지능적 보안 공격에 대한 대처 및 복구

기업을 안전하게 보호하기 위한 4단계

IBM

목차

서론

사이버 공격과 이를 감행하는 범죄자는 오늘날의 다른 여러 요소와 마찬가지로 매년 더욱 지능화되고 있습니다. 그와 동시에 IT 자원이 기업의 방화벽 바깥으로 이동하고 있으며, 각 기업은 다양한 장치에서 애플리케이션과 데이터를 배포하고 있습니다. 기업의 경계 영역만 보호하는 것으로는 충분하지 않습니다. APT(Advanced Persistent Threat)와 같은 지능적 공격은 기존의 방어 체계를 뛰어넘고 있습니다.

중대한 보안 사고로 인해 기업의 데이터, 네트워크 및 브랜드까지 타격을 입을 수 있다는 사실을 우리 모두 잘 알고 있습니다. 끊임없이 주요 정보에 대한 접근을 시도하거나 주요 인프라에 피해를 주도록 설계된 지능적 공격이 점점 더 빈번하게 발생하면서 큰 경제적 피해를 입히고 있습니다.

그 심각도는? 지능적 보안 공격에는 다음 유형이 포함될 수 있습니다.

- 지적 재산 도용
- 은행 계좌 및 기타 금융 자산 탈취
- 개별 컴퓨터와 각종 시스템에 악성 코드 유포
- 기밀에 속하는 영업 정보 및/또는 고객 정보 온라인 게시
- 주요 인프라 손상

그 빈도는? 2012년에 미국, 영국, 독일, 홍콩과 브라질의 기업 경영자와 보안 실무자 2,618명을 대상으로 실시한 조사의 결과를 보면, 이들은 매주 평균 66건의 공격을 받고 있으며 그 중에서도 독일과 미국의 수치가 각각 82건과 79건으로 가장 높았습니다. 또한 IBM X-Force 연구 개발 팀은 2012년 중반에 발표한 보고서에서 모든 취약점 영역이 증가하는 추세라고 전하면서 그 해 말에 사상 최고치에 이를 것으로 예측했습니다.[2]

그 비용은? 앞서 소개한 2012년 조사에서 추정한 바에 의하면, 보안 공격 1건당 평균 복구 비용은 최대 30만 달러에 달합니다.[3] 따라서 1년간 총 10억 달러에 가까운 비용이 발생할 수 있습니다.

설상가상으로, 이러한 지능적 공격의 배후에는 장기간에 걸쳐 공격을 준비하는 끈질긴 계획자들이 있습니다. 이들은 철저한 사전 조사를 거쳐 구체적인 취약점을 표적으로 삼으며, 기존의 익스플로잇 공격 중심에서 파괴적 공격의 성향으로 바뀌고 있는 중입니다.

이 백서에서는 기업을 안전하게 보호하기 위해 지금 실천해야 할 4단계의 사전 예방 조치를 소개합니다.

- 비즈니스 목표의 **우선 순위** 결정 및 리스크 허용 한도 설정
- 사전 예방적 보안 계획으로 기업 **보호**
- 불가피한 상황, 즉 지능적 공격에 **대비**
- 보안 인식의 문화 **증진** 및 지원

1단계: 비즈니스 목표의 우선 순위 결정 및 리스크 허용 한도 설정

지난 몇 년간의 경험에 따르면, "보안"은 상대적인 용어입니다. 영구적으로 확실한 기업 안전을 실현하겠다는 매우 강한 의지와 노력이 있더라도 현실은 그 반대로 전개되곤 합니다. 그러나 지능적 보안 공격의 위협이 날로 거세지고 있는 상황에서 기업은 정보를 지키고 사용자와 인프라를 보호해야 할 책임이 있습니다. 이러한 임무는 우선 순위의 결정에서 시작합니다.

기업의 보안에 가장 중요한 과제와 그 이유 확인

극히 당연한 얘기지만, 시간을 내어 회사의 목표에 대해 숙고하여 무엇이 가장 중요한지를 결정해야 합니다. 어느 정도의 리스크를 감수할 수 있는지 논의한 후, 회사 전반의 고유한 요구 사항에 부합하는 보안 전략을 수립할 수 있는 탄탄한 기반을 조성해야 합니다. 이러한 기준은 올바른 방향으로 진일보할 수 있는 밑거름이 됩니다.

