비즈니스 기반 보안 실현을 위한
IBM Security Framework 및 IBM Security Blueprint 소개

비즈니스 리더를 위한
보안 가이드라인

Axel Buecker
David Crowther
Foulques de Valence
Guilherme Monteiro
Michel Oosterhof
Andrew Quap
Maria Schuett
Kai Stockmann

- 표준과 베스트프랙티스를 기반으로 비즈니스 보안 참조 모델 구현
- 비즈니스 촉진 요인을 IT 보안 및 위험 관리 원칙에 연결
- 실제적인 비즈니스 시나리오 상에서 IBM Security Framework 및 IBM Security Blueprint 채택

Redbooks

개요

이 IBM® Redguide™ 출판물에서는 먼저 비즈니스와 IT 시스템의 보안 요구 사항과 이에 대한 위협을 규정하는 몇 가지 문제에 대해 살펴보겠습니다. 다음으로 관리 위험 및 비용, 비즈니스 정책 및 외부 규제 사항에 대한 준수 등을 포함하여 이런 문제들을 확연하게 보여주는 여러 가지 비즈니스 촉진 요인에 대해 식별합니다. 비즈니스와 IT 시스템을 설계, 구축, 운영 및 관리하는 과정에 있어서 보안상 주요 고려 사항이 무엇인지에 대해서도 설명합니다.

지난 수십 년 동안 산업계와 표준 기관들이 보안의 일부 측면에 대한 기준이 될 수 있는 프레임워크를 개발해왔습니다. 여기서는 2가지 일반적인 프레임워크인 CoBiT과 ISO/IEC 27002에 대해서 이야기합니다.

IT에 대한 보안 문제는 복잡하고 심오한 내용이 될 수 있습니다. 그렇기 때문에 IBM은 보안에 대한 비즈니스와 기술적 관점 사이의 커뮤니케이션 간격을 메울 수 있는 보충적인 관점을 개발하여 생각과 프로세스의 통합을 가능하게 했습니다. IBM Security Framework는 비즈니스 관점을 설명하고 IBM Security Blueprint는 기술적인 관점을 설명합니다.

IBM Security Framework는 보호가 필요한 비즈니스 자원 측면에서 보안을 설명하기 위해 개발되었으며, 비즈니스 관점과 다른 영역도 함께 다룹니다. 이 프레임워크는 IT 보안을 다음과 같은 6가지 영역으로 구분합니다.

- 사람과 아이덴터티
- 데이터와 정보
- 애플리케이션과 프로세스
- 네트워크, 서버 및 종점(Endpoint)
- 물리적 인프라스트럭처
- 보안 거버넌스, 위험 관리 및 규정 준수

IBM Security Blueprint는 핵심적인 보안 기능과 서비스들을 이런 영역들에 매핑함으로써 IBM Security Framework의 비즈니스 중심적 관점을 확장합니다. 이런 기능과 서비스는 보안 기능을 갖춘 엔터프라이즈 IT 환경에 대한 설계, 개발, 통합, 운영 및 관리에 대한 시작점으로서의 핵심적 역할을 수행합니다.

이 안내서는 보안 도메인, 기능 및 서비스를 기본으로 하고 두 가지 비즈니스 시나리오에 대해서 설명합니다. 첫 번째 비즈니스 시나리오는 암호 관리와 관련된 비용에 대한 것이고 두 번째 비즈니스 시나리오는 IBM Security Framework와 IBM Security Blueprint를 가장 적절하게 사용할 수 있는 방법을 보여주기 위한 PCI 준수에 대해서 설명합니다.

이 안내서는 구조적 가이드라인을 따라서 엔터프라이즈 보안을 이해하고 구현하고자 하는 비즈니스 리더, 보안 담당 중역, 컨설턴트들에게 소중한 정보가 될 것입니다.

IT 보안을 위한 비즈니스 전후 관계

세계화가 가속화되고 끊임 없이 지속되는 커뮤니케이션과 거래 속에서 전통적인 경계가 점점 사라지고 허물어지고 있습니다. 이렇게 새로운 글로벌 현실 속에서 사업상 개방(open for business)은 여러 조직 간에 리소스와 중요한 정보를 공유하는 것이 글로벌 경제로 진입하기 위한 사실상의 전제 조건임을 의미합니다. 참여와 고립의 차이가 기회와 위험의 차이와 같은 의미일 수 있습니다. 지금은 기업들이 기회를 포착하고 위험을 회피하기 위해서 그 어느 때보다도 컴퓨팅 시스템과 자동화에 더 많이 의존하고 있는 시대입니다. 위협이 되는 요소를 근본적으로 제거하고 지적 재산권을 보호하며 기업의 명성과 사생활 보호를 위해서 컴퓨팅 시스템에 크게 의존하고 있는 게 현실입니다.

기업들은 보안 시스템을 구축하기 위해서 기술 주도형(technology-driven) 접근법을 채택하는 경우가 많습니다. 그러나 단지 기술만 안전하게 보호한다고 해서 비즈니스 위험으로부터 비즈니스 프로세스와 비즈니스 자산을 보호할 수 있는 것은 아닙니다. 비즈니스 리더들은 보안, 위험 및 규제 사항 준수와 관련된 투자를 통해서 기업의 경쟁력을 확보하고 복잡한 규제 가이드라인을 만족시킬 수 있습니다.

일반적으로 보안 솔루션 제공업체들은 상향식(bottom-up) 접근법을 고객들에게 추천하기 때문에 기업들이 이 접근법을 통해서 보안 시스템을 구축하는 경우가 많습니다. 기업들은 찾아낸 보안 문제를 해결하기 위해서 기존의 보안 체계에 지속적으로 추가적인 보안 기능을 더하는 방식으로 그 성능을 강화하고 있습니다. 이 기술 중심(technology-centric) 방법론을 사용하면 종국에는 아주 복잡하고 일체성이 결여된 보안 인프라가 되어 버리는 경우가 많습니다. 이렇게 복잡하고 일체성이 없는 보안 인프라는 관리가 매우 어려우며 예상하지 못한 취약성이 발생할 가능성이 높고 쓸 데 없이 IT 비용이 상승하게 되어 결과적으로는 보안 인프라의 운영에 있어서 비효율성이 증가하게 되기 때문에 비즈니스가 성장하는 데 있어 촉진 요인이 되기보다는 오히려 저해 요인이 될 수 있습니다.

비즈니스 위험을 관리하기 위해서는 비즈니스 목표와 보안을 위한 기술적 요구 사항과 제약 조건을 함께 고려하는 종합적인 접근법(holistic approach)이 필요합니다. 기업들은 가능한 모든 위협을 막아내려고 노력하기 보다는 기업에 가장 적합한 보안 위험 관리 활동이 어떤 것인지 이해하고 우선 순위를 정해야 합니다. 기업 내의 위험 수용 수준을 이해하게 되면 IT팀은 기업이 반드시 해결해야 하는 위험을 줄이는 일에 쉽게 역량을 집중할 수 있습니다. 특정한 위험을 너무 과도하게 강조하면 자원과 노력을 쓸데 없이 허비하게 되며 반대로 특정 위험을 너무 과소 평가하면 큰 재난이 발생할 수 있습니다.
혁신을 지속하고 비용을 줄이는 것과 같은 비즈니스 목표와 규제 사항 준수 문제를 해결하고 내부 및 외부 위협으로부터 보호하는 운영상의 요구 사항을 동시에 지원할 수 있는 전략적이고 종합적인 보안 접근법을 마련하는 것은 쉬운 일은 아닙니다.

보안은 기업 내에서 일어나는 다른 비즈니스 활동과 분리해서 해결할 수 있는 문제가 아닙니다. 보안은 비즈니스 관점에서 파악되어야 합니다. 다시 말해서, 보안을 비즈니스 프로세스를 보호하고 강화하는 수단으로서 보는 것입니다.
그러기 위해서는 전체 비즈니스 내 사람, 데이터 및 기술을 포함하는 주요 비즈니스 영역에서의 위험을 식별하기 위한 계획 및 평가 기준이 필요합니다. 이런 계획의 과정을 통해서 비즈니스 필요성을 충족하고 비즈니스 결과를 극대화하는 기업 전체를 위한 효과적인 방어막 역할을 수행할 수 있는 비즈니스 중심 보안 청사진(business-driven security blueprint)과 전략을 설계하고 구축할 수 있습니다.

이 보안 청사진은 여러 가지 촉진 요인에 의해서 영향을 받습니다. 그러므로 이제는 필수적인 요소들을 보다 잘 이해하고 조직화할 수 있도록 이러한 촉진 요인에 대해서 자세히 살펴보겠습니다.

보안에 영향을 미치는 촉진 요인

우리는 비즈니스 촉진 요인들을 기본 요소로 인식하고 있지만 오늘날의 프로젝트의 대부분은 비즈니스와 IT 촉진 요인 두 가지 요소에 의해서 추진됩니다. 이렇게 영향을 미치는 요소들에 대해서 자세히 살펴보겠습니다.

- **비즈니스 촉진 요인 :** 비즈니스 촉진 요인은 외부 요소에 의해서 나타나는 제한 사항을 나타냅니다. 비즈니스 촉진 요인을 구체적인 수치가 있는 비즈니스 목표로 볼 수도 있습니다. 비즈니스 촉진 요인은 가치, 위험 및 경제적 비용을 측정합니다. 가치 촉진 요인은 자산의 가치, 비즈니스에 대한 시스템의 가치 그리고 비즈니스 자체의 가치를 측정합니다. 위험 촉진 요인은 규제 사항 준수, 기업 구조, 기업 이미지 및 기업의 위험 수용 등과 관련된 것입니다. 경제적 촉진 요인은 생산성 영향, 경쟁력 및 시스템 비용 등을 측정합니다.
- **IT 촉진 요인 :** IT 촉진 요인은 일반적으로 IT 환경에서 운영면에서의 제한 사항을 나타냅니다. 예를 들어, 내부 위협 및 외부 위협에 노출되는 시스템(그 환경도 포함)의 복잡성은 기업이 해결해야 하는 위험을 나타냅니다.

또한 비즈니스 촉진 요인은 관리되고 있는 현업 시스템의 이해 당사자들에 대한 중요성의 문제와 그 결과를 나타냅니다. 이런 일련의 촉진 요인들은 산업 별로 다를 수 있고 같은 산업에 속해 있다 하더라도 기업 별로 다를 수 있으며 심지어 한 기업 내에서 사용하는 서로 다른 비즈니스 애플리케이션 사이에서도 다를 수 있습니다.
IT 촉진 요인들은 IT 환경의 신뢰성에 영향을 주는 기술적 고려 사항과 관리되고 있는 현업 시스템을 전체적으로 나타냅니다. IT 촉진 요인들은 공통적인 것이며 최대한 비즈니스 촉진 요인의 전후 관계를 파악하여 고려되어야 합니다. 비즈니스 촉진 요인과 IT 촉진 요인의 결합은 보안 관리를 위한 주요 이니셔티브를 나타냅니다.
다음에 이어질 토론 내용에서 위협(threat), 위협 에이전트(threat agent) 및 취약성(vulnerability) 등과 같은 용어에 대한 여러 가지 참조 자료가 있습니다. ISO 15408에서 ISO (International Organization for Standardization)가 규정한 일반적인 기준은 다음과 같습니다.

- 위협은 보호된 자산이 남용될 수 있는 잠재성으로 특징 지울 수 있다.
- 위협 에이전트는 자산에 한 가지 가치를 메길 수 있으며 자산 소유자의 이익에 반하여 자산을 남용하거나 손상시키는 방법을 모색한다.
- 취약성은 위협 에이전트에 의해서 악용될 수 있으며 자산과 자산 소유자에 대한 위협을 나타낸다.

보안 관리 솔루션을 개발함에 있어서 직면하게 되는 문제 중 하나는 관리되고 있는 비즈니스 시스템이 운영되는 환경 내에 존재하는 위협, 위협 에이전트 및 취약성이 근본적으로 동적이며 그 범위가 매우 넓다는 것입니다.

참고 : ISO 15408과 관련 문서는 ISO 웹 사이트(http://www.iso.org)에서 확인할 수 있습니다.

보안에 영향을 미치는 비즈니스 촉진 요인

보안 의사 결정에 영향을 미치는 비즈니스 촉진 요인들은 주요 보안 이니셔티브의 두 가지 그룹 중 첫 번째 그룹입니다. 비즈니스 촉진 요인들은 산업 별로 다를 수 있고 한 비즈니스 내에서도 애플리케이션 별로 다를 수 있는 촉진 요인을 나타냅니다. 이런 촉진 요인들의 하위 집합을 산업 또는 애플리케이션에 따라서 적용할 수 있기 때문에 비즈니스 촉진 요인들은 선택할 수 있는 것으로 고려됩니다.

정확하고 안정적인 운영

정확하고 안정적인 운영은 비즈니스의 운영에 있어 정확하고 일관적으로 수행해야 하는 정도를 나타냅니다. “정확한 운영” 은 비즈니스의 운영이 일체의 오류도 없이 적절한 대응 또는 기능을 수행해야 한다는 것을 의미합니다. 그리고 “안정적인 운영” 은 항상 동일한 결과가 도출되어야 함을 의미합니다. 모든 IT 시스템은 이해 당사자들에게 예상되는 결과를 일관적으로 제공해야 합니다.

보안 이벤트와 사고는 이런 비즈니스 프로세스의 정확하고 안정적인 운영에 영향을 미칠 수 있습니다. 또한, 기본적인 IT 인프라 또는 상위나 하위 비즈니스 프로세스에 영향을 미칠 수도 있습니다. 문제가 있는 서비스(정확하지 않거나 시간에 따라서 결과가 다른 서비스)로 인해서 초래될 수 있는 결과는 서비스 소비자에게 커다란 영향을 미칠 수 있으며 결과적으로 서비스의 제공자에게도 커다란 영향을 미칠 수 있습니다.

서비스 수준 계약

이 촉진 요인은 보안 위협과 위협 에이전트가 기업이 비즈니스를 수행하는 기능에 영향을 미칠 수 있는 상황에 적용됩니다. 서비스 수준 계약(Service-level agreement, SLA)은 한 기업 내에서 허용되는 운영 조건을 결합합니다. SLA는 비즈니스 시스템 별로 또는 애플리케이션 별로 다를 수 있습니다. 시스템, 데이터 및 프로세스의 가용성은 SLA 내에서 일반적으로 참조하는 조건입니다.

IT 자산 가치

한 IT 시스템에 대한 보안 수준은 해당 시스템 내에서 발견되는 자산의 가치에 비례하여 정해질 가능성이 높습니다. 자산 가치는 해당 시스템에서 거래하는 자산의 기본적인 가치와 관련됩니다. 이런 가치는 유형적일 수도 있고 무형적인 것일 수도 있습니다. 전자 소매 업체(e-retailer)의 경우 이런 가치는 유형적인 자산입니다. 금융 서비스를 제공하는 업체의 경우 해당 시스템의 거래에서 사용되는 고객 정보 또는 기타 데이터가 자산이 될 수 있습니다. 이런 자산은 시스템 프로세스 뒤에 있는 자산입니다.

비즈니스 자산 가치 또는 브랜드 이미지 보호

이 촉진 요인은 기업의 이미지를 보호하고자 하는 기업의 욕구를 반영합니다. 보안 사고 또는 보안 공격으로 인해서 문제가 발생하게 되면 비즈니스에 직접적인 영향을 미치게 됩니다. 그러므로 보안 대책은 예상되는 결과에 맞춰 비례하여 준비해야 합니다. 기업에 대한 부정적인 견해가 확산되는 것을 막고자 하는 경우에 보안 문제가 발생하면 이 촉진 요인에 대한 조건이 더 강력하게 될 것입니다.

법규 및 규제 사항 준수

법규 및 규제 사항 준수는 비즈니스 시스템과 해당 국가 내에서의 트랜잭션에 부과된 외부 조건을 의미합니다. 여기에는 규제 기관 및 정부 기관이 정한 규칙과 정책이 포함됩니다. 보안 사고 또는 보안 공격으로 인한 민 · 형사상 책임 또는 법적인 처벌은 비즈니스에 부정적인 영향을 미칩니다. 그러므로 법규 및 규제 사항 준수를 위한 규정과 단계의 정도를 이 촉진 요인에서 고려해야 합니다. 여기에는 사생활 보호 문제, 트랜잭션 시작자 검증 기능 및 준수 여부 검증 등이 포함됩니다.

계약상의 의무

IT 시스템에 대한 보안 대책은 보안 공격 때문에 해당 비즈니스가 계약상의 의무를 지게 될 때 발생하는 결과에 맞춰 비례하여 준비해야 합니다. 계약의 구조와 조건에 따라서 재정적 손실 또는 불이익이 발생할 수 있습니다. 예를 들어, 보안 사고가 발생했을 때 해당 비즈니스는 제품 또는 서비스를 제공한다는 계약상의 의무를 이행하지 못할 수 있습니다.

