KASPERSKY lab

Kaspersky Industrial CyberSecurity: Çözümlere Genel Bakış 2018

www.kaspersky.com.tr/ics
#truecybersecurity

Kaspersky Industrial CyberSecurity: çözümlere genel bakış 2018

Endüstriyel sistemlere karşı düzenlenen saldırılar artmaktadır

Endüstriyel sistemlere yönelik siber saldırılar, bir kurgu olmaktan çıkıp gerçeklik halini almıştır ve sayıları her geçen gün artmaktadır[1]. Dört endüstriyel şirketten üçü, bir ICS siber saldırısı yaşayacağını düşünmektedir[2]. Geçtiğimiz altı yılda işletme ve tedarik zinciri aksaklıkları, dünya genelinde en çok endişe duyulan risklerden biri haline gelmiştir. Siber riskler ise 2018 yılında bu riskin hemen arkasından gelmektedir[3]. Endüstriyel ve kritik altyapı sistemleri kullanan işletmeler için risk hiç bu kadar fazla olmamıştır. Endüstriyel güvenlik, işletmenin ve saygınlığın korunmasından çok daha fazla önem taşır. Endüstriyel sistemler siber tehditlere karşı korunurken birçok önemli ekolojik, sosyolojik ve makro ekonomik etken göz önünde bulundurulmalıdır.

[1] PwC: Küresel Bilgi Güvenliği Durumu 2015

[2] Endüstriyel siber güvenliğin durumu 2017, Kaspersky Lab

[3] Allianz Risk Barometre 2018

Operasyonel teknoloji/bilgi teknolojisi

IEC 62443 no'lu otomasyon standardı tarafından tanımlanan şekliyle Endüstriyel Kontrol Sistemi (ICS); endüstriyel (teknolojik) süreçlerin emniyetli, güvenli ve güvenilir bir şekilde çalışmasını etkileyebilecek veya kontrol edebilecek personellerin, donanımların ve yazılımların toplamıdır.

Endüstriyel Kontrol Sistemleri aşağıdakileri içermekle birlikte bunlarla sınırlı değildir:

- Dağıtık Kontrol Sistemleri (DCS), Programlanabilir Mantık Kontrolörleri (PLC), Uzak Terminal Üniteleri (RTU), Akıllı Elektronik Cihazlar (IED), Veri Tabanlı Kontrol ve Gözetleme Sistemi (SCADA) ve tanılama sistemleri.
- Sürekli, toplu, ayrı ve diğer süreçlere yönelik kontrol, güvenlik sağlamak ve operasyonel işlevsellik sunmak amacıyla dahili, insan, ağ ve makine arayüzleri.

Daha üst düzey bir anlatımla her endüstriyel sistem altyapısı iki temel alana bölünebilir:

- Bilgi Teknolojisi (BT): işletme amaçları bağlamında verileri yönetmek için gerekli sistemler
- Operasyonel Teknoloji (OT): endüstriyel otomasyonun fiziksel ve endüstriyel süreçlerini yönetmek için gerekli sistemler.

BT güvenlik stratejileri veri korumasına odaklanır ve "C-I-A" modelinin amaçlarına ulaşmaya çalışır: Veri Gizliliği, Bütünlüğü ve Kullanılabilirliği. Ancak OT sistemlerinin birçoğu için siber güvenlik "veri" ile ilgili değil endüstriyel süreçlerin devamlılığıyla ilgilidir. "C-I-A" modeli açısından "kullanılabilirlik", OT için güvenlik stratejilerinin ana odak noktasıdır. Bu özellik, endüstriyel siber güvenlik ihtiyaçlarını diğer sistemlerden ayırır. Yani en etkili klasik BT siber güvenlik çözümleri bile süreçlerin kullanılabilirliğini (ve bazı durumlarda bütünlüğünü) riske sokarak OT sistemlerinde kullanılamaz hale gelir.

Riskler ve tehditler

Endüstriyel kontrol sistemlerine düzenlenen siber tabanlı saldırıların yaygınlığı konusundaki farkındalığın gelişmesine rağmen birçok BT güvenlik modeli fiziksel olarak izole sistemlerin (hava boşlukları aracılığıyla) ve "gizlilikle güvenlik" gibi yöntemlerin yeterli olacağında dair eski fikirlere bağlı kalmaya devam eder. Kritik olmayan birçok endüstriyel ağa isteğe bağlı olarak veya olmayarak internet üzerinden erişilebildiği [4] Endüstri 4.0 çağında bu yöntemler yeterli değildir. Kaspersky Lab ICS CERT tarafından yapılan kapsamlı araştırmalarda, Kaspersky Security Network çözümünden gelen veriler kullanılmıştır. Bu araştırmaların sonucunda endüstriyel PC'lere; truva atları, virüsler ve solucanlar gibi tanınmış araçlar dahil olmak üzere iş sistemleri için (BT) sorun oluşturan kötü amaçlı yazılımlarla düzenli olarak saldırıldığı ortaya çıkmıştır. 2017 yılının ikinci yarısında dünya çapındaki Kaspersky Lab ürünleri, endüstriyel altyapının bileşenleri olarak sınıflandırılan Kaspersky korumalı bilgisayarların tümünde kötü amaçlı yazılım saldırılarının %37,8'ini engellemiştir[5].

