

Yapay Zeka Üretimi Dönüştürüyor, Veri Güvenliğinin Rolü Büyüyor

Üretim dünyasında yapay zeka kullanımının yaygınlaşması, işletmeler için verinin değerini artırırken veri güvenliğini de dijital dönüşümün kritik başlıklarından biri haline getiriyor.

Mitsubishi Electric Iconics Digital Solutions tarafından geliştirilen GENESIS platformunun güncel versiyonu ise gelişmiş güvenlik özelliklerini yapay zekaya hazır API ve entegrasyon yetenekleriyle bir araya getiriyor.

Üretim tesislerinde sensörlerden makinelere, kontrol sistemlerinden kurumsal uygulamalara kadar her noktada üretilen veri miktarı hızla büyüyor. Yapay zeka ve gelişmiş analitik uygulamalarının üretim süreçlerine daha fazla dahil olmasıyla birlikte bu verilerin toplanması ve analiz edilmesinin yanı sıra doğru, güvenilir ve kontrollü biçimde erişilebilir olması da önem kazanıyor. Bu gelişmeler, yapay zeka uygulamalarında kullanılan verinin niteliği kadar güvenli ve kontrollü biçimde yönetilmesini de önemli hale getiriyor. Bu dönüşüm, endüstriyel işletmeler açısından veri güvenliğine bakışı da değiştiriyor. Bağlantılı sistemlerin ve veri alışverişinin arttığı üretim ortamlarında güvenlik, dış tehditlere karşı koruma sağlayan bir katman olmanın ötesine geçerek dijitalleşmenin sürdürülebilirliğini destekleyen temel unsurlardan biri haline geliyor.

Yapay Zeka için Önce Güvenilir Bir Veri Altyapısı

Mitsubishi Electric Iconics Digital Solutions'ın yeni nesil HMI/SCADA ve dijitalleşme platformu GENESIS; bina otomasyonu, enerji yönetimi, üretim operasyonları ve veri merkezi altyapı yönetimi gibi farklı alanlarda verilerin toplanmasını, görselleştirilmesini ve analiz edilmesini; sistemlerin merkezi olarak izlenmesini ve kontrol edilmesini sağlıyor. GENESIS'in güncel mimarisi, yapay zeka odaklı entegrasyonlara hazır API altyapısıyla otomasyon ve yapay zeka uygulamaları arasında yeni kullanım senaryolarının önünü açarken, güvenli makineden makineye kimlik doğrulama özellikleriyle sistemler arasındaki veri alışverişinin kontrollü biçimde gerçekleştirilmesini destekliyor. Böylece işletmeler, yapay zeka ve otomasyon teknolojilerinden yararlanırken güvenliği dijital altyapının merkezinde tutabiliyor.

Üretim ortamlarında farklı sistemler ve veri kaynakları arasındaki bağlantıların artması, yönetilmesi gereken saldırı yüzeyini de genişletebiliyor. Mitsubishi Electric Iconics Digital Solutions, bu risklerin yönetilmesi için endüstriyel sistemlerin doğrudan internete açık olmamasını, üretim sistemleri ile diğer kurumsal ağların birbirinden güvenli biçimde ayrılmasını, güvenlik duvarları ve VPN gibi koruma yöntemlerinin kullanılmasını öneriyor. Mitsubishi Electric Iconics Digital Solutions ayrıca aktif olarak kullanılmayan servislerin devre dışı bırakılması, ağ erişiminin kontrollü biçimde yönetilmesi ve sistemlerin güncel tutulmasıyla saldırı yüzeyinin azaltılabileceğine dikkat çekiyor.

Böylece bağlantılı üretim ortamlarında veri akışı sürdürülürken güvenliğin de bütüncül bir yaklaşımla ele alınması hedefleniyor.

Siber Güvenlik Yaklaşımı Uluslararası Standartlarla Destekleniyor

Mitsubishi Electric Iconics Digital Solutions, güvenliği yazılım geliştirme sürecinin tamamına yayılan bir yaklaşımla ele alıyor. Şifreleme, sertifika tabanlı kimlik doğrulama ve erişim kontrolleri gibi güvenlik teknolojileriyle desteklenen bu yaklaşım, uluslararası standartlarla da güvence altına alınıyor. Şirket, bilgi güvenliği yönetimine yönelik ISO/IEC 27001:2022 **Bilgi Güvenliği Yönetim Sistemi Sertifikasının** yanı sıra, endüstriyel otomasyon sistemlerinde güvenli ürün geliştirme süreçlerini kapsayan **IEC 62443-4-1 -Uluslararası Siber Güvenlik** standartlarına da sahip. Bu standartlar, güvenliğin ürün geliştirme süreçlerinin en başından itibaren farklı aşamalarında sistematik biçimde ele alındığını ortaya koyuyor. Mitsubishi Electric'in güvenlik yaklaşımının güncel örneklerinden HMI ürünü GOT3000 Serisi de endüstriyel otomasyon sistemlerinde kullanılan cihazların teknik siber güvenlik gerekliliklerini belirleyen **IEC 62443-4-2:2019 standardı** kapsamında **TÜV Rheinland** tarafından sertifikalandırıldı. Bu gelişme, Mitsubishi Electric'in endüstriyel otomasyon çözümlerinde siber güvenliği temel bir unsur olarak ele alan yaklaşımını da güçlendiriyor. Ürün geliştirme süreçlerinden cihaz seviyesindeki güvenlik gerekliliklerine uzanan bu yaklaşım, siber güvenliğin farklı katmanlarda ele alınmasını sağlıyor.