KABLOSUZ AĞ ALTYAPISINI SAĞLAMLAŞTIRMA

Güvenli mimari planlama , altyapının sağlamlaştırılmasını ele almalı ve bu en iyi uygulamaların çoğu , test veya kavram kanıtı (PoC) dağıtımında bile kablosuz altyapı dağıtılmadan önce yerinde olmalıdır. Sertleştirme önerileri , risk toleransına , tehditlere ve mevcut kaynaklara göre kuruluştan kuruluşa göre değişir. Her kuruluşun tüm kontrollerin hepsini uygulayamayacağını belirtmek önemlidir. Güvenlik açısından pek sevilmeyen bir durumdur fakat güvenlik dengeleyici eylemdir. Her kuruluş burada sunulan artıları , eksileri dikkatle değerlendirmelidir. Sunulan sertleştirme mekanizmalarının çoğu , kuruluşun çevreye ilişkin görünürlüğünü büyük ölçüde azaltırken sınırlayıcı kontroller , böyle bir ortamı uygun şekilde yönetmek için ek kaynakların ve süreçlerin mevcut olduğu kurumlar , finansal kuruluşlar gibi hedeflenen ortamlar için uygundur. Tüm kuruluşlar , daha yüksek güvenlik katmanları için ek kontroller önerilirken , sertleştirme için minimum kılavuzu izlemelidir.

Yönetim Erişiminin Güvenliğini Sağlama ; Sertleştirme için ilk görev , tüm yönetim protokollerinin şifreleme ve uygun kimlik doğrulama kullanacak şekilde yapılandırıldığından emin olmaktır. Bu görevler , şifrelenmiş protokollerin etkinleştirilmesini ve şifrelenmemiş protokollerin devre dışı bırakılmasını (SSH'nin etkinleştirilmesi ve CLI erişimi için Telnet'in devre dışı bırakılması gibi) , sistem bileşenleri boyunca tüm varsayılan parolaların kaldırılmasını , kullanıcı tabanlı oturum açmaları zorlamak için yönetim erişiminin sıkılaştırılmasını (paylaşılan oturum açmalara karşı) ve izin verilen yönetim trafiği kaynaklarını içerir. Yönetim erişiminin güvenliğini sağlamak konular şöyedir ; Şifreli yönetim protokollerine zorlama. Varsayılan kimlik bilgilerini ve parolaları ortadan kaldırma. yönetici erişimini ve kimlik doğrulamayı denetleme. Paylaşılan kimlik nilgilerinin ve anahtarların güvenliğini sağlama. Ayrıcalıklı erişimi ele alma. Ek güvenli yönetim hususlarıdır.

Şifreli Yönetim Protokollerini Zorlama ; Sertleştirme için izlenmesi gereken birkaç en iyi uygulama vardır ve şifreli yönetim protokollerini zorlamak (varsayılan kimlik bilgilerinin kaldırılmasıyla birlikte) bunlardan biridir. Özel yönetim VLAN'ı ve kısıtlı yönetim erişimi olan güvenli üretim ortamında bile , ağ cihazlarının şifreli yönetim protokolleri için yapılandırılması zorunluluktur. Bunu yaparken , kritik ve hassas yönetim trafiğinin gizlice dinleme yoluyla açığa çıkmamasını sağlarsınız. Kötü niyetli kullanıcı olduğu kadar güvenlik araçlarının da neden olduğu bir senaryodur. Çoğu ağda , trafiğin bir kısmı veya tamamı , güvenlik incelemesi veya temel analitiği doldurma amacıyla ağdan geçerken incelenir. Kullanıcı ve varlık davranışı analitiği (UEBA) , güvenlik bilgileri ve olay yönetimi (SIEM) gibi ağ tabanlı güvenlik araçları aracılığıyla veya gelişmiş filtreleme , derin paket incelemesi (DPI) , güvenli web'in SSL denetimi gerçekleştiren ağ geçidi güvenlik ürünleri aracılığıyla olabilir. Kaynak veya neden ne olursa olsun , yönetim trafiğinin açık metin olarak iletilmesini asla istemezsiniz çünkü bunun nerede gizli dinlemeye maruz kalabileceğini , içeriğinin ifşa veyahut ele geçirildiğini asla bilemezsiniz. Şifrelemeden gizliliği sağlamaya ek olarak , güvenli yönetim protokolleri , yönetici kullanıcının sisteme güçlü kimlik doğrulaması yoluyla bütünlük ekler ve mesaj bütünlüğünü içerir. Bu eklenen bütünlük özellikleri , yönetim trafiğinin sadece gizli kalmasını sağlamakla kalmaz aynı zamanda reddedilmez ve kurcalamaya karşı dayanıklı olmasını sağlar.

Şifreli Yönetim için Anahtarlar ve Sertifikalar Oluşturma ; 802.1X/EAP kimlik doğrulaması için RADIUS sunucularının uç noktalara ve isteğe bağlı olarak uç noktalara sunucuya kimlik doğrulaması amacıyla sertifikaların kullanımına değinilmiştir. Buradaki sertifikalar , cihazların yönetimini güvence altına almaya odaklanmıştır. Kimlik doğrulama için sertifikaların ve şifreleme için anahtarların kullanılması , sertifikaların ve anahtarların yönetilen cihazda bulunması gerektiği anlamına gelir. Sertifika ve anahtar oluşturmayı nasıl ele aldıkları konusunda satıcılar arasında epey farklılıklar bulunmaktadır fakat tüm ürünlerin altında yatan ortak gereksinimler var. Satıcılarınızın bununla ilgili en son belgelerini araştırmak göreviniz olmalıdır.

Sertifika ve anahtar oluşturma için satıcılar tarafından desteklenen yöntemler şöyledir ; Kendinden imzalı sertifikalar. Güvenli benzersiz donanım kimliğine bağlı sertifikalar. Üçüncü taraf veya genel kök CA'lardan verilen sertifikalar. Dahili alan CA'larından veya PKI'den verilen sertifikalar. Anahtar çiftleri kullanılarak cihazda oluşturulan anahtarlar.

Güvenli cihaz yönetim sertifikaları şu şekillerde kullanılır ; Güvenli HTTPS web UI yönetimi için. Denetleyicinin AP'lerde kimliğini doğrulamak için ve tersi için.

Güvenli cihaz yönetimi için anahtar çiftleri şunlar için kullanılır ; Güvenli Kabuk (SSH) kimlik doğrulaması. Güvenli Kabuk (SSH) şifrelemesi. SSH'ye dayalı Güvenli Kopyalama Protokolü (SCP).

Kablosuz denetleyicilerin bazı sürümleri , burada açıklanan sertifikalara veya anahtar çiftlerine dayanmayan güvenli dosya aktarımları için SFTP'yi de desteklemektedir. Uygulamalar ve satıcı desteği biraz farklılık gösterse de , güvenli yönetim için sertifikaların ve anahtar çiftlerinin oluşturulması ve kullanılmasına yönelik ortak kılavuz vardır. Ayrıca kripto söz konusu olduğunda , anahtar boyutu önemlidir. Sertifikalar için bugünün standartlarını karşılamak ve dağıtımınızı geleceğe hazırlamak için minimum değerler olarak RSA 3072-bit veya ECC P-256'yı düşünmelisiniz.

Kendinden İmzalı Sertifikalar ; Tüm kablosuz ürünler tarafından desteklenir ancak önerilmez. Bunun yerine , güvenilir altyapı için donanım tabanlı sertifikaları (destekleniyorsa) veya bir kök CA'dan (dahili veya üçüncü taraf) verilen sertifikaları kullanmalısınız. Sertifikaların amacı ; bütünlük , gizlilik , kimlik doğrulama , şifreleme sağlamaktır. Kendinden imzalı sertifika kullanarak , istemcinin sunucu sertifikasını bilinen ve güvenilen kök CA'ya karşı doğrulamasının hiçbir yolu olmadığından mekanizmanın kimlik doğrulama bölümünü etkin şekilde geçersiz kılarsınız.

Güvenlik riskine ek olarak , güvenlik değerlendirmeleri sırasında ortamda kendinden imzalı sertifikalar ve joker karakter sertifikaları kullanan kuruluşlar cezalandırılacak veya işaretlenecektir. Daha az güvenli sertifika uygulamaları hiçbir zaman önerilmez fakat altyapı yönetimini güvence altına alırken özellikle kötü uygulamalardır.

Güvenli Benzersiz Donanım Kimliğine Bağlı Sertifikalar ; On yıldan fazla süredir endüstri , değişmez güvenli donanım tabanlı kimliklere bağlı kriptografik bağlamalar için çalışmaktadır. Değeri , cihazlara birlikte çalışabilir kimlik doğrulama ve şifreleme için güçlü entegre mekanizma ile cihazlara sertifikaları manuel olarak sağlamak zorunda kalmadan sağlamasıdır. IEEE 802.1AR standardı , üretim sırasında cihaz donanımına bağlı X.509 sertifikalarını kullanarak kimlik doğrulama , sağlama ve 802.1X EAP kimlik doğrulaması dahil yönetim amaçları için kullanılacak Güvenli Cihaz Tanımlayıcılarını (DevID) belirtir. DevID'ye ek olarak , bazı ürünler ağ yöneticilerinin Yerel Cihaz Tanımlayıcıları (LdevID) ile ek sertifikalar oluşturması ile eklemesine izin verir. 802.1AR çalışması , 802.1AR ile kullanılabilen Güvenilir Platform Modülü (TPM) gibi uzun süredir devam eden girişimlere dayanmaktadır. Daha spesifik ifade edecek olursak ; bu teknoloji , Cisco'nun 802.1AR uyumlu güvenli cihaz kimliği olan Güvenli Benzersiz Cihaz Tanımlayıcısında (SUDI) bulunur. Cisco'nun denetleyicideki SUDI'si , AP birleştirme işlevleri için güvenilir sertifika , HTTPS sertifikası , SSH ve sıfır dokunuşla sağlama dahil olmak üzere çeşitli işlevler için kullanılabilir. Donanım sertifikasının süresi dolduğunda , SUDI sertifikasını kullanan tüm özellikler başarısız olacaktır ve geçici çözümler için üreticilerin saha bildirimlerine bakmanız gerekecektir. Diğer üreticiler , 802.1AR ve TPM'ye dayalı olanlar gibi güvenli donanım tabanlı kimliklere doğru ilerlemektedir. 802.1AR cihaz kimlikleri donanıma özeldir ve bulutta barındırılan yöneticiler ile sanallaştırılmış cihazlar için geçerli değildir.

802.1AR Standardı ; IEEE 802.1AR-2018 standart belgesi şu web sitesinde ücretsiz olarak yeralmaktadır. Orijinal standart 2009'da oluşturuldu ve 2018'de ECDSA (Eliptik Eğri Dijital İmza Algoritması) desteği eklemek için güncellenmiştir. 802.1AR ve donanım tabanlı sertifikaların kullanımı , EAP-TLS ile 802.1X kullanılarak bir cihazın kimliğinin doğrulanması , PKI altyapıları ile sertifika kaydı sürecinde cihazın tanımlanması yer almaktadır.

Üçüncü Taraf veya Genel Kök CA'lardan Verilen Sertifikalar ; Kablosuz denetleyiciler gibi cihazlar için sertifikalar , üçüncü taraf ve genel kök CA'lar dahil olmak üzere manuel olarak istenebilir ve yüklenebilir. Bu durumlarda , sertifikayı veren CA'dan sertifika istemek için kullanılan sertifika imzalama isteği (CSR) oluşturma talebini izleyip akabinde imzalı sertifikaları indirip manuel olarak kuracaksınız. Dahili Etki Alanı CA'larından veya PKI Manuel sertifika istekleri ile yüklemeleri , hem üçüncü taraf hem de dahili etki alanı CA'ları için desteklenir. Dahili CA'lar kullanılırken kayıt daha otomatik hale getirilebilir. Etki alanı tarafından verilen sertifikaların kaydının hizmetinde , kablosuz sistemler gibi ağ altyapısı cihazları , etki alanı altyapısından sertifika talep etmek ve yüklemek için standartlara dayalı süreçleri kullanabilir. Çoğu üründe , Basit Sertifika Kayıt Protokolü (SCEP) veya Güvenli Aktarım Üzerinden Kayıt (EST) kullanılarak desteklenir. Her iki durumda da , denetleyici , AP'ler adına sertifika isteklerini ve kurulumunu vekalet edecektir. Geçmiş deneyimlere ve mevcut satıcı belgelerine dayanarak , ürünler sertifika kaydı için bir veya diğer protokolü destekleyecektir. Dolayısıyla seçim yapmanıza gerek yoktur. Ürünün desteklediği her şeyi kullanacaksınız. Yazma sırasında , Cisco'nun IOS-XE kodu SCEP ve EST kullanır , Aruba'nın Aruba AOS 8 kodlu zinciri EST kullanır.

Genel / Özel Anahtar Çiftleri Kullanılarak Cihazda Oluşturulan Anahtarlar ; SSH gibi anahtar çiftlerine dayanan protokollerin anahtar oluşturma için satıcının kılavuzunu takip etmeniz yeterlidir. Sertifikaları kullanırken her zaman olduğu gibi , saat senkronizasyonu çok önemlidir ve sertifikaları oluşturmadan veya kullanmadan önce gerçekleştirilmelidir. Zaman senkronizasyonu ayarlarıyla birlikte , sertifika imzalama isteği (CSR) veya kendinden imzalı sertifika oluştururken FQDN'ye sahip olması için cihazın host bilgisayar adını ve etki alanını da belirtmeniz gerekir.

Sertifikalar birkaç dosya biçiminde gelir ; farklı grafik dosya biçimleri olduğu gibi , satıcılar tarafından kullanılan sertifika dosyaları da X.509 PEM (şifreli veya şifresiz) , DER , PKCS#7 , PKCS#12 olarak bulunur. En yaygın olanları , metin ASCII tabanlı olan ve -----BEGIN CERTIFICATE----- gibi okunabilir başlıklara sahip olan PEM (başlangıçta gizliliği geliştirilmiş e-posta olarak belirlenmiştir) dosya biçimleridir. PEM dosyası , tek bir sertifika , bir özel anahtar veya bir güven zinciri oluşturan (kök CA ve aracıları desteklemek için) birden çok sertifika içerebilir ve genelde .crt , .cert , .pem dosya uzantılarına sahiptir (sertifikalar için) , .key (özel anahtarlar için). DER ve PKCS biçimleri , DER ve PKCS#12'nin sertifikaları tam güven zincirleri ve PEM gibi özel anahtarlarla birlikte depolayabildiği ikili biçimlerdir fakat PKCS#7 yalnızca tek sertifikalar için bir biçimdir. AP'ler tarafından altyapıda kimlik doğrulaması yapmak için kullanılan zincirleme sertifikalar için satıcılar zincirleme sertifikaların dosya içinde belirli bir sırada olmasını isteyecektir. Genelde AP sertifikasından başlayarak ara CA sertifikası , kök CA sertifikası ve ardından Özel anahtarlar vardır. Unutulmaması gereken önemli nokta ; her satıcının farklı dosya formatlarını destekleyeceği ve gerektiğinde formatlardan dönüştürmenin mümkün olmasıdır. Nasıl yapılır ayrıntıları için satıcınızın ürün belgelerine veya veren sertifika yetkilisinin talimatlarına bakınız. " Begin Certificate " ve " End Certificate " içeren PEM sertifikasının standart okunabilir üstbilgisini ve altbilgisini bulunmaktadır. DER sertifikaları , insan tarafından okunabilir metin içermeyen ikili dosyalar içerir.

HTTPS ve HTTP'yi Etkinleştirme ; HTTPS'yi etkinleştirmek , ertifika gerektirecektir. Kendinden imzalı (önerilmez) , üretim sırasında verilen donanım tabanlı sertifika veya genel veya kuruluş içinde kök CA tarafından verilen bir sertifika olabilir. Altyapı ürünleri , ilk açılışta kendinden imzalı sertifika oluşturacak veya manuel olarak kendinden imzalı sertifika oluşturulmasına izin verecektir. Kendinden imzalı sertifikalar üretimde kullanılmamalıdır fakat yönetici başlangıçta denetleyiciye veya cihaza web kullanıcı arayüzü ile erişiyorsa, kendinden imzalı sertifika kullanan güvenli olmayan HTTP veya HTTPS'nin meydana geleceği ilk kullanım olacaktır. Denetleyiciye veya cihaza uygun sertifika yüklendikten sonra , HTTP ile erişim derhal devre dışı bırakılmalı ve bunun yerine şifrelenmiş HTTPS'yi zorunlu kılmalıdır. Kuruluşunuz cihazları web kullanıcı arayüzü ile yönetmiyorsa , hem HTTP'yi hem de HTTPS'yi devre dışı bırakabilirsiniz. Bazı ürünler , destekleniyorsa etkinleştirilmesi gereken HTTP'den HTTPS'ye otomatik yönlendirme ayarını destekleyebilir. Birçok kablosuz ürün , cihazın kablosuz üzerinden yönetilmesini sağlamak için ek ayar gerektirebilir. Bazı ürünler , kullanıcı adı ve parola kimlik doğrulaması eklenerek veya eklenmeden HTTPS yönetimi için istemci sertifikaları aracılığıyla yöneticilerin kimlik doğrulamasını da destekleyebilir. Bu durumlarda sadece yüklü sertifikaya sahip istemci cihazına HTTPS üzerinden cihaza yönetim erişimine izin verilir. Bu yapılandırmayla erişim , istemci sertifikasını kendi başına veya bir yönetici oturum açma işlemiyle birlikte gerektirebilir. Çoğu Wi-Fi ürününde HTTPS kullanımını yapılandırabilir ve web kullanıcı arayüzünde veyahut CLI'de HTTP'yi devre dışı bırakabilirsiniz.

SSH ve Telnet'i Etkinleştirme ; Yönetici erişimi için Secure Shell (SSH) ile çalışmak iki yönlüdür ; hem şifreleme mekanizması hem de kimlik doğrulama işlevi görebilir. Öncelikli SSH , CLI tabanlı uzaktan yönetim erişimi için şifrelemeyi etkinleştirmek için anahtar çiftlerini kullanır. İkincisi ve genelde gözden kaçan SSH , istemci anahtarlarını yönetim kimlik doğrulama mekanizması (sertifikalar gibi) olarak kullanabilir , kullanıcı adı ve parola bilgileriyle veyahut bunlar olmadan uygulanabilir. Diğer güvenli protokollerde olduğu gibi , anahtar çiftleri oluşturmak için gerekli adımları tamamlamanız ve ardından SSH'yi etkinleştirmeniz veya şifrelenmemiş karşılığı Telnet'i devre dışı bırakmanız gerekir. Sertifika oluşturmada olduğu gibi SSH anahtar çiftlerini oluşturmak için önce cihaz için host bilgisayar adı ve etki alanı belirtmeniz gerekir. SSHv2 , bilinen güvenlik açıklarına sahip SSHv1'e karşı kullanılmalıdır.

FIPS Modunda SSH ; Kablosuz cihazlarda etkinleştirilen FIPS gibi belirli işletim modları , şifreleme modülleri için ABD hükümeti Federal Bilgi İşleme Standardı (FIPS) 140-2 standardını karşılamak için daha güçlü şifreleme algoritmaları gerektirir. Bu modlar etkinleştirildiğinde , belirli özellikler devre dışı bırakılabilir veya belirtilen güvenlik parametrelerini karşılayacak şekilde otomatik olarak yapılandırılabilir. İkinci kullanım durumu ise yetkili kullanıcı adı-şifre kimlik bilgisi yerine veya SSH anahtarlarının kimlik bilgisi biçimi olarak kullanılmasını içerir. Anahtar tabanlı kimlik doğrulama için kullanıldığında yönetici veya otomatik sistem , o cihazda o kullanıcı tarafından kullanılmak üzere benzersiz anahtar çifti oluşturarak istemci anahtarı , SSH terminal uygulaması (PUTTY gibi) yönetici kullanıcının kimliğini kablosuz denetleyicide doğrulayarak giriş yapar. Kimlik doğrulama için SSH ortak anahtarları , PUTTYGEN (PUTTY terminal uygulamasına dahil olan eklenti) veya OpenSSL gibi ortak araç kullanılarak oluşturulabilir. Özel anahtar , bütünsel SSH anahtar yönetim sürecinin parçası olarak düzgün şekilde kaydedilerek güvence altına alınmalıdır. Akabinde kablosuz denetleyicide çiftin ortak anahtarını yükleyecek ve bir kullanıcıyla ilişkilendireceksiniz. Kullanıcının ortak anahtarı , sertifika deposuna yüklenir ve akabinde bir kullanıcıyla ilişkilendirilir. Kimlik doğrulama için SSH anahtarlarını yapılandırabilirsiniz.

