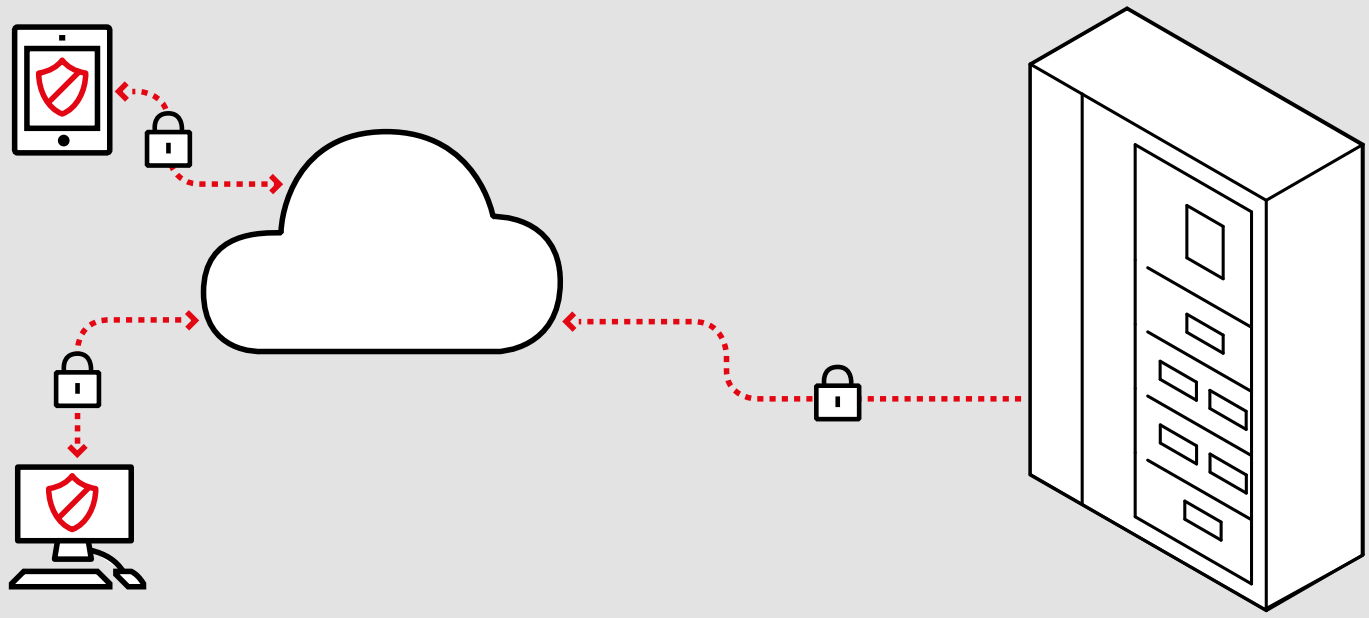
BAĞLANABİLİRLİK

Siber Güvenlik ile nasıl mücadele edilir

ABB Ability™ Energy and Asset Manager



Dijital deneyimimiz, nesne ve cihazlarımız gibi, hepimizin internet üzerinden giderek daha fazla birbirimize bağlandığımızı gösteriyor.

Bu aynı zamanda uzaktan izleme ve performans analitiği açısından büyük faydalar sağlayan “endüstriyel” bileşenler için de geçerlidir.

Tesisler, binalar ve endüstriyel süreçler için artan otomasyon ve denetim sistemlerinin kullanımı nedeniyle, elektrik sistemindeki mevcut verilerden içgörüler elde etmek için haberleşme ağlarının uygulamaları her geçen gün daha da önemli bir hale gelmektedir.

Bu veriler, bir enerji yönetimi veya varlık yönetimi çözümü için çok önemli olabilir.

Ayrıca Endüstri 4.0 trendinden güçlü bir şekilde etkilendiğimiz günlerde bağlantı kurmak gerçekten önemli bir zorluk haline geldi. Nesnelerin İnterneti, mikro şebekeler ve büyük veri, bu zorluğu gerçek bir fırsat haline getiren kilit özelliklerdir.
Öte yandan bu, siber tehditlere maruz kalma oranını artırabilir.

