최근 보안 동향을 고려한
기업의 보안 거버넌스 및 대응체계

LG유플러스 CISO 홍관희

발표 개요

- 최근 보안 동향 및 이슈
- 보안 거버넌스
- 보안 거버넌스 개선 방안
- 기업 적용 방안
- 대응 체계

최근 보안 사고 동향

최근 사이버 위협은 인공지능(AI)과 같은 신기술을 악용하여 더욱 지능화되고 있으며, 공격 대상과 범위가 전 산업 분야로 확대되고 있습니다
또한, 공격의 목표가 '시스템 파괴'에서 '데이터 무기 화'로 변화하면서, 기업 평판 및 고객 신뢰에 직접적 타격을 주는 형태로 진화중입니다.

AI 악용 공격

- 딥페이크, 딥보이스 기술을 활용한 피싱 및 협박
- LLM을 이용한 악성 스크립트 제작
- 특정 개인 및 그룹을 정교하게 타겟팅하여 공격 성공률 향상
- 디지털 성범죄 등 사회적 문제로 확산

공급망 공격

- 보안이 취약한 협력사(서드파티)를 통해 악성코드 유포
- 최종 목표 기업을 공격하기 위한 우회 경로로 활용
- 공격 통로로 활용되어 연쇄적인 피해 발생

클라우드 환경 취약점

- 클라우드 설정 오류, 접근 제어 미흡으로 데이터 유출
- 탈취된 계정 정보(IAM)를 이용한 무단 접근
- 2024년 기준, 클라우드 보안 사고를 겪은 기업의 85%가 심각한 운영 중단 경험

다중 갈취 랜섬웨어

- 데이터 암호화로 업무 또는 서비스 마비
- 중요 정보 유출 협박
- 다크웹 공개, DDoS 공격으로 추가 압박

이러한 동향은 단순히 기술적 방어를 넘어, 전사적 차원의 체계적인 보안 거버넌스와 신속한 대응 체계의 중요성을 부각시키고 있습니다.

주요 보안 사고 사례

통신사 해킹 사고

스텔스형 악성코드 'BPFDoor'를 통한 침투

- 피해 규모: 가입자 정보 (USIM 정보 등) 유출
- 이슈: CISO의 실질적 권한 부재, 네트워크 보안 조직과 정보보호 조직의 이원화

공급망 공격

보안이 취약한 협력사를 통한 악성코드 유포 및 침투

- 주요 대상: 다양한 산업군에서 다수 발생
- 이슈 협력사 보안 관리 및 감독 부재, 공급망 리스크 관리 체계 미흡

클라우드 데이터 유출

클라우드 설정 오류, 접근 제어 미흡으로 인한 데이터 유출

- 피해 현황: 2024년 클라우드 보안 사고 경험 기업의 85%가 심각한 운영 중단 경험
- 이슈: 클라우드 환경에 최적화된 보안 거버넌스 부재, 접근 제어 정책 미흡

AI 악용 공격

딥페이크, 딥보이스 기술을 활용한 피싱 및 협박, LLM을 이용한 악성 스크립트 제작

- 특징: 특정 개인 및 그룹을 정교하게 타겟팅하여 공격 성공률 향상
- 이슈: 신기술 도입에 따른 리스크 평가 및 관리 체계 부재, AI 윤리 정책 미비

공통적인 취약점

보안 사고의 근본 원인은 기술적 결함보다 보안 거버넌스의 부재에서 비롯됨 - 책임과 권한의 불균형, 통합 관리 체계 미흡, 경영진의 인식 부족

보안 사고의 근본 원인

보안 사고의 근본 원인은 기술, 관리, 인적 측면의 복합적인 문제에서 비롯됩니다.

기술적 원인

고도화된 악성코드

고도화된 BPFDoor와 같은 스텔스형 악성코드가 기존 탐지 시스템을 우회하며, 방어 기술의 한계를 보여줍니다.

