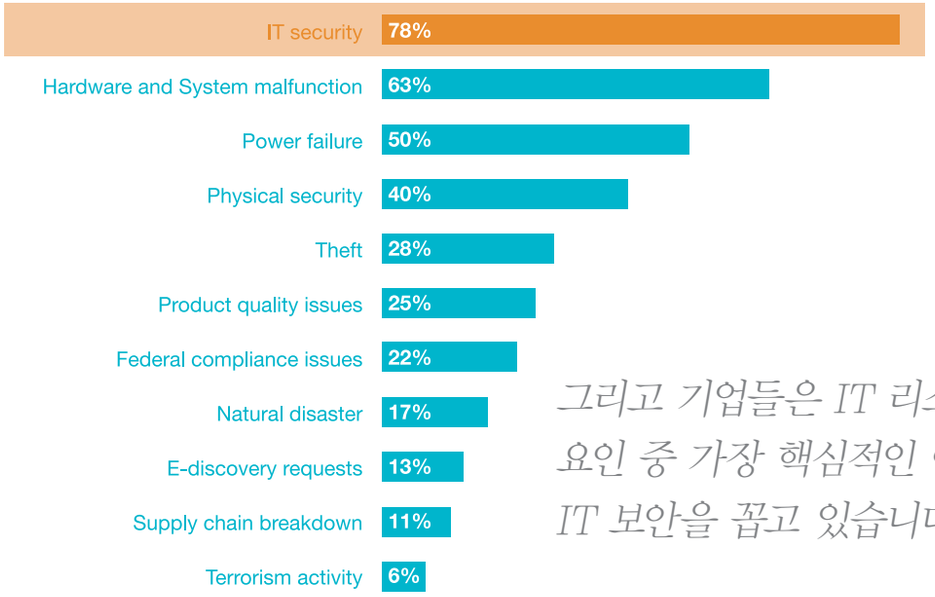

귀사의
비즈니스는
안전하십니까?
IBM Security Framework

IBM Security Framework

비즈니스의 IT 의존도가 증가됨에 따라 IT 리스크는 비즈니스 연속성 확보를 위해 기업 차원에서 관심을 기울여야 할 중요한 관리 대상으로 부각되고 있습니다

기업의 비즈니스에 영향을 주는 보안사고들이 지속적으로 증가하고 있으며 기존에 수립되고 운영되고 있는 보안체계에 대한 재검토 및 개선이 시급합니다

기업들의 IT 리스크 이슈



< Source: IBM Global IT Risk Study, 2010 >

그리고 기업들은 IT 리스크 요인 중 가장 핵심적인 이슈로 IT 보안을 꼽고 있습니다.

$226 Billion
사이버 공격으로 인한 연간 경제적 손실액

158% increase
2006년 이후 사이버 공격으로 인한 보안 사고 158% 증가

52%
기업의 보안사고 중 내부자에 인한 사고가 52%를 차지

기업 비즈니스의 연속성을 위해 무엇보다 중요한 IT 보안, 어떻게 관리하고 계십니까?

IBM Security Framework

귀사의 소중한 정보가 '탈옥' 하도록 그대로 보고만 계시지는 않습니까?

41
국내 첨단기술 유출 피해 건수(2010년)

90조
국내 첨단기술 유출 피해 금액(2010년)

13만
지난 3년간 공식 신고된 개인 정보 유출 건수

87%
내부 사용자로부터 기인한 내부 정보 유출 사고 건수

기업 경영에 심각한 타격을 미치는 **기업의 기밀정보 누출 사건**이 매년 증가하고 있습니다. 기업의 기밀 정보 누출은 곧 기업의 핵심 역량이 외부로 노출되는 것을 의미하며 기업 경쟁력 강화를 저해하는 요인으로 작용합니다.

기업의 비즈니스 연속성을 위협하는 보안 사고에 대비하기 위해 기업은 사고 발생에 따른 일시적인 대응책이 아닌 근원적인 IT 보안 인프라 개선 및 내부통제 강화 등 기술적 보안 관리 강화를 통한 해킹 등 침해 사고 발생 가능성을 최소화 해야 합니다.

사고 발생 이후 뒤늦은 대응을 하시겠습니까? 빈틈 없는 보안 강화를 통해 사전 예방이 가능합니다

개인정보보호 2.0 시대의 개막 "개인정보보호법 제정·공포"

– 모든 공공기관·사업자를 규율대사응로 9월 30일 전면 시행

2004년부터 입법논의가 시작된『개인정보보호법(법률 제10465호)』이 3월 29일 공포되고, 공포 이후 6개월이 경과되는 2011년 9월 30일부터 전면 시행된다.

정보유출에 따르는 막대한 피해를 줄이고 개인정보보호 수준을 높이기 위한 대책으로 정부는 **2011년 9월 30일 개인정보보호법**을 전면 시행합니다. 개인정보보호법 제정으로 모든 공공기관과 사업자를 규율 대상으로 확대하고, 개별법간 상이한 처리기준에 대해 개인정보 처리 단계별 공통된 보호기준과 원칙의 준수가 필요합니다.

각 기업의 정보보안을 위한 대책 마련이 시급한 지금, 정확한 분석과 예측을 통해 기업에 요구되는 보안 수준에 맞는 솔루션을 설계하고 각 기업별 요건에 따라 최적화된 보안 솔루션을 전략적으로 구축하는 스마트한 접근방식이 필요합니다.

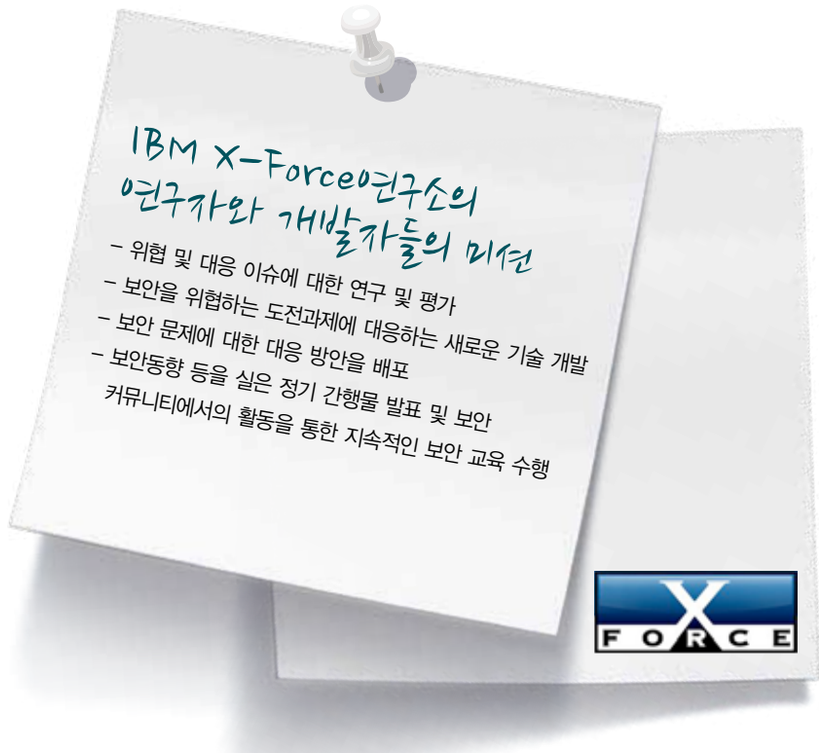
IBM Security Framework

보안의 위협 때문에 새로운 기술이 주는 엄청난 효율성과 혜택을 포기하고 있지는 않습니까?

세상은 빠르게 변화하고 있습니다. 변화하는 세상에서 기업이 경쟁력을 갖추기 위해서는 새로운 기술과 전문성을 도입하는 것이 필수적일 것입니다. 2011년을 뜨겁게 달구고 있는 모바일과 클라우드, 혹시 보안이 우려되어 도입을 망설이고 계십니까?

모바일 장치 관리를 위한 효과적 제어와 클라우드를 위한 특화된 보안을 위한 전략적인 보안 설계를 통하여 보안은 비즈니스의 장애물이 아닌, 클라우드 컴퓨팅, 소셜 네트워킹과 가상화와 같은 혁신적인 기술들을 적용하기 위한 비즈니스의 원동력이 될 것입니다.

우리회사를 위한 보안 전문가를 찾고 계십니까?



