Elektrik Gücü Altyapısı İçin Siber Güvenlik

www.kaspersky.com/ics
#truecybersecurity

İçindekiler

Giriş 1

Elektrik Tesisleri Koruma, Otomasyon ve Kontrol Sistemlerinin Bilgi Güvenliği Tehditleri Karşısında Savunmasızlığı 1

Siber Güvenlik Tehditlerine Yönelik Önleme, Tespit ve Risk Azaltma İçin Teknik Çözümler 4

- KICS for Nodes 4
- KICS for Networks 5

KICS for Nodes ve KICS for Networks: Modern Elektrik Trafo Merkezinde Dağıtım Örneği 6

Terimler ve Tanımlar 9

Elektrik Gücü Altyapısı İçin Siber Güvenlik

Modern elektrik güç sistemi, ölçeği ve insan yaşamına önemi açısından benzersiz ve karmaşık bir teknik tesistir. Elektrik enerjisinin fiziksel özellikleri ve elektrik süreçlerinin tipik yüksek hızı göz önüne alındığında bu tür bir tesisin işleyişini kontrol etmek hem organizasyonel hem de teknik açıdan karmaşık bir görevdir. Bu nedenle enerji ekipmanları ve otomasyonun acil durum koruması için tasarlanan cihazlar, enerji endüstrisinin başlamasıyla aynı anda geliştirilmiştir. Bu cihazların gereksinimleri, tasarımları ve işlevleri, artan tüketici ve çalışma taleplerine karşılık olarak korudukları elektrik güç sistemleri ile birlikte artmıştır.

Günümüzün Koruma, Otomasyon ve Kontrol Sistemi (PACS), elektrik tesislerinin tüm çalışma alanlarını kapsayan karmaşık ve birbirleriyle ilişkili bir bilgi sistemi kümesidir. Bilgi işlem ve iletişim teknolojilerinin hızlı gelişimi, elektrikli güç bileşenlerinin koruma ve otomasyon sistemlerini değiştirmiştir. Ayrıca, modern koruma ve otomasyon sistemlerine entegre edilmiş yeni kontrol özellikleri, güç kaynağı ağ tesislerinin yapı ilkelerini değiştirir.

Kontrol kalitesini geliştirmek, geleceğin elektrik gücü gelişmelerinin ve Akıllı Şebeke sistemlerine geçişin temel görevlerinden biridir. Bu nedenle kontrol sistemleri, elektriğin üretiminde, taşınmasında ve dağıtımında önemli bir rol oynar.

Bugün PACS, son derece entegre bir sistemdir ve IEC 60870, IEC 61850 ve IEC 61970 gibi açık uluslararası protokollere dayalı dijital iletişim teknolojileri kullanır. Birbirinden ayrı alt sistemlerin entegrasyonu, koruma ve kontrol sistemlerinin becerilerini geliştirerek onları daha akıllı ve daha etkili hale getirir. Ayrıca ortak standartlar, entegrasyon maliyetini önemli ölçüde azaltır ve daha yüksek düzeyde işlevsel güvenilirlik sağlar.

Güç santralinin kontrol ve korunmasına yönelik modern bir sistem, aşağıdakiler gibi farklı türde bilgi alt sistemlerini içerir:

- otomatik dağıtım kontrolü için donanım ve yazılım aygıtları
- elektrikli sistemi çalışma modlarının bakımı için otomatik kontrol
- koruma sistemleri
- otomatik acil durum koruma sistemleri
- süreç kontrol sistemleri
- otomatik elektrik gücü ölçme sistemleri
- elektrik kalitesi kontrol sistemleri

Elektrik Tesisleri Koruma, Otomasyon ve Kontrol Sistemlerinin Bilgi Güvenliği Tehditleri Karşısında Savunmasızlığı

Elektrik sistemlerinin yüksek düzeyde açıklığı ve entegrasyonu, BT ve internet teknolojilerinin günlük hayattaki yaygınlığıyla birleşince elektrik sektörü için yeni sorunlar ortaya çıkarmıştır. Elektrik santralleri için modern otomatik koruma ve kontrol sistemleri, açık protokoller aracılığıyla iletişim kuran entegre dağıtık bilgi işlem sistemleridir. Elektrik kontrol sistemleri, izole sistemler olarak inşa edildiği için bu tür sistemlerde siber güvenlik düşük önceliklidir. Ancak, global olarak entegre edilen ve kurumsal hizmetlerle bağlantılı olan modern kontrol sistemleri için siber güvenlik riskleri son derece yüksektir.

