백서

사이버 복원력 프레임워크를 구현하기 위한 5 가지 핵심 기술

후원: IBM

Frank Dickson Phil Goodwin
October 2020

IDC 견해

2020 년은 전환 시점이었습니다. IDC 의 보안 설문조사에 의하면 처음으로 클라우드의 기업 데이터 양이 온프레미스의 기업 데이터 양을 뛰어넘는 것으로 나타났습니다. 또한 워크로드의 53%가 IaaS 에서 발견되는 것처럼 대다수의 컴퓨팅이 이제 클라우드에서 돌아갑니다.

유감스럽게도 해커들이 데이터를 따라 클라우드로 이동하고 있습니다. 지난 2 년 동안 일반적인 조직에서 "문제를 바로잡는 데 추가적인 리소스가 상당히" 필요한 2.0 클라우드의 해커 침해 문제를 경험했습니다. 온프레미스 환경의 침해와 마찬가지로 IaaS 클라우드 환경에서 발생하는 침해는 수많은 요인에 따른 결과입니다. IaaS 클라우드 침해의 주요 요인으로는 지능형 맬웨어(17.7%), 보안 도구 부족(17.7%), 부실한 자격 증명(14.6%), IaaS 환경 구성의 오류(14.3%), 패치가 적용되지 않은 취약성(13.9%), 내부자 위협(13.3%), 제로 데이 취약성(8.5%) 등이 있습니다. 이에 따른 교훈을 참조하면 시장이 클라우드로 전환됨에 따라 해커들도 클라우드로 초점을 맞춰 이동했기 때문에 데이터 보안을 위해 꾸준히 노력해야 합니다.

클라우드 관련 기술과 새로운 통신 방식이 해커 침해 및 업무 장애의 근본 원인이라고 하는 것은 아닙니다. 오히려 기업에서 새로운 기술을 채택함에 따라 이에 보조를 맞춰 보호 전략을 변경해야 한다는 것을 의미합니다. 이러한 전략에는 더 강력하고 다양한 보안 메커니즘이 들어있어야 하지만 해커 침해 또는 사고가 발생할 경우 신속하게 복구할 수 있는 방법도 포함되어야 합니다.

전 세계적으로 기업은 디지털 혁신(DX)을 통해 문제를 해결하기 위해 꾸준히 노력하고 있으며, 이에 따라 기술을 비즈니스의 모든 측면과 통합하여 비즈니스 활동을 가속화하고 민첩성을 지원하며 전략적 비전과 역동적인 기회를 활용하는 프로세스가 진행됩니다. 디지털 혁신의 핵심 요소는 정보를 수익화할 수 있는 데이터 중심의 구성체가 되고 있습니다. 이와 동시에 디지털 혁신은 본질적으로 이전에는 예상하지 못했던 새로운 위험성을 가져오거나 잘 확

립되어 있는 비즈니스 프로세스의 위험 프로필을 복잡하게 만들 수도 있습니다. 결과적으로 기업은 주요 비즈니스를 지원하는 기능 간의 통합 수준을 끌어 올리고 데이터 가용성을 향상시켜 기업이 어떤 문제에도 견뎌낼 수 있는 준비가 되어 있는지 확인해야 합니다. 이것이 바로 사이버 복원력입니다.

사이버 복원력은 IT 보안, 비즈니스 연속성 및 기타 분야의 모범 사례들을 결합하여 오늘날 디지털 비즈니스의 니즈 및 목표에 보다 잘 부합할 수 있는 비즈니스 전략을 만들어 냅니다. 이 IDC 백서에서는 비즈니스 지원 기술이 위험, 공격 및 장애로 이어지는 통로가 됨에 따라 디지털 혁신이 어떻게 하면 기업과 글로벌 경제 참여자 사이의 전통적인 보호 장치를 무너뜨리게 되는 지를 설명합니다. 또한 백서에서는 사이버 복원력 실행이 어떻게 기업이 이러한 위험을 방어하고, 통제와 측정 가능한 방식으로 해커 침해 또는 장애를 복구하는 데 도움이 될 수 있는지 설명합니다. 마지막으로, 조직이 사이버 복원력 진행 과정에 참여하기 시작하는 데 도움이 될 수 있는 프레임워크를 제공하고 데이터 보호 및 복구 관행을 수정하여 오늘날 더욱 표적화되고 악의적인 공격에 더 훌륭하게 대응할 수 있는 전략을 제공합니다.

이 백서의 내용

실제로 오늘 갑작스럽게 귀하의 사업 운영이 중단되는 날입니까? 오늘 귀하의 사업이 문을 닫는 날입니까? 이것은 비즈니스 현실에 대한 비관적인 생각입니다. 비즈니스의 운영 환경을 혼란스럽게 만드는 사건은 언제든지 발생할 수 있으며 오늘날과 같이 빠르게 변화하는 비즈니스 세계에서는 매 순간이 중요합니다.

사건이 치명적이지 않아도 지속적으로 영향을 미칠 수 있습니다. 대부분의 성숙한 기업은 이미 위험 관리와 비즈니스 연속성 또는 복원 기능을 일부 실행하고 있습니다. 이러한 조직들은 심각한 영향을 미치는 대형 사건은 운영에 파급 정도를 유발할 수 있는 작고 개별적인 사건이 일어나는 것보다 발생 가능성이 낮다는 것을 알고 있을 것입니다. 예를 들어 조류 독감 공포를 생각해 보십시오. 많은 사람들은 빠르게 기동하는 공기 중에 있는 바이러스가 직원과 비즈니스 운영에 미칠 수 있는 잠재적인 영향에 대해 기업이 과도하게 집중했던 2000 년대 중반을 기억할 것입니다. 이러한 생각은 확실하게 우려할 가치는 있지만 조류 독감이나 유사한 위협이 구체화될 가능성은 아주 낮았으며 여전히 매우 낮습니다. 가능성이 낮다고 해서 조직이 잠재적 영향의 특성에 따라 운영상 우발적으로 발생할 수 있는 상황을 준비하는 것 자체를 맞지는 못했습니다. 다른 자연 재해 또는 물리적 위협에 대해서도 마찬가지입니다. 고 위험에 따른 결과에 대한 가능성은 운영자를 고민하게 만들며, 때로는 단일 사건에 따른 잠재적 위험 규모에

초점을 맞추면 조직이 비즈니스에 치명적인 영향을 미칠 수 있는 매우 실제적이고 가시적인 개별적인 위협에 집중하지 못하게 할 수도 있습니다.

디지털 혁신(DX)은 비즈니스 복원력에 대한 전통적인 관점에 저항하고 있습니다. 이는 기술이 전반적인 인간의 경험과 서로 밀접하게 얽혀 있는 프로세스입니다. 기업 입장에서 디지털 혁신은 비즈니스의 민첩성을 높이고 사용자가 연중 무휴 24 시간 작업 중단 없는 경험을 할 수 있다는 기대에 따라, 고객과 비즈니스 파트너와 보다 쉽게 연결하기 위한 목적으로 애플리케이션 및 비즈니스 프로세스 간의 더 높은 수준의 연결성을 의미합니다. 디지털 혁신은 다양한 형태로 올 수 있습니다. 기업은 기존의 인프라와 레거시 시스템을 더욱 양호하게 통합하려고 한다거나 클라우드로 천천히 넘어가거나 클라우드 우선 명령(클라우드 기반 솔루션) 환경을 가져갈 수도 있습니다. 그럼에도 불구하고 커넥티드 엔터프라이즈의 개념은 비즈니스 복원력을 평가할 때 상당히 중요합니다. 여기에 비즈니스 프로세스를 결합하거나 하이브리드 클라우드 또는 멀티 클라우드 환경을 개발하는 일이 포함되는지 여부와 무관하게, 비즈니스 시스템과 프로세스가 과도하게 연결되면 개별적인 이벤트가 전체 비즈니스를 혼란스럽게 만들 가능성이 더 커집니다. 이는 한때 작은 잔물결이었던 것이 이제는 전체 조직에 큰 충격파를 보낼 수 있게 되는 것입니다.