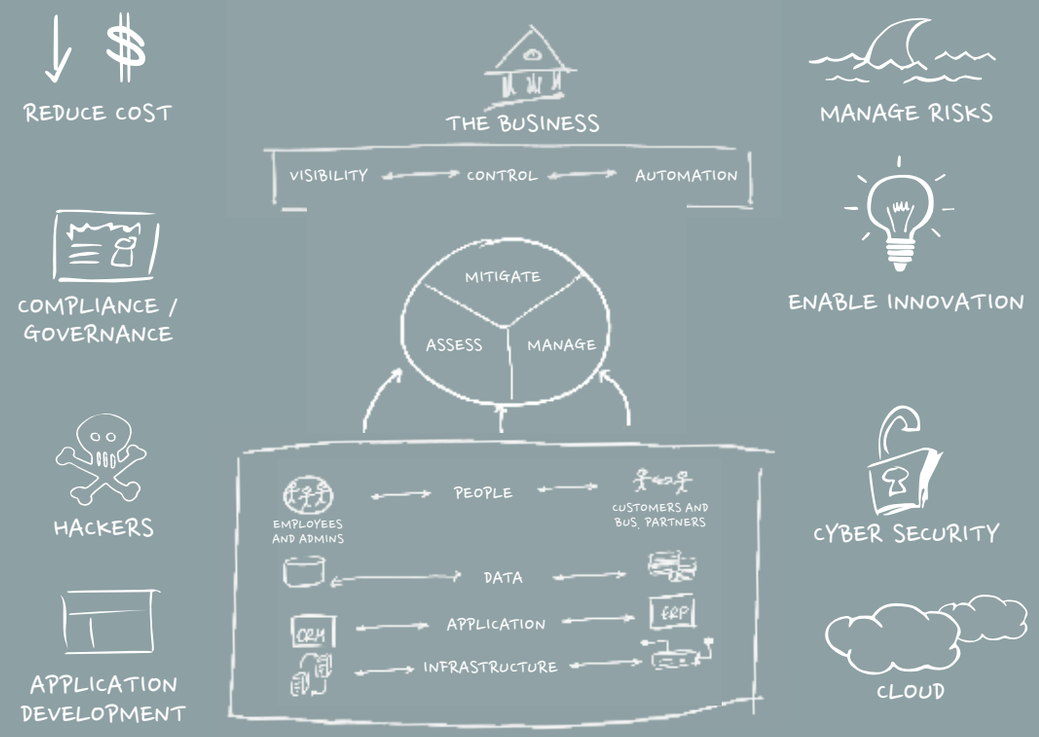
IBM X-Force Research Lab

IBM의 X-Force 연구소는 WW #1의 기업 내부의 독립된 보안연구소로,
보안 취약점 및 다양한 보안 이슈에 대한 연구 및 평가를 수행하고 있으며,
스마트폰을 비롯한 보안 취약점에 대한 가장 많은 DB를 보유하고 있습니다.

Why Security ? **Why Now ?**

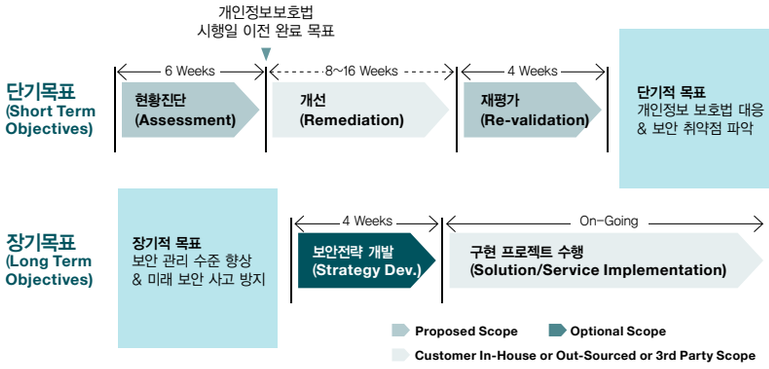
비즈니스 관점에서 바라본 보안의 핵심목표는 안전한 비즈니스 수행, 관련된 인프라의 안전한 운영을 제공하는 것입니다

"보안은 IT 서비스 운영의 가시성 (Visibility), 통제성 (Control), 자동화 (Automation)를 확보하여 비용절감, 위험관리, 규제 준수, 비즈니스 개선의 도구로 자리매김해야 합니다."



Why IBM ? **IBM Security Service**

IBM은 개인정보 보호법 준수 등 단기적 목표와 전반적 보안 대응 수준의 향상 등 장기적 목표 달성을 위해 두 개의 주요 Track으로 구성된 프로젝트 수행을 제언 드립니다

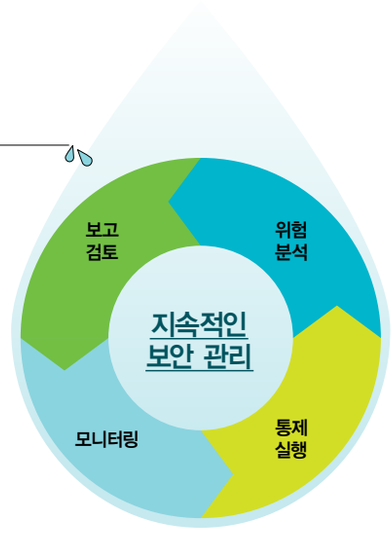


IBM Security Framework은 고객의 비즈니스 요건에 따라 최적화된 보안 솔루션의 구현을 위해 고안되었습니다

지속적인 보안 관리를 위해 전담 조직 구성, 보안 계획 및 절차 수립, 그리고 적절한 솔루션 도입이 요구되며, IBM은 보안 프레임워크를 기반으로 구체적인 방안을 제공합니다.

IBM Security Framework

거버넌스 /리스크관리 /컴플라이언스	사람과 아이덴터티	정보/데이터	어플리케이션 /프로세스	네트워크 /서버,단말	물리적 인프라
보안전략설계	계정관리	데이터 암호화 관리	어플리케이션 개발 보안	서버 보안	영상 감시 및 분석
모의해킹과 취약점 평가	접근통제	데이터 접근 통제	어플리케이션 취약점 발견	네트워크 보안	통합 관제
보안 컴플라이언스 평가	감사 및 보고	데이터 유출 방지	어플리케이션 접근 통제	단말 보안	출입 통제
보안 사고 대응					



Why IBM ? **IBM Security Framework**

보안 솔루션 도입, 왜 IBM과 함께 해야 할까요?

1 IBM의 검증된 방법론과 자산을 최대한 활용합니다. 검증된 방법론과 국내 및 글로벌에 축적된 자산을 최대한 활용하는 누구도 따라오지 못하는 IBM 만의 강력한 DB Pool!

2 국내 최고수준의 보안관리 체계와 IBM의 보안관리체계를 벤치마킹 합니다. 고객의 정보를 다루는 IBM 글로벌의 베스트 프랙티스를 참조하여 정보보안 관리 수준을 진단합니다!

3 IBM의 복합적인 IT 및 보안 전문역량과 보안 진단 전문 업체의 전문역량을 바탕으로 현실성 있고 검증된 방법으로 진단과 조치방안을 도출합니다!

IBM Security Service Client Reference

안전한 비즈니스를 통해 안정적인 기업이 되기 위한 방법,
다양한 산업별 많은 고객들이 IBM을 선택했던 이유,
영역별 고객 사례를 통해 알아보십시오.

거버넌스, 위험관리와 컴플라이언스

I사

"자사에 꼭맞는 정보 보안 거버넌스 모델을 기초로 효과적이고 지속적인 보안 전략 수립"

"정보 보안 컨설팅을 통해 프로세스 차원과 솔루션 차원의 보완 방안을 구체화 할 수 있었다. 그리고 한국 IBM은 도출된 이슈 사항을 기술의 성속도와 긴급성에 따라 우선순위를 정하여 제시해 주는 등 우리 회사만의 정보보안 거버넌스 모델 완성도를 높이는 데 큰 도움을 주었다"

Business Challenge

최신 보안 솔루션과 장비들을 구비해도 어딘가 비어있는 듯한 느낌 남아

I사는 금융 비즈니스를 하는 기업이다. 금융업의 특성상 I사는 다른 업종의 기업들보다 보안에 각별한 신경을 써왔다. 방화벽, 침입 탐지, 백신, 취약점 점검, DRM, VPN, 데이터 암호화, 보안 관제, 지문 인증 등등 엔터프라이즈 IT 인프라 곳곳에 최신 보안 솔루션들을 배치해 놓고 만에 하나 있을 수 있는 보안 사고에 대비해 왔다.

사용 중인 솔루션 포트폴리오만 놓고 보면 I사는 보안 걱정을 할 필요가 없다. 하지만 현실은 달랐다. 필요한 것을 다 구비했지만 어딘가 비는 구석이 있었다. 금융 비즈니스 상당 부분이 IT 기술 없이는 운영되지 않는 시대가 되다보니 개인 정보 보안 강화, 내부 회계 관리 제도 등 각종 법정 규제가 늘어나고 있다. 또한 개인 정보 절취나 카드 복제, 메모리 해킹 등 전자 금융 관련 범죄 수법은 날이 갈수록 정교해 지고 있다. 이런 현실을 받아들이기에 I사의 보안 인프라는 너무 경직되어 있었던 것이다.

I사 보안 담당자의 생각도 크게 다르지 않았다. 투자를 지속해 왔음에도 새로운 요구 사항이 나오게 되면 이미 갖추어 놓은 것만으로는 뭔가 부족해 또다른 솔루션을 찾게 되는 악순환이 반복되고 있다는 사실을 알고 있었다. 하지만 이 고리를 끊을 마땅한 방법을 찾지 못했다. 그러던 차에 I사는 한국IBM으로부터 흥미로운 제안을 하나 받게 된다. '정보 보안 거버넌스' 란 다소 생소하지만 가려운 곳을 긁어 주는 듯한 내용을 접하게 된 것이다.

Solution

정보 보호 거버넌스를 목표로 전사적 보안 인프라 재정비

I사의 보안 담당자는 한국IBM의 제안서를 글자 하나 허투루 보지 않고 진지하게 읽어 내려갔다. 무엇이 그를 집중하게 만들었을까? I사의 보안 담당자는 한국IBM이 사전 조사를 바탕으로 평가한 정보 보안 수준 리포트 내용에 놀라게 된다.

