Executive Series

CIO가 염두에 두어야 할 보안의 핵심 요소

불가피한 사고에 대처하기

주요 내용:

보안 사고는 피할 수 없습니다. 관건은 적절한 대비가 되어 있느냐입니다. 최고 수준의 사고 대응을 위한 시스템을 구축하려면 적절한 인력과 전문 기술, 프로세스, 전사적인 협력이 필요합니다. IBM에서는 일련의 일반적인 규칙을 수립하여 사고 발생 시 내부 행동 요령과 외부 커뮤니케이션을 위한 지침을 제공합니다.

보안 사고는 당장 내일 일어날 수도, 2년 후에 일어날 수도 있습니다. 분산 서비스 거부 공격(DDoS)이나 회사 기밀을 유출시키는 악성 코드 등 공격의 형태는 다양합니다. 형태와 특성에 관계 없이 가장 초점을 두어야 할 것은 전사적 규모의 위협을 가하는 사고가 일어날 것인지 여부가 아니라, '사고가 언제 일어날 것인가'입니다. 이후의 공격에 대해서도 마찬가지입니다. 중요한 것은, 준비가 되어 있느냐입니다.

기업이 성장하려면 사건이 발생할 때를 대비해 전문 팀을 준비하여 상시 대기해야 합니다. 이 조직은 병원의 응급실에 비유할 수 있습니다. 지정된 프로세스와 절차를 관련인 모두 숙지하고 있어야 하며, 응급실의 비상 상황에서와 마찬가지로 위협을 신속하게 파악하여 심각성과 잠재적 파급력을 판단하고, 이를 막기 위한 즉각적인 조치를 취해야 합니다.

문제는, 응급실과는 달리 보안 사고는 비즈니스의 모든 부문에 영향을 미칠 수 있다는 것입니다. 고객이나 직원에게 위험을 끼칠 수도 있고 제품에 영향을 끼칠 수도 있습니다. 파트너사의 기밀 데이터, 정부와의 관계 또는 지적 재산이 유출될 수도 있습니다. 사고의 가능성은 기업의 모든 곳에 도사리고 있습니다. 따라서, 사고 대응 팀은 모든 분야에서 전문성을 갖추어야 합니다.

사고 대응을 위한 최고의 시스템을 구축하기 위해 CIO가 취해야 할 조치는 무엇일까요? 본 문서에서 이를 정리해 보았습니다.

1. 능숙한 정규직 직원을 배치

대응 팀에는 보안 기술 전문가와 법률 전문가가 포함되어야 하며 마케팅, 인력 관리, 재무, 대정부 업무 담당자도 필요합니다. 비즈니스를 수행하는 각 지역마다 보안 팀과 백업 기능을 갖추어야 합니다. 이러한 글로벌 분배를 통해 사고 발생 시에도 전 세계의 업무가 1년 365일 쉬지 않고 진행될 수 있습니다. 더 나아가, 각 지역의 팀은 위기 발생 시 각 국가 및 비즈니스의 요구사항에 정통한 전문가를 이용할 수 있습니다. 비상 상황에서는 회사 전체에 영향을 줄 수 있는 어려운 결정을 내려야 하기 때문에 경험이 풍부한 팀이 필요합니다.

2. 문서화되고 감사 가능한 프로세스를 구축

내부 인력으로 팀을 구성할지 외부 전문가를 채용할지는 기업이 자유롭게 선택할 수 있지만, 현장에서 운영을 모니터링하고 정확한 보고서를 신속히 수집할 수 있는 시스템은 꼭 필요합니다. 모든 단계는 절차에 따라 이루어져야 하며, 모니터링과 후속 조사를 거쳐 세부 조정이 이루어져야 합니다. 적절한 채널과 팀 구성원 및 프로세스를 통한 커뮤니케이션 전략은 계획 수립의 핵심 요소입니다.

3. 기업 전체가 참여

사고를 발견하고 그에 대응하려면 부서와 직원이 각자 맡은 역할을 제대로 수행하는 것이 매우 중요합니다. 필요한 예방 조치를 취하는 것은 물론, 사고를 발견하면 지정된 채널을 통해 보고하도록 교육이 이루어져야 합니다. 이로써 모두가 대응 팀의 일원이 될 수 있으며, 훈련과 체계적인 연습을 반복하여 이를 직원들에게 각인시켜야 합니다. 이러한 과정을 통해 위험 인식 문화를 조성할 수 있습니다.