IEC 62351 "Güç sistemleri yönetimi ve ilgili bilgi alışverişi - Veri ve iletişim güvenliği" standardında elektrik santrallerinde karşılaşılan aşağıdaki bilgi güvenliği sorunları ve bunların nedenleri vurgulanmıştır:

Açık İletişim

Enerji altyapı tesislerinin yanı sıra koruma ve kontrol sistemi bileşenleri arasında açık ve korunmasız iletişim hatları:

- **Kimlik Doğrulaması Eksikliği**
  Etkileşen aracılar arasında zayıf doğrulama olması veya hiç doğrulama olmaması. Örneğin teknolojik ağdaki rastgele bir ağ cihazı, üst düzey bir sisteme yanlış veya kötü amaçlı kontrol komutları gönderebilir ve bunun sonucunda bir dağıtım operatörü yanlış bir eylem gerçekleştirebilir

- **Açık Standartlar ve Açık Veri Aktarımı**
  Kullanılan veri iletim protokolleri, herkes tarafından erişilebilir, açık ve iyi belgelendirilmiş standartlardır. Protokollerin ve kaynak kodlarının ücretsiz uygulanmasının yanı sıra analiz ve emülasyon araçları kamu tarafından erişilebilir. Genellikle bu tür şebekelerde iletilen veriler yakalamaya, okumaya, değişime ve yeniden yürütmeye açıktır. Bu durum, olası saldırganlar için erişimi ve tehdidin yürütülmesini kolaylaştırır

- **Yüksek Düzeyli Ağ İletişimleri**
  IEC 60807-5-10x ve IEC 61850 MMS protokolleri arasındaki yüksek düzeyli iletişim, bu protokollerin çalışmasının normal bir özelliğidir. Ancak bu açık iletişimler aynı zamanda, geçersiz veri paketlerinin toplu gönderimi aracılığıyla teknolojik altyapı cihazlarında (örneğin, dağıtım merkezi süreç kontrol sistemi veya koruma terminalleri) basit hizmet engelleme saldırılarını kolaylaştırabilir

- **Ortak Ağlara Bağlantı**
  Modern bir endüstriyel tesisin kurumsal ve teknolojik ağları, kontrol sisteminin neredeyse tüm hiyerarşi düzeylerinde birden çok ara bağlantıya sahip olabilir. Bu durum, teknolojik ekipmanlara dışarıdan yetkisiz erişim riskini artırır

Çalışanlar Arasında Siber Güvenlik Farkındalığı Eksikliği

Sınırlı sayıda teknik personel, genellikle bir bölgeye yayılan ve sürekli izleme olmadan çalışan çok sayıda cihazın bakımını yapar. Tesislerdeki personeller genellikle siber güvenlik hakkında temel bilgilere sahip değildir:

- **Güvenilir Olmayan Bir Ağdan Ayrıcalıklı Uzak Erişim**
  Teknik personel, kolay bakım ve rahatlık için genellikle uzak tesis ekipmanlarına tam ayrıcalıklı erişimi etkinleştirir. Bu tür bir erişim, çoğunlukla resmi ya da güvenli olmayan bir şekilde, örneğin internet erişimine sahip kurumsal iş istasyonlarından, gerçekleştirilir

- **Parola Koruması ve Kullanıcı Denetim İlkeleri Eksikliği**
  Sınırlı sayıda personel tarafından korunan çok sayıda cihaz, parola koruması ve kullanıcı kontrol ilkeleri de dahil olmak üzere cihaz erişim ilkelerini düzenlemeyi ve korumayı zorlaştırır. Sonuç olarak, teknolojik cihazlar genellikle varsayılan şifrelerle çalıştığı için yetkisiz erişim kolaylaşır

- **Eski Yazılımlar**
  IED yazılımı, teknolojik tesislerde kullanım ömrü boyunca neredeyse hiç güncellenmez. Bilinen yazılım hataları, endüstriyel süreçleri doğrudan etkilemediği sürece ortadan kaldırılmaz

- **Güvenli Olmayan İş İstasyonlarından Bakım**
  Teknolojik altyapı bakımı sırasında kullanılan iş istasyonları (dizüstü bilgisayarlar), genellikle normal kurumsal iş istasyonları olarak kullanılır. Ayrıca yazılım testi için "test laboratuvarı" ekipmanı olarak veya kişisel amaçlarla kullanılabilir

- **Düzenli Yapılandırma ve Yazılım Kontrolü Eksikliği**
  Cihaz yapılandırması ve yazılım doğrulama kontrolleri, yılda en fazla bir kere manuel ve düzensiz olarak gerçekleştirilir

Güvenlik Gerekliliklerine Uyulmaması

Bilgi Güvenliği gereklilikleri, cihaz veya yazılım tasarımında ve teknolojik altyapılar için geliştirme süreçlerinde nadiren uygulanır.

- **Saldırılara Karşı Zayıf Direnç**
  Geliştiriciler, genellikle kodlarının teknolojik altyapılarda veya altyapı unsurlarında karşılaşabileceği hedefli saldırılara veya yasa dışı faaliyetlere karşı savunmasızlığını değerlendirmez. Bu nedenle cihaz saldırılarına karşı direnç, genel olarak zayıftır

- **Geçersiz veya Yetersiz Ağ Güvenlik Ayarları**
  Ağ segmentasyonu ve teknolojik ağdaki ağ segmentleri arasında erişim kontrolü için geçersiz ayarlar ve PACS uygulama projelerinde özel ağ tasarımı çözümlerinin olmayışı, genel bir sorundur. Bu nedenle, ağ altyapı kurulumunun kalitesi, genellikle kurulum ekibinin becerilerine ve niteliklerine bağlıdır

- **Açık Kanallarla İletilen Verilerin Korunmaması**
  Açık iletişim hatları üzerinden veri aktarımı konusunda güvenli yöntemlerin eksik olması veya hiç olmaması