가장 공격에 취약한 영역 파악

기업의 보안에는 상대적으로 더 중요한 부분이 있는가 하면, 유난히 더 취약한 영역도 있습니다. 누구의 잘못을 지적하거나 책임을 전가하려는 것이 아니라, 현실을 직시하려는 것입니다. 이로써 전반적으로 더 안전한 환경을 마련할 수 있습니다.

가장 큰 위협이 될 구체적인 공격 유형 식별

지능적 공격은 피해를 극대화하도록 설계된 만큼 주요 정보의 손실이나 악용 및/또는 주요 인프라의 파손을 야기합니다. 공격자의 입장에서 회사의 정보 및 비즈니스 크리티컬 시스템을 바라볼 필요가 있습니다. 공격자라면 어떤 방식으로 가장 큰 피해를 일으킬 것인지 생각해 보십시오.

공격이 일어날 때 가장 큰 손실을 입을 영역 파악

이는 최악의 사태가 일어날 수 있는 영역을 의미합니다. 제대로 계획을 수립한다면, 가장 치명적인 곳에서 공격을 받을 경우 얼마나 심각한 피해가 발생할 것인지 정확하게 판단할 수 있습니다.

공격자의 입장에서 회사의 정보 및 비즈니스 크리티컬 시스템을 바라볼 필요가 있습니다.

온라인 게임/엔터테인먼트 사이트가 해킹을 당해 1억 건의 고객 정보 유출

예상 손실: 36억 달러

피해자: 온라인 게임 커뮤니티와 엔터테인먼트 사이트

사건 개요: 한 게임 네트워크에 "외부의 침입"이 발생하여 7천만 개의 고객 계정이 유출되었고 개인 정보와 신용 카드 데이터의 보안이 위험한 상태에 처했습니다. 이 회사는 수사가 진행되는 동안 온라인 서비스를 "중지"해야 했고, 그로 인해 대중의 반발과 부정적 언론 보도가 확산되었습니다. 엔터테인먼트 부문에서 2차 해킹이 일어나 고객 데이터가 추가로 유출되었습니다.

발생 경위: 해커들은 네트워크 보안을 뚫고 암호화되지 않은 계정 및 사용자 데이터에 액세스한 것으로 알려졌으며, 따라서 일부 신용 카드 데이터에도 접근했을 가능성이 있습니다.

피해 규모: 보도된 바에 따르면, 부정적 여론의 확산 외에도 영업 손실 및 대처 비용으로 1억 7,100만 달러 이상의 비용이 발생했습니다. 이 회사의 주가가 12% 하락하면서 시가 총액도 약 36억 달러 감소했습니다.

이 사례가 주는 교훈: 이번 해킹에 악용되었던 취약점 중 하나는 회사가 이미 알고 있는 것이었습니다. 각 기업은 정보 자산과 관련된 리스크를 관리할 프레임워크를 활용하고, 이를 뒷받침할 강력한 거버넌스 메커니즘을 구축해야 합니다.

사례로만 참조하십시오. 이 시나리오의 실제 사실과 피해 규모는 예시된 내용과 다를 수 있습니다. 추정치는 공개된 재무 정보와 게재된 기사를 토대로 한 것입니다.

2단계: 사전 예방적 보안 계획으로 기업 보호

우선 순위를 정했다면 계획을 세우고 적합한 기술을 도입한 후 모든 것을 실행에 옮길 차례입니다. 회사 차원에서 잠재적 보안 위협을 인식하고 이를 지속적으로 방지하기 위한 사전 예방 조치에 나서는 단계입니다.

사전 예방적이고 정보에 기초한 IT 보안 방식 마련

1단계에서의 우선순위에 따라 자산과 정보를 사전 예방적으로 보호하기 위한 정책과 기술을 활용하여 보안 전략을 수립하십시오. 취약점을 성공적으로 관리할 수 있도록 준비하는 것은 사전 예방적 보안 활동의 핵심적인 부분 중 하나이며, 수립된 보안 정책은 정보 보안 관리 전략의 기초가 됩니다. 이러한 정책을 통해 보안 요구 사항, 프로세스, 기술 표준을 문서화해야 합니다. 또 다른 효과도 기대할 수 있습니다. 똑똑한 보안 전략으로 취약점을 탐지하여 제거할 뿐 아니라 리스크를 최소화하고 IT 보안 관리 비용을 절약함으로써 기업 경영을 개선할 수 있습니다.