4. 위험도가 높은 사고를 식별하고 이에 집중

규모가 큰 기업은 공항에 노트북 컴퓨터를 두고 내리는 일에서부터 기업 전자 메일을 통한 피싱 공격에 이르기까지, 하루에도 수많은 사고를 처리해야 합니다. 사고 발생 시 가장 먼저 해야 할 일은 잠재적 위험이 가장 큰 사고를 찾아 대응 팀을 신속히 투입하는 것입니다. 응급실에 비유하자면, 이는 치료 우선순위를 정하기 위한 부상자 분류라고 볼 수 있습니다. 직급이 낮은 직원이 비밀번호를 공유하는 실수를 저지른 경우, 보안 분석가가 재빨리 지난 몇 주간 해당 직원의 네트워크 활동과 사내에서 액세스한 영역을 확인한 다음, 이 일이 큰 위협이 되지는 않는다고 결론을 내릴 수 있습니다.

반면, 이렇게 잘못 사용된 비밀번호가 수십억 원 규모의 수출을 협상 중인 고위 경영진의 것이라면 사고는 심각한 것으로 분류됩니다. 대응 팀은 즉시 근무지 사무실과 사고 발생 지역 모두에 조치를 취해야 합니다. 이러한 사고가 근무일 내에 해결되지 않을 수도 있으므로 다른 시간대에 속한 팀이 몇 시간 내에 업무를 인계 받아야 할 수도 있습니다. 업무는 중단되지 않고 24시간 진행될 수 있어야 하며, 인계가 빨리 이루어질수록 좋습니다.

5. 작은 사고에도 주의를 기울이기

보안이 적용되지 않은 Wi-Fi 연결을 통해 외부인이 회사 네트워크에 침입해도 아무런 피해가 발생하지 않는 경우도 있습니다. 하지만 이러한 작은 사고에도 반드시 적절한 대응을 해야 하며, 면밀히 기록해 두어야 합니다. 일차적으로 이는 몇몇 직원이 보안 절차를 지키지 않고 있으며 위험에 대한 경계심이 느슨해졌다는 의미일 수 있으므로 주의가 필요합니다. 또한, 미미해 보이는 사고들이 쌓이면 규모가 커져 나중에는 심각한 위협이 될 수 있습니다. 모든 사고를 기록하고 후속 조치를 취하지 않으면 큰 위협이 닥쳤을 때 알아채지 못할 수도 있습니다. 능숙한 사고 대응 팀을 상시 대기하여 가동하지 않는 기업은 여러 면에서 문제를 간과하게 됩니다.

6. 실시간으로 중대한 결정을 내릴 수 있도록 팀을 신뢰

사고가 발생하면 그 즉시 발생 가능한 피해를 파악하고 적절한 조치를 취해야 합니다. 이를 위해 여러 중대한 결정을 내려야 할 수 있습니다. 초기 단계에서 결정할 문제 중 하나는 공격의 대상으로 간주되는 사용자에게 알릴 것인가 혹은 대상이 되는 사용자의 네트워크 연결을 차단할 것인가 하는 것입니다. 공격이 내부자로부터 이루어진 징후가 포착될 경우 결정은 쉽지 않으며, 현지 사법 당국에 알려야 할지 여부도 결정해야 합니다.

대응 팀의 전문가는 문제를 모든 측면에서 파악해야 합니다. 대응 팀은 비즈니스의 위기를 막고 회사의 이익을 보호할 전략을 수립해야 하며, 폭넓은 전문성 외에도 어려운 결정을 신속히 내릴 수 있는 신뢰와 권한을 가지고 있어야 합니다. 다시 말해, 이러한 문제에는 기업 전체의 참여가 필요하며, 기술 팀의 수준을 능가하는 사내 혹은 서비스 공급업체를 통해 전문성을 갖추어야 합니다.

7. 반복의 고리를 끊기

어떤 사건은 몇 시간 만에 해결이 가능하지만, 악성 코드 공격이나 내부자로 인한 위협이 발생한 경우에는 긴 시간이 소요됩니다. 사고가 해결된 뒤에도 근본 원인에 대한 분석을 진행해야 합니다. 기업은 이러한 사고가 일어나게 된 과정과 원인이 된 시스템을 가려내고, 향후 유사한 일이 발생하지 않도록 대책을 수립해야 합니다. 근본적인 원인을 해결하기 위해 직원 간 커뮤니케이션 방식을 바꾸거나 추가 교육 또는 기술적 수정을 수행해야 할 수 있습니다. 이러한 측면에서 사고에 대처하는 것은 지속적인 개선 프로세스의 일환이며, 비즈니스에서 끊임 없이 일어나게 되는 일입니다.

