한국아이비엠주식회사

서울시 강남구 도곡동 467-12 군인공제회관
마케팅총괄본부 TEL:(02)3781-7800
www.ibm.com/kr

보안을 고려한 설계 (Secure by Design):

조직의 구조에 보안을 밀접하게 연관시켜야 하는 이유와 방안

웹 서비스 및 웹 애플리케이션 증가에 대한 요구사항을 지원해야 하는 회사에게
보안은 더 이상 최후의 선택이 아닌 IT 인프라의 설계부터 보안을 기반으로
IT 설계, 구성 및 운영되어야 한다는 인식의 전환이 필요합니다.
이러한 발상의 전환을 통해 변화하는 보안 범위에 따라
애플리케이션 및 서비스를 보호할 수 있는
경제적이고 안전하며 간소화된 IT 환경이 구현되어야 합니다.

보안을 고려한 설계
(Secure by Design):

조직의 구조에 보안을 밀접하게 연관시켜야 하는 이유와 방안

Contents

서문: 새로운 IT 세계

오늘날의 비즈니스 환경은 기기, 네트워크 및 시스템의 상호 연결성을 바탕으로 성장합니다. 이러한 상호 연결성은 새로운 가능성 및 도전의 세계를 엽니다.

다양한 조직들이 웹 기반 시스템, 서비스 및 애플리케이션에 대한 접근을 고객, 시민, 사용자, 클라이언트 및 파트너에게 제공함으로써 데이터 및 정보의 양은 폭발적으로 증가하고 있습니다. 몇 가지만 예로 들어보겠습니다.

- 한 보험회사의 경우, 1년 전에도 직원에게만 허용되어 수천 명에 불과했던 애플리케이션 사용자 수가 전국의 일반 고객 및 에이전트에게 온라인 서비스를 개시한 지금은 수백만 명에 이르게 되었습니다.
- 내부 리소스 팀에게만 데이터를 제공하던 정부 기관에서 지금은 국민들이 웹 상에서 직접 정보에 접근하여 정부 기관과 직접 업무를 진행하기 원하고 있습니다.
- 에너지/공공 사업 부문에서는 원격으로 웹 기반 애플리케이션을 이용해 원격으로 계량기 데이터를 수집하고 있습니다. 고객들은 온라인으로 로그인하여 요금을 지불하고, 비용을 절약하기 위해 전기 사용 패턴을 확인하고 조절합니다.

특정 산업 분야 뿐 아니라, 일반적인 IT 환경도 클라우드나 SOA(서비스 지향 아키텍처)와 같은 새로운 플랫폼의 사용으로 더 복잡해지고 더 광범위해지고 있습니다. 게다가, 온라인 접근은 하루 24시간 내내 서비스가 지원되어야 하며, 이는 온라인 서비스에 대한 기대치가 크게 변화하고 있음을 의미합니다.

이 모든 것의 바탕에는 새로운 채널, 포탈 및 서비스를 통해 데이터 및 시스템에 대한 접근을 확장 및 확대한다는 공통적이고 중요한 비즈니스 전략이 전제되어 있습니다. 그러나, 시스템이나 애플리케이션이 악용되거나 정보 보호에 문제가 있다고 드러날 경우 고객의 신뢰가 무너질 수 있습니다. 개인 데이터를 보호할 수 있는 조직의 능력에 대해 고객의 신뢰를 잃게 되면 시스템의 속도, 효율성 및 확장성은 더 이상 중요하지 않습니다. 따라서 규정을 준수하면서 가장 비용 효율적인 방법으로 애플리케이션과 접근 지점, 데이터베이스에서 데이터 저장 환경까지의 앤드투앤드 보안을 보장하지 않고는 이 전략은 효과적으로 구현될 수 없습니다.

