

DIGI 

**Uçta Uygulama
Güvenliği ve İyileştirme
Stratejileri**



SALDIRILAR HER ZAMAN HER YERDE OLABİLİR

Ripple20, SolarWinds, SACK ve Amnesia güvenlik tehditlerinin her zaman mevcut olduğunun güçlü kanıtlarıdır.

Bu e-kitap, günümüzün en tehlikeli uç güvenlik riskini ele alarak gelecekteki saldırıları yönetmek ve azaltmak için güvenlik duruşunu ve çevikliğini iyileştirme konusunda rehberlik sağlamayı amaçlamaktadır.



GÜNÜMÜZÜN EN TEHLİKELİ KENAR GÜVENLİĞİ RİSKİ NEDİR? **RAHATLIK VEYA HAREKETSİZLİK.**

Rahatlık veya eylemsizlik, yetersiz kaynaklar, uzmanlık eksikliği ve rekabet eden öncelikler gibi çok sayıda ve çeşitli faktörlerden kaynaklanır.

Bazı yaygın durumlar:

- Saldırıya açık, geniş ve kritik görev ağlarında görünüşte zararsız bağlantı çözümlerinin dağıtımı
- Özellikle uzaktan güncellemeler gerektiren merkezi olmayan donanımlara ilişkin düzensiz güvenlik yazılımı güncellemeleri
- Karmaşık mimariye sahip ve bunları kolayca yönetmek için ortak bir araç setine sahip olmayan çeşitli bağlı cihazlarının dağıtımı
- Özellikle veri merkezinin güvenliği dışındaki hayati ağ bileşenlerini korumak için sınırlı fiziksel kontroller
- Lisans anahtarları ve diğer kritik cihazlar için yetersiz güvenlik protokolleri

BEŞ PROAKTİF STRATEJİ

KENARDA GÜVENLİK DURUMUNU VE ANLIK YANITI GELİŞTİRİN

1

Bir sonraki saldırının gerçekleşeceğini varsayın, çünkü gerçekleşecek.

- Kenarın da kenarını herkese açık olarak ele alın. Farklı bağımsız koruma yöntemleri kullanarak bir katmanlama taktiği uygulayın.
- Bir güvenlik denetimi başarısız olursa veya bir güvenlik açığı istismar edilirse sisteme ilişkin güvenlik yedekliliği tasarlayın.
- Hırsızlık veya yetkisiz erişim olasılığını azaltmak için erişim denetimleri ve gözetim ile kenardaki fiziksel güvenlik önlemlerini geliştirin. Bu mümkün olmadığında, çok zorlaştırılmış ve güvenli şifrelenmiş cihazlar kullanın.

2

Sadece bugün için değil, gelecek için de tasarlayın.

- Altyapı yönetim bileşenlerini yalnızca yerel şifreleme ve diğer güvenlik özellikleriyle dağıtın.
- Bellek ve CPU kapasitesinde artışlar gerektirecek gelecekteki kriptografik algoritmaları planlayın.
- Gelecekteki güvenlik gereksinimlerini karşılamak için aygıt yazılımının otomatik güncellemelerini yapılandırın.
- Ölçeklenebilen güvenliğe sahip sistemler tasarlayın.

3

Her bağlantı bileşenini sürekli olarak değerlendirin ve periyodik güncellemeleri planlayın.

- Bir ağın her bileşeni, ne kadar küçük veya önemsiz görünürse görünsün, risk taşır. Güvenliği desteklemeyen, yalnızca güncel olmayan veya desteklenmeyen bir güvenlik aracı sunan veya en son güvenlik güncellemelerini çalıştırmak için sınırlı bellek ve disk alanına sahip olan uçtaki bağlantı donanımını değiştirin.
- Yalnızca, güvenlik önlemleri etkinleştirilmiş ve mümkün olan en güvenli ayarlara yapılandırılmış, en son sektör lideri ağ bileşenlerini, kutudan çıktığı anda dağıtın.

BEŞ PROAKTİF STRATEJİ

KENARDA GÜVENLİK DURUMUNU VE ANLIK YANITI GELİŞTİRİN

4

Güvenlik tehditlerine tepki vermek için anlık yanıt esnekliğinizi proaktif olarak artırın.

- Bağlı donanımları merkezi olarak yapılandırmak, izlemek, günlüğe kaydetmek ve denetlemek ve yeni güvenlik açıkları oluşturmadan güvenlik güncellemelerini kolayca uyarlamak, dağıtmak için Digi Remote Manager® gibi bir kurumsal yönetim sistemi (EMS) kullanın.
- Uygulamaların bir bilgi işlem ortamından diğerine sorunsuz çalışmasını sağlamak için tüm bileşenlerini içeren teknolojiler ile dağıtın, böylece basit, hızlı dağıtım, artan üretkenlik ve iyileştirilmiş güvenlik kolaylaşır.

