 실질적인 가치 창출 활동으로 만드는 데 기여할 수 있다.

헤들리는 "내부감사인은 기업의 회복탄력성을 강화하는 데 있어 파트너가 될 수 있다"고 말한다. 그들은 특히 회사 리더와 IT 팀 간의 의사소통 단절을 해소하는 데 도움을 줄 수 있다. IT 팀과 리더는 종종 서로 다른 언어를 사용하기 오해가 발생하기 쉽지만, 내부감사인은 비즈니스 리스크와 IT 리스크를 모두 이해하고 있기 때문에 그 간극을 메우는 가교 역할을 수행할 수 있다.

창(Chang)은 내부감사인이 과거의 관행에서 벗어나 사이버 리스크 및 관련 문제 해결에 대한 이해를 새롭게 형성할 수 있다고 말한다. 조직이 기존의 전통적인 비즈니스 연속성 계획이나 재해 복구 방식에서 벗어나고 있는 상황에서, 내부감사인은 조직이 보다 다면적이고 정교한 접근 방식을 채택하도록 도울 수 있다. 내부감사인은 분절된 정보와 데이터를 수집·가공하여 설득력 있는 이야기로 엮어내고, 이를 통해 더 나은 의사결정을 유도하는 '스토리텔러'의 역할을 수행함으로써 이러한 노력을 강화할 수 있다.

IT 및 보안 운영 의사결정권자를 대상으로 한 설문조사에 따르면:

- 전체 응답자의 단 2%만이 사이버 공격 발생 후 24시간 이내에 데이터를 복구하고 비즈니스 프로세스를 복원할 수 있다고 응답하였다.
- 69%는 지난 1년 동안 조직이 랜섬을 지불한 적이 있다고 답했으며, 이 중 77%는 랜섬 지불을 금지하는 명확한 정책이나 절차를 보유하고 있음에도 불구하고 지불했다.
- 42%는 자사 조직이 민감 데이터를 식별하고 관련 데이터 프라이버시 법규를 준수할 수 있다고 답했으며, 나머지는 이를 동시에 수행할 수 있는 적절한 IT 및 보안 역량을 갖추고 있지 않다고 응답했다.

출처: : Cohesity 글로벌 사이버 회복탄력성 보고서 2024(Cohesity Global Cyber Resilience Report 2024)

불리한 상황 극복

결국 회복탄력성이란 공격의 불가피성을 받아들이고, 조직의 외부 방어선이 완벽하지 않다는 것을 전제로 하는 것이라고 에콜스는 말한다. 이러한 노력의 일환으로, 조직은 자신들이 불공정한 싸움에 처해 있다는 사실을 인식해야 한다. 창(Chang)은 "조직은 자신들에게 가해지는 모든 공격을 100% 차단하려 애쓰지만, 해커는 단 하나의 문만 열면 피해를 줄 수 있다"고 말한다. 그는 "수비하는 쪽이 공격하는 쪽보다 훨씬 더 어려운 일"이라고 덧붙인다. 내부감사는 조직이 사이버 보안에서 성공할 확률을 높일 수 있도록 필요한 통찰과 정보를 제공할 수 있다.

파트 3

새로운 제로 트러스트 경계 설정

전문가 소개

아담 콘케(Adam Kohnke)

위스콘신주 매디슨에 거주하는 아담 콘케는 화학 제조 기업인 Charter Next Generation의 정보보안 관리자이다.

훌리오 티라도(Julio Tirado)

훌리오 티라도는 오클라호마주 털사에 본사를 둔 SpiritBank의 부행장이자 내부감사 및 준법감시 담당 이사이다.

네트워크 보안을 유지하기 위한 프로세스와 통제를 갖추는 것은 모든 조직에서 기본 요건이 되어야 한다. 그러나 기술이 발전하고 네트워크가 더욱 방대하고 복잡해짐에 따라, '안전한 네트워크'의 기준도 변화하고 있다. 가장 중요한 변화 중 하나는 위치 중심 보안 모델에서 데이터 중심 보안 모델로의 전환이다. 우리는 이 모델을 "제로 트러스트(Zero Trust)"라고 부른다.