Endüstriyel kontrol sistemlerini bekleyen bir başka tehlike ise fidye yazılımlardır. Fidye yazılımların çeşitliliği ve farklılığı 2015 ile 2017 yılları arasında inanılmaz derecede artmıştır. Endüstri sektörü için fidye yazılımının ortaya çıkışı büyük önem taşımaktadır. Bu tür yazılımlar, kritik sistemler üzerinde büyük bir etkiye sahiptir ve kapsamlı hasarlara neden olur. Dolayısıyla ICS, fidye yazılımları için oldukça cazip bir hedeftir. Bu durum, 2017 yılında ICS/SCADA sistemlerini etkileyen çok sayıda fidye yazılımı saldırısıyla da (özellikle WannaCry ve exPetr saldırıları) kanıtlanmıştır. Yakın gelecekte endüstriyel sistemlere saldırmak için tasarlanan fidye yazılımlarının kendine özgü amaçları olabilir. Örneğin kötü amaçlı yazılım verileri şifrelemek yerine operasyonları aksatabilir veya önemli bir varlığa erişimi engelleyebilir.

Genel tehditlerin yanı sıra, endüstriyel güvenlik, ICS'ye özel kötü amaçlı yazılım ve hedefli saldırılarla da başa çıkmak zorundadır. Bu tür saldırılar arasında şunlar sayılabilir: Stuxnet, Havex, BlackEnergy, Industroyer ve Güvenlik Enstrümanlı Sistemi hedef alan Triton... Bu liste hızla büyümektedir. BlackEnergy ve Stuxnet saldırılarından görülebileceği üzere tek bir USB sürücü veya tek bir hedefli kimlik avı e-postası görevlerine iyi hazırlanan saldırganların hava boşluğunu kapatması ve izole ağa sızması için yeterlidir.

Endüstriyel kurumlar, kötü amaçlı yazılım ve hedefli saldırılara ek olarak insanları, süreçleri ve teknolojiyi hedef alan tehditler ve risklerle de karşı karşıyadır. Bu riskleri hafife almak ciddi sonuçlara yol açabilir. Kaspersky Lab, yalnızca kötü amaçlı ve hedefli saldırılar için değil aynı zamanda birçok siber olay ve risk faktörü için de müşterilerine yardımcı olmak üzere çözümler ve hizmetler geliştirir. Bu siber olaylar ve faktörler şunları içerir:

- SCADA operatörleri ve taşeron firmalar (hizmet sağlayıcılar) tarafından yapılan hatalar
- Dolandırıcılık faaliyetleri
- Siber sabotaj
- Uyumluluk sorunları
- Farkındalık eksikliği ve adli bilişim incelemeleri için somut veriler

[4] Endüstriyel Kontrol Sistemleri ve Çevrimiçi Kullanılabilirliği 2016, Kaspersky Lab

[5] 2017'nin İkinci Yarısında Endüstriyel Otomasyon Sistemlerine Yönelik Tehdit Ortamı, Kaspersky Lab ICS CERT

Özelleştirilmiş endüstriyel güvenlik ihtiyacı

Yalnızca siber-fiziksel kurumların ve veri merkezli kurumların arasındaki farkları anlayan siber güvenlik tedarikçileri, endüstriyel kontrol sistemleri ve altyapılarının benzersiz güvenlik ihtiyaçlarını karşılayan çözümler sunabilir. Forrester Research, endüstriyel kurumlara güvenlik tedarikçisi seçerken "Özel endüstri uzmanlarını" aramalarını tavsiye eder. Forrester, Kaspersky Lab'in bu sektörde gerçekten özel uzmanlığı sahip birkaç satıcının arasında olduğunu ifade eder.

Kaspersky Lab: güvenilir endüstriyel siber güvenlik tedarikçisi

Siber güvenlik ve endüstriyel koruma alanında saygın bir lider olan[6] Kaspersky Lab, endüstriyel ve kritik altyapılara karşı sürekli gelişen tehditlere çözüm bulmak için sürekli olarak araştırma yapar ve çözümlerini geliştirir. Kaspersky Lab, operasyon yönetiminden ICS düzeyine ve sonraki düzeylere kadar endüstriye, düzenleyici kuruluşlara ve devlet kurumlarına tehdit ortamındaki değişiklikleri öngörme ve saldırılara karşı savunma yapma konusunda yardımcı olmaktadır.

