TeamViewer Güvenlik Bilgileri

Hedef Kitle

Bu belge profesyonel ağ yöneticilerine yöneliktir. Bu belgede yer alan bilgiler teknik niteliktedir ve çok ayrıntılıdır. BT profesyonelleri bu bilgilere dayanarak TeamViewer'daki güvenlik standartları hakkında ayrıntılı bir fikir edinecektir ve yazılımımızı aygıtlara kurmadan önce oluşabilecek endişelere cevap bulabilecektir. Olası güvenlik endişelerini ortadan kaldırmak için bu belgeyi müşterilerinize iletebilirsiniz.

Hedef kitlenin bir parçası olmadığınızı düşünüyorsanız, Şirket / Yazılım bölümündeki genel bilgilere başvurarak güvenliği ne kadar ciddiye aldığımız hakkında net bir fikir edinebilirsiniz.

Şirket / Yazılım

Hakkımızda

TeamViewer GmbH 2005 yılında kurulmuştur ve şirket merkezi Almanya'nın güneyinde, (Stuttgart yakınındaki) Göppingen şehrinde olup, Avustralya'da ve Amerika Birleşik Devletlerinde iştirakleri bulunmaktadır. Web tabanlı işbirliğine özel sistemler geliştiriyoruz ve satıyoruz. Kısa bir süre içerisinde, Freemium lisanslama yöntemimiz hızla büyüyerek dünya çapında 200'den fazla ülkede, 1,4 milyar aygıt üzerinde, 200 milyon TeamViewer yazılımı kullanıcısına ulaştık. Yazılım 30'dan fazla dilde sunulmaktadır.

Güvenlik Anlayışımız

TeamViewer herhangi bir anda 30 milyondan fazla kullanıcı tarafından kullanılmaktadır. Bu kullanıcılar internet üzerinden anlık destek sunmaktadır, gözetimsiz bilgisayarlara erişmektedir (yani sunucular için uzaktan destek) ve çevrimiçi toplantılara ev sahipliği yapmaktadır. Yapılandırmaya bağlı olarak, TeamViewer başka bir bilgisayarı başında duruyormuş gibi uzaktan kontrol etmek için kullanılabilir. Bir uzak bilgisayara oturum açan kullanıcı bir Windows, Mac veya Linux sistem yöneticisi ise, bu kişiye o bilgisayar üzerinde de yönetici hakları verilecektir.

Potansiyel olarak güvensiz sayılan İnternet üzerinden bu kadar güçlü bir işlevin saldırılara karşı çok dikkatli bir şekilde korunması gerektiği açıktır. Aslında, güvenlik konusu bütün gelişim hedeflerimizin başında gelmektedir ve yaptığımız her şeyin özünde yer almaktadır. Hem bilgisayarınıza erişimin güvenli olmasını hem de kendi çıkarlarımızı korumak istiyoruz: dünya çapındaki milyonlarca kullanıcı yalnızca güvenli bir çözüme güvenir ve bir işletme için uzun vadeli başarıyı ancak güvenli bir çözüm sağlar.

Dış Uzman Değerlendirmesi

TeamViewer yazılımımız, Federal BT Uzmanları ve Denetçileri Birliği (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.) tarafından beş yıldızlı kalite onayı (maksimum değer) ile ödüllendirilmiştir. BISG e.V. bağımsız denetçileri, koşulları sağlayan üreticilerin ürünlerini kalite, güvenlik ve servis özellikleri bakımından incelemektedir.

Referanslar

TeamViewer halihazırda 200 milyondan fazla kullanıcı tarafından kullanılmaktadır. (Bankacılık, finans, sağlık hizmetleri ve kamu gibi son derece hassas sektörler gibi) çok çeşitli endüstrilerde faaliyet gösteren başlıca uluslararası şirketler başarıyla TeamViewer kullanmaktadır.