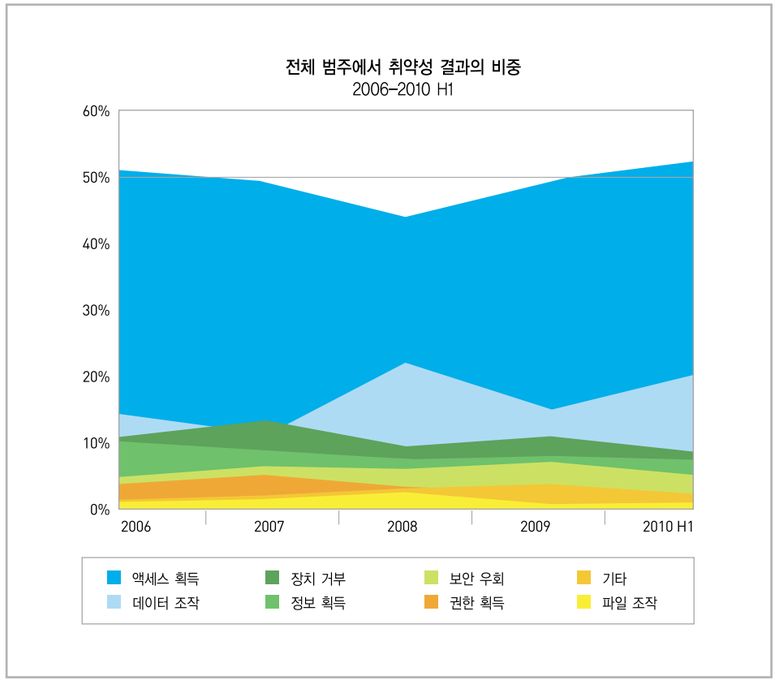
이러한 새로운 온라인 시스템에서 보안은 진정한 의미에서의 IT 운영과 전반적인 시스템 설계를 융합하기 시작했습니다. 보안은 더 이상 시스템 구현 단계 이후에 적용하는 독자적인 IT 기능이 아닙니다. 조직은 비용 효율적인 보안의 시작은 초기 단계부터 안전한 시스템 구성에 있음을 인식하고 처음부터 보안을 고려한 설계(Secure by Design)를 해야합니다. 이러한 철학은 보안이 비즈니스 프로세스, 제품 개발 및 일상적인 운영에 있어 본질적인 요소임을 시사합니다. 서비스의 테스트 및 실행 준비가 완료된 후 최종 단계로 보안이 덧붙여지는 게 아니라 초기 설계 요소가 되어야 합니다. 조직이 보안을 전체 시스템 설계에 포함시켜 구축하면 보안이 유지된 상태에서 혁신과 변화를 지향하는 민첩한 환경을 만들 수 있습니다.

보안 위협의 범위

상호 연결된 인프라에 있는 데이터 및 정보가 기하급수적으로 증가하면서 보안 문제는 계속해서 심각해지고 있습니다. 보안의 위협은 정부 시스템에 대한 테러리스트 공격에서부터 소매업체의 고객 이메일 및 모바일 장치에 영향을 주는 바이러스와 맬웨어에까지 다양하게 전개되고 있습니다. 위협은 끊임없이 진화하고, 이러한 위협의 상대적 영향, 가능성을 살펴보고 줄여나가는 데에는 깊은 지식과 노력이 필요합니다.

2010 X-Force 상반기 트렌드 및 위험 보고서는 전세계에 네트워크로 연결된 보안 운영 센터에서 가장 일반적이었던 특정 보안 관련 위협의 범위를 보여줍니다. 이 그래프에 나와있듯이, 이러한 위협은 해커가 취약성을 악용하고자 하는 동기를 얻음으로써 생겨납니다. 범죄 조직이 취약점을 악용하기 위한 동기 부여 요소로 "접근 권한 획득" 및 "데이터 조작"이 매우 높은 순위를 차지하고 있습니다. 취약성 악용의 52%에 달하는 시스템 접근 권한 획득은 공격자에게 해당 시스템에 대한 완전한 제어를 허용하여 공격자가 데이터를 가로채거나, 시스템을 조작하거나, 해당 시스템에서 다른 공격을 실행할 수 있게 합니다.

주목할 점은 데이터 조작 범주가 2010년 상반기에 21%까지 상승했다는 것입니다.



IBM X-Force 2010 상반기 트렌드 및 위험 보고서
http://www-935.ibm.com/services/us/iss/xforce/trendreports/

확실히, 데이터는 지속적인 위협을 받고 있습니다. IBM의 연구자료에 따르면 한 회사의 인프라는 하루에 60,000번 공격을 받았다고 합니다. 미국에서는 지난 5년 동안 3억5천4백만 건의 개인 정보 침해가 있었고, 이는 개인 및 회사 정보의 상당한 손상을 가져왔습니다. 2009년 1월의 한 사이버 보안 사건은 1억3천만 개의 신용 카드 정보를 노출했습니다.

조직에서 새로운 서비스를 구현하거나 새로운 고객에게 시스템을 개방하면 해당 서비스 및 시스템은 범죄의 표적이 됩니다. IBM X-Force 조사 결과에 따르면 2010년 상반기 동안만 웹 애플리케이션에 영향을 미치는 취약성 보고는 20,000건이 넘었습니다. 또한 X-Force팀의 중간 보고서에서도 상반기 동안 발생한 웹 애플리케이션 취약성은 모든 취약성 노출의 55% 이상을 차지한 것으로 드러났습니다.