Bu özelliği bulmak her zaman kolay değildir fakat Aruba Networks için kullanım kılavuzunda " Genel Anahtar Kimlik Doğrulaması "nı arayın ve Cisco için " ip ssh pubkey-chain " çevresinde benzer komutları arayınız.

Güvenli Dosya Aktarımlarını Etkinleştirme ; Dosyaları kablosuz denetleyiciye veya kablosuz denetleyiciden taşımamız gereken durumlar bulunmaktadır. Taşıma sırasında yükü korumak için dosya aktarım protokolleri de şifrelenmelidir. Cihaza veya cihazdan taşınabilecek dosyalar arasında yapılandırma dosyaları , yazılım güncellemeleri ve yamalar , AP listeleri , sertifika dosyaları , MIB dosyaları ve konuk kullanıcılar listesi , izin verilenler listesi için MAC adresleri gibi CSV dosyaları bulunur. Web kullanıcı arayüzü kullanılarak aktarılan dosyalar HTTPS protokolü ile şifrelenecektir fakat CLI aracılığıyla aktarılan dosyalar , kimlik doğrulama ve şifreleme sağlamak için güvenli kopya (SCP) veya güvenli FTP (SFTP) ile güvence altına alınmalıdır. SCP , SSH'ye dayanarak en azından şifreleme yönü için (ortak anahtar kimlik doğrulamasına karşı) SSH'yi yapılandırmak ön koşuldur. SCP , önceden yapılandırılmış olmak için SSH , kimlik doğrulama ve yetkilendirme gerektirdiğinden , birçok ürün varsayılan olarak şifrelenmemiş FTP (Dosya Aktarım Protokolü) ve TFTP'ye sahiptir. FTP'nin kimliği doğrulanmış ancak şifrelenmemiş olsa da , TFTP'nin kimliği doğrulanmamış veya şifrelenmemiştir. Bazı ürünler şifreleme için SSH'ye dayanan SFTP'yi (güvenli FTP) de desteklemektedir. SSH'yi ve ardından SCP veya SFTP'yi etkinleştirerek TFTP ve FTP'yi devre dışı bırakınız. Ya da TFTP ve FTP'yi devre dışı bırakmak genel ayar değilse yönetim işlevlerini her biri SCP veya SFTP kullanacak şekilde yapılandırınız.

Dosya transfer protokol güvenliğine göz gezdirecek olursak ;

Secure Copy (SCP) ; Doğrulanmış (Authenticated) ve şifrelenmiştir.

Secure FTP (SFTP) ; Doğrulanmış (Authenticated) ve şifrelenmiştir.

File Transfer Protocol (FTP) ; Doğrulanmış (Authenticated) ve şifrelenmemiştir.

Trivial FTP (TFTP) ; Doğrulanmamış (Non-Authenticated) ve şifrelenmemiştir.

SNMPv3'ü SNMPv2c'ye karşı etkinleştirme ; Basit Ağ Yönetim Protokolü (SNMP) , dizüstü bilgisayarlar ve yazıcılar gibi sunuculara ve uç noktalara ek olarak anahtarlar , yönlendiriciler ve kablosuz ürünler gibi ağ cihazlarını izlemek ve yönetmek için standart protokoldür. SNMP verileri , yönetim bilgi tabanlarında veya MIB'lerde düzenlenir. MIB özniteliklerini bir öğeye sahip veritabanı ve akabinde " hostname " gibi karşılık gelen yapılandırmaları olarak düşününüz. Ağa bağlı bir cihazın çoğu yönü için standart MIB öğeleri vardır ve bunlar sorgulanabilir veya değiştirilebilir. SNMP , bir günlük kaydı sistemine yönelik uyarı biçimi olan tuzak işlevi için kullanılabilir. Bilgi için cihazı yoklayan izleme sistemi yerine sistem , yapılandırılmış bir sunucuya karşılıksız olarak tuzak gönderebilir. Tuzaklar , seviyeye göre etkinleştirilebilir veya grup veyahut tuzak tipine göre yapılandırılabilir. SNMP'nin günümüzde en yaygın olarak kullanılan iki versiyonu SNMPv2C ve SNMPv3'tür. Dünyada hala SNMPv1'e güvenen ancak güvenlik nedeniyle kullanımdan kaldırılmış birkaç cihaz vardır. SNMPv2c'den önce , şifreleme ve diğer güvenlik sunan ancak karmaşıklığı nedeniyle benimsenmeyen SNMPv2 bulunmaktaydı.

SNMPv2c ; Gerçek kimlik doğrulamaya karşı topluluk dizelerine dayanır ve şifreli değildir. Topluluk dizeleri , sadece parola (RADIUS paylaşılan sırrı gibi) işlevi gören alfasayısal karakter dizeleridir. Topluluk dizileri açık metin olarak gönderilir yani ne yönetim verileri ne de topluluk dizilerinin sahte kimlik doğrulaması korunmaz.

SNMPv3 ; SNMPv3 daha sonra gerçek kimlik doğrulama , şifreleme ve veri bütünlüğü eksikliğini gidermek için oluşturulmuştur. SNMPv3 ile kullanıcılar , kimlik doğrulama şeması (MD5 , SHA) , kimlik doğrulama parolasının yanı sıra gizlilik protokolü (AES , DES) ve buna karşılık gelen gizlilik parolası ile oluşturulur ve belirlenir. SNMPv3 kullanıcısı , bir insana bağlı gerçek bir kullanıcı hesabından çok bir makine hesabıdır. Her yönetim veya izleme sistemi için kullanıcılar oluşturulur. SNMPv3 , parola tabanlı mekanizma gibi , kaba kuvvet ve sözlük saldırılarıyla tehlikeye girebilir fakat SNMPv2c'den ve öncekilerden daha iyi sınırları vardır. SNMPv3 , gizlilik ve kimlik doğrulama kontrollerine ek olarak , yanıltmayı önlemek için güvenlik mekanizmaları içerir ve açık metin kimlik bilgilerinin veya veri yüklerinin kullanımını ortadan kaldırır. Altyapınız SNMP ile yönetiliyor veya izleniyorsa , önceki sürümlere kıyasla her zaman SNMPv3 kullanılması önerilir.

SNMP VE NETCONF ; Cisco ve Aruba dahil denetleyici tabanlı kablosuz sistemler için SNMP , denetleyici veya AP'lerin yapılandırılması için değil , yalnızca izleme ve uyarı için kullanılır. Bu kullanım durumunda bile şifreli SNMPv3 sürümü hala önerilir ve SNMPv2c devre dışı bırakılmalıdır. ExtremeCloud (eski adıyla Aerohive) gibi bulut tarafından yönetilen çözümler de SNMPv2c ve güvenli SNMPv3 dahil SNMP'yi destekler. Juniper's Mist kablosuz gibi diğer bulut yerel çözümleri , güvenli API'ler kullanır ve SNMP'yi hiç kullanmaz veya desteklemezler. Bunun yerine ise bu uygulamalar yapılandırmaları zorlamak , izleme için yapılandırmaları çekmek , panolarda yapılandırmaları görüntülemek , diğer üçüncü taraf ürün entegrasyonlarını desteklemek için API'leri kullanır. Bulut ağının girişi ve ağ işlevi sanallaştırmasının (NFV) genişlemesiyle birlikte , satıcılar NETCONF ve YANG (şimdi her ikisi de IETF standartları) gibi çok daha fazla otomasyon ve entegrasyon içeren yönetim seçeneklerini tercih etmeye başlamaktadır. NETCONF ve YANG birlikte , birden çok satıcı arasında okuma ve yazma işlevlerini standartlaştırabilen standart yapılandırma protokolleri ve veri modelleme getirmektedir. SNMP MIB'lere benzer şekilde , YANG veri modeli, standartlar tarafından tanımlanan modülleri içerir. SNMP , CLI veya geleneksel yapılandırma yönteminden farklı olarak , NETCONF , yöneticinin bireysel parametreleri yapılandırmak yerine istenen son durumu veya davranışı tanımlamasına olanak tanıyan amaca dayalı ağ iletişimi için tasarlanmıştır. YANG verileri XML olarak kodlanır ve NETCONF tarafından konsol ile altyapı cihazı arasında SSH aracılığıyla taşınır. Yapılandırma değişiklikleri ve okumalar , Python komut dosyalarından komut dosyası oluşturulabilir ve yürütülebilir. Yazma sırasında , birkaç satıcı test için GitHub'da Python komut dosyalarıyla birlikte ücretsiz eğitimler ve canlı sanal alan ortamları sunar. Cisco , Juniper ve HPE Comware aygıtları , NETCONF'u destekleyen en yaygın aygıtlardan bazılarıdır.

Güvenli yönetim protokollerinin özeti şöyledir ;

Web UI Management ; Güvensiz Protokol ; HTTP , Güvenli Protokol ; HTTPS.

CLI Terminal Management ; Güvensiz Protokol ; Telnet , Güvenli Protokol ; Secure Shell (SSH).

File Transfer ; Güvensiz Protokoller ; FTP , TFTP. Güvenli Protokoller ; Secure Copy (SCP) , Secure FTP (SFTP).

SNMP ve API ; Güvensiz Protokoller ; SNMPv1 , SNMPv2 , SNMPv2c. Güvenli Protokoller ; SNMPv3 ve API.

Varsayılan Kimlik Bilgilerini ve Parolaları Ortadan Kaldırma ;

Kablosuz Yönetiminde Varsayılan Kimlik Bilgilerini Değiştirme ; Kablosuz denetleyiciler , tünel sonlandırma ağ geçitleri ve kablosuz yönetim platformları gibi şirket içi ürünler için varsayılan kullanıcıların ve kimlik bilgilerinin kaldırıldığından emin olunuz. En azından , varsayılan parolanın değiştirilmesi anlamına gelecektir ki bu da çok daha iyi bir durumdur. Hem varsayılan kullanıcı adlarını hem de parolaları değiştirmek önemlidir. Başarılı kaba kuvvet saldırısı olasılığını azaltır çünkü parola ve kullanıcı adı kombinasyonları saldırı araçlarını geride bırakır. Kötü niyetli kullanıcı sözlükleri veya gökkuşağı tablolarını kullanarak kaba kuvvet saldırısı başlatabilir. Tekrarlanan başarısız oturum açma denemelerini uyarmak için uygun izleme araçları mevcutsa , bizler için bu durum çok işimize yarayacaktır.

Şifre Uzunluk Ve Karmaşıklığı ; Bazı parola uzunlukları ve rotasyonları kısmen uyumluluk gereksinimleri tarafından öngörülse de , bu belgelerin çoğu mevcut saldırı araçlarının gerisinde kalarak öneriler söz konusu olduğunda uyum çerçevelerinden bazıları birbiriyle çelişmektedir. Günümüz dünyasında uzunluk , karmaşıklığın önüne geçiyor ve güvenlik bilincine sahip çoğu kuruluş , karmaşıklık zorlaması olmayan ancak minimum uzunluğu olan parolalara yönelmiştir. Ek olarak , daha uzun parolalar , daha katı parola rotasyon programlarını hafifletebilir ve birçok kuruluş , önceki standart 90 günde bir olan parola rotasyonu uygulamasını yılda bir kez tercih eder.

Halihazırda bunlar , birçok sektördeki çeşitli büyük kuruluşların CISO'larından ve güvenlik analistlerinden gelen öneriler şöyledir ;

Kullanıcı parolaları ; Minimum 14–16 karakter , karmaşıklık gereksinimi yok , MFA ile katmanlı , bir yıllık rotasyona sahip.

Ayrıcalıklı hesap parolaları ; Minimum 24-26 karakter , karmaşıklık gereksinimi yok , değişken rotasyonlar , MFA ile katmanlıdır.

Farklı ürünler farklı yönetim protokollerini destekler ve ürünlerin varsayılan konsol erişimi , varsayılan CLI / terminal kimlik bilgileri ve varsayılan web UI yönetimi gibi bir dizi varsayılan kimlik bilgileriyle önceden yapılandırılmış olarak gelmesi nadir değildir. Bu varsayılan hesaplar , daha sağlam güvenlik özelliklerine sahip ürünlerde daha az yaygın hale gelerek yine de yaygın bir durumdadır. Son olarak , normal yönetim arabirimlerine ek olarak , yüksek düzeyde tümleşik platformlar , satıcının diğer ürünleriyle veya entegre üçüncü taraf çözümleriyle entegrasyonlar için kullanılan kimlik bilgilerine sahip olabilir. Paket servisi , muhtemelen birden fazla olduğunu bilerek tüm varsayılan kullanıcıları ve kimlik bilgilerini bulmaktır. Bulut tarafından yönetilen ürünler için satıcının destek ekibi tarafından sistemin arka ucunda verilen erişim dışında genelde varsayılan kimlik bilgileri veya kullanıcılar yoktur. Avantaj ; varsayılan kullanıcı olmamasıdır. Dezavantajı ise yönetim arayüzünüzün internetin tamamına açık olması , yönetim erişimini güvence altına almak için güçlü parolalar ve çok faktörlü kimlik doğrulamanın kullanılmasıdır.

AP'lerde Varsayılan Kimlik Bilgilerini Değiştirme ; Yönetim platformları ve denetleyiciler , varsayılan parolaların gizlendiği tek yer değildir. Her denetleyici tabanlı üründe , AP'ler varsayılan kullanıcı adı ve parolalarla önceden yapılandırılır veya denetleyici aracılığıyla yapılandırılır. Bu , kontrolör veya yönetim yazılımı içinde merkezi olarak yapılandırılabilir ve ayarlanabilir.

Varsayılan SNMP Dizelerini Kaldırma ; Geçmişte , satıcıların SNMPv2c için varsayılan topluluk dizelerini içermesi ve SNMPv2c'nin varsayılan olarak etkinleştirilmesi yaygın idi. Daha güvenli SNMPv3'ü kullanmayı seçmiş ve doğru şekilde yapılandırmış olsanız bile , satıcının varsayılan ayarları nedeniyle altyapının risk altında olması muhtemeldir. SNMPv2c ayarlarını her zaman kontrol ederek iki kez kontrol edin ve yeniden kontrol edip etkin olmadığından (SNMPv3 kullanıyorsanız) veya etkinleştirilmişse topluluk dizelerinin özel olduğundan emin olunuz. SNMPv2c topluluk dizeleri düz metin olarak gönderildiğinden , başka hiçbir şey için gerçek parola olan dizeleri yapılandırmayınız. SNMP dizeleriniz , kullanılıyorsa , " rastgele dize " olmalıdır. SNMPv2 etkinleştirilmemiş olsa bile , varsayılan dizenin yapılandırılmadığından emin olunuz. Satıcı kodu yükseltmelerinin SNMPv2c gibi protokolleri değiştirdiği durumlar olduğu için , bu muhtemelen düzenli olarak kontrol etmeniz gereken ayardır. Hala büyük ölçüde SNMP'nin şifrelenmemiş ve kimliği doğrulanmamış SNMPv2c özelliğine dayanan birçok büyük dağıtım vardır. SNMPv3 yaklaşık 20 yıldır piyasada ve 2004'ten beri IETF tarafından RFC'ye verilen en yüksek onur olan tam internet standardı olarak taçlandırılmıştır.

Yönetici Erişimini ve Kimlik Doğrulamayı Denetleme ; Yönetim erişimini güvence altına alma görevi, yönetim erişimini ve kimlik doğrulamasını kontrol ederek devam eder. Bu konu, yönetim erişimini yalnızca ona ihtiyacı olan kişilerle (veya kişi olmayan kuruluşlarla) onaylanmış ağlardan veya kaynaklardan kısıtlamak ve erişimin günlüğe kaydedilmesini ve denetlenebilir olmasını sağlamak için kullanılabilen ayrı hususları ve özellikleri ele almaktadır.

Kullanıcı Tabanlı Oturum Açmaları Zorlama ; Kolay ve son derece etkili yönetim denetimi , yönetici veya kök hesaplar gibi paylaşılan hesaplar ile kimlik bilgileri yerine kullanıcı tabanlı oturum açmaların uygulanmasıdır. Segmentasyonun yanı sıra , güvenlik kontrolü veya uyumluluk çerçevesi için en yaygın gereksinimlerden biri de paylaşılan ve grup hesabı kimlik bilgilerinin kısıtlanmasıdır. NIST SP 800-53 , paylaşılan hesapların kullanımını kısıtlamak için bir dizi kontrol , temel ve paylaşılan hesabın gerekli olması durumunda izleme ve yaşam döngüsü yönetimi için ek kontroller belirtir. Aynı kontrol paketi , paylaşılan hesaplarda kimlik bilgileri kasası için gereksinimleri de belirtir. Yönetici erişiminin , kimliği doğrulanmış ve şifrelenmiş olmasının yanı sıra , atıfta bulunularak günlüğe kaydedilmesi ve denetlenebilir olması gerekir. Bu hedefi desteklemek için tüm kuruluşların kullanıcı tabanlı yönetim oturum açma işlemlerine güvenmeleri önerilir. Çoğu üründe , öncelikle RADIUS veya TACACS+ aracılığıyla AAA (kimlik doğrulama , yetkilendirme ve hesap oluşturma) protokolleri aracılığıyla veya alternatif olarak kimlik doğrulama sunan ancak muhasebeleştirmeyen LDAP bağlantısı aracılığıyla desteklenir. Kullanıcı tabanlı yönetim kimlik doğrulaması seçenekleri şunları içerir ; Radius , TACACS+ , LDAP'den şirket içine , SAML ile LDAP'den buluta (Azure SSO hizmetleri ve ADFS aracılığıyla).

TACACS+ , kullanıcı tabanlı yönetim kimlik doğrulaması için yalnızca bir seçenektir ve birçok kuruluş , yönetici erişim kimlik doğrulaması için RADIUS kullanmayı tercih ederek , kullanıcı tabanlı 802.1X / EAP kimlik doğrulaması için halihazırda mevcut olan altyapıdan yararlanmalarına olanak tanır. AAA (RADIUS veya TACACS+) kullanarak kimlik doğrulama yapılandırmaları , komut dosyaları veya API'ler aracılığıyla aynı anda birden fazla cihaza (kenar anahtarları veya AP'ler gibi) aktarılabilir ve geleneksel bir kablosuz denetleyicide kolayca yapılandırılabilir.

Radius / Yönetim Erişimi İçin TACACS+ ; Ayrıntılı yetkilendirme ilkeleri ideal olsa da , tüm kuruluşlarda gerekli değildir ve uyumluluk gereksinimlerinde belirtilmez (en az ayrıcalık ilkesini uygulama ihtiyacı dışında). Küçük kuruluşlar için TACACS+ tarafından sağlanan ayrıntılı politikalar gerekli değildir ve kimlik doğrulama ve muhasebe için RADIUS yeterlidir.

Karmaşık altyapıları , çok katmanlı mimarları , yöneticileri ve operasyon kullanıcıları olan büyük kuruluşlar için TACACS+'nın ek kontrolü ve denetimi istenilir. Bulut aracılığıyla hem son kullanıcı hem de yönetim kullanıcısı kimlik doğrulamasını destekleyen SaaS tabanlı bulut RADIUS platformları vardır. Kurumsal düzeyde koruma gerektiren konut ve kişisel kullanıcılar için harika seçenek olup işletmeler ve küçük kuruluşlar için çoğunda etki alanı hizmetlerine sahip en az bir sunucu bulunur ve mümkünse RADIUS hizmetlerini yerel olarak etkinleştirmek tercih edilir.