재정적 손실 및 책임

보안 사고가 발생하면 비즈니스에 직접적인 재정적 손실이나 간접적인 재정적 손실이 발생할 수 있습니다. 직접적인 재정적 손실에는 자산의 도난, 서비스의 도난 또는 사기 행위 등이 포함됩니다. 간접적인 재정적 손실에는 민 · 형사적인 판결에 따른 손실, 선한 의지의 손실 또는 우선 순위가 바뀐 예산 배정 등이 포함될 수 있습니다. 이 촉진 요인은 IT 시스템에 대한 보안 대책이 이런 결과에 비례하여 마련되어야 한다는 사실을 명확하게 드러냅니다.

중요 인프라

이 촉진 요인은 보안 위협 또는 위협 에이전트가 비즈니스의 일부 커뮤니티 또는 대부분의 인구에 또는 둘 모두에 공통적이거나 공유되는 서비스 또는 리소스에 큰 영향을 미칠 수 있는 경우에 적용됩니다.

예로는 통신, 전력, 운송 시스템, 컴퓨팅 등과 같은 것을 들 수 있습니다. 제공업체들에게 중요 인프라 손실이 발생하면 물결 효과가 발생하여 2차적인 손실이 발생하고 이렇게 영향을 받은 업체들의 보안 의사 결정이 뒤따르게 됩니다. 위험 분석의 중요한 부분 중 하나는 중요한 인프라를 식별하는 것입니다.

안전 및 생존

이 촉진 요인은 보안 위협과 위협 에이전트가 인간의 삶, 정부의 기능 및 사회 경제적 시스템의 측면에 큰 영향을 미칠 수 있는 경우에 적용됩니다. 안전과 생존에 대한 영향에 대해서 고려되어야 하는 프로세스의 예로는 중요 인프라의 연속성, 의료 체계, 삶에 대한 지원 또는 영향력이 크거나 시간에 따라 달라지는 프로세스 등을 들 수 있습니다.

보안에 영향을 미치는 IT 촉진 요인

IT 촉진 요인은 중요 보안 이니셔티브의 두 번째 그룹입니다. IT 촉진 요인은 관련된 실패와 사고로 인해서 초래된 위험과 결과에 상응하는 방식으로 모든 근대적인 IT 솔루션에서 고려해야 하는 공통적인 촉진 요인입니다.

내부 위협 및 위협 에이전트

보안 관련 실패 및 사고는 IT 시스템을 운영하고 제어하는 기업의 물리적 및 논리적 경계 내에서 발생하는 위협 또는 위협 에이전트에 의해서 발생합니다. 이런 위협과 위협 에이전트는 기술 또는 사람과 연관 지을 수 있습니다.
내부 위협의 예로 제대로 설계되지 않아서 적합한 통제가 없는 시스템을 들 수 있습니다. 내부 위협 에이전트의 예로는 악의적인 범죄를 저지를 목적으로 IT 시스템에 접근하거나 비즈니스 또는 관리 프로세스에 영향을 미칠 수 있는 능력을 악용하는 사람을 들 수 있습니다.

외부 위협 및 위협 에이전트

보안 관련 실패와 사고는 IT 시스템을 운영하고 제어하는 기업의 물리적 및 논리적 경계 밖에서 발생하는 위협 또는 위협 에이전트에 의해서 발생합니다. 이런 위협과 위협 에이전트도 기술 또는 사람과 연관 지을 수 있습니다. 외부 위협과 위협 에이전트는 논리적 또는 물리적 경계를 침입하여 내부 위협 또는 위협 에이전트가 되거나 논리적 또는 물리적 경계 밖에서 비즈니스 또는 관리 프로세스에 영향을 미칠 수 있는 방법을 모색합니다.
외부 위협의 예로는 전력 공급망, 네트워크 연결망 또는 물리적 혹은 논리적 네트워크 경계를 침투하는 컴퓨터 바이러스 또는 웜 바이러스 등과 같이 기업 경계의 외부에 있는 하나 이상의 비즈니스 또는 관리 프로세스에 대한 단일 실패 지점이 될 수 있습니다. 외부 위협 에이전트의 예로는 해커 또는 개인의 전자 신분증 또는 신분 정보를 이용하여 내부자로서 행동할 수 있는 능력을 가진 외부자를 들 수 있습니다.

IT 서비스 관리 서약

이 촉진 요인은 IT 시스템의 운영관리에 실패하면 비즈니스의 보안에 문제가 발생할 수 있다는 사실을 명확히 합니다. 이 촉진 요인은 IT 서비스 전달과 IT 서비스 지원 등의 2가지 구성 요소로 나눌 수 있습니다.

- **서비스 전달 서약**
  시스템이 스스로를 관리하는 기준을 충족하지 못하는 것은 비즈니스 또는 관리 프로세스 모두에 대한 보안 문제가 발생한 것으로 볼 수 있습니다.
  서비스 전달에 대한 보안 노출의 예로는 IT 운영 프로세스가 중요한 사건에 시의적절하게 대응하지 못하는 경우를 들 수 있습니다. 또 다른 예로는 IT 복원 프로세스가 서비스 거부 공격에 대해서 시의적절하게 대응하지 못하여 그 피해로부터 시스템을 복구하지 못하고 결과적으로 비즈니스 프로세스에 대한 용량의 손실 또는 대응 시간의 손실이 발생하는 경우를 들 수 있습니다.

▶ **서비스 지원 서약**

비즈니스 또는 IT 관리 시스템이 서비스 수준 계약(Service-Level Agreement, SLA)을 충족하지 못하는 경우 비즈니스 또는 관리 프로세스에 대한 보안 노출로 볼 수 있습니다.

서비스 지원에 대한 보안 노출의 예로는 고객 관계 프로세스가 접근 제어 목록에서 사용자를 시의적절하게 추가, 수정 또는 제거하지 못하는 경우를 들 수 있습니다.

IT 환경 복잡성

IT 환경의 복잡성도 IT 시스템의 보안에 영향을 미칠 수 있습니다. IT 환경은 비즈니스 시스템이 구축되는 인프라를 나타냅니다.

예를 들어, 인트라넷 또는 엑스트라넷에 연결되어 있는 모든 IT 환경은 내부 또는 외부 위협 또는 위협 에이전트에 노출되어 있으며 특정한 보안 대응책을 필요로 합니다. 시스템을 위한 독립 실행형 시설은 가장 낮은 복잡성을 나타냅니다. 다른 시스템과 다른 회사들이 포함된 호스팅 시설은 더 복잡한 환경을 나타냅니다. 많은 수의 시스템이 포함되어 있고 다양한 네트워크 액세스 경로가 있으며 복잡한 아키텍처를 갖는 환경은 복잡한 IT 환경입니다.

비즈니스 환경 복잡성

대부분의 비즈니스가 IT에 의존하고 있기 때문에 대부분의 비즈니스 환경은 상호 연결된 일련의 비즈니스 집합이며 각각의 비즈니스 집합은 각각 복잡한 IT 환경, 비즈니스 프로세스 및 IT 관리 프로세스를 갖고 있습니다. 이런 복잡성이 IT 시스템의 보안에 영향을 미칠 수 있습니다.

감사 및 추적 가능성

이 촉진 요인은 시스템 내에 저장되어 있는 정보(관리 데이터 또는 비즈니스 데이터와 관련된 정보)에 대한 감사를 지원하기 위해서 IT 시스템이 필요함을 명확히 해줍니다.

IT 취약성: 구성

구성 취약성은 잠재적으로 모든 IT 시스템에 존재하며 시스템과 시스템이 설계되고 설정되어 있는 상태를 기반으로 해서 잠재적인 공격에 허점을 노출합니다.

IT 취약성: 결함

소프트웨어 결함은 잠재적으로 모든 IT 시스템에 존재합니다. 이런 결함은 시스템 또는 구성 요소 설계에서 발견되지 않았고 확실하게 드러나지 않는 취약성을 나타냅니다. 그렇기 때문에 결함은 원래 설계된 의도에서 벗어난 예상치 못한 사태입니다. 예로는 운영 체제 또는 애플리케이션이 구현된 후에 발견되는 버그 등을 들 수 있습니다.

IT 취약성: 악용

모든 IT 시스템에서 소프트웨어의 기본 설계는 해당 IT 시스템, 비즈니스 또는 관리 프로세스에 대한 공격의 일부로서 위협 또는 위협 에이전트에 의해서 악용될 수 있습니다. 여기에는 시스템에 들어 있는 기능을 시스템, 구성 요소 또는 근원적인 데이터를 손상시키기 위한 목적으로 사용하는 것이 포함됩니다. 어떤 사람들은 익스플로잇(exploit)을 결함 및 악용 방식으로 정의하기도 하지만 익스플로잇에는 시스템을 공격하기 위해서 정상적인 설계 내 취약점을 악용하여 전혀 새로운 방식의 사용을 통한 경우도 포함되기 때문에 우리는 결함의 이용과 악용 방식을 별개의 것으로 취급합니다.

IT 보안 관리

IT 보안 관리는 관리된 비즈니스 시스템에 대한 복원 능력 및 위험 관리 목표에 따라서 앞에서 기술한 비즈니스 및 기술적 문제를 해결할 수 있도록 정의된 일련의 관리 활동을 의미하는 용어입니다.

IT 보안 관리 솔루션을 개발하고 배포하는 데 있어서 가장 어려운 문제는 관리되고 있는 비즈니스 시스템의 설계와 운영 모두에 영향을 미치는 복잡한 일련의 요구 사항들을 제시하는 비즈니스 및 IT 촉진 요인을 실현하는 것입니다. 앞에서 설명한 비즈니스 촉진 요인과 IT 촉진 요인들은 상호 배타적이 아니며 상호 추가적이고 의존적인 것입니다.

먼저, 우리는 이런 촉진 요인들이 서로 어떻게 연관되는 지에 대해서 자세히 살펴보겠습니다. 그리고 위험 관리 원칙에 대해서 조금 더 자세히 살펴본 다음 마지막으로 엔터프라이즈 보안에 대한 전체적인 접근법을 제공하는 몇 가지 공통적인 산업 접근법을 소개하겠습니다.

보안의 부가적인 계층

그림 1에는 비즈니스 촉진 요인(세로 축)과 IT 촉진 요인(가로 축)의 상호 관계가 간단하게 표현되어 있습니다. 그림 1에는 비즈니스 촉진 요인과 IT 촉진 요인의 모든 관계와 결합된 보호 계층에 대한 관계가 표현되어 있습니다.

	IT 취약성 – 악용	IT 취약성 – 악점	IT 취약성 – 구성	감사 및 추적 가능성	데이터 기밀성 및 무결성	IT 환경 복잡성	비즈니스 환경 복잡성	내부 위협 및 위협 에이전트	외부 위협 및 위협 에이전트
안전 및 생존	비즈니스 보안								
중요 인프라									
재정적 손실 또는 책임									
계약상의 의무									
법규 및 규제 사항 준수									
비즈니스 자산 가치 또는 브랜드 이미지									
IT 자산 가치	정보 보증								
서비스 수준 계약	운영 보안								
정확하고 안정적인 운영									

그림 1 IT 보안 관리의 부가적 레이어

3가지 부가적인 보안 대응 또는 계층이 있습니다.

운영 보안 인프라와 서비스 수준 관리에 대한 적절하고 안정적인 운영에 초점을 맞춘 대응적 대책 및 능동적 대체의 혼합체이다.

정보 보장 가치가 있는 정보 자산을 보호하도록 지정된 대책이다.
참고: 적절한 운영 보안은 적절한 정보 보장을 전제로 한다.

비즈니스 보안 비즈니스 특정 위험 및 결과를 해결하는 다양한 대책이다.
참고: 적절한 운영 보안과 정보 보장은 적절한 비즈니스 보안을 전제로 한다.

어떤 IT 보안 관리 계층이 필요한 지에 대한 의사 결정은 이 안내서 3페이지의 “보안에 영향을 미치는 촉진 요인”에 언급된 촉진 요인에 대한 분석을 통해서 이뤄져야 합니다. 이런 촉진 요인들을 평가할 때 이런 분석 자료는 사용 사례에서 관련 내용을 제공합니다. 또한 이런 분석을 통해서 IT 보안 관리를 비즈니스 및 IT 관리 모델에 통합할 수 있습니다.

효과적인 IT 보안 관리 시스템을 위해서는 필수적으로 위험 관리를 이해해야 합니다. 이제 위험 관리(risk management)의 원칙에 대해서 자세히 살펴보겠습니다.

위험 관리

모든 기업은 위험에 직면하고 있습니다. 위험 분석(Risk analysis)은 오류 발생가능 사항, 오류 상태가 발생하는 방식 그리고 해당 이벤트에 의해서 발생할 수 있는 손상 결과 등에 대해서 회사 자산을 평가하는 작업입니다. 분석해야 할 요소에는 다음과 같은 것들이 있습니다.

- **위협** : 위험을 일으키는 이벤트, 압력 또는 사람입니다. 위협은 취약성을 악용하려는 이벤트일 수도 있습니다.
- **가능성** : 이 위협이 발생할 수 있는 가능성입니다.
- **손상** : 위협이 악용될 경우에 입게 되는 영향입니다. 손상에는 서비스, 매출, 잠재 매출 및 이미지 손실 그리고 다른 비즈니스 특정 요소의 손실이 포함됩니다.
- **트레이드오프** : 보완적인 솔루션을 만들기 위해서 2개의 경쟁적인 비즈니스 촉진 요인을 평가하고 각 비즈니스 촉진 요인의 장단점을 평가하는 것입니다. 이런 트레이드오프를 분석하기 위해서 일반적으로 사용하는 기법은 비즈니스 영향 분석(business impact analysis)입니다.

위험 분석의 결과는 조직에 대한 위험의 집합체입니다. 다음 단계인 위험 감소(risk mitigation)에서 기업은 이런 위험을 어떻게 처리할 지에 대해서 판단합니다. 각각의 위험 부문에 대해서 다음과 같은 옵션을 선택할 수 있습니다.

- **위험 감소**: 통제 또는 기술을 통해서 위험을 감소시킵니다.
- **위험 전가**: 위험을 다른 객체(예. 보험 등)에 가져다 놓음으로써 위험 요소를 제거합니다.
- **위험 수용**: 이익을 기반으로 해당 위험이 허용 가능한 지 여부를 결정합니다.
- **위험 무시**: 해당 위험을 감소시키거나 이전하거나 허용하지 않는 것이다. 해당 위험을 허용하는 것과 같은 것이지만 책임은 없습니다.

목표는 식별된 위험을 감소시키는 것입니다. 보안 정책(security policy)을 사용하면 위험을 더 잘 관리할 수 있는 메커니즘을 정의할 수 있습니다. 이 정책은 9페이지의 그림 2에서 볼 수 있듯이 위험을 허용 가능한 수준으로 낮추기 위해서 프로세스와 기술을 조합하는 것입니다.

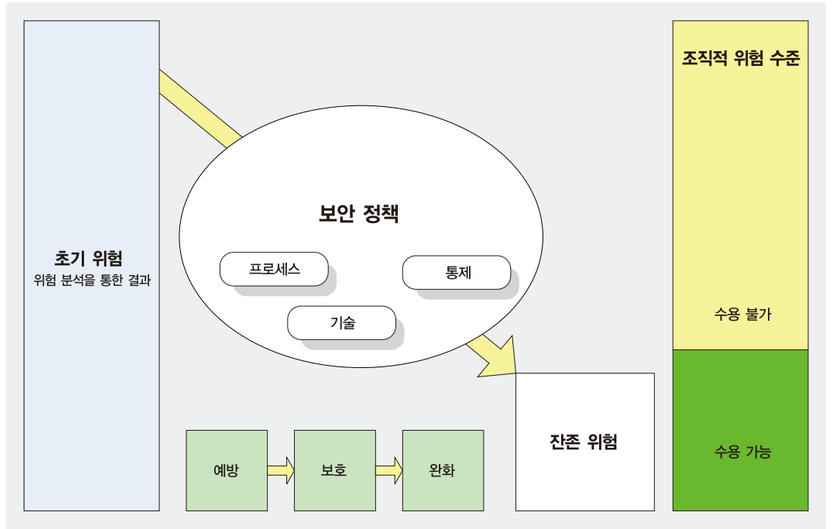

그림 2 위험 줄이기

그림 2에서 왼쪽에 초기 위험 수준이 표시되어 있습니다. 보안 정책은 해당 위험을 줄이기 위한 통제, 프로세스 및 기술에 대한 지침을 제공합니다. 보안 정책은 심각도를 줄임으로써 위험을 예방하고 그 위험으로부터 시스템을 보호하고 그 영향을 감소시킵니다. 위험은 제거되는 것이 아니고 감소되는 것입니다. 기업은 허용 가능한 위험 수준이 어느 정도인지를 양적으로 또는 질적으로 결정합니다. 이 과정은 위험과 이익의 균형점을 찾기 위한 비즈니스 영향 분석 또는 기타 기법을 사용하여 수행합니다. 예를 들어, 시장 출시 시간과 사용 편의성 등과 같은 촉진 요인을 수용하기 위해서 더 높은 수준의 위험을 허용하도록 결정하는 기업이 있을 수도 있습니다. 보안 정책은 잔존 위험을 해당 보안 정책을 채택한 기업이 허용하는 수준 또는 그 이하로 낮춰야 합니다. 이 잔존 위험은 해당 위험을 더 이상 감소시킬 수 있는 능력이 없는 경우 또는 해당 위험을 일정 수준 이하로 감소시키기 위해서 추가적인 투자를 하지 않기로 비즈니스 적으로 결정하는 경우에 발생합니다.