기존의 취약점 파악 및 해결

이는 간단하면서도 상당한 자원을 필요로 하는 프로세스가 될 수 있습니다. 모든 시스템의 모든 운영 체제에서 최신 보안 패치를 적용하고 유지하는 것을 예로 들 수 있습니다. 한편 비즈니스 애플리케이션의 문제처럼 탐지하고 해결하기가 더 까다로운 취약점도 있습니다.

기존 보안 위협 처리

아직 지능적 공격의 표적이 되지 않았다고 확신할 수 있습니까? 특히, APT와 같이 치명적인 공격은 최대한 오랫동안 드러나지 않은 상태로, 눈에 띄는 네트워크 트래픽을 발생시키지 않으면서 각 호스트를 차례로 공략합니다. 모든 APT의 핵심에는 원격 제어 기능이 있는데, 공격자는 이를 통해 표적으로 삼은 조직 내 특정 호스트로 이동하고, 로컬 시스템을 조작하고, 중요 정보에 지속적으로 접근합니다. 스스로를 보호하기 위해서는 회사의 시스템과 침입자 간의 원격 제어 통신을 탐지하는 툴이 필요합니다.

보안 정책, 절차 및 기술의 실효성을 테스트하는 데 각별한 관심을 기울이는 것이 그 어느 때보다도 중요합니다.

테스트 강화

지능적 공격의 등장으로 어떤 기업이든 공격으로부터 안전하다고 장담할 수 없게 되었습니다. 따라서 보안 정책, 절차 및 기술의 실효성을 테스트하는 데 각별한 관심을 기울이는 것이 그 어느 때보다도 중요합니다. 이는 정당한 주의와 관리의 책임을 규정한 법적 요건의 핵심 요소이기도 합니다. 이 요건을 제대로 이행하지 않을 경우 기업 경영진이 보안 사고의 결과에 대한 책임을 지게 됩니다.

보안 환경이 갈수록 빠른 속도로 변화하고 있으므로 정기적인 테스트 및 검토를 위한 정책을 마련하고 이행하는 것도 중요합니다.

똑똑한 보안 인텔리전스 방식 선택

IT 부서를 공황 상태로 몰아넣지 않으면서 이 모든 것을 해결할 방법이 있을까요? 보안 인텔리전스 및 분석 툴은 적극적으로 각종 보안 기술을 모니터링하고 데이터 활동의 상관성을 분석하면서 해당 환경의 현황에 대한 가시성과 통찰력을 제공합니다. 따라서 공격으로 의심되는 활동 유형을 찾아내고 조사할 수 있습니다. 멀티벤더 환경의 전반에서 하나의 공통 언어로 통신하므로 복잡성이 최소화되고 IT 부서의 부담도 줄일 수 있으며, 시간 및 비용 절감의 효과도 기대할 수 있습니다.

거버넌스 절차 수립, 리스크에 대한 책임 부여

지능적 공격과 같은 보안 위협을 막아내도록 설계된 보안 프로그램과 정책의 실효성은 조직의 모든 구성원이 규칙을 따르도록 얼마나 효과적으로 감독하느냐에 따라 달라집니다. 그러므로 장기적으로 모든 것을 관리하기 위한 계획을 마련해야 합니다. 여기에는 보안 정책을 모니터링하고 관리할 담당자, 리스크 상황을 관리하고 있음을 입증할 방식 등을 결정하는 것도 포함됩니다. 모든 주요 비즈니스 영역에서 보안 프로그램에 대한 책임과 리더십을 갖게 하십시오. 주요 리스크 영역 모두에서 책임과 인식을 확대함으로써 보안 제어 기능에 대한 이해와 실천을 강화할 수 있습니다. 이는 궁극적으로 더 안전한 비즈니스 환경의 조성으로 이어집니다.

