DELL Technologies

MITM(Man-in-the-Middle): Dell Technologies와 함께 사이버 보안 및 회복탄력성 강화

MITM(Man-in-the-Middle) 공격의 위협 증가

MITM(Man-in-the-Middle) 공격은 여전히 가장 교묘하고 위험한 사이버 보안 위협 중 하나입니다. 악의적인 행위자가 들키지 않고서 비공개 통신을 가로채고 변경하는 이러한 공격은 여러 산업에서 크고 작은 모든 기업을 표적으로 삼습니다. 전자 상거래 플랫폼에서 금융 기관에 이르기까지, 어떤 조직도 이러한 위험으로부터 자유롭지 않습니다. MITM 공격은 데이터 도난, 금융 부정 행위, 평판 훼손으로 이어지는 경우가 많아 점점 더 디지털화되는 환경에서 커다란 위협이 되고 있습니다.

Dell Technologies는 기업이 이러한 지능형 공격으로부터 스스로를 보호할 때 직면하는 고유한 당면 과제를 잘 알고 있습니다. Dell Technologies는 혁신적이고 확장 가능한 보안 솔루션을 제공함으로써 기업이 MITM 위협을 무력화하고 자산을 보호하며 비즈니스 무결성을 유지할 수 있도록 지원합니다.

MITM(Man-in-the-Middle Attack)이란?

MITM(Man-in-the-Middle) 공격은 사이버 범죄자가 두 당사자 사이에서(예: 직원과 기업 서버 사이에서 또는 고객과 비즈니스 웹사이트 사이에서) 통신을 비밀리에 가로챌 때 발생합니다. 공격자의 목표는 기밀 데이터를 훔치는 것부터 악의적인 목적으로 통신을 조작하는 것까지 다양할 수 있지만 그 결과는 한 가지입니다. 바로, 신뢰 훼손과 보안 침해입니다.

일반적인 MITM 기법

공격자가 가장 많이 사용하는 방법 중 몇 가지는 다음과 같습니다.

Wi-Fi 도청: 사이버 범죄자들이 안전하지 않거나 손상된 공용 Wi-Fi 네트워크를 악용하여 통신을 가로챕니다.

DNS 스푸핑: 공격자가 DNS 레코드를 변조하여 사용자를 사기성 웹사이트로 다시 라우팅함으로써 의심을 받지 않고 기밀 정보를 수집합니다.

세션 하이재킹: 공격자가 활성 세션 자격 증명을 알아내어 개인 계정에 무단으로 액세스합니다.

SSL 스트라이핑: 이 기법은 보안 HTTPS 연결을 취약한 HTTP 연결로 다운그레이드하여 기밀 정보를 노출합니다.

이러한 적응 능력으로 인해 MITM 공격은 겉보기에 합법적인 것처럼 보이는 일상적인 비즈니스 트랜잭션과 상호 작용을 악용하므로 특히 악의적입니다.

비즈니스에 미치는 영향

MITM 공격의 파급 효과는 즉각적인 인시던트를 훨씬 뛰어넘습니다. 가장 해로운 결과 중 일부는 다음과 같습니다.

매출 손실

자격 증명 도난과 운영 침해로 인해 직접적인 손실뿐만 아니라 복구 비용까지 재정적 부담이 늘어나는 경우가 많습니다.

운영 차질

공격 해결에 소요되는 시간과 리소스는 중요한 비즈니스 기능을 저해하여 생산성과 성장에 영향을 미칩니다.

신뢰 붕괴

고객의 개인 정보가 침해되면 고객의 신뢰도가 급격히 떨어져서 장기적인 평판 훼손으로 이어질 수 있습니다.

규제 후속 조치

엄격한 규정 준수 요건이 적용되는 업계의 기업들은 데이터 침해 후 벌금이나 제재를 받을 수 있습니다.