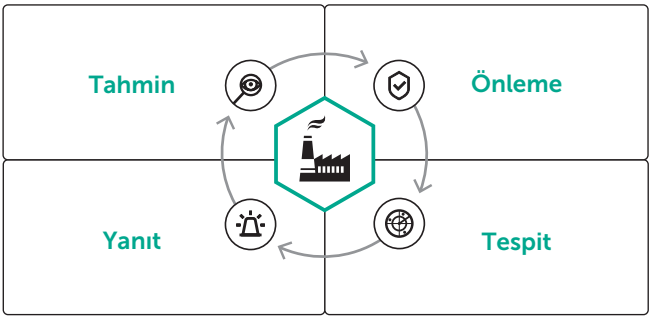
Güvenilir bir güvenlik sağlayıcısı ve iş ortağı olan Kaspersky Lab, yıllardır kötü amaçlı yazılımlara karşı koruma konusunda Kaspersky çözümlerine güvenen endüstriyel kurumları yönlendirmiştir. Şirket; Emerson, SAP, Siemens, Schneider Electric ve Industrial Internet Consortium dahil olmak üzere birçok saygın endüstriyel otomasyon tedarikçisi ve kurumu ile işbirliği yapmıştır. Bu kurumlarla birlikte çalışarak üst düzey hedefli saldırılar dahil olmak üzere mevcut ve yeni ortaya çıkan tehditlere karşı endüstriyel ortamları korumak için uyumluluk, özelleştirilmiş prosedürler ve işbirliği çerçeveleri oluşturmuştur.

Kaspersky Lab, endüstriyel siber güvenlik piyasasına özgü piyasa ihtiyaçlarını karşılamak için özel çözümlerden oluşan bir portföy geliştirmiştir: Kaspersky Industrial CyberSecurity (KICS). Bu çözümler, SCADA sunucuları, HMI, mühendislik iş istasyonları, PLC'ler ve endüstriyel ağ bağlantıları dahil olmak üzere tüm ICS katmanlarında siber tehditlere karşı etkili güvenlik sağlar ve endüstriyel süreçlerin sürekliliğini ve tutarlılığını etkilemez.

Kaspersky Industrial CyberSecurity; Kaspersky Lab'in kapsamlı ve çok katmanlı güvenlik stratejisini sürdürmek için koruma metodojilerinden oluşan bir birleşim sunar. Özel endüstriyel önleme ve tespit teknolojileri aracılığıyla olası saldırı vektörlerini öngörmeden siber olaya proaktif olarak yanıt vermeye kadar endüstriyel siber güvenliğin her alanında bütünsel bir yaklaşım benimsemek, kuruluşunuzun kesintisiz ve güvenli bir şekilde çalışması için en önemli güvencedir.

[6] Operasyonel Teknoloji Güvenliği İçin Gartner Piyasa Kılavuzu, 2017

Uyarlanabilir Güvenlik Mimarisi



Kaspersky Industrial CyberSecurity: Hizmetler

Hizmetlerimiz KICS portföyünün önemli bir kısmını oluşturur. Endüstriyel siber güvenlik değerlendirmesinden olay yanıtına kadar güvenlik hizmetlerinin tam döngüsünü sunarız.

Bilgi (eğitim ve istihbarat)

- **Eğitimler:** Kaspersky Lab, siber güvenlik uzmanları ve OT yöneticileri/ICS operatörleri için tasarlanmış eğitim kursları sunar. Örneğin "Gelişmiş Endüstriyel Siber Güvenlik" eğitimi sırasında katılımcılar ilgili siber tehditleri, bu tehditlerin gelişim trendlerini ve bunlara karşı koruma için en etkili yöntemleri öğrenir. Beceri geliştirme kursları, ayrıca güvenlik uzmanlarının Endüstriyel Kontrol Sistemi (ICS) Sızma Testi ve Adli Bilişim dahil olmak üzere belirli alanlardaki becerilerini geliştirmeyi amaçlar.

- **Farkındalık Programları:** Kaspersky Lab, ilgili siber güvenlik sorunları hakkındaki farkındalığı artırmanın yanı sıra bu sorunları ele almak ve çözmek için gerekli becerileri geliştirmek amacıyla güvenlik yöneticileri ve mühendislere yönelik eğitim "oyunları" sunar. Örneğin, Kaspersky Industrial Protection Simulation (KIPS), endüstriyel otomasyon sistemlerinde gerçek dünyada karşılaşılan siber saldırıları simüle ederek endüstriyel siber güvenlik sağlama ile ilgili temel konuları gösterir.