보안 투자의 가치 입증 및 문서화

의문의 여지 없이, 각 기업은 효과적인 보안 프로그램을 개발하고 유지하는 데 필요한 예산을 확보해야 합니다. 아직 일어나지 않은 보안 공격을 염두에 두고 그러한 프로그램의 가치를 수치화하기란 쉽지 않으므로, 현재 어떤 노력을 기울이고 있으며 그것이 왜 중요한지 지속적으로 알리는 것이 좋습니다. 이를테면 주요 시스템과 데이터에 침투했거나 그럴 가능성이 있는 심각한 공격 활동에 대해 보고함으로써 보안 기술 투자의 가치를 입증하고, 취약점을 파악하고, 진행 중인 공격을 차단하고, 능률화의 기회를 발굴하고, 추진 중인 보안 방식에 대한 신뢰를 높일 수 있습니다.

49%

의 IT 임원들이 현재 보안 조치의 실효성을 수치화하지 못해 어려움을 겪고 있다고 밝힙니다.[4]

허점이나 불필요한 중복이 없도록 철저히 검토

팀을 이뤄 일하지만 계획에서 특정 측면을 책임지고 있을 경우, 내가 미처 하지 못한 일을 다른 누군가가 처리했을 것으로 속단하기 쉽습니다. 이와 같이, 여러 사람이 같은 일을 하게 되는 경우가 종종 발생합니다. 따라서 명료성과 완전성에 대한 최종 점검이 필요합니다. 보안 인텔리전스, 분석, 모니터링 등의 항목이 모두 포함되었는지 확인하여 불필요한 복잡성과 지출을 피해야 하며, 여러 기술을 통해 지속적인 모니터링, 관리, 실시간 의사결정을 간소화할 기회를 모색하십시오.

소매업체에서 18개월 이상 계속된 고객 데이터 유출 – 4,500만 건 이상 유출

예상 손실: 최대 9억 달러

피해자: 전국적인 할인 소매업체

사건 개요: 이 회사의 시스템에서 고객의 신용 카드 및 직불 카드 번호 약 4,500만 개가 유출된 것으로 보이지만, 사건의 성격과 지속 기간 때문에 실제 유출 규모를 파악하는 데 어려움이 있습니다. 이 데이터는 범죄자들에게 팔려 사기 구매에 이용되었습니다.

발생 경위: 보도된 바에 따르면, 이 회사는 불필요하고 방대한 개인 정보를 수집하여 지나치게 오랜 기간 동안 보관했고, 이를 보호하는 데 낡은 암호화 기술에 의존했습니다. 해커들은 초기에 소매 매장의 안전하지 않은 무선 연결을 통해 중앙 데이터베이스에 액세스한 것으로 보입니다. 이 회사는 결제 서비스 업계의 표준 요건을 준수하지 않은 것으로 추후 확인되었습니다.

피해 규모: 같은 유형의 보안 사고 중 가장 큰 규모로 알려지면서 광범위한 언론 보도가 이어졌습니다. 각종 소송 비용, 무거운 벌금, 조정 비용과 함께 이미지 실추 및 기타 간접적인 비용이 더해져 그 피해 규모는 헤아릴 수 없는 수준에 이르렀습니다.

이 사례가 주는 교훈: 변화하는 보안 위협과 기술 때문에 과거에는 적합했던 보호 수단이 더 이상 유효하지 않을 수 있으므로 인프라 및 정보 리스크에 대한 정기적인 재평가가 필수적입니다.

사례로만 참조하십시오. 이 시나리오의 실제 사실과 피해 규모는 예시된 내용과 다를 수 있습니다. 추정치는 공개된 재무 정보와 게재된 기사를 토대로 한 것입니다.

3단계: 불가피한 상황, 즉 지능적 공격에 대비

최대의 노력을 들여 보안 정책, 절차와 기술을 구현했다면 이제 만일의 보안 사고를 어떻게 처리할지 생각할 차례입니다. 한 분석가가 최근 지적한 대로, 대기업의 보안 관리자 및 최고 정보 보안 책임자 대부분은 보안 사고가 일어나는 것이 시간 문제임을 인식하고 있습니다.[5]

세부적이고 통합적인 대응 계획 수립

보안 사고에 대한 대응을 관리할 수 있는 통합적이고 범기업적인 정책과 프로세스가 필요합니다. 이미 계획을 수립했다면, 최근에 이를 테스트하여 그 실효성을 확인했습니까?

