19_안전한 비즈니스 환경을 위한 정보보호 가이드

#1
이번 시간에는 안전한 비즈니스 환경을 위한 정보보안 방법에 대해 알아보겠습니다.
기업이 이사회와 최고경영진을 중심으로 지배구조를 안정적으로 작동시켜야 운영이 매끄럽게 이루어질 수 있을 텐데요. 그렇다면, 지배구조를 안정적으로 작동시키기 위해서는 기업을 어떻게 운영해야 할까요?

#2
※ 기업 경영과 보안 위험
기업은 이사회와 경영진 등 최고 경영층의 지휘하에 전체 조직을 운영하며 사업 목표를 달성해 나갑니다. 이 과정에서 최고 경영층은 발생할 수 있는 경영 리스크를 관리하고, 사업이 법과 규제의 범위 내에서 진행되도록 통제합니다. 핵심 기술, 중요 영업비밀, 고객정보의 유출과 같은 보안 사고가 기업 경영에 큰 영향을 미치기 때문입니다. 따라서, 전사적으로 중요한 정보보호 업무는 최고 경영층의 참여와 경영적 판단이 필요하며, 이를 위한 체계적인 구조와 절차를 마련해야 합니다.

#3
※ 최고경영층을 중심으로 작동하는 정보보호 거버넌스
- 보안 과제를 수행하는 실행조직은 그 진행 상황을 경영진에게 보고하고, 최고경영층은 이 보고 내용을 검토하고 평가합니다.
- 필요한 경우, 최고경영층은 전략적, 정책적 관점에서 실행조직에 구체적인 지시를 내립니다.
- 최고경영층은 실행조직의 작업 결과를 검토하고 평가하며, 이 결과를 이해관계자와 공유합니다.
- 보안 활동의 효율성을 평가하기 위해 최고경영층은 객관적이고 전문적인 기관에 검토를 의뢰하고 그 결과를 분석합니다.
- 실행조직은 최고경영층과의 지속적인 소통을 바탕으로 정보보호 업무를 수행하며, 필요한 경우 다른 조직과 협업하여 업무를 진행합니다.

#4
※ 최고경영층이 수행해야 하는 정보보호 업무

- 정보보호 조직의 구성 및 권한 부여: 최고경영층은 정보보호 업무를 총괄할 임원급의 정보보호최고책임자(CISO)를 임명하며, 이에 필요한 권한을 부여합니다. 또한, 정보보호 조직을 설립하고, 필요한 인력을 배치하여 정보보호 업무의 효과적인 수행을 보장합니다.
- 정보보호 사업 계획 및 투자 승인 및 지원: 최고경영층은 정보보호 관련 사업 계획과 투자를 심사하고 승인합니다. 이는 정보보호를 위한 예산과 자원을 확보하고, 기업의 정보자산 보호 및 보안 대책을 강화하기 위한 지원을 의미합니다.

#5
※ 기업의 정보보호 강화 및 효과적인 관리를 위해 고려해야 하는 사항들
기업이 정보보호를 강화하고 효율적으로 관리하기 위해서는 전체 조직 간의 원활한 소통과 협업이 필수적입니다. 이를 위해 최고경영층은 정보보호에 관한 거버넌스를 체계적으로 수립하고, 이에 따라 정보보호 조직 체계와 협업 체계를 구축해야 합니다. 이런 체계를 통해 일상적인 정보보호 업무를 실행하고, 사업 및 경영 목표 달성을 위한 보안 및 위험 관리 활동을 원활하게 진행할 수 있습니다

#6
※ 정보보호 관리 체계를 수립하는 3요소
- 정보보호 조직 및 인력 구성: 기업은 자체적으로, 체계적이고 지속적인 정보보호를 실시하기 위해 필요한 조직과 인력을 갖춰야 합니다.
- 정보보호 사업 추진 및 예산 할당: 중요 정보자산을 보호하기 위해 정보보호 사업을 추진하고, 필요한 예산을 할당해야 합니다.
- 전사적 정보보호 활동: 정보보호 활동은 단순히 정보보호 조직에만 국한되지 않고, 기업 전반의 여러 조직이 함께 참여하여 수행해야 합니다.

#7
※ 정보자산 관리 방법
- 정보자산 식별 및 목록(대장) 관리: 기업의 업무 특성에 맞게 정보자산을 분류하고 식별하여 목록으로 정리해야 합니다. 정보자산은 정보시스템, 정보보안시스템, 물리보안시스템, 정보 등으로 구분될 수 있습니다. 이렇게 중요 정보자산을 식별하여 이를 보호 대상으로 지정하고, 그에 대한 목록을 작성해야 합니다.