사이버 복원력은 이러한 이유로 인해 보안 전문가뿐만 아니라 비즈니스 연속성 및 위험 관리 계획을 담당하는 사람들에게 가장 큰 관심사가 되었습니다. 사이버 복원력은 사이버 보안, 위험 관리 및 비즈니스 연속성/복원력 관행을 병합하여, 사건 감지 및 복구에서부터 지속적인 프로세스 개선에 이르기까지 사이버 대응 능력을 개선하는 데 초점을 맞춘 규정을 만듭니다. 고객은 시스템 장애 및 중단에 초점을 맞춘 기존의 비즈니스 연속성 전략은 진화해야 하고, 데이터를 악의적으로 표적 삼는 사이버 기반의 위협에 집중해야 하는 것으로 인식하고 있습니다. 시스템 중단에 초점을 맞춘 기존의 복구 절차는 데이터를 손상시키는 사이버 위협으로부터 사용자를 보호하지 못할 가능성이 높습니다.

디지털 혁신의 부상 및 결함

비즈니스 관행, 제품 및 조직의 디지털 혁신을 위한 지출은 COVID-19 로 인한 경제적 어려움에도 불구하고 가속화될 것입니다. 2021 년에 디지털 혁신(DX) 기술 및 서비스에 대한 글로벌 지출은 16.6% 증가하여 1.54 조 달러로 증가할 것입니다. 이러한 성장은 2020 년에 예상되는 10.4%의 성장보다 훨씬 클 것으로 보는데, 그 이유는 2021 년에 기업들은 IDC 가 언급한 경제 침체의 "곡선 평탄화(낮게 유지되는) 현상"인 COVID-19 세계적 유행병이 경제에 미치는 부정적인 영향에 대응하기 위해 디지털 혁신을 구현할 계획이기 때문입니다(그림 1 참조). 경제적 요인에 가장 큰 영향을 받는 산업에서도 디지털 혁신에 대한 지출이 지속적으로 증가할 것입

니다. 호텔, 테마 파크, 카지노, 영화관을 비롯한 개인 및 소비자 서비스 산업은 2021 년에 디지털 혁신에 대한 지출이 16.0% 증가하는 것을 보게 될 것입니다. 2021 년 디지털 혁신에 대한 지출이 가장 크게 증가할 것으로 예상되는 산업은 건설(27.9%)과 소매 분야(20.3%)입니다.

그림 1

곡선 평탄화: 기술이 비즈니스 복원력 기능을 구축하고 민첩성을 활성화하는 방법

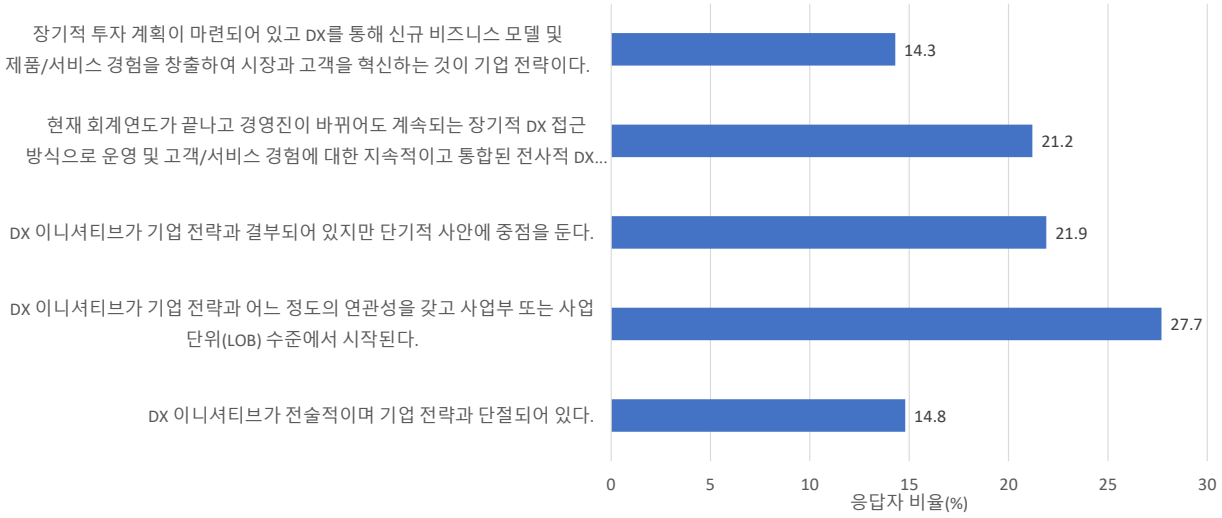
출처: IDC, 2020 년

디지털 혁신에 관한 조직의 입장은 다양합니다. 많은 조직이 "장기적인 투자 계획이 수립되어 있고 기업 전략은 디지털 혁신을 사용하여 새로운 비즈니스 모델과 제품/서비스 경험을 창출함으로써 시장과 고객을 변화시키는 것"이라는 전향적인 입장을 취하고 있습니다. 일부 조직은 보다 적극적인 방법을 찾고 있습니다. 조직의 입장과는 무관하게 디지털 혁신이 그들 마음에 가장 먼저 떠오르고 있는 것은 분명해 보입니다(그림 2 참조).

