백서

사이버 레질리언스 프레임워크를 실현하는 5가지 핵심 기술

연구 의뢰: IBM

Frank Dickson Phil Goodwin

2019년 8월

업데이트 정보

이 백서는 2018년 6월에 최초로 발행되었습니다(IDC #US44001318). 초판의 애널리스트 1명 및 발행일만 변경되었습니다.

IDC 견해

IDC의 최근 보안 설문조사에 따르면, 보안 전문가의 50%는 클라우드를 보호하는 데 대부분 시간을 보내고 있습니다. 그리고 상당수가 지난 12-18개월 동안 클라우드 관련 보안 위반을 경험한 바 있습니다. 응답자의 약 23%는 랜섬웨어 공격을, 22%는 IoT 보안 위반을, 23%는 DDoS 공격을 겪었다고 밝혔습니다. 이러한 공격의 약 75%는 클라우드 관련 사고에서 비롯된 것이었습니다.

클라우드 관련 기술과 새로운 커뮤니케이션 방식이 보안 위반 및 비즈니스 장애의 *근본* 원인이라는 뜻은 아닙니다. 기업에서 새로운 기술을 도입할 때 그에 따라 보호 전략도 바뀌어야 함을 의미합니다. 이러한 전략에는 더 강력하고 다양한 보안 메커니즘뿐만 아니라 보안 위반 또는 사고가 발생할 때 신속하게 복구할 방법도 포함되어야 합니다.

세계 각지에서 기업의 디지털 트랜스포메이션, 즉 비즈니스의 모든 영역에 기술을 통합하여 비즈니스 활동의 속도를 높이고, 애자일 조직으로 거듭나며, 전략적 비전과 역동적인 기회를 활용하는 프로세스가 꾸준히 진행되는 중입니다. 정보를 수익화할 수 있는 데이터 중심의 조직이 디지털 트랜스포메이션의 핵심 요소로 자리 잡고 있습니다. 아울러 디지털 트랜스포메이션은 지금까지 예상하지 못했던 새로운 위험, 또는 기존 비즈니스 프로세스에 내재된 위험을 가중시키는 새로운 위험을 수반합니다.

따라서 기업들은 주요 비즈니스 지원 기능을 더 긴밀하게 통합하고 데이터 가용성을 강화하여 어떤 과제도 능히 해낼 수 있는 체질을 갖추려 합니다. 이것이 바로 사이버 레질리언스(cyber-resilience)입니다.

사이버 레질리언스는 IT 보안, 비즈니스 연속성 및 기타 영역의 우수 사례를 접목하여 오늘날 디지털 비즈니스의 필요 및 목표에 부합하는 비즈니스 전략을 마련합니다. 본 IDC 백서에서는 디지털 트랜스포메이션과 함께 비즈니스 지원 기술이 위험, 공격, 장애의 유입 경로가 되면서 지금까지 기업과 다른 글로벌 경제 구성원 사이에 있던 방어막이 어떻게 사라지고 있는지 살펴봅니다. 더 나아가 사이버 레질리언스 정책을 통해 이러한 위험으로부터 보호

하고, 측정 가능한 통제된 방식으로 보안 위반 또는 장애로부터 복구하는 방법을 소개합니다. 마지막으로, 사이버 레질리언스 여정을 시작하는 기업을 위한 프레임워크, 그리고 갈수록 표적화되는 최신 악성 공격에 더 효과적으로 대응하기 위해 데이터 보호 및 복구 관행을 수정하는 전략도 제시합니다.

백서 개요

오늘 회사의 업무가 느닷없이 마비된다면 어떨까요? 오늘 갑작스럽게 회사가 문을 닫는다면? 이는 비즈니스의 실상을 매우 비관적인 시각으로 바라본 것입니다. 하지만, 비즈니스 운영 체계를 뒤흔드는 사건은 언제라도 생길 수 있습니다. 빠르게 변화하는 오늘날의 비즈니스 환경에서는 매분 매초가 중요합니다.

어떤 사건이 치명적인 타격은 아니었더라도 그 여파가 계속될 수 있습니다. 성숙한 기업 대부분은 이미 위험 관리를 실행하는 중이고, 어떤 형태로든 비즈니스 연속성 또는 레질리언스 기능을 구현했습니다. 이들은 대형 사건이 일어나 엄청난 충격을 주는 것보다는 작은 사건이 산발적으로 일어나 운영에 영향을 미치는 경우가 많다는 사실을 잘 알고 있습니다. 한 예로 조류 독감의 공포를 생각해 보세요. 2000년대 중반, 기업들은 공기를 통해 빠르게 전파되는 바이러스가 직원 건강 및 비즈니스 운영에 미칠 수 있는 영향에 극도로 신경을 썼습니다. 물론 관심을 가져야 할 문제이지만, 조류 독감 또는 이와 유사한 위협이 실현될 가능성은 그때나 지금이나 모두 낮은 편입니다. 이렇게 가능성이 낮다고 해서 각 기업이 잠재적 위험성에 따른 비상 대책을 마련하지 않은 것은 아닙니다. 다른 자연 재해 또는 물리적 위협도 마찬가지입니다. 실제로 발생했을 때 큰 피해를 일으킬 위험 요인이 주목받기 마련입니다. 그리고 어느 한 사건의 잠재적 규모에 집중하다가 매우 현실적이고 구체적인 별개의 위협, 즉 비즈니스에 큰 타격을 줄 수도 있는 위협을 놓치기 쉽습니다.