- 정보자산 목록(대장) 관리: 정보자산 목록에는 정보자산명, 자산번호, 모델명, 용도, 관리자 및 관리 부서, 중요도 등의 정보가 포함되어야 합니다. 정보자산의 변경 또는 폐기 시에는 목록을 업데이트하여 항상 최신 상태를 유지해야 합니다.

#8
- 정보자산별 관리자 지정 및 중요도 결정: 각 정보자산에 대해 관리자를 지정하고, 중요도를 평가하여 적절하게 관리해야 합니다. 이때, 중요도는 정보자산의 가치와 피해 발생 가능성을 기반으로 정하며, 핵심 정보는 추가적인 보호를 위해 필요한 예산과 인력을 배정해야 합니다.

- 관리자 지정: 각 정보자산에 대한 관리자를 정하고 해당 업무를 맡깁니다. 만약, 정보자산의 양이 많을 경우, 관리자 외에도 정보자산 관리책임자를 별도로 지정할 수 있습니다.

- 중요도 결정: 중요도 등급을 설정하여 정보자산을 분류하고, 그에 맞는 보호 수준을 정합니다. 중요도를 정할 때는 정보자산의 가치와 피해 발생 가능성을 함께 고려해야 합니다.

#9
이어서 사내 PC 보안에 대해 알아보도록 하겠습니다. 사내 PC는 기업의 중요한 데이터와 자산에 엑세스하며 저장되는 장소입니다. 기업의 경쟁력 및 지속가능성 유지에 매우 중요한 요소인 만큼, 사내 PC 보안은 기업 운영에 필수적이라고 볼 수 있습니다.

#10
※ 사내 PC 보안 관리 방안
- 공유폴더 관리: 공유폴더는 여러 사람이 사용할 수 있도록 네트워크를 통해 연결되는 만큼, 타 사용자가 임의로 삭제하거나 위변조하지 못하도록 권한을 설정해야 합니다.
- 시스템 기본 공유 제거: 운영체제는 네트워크나 컴퓨터 환경에서 프로그램 및 서비스를 관리하기 위해 자동으로 시스템 기본 공유 항목을 생성합니다. 이러한 기본 공유를 제거하지 않을 경우, 비인가자가 시스템의 모든 자원에 접근

할 수 있는 위험한 상황이 발생할 수 있습니다.

#11
- 계정 및 비밀번호 관리: 비밀번호 없이 로그인이 가능한 계정이나 불필요한 계정이 존재하는 경우, 이를 통한 불법 접근으로 중요 데이터의 유출이나 해킹 피해가 발생할 위험이 있습니다. 이러한 위험을 방지하기 위해 기업은 계정과 비밀번호 관리에 주의를 기울여야 합니다.
- 비밀번호 생성 전략: 비밀번호는 다른 사람이 쉽게 예측할 수 없도록, 최소 10자리 이상이며 영문자, 숫자, 특수문자를 조합하여 설정해야 합니다. 기업은 직원들에게 강력한 비밀번호의 중요성을 권장하고 이에 대해 교육해야 합니다.

#12
※ PC에서 불필요한 서비스를 제거하는 방법
운영체제 설치 시 많은 서비스들이 기본적으로 함께 설치되는데, 이 중 일부는 사용되지 않거나 보안 취약점을 가지고 있어 관리되지 않는 경우가 있습니다. 이러한 서비스들은 제거하는 것이 필요합니다. 시스템에서 발생하는 모든 행위의 이력을 기록하는 이벤트 및 로그는 불법적인 접근 시도나 보안 사고 발생 시 원인 분석과 경로 추적에 필수적입니다. 이를 위해 이벤트 뷰어 설정과 감사 정책을 적절히 관리해야 합니다.

#13
※ PC 보안 솔루션의 기능
기업에서는 PC 라이선스 관리, 하드웨어 관리, 매체 제어, 네트워크 보안, 메일 관리 등의 기능을 활용하여 중요 정보의 불법적인 유출을 방지합니다. 이러한 조치들은 데이터 유출을 차단하는 데 중요한 역할을 합니다.