Çözümümüzün kullanılmasına ilişkin bir izlenim edinmek için İnternet üzerinde çok sayıda bulabileceğiniz referanslarımıza göz gezdirmenizi öneririz. Yoğun bir inceleme sürecinden sonra TeamViewer kullanmaya karar veren diğer şirketlerden birçoğunun büyük ihtimalle benzer güvenlik ve ulaşılabilirlik gereksinimlerine sahip olduğunu keşfedeceksiniz. Ancak, kendi izleniminizi oluşturmanız için, bu belgenin kalanında bazı teknik ayrıntılara yer verilmiştir.

TeamViewer Oturumları

Bir Oturum Oluşturma ve Bağlantı Türleri

TeamViewer bir oturum oluştururken ideal bağlantı türünü belirler. Ana sunucularımız ile tokalaşma sonrasında, (standart ağ geçitleri, NAT'lar ve güvenlik duvarları arkasında bile) vakaların %70'inde UDP veya TCP Aracılığıyla bir doğrudan bağlantı kurulur. Bağlantıların kalanları yüksek derecede yedekli yönlendirici ağımız aracılığıyla TCP veya https tüneli üzerinden yönlendirilir. TeamViewer ile çalışmak üzere herhangi bir port açmanız gerekmez.

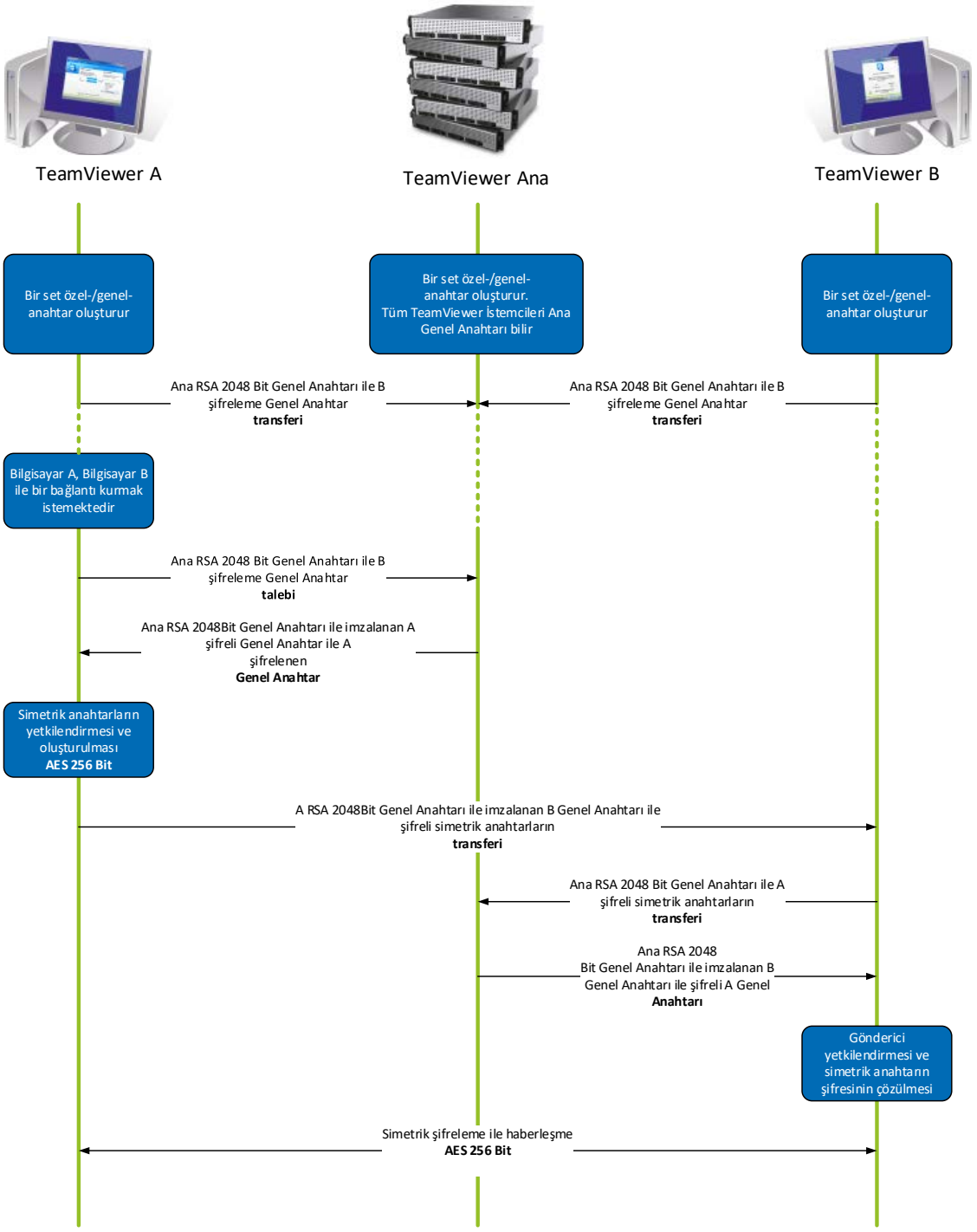
Şifreleme ve Doğrulama paragrafında açıklandığı gibi, şifrelenmiş veri trafiğini yönlendirme sunucularının işleticileri olarak bizim okumamız bile mümkün değildir.