Siber Güvenlik nedir?

Siber Güvenlik = Risk yönetimi
- %100 veya mutlak güvenlik diye bir şey yoktur
- Siber Güvenlik ulaşılması gereken bir nokta değil, sürekli gelişen bir hedeftir - bir ürün değil, dinamik bir süreçtir
- Siber Güvenlik tamamen risk yönetimi ile ilgilidir

Güç otomasyonunda siber güvenlik
Modern otomasyon, koruma ve kontrol sistemleri son derece özelleşmiş IT sistemleridir:
- Kullanıma hazır ticari IT bileşenlerinden yararlanır
- Standartlaştırılmış, IP tabanlı haberleşme protokollerini kullanır
- Dağıtık ve yüksek oranda birbiriyle bağlantılıdır
- Mobil cihazlar ve veri depolama ortamını kullanır
- Yazılıma dayalıdır (ABB teklifinin >%50'si yazılımla ilgilidir)

Siber Güvenlik sorunları
- Eski, izole sistemlere kıyasla daha fazla saldırı alanı
- Harici (OT olmayan) sistemlerle haberleşme
- IT dünyasından / üzerinden saldırılar

Dijital deneyimimiz, nesne ve cihazlarımız gibi, hepimizin internet üzerinden giderek daha fazla birbirimize bağlandığımızı gösteriyor. Bu durum endüstriyel nesneler için de geçerlidir ve onların siber tehditlere maruz kalma oranını arttırır. Siber saldırganlar, ekonomik, politik veya askeri avantajlar elde etmek amacıyla kişisel veya hassas bilgiler elde etmeyi ve sistemlere yetkisiz erişimi hedefler.

Bağımsız veya izole bir sistem bile %100 güvenli olarak tanımlanamaz. Yazılım güncellemeleri veya yeni yazılım kurulumları, sistem için risklere neden olabilir.

Siber saldırıların tehditlerinin farkında olmamız, herhangi bir zararı önlemek için risk azaltma faaliyetlerini uygulamaya koymamız, savunmasız durumların önlenmesi amacıyla sürekli izlememiz gerektiği için siber güvenliği bir risk yönetimi prosedürü olarak düşünmeliyiz.

Siber Güvenlik Tehditleri

Kasıtlı saldırılar
Standart internet teknolojilerinin kullanımıyla birlikte, standart internet tehditlerine, virüslere ve bilgisayar korsanlarına da maruz kalırsınız.



%9.4
Bilgisayar korsanları ve **teröristlerin** yarattığı güvenlik tehditleri



%10.6
İçeriden gelen güvenlik tehditleri

BİLGİSAYAR KORSANLARI | TERÖRİSTLER | İÇERİDEKİ TEHDİTLER

Kasıtsız saldırılar
Korkutan bir diğer tablo da çoğu siber güvenlik tehdidi ve olayının kasıtsız olması ve endüstriyel ağlarda meydana gelmesidir.



%11.2
İnsan hatası sonucu oluşan güvenlik tehditleri



%30.4
Kötü amaçlı yazılımlardan (malware) kaynaklanan güvenlik tehditleri



%38.4
Cihaz ve yazılım hatalarından kaynaklanan güvenlik tehditleri

İNSAN HATASI | KÖTÜ AMAÇLI YAZILIMLAR | CİHAZLAR

ABB'nin yanıtı
Dijital çözümlerimiz geçmişte tesis içinde (on-premise) uygulandı ve teklifler "uç (edge) sistemlerle" başladı. Bugün, bu daha çok "sis bilişim" olarak adlandırılıyor (çünkü sis, buluttan farklı olarak yere daha yakındır).

ABB, sahada bulunan kritik göreve sahip otomasyon sistemleri oluşturma konusunda kapsamlı deneyime sahiptir. Sistemlerimizin çoğu artık bulut tabanlı ABB Ability™ platformumuza bir bağlantıyla genişletiliyor.

ABB Ability™, hem bir dizi endüstriyel dijital çözümü hem de kurulu oldukları platformu ifade eder. Bu endüstriyel çözümleri 3 ana pazarımız için sunuyoruz: şebekeler, sanayi ve ulaşım & altyapı.

