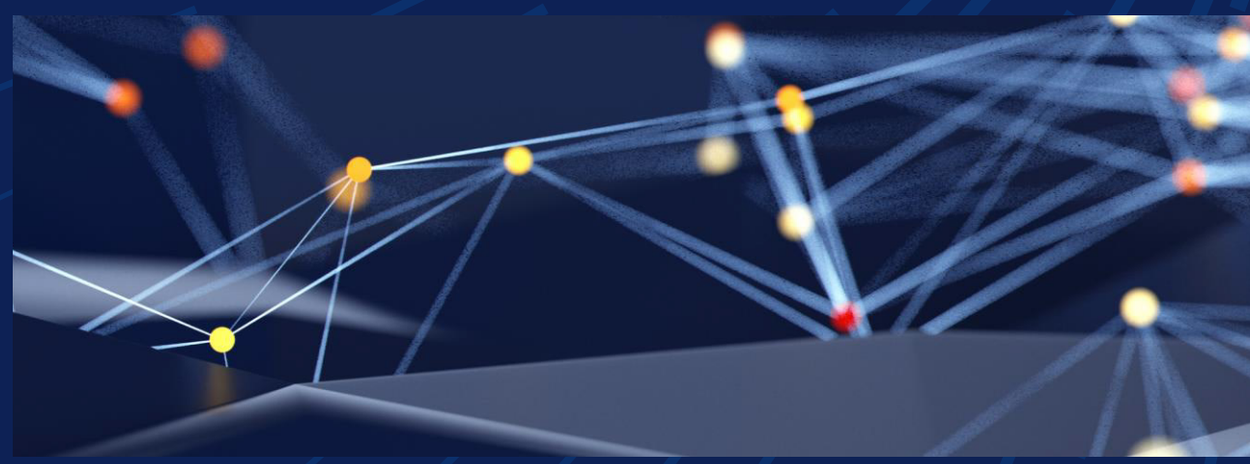
사이버 보안의 미래:

새로운 디지털 시대에 적응



사이버 보안 전문가는 공격을 방지하고 복구 계획을 수립하는 데 집중하는 편이지만 전반적인 보안 환경은 지속적으로 변화하고 있습니다. 따라서 다가올 미래에 대비하는 것이 중요합니다.

미래를 내다보면 포스트 퀀텀 암호화, 규제 환경의 변화, 새로운 위협이라는 세 가지 영역이 두드러집니다. 조직은 사용 가능한 솔루션을 계획하고 구현하여 지금 바로 행동에 나서야 합니다.

포스트 퀀텀 암호화의 등장

양자 컴퓨팅은 산업을 혁신할 가능성을 가지고 있으며, 기존 컴퓨터의 범위를 훨씬 넘어서 문제를 해결할 수 있는 놀라운 컴퓨팅 성능을 제공합니다. 하지만 이러한 능력이 현재의 암호화 방법을 쓸모없게 만들 수도 있습니다. 오늘날의 보안 통신 대부분을 뒷받침하는 RSA와 ECC와 같은 알고리듬은 충분히 발전된 양자 컴퓨터에 의해 몇 초 만에 해독이 가능합니다. 이러한 위협으로 포스트 퀀텀 암호화이 등장이 시급해졌습니다.

PQC(포스트 퀀텀 암호화)는 양자 컴퓨팅 시대에 보안을 유지하는 암호화 알고리듬 개발을 중심으로 발전합니다. NIST(National Institute of Standards and Technology)는 이러한 위험이 임박했음을 인식했으며 양자 내성 알고리듬을 표준화하는 데 앞장서고 있습니다.

기업의 경우 이러한 전환에 반드시 대비해야 합니다. PQC 솔루션을 조기에 도입하면 공격자가 양자 컴퓨팅 기능에 액세스할 때 데이터가 안전하게 유지됩니다.

Dell의 사이버 보안 부문 VP이자 사업부 보안 책임자인 Bobbie Stempfley 씨가 지적한 것처럼 조직은 다음 두 가지 핵심 영역에 초점을 맞춰 프로세스를 시작해야 합니다.

현재 사용 중인 모든 암호화 모델을 식별하고 인벤토리화하는 것입니다.

저장 상태 데이터뿐만 아니라 전송 중인 데이터도 고려해야 합니다. 키 관리, 코드 서명, 디바이스 식별, 보안 액세스 및 텔레메트리에 대해 생각해 보십시오. 포괄적인 인벤토리를 생성한 다음 로드맵을 구축합니다.

공급업체의 상태를 파악합니다.

현대의 기업은 수천 개의 공급업체를 보유할 수 있으므로 이로부터 발생할 수 있는 위험을 인식해야 합니다. 또한 변화에 대한 계획을 세워야 합니다.

이러한 초기 단계를 넘어서, 위험 평가를 수행하여 취약한 시스템을 파악하고, 전환 기간 동안 운영을 유지할 수 있도록 하이브리드 암호화 모델을 구현하고, 이미 양자 보안 솔루션을 모색하고 있는 공급업체들과 협업하되, 하나의 공급업체나 기술이 턴키 솔루션을 제공하는 경우는 없다는 것을 명심하십시오.

세계화에 따른 규제 변화

사이버 보안의 미래를 형성하는 또 다른 중요한 동인은 규제 환경의 변화입니다. 이제 규제는 규정 준수에 그치지 않고 상호 연결된 데이터 중심 환경에서 책임감을 갖고 기술 업그레이드를 주도하면서 시민들을 보호하는 핵심 프레임워크가 되고 있습니다. 하지만 빠르게 진화하는 가운데 여러 지역에 걸쳐 큰 폭으로 변화하면서 규정 준수의 복잡성이 증가하고 있습니다.