보안 사고 대응 계획에서는 공격을 차단하고 공격에 의해 손상된 부분을 파악할 방법과 함께, 회사의 재정과 평판에 미칠 영향을 산정할 방법을 명시해야 합니다. 또한 직원, 유출된 정보의 당사자 및 미디어와의 커뮤니케이션에 대한 지침도 제시해야 합니다.

신속한 대응에 필요한 자원 및 툴 확보

공격을 받은 후 해결하는 시간이 길어질수록 피해가 더욱 커지고 부담해야 할 비용도 늘어날 것입니다. 한편 최근에 IBM의 의뢰로 실시된 평판 리스크 관련 설문 조사에서 기업 고위 임원의 약 78%는 비교적 가벼운 보안 사고(예: 웹 사이트 가동 중단)의 경우 6개월 이내에 복구 가능하다고 밝혔습니다. 그러나 사이버 범죄로 인해 실추된 이미지는 회복하는 데 매우 오랜 시간이 걸립니다. 여기에는 문제가 완전히 해결되었다는 메시지를 제대로 전달하기가 더 어려울 수 있다는 점도 원인으로 작용합니다.[6]

적극적으로 보안 사고에 대처하고 이를 조사하는 데 필요한 자원 또는 기술력의 확보가 보안 사고의 영향을 최소화하는 데 필수적입니다.

적극적으로 보안 사고에 대처하고 이를 조사하는 데 필요한 자원 또는 기술력의 확보가 그러한 사고의 영향을 최소화하는 데 필수적입니다. 기업의 평판이 영업 활동에 중대한 영향을 미치고 사업의 속성상 지능적 공격으로 인한 리스크가 클 경우, 지속적인 보안 위협 모니터링 및 관리 기능의 도입을 고려할 필요가 있습니다. 이 방식에서는 방어 기능을 강화하고 사고 대응을 자동화하고 광범위한 보안 위협에 대한 포렌식(Forensic) 분석을 실시하는 기술을 활용합니다.

전사적 범위에서 일관성 있게 책임 부여

어떤 기업이든 언젠가는 어떤 유형의 지능적 공격을 받게 된다는 사실을 인정하십시오. 사고 대응 계획에서 누가 무엇을 할지, 모든 관계자가 어떻게 정보를 공유할지 명시해야 합니다. 공격을 효과적으로 탐지하고 해결하고 차단하기 위해서는 전사적 차원의 공조가 필수적입니다. 모든 관계자가 각자 역할을 맡고 자신의 역할을 제대로 이해하는 것이 중요합니다. 이해 관계자들이 지능적 공격의 발생 횟수 및 범위를 최소화하기 위해 각자의 영역에서 어떤 절차로 대비할 것인지 결정하십시오.

결제 서비스 업체의 핵심 비즈니스 시스템에 일어난 침해 사고로 1억 3천만 명의 고객에게 피해 발생

예상 손실: 최대 5억 달러

피해자: 결제 서비스 업체

사고 개요: 한 결제 처리 시스템에서 약 1억 3천만 개의 고객 신용 카드 및 직불 카드 번호가 유출되어 사기 거래에 이용되었습니다.

발생 경위: 악성 소프트웨어가 처리 시스템에 침투하여 거래 승인 과정에서 암호화되지 않은 상태로 전송되는 결제 데이터를 수집한 것으로 보입니다. 카드 데이터에는 카드 번호, 유효 기간을 비롯하여 결제 카드의 뒷면 마그네틱선에 수록된 각종 정보도 포함됩니다.

피해 규모: 많은 관심이 집중된 대형 사고였기 때문에 각 언론에서도 앞다퉈 보도했습니다. 이 회사는 재판, 조정, 각종 비용으로 1억 4천만 달러 이상을 부담한 것으로 알려졌습니다. 게다가 사건 후 3개월 만에 시가 총액은 약 5억 달러 감소했습니다.

이 사례가 주는 교훈: 이 회사는 직접적이고 적극적인 위기 대응을 통해 고객 이탈을 최소화했습니다. 산업 표준화 기관에서 공유 및 활용되는 정보를 통해 보안 상태를 강화했고 결국 시가 총액 손실을 만회했습니다.

사례로만 참조하십시오. 이 시나리오의 실제 사실과 피해 규모는 예시된 내용과 다를 수 있습니다. 추정치는 공개된 재무 정보와 게재된 기사를 토대로 한 것입니다.