실제 사례

한 가지 놀라운 사례로, 암호화되지 않은 온라인 지불 플랫폼이 SSL 스트라이핑 공격의 피해를 입은 글로벌 소매 기업이 있습니다. 공격자는 결제 중에 고객으로부터 신용 카드 정보를 가로챘습니다. Dell Technologies의 엔드포인트 보호 툴을 비롯한 신속한 탐지 및 전략적 보안 조치를 통해 이 회사는 공격을 차단하고 장기적 피해를 완화할 수 있었습니다. 이 시나리오는 즉각적인 위험과 계층화된 방어의 필요성을 잘 보여줍니다.

359억

전 세계적으로 알려진 데이터 침해 건수

출처: 2024년 5월: PureWL 보고서

Dell Technologies와 함께 MITM 공격에 대응

Dell Technologies는 MITM 위협이 피해를 입히기 전에 차단하도록 설계된 포괄적이고 미래 지향적인 툴을 조직에 제공합니다.

Dell Trusted Device로 엔드포인트 보호

엔드포인트는 MITM 위협이 자주 발생하는 곳이므로 우선적으로 보호해야 합니다. Dell Trusted Device는 최첨단 보안을 하드웨어에 직접 내장합니다. 예:

- **Dell SafeBIOS**는 부트 순서 무단 변조로부터 시스템 무결성을 보호합니다.
- **SafeID**는 사용자 인증 데이터를 보호하여 또 다른 보호 계층을 제공함으로써 자격 증명 도난을 철저히 방지합니다.
- **Dell SafeData**는 기업 방화벽 내부와 외부의 기밀 정보를 보호하는 포괄적인 암호화 기능을 제공함으로써 가로챈 데이터를 읽을 수 없게 만듭니다.

엔드포인트 시스템에 대한 신뢰를 강화하기 위해 이러한 기능이 글로벌 기업에 배포되었습니다. 예를 들어, 한 다국적 제조 회사는 Dell Trusted Device를 사용하여 기업 노트북에 대한 표적 MITM 공격으로부터 재택/원격 근무자를 방어함으로써 고위험 출장 시나리오에서도 안전한 연결을 보장했습니다.

CrowdStrike를 통한 고급 탐지

MITM 위협은 실시간으로 탐지하고 대응하는 것이 중요합니다. Dell Technologies의 생태계와 통합된 CrowdStrike는 인공 지능 및 행동 분석을 활용하여 의심스러운 활동을 모니터링하고 무력화합니다. 지속적인 모니터링은 위협이 종종 숨어 있는 하이브리드 환경 전반에서 보호를 보장합니다. 기업은 이상 징후를 사전 예방적으로 식별함으로써 피해가 발생하기 전에 잠재적 MITM 시도를 제거할 수 있습니다.

예를 들어, 한 금융 기관은 고급 탐지 기술을 사용하여 고객 대상 포털에 대한 침입을 성공적으로 탐지하고 완화했습니다. 이 플랫폼의 AI는 SSL 스트라이핑을 나타내는 비정상적인 네트워크 활동을 식별하여 문제를 즉각적으로 해결했습니다.

Dell PowerProtect로 Data Protection 강화

고급 방어 체계를 갖춘 조직도 보안 침해를 경험할 수 있습니다. 그래서 Dell PowerProtect가 필요합니다. Dell PowerProtect는 불변성 및 에어 갭 스토리지와 같은 기능을 통해 공격 중에 중요한 비즈니스 데이터를 변경, 파괴, 액세스할 수 없도록 보호합니다. PowerProtect Cyber Recovery 볼트는 기본 네트워크로부터 기밀 데이터를 격리함으로써 추가적인 보안을 제공합니다. 따라서 최악의 경우에도 민감한 정보가 손상되지 않고 복구 가능합니다.

이 기술은 DNS 스푸핑 공격을 겪은 의료 기관에서 중요한 역할을 했습니다. 이 기관은 PowerProtect의 변경 불가능한 백업 및 복구 볼트를 활용하여 데이터 손실 없이 신속하게 운영을 복원했습니다.