취약점 관리 미흡

제로데이 공격뿐만 아니라 이미 알려진 취약점에 대한 신속한 패치 및 관리가 이루어지지 않아 공격의 빌미를 제공합니다.

보안 설정 오류

특히 클라우드 환경에서 복잡한 설정과 관리 미흡으로 인해 데이터가 외부에 노출되는 사고가 빈번하게 발생합니다.

관리적 원인

부실한 보안 거버넌스

CISO의 권한 부재, 조직 간의 단절, 통합 관리 체계 미흡 등은 가장 핵심적인 관리적 원인입니다.

공급망 리스크 관리 부재

협력 업체의 보안 수준을 점검하고 관리하는 체계가 없어 공급망이 공격의 통로로 악용됩니다.

사고 대응 프로세스 미비

침해 사고 발생 시 신속하게 탐지, 분석, 복구, 보고로 이어지는 체계적인 대응 프로세스가 부재하여 피해가 확산됩니다.

인적 원인

사회공학적 기법

이메일 피싱, 스미싱 등 사용자의 심리를 이용한 공격은 여전히 가장 효과적인 초기 침투 경로 중 하나입니다.

내부자 위협

악의적인 의도를 가진 내부자뿐만 아니라, 보안 규정을 준수하지 않거나 실수로 정보를 유출하는 비의도적 내부자 역시 큰 위협입니다.

보안 인식 부족

전사적인 보안 교육 및 훈련이 부족하여 임직원들이 보안의 중요성을 인지하지 못하고 위험한 행동을 하는 경우가 많습니다.

기술적 보안 강화 방안

진화하는 사이버 위협에 효과적으로 대응하기 위해 **최신 기술을 활용한 보안 강화 방안이 필요**합니다.

AI 및 머신러닝 기반 위협 탐지 및 분석

- AI 기반 보안 솔루션(SIEM, SOAR 등)을 통한 방대한 로그 데이터 실시간 분석
- 알려지지 않은 신종 위협이나 비정상 행위 조기 탐지
- 위협 탐지 시 차단, 격리 등 초동 조치 자동화로 대응 시간 단축

신속한 대응 | 자동화 | 지능형 위협 대응

빅데이터 활용 리스크 가시성 확보

- 전사 시스템의 모든 보안 관련 데이터 수집 및 분석
- 잠재적 리스크 식별 및 공격 표면 종합적 관리
- 데이터 기반의 객관적인 보안 투자 의사결정 지원

종합적 분석 | 선제적 위험 관리 | 투자 효율성

클라우드 보안

- 클라우드 환경의 설정 오류나 취약점 자동 탐지 및 해결
- 클라우드 인프라의 보안 지속적 강화
- 복잡한 클라우드 환경에서 거버넌스 공백 방지

설정 관리 | 규정 준수 | 취약점 관리

기술적 보안 강화는 단순한 솔루션 도입이 아닌, 보안 거버넌스를 효율적으로 지원하고 구현하는 수단으로 활용되어야 합니다.

보안 거버넌스 차원의 이슈

반복되는 대규모 보안 사고의 이면에는 기술적 결함이 아닌 **기업의 보안 거버넌스의 실패**가 근본 원인으로 존재합니다. 이러한 실패는 다음과 같은 공통 적인 패턴으로 나타납니다

보안 책임 및 권한의 불균형

CISO가 명목상 존재할 뿐, 실제 핵심 인프라에 대한 통제 권한 없이 IT 보안 등 일부 영역에만 관여하는 경우가 많습니다. 최근 통신사 해킹 사태는 CISO가 네트워크 보안에 대한 실질적 권한 없이 책임만 지는 구조적 문제를 명확히 보여주었습니다.