디지털 트랜스포메이션은 비즈니스 레질리언스에 대한 전통적인 시각에 이의를 제기합니다. 디지털 트랜스포메이션은 인간 경험의 전 범위에서 기술이 밀접하게 연결되는 프로세스입니다. 기업의 디지털 트랜스포메이션은 애플리케이션과 비즈니스 프로세스 간에 더 차원 높은 연결이 이루어져 애자일 비즈니스로 거듭나고 고객 및 비즈니스파트너와 더 신속하게 소통하면서 사용자에게 연중무휴 24시간 중단 없는 경험을 제공하는 것을 의미합니다. 디지털 트랜스포메이션은 여러 가지 형태로 나타날 수 있습니다. 기존 인프라 및 레거시 시스템을 더 효과적으로 통합하길 원하거나, 서서히 클라우드로 전환하는 중이거나, 아예 클라우드를 최우선에 두는 경우도 있습니다. 어떻든 커넥티드 엔터프라이즈의 개념은 비즈니스 레질리언스를 평가할 때 중요합니다. 이를 위해 여러 비즈니스 프로세스를 연결하거나 하이브리드 클라우드 또는 멀티클라우드 환경을 개발하는 등 어떤 방식을 채택하더라도 비즈니스 시스템과 프로세스가 더 긴밀하게 연결되므로, 하나의 개별 이벤트로 인해 비즈니스 전체가 잘못될 가능성이 커집니다. 한때는 잔물결이었던 것이 조직 전체에 충격파를 보낼 수도 있습니다.

이런 이유로 사이버 레질리언스는 보안 전문가뿐만 아니라 비즈니스 연속성 및 위험 관리 계획 책임자에게도 매우 중요한 과제가 되었습니다. 사이버 레질리언스는 사이버 보안, 위험 관리, 비즈니스 연속성/ 레질리언스를 융합한 분야로서 이벤트 탐지 및 복구부터 지속적인 프로세스 개선까지 모든 범위에서 사이버 대응 역량을 강화하는 데 중점을 둡니다. 고객들은 시스템 오류 및 장애에 집중하는 기존 비즈니스 연속성 전략에 머무르지 않고 데이터를 노리는 악의적인 사이버 기반 위협에 초점을 맞출 필요성을 깨닫고 있습니다. 시스템 가동 중단에 대한 기존 복구 절차로는 데이터를 손상시키는 사이버 위협을 차단하기 어렵습니다.

