Kaspersky Embedded Systems Security

kaspersky

Gömülü sistemler için özel olarak tasarlanmış hepsi bir arada güvenlik (ve daha fazlası)

Gömülü sistemler etrafımızda pek çok yerde kullanılır ve bu sistemlerle her gün etkileşim kurarız. PoS sistemleri ve ATM'lerden tıbbi cihazlara ve otomatik yakıt istasyonlarına kadar her şey için onları kullanıyoruz. Gömülü sistem pazarı büyüdükçe siber suçlular ortaya çıkıyor ve taktiklerini, tekniklerini ve prosedürlerini bu yaygın sistemlerin özelliklerine uygun olacak şekilde geliştiriyor.

Gömülü sistemlerde güvenlik sıkıntıları

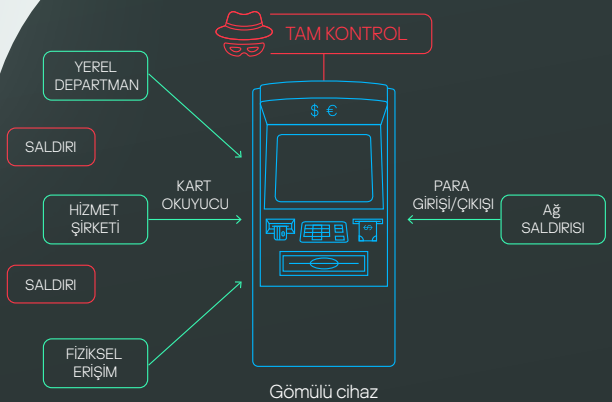
1. **Eski ve saldırıya açık yazılımlar.** Uzun kullanım süreleri, sömürülmeyi bekleyen yamasız zayıf noktalar içeren işletim sistemlerinin ve uygulamaların destek dışı çalıştırılması anlamına gelebilir.
2. **Sorunlu güvenlik güncellemeleri.** Yazılım desteklendiğinde dahi yamalama açıkları olabilir. Coğrafi olarak dağılmış birden fazla cihazın güncellenmesi, güncelleme amacıyla çevrimdışı hâle getirilmelerinin gerekmesi (böylece geçici olarak Hizmet Reddi gerçekleşmesi) ve dağıtılmadan önce güncellemeleri test etme ihtiyacı ile ilgili sorunların tümü, yamalama gecikmelerine katkıda bulunabilir.
3. **Süreç devamlılığı.** Tıbbi cihazlar gibi belirli türlerdeki cihazların geçici olarak hizmet dışı bırakılması dahi pek çok soruna yol açarak yamalama açığı süresini daha da artırabilir.
4. **Kamuya açık alanlar.** Birçok gömülü cihaz, kamuya açık alanda çalıştırılır; bu da müdahale riskini önemli ölçüde artırır. Ağ düzeyinde savunma, cihazı doğrudan fiziksel olarak kötü amaçlı yazılım bulaşmasına karşı koruyamaz.
5. **Nitelik itibarıyla riskli yapı.** Gömülü cihazlar, sıklıkla finansal işlemlerle doğrudan ilişkilendirilmeleri ve hassas kişisel bilgileri işlemeleri nedeniyle siber suçlular için özellikle çekici hedeflerdir.

Tehdit alanı

Hizmet Olarak Kötü Amaçlı Yazılım gibi suça yönelik yeni iş modelleri ortaya çıkmaya devam ediyor ve potansiyel saldırganlar için beceri çıtasını düşürüyor. Windows'un eski sürümleri için destek çoktan sona ermiş olsa da bu sürümlerin kullanımı devam ediyor (Windows XP halen gömülü cihazlarda en yaygın kullanılan işlem sistemidir). Milyonlarca gömülü cihaz ve bilgisayar, herhangi bir nedenle güncellenmemiş olan eski ve saldırılara açık işletim sistemlerini kullanmaya devam ediyor. Bu, korsanlara açık bir davet anlamına geliyor.

Bu sırada Linux tabanlı gömülü sistemlerin popülerliği hızla artıyor ve bu durumu takip eden siber suçlular, Linux tabanlı gömülü sistemlerin özelliklerine göre tekniklerini uyarlıyor ve tamamen yeni araçlar geliştiriyor. Linux'un yapısı gereği sahip olduğu güvenliğin olduğundan daha başarılı görülmesi tehlikelidir ve saldırganlar dikkatlerini Linux tabanlı gömülü cihazlara nispeten kısa bir süre önce çevirmiş olsalar da kaybettikleri zamanı telafi etmektedirler. Linux tabanlı gömülü cihazlar için mevcut siber güvenlik tekliflerinin Windows için mevcut olanlara kıyasla sınırlı olması da durumu kötüleştirmektedir.