통합 거버넌스 부재

정보보호 조직과 네트워크 운영, 개발 등 타 부서 간의 협력 체계가 미흡하고 보안이 각 부서의 개별 과제로 취급되어 전사적 대응이 어렵습니다. 이는 조직 내 정보 단절과 책임 전가로 이어져 보안 공백을 야기합니다.

리스크 기반의 자율 보안 체계 미흡

많은 기업이 규정 준수에만 급급하여 수동적인 보안 활동에 머무르고 있습니다. 비즈니스 환경과 리스크를 스스로 분석하고 이에 비례한 보안 방안을 수립하는 능동적인 자율보안체계 구축이 미흡한 실정입니다.

경영진의 인식 부족 및 투자 소극성

보안을 비용으로만 인식하고 기업의 핵심 가치나 비즈니스 전략과 연계하지 못하는 경우가 많습니다. 이는 보안 전문 인력 및 예산 부족으로 이어져 보안 체계의 근본적인 취약점을 만듭니다.

컴플라이언스 중심 보안

전정한 보안이 아닌 규제 준수나 인증 획득에만 초점을 맞추는 “체크리스트 보안”은 수동적인 자세로 진화하는 새로운 위협에 대응력을 상실합니다.

보안 거버넌스란 무엇인가?

보안 거버넌스(Security Governance)는 조직의 정보 자산을 보호하고 비즈니스의 연속성을 보장하기 위한 체계적인관리 활동을 의미합니다 기업의 정보보호 활동이 방향을 **설정 받고 (Directed), 통제되며(Controlled), 책임을 지는(Accountable) 체계** 입니다.

보안 거버넌스의 핵심 요소

전략적 방향 제시 (리더의 방향 설정)

기업의 비즈니스 목표와 연계된 정보보호 목표와 전략을 수립합니다. 보안이 단순한 기술적 문제가 아닌 경영 전략의 일부로 자리매김하도록 합니다.

위험 관리

조직이 수용 가능한 위험 수준을 정의하고, 위험 기반의 합리적인 의사결정을 지원합니다. 모든 보안 활동은 식별된 위험에 비례하여 이루어집니다.

책임 있는 자원 사용

정보보호 활동에 필요한 예산, 인력 등 자원을 효과적으로 할당하고 관리합니다. 중복 투자를 방지하고 투자 효과(ROI)를 극대화합니다.

성과 측정 및 모니터링

수립된 보안 프로그램의 성공과 실패를 지속적으로 모니터링하고 평가하여 개선 활동으로 연계합니다. 성과 지표를 통해 객관적인 관리가 가능합니다.

결국 보안 거버넌스는 최고 경영진의 주도하에 정보보호를 기업의 핵심 가치로 인식하고,전사적인 참여를 통해 보안 활동을 비즈니스 프로세스에 내재화하는 과정입니다.

보안 거버넌스의 중요성

잘 수립된 보안 거버넌스는 단순한 비용 통제를 넘어 기업에 실질적인 전략적 가치를 제공합니다. 거버넌스는 **보안의 언어**와 **비즈니스의 언어**를 연결하는 핵심적인 **'번역 계층(Translation Layer)'** 역할을 합니다.

전략적 연계

보안 활동이 비즈니스 목표 달성을 직접적으로 지원하고, 시장 경쟁에서 승리하는 데 기여하는 전략적 자산으로 작용

가치 제공

한정된 보안 투자 자원을 최적화하여 비즈니스 가치 극대화, 위험 기반으로 가장 중요한 자산에 자원 집중

위험 관리

사이버 위협을 식별, 평가, 처리하는 체계적 프로세스 구축으로 사고 발생 후 수습이 아닌 사전 통제 가능한 상태로 전환

자원 최적화

인력, 예산, 기술 등 보안 자원이 효율적으로 사용되도록 보장, 중복 투자 방지와 일관된 보안 아키텍처 수립

성과 측정

KPI, KRI 등 객관적 지표로 보안 효과성 측정, "우리는 안전한가?"라는 질문에 데이터 기반의 구체적 답변 제공

준법 및 보증

법률, 규제, 계약상 의무 준수로 과징금/법적 분쟁 위험 최소화. 고객, 파트너, 투자자에게 신뢰 제공으로 경쟁 우위 확보

CISO는 단순히 뛰어난 기술 전문가가 아니라, **거버넌스의 언어와 프로세스를 활용하여 보안의 필요성을 비즈니스 가치와 리스크 감소의 관점에서 설득**하고, 이를 통해 조직의 전폭적인 지원과 자원을 확보해내는 비즈니스 리더입니다.