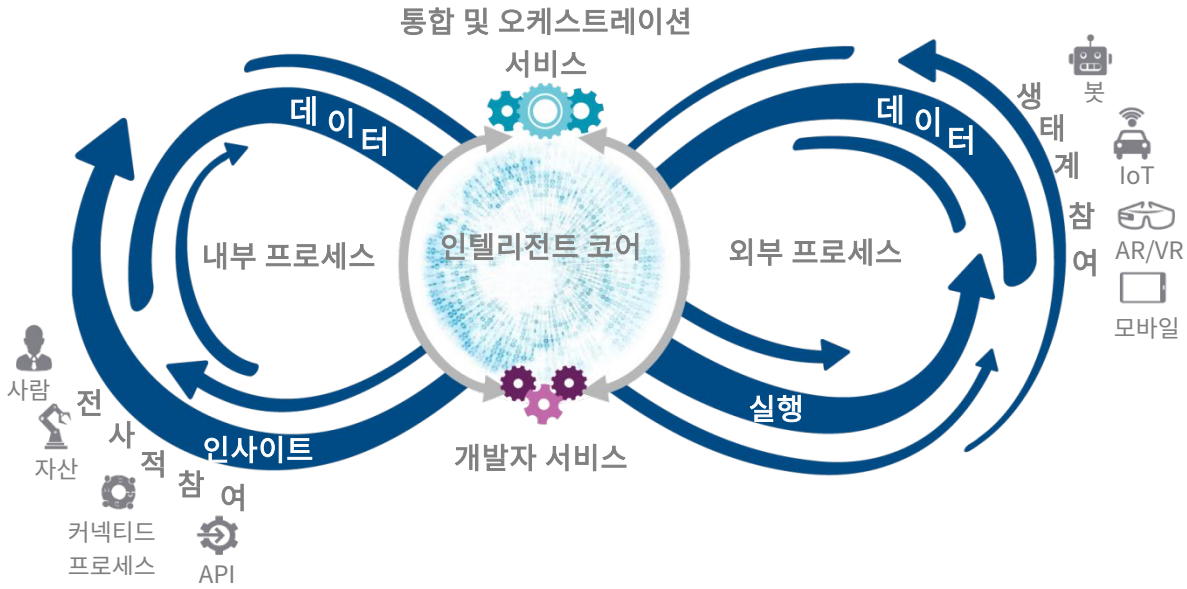
디지털 트랜스포메이션의 도래와 취약점

2017년 기준으로 기업들이 연결성(connectivity)과 인텔리전스(intelligence)를 모두 갖춘 기술 기반 조직이 되기 위해 투자한 금액이 무려 1조 1천억 달러에 달합니다. 2018년에는 1조 3천억 달러가 더 투입될 것으로 보입니다. 2021년에는 전 세계 기업이 트랜스포메이션을 시도하는 데만 연간 최대 2조 1천억 달러가 쓰일 것으로 보이며, 이 수치는 계속 늘어날 전망입니다. IDC는 2020년이 되면 약 60%의 기업에서 디지털 트랜스포메이션 여정을 시작할 것이며, CIO의 70%가 이 혁신에 필요한 애자일 인프라를 뒷받침하는 클라우드 최우선 전략을 마련할 것으로 예상합니다. 다시 말해 앞으로 최대 3년에 걸쳐 광대한 디지털 트랜스포메이션 성장의 기회가 기다리고 있음을 의미합니다.

이렇게 적극적으로 투자하는 이유는 무엇일까요? 요컨대 기업들은 디지털 트랜스포메이션이 이 하이퍼커넥티드 세상에서 앞으로 나아갈 길이라고 생각합니다. 기업이 생존하려면 혁신적인 애자일 조직이 되어야 합니다. 아울러 새로운 제품과 서비스를 활용하여 빠르고 확장 가능한 방식으로 시장을 공략하는 한편 핵심 고객과의 소통 및 신규 시장 개척에 필요한 주요 인사이트도 개발하는, 준비된 상태여야 합니다. 사실 IDC는 대부분 기업에서 트랜스포메이션이 본격화되면 인텔리전트 코어 인프라를 활용하게 되고, 이 과정에서 간단하지만 중단 없는 프로세스를 통해 비즈니스 활동 관련 인사이트로부터 실행 가능한 인텔리전스를 얻으리라 확신합니다. IDC는 이를 디지털 트랜스포메이션 플랫폼이라고 부릅니다(그림 1). 이 플랫폼은 그 중심에 있는, 다양하고 분산된 동적 데이터를 바탕으로 기회를 창출합니다.

그림 1

디지털 트랜스포메이션 플랫폼: 인텔리전트 코어를 위한 프레임워크



출처: IDC, 2018

데이터가 없으면 이 모델은 실패합니다. 데이터를 상품화하고 수익화할 수 없습니다. 데이터를 활용하여 애자일 비즈니스로 거듭날 수 없습니다. 이렇게 데이터가 비즈니스 생존에 결정적 역할을 하므로 데이터 무결성 및 접근성이 무엇보다 중요합니다. 그러나 디지털 트랜스포메이션 플랫폼에 중요한 데이터의 속성과 위치는 계속 변화합

니다. 데이터가 점점 더 다양해지면서 이제는 정형화된 시스템뿐만 아니라 비정형 데이터, 이를테면 시계열 데이터, 시스템 생성 데이터, 스트림 데이터까지 포괄합니다. 또 점점 더 역동적인 데이터가 됩니다. 배치(batch) 실행을 기반으로 할 뿐만 아니라 근본적으로 실시간의 속성을 갖습니다. 이는 그 수가 점점 늘어나는 센서 및 디바이스로부터 텔레메트리 데이터가 생성되기 때문입니다. 게다가 데이터는 점점 더 분산됩니다. 즉, 중앙 데이터센터뿐만 아니라 에지(edge) 위치, 각종 디바이스, 클라우드 서비스에도 자리합니다. 데이터가 다양해지고 역동성을 띠고 분산되면, 효과적인 사이버 레질리언스 프로그램을 도입하기가 쉽지 않습니다.

데이터가 유일한 고려 사항도 아닙니다. 대부분의 기업에서 디지털 트랜스포메이션 여정은 느슨하게 연결된 일련의 시스템에서 출발하여 상호 연결 시스템을 구축하는 것이 목표입니다. 루브 골드버그 장치(Rube Goldberg machine)의 관점에서 디지털 트랜스포메이션에 대해 생각해볼까요? 루브 골드버그는 엔지니어, 발명가이자 퓰리처상을 받은 만화가였습니다. 그는 일반 가정용품을 연결하여 사소한 기능을 수행하는 복잡한 시스템을 고안하고 그리면서 유명해졌습니다. 뭔가 익숙하게 들리지 않나요? 기업은 HR 시스템, 계약 관리, ERP 시스템, 고객 응대 애플리케이션 등을 연결하면서 이들이 하나의 공통된 비즈니스 목표를 향해 움직이기를 기대합니다. 따라서 비즈니스 위험을 최소화할 책임이 있는 이들은 디지털 트랜스포메이션에 대해 부담을 느낍니다.