그림 2

디지털 혁신에 대한 입장

Q. COVID-19 세계적 유행병이 발생하기 전에 귀하의 조직은 디지털 혁신과 관련해서 어디쯤에 있었는지 어떻게 평가하시겠습니까?



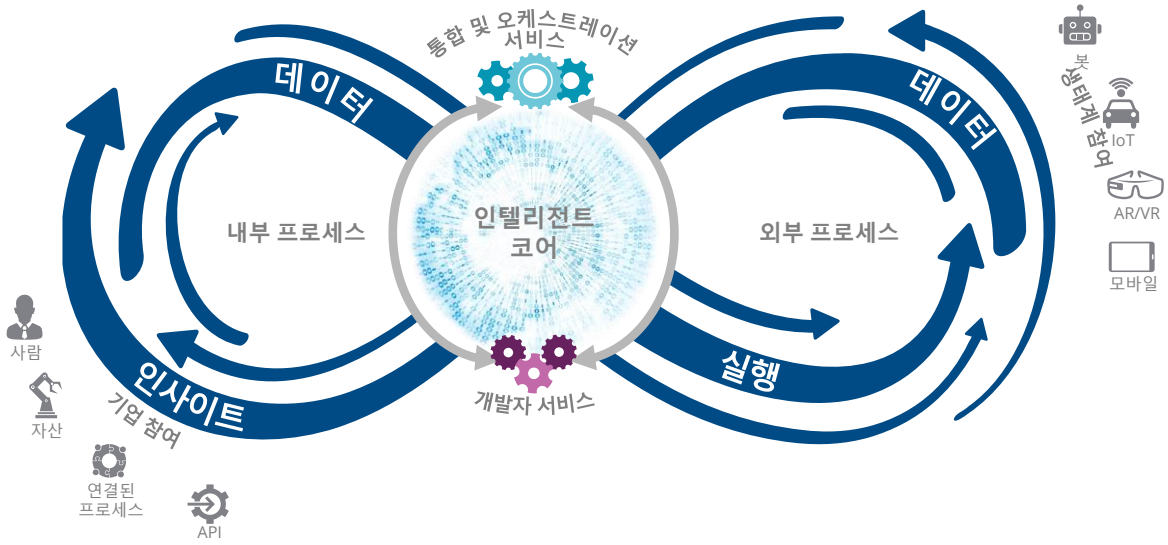
n = 880

출처: IDC 의 COVID-19 Impact on IT Spending Survey, 2020 년 6 월 4 일~15 일

비용 지출을 왜 그렇게 많이 할까요? 간단하게 말하면 기업은 디지털 혁신이 하이퍼 커넥티드 세계에서 성공을 위해 앞으로 나아갈 길이라고 믿기 때문입니다. 기업은 생존을 위해 혁신과 민첩성을 찾아야 하며 핵심 고객에게 접근하고 새로운 시장을 개척하는 데 필요한 핵심적인 인사이트를 개발하면서 새로운 제품과 서비스를 통해 시장에 대규모로 빠르게 진출할 수 있는 준비가 되어 있어야 합니다. 실제적으로 IDC 는 대부분의 조직이 혁신의 절정에 도달하게 되면 비즈니스 활동 인사이트를 능률적이고 지속적인 프로세스와 더불어 실행 가능한 인텔리전스로 전환하는 인텔리전트 코어 인프라를 활용하게 될 것이라고 믿고 있습니다. IDC 는 이를 디지털 혁신 플랫폼이라고 설명합니다(그림 3 참조). 이 플랫폼은 그 중심에서 다양하고 분산된 동적 데이터를 기반으로 하여 새로운 기회를 창출합니다.

그림 3

디지털 혁신 플랫폼: 인텔리전트 코어를 위한 프레임워크



출처: IDC, 2020 년

데이터가 없으면 사업 모델은 실패합니다. 더 이상 데이터가 생산되지 않고 수익도 창출될 수 없습니다. 비즈니스 민첩성을 위해 더 이상 데이터를 활용할 수도 없습니다. 이런 이유로 데이터는 비즈니스 생존에 상당히 중요한 것이며 데이터 무결성과 접근성을 중요하게 만듭니다. 그러나 디지털 혁신 플랫폼과 관련된 데이터의 속성과 위치는 계속해서 변경됩니다. 데이터는 구조화된 시스템뿐만 아니라 시계열 데이터, 기계 생성 데이터 및 스트림 데이터와 같은 구조화되지 않은 데이터 등을 아우르며 점점 다양해지고 있습니다. 또한 데이터는 점점 더 역동적으로 작용합니다. 이는 배치 실행 기능을 기반으로 할뿐만 아니라 점점 더 많은 센서와 장치를 통해 텔레메트리 데이터가 생성됨에 따라 사실상 실시간 데이터입니다. 또한 데이터는 핵심적인 데이터 센터뿐만 아니라 에지 위치, 장치 및 클라우드 서비스에도 점점 더 많이 분산되고 있습니다. 하지만 다양하면서 역동적이고 분산된 데이터는 효과적인 사이버 복원 프로그램을 사용할 수 있는 능력을 더욱 악화시킵니다.

그렇다고 데이터가 유일한 고려 사항이라고 말하는 것은 아닙니다. 대부분의 조직에서 디지털 혁신의 진행 과정은 상호 연결된 시스템을 기반으로 구축되기를 바라는 느슨하게 연결된 일련의 시스템에서 시작됩니다. Rube Goldberg 기계의 관점에서 디지털 혁신을 생각해 봅시

다. 일반인에게는 Rube Goldberg 는 엔지니어, 발명가 및 퓰리처 상을 수상한 만화가였으며, 궁극적으로 그는 일상적인 작업을 완료하기 위해 함께 사용되는 일반적인 가정 용품을 복잡하게 묘사한 시스템의 그림으로 널리 명성을 얻었습니다. 이것이 친숙하게 들린다면 그렇게 해야 합니다. 기업은 공통적인 사업 지향적 방향으로 운영되기를 희망하면서 HR 시스템, 계약 관리, ERP 시스템, 고객 대면 애플리케이션 등을 하나로 묶어 통합하고 있습니다. 이는 디지털 혁신이 비즈니스 위험을 경감시키는 일을 담당하는 사람들에게 과제를 해결하는 것을 보여주기 시작하는 부분입니다.

빗자루 손잡이를 자전거의 바퀴살에 넣으면 어떻게 될까요? 바퀴살이 어느 것에도 연결되어 있지 않으면 아무 일도 일어나지 않을 것입니다. 하지만 바퀴살은 상호 연결되어 있습니다. 하나 또는 두 개의 바퀴살이 이물질에 의해 회전하는 데 방해를 받으면 바퀴 전체가 회전을 멈추게 됩니다. 이것은 상호 연결된 비즈니스 시스템의 위험성과 같습니다. 단일 시스템에 장애가 발생해도 비즈니스가 중단될 수 있다는 것을 의미합니다.

이는 사이버 복원력 측면에서 보면 단일 비즈니스 프로세스가 다른 비즈니스 프로세스의 게이트웨이가 될 수 있다는 것을 의미합니다. 하나의 프로세스 공격 표면이 거의 다른 모든 프로세스에 우회적인 액세스 권한을 부여할 수 있다는 것을 의미하기도 합니다.

디지털 혁신 진행 과정의 과제

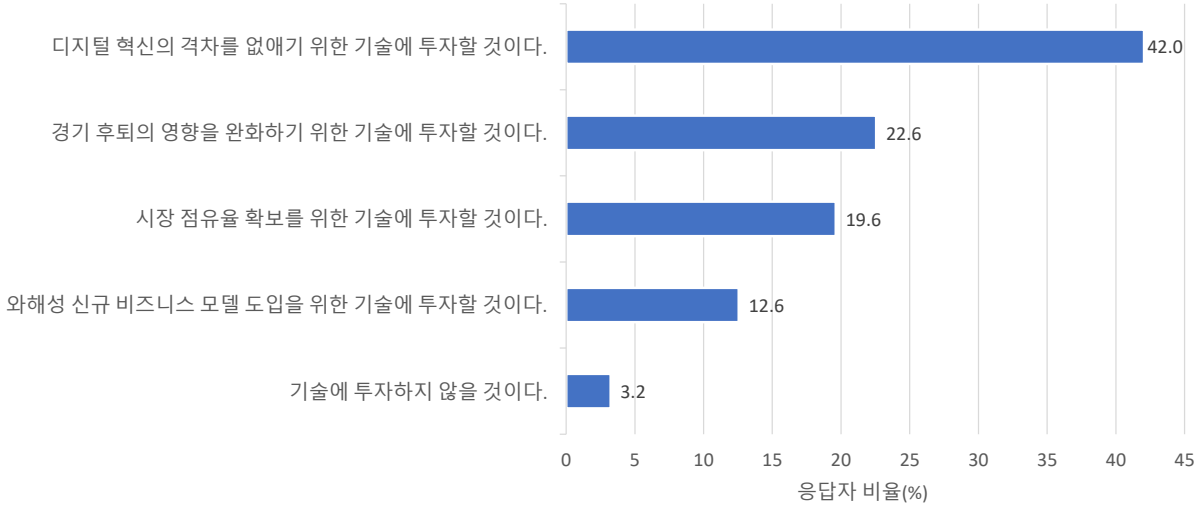
디지털 혁신에 대한 지출이 인상적이기도 하지만, IDC 는 조직의 사이버 보안 전략에 상당한 영향을 미치기 시작하는 외부적 압력이 증가하는 것을 벌써부터 확인하고 있습니다. 앞서 언급했듯이 시스템의 상호 연결, 클라우드 및 IoT 와 같은 외부 서비스에 지속적으로 의존하는 것은 오늘날 많은 조직이 준비하지 않은 위험을 초래하게 될 것입니다.

