THE CONNECTED ENTERPRISE İÇİN ENDÜSTRİYEL AĞLARI GÜVENLİK ALTINA ALMAK

Gregory Wilcox
Rockwell Automation Küresel Ağlar İş Geliştirme Müdürü

Bugünlerde çoğumuz bir ülkenin en büyük satıcılarını ve finans kurumlarını etkileyen büyük veri sızıntılarından haberdarız. Ancak kamuoyunda iyi bilinen bu saldırılar, madalyonun yalnızca bir yüzü. Bilgisayar korsanları ve kötü niyetli şahıslar, kredi kartları ve banka hesap bilgilerinden daha fazlasının peşinde; artık üreticileri ve endüstriyel işletmecileri de hedef alıyorlar.

Örneğin Havex, özellikle enerji sektörü ve diğer sektörlerdeki endüstriyel kontrol sistemlerini hedef alan zararlı bir yazılım. 2014'te güvenlik firması F-Secure; çoğu Avrupa'da bulunan Havex'ten etkilenmiş sistemler saptadı ve kurbanlardan birini "Alman endüstriyel uygulama veya makine üreticileri", diğerini de "Fransız bir makine üreticisi" olarak tanımladı.

ABD'de Ulusal Güvenlik Bakanlığı'nın Endüstriyel Kontrol Sistemleri Siber Acil Durum ekibi; BlackEnergy adıyla bilinen bir başka zararlı yazılımın, çok bölümlü şirketlerde internete bağlı insan-makine arayüzlerine bulaştığını belirtti. Güvenlik firması CyberX; bu zararlı yazılımın üçüncü türevi olan BlackEnery 3'ü inceledi ve "saldırganların ilk bulaşmayı, bu ağların iç kısımlarından sızdırdıkları verileri işlemek üzere geliştirebildiklerine ilişkin ipuçları bulunduğunu" bildirdi.

Endüstriyel ağdaki bu sızıntılar, akşam haberlerine konu olmayabilir. Ancak işletmenizde geniş çaplı bağlanabilirlik ve artmış bilgi paylaşımı modeline yönelirken endüstriyel güvenliğe öncelik vermeniz gerektiğine ilişkin ikna edici bir kanıt olarak görülmelidir.

"Connected Enterprise" İçin Güvenlik

Üreticiler ve diğer endüstriyel işletmeler; işlemlerindeki görünürlüğü artırmak, gezgin teknolojileri işletmeye yerleştirmek ve uzaktan erişimin üstünlüklerinden faydalanma arayışında oldukları için bilgi teknolojileri (Information Technology-IT) ve işlemsel teknolojilerdeki (Operational Technology-OT) yakınsamayı giderek artan bir şekilde benimsiyorlar. Buna; Rockwell Automation "The Connected Enterprise" diyor.

İşletme katından fabrikaya kadar ağlar bağlanmış olsa ve daha çok giriş noktası oluşturulsa bile bu ağların güvenliğinin sağlanması gerekiyor. Endüstriyel ağlar, teknoloji birlikteliğini ve aygıt işbirliğini başarmaya hizmet etmek üzere açık kalıyorlar. Bundan dolayı, işletmeler, hem yapılandırılma hem de mimari tasarım aracılığıyla güvenliği sağlamak zorundalar.

ISA, NIST ve DHS/Idaho Ulusal Laboratuvarı standartları; bir ağın tüm sınırlarında savunulabilmesi için, endüstriyel arındırılmış bölge (Industrial Demilitarized Zone-IDMZ) kullanılarak yapılandırılmış bir altyapı öneriyor. IDMZ; endüstriyel bölge ile işletme bölgesi arasında bir engel yaratır. Bu engel; iki bölge arasında doğrudan dolaşımın yarattığı trafiği önlemeye yardımcı olurken, veri paylaşımı ve hizmetler için kullanıma izin verir.