Şifreleme ve Doğrulama

TeamViewer Trafiğinin güvenliği, RSA açık/özel anahtar alışverişi ve AES (256 bit) oturum şifreleme kullanılarak sağlanır. Bu teknoloji http/SSL için kıyaslanabilir bir biçimde kullanılmaktadır ve günümüz standartlarında tamamen güvenli sayılmaktadır. Özel anahtar istemci bilgisayardan hiçbir zaman ayrılmadığından, bu prosedür, TeamViewer yönlendirme sunucuları da dahil olmak üzere birbirine bağlı bilgisayarların veri akışını çözememesini sağlar.

Her TeamViewer istemcisi ana kümenin açık anahtarını uygulamıştır ve böylelikle ana kümeye giden iletileri şifreleyebilir ve ana küme tarafından imzalanan iletileri kontrol edebilir. PKI (Açık Anahtar Altyapısı), man-in-the-middle (iki nokta arasındaki bağlantıya yetkisiz müdahale) saldırılarını etkin bir şekilde önler. Şifrelemeye rağmen, parola hiçbir zaman doğrudan gönderilmez; sadece bir kimlik sorma-yanıt verme prosedürü aracılığıyla gönderilir ve sadece yerel bilgisayara kaydedilir.

Kimlik doğrulama sırasında, Güvenli Uzak Parola (SRP) protokolü kullanıldığı için parola hiçbir zaman doğrudan aktarılmaz. Yerel bilgisayarda yalnızca bir parola doğrulayıcı saklanır.



TeamViewer şifreleme ve doğrulama

TeamViewer ID'lerinin Doğrulanması

TeamViewer ID'leri çeşitli donanım ve yazılım özelliklerine dayanmaktadır ve TeamViewer tarafından otomatik olarak oluşturulur. TeamViewer sunucuları her bağlantıdan önce bu ID'lerin geçerliliğini kontrol eder.

