DELL Technologies

악의적 내부자: Dell Technologies와 함께 사이버 보안 및 회복탄력성 강화

악의적인 내부자 공격의 증가하는 위협

악의적인 내부자 공격은 오늘날의 비즈니스 환경에서 가장 시급한 사이버 보안 위협 중 하나가 되었습니다. 외부 위협과 달리, 악의적인 내부자는 조직 내에서 어느 정도의 신뢰와 액세스 권한을 이미 보유하고 있으므로 이들의 행동은 상당한 피해를 주고 탐지하기 어렵습니다. 기밀 데이터에 접근하는 것부터 시스템을 방해하는 것까지, 내부자 공격은 중요한 운영을 마비시키고 심각한 재정적 및 평판적 손실을 초래할 수 있습니다.

Dell Technologies는 이러한 공격으로 인한 위험이 증가하고 있음을 인지하고 비즈니스가 악의적인 내부자로 인한 위험을 식별, 방지 및 완화할 수 있도록 혁신적이고 확장 가능한 솔루션을 개발합니다. Dell Technologies는 최첨단 기술과 전문가 주도 서비스를 결합하여 조직이 이러한 내부 위협에 미리 대비할 수 있도록 지원하고 있습니다.

악의적인 내부자 공격이란 무엇입니까?

악의적인 내부자 공격은 조직 내의 개인들이 자신의 액세스 권한을 악용하여 데이터를 손상시키거나 운영을 중단시키거나 개인, 재무 또는 경쟁 목표를 위해 기밀 정보를 추출할 때 발생합니다. 이러한 개인은 직원, 계약자, 파트너 또는 회사 시스템과 네트워크에 합법적으로 액세스할 수 있는 사람일 수 있습니다.

악의적인 내부자 공격의 작동 방식

악의적인 내부자는 신뢰받는 위치를 악용하여 기존의 보안 방어 체계를 우회합니다. 일반적인 기법은 다음과 같습니다.

1. **데이터 도난:** 기밀 고객 데이터, 지적 재산 또는 재무 기록을 유출합니다.
2. **방해 행위:** 비즈니스 운영을 방해하거나 평판을 훼손하기 위해 의도적으로 IT 시스템을 손상시킵니다.
3. **자격 증명 남용:** 도용되거나 오용된 자격 증명을 사용하여 액세스 권한을 격상하거나 더미 계정을 생성합니다.
4. **외부 공격자와의 협업:** 금전적 이득을 위해 외부 사이버 범죄자와 액세스 권한 또는 기밀 정보를 공유합니다.

신뢰, 내부 지식 등 두가지 이점을 활용하여 악의적 내부자는 외부 공격자에 비해 매우 위험합니다.

비즈니스에 미치는 영향

악의적인 내부자 공격의 피해는 광범위하며, 금전적 손실을 넘어 심각한 수준에 이르고 있습니다. 비즈니스는 다음과 같은 결과에 직면할 수 있습니다.

금전적 손실

민감한 정보 도용, 사기 또는 방해 행위는 수백만 달러에 달할 수 있는 수익 및 복구 비용으로 이어집니다.

운영 중단

시스템 방해 행위나 데이터 파괴는 운영을 중단시켜 지연, 기회 상실 및 생산성 저하를 초래할 수 있습니다.

평판 손상

내부자에 의한 침해 또는 공격은 클라이언트 및 이해 관계자의 신뢰를 손상시켜 고객 충성도와 시장 인식에 영향을 미칩니다.

규정 미준수

업계마다 다르지만, 내부자 공격은 의료나 금융과 같은 기밀 데이터가 유출될 경우 막대한 벌금과 처벌로 이어질 수 있습니다.

실제 사례

2020년에 주요 금융 기관에서 근무하던 IT 계약업체가 의도적으로 중요한 시스템 구성을 삭제하여 **10시간 이상**의 네트워크 중단을 야기했습니다. 이러한 방해 행위는 **수백만** 달러의 재정적 손실, 막대한 복구 비용, 그리고 평판 손상으로 이어졌습니다. 이러한 인시던트는 내부자 위협의 파괴적인 잠재력을 보여주고 강력한 탐지 및 예방 조치의 시급성을 강조합니다.