공통 산업 접근법

3페이지의 “보안에 영향을 미치는 비즈니스 촉진 요인”에 기술되어 있는 비즈니스 요인들로 인해서 기업 내 IT 거버넌스를 구현하는 데 도움이 되는 국제적으로 수용되는 프레임워크와 모범 사례를 채택하는 기업의 수가 계속 늘고 있습니다. Control Objectives for Information and related Technology[1] (CobiT), International Organization for Standardization 27002:2005[2] (ISO/IEC 27002:2005), Information Technology Infrastructure Library[3] (ITIL) 등은 세계적으로 IT 거버넌스와 규제 사항 준수를 위한 가장 믿을 수 있는 프레임워크로 부상했습니다. 우리는 다음 섹션에서 IT 보안에 더 초점을 맞추고 있는 CobiT 및 ISO/IEC 27002:2005(IT 서비스 관리 요소에 더 초점을 맞추고 있는 ITIL과 대조됨)에 대해서 자세히 알아보겠습니다.

---

1 CobiT에 대한 자세한 정보를 보시려면 http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981로 이동하십시오.

2 ISO/IEC 27002:2005의 사본을 구입하시려면 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297로 이동하십시오.

3 ITIL®에 대한 자세한 정보를 보시려면 http://www.itil-officialsite.com/home/home.asp로 이동하십시오.

정보 및 관련 기술에 대한 제어 목표

Control Objectives for Information and related Technology (CobiT)는 1996년에 Information Systems, Audit and Control Association (ISACA) 및 IT Governance Institute (ITGI)에서 개발한 일련의 IT 관리용 모범 사례(프레임워크)입니다. CobiT은 IT 거버넌스와 통제에 대해 국제적으로 인정된 프레임워크입니다. 최신 버전은 2007년에 IT 거버넌스 협회가 발행한 4.1 버전입니다. 여기에는 다음과 같은 섹션이 포함되어 있습니다.

- Executive summary (경영자 요약) – CobiT 주요 개념과 원칙을 설명한다.
- CobiT framework (CobiT 프레임워크) – CobiT 접근법을 설명한다.
- Control objectives (통제 목표) – 각 IT 프로세스를 효과적으로 통제할 수 있도록 하기 위해서 관리해야 하는 일련의 통제 요구 사항을 정의한다.
- Management guidelines (관리 가이드라인) – IT 프로세스의 성능을 측정하고 비교하며 향상시킬 수 있는 도구에 대해서 설명한다.
- Implementation guide (구현 가이드) – CobiT을 구현하기 위한 일련의 도구 집합을 제공한다.
- IT Assurance guide (IT 보장 가이드) – 통제 목표가 성취되었는지 여부를 평가하는 방법에 대해서 설명한다.

CobiT의 바탕이 되는 기본 개념은 모든 기업이 비즈니스 의사 결정을 지원해야 한다는 비즈니스 정보(business information)에 주목하는 것입니다. 비즈니스 정보 자체는 다시 IT 관련 리소스의 결과물이며 CobiT에서는 이것을 애플리케이션, 정보, 인프라 및 사람으로 정의합니다. 마지막으로, 이런 IT 관련 리소스는 IT 프로세스에 의해서 관리되며 특정한 비즈니스 정보 기준(효과성, 효율성, 기밀성, 무결성, 가용성, 안정성 및 규정 준수)을 충족합니다. CobiT은 다음과 같이 4가지 영역으로 그룹화되어 있는 34가지 고수준 프로세스를 정의하고 있습니다.

1. 계획 및 조직화(Plan and organize)
이 영역은 IT 전략(IT가 어떻게 비즈니스 목표 달성에 일조할 수 있을 것인가?)에 초점을 맞추고 있습니다.
2. 획득 및 구현(Acquire and implement)
이 영역의 주제는 IT 전략을 실현하기 위한 IT 솔루션의 식별, 개발 또는 획득 및 통합입니다.
3. 전달 및 지원(Deliver and support)
이 영역은 전체적인 IT 서비스를 전달하고 지원하는 것에 대한 것입니다.
4. 모니터링 및 평가(Monitor and evaluate)
이 도메인은 모든 IT 프로세스의 품질과 규정 준수 여부를 확인하기 위해서 지속적으로 평가하는 것에 초점을 맞추고 있습니다.

이런 34가지 프로세스는 210개의 통제 목표에 의해서 제어됩니다. 그러므로 CobiT을 구현할 때는 하향식 접근법을 선택하는 것이 좋습니다. 그 이유는 IT 전략을 비즈니스 목표에 맞추기 위해서는 우선 비즈니스 목표를 명확하게 정의해야 되기 때문입니다.

ISO/IEC 27002:2005

International Organization for Standardization 27002:2005 (ISO/IEC 27002:2005)의 전신인 The British Standard 7799[4]는 세계에서 가장 널리 알려져 있는 보안 표준입니다. 마지막 주요 출판은 1999년 5월이었으며 이 버전에는 이전 버전과 비교하여 여러 가지 강화된 기능과 향상된 기능이 포함되었습니다. 2000년 12월에 다시 출판되었을 때 이 표준은 International Organization for Standardization 17799 (ISO/IEC 17799)로 진화되었습니다. 17799는 2005년에 다시 여러 개정판이 더해져서 ISO/IES 17799:2005(E)로 다시 출판되었습니다. ISO17799라는 이름은 추가적인 수정 없이 정보 보안 관리 표준을 위한 새로운 ISO/IEC 번호 지정 체계로 채택되었으며 현재는 ISO/IEC 27002:2005로 식별되고 있습니다.

4 Risk Server(위험 서버), Security Risk Analysis(보안 위험 분석), ISO17799, Information Security Policies(정보 보안 정책) 및 Audit(감사) 그리고 Business Continuity(비즈니스 연속성)에 대한 정보는 http://www.riskserver.co.uk/에서 찾아보실 수 있습니다.

ISO/IEC 27002:2005는 보안 문제에 대해서 포괄적으로 다루고 있습니다. 여기에는 수 많은 통제 요구 사항(일부는 매우 복잡함)이 포함되어 있습니다. 그렇기 때문에 ISO/IEC 27002:2005를 준수하는 것은 간단한 문제가 아니며 보안 문제에 가장 큰 관심을 갖고 있는 기업들에게 조차도 쉬운 일이 아닙니다.

ISO/IEC 27002:2005에 접근할 때는 단계별로 차근차근 접근하는 것이 좋습니다. 처음 시작할 때 가장 좋은 것은 우선 현재의 위치 또는 상황에 대해서 평가하는 것이고 다음으로 ISO/IEC 27002:2005 준수를 위해서 필요한 변경 사항을 식별하는 것이 좋습니다. 그런 다음에야 계획과 구현 작업이 확실하게 수행될 수 있습니다.

ISO/IEC 27002:2005에는 전체적인 엔터프라이즈 보안 접근법을 적용할 때 고려해야 하는 11가지 서로 다른 범주가 포함되어 있습니다. 11가지 범주는 다음과 같습니다.

1. 보안 정책
2. 정보 보안을 위한 조직
3. 자산 관리
4. 인적 자원 보안
5. 물리적 보안 및 환경적 보안
6. 커뮤니케이션 및 운영 관리
7. 접근 제어
8. 정보 시스템 구입, 개발 및 유지 보수
9. 정보 보안 사건 관리
10. 비즈니스 연속성 관리
11. 규정 준수

이제 IBM Security Framework (ISF)를 소개할 때가 되었습니다. IBM Security Framework의 목표는 사용자의 보안 상태를 보다 효과적으로 평가할 수 있게 해주는 모범 사례와 공개 표준을 기반으로 광범위한 보안 모델을 제공하고 사용자의 비즈니스 성장을 지원할 수 있는 전사적인 보안 아키텍처를 효율적으로 구현할 수 있게 하는 것입니다.

IBM Security Framework는 비즈니스 문제 지향적이기 때문에 '어떻게'가 아닌 '무엇을'에 초점을 맞추고 있습니다. IBM Security Framework를 사용하면 사용자의 요구 사항을 고려하여 구체적인 IT 구성 요소 또는 IT 서비스가 아닌 포괄적인 비즈니스 솔루션을 개발할 수 있습니다.

IBM Security Framework

요즘의 비즈니스 리더들은 CFO들이 자신의 영역에서 위험을 관리하는 것과 같은 방식으로 각자의 분야에서 위험을 관리하도록 요청 받고 있습니다. 비즈니스 리더들은 보안 위험과 그것이 IT에 미치는 잠재적인 영향에 대해서 비즈니스 관점으로 중역들과 의사 소통해야 합니다. 또한, IT 보안 통제와 비즈니스 프로세스에 정렬해야 하고 IT 위험을 비즈니스 관점에서 모니터링하고 정량화해야 하며 중역 수준에서 비즈니스 수준의 통찰력을 동적으로 촉진해야 합니다. 규정 준수를 강화하는 방향으로 보안 운영 작업을 조율하고 위험을 관리하여 비즈니스 결과를 극대화해야 합니다.

한 기업이 비즈니스 프로세스에 보안을 강화할 때 비즈니스 중심 접근법이 비즈니스 목표와 보조를 맞추면서 전체적이고 시너지 효과를 낼 수 있는 방향으로 서로 다른 모든 보안 영역들이 함께 작동할 수 있게 만드는 안내자 역할을 수행해야 합니다. 그렇지 않으면, 해당 기업의 위험에 대한 입장은 IT와 비즈니스 전략 간의 우선 순위 불일치로 인해서 매우 취약해집니다. 비즈니스 촉진 요인을 IT 보안 영역에 매핑하기 위해서 표준 기반 접근법을 사용하는 것은 보통 매우 어려운 일이며 추가적인 작업인 경우가 많습니다.

IBM은 그림 3에서 볼 수 있는 종합적인 IT 보안 프레임워크를 개발했습니다. 이 IT 보안 프레임워크를 사용하면 비즈니스 중심 보안에 대한 전체적인 접근법을 사용할 때 모든 필요한 IT 보안 영역을 적절하게 해결할 수 있습니다.

그림 3 IBM Security Framework

IBM은 기업들이 IBM Security Framework와 보조를 맞춰서 보안에 대한 비즈니스 중심의 전체적인 접근법을 채택할 수 있게 해주는 완벽한 솔루션 및 서비스를 제공합니다.

IBM은 광범위한 전문가 서비스, 관리 서비스 그리고 하드웨어 및 소프트웨어를 제공하여 IBM Security Framework에 의해서 처리되는 다음과 같은 보안 영역을 해결할 수 있도록 사용자를 돕습니다.

보안 거버넌스, 위험 관리 및 규정 준수

모든 기업은 비즈니스 전략과 비즈니스 운영에 지침이 되는 원칙과 정책을 정의하고 서로 커뮤니케이션해야 합니다. 또한, 모든 기업은 비즈니스와 운영 상의 위험을 평가하고 기업에 맞는 보안 관리 활동의 실행과 유효성 검사를 위한 벤치마크의 역할을 수행할 기업 보안 계획을 개발해야 합니다.

이런 원칙 및 정책, 기업 보안 계획 및 부가적인 품질 향상 프로세스 등은 기업 보안 거버넌스, 위험 관리 및 규정 준수 모델을 나타냅니다. 구체적으로, 나머지 보안 영역에 대한 요구 사항과 규정 준수 기준은 다음과 같습니다.

- 사람 및 아이덴터티
  이 영역은 적절한 사람이 적절한 자산에 적절한 시간에 접근할 수 있게 하는 방법에 대한 측면을 다룹니다.
- 데이터 및 정보
  이 영역은 조직 전체에서 전송 중이거나 저장되어 있는 중요한 데이터를 보호하는 방법에 대한 측면을 다룹니다.
- 애플리케이션 및 프로세스
  이 영역은 애플리케이션과 비즈니스 서비스 상의 보안을 유지하는 방법에 대한 측면을 다룹니다.
- 네트워크, 서버 및 종점(Endpoint), IT 인프라
  이 영역은 모든 IT 시스템 구성 요소에 걸쳐서 새롭게 등장하는 위협에 대처하는 방법에 대한 측면을 다룹니다.
- 물리적 인프라
  이 영역은 물리적 공간에서 사람 또는 사물에 대한 이벤트의 보안을 유지할 수 있는 디지털 통제의 기능을 활용하는 방법에 대한 측면을 다룹니다.

지금부터 이런 영역에 대해서 구체적으로 살펴보겠습니다.

사람 및 아이덴터티

기업들은 비즈니스를 수행하고 비즈니스 운영을 지원하는 자산과 서비스를 보호해야 합니다. 자산과 서비스를 보호하는 한 가지 방법은 접근 통제(access control)를 이용하는 것입니다. 효과적인 접근 통제 서비스를 제공하는 기능은 사람과 아이덴터티를 기업의 보안 거버넌스, 위험 관리 및 규정 준수 모델에 의해 정의된 것에 따라서 관리하는 기능을 기반으로 합니다.

보안 거버넌스, 위험 관리 및 규정 준수는 아이덴터티를 관리하는 방법과 접근 통제를 수행하는 방법에 대한 지침을 제공합니다. 기업들은 사람들을 등록하고 등록된 사람들을 아이덴터티와 매핑합니다. 사람과 기업 간의 관계는 역할(role), 권한(rights), 비즈니스 정책(business policies) 및 규칙(rules)의 관점에서 표현됩니다. 사람을 등록하고 등록된 사람들과 기업과의 관계를 기술하는 기능은 나머지 다른 보안 영역(데이터 및 정보, 애플리케이션 및 프로세스, 네트워크, 서버 및 종점(IT 인프라) 및 물리적 인프라)에 대해서 보안을 유지할 수 있게 해주는 중요한 역할을 담당합니다.

운영 면에서 볼 때, 한 기업 내에서 인증된 역할로 활동하거나 확장된 관계의 일부로 행동하는 사람은 인프라, 데이터, 정보 및 서비스에 접근할 수 있습니다. 또한, 인증되지 않은 역할로 활동하는 사람은 비즈니스 정책과 계약에 맞지 않게 행동하는 경우 인프라, 데이터, 정보 및 서비스에 접근할 수 없습니다.

아이덴터티 시스템 내에서 사람들에게 신뢰정보(credential)가 발급될 수 있습니다. 신뢰정보는 물리적 ID 카드 또는 논리적 토큰 또는 사용자 식별자 등 다양한 형태를 띨 수 있습니다. 신뢰정보의 신뢰성(trustworthiness) 또는 강도(strength)는 비즈니스 정책 및 위험 관리의 중요한 측면입니다. 아이덴터티의 생명 주기를 효과적으로 관리할 수 있는 능력, 다시 말해서 노동력, 고객 또는 사용자 커뮤니티로 구성된 동적인 인구 구성에 대해서 아이덴터티를 생성하고 제거하며 역할을 변경하는 것은 매우 중요한 능력입니다. 예를 들어, 아이덴터티와 신뢰정보의 생명 주기는 비즈니스 주기, 고용 주기, 고객 관계, 계약, 비즈니스 또는 일정 등에 의해서 영향 받을 수 있습니다.

아이덴터티 시스템은 적절한 일련의 접근 통제와 함께 사용되어야 합니다. 아이덴터티 시스템은 여러 가지 기술 아키텍처를 포함할 수 있는 IT 인프라 전체에서 사용자 역할, 권리 및 권한을 관리해야 합니다. 또는 특정 사용자가 적절한 자산과 서비스에 접근할 수 있게 하기 위해서 여러 개의 아이덴터티 및 접근 통제 시스템이 필요할 수도 있습니다.

아이덴터티 및 접근에 대한 규정 준수는 보통 외부에서 기인한 규정 준수인 경우가 많습니다. 예를 들어, 법규화된 사생활 보호 및 증거 기록 등의 활동은 포괄적인 사용자 프로비저닝 및 ID 관련 기록 보관의 구현을 위한 확실한 촉진 요인입니다.

그림 4에는 요약된 내용과 함께 사람 및 아이덴터티 영역 내에서 처리되어야 하는 몇 가지 추가적인 측면이 기록되어 있습니다.