신속한 대응 및 복구 서비스

Dell Technologies의 Data Protection Services는 보안 침해 발생 시 전문가가 주도하는 신속한 복구를 제공하여 기술을 보완합니다. 원격 데이터 복구에서 인시던트 대응에 이르기까지, 이러한 솔루션은 다운타임을 완화하고 운영 중단을 최소화합니다. 초를 다투는 상황에서 신뢰할 수 있는 파트너가 있으면 안심하고 복구할 수 있습니다.

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 제로데이 공격에 대한 방어를 강화합니다.

다계층 접근 방식으로 보안 강화

MITM 공격에 완전히 대처하기 위해 조직은 다각적인 보안 전략을 구현해야 합니다. Dell Technologies는 다음과 같은 실행 가능한 단계를 강조합니다.

- **제로 트러스트 원칙 채택:** 기업 네트워크 내부와 외부를 가리지 않고 모든 지점에서 모든 활동과 사용자 액세스를 확인합니다.
- **고급 암호화 사용:** 모든 통신에 대한 포괄적인 암호화는 공격자가 가로챈 데이터를 사용할 수 없게 만듭니다.
- **MFA(Multi-Factor Authentication) 구현:** MFA는 시스템에 인증 계층을 추가하여 무단 액세스 취약성을 크게 낮춥니다.
- **직원 교육:** 피싱 수법, 의심스러운 Wi-Fi 사용, 확인되지 않은 링크와 같은 위험을 강조하여 직원들의 경계심을 강화합니다.
- **정기적인 시스템 테스트:** 빈번한 침투 테스트 및 업데이트는 취약성을 식별하고 방어 체계를 최신 상태로 유지하는 데 도움이 됩니다.

이러한 관행과 더불어 Dell Technologies의 포괄적인 보안 오퍼링을 사용하면 진화하는 위협에 대한 강력하고 적응력이 뛰어난 방어 체계를 갖출 수 있습니다.

전략적 파트너십의 가치

Dell Technologies는 CrowdStrike 및 Secureworks와 같은 선도적인 사이버 보안 회사들과 협업하여 오퍼링을 더욱 강화합니다. 이러한 파트너십 전반에 걸쳐 전문 지식을 통합함으로써 Dell Technologies는 가능한 모든 공격 벡터를 해결할 수 있습니다. 예를 들어 CrowdStrike는 위협 인텔리전스로 Dell 플랫폼을 강화하여 엔드포인트 보호를 강화하고, Secureworks는 진화하는 위험에 대해 실행 가능한 통찰력을 제공하여 지속적인 준비와 적응을 보장합니다.

Dell Technologies Advantage

Dell Technologies를 선택한다는 것은 사이버 보안 혁신의 신뢰할 수 있는 리더와 파트너십을 맺는 것을 의미합니다. 엔드포인트 보호, 데이터 복구, 협업 파트너십을 통해 Dell Technologies의 포괄적인 솔루션은 조직이 공격자보다 앞서 나갈 수 있도록 지원합니다.

Dell Technologies의 포괄적인 MITM 솔루션으로 비즈니스를 보호하고, 고객 신뢰를 유지하고, 미래 지향적인 운영을 실현하십시오. 안전하고 회복탄력성이 뛰어난 비즈니스 미래를 만들기 위해 오늘 바로 저희에게 연락주십시오.

Dell Technologies와의 파트너십을 맺으면 사이버 위협에 적극적으로 대응하고, 고객 및 이해관계자와 지속적인 신뢰를 쌓고, 점점 더 불안전해지는 디지털 세상에서 운영 성공을 보장할 수 있습니다. 더 안전한 미래는 Dell Technologies와 함께 시작됩니다.

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

Dell 솔루션에 대한 자세한 정보

Dell Technologies 전문가에게 문의

추가 리소스 보기

#HashTag로 대화에 참여하기

DELL Technologies