İşletmelerin sistemlerini ve verilerini güvende tutmak için her zamankinden daha akıllıca davranması gerekiyor. Güçlü tehdit istihbaratı, isteğe bağlı kötü amaçlı yazılım algılaması ve açıklardan yararlanmayı önleme, kapsamlı sistem güçlendirme denetimleri ve esnek yönetim özelliklerine sahip olan Kaspersky Embedded Systems Security, gömülü sistemler için özel olarak tasarlanmış hepsi bir arada güvenlik aracıdır. Çoğu siber güvenlik tedarikçisi tarafından artık desteklenmeyen eski sistemler için benzersiz düzeyde koruma sağlamaktadır ve şimdi Linux işletim sistemini çalıştıran daha modern cihazlar için de aynı düzeyde koruma sunmaktadır.



Gömülü sistemlere yönelik tüm başarılı saldırıların yarısından fazlasında içeriden kişilerin (bir çalışan veya üçüncü taraf hizmet sağlayıcısı) etkinliği söz konusudur

Fiziksel düzeydeki saldırılar

- Kara kutu saldırıları
- PIN tuş takımı değişimleri/kopyalayıcı cihazlar
- Gizli kameralar
- Patlamalar

Yazılım düzeyindeki saldırılar

- Uzaktan/yerel kötü amaçlı yazılım yüklemesi
- Bellek yoklayıcılar/işletim sistemi saldırıları
- Aracı yazılım bulaşması/değişiklikleri

Ağ düzeyindeki saldırılar

- VPN açıkları
- RDP'ye kaba kuvvet uygulanması
- Uzaktan kod yürütmeye izin veren ağ girişimleri
- Uzaktan yükleme

Gömülü sistemler: tipik saldırı vektörleri

Gömülü sistemlerde güvenlik sıkıntıları

6 **Katı düzenlemeler.** Sıklıkla işledikleri finansal ve kişisel tanımlayıcı bilgiler nedeniyle, birçok gömülü cihaz güvenlik konusunda özellikle dikkatli bir yaklaşım benimsenmesini şart koşan yönetmeliklere tabi olarak çalıştırılır.

7 **İç tehditler.** Kaspersky verilerine göre, gömülü sistemlere yönelik tüm başarılı saldırıların %50'sinden fazlasında içeriden kişilerin (bir çalışan veya üçüncü taraf hizmet sağlayıcısı) etkinliği söz konusudur.

8 **Linux'un yaygınlaşması.** Daha fazla esneklik sunan ve daha çeşitli yapılandırmaların kullanımına olanak tanıyan gömülü platformlar hızla ivme kazanıyor. Siber suçlular bu durumu takip ediyor ve modern, özel güvenlik çözümü seçenekleri, Windows için mevcut olanlara kıyasla çok daha sınırlı kalıyor.

Öne Çıkan Noktalar

Her türlü gömülü cihaz senaryosu için en ideal koruma:
Kaspersky Embedded Systems Security, farklı güç seviyelerine ve uygulama senaryolarına sahip cihazlar için en ideal güvenliği sağlamak üzere çok katmanlı koruma sunmaktadır. Buna Windows ve Linux gibi farklı İşletim Sistemlerine dayanan platformların desteklenmesi de dâhildir

Hem eski hem de yeni sistemleri korur
Kaspersky Embedded Systems Security; Windows XP, 7, 8, 10, ve 11'de tam işlevsellikle çalışacak biçimde optimize edildi. Kaspersky, yakın gelecekte Windows XP'yi desteklemeyi sürdürecek ve böylece müşterilere hazır olduklarında yükseltme yapmaları için yeterince süre tanıyacaktır. Kaspersky Embedded Systems Security ayrıca Windows veya Linux işletim sistemini çalıştıran en yeni mimarileri de desteklemektedir.

Az kaynak, yüksek düzeyde koruma
Kaspersky Embedded Systems Security, düşük teknik özellikli donanımlarda bile etkili biçimde çalışacak şekilde geliştirildi.