- **İstihbarat Raporları:** Özel Endüstriyel Kontrol Sistemleri Acil Durum Müdahale Ekibi'miz tarafından hazırlanan güncel tehdit istihbaratı raporları hazırlanır.

Uzman hizmetleri

- **Siber Güvenlik Değerlendirmesi:** Kaspersky Lab, BT/OT güvenliğinin operasyonlara olası etkisi konusunda endişelenen kurumlar için operasyonları minimum düzeyde etkileyen endüstriyel siber güvenlik değerlendirmesi gerçekleştirir. Operasyonel ihtiyaçlar bağlamında güvenlik gerekliliklerini oluşturmak için ilk adım olan bu değerlendirme, koruma teknolojilerinin dağıtımını gerektirmeden siber güvenlik düzeyleri konusunda önemli bilgiler sağlar.

- **Çözüm Entegrasyonu:** Bir kuruluşun endüstriyel kontrol sistemleri benzersiz bir mimariye sahipse veya endüstride yaygın olarak kullanılmayan özel donanım ve yazılım bileşenlerini temel alıyorsa Kaspersky Lab, önerilen siber güvenlik araçlarını bu sistemlerle çalışacak şekilde uyarlayabilir. Bu hizmet, özel SCADA, PLC'ler ve endüstriyel iletişim protokolleri dahil olmak üzere benzersiz yazılım ve donanım sistemleri için destek sağlar.

- **Olay Yanıtı:** Siber güvenlik olayı durumunda uzmanlarımız verileri toplar ve analiz eder, olay zaman çizelgesini yeniden oluşturur, olası kaynakları ve amacı belirler ve onarım Plan'ı oluşturur. Ayrıca Kaspersky Lab, kötü amaçlı yazılım analizi hizmeti sunar. Bu hizmet kapsamında Kaspresky Lab uzmanları sağlanan tüm kötü amaçlı yazılım numunelerini sınıflandırır, işlevlerini ve davranışlarını analiz eder ve sistemlerinizden atılması ve kötü amaçlı eylemlerinin geriye alınması için öneriler ve planlar hazırlar.

Kaspersky Industrial CyberSecurity: Merkezi Güvenlik Yönetimi

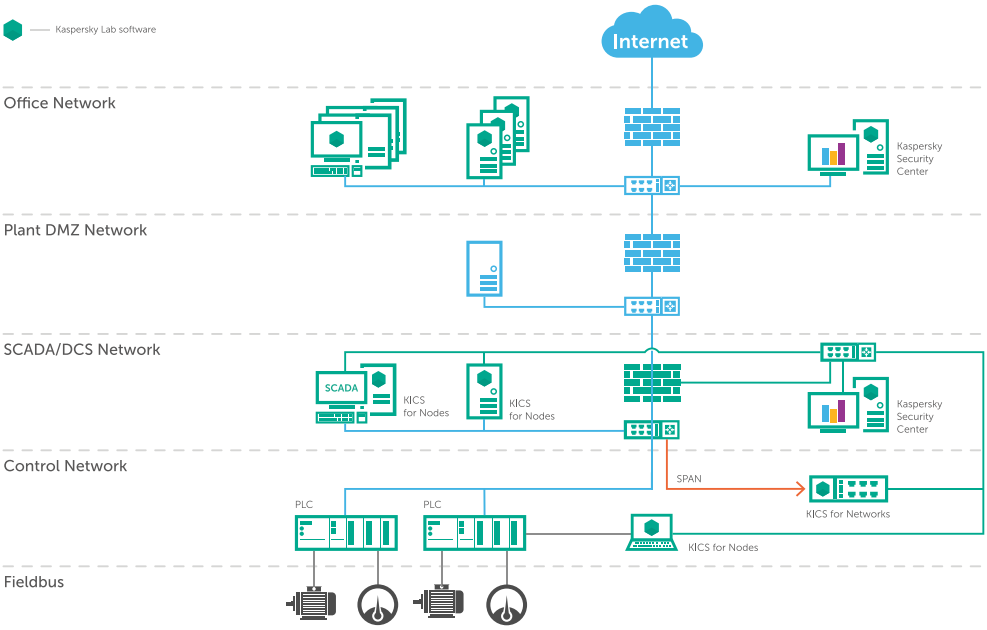
Kaspersky Security Center

Tüm saldırı vektörlerine karşı üst düzey koruma sağlamak için Endüstriyel üretim bölümü güvenliği hem düğüm hem de ağ düzeyinde çalışmalıdır. Optimum kontrol, yönetim kolaylığı ve görünürlük sağlamak için KICS, diğer tüm Kaspersky Lab teknolojileri gibi tek bir yönetim konsolundan yani Kaspersky Security Center çözümünden yönetilir. Bu sayede şunlar sağlanır:

- Güvenlik ilkeleri için merkezi yönetim: farklı düğümler ve gruplar için farklı koruma ayarları belirleme özelliği.
- Tam süreç bütünlüğü sağlamak için güncellemelerin ağ içinde kullanılmaya başlanmasından önce test edilmesi.
- Güvenlik ilkeleri ve acil eylemlerle uyumlu rol tabanlı erişim.