"보안 거버넌스는 비용이 아닌 기업의 핵심 가치를 보호하고 비즈니스 전략을 지원하는 투자입니다."

보안 거버넌스 체계 개선 방안

효과적인 보안 거버넌스는 조직의 구조와 문화에 깊이 뿌리내려야 합니다. 다음과 같은 조직 차원의 개선 방안을 통해 보안 거버넌스를 강화할 수 있습니다.

최고경영진의 리더십 확보

- 보안을 단순한 IT 비용이 아닌 비즈니스 리스크 관리의 핵심 요소로 인식
- 이사회 및 최고경영진이 보안 전략과 투자에 대한 최종 의사결정에 적극적 참여
- 경영진 성과평가에 보안 관련 지표 포함

보안 전담 조직 및 위원회 운영

- 전담 조직: 위협 분석, 보안 아키텍처, 침해 대응 등 전문 분야별 인력으로 구성된 조직 운영
- 보안 위원회: CISO를 위원장으로 IT, 법무, 인사, 재무 등 주요 임원, 부서장이 참여하는 정기적 위원회 운영
- 부서 간 협업 및 정보 공유 체계 구축

CISO의 독립성 및 권한 강화

- CISO를 CEO 또는 이사회 직속으로 편제하여 독립적 의사결정 보장
- 전사적 보안 활동에 대한 실질적인 권한과 책임 부여
- CISO가 주요 비즈니스 의사결정에 참여할 수 있는 체계 마련

명확한 역할과 책임(R&R) 정의

- RACI(Responsible, Accountable, Consulted, Informed) 차트 활용
- 보안 활동의 각 단계별 담당 부서와 담당자의 역할과 책임을 명확히 문서화 및 공유
- 책임 소재의 불분명함으로 인한 대응 지연 방지

보안 거버넌스의 정책적·제도적 개선 제안

CISO 지정 제도 실효성 강화

- 겸직 제한 규정 강화로 정보보호 업무 전념 환경 조성
- 일정 규모 이상 기업 CISO의 이사회 보고 의무화
- 실질적인 권한 부여를 통한 책임과 권한의 균형 확보
- CISO 자격 요건 및 교육 프로그램 강화

ISMS-P 인증 제도 개선

- 형식적 인증 심사에서 실질적 보안 수준 평가로 전환
- 기업 비즈니스 특성과 실제 위협 환경을 고려한 평가
- 인증 획득 기업에 대한 인센티브 강화로 자발적 참여 유도
- 인증 유지 비용 절감 및 행정 부담 경감 방안 마련

민관 협력 기반 정보 공유 활성화

- 정부 주도 '사이버 위협 정보공유' 기능 강화
- 신종 위협 정보, 침해사고 분석 결과 등 신속 공유
- 정보 공유 참여 기업에 법적 면책 조항 적용
- 산업별 특화된 위협 정보 공유 체계 구축 지원

기대 효과

- 전문성 있는 보안 리더십 확보
- 실질적인 보안 수준 향상
- 집단 지성을 활용한 사이버 위협 대응력 강화

보안 거버넌스와 사고 대응체계의 연관성

보안 거버넌스와 사고 대응체계는 분리된 개념이 아닌, 기업의 보안 역량을 결정하는 **상호 유기적 관계**입니다.
효과적인 보안 거버넌스는 체계적인 사고 대응의 기반이 되며, 잘 작동하는 사고 대응체계는 거버넌스의 실효성을 증명합니다