더욱이 디지털 혁신은 위기의 시기에도 지연되지 않고 가속화되고 있습니다. 최근 IDC 설문조사에 의하면 응답자 중에 3%를 제외한 모든 응답자가 경제 침체를 해결하기 위해 기술에 투자하려고 했습니다(그림 4 참조).

그림 4

경제 침체를 해결하기 위한 기술 투자 전략

Q. 귀하의 조직에서 디지털 혁신 노력과 관련된 기술 투자에 대해 주로 생각하고 있는 방식과 가장 일치하는 문장은 무엇입니까?



n = 880

출처: IDC 의 COVID-19 Impact on IT Spending Survey, 2020 년 6 월 4 일~15 일

공격적인 투자가 인상적이긴 하지만, 이러한 조직 중에 얼마나 많은 조직이 데이터와 애플리케이션(정보)의 가용성이 디지털 혁신을 성공시키는 핵심이라는 것을 인식하고 있는지는 분명하지 않습니다. 가용성이 없으면 데이터로 수익을 창출할 수 없습니다. 정보 가용성이 높아질수록 기업은 가용성에 어려움을 겪고 있는 기업에 비해 상대적으로 경쟁 우위를 확보할 수 있습니다. IDC 가 안티 디도스(anti-DDoS) 제품 및 서비스에 대한 지출이 증가했음에도 불구하고 많은 고객은 전체 데이터 액세스 프로세스를 통해 데이터/정보 가용성을 한쪽에서 다른 쪽 끝까지 신속하게 보존할 수 있는 기능을 제공하는 정보 가용성에 필요한 일관된 전략을 제시하는 데 어려움을 겪고 있습니다.

조직의 또 다른 외적 과제는 규정 준수 사항이 증가하는 것입니다. 2025 년까지 기업 데이터의 70% 이상이 규정 준수 대상에 해당될 것입니다. 해당 데이터는 특별한 처리가 필요할 뿐만 아니라, 조직이 데이터를 부적절하게 보호하면 엄중한 처벌을 받을 수 있는 추가적인 위험이 유발될 수 있습니다.

클라우드 및 IoT 에 대한 의존성 증가

사용자에게 마찰 없는 데이터 가용성을 제공하고 최소 권한을 준수하는 데이터 액세스를 규정하는 것은 종종 비즈니스에 큰 영향을 미치는 장애 요소이면서, 이와 동시에 각각에 영향을 미칠 수 있는 조직의 능력이 제한될 수 있습니다. 더 많은 기업이 업무상 중요한 기능을 위해 클라우드 및 IoT 장치에 의존함에 따라 민감한 데이터에 원활하면서 규정을 준수하는 액세스 기능을 제공하는 것이 점점 더 어려워지고 있습니다.

오늘날 조직은 하이브리드 클라우드를 사용하고 있으며 미래에 나오는 대부분의 애플리케이션은 클라우드를 지원할 것입니다. 최근 IDC 설문조사에 의하면 조직은 현재 워크로드의 53%가 IaaS 클라우드 모델에 배포되어 있다고 보고했습니다. 보안은 하이브리드 클라우드를 채택하는 원동력이자 방해 요소이기도 합니다. 이제 중요한 데이터는 수많은 지역, 데이터 센터 및 클라우드에 분산되어 있습니다. 이러한 데이터는 배치된 위치와 무관하게 기업 요건에 따라 보호되어야 합니다. 설문조사에 참여한 조직은 전체 기업 데이터의 절반이 클라우드에 저장되어 있을 것으로 추정합니다. 클라우드에 저장된 데이터 중에 48%는 민감한 데이터로 간주됩니다. 이에 따라 백업, 복구 및 데이터 비용/가치 평가가 최우선 순위에 들어갑니다.

기업은 클라우드뿐만 아니라 IoT 장치에서도 점점 더 민감한 데이터를 모으고 있습니다. 이러한 장치는 전체 시스템보다 처리 능력이 떨어지는 경우가 많지만 해킹 공격자는 IoT 장치를 공격 전략의 일부로 활용할 수 있는 능력을 보여주었습니다. IoT 장치 주변에 일반적인 보안이 미흡하게 통합된 이러한 기능은 조직이 기존의 컴퓨팅 장치 외에도 액세스, 모니터링 및 보안이 어려울 수 있는 IoT 장치를 해킹으로부터 방어할 수 있는 가장 좋은 방법을 결정해야 한다는 것을 의미합니다.

점점 더 복잡해지는 운영 중단

IDC 는 조직이 클라우드를 보호하는 능력에 있어서 더 많은 자신감을 보이고 있으며 클라우드로 이동하는 속도가 증가하고, 클라우드 기반의 보안 솔루션을 채택하는 일도 늘어나고 있지만 그 어느 때보다 조직에서 준비가 미흡한 것으로 보이는 한 가지 과제는 서서히 다가오는 잠재적인 해킹 침해에 대한 문제입니다.

최근 IDC 고객 설문조사에 의하면 응답자의 73%가 지난 2 년 동안 문제를 수습하기 위해 상당한 추가 리소스를 지출해야 하는 일과 관련된 IaaS 환경의 주요 보안 침해를 경험했다고 응답했습니다. 실제로 지난 2 년 동안 발생한 해킹 침해 건수의 중간값은 2.0 이었습니다.

백업 및 재해 복구(DR)에 대한 이전의 접근 방식은 최신 해킹 위협을 보호하기에는 기능이 충분하지 않습니다. IDC 모범 사례에서는 임무 수행에 필수적인 애플리케이션의 경우 1 시간 RTO, 중요하지 않은 애플리케이션의 경우엔 4 시간 RTO 를 권장합니다. 부정확하게 설계된 경우 특정 시점(스냅샷)의 복사본은 불완전하고 비효율적이며 공격에 취약할 수 있습니다. 흔히 접근 방식은 플랫폼 또는 구성 손상과 같은 환경 복구가 아닌 시스템 수준의 복구를 위해 설계되었습니다. 불량한 유지 관리 및 감염 테스트는 온전한 시점의 데이터 복사 방지 체계를 방해할 수도 있습니다.

IDC 조사에 의하면 작업 정지 시간의 "평균" 비용은 시간당 20 만 달러를 초과하지만 이는 회사 규모와 산업에 따라 달라집니다. 일부 조직에서는 IT 의사 결정권자가 Oracle E-Business Suite 또는 SAP Business One 과 같은 주요 ERP 애플리케이션의 작업 정지 시간이 시간당 20 만 달러를 초과할 수 있다고 보고했습니다. 일반적으로 이러한 비용은 개선 계획 및 인프라 구축을 결정할 때 조직을 안내하는 데 사용할 수 있습니다. 추정되는 비용에는 심각할 수도 있는 규제 비용을 포함하여 실제적인 수익 손실 및 복구 비용이 포함됩니다. 이러한 추정 비용에는 당혹스러운 보안 침해로 인해 발생할 수 있는 평판 비용 및 장기적인 브랜드 손상에 따른 비용은 포함되지 않습니다. 그러나 추정되는 비용은 조직이 침해 복원 인프라 전략에 대한 적절한 지출을 결정하는 데 사용할 수 있습니다. 다음은 최근 랜섬웨어의 예시입니다. 어느 다국적 IT 서비스 회사는 2020 년 4 월에 서버가 암호화되고 재택 근무 기능이 차단되며, 랩톱을 자동화하고 프로비저닝하는 데 사용되는 도구가 무력화되는 Maze 랜섬웨어가 자사의 네트워크를 침해했다는 사실을 공개적으로 인정했습니다. Maze 는 사이버 범죄자들이 감염된 시스템에서 데이터를 암호화할 뿐만 아니라 데이터를 추출하여 해당 데이터를 공개적으로 노출하겠다는 위협을 통해 더 높은 몸값을 갈취할 수 있다는 점에서 특히 악의적인 형태의 랜섬웨어라고 할 수 있습니다. 이로 인해 이 IT 서비스 회사에 미치는 영향에 따라 예상되는 서비스 복원 및 개선과 관련된 추가적인 법률 비용과 전문 서비스 비용이 2020 년 상반기에 5 천만 달러에서 7 천만 달러 범위로 추정되었습니다.