위협 수준 증가와 더불어 PII(개인 식별 가능 정보)의 개인 정보 수집, 사용, 접근 및 보관에 대한 새로운 개인 정보 보호 법규의 지속적 흐름을 주의깊게 주시할 필요가 있습니다. 많은 경우, 특정 온라인 시스템이나 애플리케이션의 사용자들에게 다양한 접근 권한 수준을 규정하는 것이 필요하다는 것을 알 수 있습니다.

예를 들어, 미국의 새로운 개인건강정보보호법(HIPAA)에서 특정 연령에 도달한 십대의 병원 기록에 대해 당사자에게는 허용하되 동일한 데이터에 대한 부모의 접근은 금지할 수 있습니다. 그리고 의사가 환자의 의료 기록을 볼 수 있지만 보험 청구 정보에 대한 의사의 접근은 금지하는 규정이 있을 수도 있습니다. 어느 경우에서든 부당한 접근과 부적절한 데이터 공유는 법적 혹은 사업적 문제를 야기할 수 있습니다.

새로운 보안의 위협은 동적이면서 다양합니다.
데이터 프라이버시 규정과 연관된 위협을 다루는데 있어 단일 보안 제품으로의 접근법은 효과가 없습니다. 대신, 조직에서 새로운 서비스나 애플리케이션을 구현할 때 보안이 시스템 설계의 필수 부분이 되는 전체적이고 통합된 보안 접근법을 고려해야 합니다.

새로운 접근법이 필요한 이유

예전에는 조직 내 사업 부서에서 새로운 애플리케이션이나 서비스를 요청이 들어오면, 개발 팀에서 급히 만들어 IT 관리 부서로 넘겨 버리곤 했습니다. "속도나 비용 효율성 혹은 확장성"같은 시스템 품질이 보안보다 중요하게 생각되었고, 대개 적절한 보안 제어가 갖춰졌는지 여부를 고려하지 않고 애플리케이션이나 서비스가 만들어졌습니다. 하지만 이러한 방법은 보안 격차가 발생하면 이를 메꾸기 위해 원래 애플리케이션이나 서비스 위에 계속해서 IT가 구축됨에 따라 매우 빠른 속도로 복잡해지게 됩니다, 결국 보안 관리는 어려워지고 비용은 증가하여 보안이 비즈니스 성장을 저해하는 요소가 되고 말았습니다.

이 접근법은 위협의 관점에서도 효과가 없습니다. 새로운 사이버 공격, 기술 취약점 및 획기적인 사이버 범죄가 날마다 표면 위로 떠오르고 있습니다. 현재의 데이터 프라이버시와 정보 접근 간의 복잡한 관계는 서비스 시작 단계부터 보안을 우선적으로 고려할 것을 요구합니다.

조직은 서비스 수명 주기의 모든 단계에 보안을 포함시켜 보안 시스템을 구축해야 합니다. IBM은 보안을 고려한 설계(Secure by Design) 철학에 따라 안전한 인프라를 구축하는 데 있어 필요한 다음과 같은 세 가지 기본 요소를 제안합니다.

- 솔루션 작동 환경에서의 위협과 배포 후 시스템이나 구성요소가 직면할 예상 위험에 대한 지식
- 보안 수칙을 제공하거나 실행하도록 하는 기술의 활용
- 보안 설계의 유효성에 대한 지속적인 검증

이러한 요소를 고려하면 보다 비용 효율적이고 안전하며 간소화된 IT 환경을 만들 수 있습니다. 보안을 고려한 설계(Secure by Design) 철학은 시스템, 애플리케이션, 네트워크 및 데이터가 모든 비즈니스 프로세스의 일부로 효과적으로 보호되도록 하여 조직이 안전한 환경에서 혁신하고 성장할 수 있도록 도와줍니다.

보안을 고려한 설계(Secure by Design):
조직의 구조에 보안을 밀접하게 연관시켜야 하는 이유와 방안

보안 참조 프레임워크에 대한 필요성

오늘날의 IT 환경에서 단일 제품으로 조직의 모든 보안 문제를 해결할 수는 없습니다. 개별 제품들은 해커, 사이버 범죄자 및 기타 무단 침입자와 범죄자가 보안 시스템에 침입할 수 있는 여지를 제공합니다. 여러 제품을 개별적으로 배포할 경우 혼란만 가중될 수도 있습니다. 또한, 조직이 직면할 수 있는 위협 및 취약성의 범위를 커버할 수 있는 단일 솔루션은 없는 상태입니다. 규정 준수 가이드라인을 기반으로 만들어진 IBM 보안 프레임워크는 이러한 문제를 해결하기 위해 새로운 애플리케이션이나 서비스 제공을 위한 특정 조직 및 규정 준수 요구사항을 해결할 수 있는 포괄적인 기능을 제공하고 있습니다.