보안 거버넌스
전략 수립, 정책 결정, 자원 할당

⇄ 유기적 관계

사고 대응체계
탐지, 분석, 대응, 복구

방향성 제시와 실행

- 거버넌스: 비전과 목표에 맞는 보안 정책 및 표준 수립
- 대응체계: 정해진 지침과 권한 내에서 침해사고 대응 실행
- 거버넌스가 대응체계의 나침반 역할 수행

자원 할당과 역량 확보

- 거버넌스: 예산, 인력, 기술 등 핵심 자원 배분
- 대응체계: 할당된 자원으로 위협 대응 역량 구축
- 최신 위협 대응을 위한 충분한 역량 보장

의사결정 체계

- 거버넌스: 보안 관련 의사결정 구조 정의
- 대응체계: 사전 정의된 권한으로 신속한 결정
- 명확한 결정 체계가 대응 지연 방지

"**잘 연계된 거버넌스와 대응체계**는 사고 발생 시 혼란을 최소화하고, 전사적으로 일관된 대응을 가능하게 하여 **비즈니스 연속성을 확보**합니다."

보안 거버넌스와 사고 대응체계연계의 중요성

보안 거버넌스와 사고 대응체계의 유기적인 연계는 다음과 같은 측면에서 기업의 생존과 직결되는 중요한 요소입니다.

신속하고 일관된 대응

잘 연계된 체계는 사고 발생 시 혼란을 최소화하고 전사적으로 일관된 대응을 가능하게 합니다. 모든 구성원이 거버넌스에 의해 정립된 동일한 목표와 절차를 따르므로, 우왕좌왕하지 않고 신속하게 위협을 통제하고 피해를 최소화할 수 있습니다.

비즈니스 연속성 확보

사고 대응은 단순히 기술적 문제를 해결하는 것을 넘어 비즈니스에 미치는 영향을 최소화하는 것이 목표입니다. 보안 거버넌스는 비즈니스 중요도를 평가하고 핵심 자산을 식별하며, 사고 대응체계는 이를 바탕으로 복구 우선순위를 정해 비즈니스 연속성을 확보합니다.

규제 준수 및 신뢰도 제고

개인정보보호법, 정보통신망법 등 여러 규제는 기업에게 침해사고 발생 시 통지 및 보고 의무를 부과합니다. 거버넌스와 연계된 대응체계는 이러한 법적 요구사항을 체계적으로 이행하도록 보장하며, 고객과 투자자에게 기업의 위기관리 능력에 대한 신뢰를 줍니다.

지속적인 보안 수준 향상

사고 대응 과정과 결과, 그리고 '사후 검토(Post-Mortem Review)'를 통해 얻은 교훈은 다시 보안 거버넌스에 피드백됩니다. 이 피드백을 통해 기존의 정책, 통제, 프로세스의 약점을 보완하고, 이는 곧 기업의 보안 수준을 지속적으로 향상시키는 선순환 구조를 만듭니다.

보안 거버넌스와 사고 대응체계연계 강화 방안

보안 거버넌스와 사고 대응체계의 연계를 강화하기 위한 실질적인 방안

역할과 책임(R&R)의 명확화

- 보안 거버넌스 조직(이사회, CISO)과 사고 대응 실무 조직(CERT/CSIRT) 간의 역할, 책임, 권한을 명확히 문서화
- 중대 사고 발생 시 의사결정권자, 보고 라인, 대외 커뮤니케이션 책임자를 사전에 지정
- RACI 차트 등을 활용한 책임 소재 명확화

통합된 프로세스 구축

- 사고 대응 계획을 보안 거버넌스 프레임워크의 핵심 요소로 포함
- 위험 평가, 자산 관리 등 거버넌스 활동의 결과를 사고 대응 시나리오 및 훈련에 직접 반영
- 보안 정책과 대응 절차의 일관성 확보를 위한 통합 문서 체계 구축