증가하는 지능형 해킹 공격

또한 IDC 는 지능형 해킹 공격 수가 계속해서 증가하고 있는 것으로 보고 있습니다. 업계 통계에 따르면 많은 해킹 공격이 200 일이 넘도록 탐지되지 않은 상태로 유지되기도 합니다. 네트워크에 숨어 있는 시간이 아주 길어지면 공격자가 백업 세트에 침입할 수 있는 맬웨어를 심을 수 있어서, 결과적으로 복구 데이터까지도 감염됩니다. 해킹 공격은 몇 주 또는 몇 달 동안 휴면 상태로 유지되어 맬웨어가 시스템 전체로 전파될 수 있습니다. 해킹 공격을 탐지한 후에도 조직 전체에 널리 퍼져 있는 맬웨어를 제거하는 것은 매우 어려울 수 있습니다.

상황 개요

사이버 복원력 개념

인프라 리소스가 클라우드 및 IoT 장치 전반에서 점점 더 많이 사용되고 있습니다. 하지만 기존의 방어 수단은 새로운 위협에 성공적으로 대응하는 데 효과가 없는 것으로 입증되었습니다. 결과적으로 조직은 보안에 대한 새로운 접근 방식을 취해야 합니다. 오늘날의 해킹 위협 환경에서는 데이터 라이프 사이클을 포괄하는 통합 솔루션이 필요합니다. 조직은 사이버 복원력 기능을 구축하기 위해서 방어와 탐지, 대응과 복구 사이의 라이프 사이클 단계를 단축하는 데 집중해야 합니다. 최근 실시한 IDC 설문조사에 의하면 응답자들은 클라우드 보안을 위한 중요한 기술 관행의 일환으로 "강력한 복원력 계획 수립" 방안을 확인하였습니다.

사이버 복원력 프레임워크

사이버 복원력은 조직이 해킹 공격을 견딜 수 있도록 설계된 프레임워크입니다. 이는 단일 보호 계층이나 단일 제품이 아니라 조직이 어떤 해킹 공격도 치명적이지 않도록 방어 환경을 구성하는 방법입니다. 사이버 복원력은 공격으로부터 복구 수단을 제공하는 반복적인 프로세스입니다. 일단 우회적으로 침입하면 쓸모 없게 되는 전통적인 방어 방법과 비교할 때, 사이버 복원력은 조직 전체에 걸쳐 지속적으로 경계를 할 수 있게 합니다.

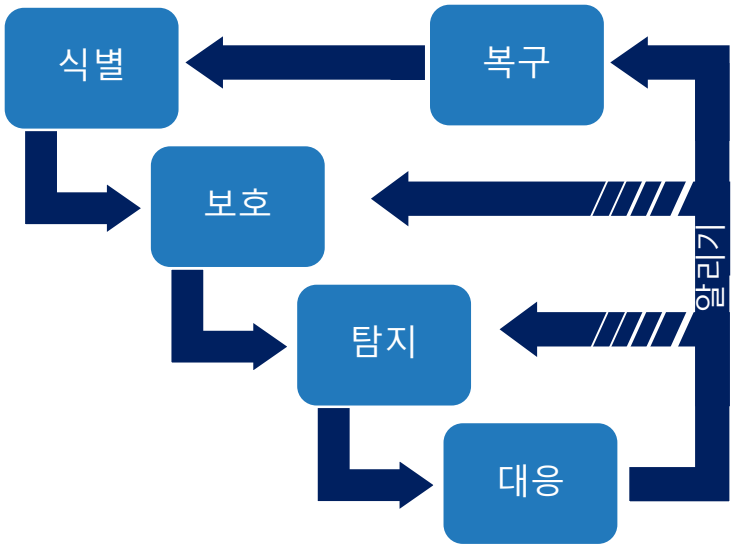
사이버 복원력 프레임워크의 5 가지 구성 요소는 다음과 같습니다(그림 5 참조).

- 식별: 핵심 자산 및 프로세스 매핑, 위험 및 준비 상태 평가 등
- 보호: 기존의 1 차 방어 보안 메커니즘
- 탐지: 보안 분석, 실시간 구성 데이터의 무결성 확인
- 대응: 보안 침해 또는 장애에 대한 대응
- 복구: 조정된 복구 메커니즘

사이버 복원력 프레임워크의 주요 이점은 비즈니스를 발전시킨다는 점입니다. 전통적으로 보안은 비즈니스의 오버레이로 작동해 왔습니다. 사이버 복원력은 보안 기능을 회사 자체에 통합하여 기업의 모든 영역에 5 가지의 구성 요소를 제공할 수 있게 합니다.

그림 5

사이버 복원력 프레임워크



출처: IDC, 2020 년

해킹 공격 대 여파

업계에서는 해킹 공격이 몇 번이고 계속해서 성공할 수 있다는 것을 보여주었습니다. 보안은 복잡하며 환경이 전적으로 안전하다는 것을 증명할 방법이 없습니다. 해커는 계속적으로 혁신적인 방법을 사용하여 조직에 침투하는데, 성공적인 공격을 시작하기 위해 필요한 모든 전술을 활용합니다. 조직이 기대할 수 있는 최선책은 강화된 인프라, 감사 가능한 기능과 프로세스, 잘 훈련된 사용자, 크랙 보안 직원 및 지속적인 모니터링 프로세스입니다. 이는 좋은 방책일 수 있습니다. 그러나 대부분의 조직에서는 공격 이후에 발생하게 되는 일에 새로운 초점을 맞추는 것이 핵심적인 일일 수 있습니다. 통제, 견제 및 균형에 대한 긴 점검 목록을 통해 해킹 공격이 어느 시점에서 성공할 것이라는 것을 미리 알고 있다면 공격 여파에 대비하는 것이 합리적이지 않을까요? 해킹 공격이 성공했을 때 기업은 탐지와 대응 사이의 주기, 대응과 복구 사이의 주기를 단축할 수 있는 방법을 찾아야 합니다. 성공적인 사이버 해킹 공격 이후에도 비즈니스가 지속적으로 정상 운영에 가까우면 가까울수록 좋습니다.

사업체는 잘못이 용서되지 않습니다. 공격이 얼마나 진행되었는지 또는 공격자가 조직에 어떻게 침투했는지는 신경 쓰지 않습니다. 사업은 지속되어야 하지만 지속성은 충분하지 않습니다. 오늘날 특히 위기 시점에서 고객은 지속성을 요구하고 있습니다. 이 디지털 세상에서 그들은 서비스를 항상 사용할 수 있기를 바라며 기업에서는 단순히 서비스 사용을 중단할 여유가 없

습니다. COVID-19 세계적 유행병이 닥치기 전에는 탄력적인 비즈니스 운영과 고객 경험 프로그램이 최하위 우선 순위였습니다. 하지만 세계적 유행병이 닥친 이후에 이들의 우선 순위가 1 위, 2 위가 되었습니다. 위기 상황에서는 지속적인 운영과 고객 관리가 최우선 과제입니다(그림 6 참조).