Kaspersky Security Center, yalnızca birden çok bölgedeki endüstriyel katmanlar için değil aynı zamanda bu katmanların çevresindeki işletme bölümleri için de kontrol kolaylığı ve görünürlük sunar.

Kaspersky Industrial CyberSecurity bileşenleri dağıtımı



Kaspersky Security Gateway

KICS ayrıca SIEM'ler, MES'ler ve Ticari İstihbarat çözümleri gibi diğer sistemlere de olayla ilgili verileri gönderir. Tespit edilen tüm olaylar ve anormallikler; CEF 2.0, LEEF ve Syslog protokolleri aracılığıyla SIEM, e-posta, syslog sunucuları ve ağ yönetim sistemleri dahil olmak üzere 3. taraf sistemlerine bildirilir. Siber saldırıları tespit etmek, araştırmak ve bunlarla mücadele etmeye yardımcı olmanın yanı sıra ayrıntılı endüstriyel ağ izleme öngörücü bakımı destekler.

İnsan-Makine Arabirimleri ile (HMI) Entegrasyon

Çözüm, bildirimleri doğrudan İnsan Makine Arayüzlerine gönderebilir. Bu sayede endüstriyel üretim bölümü çalışanları anında yanıt verme ve siber olayın üst birimlere bildirilmesi için daha net bilgiler elde edebilir.

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes, Endüstriyel Kontrol Sistemi ortamlarında operatör düzeyindeki tehditlerle mücadele etmek için özel olarak tasarlanmıştır. Endüstriyel Kontrol Sistemleri'ni/SCADA sunucularını, İnsan-Makine Arayüzleri'ni ve mühendislik iş istasyonlarını; insan faktörü, genel kötü amaçlı yazılımlar, hedefli saldırılar veya sabotajdan kaynaklanan çeşitli siber tehdit türlerine karşı korur. KICS for Nodes; SCADA, PLC ve DCS gibi endüstriyel otomasyon sistemlerinin yazılım ve donanım bileşenleri ile uyumludur.

Tehditler ve risk faktörleri	Kaspersky Lab teknolojileri
Yetkisiz yazılım çalıştırma	Beyaz listeye alma; önleme veya yalnızca tespit (engelleme yerine kayıt) modları
Kötü Amaçlı Yazılım	Kötü amaçlı yazılımlara karşı imza tabanlı gelişmiş koruma motorları; Kaspersky Lab'in genel bulutunu (KSN) veya özel bulutunu (KPSN) kullanan bulut tabanlı tespit motoru
Fidye yazılımları dahil şifreleyiciler	Şifreleyicilere karşı koruma
Ağ saldırıları	Ana bilgisayar tabanlı koruma duvarı
Yetkisiz cihaz bağlantısı	Cihaz kontrolü
Yetkisiz kablosuz bağlantılar	Wi-Fi ağ kontrolü
PLC programları sahtekarlığı	PLC bütünlük kontrolü
Endüstriyel Kontrol Sistemleri'ne özgü tehditler: hava boşlukları, ICS yazılımı/süreçleri için hatalı pozitifler vb.	Lider endüstriyel teknoloji tedarikçilerinin yazılımlarında test edilen güvenilir güncellemeler; lider endüstriyel otomasyon tedarikçileri tarafından onay.

Uygulamaları Beyaz Listeye Alma

Endüstriyel Kontrol Sistemleri uç nokta yapılandırmalarının nispeten daha statik bir yapıda olduğu için bütünlük kontrolü ölçümleri dinamik ve kurumsal ağlara kıyasla çok daha etkilidir. KICS for Nodes çözümündeki bütünlük kontrolü teknolojileri şunları içerir:

- Beyaz liste (endüstriyel kontrol ağları için en iyi uygulama) veya kara liste ilkelerine göre uygulama yükleme ve başlatma kontrolü.