- **Rol Tabanlı Erişim Kontrollerinin Olmaması**
  Rol tabanlı erişim kontrollerinin olmaması, cihazlara yanlış erişim izinleri sağlayabilir ve kullanıcıların resmi görevlerine karşılık gelmeyen erişim izinleri verilebilir

- **Uygulama Başlatma Kontrol Çözümlerinin Olmaması**
  Bilgisayar sistemlerini yetkisiz uygulama başlatma işletiminde koruyabilecek uyumlu çözümlerin olmaması, genellikle endüstriyel ortamlardan sistemleri yetkisiz yazılım başlatma işlemine karşı savunmasız bırakır. Uygulama başlatma kontrolüne yönelik genel araçlar, endüstriyel sistemlerle kullanıldığında genellikle uyumlu veya etkili bir şekilde çalışamaz (teknolojik yazılımla uyumsuzluk, belirli teknolojik sistemlerde yetersiz kaynaklar vb.)

- **Güvenlik Olayı Kayıt Aracının Eksikliği veya Yetersizliği**
  Süreç kontrol sistemlerinde belirli izleme araçları ve siber güvenlik olay kayıt araçları yoktur veya işlevleri, bir durumun doğru yorumlanmasını sağlamak için yeterli değildir

Yüklenici Erişim Kontrolünün Yarattığı Sorunlar

Belirli bakım işleri için sözleşmeli işletmelerin kullanılması oldukça yaygın bir uygulamadır. Bu uygulama süresince yüklenici şirketlere, diğer sistem bileşenleri üzerinde etkisi olmayan kısıtlı sayıda ekipmana yalnızca geçici erişim izni sağlamak çok önemlidir. İş tamamlandıktan sonra erişimin iptal edilmesi hayati bir gerekliliktir.

Güvenlik Açığı Bulunan Bileşenlerde Uzun Kullanım

Koruma ve kontrol sistemlerinin ve cihazların ömrü 20-30 yıl arasındadır. Güvenli olmayan ve bugün kurulan sistemler ancak 20-30 yıl sonra değiştirilecektir. Güvenli çözümler (örneğin şifreleme kullanan çözümler), genellikle standart güvenlik açığı bulunan çözümlerle uyumlu olmadığı için kısmi yükseltmeler çoğu zaman son derece zordur.

Yukarıda listelenen teknik sorunlara ek olarak önemli kurumsal sorunlar da vardır. İlk olarak, otomatik sistemlerde şüpheli etkinlik tespit edildiğinde alınacak eylemleri tanımlayan kılavuzların eksikliği sorun oluşturur. İkinci olarak bilgi teknolojileri aracılığıyla kontrol sistemleri üzerindeki kötü amaçlı etkiler dahil olmak üzere teknolojik ortamlardaki sorunların incelenmesiyle ilgili belge ve uygulamaların eksikliği olumsuzluklara neden olur. Örneğin teknolojik sorunların incelenmesine ve sınıflandırılmasına yönelik bazı başvuru belgeleri, hazırlandığı yıllardan dolayı siber güvenlik olaylarını arızanın olası nedenleri arasında değerlendirmez. Bu nedenle siber olay gerçekleşmesi durumunda olayın gerçek nedenleri ortaya çıkmayacaktır. Sonuç olarak uygun önlemler alınamayacağı için olayın tekrarlanma ihtimali yükselecektir.

Yukarıdaki bilgiler, açıkça birden çok sistemsel sorun olduğunu göstermektedir:

- Koruma ve güç ekipmanları kontrolü için modern elektrik güç sistemleri, izole ve kapalı sistemler değildir
- Koruma, otomasyon ve kontrol sistemleri yeterli yerleşik siber güvenlik işlevlerine sahip değildir
- Organizasyonel ve teknik açıdan olumsuz etkilerin tespiti, mevcut koşullar altında son derece zordur
- Saldırı tespit edildiğinde nasıl yanıt verileceğine dair açık yönergeler yoktur

Siber Güvenlik Tehditlerine Yönelik Önleme, Tespit ve Risk Azaltma İçin Teknik Çözümler

IEC 62351 "Güç sistemleri yönetimi ve ilgili bilgi alışverişi - Veri ve iletişim güvenliği" standardı, elektrik santrallerinde karmaşık bilgi güvenliği sağmaya yönelik olası araçları ayrıntılı olarak açıklar. Ancak önerilen çözümlerin çoğu otomasyon cihazları, format ve iletişim protokol prosedür değişiklikleri gerektirdiği anda otomasyon cihazlarının tamamen değiştirilmesiyle uygulanır.

IEC 62351 standardının tam olarak uygulanması mevcut koşullar altında uzak bir ihtimal olarak görülmesine rağmen gerekliliklerin bir kısmı yerine getirilebilir ve modern sistemlere uygulanabilir.

