Samil PwC Governance Center Online Library

리스크관리와 내부통제 :

랜섬웨어에 대비한 이사회 고려사항

삼일 PwC 거버넌스센터

pwc 삼일회계법인

랜섬웨어 공격은 위협 행위자의 증가, 공격의 정교화, 기업의 데이터를 볼모로 한 거액의 금전 요구 등과 함께 계속해서 늘고 있다. 공격의 확산은 부분적으로 서비스형 랜섬웨어(RaaS, Ransomware-as-a-Service) 개발로 인해 발생했는데, RaaS 는 별도의 프로그래밍 전문지식이 없어도 비용만 지급하면 랜섬웨어 공격을 할 수 있게끔 서비스 형태로 제공되는 랜섬웨어를 말한다. 이러한 상황에서 기업의 디지털 전환 및 원격 근무와 더불어 제 3 자와 거래하는 기업의 수가 증가함에 따라, 랜섬웨어 공격에 대한 취약성이 더욱 커지고 있다. 또한 위협 행위자들은 기업의 지급 능력과 대외적으로 알려진 네트워크 취약성을 기반으로 범죄 대상에 대한 전략을 구축하고 있다.

랜섬웨어 공격 대비

경영진의 역할은 광범위하게는 사이버 보안 위험을, 구체적으로는 랜섬웨어 위험을 관리하는 것이다. 따라서 이사회는 위험 관리 프로그램의 핵심적인 기본 요소를 이해하고, 이사회가 보고 받는 내용이 충분하다고 판단할 수 있어야 한다. 이사회는 이렇게 진화하는 위험을 어떻게 파악할 수 있을까? 그리고 이사회가 이 주제에 대해 고위 경영진과 의미 있는 논의를 하기 위해서는 어떻게 해야 할까? 가장 좋은 시작은 질문을 하는 것이다. 대화를 시작하기 위해 어떤 질문을 할 수 있을까?

이사회가 경영진에게 해야 할 질문

적절한 "사이버 보안 위생(cyber hygiene)"

경영진은 랜섬웨어 공격을 방지하기 위한 기본적인 사이버 보안 위생 통제(예: 네트워크 세분화, 데이터 백업, 다중 인증(MFA, Multi-Factor Authentication), 암호 제어, 원격 데스크톱 프로토콜(RDP, Remote Desktop Protocol) 보호 또는 비활성화)를 구축했는가?

랜섬웨어 정책

경영진은 랜섬웨어 관련 정책을 수립했는가? 동 정책에는 금전 지급 여부와 지급 방법(예: 중개인을 통해, 암호화폐를 사용하여)을 명시하였는가?

복구 계획

경영진은 기업의 사이버 복구 기능을 평가했는가? 여기에는 미션 크리티컬 시스템[1]의 정의 및 종속성, 복구

[1] 미션 크리티컬 시스템은 사업이나 조직의 생존에 필수적인 시스템이다. 미션 크리티컬 시스템이 실패되거나 간섭을 받으면 사업 운영에 상당한 영향을 받는다. 임무에 필수적인 장비와 미션 크리티컬 애플리케이션은 미션 크리티컬 시스템으로도 알려져 있다. 미션 크리티컬 시스템의 예는 다음과 같다: 온라인 뱅킹 시스템, 철도/항공기 운영 및 통제 시스템, 전력 시스템, 그리고 실패 시 사업과 사회에 부정적인 영향을 미치는 수많은 기타 컴퓨터 시스템.
(출처: 위키백과, https://ko.wikipedia.org/wiki/%EB%AF%B8%EC%85%98_%ED%81%AC%EB%A6%AC%ED%8B%B0%EC%BB%AC)

우선순위 결정, 세분화된 백업 및 복구 네트워크 유지 관리, 사이버 복구 계획 등이 포함될 수 있다.

모의 훈련

랜섬웨어 공격에 적절히 대응하고 복구할 수 있도록 관련 이해관계자가 랜섬웨어에 초점을 맞춘 모의 훈련이나 실시간 복구 훈련에 참여했는가? 이사회를 대상으로 한 간략한 보고나 설명이 있었는가, 아니면 이사회 구성원이 참관하였는가?