한국IBM은 정보보안 거버넌스 모델 하에 I사를 위한 참조 모델을 만들었다. 이 모델은 보안 목적, 보안 관리 프로세스, 보안 관리 대상을 주요 축으로 하고 있다. 여기까지는 흔히 접할 수 있는 내용이다. I사 보안 담당자의 눈길을 사로 잡은 것은 정보보안 거버넌스 모델을 가지고 한국IBM이 평가한 I사의 기술적, 절차적 보안 수준이었다. 한국IBM은 인증, 접근 통제, 침해 방지, 내부 정보 유출 방지, 모니터링을 평가 기준으로 하여 I사의 PC, 네트워크, 서버, 애플리케이션, 데이터베이스의 보안 수준을 점검했다. 그 결과는 I사의 보안 담당자의 눈을 의심케 했다. 엔터프라이즈 보안과 관련해 I사가 하나 둘 늘려온 보안 솔루션들 간 편차가 너무 심하게 나타난 것이다.

전체 평가 항목 중 가장 낮은 점수를 받은 것들은 개인 방화벽, 이메일 통제, 계정 관리, 네트워크 접근 통제, 데이터베이스 로그 분석 등이었다. 총 다섯 레벨로 평가가 이루어졌는데 최고 등급인 레벨 5는 하나도 없었다. 보안 패치, 백신, 취약점 점검, VPN, 유해 트래픽 통제, 백업·복구, 스팸 메일 차단, 메일 암호, PKI 정도가 레벨 4로 점수가 매겨졌을 뿐이었다.

한국IBM은 I사의 보안 허점을 메우기 위한 방안도 제시하였다. 크게 인증, 접근 통제, 침해 방지, 내부 정보 유출 방지, 모니터링 등이 시급한 개선 현안으로 분류되었다. I사는 한국IBM의 제언을 받아들여 단기, 중기, 장기 일정 계획을 세워 기존 솔루션의 확대 구축, 신규 솔루션 도입, 관리적 영역 보완 등의 후속 작업을 추진하고 있다.

Benefit

보안 목적, 관리 대상, 프로세스를 아우르는 정보 보안 거버넌스 모델 확립

I사는 컨설팅을 통해 평소 가지고 있던 보안에 대한 인식을 전환하게 되었다. 풀어 설명하자면 "장비와 솔루션이면 다된다" 식이 아니라 정보 보안은 IT의 일부가 아니라 비즈니스와 긴밀히 연계되어 있다는 인식의 전환을 이끌어 냈다. 이는 곧 조직 차원의 변화로 이어지게 되었다. I사는 정보 보안을 특정 부서 관계자만의 일이 아니라 조직 구성원 모두가 일상적 업무에서 수행해야 하는 것으로 바라보게 되었다. 즉, "누군가 책임지겠지" 또는 "누군가 관리하겠지" 라는 방관자적 자세가 아니라 모두가 함께 신경 쓰고 조심해야 하는 것으로 받아들이게 된 것이다.

한편 이번 컨설팅을 통해 I사는 정보 보안 기술 로드맵을 완성하게 되었다. I사는 인식 전환을 시작으로 자사의 보안 투자를 필요할 때마다 하는 식이 아니라 '정보 보안 거버넌스' 란 큰 전략 하에 보완이 시급한 과제 등을 명확히 하여 단기, 중기, 장기 관점에서의 투자 및 운영하는 방향을 확고히 정했다.

- **Industry** : 금융
- **Business Challenge** : 보안 솔루션을 잘 갖추었음에도 각종 규제 및 신종 공격 기술 등장에 대응하는 데 한계
- **Solution** : 컨설팅을 통해 기존 환경의 문제점을 진단하고 이에 대한 개선 방향 도출
- **Benefit** : 보안에 대한 전사적 인식 전환과 자사에 딱맞는 정보 보안 거버넌스 모델 찾아
- **IBM Service** : 정보 보안 거버넌스 컨설팅

거버넌스, 위험관리와 컴플라이언스

J사

"글로벌 경영을 원활히 지원하는 보안 전략과 체계 마련"

"정보 보안 거버넌스는 하나의 솔루션으로 구현할 수 있는 성격의 것이 아니다. 그리고 선진 모델이 있다 해도 이게 모든 기업에 들어맞는 것도 아니다. 정보 보안 거버넌스는 기술이 아니라 조직 문화 차원의 과제이기 때문이다. 우리 회사의 경우는 한국IBM의 컨설팅 서비스를 통해 가장 잘 맞는 모델을 찾을 수 있었다"

Business Challenge

글로벌 비즈니스 네트워크를 안전하게 운영하기 위한 노력

J사는 제조 기업으로 국내는 물론 해외에도 비즈니스 거점을 운영하고 있다. 이처럼 비즈니스 네트워크가 방대하다 보니 본사와 주요 거점 간 의사소통이 빈번하고, 자료 공유 및 교환 역시 광범위한 조직 상에서 이루어진다.

이런 유형의 조직은 근본적으로 잠재적 위험을 어느 정도 안고 가게 된다. 본사와 지사를 전용선으로 연결해 폐쇄적으로 사내 망을 운영할 수 있는 것도 아니다 보니 인터넷 상에 존재하는 각종 보안 위협으로부터 100% 안전하다 자신할 수 없기 때문이다. J사가 글로벌 비즈니스 네트워크 전체를 대상으로 정보 보호 거버넌스 모델 수립 프로젝트를 추진하게 된 이유다.

J사는 정보 보호 거버넌스 체계 정립에 가장 적합한 파트너로 한국IBM을 지목했다. 그 이유는 간단했다. 객관적인 시각에서 현황을 파악하고 개선안을 도출할 수 있을 것이란 믿음에서였다. J사는 보안 전문 업체들의 경우 보통 자사가 보유한 기술의 범위를 넘어서는 시야를 갖지 못한다고 판단했다. 이런 생각을 가질 수 있었던 것은 J사가 엔터프라이즈에서의 보안이란 결국 PC, 서버, 네트워크, 관리, 조직 더 나아가 비즈니스까지 고려해야 한다는 점을 간파하고 있었기 때문이다.

한국IBM에 대한 J사의 평가는 실제 프로젝트에 들어가면서 틀리지 않았음이 입증된다. 한국IBM은 정보보호 거버넌스 구성 요소로 전략, 거버넌스 프레임워크, 변화 관리, 정보 보호 자문, 위험 관리, 규제 준수 프로그램 등을 제시했다. 이 요소들을 가지고 한국IBM은 J사가 참조할 수 있는 선진 사례 분석에 들어간다. 당시 정밀 분석 대상으로 선정된 사례는 IBM과 ISACA였다.

Solution

정보 보호 거버넌스 진단 및 이행 계획 수립

J사와 한국IBM은 선진 사례를 검토하는 한편 현황 분석도 추진했다. 이 작업 역시 한국IBM이 제시한 여섯 가지 정보보호 거버넌스 구성 요소를 기준으로 진행되었다. 한국IBM은 가능한 모든 정보를 모았다. 한국IBM은 J사의 건물, 공장 등 시설 현황 자료부터 시작해 정책, 목표, 계획서, 절차서, 규격, 지침서, 시방서, 도면, 계약서, 회의록, 심사 보고서, 프로그램 모니터링 및 측정 결과와 같은 기록물들을 빠짐 없이 챙겼다. 이와 함께 J사의 주요 보안 실무자들을 대상으로 심층 인터뷰를 하는 한편 웹 애플리케이션에 대한 모의 해킹 등 기술적 검증도 시행하였다.

다방면에 걸쳐 정밀하게 현황 진단을 해본 결과 굵직한 이슈들이 걸러졌다. 주요 이슈들을 소개하자면 먼저 전략 부문에서는 규정과 지침이 미흡하고, 모니터링 체계 역시 잘 갖추어져 있지 않다는 등의 문제가 도출되었다. 다음으로 변화 관리 측면에서는 각종 보안 규제를 위반했을 때 이에 대한 상벌 규정이 모호하고 그 실효성이 낮는 점이 지적되었다. 위험 및 자원 관리 요소에서는 프로세스가 없다는 점이 이슈였다. 성과 관리 부문에서는 상시 실적 분석 및 대안 마련이 이루어지지 않고 있다는 것이 문제였다.

진단 과정을 마친 J사는 변화 방향을 잡고 6개월 이내 해결해야 하는 단기 과제, 1년 내 추진할 중기 과제, 향후 이뤄가야 할 장기 과제 등 추진 로드맵을 세워 정보 보호 거버넌스 체계로의 첫 걸음을 내디뎠다.

Benefit

글로벌 비즈니스 현장에 공통 적용할 수 있는 거버넌스 방안 찾아

J사의 보안 관계자는 한국IBM의 도움으로 안전한 글로벌 비즈니스 지원이란 숙원 사업을 성공적으로 마칠 수 있었다. J사는 한국IBM과 함께 정보 보호 관리 체계 모델을 완성했다. 글로벌 비즈니스에 공통적으로 적용하기 위한 정보 보호 거버넌스 모델을 마련한 것이다. 이를 지침삼아 J사는 정보 보호 규정 및 지침, 변화 관리 프로그램, 정보 보호 프로세스, 글로벌 정보 보호 협력 네트워크, 보안 진단 기준 및 프로세스, 성과 관리 프로그램 등을 일관성 있게 개선해 나아갔다.