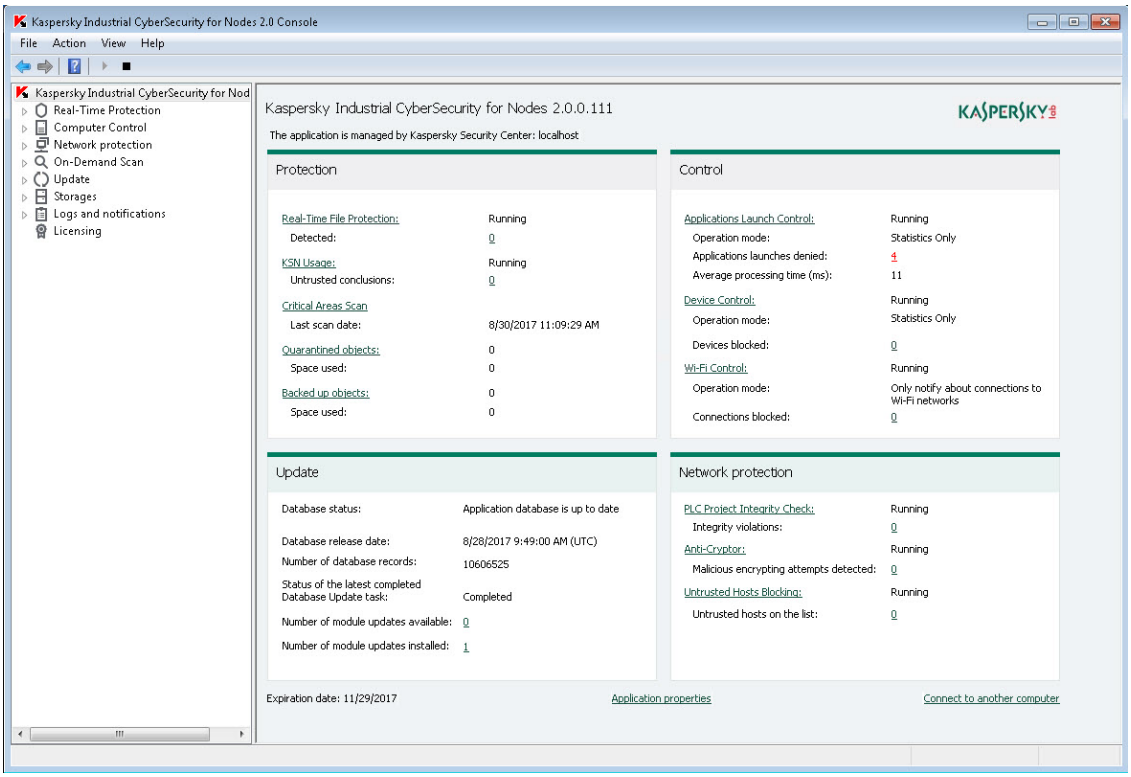
Kaspersky Industrial CyberSecurity (KICS), endüstriyel altyapılar için bu gereksinimleri karşılayan bütünsel bir çözümdür.

Çözüm iki bileşenden oluşur:

- KICS for Nodes: endüstriyel ağ uç nokta korumasına yönelik bileşen (mühendislik istasyonları, operatör istasyonları, SCADA sunucuları gibi)
- KICS for Networks: ağ bütünlüğü denetimi ve derin uygulama protokolü denetleme özelliklerine sahip endüstriyel ağ izleme bileşeni (elektrik altyapıları için IEC 60870-5-104, IEC 61850 vb.)

KICS for Nodes

KICS for Nodes, endüstriyel sistemlere yönelik özelleştirilmiş bir üründür. Bilgisayar yazılımı uygulaması olarak Windows işletim sistemini kullanan HMI panellerinin yanı sıra teknolojik sunucuları, mühendislik iş istasyonlarını ve operatör iş istasyonlarını korumak için tasarlanmıştır.



Resim 1. KICS for Nodes yerel arabirimi

Çözümün ana işlevleri:

- Uygulama beyaz listesi oluşturma (Uygulama başlatma kontrolü): Açıkça izin verilenler dışında tüm uygulamaların başlatılmasını engeller. Koruma bileşeni, dağıtım aşamasında kolay kurulum ve hata ayıklamayı desteklemek için test modu sağlar
- Cihaz kontrolü: Yöneticilerin korunan endüstriyel ana bilgisayarlara hangi cihazların bağlanabileceğini tanımlamasına ve belirtmesine olanak tanır. Bu teknoloji, endüstriyel sistemlerin yetkisiz cihaz bağlantılarından korunmasını sağlar. Teknoloji, kolay yönetim ve toplu cihaz kullanımı için maskeleri destekler
- Wi-Fi ağ kontrolü: Yetkisiz Wi-Fi ağlarına bağlanma girişimlerini izleme olanağı sunar
- Kötü amaçlı yazılım tespiti (fidye yazılımları dahildir): Windows iş istasyonlarını bilinen, bilinmeyen ve gelişmiş tehditlere karşı korumak için imza ve sezgisel algoritma tabanlı koruma yöntemlerini birleştirir. Özel Şifrelemeye Karşı Koruma teknolojisi, fidye yazılımı saldırılarını önler
- Ana bilgisayar tabanlı güvenlik duvarı: Ağ bağlantılarını endüstriyel ana bilgisayarlarla sınırlama özelliği sağlar
- PLC bütünlük kontrolü: Projelerdeki değişikliklerin düzenli olarak kontrol edilmesiyle denetleyici yapılandırması üzerinde ek kontrol sağlar