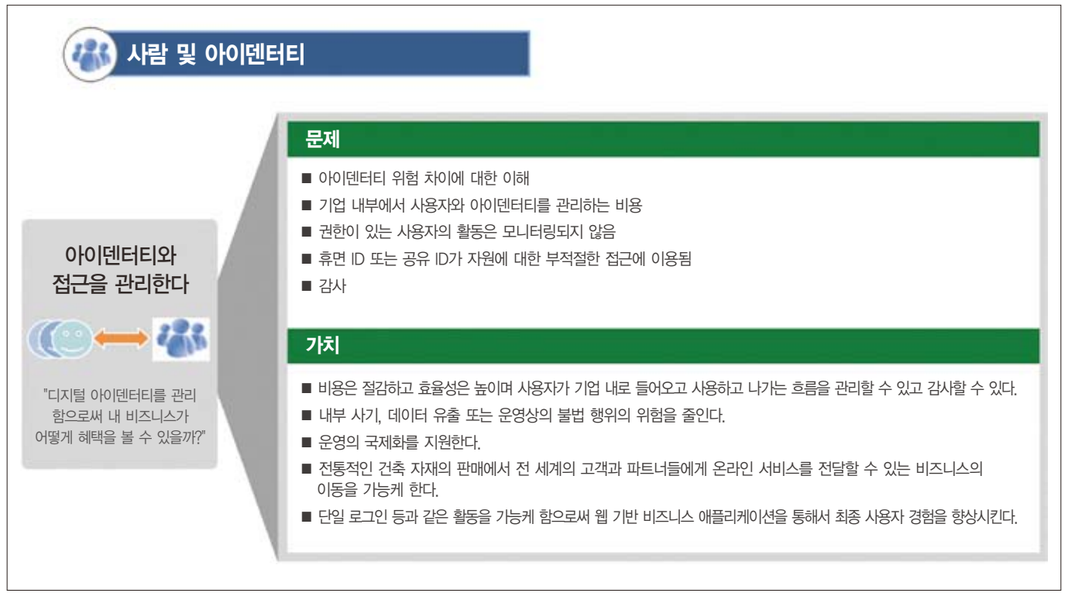

그림 4 사람 및 ID 도메인

데이터 및 정보

기업들은 통제해야 하는 원시 데이터(raw data)와 문맥화된 정보(contextualized information)를 모두 보호해야 합니다. 보안 거버넌스, 위험 관리 및 규정 준수는 데이터와 정보의 가치에 대한 지침을 제공할 뿐만 아니라 데이터와 정보에 대한 위험을 어떻게 관리해야 하는 지에 대해서도 지침을 제공합니다.

데이터 및 정보 보호를 위한 효과적인 계획에는 데이터 및 정보의 접근, 변환, 이동 및 정리 작업을 담당하는 속성, 정책 및 강화 메커니즘 및 서비스와 함께 카탈로그의 유지 또는 이런 자산의 목록이 포함됩니다.

이 데이터 및 정보 보호 계획은 비즈니스 프로세스, 비즈니스 트랜잭션 또는 비즈니스 및 인프라 지원 프로세스에 적용될 수 있습니다. 데이터 및 정보의 보호는 데이터 및 정보의 생성에서 폐기에 이르기까지 전체 생명 주기와 데이터 및 정보의 다양한 상태, 위치 및 예시에 적용되며 데이터 및 정보가 저장되거나 물리적 또는 전자적으로 이전될 때에도 적용됩니다.

데이터라는 용어는 전자적으로 인코딩된 자산에 광범위하게 적용될 수 있습니다. 여기에는 기술적 위험(악의적인 코드의 출현)과 비즈니스 위험(라이센스 계약의 위반)으로부터 보호되어야 하는 소프트웨어, 펌웨어도 포함됩니다.

데이터 및 정보의 보호는 다른 모든 운영적 보안 영역의 정의 및 운영과 상호 의존적입니다. 데이터 및 정보에 대한 보호 측면에서 한 기업의 규정 준수 정도를 측정하고 보고서를 작성하는 것은 기업 보안 계획의 효과성을 보여주는 실체적인 계량입니다. 데이터 및 정보 규정 준수 보고서를 통해서 모든 영역의 통제, 서비스 및 메커니즘의 강점과 약점을 볼 수 있습니다.

그림 5에는 내용 요약과 함께 데이터 및 정보 도메인 내에서 해결해야 하는 몇 가지 추가적인 측면이 기술되어 있습니다.

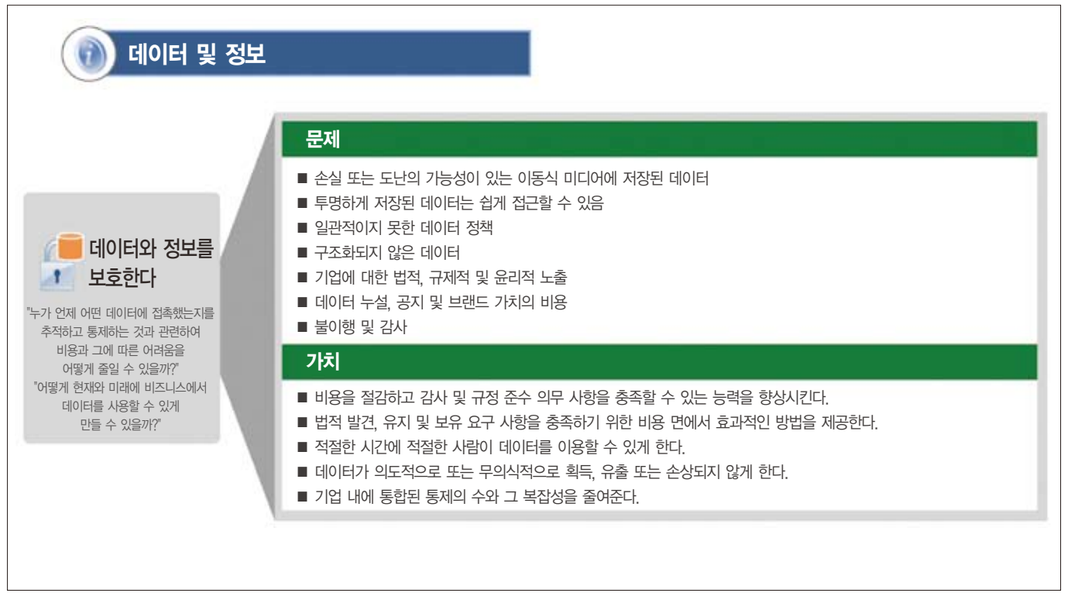

그림 5 데이터 및 정보 영역

애플리케이션 및 프로세스

기업들은 기업의 비즈니스 핵심적인 애플리케이션을 설계 단계에서부터 구현 및 실사용에 이르기까지 전체 생명 주기에 걸쳐서 외부 및 내부 위협으로부터 능동적으로 보호해야 합니다. 애플리케이션 생명 주기 전체에 걸친 통제가 실현되면 나머지 다른 보안 영역에서도 효과적인 통제와 규정 준수를 실현할 수 있습니다.

예를 들어, 애플리케이션이 서비스 지향성 아키텍처(SOA)를 통해서 전달되는 고객 관계 관리(CRM) 시스템 등과 같이 내부적으로 초점이 맞춰진 것이거나 또는 새로운 고객 포털 같이 외부적으로 대면하고 있는 애플리케이션이든 그에 관계없이 해당 애플리케이션이 새로운 위험을 초래하는 것이 아니고 비즈니스에 새로운 힘을 불어넣는 것이 되게 하려면 명확하게 정의된 보안 정책과 프로세스가 반드시 필요합니다.

보안 영역 내에서의 프로세스에 대한 서비스 관리를 포함하여 모든 비즈니스 및 비즈니스 지원 프로세스에 대한 서비스 관리는 비즈니스가 적절한 위험 관리 및 규정 준수 지침 내에서 운영되게 하기 위해서 필수적으로 필요한 부분입니다. 보안에 대한 서비스 관리에는 반드시 중앙 집중식 인증, 접근 및 감사 정책 관리 그리고 웹 애플리케이션 취약성 스캐닝 및 침입 방지 등과 같은 다양한 기능이 포함되어야 합니다.

그림 6에는 내용 요약과 함께 애플리케이션 및 프로세스 영역 내에서 해결해야 하는 몇 가지 추가적인 측면이 기술되어 있습니다.

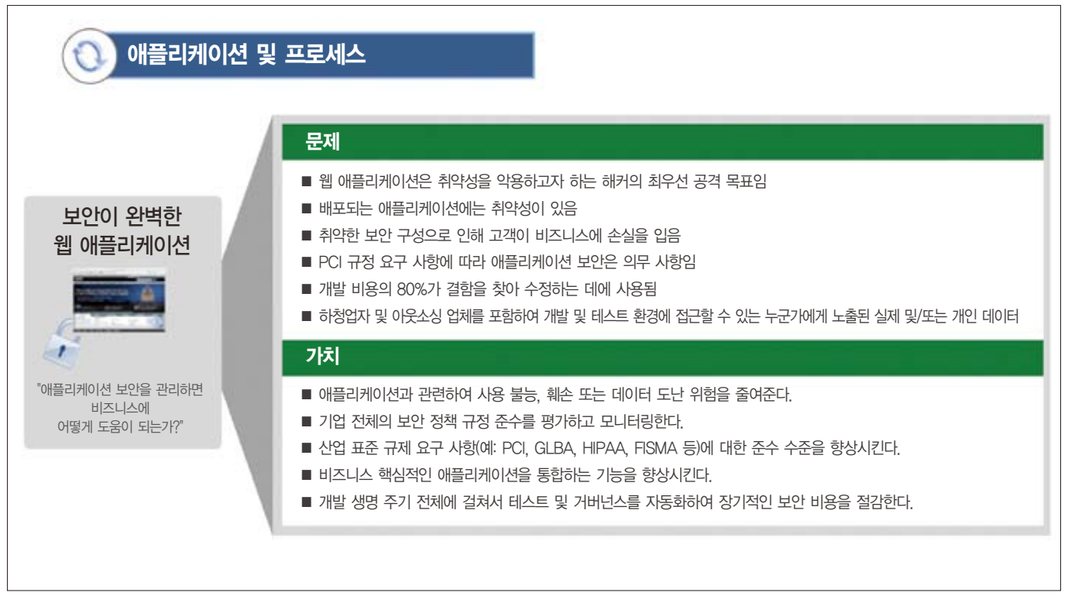

그림 6 애플리케이션 및 프로세스 영역

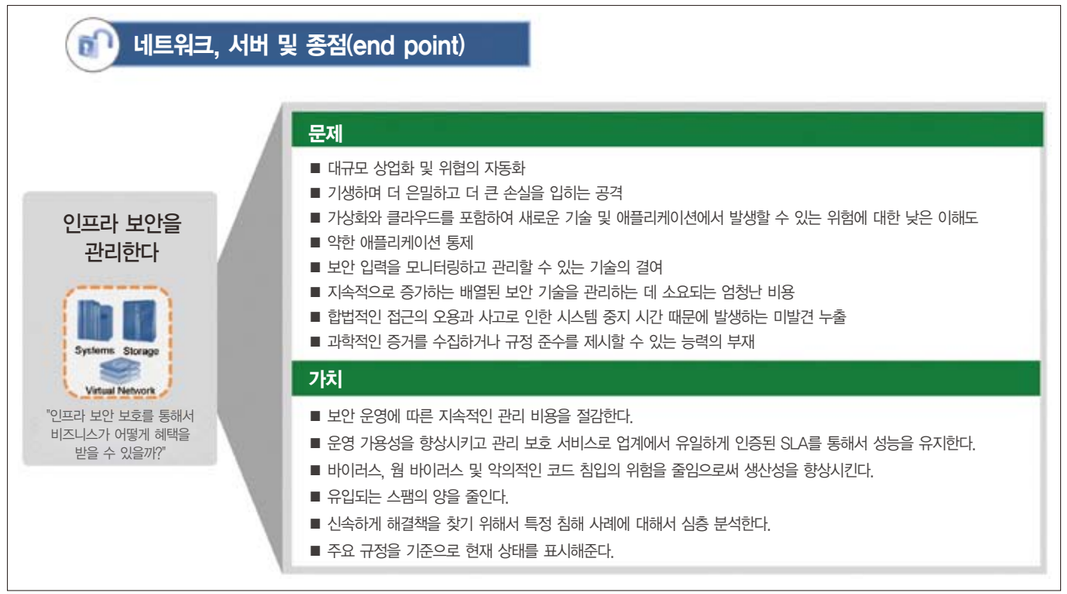

그림 7 네트워크, 서버 및 종점(Endpoint) 영역

네트워크, 서버 및 종점(Endpoint)

기업들은 빈틈이 발생하는 것을 방지하거나 줄이기 위해서 비즈니스의 운영과 IT 인프라에 위협과 취약성이 있는지 여부를 예방적이고 능동적으로 모니터링해야 합니다.

보안 거버넌스, 위험 관리 및 규정 준수는 기술 기반 위험의 비즈니스 관계에 지침을 제공할 수 있습니다. 실무에서는 사건 대응의 기술적 측면은 물론이고 기술 기반 위협의 정의, 배포 및 관리 등을 운영 관리 직원이 대신할 수 있으며 서비스 제공업체에 아웃소싱을 할 수도 있습니다.

기업의 네트워크, 서버 및 종점에 대한 보안 모니터링과 관리는 시스템 구성 요소와 사람 그리고 그것이 지원하는 비즈니스에 부정적인 영향을 미칠 수 있는 새로운 위협을 막아내기 위한 매우 중요한 작업입니다. 새로운 보안 위협을 식별하고 인프라를 그것으로부터 보호하는 것에 대한 필요성은 조직적이고 재정적인 이득을 목적으로 하는 네트워크 침입 시도가 발생하게 되면서 크게 높아졌습니다. 세상에 완벽한 기술은 없지만 IT 인프라에 배포되어 있는 네트워크, 서버, 종점의 유형 그리고 이런 구성 요소가 구축, 통합, 시험 및 유지되고 있는 방식에 따라서 보안, 모니터링 및 관리의 초점과 강도가 달라질 수 있습니다.

기업들은 가상화 기술을 이용하여 더 짧은 시간 내에 더 민첩하게 서비스를 전달하고자 하는 목표를 달성합니다. 기업들은 이 환경 내에 보안 구조를 구축함으로써 가상화의 목표(예: 향상된 물리적 자원 이용률, 향상된 하드웨어 효율성 및 전력 비용의 절감)를 달성할 수 있습니다. 동시에 가상 시스템의 보안은 물리적 시스템의 보안과 마찬가지로 강력하게 유지할 수 있습니다.

그림 7에는 내용 요약과 함께 네트워크, 서버 및 종점 영역 내에서 해결해야 하는 몇 가지 추가적인 측면이 기술되어 있습니다.

물리적 인프라

기업 보안 계획을 효과적으로 구현하기 위해서는 물리적 인프라와 연관되어 있는 비즈니스 위험과 기술적 위험을 반드시 이해하고 해결해야 합니다. 보안 거버넌스, 위험 관리 및 규정 준수 영역은 위험의 유형과 물리적 보안을 위한 계획과 대응의 유형에 대한 지침을 제공합니다.

기업의 인프라를 보호한다는 것은 비즈니스 연속성에 영향을 미칠 수 있는 물리적 인프라의 실패 또는 손실에 대해서 사전 조치를 취하는 것을 의미합니다. 기업의 인프라를 보호하는 것은 유틸리티 서비스의 손실, 물리적 접근 통제 실패에 의한 정보의 노출 또는 중요한 물리적 자산의 손실 등으로 인한 영향 등과 같은 간접적인 위협과 취약성으로부터 인프라를 보호하는 것이 될 수도 있습니다. 효과적인 물리적 보안을 위해서는 자산, 직원, 고객, 일반 대중 및 지역 날씨 등을 포함한 다양한 소스에서 입력되는 데이터와 정보를 서로 연관 지을 수 있게 해 주는 중앙 집중식 관리 시스템이 필요합니다.

예를 들어, 기업의 IT 자산에 대한 접근을 확실하게 관리하기 위해서는 카메라와 중앙 집중식 모니터링 장치를 이용하여 데이터 센터 주변의 보안을 유지하는 것이 매우 중요합니다. 그러므로 은행, 소매점 또는 공공 기관 등과 같이 도난이나 사기 행위가 우려되는 조직들이라면, 모니터링, 분석 및 중앙 집중식 통제가 포함된 통합된 물리적 보안 검색 전략을 정의하고 구현해야 합니다. 이 접근법을 이용하면 기업들이 여러 가지 소스에서 핵심적인 데이터를 추출할 수 있으며 수동으로 모니터링하는 환경에서보다 더 신속하게 위협에 대응할 수 있습니다. 결과적으로 비용과 손실 위험을 줄일 수 있습니다.

그림 8에는 내용 요약과 함께 물리적 인프라 영역 내에서 해결해야 하는 몇 가지 추가적인 측면이 기술되어 있습니다.