4단계: 보안 인식의 문화 증진 및 지원

수천 대의 장치에서 수십 가지의 공용 웹 기반 서비스를 통해 각종 정보가 쏟아져 들어오면서, 기업의 네트워크를 보호하는 일은 갈수록 어렵고 복잡해지고 있습니다. 한 조사에 따르면, 기업의 스마트폰 사용자 중 91%가 회사 이메일 시스템에 접속하지만 모바일 보안 소프트웨어 설치를 의무화한 곳은 1/3에 불과했습니다.[7] 범죄자를 비롯하여 누구라도 수월하게 액세스할 수 있는 환경인 것입니다.

전사적 범위에서 리스크 인식의 문화 조성 및 지원

이제는 엔터프라이즈 보안의 사명을 기술 팀과 그 시스템의 전유물로 한정하지 않고 회사의 모든 구성원 및 거래 상대에게 확장하여 적용해야 합니다. 각자가 보안 사고의 위험성을 안고 있으므로 모든 사람이 솔루션에 동참해야 합니다. 리스크를 인식하는 문화, 즉 사내 프로세스의 각 단계에서 모든 의사 결정과 절차에 보안의 중요성을 인식하는 문화를 조성하고 장려해야 성공에 이를 수 있습니다. 다시 말해, 데이터 보안 절차는 외출할 때 현관문을 잠그는 것처럼 습관으로 자리잡아야 합니다.

모든 직원이 각자의 할 일 이해

회사의 문화를 바꾸는 것은 매우 어려운 일일 수 있습니다. 그러나 보안 개선에 동참하는 것의 중요성을 알리고, 모든 사람에게 보안 문제를 파악하고 보고하는 방법을 교육하는 것으로 시작함으로써 올바른 방향으로 나아갈 수 있습니다.

IBM 보안의 핵심 원칙

IBM은 비즈니스 수행 방식의 발전과 리스크 제어의 필요를 균형적으로 추구하기 위해 끊임없이 노력하고 있습니다. IBM의 종합적인 대응 솔루션은 기술, 프로세스 및 정책의 수단을 모두 포함하며 10가지 핵심 원칙을 실천합니다.

1. 리스크 인식의 문화 조성 – 이러한 문화에서는 직원들이 보안에 대해 부주의하게 행동하는 것을 회사 차원에서 절대 허용하지 않습니다. 경영진은 최상위 단계부터 적극적으로 이러한 변화를 추진하고, 진행 상황을 점검하기 위한 툴을 구현해야 합니다.

2. 사고 관리 및 대응 – 지능형 분석 및 자동 대응 기능을 구현하기 위한 전사적 차원의 공조가 필수적입니다. 자동화되고 통합된 시스템을 구축함으로써 운영 상황을 모니터링하고 신속하게 대응할 수 있습니다.

3. 사용자 보호 – 각 워크스테이션, 랩탑 또는 스마트폰은 악성 공격의 진입로가 될 수 있습니다. 각 장치의 설정을 모두 중앙에서 관리하고 적용해야 하며, 사내의 데이터 흐름을 분류하여 반드시 올바른 사용자에게 전달해야 합니다.

4. 설계상의 보안 – 정보 시스템의 최대 취약점 중 하나는 먼저 서비스를 구현한 다음 보안을 추가하는 관례로 인한 것입니다. 유일한 해결책은 처음부터 보안을 구현하고 정기적인 테스트를 통해 그 준수 현황을 점검하는 것입니다.

5. 흠 없이 안전한 상태로 유지 – 각종 소프트웨어의 업데이트를 관리하는 것이 불가능해 보일 수도 있습니다. 안전한 시스템에서는 실행 중인 모든 프로그램을 추적할 수 있고, 최신 버전임을 확신할 수 있으며, 새로 출시되는 업데이트와 패치를 즉시 설치할 수 있습니다.

6. 네트워크 액세스 제어 – 모니터링되는 액세스 지점을 통해 등록 데이터를 전송하면 악성 코드를 훨씬 수월하게 적발하고 격리할 수 있습니다.

7. 클라우드의 보안 – 기업의 어떤 IT 서비스를 클라우드 환경으로 이전하게 되면 사기 범죄자를 비롯한 다양한 사람들이 정보에 더 쉽게 액세스할 수 있게 됩니다. 따라서 다른 사용자와 격리하고 보안 위협을 모니터링할 수 있는 툴과 절차를 마련하는 것이 중요합니다.