J사는 자사의 조건에 부합하는 정보 보호 거버넌스 모델을 찾은 덕에 나날이 늘어가는 법, 규제 관련 컴플라이언스에 보다 효과적으로 대응이 가능해 질 것으로 예상하고 있다. 해외 시장까지 감안해야 하는 J사에게 있어 하나의 기준 모델을 가지고 일사분란하게 움직일 수 있다는 것이 같은 운영상, 비용상 이점은 크다. 이 외에도 전세계적으로 비즈니스를 펼쳐가는 J사의 각종 영업 및 산업 기밀 역시 보다 체계적으로 보호할 수 있게 된 점도 정보 보호 거버넌스 모델 확립의 효과로 빼놓을 수 없다.

- **Industry** : 제조
- **Business Challenge** : 글로벌 비즈니스 네트워크에 공통적으로 적용할 기준 모델 필요
- **Solution** : 기존 환경에 대한 철저한 분석과 진단을 바탕으로 개선 과제 도출
- **Benefit** : 컴플라이언스 대응 및 영업, 산업 관련 정보에 대한 보호 수준 높여
- **IBM Service** : 정보 보안 거버넌스 컨설팅

사람과 아이덴티티

D은행

"주요 IT 자산 접근에 대한 내부 통제 강화로 인프라 전반의 보안성 향상"

"여러 솔루션을 검토한 끝에 메인프레임부터 각종 엔터프라이즈용 소프트웨어 등 IT 환경 전반에 대한 이해도가 높고, 복합적인 환경 속에서 컨설팅과 커스터마이징을 수행할 수 있는 경험과 역량을 갖춘 IBM의 계정관리 솔루션 및 서비스를 선택했다"

Business Challenge

주요 IT 자산 접근에 대한 사용자 통제 이슈

D은행은 여타 마찬가지로 수많은 업무 시스템들을 운영하고 있다. D은행의 비즈니스 심장부라 할 수 있는 주요 IT 자산에 대한 접근은 전통적으로 구분되어졌다. 일반 사용자들이 엔터프라이즈 포탈 등을 통해 SSO(Single Sign On)으로 모든 서비스에 접근하는 것과 달리 미션크리티컬한 비즈니스 자산인 메인프레임, 서버, 데이터베이스 등 기간계 시스템에는 담당자들이 각각의 계정과 권한을 가지고 로그인을 해왔다.

이런 방식의 단점은 사람에 의한 보안 사고 발생 위험을 잠재적으로 내포하고 있다는 것이다. 또한 주요 자산에 대한 아이디와 패스워드가 자동화 된 체계 속에서 중앙집중적으로 관리되지 못할 경우 IT 인프라에 장애나 침해 사고 발생시 이에 대한 빠르고 정확한 원인 추적도 어렵다. 이같은 문제들을 근본적으로 풀어낼 해결책을 모색하던 D은행은 '내부 사용자 통제 강화' 라는 카드를 빼들게 된다. 그리고 이를 기술적으로 구현하기 위해 통합 계정 권한 관리 솔루션 도입 검토에 들어간다.

Solution

서버, 네트워크, 데이터베이스 등 주요 IT 인프라에 대한 보안 통제 인프라 확립

D은행이 물망에 올린 IAM 솔루션들은 대부분 세계적으로 이름을 날리는 제품들이었다. D은행이 고심 끝에 고른 제품은 IBM Tivoli Identity Manger였다.

D은행은 IAM(Identity & Access Management)은 그 특성상 다양한 데이터베이스, 시스템, 애플리케이션 등과 세밀한 연동이 필요하다고 보았다. 이같은 기준으로 평가한 결과 IBM의 솔루션이 최선으로 나타났다.

D은행은 크게 계정 관리, 권한 관리, 통합 관리, 복합 인증이라는 네 부문으로 수행 과제를 구분해 작업에 들어갔다. 먼저 계정 관리의 경우 보안 관리자, 시스템 관리자, 개발자 등이 자신들이 관리 또는 이용하는 시스템에 접근할 때 이용했던 계정들을 워크플로우 기반으로 체계화 하는 작업이 진행되었다. 권한이나 통합 관리 부문 역시 핵심은 워크플로우 상에서 접근, 통제, 추적 등의 활동이 이루어지도록 한다는 것이었다. 최고 관리자 권한을 가진 사용자가 시스템 단위로 계정을 생성하고 만들어진 아이디와 패스워드들은 관리 대장 등을 통해 정리되는 것이 일반적인 방식이라면, D은행은 '요청·사용 → 승인 → 배포·적용 → 검토·조정' 등과 같이 사전에 약속된 절차에 따라 계정 관리가 가능하도록 워크플로우를 자동화 하였다. 그리고 이들 흐름이 원활이 이어지는 가운데. 보다 보안성을 높이기 위해 서버 PKI 인증을 구축하였다.

D은행은 일원화 된 통합 계정 권한 관리 체계를 수립한 후 사용자 로그 분석 기능 개선, 추가 도입 서버에 대한 계정 매핑 및 관리자들의 역할에 따른 프로비져닝 정책 정의 및 구현, 정책 기반 권한 관리 적용 대상 서버 확대, 메인프레임 RACF 권한 관리 기능 추가, IT 부서 담당자를 대상으로 한 지문 인증 확대 구축 등의 후속 작업을 수행해 나가고 있다.

Benefit

미션크리티컬한 시스템 접근에 대한 투명성 확보

IBM의 Tivoli Identity Manger 도입 후 D은행의 핵심 자산에 대한 접근 편의성은 개선되고 보안과 통제 수위는 높아졌다. IT 부서 실무 관계자들은 피부에 와닿고 있다. 계정 신청부터 인증까지 원스탑으로 처리되기 때문에 관리자들은 자산에 대한 접근 편의성이 개선되었다고 느끼고 있다. 그리고 기본적인 계정 관리뿐 아니라 사용자 접근에 대한 실시간 탐지 및 이상 징후가 있는 접근에 대한 경보, 사후 감사 등 과거에는 여러 사람의 손이 가던 일들이 단일 콘솔 상에서 처리되면서 통제 수위는 더욱 높아졌다.

한편 시스템 기준이 아니라 사람과 역할에 따른 계정 및 권한 관리가 가능해진 점도 IBM의 Tivoli Identity Manger 도입의 주요 효과다. Tivoli Identity Manger는 조직별 권한 위임 기능을 지원한다. 이에 따라 계정 관리자는 협력사별, 조직별, 역할별로 관리자를 따로 생성하고 각 관리자는 자신이 속한 부서 혹은 자신에게 권한이 부여된 부서 자원을 관리할 수 있게 된다.
D은행은 이 기능이 외주 개발 프로젝트 등과 같이 협력사 직원들이 파견되었을 때 이들을 관리하는 데 유용하게 쓰일 것으로 기대하고 있다. 금융권은 매년 신규로 개발되는 업무 시스템들의 수가 많은 업종 중 하나다. D은행은 외주 개발사 담당자들을 위해 제공되는 개발이나 테스트 머신 등과 같이 특별히 신경쓰지 못하던 시스템들까지도 Tivoli Identity Manger를 통해 계정 관리가 가능해질 것으로 내다보고 있다.

- **Industry** : 금융
- **Business Challenge** : 비즈니스 심장부인 주요 IT 자산에 대한 계정 및 권한 관리의 복잡도 증가
- **Solution** : 계정 및 권한 관리를 중앙집중화 하고, 일련의 워크플로우를 자동화
- **Benefit** : IT 자산으로의 접근 통제 수위는 높이고, 사용자들의 접근 편의성은 나아져
- **IBM Service** : IBM 계정관리 보안진단 및 구축 서비스

사람과 아이덴티티

E금융사

"인사 정보와 계정 관리 통합으로 IAM 거버넌스 수준 높여"

Business Challenge

조직 변화에 유연하지 못한 계정 관리 체계

21세로 접어들면서 금융기관은 물론이고 다른 분야 기업들 모두 각종 업무 시스템의 가짓수와 규모가 빠르게 늘고 있음을 자각하고 있다. IT가 비즈니스를 움직이는 경영의 엔진이 되어가고 있다는 사실과 함께 기업들은 한 가지 패턴을 발견하게 된다. IT 환경이 거대해지는 가운데 사용자 계정 및 접근 권한 생성·수정·삭제 관련 비용과 그에 대한 관리 복잡도가 늘어가고 있음을 알아챈 것이다.

E금융사의 경우도 대외 경쟁이 치열해지면서 신상품 개발과 출시, 블루오션 개척 등의 이유로 조직 유동성이 높아지면서 계정 관리의 비효율성과 높은 비용 이슈에 직면하게 된다. 즉, SSO(Single Sign On)의 주요 기능인 계정 관리 시스템만 가지고는 조직의 변동성을 쫓아가는 데 어려움이 컸던 것이다.

E금융사의 관리자는 부서 이동이나 직무 변경 등이 발생하면 해당 사용자의 접근 권한 조정 등을 일일이 수작업으로 처리했다. 그러다 보니 사용자는 새로운 계정 권한을 재부여받기까지 대기해야 하는 불편함을 감수해야 했고, 이는 곧 업무 연속성에 영향을 끼치는 요인이 되었다. 이는 비단 사용자와 관리자만의 문제가 아니다. 전사 관점에서 보면 인적 자원 운영과 관련해 생각치 못한 비용 손실이 발생하는 것이라 볼 수 있다.