정기적인 소통 및 훈련

- 경영진이 참여하는 정기적인 보안 위원회를 통해 주요 위협 동향과 사고 대응 현황 공유
- 경영진부터 실무자까지 모두 참여하는 모의 침해사고 훈련을 연 1회 이상 실시
- 거버넌스와 대응 절차가 실제 상황에서 효과적으로 작동하는지 검증하고 개선점 도출

성과지표(KPI) 연계 및 피드백 루프 구축

- 사고 대응 성과(평균 탐지 시간, 평균 복구 시간 등)를 보안 거버넌스의 성과지표와 연계하여 관리
- 모든 침해사고 후 사후 검토 보고서를 작성하고, CISO와 경영진에게 보고
- 사고 대응 결과를 정책 및 투자 결정에 반영하는 공식적인 피드백 채널 제도화

💡 효과적인 연계는 일회성이 아닌 지속적인 프로세스로서, 전사적 참여와 경영진의 의지가 핵심입니다.

기업 맞춤형 거버넌스 구축 전략

기업 환경 분석 및 목표 설정

- 기업의 규모, 산업 분야, 비즈니스 전략, 규제 환경(법규, 지침) 등 내외부 환경 종합 분석
- 분석 결과를 바탕으로 보안 거버넌스를 통해 달성하고자 하는 명확한 목표 설정
- 예: 규제 준수, 핵심 자산 보호, 비즈니스 연속성 확보 등

프레임워크 선정 및 조합

- 단일 프레임워크보다 여러 프레임워크의 장점을 결합한 하이브리드 모델 고려
- NIST CSF를 기본 틀로 사용하고, ISO/IEC 27001의 통제 항목 참조
- 국내 법규 준수를 위해 ISMS-P 요구사항을 통합하여 적용
- 기업의 고유한 특성과 위험 환경에 맞는 최적의 조합 설계

맞춤형 통제 항목 설계 및 구현

- 선정한 프레임워크를 기반으로 핵심 자산과 고유한 위협 요소를 식별
- 식별된 위협에 대응하기 위한 맞춤형 보안 통제 항목 설계
- 기술적 보호조치뿐만 아니라, 관리적·물리적 보호조치를 포함한 다계층 방어 체계 구축
- 기업 문화와 조직 구조를 고려한 실행 가능한 통제 방안 수립

지속적인 평가 및 개선

- 구축된 거버넌스 체계가 효과적으로 운영되는지 정기적으로 성과 측정 및 평가
- 변화하는 위협 환경, 기술 발전, 비즈니스 환경 변화에 맞춰 거버넌스 체계 검토
- PDCA(Plan-Do-Check-Act) 순환 구조를 통한 지속적인 개선 프로세스 정착
- 보안 성숙도 모델을 활용한 객관적인 수준 진단 및 발전 방향 설정

결론

핵심 요약

보안 거버넌스의 핵심

- 보안을 비용이 아닌 비즈니스 가치와 연계된 전략적 투자로 인식
- CISO에게 실질적 권한 부여 및 전사적 통합 거버넌스 구축
- 리스크 기반의 자율 보안체계로 능동적 대응 역량 강화

대응 체계의 핵심

- 명확한 역할과 책임(R&R)을 통한 신속하고 일관된 대응
- AI 및 자동화 기술을 활용한 위협 탐지 및 초동 조치
- 사고 대응 결과의 거버넌스 체계로의 피드백 순환 구조

"최근 사고 사례는 모든 기업이 기술적, 관리적, 거버넌스 측면에서 총체적인 보안 역량을 갖추어야만 급변하는 사이버 위협 환경에서 생존하고 성장할 수 있다는 경각심을 일깨워준 중요한 계기가 되었습니다."