그림 6

C-Suite 우선 순위: COVID-19 이전 및 COVID-19 이후

COVID-19 이전 우선 순위(2020년 1월)

우선 순위	기업의 미래 의제 항목
1	디지털 신뢰 프로그램
1	디지털 인프라 복원력
3	데이터 프로그램 (비즈니스 운영, 제품 및/또는 생태계에 대한 인사이트 확보)
4	직장 혁신
4	제품/경험 혁신을 주도하는 소프트웨어 개발 기능
4	새로운 산업 생태계
7	탄력적인 비즈니스 운영
8	고객 경험 프로그램
9	연결 프로그램

COVID-19 이후 우선 순위(2020년 5월)

우선 순위	기업의 미래 의제 항목
1	탄력적인 비즈니스 운영
2	고객 경험 프로그램
3	데이터 프로그램 (비즈니스 운영, 제품 및/또는 생태계에 대한 인사이트 확보)
4	연결 프로그램
5	제품/경험 혁신을 주도하는 소프트웨어 개발 기능
6	디지털 신뢰 프로그램
7	새로운 산업 생태계
8	디지털 인프라 복원력
9	직장 혁신

n = 483(COVID-19 이전 우선 순위); n = 908(COVID-19 이후 우선 순위)

참고: 응답자는 글로벌 기술 의사결정권자입니다.

출처: IDC 의 CxO View of the Future Enterprise in the Digital Economy Survey, 2020 년 1 월~2 월 및 IDC 의 COVID-19 Impact on IT Spending Survey, 2020 년 5 월 7 일~14 일

탐지, 대응 및 복구 작업에서 운영 시간을 줄이는 전략을 활용함으로써 조직은 사고 비용을 절감할 수 있을 뿐만 아니라 궁극적으로 경쟁적 우위를 창출할 수 있습니다. IDC 는 혼란을 최소화할 수 있는 기업이 소비자 및 비즈니스 파트너와 신뢰를 구축하는 데 있어서 준비가 잘 되어 있지 않은 기업에 비해 상당한 이점이 있을 것이라고 믿고 있습니다.

향후 전망

사이버 복원력의 5 가지 핵심 기술

사이버 복원력 프레임워크는 표면적으로는 직관적으로 보일 수 있지만 기술 선택을 신중하게 해서 구현해야 합니다. 사이버 복원력 환경을 만들 수 있는 제품은 하나도 없지만 조직이 사이버 공격으로 인한 비즈니스 중단 가능성을 해결하기 위해 구현할 수 있는 핵심 기술이 있

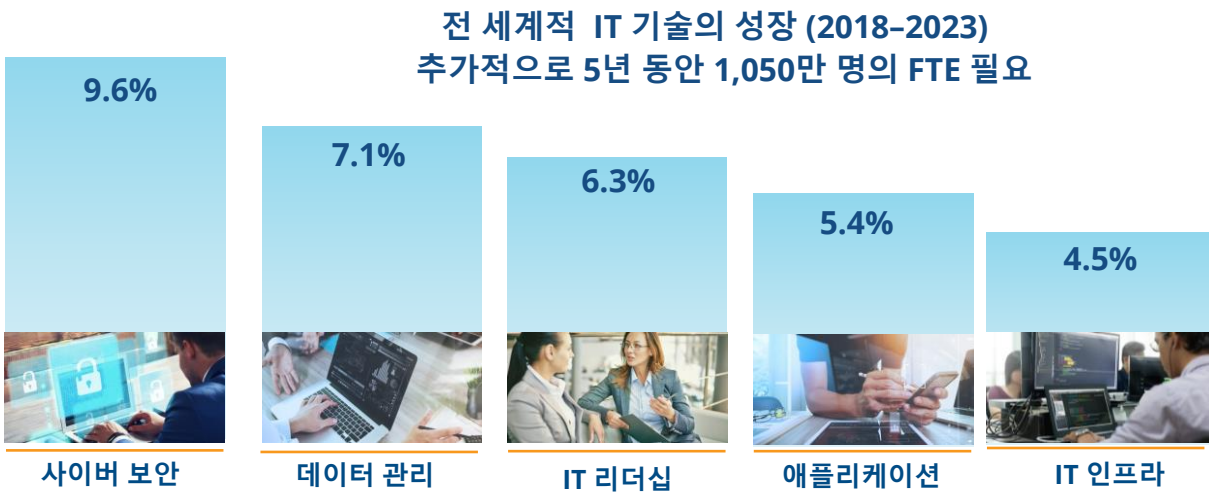
습니다. 다음 섹션에서 설명하는 5 가지 기술은 조직이 사이버 복원력 기능을 만들 수 있게 하는 중요한 역할을 합니다.

플랫폼 및 애플리케이션 데이터 복구를 위한 자동화 및 오케스트레이션

자동화는 보안 전문가에게는 한 동안 무서운 용어였습니다. 자동화 솔루션이 존재하기 때문에 자동 대응에 대한 관심이 업계 전반에 널리 퍼져 있습니다. 그러나 오늘날 광범위하게 자동화된 해킹 공격 환경에서는 IT 기술 부족 현상이 계속해서 성가신 문제가 되고 있고 이에 따라 인텔리전스 자동화가 핵심이 되며, 향후 5 년 동안 추가적으로 1,050 만 명의 FTE 가 필요합니다(그림 7 참조). 솔루션으로 기존의 방법에만 의존할 것이 아니라 보안 전문가는 오케스트레이션 및 자동화를 대응의 일부로 만들어 나가야 합니다.