즉, 이러한 규제는 규정 미준수에 대한 처벌을 넘어 더 효과적인 사이버 보안 관행을 위한 촉매제 역할을 합니다. 규제 요건에 맞춰 정책을 적극적으로 조정하는 기업은 새로운 차원의 신뢰와 운영 효율성을 실현할 수 있습니다. 이를 위해 조직은 법률상의 변화에 적응하고, 정기적인 규정 준수 감사를 실시하고, 직원이 최신 표준에 따라 기밀 정보를 처리할 수 있도록 교육에 투자할 수 있는 유연성을 유지할 수 있는 거버넌스 프레임워크를 구축해야 합니다.

보안 분야의 경영진은 규정 준수를 준비할 때 이해하기 쉽도록 하고 사람들이 이를 제대로 이해하도록 하는 것이 중요합니다. 보안 전문가들은 보안 관련 용어로 이야기하는 경우가 많아 고객, 규제 기관 및 기타 이해 관계자들에게 그 의미가 잘 전달되지 않을 수 있습니다. 제대로 이해할 수 있도록 하는 것은 보안 전문가의 책임이지, 이를 해석하는 청취자의 책임이 아닙니다.

"가구가 다 들어찬 집을 들어서 옮기는 것처럼 양자 내성 암호로 전환하는 것을 생각해 보십시오. 아주 복잡할 것이며, 문제는 이 과정에서 그 무엇도 망가트리지 않는 것입니다."

Bobbie Stempfley
Dell Technologies 사이버 보안 부사장 겸 사업부 보안 책임자

위협(및 방어) 환경의 진화

AI는 비즈니스를 혁신하고, 생산성을 높이며, 인간의 잠재력을 발휘할 수 있는 새로운 기회를 발굴하고 있습니다. 사이버 보안에 있어 AI는 악의적인 공격자와 방어자 모두에게 다음과 같은 이점을 제공합니다.

악의적 이용: AI는 정교하게 사람을 속이는 스피어 피싱 및 딥페이크처럼 보다 정교한 공격을 가능하게 해줍니다.

방어적 사용: AI는 다음을 통해 방어자를 돕습니다.

- 방대한 양의 보안 데이터를 신속하게 처리.
- 보다 효과적인 위협 우선순위 지정.
- 탐지 및 대응 성능 향상.

보안 툴이 계속해서 개선되는 가운데 자연어 처리를 통해 보안 전문가가 시스템과 보다 직접적으로 상호 작용하고 시스템이 사전 예방적으로 사이버 보안 조치를 취할 수 있습니다.

조직은 이러한 기능들을 활용하기 위해 노력해야 하며 이와 동시에 교육 및 기타 방어 메커니즘을 최신 상태로 유지해야 합니다. 교육은 직원들이 보다 정교한 공격의 피해자가 되는 것을 방지하는 가장 좋은 방법입니다.

비밀번호 없는 방식으로 전환

비밀번호는 더 이상 ID 및 액세스 관리에 있어 가장 안전한 방법이 아닙니다.

기존의 비밀번호 기반 시스템은 최근의 사이버 보안 요구 사항에 적합하지 않은 시스템이 되어가고 있으며, 심각한 취약성을 드러내고 있습니다. 비밀번호는 자격 증명 자동 공격, 피싱 및 무차별 대입 공격 시도와 같은 공격에 취약해서 조직이 불필요한 위험에 노출되는 경우가 종종 있습니다. 또한 비밀번호 재사용 또는 취약한 비밀번호 생성과 같은 부적절한 사용자 행동이 이러한 취약성을 가중시킵니다.

생체 인식, 인증서 및 하드웨어 토큰과 같이 비밀번호 없는 인증 방법은 비밀번호와 관련된 위협 전체를 없애고 더욱 강력하면서 안전한 대안을 제공합니다. 비밀번호가 없는 시스템으로의 전환은 ID 및 액세스 관리의 중요한 발전으로, 보안 조치는 증가하는 사이버 위협에 맞춰 조정됩니다.

비밀번호 미사용 기술을 채택하면 공격 노출 지점 감소, 더 빠르고 원활한 로그인을 통한 사용자 경험 개선, 비밀번호 관련 인시던트 감소를 통한 IT 비용 절감 등 다양한 이점이 발생할 수 있습니다. 발전된 방법을 사용하면 보안 태세를 강화하고 조직의 규정 표준 준수가 가능합니다. 비밀번호 없는 시스템으로의 전환은 단순한 추세에 그치지 않고 개인과 조직 모두에 있어 보다 안전하고 효율적인 디지털 생태계를 구축하는 필수 단계가 되어가고 있습니다.

결론

사이버 보안은 양자 컴퓨팅, 규정 변화, 점점 더 정교해지는 위협으로 인해 대대적인 변화에 접어들고 있습니다. 여기에 대비하기 위해 조직은 포스트 퀀텀 암호화, AI 기반 방어, 비밀번호 없는 인증과 같은 혁신을 수용해야 합니다. 기업은 준비, 협업 및 전략적 투자를 우선시하면서 보다 안전하고 회복탄력성이 뛰어난 디지털 환경을 구축할 수 있습니다. 지금이 행동해야 할 때이죠.

도움이 될 수 있는 Dell 제품 및 솔루션

주요 **Dell** 솔루션	설명
Cybersecurity Advisory Services	지금의 위협과 새로운 위협을 포함하여 진화하는 위협 환경에 대비하는 데 도움이 되는 전문가 지침을 제공합니다.
vCISO	가상 최고 정보 보안 책임자이자 사이버 보안 전문가로 위험을 식별 및 관리하는 데 도움을 줄 수 있으며 전략적 의사 결정을 안내할 수 있습니다.

dell.com/cybersecuritymonth에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.