KICS for Nodes, Kaspersky Security Center tabanlı bir güvenlik altyapısı kontrol sistemine entegrasyondan sonra merkezi olarak yönetilebilir ve aşağıdaki işlevleri yerine getirebilir:

- Merkezi yönetim ve güvenlik ilkesi kontrolü: Bu özellik, hem bağımsız cihazlar hem de gruplar için güvenlik ayarlarının yapılandırılmasını sağlar
- Korumalı ağ düğümlerinde virüsten koruma veritabanlarının merkezi olarak güncelleştirilmesi (teknolojik ağ internete bağlı olmasa bile): Bu özellik, güvenlik aracılarının teknolojik ağdaki tek bir kontrol sunucusundan güncelleştirilmesi sayesinde yüksek düzeyde güvenliği desteklemeye yardımcı olur. Güncellemeler, yeniden iletim düğümünden (BT ağına veya DMZ'ye kurulur) doğrudan kontrol sunucusuna indirilebilir veya USB cihazları aracılığıyla kontrol sunucusuna aktarılabilir
- Dağıtımdan önce yeni güncellemeleri test etme: Bu işlev, endüstriyel ana bilgisayarlara dağıtımdan önce, güncellemelerin endüstriyel yazılıma uyumluluk açısından kontrol edilmesini sağlar
- Ayrı ilke yönetimi ve güvenlik aracısı eylemleri için rol tabanlı model: Bu işlev, kontrol sunucusunda yetkisiz güvenlik ilkesi değişiklikleri olasılığını ortadan kaldırır ve korumayı devre dışı bırakmayı ya da uç nokta çözümü ayar değişikliklerini önler
- Uç nokta güvenlik olayları verilerinin merkezi olarak toplanması: Bu işlev, kayıtlı olaylara bağlı olarak kapsamlı bilgi güvenliği veri analizi sağlar, olayların kesin nedenlerinin belirlenmesine yardımcı olur ve risk azaltma planının hazırlanmasını sağlar

KICS for Nodes çözümünün çalışması, normal koşullarda endüstriyel süreçleri etkilemeyen yaklaşımlara dayalıdır.

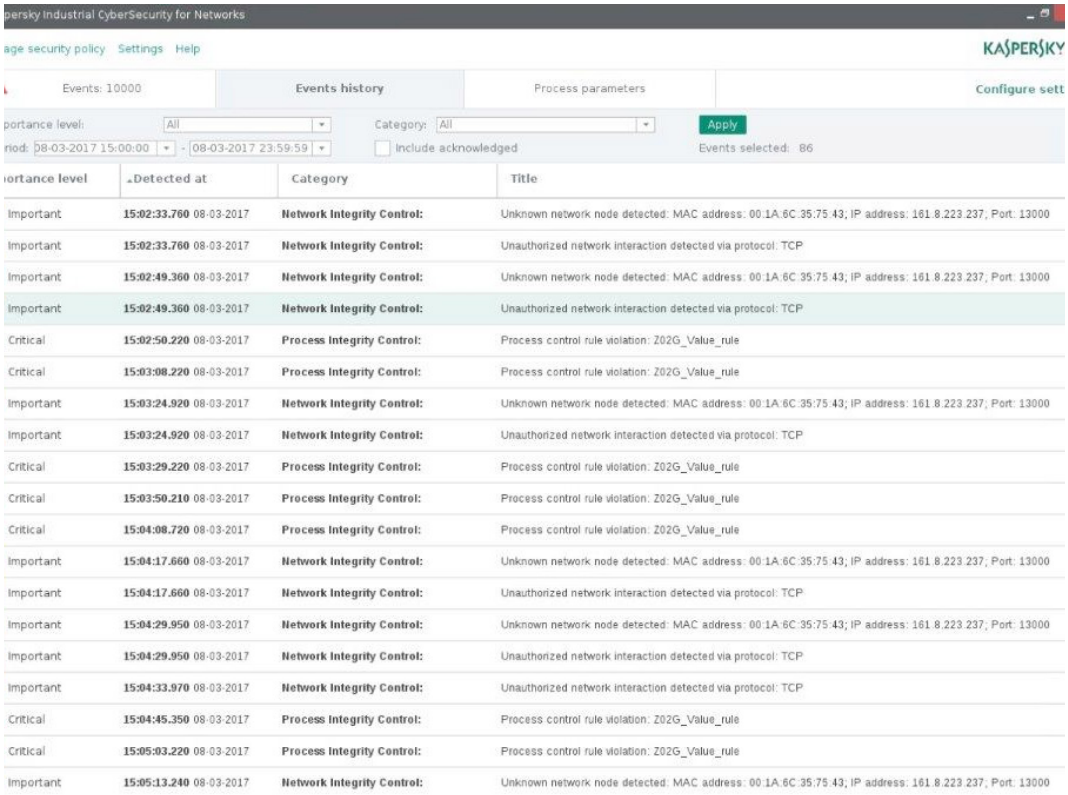
KICS for Networks

KICS for Networks, endüstriyel ağ izleme için özel bir yazılım çözümüdür. Bu çözüm, endüstriyel sürece müdahale etmeden, anormallikleri tespit edebilir ve endüstriyel ağ trafiğinden alınan önemli bilgi olaylarını kaydedebilir.