사고 발생 시 대처 방법 – 보안 사고 해결을 위한 외부와의 커뮤니케이션

보안 위반이 발생하면 외부와의 커뮤니케이션이 어려워질 수 있습니다. 피해가 급속도로 확산되어 조직의 평판이 나빠지고 비즈니스가 악화될 수도 있습니다. 성공적인 커뮤니케이션의 열쇠는 미디어에서 신속한 대응이 강조되도록 하고, 이러한 사고가 얼마든지 발생할 수 있는 흔한 일임을 인식시키는 것입니다. 다음은 보안 사고가 발생하기 전에 고려해야 할 몇 가지 팁입니다.

- **설득력 있는 배경 정보 제공.** 조직의 시스템을 보호하고 사고를 감지하고 영향을 최소화하는 데 필요한 적절한 프로세스를 갖추고 있음을 명확하고 설득력 있게 알려야 합니다. 기업의 데이터 관리 노력에 대한 배경 정보가 없다면 대중은 사고 이후의 모든 내용을 단지 눈가림을 위한 제스처라고 간주해 버립니다.
- **최악의 상황에 대비한 계획 수립.** 해커가 조직에서 정보를 빼내었다는 데 그게 사실이냐는 기자의 전화를 받을 수 있습니다. 대응 방법이 없어 보이는 새로운 형태의 악성 코드가 발견될 수도 있습니다. 시나리오 계획은 유용할 수 있지만 과도해서는 안 됩니다. 책장에 정리되어 있는 각종 시나리오 중 실제로 일어날 확률이 있는 것은 많지 않기 때문입니다.
- **연락 대상 결정.** 기자, 블로거, 공공 정책 기관 등은 조직에서 제공하는 정확한 정보를 전달할 수도 있고, 소문을 실어 날라 걷잡을 수 없이 확산시킬 수도 있습니다. 조직에 대한 내용을 정기적으로 다루어줄 리포터와 해당 산업 분야를 다루는 블로거, 참여 중인 소셜 미디어 사이트의 목록을 작성하십시오.
- **최초 입장 발표 시기 선택.** 커뮤니케이션에 성공하는 프로그램과 브랜드 가치의 하락을 막는 데 실패하는 프로그램 사이에는 단 한가지 차이점이 있습니다. 신속한 입장 발표를 통해 소문을 잠재우고 싶을 수도 있습니다. 100% 확신을 갖기 위해 입장을 발표하기 전 모든 사실을 파악하려 할 수도 있습니다. 하지만 둘 다 잘못된 방법입니다. 서두르면 가정과 부정확한 초기 평가에 의존한 발표에 그치게 될 것이고, 지연되면 부정확한 보고서가 진실인 것으로 받아들여질 수 있습니다.
- **세부사항 홍보.** NTSB(National Traffic Safety Board)의 사례를 눈여겨보십시오. NTSB는 사실을 가능한 신속히 알려 억측을 막고, 이를 뒷받침하기 위해 상황에 대한 업데이트를 정기적으로 제공합니다. 또한, 내부 평가에서 발견된 위반을 알리고 발생 상황과 영향을 받을 수 있는 대상이 취해야 할 조치, 이러한 사고의 재발을 막기 위한 조치에 초점을 맞춥니다. 사법 당국과의 협조, 포렌식 수사, 지원 라인 구축, 고객의 특별한 지원 등 문제 해결을 위해 어떤 노력을 기울이고 있는지를 밝히고 사람들로부터 인정받는 것이 중요합니다.
- **언론 및 소셜 미디어 모니터링.** 성공적인 모니터링 프로그램은 특정 메시지 전달의 효과를 판단하고 정보 리포터가 찾고 있는 정보를 바로 제공할 수 있습니다. 많은 조직이 미디어 모니터링 책임을 하위 레벨의 전문가 또는 관리 직원에게 일임하는 실수를 범하는데, 이로 인해 경험이 풍부한 전문가만의 노하우를 활용하지 못하게 됩니다.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
August 2012

WGW03011USEN-00