8. 인근 영역에 대한 감시 – 기업의 보안 문화는 기업의 경계를 넘어 확장되어야 하며, 협력업체와 공급업체까지 포괄하는 베스트 프랙티스가 마련되어야 합니다. 이는 한 세대 전에 품질 관리를 위해 수립되었던 프로세스와 유사합니다.

9. 회사의 자산 보호 – 각 기업은 중요 자산, 즉 과학 또는 기술 데이터, 기밀 문서, 고객의 개인 정보 등을 인벤토리화하고 특별히 취급해야 합니다. 우선 순위에 오른 각 항목은 회사의 생존을 좌우하는 자산으로 간주하고 보호, 추적 및 암호화해야 합니다.

10. 사용자 관리 및 추적 – 기업에서 "ID 라이프사이클"을 제대로 관리하지 못하면 암흑 속에서 운영하는 것과 다를 바 없으며, 침입에 취약해질 수 있습니다. 사용자를 식별하고, 사용 권한을 관리하고, 퇴사한 사용자의 권한을 즉시 삭제하는 시스템을 구현함으로써 이러한 리스크를 해소할 수 있습니다.

*그림 1. **10대 핵심 실천 원칙:** 성공적인 보안 프로그램은 유연성과 혁신의 균형을 유지하면서 전사적 차원에서 이해하고 실천할 수 있는 일관성 있는 안전 장치를 마련하고 유지합니다.*

당장 시작 - 공격으로 피해를 입기 전에

IBM X-Force는 2012년 상반기에만 4,400건 이상의 새로운 보안 취약점을 보고했습니다. 이러한 추세가 계속된다면 2010년에 기록했던 약 9,000건을 넘어설 전망입니다. 뿐만 아니라 IBM X-Force에서 2012년 상반기에 파악한, 패치가 없는 취약점의 비율도 2008년 이후 가장 높았습니다.

많은 기업이 비밀번호 및 개인 데이터 유출로 인한 막대한 피해를 감수해야 했습니다. 이러한 공격은 갈수록 지능화되고 있습니다.

예를 들어, 공격자는 공개된 소셜 미디어 사이트에서 얻은 약간의 개인 정보만으로도 고도의 사회공학적 "수법"을 구사하여 표적 계정에 대해 무제한적인 액세스 권한을 확보할 수 있습니다. 모바일 사업자로 하여금 사용자의 음성 사서함을 재배치하게 하여 이중(2-factor) 인증 체계도 통과할 수 있습니다. 어떤 기업이든 언젠가는 이러한 공격을 받을 수 있습니다. 실제로 IBM이 최근 실시한 평판 리스크 및 IT에 관한 설문 조사에서 고위 임원의 61%는 데이터 유출, 데이터 도용과 사이버 범죄가 회사의 평판을 위협하는 가장 큰 요소라고 밝혔습니다.[8]

어떤 기업이든 언젠가는 공격을 받게 될 것입니다.

도움을 받는 것은 현명한 선택

지능적 공격으로부터 회사를 보호한다는 것은 엄청난 부담으로 다가올 수도 있습니다. 논의하고, 고려하고, 염려해야 할 것이 많습니다. 그러나 한 번에 하나씩 해나가면 됩니다. 홀로 모든 것을 해결할 필요도 없습니다.

IBM Security Services 컨설턴트는 보안 전략의 모든 측면에서 계획, 구현과 관리를 지원합니다. 이들은 공공 및 민간 분야에서 기업의 보안 관리 및 컨설팅 팀, 정부 기관의 수사 조직, 법 집행 및 연구 개발 기관 등과 공조하면서 기술력을 갈고 닦은 수준 높은 보안 전문가들입니다.

컨설팅 서비스 제공에 더해, IBM은 1995년부터 보안 관제 서비스(Managed Security Services)의 책임, 안정성 및 보호 기준을 마련하는 데 기여해 왔습니다. 보안 관제 서비스는 장치 유형 또는 벤더와 상관없이 연중무휴로 또는 필요에 따라 보안 운영의 모니터링 및 관리 업무를 IBM에 아웃소싱함으로써 고객의 정보 보안 수준을 높이고, 총 소유 비용을 줄이고, 규정 준수를 입증할 수 있도록 지원합니다.