ATM ve POS saldırılarında artış
Kaspersky'nin araştırma verilerine göre ATM ve POS sistemlerine yönelik saldırı sayısında 2022 yılında önemli bir artış görülmüştür ve bu artış devam etmektedir (2020 yılına kıyasla %19 artış ve 2021'de %4 artış).

Temel özellikler

Sistem güçlendirme (güvenlik kontrolleri). Uygulama, cihaz ve güncelleme denetimlerinden oluşan bu sistem güçlendirici teknolojiler sadece güvenilir uygulamaların, çevre birimlerinin ve güncelleme kaynaklarının kullanımına izin verir. Böylece kötü amaçlı yazılımlar ve kötü amaçla kullanılabilecek uygulamalar dâhil olmak üzere yetkisiz programların başlatılması ve çalıştırılması önlenir.

İsteğe bağlı olarak kötü amaçlı yazılımlardan korunma. İsteğe bağlı güvenlik katmanı; bilinen, bilinmeyen ve gelişmiş tehditleri hassas algılama mantığı ile, yerel ve bulut tabanlı tehdit istihbaratının yanı sıra kurum içinde veya bulut üzerinde çalıştırılan buluşsal modeller ve makine öğrenimi modelleri kullanarak algılar.

Açıklardan yararlanmayı önleme[1]. Default Deny modunda uygulama denetimini atlatmak üzere tasarlanan saldırılar ve dosyasız teknikler kullananlar dâhil olmak üzere daha gelişmiş saldırıların karşılanmasına yardımcı olarak, Windows sistem bileşenlerinin ve üçüncü taraf uygulamalarının çalıştırılmasıyla ilgili açıklardan yararlanılmasını önler.

Ağ tehdit koruması. Hedef alınan cihaza erişmeyi amaçlayan bağlantı noktası tarama ve kaba kuvvet saldırılarına ve ağ ile ilgili açıklardan yararlanan siber saldırılara karşı koruma sağlayarak işletim sistemine izinsiz girişleri önler. Bu sayede gömülü sistemlere yöneltilmiş başlıca saldırı vektörlerinden birini engellemiş olursunuz.

Bütünlük izleme ve uyum desteği. Dosya bütünlüğü ve kayıt defteri erişimi izleme üst simge özelliği belirli kayıt defteri anahtarları, dosyalar ve klasörler üzerinde yapılan işlemleri takip eder ve istenmeyen değişiklikleri engelleyebilir. Bu özellik sadece kötü amaçlı yazılıma dayalı girişlerin değil, aynı zamanda kritik kaynaklara doğrudan erişimin/çevrimdışı değişikliklerin de tespit edilmesine yardımcı olur. Bu önlemler veri koruma yönetmeliklerinde sıklıkla özel olarak tavsiye edilir ve etkinleştirilmeleri uyumun sürdürülmesine yardımcı olur.

Düşük güçlü ve eski sistemleri destekler. Windows XP SP2'ye kadar, kullanımdan kalkmış donanım ve desteklenmeyen işletim sistemleri ile çalışan düşük güçlü gömülü sistemleri bile destekler. Yükseltme yapmaya hazır olana kadar eski cihazları veya masaüstü bilgisayarları güvenle çalıştırmaya devam edebilirsiniz.

Günlük Denetimi[1]. Windows olay günlüklerinin takibine ve denetimine dayalı olarak olası koruma ihlalleri saptanır. Uygulama bir siber saldırı girişimine işaret edebilecek anormal bir davranış saptadığında yöneticiye bildirimde bulunur.

Kurum içinde veya bulutta esnek yönetim. İhtiyaçlarınıza bağlı olarak, kurumsal gömülü sistemlerinizin güvenliği kurum içindeki bir yönetim sunucusundan veya Kaspersky Security Center SaaS bulut konsolundan ve bunun yanı sıra diğer Kaspersky çözümleri kullanılarak yönetilebilir. Sıkı gizlilik gerektiğinde kurum içi yönetim faydalıdır. Tedarikçi tarafından işletilen bulut üzerindeki SaaS konsolu ise hem sermaye hem işletim harcamalarından tasarruf edilmesini sağlayarak güvenli çalışma süreçleri için hızlı bir başlangıç yapmaya olanak tanır ve daha az bakım zahmeti gerektirir.