※ PC 보안 솔루션 구축 시 고려사항
- PC 보안에 대한 정책을 수립하는 것이 기업 환경에 맞는 보안 솔루션 도입의 첫걸음입니다.
- 임직원 및 상주 외주 인력과 같은 다양한 사용자들에 대한 관리와 인사 정보와의 연동을 통해 사용자 관리가 필요합니다. 이를 위해서는 사용자에 대한 강력하면서도 유연한 관리 방안을 사전에 정의해야 합니다.
- PC 보안 솔루션은 주로 에이전트 방식으로 PC에 설치되므로, 다양한 운영체제를 지원하는지 확인하는 것이 중요합니다. 또한, 장애 발생 시 대응 방

안도 고려해야 합니다.

#14
정보보안 유출 대개 기업 내부 정보의 유출은 직원들의 고의적인 행위나 실수로 인해 발생합니다. 퇴사한 직원과 같이 회사의 내부 상황을 잘 아는 사람들에 의한 유출도 가능합니다. 그렇다면 이러한 유출 사고를 방지하기 위해 기업 내부에서는 어떤 조치를 해야 할까요?

#15
※ 보안 교육의 시기와 대상
임직원의 보안 의식 강화를 위해 주기적인 보안 교육 계획을 수립하고, 직무에 따라 전문적인 교육을 제공해야 합니다. 최초 보안 교육은 임직원이 입사할 때 진행하며, 정기 교육은 연간 최소 1회 전체 임직원을 대상으로 실시합니다.
인원이 적은 경우, 기업들은 종종 분기별 또는 반기별로 보안 교육을 진행합니다. 하지만 입사 인원이 적을지라도, 1시간 정도의 짧은 교육이라도 입사 후 한 달 이내에 실시하는 것이 교육 효과가 높습니다. 이는 관련 조직과 인력 간의 친분 형성에도 도움이 되어 정보보호 업무 수행에 긍정적인 영향을 미칩니다.

#16
※ 정보보안 교육의 필요성
산업기술, 영업비밀, 고객정보 등 기업의 중요한 정보는 보유하고 있거나 접근 권한이 있는 내부자, 혹은 접근 권한이 없음에도 불법적인 방법으로 접근한 내부자에 의해 외부로 유출될 위험이 있습니다. 퇴사한 임직원들은 회사 외부인이지만, 때때로 자유롭게 사무실을 출입하거나 회사 시스템을 이용하는 등 보안 규칙이 적용되지 않는 경우가 발생하기도 합니다. 이런 내부자에 의한 중요 정보 유출은 많은 기업에서 가장 심각한 보안 위협으로 인식되고 있습니다.

#17
※ 보안서약서와 비밀유지서약서의 차이점
비밀유지서약서는 기업이 보유한 영업비밀, 산업기밀 등 중요한 정보를 외부에 누설하거나 유출하지 않겠다는 약속입니다. 반면에 보안서약서는 비밀 유지뿐만 아니라 PC, 서버, 저장 매체 사용 및 기업의 정보보호 규정 준수 등의 내용을 포함할 수 있습니다. 서약서의 선택은 기업의 필요에 따라 결정됩니다.

#18

※ 보안서약서 및 비밀유지서약서 작성 방법

모든 임직원, 임시직원, 외부인은 기업의 보안 정책, 관련 법규, 비밀 유지 의무 및 위반 시 책임 등을 명확히 이해하고 준수하기 위해 보안서약서를 작성합니다. 이를 통해 정보자산에 접근할 수 있는 모든 사람들이 보안 관련 사항을 충분히 인지하도록 합니다. 기업은 이러한 보안서약서를 안전하게 보관하고 쉽게 접근 가능한 곳에서 관리해야 합니다. 비밀유지서약서는 입사 시 영업비밀의 관리와 사용에 초점을 맞춰 작성되며, 퇴사 시에는 이를 개인적으로 활용하거나 제3자에게 전달하지 않도록 강조해야 합니다. 필요한 경우, 같은 업종으로의 이직을 금지하는 전직금지약정을 설정할 수도 있습니다.

#19

※ 외부자에 의한 정보보안 사고가 발생하는 경로

산업기술, 영업비밀, 개인정보 등 기업의 중요 정보가 외부자에 의해 유출되는 사고가 종종 발생합니다. 퇴사한 전 직원, 협력 업체 직원, 방문자 등이 기업 내부에 출입하거나 상주하는 경우가 많으며, IT 개발이나 고객상담 업무를 외부 업체에 위탁하는 경우도 있습니다. 또한, IDC(Internet Data Center), 웹 호스팅, 클라우드 서비스와 같은 외부 시설이나 서비스의 사용이 증가함에 따라 정보자산의 외부 유출 위험도 커지고 있습니다. 이러한 피해를 예방하고 사고 발생 시 피해를 최소화하기 위해 외부자에 대한 보안 관리를 철저히 해야 합니다.