자전거 바퀴살에 빗자루 손잡이를 끼우면 어떻게 될까요? 바퀴살이 어디에도 연결되지 않았다면 아무 일도 없겠지만, 바퀴살은 연결되어 있습니다. 바퀴살 한두 개에 외부 물체가 걸리면 바퀴 전체가 돌지 않게 됩니다. 상호 연결된 비즈니스 시스템도 이런 위험 부담이 있습니다. 어느 한 시스템에 오류가 생기면 비즈니스가 중단될 수도 있습니다.

사이버 레질리언스의 관점에서 보면, 어떤 하나의 비즈니스 프로세스가 다른 비즈니스 프로세스로 연결되는 관문이 될 수도 있습니다. 그러면 어떤 프로세스의 공격 노출 영역(attack surface)을 통해 거의 모든 프로세스에 대한 측면 접근이 가능하게 됩니다.

디지털 트랜스포메이션 여정의 과제

디지털 트랜스포메이션에 대해 대규모의 투자가 이루어지고 있으나, IDC는 점점 더 많은 외부 요인이 기업의 사이버 보안 전략에 지대한 영향을 미치기 시작했음에 주목합니다. 앞서 언급한 대로, 시스템끼리 상호 연결되고 외부 서비스(클라우드, IoT 등)에 계속 의존하는 상황 때문에 발생할 위험 요소에 대비한 곳은 아직까지 많지 않습니다.

IDC는 2020년에 약 60%의 기업이 디지털 트랜스포메이션 여정을 시작하고 70%의 CIO가 클라우드 최우선 전략을 마련할 것으로 예상합니다. 수치상으로는 굉장하지만, 과연 데이터 및 애플리케이션(정보) 가용성이 디지털 트랜스포메이션 성공의 핵심 요소임을 알고 있는 곳이 얼마나 될까요? 사용할 수 없는 데이터로 수익을 낼 수는 없습니다. 정보 가용성이 우수한 기업은 그렇지 않은 곳보다 경쟁에서 유리합니다. IDC의 조사에 따르면, DDoS 차단 제품 및 서비스에 대한 투자는 늘었지만 일관된 정보 가용성 전략, 즉 데이터 액세스 프로세스의 전 범위에서 데이터/정보 가용성을 신속하게 보장하는 전략을 마련하는 데 고전하는 고객이 많습니다.

규제 준수가 강화되는 현실도 어려움을 가중시키는 외부 요인입니다. 2025년에는 기업 데이터의 70% 이상이 규제 준수 대상이 될 것입니다. 이러한 데이터는 특별히 취급해야 하고, 더 큰 위험 부담도 감수해야 합니다. 데이터를 제대로 보호하지 못해 무거운 처벌을 받을 수도 있습니다.

점점 더 중요해지는 클라우드와 IoT

데이터 가용성과 규제 준수 모두 비즈니스에 큰 영향을 미치는 외부 요인일 뿐만 아니라, 비즈니스에 의해 간접적인 영향만 받는다는 공통점이 있습니다. 이 사실은 비즈니스 크리티컬 기능에서 클라우드 및 IoT 디바이스에 의존하는 기업이 늘면서 더욱 분명해집니다.

오늘날 기업들은 하이브리드 클라우드를 사용하고 있으며, 향후 등장할 애플리케이션 대부분은 클라우드를 지원할 것입니다. 최근 한 설문조사에서는 기업의 워크로드 중 절반가량이 하이브리드 클라우드 모델에 구축되는 것으로 나타났습니다. 이 조사 대상 기업들은 2년 이내에 워크로드의 62%를 하이브리드 클라우드에서 실행할 계획입니다. 보안은 하이브리드 클라우드 도입에 긍정적인 요소이자 부정적인 요소입니다. 이제는 중요 데이터가 수많은 지역, 데이터센터, 클라우드에 분산되어 있습니다. 이 데이터는 실제 저장 위치에 관계없이 기업의 요구사항에 따라 보호해야 합니다. 이번 설문에 참여한 기업들은 향후 12개월간 하이브리드 클라우드를 위한 데이터 서비스의 지출이 40% 늘어날 것으로 예상합니다. 백업 복구 및 데이터 비용/가치 평가는 최우선 과제입니다.

기업은 클라우드뿐만 아니라 IoT 디바이스에서도 점점 더 많은 중요 데이터를 수집하고 있습니다. 이러한 디바이스는 대개 일반 시스템보다 처리 성능이 떨어지는 편이지만, 공격자가 IoT 디바이스를 공격 전략에 포함시켜 활용할 수 있음이 입증되었습니다. 게다가 IoT 디바이스 중심의 보안이 아직 자리잡지 못했기 때문에 각 기업은 기존 컴퓨팅 디바이스뿐만 아니라 평가, 모니터링, 보안이 쉽지 않을 수도 있는 이 IoT 디바이스를 가장 효과적으로 보호할 방법까지 찾아야 합니다.