- Uygulamanın dosyalar, klasörler, sistem kaydı gibi işletim sistemi kaynaklarına erişiminin kontrol edilmesi.
- .exe, .dll, .ocx, sürücüler, ActiveX, komut dosyaları, komut satırı yorumlayıcıları ve çekirdek modlu sürücüler dahil olmak üzere tüm yürütülebilir dosyaların kontrolü.
- Uygulama bilinirliği verilerinin güncellenmesi.
- Kontrol edilen uygulama listelerini yönetmek için ön tanımlı veya müşteri tanımlı uygulama kategorileri.
- Farklı kullanıcılar için hassas uygulama ayarları.
- Önleme veya yalnızca tespit modları: beyaz listede olmayan tüm uygulamaların engellenmesi veya "izleme" modunda beyaz listede olmayan uygulamaların çalışmasına izin verilmesi ancak bu etkinliğin Kaspersky Security Center'a kaydedilerek değerlendirilmesi.

Cihaz kontrolü

Cihaz kategorisi, cihaz ailesi veya belirli cihaz kimlik bilgilerine göre çıkarılabilir cihazlara, çevre ve sistem veri yollarına erişim yönetimi.

- Hem beyaz liste hem de kara liste yaklaşımları için destek.
- Tek bir kullanıcı/bilgisayar veya kullanıcı/bilgisayar grubuna granüler, bilgisayar başına, kullanıcı başına ilke belirlenmesi.
- Önleme veya yalnızca tespit modu.

Ana bilgisayar tabanlı koruma duvarı

Sunucular, insan makine arayüzleri veya iş istasyonları gibi korumalı düğümler için ağ erişim ilkelerinin belirlenmesi ve uygulanması. Temel işlevler şunları içerir:

- Kısıtlamalı portlar ve ağlar üzerinde erişim kontrolü.
- Sözleşmeli şirketlerin dizüstü bilgisayarları gibi iç kaynaklardan yapılan ve endüstriyel ağa katılır katılmaz ana bilgisayarı taramaya veya virüs bulaştırma niyetindeki kötü amaçlı yazılımları içeren ağ saldırılarının tespiti ve engellenmesi.

Wi-Fi ağ kontrolü

Bu özellik, yetkisiz Wi-Fi ağlarına bağlanma girişimlerini izler. Wi-Fi Kontrolü görevi Baştan Yasaklı teknolojisine dayalıdır. Bu teknoloji, görev ayarlarında "izin verilmeyen" tüm Wi-Fi ağlarını otomatik olarak engeller.

PLC bütünlük kontrolü

Bu özellik, seçili bir Kaspersky Lab korumalı sunucu üzerinde düzenli kontroller aracılığıyla PLC yapılandırmaları için ek kontrol sağlar. Elde edilen denetim toplamı kaydedilen "Etalon" değerleri ile kıyaslanır ve sapmalar bildirilir.

Dosya Bütünlüğünü İzleme

Bu özellik, görev ayarlarında belirtilen izleme kapsamındaki dosya ve klasörlerde gerçekleştirilen eylemleri izlemek için tasarlanmıştır. Bir SCADA sunucusunda depolanan SCADA projelerindeki değişiklikler gibi korumalı sunucudaki bir güvenlik ihlaline işaret eden dosya değişikliklerini tespit etmek için bu özelliği kullanabilirsiniz.

Kötü amaçlı yazılımlara karşı gelişmiş koruma

Kaspersky Lab'in sınıfının en iyi proaktif kötü amaçlı yazılım tespit ve önleme teknolojileri ağır kaynak tüketimi ve sistem kullanılabilirliği gerekliliklerini karşılamak için uyarlanmış ve yeniden tasarlanmıştır. Kötü amaçlı yazılımlara karşı gelişmiş koruma teknolojimiz statik veya nadiren güncellenen ortamlarda bile etkili bir şekilde çalışması için tasarlanmıştır. Kaspersky Lab'in kötü amaçlı yazılımlara karşı koruma çözümü her türlü teknolojiyi kapsar. Bu teknolojilere aşağıdakiler dahildir:

- İmza tabanlı kötü amaçlı yazılım tespiti.
- Eş zamanlı ve istek üzerinde tespit.
- Bellekte (yerleşik) tespit.
- Özel Şifreleme Yazılımlarına Karşı Koruma teknolojisi aracılığıyla fidye yazılımı tespiti.
- Üst düzey kötü amaçlı yazılım tespit hizmeti sunan Kaspersky Security Network (KSN) ve Kaspersky Private Security Network (KPSN) teknolojileri.