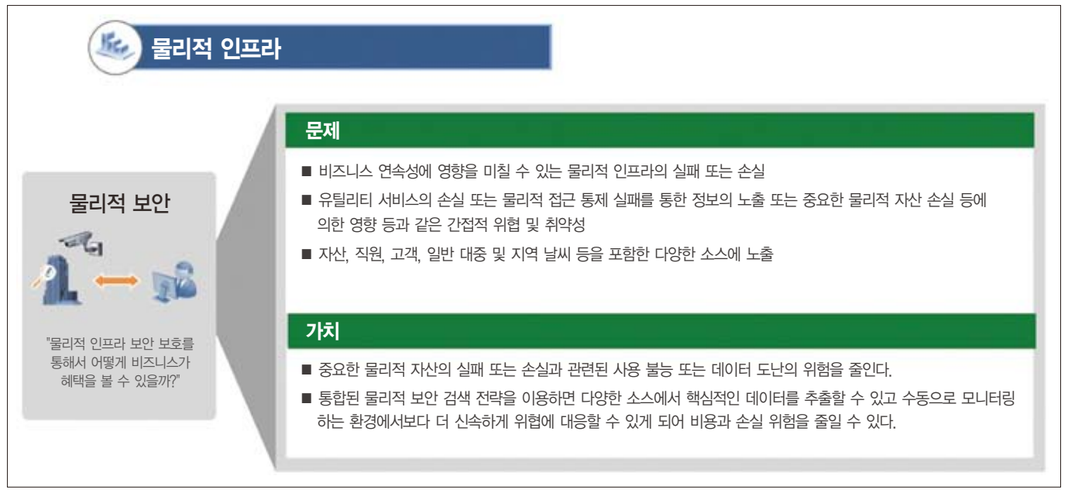

그림 8 물리적 인프라 영역

IT 보안 영역을 해결하고 비즈니스 솔루션에 매핑한 후에는 보다 더 기술적인 보안 아키텍처를 만드는 데 초점을 맞춰야 합니다. 다음은 사용자와 IT 보안 전문가들이 모든 영역과 환경 전반에 걸친 기초적인 서비스는 물론이고 모든 영역과 환경에서 사용할 수 있는 구조적 원칙을 식별할 수 있도록 안내하는 IBM Security Blueprint에 대해서 설명하겠습니다.

IBM Security Blueprint는 적용 가능한 모범 사례와 IT 표준을 강조합니다. 구체적인 솔루션을 구축하기 위해서는 구체적인 아키텍처, 설계 및 구현 과정을 거쳐야 합니다. IBM Security Blueprint는 이런 측면을 만드는 작업에 도움이 될 수는 있지만 이런 측면을 대체하는 것은 아닙니다.

IBM Security Blueprint

IBM Security Framework는 비즈니스 지향성 IT 보안을 여러 개의 영역으로 구분합니다. 다음 차례는 기업의 목표를 정의하고 구현할 수 있게 해주는 구조적 프레임워크를 구현하기 위해서 이런 영역을 심층적으로 분석하는 작업입니다. 이 구조적 프레임워크를 IBM Security Blueprint라고 합니다.

IBM Security Blueprint는 비즈니스 보안 요구 사항 또는 IBM Security Framework에 의해서 범주화된 우려사항에 대응하기 위해 필요한 보안 기능과 서비스를 범주화하고 정의하기 위해서 제품과 솔루션에 대해 관용적인 접근법을 사용합니다.

IBM Security Blueprint에서 IBM이 목표로 하는 것은 모든 도메인과 모든 도메인 전체에 포함된 기초적인 서비스에 대해서 유효한 구조적 원칙을 식별하는 것입니다. 또한 IBM Security Blueprint는 적용 가능한 모범 사례와 IT 표준을 강조합니다.

IBM Security Blueprint는 IBM Security Framework를 기반으로 IT 솔루션을 구축하는 방법에 초점을 맞추고 많은 고객 관련 시나리오에 대하여 연구한 결과를 기반으로 개발되었습니다. IBM Security Blueprint의 개발 의도는 사용자의 기업 내에서 보안 솔루션을 설계하고 배포하는 작업에 도움이 되는 로드맵으로 사용될 수 있게 하는 것입니다.

구체적인 솔루션을 구축하려면 구체적인 아키텍처, 설계 및 구현이 요구됩니다. IBM Security Blueprint를 이용하면 솔루션 구축이 쉬워집니다. 그러나 이런 것들을 대체할 수는 없습니다. 이 점에서 IBM Security Blueprint를 따라 작업을 진행하면 업계 최고의 모범 사례를 찾을 수 있고 그것을 기존의 보안 제품과 서비스에 매핑할 수 있습니다.

IBM은 IBM 서비스 지향성 아키텍처[5] 접근법을 기반으로 IBM Security Blueprint에 고도의 서비스 지향성 관점을 사용하고 있습니다. 서비스가 다른 서비스를 사용하고 정의합니다. 예를 들어, 정책 관리 및 접근 통제를 거의 모든 다른 서비스에 적용할 수 있습니다.

IBM Security Blueprint의 위치와 기능의 자세한 내용은 그림 9를 보십시오.

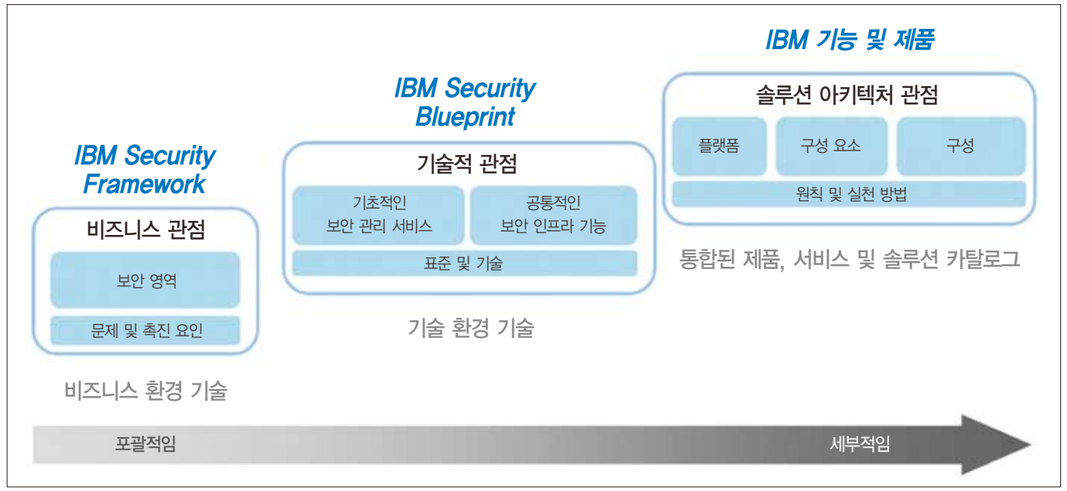

그림 9 IBM Security Blueprint 위치

이 도표의 왼쪽 부분은 앞의 11페이지에서 다루고 있는 "IBM Security Framework" 를 나타내며 보안 영역을 정의합니다. 이런 영역은 보안에 대한 비즈니스 관점을 나타냅니다.

그림 9의 중간 부분은 3개의 빌딩 블록으로 구성된 IBM Security Blueprint를 나타냅니다. 기초적인 보안 관리 서비스(Foundational Security Management Services)는 IBM Security Framework에서 설명한 필요한 기능을 개발하기 위해서 구현해야 하는 최고 수준의 보안 관리 서비스를 의미합니다. 이런 기초적인 보안 관리 서비스는 프레임워크에서 정의된 비즈니스 요구 사항이 이런 요구 사항을 충족하기 위해서 최고 수준의 IT 서비스로 변환되는 계층입니다. 이 지점에서 순수한 비즈니스 관점이 실질적인 IT 시스템으로 넘어서는 것입니다.

공통적인 보안 인프라 기능(Common Security Infrastructure features)에는 기초적인 보안 관리 서비스에서 최고 수준 서비스가 사용하는 인프라 요소와 서비스가 포함됩니다. 이 빌딩 블록은 기존 인프라와 시스템도 총망라하고 있습니다.

이런 2가지 IBM Security Blueprint 빌딩 블록은 모두 공개 표준 및 기술을 기반으로 합니다.

IBM Security Framework와 IBM Security Blueprint는 모두 구조적 원칙과 실천법을 따르는 플랫폼, 구성 요소 및 구성을 궁극적으로 기술하는 IT 솔루션 아키텍처 관점(IT Solution Architecture View)을 더 잘 설계할 수 있게 도와줍니다.

---

5 IBM Service-Oriented Architecture(서비스 지향성 아키텍처)에 대한 세부적인 설명은 IBM Redbooks® publication Understanding SOA Security Design and Implementation, SG24-7310에서 확인하실 수 있습니다.

그림 10에는 IBM Security Blueprint의 전체 구성이 표시되어 있습니다[6].

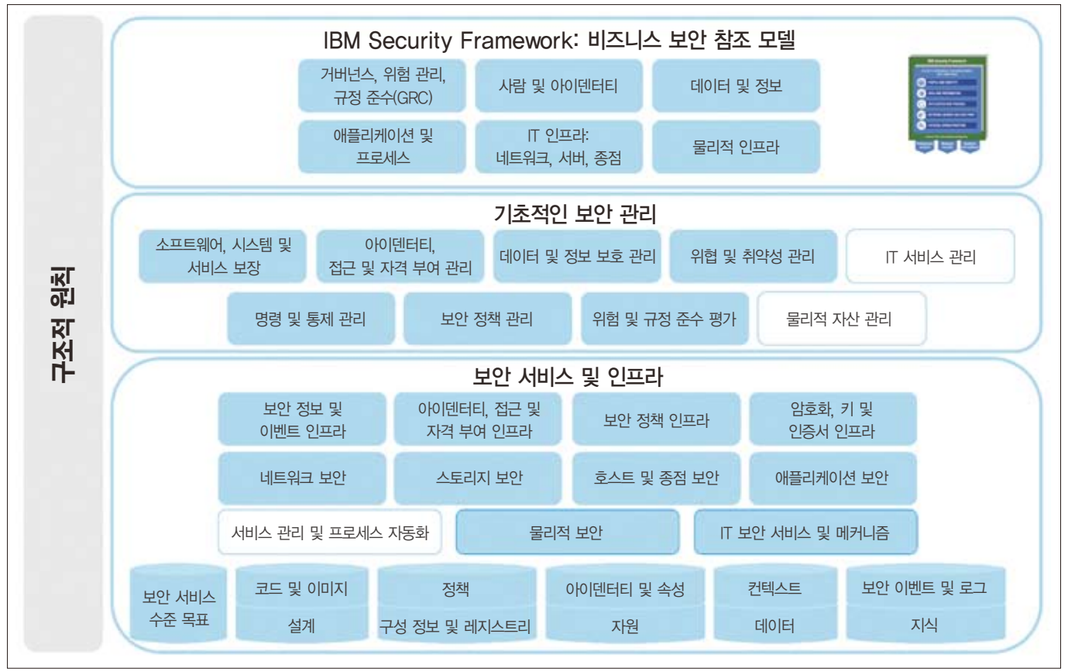

그림 10 IBM Security Blueprint

기초적인 보안 관리

기초적인 보안 관리 계층에는 IBM Security Framework에 직접 매핑이 가능한 최고 수준의 서비스가 포함되어 있습니다. 하위 계층에는 그 자체가 다음과 같은 IBM Redbooks 출판물[7]에 보다 구체적으로 설명되어 있는 여러 가지 개별적인 서비스와 링크된 서비스로 구성되어 있습니다.

- IBM Enterprise Security Architecture for People and Identity, SG24-7751
- IBM Enterprise Security Architecture for Governance, Risk and Compliance, SG24-7750
- IBM Enterprise Security Architecture for Data and Information, SG24-7752

21페이지의 그림 11에 표시된 것처럼 일련의 기초적인 보안 컨트롤이 폐쇄 루프 관리 시스템을 형성합니다.

---

6 이 다이어그램이나 다른 다이어그램에 표시된 흰 박스는 완전히 보안과 관련된 것이 아니지만 다른 IT 서비스 영역과 연결되어 있을 수 있는 서비스를 나타낸다.
7 이런 IBM Redbooks 출판물은 현재 준비 중에 있으며 2009년 하반기에 출판될 것이다.

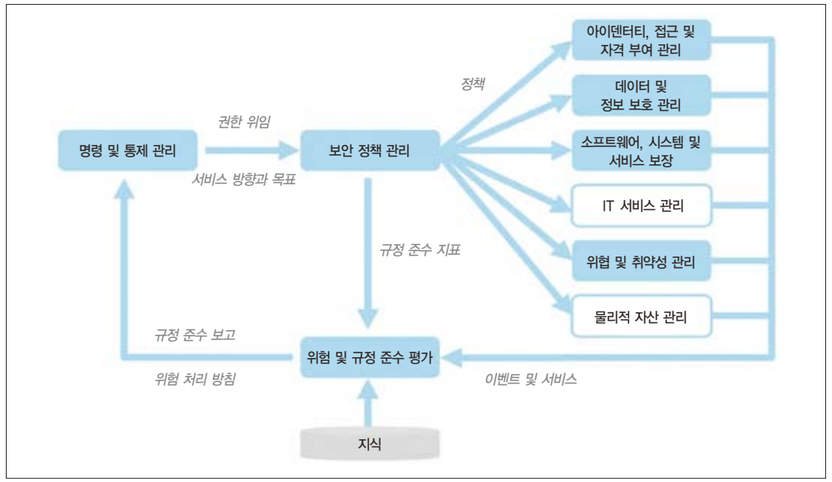

그림 11 기초적인 보안 컨트롤 폐쇄 루프

각각의 기초적인 보안 관리 컨트롤에 대해서 자세하게 살펴보겠습니다.

- 위험 및 규정 준수 평가(Risk and Compliance Assessment)를 사용하면 IT 조직이 조직 내 운영 위험에 영향을 미칠 수 있는 IT 관련 위험에 대한 식별, 정량화, 평가 및 보고서 작성을 위해서 보안 정보 및 보안 이벤트를 수집, 분석하고 그에 대한 보고서를 작성할 수 있습니다. 이 구성 요소는 위험 집합 및 보고서 작성(risk aggregation and reporting), IT 보안 위험 프로세스(IT security risk processes), 비즈니스 통제 관리(business controls management), 복구 및 연속성 관리(resiliency and continuity management), 규정 준수 보고서 작성(compliance reporting) 및 법률 검색 서비스(legal discovery services) 등을 담당합니다.

- 명령 및 통제 관리(Command and Control Management)는 보호, 대응, 연속성 및 복구를 위한 비IT 자산과 서비스용 운영 보안 기능(operational security capabilities)뿐만 아니라 보안 관리(security management)를 위한 명령 센터를 제공합니다. 명령 및 통제 관리는 물리적 보안 및 운영적 보안이 사무실, 자산, 사람, 환경 및 유틸리티에 대해서 유지되도록 보장하는 일과 사무실, 주변 및 영역에 대한 감시와 모니터링을 제공하는 일 그리고 출입 통제를 강화하는 일, 사람과 자산의 위치를 파악하고 추적하며 식별하는 일 및 연속성과 복구 동작을 위한 중점 부분을 제공하는 일 등과 같은 문제를 담당합니다.

- 보안 정책 관리(Security Policy Management)는 보안 정책을 작성, 발굴, 분석, 변환, 분배, 평가 및 강화할 수 있도록 모든 서비스와 레포지토리를 제공합니다.

- 아이덴터티, 접근 및 자격 부여 관리(Identity, Access, and Entitlement Management)는 역할과 아이덴터티, 접근 권한 및 권한 부여와 관련된 서비스를 제공합니다. 이런 서비스를 적절하게 사용하면 자원에 대한 접근이 적절한 시간에 적절한 ID에 적절한 목적으로 주어지게 할 수 있습니다. 이런 서비스를 사용하여 자원에 접근하는 활동을 모니터링하고 감사하여 불법적이거나 허용되지 않은 상태에서 사용하는 행위를 탐지할 수도 있습니다.

- 데이터 및 정보 보호 관리(Data and Information Protection Management)는 정보의 특성과 비즈니스 가치에 따라서 구조화된 데이터와 구조화되지 않은 데이터를 불법적인 접근으로부터 보호하는 서비스를 제공합니다. 사용 및 접근 모니터링 서비스 그리고 감사 서비스도 제공합니다.

- 소프트웨어, 시스템 및 서비스 보장(Software, System, and Service Assurance)은 전체 소프트웨어 생명 주기에 걸쳐서 소프트웨어, 시스템 및 서비스가 설계, 개발, 시험, 운영 및 유지되는 방식을 기술하여 예측할 수 있고 보안이 설정된 소프트웨어를 만들 수 있게 해 줍니다. 이 구성 요소는 구조화된 설계, 위협 모델링, 소프트웨어 위험 평가, 보안을 위한 설계 검토, 소소 코드 검토 및 분석, 소스 코드 통제 및 접근 모니터링, 코드/패키지 서명 및 확인, 품질 보장 시험 및 공급업체 및 타사 코드 확인 등을 담당합니다.

- IT 서비스 관리(IT Service Management)는 보안 관리를 위한 프로세스 자동화와 워크플로우 기초를 제공합니다. 특히, 변경 및 배포 관리(Change & Release Management) 프로세스는 보안 관리에서 중요한 역할을 담당합니다.

- 위협 및 취약성 관리(Threat and Vulnerability Management)는 배포된 시스템의 보안을 유지하기 위해서 배포된 시스템에서 취약성을 찾아내고 외부 소스로부터 취약성에 대한 보고서를 수신하며 적절한 대응 방법을 결정하고 적극적으로 현 상태를 개선하는 서비스를 제공합니다.

- 물리적 자산 관리(Physical Asset Management)는 물리적 자산의 위치 및 상태에 대한 인식과 함께 물리적 보안 통제에 대한 인식을 제공하며 물리적 시스템에 대한 보안 정보를 IT 보안 통제와 맞춥니다.