장애의 복잡성 증가

IDC의 조사에 따르면, 기업들이 클라우드 보안 능력에 대해 더 자신감을 느끼게 되었고 클라우드 이전 속도 및 클라우드 기반 보안 솔루션 도입도 늘고 있지만, 장애의 복잡성이 증가하는 문제에 대한 대비는 그 어느 때보다 허술합니다.

최근 IDC 고객 설문조사에서 최근 5–24시간 동안 DDoS 공격을 받았다는 응답이 56%였습니다. 최근 1–7일간 공격을 받았다는 응답도 8%였습니다. 더 우려스러운 점은 응답자의 6%가 공격이 8일 이상 지속되었다고 밝힌 것입니다.

백업 및 재해 복구(DR)로는 최신 위협으로부터 확실히 보호할 수 없습니다. IDC 우수 사례에서는 미션 크리티컬 애플리케이션에 대해 1시간의 RTO를, 일반 애플리케이션에 대해서는 4시간의 RTO를 권장합니다. 특정 PIT(point-in-time)(스냅샷)에 대한 복사본은 제대로 설계되지 않으면 불완전하고 비효율적이며 공격에 취약합니다. 이러한 접근 방식은 플랫폼 또는 구성(configuration) 손상에 대비한 환경 차원의 복구가 아니라 시스템 레벨의 복구로 설계되는 경우가 많습니다. 유지보수 및 테스트 시의 부실한 보안 위생(hygiene) 수준 때문에 PIT 데이터 복사본을 이용하는 보호 방식이 제 기능을 못할 수도 있습니다.

IDC가 조사한 바에 따르면, 가동 중단시간에 대한 "평균" 비용이 시간당 20만 달러를 넘어섰습니다. 물론 회사 규모 및 업종에 따라 달라질 수 있습니다. 교정(remediation) 계획 및 인프라 구축과 관련된 의사결정에서 이 비용 수치를 길잡이로 활용할 수 있습니다. 비용 추정에는 실제 매출 손실 및 복구 비용이 포함됩니다. 규제 준수 관련 비용도 해당되는데, 막대한 금액이 될 수도 있습니다. 이 추정치에는 포함되지 않지만, 이미지를 실추시키는 보안 위반으로 인한 평판 비용 및 장기적인 브랜드 가치 손상 비용도 발생합니다. 보안 위반 교정 인프라 전략에서 조직 차원의 적정 지출 규모를 결정하는 데 이 비용 추정 데이터를 참조할 수 있습니다. 최근 발생한 랜섬웨어 공격을 예로 들어볼까요? 애틀랜타는 일부 도시 서비스를 마비시킨 랜섬웨어 사고가 일어난 후 3주간 비상 조치 비용으로

3백만 달러 가까이 썼습니다. 보도에 따르면, 방어 기능 복구 및 강화를 위해 추가로 950만 달러를 요청한 것으로 알려졌습니다. 950만 달러 상당의 리소스를 추가로 투입하는 게 과하게 느껴질 수도 있지만, 조만간 랜섬웨어 공격이 또 일어나고 그때마다 3백만 달러의 비용을 부담하기보다는 950만 달러의 일회성 투자로 방어 체계를 강화하는 편이 훨씬 더 합리적입니다.

지능형 공격 증가

IDC는 지능형 공격 건수도 계속 늘어날 것으로 예상합니다. 업계 통계를 보면, 200일 넘게 발견되지 않은 공격도 많습니다. 공격자가 그토록 오랫동안 네트워크에 숨어 있으면서 심어 놓은 악성코드가 백업 세트로 전파됩니다. 결국 복구 데이터도 감염됩니다. 공격자가 몇 주 또는 몇 달간 잠복하면서 시스템 전체에 악성코드를 유포할 수도 있습니다. 공격을 밝혀내더라도, 조직 곳곳에 퍼져 있는 악성코드를 제거하는 것 역시 매우 힘든 일입니다.

상황 개요

사이버 레질리언스 개념

클라우드 및 각종 IoT 디바이스에서 인프라 리소스를 사용하는 경우가 늘고 있습니다. 그러나 새로운 위협을 성공적으로 막아내기 위해 도입한 기존의 방어 기능은 제 역할을 하지 못합니다. 따라서 보안에 대한 새로운 접근이 필요합니다. 오늘날의 위협 환경에는 데이터 라이프사이클을 포괄하는 통합 솔루션이 필요합니다. 각 기업에서는 방어부터 탐지, 대응, 복구에 이르는 라이프사이클 단계를 단축하여 사이버 레질리언스 기능을 구현하는 데 집중해야 합니다.

사이버 레질리언스 프레임워크

사이버 레질리언스는 기업이 공격을 견뎌내도록 지원하고자 개발된 프레임워크입니다. 하나의 보호 계층 또는 하나의 제품이 아니라, 어떤 이벤트로도 치명적인 피해를 입지 않도록 방어 체계를 구축하는 방법입니다. 사이버 레질리언스는 공격을 당했을 때 복구할 수단을 제공하는 반복형 프로세스입니다. 기존 방어 체계는 우회하는 데 성공하면 무용지물이 되지만, 사이버 레질리언스에서는 전사적 차원의 지속적인 경계가 이루어질 수 있습니다.