그림 7

IT 기술 부족



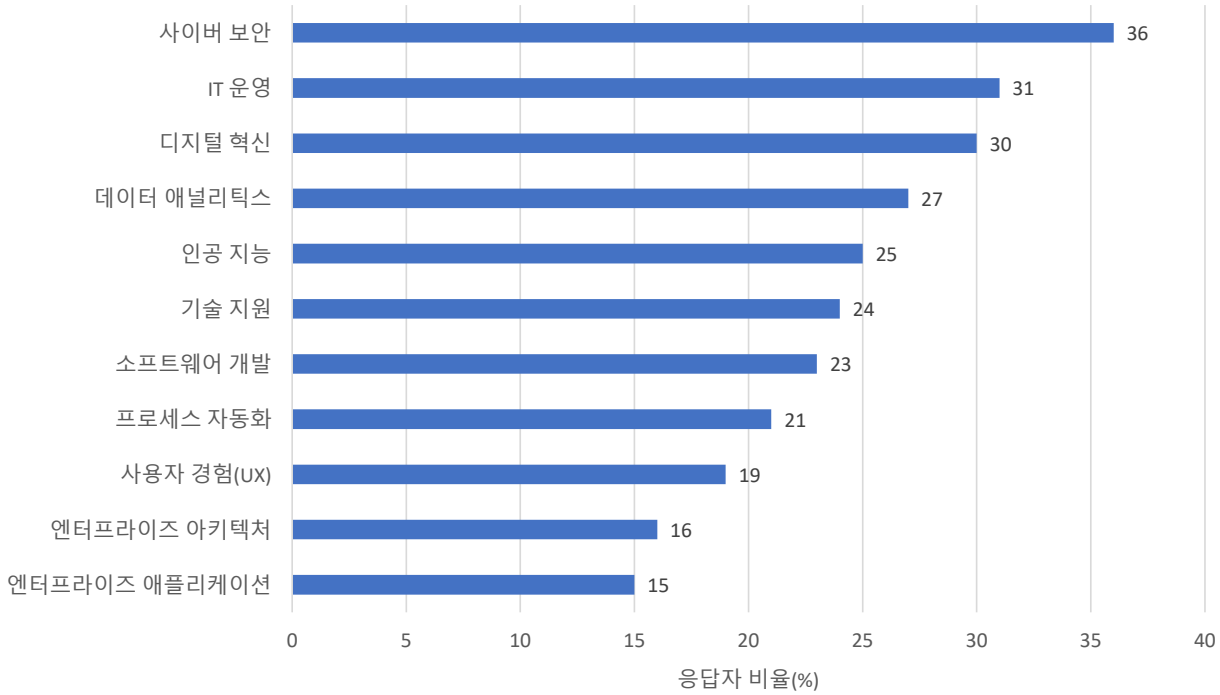
출처: IDC, 2020 년

위기 시점에서는 부족한 기술에 대한 수요만 증가합니다. 조직은 사이버 보안 및 IT 운영을 COVID-19 세계적 유행병으로부터 회복하는 데 필요한 최고의 IT 기술로 인식하고 있습니다(그림 8 참조).

그림 8

경제 회복의 첫 번째 파동에서 구축/재구축/고용에 필요한 중요한 IT 기술

Q. [COVID-19 세계적 유행병으로부터] 경제 회복의 첫 번째 파동에서 조직이 구축/재구축/고용하는 데 필요한 가장 중요한 IT 기술은 무엇입니까?



n = 888

출처: IDC 의 COVID-19 Impact on IT Spending Survey, 2020 년 6 월 4 일~15 일

오케스트레이션은 인간을 방정식 틀에서 벗어나게 하거나 맹목적인 정책 변경을 허용하는 것이 아니라 분석가를 증가시키고 정보에 대한 빠른 액세스 기능과 수동으로 할 수 있는 것보다 빠르게 대응할 수 있는 능력을 제공하는 것입니다. 또한 애플리케이션을 성공적으로 복구하려면 상호 연결된 시스템 및 데이터의 다중 단계적 복구가 필요합니다. 이러한 시스템을 수동으로 복구하면 인적 오류가 발생할 수 있으며 검증 및 테스트된 소프트웨어 템플릿을 통해 복구 프로세스를 코드화하면 복구 프로세스의 위험성을 완화시킬 수 있습니다.

전파된 맬웨어에 대한 페일 세이프 복사본의 에어갭으로 보호

에어갭(air gap)은 시스템 또는 네트워크를 다른 시스템이나 네트워크에서 물리적 또는 가상으로 분리하는 것을 말합니다. 예를 들어 기업은 매우 민감한 데이터가 들어있는 네트워크 또는 시스템을 일상적으로 운영되는 네트워크에서 완전히 분리하도록 선택할 수 있습니다.

경계 영역이 사라지고 기업은 조직 전체에서 데이터의 유동성을 기대하고 있지만 네트워크의 에어갭 세그먼트를 생성하는 능력은 그 어느 때보다 중요합니다. 최근 랜섬웨어 감염에서 볼 수 있는 것처럼 자동화된 맬웨어는 네트워크를 빠르게 침투하여 급격한 혼란을 유발시킬 수 있게 설계할 수 있습니다. 이로 인해 영향을 받는 시스템에 따라 정보가 내부에 노출되거나 잠재적으로 외부에 노출됩니다. 오늘날 모범 사례는 중요한 데이터의 에어갭 복사본을 생성하여 외부 노출을 완화하고 운영 중단 시간을 줄여 조직을 보호하며 불필요한 비용을 방지하는 것입니다.

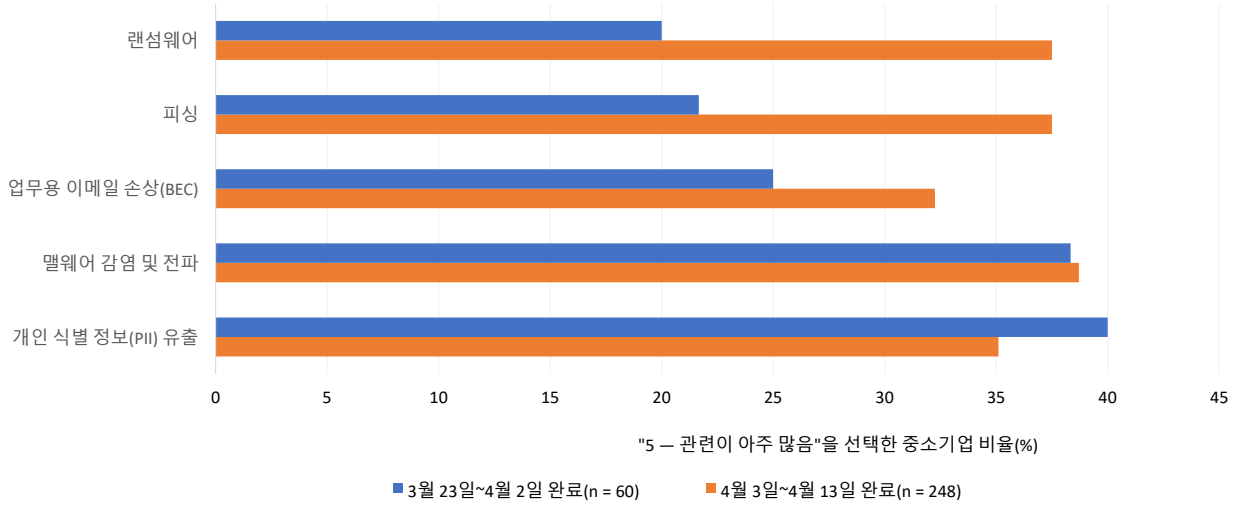
데이터 손상이나 삭제를 방지하기 위한 WORM(Write-Once, Read-Many)/불변 스토리지 기술

최근 랜섬웨어의 공격이 성공하는 것은 데이터의 손상 또는 삭제에 대한 강력한 보호 기능이 필요하다는 것을 보여줍니다. 사이버 범죄자들은 기회 주의자로서 공격할 수 있는 약한 순간을 노리고 있습니다. 최근 COVID-19 관련 맬웨어의 급증이 하나의 예시입니다(그림 9 참조).

그림 9

세계적 유행병과 함께 진화하는 위험에 대한 견해

Q. 다음 위험을 완화하는 데 있어서 보안 제품의 관련성을 평가해 주십시오 (1 = 관련 없음, 5 = 관련이 아주 많음).



출처: IDC 의 North America SMB Security Survey, 2020 년

공격자가 자신의 흔적을 숨기기 위해 로그를 삭제하는 것은 잘 알려져 있지만 데이터를 삭제하거나 손상시키면 비즈니스를 망칠 수 있습니다. RobbinHood, Maze, REvil 및 기타 최근 랜섬웨어 공격의 여파로 인해 많은 조직이 몸값을 지불한다고 하더라도 공격자가 암호화 키를 넘겨주지 않는다는 사실을 확인할 수 있었습니다. 어떤 경우에는 공격자가 제공한 키가 전혀 작동하지도 않았습니다.