Ayrıca bunlara benzer standartlar; derin savunma (defense-in depth-DiD) güvenliği ile daha sıkılaştırılmış bir altyapı kullanmayı önerir. DiD, hem dış saldırılara hem de daha yaygın görülen içsel tehditlere karşı koyan bütünsel ve çok katmanlı bir yaklaşımdır. DiD güvenliği; güçlendirilmiş araçlar ve güvenli hale getirilmiş bağlantı kapılarından ağların bölümlenmesine, ağlara erişimi yalnızca yetkili kullanıcı ya da trafikle sınırlamayı sağlayacak tamamlayıcı politika ve yöntemlere varıncaya kadar her düzeyde koruma gerektirir.

Katmanlı Güvenlik

Bir ağın fiziksel katmanının güvenli hale getirilmesi; fiziksel erişimin yetkili personel ile sınırlandırılmasıyla olur. Makineler, takozlar ile kontrol odaları gibi alanlara girişin kısıtlanması ve kontrol paneli, cihaz ve kablolara erişimin sınırlandırılması için kilitler, kapılar ve biyometri gibi güvenlik ölçütlerinin kullanımı bu kapsamdadır.

Bilgisayarı güçlendirmek için yama yönetimi ve Anti-X yazılımlar gibi önlemler gerekir. Yamanması ve yönetilmesi gereken sistemlerin sayısını azaltmak için; kullanılmayan uygulamalar, protokoller ve hizmetleri kaldırmanız önerilir. Kapı girişlerini daha iyi kontrol etmek için; gerekli olmayan kapıları kapatın ve kilitleme sistemleri ya da anahtarlanmış bağlantı parçalarını kapatarak fiziki kapıları koruyun. Ayrıca çalışanların, gözlem ve tanılama amacıyla bakım noktaları gibi farklı kapılardan geçmek için sistemde oturum açmasını zorunlu kılın.

Bilgisayar ağları, çoğu işletmede zaman içinde büyürler ve savunulması zor, yatay ağlar haline gelirler. Daha küçük güvenli alanlar oluşturmak; erişim kontrol politika ve yöntemlerinin uygulanmasını basitleştirmek için genel ağı sanal yerel ağlara (LAN) ayırmak bir çözümdür.

Çoğu iletişim engellenirken, istisnai olarak birkaçına izin vermek temel bir kuraldır. (Özel olarak izin verilmemiş olan iletişim engellenecektir.) Belli kullanıcılara, kaynaklara, hedeflere ve protokollere ayrıca izin verilebilir ya da engellenebilir.

Uygulanan politikalar ve güvenlik mekanizmaları işletmeden işletmeye değişecektir. Ancak her işletmenin uyması gereken bazı temel ilkeler vardır:

- IT ve OT grupları arasında iletişim kurmak ve işbirliği sağlamak.
- Endüstriyel otomasyon kontrol sistemi (IACS) güvenlik standartlarına uyum sağlamak.
- ISA, NIST ve DHS standartlarını takip etmek ve uygun endüstrilerce geçerli kabul edilmiş referans modelleri ve mimarileri kullanmak.
- İşletme güvenlik politikasına ek olarak ayrıca bir endüstriyel güvenlik politikası geliştirmek.
- Endüstriyel otomasyon ve güvenlik konularında uzman ortaklarla çalışmak.

Endüstriyel Kablosuz Ağ Güvenliği

Kablosuz ağ teknolojisi imalat ve diğer endüstriyel çevreler için yeni bir şey değildir. Uzun süredir noktadan noktaya veri aktarımında, yönetsel kontrol ve veri ediniminde kullanılmaktadır. "Connected Enterprise" içindeki yaşamsal önemdeki uygulamalar ve gerçek zamanlı kontrol misyonu ile ilgili kablosuz teknoloji üzerinde artan inanç, yeni teknolojik talepler oluşturmaktadır.

Artık endüstriyel firmalar, kesintisiz kontrol ve veri erişimini sürdürmek için gecikme düzeyi ve sapması düşük seviyede olan, sağlam kablosuz bağlantılara ihtiyaç duyuyor. Araya girip veriyi gözetleme, kimlik sahtekarlığı ve hizmet engelleyici saldırılar gibi risklerden kablosuz ağı korumak için de güvenlik konusu hayati önem taşıyor.