Solution

계정 관리 시스템과 인사 시스템 간 연계

E금융사는 계정 관리 체계가 기업의 조직 변동에 관계없이 그 기능성을 유지하기 위해서는 한 가지 답이 유일하다고 봤다. 바로 계정 관리 시스템에 인사 정보를 연계하는 것이다. E금융사는 어떤 기술을 가지고 문제 해결에 나설 것인지 살핀 끝에 국내 유수 금융사들의 IAM(Identity & Access Management) 사례를 통해 기능성이 검증된 IBM의 Tivoli Identity Manger를 가지고 본 프로젝트를 시작한다.

E금융사는 Tivoli Identity Manger의 사용자 정보 동기화 모듈(TDI)을 사용해 계정 관리 시스템의 사용자 정보와 인사 시스템에 담긴 사용자 프로파일 간 동기화를 구현하였다. 동기화 흐름을 설명하자면 인사 등록이나 부서 이동·직무 변동 등이 발생했을 경우 곧바로 계정 관리 정책에 따라 계정의 생성, 변경, 삭제 프로세스가 자동으로 진행된다. 그 결과 관리자는 수작업에 대한 부담을 덜고 ID와 패스워드 정책, 승인 워크플로우, 감사 보고서, 프로비져닝 정책 등의 관리에만 신경 쓰면 되게 되었다.

Benefit

부서 이동이나 직무 변경 시에도 즉각적인 업무 연속성 보장

E금융사의 일반 사용자와 관리자 모두 인사정보와 계정 관리 시스템 연결의 수혜자다. 먼저 사용자는 인사 변동에 따른 계정 권한을 적시에 받지 못해 며칠간 각종 사내 시스템이나 서비스에 접근하지 못하는 일이 없어졌다. 예를 들어 부서 이동이나 직무 변동이 있을 경우 Tivoli Identity Manger는 프로비져닝 정책에 따라 기존 계정을 자동으로 삭제하고, 신규 계정을 자동 생성한다. 이 계정은 승인 과정을 거쳐 바로 사용이 가능해진다.

관리자의 경우 과거 일일이 수작업으로 처리하던 인사 변동 관련 계정 관리 작업이 자동화 되어 일이 크게 줄었다. 예를 들어 새로 입사를 할 경우 Tivoli Identity Manger 계정이 자동 생성이 된다. 관리자는 자신이 만들어 둔 워크플로우에 따라 계정 신청과 승인 절차만 처리하면 된다.

이 밖에도 유휴 ID 관리도 자동화 되었다. 보안 관리자라면 누구나 유휴 ID가 엄청난 보안 위협이 된다는 사실을 안다. 유휴 ID는 관리자의 실수로 퇴사자의 ID가 삭제되지 않았을 때 생길 수 있다. 이 외에도 인사 부서에서 IT 부서로 인사 정보 변동을 알려주지 않았을 때도 삭제되지 않고 남아 있을 수 있다.

이런 유휴 ID를 누군가 악의적인 목적으로 사용해 사내 서버나 데이터베이스, 애플리케이션에 접근한다면, 그 결과는 불을 보듯 뻔한 것이다. 다행히도 E금융사의 관리자는 Tivoli Identity Manger 덕에 유휴 ID로 인한 보안 사고 걱정을 하지 않는다. 퇴사 또는 외주 협력사 직원의 근무 기간 만료 정보를 인사 데이터베이스에서 참조해 자동으로 계정을 삭제해 버린다.

"부서 이동이나 직무 변동 등이 발생했을 때 가장 먼저 이들 정보가 기록되는 인사 시스템에서 바로 정보를 받아 이를 계정 체계에 반영해야만 추가적인 후속 작업을 피할 수 있는데, 이를 자동화 하기 위한 수단으로 IBM의 계정관리 솔루션 및 서비스가 적격이다"

- **Industry** : 금융
- **Business Challenge** : 인사 변동 정보를 즉시 반영 못함으로 인한 업무 연속성 이슈 발생
- **Solution** : 인사 정보를 계정 관리 시스템에 연계하여 인사 부문까지 포괄하여 IAM 워크플로우 자동화
- **Benefit** : 업무 연속성 보장 및 유휴 ID에 따른 보안 위협 사전 제거
- **IBM Service** : IBM 계정관리 보안진단 및 구축 서비스

데이터와 정보

S사

"민감한 정보로 가득한 BI 환경의 안전 보장, 데이터베이스 보안에서 답 찾아!"

Business Challenge

전사적 BI 확산 그리고 민감한 데이터 소스 보안의 필요성

'빅 데이터' 시대를 맞아 기업은 규모와 업종을 떠나 늘어만 가는 데이터 홍수 속에서 어떻게 가치 있는 정보를 정제해 내고 이를 전략적 의사결정에 반영할 것인가에 큰 관심을 보이고 있다. 이같은 기업들의 관심은 행동으로 이어지고 있고, 몇몇 선도적인 기업들을 통해 전통적인 BI(Business Intelligence)는 외연의 확장을 거듭하고 있다. 선도 기업들이 이뤄낸 성과는 바로 '비즈니스 분석 및 최적화' 이다. 이는 경영진이나 소수 분석가를 위한 정보 분석이 아니라 조직 전반을 아우르는 개념이다. 기술적으로 보자면 BI뿐 아니라 정보 관리, 정보 거버넌스 등까지 포함하는 넓은 의미로 해석된다.

BI 관련 선도 사례 중 IT 서비스 업계의 준거 사이트로 최근 정보 거버넌스에 도전한 S사가 꼽힌다. IT 서비스 기업인 S사는 자사의 BI 시스템 이용자 수가 2천 명에 달하고, 대부분 고객들을 대상으로 IT 관련 프로페셔널 서비스를 제공하는 전문가들이다 보니 이들이 수집하고 분석하는 정보는 대외비로 분류될 정도로 민감하다는 것을 잘 알고 있었다. 이처럼 강력한 보안이 요구되는 BI 환경에 S사는 최근 클라우드 사상을 투영해보는 실험을 단행하였다. 이 과정에서 S사는 접근성과 유연성 높은 BI 환경의 경우 데이터 소스 차원의 보안이 반드시 전제되어야 한다는 사실을 절감하고 정보 거버넌스 관련 프로젝트 추진을 결심한다.

S사는 자사의 요구 사항을 전통적인 보안 방식이 충족시킬 수 있는지를 먼저 살펴보았다. 결론은 기존에 쓰이던 방식과 솔루션은 정보 거버넌스의 핵심 요소 중 하나인 데이터베이스 보안에 취약하다는 것이었다. 예를 들자면 데이터베이스 암호화는 권한을 가진 내부 사용자로부터의 보호 장치 마련이 마땅치 않고, IDS나 IPS는 데이터베이스 프로토콜 및 활동 패턴을 인식해 방어하는 기능성이 부족하다. 기존 보안 도구 및 방식의 한계를 확인한 S사는 데이터 거버넌스가 고려된 보다 포괄적인 도구를 알아보게 된다.

Solution

데이터 거버넌스 관점에서 접근한 BI 보안

H사는 향후 자사의 BI 전략 및 확산 계획 등을 감안해 여러 솔루션들을 살폈고, 최종 결선 무대에 IBM Infosphere Guardium과 C사의 솔루션을 올렸다. IT 서비스 기업 입장에서 살피다 보니 상대적으로 더욱 세밀한 부분까지 기술 비교가 이루어졌다. S사는 정보 거버넌스의 출발점은 데이터 그 자체라 보고 데이터 침해 방지, 데이터 무결성 보장, 컴플라이언스 지원 및 자동화 기능 등을 꼼꼼히 따져 보았다. 대비되는 것들부터 다른 점까지 빠짐없이 비교해본 S사가 손을 들어준 것은 IBM Infosphere Guardium이었다.

S사는 다양한 종류의 데이터베이스에 담긴 데이터들에 대한 보안을 라이프사이클 관점에서 정의하고 각 단계별로 요구되는 관리적 요소들을 IBM Infosphere Guardium의 기능으로 구현했다. 간단히 소개하자면 S사는 모니터링, 감사 및 보고, 취약성 평가, 지속적인 정책 갱신 등으로 라이프사이클의 주요 단계를 구분했다.

"향후 계열사를 대상으로 BI 관련 데이터베이스 보안 확산을 고려 중이다. IBM Infosphere Guardium은 애플리케이션과 데이터베이스 종류에 종속적이지 않고, Multiple S-Tap과 Collector 기능을 사용면 확장된 구조의 분산 환경에도 사용이 가능해 적용이 어렵지 않을 것으로 기대하고 있다"

라이프사이클 중 구현의 우선순위가 높았던 부문은 모니터링이었다. S사의 BI 시스템의 사용자 수가 소수 분석가나 임원에 그치는 것이 아니라 전사 차원이다 보니 사용자의 활동에 대한 모니터링에 무게감을 둔 것이다. S사는 일반 사용자뿐 아니라 계정 권한 등급이 높은 사용자까지도 철저히 모니터링 하고 정책에 위배되는 접근에 대해서는 자동으로 차단이 이루어지게 하였다.