제로 트러스트(Zero Trust)란 무엇인가?

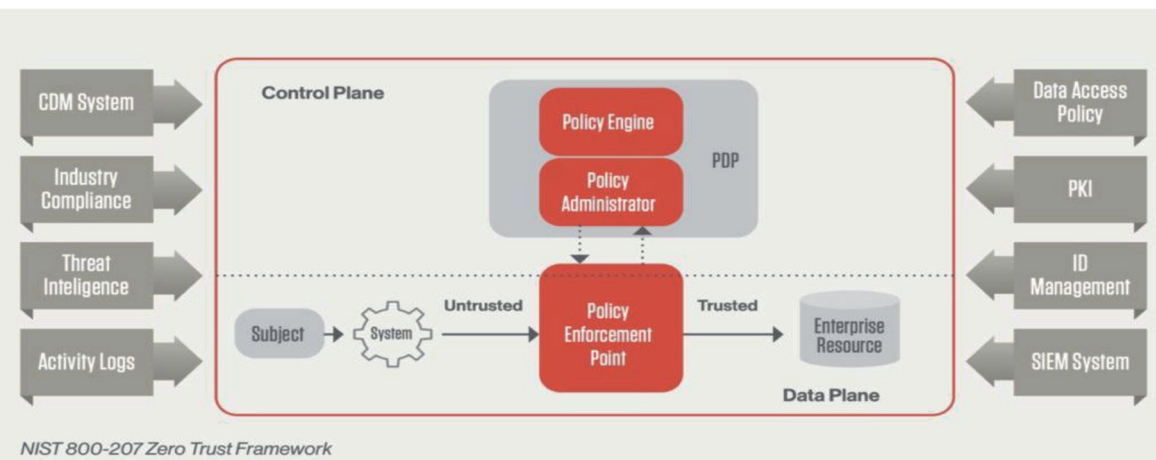
일반적으로 제로 트러스트 보안 프레임워크는 조직 내부와 외부를 포함하여 네트워크 내에서 활동하는 모든 사용자가 애플리케이션과 데이터에 접근하기 전에 인증받을 것을 요구하며, 이후에도 정기적으로 지속적인 검증을 거쳐야 한다. 그 명칭에서 알 수 있듯이, 이 시스템에서는 "신뢰(trust)", 더 구체적으로는 "신뢰하되 검증하라(trust but verify)"라는 개념이 적용되지 않으며, 조직과 관련된 자산에 대한 모든 접근은 조직의 정책에 따라 지속적으로 정당화되고 평가되어야 한다.

기존의 사이버 보안 모델은 네트워크의 위치를 기반으로 설계되었지만, 제로 트러스트 시스템에서는 "네트워크"의 개념이 덜 엄격하게 정의된다. 조직의 네트워크는 로컬에 있을 수도 있고, 클라우드 기반일 수도 있으며, 또는 이 둘의 하이브리드 형태일 수도 있다. 특히 COVID-19 팬데믹 이후 원격 근무 시대가 도래함에 따라, 하이브리드 혹은 완전한 클라우드 기반 시스템이 표준이 되었고, 사이버 보안 프레임워크 역시 이에 맞춰 진화해야 했다.

다음과 같은 여러 공식적인 제로 트러스트 프레임워크가 존재한다:

- 미국 국립표준기술연구소(NIST)의 **표준 800-207**: 2021년부터 미국 연방 기관에서 사용이 의무화된 프레임워크이다 (그림 1 참조).
- Google의 **BeyondCorp.**
- Microsoft의 **제로 트러스트 전략(Zero Trust Strategy).**
- 미국 사이버보안 및 기반시설 보안국(CISA)의 **제로 트러스트 성숙도 모델(Zero Trust Maturity Model).**

그림 1



출처: *제로 트러스트 네트워크(Zero Trust Networks) | 미국 국립표준기술연구소(NIST)*

이들 프레임워크는 각각 고유한 특성을 가지고 있지만, 공통적으로 다음과 같은 기본 원칙을 공유한다:

- 모든 자원에 대해 지속적으로 접근을 검증한다.
- 외부 또는 내부 침해 발생 시 피해 범위를 최소화한다.
- 상황(context)을 파악하기 위해 IT 인프라로부터 행동 기반 데이터(behavioral data)를 활용한다.