RADIUS ve TACACS+ , yönetim kimlik doğrulaması ve yetkilendirme için kullanılabilir ancak yetkilendirme ve güvenlik özelliklerinin ayrıntı düzeyi bakımından farklılık göstermektedir. Özellikle TACACS+ , özel yetkilendirme ilkelerini destekleyerek süper kullanıcının yönetici kullanıcının cihazda hangi ayrı komutları verebileceğini belirlemesine olanak tanır. TACACS+ uygulamalarında ayrıntı düzeyi değişiklik gösterir fakat genelde iki modelden birini izler ; Ayrıcalık seviyesinin yetki haklarıyla eşleştirilmesi ve belirli komutların yetkilendirme haklarıyla eşleştirilmesi. Ayrıcalık düzeyinin haklara eşlenmesine örnek olarak , TACACS+ ile kimliği doğrulanmış web UI erişimi için Cisco'nun 9800'deki mevcut kod sürümü , 1-10 ayrıcalık düzeylerine sahip kullanıcıları izleme sekmesi özelliklerine erişimle eşleştirir ve ayrıcalık düzeyi 15'e sahip kullanıcılar tam yönetime sahiptir. Bu web kullanıcı arayüzü örneğidir ; SSH için uygulandığında , web kullanıcı arayüzündeki temel iki katmana karşı komut başına politikalar uygulanabilir. Belirli komutlara örnek olarak ise Aruba denetleyicileri , yönetim için ClearPass Policy Manager , TACACS+ ilkeleriyle birlikte kullanıldığında komut başına yetkilendirmeyi destekler. Yönetim kullanıcısının hakları , tüm ayrıcalık katmanıyla eşlemeye karşı yalnızca belirli komutların yürütülmesine izin verecek şekilde kısıtlanabilir.

Endüstri Adaptasyonu ;

Radius ; Açık standarttır.

Tacacs+ ; Eylül 2020'ye kadar , üçüncü taraflarca lisanslanması gereken tescilli Cisco protokolü , yeni IETF RFC 8907'dir.

Doğrulama Güvenliği ;

Radius ; Kullanıcı adı, başka yollarla veya RADSEC ile güvence altına alınmadığı takdirde açık metin olarak gönderilebilir.

Tacacs+ ; Tüm kimlik doğrulama öğeleri şifrelenir.

Yetkilendirme Ayrıntısı ;

Radius ; Kimlik doğrulama ve yetkilendirme birbirine bağlıdır, ayrıntılı yetkilendirme politikaları yoktur.

Tacacs+ ; Parçalı ilkeler için katmanlı ayrıcalık eşlemesini veya komut başına yetkilendirmeyi destekler.

Loglama ve Accounting ;

Radius ; Doğrulanmıştır. (Authencation)

Tacacs+ ; Kimlik doğrulama artı ayrıntılı yetkilendirme.

Protokoller ;

Radius ; UDP

Tacacs+ ; TCP

Yönetim kimlik doğrulaması için RADIUS veya TACACS+ kullanılsın , yapılandırmalar kablosuz altyapıdaki benzer AAA yapılandırmalarıdır ve 802.1X/EAP son kullanıcı kimlik doğrulaması için izlenen adımları taklit eder. LDAP'ye karşı kimlik doğrulama için alan adları , gruplar ve nesneler için parametrelerle birlikte temel bir bağlantı yapılandırılır.

Aruba , Cisco , Extreme , Fortinet , Juniper Mist ; TACACS+ , Cisco tescilli protokolü olmasına rağmen , diğer satıcılar bunu lisanslar (CDP gibi) ve ürünlerinde destekler. Eylül 2020 itibariyle IETF , TACACS+'a dayalı resmi RFC'ye sahiptir. Protokolün standart olarak açılmasıyla birlikte , daha fazla ürün TACACS+'ı destekliyor olabilir fakat diğer birçok satıcı zaten bunu lisansladı ve kimlik doğrulama ürünlerine TACACS+ sunucu hizmetleri için destek ekledi. Şimdiye kadar , TACACS+ için RFC'nin , şu anda lisanslı olan özelliklerin birçoğunu çıkarmıştır. Aruba Networks , ClearPass Policy Manager (CPPM) ürününde TACACS+'ı destekler.

Hesap ekibinizle lisans türlerinizi doğrulayınız ; Aruba yıllar içinde lisanslama modellerini değiştirerek tüm lisanslar TACACS+'ı içermese de yeni oluşturulan RFC ile değişebilir. Fortinet FortiAuthenticator , TACACS+ desteği de içeren sağlam kimlik doğrulama ürünüdür. FreeRADIUS artık TACACS+ sunucu hizmetleri için de destek sunuyor. Bulut tarafından yönetilen ürünlere gelince , Extreme , eski şirket içi ürünlerinden RADIUS ve TACACS+'ı , buluttan SAML2 entegrasyonunu destekler. Juniper Mist yalnızca buluttur ve ayrıca SAML'nin yanı sıra Azure ile çoklu oturum açmayı (SSO) destekler.

Yönetim VLAN'ı Oluşturma ; Yönetim VLAN'ları , satıcılar tarafından en iyi uygulama olarak önerilmektedir ve çeşitli siber güvenlik kontrol çerçeveleri tarafından da gereklidir. Yönetim VLAN'ı , altyapı cihazlarının yönetimi için tanımlanan VLAN olabilir veya belirli kablolu uygulamalarda yönetim VLAN'ının atanmasıyla daha resmi uygulama olabilir. Bazı kablolu ürünlerde VLAN'ı resmi olarak " yönetim VLAN'ı " olarak belirlemek , belirli özellikleri ve bu ağ ile ağa erişimi otomatik olarak kilitleyecektir. Altyapının bir kısmının veya tamamının yönetimi için kullanım olarak tanımlanan VLAN , VLAN'ın oluşturulmasını , adlandırılmasını , yönlendiriciler de IP arayüzünün atanmasını ve altyapı cihazlarıyla ilgilenir. ACL'ler için ek kablolu yapılandırmalar , yönetim trafiğini istemci veri trafiğinden ve diğer VLAN'lardan bölümlere ayırmak için kullanılmalıdır. Açıkça büyük ortamlarda , birden çok yönetim VLAN'ı olacaktır. Ortamın ve organizasyonun boyutuna bağlı olarak , çeşitli altyapı aygıtları (anahtarlar , yönlendiriciler , sunucular ve kablosuz denetleyiciler gibi) için tek bir yönetim VLAN'ı kullanılabilir veya kablosuz altyapının kendi yönetim VLAN'larına ihtiyacı olabilir. Bu durumda , bir veya daha fazla AP yönetim VLAN'ı ve şirket içi denetleyicilerin bulunduğu bir veya daha fazla VLAN olabilir. Yönetim VLAN'ları , güvenlik mimarisi için iki temel avantaj sunar ; Bütünlük ve gizlilik için yönetim trafiğinin bölümlere ayrılmasını sunmaktadır. Kullanılabilirlik için yönetim trafiğinin bölümlendirilmesini sunmaktadır. Bütünlük ve gizlilik için bölümlere ayırma , yönetim trafiğinin , yönetim erişimi için yetkilendirilmemiş kullanıcılardan veya cihazlardan gelen gizli dinleme , ekleme veya değişiklikten korunmasına yardımcı olur.

Kullanılabilirlik için segmentlere ayırma , yayın alanlarını azaltma ve yayın fırtınaları (ağ döngüleri aracılığıyla genelde oluşur) , aşırı abone olunan ağ segmentleri (diğer veriler nedeniyle yönetim trafiğinin geciktiği yerlerde) nedeniyle hizmet reddi (DoS) kesintilerinden koruma ek avantajını sunar. Kablosuz altyapı cihazlarınız şu anda yönetim VLAN'ında yapılandırılmamışsa , tüm ortamlarda bunları taşımanız veya diğer cihazları şu anda yapılandırılmış ağlarından taşımanız şiddetle önerilir. Yönetim VLAN'ı ekleyen ortamlar için bu amaçla anahtar satıcısının varsayılan VLAN'ını kullanmamak en iyi uygulamadır. Kenar anahtarlarınız 1 varsayılan VLAN kimliğiyle yapılandırılmış olarak geliyorsa , bunu yönetim VLAN'ı için kullanmayınız. Bunu yaparsanız , kullanılmayan bir bağlantı noktasına bağlanan herhangi bir uç nokta veya kullanıcı en korunan yönetim ağınızda olacaktır.

İzin Verilen Yönetim Ağlarını Tanımlama ; Hem kablolu hem de kablosuz ağ ürünleri , genelde izin verilen yönetim ağlarının özelliklerini destekler. İzin verilen yönetim ağlarının , bir veya daha fazla alt ağ tarafından izin verildiği şekilde tanımlanabilen yönetim trafiği için temel erişim kontrol listesi (ACL) uyguladığı yönetim VLAN'ından küçük bir farklılıktır. Diğer ağlardan alınan yönetim trafiği basitçe yok sayılır. Örnek olarak da birçok kablosuz üründe , kablosuz arabirim aracılığıyla bağlanan istemcilerin yönetimine açıkça izin vermeniz gerekebilir.

Paylaşılan Kimlik Bilgilerinin ve Anahtarların Güvenliğini Sağlama ; Bu konu , paylaşılan kimlik bilgilerini güvence altına almak ve ayrıcalıklı erişimi ele alır. En iyi uygulamalar , kullanıcı tabanlı yönetim oturum açmalarını gerektirse de , hemen hemen her ortamın bazı paylaşılan kimlik bilgileri veya sistem sağlama için gereken yönetici ve kök hesapları gibi kullanıcı tabanlı olmayan hesapları olacaktır. Kullanıcı tabanlı yönetim kimlik doğrulaması yapılandırıldıktan sonra bile , belirli bir miktarda paylaşılan kimlik bilgileri kalarak bunların ele alınması gerekir. Artan güvenlik tehditleri , uzaktan çalışma , sistemlere üçüncü taraf erişimi ve sıfır güven girişimleri çağında , kimlik bilgileri kasası kritik ağ güvenliği aracı olarak merkezi aşamaya geçmektedir. Kimlik bilgileri kasası , kurumsal parola yönetim aracına benzer. Olgun kasalama ürünleri , şu sırları yönetmek için tasarlanmıştır ; Sertifikalar. Sertifika özel anahtarları. SSH anahtarları. API anahtarları. Paylaşılan ve grup parolaları. Hizmet hesabı kimlik bilgileri. Kişi olmayan varlıklar (NPE) için diğer kimlik bilgileri.

Vaulting araçlarıyla sırların yönetimi merkezileştirilir ve bu nedenle kuruluş tarafından kontrol edilebilir , kimlik ve erişim yönetimi (IAM) güvenlik uygulamalarına entegre edilebilir. Bu araçlar kuruluşların NIST ile eşleme gibi güvenlik uyumluluğu gereksinimlerini karşılamalarına yardımcı olur. NIST SP 800-53 revizyon 5'te , kontrol öğesi AC-2 (9) , paylaşılan ve grup kimlik bilgilerinin kısıtlanmasını zorunlu kılarak kontrol öğesi IA-2(5) , " Paylaşılan hesaplar veya kimlik doğrulayıcılar kullanıldığında , paylaşılan hesaplara veya kaynaklara erişim izni vermeden önce kullanıcıların bireysel olarak kimliklerinin doğrulanmasını gerektirir. ". " AC " kontrolleri Erişim Kontrolü , " IA " kontrolleri ise Tanımlama ve Kimlik Doğrulamadır. Kimlik bilgileri kasası çözümleri tam da bunu ve daha fazlasını yapar. Kuruluşumuzun kullanıcı tabanlı yönetim kimlik doğrulamasına sahip olduğu ancak bir nedenden dolayı RADIUS sunucusuna erişilemediği ve sistemin yerel kimlik doğrulamaya geri dönmesi gereken senaryo olduğunu varsayarsak ; doğrudan yönetici kullanıcısıyla ve ilişkili parolayla

oturum açmak yerine , terminal uygulaması kimlik bilgileri kasası aracına bağlanılır. Çoğu kasa ürünü , gelişmiş kimlik bilgileri yaşam döngüsü yönetimine sahiptir ve kimlik bilgilerini önceden tanımlanmış programa göre güncelleyebilir ve döndürebilir. Kuruluş her 90 günde bir SSH anahtarlarını veya API anahtarlarını değiştirirse , kasaya alma aracı bu işlemleri otomatikleştirebilir veya etki alanındaki hizmet hesabının parolasını güncelleyebilir. BT yöneticileri ve mimarları genelde gereğinden fazla genişler ve günlük olarak problemleri çözerler. Bu günlük mücadelede , hassas kimlik bilgilerinin güvenli olmayan şekilde oluşturulması ve saklanması yaygındır. Sadece çok büyük veya çok düzenlemeye tabi şirketler uygun kimlik yönetimine sahip olma eğilimindedir. Kuruluşunuzun şu anda kimlik bilgileri kasası çözümü yoksa , bunun için bütçe ayırması için başvuruda bulunabilirsiniz. Bütünsel güvenlik stratejisi için kritik bir bileşendir ve çok uygun fiyatlı ürünler ile muhtemelen bazı ücretsiz ile açık kaynak seçenekleri vardır. Bağlam açısından , popüler kimlik bilgisi kasası uygulamaları arasında Azure Key Vault , Amazon AWS Key Management , Beyond Trust'ın ürünleri gibi ürünler bulunur ve bunların tümü yalnızca SSH anahtarlarını depolamak için değil , aynı zamanda depolamak için de kullanılabilir.

SSH Anahtar Yönetimi ; SSH anahtarları dikkatli şekilde yönetilmeli ve BT yöneticilerinin bilgisayarlarında ister istemez oluşturulup kaydedilmemelidir. Tek başına kimlik bilgisi olarak kullanıldığında , SSH anahtarları gerçekten iyi anahtarlarıdır ve bu şekilde korunmalıdır. Olgun ve güvenlik bilincine sahip kuruluşlar , SSH anahtarı yaşam döngüsü ve kullanımları , ara sıra keşif ve tarama dahil olmak üzere SSH anahtarlarının envanterini , SSH anahtarını döndürme , anahtar kasası oluşturma , emanete alma , SSH sürümlerinin ve anahtarın doğrulanması için politikaları içeren SSH anahtar yönetim programına sahip olmalıdır. Ulusal Bilim ve Teknoloji Enstitüsü (NIST) , şu web sitesinde bulunan kurumlar arası raporu 7966'da (NISTIR 7966) SSH erişim yönetimi için derinlemesine rehberlik sağlar.

Ayrıcalıklı Erişime Yönelik ; Ayrıcalıklı hesaplar , yükseltilmiş ayrıcalıklara veya standart kullanıcının yetkilendirildiğinin üzerinde ve ötesinde erişime sahip hesaplar olarak tanımlanır. Geleneksel olarak , ayrıcalıklı hesapların yönetimi , belirli veri kümelerine veya uygulamalara (sağlık kayıtları , mali kayıtlar , kişisel olarak tanımlanabilir bilgiler (PII) gibi düzenlenmiş kayıtları içerenlere) erişen kullanıcılar ve hizmetler için erişim haklarına odaklanmıştır. Uzaktan erişim , bulut tarafından yönetilen hizmetler (SaaS , PaaS , IaaS teklifleri dahil) ve artan güvenlik tehditleri , altyapı bileşenleri için yönetici hesaplarının kontrolünü içerecektir. Kuruluşun kimlik ve erişim yönetimi (IAM) veya güvenlik uyum ekipleri tarafından yürütülen girişim olduğunu anlayarak ayrıcalıklı erişimin önemli noktaları vardır. Ağ ve sistem yöneticileri için alakalı ve güncel konudur ve mimari stratejiniz , altyapıya yönetici erişimini güvence altına almak için süreçleri ve araçları içermelidir.

Ayrıcalıklı Hesapların ve Kimlik Bilgilerinin Güvenliğini Sağlama ; Ayrıcalıklı hesapların yanı sıra hizmetler , uygulamalar ve mikro hizmetler tarafından kullanılan API anahtarları ve belirteçlerin yanı sıra SSH anahtarlarını içerebilen ayrıcalıklı kimlik bilgileri bulunmaktadır. Bir kişiden ziyade bir şeye yetki vermek , zorluklar ortaya çıkararak birçok eski kimlik doğrulama modelini (donanım belirteçleri gibi) bozar. Kullanım durumlarındaki bu değişimleri desteklemek için düzenlemeler , endüstrinin şu anda şahıs olmayan varlıklar (NPE) olarak adlandırdığı şey tarafından erişim güvenliğini ele almaya başlıyor. Kişi olmayan varlıklar konusu , robotik süreç otomasyonunun (RPA) yanı sıra konteynerler ve mikro hizmetler gibi iş yüklerinin güvenliği tartışılırken en yaygın olanıdır fakat API'lerin kullanımı daha yaygın hale geldikçe altyapıya da yayılmaktadır. Uyumluluk ve güvenlik politikası için tanımlanan ayrıcalıklı hesaplara ve ayrıcalıklı kimlik bilgilerine örnekler ; Yerel ana bilgisayar yönetici hesapları. Süper kullanıcı hesapları (kablosuz erişime yönetim erişimi dahil). Etki alanı yönetici hesapları. Ayrıcalıklı iş kullanıcısı. SSH anahtarları , API anahtarları ve diğer sırlar. Hizmet ve uygulama hesapları. Acil durum hesapları.

Gerekmedikçe karmaşıklık eklemek asla mantıklı değildir fakat ayrıcalıklı hesapları korumak , hesabın kötüye kullanılması ve kimlik bilgilerinin kaybolması , çalınması nedeniyle ağ güvenliği mimarisinin ana teması olarak ortaya çıkacaktır. Ayrıcalıklı hesap yönetimi , güvenlik ihlallerinde ve olaylarda o kadar baskın bir faktördür ki , Verizon'un Veri İhlal Araştırmaları Raporu (DBIR) artık raporda kendi risk sınıflandırması olarak ayrıcalıklı erişimi içermektedir.

Ayrıcalıklı Erişim Yönetimi ; Ayrıcalıklı erişimi yönetme uygulamasına ayrıcalıklı erişim yönetimi (PAM) denir ve kurumsal politikalar , süreçler ve araçlar veya uygulamalar şeklinde gelir. PAM yalnızca en iyi uygulama değildir. Sarbanes-Oxley (SOX) , Federal ve Kuzey Amerika Enerji Düzenleme Komisyonu (FERC / NERC) , HIPAA ve eyalet düzeyindeki düzenlemeler dahil olmak üzere çoğu düzenlemede özel olarak zorunlu denetim olarak adlandırılır. Kaliforniya Bilgi Uygulama Yasası gibidir. AB'nin Genel Veri Koruma Yönetmeliği'nde (GDPR) ana hatlarıyla belirtilenler gibi veri gizliliğine yönelik uluslararası düzenlemeler , PAM'yi özel olarak zorunlu kılmayabilir fakat kuruluşun verileri nasıl topladığını ve sakladığını , buna kimin erişimi olduğunu değerlendirmesini şart koşar. Ayrıcalıklı erişim yönetimi süreçleri ve araçları şunları içerir ; Ayrıcalıklı hesap ve kimlik bilgileri kasası. Erişimin izlenmesi ve uyarılması. Erişim ve hesapların düzenli denetimi. Ayrıcalıklı hesap yaşam döngüsü yönetimi. Uygun parola / parola güvenliği. En az ayrıcalık ilkesinin uygulanması.

Ayrıcalıklı Uzaktan Erişim (PRA) ; Ayrıcalıklı uzaktan erişim , korumalı sistemlere İnternetten veya diğer güvenilmeyen ağlar üzerinden erişmenin benzersiz yönlerini ele almak için tasarlanmış ayrıcalıklı erişim yönetiminin alt kümesidir. Yerinde olsalar bile , çalışanların ve üçüncü tarafların erişimini yönetmek için kullanılabilir. PAM gibi ayrıcalıklı uzaktan erişim de politikalar , süreçler ve araçlar gerektirir fakat uzaktan erişim araçları genellikle standart PAM araçlarından farklıdır yani bu amaç için kullanılan ayrı ürün olabilir. İleriye doğru ayrıcalıklı uzaktan erişime büyük ölçüde güvenecek ağ mimarları , mühendisler ve sistem yöneticileri dahildir. Sıfır güven stratejilerinin gün yüzüne çıkması ve giderek daha fazla kullanıcının sistemlere uzaktan erişmesiyle , eski VPN erişiminin olduğu günler , kullanıcıların internete düştüğü günlerdi. Ayrıcalıklı uzaktan erişim ürünlerine ilişkin özellikler değişiklik gösterir fakat PAM'ın faydalarına ek olarak , amaca yönelik uzaktan erişim aşağıdakileri de ele alır. Denetim amacıyla ayrıntılı değişiklik günlüklerinin tutulması da önemlidir. Çeşitli konsolları ve uygulamaları desteklemektedir (web kullanıcı arayüzü veya SSH erişimi için). Etki alanı dışındaki kullanıcılar (satıcıların sistemleri ve destek mühendisleri gibi) dahil olmak üzere üçüncü tarafların erişimini kolaylaştırmaktadır. Çok faktörlü kimlik doğrulamayı zorlamaktadır.