Benefit

BI를 넘어 비즈니스 분석 및 최적화 단계로 가는 교두보 마련

S사는 IBM Infosphere Guardium을 통해 정보 거버넌스의 핵심 중 하나인 데이터베이스 보안이 뿌리내리게 하였다. 향후 자사 BI가 '비즈니스 분석 및 최적화' 라는 보다 크고 진보된 틀을 갖추어 갈 것으로 기대하고 있다.

물론 아직은 첫발을 내디딘 상태이긴 하지만 정보 거버넌스가 갖는 이점은 이미 S사 관계자들의 눈에 들어오고 있다. 예를 하나 들자면 예전에는 사용자들이 데이터 소스에 접근해 어떤 일들을 하는지 매일같이 투명하게 알 방법이 없었다. 그렇다고 알고 싶을 때마다 매번 데이터베이스들의 접속 로그를 뒤져볼 수도 없는 일이었다. 그나마 정기적으로 하는 감사의 경우도 데이터베이스 성능 이슈가 발생해 마음 놓고 하기 어려웠다.

그러던 것이 이제는 BI 시스템이 참조하는 모든 데이터 소스 상에서 이루어지는 일들을 중앙에서 한눈에 파악할 수 있게 되었다. 로컬에서의 접근에 대한 보안 관리가 실시간으로 이루어지기에 가능한 일이다. 이처럼 실시간으로 데이터베이스 상에서 이루어지는 활동들을 바라보지만 성능 이슈는 없다. IBM Infosphere Guardium는 실시간 보안 및 모니터링을 수행해도 최소한의 영향만을 성능에 끼친다. S사는 이를 대략 5% 이하인 것으로 파악하고 있다.

- **Industry** : 서비스
- **Business Challenge** : BI를 전사 차원에서 활용하는 조직의 특성상 민감한 정보가 담긴 데이터 소스에 대한 보안 필요
- **Solution** : 라이프사이클 기반의 데이터베이스 보안 체계를 BI 환경에 이식
- **Benefit** : 데이터 암호화뿐 아니라 철저한 모니터링과 접근 차단으로 BI 시스템에 대한 보안 거버넌스 기초 확립
- **IBM Service** : IBM 데이터 보안진단 및 구축 서비스

애플리케이션과 프로세스

A사

"수작업에 의존하던 웹 서비스 보안, 자동화된 프로세스와 툴로 안정성 레벨업!"

"기존에는 주로 웹 관련 취약성 점검에 초점이 맞추어졌다면, IBM의 애플리케이션 취약성 점검 솔루션및 서비스 도입후에는 특정 웹 애플리케이션 수준의 보안 점검이 아니라 서비스 관점에서 네트워크, 웹 애플리케이션, 시스템까지 'End-to-End' 를 포괄하게 되었다"

Business Challenge

웹 서비스 보안에 대한 사회적 경각심 높아져

A사는 온라인상에서 게임 서비스를 제공하는 기업이다. A사와 같이 대고객 서비스의 접점이 웹인 기업들의 끊임없는 고민 중 하나는 바로 '보안' 이다. 개인 정보 유출이나 기업 정보 유출 사고가 증가하면서 정보 보안에 대한 기업들의 사회적 책임과 의무의 중요성이 커지고 있다. 특히 온라인 서비스 기업은 모든 비즈니스 활동이 웹에서 일어나기 때문에 책임과 의무의 무게감이 더욱 크게 다가온다.

A사의 경우 지속적으로 신규 서비스를 자사의 게임 포탈을 통해 고객에게 제공해 오면서 방문자 수 증가 못지않게 악의적인 해킹 시도 역시 함께 늘어남을 경험하였다. 이에 내부적으로 보안 사전 점검 프로세스를 확립하여 모의 해킹 시도 및 점검 등을 일상적인 관리 업무 차원에서 해왔다. 이처럼 나름의 대비책을 가지고 늘어가는 웹 애플리케이션 대상 공격에 대비해온 A사는 언제부터인가 자사의 프로세스와 방법론이 가지고 있는 비효율성에 눈을 뜨게 된다.

대부분의 작업이 수작업으로 이루어지다 보니 전적으로 관리자의 능력에만 의지하게 되고, 자동화된 점검 도구와 리포트 체계가 없다 보니 취약성 점검 활동 자체가 연속성을 띈다기보다 일회성 차원에 그치는 경우가 많았던 것이다. 이에 A사는 선진 프로세스와 도구 도입에 나서게 된다.

Solution

수작업으로 이루어지던 취약성 점검 AppScan으로 자동화

A사는 국내외 애플리케이션 진단 관리 관련 서비스 및 도구들에 대한 조사를 수행한 후 IBM의 AppScan 도입을 결정하였다. IBM의 AppScan은 애플리케이션 속까지 들여다 보는 깊이가 상당하다는 점 그리고 진단 범위가 모의 해킹 형태 정도로 협소한 다른 업체와 달리 라이프사이클 관점에서 점검, 조치, 이행 등을 수행할 수 있다는 점을 높이 평가받았다.

A사는 이번 프로젝트를 단순히 새로운 보안 툴을 하나 더 들여오는 것이 아니라 조직과 체계 정비 관점에서 접근했다. 실제로 IBM의 검증된 애플리케이션 진단 관리 방법론에 기초해 기존 수작업에 의존하던 업무 프로세스를 개선하고, 관리자들이 글로벌 시장에서 검증된 도구인 AppScan을 통해 일련의 업무를 수행할 수 있도록 하였다.

그 결과 A사의 웹 애플리케이션 보안 점검 업무는 AppScan 도입 이전과 이후 큰 차이를 보이게 되었다. 기존에는 모의 해킹 및 일일 점검 정도를 하고 보고서를 쓰는 정도의 단순한 일상의 반복이 있었다. 그러던 것이 AppScan 도입 후부터는 일련의 사이클이 생겼다. 분석, 정보 수집, 애플리케이션 테스트 및 결과 보고, 발견된 문제점에 대한 조치 이생 및 후속 계획 수립이라는 라이프사이클상에서 관리 활동이 지속적으로 실행되게 된 것이다.

Benefit

보안 취약성 점검 효율과 웹 서비스 보안 안정성 모두 높여

A사는 IBM의 도움을 통해 체계화 되고 자동화 된 웹 애플리케이션의 인프라 취약점 및 구성 오류 점검의 큰 틀을 완성할 수 있었다. 이 틀은 실제 A사의 보안 점검 활동을 진두지휘하는 일선 관리자들로부터 큰 호응을 이끌어 내고 있다. 보안 관련 업무가 훨씬 간소화되고, 정교해졌음을 실무자들이 체감하고 있는 것이다.

예를 몇 가지 들자면 첫 번째로 수작업이 없어졌다. 모의 해킹, 일상적인 보안 점검 등을 위해 스크립트를 짜거나, 사전에 마련된 점검 일지에 따라 눈으로 확인하고 관련 리포트를 생성하던 일이 모두 도구 차원에서 자동화 되었다. 그 결과 일상적인 보안 점검에 소요되던 시간이 하루 8시간에서 3시간 이내로 줄었다.

두 번째 변화는 신규 서비스 취약성 점검 시간이 7일에서 1일로 약 80%가량 단축된 것이다. 기존에는 웹 취약성 점검 후 서비스를 올리기 전에 취약성 결과 정리, 개발팀에 문제 해결 요청, 사후 검증 등 서비스를 올리기까지 대략 일주일 정도가 소요되었는데, 이게 하루 이내에 처리가 가능해 졌다. 이는 곧 A사가 고객에게 서비스를 제공하는 민첩성 증대로도 그 효과가 이어졌다.

한편, 웹 서비스 전반의 보안 수준 역시 과거와 차원이 달라지는 것을 A사 관계자들은 체감하고 있다. 기존에는 주로 사내 관리자의 경험에 전적으로 의존하는 형태였는데, AppScan 도입 후부터는 최신 해킹 패턴을 기준으로 대내외 서비스를 항시 점검할 수 있는 체제가 되었기 때문이다.

- **Industry** : 엔터테인먼트
- **Business Challenge** : 웹 애플리케이션 관련 보안 위협 증가
- **Solution** : 내부적으로 수작업으로 수행하던 사전 보안 점검 활동을 검증된 방법론과 자동화 도구를 통해 개선
- **Benefit** : 모의 해킹 및 취약성 분석 등의 관리 업무 자동화, 신규 서비스 퍼블리싱에 필요한 보안 점검 시간 80% 단축
- **IBM Service** : 애플리케이션 진단 관리 서비스, 보안 진단 툴 'AppScan'

애플리케이션과 프로세스

B사

"애플리케이션 개발 단계부터 배포까지 철저한 보안 취약성 점검"

"새로운 웹 애플리케이션 진단 및 인증 프로세스는 IBM의 애플리케이션 취약성 점검 솔루션 및 서비스 도입을 통해 자동화 되어, 특별히 전담 인력을 늘리지 않고도 거의 모든 웹 애플리케이션을 배포 전에 살펴볼 수 있는 체제가 어렵지 않게 자리잡히게 되었다"

Business Challenge

외주 개발사의 애플리케이션에 대한 사전 보안 검사의 어려움

B사는 커뮤니케이션 관련 기업이다. 시장의 발전 속도가 빠르고 이에 따라 신규 서비스 출시 역시 비례적으로 늘고 있다. 이런 대내외적인 변화로 인해 B사는 매년 수많은 개발 프로젝트를 외주 개발사를 통해 추진한다. 이들 업체를 통해 개발되는 것은 주로 웹 애플리케이션으로 사내 업무용부터 대고객 서비스를 위한 것까지 그 종류가 다양하다. 이처럼 해마다 쌓여가는 새로운 웹 애플리케이션이 어느 순간부터 B사에 있어 부담으로 다가오기 시작한다. 웹 애플리케이션이 새로운 보안 허점이 되어 관련 보안 사고 역시 증가세를 이어간 것이다.