ABB Ability™ platformu, ABB'nin bu çözümleri daha hızlı ve verimli bir şekilde hayata geçirmesini sağlayan bir teknoloji dizisidir.

Platformu, Microsoft Azure bulut hizmetleri, IBM Watson makine öğrenmesi & yapay zeka ve SAP HANA'nın büyük veri sorgu araçları gibi sınıfının en iyisi sektör teknolojileri ile oluşturuyoruz.

Bulut teknolojisi, herhangi bir yeni çözümde geliştirmelerin ve bakımın ölçeklenebilirliğini ve esnekliğini önemli ölçüde artırma şansı sunarken, eski ve tesis içi sistemlere yönelik küresel erişimi artırır.
Ayrıca kimliği doğrulanmış ve yetki sahipleri tarafından verilere her yerden ve ihtiyaç duyulduğu her anda erişilebilir.

Endüstriyel sistemlerin güvenliğini sağlamak, dizüstü bilgisayarları veya cep telefonlarını korumaktan daha zordur.
Haberleşme ve verilerin güvenliğini sağlamaya ek olarak, programların kurcalanmamasını da sağlamak gerekir.
Cihazları daha devreye alırken (boot) korumalıyız, yazılım güncellemelerinin bilinen kaynaklardan geldiğinden, aynı zamanda değiştirilmediğinden ve tehditler gerçekleşirken tespit edip bunlarla başa çıkabileceğimizden emin olmalıyız.

ABB Ability™: güvenlik, veri ve IP
Kritik görevli uygulamalar için çözümleri ve verileri güvenli hale getirir



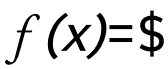
Sistemlerinizi güvence altına alıyoruz:
- Güvenli işlem
- Tehdit algılama
- Güvenli haberleşme
- Güvenli güncelleme
- Güvenli çalıştırma

ABB siber güvenlik standartları



Sistemlerinizi güvence altına alıyoruz:
- Kimlik
- Ölçüm verileri
- Verilerinizle ne yaptığımızı biliyorsunuz
- Verileri yalnızca sizin izninizle paylaşıyoruz

ABB IoT veri manifestosu



IP'niz size ait:
- ABB Ability™ çözümlerini kullanırken fikri mülkiyet kaybı olmaz

ABB fikri mülkiyet görüşü

Müşterimizin tesislerinden gelen veriler değerlidir ve onların bilgisi & onayı olmadan başkalarıyla paylaşılamaz.

ABB Ability™ çözümleri, müşterilerin verilerine ve sistemlerinin IP'sine sahip olmalarını sağlar.

ABB Ability™ Energy & Asset Manager uygulaması
ABB Ability™ Energy & Asset Manager, elektrik sisteminin durumunu izlemek, optimize etmek, kontrol etmek ve tahminler yürütmek için tasarlanmış yenilikçi bulut tabanlı bir platformdur.

Platform; veri toplama, işleme ve depolama için son teknoloji ürünü bir bulut mimarisi üzerine inşa edilmiştir. ABB Ability™ bulut mimarisi, performansı artırmak, en yüksek güvenilirliği ve emniyeti garanti etmek için Microsoft ile birlikte geliştirilmiştir.

ABB, Microsoft ve IT güvenliği konusunda uzman bir iş ortağı sayesinde, **ABB Ability™ Energy & Asset Manager** son teknoloji siber güvenliği garanti edebilir:

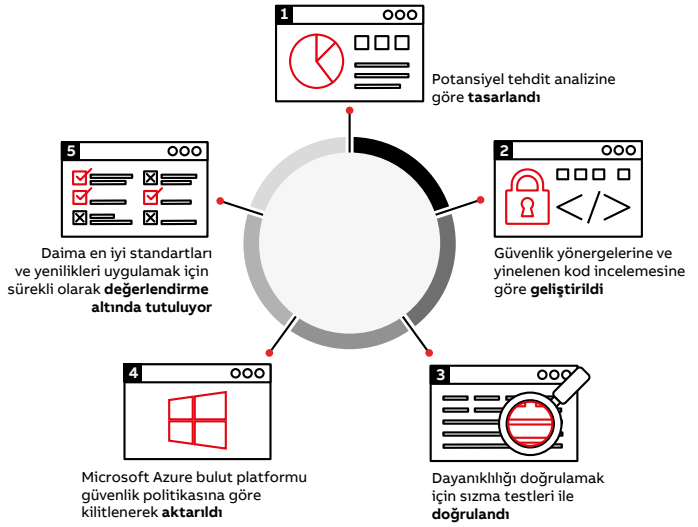
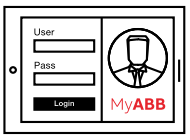