PAM VE PRA ; Popüler satıcılardan bazıları Beyond TrusT , CyberArk , Thycotic'dır. Her ürün çözümünün kendi işleyişi ve farklı tür ile büyüklükteki kuruluşlara uyan farklı teklifleri vardır ve ürünler şirket içi , bulut veya her ikisini birden içerebilir. Ağ mühendisi olarak , Beyond Trust'ın , kendi yerel aracınızı (PUTTY gibi) kullanarak uzak cihazlara güvenli şekilde SSH'yi proksi terminali aracılığıyla zorlamak gibi bazı özellikle zorlayıcı özelliklere sahip olduğunu söyleyebiliriz. Üçüncü tarafların kendi masaüstünüzü paylaşmak zorunda kalmadan bir oturuma katılmasına izin verilmesini de destekler. Satıcının TAC mühendisinden uzaktan devreye girip yardım etmesini istediğinizde olmazsa olmazdır. Üçüncü taraf varsa , bunu ön onay veya isteğe bağlı istek / onay yoluyla sizle veya siz olmadan yapabilirler. Herhangi bir değişikliği görüntülemek , yeniden oynatmak veya denetlemek için sistemin tüm oturumu otomatik olarak kaydetmesini sağlayabilirsiniz. Aynı derecede önemli olan SSH ve API anahtarlarının güvenliğini de içeren kimlik bilgisi kasası oluşturma , güvenli erişim yönetimi tam paketini destekler. Diğer ürünler muhtemelen benzer özelliklere sahiptir. PAM veya PRA istiyorsanız IAM'nizle neyin entegre olduğunu ve ihtiyaçlarınıza en iyi şekilde hizmet ettiğini görmek için birkaç seçeneği test ediniz.

Ek Güvenli Yönetim Hususları ; Kendi bölümlerini garanti etmeyen ancak güvenlik mimarinizde bahsetmeye ve dikkate almaya değer birkaç yan konu bulunmaktadır.

Güvenli Parolaları Zorlayınız ; Kriptografik saldırılara dayanıklı güçlü parolaları zorunlu kılmak için kuruluşun kılavuzunu izleyiniz. Parola uzunluğu en önemli faktördür ve karmaşıklık ikinci faktördür. TACACS+ , RADIUS veya LDAP aracılığıyla yapılanlar gibi dizin tabanlı kullanıcı oturumlarının yanı sıra yerel yönetim hesaplarına parola güvenliği uygulanmalıdır.

Sistem Oturum Açma Başlıkları ; Oturum açma başlıkları , altyapının yönetici erişimi gibi kısıtlı sistemde oturum açmaya çalışmadan önce kullanıcıyı uyarır. Oturum açma banner'larının yasal sonuçları vardır ve çoğu sağlamlaştırma kılavuzunda en iyi uygulama olarak önerilir. Oturum açma başlığı , yetkisiz

kullanıcıyı sisteme erişme girişimleri hakkında uyaran uygun dil içermelidir. Bazı satıcıların özelliklerinin , etkinleştirildiğinde oturum açma başlıklarının kullanımını desteklemediğini belirtmekte fayda vardır ve bu nedenle lütfen ürün belgelerinize bakın.

Eşzamanlı Yönetim Oturumlarını Sınırlayın ve Zaman Aşımlarını Ayarlayın ; Ağ cihazları , çoğu zaman , birden fazla sayıda oturum açma arasında değişen yapılandırma seçeneklerini destekleyen birçok ürünle , terminal VTY (sanal terminal) ayarları aracılığıyla maksimum sayıda eşzamanlı yönetici oturumunun yapılandırılmasına izin verir. En iyi uygulama , sadece yöneticileri değil , SSH kullanıyor olabilecek güvenlik , yönetim ve izleme sistemlerini de hesaba katarak eşzamanlı yönetici oturumları için makul maksimum değer yapılandırmaktır. Maksimum oturumların yanı sıra , sisteme tüm yönetici erişimleri için yapılandırılmış zaman aşımları olmalıdır.

Çok Faktörlü Kimlik Doğrulama (MFA) ; Çoğu uyumluluk düzenlemesi , sistemlerin idari erişiminde MFA'yı etkinleştirmek için gereksinimleri tanımlasa da , doğrudan kontrol olarak hala nispeten nadirdir. Nasıl uygulandığına bakılmaksızın , yerel veya uzak tüm yönetim erişimi için MFA şiddetle önerilir. Bulut çözümlerine (Juniper Mist , Meraki , ExtremeCloud , Aruba Central gibi bulut tarafından yönetilen ağ iletişimi gibi) uzaktan erişim ve yönetim erişimi için bunu çok önemli bir gereklilik olarak düşününüz.

Yönetimsel Erişim ve Girişimlerin Günlüğe Kaydedilmesi ve İzlenmesi ; Kablosuz altyapı ve yönetim dahil olmak üzere sistemlere yönetim erişimi günlüğe kaydedilmeli ve uygun şekilde izlenmelidir. Bu tür günlüğe kaydetme ve uyarı , çoğu güvenlik yönetmeliğinde gereklilik olarak belirtilmiştir. Mimari planlamanızın bir parçası olarak, yönetici oturum açma parolası yeniden denemelerinin izlenmesini dahil ediniz. Saldırganlar , bir operatörü kötü niyetli kullanıcıya numara taşıması ve metin mesajlarına erişmesi için kandırmak için SIM takas tekniklerini kullanabilir.

Altyapının Bütünlüğü İçin Tasarım ; Altyapının kendi kendine kimliğini doğrulamayı , yazılım ve konfigürasyonların bütünlüğünü sağlamayı , güvenli yedeklemeleri ele almayı , altyapı bileşenlerini fiziksel olarak güvenceye almayı ve kullanılmayan protokolleri azaltmay içerir.

Altyapı bütünlüğü şu başlıklar halinde düzenlenmiştir ; Yapılandırmalar. Değişiklik Yönetimi ve Yedeklemeleri Yönetme. Günlüğe Kaydetme , Raporlama ve Uyarıları Yapılandırma. Yükseltmeler ve Yamalar için Yazılım Bütünlüğünü Doğrulama. 802.11w Korumalı Yönetim Çerçeveleriyle Çalışma. AP'leri Yöneticiye Sağlama ve Güvence Altına Alma. Kablolu Altyapı Bütünlüğü Ekleme. Fiziksel Güvenliği Planlama. Kullanılmayan Protokolleri Devre Dışı Bırakma.

Yapılandırmaları , Değişiklik Yönetimini ve Yedeklemeleri Yönetme ; Konfigürasyon yönetimi ne yazık ki çoğu zaman göz ardı edilir fakat altyapı bütünlüğünün önemli bir unsuru olmaya devam etmektedir. Birçok ağ yöneticisi için yaygın uygulama ; planlanmış yükseltmeden önce iyi bilinen yapılandırmayı kaydetmektir fakat yapılandırmaların yönetimi , değişiklik yönetimi , temeller ve yedeklemelerle ilgili politikalar , süreçler ve etkinlikler çoğu durumda yok sayılır. Sektörde çalışıyorsanız veya NIST standartlarına uyuyorsanız , kuruluşunuzun muhtemelen sağlam yapılandırma yönetimi programı vardır. Henüz tam olarak orada değilseniz , güvenlik mimarinize dahil etmeniz gereken birkaç önemli öğeyi burada bulabilirsiniz.

Yapılandırma Değişikliği Yönetimi ; Değişiklik kontrol süreçleri , konfigürasyon bakımının yaşam döngüsünü ele alarak çok çeşitlidir. Küçük veya düzenlemeye tabi olmayan ortamlarda , değişiklik yönetimi süreci belgelenmemiş olabilir ve yöneticiden bir yöneticiye basit bildirim veya bakım aralığı talebi yeterlidir. Büyük ve düzenlenmiş ortamlar , şunlardan bazılarını veya tümünü içeren değişiklik yönetimini katı şekilde uygulamakla yükümlüdür ; Bir konfigürasyon değişikliği uygulamak için resmi istek. İş etkisi , teknik etki ve güvenlik riski açısından değişikliğin analizi ve derecelendirilmesi. Kontrollü test veya laboratuvar ortamında planlanan değişikliğin test edilmesi ve doğrulanması. Bir değişiklik yönetim kurulu veya onay komitesi tarafından gözden geçirme. Öncesi , sırası ve sonrası bildirimler dahil olmak üzere değişikliğin uygulanması . Üretim ortamındaki değişikliğin test edilmesi ve doğrulanması. Geri alma prosedürleri de dahil olmak üzere her adımda ayrıntılı belgeler ve onaylar.

Daha geçici şekilde çalışan profesyoneller için sadece yapılandırma değişikliği planlamanın ötesinde görevleri dahil etmeleri önerilir. Bu adımlar , olgun değişim yönetimine sahip olmayan kuruluşlar için uygun olan minimum bir yapı ve dokümantasyon sağlar ;

1. Planlanan değişikliği belgeleyin ; Değişikliğin nedenini ve beklenen sonuçları , çözülmesi veya izlenmesi gereken bilinen sorunları yakalayınız. Yapılandırma doğrulamasını gerçekleştirmek için yapılan testleri ve güvenlik kontrollerini doğrulamak için gereken ek testleri belgeleyin. İdeal olarak , web kullanıcı arayüzü , SSH ve değişiklikle ilişkili komutlar veya adımlar aracılığıyla değişikliğin nasıl uygulanması gerektiğini ve gerekirse geri alma adımlarını belgeleyin. Kuruluşun varlık ve konfigürasyon yönetimi için bir platformu yoksa ancak dahili biletleme sistemi varsa bunu kullanınız. En azından bu bilgilerle metin dosyası veya belge oluşturun ve güvenli , paylaşılan bir depolama alanında bir dosya başlatın.

2. Planlanan değişikliği en az bir teknik eş veya yönetici ile gözden geçirin. Kuruluşunuzun değişiklik yönetimi incelemeleri ve onayları için resmi süreçleri olup olmadığını sağlık kontrolü olarak , planlanan değişikliği en az bir teknik meslektaşla veya doğrudan yöneticinizle gözden geçirin.

3. İsteğe bağlı olarak test veya laboratuvar ortamında planlanan değişikliği doğrulayınız. Çeşitli nedenlerle şiddetle tavsiye edilir fakat bazı kuruluşların test veya laboratuvar ortamlarına erişimi yoktur. Bulunduğunuz ortamın plansız kesintilere karşı toleransı düşükse , laboratuvar ekipmanı , uygun olduğunda sanal cihazlar için talepte bulunmak muhtemelen zaman ve çabaya değer.

4. Değişiklik penceresini planlayın ve belgeleyiniz ; Devam etmeden önce , mevcut yapılandırmayı güvenli şirket tarafından yönetilen depolama konumuna yedekleyiniz. Değişikliğin gerçekleşmesi için bakım penceresini planlayın ve değişikliklerin ne zaman yapıldığı veya sisteme taahhüt edildiği tarih ve zaman damgaları dahil olmak üzere faaliyetleri belgeleyiniz. Yükseltme veya yapılandırma değişikliğinden sonra bir sorun olursa , daha sonraki sorun giderme ve teknik destek için son derece yararlıdır.

5. Üretimdeki değişikliği test edin ve doğrulayınız ; Çoğu değişiklik için üretimde test etme ve doğrulama iki aşamalı bir görevdir. İlk olarak , değişiklik anında anında test gerçekleştirilir ve daha sonra , sistem tam yük altındayken çalışmayı doğrulamak için çoğu zaman bir pencere tanımlanır.

Gerçek dünya senaryosu kullanılarak açıklanan süreç şöyledir ; Kablosuz mimar , daha güvenli WPA3-Yalnızca Kişisel güvenlik modunu kullanmak için mevcut WPA2-Kişisel SSID'yi değiştirmeyi planlamaktadır. Radyo düğmesi kullanılarak SSID'ler için şablonun altındaki web kullanıcı arayüzünde gerçekleştirilir. Bilinen sorun ise WPA3-Personal'ı destekleyecek şekilde güncellenmeyen uç noktaların bağlanamamasıdır. Kuruluş bunun farkındadır , çevreyi izlemiştir ve ilerlemeye hazırdır. Değişiklikten sonraki test , bağlanabildiğinden emin olmak için WPA3-Kişisel özellikli istemcinin SSID'ye bağlanmasını ve yalnızca WPA2-Bireysel özellikli cihaza bağlanmaya çalışılmasını ve bağlanamadığını doğrulamayı içerir , bu da yapılandırmanın çalıştığını kanıtlar. Mimar , ağ operasyon ekibi , yardım masası ekibi ve yöneticisi ile planlanan değişiklikleri gözden geçirerek bakım penceresi üzerinde anlaşmaya varır. Mimar , üretim denetleyicileriyle aynı kodu çalıştıran küçük fiziksel denetleyici kullanarak süreci laboratuvarda test eder. Hem WPA2-Kişisel hem de WPA3-Kişisel istemci test edilir ve sonuçlar tanımlanan beklenen sonuçlarla eşleşir. Mimar , planlı bakım penceresi sırasında değişikliği yaparak değişikliğin tarih ve saatini belgeler , aynı müşteri testlerini üretim ortamında tekrarlar ve değişikliğin doğru çalıştığını onaylar. Ertesi gün , ağ operasyonları ekibi , güncellenen WPA3-Kişisel ağdaki başarısız bağlantı istekleri ve bağlanamayan WPA2-Kişisel cihazlara sahip kullanıcılardan gelen yardım masası alanları çağrıları için ortamı izler.

Olası gerçek dünya senaryosu olmasına rağmen , bu örnek büyük ölçüde basitleştirilmiştir ve birçok değişiklik yönetimi görevi birden çok değişiklik , birden çok test dizisi içerir ve satıcı hatası gibi bilinmeyen veyahut istenmeyen sonuçlara yol açabilir.

Değişim yönetimi için olgun süreçlerin yokluğunda , en iyi uygulama , burada açıklanan durum tespiti görevlerini dahil etmek , her şeyin iyi belgelendiğinden emin olmak ve sürece en az bir diğer tarafı veya kişiyi dahil etmektir.

NIST SP 800-53'de Değişiklik Yönetimi ; NIST Özel Yayını 800-53 Bilgi Sistemleri ve Kuruluşları için Güvenlik ve Gizlilik Kontrolleri , diğer birçok uyumluluk çerçevesi ve düzenlemesi tarafından referans alınan kapsamlı çerçevedir. Konfigürasyon Yönetimi (CM) paketindeki temel yapılandırmalar ve kontrol değişiklik süreçleri dahil olmak üzere değişiklik yönetimi için ayrıntılı rehberlik içerir. Spesifik olarak , revizyon 5'te bunlar , CM-1 İlke ve Prosedürler , CM-2 Temel Konfigürasyon , CM-3 Konfigürasyon Değişiklik Kontrolü bölümlerinde ele alınmaktadır. Etki analizi , izleme ve diğer ilgili görevler için ek destekleyici kılavuz sağlanır.

Yapılandırma Temelleri ; Büyük ve karmaşık ortamlar , kuruluşun iş ve güvenlik gereksinimlerini karşılayan yapılandırmalar için onaylanmış şablon görevi gören temel yapılandırmaların oluşturulması ve yönetimine ilişkin süreçlere ve uygulamalara sahip olmalıdır. Temel yapılandırmalar , belirli bir türdeki sistemlerin uygulanması için kuruluş onaylı durumu tanımlar. Her yerinde yüzlerce lokasyona ve yerel kablosuz altyapıya sahip şirket , her birinde güvenli kablosuz dağıtmak için standart yapılandırma temeli oluşturacaktır. Taban çizgileri , spesifikasyonları olan ayrıntılı belgeler veya iyi belgelenmiş yapılandırma dosyası şablonları veya komut dosyaları olabilir. Konum veya coğrafya türüne bağlı olarak yapılandırma temel çizgileri ve öğeler içinde değişkenler de olabilir. Küçük ortamlar , resmi yapılandırma temellerine sahip olmayabilir çünkü bunları belgeleme süresi elde edilen değer için gerçekçi olmayabilir ve elbette birçok ortamda sadece sınırlı kablosuz altyapı olabilir. Bununla birlikte , bazı sektörlerdeki küçük kuruluşlar ve NIST veya ISO standartlarına göre belirli yönergeleri karşılaması gereken kuruluşlar için onaylanmış bir güvenli yapılandırma temel çizgisini belgeleme zorunluluğu olabilir.

Yapılandırma Yedeklemeleri ve Geri Alma Desteği ; Konfigürasyon yönetimi , konfigürasyon yedeklerinin onaylanmış bir yerde tutulmasını ve uygun şekilde güvenliğini sağlamayı kapsar. Kuruluşun boyutu ne olursa olsun , onaylanmış konum kablosuz yöneticinin dizüstü bilgisayarı değildir. Onaylı yedekleme konumu , diğer yetkili yöneticiler veya sistemler tarafından erişilebilen , belirlenmi ş, güvenli havuz olmalıdır. Depo ağ yönetim aracı (Cisco Prime , Cisco DNA Center , HPE Intelligent Management Center , HPE OneView , SolarWinds , Aruba Fabric Composer vb.) olabilir veya bulutta ve ağ depolamasında belirlenmiş bir yer olabilir. Yedekler otomatik bir programda (SCP veya SFTP kullanılarak) güvenli dosya aktarımı yoluyla gönderilebilir. İdeal olarak , konfigürasyon yedekleme yönetimi , kablosuz altyapının konfigürasyon yedeklemesini otomatikleştirmeyi destekleyen bir platform , noktaları veya değişiklikleri not etmek için konfigürasyon dosyalarına açıklama eklemek için ek işlevsellik , vurgulamak için fark gerçekleştirmek için araç veya iki konfigürasyon dosyasını karşılaştırmak için araç içerir. Değişiklikler , planlanmamış yapılandırma değişikliklerinde uyarı verme yöntemleri ve güvenlik yapılandırmalarını onaylanmış temel değerlere göre doğrulamaya yönelik araçlardır. Yedeklemeler , bulut havuzuna ikinci eşitleme ile şirket içi gibi veyahut coğrafi olarak farklı iki veri merkezinde katmanlandırılmalı ve depolanmalıdır. Geri alma desteği başka bir husustur ve yedekleme planı , geri alma gerektiğinde uygun sayıda önceki revizyona ve bir geri yükleme için destek alımına izin vermelidir.

Yetkisiz Değişiklikleri İzleme ve Uyarı Verme ; Sistem konfigürasyonundaki değişiklikler izlenmeli ve uyarılmalıdır. Destekleniyorsa sistemin kendi içinde veya SIEM veya günlük sunucusuna syslog veya SNMP tuzakları aracılığıyla veya daha önce açıklanan ağ yönetimi ürünleri aracılığıyla uygulanabilir.

Günlüğe Kaydetme , Raporlama , Uyarı ve Otomatik Yanıtları Yapılandırma ; Altyapının sağlamlaştırılması , güvenlik kontrollerini atlama veya ihlal etme girişimlerinin izlenmesini ve uyarılmasını gerektirir. Kablosuz için uygun izleme ve uyarı , yalnızca yönetim erişimini değil , aynı zamanda istemci erişimini ve veri güvenliğini de kapsar. Sağlamlaştırma bağlamında ; günlüğe kaydetme , raporlama ve uyarı şunları tanımlayacak şekilde tasarlanmalıdır ; Yetkisiz yapılandırma değişiklikleri. Karıştırma dahil kablosuz (RF) ortama yapılan saldırılar. Sahtekarlık ve DoS saldırıları dahil kablosuz veri altyapısına yönelik saldırılar. Kablosuz ağdan başlatılan kablolu ağa saldırılar. Yönetici oturum açma girişimleri (başarısız ve başarılı) ve kullanım günlüğü. Hileli ve yetkisiz cihazlar (uç noktalar ve altyapı). Anormal davranış.

NIST SP 800-53 ile uyumlu kuruluşlar için izleme ve bakımla ilgili gelecek bölüme ek olarak , izleme hakkında daha fazla bilgi için Sistem ve Bilgi Bütünlüğü (SI) konu alanındaki kontrol kılavuzuna bakınız.