B사는 가능한 사후 대처가 아니라 사전에 문제를 해결하기 위해 웹 애플리케이션에 대한 사전 취약점 분석을 수행해왔다. 이런 노력에도 불구하고 웹 애플리케이션에 대한 보안 우려는 해가 갈수록 더해갔다. 인력은 한정되어 있지만 새로 개발되는 웹 애플리케이션 수는 늘어만 갔기 때문이다. B사의 경우 보안 진단을 거치는 비율은 30% 수준, 나머지 70% 가까이 별다른 통제나 제재 없이 바로 웹상에서 고객 또는 사내 직원들을 대상으로 서비스 되었다. 즉, 전수 조사에 한계가 있다 보니 외주 개발사가 만들어 가지고 오는 웹 애플리케이션의 상당수가 보안 점검 없이 바로 서비스 되었던 것이다.

Solution

AppScan으로 웹 애플리케이션 진단 프로세스 확립

B사는 웹 애플리케이션에 대한 전수 조사가 모든 문제 해결의 가장 빠른 길이라 생각했다. 어떻게 하면 사내외에서 개발되는 모든 웹 애플리케이션을 사전에 진단할 수 있을까? B사가 찾은 답은 진단 프로세스를 확립하고, 사전 점검을 전문 도구를 통해 자동화 하는 것이었다. 여러 보안 관련 업체와의 협의를 거친 끝에 B사는 한국IBM의 AppScan을 최종 낙점했다.

B사는 파트너로 선정된 한국IBM과 함께 진단 프로세스 확립 작업을 하였다. 양사는 외주 개발사까지 통제 아래 두기 위해서는 여러 이해 관계자가 애플리케이션 개발 프로세스상에서 긴밀히 상호 협력을 해야 한다는 것을 전제로 진단 프로세스를 확립했다.

이를 설명하자면 B사의 정보보호팀은 외주 개발사가 만든 웹 애플리케이션을 대상으로 진단을 수행하고, 이에 대한 결과 리포트를 B사의 운영팀으로 건네준다. 운영팀은 보고서를 토대로 취약점을 확인하고, 이에 대한 수정 요청을 외주 개발사에 한다. 보안 관련 수정을 마친 외주 개발사는 다시 B사 운영팀에 수정된 코드를 전달한다. 그리고 B사 운영팀은 수정된 웹 애플리케이션을 다시 B사 정보보호팀에 인증 심의를 요청한다. B사 정보보호팀은 보안 점검 결과와 수정 내역을 확인한 후 승인을 한다. 이런 과정을 거친 최종 승인 웹 애플리케이션만이 실제 시스템상에 배포된다.

Benefit

웹 애플리케이션 관련 보안 사고 90% 가까이 줄어

B사가 AppScan을 통해 자동화 한 프로세스는 웹 애플리케이션 개발 라이프사이클 전반에 긴밀히 연계되어 있다는 점에서 그 의미와 가치를 찾을 수 있다. 쉽게 말해 ALM(Application Lifecycle Management)과 웹 애플리케이션 진단 및 인증 프로세스가 조우하는 그런 이상적인 체계를 마련한 것이다. 이처럼 개발 단계부터 치밀한 점검이 이루어지게 되면서 30%에 머물던 애플리케이션 보안 진단률이 95%까지 올라갔다. 외주 개발사에 의해 만들어지는 애플리케이션이 정식으로 사용되기 전 단계에서 전수 조사를 하는 수준이 된 것이다.

이처럼 높아진 사전 점검률은 곧 웹 애플리케이션으로 인한 보안 사고가 줄어드는 효과로 이어지고 있다. B사가 내부적으로 집계한 바에 따르면 대략 90%가량이 줄어들었다고 한다. 모든 IT 관련 보안 사고의 근본적 원인은 보안에 대한 고려 없이 개발된 애플리케이션인 경우가 많다. 이는 역으로 생각하면 개발 단계부터 철저히 보안을 고려해 아키텍처를 잡고, 코딩을 하게 되면 보안 이슈를 일으킬 수 있는 문제 상당수를 미연에 잡아낼 수 있다는 것으로도 해석할 수 있다. 개발 단계에서 사전 진단을 수행해, 보안 취약점 발견 및 수정 작업을 한 후 배포하도록 하는 B사의 프로세스 확립이 보안 사고를 90%까지 낮출 수 있었던 이유다.

한편, B사는 개발뿐 아니라 운영 단계에 있는 웹 애플리케이션에 대한 주기적인 점검 또한 상시화 하는 등 진단 프로세스를 더욱 견고히 해 나아갈 계획이다.

- **Industry** : 커뮤니케이션
- **Business Challenge** : 외주 개발사가 만든 웹 애플리케이션 상당수가 보안 검토 없이 배포
- **Solution** : 배포 전인 개발 단계부터 철저히 보안 진단을 수행할 수 있도록 자동화 도구 도입
- **Benefit** : 웹 애플리케이션 관련 보안 사고 90%가량 감소
- **IBM Service** : 애플리케이션 진단 관리 서비스, 보안 진단 툴 'AppScan'

네트워크와 서버, 단말

G대학

"스마트 캠퍼스 시대에 딱 맞는 능동적 네트워크 보안 메커니즘 완성"

Business Challenge

트래픽 폭주와 보안 위협의 공존

대학 정보화 관계자들이 공통적으로 호소하는 애로 사항을 꼽으라면 매 학기마다 되풀이 되는 트래픽 폭주가 떠오른다. 수강 신청 시즌만 되면 되풀이되는 트래픽 폭주, 이를 한바탕 넘기고 난 후 가슴을 쓸어내리는 모습은 대학 정보화 관계자들 사이에서는 낯설지 않다.

여기에 더해 최근 몇 년 사이 학내에 Wi-Fi가 깔리기 시작하고 학생들이 넷북, 태블릿, 스마트폰 등으로 시간과 장소 구분 없이 인터넷과 각종 앱을 이용하면서부터 대학 정보화 관계자들에게 한 가지 고민이 더해졌다. 특정 시기에 집중되었던 트래픽이 이제는 평상시에도 그 증가세를 예의주시해야 하고, 학생들이 이용하는 기기들이 다변화 되면서 바이러스나 웜 등 각종 위험 요소의 유입 경로도 다양해져 네트워크 단의 안정성과 보안성 보장이 현안으로 떠오른 것이다. G대학의 정보화 부서 역시 이러한 과제로부터 자유롭지 못했다.

G대학은 중장기 IT 투자 계획 중 하나로 늘어나는 트래픽을 수용하기 위해 백본망을 10Gbps 급으로 올릴 예정이었지만, 이 계획이 추진될 때까지 트래픽 폭주와 네트워크를 타고 오는 각종 악성 코드와 웜들을 손 놓고 바라만 볼 수 없는 일이었다. 이에 G대학은 현시점에서 네트워크 인프라의 안정성과 보안성을 높이고 향후 10Gbps 환경까지 아우를 방안을 찾아 나서게 되었다.

Solution

IPS 도입으로 효과적인 폭주 제어와 악의적인 코드 및 웜 유입 방지

현재 네트워크 토폴로지 상에서도 제 역할을 해내고 향후 10Gbps 인프라에서도 그 쓰임이 유용한 도구가 무엇일까? G대학 정보화 부서는 주저하지 않고 IBM Security Network Intrusion Prevention System(IPS)에 눈길을 보냈다. 2000년대 중반 보안 관련 프로젝트를 하면서 들여와 사용해 본 경험이 있다 보니 IBM Security Network IPS가 보안뿐 아니라 네트워크의 가용성과 안정성 부문까지 포괄하는 장비란 것을 잘 알고 있었던 것이다. 또한, 향후 10Gbps 백본망 상에서도 IBM Proventia Security Controller만 추가 배치하면 IBM Security Network IPS를 지속적으로 활용하는데 문제가 없다는 것도 알았다.

본 프로젝트에 들어간 G대학은 IBM Security Network IPS를 평소 트래픽 폭주로 서비스 지연이 잦았던 서버 팜의 앞 단에 위치시켰다. 인터넷 구간과 서버 망 구간에 경계를 두고 중간에서 서버로 유입되는 유해 코드나 웜 또는 DoS/DDoS 공격을 막아내기 위한 위치 선정이었다.

한편, G대학은 교육 기관이 기업에 비해 상대적으로 보안 취약성이 높은 실습실 PC 등 관리의 사각지대에 놓인 데스크톱이 DoS/DDoS 공격의 좀비로 활용되곤 한다는 것도 간과 하지 않았다. G대학은 외부에서 들어오는 IP 뿐 아니라 교내망을 거쳐 밖으로 나가는 IP까지 차단할 수 있는 IBM Security Network IPS의 기능을 활용해 DoS/DDoS에 대한 전방위 방어를 하고 있다.