예상 비용

2024년 Ponemon Institute 연구에 따르면 내부자 관련 사고의 평균 비용은 **499만 달러**로 추정되며, 모든 침해 사고의 거의 **55%**를 차지합니다. 이 수치에는 탐지, 복구 및 완화 비용이 포함되어 있으며, 이는 조직이 내부자 위험에 대한 사전 예방적 방어에 투자해야 할 중요한 필요성을 보여줍니다.

83%

지난 1년 동안 최소 한 건의 내부자 공격을 보고한 조직의 비율

출처: 2024년: Cybersecurity Insiders 보고서

Dell Technologies와 함께 악의적인 내부자 공격에 대응

Dell Technologies는 악의적인 내부자 위협에 대응할 수 있는 포괄적인 툴 및 서비스 생태계를 제공하여 조직이 예상치 못한 상황에 대비할 수 있도록 지원합니다.

Dell Trusted Device로 엔드포인트 보호

엔드포인트는 종종 내부자 위협의 진입점 역할을 합니다. Dell Trusted Device는 최첨단 보안 기능을 하드웨어에 통합하여 엔드포인트를 강화하고 기밀 데이터를 보호합니다.

- **Dell SafeBIOS:** 펌웨어 무결성을 보장하여 하드웨어 수준에서 시스템 운영을 조작하려는 시도를 차단합니다.
- **SafeID:** 자격 증명 데이터를 보호하여 무단 액세스 및 자격 증명 남용을 방지합니다.
- **SafeData:** 기밀 데이터를 포괄적으로 암호화하여 가로채거나 추출한 정보를 악의적인 내부자가 읽을 수 없도록 합니다.

조직은 이러한 솔루션을 배포하여 위협이 내부적으로 발생하든 외부적으로 발생하든 관계없이 엔드포인트를 안전하게 보호할 수 있습니다.

CrowdStrike를 통한 사전 예방적 위협 탐지

내부자 위협을 식별하려면 사용자 행동을 파악하고 모니터링해야 합니다. Dell 솔루션에 통합된 CrowdStrike는 인공 지능과 행동 분석을 활용하여 내부자 위협을 나타내는 이상 징후를 탐지합니다.

예를 들어, 업무 외 시간 동안 비정상적인 데이터 전송이나 네트워크의 중요 영역에 대한 무단 액세스가 즉시 감지되어 신속한 대응이 가능합니다. 최근 미국의 한 의료 조직은 사전 예방적 위협 탐지를 활용하여 환자 데이터를 유출하려는 직원의 시도를 파악하고 차단하여 막대한 비용 손실을 방지했습니다.

Dell PowerProtect를 통한 향상된 데이터 보호

Dell PowerProtect는 안전한 백업, 에어 갭 스토리지 및 중요 데이터의 변경 불가능한 복사본을 통해 강력한 방어선을 제공합니다. 기밀 정보가 변경이나 삭제되지 않도록 보호함으로써, 데이터 무결성을 대상으로 하는 내부자 공격을 효과적으로 무력화할 수 있습니다.

예를 들어, 한 제조 회사에서는 불만을 품은 직원이 설계 파일을 파괴하려고 시도했습니다. Dell PowerProtect의 복구 볼트를 통해 회사는 몇 시간 내에 운영을 복구하여 중단을 방지하고 비즈니스 연속성을 유지할 수 있었습니다.

Dell Professional Services를 통한 신속한 인시던트 복구

내부자 위협이 인시던트로 확대되면 신속한 복구가 필수적입니다. 원격 데이터 복구 및 인시던트 대응을 비롯한 Dell Professional Services는 비즈니스가 데이터와 시스템을 신속하게 복구할 수 있도록 보장합니다. Dell 전문가가 프로세스를 주도하여 다운타임을 최소화하고 영향을 완화합니다.

이는 악의적인 내부자 위협에 도움이 될 수 있는 Dell 솔루션 포트폴리오의 몇 가지 예에 불과합니다.