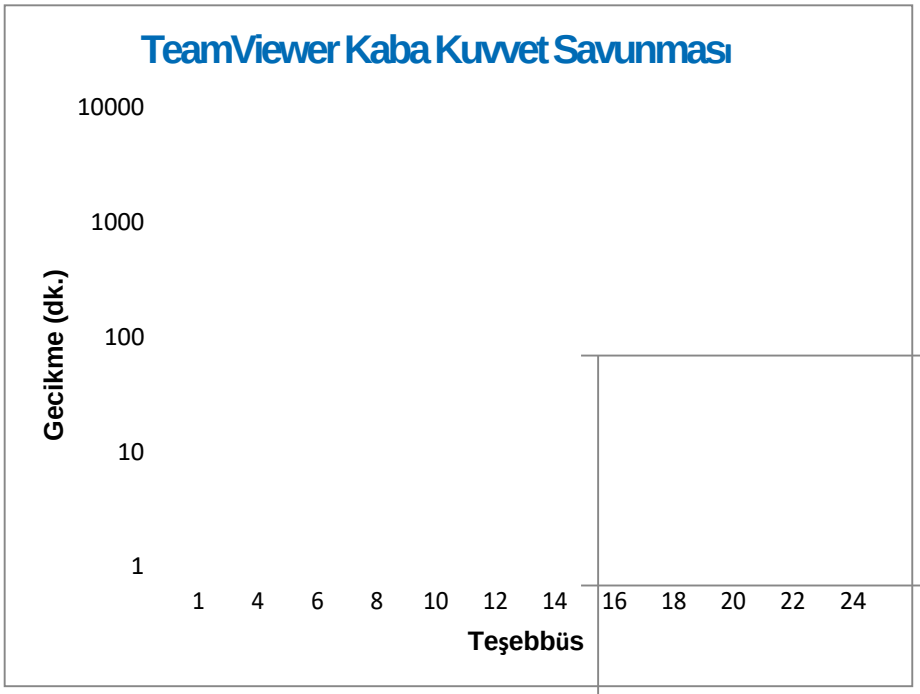
Kaba Kuvvet Saldırısına Karşı Koruma

TeamViewer'ın güvenliği hakkında bilgi edinmek isteyen potansiyel müşteriler düzenli olarak şifreleme konusunda sorular sormaktadır. Anlaşılır biçimde, en çok korkulan şey, bir üçüncü tarafın bağlantıyı izleyebiliyor olması veya TeamViewer erişim verilerinin ele geçirilmesi riskidir. Ancak, kaba saldırıların genellikle en tehlikeli saldırılar olduğu bir gerçektir.

Bilgisayar güvenliği bağlamında, kaba kuvvet saldırısı, bir kaynağı koruyan parolayı tahmin etmeye yönelik bir deneme-yanılma yöntemidir. Standart bilgisayarların işlem gücü arttıkça, uzun parolaların tahmin edilmesi için gereken süre giderek kısalmıştır.

TeamViewer, kaba kuvvet saldırılarına karşı savunma olarak bağlantı teşebbüsleri arasındaki gecikmeyi katlayarak artırmaktadır. Böylelikle 24 teşebbüste bulunulması 17 saat kadar sürmektedir. Gecikme süresi ancak doğru parola girildikten sonra sıfırlanır.

TeamViewer müşterilerini belirli bir bilgisayardan gelen saldırılardan korumanın yanı sıra birden fazla bilgisayardan gelen, botnet saldırıları olarak bilinen, belirli bir TeamViewer ID'sine erişmeye çalışan saldırılardan da korumaya yönelik bir mekanizmaya sahiptir.



Çizelge: Bir kaba kuvvet saldırısı sırasında n sayıda bağlantı teşebbüsünden sonra geçen süre

Kod İmzalama

Ek bir güvenlik özelliği olarak, bütün yazılımlarımız VeriSign Kod İmzalama aracılığıyla imzalanır. Bu şekilde, yazılımın yayıncısı her zaman kolaylıkla tanımlanabilir. Yazılım sonradan değiştirilmişse, dijital imza otomatik olarak geçersiz olur.

Veri Merkezleri ve Omurga

TeamViewer servisleri için mümkün olan en iyi güvenliği ve kullanılabilirliği sağlamak üzere, bütün TeamViewer sunucuları ISO 27001 uyumlu veri merkezlerinde bulunmaktadır ve çoklu yedek taşıyıcı bağlantılar ve yedek güç beslemeleri ile güçlendirilmiştir. Ayrıca, yalnızca en ileri teknolojiye sahip marka donanımı kullanılmaktadır. Buna ilaveten, hassas verilerin saklandığı bütün sunucular Almanya'da veya Avusturya'da bulunmaktadır.