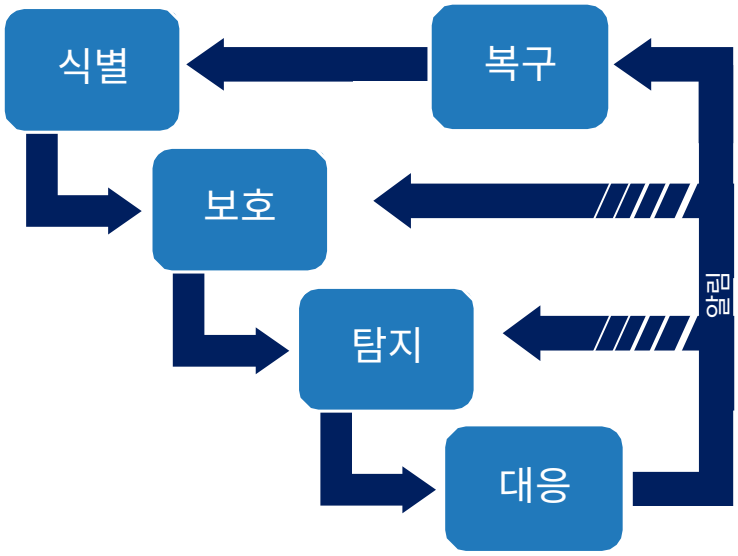
사이버 레질리언스 프레임워크는 5가지 요소로 구성됩니다(그림 2).

- **식별:** 중요 자산 및 프로세스 매핑, 위험 및 준비 수준 평가 등
- **보호:** 일반적인 1차 방어선 보안 메커니즘
- **탐지:** 보안 분석
- **대응:** 보안 위반 또는 장애 처리
- **복구:** 종합 복구 메커니즘

사이버 레질리언스 프레임워크의 핵심 장점은 선제적으로 행동한다는 것입니다. 기존의 보안은 비즈니스 환경에 덮어씌우는 형태로 작동했습니다. 사이버 레질리언스는 비즈니스 자체에 보안을 통합하므로 이 5가지 구성요소가 비즈니스의 모든 영역에 적용될 수 있습니다.

그림 2

사이버 레질리언스 프레임워크



출처: IDC, 2018

사고와 여파

업계에서 공격이 성공을 거두는 사례가 늘고 있습니다. 보안은 복잡합니다. 그리고 어떤 환경이 안전하다고 입증할 방법도 없습니다. 공격자는 성공적인 공격에 필요한 모든 수단을 동원하고 끊임없이 혁신적인 방법으로 침투를 시도합니다. 이에 맞설 최선의 방법은 인프라를 강화하고 감사 가능한 기능 및 프로세스를 마련하고 사용자를 잘 훈련시키고 실력 있는 보안 팀을 육성하고 지속적인 모니터링 프로세스를 실행하는 것입니다. 그러면 유리한 입장에서 시작할 수 있습니다. 하지만 대부분 조직에서는 공격 이후의 상황을 새로운 관점으로 바라보고 대처하는 것이 무엇보다 중요합니다. 온갖 통제, 점검, 조정 기능이 있더라도 언젠가는 공격이 성공한다는 것이 기정사실이라면, 공격 이후 상황에 대비하는 것이 현명하지 않을까요? 공격이 성공하더라도 탐지부터 대응까지 그리고 대응부터 복구까지의 시간을 단축할 방법을 찾아야 합니다. 사이버 공격이 성공했더라도 거의 차질 없이 비즈니스가 운영될수록 좋습니다.

비즈니스 세계는 냉혹합니다. 공격이 얼마나 지능적인지 또는 공격자가 어떻게 침투에 성공했는지에 연연하지 않습니다. 기업은 끈질겨야 합니다. 탐지, 대응, 복구에 소요되는 시간을 단축하는 전략을 구사함으로써 사고 비용을 절감하고 궁극적으로는 기업의 경쟁 우위를 강화할 수 있습니다. IDC는 비즈니스상의 차질을 최소화하는 기업이 준비되지 않은 기업보다 훨씬 더 유리한 입장에서 소비자 및 비즈니스파트너의 신뢰를 얻을 수 있다고 확신합니다.

전망

사이버 레질리언스의 5가지 핵심 기술

사이버 레질리언스 프레임워크가 직관적으로 보일 수도 있으나, 신중한 기술 선택 과정을 거쳐 구현해야 합니다. 하나의 제품으로 사이버 레질리언스 환경을 만들 수는 없습니다. 여러 핵심 기술을 구현하여 사이버 공격으로 인한 비즈니스 차질을 해소하는 것이 관건입니다. 여기서 소개할 5가지 기술은 레질리언스 환경을 구현하는 데 도움이 되는 중요한 기술입니다.