Dell PowerSwitch Networking 및 SmartFabric OS를 통한 고급 네트워크 보안 및 마이크로 세분화

인프라스트럭처 전반에 걸쳐 고급 네트워크 세분화, 엄격한 액세스 제어 및 실시간 트래픽 분석을 제공하여 제로 데이 공격에 대한 방어를 강화합니다.

다중 계층 보안 접근 방식의 중요성

내부자 위험에 대한 효과적인 방어를 위해서는 여러 계층의 보호가 필요합니다. 다중 계층 보안 전략을 구현하면 어떤 취약성도 위협이 되지 않습니다. 주요 단계는 다음과 같습니다.

방어 기능을 강화하기 위한 주요 단계

- **제로 트러스트 원칙:** 모든 액세스 요청을 지속적으로 검증하고 경계 내에서도 본질적으로 어떤 엔터티도 신뢰할 수 없다고 가정합니다.
- **RBAC(Role-Based Access Controls):** 역할에 필요한 시스템 및 데이터로만 직원 액세스를 제한합니다.
- **고급 암호화 솔루션:** 저장된 데이터와 전송 중인 데이터를 암호화하여 데이터 도난을 효과적으로 무력화합니다.
- **직원 인식 및 교육:** 악의적 활동에 우발적으로 참여하는 것을 방지하기 위해 보안 인식 프로그램을 정기적으로 실시합니다.
- **정기적인 시스템 테스트:** 침투 테스트 및 취약성 검사를 수행하여 방어 체계의 신뢰성을 유지합니다.

Dell Technologies의 솔루션으로 강화된 이러한 관행들은 악의적 내부자에 대비하는 강력하고 총체적인 보호 프레임워크를 구축합니다.

전략적 파트너십을 통한 방어 강화

Dell Technologies는 **CrowdStrike** 및 **Secureworks**를 비롯한 업계를 선도하는 사이버 보안 공급업체와 협력하여 솔루션을 강화하고 있습니다. CrowdStrike는 엔드포인트 보안을 강화하고 손상 지표에 대한 중요한 Threat Intelligence를 제공하며, Secureworks는 지능형 공격 탐지 및 대응 서비스를 제공합니다. 이러한 협업을 통해 Dell의 고객은 통합된 최첨단 기술 생태계의 이점을 누릴 수 있습니다.

사이버보안을 위해 Dell Technologies를 선택해야 하는 이유

Dell Technologies는 다중 계층 사이버 보안 솔루션의 업계 표준을 지속적으로 정립하고 있습니다. 비즈니스는 업계를 선도하는 Dell의 전문 지식, 긴밀한 파트너십, 오늘날의 진화하는 위협 환경에 적응하는 혁신적인 제품군의 이점을 누릴 수 있습니다. 엔드포인트 보안부터 내부자 탐지, 인시던트 복구에 이르기까지 Dell Technologies는 신뢰를 구축하고 성장을 뒷받침하게 하는 완전한 회복탄력성 프레임워크를 제공합니다.

Dell Technologies와 함께 회복탄력성이 뛰어난 미래를 위한 노력

Dell Technologies의 포괄적이고 확장 가능한 솔루션으로 악의적인 내부자 위협으로부터 비즈니스를 보호하십시오. Dell과의 파트너십을 통해 운영을 보호할 뿐만 아니라 비즈니스 연속성을 보장하고, 고객 신뢰를 증진하며, 조직의 미래 지향성을 높일 수 있습니다. 지금 바로 Dell Technologies에 문의하여 사전 예방적 방어 구현에 대해 자세히 알아보십시오.

Dell Technologies는 내부자 위협에 대응하고, 중요한 자산을 보호하며, 역동적인 디지털 환경에서 비즈니스를 성장시킬 수 있도록 지원하는 신뢰할 수 있는 파트너입니다. 미래의 보안은 곧 성공의 미래이며, Dell Technologies과 도와드립니다.

Dell.com/SecuritySolutions에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.

Dell 솔루션에 대한 자세한 정보

Dell Technologies 전문가에게 문의

추가 리소스 보기

대화에 참여: #HashTag

DELL Technologies