Güvenilir güncellemeler

Kaspersky Lab güvenlik güncellemelerinin, korumalı sistemlere erişim konusunda hiçbir etkisi olmaması için uyumluluk kontrolleri; hem veritabanlarının/bileşenlerin yayınlanmasından hem de sistem yazılımı/yapılandırmaları güncellemelerinden önce gerçekleştirilir. Olası kaynak tüketimi sorunları farklı seçeneklerin uygulanmasıyla çözülebilir:

- Kaspersky Lab, veritabanı güncellemesi uyumluluk testlerini SCADA tedarikçisi yazılımıyla Kaspersky Lab sınama ortamında gerçekleştirebilir.
- SCADA tedarikçiniz uyumluluk testlerini gerçekleştirebilir.
- Kaspersky Lab, güvenlik veritabanı güncellemelerini sizin yerinize kontrol eder: SCADA sunucusu, iş istasyonu ve HMI görüntüleri Kaspersky Lab test ortamına entegre edilmiştir.
- Kaspersky Lab güvenlik güncellemeleri tesisinizde test edilebilir ve Kaspersky Security Center ile otomatikleştirilebilir.

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Lab'in ağ düzeyi güvenlik çözümleri, endüstriyel iletişim protokolü (Modbus, IEC yığını, ISO v.b) katmanında çalışır. Gelişmiş Derin Paket İnceleme (DPI) teknolojisi aracılığıyla endüstriyel trafiği analiz ederek anormallikleri arar. Ayrıca ağ bütünlüğü kontrolü ve IDS özellikleri de sunulur.

Tehditler ve risk faktörleri	Kaspersky Lab teknolojileri
Endüstriyel ağda yetkisiz ağ cihazlarının görünmesi	Ağ Bütünlük Kontrolü yeni/bilinmeyen cihazları tespit eder
Endüstriyel ağda yetkisiz iletişimlerin görünmesi	Ağ Bütünlüğü Kontrolü bilinen/bilinmeyen cihazlar arasındaki iletişimi izler
Aşağıdakiler tarafından oluşturulan kötü amaçlı PLC komutları: • Operatörün veya 3. tarafın (taşeron firma) hatası • Kötü niyetli çalışanlar (dolandırıcılık faaliyetleri) • Saldırgan/Kötü Amaçlı Yazılım	Teknolojik Derin Paket İncelemesi, PLC'lere gelen ve giden iletişimi ve teknolojik süreçlerin komut ve parametre değerlerinin kontrolünü analiz eder.
Ağ saldırıları	Gelişmiş İzinsiz Giriş Tespit Sistemi, endüstriyel yazılımlardaki ve donanımdaki güvenlik açıklarından yararlanan yazılımlar dahil olmak üzere bilinen tüm ağ saldırı modellerini tanımlar
İnceleme ve adli bilişim için veri eksikliği	Adli bilişim araçları: şüpheli endüstriyel ağ olayları ve tespit edilen saldırıları izler ve güvenli bir şekilde kaydeder

Sistemleri etkilemeden endüstriyel ağ trafiği denetimi

KICS for Networks, olası saldırganlar için görünmez kalırken anormallikler için pasif ağ trafiği izleme ve ağ güvenliği sağlar. Kurulum, bağlantı noktası yansımasını etkinleştirmek/yapılandırmak kadar kolaydır, yazılımsal/sanal veya donanımsal cihazlar endüstriyel ağ ekipmanına mevcut anahtarın veya TAP cihazının SPAN bağlantı noktası aracılığıyla kolaylıkla entegre edilebilir. KICS for Networks çözümü modüler mimariye sahiptir. Sensörler merkezi kontrol biriminden ayrı olarak dağıtılabilir.

Anormallik tespiti için endüstriyel Derin Paket İncelemesi

KICS for Networks; endüstriyel kullanıcılarına süreç kontrol komuta akışı ve telemetri verilerini izleme ve etkinleştirme için güvenilir bir platform sağlar:

- PLC'yi yeniden yapılandıracak veya PLC durumunu değiştirecek her türlü komutun tespiti.
- Teknoloji süreçlerinde kontrol parametrelerinin değişimi.
- Mühendislerden, SCADA operatörlerinden veya sistemlere doğrudan erişim sağlayabilen şirket personelinden kaynaklanan "gelişmiş" kötü niyetli çalışan müdahalesi riskini azaltmanın yanı sıra dış tehditlere karşı koruma.

Makine öğrenimi

Endüstriyel Derin Paket İnceleme teknolojimiz yalnızca standart kural tabanlı bir yaklaşımla yapılandırılmaz. Ayrıca güçlü bir LTSM (Uzun-Kısa Süreli Bellek) tabanlı tahmin modeli aracılığıyla endüstriyel süreçlerdeki anormallikleri tespit eder. Makine öğrenimi özelliği, endüstriyel anormallik tespitini bir üst düzeye taşıyarak en karmaşık ve sıklıkla yeniden yapılandırılan ağlarda bile olay keşfini mümkün kılar.