IBM Managed Security Services는 인터넷 공격으로부터 기업의 정보 자산을 보호하는 데 필요한 보안 인텔리전스, 전문성, 툴과 인프라를 자체적으로 보안 자원을 두는 것보다 훨씬 저렴한 비용으로 상시 제공합니다.

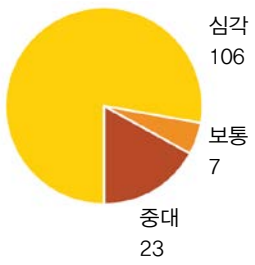
무료 보안 상태 점검 서비스로 시작

그렇다면 귀사는 현재 얼마나 취약한 상태일까요? IBM Security Services의 무료 보안 상태 점검을 통해 확인할 수 있습니다. IBM은 귀사가 선택한 최대 10개의 IP 주소 또는 하나의 웹 도메인을 대상으로 3주간, 주 1회씩 검사를 실시합니다. 발견된 취약점은 심각도 등급에 따라 분류되며, 이를 해결할 단계적 지침이 상세 분석 보고서에 포함되어 제공됩니다. 뿐만 아니라 검사가 진행되는 기간에 귀사는 IBM Managed Security Services의 Virtual Security Operations Center 포털에 액세스하여 다양한 인텔리전스 서비스와 보안 위협 관련 정보를 이용할 수 있습니다.

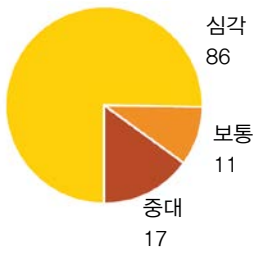
보안 상태 점검으로 알 수 있는 것

다음은 몇몇 고객 유형에 대해 보안 상태 점검을 실시한 결과의 예로서, 연속 3회 실시되는 주간 검사 중 1회를 마치고 발견한 취약점의 평균 개수를 보여 줍니다. 가장 안전하다는 기업도 위험 수준이 상당히 높은 것으로 드러났으며, 다수의 영역에서 이러한 위험이 나타나고 있습니다. 오늘날의 역동적인 비즈니스 환경에서는 더 이상 경계가 존재하지 않습니다. 따라서 어떤 기업이든 이러한 취약점과 위험성을 가지고 있을 가능성이 있습니다.

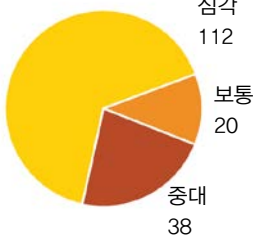
대학



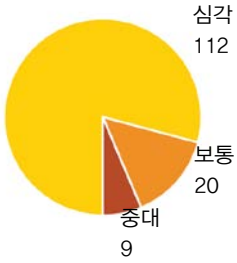
보험사



가상 호스팅/웹 호스팅 업체



시 정부



추가 정보

IBM Security Services로 지능적 보안 위협을 더 효과적으로 차단하고 비용 부담을 줄일 수 있는 방법에 대한 자세한 내용은 IBM 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 다음 웹 사이트에서 확인하십시오. ibm.com/services/security

보안 상태 점검 무료 서비스를 이용하려면 다음 사이트에서 등록하십시오. ibm.com/security-scan

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

Produced in the United States of America
February 2013

[1] Ponemon Institute LLC, *The Impact of Cybercrime on Business: Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil sponsored by Check Point Software Technologies*, May 2012.
[2] IBM X-Force 2012 Mid-year Trend and Risk Report, September 2012.
[3] See note 1 above.
[4] *Security Intelligence Can Deliver Value Beyond Expectations And Needs To Be Prioritized*, a commissioned study conducted by Forrester Consulting on behalf of IBM Global Technology Services, May 2012.
[5] Blog post: *"Okay, Breaches Are Inevitable: So Now What Do We Do?"* by Paula Musich, Current Analysis, July 20, 2012.
[6] IBM Global Technology Services, Reputational risk and IT, September 2012.
[7] Kaspersky Labs, Enterprise Mobile Security Survey, December 2010.
8 See note 6 above.

Please Recycle

SEW03029-USEN-00