이러한 시스템으로의 전환은 상당한 변화처럼 보일 수 있지만, 이는 기존 시스템을 대체하기 위한 것이 아니라는 점에 주목할 필요가 있다. 화학 제조 기업 Charter Next Generation의 정보보안 관리자 아담 콘케는 "제로 트러스트는 현재의 네트워크 보호 모델이나 인프라를 완전히 대체하려는 것이 아니라, 이를 보완하여 네트워크 보호를 강화하려는 것"이라고 설명한다. 그는 "기존 시스템인 방화벽, 웹 프록시, 경계 격리 메커니즘(boundary isolation mechanisms) 등은 제대로 작동하지 않았기 때문에, 제로 트러스트는 이를 확장하는 개념"이라고 덧붙인다.

IBM에 따르면, 2024년 단일 데이터 침해 사고의 평균 비용은 488만 달러에 달했다. 또한, 침해 사고의 평균 지속 기간은 식별에서 완전한 차단까지 총 292일에 이르렀다. 이는 기존의 네트워크 보호 방식만으로는 충분하지 않으며, 이에 대한 집중적인 개선이 필요함을 명확히 보여준다.

내부감사의 역할

세부 사항은 다양할 수 있지만, 내부감사인은 제로 트러스트 시스템의 구현 및 유지 관리와 관련된 다양한 책임을 맡을 수 있다. 다음은 내부감사 평가가 가장 큰 가치를 발휘할 수 있는 주요 영역을 예시로 제시한 것이다.

보호 표면(Protected Surfaces)의 정의

기존 사이버 보안 시스템은 기업 네트워크의 경계 내에서 보안 매개변수를 정의하는 데 중점을 두었다. 방화벽과 VPN 시스템은 이러한 개념을 기반으로 설계되었으며, 민감 정보나 취약 정보를 네트워크 경계(parameters)로부터 최대한 멀리 떨어뜨리는 방식으로 보호해 왔다. 그러나 제로 트러스트 시스템(zero-trust system)에서는 경계보다는 데이터, 애플리케이션, 자산, 서비스(Daas: Data, Applications, Assets, Services)의 집합에 초점을 맞춘다. 이러한 집합을 통칭하여 "보호 표면(protect surfaces)"이라 부른다.

이러한 보호 표면이 적절하게 식별되었는지를 보장하는 것은 포괄적인 내부감사 평가에서 핵심적인 요소가 되어야 한다.

SpiritBank의 부행장이자 내부감사 및 준법감시 담당 이사인 훌리오 티라도는 "평가는 조직의 데이터 분류 정책을 검토하여 시스템과 데이터가 적절히 분류되어 있는지, 그리고 각 항목에 대해 마련된 보호 정책이 적절한지를 확인하는 데 집중해야 한다"고 말한다.

티라도는 보호 표면은 단지 데이터에만 국한되지 않는다고 덧붙인다. 민감 정보에 접근하는 데 사용되는 물리적 자산 또한 재고가 체계적으로 관리되고, 정기적으로 평가될 수 있도록 관련 프로세스와 절차가 마련되어 있어야 한다.