플랫폼과 애플리케이션 데이터를 복구하기 위한 자동화 및 오케스트레이션

*자동화*는 오래 전부터 보안 전문가에게 두려움의 대상이었습니다. 자동화 솔루션이 등장했을 때부터 자동화된 대응에 대한 우려가 업계 전반에 확산되었습니다. 하지만 지금과 같이 광범위하게 자동화된 공격 환경에서는 인텔리전스 자동화가 해결의 열쇠입니다. 자동화를 해결책으로 여기기보다는 오케스트레이션과 자동화를 연계하는 대응 수단을 마련해야 합니다.

오케스트레이션은 인적 요소를 배제하거나 맹목적인 정책 변경을 허용하는 게 아닙니다. 애널리스트가 즉시 정보에 액세스하고 수작업 방식보다 신속하게 대응하도록 지원하면서 애널리스트의 역량을 강화하는 것입니다. 더 나아가 애플리케이션을 성공적으로 복구하려면 여러 단계에 걸쳐 상호 연결 시스템 및 데이터를 복구해야 합니다. 이러한 시스템을 수작업으로 복구하면 사람의 실수가 일어나기 마련입니다. 검증 및 테스트를 거친 소프트웨어 템플릿으로 복구 프로세스를 코드화하면 복구 프로세스의 위험 부담을 줄일 수 있습니다.

전파된 악성코드로부터 안전한 에어갭 복사본 보호 기술

에어갭(Air-gapping)이란 시스템 또는 네트워크를 다른 시스템 또는 네트워크로부터 물리적으로 또는 가상의 방식으로 격리하는 것을 말합니다. 이를테면 매우 중요한 데이터가 들어 있는 네트워크 또는 시스템을 일상 업무용 네트워크와 완전히 격리할 수도 있습니다.

경계가 사라지고 전사적 범위에서 데이터의 유동성이 요구되고 있지만, 에어갭 네트워크 세그먼트를 생성하는 기능이 그 어느 때보다 중요해졌습니다. 최근 랜섬웨어 감염 사례에서 확인된 것처럼, 악성코드를 자동화하여 빠르게 네트워크를 돌아다니며 피해를 입히도록 설계할 수 있습니다. 그러면 해당 조직은 시스템 감염 상황에 따라 내외부적으로 위험에 노출되는 셈입니다. 오늘날에는 중요 데이터의 에어갭 복사본을 만들어 외부 노출을 최소화하고 운영 중단으로부터 보호하며 불필요한 비용 지출을 방지하는 것이 가장 좋습니다.

WORM/변경 불가 스토리지 기술로 손상 또는 삭제 방지

최근 NotPetya와 같은 랜섬웨어 공격의 성공 사례를 보면, 데이터 손상 또는 삭제 위험에 대한 더 확실한 보호 장치가 필요합니다. 잘 알려진 것처럼, 공격자는 흔적을 숨기기 위해 로그 지우기를 시도합니다. 그러나 데이터가 삭제되거나 손상되면 비즈니스가 치명타를 입을 수도 있습니다. 최근 WannaCry를 비롯한 여러 랜섬웨어가 휩쓸고 간 후, 돈을 내더라도 공격자가 암호화 키를 넘긴다고 확신할 수 없음을 기업들은 깨달았습니다. 공격자가 제공한 키가 아예 작동하지 않을 때도 있었습니다.

데이터를 변경할 수 없게 만드는 기술을 갖춰야 합니다. WORM(write once, read many)/변경 불가 스토리지(immutable storage) 기술로 이 요구사항을 해결할 수 있습니다. WORM/변경 불가 스토리지 기술을 통해 데이터의 무결성 및 비즈니스 레질리언스를 유지할 수 있습니다. 이 속성들은 최근 가장 심각한 공격의 표적이 된 바 있습니다. 소프트웨어 및 하드웨어 계층에서 다양한 형태의 WORM 기술이 있습니다. 둘 다 데이터 변조를 방지하는 수단이므로 전자 정보 관리 체계(electronic chain of custody)로 활용할 수 있습니다.

효율적인 PIT 복사본 및 데이터 검증 기술로 복구 가능한 데이터를 신속히 파악

공격이 발생하면 안전한 데이터 복사본을 찾아 신속하게 복구해야 합니다. 앞서 말한 대로, 1년 가까이 네트워크에 숨어 있는 공격자도 많아 백업까지 감염되곤 합니다. 따라서 고효율의 PIT(point-in-time) 기술을 사용하여 데이터의 복사본을 여러 개 관리해야 합니다. 이 복사본에 대해 지속적으로 데이터 검증을 수행하여 혹시라도 감염되었다면 일찍 찾아내 치료해야 합니다. 이러한 지속적인 데이터 검증은 복구 프로세스에 사용할 안전한 데이터 복사본을 신속하게 찾는 데에도 도움이 됩니다. 백업 데이터 검증에는 다양한 방식이 있습니다. 하드웨어 및 소프트웨어에 내장된 기능을 사용하여 데이터가 감염되지 않았는지 확인합니다.