보안 서비스 및 인프라

- 보안 정보 및 이벤트 관리 인프라(Security Information and Event Management Infrastructure)는 로그 수집과 상관 관계 분석 과정을 자동화할 수 있는 인프라를 제공합니다. 보안 정보 및 이벤트 관리 인프라를 사용하면 기업들은 사고가 발생했을 때 자동으로 그것을 인식, 조사하고 대응할 수 있으며 보안 운영 및 정보 위험 관리 기능의 향상을 목표로 하여 사고 추적 및 처리를 일관화할 수도 있습니다.

- 아이덴터티, 접근 및 자격 부여 인프라(Identity, Access, and Entitlement Infrastructure)는 전체 디렉토리에 걸쳐서 사용자 정보에 대한 프로비저닝, 암호, 단일 로그인, 접근 통제 및 동기화를 위한 서비스를 제공합니다.

- 보안 정책 인프라(Security Policy Infrastructure)는 IT 시스템에 일관적인 방식으로 보안 정책을 개발하여 구현하는 과정을 관리하고 이런 보안 정책의 개발을 자동화하는 서비스를 제공합니다.

- 암호화, 키 및 인증서 인프라(Cryptography, Key, and Certificate Infrastructure)는 암호화 작업을 효율적으로 수행할 수 있는 서비스를 제공하고 암호화 키를 관리할 수 있는 운영 프로세스 및 기능을 제공합니다.

- 네트워크 보안(Network Security)은 심층적인 방어, 심도 있는 검사 및 프로토콜에 대한 분석, 애플리케이션 수준 페이로드를 제공하기 위한 다중 계층 네트워크 보안과 네트워크 규격 상 모든 수준에서 보호하기 위한 사용자 콘텐츠로 구성되어 있습니다. 네트워크 보안은 최신의 고도로 가상화된 환경을 위해서 가상 네트워크로 확장됩니다.

- 스토리지 보안(Storage Security)은 격리 및 암호화 기능을 통해서 사용, 전송 및 저장되어 있는 데이터를 보호하기 위한 데이터 중심 보안 기능을 제공합니다. 스토리지 보안은 스토리지 자산의 목록을 작성하고 분류하며 통제 정책을 스토리지 자산 목록과 연결하는 서비스도 제공합니다.

- 호스트 및 종점 보안(Host and Endpoint Security)은 호스트 및 네트워크 기반 기술을 이용하여 휴대 전화, 데스크톱 컴퓨터 및 휴대용 컴퓨터 등과 같은 서버 및 사용자 장치 등에 보호 기능을 제공합니다. 이 보호 기능은 가상화 인프라에 통합되어 가상 환경에도 보안 기능을 제공합니다. 호스트 및 종점 보안에는 악의적인 공격으로부터 보호하기 위해서 호스트 OS 및 시스템 리소스에 대한 하드웨어 기반 증명이 포함되어 있습니다.

- 애플리케이션 보안(Application Security)은 배포된 애플리케이션에 대한 테스트, 모니터링 및 감사를 위한 인프라를 제공합니다.

- 서비스 관리 및 프로세스 자동화(Service Management and Process Automation)는 사고, 문제, 변경 사항 및 구성 관리 등과 같은 서비스 관리 프로세스를 처리할 수 있는 인프라 서비스로 구성되어 있습니다. 프로세스 자동화는 보안 관련 활동을 포함하여 IT 활동을 자동화하기 위한 기본 프레임워크 기반 서비스입니다.

- 물리적 보안(Physical Security)은 물리적 보안에 대한 인식을 높이고 그런 인식을 IT 보안에 접목하기 위한 IT 인프라 서비스를 제공합니다. 여기에는 직원 명찰, RFID 판독기, 감시 시스템 및 관련 기술 또는 자산이 포함될 수 있습니다. 물리적 보안에는 감시, 움직임 감지, 물체 및 인체 식별 및 추적, 출입 통제, 환경 시스템 모니터링, 주변 컨트롤 및 전력 및 유틸리티 시스템 모니터링 등이 포함될 수 있습니다.

- IT 보안 서비스 및 메커니즘(IT Security Services and Mechanisms)은 IT 시스템이 보안 정보와 구성 정보를 수집할 수 있도록 도구를 제공합니다.

구조적 원칙

IBM 보안 아키텍트들은 서비스 분류와 함께 다음과 같은 구조적 원칙(Architectural Principles)을 정의했습니다. 이런 구조적 원칙은 모든 수준의 프레임워크, 블루프린트, 솔루션 설계에 적용할 수 있으며 IBM 제품 및 솔루션에 대한 지침으로 활용할 수도 있습니다.

- 개방성
  개방성은 엔터프라이즈 환경에서 매우 중요한 원칙입니다. 개방성에는 모든 주요 플랫폼, 런타임, 언어에 대한 지원과 주요 산업 표준, 공개된 인터페이스 및 알고리즘, 모호하지 않은 보안, 문서화된 신뢰 및 위협 모델에 대한 지원 그리고 공통적인 기준에 대한 지원과 유사한 공식 보안 검증 프로그램 등이 포함되어 있습니다.

- 기본적인 보안
  보안은 IT 솔루션에 있어서 최우선으로 갖춰야 할 사항이며 보안 정책은 제품을 구입함과 동시에 갖춰져 있어야 합니다. 기본적인 보안은 구성에 대한 일관적인 정의 및 관리, 제품 전체에 적용되는 일관적인 일련의 보안 역할과 사람과의 매핑, 일관적인 보안 관리 사용자 인터페이스 등을 사용함으로써 마련됩니다.

- 신뢰성을 위한 설계
  요즘과 같은 IT 환경의 경우에는 규정 준수 영역에 많은 요구 사항이 따르게 마련입니다. 모든 보안 관련 활동을 로그하고 감사하는 것이 중요합니다. 감사 인프라는 이런 이벤트를 처리할 수 있도록 확장성이 있어야 하며 감사 정보는 변할 수 없으며 거부할 수 없는 것이어야 합니다.

- 규제에 대한 설계
  IT 보안 프로젝트에서는 규제 사항으로 인해 여러 가지 많은 요구 사항이 발생합니다. 규제 사항은 시간이 지남에 따라서 변하게 마련입니다. 이런 규제 사항을 처리하기 위해서는 정부 규제에 의해 설정된 제한 사항과 산업 표준 그리고 규정, 표준 및 비즈니스 정책 그리고 그것들을 구현하기 위해 사용되는 보안 정책 간에 추적성 등을 유연하게 지원해야 합니다.

- 개인정보 보호를 위한 설계
  데이터가 공유되는 현재와 같은 IT 환경에서는 개인정보 보호의 중요성이 점점 더 커지고 있습니다. 솔루션은 신분을 확인할 수 있는 정보의 사용과 그에 상응하는 데이터 보호 메커니즘을 강조해야 하며 알림, 선택 및 접근의 원칙을 사용해야 합니다.

- 확장성을 위한 설계
  좋은 솔루션은 동일한 프레임워크 아래에서 다양한 메커니즘을 지원할 수 있도록 구성 요소를 기반으로 하며 메커니즘의 관리와 메커니즘 자체를 구분합니다. 이미 배포된 시스템은 기존 관리 프레임워크 내에 새로운 메커니즘이 추가되고 확장되는 것을 허용해야 합니다.

- 공유를 위한 설계
  여러 개의 솔루션이 공유된 서비스 센터 등과 같은 하나의 IT 환경을 공유할 수 있습니다. 이런 목표를 달성하기 위해서는 보안 서비스와 관리가 여러 개의 도메인으로 확장할 수 있어야 합니다. 각 도메인은 잠재적으로 자체적이고 독립적으로 보안 정책, ID, 모델 등을 제공하고 설정할 수 있습니다. 아키텍처는 통제 확장의 관점에서 생성된 추측과 제한 사항에 대해서 명시적으로 문서화해야 합니다.

▶ 소비성을 위한 설계.
모든 보안 서비스는 다양한 독자들이 쉽게 사용할 수 있어야 합니다. 다양한 독자에는 보안 정책과 기타 보안 서비스를 만들고 업데이트하며 관리하는 보안 서비스와 관리 시스템을 통해서 애플리케이션을 개발하고 통합하는 프로그래머와 보안 활동을 관리하고 감사하며 보호된 자원에 대한 접근 권한을 요청하는 사람들이 포함됩니다.

▶ 다단계 보호.
심층적인 방어(Defense in depth)는 일반적인 원칙이며 여러 수준의 강화와 보호를 통해서 성취할 수 있습니다. 자원은 설계할 때부터 방어의 첫 번째 계층으로서 스스로를 보호할 수 있도록 설계해야 합니다. 침입을 격리(isolation)와 구역(zoning)을 통해 막아낼 수 있습니다. 여러 수준을 이용하면 가장 외부에 있는 접근 가능 계층의 공격 표면을 최소화할 수 있습니다. 최소한의 권리(least privilege)는 유사한 기초적인 원칙입니다. 마지막으로 시스템에는 실패 미발생 원칙을 적용해야 합니다.

▶ 보안 관리, 강화 및 신뢰성의 분리
보안 관리 서비스(아이덴터티, 인증, 감사 등)는 일관적인 모니터링과 강화가 가능하도록 전용 및 공유 보안 인프라를 통해서 제공되어야 합니다. 강화(암호화, 정책 강화 또는 물리적 격리를 통한 강화) 자체는 일반적으로 리소스에 배포되어 폐쇄됩니다.

▶ 보안에 중요한 자원들은 자체의 보안 컨텍스트를 인식해야 합니다.
자원과 활동자는 자신의 환경(물리적 위치 및 논리적 위치 포함)과 보안 상태 및 컨텍스트를 인식하고 그 상태를 유지합니다.

▶ 모델 기반 보안.
모델은 아이덴터티 및 신뢰, 데이터, 정책, 애플리케이션, 보안 정보 및 이벤트 그리고 암호화 키에 운영 환경, 공통적인 모델 및 일관적인 형식을 반영합니다. 모델은 스택(예: 네트워크 ID는 애플리케이션 수준 ID에 연결되어 있음)과 유닛(예: 정책과 신뢰는 연합 내에서 협의되고 이해됨) 전체에서 일관적으로 해석됩니다. 모델은 현실(정책 및 모델 발견으로부터의 피드백)에 맞춰서 일관적으로 검증됩니다.

▶ 접근법, 메커니즘 및 소프트웨어 구성 요소의 일관성
하나의 자원에 대해서 2가지의 독립적인 보호 계층을 사용하면 보안이 향상될 수 있습니다. 그러나 2가지 자원에 대해서 동일한 목적으로 2가지 다른 메커니즘을 사용하면 둘 중 하나가 망가질 가능성이 높아집니다. 또한, 관리 노력도 더 많이 필요합니다.

IBM Security Blueprint에는 일반적으로 사용되는 표준과 메커니즘이 정리되어 있습니다.
여기에는 IBM Security Blueprint에 대한 개요도 포함되어 있습니다. 다음 섹션에서는 IBM Security Framework와 IBM Security Blueprint를 어떻게 적용하는 지에 대해서 보여주는 2가지 비즈니스 시나리오 예제에 대해서 설명하겠습니다.

비즈니스 시나리오

IBM Security Framework와 IBM Security Blueprint를 배포함으로써 어떤 혜택을 받을 수 있는 지 보여드리기 위해서 2가지 시나리오에 대해서 설명하겠습니다. 첫 번째 시나리오에서는 암호 관리 관련 비용을 절감하는 비즈니스 문제를 해결하는 것에 대해서 알아봅니다. 두 번째 시나리오에서는 폭넓은 범위의 IT 보안과 관련이 있는 PCI 규정 준수에 대해서 자세히 살펴보겠습니다.

암호 관리 관련 비용 절감

이 시나리오는 다음과 같은 섹션으로 구성되어 있습니다.
▶ 암호 관련 비용 절감에 대한 비즈니스 컨텍스트
▶ 문제 기술 및 요구 사항
▶ IBM Security Framework 매핑
▶ IBM Security Blueprint 서비스

암호 관련 비용 절감에 대한 비즈니스 컨텍스트

현재, 애플리케이션과 시스템을 사용하는 사용자들은 점점 더 그 수가 늘고 있는 ID와 암호 쌍을 관리해야 합니다. 규정과 정책(숫자와 알파벳이 아닌 문자를 포함하고 특정한 문자 수 이상으로 지정하는 것 등)을 통해서 이런 암호는 복잡하게 지정해야 하고 단기간 내에 다른 것으로 변경하도록 요구되고 있습니다. 그렇기 때문에 사용자가 암호를 잊어버렸거나 제 시간에 암호를 재설정하지 않는 경우에 생산성 저하의 원인이 되기도 합니다. 암호를 재설정하는 업무는 헬프 데스크 기능의 주요 활동 중 하나이며 한 번의 전화 요청을 해결하기 위해서 평균 25달러의 비용이 소요되고 전체 통화량의 40%까지 차지하고 있습니다. 암호 재설정과 관련된 통화의 양을 크게 줄일 수 있다면 비용도 크게 절감할 수 있을 것입니다.

생산성 저하를 유발하는 또 다른 요소는 사용자들이 별도의 다른 애플리케이션이나 시스템에 액세스할 때는 항상 사용자의 신용장을 제공해야 한다는 사실입니다. 제한 시간이 다 되어서 사용자의 세션이 만료된 경우도 마찬가지입니다.

문제 기술 및 요구 사항

비즈니스 컨텍스트에서 설명한 것처럼 우리의 목표는 암호와 관련된 헬프 데스크 통화의 양을 줄이고 암호와 관련된 지체 시간을 줄임으로써 사용자의 생산성을 향상시키는 것입니다. 또 다른 내재된 요구 사항은 관련된 애플리케이션과 솔루션 시스템이 현재의 보안 수준을 유지해야 한다는 것입니다. 암호 관련 문제를 해결하기 위해서 인증 메커니즘의 강도를 낮추거나 제거하는 것은 절대로 솔루션이 될 수 없습니다.

현 시점에서 우리는 우리의 문제를 해결할 수 있는 솔루션에 다가가기 위해서 2가지 가능한 논거에 대해서 명확하게 생각해 볼 수 있습니다.

▶ 단일 로그인 접근법을 이용하면 사용자들이 하나의 독립적인 인증 프로세스를 이용하는 여러 가지 별도의 시스템을 더 편리하게 이용할 수 있다.
▶ 암호 재설정 셀프 서비스 기능을 이용하면 사용자들이 스스로 새로운 암호를 요청할 수 있기 때문에 헬프 데스크의 통화량을 줄일 수 있다.

이 솔루션을 위해서 필요한 구조적 빌딩 블록과 기초적인 서비스에는 어떤 것들이 있는가? 투자 대비 효과를 극대화하기 위해서 비즈니스 솔루션을 위해 필요한 모든 IT 시스템을 어떻게 식별하고 연관 지을 수 있는가? IBM Security Framework와 IBM Security Blueprint를 사용하면 어느 곳에서 어떻게 도움이 되는지에 대해서 자세히 살펴보겠습니다.

IBM Security Framework 매핑

11페이지의 "IBM Security Framework"와 보안 영역과 관련된 다음과 같은 내용에 대해서 연구한 끝에 우리는 사람과 아이덴터티(People and Identity) 영역에 초점을 맞추기로 결정했습니다. 우리의 문제 기술은 애플리케이션에 접근하기 위해서 인증하고 권한을 요청하며 동시에 개인 정보(이 경우에는 암호)를 유지하는 사용자와 관련된 내용입니다. 그림 12에 정리되어 있습니다.

사람과 아이덴터티 영역에 즉각 일치하는 것이 있을 수 있다고 하더라도 혹시 부분적으로 일치하는 것이 있는지 여부를 확인하기 위해서 다른 IBM Security Framework 영역도 주의를 기울이며 고려하는 것이 중요합니다. 그러나 이 경우에는 데이터 및 정보, 애플리케이션 및 시스템, 물리적 인프라, 보안 거버넌스, 위험 관리 및 규정 준수, 네트워크, 서버 및 종점 등과 같은 다른 영역은 당연히 제외해도 됩니다. 여러분이 어떤 이유로 특정 측면을 고려하고 다른 측면을 제외하는 지에 대해서 일관적으로 문서화하는 것이 좋습니다.

그림 12 IBM Security Framework 매핑

IBM Security Blueprint 서비스

사람과 아이덴터티 영역에 초점을 맞출 것이기 때문에 이제 다음 단계는 블루프린트를 세부적으로 검토하는 것입니다. IBM Security Blueprint에서 각각의 IBM Security Framework 도메인에 대해서 관련된 서비스를 연결할 수 있습니다. 이 내용은 27페이지의 그림 13에 기술되어 있습니다. 그림에는 사람과 아이덴터티 영역과 관련된 서비스가 파란색으로 표시되어 있습니다.

2가지 기초적인 보안 관리 서비스(아이덴터티, 접근 및 자격 부여 관리(Identity Access and Entitlement Management) 및 보안 정책 관리(Security Policy Management))가 중간 계층에 표시되어 있습니다. 암호 관리와 관련된 문제와 작업은 보안 정책과 관련이 없기 때문에 대부분이 첫 번째 영역에 속합니다. 사람과 아이덴터티 영역과 관련된 보안 서비스 및 인프라(Security Services and Infrastructure)는 도표의 아래 부분에 표시되어 있습니다. 복잡하지 않게 하기 위해서 이 안내서에서는 더 이상 세부적으로 분석하지 않겠습니다.