사이버 보험

경영진은 사이버 보험의 비용과 혜택을 고려했는가? 보험이 있는 경우, 해당 보험이 랜섬웨어 보상도 보장하는가? 만약 그렇다면, 공격이 발생하기에 앞서 경영진과 이사회가 알아야 하는 조건은 무엇인가?

추가 자원

경영진은 랜섬웨어 대응을 지원하는 데 필요한 자원(예: 감독당국, 외부 법률자문인, 암호화폐로 대가를 지불하는 것을 지원할 중개인, 공격을 신속하게 조사하고 억제 및 복구하기 위한 기술적 전문지식과 추가 자원을 제공하는 대응 업체 등)을 갖추고 있는가? 적절한 담당자와 전문가가 있는가?

랜섬웨어 공격 발생

공격의 대가로 금전을 지급할 때 평판, 법률, 재무 및 운영을 포함하여 고려해야 할 중요한 사업 관련 영향이 있다. 경영진은 금전을 지급하지 않는 것이 운영에 미치는 영향을 고려했는가? 경영진이 금전을 지급하지 않을 경우, 운영을 성공적으로 복구할 수 있다고 확신하는가? 반대로 금전을 지급할 경우, 이해관계자에게 미치는 브랜드 영향을 고려했는가? 공격자에게 금전을 지급하는 것은 위험에 기반한 결정이다. 경영진은 금전을 지급하기로 결정하기 전에 다양한 위험을 평가해 볼 필요가 있다.

금전을 지급하기 전에 평가해야 할 위험

- **데이터에 대한 접근 권한을 되찾는다는 보장은 없다.**
  과거의 공격 패턴에 기반하여, 위협 행위자가 어떠한 행동을 할 수 있는지에 대해 우리는 무엇을 알고 있는가? 위협 행위자가 합의한 사안을 지키지 않고 데이터를 제공하지 않을 경우, 의존할 데이터 백업이 있는가?

- **법적 및 규제적 영향**
  위협 행위자에게 금전을 지급하는 것이 합법적인가? 기업이나 보험사의 금전 지급은 범죄 집단, 테러리즘,

제재 대상 조직, 테러 지원국 및 자금세탁방지법 위반에 해당될 수도 있다.

- **의도치 않은 범죄 활동 지원**
  기업은 위협 행위자의 범죄 활동을 지원할 의향이 있는가? 의도하지 않았더라도, 기업의 금전 지급은 위협 행위자들이 취약한 기업에 침투할 수 있는 더 발전된 방법을 개발하도록 사이버 범죄 활동에 자금을 지원하는 것이 되고, 범죄 행위가 계속되도록 장려하는 결과를 낳을 수 있다.

- **추가 공격의 위험 증가**
  금전을 지급하면 또다른 위협 행위자의 표적이 될 수 있을까? 금전 지급은 동일한 범죄 집단이나 다른 위협 행위자에 의한 두 번째 표적이 될 위험을 크게 증가시킨다.

- **이중 갈취**
  초기 갈취의 일부로 "추가" 요청이 있는가? 암호 해독 키를 받기 위한 첫 번째 금전 지급 후에 추가적인 금전 요구가 이어질 수 있다. 범죄자들은 기업에서 유출된 민감 정보를 다른 곳에 유출하거나 판매하지 않는다는 명목으로 이러한 요구를 할 수 있다.

- **보험의 영향**
  보험사의 보험금 지급을 위해 기업은 협상을 시도했다는 증거를 제출해야 하는가? 보험사가 금전 지급을 권고했는데 기업이 지불하지 않기로 결정하거나 그 반대인 경우, 보험금을 상실하는가?

랜섬웨어 공격에 대한 대응 방안 구축은 피해자가 될 때까지 기다려서는 안 된다. 지금 경영진에게 질문을 하고, 이사회의 역할이 기업의 전반적인 대응 전략에 어떻게 부합하는지 이해하는 것이 무엇보다 중요하다.