재해 복구 및 운영 복구 테스트 프로세스에서는 반드시 데이터 검증을 거쳐야 합니다. 첫째, 백업/복제 데이터의 무결성을 확인하고 백업/복제가 정상적으로 작동하는지 점검합니다. 둘째, 백업/복제 데이터를 검사하여 예전에 프로덕션 데이터에 발생했던 감염이 백업/복제 데이터에 확산되지 않았음을 확인합니다. 백업 대상 시스템에 따라, 다양한 데이터 검증 기술을 사용할 수도 있습니다. 이를테면 데이터베이스 시스템에서 기본 제공하는 분류 및 검사 툴로 더 포괄적인 데이터 보호 솔루션의 기능을 보완하면 효과적입니다.

규제 준수 보고 및 보증

규제 준수가 조직의 전반적인 보안 수준을 높이는 데 기여하지 않는다는 오명을 쓰기도 하지만, 실상은 데이터에 대한 올바른 통제 장치가 마련되어 제대로 작동하고 있음을 검증하면 큰 도움이 될 수 있습니다. 게다가 불이행에 대한 처벌이 강화되고 있으므로, 효과적인 보고 기능을 갖추면 규제를 준수하고 있음이 입증될 뿐만 아니라 고비용의 감사 및 과징금을 피할 수 있어 시간과 비용이 절약됩니다.

과제/기회

사이버 보안은 오늘날 비즈니스 환경의 대표적인 과제입니다. 보안 위협의 속도 및 규모가 증가하고 있으므로, 크고 작은 기업 모두 대비해야 합니다. 따라서 사이버 레질리언스 전략을 세우고 이행하는 것이 훨씬 더 중요해졌습니다. 효과적인 사이버 레질리언스 전략은 폭넓은 범위에서 다양한 이해 관계자와 구성원을 수용해야 합니다. 주요 이해 관계자에는 보안, 운영, 엔지니어링, 법무, 위험 관리 팀뿐만 아니라 데이터 소유자 및 현업 부서의 임원도 포함됩니다. 따라서 우선 목표와 지식 수준이 제각각인 여러 조직 간의 협업과 계획이 요구됩니다. 이러한 조직 차원의 역동성은 규모가 큰 조직에서 겪는 문제이지만, 최고 경영진의 전략 계획 및 우선 순위 설정을 통해 해결할 수 있습니다.

결론

사이버 레질리언스는 데이터 및 애플리케이션 가용성의 필수 조건입니다. 디지털 트랜스포메이션 여정의 핵심 요소이기도 합니다. 올바른 사이버 레질리언스를 갖추지 못한 기업은 비즈니스를 마비시킬 수도 있는 각종 공격에 더 취약해집니다. 악성 공격뿐만 아니라 여러 지역 및 업종을 포괄하는 규제도 늘어나고 있습니다. 이에 따라 통제 장치를 계속 검증하지 않으면 무거운 처벌을 받을 수도 있습니다.

악성코드 탐지, 백업, DR만으로는 부족합니다. 통합 라이프사이클 관리를 통해 플랫폼을 비롯한 모든 위협 요소로부터 데이터 가용성을 보호해야 합니다. 또한, 사이버 레질리언스는 온프레미스 및 클라우드 저장소를 모두 포함해야 합니다. 아울러, IT 팀은 포괄적인 사이버 레질리언스 모델을 채택하고, 다양한 사이버 위협을 해결할 제품을 찾아야 합니다.

사이버 레질리언스는 공격 이후 복구를 위한 프레임워크이기도 합니다. 그러나 이 프레임워크의 각 단계를 제대로 수행하려면 확실한 기술의 모음이 뒷받침되어야 합니다. 이제 보안은 제각기 다른 수준의 기밀 보호, 무결성, 접근성으로 설명할 수 없습니다. 이 3가지 영역을 항상 모두 포함해야 합니다. 사이버 레질리언스를 구현한 기업은 향후 고객이 비즈니스 가용성의 허점을 발견하게 될 때 유리한 입장에서 도울 수 있습니다. 또한, 레질리언스를 갖춘 조직은 능숙하게 공격에 대처하고 복구할 수 있습니다.

IDC 소개

International Data Corporation(IDC)은 정보 기술, 통신, 소비자 기술 시장을 위해 시장 분석 및 자문 서비스를 제공하고 각종 이벤트를 개최하는 대표적인 글로벌 기업입니다. IDC는 IT 전문가, 기업 경영진, 투자 커뮤니티가 사실에 기초하여 기술 도입 및 비즈니스 전략에 관한 결정을 내리도록 지원합니다. 전 세계 110여 개국에서 1,100명이 넘는 IDC 애널리스트들이 글로벌 및 지역 차원에서 기술 및 산업 동향과 기회를 분석하고 조언하는 전문 서비스를 수행하고 있습니다. IDC는 50여 년간 고객의 핵심 비즈니스 목표 달성에 더없이 중요한 전략 인사이트를 제공해 왔습니다. IDC는 세계 최고의 기술 미디어, 리서치, 이벤트 기업인 IDG의 자회사입니다.

글로벌 본사

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com www.idc.com