5

Güvenliği tüm bağlantı çözümlerine proaktif bir şekilde entegre edin.

- Digi TrustFence® gibi bir güvenlik çerçevesiyle güvenli, bağlantılı ürünler oluşturmayı basitleştirin.
- Güvenli önyüklemeden güvenli bağlantı noktalarına, kullanıcı düzeyine göre şifreleme ve kimlik doğrulamaya kadar her erişim noktasına güvenlik kontrolleri ekleyin.





IP ÜZERİNDEN USB ÇALIŞMA PLATFORMU BAHSEDİLEN TÜM BEŞ PROAKTİF STRATEJİYİ SAĞLAR

Digi AnywhereUSB® Plus — Sektör Lideri USB Bağlantısı Daha Fazla Hız,
Daha Fazla Güç ve Daha Fazla Güvenlik

Digi TrustFence'i entegre eden ve Digi Remote Manager ile birleştirilen Digi AnywhereUSB Plus, uçta güvenlik durumunu ve anlık yanıtı iyileştirmek için beş proaktif stratejinin tamamını karşılar.

DIGI ANYWHEREUSB PLUS GÜVENİLİR VERİ AKTARIMI VE USB CİHAZ ŞARJI SAĞLAR



AnywhereUSB Plus ile Maksimum USB Hızı

Digi AnywhereUSB Plus, USB 3.1 gen 1 Tip A portlarını kullanır. Doğrudan bağlantı ortamlarında, bu portlar AnywhereUSB Plus'ta teorik olarak 5 Gbps'ye kadar performans sağlayabilir ancak AnywhereUSB protokolünün doğası ve ağın etkisi nedeniyle daha yavaş olacaktır.

Aktarım hızlarını en üst düzeye çıkarmak için, tüm USB kablolarınız USB 3.1 veya üzeri için derecelendirilmiş olmalı, cihazları doğrudan AnywhereUSB Plus'a bağlamalı ve AnywhereUSB Plus'ın aşağı akışına (USB port genişletme) ek bir USB Hub eklememelisiniz. Ayrıca, ağ tarafındaki herhangi bir kapasite kısıtlamasından haberdar olmak için cihazlara erişecek olan AnywhereUSB Plus ile Kullanıcı Bilgisayar arasındaki ağ bağlantısını da izleyin.

Digi AnywhereUSB Plus, USB 2.0 ile geriye dönük uyumludur.



Birçok USB Yapılandırma Seçeneği ve Avantajı

Digi, küçük, orta ve yüksek yoğunluklu cihaz yönetimi için 2, 8 veya 24 USB portlu çözüm esnekliğini sunar.

Erişimi kontrol ederek ve belirli portları veya port gruplarını bireysel veya grup düzeyinde atayabilirsiniz. Farklı kullanıcılar, yönetilen diğer cihazlara erişimi etkilemeden yalnızca ihtiyaç duyduklarında çalışmak üzere onaylandıkları ekipmana erişebilirler.



Digi AnywhereUSB 2 Plus

2 USB 3.1 Gen 1 Ports
Tek 10M / 100M / 1 Ethernet 5 VDC



Digi AnywhereUSB 8 Plus

8 USB 3.1 Gen 1 Port
Teke 10M / 100M / 1G / 10G Ethernet
12 VDC Tek SFP+



Digi AnywhereUSB 24 Plus

24 USB 3.1 Gen 1 Port
Çift 10M / 100M / 1G / 10G Ethernet
Çift Güç Kaynağı 100-240 VAC
Çift SFP+

DIGI ANYWHERE USB PLUS GÜVENLİK DURUMUNUZU VE ANLIK YANIT ESNEKLİĞİNİZİ ARTTIRIR



Sektör Lideri Güvenliğe Sahip USB Hub

Digi AnywhereUSB Plus'ın TLS sertifika tabanlı güvenliği, ağ genelinde hassas finansal, kişisel ve teknik verileri korumak için benzersiz bir şekilde şifrelenmiştir. Digi TrustFence cihaz üzerinde yerleşiktir. Görev açısından kritik uygulamalar için tasarlanan Digi TrustFence, cihaz güvenliğini, cihaz kimliğini ve veri gizliliği yeteneklerini USB cihaz ağınıza kolayca entegre etmenizi sağlayan bir temel görevi görür. Digi TrustFence, yeni ve gelişen tehditlerle birlikte büyüeyebilen ve uyum sağlayabilen IoT cihazlarına güvenlik sağlar.