Yükseltmeler ve Yamalar için Yazılım Bütünlüğünü Doğrulama ; Kablosuz altyapıyı güvenli tutmak , yazılım bütünlüğünü doğrulamak için düzenli güvenlik düzeltme eki ve isteğe bağlı adımlar gerektirir.

Yazılım Bütünlüğünü Doğrulama ; Bugünlerde her şey birbirine bu kadar bağlıyken ve yığınla internet kaynakları , bilgi tabanları , bloglar , makaleler ve dosya depolarıyla birlikte , yazılım bütünlüğünü doğrulamak , üzerinde düşünülmeye değer fazladan adımdır. Dosya veya kod bütünlüğü denetimi ile kodu oluşturan kişi (kablosuz satıcı gibi) standart hash algoritma kullanarak dosyadan ayrı olarak hash çıktısını sağlayacaktır. Bu dosyayı indirdiğinizde , içeriğin değişmediğini doğrulamak için aynı hash algoritmayı kullanarak dosyanın değiştirilmediğini (kötü amaçlı kurcalama veya yanlışlıkla bozulma yoluyla) doğrulayabilirsiniz.

Hash Fonksiyonları ; Hash işlevlerine aşina değilseniz , girdi alan ve onu sabit uzunluklu alfasayısal değere indirgeyen işlev gerçekleştiren tek yönlü algoritmalardır. Hash'ler kriptografik fonksiyon olarak kabul edilir fakat iki yönlü şifreleme algoritmalarından farklı olarak , hash'i tersine çevirmeye gerek ve hiçbir yöntem yoktur. Dolayısıyla tek yönlü tanımlayıcıdır. Popüler hash algoritmalar arasında MD5 , SHA-1 ve SHA-256 bulunur. Hash'lere ilişkin fikir edinmek için ham metin veya dosyaların hash işlevlerini gerçekleştiren çevrimiçi araçlar için hash oluşturucu veya sha1 oluşturucu araması yapabilirsiniz. Aynı işlevleri gerçekleştiren Windows da dahil olmak üzere işletim sistemlerinde yerleşik araçlar da vardır.

Kablosuz Satıcı Dosyaları Doğrulama ; Belirli talimatlar için satıcınıza danışınız. Cisco'dan "İndirilen Dosyanın Bütünlüğünü Doğrulama" başlıklı Cisco belge kimliği 211350 , depolama ürünlerinden biri için bir SSS'de bununla ilgili talimatları içerir. Cisco DNA Center altında " Bütünlük Doğrulaması "nı da arayabilirsiniz. Aruba Networks ve diğer satıcılar , uygun olduğunda benzer kılavuzlara sahiptir. Bulut tabanlı yönetim çözümleri , satıcı tarafından yönetilen ve sürdürülen yazılım platformlarına veya mikro hizmetlere sahiptir. Bu nedenle , kuruluşun yazılım indirmeye ve yüklemeye ihtiyacı olmayacak , dolayısıyla bütünlük kontrollerinin bu özel kullanım durumuna gerek kalmayacak. Satıcı , bu kontrolleri kendi bulut yönetimi ve AP ekosistemi içinde gerçekleştirecektir.

Yükseltmeler ve Güvenlik Yamaları ; Geleneksel şirket içi kablosuz denetleyicileri yükseltmenin sancılı deneyim olduğu belirtilmişti. Konu , yanlış giden yükseltmelerle ilgili Wi-Fi uzmanlarının , denetleyici yükseltmelerinin yalnızca kesinlikle gerekli görüldüğünde (genellikle kod yükseltmesi veya yama gerektiren kullanıcıyı etkileyen sorun olduğunda) gerçekleştirildiği konusundaki genel duyarlılığını içeriyordu. Sistemleri güncel tutmak ve yamaları güvenli altyapıyı sürdürmek için kesinlikle çok önemlidir. Bunun istisnası yoktur. Mükemmel bir dünyada , ağ operasyonları ve güvenlik operasyonları bir araya gelerek güvenlik operasyonları merkezindeki (SOC) yeni bulunan arkadaşlarınız , yamalar gerektiğinde tarama ve uyarı da dahil olmak üzere güvenlik açığı yönetim programının bölümlerinden sorumlu olacaktır. Yükseltmeyi planlamanız ve gerçekleştirmeniz gerekeceği gerçeğini ortadan kaldırmaz fakat güvenlik nedeniyle gerçekten gerekli olan güncellemelere odaklanmanıza yardımcı olabilir. Çoğu kuruluşta , ağ yöneticileri birçok şapka takıyor ve yönettikleri her sistem için her kod sürümünün her satırını okumaları ve yükseltmeler , yamalar hakkında kararlar almaları mantıksızdır. Bir yama bir sorunu çözebilir fakat tüm düzeltmeler ve özellikler her ortamda kullanımda değildir. Tüm bunları bilmek ve bunun getirdiği yükü anlamak , güvenlik yamalarına yönelik düzenli güncellemelerden kaçınılması gereken bir şey değildir. Bunu mimari planlamanıza dahil ediniz. Güncellemelerin iş yükünü gerçekten sürdüremiyorsanız , bu iş yükünün çoğunu hafifletecek bulut tarafından yönetilen platform için seçenekleri tartışın veya liderliğinize ek personel veyahut kaynak ekleme veya yönetilen hizmet kullanma konusunda yaklaşınız. Güvenlik düzeltme ekinin nasıl gerçekleştiği önemli değil , sadece yapılması gerekiyor.

802.11w Korumalı Yönetim Çerçeveleriyle Çalışma ; 802.11 WLAN'larda yönetim çerçeveleri , kontrol çerçeveleri ve veri çerçeveleri vardır. Veri çerçeveleri , istemci verilerini içerir ve kimliği doğrulanmış istemci ile SSID güvenlik profilinde tanımlandığı gibi şifrelenir. 802.11 WLAN'ların on yıllarında , yönetim çerçevelerinin hiçbir bütünlük biçimi yoktu. Ne kimlikleri doğrulandı ne de şifrelendiler. Korumasız yönetim çerçevelerinin sonucu çok yönlüdür. Yönetilen kurumsal uç noktanın sahte AP'ye bağlanmasını önlemek için kimlik sahtekarlığı yapan kurumsal Wi-Fi sistemi gibi güvenlikle ilgili belirli özellikler sunmak için bu boşluktan yararlanan sayısız meşru kablosuz işlem vardır. Birçok geleneksel kablosuz IPS (WIPS) işlevi , korumasız yönetim çerçevelerinden yararlanmıştır. Tabii ki daha büyük endişe kaynağı , açıkta kalan yönetim çerçevesi modelinin kablosuz altyapıyı bir dizi kötü niyetli saldırı , kötüye kullanım ve kötüye kullanıma karşı savunmasız bıraktığı gerçeğidir. Bu boşluğu gidermek ve kablosuz altyapının kablosuz altyapısının bütünlüğünü desteklemek için 802.11 standardı , ek korumalar içerecek şekilde güncellenmiştir. PMF için 802.11w standardının altyapı bütünlüğünde (AP sahtekarlığını önleme dahil) rol oynayan bileşenleri vardır. Cisco'nun 802.11w PMF'den farklı olan ve altyapı güvenliği için tasarlanmış paket olan Infrastructure PMF adlı tescilli özelliği de vardır. Yönetim Çerçevesi Koruması için IEEE 802.11w standardı (diğer adıyla PMF veya MFP) 2009'dan beri mevcuttur ve desteklenmektedir fakat şimdi yalnızca yeni WPA3 güvenlik standartları paketinin bir parçası olarak gereklidir. WPA3'ü (WPA2'ye karşı) tanımlayan korumalı yönetim çerçevelerinin kullanımıdır. Yönetim çerçevelerinin sahteciliğini önleyiniz (SA sorgusu aracılığıyla). AP'nin veya uç noktanın sahteciliğini önleyiniz. Tekrar saldırılarını önleyin,z. Belirli yönetim çerçevelerinin gizlice dinlenmesini engelleyiniz.

Wi-Fi Yönetim Çerçeveleri ; Wi-Fi yönetim çerçeveleri , ağları bulmak , birleştirmek ve ağlardan ayrılmak için AP'ler ve uç noktalar arasında kullanılır ve şunları içerir ; İşaretler ve araştırma istekleri ve yanıtları. İlişkilendirme ve yeniden ilişkilendirme istekleri ve yanıtları. Ayrılma bildirimleri ve istekleri. 802.11 kimlik doğrulaması ve kimlik doğrulamasının kaldırılması. Burada atıfta bulunulan 802.11 kimlik doğrulamasının tüm uç noktaların bir ağa katılmak için geçtiği ilişkilendirme sürecinin bir parçası olduğunu ve ağ kimlik doğrulaması (802.1X/EAP gibi) olmadığını unutmayınız.

Korumasız Çerçeve Tipleri ; Uç noktaların bir ağı bulma ve birleştirme işlemleri , ağa katılmadan önce bile belirli çerçevelerin herhangi bir uç nokta tarafından erişilebilir olmasını gerektirir. Bu durumlarda , tarafların bütünlüğünü şifrelemek veya doğrulamak mümkün değildir. Bir kenara , yönetim çerçevesi korumasını 4 yönlü el sıkışmadan önceki çerçeveleri ve kontrol çerçevelerini içerecek şekilde genişletmek için çözümler öneren ve savunan bazı uzmanlar vardır.

Bu korumasız yönetim çerçeveleri şunları içerir ; İlişkilendirmeden önce işaret ve araştırma isteği / yanıtları. Anons trafik gösterge mesajı (ATM). 802.11 kimlik doğrulaması. İlişkilendirme isteği / yanıtı. Spektrum yönetimi eylemleri.

Korumalı Çerçeve Tipleri ; Bir uç nokta ağa katıldıktan sonra (4 yönlü el sıkışma yoluyla) , AP ve uç nokta , şifreleme anahtarlarını türetmek için bilgi alışverişinde bulunur ve daha sonra , şifreli paket alışverişinin yanı sıra kimliklerini birbirlerine kanıtlayabilirler. Korunan yönetim çerçeveleri şunları içerir ; İlişkilendirmeden sonra işaret ve araştırma isteği / yanıtları. İlişkiyi kesme (AP veya oturumu sonlandıran uç nokta). 802.11 kimlik doğrulamasının kaldırılması (uç noktadan AP'ye). Blok alındı bildirimleri , QoS , spektrum yönetimi ve Hızlı BSS Geçişi (FT) gibi belirli eylem çerçeveleri. Yayın olarak gönderilen kanal değişikliği duyuruları. Uç noktaya tek noktaya yayın olarak gönderilen kanal değişikliği duyurusu.

802.11 kimlik doğrulamasını kaldırma ve ilişki kesme çerçeveleri , en sık yanıltılan (kötü amaçlı veya kasıtlı olarak WIPS'den) iki tür etkileşimdir. Yeni güvenlik ilişkisi (SA) sorgu işlevi , AP'nin bir uç noktadan gelen belirli istekleri işlemeden önce ilişkilendirme tablosunu kontrol edeceği bir arama adımı ekler (ilişki kesme gibi). İlişkilendirme girişi mevcutsa , talebin korumalı çerçeveler aracılığıyla gönderilmesi gerekecek veya reddedilecek / yok sayılacaktır. Çerçevelerin sahteciliğini önleme mekanizmasının bir parçasıdır. Şifrelenmiş tek noktaya yayın değiş tokuşları için mevcut şifre paketleri ve anahtarlar kullanılır. Özellikle tek noktaya yayın trafiğinin şifrelenmesi için gönderenin ikili geçici anahtarı (PTK) kullanılır. Yayın ve çok noktaya yayın yönetim çerçevesi koruması için yeni anahtar belirtilir ; bütünlük grubu geçici anahtarı (IGTK) ile mesaj bütünlüğü denetimi (MIC) işlevi. IGTK , 4 yönlü el sıkışmanın 3. mesajına eklenir ve bundan sonra 802.11w , yayın ve çok noktaya yayın yönetim çerçevelerini korumak (bütünlük değil şifreleme) için yayın bütünlüğü protokolünü (BIP) kullanır. BIP'nin amacı ; gizlilik değil , bütünlük ve yeniden oynatma korumasıdır.

Doğrulanmış ve Şifrelenmiş ; 802.11w etkinleştirildiğinde , bazı çerçeveler korunmaz. Diğerleri gönderici doğrulanarak bütünlükle korunur ve alt küme de şifrelenir. Hangi çerçevelerin şifrelendiğine karşı hangi çerçevelerin yalnızca bütünlük sunduğu şu şekilde özetlenebilir ; 4 yönlü el sıkışmadan sonra , tek noktaya yayın çerçeveleri şifrelenir (hem gizlilik hem de bütünlük sunar).4 yönlü anlaşmadan sonra , yayın ve çok noktaya yayın çerçevelerine yalnızca bütünlük sağlanır. Şifreli tek noktaya yayın yönetim çerçeveleri , eylem çerçevelerini , ayrılma çerçevelerini ve kimlik doğrulamasını kaldırma çerçevelerini içerir. İçerikler PTK ile şifrelenir ve yük şifrelenirken başlıklar (uç nokta MAC adresi dahil) şifrelenmez. PMF ile güvenli uç noktalar için çok noktaya yayın ve yayın trafiği , bütünlük sağlamak ve mesajın sahte değil , kanıtlanmış kaynaktan geldiğinden emin olmak için az önce tartışılan IGTK ile BIP'yi kullanır. PMF ile şifrelenen verilere örnek ; ayırma ve kimlik doğrulamasını kaldırma neden kodlarıdır. Bu , birçok Wi-Fi aracının neden kodlarını ve diğer verileri sorun giderme amacıyla izleme ve kullanma yeteneğini etkileyecektir.

WPA3, Geçiş Modları ve 802.11w ; 802.11w'nin çalışmasını belirleyen senaryolar şunlardır ; WPA3 ilişkilendirmeleri (Kişisel ve Kurumsal dahil) , Korumalı Yönetim Çerçevelerinin (PMF) kullanılmasını gerektirir. Yalnızca WPA3 Modları yalnızca WPA3 istemcilerini destekler ve tüm istemcilerin katılması için PMF gerekir. WPA3 Geçiş Modları , 802.11w / PMF'nin desteklendiği / isteğe bağlı olduğu , WPA3 istemcilerinin PMF kullanacağı hem WPA2 hem de WPA3'ü destekler. WPA2 , destekleniyorsa / yapılandırılmışsa PMF kullanabilir ve WPA3 olarak sınıflandırılacaktır. PMF'yi desteklemeyen WPA2 istemcileri , PMF olmadan katılacak. WPA2 ağları isteğe bağlı olarak etkinleştirilebilen ancak isteğe bağlı olan PMF'yi destekler. OWE ile Geliştirilmiş Açık (şifreli açık ağlar) PFM kullanımını gerektirir.

PMF VS. MFP VS. CISCO MFP ; 802.11w standardı , Wi-Fi Alliance tarafından Korumalı Yönetim Çerçeveleri (PMF) olarak adlandırılır ve IEEE belirtiminde Yönetim Çerçevesi Koruması (MFP) olarak adlandırılır. Bunların ikisi de aynı şeydir (802.11w) fakat Cisco'nun altyapı bütünlüğü için kontroller topluluğu olan Altyapı Yönetimi Çerçeve Koruması (MFP) olarak da adlandırılan satıcıya özel özellik paketi ile karıştırılmamalıdır.

802.11w için Uyarılar ve Hususlar ; PMF , yüksek bütünlüklü altyapıya doğru adımlar atmaktadır. Bazı sınırlamalar ve güvenlik hususları şunları içerir ; Kontrol çerçeveleri , 2. Katman DoS saldırılarına karşı hiçbir koruma sağlamayan CTS ve RTS (göndermeye açık ve göndermeye yönelik istek) dahil korunmaz. 4 yönlü el sıkışma korumalı değildir yani uç nokta , ağa ilk bağlantıda ortadaki adam saldırılarına ve kötü ikiz saldırılarına açıktır. 4 yönlü el sıkışma ile PMF'nin kurulması arasındaki küçük zaman penceresinde kimlik doğrulamasının kaldırılması veya ayrılma paketlerinin yanıltıcı olabileceği çok sayıda zaman vardır. WPA-Kişisel ağlarda , PMF , çevrimiçi veya çevrimdışı sözlük saldırılarına karşı parola güvenlik açıklarına karşı koruma sağlamaz. WPA2 ve WPA3'ü destekleyen WPA3 geçiş ağlarında PMF gerekli değildir ve bazı istemciler saldırılara karşı savunmasız olacaktır. Ağa katılmayan uç noktalara yönelik yayın ve çok noktaya yayın trafiği geliştirmelerine yönelik geliştirmeler fakat kötü niyetli kullanıcılardan veya ağa bağlı ve yayın bütünlüğü protokolüne (BIP) katılan cihazlardan hiçbir koruma sağlamaz.

802.11w'yi WPA2 Ağlarında 802.11r Roaming ile Kullanma ; Birkaç satıcının 802.11w korumalı yönetim çerçeveleri + 802.11r Hızlı Geçiş (FT) roaming kombinasyonunu WPA2 ağlarında desteklemez ve önermez. 802.11w PMF'li WPA2'nin yalnızca SHA1 hash algoritmasını desteklediğini ve FT ile diğer kimlik doğrulama , anahtar yönetimi (AKM) paketleri bir saniye kullanılır. Çalışma grubu o zamandan beri bunu düzeltti ve PMF , Wi-Fi sistemi ve uç noktalar güncellendiği sürece WPA2 ağlarında desteklenmelidir. Bir uç nokta PMF kullanarak bağlanırsa , WPA3 istemcisi olarak sınıflandırılacağını unutmayın. WPA2 ve WPA3 arasındaki fark , WPA'ya karşı WPA2'de olduğu gibi bir bilgi öğesi tarafından tanımlanmaz.

AP'leri Yöneticiye Sağlama ve Güvenceye Alma ; Güvenilir altyapı , bileşik bileşenlerinin bilinmesine , doğrulanmasına ve birbirlerine yetkilendirilmesine dayanır. Kablosuz altyapı içinde amacımız ; çevreyi kontrol etmek ve yönetim sistemimize yalnızca yetkili AP'lerin bağlı olduğundan , yönetim sistemi ile AP'lerin karşılıklı olarak doğrulandığından , AP yetkilendirmeleri ve uygun gruplara atama konusunda bilinçli olduğumuzdan emin olmaktır. İsteğe bağlı olarak , yol boyunca istemci trafiğini kapsüllemek veya şifrelemek isteyebiliriz. İstemci trafiğini yönlendiren kurallar için güvenlik reçete etme disiplini , kontrol düzlemi güvenliği olarak tanımlanır ve altyapı bileşeni kimlik doğrulaması , cihazları altyapıya onaylama ve cihazlar arasındaki iletişimi güvence altına alma gibi birçok yönü kapsar. Özünde , kontrol düzlemi güvenliği , altyapı cihazlarına bütünlük ve gizlilik getirir. Kontrol düzlemi güvenliği , bulut tarafından yönetilen mimarilerde şirket içi kontrolör mimarilerine göre biraz farklı yönetilir fakat kapsayıcı kavramlar ve görevler aynı kalır. Görevlere sorumluluk yüklediğimizde farklılık ortaya çıkar ; bulut tarafından yönetilen platformlarda , AP'lerin benzersiz bir kimliğe ve yönetim platformuna güvenli bağlantıya sahip olmasını sağlamak gibi belirli görevleri yerine getirme sorumluluğu satıcıya aittir.

Yönetim ve kontrol düzlemi güvenliğinin yürütülmesi şu başlıklarda ele alınmaktadır ; AP'leri Onaylama veya İzin Verilenler Listesi. AP'ler için Sertifikaları Kullanma. AP'lerden Denetleyiciye veya Tünel Ağ Geçidine Güvenli Tünelleri Etkinleştirme. Varsayılan AP Davranışını Adresleme.