참고: 아이덴터티 생명 주기 관리 내의 일부 작업은 저장되어 있을 때와 전송될 때에 보호되어야 하는 암호 또는 디지털 인증서 같은 개인 식별 정보(PII)의 수집과 비밀의 발행 작업과 관련되기 때문에 보다 전형적인 실제 배포 상황에서는 데이터 및 정보 보호 관리(Data and Information Protection Management)를 강조하는 것을 고려하고자 할 수도 있습니다. 다시 한 번 강조하지만, 어떤 이유로 특정 측면을 고려하고 다른 측면을 제외하는 지에 대해서 일관적으로 문서화하십시오.

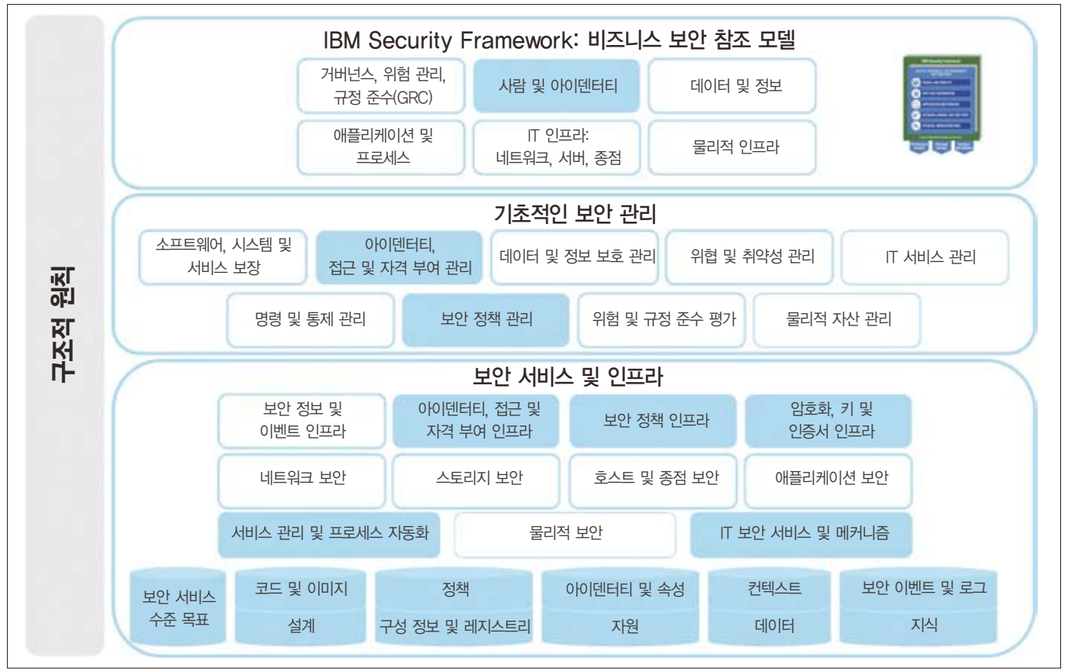

그림 13 사람과 아이덴터티 영역에 초점을 맞춘 IBM Security Blueprint

예를 들어, 그림 14처럼 아이덴터티, 접근 및 자격 부여 관리(Identity, Access and Entitlement Management) 서비스는 더 세부적으로 분해할 수 있습니다. 이렇게 더 세부적인 내용을 이용하면 사용자의 요구 사항을 해결하기 위한 완벽한 아키텍처를 디자인할 수 있습니다.

그림 14 아이덴터티, 접근 및 자격 부여 관리에 대한 IBM Security Blueprint 세부 사항

2가지 솔루션 접근법을 세밀하게 관찰하고서 우리는 25페이지의 "문제 기술 및 요구 사항" 에 단일 로그인 및 셀프 서비스 암호 재설정을 정의했습니다. 적용 가능한 블루프린트 서비스는 그림 14에서 찾을 수 있습니다.

셀프 서비스 암호 재설정 기능은 아이덴터티 생명 주기 서비스(Identity Lifecycle services)의 일부분입니다. 아이덴터티 생명 주기 서비스에는 아이덴터티 발행(Identity Issuing), 아이덴터티 프로비저닝(Identity Provisioning), 아이덴터티 재인증(Identity Recertification) 및 아이덴터티 폐기(Identity Revocation)가 포함됩니다. 이런 기능은 대부분의 아이덴터티 관리 솔루션이 제공하는 주요 기능들입니다.

단일 로그인 기능은 자체적인 서비스로 구현되며 신뢰 정보 관리(Credential Management)와 관련된 일련의 서비스의 일부입니다. 또한 단일 로그인 기능은 기존 인증 서비스와 통합되어야 하기 때문에 인증(Authentication) 서비스와 긴밀하게 관련되어 있습니다. 인증은 보안 서비스 및 인프라(Security Services and Infrastructure) 계층에 위치하고 있습니다.

이 시나리오에서 다음 단계는 보안 정책 관리 서비스와 그 블루프린트를 세부적으로 검토하는 작업입니다. 복잡해지는 것을 피하기 위해서 우리는 지금 이 단계를 거치지 않습니다.

이 분해 연습을 통해서 사용자는 사용자의 솔루션에 필요한 구조적 빌딩 블록과 기초적인 서비스를 더 일관적으로 정의할 수 있게 됩니다. 이 연습을 통해서 투자 효과를 극대화할 수 있도록 사용자의 비즈니스 솔루션에 필요한 모든 IT 시스템을 식별하고 연관 지을 수 있는 방법에 대한 개요를 볼 수 있습니다. 그렇게 하는 과정에서 사용자는 현재 간과되고 있는 시스템과 서비스도 발견할 수 있습니다. 여러분이 내리는 결정 사항을 일관적으로 문서화하면 올바른 결정을 하는 데 도움이 되며 충분한 조사를 수행할 수 있습니다.

다음 단계에는 구체적인 솔루션 아키텍처, 설계 및 구현을 구축하는 작업이 포함됩니다. 이 디자인과 구조적 원칙 그리고 업계 최고의 모범 사례를 따르면 적절한 보안 제품과 서비스를 선택할 수 있습니다.

이제 다른 예제를 살펴보겠습니다.

PCI DSS 규정 준수 필요성 충족

이 시나리오는 다음과 같은 섹션으로 구성되어 있습니다.

- ▶ PCI DSS 규정 준수 필요성을 충족하는 것에 대한 비즈니스 컨텍스트
- ▶ 문제 기술 및 요구 사항
- ▶ IBM Security Framework 매핑
- ▶ IBM Security Blueprint 서비스

PCI DSS 규정 준수 필요성을 충족하는 것에 대한 비즈니스 컨텍스트

주요 카드 지불 제공업체들이 함께 협력하여 일련의 데이터 보안 표준을 개발했고 그 데이터 보안 표준을 강화하기 위한 위원회도 만들었습니다. Payment Card Industry Data Security Standard[8] (PCI DSS)가 전 세계적으로 통용되는 요구 사항이 되긴 했지만 아직도 준수하지 않는 기업이 있습니다. 많은 기업들은 규제 사항 준수가 어렵고 혼란스런 영역이라고 생각하고 있으며 PCI DSS를 준수하는 것을 또 하나의 짐으로 생각하고 있습니다.

그러나, IBM은 많은 기업들이 PCI 표준을 기회가 될 수 있다고 생각하고 있습니다[9]. 이 표준은 아주 잘 디자인되어 있기 때문에 위험 관리 전략을 발전시키는 데 있어서 기초 역할을 실질적으로 수행할 수 있습니다.

8 PCI Security Standards Council은 신용카드 데이터 보호를 위한 보안 표준의 지속적인 개발, 강화, 보관, 보급 및 구현을 추진하는 개방적인 글로벌 포럼입니다. 웹 사이트(https://www.pcisecuritystandards.org/)에서 이 포럼에 대한 자세한 정보를 보실 수 있습니다. .

이 시나리오에서 외부 규정에 의한 규정 준수 요구 사항과 관련하여 비즈니스 상황에 대해서 생각해 보겠습니다. 우선 간단하게 PCI DSS 표준과 IBM Security Framework 및 IBM Security Blueprint를 이용하여 PCI DSS 표준을 준수할 수 있는 방법에 대해서 설명하겠습니다.

신용카드 정보를 전송, 처리 또는 저장하는 모든 기업은 반드시 이 표준을 따라야만 합니다. 이 표준에 대한 준수 의무는 PCI Security Standards Council에서 강제하는 것이 아니라 개별적인 신용카드 회사에서 강제하는 것입니다.

이 시나리오에서는 상점 또는 서비스 제공업체의 관점에서 PCI 규정 준수에 대해서 설명하겠습니다. 상점 또는 서비스 제공업체는 신용카드를 받고 카드 소지자에게 서비스를 제공하는 측입니다.

문제 기술 및 요구 사항

상점 또는 서비스 제공업체가 신용카드 업계로부터 PCI-DSS 표준[10]을 따르라는 요청을 받습니다. 상점 또는 서비스 제공업체의 유형에 따라서 자가 진단 설문지를 이용하여 수행하거나 공인된 보안 평가자에 의해 수행됩니다.

한 눈에 볼 수 있도록 구체적인 요소가 정의되는 기본적인 원칙과 부가적인 요구 사항을 정리해 보겠습니다.

- ▶ 보안이 유지되는 네트워크를 구축하고 유지하라.
  요구 사항 1: 카드 소유자 데이터를 보호하기 위해서 방화벽을 설치하고 구성을 유지하라.
  요구 사항 2: 시스템 암호와 기타 보안 매개 변수로 제품 공급업체의 기본값을 사용하지 마라.

- ▶ 카드 소유자 데이터를 보호하라. 요구 사항 3: 저장된 카드 소유자 데이터를 보호하라.
  요구 사항 4: 개방된 공중 네트워크에서 카드 소유자 데이터를 전송할 때는 암호화하라.

- ▶ 취약성 관리 프로그램을 유지하라.
  요구 사항 5: 안티바이러스 소프트웨어를 사용하고 주기적으로 업데이트하라.
  요구 사항 6: 보안이 유지되는 시스템과 애플리케이션을 개발하고 유지하라.

- ▶ 강력한 접근 통제 방법을 구현하라.
  요구 사항 7: 상업적으로 접근하는 자가 카드 소유자 데이터에 접근하지 못하게 제한하라.
  요구 사항 8: 컴퓨터에 접근하는 모든 사람에게 고유한 ID를 지정하라.
  요구 사항 9: 카드 소유자 데이터에 대한 물리적 접근을 제한하라.

- ▶ 네트워크를 주기적으로 모니터링하고 테스트하라.
  요구 사항 10: 네트워크 리소스와 카드 소유자 데이터에 접근하는 모든 사항을 추적하고 모니터링하라.
  요구 사항 11: 보안 시스템과 프로세스를 주기적으로 테스트하라.

- ▶ 정보 보안 정책을 유지하라.
  요구 사항 12: 정보 보안 문제를 해결할 수 있는 정책을 유지하라.

위에 기술된 원칙에서 보듯이, PCI DSS는 정보 보안 원칙의 많은 부분을 아우르는 표준입니다.

9 IBM의 백서인 Profiting from PCI compliance (December 2007)에서 IBM은 PCI 규정 준수와 관련하여 설계된 전략을 수립함으로써 얻을 수 있는 효율성에 대해서 살펴보았습니다. 이 백서는 ftp://ftp.software.ibm.com/software/tivoli/whitepapers/GTW01773-USEN-00.pdf에서 보실 수 있습니다.

10 PCI DSS 표준은 누구나 이용할 수 있으며 자세한 내용은 https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml에서 보실 수 있습니다.

IBM Security Framework 매핑

Because meeting PCI DSS 규정 준수를 충족시키는 것이 외부 규정에 의해 강제되는 것이기 때문에 우리는 보안 거버넌스, 위험 관리 및 규정 준수 영역을 세부적으로 조사해야 한다는 것을 알고 있습니다. 그러나 다시 한 번 다른 모든 IBM Security Framework 영역도 고려해야 합니다. 31페이지의 그림 15에는 IBM Security Framework의 적용 가능한 영역이 표시되어 있습니다.

그림 15 IBM Security Framework mapping

PCI DSS가 폭넓게 적용할 수 있는 IT 보안 표준이기 때문에 PCI DSS 규정 준수 요구 사항에 관해서 모든 IBM Security Framework 영역을 조사하고 문서화해야 한다는 사실은 별로 놀라운 일이 아닙니다.

표 1에는 IBM Security Framework 영역에 대한 고수준 PCI DSS 원칙의 매핑이 기록되어 있습니다.

표 1 PCI DSS 원칙의 IBM Security Framework에 대한 매핑

PCI DSS 원칙	IBM Security Framework 영역
보안 네트워크를 구축하고 유지하라.	IT 인프라 그리고 네트워크, 서버 및 종점
카드 소유자 데이터를 보호하라.	데이터 및 정보, 애플리케이션 및 프로세스
취약성 관리 프로그램을 유지하라.	IT 인프라 그리고 네트워크, 서버 및 종점
강력한 접근 통제 방식을 구현하라.	사람 및 아이덴터티
네트워크를 주기적으로 모니터링하고 테스트하라.	IT 인프라 그리고 네트워크, 서버 및 종점
정보 보안 정책을 유지하라.	보안 거버넌스, 위험 관리 및 규정 준수

IBM Security Blueprint 서비스

PCI DSS에 의해 정의된 보안 원칙에는 많은 요구 사항이 포함되어 있고 다시 이 요구 사항은 더 세부적인 요구 사항과 필요한 보고서 작성 기능으로 구성되어 있습니다.

표 2에는 PCI DSS 요구 사항이 기록되어 있고 IBM Security Blueprint 하위 계층에 매핑되어 있습니다. 이 연습을 하면 더 세부적으로 조사해야 하는 필요한 모든 IT 보안 서비스를 찾는 데 도움이 됩니다.

표 2 PCI DSS 요구 사항의 IBM Security Blueprint에 대한 매핑

PCI DSS 요구 사항	Security Blueprint 하위 계층
카드 소유자 데이터를 보호하기 위해서 방화벽을 설치하고 구성을 유지하라.	▶ 위협 및 취약성 관리 ▶ 네트워크 보안 ▶ 호스트 및 종점 보안
시스템 암호와 기타 보안 매개 변수로 제품 공급업체가 제공한 기본값을 사용하지 마라.	▶ 소프트웨어, 시스템 및 서비스 보장 ▶ 네트워크 보안 ▶ 호스트 및 종점 보안
저장된 카드 소유자 데이터를 보호하라.	▶ 보안 정책 관리 ▶ 데이터 및 정보 보호 관리 ▶ 암호화, 키 및 인증서 인프라 ▶ 스토리지 보안 ▶ 아이덴터티, 접근 및 자격 부여 관리
공개된 공중 네트워크에서 카드 소유자 데이터를 전송할 때는 암호화하라.	▶ 보안 정책 관리 ▶ 암호화, 키 및 인증서 인프라 ▶ 네트워크 보안
안티바이러스 소프트웨어를 사용하고 주기적으로 업데이트하라.	▶ 위협 및 취약성 관리
보안이 유지되는 시스템과 애플리케이션을 개발하고 유지하라.	▶ 소프트웨어, 시스템 및 서비스 보장 ▶ 애플리케이션 보안 ▶ 아이덴터티, 접근 및 자격 부여 관리 ▶ 데이터 및 정보 보호 관리 ▶ 변경 및 배포 관리 ▶ 스토리지 보안 ▶ 위협 및 취약성 관리
상업적으로 접근하는 자가 카드 소유자 데이터에 접근하지 못하도록 제한하라.	▶ 아이덴터티, 접근 및 자격 부여 관리 ▶ 애플리케이션 보안
컴퓨터에 접근하는 모든 사람에게 고유한 ID를 지정하라.	▶ 아이덴터티, 접근 및 자격 부여 관리
카드 소유자 데이터에 대한 물리적 액세스를 제한하라.	▶ 물리적 보안 ▶ 물리적 자산 관리
네트워크 리소스 및 카드 데이터에 대한 모든 액세스를 추적하고 모니터링하라.	▶ 네트워크 보안 ▶ 보안 정보 및 이벤트 인프라
보안 시스템과 프로세스를 주기적으로 테스트하라.	▶ 네트워크 보안 ▶ 위협 및 취약성 관리 ▶ 소프트웨어, 시스템 및 서비스 보장 ▶ 위험 및 규정 준수 평가 ▶ IT 서비스 관리 ▶ 호스트 및 종점 보안
정보 보안 정책을 유지하라.	▶ 위험 및 규정 준수 평가 ▶ 아이덴터티, 접근 및 자격 부여 관리 ▶ 사건 관리 ▶ IT 서비스 관리 ▶ 보안 정책 관리 ▶ 명령 및 통제 관리

이것으로 간단한 2가지 비즈니스 시나리오에 대한 검토를 마치겠습니다. 개별적인 비즈니스 및 기술적 요구 사항에 따라서 IBM Security Framework와 IBM Security Blueprint 서비스를 매핑하는 방법을 설명했습니다.