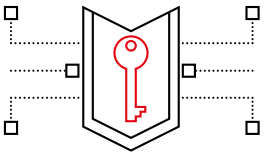
ABB Ability™ EAM
Siber Güvenlik için destekleyici ana özellikler

Kimlik



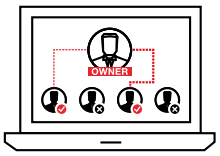
Kişisel **MyABB** hesabı üzerinden kimlik doğrulama

Güvenlik



Şifreli haberleşme kanalı, bankacılık ve diğer önemli uygulamalar ile aynı protokolü kullanır

Gizlilik



Yalnızca sahip rolündeki kişi, verilere ilk erişime sahiptir ve diğer kullanıcıların rolünü şekillendirebilir

Elektronik İmza

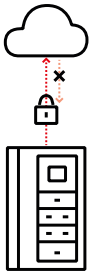


Bağlı her bir cihaz **benzersiz bir şekilde tanımlıdır**

Uçtan uca süreç

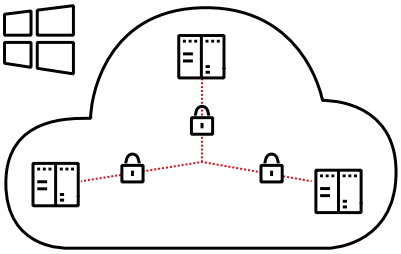
Aygıttan buluta

- Benzersiz tanımlama için **beyaz liste**
- **Lokal** devreye alma
- **Komut gönderme yok**
- **Şifreli** haberleşme kanalı



Bulutta

- Microsoft **Azure** güvenliği
- Son teknoloji siber güvenlik standartlarına sahip sertifikalı **veri merkezlerinde** veri depolama
- **Şifreli** haberleşme kanalı



Tarayıcıdan

- ABB SSO aracılığıyla benzersiz **kimlik doğrulama**
- Verilere yalnızca **yetkilendirme** ile erişim
- **Komut gönderme yok**
- **Şifreli** haberleşme kanalı

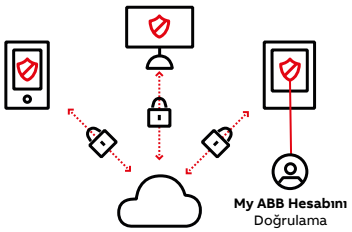


ABB Elektrik Sanayi A.Ş.
Organize Sanayi Bölgesi 2. Cadde No: 16
34776 Yukarı Dudullu - İstanbul
Tel : 0216 528 22 00
Faks : 0216 365 29 45

ABB Müşteri İletişim Merkezi
Tel : +90 850 333 1 222
Faks : +90 850 333 1 225
E-posta : contact.center@tr.abb.com

www.abb.com.tr

Önceden bildirimde bulunmaksızın teknik değişiklikler yapma veya bu belgenin içeriğini değiştirme hakkını saklı tutarız. Satın alma siparişleri ile ilgili olarak, üzerinde anlaşmaya varılan ayrıntılar geçerli olacaktır. ABB, bu belgedeki olası hatalar veya olası bilgi eksikliğinden dolayı herhangi bir sorumluluk kabul etmez.

Bu belgedeki ve içerdiği konu ve resimlerle ilgili tüm hakları saklı tutmaktayız. ABB'nin önceden yazılı izni olmaksızın herhangi bir şekilde çoğaltılması, üçüncü şahıslara ifşa edilmesi veya içeriğinin kullanılması - tamamen veya kısmen - yasaktır.
Telif hakkı© 2017 ABB
Her hakkı saklıdır

1SDC210111D0201 - 2018.03