AP'leri Onaylama veya İzin Verilenler Listesi ; Her denetleyici veya yönetim platformu , AP'leri onaylamak için yönteme veya birkaç yönteme sahip olacaktır. Bu süreç , AP'lerin seri numarasına veya MAC adresine göre ön yetkilendirilmesinde olduğu gibi önceden gerçekleşebilir veya AP'nin denetleyiciyi veya yönetim sistemini keşfettikten sonra , platforma tam olarak uyarlanmadan önce gerçekleşebilir. Ayarlar , diğer şeylerin yanı sıra AP izin verilenler listesi (beyaz liste olarak da bilinir) , AP benimseme , AP onayı veya AP yetkilendirme olarak adlandırılabilir. Sektördeki genel eğilim , satıcıların varsayılan davranışı daha güvenli yapılandırmalarla değiştirerek artırılmış güvenlik duruşlarını desteklemesi olmuştur. Geçmişte bir satıcı , denetleyiciyi keşfeden , onları yetkilendiren ve varsayılan gruba koyan AP'leri otomatik olarak benimseyen varsayılan ayara sahip olabilir. Zamanla , varsayılan davranış değişerek günümüz de yeni AP'leri bekleme durumunda göstererek ağ yöneticisini bunları manuel olarak onaylamaya veya önceden tanımlanmış kural aracılığıyla onaylamaya zorlayacak ve ardından bir gruba atayacaktır.

AP'ler tarafından kontrolör veya yönetim platformunun otomatik olarak keşfedilmesi beklenmektedir. Kontrolleri uyguladığımız yer orası değildir. AP yöneticiyi bulduğunda veya istenirse önceden , AP'nin benimsenmesini yöneticiden kontrol ederiz. Güçlendirme stratejinizin bir parçası olarak , AP'nin benimsenmesini dikkatli şekilde planlayın ve şu en iyi uygulamaları izleyiniz ; AP'lerin yöneticiye otomatik olarak kabul edilmesine izin verme. Tüm beklenen AP'lerin yöneticide olduğunu ve hiçbirinin eksik olmadığını doğrulayınız. Toplu benimseme için AP yönetim ağlarının IP alt ağı gibi en makul ayrıntı düzeyini kullanınız. Envanteri ara sıra denetleyin ve beklenmedik şekilde yöneticiden ayrılan veya yöneticiye katılan AP'leri uyarınız.

Bulut tarafından yönetilen ürünlerde yetkilendirme biraz hantallaşabilir, çünkü bazen AP tahsisi yerine getirme tedarik zinciri sürecine bağlıdır. Bazı satıcı çözümlerinin AP'leri siparişi işleyen distribütör aracılığıyla kuruluşa bağlayacağı anlamına gelir. Distribütör , üretici ve satıcı arasındaki perde arkasındaki şirkettir ve genelde üreticinin sistemleriyle derinden entegredirler ve bu hesap sağlama işlevleri gibi görevleri yerine getirirler. Bazı satıcılarda AP'nin envanterinizde listelenip dağıtımcı tarafından oraya yerleştirilebileceğidir. Bu noktada , AP'yi bir siteye veya gruba yetkilendirmek ve atamak için her zamanki gibi ilerlersiniz. Bunun dezavantajı , büyük kuruluşlarda , birden fazla lokasyona sahip olanlarda veya merkezi tedariki olmayan departmanlarda AP'lerin yanlış yere gidebilmesidir.

AP'ler için Sertifikaları Kullanma ; AP'leri yöneticiye doğrulamanın bir yolu sertifikalardır ve bu sertifikalar daha sonra şifreleme için kullanılabilir. Bulut ve denetleyici mimarilerinin farklılık gösterdiği başka bir alandır.

Bulut tarafından yönetilen AP'ler , üretim sırasında önceden yüklenmiş sertifikaya sahip olacaktır. AP telefonları internet üzerinden bulut yöneticisine ev sahipliği yaparak benzersiz şekilde tanımlanması ve uygun müşteri hesabına sağlanması için gereken her şeye sahiptir. Denetleyici tarafından yönetilen AP'lerde önceden yüklenmiş sertifika da olabilir fakat denetleyicinin , denetleyiciye kaydolduklarında ve onaylandıklarında AP'lere sertifika vermesi daha yaygındır. Alternatif olarak da çoğu kurumsal ürün , AP'leri veya diğer altyapıyı mevcut PKI altyapısına kaydetmek için standart protokollerin kullanımını destekler. Güvenli Aktarım Üzerinden Kayıt (EST) ve Basit Sertifika Kayıt Protokolü (SCEP) , Wi-Fi satıcıları tarafından desteklenen iki protokoldür. Denetleyici tarafından yönetilen AP'ler önceden yüklenmiş sertifikayla gönderilmeyebilirken , denetleyicilerin kendilerine önceden sertifika sağlandığını görmek giderek daha popüler hale gelmektedir. Özellikle , satıcılar TPM yongalarını ve IEEE 802.1AR'ı kullanmaya başlamaktadır. Sertifikalar yerindeyken , yönetici AP ile yönetici arasında şifrelemeyi yapılandırma seçeneğine sahiptir.

AP'lerden Denetleyiciye veya Tünel Ağ Geçidine Güvenli Tünelleri Etkinleştirme ; Kurumsal düzeyde denetleyici tabanlı ürünlerin her yerde AP'den denetleyiciye giden trafiği kablo üzerinden şifreleme seçeneği sunduğu döneme geldik. Şifreli tüneller , hem yönetim trafiğini hem de istemci trafiğini güvence altına almak için kullanılabilir. Verilerin kablo üzerinden şifrelenmesi , on yılı aşkın süredir yönetmeliklerin temelini oluşturuyor. İleriye dönük olarak , sıfır güven girişimleri , tüm veri yolu boyunca yaygın şifreleme misyonunu daha da ileriye taşıyacaktır. Şifreleme senaryosunda olduğu gibi , şifreli tünel iki uç veya sonlandırma , karşılıklı kimlik doğrulama ve şifreleme anahtarları gerektirir.

İstemci verileri tünel oluşturma veya köprü oluşturma , SSID başına ve bazı durumlarda bundan daha ayrıntılı olarak yapılandırılabilir. Güvenli bir yönetim düzlemi bakış açısından , bulut tarafından yönetilen çözümler , önceden sertifikalarla donatıldıkları ve bulut yöneticisine güvenli şekilde bağlanmaya hazır oldukları için burada biraz öne çıkmaktadır. Yönetici internette olduğundan , tanım gereği trafik güvenilmeyen ağdan geçecektir ve bu nedenle yönetim düzlemi için şifreleme talep eder. Yerel tünel sonlandırma aracı (ArubaOS 10'da Mist Edge cihazı veya Aruba Gateway cihazı gibi) içeren bulut tarafından yönetilen çözümler için şifreleme , istemci trafiği için veri düzlemine genişletilebilir. Yapılandırma seçenekleri denetleyicininkine benzer fakat özellik derinliği satıcıya göre değişecektir. AP'ler ile denetleyici veya tünel sonlandırma ağ geçidi arasında şifrelemeyi etkinleştirmenin işleme ve bant genişliği ek yüküne neden olacağına dikkat etmek önemlidir. Donanım modellerinde maksimum sayıda AP için satıcılar tarafından belirlenen sınırlar veya önerilen aralıklar olabilir. Sınırlamaları ve diğer hususları tartışmak için lütfen satıcı ekibinize veya belgelerinize danışınız.

Aruba Ve Cisco Marka Cihazlarda Şifrelemeyi Etkinleştirme ; Bu ayarları Cisco denetleyici mimarisinde arıyorsanız , AP benimseme , AP birleştirme profilleri ve şifreli tüneller için DTLS'li CAPWAP için AP yetkilendirme listelerine bakabilirsiniz. Aruba ArubaOS denetleyici mimarisiyle çalışıyorsanız , AP beyaz listeleri , sağlama ve CPSec kontrol düzlemi güvenliği kılavuzunu inceleyiniz. İdeal olarak , kontrol düzlemi güvenliğiniz , kablosuz şifrelemenizi karşılar veya aşar.

Varsayılan AP Davranışını Ele Alma ; AP sağlamadaki son en iyi uygulama , yeni keşfedilen AP'nin varsayılan davranışını kontrol etmektir. İster bulutta ister denetleyici platformunda çalışıyor olun , bu kılavuz aynıdır. Otomatik benimsemeye izin vermeme talimatının yanı sıra , kabul edildikten veya izin verildikten sonra fakat tam olarak yapılandırılmadan veya bir siteye veya gruba atanmadan önce AP'ye ne olacağını da yönetmek istersiniz. Platform varsayılan bir grup içeriyorsa , o grubu asla canlı ağ için kullanmayınız. Varsayılan grubu bir tutma yeri olarak kabul ederek varsayılan grubun SSID'leri yayınlamak , radyo yönetim profilleri vb. için yapılandırılan politikalarla ilişkili olup olmadığını araştırınız. Nihai hedef , AP'ye katılırken AP üzerinde tam kontrol uygulamaktır. Her ne şekilde gerekiyorsa , denetleyicide AP kabul edildiğinde ve buna izin verildiğinde , bundan sonra ne olursa olsun , ağları yayınlamaya başlamadığından emin olunuz.

Kablolu Altyapı Bütünlüğü Ekleme ; Sağlamlaştırma , AP'ler ve kablolu ağ arasında bütünlük eklemeyi içerebilir. Yönlendirmeden DNS , SNMP ve ötesine kadar ağlarda kullanılan her protokol için sıkılaştırıcı disiplinler vardır.

AP'nin kablolu altyapıda kimliğinin doğrulanmasına ve AP'lere hizmet veren uç bağlantı noktası VLAN'larının yönetilmesine şu anda odaklanmalıyız. Bütünlük kontrolleri geçerli en iyi uygulamalar , üksek düzeyde güvenlik ihtiyacı olan ve ek operasyonel yükü yönetmek için uygun personel kaynaklarına sahip kuruluşlar için ayrılmıştır.

Kamusal Alanlarda Ağ Portlarının Kontrolü ; Yüksek güvenlik gereksinimlerinin yanı sıra , genel veya güvenilmeyen kullanıcılar tarafından fiziksel olarak erişilebilen AP'lere sahip ortamlar , ayrıntılı erişim kontrol politikalarıyla birlikte bu kontrolleri de dikkate almalıdır. Spesifik olarak , tünel modundaki AP'ler için sadece AP yönetim VLAN'ından denetleyicilere / kontrollere erişime , ek güvenlik izlemeye izin veren kuralcı ACL'ler olmalıdır. Uçta trafiği köprüleyen AP'ler bu görevi daha zor hale getirir ve çoğu durumda köprülü AP bağlantı noktasına veya kablosuna fiziksel erişim bir sorunsa , katı AP kimlik doğrulaması kullanılmalı veya bu AP'lerde trafiği köprülemek yerine tünel oluşturmayı düşünmelisiniz.

Edge Switch'te AP'lerin Kimlik Doğrulanması ; Kuruluşların AP kimlik doğrulaması yoluyla bu düzeyde kablolu yan sertleştirme gerçekleştirmesi genelde yönetilebilir değildir. Ancak , bu düzeyde bütünlük gerektiren kuruluşlar vardır. Bu yüzden burada bazı nasıl yapılır ve dikkat edilmesi gereken şeylerle birlikte verilmiştir. Çoğu ortam için paranızın karşılığını fazlasıyla verecek başka pek çok sertleştirme görevi vardır. AP'leri denetleyiciye veya yöneticiye sağlamanın yanı sıra 802.1X veya MAC adresi bağlantı noktası güvenliğini kullanarak AP'leri doğrulayabilir veya kablolu altyapıya bağlayabiliriz. İstemci tabanlı kimlik doğrulamalarda olduğu gibi , AP'ler de 802.1X/EAP , MAB ile 802.1X , MAC adresini bağlantı noktasına veya anahtara bağlamaya dayalı 1X olmayan bağlantı noktası güvenliği kullanabilir..

AP'lerin 802.1X / EAP ile bağlantı noktalarına kimlik doğrulaması ; 802.1X kullanarak uç anahtarda AP'lerin kimliğini doğrulamayı planlıyorsanız , gereksinimler , uç anahtarın AAA yapılandırmalarını desteklemesi gerekmesidir. Her kurumsal düzeyde anahtarlama ürününde desteklenir ve AP'nin 802.1'e sahip olması gerekir. Denetleyici tabanlı AP'ler , tam 802.1X kimlik doğrulamasını destekler ve çoğu ürün , MSCHAPv2 , EAP-TTLS veya EAP-TLS ile EAP-PEAP ile yapılandırılabilir.

Ürünler de 802.1X AP Ayarlarını Bulma ; Bu ayarları Cisco denetleyicisinde arıyorsanız , CAPWAP DTLS profilinin bir parçası olarak ve CLI'deki dot1x yapılandırma ayarları içinde yapılandırılırlar. Aruba kılavuzlarında , bunu yapılandırmaya ilişkin talimatlar için AP'de 802.1X istek desteğini etkinleştirmeyi arayınız. Her iki satıcı da fabrikada yüklenen veya denetleyici tarafından verilen AP sertifikalarının kullanımını destekler. Bulut tarafından yönetilen AP'lerin 802.1X'e katılma olasılığı daha düşüktür fakat en güncel özellik desteği için satıcınıza danışınız.

AP'lerin 802.1X ve MAC Kimlik Doğrulama Baypas (MAB) ile bağlantı noktalarına kimlik doğrulaması ; 802.1X sağlayıcısı olmayan AP'lerle sağlamlaştırma gerektiren ortamlar için ikinci seçenek , MAC Authentication Bypass veya MAB ile kimliklerini doğrulamaktır. 802.1X protokolünün bir alt işlevi olduğundan , kenar anahtarı bağlantı noktaları , eklenen MAB komutlarının yanı sıra birkaç satır AAA komutu gerektirecektir. Bu modelin avantajı , AP yerel olarak 802.1X'i desteklemese bile AP'lerin anahtar bağlantı noktasında (merkezi olarak kimlik doğrulama sunucusu tarafından) doğrulanabilmesidir. Bu da , 802.1X'i kenar anahtarında MAB ve AP'lere hizmet veren bağlantı noktaları ile yapılandırmanız gerektiği , AP'nin kendisinde ek yapılandırma gerekmediği anlamına gelir.

AP'leri MAC adresiyle bağlantı noktalarına veya anahtarlara bağlama ; AP'yi , AP'nin MAC adresiyle yerel olarak (kimlik doğrulama sunucusu aracılığıyla) uç anahtara yetkilendirmek için anahtar bağlantı noktalarında 802.1X (AAA) yapılandırmak yerine , bağlantı noktası güvenlik komutu kullanacaksınız. Anahtar satıcınızın belgelerine bakınız fakat genelde yapılandırma kılavuzlarının bağlantı noktası güvenliği bölümünde bulunur. Çoğu ürün , bağlantı noktasını sabit veya statik MAC adresi , öğrenilmiş veya dinamik MAC adresi ve ardından yapışkan MAC gibi seçenekler için yapılandırma gibi çeşitli seçenekleri destekler. Bu rotaya giderseniz , maksimum MAC adresi yapılandırmalarına özellikle dikkat ediniz. Köprülü modda AP ile kullanıldığında , kenar anahtarı istemci MAC adreslerini görecek ve anahtarın bir MAC sayısı ihlali nedeniyle bağlantı noktasını kilitlediğini görebilirsiniz.

Güvenlik ve yönetilebilirlik için kişisel bir tercih olarak , port MAC bağlama gibi yerel yetkilendirme gerçekleştiren mimarilerden kaçınarak bu düzeyde sertleştirme gerekiyorsa 802.1X veya MAB kullanmayı tercih edebilirsiniz. Kurumsal dağıtımlarda , merkezi görünürlük ve yönetim eksikliği , hızla hantal hale gelen operasyonel ek yük ekleyerek MAC bağlama güvenli kabul edilmez. Bu nedenle potansiyel olarak ağır yönetim yükü ile minimum güvenlik geliştirmesidir. Kablolu 802.1X kimlik doğrulamaları çok fazla ek yük getirerek onu yönetecek kaynaklara sahip olan veya ek korumaya ihtiyaç duyan alanlara odaklanan kuruluşlar için ayrılmalıdır. AP , bu kontrollerden herhangi biri etkinleştirilirse , ağda kimliği doğrulanana kadar trafiği geçemez veya istemci hizmeti gerçekleştiremez.

Edge Port VLAN'larını Belirtme ; Herhangi bir ortam için en iyi uygulama olan görünüşte küçük bir görev , her uç bağlantı noktasında sadece gerekli VLAN'lara izin vermektir. VLAN'ların azaltılmasını veya AP yönetimi için belirlenmiş yerel / etiketlenmemiş VLAN'ın belirlenmesini gerektirebilir. Ve bu görev önemsiz gibi görünse de kablolu ve kablosuz ürünlere bağlı olarak zaman alıcı olabilir. Juniper's Mist ürünleri gibi bazı satıcılar , AP'leri ek kablolu veri toplamak ve yönetici konsolunda VLAN uyumsuzlukları gibi durumları bildirmek için kullanır. Çoğu üründe , manuel süreç olmuştur. Mevcut kaynaklara bağlı olan başka bir en iyi uygulamadır. Potansiyel olarak ağır operasyonel maliyet ve ortamların genelde dinamik doğası nedeniyle , değişiklik yönetimi süreçlerini uygulamayan kuruluşlarda zamanın en iyi kullanımı olmayabilir. İdeal olarak , bu görevi bir kez gerçekleştirebilir ve ardından daha önce açıklanan bu yeni değişiklik yönetimi kontrolleri ve temel yapılandırmalar aracılığıyla uç bağlantı noktalarında uygun VLAN'ların yapılandırıldığından emin olabilirsiniz.

VLAN Hopping ; Her birkaç yılda bir yeniden ortaya çıkan bir konu , VLAN ana hat bağlantı noktaları güvenli olmayan şekilde yapılandırıldığında veya varsayılan VLAN kullanımda olduğunda veya bağlantı noktasında gerekli olmayan etiketlenmiş VLAN'lara sahip olduğunda meydana gelen VLAN atlamalı VLAN yapılandırmalarından yararlanılmasıdır. Bir senaryoda , saldırgan anahtarı taklit edebilir , ağa bağlanabilir ve uç anahtarı , saldırganın eş anahtar olduğunu düşünmesi için kandırabilir. Otomatik VLAN sağlama protokolleri kullanılıyorsa , kurumsal anahtar , uygulamaya bağlı olarak , saldırganın bağlantı noktasını atanmış VLAN'la veya tüm VLAN'larla ana hat olarak sağlar. Çift Etiketleme adı verilen başka bir senaryo da ise ilk anahtara yerel VLAN olarak görünen başlıklarda çift yığınlama yaparak 3. Katman ACL'lerini atlayabilir. Bu saldırı , etiketlenmemiş / yerel VLAN ile yapılandırılmış bağlantı noktalarından yararlanır ve ana hat / etiketli VLAN bağlantı noktaları gerektirmez. Bunlar meşru saldırılar olsa da , büyük güvenlik endişeleri şemasında daha az önemli olarak kabul edilirler. Her ikisi de ortama fiziksel erişim gerektirir ve Çift Etiketleme saldırısı tek yönlüdür (paketler yalnızca bir yöne gidebilir) ve saldırganın hedef IP , VLAN hizmeti bilmesini gerektirir , bu da saldırganın hedef kaynakla etkileşime girme riskini büyük ölçüde sınırlar. Sertleştirme kapsamındaki diğer bazı konularda olduğu gibi penetrasyon test cihazları ve kötü niyetli kullanıcılar ağa saldırmak için sayısız başka kolay yollara sahiptir ve bu en iyi uygulama olsa da , diğer güvenlik açıklarının varlığında kaynakları boşa harcaması önerilen görev değildir.

Fiziksel Güvenliği Planlama ; Birçok ağ saldırısı , kötü niyetli bir kişi tarafından altyapıya fiziksel erişime dayanır. Ve birçok ortam , varlıkların fiziksel erişime karşı belirli bir düzeyde korumaya sahip olduğunu varsayar ; bina erişimi anahtar veya RFID rozeti gerektirir. Sunucu odası ek erişim hakları vb. gerektirir. Ancak çoğu durumda , her ağ bağlantı noktasının fiziksel olarak korunduğunu veya kötü niyetli kullanıcının birine erişemeyeceğini varsaymak adil değildir. Bağlantı noktası güvenlik protokolü veya kablolu uç bağlantı noktalarını kontrol eden ağ erişim denetimi (NAC) ürünü olmadan , birçok bağlantı noktası yanlış kullanıma karşı savunmasız kalır. Her durumda , ağ güvenliği mimarisi , uç anahtar bağlantı noktaları dahil olmak üzere ağa giriş noktalarını kontrol etmelidir. Genel olarak erişilebilir alanlarda olabilecek AP'lere bağlanan bağlantı noktaları dahil olmak üzere ağ dolaplarında ve uç bağlantı noktalarında fiziksel güvenlik kontrolleri tasarlamak anlamına gelir.