요약

이 IBM Redguide 안내서에서 우리는 비즈니스와 기업의 운영 보안 설계에 영향을 미칠 수 있는 IT 관련 촉진 요인에 대해서 설명했습니다. 위험 관리와 같은 중요한 IT 보안 원칙에 대해서 간략하게 설명했으며 비즈니스와 IT 관련 촉진 요인으로부터 고안된 추가적인 보안 계층을 소개했습니다. 또한 IT 보안 문제를 해결하는 데 있어서 가장 일반적으로 사용되고 있는 2가지의 접근법에 대해서도 설명했습니다.

IT 보안이 건전한 비즈니스 운영을 위한 하나의 수단임을 이해하고 우리는 IBM Security Framework와 IBM Security Blueprint를 소개했습니다. IBM Security Framework와 IBM Security Blueprint는 기업 전체에 적용되는 전체적인 솔루션을 위한 생각과 프로세스를 통합할 수 있도록 보안에 대한 비즈니스 관점과 IT 관점 사이의 차이를 메워줍니다.

IBM Security Framework와 IBM Security Blueprint는 모두 궁극적으로 구조적 원칙과 실천 방법을 따라서 플랫폼, 구성 요소 및 구성을 기술할 수 있는 IT 솔루션 아키텍처 관점을 구현할 수 있도록 설계되었습니다.

이 분야의 모든 IBM 제품에 대한 소개와 구조적 개요를 포함하여 엔터프라이즈 보안에 대한 IBM의 접근법을 이해하기 위해서는 "추가 정보를 얻을 수 있는 기타 리소스"에 정리되어 있는 IBM Enterprise Security Architecture에 대한 IBM Redbooks 출판물을 참조하십시오.

추가 정보를 얻을 수 있는 기타 리소스

IBM Security Framework와 IBM Security Blueprint에 대한 자세한 정보와 두 제품이 어떤 식으로 IBM 보안 제품과 연관되는 지에 대해서 알아보시려면 다음과 같은 IBM Redbooks 출판물[11]을 참조하십시오.

- IBM Enterprise Security Architecture for People and Identity, SG24-7751
- IBM Enterprise Security Architecture for Governance, Risk and Compliance, SG24-7750
- IBM Enterprise Security Architecture for Data and Information, SG24-7752

IBM Security Framework에 대한 입문서는 다음 웹 사이트에서 찾아보실 수 있습니다.

http://www.ibm.com/security/outlook.html

IBM Security Framework가 사용되고 있는 보안된 클라우드 컴퓨팅(Securing Cloud Computing)에 대한 가트너 그룹의 문서도 읽어보십시오.

http://mediaproducts.gartner.com/gc/webletter/ibm_stg/issue3/article2.html

다음 사이트에서 인터렉티브한 IBM 보안 커뮤니티에 참여해 보십시오.

https://www.ibm.com/communities/service/html/communityview?communityUuid=0629bb73a904-45b1-86d1-20374d1f1c3e

11 이런 IBM Redbooks 출판물은 현재 준비 중에 있으며 2009년 후반기에 출판될 것입니다. IBM은 모든 IBM Security Framework 도메인을 설명하는 일련의 IBM Redbooks 출판물을 출판할 것입니다.

단일 로그인 솔루션 문제를 해결하는 IBM의 제품에 대한 자세한 내용을 보시려면 백서인 Addressing single sign-on inside, outside, and between organizations, December 2008를 참조하십시오. 백서는 다음 사이트에서 찾아보실 수 있습니다.

ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/tiw14018usen/TIW14018USEN.PDF

PCI DSS 솔루션용 IBM 제품에 대한 자세한 정보는 다음 사이트에서 찾아보실 수 있습니다.

http://www.ibm.com/software/tivoli/governance/security/pci.html

이 문서를 제작한 팀

이 IBM Redguide 출판물은 오스틴 센터의 International Technical Support Organization에서 근무하는 다양한 국적의 전문가들로 이뤄진 팀이 제작했습니다. 이 출판물의 저작은 IBM Enterprise Security Architecture에 대한 세 가지 IBM Redbooks 출판물 중에서 첫 번째 단계의 일환입니다.

Axel Buecker는 오스틴 센터의 International Technical Support Organization에서 근무하는 공인 컨설팅 소프트웨어 IT 전문가입니다. Alex는 소프트웨어 보안 아키텍처 및 네트워크 컴퓨팅 기술 분야에 대한 다양한 저술 활동을 하고 있으며 전 세계의 IBM 교실에서 학생들을 가르치고 있습니다. Alex는 독일의 브레멘 대학에서 컴퓨터 공학 학위를 받았으며 워크스테이션 및 시스템 관리, 네트워크 컴퓨팅, e-비즈니스 솔루션과 관련된 다양한 분야에서 22년 동안 풍부한 경험을 쌓았습니다. Alex는 2000년 3월에 ITSO에 참여했으며 그 전에는 독일의 IBM에서 소프트웨어 보안 아키텍처 분야의 수석 IT 전문가로 근무했습니다.

David Crowther는 IT 업계에 30년이 넘게 몸담고 있으며 IBM에서 23년 동안 일하고 있습니다. 그는 IBM에 몸담고 있는 동안 기술 사전 판매, 서비스 및 지원 분야에서 일했으며 현재는 IBM의 BetaWorks에서 일하고 있습니다. David은 BetaWorks에서 Tivoli® Security 및 Provisioning 제품의 초기 베타 프로그램을 관리하고 있습니다. 또한, 가능화 워크숍을 운영하고 기술 지원을 제공하며 새로운 제품에 대한 주제 전문가로 활동하고 있습니다. David은 대형 시스템, 네트워킹, 보급력이 높은 제품, Lotus®, 보이스 및 WebSphere®를 포함하여 여러 가지 다른 IBM 브랜드의 제품에 대한 베타 프로그램 실행과 제품 지원 분야에서 폭넓은 경험을 갖고 있습니다. David은 컨설팅 IT 전문가이며 공인된 IT 전문가이고 공인된 엔지니어입니다. 그는 캠브리지 대학에서 전자 공학 석사 학위를 취득했습니다.

Foulques de Valence는 IBM Systems Lab Services팀의 보안 및 웹 IT 아키텍트 회원입니다. 그는 미국과 기타 여러 국가에서 다국적 기업과 포춘 500대 기업을 대상으로 컨설팅 서비스를 제공하고 있습니다. 그의 전문 분야는 보안, SOA, WebSphere 제품 그리고 IBM System z®인프라입니다. Foulques는 여러 가지 IBM 보안 솔루션에 대한 출판물을 공동 저술했습니다. 또한 보안에 대해서 학생들을 가르치기도 하고 국제 회의에서 연설을 하기도 합니다. 이전에는 IBM France에서 SOA, J2EE™ 및 z/OS®를 전문 분야로 하는 IT 아키텍트로 근무했습니다. 그는 프랑스의 Ensimag에서 컴퓨터 공학 및 엔지니어링 분야에서 석사 학위를 취득했습니다. 그는 미국 버펄로에 있는 뉴욕 주립대와 캘리포니아에 있는 스탠포드 대학에서 학업을 계속 했습니다.

Guilherme Monteiro는 브라질의 IBM 비즈니스 파트너인 Companhia de Sistemas에서 근무하는 IT 보안 아키텍트이며 그의 전문 분야는 보안 솔루션입니다. 그는 1999년부터 IBM 보안 솔루션에 관여했으며 디렉토리, 액세스 관리, ID 관리, 디렉토리 통합, 위험 관리를 구현하고 주요한 브라질 기업들을 위해서 고객 맞춤형 솔루션을 개발하고 있습니다. 그가 소속되어 있는 회사는 Linux®보안 솔루션에도 확고한 전문성을 보유하고 있으며 이 플랫폼에 대한 여러 건의 성공적인 구현 사례를 통해서 풍부한 경험을 축적하고 있습니다.

Michel Oosterhof는 네덜란드에 있는 IBM Tivoli Software에서 수석 IT 전문가로 일하고 있습니다. 그는 IT 업계에 11간 몸담고 있습니다. 그는 University of Twente에서 응용 물리학 분야에서 석사 학위를 취득했습니다. ID 및 액세스 관리도 그의 전문 분야 중 하나입니다. 그는 현재 Tivoli 보안 제품을 위한 기술 세일즈 전문가로 일하고 있습니다.

Andrew Quap은 텍사스의 오스틴에 있는 IBM Software Group에서 소프트웨어 엔지니어로 근무하고 있습니다. 그는 IBM 보안 제품과 관련된 업무에 10년 이상 매진했으며 현재는 Tivoli Federated Identity Manager 제품을 위한 수준 2 기술 수석으로 일하고 있고 Tivoli Access Manager, Tivoli Access Manager for OS, Tivoli Security Policy Manager 및 Virtual Member Manager 구성 요소를 지원하는 팀에서 근무하고 있습니다. 그는 고객에게 관리된 베타 프로그램을 안내하는 소개용 자료를 만들었습니다. 그는 오스틴에 있는 텍사스대에서 전기 컴퓨터 엔지니어링 분야에서 학사 학위를 취득했습니다.

Maria Schuett는 미국, 미네소타주의 세인트폴에 소재한 IBM 비즈니스 파트너인 AdminWorks, Inc.에서 보안 아키텍트로 근무하고 있습니다. Maria는 정보 보안 및 기술 분야에 15년 이상 경험을 쌓고 있습니다. 그녀는 2004년부터 IBM Tivoli Security 솔루션에 관여했으며 구체적으로 주정부, 보건 당국 및 보험 업계에 솔루션을 제공하면서 2000년부터 IBM Tivoli Access Manager for e-business와 관련된 업무를 담당하고 있습니다. 그녀는 동부 미시건 대학에서 컴퓨터 공학 학사 학위를 취득했고 스쿨크레프트 컬리지에서 엔지니어링 분야 준학사 학위를 취득했습니다. ITIL과 Archer SmartSuite®Framework for GRC 등이 그녀의 전문 분야입니다. 그녀는 고객들을 위해서 Tivoli Identity and Access Manager with ITIL에 대한 지원을 포함하여 인프라 복원력 전략에 대한 백서를 저술했습니다.

Kai Stockmann은 IBM Germany에서 IT 보안 전문가로 근무하고 있습니다. 그는 독일에서 5년 동안 보안 능력(Security Competency)과 관련된 업무를 수행했습니다. 그 곳에서 그는 규정 준수 및 규제 프로그램을 담당하는 책임 아키텍트 역할을 수행하고 있습니다. 이 역할을 수행하면서 그는 보안과 규정 준수 분야에 많은 경험을 쌓았습니다. 그는 IT 위험 평가, 거버넌스 및 규정 준수 관리 등의 분야를 전문으로 하고 있습니다. Kai는 이 역학을 수행하면서 동시에 IMT Germany에서 감사와 검토 작업에도 참여하고 있습니다. 그는 독일의 University of Stuttgart에서 비즈니스 정보 공학 분야 학사 학위를 취득했으며 CobiT 및 ITIL 인증을 받았습니다.

이 프로젝트에 기여하신 다음 분들에게 감사의 마음을 전합니다.
Wade Wallace
International Technical Support Organization, Austin Center
Maryann Hondo, Calvin Powers, Dr. Michael Waidner, Jim Whitmore 그리고 모든 IBM Security Architecture Board 팀

유명한 저자되기

2주에서 6주로 구성되는 레지던시 프로그램에 참여하십시오! 최첨단 기술에 대한 직접적인 경험을 쌓으면서 특정 제품 또는 솔루션에 대해서 다루는 책을 저술하는 작업을 도와주십시오. 참여자는 IBM 기술 전문가, 비즈니스 파트너 및 고객들과 함께 팀을 이뤄 작업할 수 있는 기회를 얻게 됩니다.

여러분의 노력은 제품 인수 및 고객 만족도 향상에 도움이 될 것입니다. 참여자는 보너스로 IBM 개발 연구소와의 연락 네트워크를 갖게 될 것이며 생산성과 마케팅 능력을 향상시킬 수 있게 됩니다.

레지던시 프로그램에 대해서 자세히 알아보십시오. 레지던시 색인을 검색해 보시고 다음 사이트에서 온라인으로 지원하십시오.
ibm.com/redbooks/residencies.html

독자 의견 환영

여러분의 의견은 우리에게 매우 소중한 자료입니다.

우리는 우리가 제작한 자료가 독자들에게 가능한 많은 도움이 되기를 바랍니다. 이 출판물이나 다른 IBM Redbooks 출판물에 대한 여러분의 의견을 아래와 같은 방법을 통해서 저희에게 보내주십시오.

- 다음 사이트에 있는 온라인 Contact us review Redbooks 양식을 이용하십시오.
  ibm.com/redbooks
- 이메일을 통해서 의견을 보내주십시오.
  redbooks@us.ibm.com
- 우편으로 의견을 보내주십시오.
  IBM Corporation, International Technical Support Organization Dept. HYTD Mail Station P099 2455 South Road Poughkeepsie, NY 12601-5400

공지 사항

이 정보는 미국에서 제공되는 제품과 서비스용으로 저작된 것입니다.

IBM은 이 문서에서 설명한 제품, 서비스 또는 기능을 미국이 아닌 다른 나라에서 제공하지 않을 수 있습니다. 여러분이 거주하고 있는 국가에서 현재 이용할 수 있는 제품과 서비스에 대한 정보가 필요하시면 해당 지역의 IBM 대리점에 문의하십시오. IBM 제품, 프로그램 또는 서비스에 대한 모든 참조 자료는 해당 IBM 제품, 프로그램 또는 서비스만 사용될 수 있다는 것을 기술하거나 의미하기 위한 의도가 없습니다. IBM 지적 재산권을 침해하지 않으며 동등한 기능을 갖는 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 IBM 제품, 프로그램 또는 서비스가 아닌 것의 작동 성능을 평가하고 확인하는 것은 사용자의 책임입니다.

이 문서에서 설명한 주제와 관련하여 IBM이 특허를 갖고 있거나 특허를 신청해 놓았을 수 있습니다. 이 문서를 제공하는 것이 독자에게 해당 특허에 대한 라이센스를 제공하는 것을 의미하는 것은 아닙니다. 독자는 다음 주소로 라이센스 요청서를 보낼 수 있습니다.

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

다음 단락은 영국과 해당 조항이 국내법과 맞지 않는 기타 국가에는 적용되지 않습니다. INTERNATIONAL BUSINESS MACHINES CORPORATION은 이 출판물을 특허 불침해에 대한 내포된 보증, 특정 목적을 위한 상업성 또는 적합성 등을 포함하며 이에 제한되지 않고 표현되거나 내포된 일체의 보증 없이 "있는 그대로" 제공합니다. 일부 국가는 특정 트랜잭션에 대해서 표현되거나 내포된 보증에 대한 부인을 허용하지 않습니다.

이 문서에는 기술적으로 부정확한 정보 또는 오탈자가 포함되어 있을 수 있습니다. 이 문서는 주기적으로 변경 사항을 적용할 것입니다. 변경된 사항은 이 출판물의 새 버전에 적용될 것입니다. IBM은 언제든지 공지 없이 이 출판물에 기술되어 있는 제품 및/또는 프로그램에 대한 내용을 수정 및/또는 변경할 수 있습니다.

IBM은 독자들에게 책임이 발생하지 않는 한도 내에서 적합하다고 판단되는 방식으로 독자들이 제공한 정보를 사용하거나 배포할 수 있습니다.

이 문서에는 일상적인 비즈니스 업무에서 사용되는 데이터 예제와 보고서가 포함되어 있습니다. 데이터 예제와 보고서를 가능한 완벽하게 예시하기 위해서 제시된 예제에는 개인, 회사, 브랜드 및 제품의 이름이 포함되어 있습니다. 예시된 모든 이름은 가상의 것이며 실제 비즈니스 엔터프라이즈가 사용하는 이름이나 주소와 유사한 경우가 있더라도 그것은 완전히 우연의 일치일 뿐입니다.

저작권 라이센스:

이 문서에는 다양한 운영 플랫폼에서의 프로그래밍 기법을 예시하기 위해서 소스 언어로 제작된 예제 애플리케이션 프로그램이 포함되어 있습니다. 독자는 예제 프로그램이 목표로 하여 저작된 운영 플랫폼의 애플리케이션 프로그래밍 인터페이스에 일치하는 애플리케이션 프로그램의 개발, 사용, 마케팅 또는 배포를 목적으로 IBM에 비용을 지불하지 않고도 어떤 형태로든 이런 예제 프로그램을 복사, 수정 및 배포할 수 있습니다. 이런 예제는 모든 상황 하에서 완벽하게 테스트를 거치지 않았습니다. 그러므로 IBM은 이런 프로그램의 안정성, 서비스 성능 또는 기능을 보장할 수 없습니다.
이 문서(REDP-4528-00)는 2009년 7월 22일에 저작되거나 업데이트되었습니다.

IBM Korea
(135–700) 서울시 강남구 도곡동
467–12 군인공제회관빌딩 마케팅총괄본부
TEL : (02) 3781–7800
www.ibm.com/kr