"평가는 조직의 데이터 분류 정책을 검토하여 시스템과 데이터가 적절히 분류되어 있는지, 그리고 각 항목에 대해 마련된 보호 정책이 적절한지를 확인하는 데 집중해야 한다"

- 훌리오 티라도, SpiritBank

거래 흐름 도식화 검증

보호 표면이 식별되었음을 확인한 후, 평가 프로세스의 다음 단계는 이러한 모든 DAAS(Data, Applications, Assets, Services) 시스템들이 서로 어떻게 상호작용하는지에 대해 이해관계자들이 명확히 인식하고 있는지를 검증하는 것이다. IT 팀은 이 시스템들이 서로에게 접근하는 방식과 그 사용이 어떤 결과를 초래할 수 있는지를 설명하는 복잡한 포트(port), 네트워크 트래픽 기준, 프로토콜 등의 상호 연결망을 상세히 도식화한, 문서화된 다이어그램을 보유하고 있어야 한다.

대부분의 조직에서 내부감사 기능이 이러한 다이어그램의 정확성을 독립적으로 검증할 수 있는 충분한 지식이나 경험을 갖추고 있지 않을 수 있지만, 콘케는 내부감사부서가 이해관계자 또는 신뢰할 수 있는 제3자와 협력하여, 묘사된 내용이 충분한지 보증하기 위한 검증 테스트가 수행되었는지를 확인할 수 있다고 말한다. 그는 "중요한 것은 각 다이어그램에 관련된 DAAS가 포함되어 있는지, 충분한 세부정보가 제공되어 있는지, 그리고 앞 단계에서 정의된 초기 보안 정책이 수정되었는지 또는 추가적인 통제가 필요한지를 확인하는 것"이라고 강조한다.

제로 트러스트 정책의 수립 및 지속적 개선 검증

제로 트러스트 정책은 각 보호 표면별로 구체적으로 수립되어야 하며, 다음과 같은 핵심 질문에 대한 답을 포함해야 한다:

- 누구에게 조직의 DAAS 시스템 접근이 허용되어야 하는가?
- 어떤 애플리케이션이 조직의 DAAS 시스템에 접근할 수 있는가?
- 언제 기업의 DAAS 시스템에 접근이 이루어져야 하는가 또는 이루어지고 있어야 하는가?
- 조직의 DAAS 시스템은 어디에 위치해 있는가?
- 왜 조직의 DAAS 시스템에 접근해야 하는가?
- 어떻게 조직의 DAAS 시스템에 대한 접근이 허용되어야 하는가?

제로 트러스트 정책의 타당성과 적절성을 평가하기 위해서는, 조직 네트워크가 확장되고 진화함에 따라 IT 이해관계자들과의 지속적인 상호작용이 필수적이다. 티라도는 "제로 트러스트는 도달점(destination)이 아니다"라며, "보안 정책과 DAAS 보호 요건은 프로세스가 전개됨에 따라 함께 진화해야 한다"고 말한다.

티라도는 네트워크에 유입되거나, 유출되거나, 내부를 통과하는 모든 유형의 트래픽을 다룰 수 있는 점점 지속적으로 개선되는 정책을 마련하는 것이 목표가 되어야 한다고 강조한다. 그는 "네트워크 내에 출처나 목적을 식별할 수 없는 것이 존재해서는 안 된다"고 말하며, "내부감사인은 평가 시 검토가 수행되고 있는지, 그 검토가 충분한 수준으로 이루어지고 있는지, 그리고 현행 정책이 그 결과를 정확히 반영하고 있는지를 판단해야 한다"고 덧붙인다.

제로 트러스트 구조 모니터링

앞선 예시들에서 알 수 있듯이, 지속적인 모니터링은 제로 트러스트 프레임워크의 성공에 있어 매우 중요하다. 기존 시스템에서는 보통 보안 매개변수에 초점을 맞춰 모니터링이 이루어졌지만, 제로 트러스트 시스템의 모니터링은 사용자, 장치, 서비스 중심으로 수행된다. 영국 국가사이버안보센터(National Cyber Security Centre)는 제로 트러스트 가이드라인에서 "네트워크의 성능을 측정하고, 네트워크에 연결된 모든 장치를 식별하며, 불법 장치 및 악의적 활동을 탐지하기 위해 네트워크에 대한 모니터링을 수행해야 한다"고 강조하고 있다. 이는 온프레미스 서비스(On-premise Services)를 운영하는 경우에 특히 중요하지만, 모