ISO 27001 belgeli olmak, yalnızca yetkili kişilere veri merkezine erişim izni verilmesini ve donanım ile veriler için mümkün olan en iyi güvenliğin garanti edilmesini sağlamak üzere erişim kontrolü, video kamera ile izleme, hareket detektörleri, 7x24 izleme ve saha güvenlik personeli kullanılması anlamına gelir. Ayrıca, verimerkezine tek giriş noktasında ayrıntılı bir kimlik kontrolü bulunmaktadır.

TeamViewer Hesabı

TeamViewer hesapları özel TeamViewer sunucuları üzerinde barındırılır. Erişim kontrolü hakkında bilgi için lütfen yukarıdaki Veri Merkezi ve Omurga bölümüne başvurun. Yetkilendirme ve parola şifreleme için, geliştirilmiş bir parola doğrulamalı anahtar anlaşması (PAKE) protokolü olan Güvenli Uzak Parola protokolü (SRP) kullanılır. Sisteme sızan veya iki nokta arasındaki bağlantıya yetkisiz müdahale eden kişi bir parolayı kaba kuvvet ile tahmin etmek için yeterli bilgi edinemez. Bu, zayıfparolalar kullanılarak bile kuvvetli bir güvenlik sağlanabileceği anlamına gelir. TeamViewer hesabı içerisindeki hassas veriler, örneğin bulut depolama oturum açma bilgileri, AES/RSA 2048 bit ile şifrelenerek saklanır.

Management Console

TeamViewer Management Console, kullanıcı yönetimine, bağlantı raporlamaya ve Bilgisayarlar ve Kişilerin yönetilmesine yönelik web tabanlı bir platformdur. ISO-27001 belgeli, HIPAA uyumlu veri merkezlerinde barındırılmaktadır. Bütün veri aktarımları güvenli İnternet ağ bağlantıları standardı olan TSL (Taşıma Katmanı Güvenliği) şifrelemesi kullanan güvenli bir kanal üzerinden gerçekleştirilmektedir. Hassas veriler ayrıca AES/RSA 2048 bit ile şifrelenerek saklanır. Yetkilendirme ve parola şifreleme için Güvenli Uzak Parola protokolü (SRP) kullanılır. SRP, 2048 bit katsayısı kullanan iyi yapılandırılmış, sağlam, güvenli parola tabanlı bir doğrulama ve anahtar alışverişi yöntemidir.

Politika Tabanlı Ayarlar

Kullanıcılar, TeamViewer Management Console içerisinden özellikle kendilerine ait aygıtlara TeamViewer yazılım kurulumları için politikalar tanımlama, dağıtma ve uygulama imkanına sahiptir. Ayar politikaları kendilerini oluşturan hesap tarafından dijital olarak imzalanır. Bu, yalnızca aygıtın ait olduğu hesabın aygıta politika atama iznine sahip olmasını sağlar.

TeamViewer'da Uygulama Güvenliği

Kara ve Beyaz Liste

Özellikle TeamViewer gözetimsiz bilgisayarların bakımı için kullanıldığında (yani TeamViewer is bir Windows servisi olarak kurulduğunda), bu bilgisayarlara erişimin bir dizi özel istemci ile sınırlanmasına ilişkin ek güvenlik seçeneği ilgi çekici olabilir.

Beyaz liste işlevi ile hangi TeamViewer ID'lerinin ve/veya TeamViewer hesaplarının bir bilgisayara erişme iznine sahip olduğunu açıkça belirtebilirsiniz. Kara liste işlevi ile belirli TeamViewer ID'lerini ve TeamViewer hesaplarını engelleyebilirsiniz. Yukarıda açıklanan “politika tabanlı ayarlar”ın bir parçası olarak “Management Console” altında merkezi bir beyaz liste bulunmaktadır.