Ağ Alanlarına Güvenli Erişim ; Sunuculara , depolamaya , ağ cihazlarına (kablosuz denetleyiciler dahil) , ağlara veya veri dolaplarına fiziksel erişimin güvence altına alınması , iyi ağ sağlığı için en temel en iyi uygulamalardan biridir.

İdeal olarak bu varlıklar , sadece anahtar değil , aynı zamanda RFID rozeti , biyometrik giriş veya erişimi belirli bir kişiyle ilişkilendirmenin bir yolu anlamına gelen , kimlik tabanlı erişimi zorunlu kılan yerlere yerleştirilmelidir. Kimlik tabanlı erişim denetimi mümkün değilse , bir sonraki en iyi seçenek donanım kilidi gibi bazı fiziksel denetimlerdir. Kilitlerin , kırılmanın veya almanın ne kadar zor olduğunu gösteren kasalar gibi derecelendirmeleri vardır. Ağ dolaplarına ve veri merkezlerine fiziksel erişimin korunmaması şunlara neden olabilir ; dahili personel dahil yetkisiz kişilerce erişim olacaktır. İstenmeyen yeniden yapılandırma , ağ kablosu ekleyen veya bağlanan biri aracılığıyla olabilir. Ağ döngüsünün yanlışlıkla devreye girmesiyle hizmet reddi , yayın fırtınası olabilir. Anahtar veya denetleyici gibi sistem bileşenini çevrimdışı duruma getirerek hizmet reddi oluşturulabilir. Yönetim platformu veya güvenlik izleme gibi izleme sistemini çevrimdışına alarak görünürlüğün alt üst edilmesi sağlanabilir. Çok yüksek nem veya harici satıcı tarafından belirtilen çalışma sıcaklığı aralıkları gibi uygun olmayan sistem ortamından kaynaklanan kesintiler olabilir.

AP'lere ve Edge Bağlantı Noktalarına Erişimin Güvenliğini Sağlama ; Tüm veri yolunun fiziksel kontrolünü sürdürmek önemlidir.Ağ kablolarının her iki ucu ve sonlandırılması anlamına gelir. Ağ iletişimi dolapları ve veri merkezlerinin dışında , AP'lere hizmet verenler de dahil olmak üzere , ortam genelinde dağıtılan ağ kesintilerine koruma genişletilmelidir. Sonuçta amaç ; saldırganın AP'yi kaldırmasına ve AP'nin ağ bağlantısını üretim ağına sızmak için kullanmasına karşı koruma sağlamaktır. Diğer bazı kontrollerin (segmentasyon , anahtara AP kimlik doğrulaması , bağlantı noktası güvenliği ve izleme) dışında , AP'lere erişimi zorlaştırarak veya kaldırmayı zorlaştırarak bu davranışı engelleyebiliriz. Saldırgan AP ağ bağlantı noktasına erişim kazanırsa şu eylemler gerçekleştirilebilir ; Kablolu ağ üzerinden kablosuz altyapıya karşı hizmet reddi (DoS) saldırısının başlatılması gerçekleştirilebilir. Diğer kablolu kaynaklara karşı hizmet reddi (DoS) saldırısının başlatılması sağlanabilir. Kablolu ağ içindeki uç noktalara ve hedeflere yanal hareketler yapılabilir. Ağ trafiğinin koklanması olabilir. Kötü niyetli yüklerin enjeksiyonu olabilir. Paketleri bozmak veya yeniden yönlendirmek için anahtarlama ve yönlendirme işlevlerine enjeksiyon sağlanabilir.

Kablosuz ikilemlerle doludur ve AP montajı istisna değildir. Çoğu Wi-Fi tasarım uzmanı ve satıcısı , müşterileri AP'leri tavan ızgarasının altına monte etmeye yönlendirecek ve genelde AP'yi gizleyerek RF sinyallerini engellemeyecektir. AP'ler sadece takılıyor ve geçen herkes tarafından görülebiliyor. AP bir duvara monte edilmişse veya standart tavanın altına monte edilmişse , saldırganın onu ele geçirmesi önemsizdir. Bu nedenle , AP'yi fiziksel olarak güvenceye almak ağ altyapısını korumanın anahtarıdır. AP'yi fiziksel olarak güvence altına almanın , caydırıcıdan kırılması neredeyse imkansız olana kadar çeşitli düzeyler ve yöntemler vardır. En azdan en çok güvenliye doğru sıralanırlar ; Kurcalama engellemeli montaj donanımı. Mandal kilitli donanım ve muhafazaların montajı. Tuş kilitli donanım ve muhafazaların montajı.

AP yuvaları , çeşitli form faktörleri ve malzemelerle gelir. Bazıları tam muhafazalardır (kutular) , diğerleri ise mevcut tavan ızgaralarına uyacak veya tavan ızgarasının alt tarafına eklenecek şekilde tasarlanmıştır. Direkler gibi gizli montajların yanı sıra yüzey montajları ve dik açılı montajlar da vardır. Çoğu , kurcalamayı caydırıcı veya tuş kilitli olarak mevcuttur. Birçok kutu muhafazasında mandal kilitleri de olabilir.

Altyapı Cihazlarında Ön Panel ve Konsol Erişimini Kilitleme ; Kablosuz denetleyiciye , AP'lere ve diğer ağ cihazlarına fiziksel erişimi kontrol etmek yeterli değilse veya uygun değilse , donanımın kendisinde bulunan yönetim işlevlerinin devre dışı bırakılması veya kilitlenmesi sağlamlaştırmayı içerebilir. Kötü niyetli kullanıcı , ön panel ve konsol güvenliği olmayan sistem cihazlarına fiziksel erişim sağlarsa , hizmet reddinden yeniden yapılandırmaya ve meşru sistem sahiplerini kilitlemeye kadar bir dizi saldırı gerçekleştirebilir.

Ön panel ve konsol güvenliği olmadan , sistem saldırganın şu eylemlerden birini veya birkaçını gerçekleştirme riski altındadır ; Yetkisiz yeniden başlatmalar (güç kaynağını kaldırarak da mümkün olabilir) . Fabrika ayarlarına sıfırlama (yapılandırmayı siler). Parola sıfırlama (bazı ürünler parolaları temizlemek için bir düğme dizisi içerir). Yeniden yapılandırma (sistem güvensiz , erişilemez veya başka bir şekilde tehlikeye atılabilir). Parolaları kurcalama (saldırgan parolaları değiştirebilir ve meşru yönetim yöneticilerini kilitleyebilir). Kötü amaçlı yükleri yükleyiniz (USB veya konsol aracılığıyla yazılım yüklemeleri yoluyla).

Denetleyiciler için ön panel erişimini sağlamlaştırma , donanım aygıtındaki bağlantı noktalarını kontrol etmeyi veya kilitlemeyi , USB'yi devre dışı bırakmayı , hizmetleri sıfırlamak veya yeniden yüklemek için fiziksel düğmeleri devre dışı bırakmayı ve konsol erişimini veya donanıma fiziksel erişimi olan bir kişinin kullanabileceği herhangi bir yönetim özelliğini kilitlemeyi içermektedir. Satıcılar ayrıca ön panel güvenliğini ve diğer özellikleri uygulayacak FIPS uyumlu ürünlerle önceden güçlendirilmiş yapılandırma sunar. Çoğu AP'de diğer şeylerin yanı sıra konsol bağlantı noktaları ve USB bağlantı noktaları bulunur. Yönetim işlevlerine yönelik bu ek girdiler , saldırganın AP'nin yapılandırmasına sızarak altyapıyı tehlikeye atmasını önlemek için denetleyici veya yönetim sistemi aracılığıyla devre dışı bırakılabilir. Konsol bağlantı noktaları tek AP güvenlik açığı değildir. Bazı satıcılar tarafından üretim sırasında hala kullanılan Ortak Test Eylem Grubu (JTAG) bağlantı noktaları , AP'lerdeki baskılı devre kartlarında (PCB) bulunur. Test , programlama ve tanılama için kullanılan JTAG bağlantı noktaları , cihaza tam erişim sağlayabilir ve nadiren güvenlidir. Bir saldırganın ne aradığını bilmesi gerekir fakat hassas ortamlarda AP'leri fiziksel olarak güvenli hale getirmenin başka bir nedenidir.

Kurumlar ve yüksek riskli ortamlar , ek kontrollerle konsol erişim güvenliğini bir adım daha ileri götürmek isteyebilir ; Kullanılmayan konsol / yönetim bağlantı noktalarının üzerine yerleştirilmiş kurcalamaya açık etiketler (TEL). Konsol aracılığıyla TAC desteği parola kurtarmasını devre dışı bırakınız.

Kurcalamaya açık etiketler , kullanılmayan fiziksel bağlantı noktalarına yalnızca acil durumlarda , izin veriliyorsa erişilmesini sağlayabilir. Etiket , bağlantı noktalarını kapatmak için kullanılır ve bağlantı noktasına erişmek için çıkarılırsa , belirgin olacaktır. Bunlar bir kuruluş için özel olarak yazdırılabilir ve yalnızca acil durumlarda kullanılması gereken konsol bağlantı noktası gibi yönetim erişim bağlantı noktalarına yerleştirilebilir. Çoğu üretici , teknik yardım merkezi (TAC) destek süreçlerinin bir parçası olarak bir tür parola kurtarmayı destekler. Bu durumlarda , hesapta yetkilendirilmiş birinin cihaza fiziksel konsol erişimine ihtiyacı olacaktır ve bu sırada satıcı TAC'yi kısa bir geçerlilik süresi olan tek seferlik bir şifre için kullanabilirler. Bu atlamayı önlemek için parola kurtarma devre dışı bırakılabilir.

İlgili NIST SP 800-53 Kontrolleri ; Kontrolleri NIST'e eşleyen kuruluşlar için Fiziksel ve Çevresel Koruma (PE) grubu , diğerleri arasında Fiziksel Erişim Kontrolü , Fiziksel Erişimi İzleme ve Varlık İzleme ve İzleme dahil olmak üzere fiziksel güvenlikle ilgili çeşitli kontrolleri içerir.

Kullanılmayan Protokolleri Devre Dışı Bırakma ; Kullanılmayan fiziksel bağlantı noktalarını devre dışı bırakmakla aynı şekilde , sağlamlaştırma , sadece şifrelenmemiş yönetim protokollerini değil , kullanılmayan tüm protokolleri devre dışı bırakmayı kesinlikle içermelidir. Kullanılmayan protokoller genelde göz ardı edilerek ağ ve güvenlik işlemleri için kör nokta haline gelir. İdeal dünyada , SOC veya birisi , güvenlik açığı yönetim programının parçası olarak dahili olarak güvenlik açığı taramaları yürütür. Bu taramalar , bilinen güvenlik açıklarına sahip hizmetleri kullanan risk altındaki cihazları kesinlikle belirlemeye yardımcı olacaktır fakat ağ tasarımınızda hala yeri olmayan bilinen iyi protokoller olabilir. Devre dışı bıraktığınız hizmetler , bağlantı noktaları veya protokoller altyapınıza bağlı olacaktır fakat şunlardan bazılarını veya tümünü içerebilir ; Sıfır Dokunuşla Sağlama. BootP Hizmeti. IPv6. Yankı , atma ve ücretlendirme için UDP desteği. Tüm şifrelenmemiş yönetim protokolleri (http , Telnet , FTP , TFTP , SNMPv2c vb.). Kullanılmayan şifreli yönetim protokolleri (HTTPS).

Güvenlik konusunda daha bilinçli kuruluşlar ve savunma kurumları için genelde gözetim organları tarafından ek sertleştirme önerilir ; ICMP. Keşif protokolleri (LLDP ve CDP gibi). Echo , atma ve ücretlendirme için TCP ve UPD desteği. IP kaynak yönlendirmesi. Kullanılmayan IP yönlendirme protokolleri (özellikle kontrol cihazına / kontrol cihazından). ARP proksisi. Fiziksel bağlantı noktaları kullanımda olmaması. Bazı protokollerin (ICMP , CDP / LLDP , Echo gibi) devre dışı bırakılması ağ izleme ve yönetim araçlarını bozabilir. Daha aşırı sertleşmeyi izlemeyi planlıyorsanız , kuruluşun ayrıntılı belgeler , onaylar , varlık envanteri ve sıkı değişiklik yönetimi dahil olmak üzere bunu destekleyecek uygun süreçlere ve politikalara sahip olduğundan emin olunuz. Kullanılmayan protokolleri devre dışı bırakmak , en az ayrıcalık için NIST SP 800-53 Yapılandırma Yönetimi (CM) paketinde ayrıntılı olarak açıklanan kontrollerin bir parçasıdır.

Eşler Arası ve Köprülü İletişimleri Kontrol Etme ; İstemci trafiğini kısıtlamak , geleneksel altyapı güçlendirmesinin sınırına düşse de ilgili ve güncel bir konu olmaya devam etmektedir.

Ağdaki riskli trafiği ve davranışı ortadan kaldırarak veya azaltarak bütünlüğü desteklemek için birkaç özel yönteme yani sertleştirme görevlerine göz gezdirecek olursak ; Geçici ağları engelleme. İstemcilerde kablosuz köprülemeyi engelleme. İstasyonlar arası trafiği , çok noktaya yayını ve mDNS'yi filtreleme.

Ev ağları ve kişisel kullanım için tasarlanan cihazlar , hiçbir zaman kurumsal bir ortamda ve kesinlikle güvenli ağ altyapısında kullanılmak üzere tasarlanmamıştır. Tanım olarak ; DNS , DHCP ve kimlik doğrulama sunucuları gibi resmi ağ hizmetlerinin yokluğunda çalışmak üzere oluşturulmuşlardır. Tüketici ve kişisel cihazların güvenli kurumsal altyapı içinde yeri yoktur. İzin verilmesi önerilmeyen tüketici ve ev cihazları şöyledir ; Ticari kullanım için tasarlanmamış aydınlatma , sensörler , kameralar dahil ev otomasyon ürünleri. Aşırı güvenlik ve gizlilik riskleri getiren Amazon Echo paketi , Google Home ve Apple HomePod gibi ses destekli cihazlar.

İdeal alternatif , kuruluşun bağlantı ve güvenlik gereksinimlerini karşılayan benzer teknolojinin ticari düzeyde versiyonunu aramaktır. Bu cihazlar kesinlikle herhangi bir nedenle ortam içinde kullanılması gerekiyorsa , kurumsal cihazlarla değil , özel kablosuz ağ üzerinde olmalıdırlar. Birçok profesyonel ve teknik olmayan yönetici , IoT cihazlarından oluşan hiper bağlantılı ekosisteminden kaynaklanan risklerden korkmaktadır. Ağdaki tüketici cihazları ve protokolleri , karşı karşıya olduğumuz en büyük risklerden biridir. Saldırganların ağa kolay erişmesine izin veriyorlar ve çoğu IoT uygulamasının aksine , bu tüketici cihazları , kullanımın doğası gereği , çoğunlukla akıllı telefonlarımıza , tabletlerimize , dizüstü bilgisayarlarımıza ve yazıcılarımıza bağlanmaktadır. Onları etkileşime girmeleri gereken uç noktalardan izole etmek mümkün değildir. Bir çalışanın uygun bulduğu veya müzik dinlemek istediği için Apple HomePod'a izin vermek , ağı artan riske maruz bırakmak için kesinlikle geçerli bir neden değildir. Kuruluşunuzun ağdaki tüketici ve kişisel cihazlara yönelik politikası yoksa , bu bir öncelik olmalıdır. Bu cihazları ve riskli protokolleri tanımlamaya , bulmaya , engellemeye yönelik araçlar , Wi-Fi ürünlerinde kolayca bulunur. Tüketici düzeyinde protokoller (Bonjour gibi) kullanabilen ancak kurumsal ortamlarda meşru kullanım durumları olan diğer cihazlar şunları içerir ; Dijital TV ve ekran yayını. Belirli kablosuz yazdırma uygulamaları.

Geçici Ağları Engelleme ; Eş kablosuz cihazların birbirleriyle iletişim kurmasının birkaç yolu vardır; ikisi ; Kurumsal AP aracılığıyla akran iletişimi. Geçici ağda eş iletişim.

Burada endişe verici olan ikincisi ad-hoc ağlardır. Geçici ağlarla , uç noktalar doğrudan , kablosuz olarak ve kontrol ettiğiniz , görebildiğiniz altyapının herhangi bir bölümü aracılığıyla iletişim kurar. Görünürlük eksikliği , güvenlik açıklarına neden olarak kuruluşun veri yolunu uygun şekilde kontrol etmesini ve güvenliğini sağlamasını engeller. Geçici ağlar , kurumsal Wi-Fi sistemi aracılığıyla gerçekleştirilmediğinden tam olarak bu şekilde kontrol edilemezler. Geçici ağları belirlemek ve önlemek için yapabileceğiniz eylemler ; Geçici ağları destekleyen aygıtlarda kablosuz arabirimleri devre dışı bırakınız. Uç noktalarda geçici ağ desteğini devre dışı bırakınız. Kurumsal Wi-Fi'yi , geçici ağlar için havayı izlemek ve mevcudiyetleri konusunda uyarmak üzere yapılandırınız.

İstemcilerde Kablosuz Köprülemeyi Engelleme ; Uç nokta yapılandırmasını içeren ve kurumsal Wi-Fi tarafından kontrol edilmeyen başka bir işlev de kablosuz arabirimin diğer ağ arabirimlerine (kablolu arabirim gibi) bağlanmasıdır. Geçici ağ oluşturma da olduğu gibi , iyileştirme eylemleri benzerdir ; Uç noktalarda arayüz köprülemeyi devre dışı bırakınız. Köprülemenin etkin olup olmadığını uyarmak için uç nokta güvenliğini veya uç nokta algılama yanıt araçlarını yapılandırınız. Kurumsal Wi-Fi'yi , köprülü istemciler için ağları izlemek ve varlıkları konusunda uyarmak üzere yapılandırınız.

Arayüz köprüleme , paylaşım istemcisi tarafından sunulan geçici ağ ile diğer uç noktalara hizmet vermek için de genişletilebilir.

AWDL ile güvenli ağdan yararlanma ; Bazı özel açıklardan yararlanmayla ilgileniyorsanız , Apple AWDL aracılığıyla gerçekten hava boşluklu ağdan kaçabilirsiniz.

İstasyonlar Arası Trafiği , Çok Noktaya Yayını ve mDNS'yi Filtreleme ; Kurumsal Wi-Fi sisteminden geçen eş trafik için filtreleme ve güvenlik kontrollerini kapsamaktadır. Wi-Fi üzerinden istemciden istemciye etkileşimler , standart 2. katman bitişikliği (tıpkı anahtardaki aynı VLAN üzerindeki iki uç nokta gibi) veya mDNS , Link- gibi eş tabanlı çok noktaya yayın ve yayın protokolleri aracılığıyla gerçekleşebilir.

SSID İstasyonlar Arası Engelleme ; İstasyonlar arası engellemenin farklı adları vardır fakat satıcı uygulamasında , aynı SSID'deki kablosuz istemcilerin birbirleriyle doğrudan iletişim kurmasını engellemenin faydasıdır. Anahtardaki aynı VLAN içindeki iki kablolu uç nokta arasındaki trafiği engellemeye benzer. İstasyonlar arası engelleme , uç noktaların asla birbirleriyle konuşamayacağı anlamına gelmez. İstemcileri , kuralların uygulanabileceği ve trafiğin değerlendirilebileceği , izin verileceği veya engellenebileceği işlenecek AP veya denetleyiciden geçmeye zorlar. Uzun zaman önce istasyonlar arası engellemeyi etkinleştirmek , Wi-Fi dağıtımı için fiili bir durumdu. Kontrolsüz tüketicileştirme ve ev kullanımı protokollerinin kurumsal ağa dahil edilmesi , endüstrinin varsayılan olarak eş iletişimini değiştirmesine ve etkinleştirmesine neden oldu. O zamandan beri daha ayrıntılı kontroller eklendi. Tüketici teknolojisi bir yana , çoğunlukla , güvenli kurumsal ortamlar , doğrudan akran istemci iletişimine ihtiyaç duymamalı ve buna izin vermemelidir. Bunu gerektiren bir durum varsa , Wi-Fi altyapısı içinde açıkça bir izin verme politikası uygulanabilir. Örtülü güvenin kaldırılması ve yanal hareketin sınırlandırılması gereken fidye yazılımı ve sıfır güven girişimlerinin hararetinde özellikle kritik bir kontroldür.