Güvenlik ve varlık envanteri için ağ bütünlüğü kontrolü

KICS for Networks; SCADA sunucuları, insan makine arayüzleri, mühendislik iş istasyonları, PLC'ler, IED'ler ve RTU'lar dahil olmak üzere Ethernet'e bağlı tüm ağ varlıklarının tanımlanmasını sağlar. Tüm yeni ve bilinmeyen cihazlar ve bunların iletişimleri otomatik olarak tespit edilir. Bu sayede, güvenlik ekipleri saldırganlar tarafından sıklıkla hedef alınan savunmasız OT/BT varlık yönetimi araçlarını kullanmak yerine kendi güvenilir ve emniyetli ağ varlık envanterlerini geliştirebilir.

Adli bilişim araçları

Kaspersky Lab çözümü, endüstriyel kullanıcılara veri analizi ve adli bilişim için araç sağlayan güvenli kayıt sistemi sunar. Ayrıca bu sistem Endüstriyel Kontrol Sistemleri günlüklerinde değişiklik yapılmasını önler.

Kaspersky Industrial CyberSecurity İçin Ek Hizmetler

Kaspersky Security Network

Kaspersky Security Network (KSN) bulut tabanlı ve karmaşık dağıtımlı bir mimaridir. Bu çözüm dünya genelindeki milyonlarca düğümden güvenlik tehdit istihbaratlarını toplamak ve analiz etmek için geliştirilmiştir. KSN yalnızca en yeni tehditleri ve sıfır gün saldırılarını tespit edip engellemez aynı zamanda çevrimiçi saldırı kaynaklarının yerini saptar ve kara listeye alır, web siteler ve uygulamalar için bilinirlik verileri sağlar.

Endüstriyel çözümler de dahil olmak üzere tüm Kaspersky Lab kurumsal çözümleri, gerektiğinde KSN'ye bağlanabilir. Temel avantajları şunlardır:

- Daha iyi tespit oranları.
- Daha kısa tepki süresi: Geleneksel imza tabanlı yanıtlar saatler sürebilir: KSN yaklaşık 40 saniye içinde yanıt verir.
- Daha düşük hatalı pozitif oranları.
- Tesis içi güvenlik çözümleri için daha az kaynak tüketimi.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity, operasyonel sürekliliği ve endüstriyel süreçlerin uyumunu etkilemeden SCADA sunucuları, HMI panelleri, mühendislik iş istasyonları, PLC'ler, ağ bağlantıları ve mühendisler dahil olmak üzere operasyonel teknoloji katmanlarının ve kuruluşunuzdaki unsurların güvenliğini sağlamak için tasarlanmış teknoloji ve hizmetlerden oluşan bir portföydür.

Daha fazla bilgi için şu adresi ziyaret edin:
www.kaspersky.com/ics

Kaspersky Private Security Network (KPSN)

Kaspersky Lab, kendine özgü veri gizlilik endişeleri olan kurumlar için Kaspersky Private Security Network seçeneğini geliştirmiştir. Bu seçenek KSN'nin neredeyse tüm avantajlarını sağlar ancak hiçbir şekilde ağ dışına bilgi göndermez.

KPSN, kurumların kendi veri merkezlerinde dağıtılabilir ve kurum içindeki BT uzmanları sistem üzerindeki tüm kontrole sahip olabilir. Yerel KPSN kurulumları ülkeye özgü uyumluluk gerekliliklerini veya sektöre özgü diğer mevzuatlar gerekliliklerini karşılamaya yardımcı olur.

Temel KPSN işlevleri:

- Dosya ve URL bilinirlik hizmetleri: Dosyalar için MD5 karmaları, URL'ler için kurallı ifadeler ve kötü amaçlı yazılım davranış modelleri merkezi olarak depolanır, sınıflandırılır ve hızlıca müşterinin
- Kayıt Yönetimi Sistemi'ne (RMS): Bazen güvenlik yazılımları hata yaparak dosyaları ve URL'leri güvenilir/güvenilir olmayan olarak yanlış sınıflandırır. RMS, kaliteyi geliştirmek için sürekli analiz sağlamasının yanı sıra hataları düzelterek "hatalı pozitifler" için caydırıcı olur
- Bulut tabanlı istihbarat ve bilgiler.

Endüstriyel Kontrol Sistemleri siber güvenliği hakkında her şey için:
https://ics-cert.kaspersky.com
Siber Tehdit Haberleri: **www.securelist.com**

#truecybersecurity

www.kaspersky.com.tr

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

* 3. Dünya İnternet Konferansı'nda Dünya'da Lider Bilimsel ve Teknolojik İnternet Başarı Ödülü

** Çin Uluslararası Endüstri Fuarı (CIIF) 2016 özel ödülü