조직은 변경할 수 없는 데이터를 제공할 수 있는 기술이 필요합니다. WORM(Write-Once, Ready-Many)/불변 스토리지 기술로 이러한 기업 니즈를 해결할 수 있습니다. WORM/불변 스토리지 기술을 사용하여 조직은 데이터의 무결성을 유지하고 최근에 가장 심각한 손상을 입혔던 해킹 공격에 맞서기 위해 비즈니스 복원력 기능을 유지할 수 있습니다. 소프트웨어 레이어와 하드웨어 레이어에는 여러 형태의 WORM 기술이 있습니다. 양쪽 모두 데이터가 변조되지 않도록 보장하고 전자적인 관리 체인을 부여하는 수단을 제공합니다.

복구 가능한 데이터를 신속하게 식별하기 위한 효율적인 시점의 복제본 및 데이터 검증

일단 해킹 공격이 발생하면 조직은 가장 최근의 양호한 데이터 복사본("골든 복사본")을 검증하고 신속하게 복구할 수 있는 방법이 필요합니다. 앞서 언급을 했듯이 많은 공격자들이 네트워크 내부에서 거의 1 년 동안 머물고 있으며 이에 따라 백업도 감염되는 경우가 많습니다. 이것이 여러 데이터 복사본을 유지 관리하기 위해 매우 효율적인 시점의 백업 기술이 필요한 이유입니다. 잠재적인 감염을 사전에 식별하고 수정 조치를 취하기 위해서는 이러한 복사본에 대한 지속적인 데이터 검증이 필요합니다. 또한 이는 복구 프로세스에 필요한 양호한 데이터 복사본을 빠르게 식별하는 데 도움이 됩니다. 데이터가 감염되지 않았는지 확인하기 위해 하드웨어와 소프트웨어 모두에 통합된 기능을 사용하여 백업 데이터를 확인할 수 있는 다양한 접근 방식이 있습니다.

재해 및 운영 복구 테스트 프로세스에서는 데이터 확인이 필수적인 요소입니다. 첫째, 백업/복제된 데이터가 무결성 상태이고 백업/복제가 예상대로 수행되었는지 확인합니다. 둘째, 백업/복제된 데이터를 검사하여 운영 데이터에서 발생한 동일한 감염이 백업/복제된 데이터로 확산되지 않았는지 확인합니다. 백업 중인 시스템에 따라 사용자는 여러 가지 데이터 확인 기술을 사용할 수 있습니다. 예를 들면 데이터베이스 시스템에는 광범위한 데이터 보호 솔루션 환경에서 기능을 보완하는 데 유용한 기본 분류 기능 및 검사 도구가 있을 수 있습니다.

가시성과 통제력을 확보하기 위한 통합 대시보드 및 오케스트레이션 리포트

규정 준수는 종종 조직의 전반적인 보안을 향상시키지 못한다고 하는 쪽으로 나쁜 평판을 얻고 있지만, 실제로는 적절한 통제의 타당성이 확립되어 있으며 데이터에 대한 효과적인 운영이 매우 효과적일 수 있어서 사전적인 예방 관리가 가능하다는 것입니다. 또한 규제를 준수하지 않는 것에 대한 벌금이 증가함에 따라 효과적인 리포트를 통해 조직이 규정을 준수하고 있다는 것을 입증할 수 있고, 이에 따라 비용이 많이 들어가는 감사 및 잠재적인 벌금과 관련된 시간과 비용을 절약할 수 있습니다. 감사 리포트는 어렵거나 진부할 필요가 없습니다. 효과적인 대시보드, 사전 구성 및 자동화된 리포트는 작업을 관리할 책임이 있는 사람들의 의욕을 획기적으로 향상시킵니다.

당면 과제/기회

오늘날의 비즈니스 환경에서 사이버 보안은 가장 우선적인 과제입니다. 보안을 위협하는 속도와 볼륨은 모든 규모의 조직에서 앞질러 나가야 하는 과제입니다. 이는 사이버 복원력 전략

의 계획 및 배포에 더 중요하다고 할 수 있습니다. 효과적인 사이버 복원력 전략은 해당 범위와 이해관계자가 광범위하며 다양한 구성 요소가 통합됩니다. 주요 이해관계자에는 보안, 운영, 엔지니어링, 법률 및 위험 전문가뿐만 아니라 데이터 소유자와 LOB(영업 부문) 임원도 포함됩니다. 이를 위해서는 우선 순위 및 지식의 깊이가 다른 조직 상호 간의 협업과 계획이 필요합니다. 이러한 조직적 역동성은 대규모 조직에서 흔히 볼 수 있는 문제지만 경영진 수준의 전략 계획 및 우선 순위 설정을 통해 해결할 수 있습니다.

결론

사이버 복원력은 데이터 및 애플리케이션 가용성의 핵심입니다. 또한 디지털 혁신(DX) 진행 과정의 핵심 구성 요소이기도 합니다. 조직은 적절한 사이버 복원력 기능이 없으면 비즈니스를 마비시킬 수 있는 해킹 공격에 점점 더 취약해 질 것입니다. 악의적인 공격 외에도 다양한 지역과 산업에 걸쳐 점차 늘어나고 있는 규제로 인해 지속적인 통제 검증 없이는 기업이 심각한 벌금에 처해질 수 있습니다.

실행되는 기능은 단순한 맬웨어 탐지, 백업 또는 DR 그 이상입니다. 최고 정보 책임자(CIO), 최고 정보 보안 책임자(CISO), 최고 위험 책임자(CRO), IT 운영진을 포함한 모든 비즈니스 부서의 주요 이해관계자가 모두 협력하여, 플랫폼을 비롯해 모든 위협에 대응하는 데이터 가용성을 제공하는 통합적인 라이프 사이클의 접근 방식입니다. 사이버 복원력 기능은 온프레미스와 클라우드 저장소 모두에 있어야 합니다. IT 조직은 사이버 복원력에 대한 포괄적인 접근 방식을 취하고 광범위한 사이버 위협을 해결하고 해킹 공격으로부터 신속하게 복구할 수 있는 기능을 제공하는 제품을 찾아야 합니다.

결론적으로 사이버 복원력은 해킹 공격으로부터 복구를 하기 위한 프레임워크입니다. 그러나 프레임워크의 각 단계를 다룰 수 있으려면 탄탄한 기반 기술들이 필요합니다. 보안은 더 이상 기밀성, 무결성 및 접근성에 대한 다양한 수준의 측면으로는 설명할 수 없으며, 항상 이들 세 가지 축을 모두 포괄해야 합니다. 사이버 복원력을 구현하는 조직은 고객이 비즈니스 가용성에서 그 차이를 발견하게 될 것이므로 미래에 경쟁적 우위를 차지하게 될 것입니다. 탄력적인 조직은 해킹 공격에 적응하고 신속하게 복구할 수 있는 조직입니다.

IDC 소개

IDC(International Data Corporation)는 정보 기술, 통신 및 소비자 기술 시장을 위한 마켓 인텔리전스, 자문 서비스 및 이벤트를 제공하는 세계적 선도 기업입니다. IDC 는 IT 전문가, 기업 경영진 및 투자 업계가 기술 구매 및 사업 전략에 있어 사실에 근거한 결정을 내릴 수 있도록 돕습니다. 1,100 명 이상의 IDC 애널리스트들이 전 세계 110 여 개국에서 전 세계는 물론 특정 국가와 지역을 대상으로 기술 및 업계의 기회와 동향에 관한 전문 지식을 제공합니다. 50 년 동안 IDC 는 고객이 주요 사업 목표를 달성하는 데 도움을 주는 전략적 통찰을 제공해 왔습니다. IDC 는 세계 유수의 기술 미디어, 연구조사 및 이벤트 회사인 IDG 의 자회사입니다.

글로벌 본사

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