Çözümün ana işlevleri şunlardır:

1. Ağ bütünlüğünü izleme:

- Kullanılabilir tüm LAN düğümlerinin ve aralarındaki iletişimin tespit edilmesine ve kaydedilmesine olanak tanıyan kendi kendine eğitim modu. Bu veriler, değişiklik izleme için başvuru noktası olarak kullanılabilir
- Teknolojik ağın kontrollü segmentlerine bağlanan yeni ağ cihazlarının IP ve MAC adresi tabanlı tespiti ve kaydı
- Şu özelliklere göre düğümler arasındaki yeni ağ iletişiminin tespit edilmesi ve kaydedilmesi: gönderici düğüm adresi, alıcı düğüm adresi, ağ protokolü, bağlantı noktası, izin verilen bağlantı sayısı vb.



Resim 2. KICS for Networks yerel arabirimi

2. Derin paket denetimi:

- Yapılandırmaya göre önemli teknolojik protokol mesajlarının incelenmesi, analizi ve kaydı:
  - Endüstriyel ağ protokolleri (IEC 61850, IEC 60870-5-104) aracılığıyla cihaz yönetimi komutlarının (örneğin Açma/Kapatma) tespiti
  - Endüstriyel ağ protokolleri (IEC 61850, IEC 60870-5-104) aracılığıyla koruma ve kontrol sistemi çalışma parametrelerini (örneğin, ayar noktası grup anahtarı) değiştirme komutlarının tespiti
  - Kontrollü ağ segmenti aracılığıyla hizmet yazılımında IED kontrolü ve parametrelendirme girişimlerinin tespiti
- Genel telemetre iletisi izleme

3. Etkinlik depolama:

- KICS for Networks, tespit edilen olayların dahili ve güvenli bir veritabanında depolanmasını sağlar
- Bu bilgiler, depolama süresi ve arşiv boyutu sınırıyla kısıtlanmıştır. Resim 3'te gösterilen çözüm örneği, KICS for Networks ve KICS for Nodes dağıtım senaryoları için olası bir dağıtım senaryosunu gösterir

KICS for Nodes ve KICS for Networks: Modern Elektrik Trafo Merkezinde Dağıtım Örneği

Güvenli koruma ve kontrol sistemi, halka topolojisinin iki LAN segmentini içerir. Elektrik trafo merkezinin ilk segmenti, IED'ler arasında iletişim sağlayan santral veri yoludur (IEC 61850 standardına göre). Ayrıca trafo veri yolu, trafo denetleyicileri ve uzaktan ölçüm ağ geçitleri, dağıtım kontrolünün daha üst düzeyleriyle bilgi amaçlı etkileşim sağlar. LAN segmenti, mühendislik yazılımı aracılığıyla koruma ve kontrol sistemi ekipmanına erişim sağlar. Hizmet erişimi hem yerel olarak hem de uzaktan sağlanabilir. Yerel hizmet erişimi, doğrudan IED'lere veya santral veri yolu LAN'ına bağlı bir dizüstü bilgisayar kullanılarak sağlanır. Hizmet erişimi, uzak bir iş istasyonundan da yapılabilir. Stabil çalışma sırasında ağ düğümleri arasındaki hızlı iletişim IEC 61850 MMS protokolüne göre gerçekleşir. Koruma ve kontrol sistemi cihazlarının parametrelendirilmesiyle ilgili hizmet iletişimleri, ekipman üreticisinin dahili uygulama protokolleri kapsamında sağlanır.

Veri yolunun fiziksel LAN segmenti, iki bağlı anahtardan oluşan halka ağdır. Tüm cihazlar, anahtarlara çift düğüm noktası (DAN) olarak bağlanır. Bu nedenle segmentte daha yüksek düzeyde ağ güvenilirliği sağlayan tek arıza noktası yoktur. IED'ler, dahili anahtarlarla donatılmıştır ve zincirler halinde birleştirilmiştir. Zincirlerin uçları, halka ağ anahtarlarına bağlanır. Dolayısıyla bir zincirin cihazları arasındaki trafik, halka ağ anahtarları aracılığıyla iletilmez. Halka topolojisi ağ kontrolü, RSTP kullanılarak yürütülür. Ağ anahtarı, bir VPN aracılığıyla endüstriyel ağa uzaktan hizmet erişimi sağlamak için eklenmiştir.

İkinci segment (operatör ağı segmenti), operatör iş istasyonları ve süreç kontrol sistemi sunucusunun etkileşimi için tasarlanmış bir halka ağ topolojisi ile temsil edilir.

Ağ Kontrol Merkezi ve Sistem Operatörü ile etkileşim, doğrudan otomasyon sistemine bağlı bir trafo merkezi denetleyicisi aracılığıyla sağlanır (Bkz. Resim 3). Bilgi alışverişi, IEC 60870-5-104 protokolü aracılığıyla gerçekleştirilir.