Aşağıdaki özellikler her Digi AnywhereUSB Plus cihazında tümleşik olarak sağlanır:

- Her hub için benzersiz parola
- Yapılandırılabilir ağ hizmeti port numaraları
- Web kullanıcı arayüzüne ve CLI'ye güvenli erişim ve kimlik doğrulama
- Tek parola, tek izin düzeyi

- mDNS, HTTP/HTTPS ve SSH gibi ağ hizmetlerini seçimli olarak etkinleştirme ve devre dışı bırakma yeteneği
- **AnywhereUSB Plus trafiğine şifreli erişim:** IP-Üzerinden-USB trafiğine erişim varsayılan olarak şifrelenir ve doğrulanır, devre dışı bırakılamaz
- Digi AnywhereUSB Plus'ı uzaktan ve güvenli bir şekilde yönetmenizi sağlayan Digi Remote Manager ile kapsamlı yönetim yetenekleri
- Digi TrustFence® çerçevesi tarafından korunur



LİSANS ANAHTARLARI GÜVENLİK RİSKİ OLUŞTURABİLİR

Anahtarlara Erişimi Kontrol Edin

Digi AnywhereUSB Plus, çalışanların ekipman veya bilgisayarlara bağlanmasını ve bunlarla etkileşim kurmasını sağlarken, lisans anahtarlarının çalınmasını, kaybolmasını veya hasar görmesini önler.

Digi AnywhereUSB Plus hub'ları, aynı anda 127 lisans anahtarını barındıracak şekilde birbirine bağlanabilir.



IP-ÜZERİNDEN-USB KAYNAKLARINIZI GÜVENLİ OLARAK KURMAK, YAPILANDIRMAK VE YÖNETMEK



DIGI ANYWHEREUSB PLUS CİHAZINIZA
DIGI REMOTE MANAGER
YAZILIMI EKLEYİN

- Hızlı cihaz dağıtımı ve daha kolay varlık yönetimi için sektör lideri bulut ve uç araçları
- İki yönlü iletişimlerle IoT cihazlarınızı, varlık performansını ve güvenliğini izleyin
- İşlevselliği geliştirmek, uyumluluğu korumak ve dağıtımınızı ölçeklendirmek için toplu aygıt yazılımı ve yazılım güncellemelerini otomatikleştirin
- Daha önce erişilemeyen uç cihazlardan verilere erişin
- Üçüncü taraf uygulamalarla daha derin uygulamalar ve kontrol elde etmek için cihaz verilerini açık API'ler aracılığıyla entegre edin
- Ağ sağlığı ve cihaz koşulları hakkında gerçek zamanlı uyarılar ve ayrıntılı raporlar alın

BAĞLAN'ALIM

ABD

Kanada

EMEA

Diğer

Matt.Propes@digicom

Chris.DeHoog@digicom

Jean-Marie.Dubois@digicom

Businessdevelopment@digicom

Digi, kritik görev iletişim ekipmanlarından profesyonel hizmetlere, uygulamanızın güvenli, güvenilir ve en yüksek performansta tasarlanmasına, kurulmasına, test edilmesine ve çalışmasına kadar projenizin her yönünü destekleyen eksiksiz bir IoT çözümleri sağlayıcısıdır.

Digi, "Nesnelerin İnterneti"ndeki "nesneleri" birbirine bağlama konusunda 35+ yıllık deneyime sahiptir - cihazlar, araçlar, ekipmanlar ve varlıklar.

Digi'ye ait 160'tan fazla patent vardır ve Digi ürünleri ile 100 milyondan fazla cihaz birbirine bağlanmıştır.

Pazarın en köklü firmalarından biri olan BağLAN, bağlantı konusundaki uzmanlığını, mevcut ve gelişmekte olan teknolojiler doğrultusunda kullanıcılara doğru ve güvenilir ürünler, çözümler sunarak aktarmaktadır. Katma değerli distribütör olarak tanımlanabilecek BağLAN, WWAN (3G/4G/LTE/5G), M2M, IoT, SCADA, Video over IP, WLAN, LPWAN, LoRAWAN bağlantılarında/ürünlerinde uzmanlaşmıştır.

BağLAN 2008 yılından beri Digi Türkiye distribütörü/Yetkili Çözüm Ortağı olarak çalışmakta olup, Türkiye genelinde yüzlerce Anywhere USB satışını gerçekleştirmiştir.



Türkçe Tercüme BağLAN Ltd. Şti. 2024

www.baglan.com.tr bilgi@baglan.com.tr