> 네트워크의 성능을 측정하고, 네트워크에 연결된 모든 장치를 식별하며, 불법 장치 및 악의적 활동을 탐지하기 위해 네트워크에 대한 모니터링을 수행해야 한다.
>
> - 영국 국가사이버안보센터 (National Cyber Security Centre)

바일 장치 관리(Mobile Device Management) 또한 점점 더 일반화됨에 따라 동일한 수준으로 고려되어야 한다.

"우리 회사 같은 기업들은 사용자가 동의하는 한 해당 장치에 대한 일정 수준의 제어를 제공하는 모바일 기기 관리(Mobile Device Management, MDM) 소프트웨어를 배포할 것이다"라고 티라도는 말한다. "이 소프트웨어는 활동을 모니터링하고, 위험한 사이트에 대한 접근을 제한하며, 해당 기기에 설치할 수 있는 특정 소프트웨어를 제한하고, 해당 시스템에 업데이트를 배포하기 위한 제어 기능을 제공할 것이다."

또한 모니터링은 시스템의 실제 사용뿐만 아니라 사용되는 시간의 길이까지 포함해야 한다. 영국 국가사이버안보센터(National Cyber Security Centre)는 "정상적인 근무 시간이나 일반적인 근무 위치와 같은 사용자 행동은 모니터링해야 할 중요한 지표이다"라고 명시하고 있다.

네트워크의 특정 요구를 충족하도록 설계된 다양한 모니터링 시스템이 존재하지만, 일반적으로 이러한 시스템은 수집된 데이터를 중앙으로 전송하여 분석이 가능하도록 한다. 시간이 지나면서 이 정보는 거래량, 자산 간 통신, 사용자 활동 등과 같은 변수에 대해 '정상적인 행동'을 구성하는 기준선(baseline)을 설정하게 된다.

내부감사인은 평가를 통해 이러한 데이터에 대한 정기적인 검토가 이루어지고 있는지, 경영진이 해당 업무에 대해 적절한 책임을 지고 있는지를 확인할 수 있으며, 그 결과로 도출된 기준선이 네트워크의 실제 상황을 정확하게 반영하는지 확인할 수 있다.

"내부감사인에게 있어 많은 부분은 결국 거버넌스 문제로 귀결된다"고 티라도는 말한다. "시스템이 스스로 유지되지는 않기 때문에, 경영진은 시스템 보안에서 자신들이 맡은 역할을 인식해야 한다. 보안 정책의 변경은 기준선이 '정상'과 '비정상'으로 정의하는 것에 따라 결정된다. 이 기준선은 경영진의 검토를 통해 설정되는 것이다."

기준선 수립

사이버 보안 또는 리스크 관리의 많은 요소들과 마찬가지로, "모두에게 맞는 하나의 모델"은 존재하지 않으며, 이에 따라 내부감사 기능이 기여하는 방식도 크게 달라질 수 있다. 티라도(Tirado)는 "이는 가용 자원(resources)에 따라 다르다. 조직의 규모에 따라 다르며, 내부감사팀의 임무에 따라 달라진다"고 말한다.

그는 기준선을 설정하기에 좋은 출발점은 일반적인 감사 시스템과 마찬가지로 검증 제공 프로세스를 도식화하는 것이라고 말한다. "예를 들어, 사베인스-옥슬리(Sarbanes-Oxley)를 생각해보자"라고 그는 덧붙인다. "모든 상장기업은 재무제표와 관련된 내부통제를 도식화하여 해당 매트릭스를 개발해야 한다. 그리고 이러한 도식화의 일환으로, 특정 기간(예: 1년)동안 테스트 절차를 수립하게 된다. 제로 트러스트에 대해서도 동일한 접근방식을 취할 수 있으며, 회사의 규모, 가용 자원 등을 고려하여 연중에 걸쳐 검증을 세분화하여 진행해야 한다."