[1] Yalnızca Windows işletim sistemi için

Güvenlik duvarı yönetimi. İşletim Sisteminin Güvenlik Duvarı doğrudan Kaspersky Security Center'dan yapılandırılabilir ve tek bir birleşik konsol yoluyla sizin için yerel güvenlik duvarı yönetimi kolaylığı sağlar. Gömülü sistemler, etki alanı içinde olmadığında ve Windows/Linux güvenlik duvarı ayarları merkezî olarak yapılandırılamadığında bu önemlidir.

Zayıf bağlantı toleransı. Pek çok türde gömülü cihaz genellikle uzakta bulunduğundan zayıf hücresel kapsama veya yakın radyo kaynaklarının neden olduğu parazit gibi nedenlerden kaynaklanan zayıf bağlantı, alışılmadık bir durum değildir. Kaspersky Embedded System Security, çok düşük bant genişliklerinde dahi kararlı kalır ve uzun süre boyunca bağlantı olmadığında dahi güvenilir koruma sağlar.

Profesyonel Hizmetler ve Üst Düzey Destek

Bir güvenlik çözümünün yaşam döngüsünü uygun şekilde sürdürmek çaba gerektirir ve gömülü cihazları sıradan uç noktalarından ayıran özellikleri nedeniyle gömülü cihazların güvenliğini sürekli olarak sağlamak özellikle zahmetli olabilir. Kaspersky Professional Services, dağıtım ve güncelleme, yapılandırma ve performans optimizasyonundan yeni donanıma geçişe kadar bu yaşam döngüsünün her aşamasında destek sunar. Üst Düzey Desteğimiz ise benzersiz uzmanlıkla desteklenen özel bir teknik hesap yöneticisi ile olayların öncelikli olarak ve uzmanlıkla çözülmesini garanti eder.

İlgili ürünler ve hizmetler

Kaspersky Tehdit İstihbaratı: Güvenlik uzmanlarımız tarafından analiz edilen istihbarat kaynaklarını, tehdit veri akışlarını ve şirket içi araştırmaları bir araya getirerek, kuruluşunuzu hedef alan siber tehditlere kapsamlı bir bakış sunan çok yönlü bir hizmet yelpazesidir.

Ödeme Sistemleri Güvenlik Değerlendirmesi: ATM ve POS cihazlarınızın kapsamlı analizi size mevcut güvenlik düzeylerinizin net bir görünümünü sunarak güvenliğinizi daha da artırmanıza, yapılandırmasını optimize etmenize ve varsa güvenlik açıklarını kapatmanıza olanak tanır.

Kaspersky Endpoint Security for Business: Uç noktalarınızı, sunucularınızı, iş istasyonlarınızı ve mobil cihazlarınızı en çok test edilen ve en fazla ödül kazanan güvenlikle koruyan dünyaca ünlü uç nokta koruma platformudur. Hepsi tek bir konsol üzerinden yönetilir.

Sektörler

- Finansal Hizmetler
- Ulaşım ve Turizm (Biletlendirme)
- Perakende
- Restoranlar ve Konaklama
- Sağlık
- Kamu Sektörü ve Ticaret Dışı Sektörler
- Eğlence

Cihazlar

- ATM'ler
- Bilet makineleri
- Yakıt istasyonları
- Ödeme Noktaları
- Satış Noktası
- Tıbbi ekipman
- Eski uç noktalar
- Slot ve oyun makineleri

Gömülü cihazların kullanıldığı sektörlerin detayları için tıklayınız

Siber Tehdit Haberleri: securelist.com
Kaspersky Teknolojileri: kaspersky.com/technowiki
BT Güvenlik Haberleri: business.kaspersky.com
KOBİ'ler için BT Güvenliği: kaspersky.com.tr/business
Kurumlar için BT Güvenliği: kaspersky.com.tr/enterprise

www.kaspersky.com.tr

Kanıtlanmış başarılara sahibiz. Bağımsızız. Şeffafız. Teknolojinin hayatlarımızı geliştirdiği, daha güvenli bir dünya oluşturmakta kararlıyız. Bu nedenle teknolojiyi, sunduğu sonsuz sayıdaki fırsattan herkes yararlanabilsin diye daha güvenli hâle getiriyoruz. Daha güvenli bir **gelecek** için siber güvenliğe önem verin.

Daha fazla bilgi için: kaspersky.com/about/transparency

Proven. Transparent. Independent.