모든 보안 요구를 충족시키기 위해 일관성 없는 제품들에 의존하는 대신, 보안 프레임워크는 접근, 감사, 네트워크 및 데이터 보호와 같은 다양한 영역에 필요한 기술을 정확히 찾아내어 통합된 보안 기능을 갖춘 애플리케이션이나 서비스를 제공하도록 도와줄 수 있습니다.

관리 편이성 및 효율성을 위해 보안 프레임워크 구성요소를 모듈 방식으로 배포할 수 있지만, 비용을 줄이고 생산성을 향상시키기 위해서는 새 시스템을 처음 만들 때 보안 요구사항을 포괄적으로 보고 고려하는 것이 필요합니다. 프레임워크는 또한 오늘날의 새로운 온라인 비즈니스에서 일어나는 다양한 취약점 및 위협으로부터 데이터와 네트워크를 안전하게 보호할 수 있도록 해 줍니다. IBM 보안 프레임워크는 보호해야 할 조직 리소스 관점에서 보안을 기술하도록 개발되었습니다. IBM은 통합된 포괄적인 관점에서의 보안을 구성할 수 있는 5가지의 핵심 영역을 명시하고 있습니다.

- 사람과 아이덴티티
- 데이터 및 정보
- 애플리케이션과 프로세스
- 네트워크, 서버 및 엔드포인트
- 물리적 인프라

이러한 핵심 영역은 하드웨어, 소프트웨어, 전문/관리서비스나 이들의 조합으로 다루어질 수 있습니다.

출처: http://www.redbooks.ibm.com/redpapers/pdfs/redp4528.pdf

모든 경우에 동일한 솔루션이 요구되는 것은 아닙니다. 조직에서 다양한 이해 당사자들의 요구사항을 충족시키기 위해 모듈별로 보안을 구축할 수 있습니다.

IBM 보안 프레임워크를 사용하면 조직의 목표에 따라 핵심 영역에 걸쳐 애플리케이션이나 서비스에 대한 보안 요구사항을 처리할 수 있습니다. 프레임워크를 통해 필요한 보안 기능 및 서비스를 분류하고 정의할 수 있습니다.

시작하기

보안을 고려한 설계(Secure by Design) 철학을 통해 이해 당사자들은 함께 협력하여 조직의 요구를 기반으로 보안 문제를 정의하고 처리해야 합니다. 가장 중요한 보안 문제를 식별하고, 이를 추후 고려사항이 아닌 IT 보안을 위한 조직의 매우 중요한 요구사항으로 보고 처리하는 것이 목표입니다.

예를 들어, 약 3백만 개의 가구와 사업체에 전력을 제공하는 텍사스 소재 송전업체인 Oncor에서 통합된 스마트 그리드를 만들기로 결정했을 때, 이 회사는 에너지 사용 및 비용에 대한 추적을 개선하는 것 외에도 모든 고객과 기업의 전력 사용 데이터를 보호할 필요가 있다는 것을 깨달았습니다.

Oncor는 에너지 인프라에서 온라인 포탈을 통해 소비량을 모니터링하고 추적할 수 있게 해 주는 AMS(고급 계량 시스템)를 구현했습니다. 이를 통해 Oncor와 고객들은 에너지 소비를 더 잘 추적할 수 있게 되었습니다. 이 시스템은 회사가 이전에 계량기를 읽기 위해 직접 직원을 보내는 데 들었던 비용을 줄일 수 있게 해 주고, 데이터 보안 및 모든 규정 준수를 보장해 줍니다.

AMS의 배포로 Oncor가 현재까지 절약한 금액은 1억7천6백만 달러를 웃돌고 있으며, 그 결과 엔드유저의 추가 요금도 절감되었습니다.

또 다른 예를 들면, 철도 회사 CSX에서는 실시간 RPO(복구 목표 지점)를 갖춘 안전하고 신뢰할 수 있는 재해 복구 계획을 원했습니다. 20년간 CSX 파트너였던 IBM은 워싱턴 DC와 2개의 캐나다 주를 포함한 23개의 주에 서비스를 제공하고 있습니다.

작동 중단은 가장 중대한 문제이므로 CSX는 사용자가 많은 사이트의 "Tier 1" 애플리케이션을 핫 사이트에 미러링할 필요가 있다고 결정했고, 이 사이트는 현재 IBM에서 호스팅하고 있습니다. 또한, CSX 비즈니스 파트너의 요구사항이 급격히 증가했기 때문에 확장성과 복구 기능을 향상시키기 위한 애플리케이션의 오프사이트 가상화를 IBM에서 지원하고 있습니다.