Endüstriyel WLAN uygulamaları için önerilen güvenlik mekanizması; Gelişmiş Şifreleme Standardı (Advanced Encryption Standard-AES) seviyesinde şifreleme ile Wi-Fi Korumalı Erişim (Wi-Fi Protected Access 2-WPA2) güvenlik standardıdır. WPA2 bugün endüstriyel ortamlarda kullanılabilecek en gelişmiş güvenlik standardını sunarken; AES şifrelemesi donanım düzeyinde uygulanır ve böylece uygulamaların performansını etkilemez.

IACS ortamlarında otonom ve birleşik olarak bilinen iki farklı WLAN mimarisi kullanılıyor.

Genellikle küçük ölçekli düzenlemelerde ve bağımsız kablosuz uygulamalarda kullanılan otonom mimaride, WPA2 hem önceden paylaşılan anahtar doğrulamasını hem de 802.1X/Genişletilebilir Doğrulama Protokolü'nü (Extensible Authentication Protocol-EAP) destekleyebilir. Bu iki doğrulama yönteminden hangisinin en uygun yöntem olduğuna karar vermek; işletmenin güvenlik politikası, altyapı desteği ve uygulama kolaylığına bağlıdır.

Önceden paylaşılan anahtar doğrulama; mimaride yer alan tüm cihazlarda geçerli aynı parolayı kullanır. Bunun sonucu olarak, belirli kullanıcılar için erişim sınırlaması yapılamaz ve parolaya sahip olan herkes WLAN ağına giriş yapabilir. Bundan dolayı önceden paylaşılan anahtar doğrulaması; daha çok müşterilerin sıkı bir şekilde kontrol edildiği küçük WLAN ağlarına daha uygundur.

802.1X/EAP doğrulama yönteminde; WLAN ağına erişimi sağlamak için bir EAP yapısı kullanılıyor. Bağlantı kapısını esas alan erişim kontrolü için 802.1X IEEE standardına bağlı olan bu doğrulama yöntemi; kullanıcı kimliklerine dayalı olarak veriye erişim için sağlam bir kontrol getirir ve önceden paylaşılan anahtar doğrulamanın, güvenlik gerekliliklerini karşılayamadığı durumlarda kullanılabilir.

Genellikle büyük ölçekli, daha fazla müşteri ve uygulamanın yer alacağı fabrika çapındaki ağlarda kullanılan birleşik mimarilerde; EAP Taşıma Katmanı Güvenliği (Transport Layer Security) türü doğrulama yöntemi, fabrika çapındaki WLAN ağının güvenliğinin sağlanması için kullanılmalıdır. Bu yöntem; Endüstriyel Bölge Düzeyi 3'de yer alan bir RADIUS sunucusuna ihtiyaç duyar. Yerel EAP sertifikaları ise kontrolör üzerinde bulunmalı.

Bir WLAN mimarisi için seçilen donanım; özellikle işletmenin güvenliğini ve güvenilirlik hedeflerini desteklemelidir. Bunun için geniş ölçüde kabul gören IEEE 802.11 a/b/g/n standartlarına uyumlu ve bir dizi işletim gereksinimini karşılayacak 2.4 GHz ve 5 GHz spektrumu sağlayabilen kablosuz erişim noktası (WAP) ve çalışma grubu köprüsü (Workgroup Bridge-WGB) gerekir.

Birleşik bir mimaride, WLAN kontrolü gerçekleştirmek; erişim noktasından kontrol şifrelemesine kadar tam bir Kablosuz Erişim Noktası Yapılandırması ve Kontrolü (Control and Provisioning of Wireless Access Points-CAPWAP) sağlar. Bu; sahte erişim noktalarını ve hizmet engelleme saldırılarını önlemeniz için yardımcı olacaktır.

Güvenlik için bu çözümleri uygulamak işletmelerin bir yandan kablosuz teknolojinin gücünden faydalanabilmelerini, diğer yandan işlemlerini ve fikri mülklerini kablosuz ağlardan gelen tehditlere karşı koruyabilmelerini sağlayacaktır.