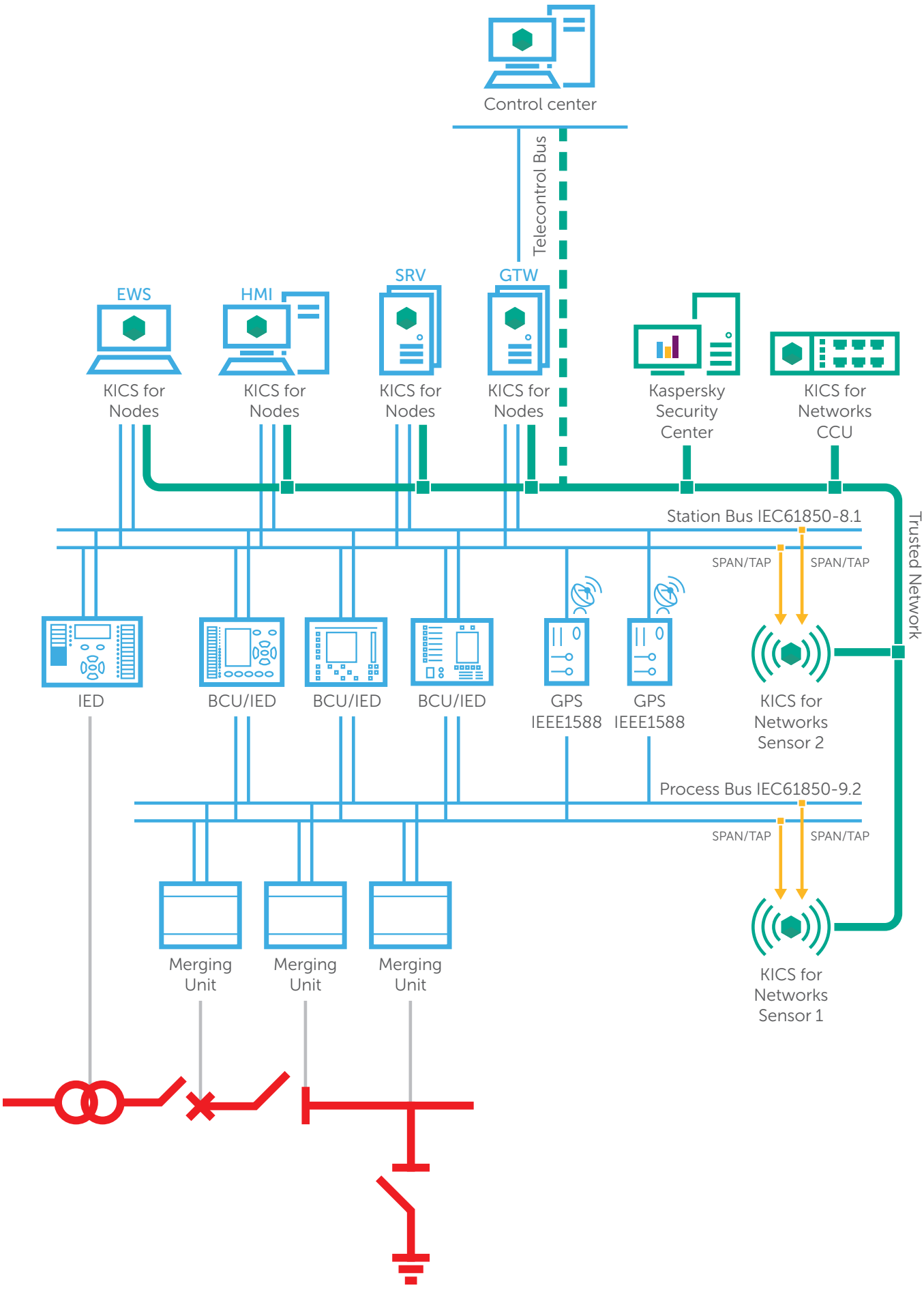
KICS for Networks kurulumu, teknolojik ağ altyapısının tam olarak izlenmesi için seçili ağ segmentlerinin her birinde gereklidir. Dolayısıyla belirtilen şema için üç adet KICS for Networks sunucusu kurulmalıdır. Bu sunuculardan birisi santral veri yolu segmenti, diğeri operatör ağ segmenti ve sonuncusu daha yüksek kontrol düzeylerine iletişim hattı için kurulmalıdır. KICS for Networks çözümünü altyapı sunucularına bağlamak için her ağ segmentindeki SPAN trafiğinin tamamını ilgili sunucuya iletmek üzere anahtarlama ekipmanının yeniden yapılandırılması gereklidir.

KICS for Networks sunucusu, ağ anahtarlarının SPAN bağlantı noktalarına bağlanır. Bu yapılandırma, endüstriyel süreçleri etkilemeden yalnızca endüstriyel trafiği alma imkanı sunar. KICS for Networks, endüstriyel trafiği işler ve şüpheli olayları tespit eder. Kayıtlı olaylarla ilgili veriler şifrelenir ve güvenli bir şekilde depolanır. Ayrıca olaylar şifreli bir kanal aracılığıyla Kaspersky Security Center çözümüne iletilir ve güvenlik uzmanlarına tespit edilen olayların nihai listesi sunulur.