- 제로 트러스트 모델의 초기 단계에서 고려할 수 있는 간단한 통제 항목의 예는 다음과 같다:
- 데이터 암호화
- 보안 인식 교육
- 사고 대응 계획
- 엔드포인트 탐지 및 대응 시스템 (Endpoint Detection and Response systems)
- 마이크로 세분화(Micro-segmentation)
- 컴플라이언스 모니터링
- 행동 분석 및 사용자 행위 분석(User and Entity Behavior Analytics)

하지만 모든 사례에서 공통적으로 관통하는 핵심은, 내부감사가 제로 트러스트 시스템의 구현과 지속적인 개선을 지속적으로 옹호해야 할 의무가 있다는 점이다. 제로 트러스트 모델이 중점을 두는 요소에 따라 이러한 업무를 지원하는 다양한 시장 자원이 존재한다. 예를 들어, 랜섬웨어 리스크와 관련해서 티라도는 FBI와 민간 부문의 협력을 통해 개발된 무료 정보 공유 도구인 인프라가드(InfraGard)를 활용한다. 티라도는 매일 아침 단 몇 분이면 이 도구를 통해 산업 내외부에서 발생한 최신 랜섬웨어 공격 및 데이터 유출에 대한 정보를 신속하게 파악할 수 있다. 그는 "이러한 공격의 규모는 경계 기반 보안 모델을 넘어선 접근 방식을 요구한다"고 설명하며, "리스크 환경이 어떤 모습인지, 그리고 무엇이 위협받고 있는지를 이해관계자에게 지속적으로 알리는 것이 내부감사의 최우선 과제다."라고 강조한다.

또한, 이 전환이 반드시 한 번에 이루어져야 하는 것은 아니라는 점도 주목할 필요가 있다. "부분적인 형태라도 제로 트러스트 모델은 엄청난 가치를 지닌다"고 티라도는 말한다. "결국 제로 트러스트 모델은 통제 항목들이 나열된 스프레드시트 열(column)로 귀결된다. 그게 20개일 수도 있고, 어쩌면 10개나 12개일 수도 있다. 그래도 5개보다는 훨씬 낫다."

기반은 이미 마련되어 있다

네트워크의 핵심적인 철학적 변화에도 불구하고, 내부감사인은 제로 트러스트의 개념을 대해 이해했다면 내부감사 기능의 책임이 예전과 완전히 달라져야 하는 것은 아니라는 점을 인식해야 한다. 제로 트러스트의 구현은 특정 상용 도구의 도입 가능성을 제외하고는 구조(architecture)나 인프라의 변경은 필요하지 않기 때문에, 이를 검증하는 시스템 또한 필요하지 않다.

실제로 모든 감사업무의 핵심 요소는 식별, 커뮤니케이션, 검증이며, 이러한 책임은 여전히 유효하다. 흔들리지 않는 자세, 국제내부감사 표준에 대한 준수, 그리고 학습하려는 의지만 있다면, 제로 트러스트 네트워크 구조로의 전환은 조직이 더 이상 두려워할 일이 아니다.

이전 호

Global Perspectives and Insights의 이전 호를 보려면 **theiia.org/GPI** 를 방문하세요.

독자 의견

질문이나 의견은 **globalperspectives@theiia.org**로 보내주세요.

세계내부감사인협회(IIA) 소개

세계내부감사인협회(IIA)는 전 세계적으로 255,000명 이상의 회원을 보유하고 있으며, 200,000개 이상의 국제공인내부감사사(CIA)® 자격을 부여한 비영리 국제 전문가 협회입니다. 1941년에 설립된 IIA는 전 세계 내부감사 분야의 표준, 자격인증, 교육, 연구 및 기술 지침을 선도하는 기관으로 인정받고 있습니다. 자세한 내용은 **theiia.org**에서 확인할 수 있습니다.