Sohbet ve Video Şifreleme

Sohbet geçmişleri TeamViewer hesabınızla ilişkilendirilir ve dolayısıyla "TeamViewer Hesabı" başlığı altında açıklandığı biçimde aynı AES/RSA 2048 bit şifreleme güvenliği kullanılarak şifrelenir ve saklanır. Bütün sohbet iletileri ve video trafiği AES (256 bit) oturum şifreleme ile uçtan uca şifrelenir.

Gizli Çalışma Kipinin Bulunmaması

TeamViewer'ın tamamen arka planda çalışmasını sağlamanıza imkan tanıyan hiçbir işlev bulunmamaktadır. Uygulama arka planda bir Windows servisi olarak çalışıyor olsa bile, TeamViewer sistem tepsisindeki bir simge aracılığıyla her zaman görünür.

Bir bağlantı kurulduktan sonra sistem tepsisinin üzerinde her zaman görünür halde küçük bir kontrol paneli bulunur. Dolayısıyla, TeamViewer'ın bilgisayarların veya çalışanların gizli bir şekilde izlenmesi için uygun olmaması amaçlanmıştır.

Parola Koruması

Anlık müşteri desteği için, TeamViewer (TeamViewer QuickSupport) bir oturum parolası (tek kullanımlık parola) oluşturur. Müşteriniz size parolasını söylerse, ID'sini ve parolasını girerek bilgisayarına bağlanabilirsiniz. Müşterinizin bilgisayarlarına yalnızca davet edilmeniz halinde bağlanabilmeniz için, TeamViewer müşteri tarafında yeniden başlatıldıktan sonra yeni bir oturum parolası oluşturulur.

(Örneğin sunucular üzerinde) gözetimsiz uzaktan destek için TeamViewer kullanıldığında, bilgisayara erişim güvenliğini sağlayan bağımsız, sabit bir parola belirleyin.

Gelen ve Giden Erişim Kontrolü

TeamViewer'ın bağlantı kiplerini bağımsız olarak yapılandırabilirsiniz. Örneğin, uzaktan destek veya toplantı bilgisayarınızı hiçbir gelen bağlantının kurulamayacağı biçimde yapılandırabilirsiniz.

İşlevlerin fiilen ihtiyaç duyulan özelliklerle sınırlandırılması, her zaman potansiyel saldırılar için olası zayıf noktaların sınırlandırılması anlamına gelir.

İki Faktörlü Kimlik Doğrulama

TeamViewer, HIPAA ve PCI uyum gereksinimleri konusunda şirketlere yardımcı olur. İki faktörlü kimlik doğrulama, TeamViewer hesaplarını yetkisiz erişimden korumak için ilave bir güvenlik katmanı sağlar.

Hem kullanıcı adı hem de parola kullanılmasına ilaveten, kullanıcı kimliğini doğrulamak için bir kod girmek zorundadır. Bu kod zamana dayalı tek kullanımlık parola (TOTP) algoritması ile oluşturulur. Dolayısıyla kod yalnızca kısa bir süre boyunca geçerlidir.

TeamViewer, iki faktörlü doğrulama ve beyaz liste yoluyla erişimin sınırlandırılması aracılığıyla, HIPAA ve PCI belgelendirmeleri için gerekli bütün kriterlerin sağlanmasına yardımcı olur.

Güvenlik Testi

Hem TeamViewer altyapısı hem de TeamViewer Yazılımı düzenli olarak penetrasyon testlerine tabi tutulur. Testler, güvenlik testleri konusunda uzmanlık sahibi bağımsız şirketler tarafından yürütülür.

Diğer sorularınız için:

Diğer sorularınız veya daha fazla bilgi için, (Türkiye) +90 212 414 2751 ve (Almanya) +49 (0) 7161 60692 50 numaralı hatlar üzerinden bize ulaşın veya support@teamviewer.com adresine e-posta gönderin.

İletişim

TeamViewer GmbH
Jahnstr. 30
D-73037 Göppingen
Almanya
service@teamviewer.com