KICS for Nodes yazılımı, Windows işletim sistemini kullanan bilgisayar altyapısını korumak için her endüstriyel ana bilgisayara kurulmalıdır. KICS for Nodes, aynı zamanda tespit edilen olayları Kaspersky Security Center sunucusuna gönderir. Endüstriyel ana bilgisayarlar, kontrol ağı segmentine bağlanmak için ek bir ağ arabirimi içermelidir.

Tüm kontrol ağı iletişimleri şifrelenir. Kontrol ağı hatası durumunda, KICS for Networks ve KICS for Nodes bileşenleri bağımsız modda çalışmaya devam eder. Ağ segmenti çalışması düzeltildikten sonra toplanan veriler Kaspersky Security Center sunucusuna iletilir.

KICS, SIEM sistemleriyle entegrasyonu destekler. Kaspersky Security Center, SIEM sistemi ile şifreli bir kanal düzenler ve yapılandırılan olayları SIEM sistemine (HP ArcSite, IBM QRadar Syslog formatı aracılığıyla diğerleri) aktarır. Bildirimler, ayrıca e-posta ve SMS aracılığıyla gönderilebilir.



Resim 3: Kaspersky Industrial CyberSecurity bileşenleri dağıtımı

Terimler ve Tanımlar

CD: Bilgi İşlem Cihazı. Önceden tanımlanmış program mantığına göre veri işlemeyi yürütebilen teknik bir araç.

CSPS: Siber Güvenlik Koruma Sistemi. Korunan tesislere siber güvenlik sağlamak için tasarlanmış otomatik bir sistem.

IED: Akıllı Elektronik Cihaz. Geniş dijital iletişim özelliklerine sahip özel bir mikroişlemci tabanlı çok amaçlı bilgisayar.

Endüstriyel siber güvenlik: BT/OT düzeyinde endüstriyel sürecin kullanılabilirliğini, bütünlüğünü ve gizliliğini sağlayan koruma durumu.

LAN: Yerel Ağ. Yerel olarak yönetilen ortam aracılığıyla bağlanmış ve sınırlı alan konumu ilkesine göre gruplandırılmış sabit ağ birimleri kümesini kapsayan bilgisayar ağı.

PACS: Koruma, Otomasyon ve Kontrol Sistemi. Tesise kurulan, farklı amaçlara sahip otomatik ve otomatikleştirilmiş kontrol sistemlerinin birleşimi anlamına gelen kapsayıcı terim.

PCS: Süreç Kontrol Sistemi. Kontrol edilen tesiste kapsamlı yerinde otomatik ve otomatikleştirilmiş süreç kontrolü sağlayan ve uzak dağıtım merkezinden uzaktan kontrole olanak tanıyan endüstriyel otomasyon ve iletişim araçlarına dayalı insan-makine sistemi.

Koruma Sistemi: dengeli sistem performansı sağlamak için kontrollü elektrik gücünün hasarlı bölümlerinin anında tespit edilmesine ve bağlantısının kesilmesine yönelik IED kompleksi.

SCL – Trafo Merkezi Yapılandırma Dili. Elektrik trafo cihazlarının yapılandırılması için IEC 61850-6 protokolünde belirtilen dil ve sunum biçimi. Cihaz bilgi modelinin, veri kümelerinin ve iletişim hizmetlerinin sunumuna ilişkin kaynakları içerir. XML dili temel alınır.

Akıllı Şebeke: – tüm kaynakların (doğal, sosyal, üretim ve insan kaynakları) etkili bir şekilde kullanılması için kuruluşun çoklu aracı ilkesinin yanı sıra kuruluşun faaliyetlerinin ve gelişiminin kontrolüne dayalı yeni nesil elektrik sistemi. Bu sistem, modern teknolojilere ve birleşik akıllı hiyerarşik kontrol sistemine göre tüm öznelerinin (tüm üretim, elektrik ağları ve tüketici türlerine göre) esnek etkileşiminden dolayı tüketiciler için güvenli, nitel ve verimli güç kaynağı sağlar.

SPAN – Anahtar Bağlantı Noktası Analiz Cihazı. Analiz amacıyla yönetilen anahtarın belirli bağlantı noktalarından yansıtılan ağ trafiğini toplamak için kullanılan ağ anahtarı bağlantı noktası.

Santral Veri Yolu – süreç işlevlerini (hücre düzeyinde) uygulayan akıllı cihazlar aracılığıyla veri aktarımı sağlayan hızlı ve son derece güvenilir bilgisayar ağı ve SCADA, telemekanik ağ geçidi, vb. gibi genel trafo merkezi işlevlerini (trafo düzeyi) uygulayan cihaz, donanım ve yazılım kompleksleri. Bazı durumlarda santral veri yolu, hücre düzeyindeki cihazlar arasında yatay iletişim sağlayabilir. Santral veri yolları, iletişimlerde elektromanyetik parazit oluşumunu önlemek için genellikle fiber optik veri aktarım aracıyla yapılır.

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**

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

© 2017 AO Kaspersky Lab. Tüm hakları saklıdır. Tescilli ticari markalar ve hizmet markaları ilgili sahiplerinin mülkiyetindedir.

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* 3. Dünya İnternet Konferansı'nda Dünya'da Lider Bilimsel ve Teknolojik İnternet Başarı Ödülü
** Çin Uluslararası Endüstri Fuarı (CIIF) 2016 özel ödülü