"IBM은 다른 보안 솔루션 업체들보다 네트워크나 시스템의 보안 취약점을 빨리 찾는 편이다. 그리고 IBM X-FORCE 보안연구소가 각종 변종을 포괄적으로 막아내기 위해 작성해 배포하는 시그니처(Signature) 역시 신속하게 제공돼 Zero-day 공격 시대보다 효과적인 방어를 수행할 수 있다"

Benefit

대학 네트워크의 안정성과 서버 가용성 그리고 서비스 품질 모두 높여

설치를 마친 후 G대학은 트래픽 폭주나 보안 이슈 때문에 네트워크 대역폭이 고갈되거나, 서버에 직접적인 장애가 날 것이란 걱정에서 자유로워졌다. 방화벽을 우회해 들어오는 지능화 된 공격부터 시작해, 수강 신청이나 DoS/DDoS 등 트래픽이 과도하게 몰리는 등 학내 네크워트 상에서 일어나는 다양한 예외 사항들을 사전에 처리하는 IBM Security Network IPS 방어 메커니즘 덕분이다.

이처럼 G대학은 네트워크 안정성, 가용성, 보안성 삼박자를 모두 갖춘 장비인 IBM Security Network IPS를 통해 네트워크를 최적의 상태로 유지할 수 있게 되었다. 이는 관리자에게만 의미있는 것이 아니다. 교직원 및 재학생 모두에게도 뜻깊은 일이다. 학사 행정 시스템이나 대학 포탈 등에 접근함에 있어 언제나 일정 수준 이상의 서비스 품질(Quality of Experience)을 보장받을 수 있게 되었기 때문이다.

이 밖에도 IBM Security Network IPS는 G대학에게 비용 절감 효과도 안겨주고 있다. G대학은 향후 10Gbps로 백본망을 업그레이드 한 이후에도 10Gbps급 신형 IPS로 교체하지 않아도 돼 이번에 도입에 장비에 대한 투자분을 보호하게 되었다.

- **Industry** : 교육
- **Business Challenge** : 스마트 시대를 맞아 특정 시기에 몰리던 트래픽이 평소에도 꾸준히 늘어
- **Solution** : IPS를 도입해 트래픽 폭주 방지 및 각종 보안 침해 사전 대응 체계 정립
- **Benefit** : 네트워크 단의 보안 강화, 서버 자원에 대한 보호 및 서비스 연속성 보장 용이
- **IBM Service** : IBM 네트워크/시스템/단말 취약성 진단 서비스

물리적 인프라스트럭처

C기관

"CCTV에 지능을 부여해 교통 정보 시스템의 스마트 지수 급상승"

"프로젝트 내용을 보면 오랜 시간이 걸렸을 듯 하지만 실제 일정은 2주가량에 불과했다. VDS로 동일한 목표에 도전했다면, 더 많은 시간과 비용이 들었겠지만 C기관은 영상 분석이라는 소프트웨어적인 방법을 통해 시간과 비용 두 마리 토끼를 잡는 성과를 거둘 수 있었다"

Business Challenge

미래형 교통 체계 조기 정착을 위한 노력

C기관은 교통 관련 공공 안전 업무를 수행하는 기관이다. 다른 지역자치단체와 마찬가지로 C기관이 속한 지역도 인간 중심의 신교통 공간이라 일컬어지는 지능형 교통 체계(ITS: Intelligent Transport Systems)의 윤곽이 그 모습을 서서히 드러내고 있다.

지능형 교통 체계 구축이라는 대장정의 길에 오른 C기관은 2011년 의미있는 이정표 하나를 세운다. 지능형 교통 체계의 핵심 요소 중 하나인 도시 교통 정보 시스템(UTIS: Urban Traffic Information System)에 지능형 영상 분석 기술을 접목해 더욱 스마트 한 시스템을 만들어 낸 것이다.

C기관이 CCTV 환경에 지능형 영상 분석 기술을 접목한 것은 발상의 전환과도 같은 것이었다. 일반적으로 도시 교통 정보 시스템이 스마트 해지기 위해서는 VDS(Vehicle Detection System) 등과 같은 별도의 추가적인 장치를 주요 도로나 교차로 등에 설치해야 한다.

VDS란 도로의 한 지점을 통과하는 차량을 감지해 교통 정보를 수집하는 시스템으로 루프 검지기, 영상 검지기, 레이저 검지기 등 다양한 유형이 시장에 나와 있다. C기관은 VDS와 같이 추가적인 요소들을 도로 곳곳에 설치할 경우 높은 비용이 수반된다는 점을 인지하고, 다른 대안이 없는지를 수소문했다.

Solution

CCTV 시스템과 지능형 영상 분석 기술의 만남

C기관의 레이더에 감지된 대안은 IBM의 Smart Vision Suit(SVS)이었다. VDS 설치 없이 이미 운영하고 있던 CCTV에 담기는 영상만 가지고도 의미있고, 가치있는 정보 수집이 얼마든지 가능하다는 점이 C기관의 눈길을 사로잡은 것이다.

C기관은 한국IBM 관계자를 통해 SVS가 도시 교통 정보 시스템에 어떻게 적용될 수 있는지에 대한 사전 검증에 나섰다. 당시 C기관은 CCTV의 영상을 분석해 중요 이벤트와 경보 상황을 메타 데이터로 저장이 가능하다는 것 그리고 경보 상황 발생 시 담당자에게 실시간으로 전달되어 즉각적인 조치를 취하는 것이 가능하다는 것을 확인했다. 또한, 사고 등 특정 상황에 대한 조회가 필요할 경우 해당 영상 정보에 대한 검색 역시 간편하다는 점도 알 수 있었다.

모든 검토를 마친 C기관은 SVS의 영상 분석 기술과 알고리즘을 활용해 Traffic Monitoring Extension 모듈을 구현하는 프로젝트에 착수했다. 이 모듈은 C기관이 운영하고 있던 도시 교통 정보 시스템에 차량 속도, 교통량 등에 대한 실시간 정보를 제공하는 역할을 한다. 간단히 설명하자면 CCTV에 찍힌 영상을 분석해 주요 정보를 메타 데이터로 전환해 도시 교통 정보 시스템에 넘겨 주는 것이라 보면 된다.

Benefit

도시 교통 정보 시스템 정확도 90% 이상 개선

국민 편의 증진과 안전 도모를 위해 교통 운영·관리 체계에 IT 기술을 접목해 자동화·과학화 하는 것은 전국 모든 지자체에서 지향하는 목표다. C기관은 IT 기술 접목이란 부문에서 새로운 준거 사이트로 떠오를 전망이다. 비용 대비 효율성 높은 방식을 택한 결과 보다 적은 비용으로, 보다 빠르고 효과적으로 도시 교통 정보 시스템에 지능을 부여한 사례이기 때문이다.

SVS 적용 후 C기관 현업 관리자들은 달라진 도시 교통 정보 시스템의 능력에 놀라움을 감추지 못하고 있다. 과거에는 교통량 등 관련 정보 측정 및 분석이 자동화 되어 있지 않았었는데, SVS 덕에 필요한 정보가 자동으로 CCTV 영상에서 추출되어 관리자에게 전달되게 되었다.

어떤 정보들이 올라오느냐 하면 CCTV가 찍은 영상을 통해 직진 차량, 좌우 회전 차량, 유턴 차량, 중앙선 침범 차량 등의 수가 데이터화 된다. 그리고 1분 단위의 평균 속도 등의 데이터도 추출된다. 이처럼 다양한 교통 정보가 거의 실시간에 가깝게 올라오다 보니 C기관에서 운영하던 기존 도시 교통 정보 시스템(UTIS)의 정확도가 90% 이상 개선될 수 있었다. 또한, 다양한 정보가 자동으로 수집, 분석되다 보니 자연스럽게 C기관의 관계자들의 교통량 측정 등에 업무 시간을 할애할 필요도 없어졌다.

한편, C기관은 별도의 VDS를 도로 곳곳에 설치하는 대신 소프트웨어적인 방법을 선택한 결과 시스템 구축과 유지보수 비용 모두를 절감할 수 있었다.

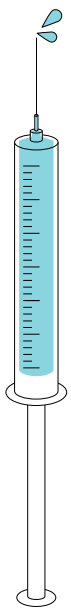
- **Industry** : 공공
- **Business Challenge** : 도시 교통 정보 시스템을 고도화 하기 위한 기술적 접근 방안 모색
- **Solution** : 별도의 추가 장치 설치 없이 영상 분석 기술 적용
- **Benefit** : 도시 교통 정보 시스템의 정확도 90% 이상 개선
- **IBM Service** : IBM Smart Vision Suit, Traffic Monitoring Extension

Copyright IBM Corporation 2010
한국아이비엠주식회사
(135-270) 서울시 강남구 도곡동 467-12
군인공제회관빌딩

Tel : 02 3781 7800
www.ibm.com/kr

All Rights Reserved

IBM과 IBM 로고는 미국 및 다른 국가에서의 IBM사의 등록상표입니다. 기타 회사, 제품, 서비스 명칭은 다른 회사의 등록상표 또는 서비스 상품일 수 있습니다.



KR1B903D