이상은 보안을 고려한 설계(Secure by Design) 철학을 통해 새로운 서비스의 보안을 지원하고 조직이 사용자 및 파트너에 대한 온라인 접근 범위 확장을 진행할 수 있게 된 수백 가지 사례 중 두 가지 예 입니다.

사례: DGCX

DGCX(Dubai Gold & Commodities Exchange)가 복잡한 온라인 거래 시스템을 배포했을 당시, 즉각적으로 대응 가능한 무중단 서비스를 제공하고자 했고 보안은 시스템의 구축단계부터 핵심 요소였습니다.

"이것은 재무 데이터이므로 우리는 당연히 허가되지 않은 접근으로부터 데이터를 보호해야 합니다." 라고 DGCX의 기술 책임자 Basab Banerjee씨는 말합니다.

이 회사는 방화벽을 배포하는 일반적 보안 방법을 사용해 왔지만 주요 데이터를 보호하기 위해 보다 안전한 보안 조치가 필요하다는 것을 깨달았습니다. 또한 보안 조치를 늘려 시스템 성능에 영향을 미치고 싶지도 않았습니다.

시장 조사를 한 이후에 DGCX는 다음과 같은 이유로 IBM Security Network Intrusion Prevention System(이전의 IBM Proventia Network Intrusion Prevention System)과 IBM Security Server Protection(이전의 IBM Proventia Server Intrusion Prevention System)를 선택했습니다.

"우리는 시장에서 몇 가지 조사를 했습니다. 어느 제품을 선택해야 성능에 영향을 주지않고 필요한 보안을 제공하기에 적합할지 조사했지요." 라고 Banerjee씨는 이야기 합니다.

IBM 보안 어플라이언스는 제로데이(zero-day) 공격으로부터 보호하고 무단 네트워크 침입을 방지하는 데 도움이 됩니다.

"확장성은 주요 고려 사항 중 하나였습니다." 안정성 또한 주요 측면이었다고 Banergee 씨는 덧붙여 말합니다.

IBM 제품이 설치된 이후 DGCX는 꾸준한 비즈니스 성장을 거듭하고 있으며, 이는 업타임 목표 달성과 고객 서비스 레벨을 충족이 이루어 낸 결과였습니다.

"DGCX의 모든 비즈니스는 네트워크 가용성 및 성능에 의존하고 있고, IBM 제품은 업타임 시간을 유지하는데 도움이 됩니다. 3년 전에 제품을 설치한 이후로 99.9퍼센트 이상의 시스템 가동률을 유지해오고 있습니다." Banergee 씨가 말했습니다.

회사에 따르면 같은 기간 동안 웜 또는 바이러스와 연관된 보안 위반 및 아웃티지 또한 방지되었다고 합니다.

"로컬 지원팀은 훌륭했습니다." Banerjee 씨가 덧붙여 말합니다. "우리 네트워크는 매우 복잡합니다. IBM 팀의 지원이 없었다면 설치하는 데 훨씬 더 오랜 시간이 걸렸을 겁니다."

보안을 고려한 설계(Secure by Design):
조직의 구조에 보안을 밀접하게 연관시켜야 하는 이유와 방안

결론

자료 목록:

IT 관리자들은 외부에서 접근 가능한 포탈 및 서비스에 대해 전례 없이 심각한 어려움에 직면하고 있습니다. 말 그대로 하룻밤 사이에 다양한 시스템에 수백만 명의 사용자가 추가되면서 이러한 온라인 서비스의 보안 문제는 예전의 네트워크 보안 문제보다 훨씬 더 복잡한 것으로 나타나고 있습니다.

예를 들어 클라우드 컴퓨팅 및 가상화와 같은 새로운 컴퓨팅 패러다임을 채택하는 경우, 점점 더 정교해지는 위협 환경에 맞서 증가하는 위험과 복잡성을 처리할 수 있는 새로운 방법이 필요합니다.

보안을 고려한 설계(Secure by Design) 철학을 택함으로써 조직은 새로운 애플리케이션 및 서비스에 필요한 포괄적이고 통합된 보안을 수립할 수 있습니다.

올바른게 구현된다면, 이러한 보안 접근법은 데이터를 보호하고 취약성으로부터 안전하게 지킬 뿐 아니라 기업에 새로운 비즈니스 계획 추진에 필요한 경쟁 우위를 제공할 수 있습니다,