Juniper Mist platformunda istasyonlar arası engelleme , çok noktaya yayın filtreleme ve Bonjour ağ geçidi seçeneklerin bulunmaktadır. Aruba denetleyicileri ve Aruba Central bulutu iki benzer seçeneğe sahiptir. VLAN İçi Trafiğini Reddet seçeneği , aynı ağdaki uç noktalar arasındaki hem 2. katman hem de 3. Katman trafiğini engeller. Kullanıcı Arası Köprülemeyi Reddet , ARP dahil aynı ağdaki uç noktalar arasındaki IP olmayan (2. katman) trafiği engeller.

İstasyonlar Arası Bloklama ; Juniper Mist bu özelliği eş izolasyon olarak ifade eder ve SSID'de yapılandırılır. Cisco denetleyici mimarisinde , eşler arası engelleme olarak yapılandırılır ve SSID'ye göre uygulanır. Aruba Networks , ayarı kullanıcılar arası trafiği reddet olarak ifade eder ve global olarak denetleyici içinde veya SSID başına uygulanabilir.

Eş Tabanlı Sıfır Yapılandırma Ağı ; Aple'ın Bonjour , mDNS ve diğer sıfır konfigürasyonlu ağ mekanizmaları gibi eş tabanlı çok noktaya yayın protokolleri vardır. Zeroconf ağ iletişimi , TCP / IP'ye dayalı ancak DHCP ve DNS gibi standart kurumsal etki alanı hizmetlerinin yokluğunda çalışmak üzere tasarlanmış protokoller paketini tanımlar. Bunlar en iyi , eş tabanlı kendi kendini organize eden ağlar olarak düşünülür. Zeroconf işlemlerinin bir kısmı şunları içerir ; Yerel bağlantı adresleme , DHCP'den istemci IP adresleriyle çalışan veya bunların yerini alan otomatik adres yapılandırması (Otomatik Özel IP Adresleme). Kurumsal DNS girişleri yerine host bilgisayar adının uç noktadan kendi kendini tanımlaması. Yetkili DNS sunucusuna karşı ağdaki tüm erişilebilir sıfır konf eşlerine çok noktaya yayın kullanan mDNS gibi eş adı hizmeti çözümlemesi. UPnP'de DNS-SD ve SSDP gibi DNS tabanlı hizmet keşfi. Evrensel Tak ve Çalıştır (UPnP) protokolleri.

Eş bulma ve iletişim için Bonjour hizmetlerini , zeroconf ve mDNS'yi kullanan teknolojilerin bir örneği ; Amazon TV. Google ChromeCast. Roku Medya Oynatıcı Çeşitli yazdırma uygulamaları. Phillips Hue Işıkları. Yayın. Apple TV. AirServer Yansıtma. Apple AirTunes. Apple AirPrint. Apple Dosya Paylaşımı. Apple iTunes.

Kurumsal ağda sıfır konf protokollerini destekleyen zorluklar iki yönlüdür ; Hafifletme için çok az veya hiç seçeneği olmayan ağ ve uç noktalar için çok yüksek düzeyde risk oluştururlar. Kurumsal ağlarda yaygın ve önerilen mimaride olduğu gibi , IP alt ağlarında değil , 2. katman bitişik ağlarda çalışmak üzere tasarlanmıştır.

Daha sonraki önerilerde Link-Local Multicast Name Resolution (LLMNR) referans alınacaktır. mDNS'ye benzer Windows protokolüydü fakat mDNS , IETF RFC olarak onaylandı ve Windows , mDNS'yi desteklediğinden , LLMNR'nin kullanılmaması muhtemeldir. Ortamda varsa , mDNS ve Bonjour ile aynı şekilde yönetilmelidir. Bu protokoller , kurumsal ağlarda kullanılmak üzere hiçbir zaman tasarlanmamıştır.

Bonjour ve mDNS Protokollerini Devre Dışı Bırakma ve Filtreleme ; mDNS , riskli bir protokoldür. Zeroconf protokolleri eş tabanlıdır ve herhangi bir kimlik doğrulama veya yetkili kaynak içermez. Kurumsal hizmetleri atlarlar ve genellikle izleme araçları tarafından görünmez veya rapor edilmezler.

Bonjour ve mDNS üzerinden ağlara ve uç noktalara yapılan saldırılar sayısızdır. Bu teknolojilerle ilgili güvenlik konuları şunları içerir ; mDNS paketleri , hedeflerin açık bağlantı noktası bilgilerini paylaşarak , güvenlik açığı taraması ve saldırı bulma araçlarıyla aynı düzeyde güvenlik ayrıntıları sağlar. mDNS tam dizin ve dosya yapılarını da gösterebilir. mDNS ve zeroconf protokolleri , kimlik doğrulama biçimi içermez. Eş cihazı veya hizmeti yanıltmayı ve hassas bilgileri toplamayı , uç noktaya kötü amaçlı yükleri göndermeyi kolaylaştırır. Bonjour ve mDNS , DNS , DHCP dahil olmak üzere kurumsal etki alanı hizmetlerini atlar. Varsayılan Bonjour davranışı , genellikle (çok noktaya yayın yoluyla) host bilgisayar adını cihaz sahibinin adı ve soyadı olarak paylaşarak birçok hükümet düzenlemesine göre PII (kişisel olarak tanımlanabilir bilgiler) olarak sınıflandırılan bilgiler de dahil olmak üzere kullanıcının kimliğini açığa çıkarır. IETF RFC belirtimine göre , kuruluşu mDNS'ye karşı tam olarak güvence altına almak , kuruluş içinde kimliği doğrulanmış ve şifrelenmiş DNS protokollerine geçiş dahil olmak üzere kuruluş ortamında kapsamlı değişiklikler yapılmasını gerektirir. Bazı durumlarda saldırgan meşru trafiği ele geçirebilir veya yanıltabilir , kullanıcıları kötü niyetli web sitelerine ve yüklere yönlendirebilir. Çok noktaya yayın doğası nedeniyle , mDNS ; büyük ağlarda yüzlerce hatta binlerce cihazdan gelen çok noktaya yayın trafiğiyle dolup taşan gereksiz hacimlerde trafik oluşturur. Bonjour , cihazlar arasında görünürlük , güvenlik denetimi veya kontrol olmaksızın eşler arası iletişime izin vererek ek güvenlik açıkları sunar. mDNS , istenen davranış bu olsa da olmasa da tüm yapılandırılmamış ve açık yerel alan adlarını otomatik olarak çözer.

Bonjour ve mDNS söz konusu olduğunda bilgi güvenliği topluluğu adım adım ilerlemektedir. Güvenli kurumsal ağlar için uygun değildir. Apple dahil hemen hemen her üreticinin sağlamlaştırma kılavuzları , Bonjour'un uç noktalarda devre dışı bırakılmasını ve ağda filtrelenmesini önerir. NIST SP 800-179 , " Bonjour çok noktaya yayın reklamları , Bağımsız dışındaki tüm ortamlarda devre dışı bırakılmalıdır " açıkça belirtir. Trustwave'in SpiderLabs güvenlik ekibi , mDNS'nin uç noktanın açık bağlantı noktalarının durumunu (tüm eşlere , şifrelenmemiş) çok noktaya yayınladığını gösterdi.

mDNS için IETF RFC'de yer alan güvenlik hususlarından alıntılar şunları içerir ;

“ İşbirliği yapan bir grup katılımcının olduğu ancak müşterilerin aynı fiziksel bağlantı üzerinde hiçbir host bilgisayar olmadığından emin olamadığı ortamda , işbirliği yapan katılımcıların IPsec imzalarını veya DNSSEC [RFC4033] imzalarını kullanmaları gerekir. Çok noktaya yayın DNS mesajlarını güvenilir katılımcılardan çok noktaya yayın DNS mesajlarından güvenilmeyen katılımcılardan ayırt edebilirler.”

“ Global DNS adları için DNS sorguları mDNS çok noktaya yayın adresine gönderilirse DNSSEC kullanmak özellikle önemlidir çünkü kullanıcı , gerçek host bilgisayarla iletişim kurarken , aslında yalnızca bu ad gibi görünen bazı yerel host bilgisayarlarla gerçekten iletişim kurar. ' .local. ' ile biten adlar için daha az kritiktir çünkü kullanıcı bu adların yalnızca yerel öneme sahip olduğunun ve hiçbir küresel otoritenin ima edilmediğinin farkında olmalıdır.”

“Çoğu bilgisayar kullanıcısı, tam nitelikli alan adının sonundaki noktayı yazmayı ihmal eder. Bu da onu göreceli alan adı yapar. Ağ kesintisi durumunda , girilen adı olumlu şekilde çözme girişimleri başarısız olur ve varsa ".local." dahil arama listesinin uygulanmasına neden olur. Kötü niyetli host bilgisayar , "www.xxx.com" gibi görünebilir. Com.local önlemek için host bilgisayar , varsa , iki veya daha fazla etiket içeren göreli (kısmen nitelenmiş) host bilgisayar adına ".local." arama son ekini eklememelidir.

UPnP Protokollerini Devre Dışı Bırakma ve Filtreleme ; uPnP ; protokol yalnızca bazı otomatik keşif işlevlerini yerine getirmekle kalmaz aynı zamanda güvenlik duvarlarını yeniden yapılandırma, gelen delikleri açma ve aşırı güvenlik riski oluşturma özgürlüğünü de alır. 2016'da büyük Mirai botnet saldırısına yol açan kapıları açan da UPnP oldu. UPnP tarafından açılan delikler aracılığıyla ağların içindeki cihazlara bağlanarak ve ticari cihazlar için yalnızca küçük varsayılan kullanıcı adı ve şifre listesi kullanarak Mirai virüs bulaştı. “ CallStranger ” adlı geri arama güvenlik açığı , bir saldırganın veri hırsızlığı ve DDoS saldırıları dahil olmak üzere çeşitli saldırılar gerçekleştirmesine olanak tanır. Bu yeni değildir ve yıllar önce düzeltme yayınlandı ancak araştırmacılar , UPnP çalıştıran birçok cihaz kolayca veya sıklıkla yükseltilmediğinden CallStranger'ın önümüzdeki yıllarda bir tehdit olarak kalmasını bekliyor. UPnP için öneri basittir ve hiçbir koşulda ağlarda etkinleştirilmemelidir. Belirli eylemler şunları içerir ; Tüketici internet yönlendiricileri veya güvenlik duvarları kullanan ev ve küçük ofislerde , yönetim yapılandırmasına erişin ve UPnP'yi devre dışı bırakın. Kurumsal ortamlarda , tüketici yönlendiricilerine ilkeye göre izin verme , bunları tanımlamak için izleme kontrolleri uygula. IoT uç nokta cihazlarında ve ağ geçidi sistemlerinde varsayılan şifreleri değiştiriniz.

Pentest Cihazından mDNS ve Zeroconf İle İlgili Mesaj ; Hem mDNS hem de zeroconf'un şirket ağlarında olması asla amaçlanmamıştır. Kelimenin tam anlamıyla , dahili ad sunucusuna veya ağ hizmetlerini yapılandırma yeteneğine sahip BT ekibine sahip olmayan daha küçük ağlar için tasarlanmıştır. mDNS , LLMNR ve NetBIOS adlarından gelen istekleri dinleyerek istekte bulunana saldırı makinemizin aradığı sistem olduğunu söyleyen sahte yanıtları dinler. Kurbanı bizim aracılığımızla bağlantı kurmaya zorlayarak trafiğin ortasındaki adam olmamıza izin verir. Zeroconf , sıfır güvenin tam tersi gözükmektedir ; İlkin ağa güvenmeye ve ağdaki herhangi birinin sağladığı her şeyi kabul etmeye odaklanmıştır. İkincisi ise ağa veya üzerindeki herhangi birine güvenemeyeceğiniz varsayımına göre tasarlanmıştır.

Zeroconf Networking'e Karşı Güvenliğe Yönelik Öneriler ; Yüksek güvenlikli ortamlarda , zeroconf protokolleri tamamen devre dışı bırakılmalı ve sıkı şekilde uygulanmalıdır. Bu görevler şunları içermektedir ; Bonjour , mDNS , LLMNR ve UPnP dahil olmak üzere uç noktalarda tüm zeroconf protokolü desteğini devre dışı bırakınız. Ağdaki Bonjour dahil tüm mDNS ve zeroconf trafiğini izleyin ve filtreleyin / engelleyiniz. Uç nokta güvenlik uygulamalarını veya uç nokta algılama ve yanıtını (EDR) kullanarak uç noktada zeroconf protokollerini izleyin ve kısıtlayınız. Bu kılavuzu yansıtmak için kurumsal ve kabul edilebilir kullanım ilkeleri oluşturun veya güncelleyiniz. Duruşu doğrulamak için değerlendirmeleri ve penetrasyon testlerini kullanınız.

Ağ üzerinde sıfır konf protokollerine izin verme riskini kabul etmeye hazır olan kuruluşlar için (tüm sıkılaştırma ve güvenlik yönlendirmelerine karşı) öneriler şöyledir ; Cihazlarda UPnP'yi devre dışı bırakın ve ilkeye göre UPnP'ye izin vermeyiniz. UPnP trafiğini izleyin ve filtreleyin / engelleyiniz. Kuruluş tarafından yönetilen uç noktaların zeroconf ağına katılmasına izin vermeyin ve bu cihazlarda Bonjour'u devre dışı bırakınız. Politika tarafından izin veriliyorsa , Bonjour ve mDNS'ye sadece internet veya kişisel cihaz kullanımı için belirlenmiş ağlarda (misafir ağları veya konut salonları gibi) izin verin ve bu ağları kuruluş tarafından yönetilen güvenli ağlardan uygun şekilde bölümlere ayırınız. mDNS için en azından tüm uç noktalarda / cihazlarda mDNS reklamlarını devre dışı bırakınız. Bu kılavuzu yansıtmak için kurumsal ve kabul edilebilir kullanım ilkeleri oluşturun veya güncelleyiniz. Güvenli ağların duruşunu doğrulamak için değerlendirmeleri ve sızma testlerini kullanınız.

mDNS ve zeroconf ağ protokolleri ile ilgili sorunlar , güvenlik araştırmacıları ve pentest’çiler tarafından yapılan çok sayıda açıktan yararlanma raporu , bunların kurumsal kullanım için tasarlanmadığına dair IETF RFC kılavuzu ve teknoloji üreticileri (Apple dahil) tarafından açık kılavuzluk ile iyi bir şekilde belgelenmiştir. NIST , bu protokolleri güvenli kurumsal ortamlarda devre dışı bırakmak için önerilerde bulunmaktadır. Teknik profesyonellerin bu veri hacmiyle daha fazla donanmış bilgilere sahip olmalarını ve liderlerine Bonjour ve mDNS ile ilişkili risk düzeyine dair sağlam kanıtlarla yaklaşabilmeleri gerekmektedir.

Katmanlı Sertleştirme için En İyi Uygulamalar ; Diğer en iyi uygulamalarda olduğu gibi , her zaman istisnalar ve aykırı değerler olacaktır. Gerçek en iyi uygulamanın her yerde uygulanabilir olduğu iddia edilebilirken , gerçek şu ki kuruluşların sahip oldukları kaynaklarla çalışması gerekmektedir.

Düşük Güvenlikli Ortamlar ; Düşük güvenlikli ortamlar , laboratuvarlar ve kavram kanıtı (PoC) dağıtımları için bile minimum yapılandırmayı içerir. Bu katman , aynı zamanda çok sayıda BT kaynağı veya geniş bir ayak izi olmayan küçük bir kuruluş için de uygundur.

Orta Güvenlikli Ortamlar ; Orta düzeyde güvenlikli ortam kontrolleri , sağlık ve finans gibi orta düzeyde düzenlenmiş endüstriler dahil olmak üzere olgun ve güvenlik bilincine sahip kuruluşlar için temel olduğunu düşündüğüm şeylerdir.

Yüksek Güvenlikli Ortamlar ; Yüksek güvenlikli ortamlar , istisnai olarak kilitlenmiş ortam için gereksinimleri ifade eder. Bu kontrollerin çoğu , federal hükümetler ve savunma kurumlarının sertleştirme gereksinimlerinde belirtilmiştir.

Kuruluşunuz veya ortamınız bu üç katman arasında yer alabilir veyahut benzersiz koşullara sahip olabilir. Katmanların her biri bir öncekinin üzerine kuruludur yani düşük güvenlikli ortamlar için kontrol taslağı orta katman tarafından takip edilmeli veya bunun üzerine inşa edilmelidir. Aynısı orta ila yüksek düzeydedir.

Yönetim Erişiminin Güvenliğini Sağlama ;

Düşük (Minumum yapılandırma); Şifrelenmiş yönetim protokollerini zorunlu kıl , Varsayılan Parolaları Kaldır , Kullanıcı Tabanlı Oturum Açmaları Zorla , Güvenli Parolaları Zorla , Uzaktan Erişim için MFA'yı Zorla.

Orta ; Yönetim VLAN'ı Oluşturun, Paylaşılan Kimlik Bilgilerini ve Anahtarları Güvenlileştirin, Temel Ayrıcalıklı Erişim Yönetimini Kullanın, Eşzamanlı Oturum Zaman Aşımlarını Ayarlayın, Yönetici Erişimini ve Girişimlerini İzleyin ve Uyarı.

Yüksek ; İzin Verilen Yönetim Ağlarını Tanımlayın , FIPS Modunu Etkinleştirin , Gelişmiş Ayrıcalıklı Erişim Yönetimini Kullanın , Oturum Açma Başlıklarını Uygulayın , Tüm Yönetici Erişimi için MFA'yı Uygulayın.

Ek Güvenlik Yapılandırmaları ; En temel uyumluluk çerçevelerini karşılamaya ve sızma test cihazlarının , kötü niyetli kullanıcıların ağlara erişmek için yararlandıkları güvenlik açıklarını çözmeye yönelik faaliyetleri vurgulanmıştır. Değinilmesi gereken birkaç uç nokta da şöyledir ; Güvenlik İzleme , Rogue Detection ve WIPS. SSID'leri Gizlemeye veya Gizlemeye İlişkin Hususlar. İstemciler için DHCP Gerektirme. İstemci Kimlik Bilgileri Paylaşımını ve Taşımayı Ele Alma.

Entegre Dizayn ;

Düşük (Minumum yapılandırma); Yapılandırmaları Yedekleyin, Düzenli Güvenlik Düzeltme Eki Planlayın , Kuruluşun Sahip Olduğu AP'leri Onaylayın veya Beyaz Listeye Alın , AP'lerin Varsayılan Davranışını Kontrol Edin. Fiziksel Olarak Güvenli veya MAB'den Mantıksal Olarak Güvenli AP tasarımı (Genel Alanlardaki Bağlantı Noktaları / Kablolar) , Ağ Dolaplarını ve Veri Merkezi Odalarını Kilitleyin , IPv6'yı Devre Dışı Bırak, BootP (kullanılmıyorsa).

Orta ; Temel Değişiklik Yönetimi İşlemlerini , Belge Yapılandırmalarını , Yapılandırma Değişikliklerinde Uyarı , Güvenlik Açığı Yönetim Programını Uygulama , Kimlik Doğrulama için AP'lere Sertifika Verme , AP'yi Mantıksal Olarak Güvenli Hale Getirmek için 802.1x ve MAV kullanın (Genel Alanlardaki Bağlantı Noktaları / Kablolar) , Ağa Kimlik Tabanlı Erişimi Zorunlu Kılın Dolaplar ve Veri Merkezleri , Denetleyicide Ön Panel Güvenliğini Yapılandırma , Kullanılmayan (HTTP) Yönetim Protokollerini Devre Dışı Bırakma , Kullanılmayan bağlantı noktalarını yalnızca internete veya black hole VLAN'ına manuel olarak veya NAC ürünü ile atama.

Yüksek ; Gelişmiş Değişiklik Yönetimi Süreçlerini Uygulayın , Yapılandırma temellerini oluşturun , yazılım bütünlüğünü doğrulayın , el değmeden yetkilendirmeyi devre dışı bırakın , Kablo üzerinden Şifreleme için AP'lerde sertifika kullanın , Tüm AP Bağlantı Noktalarını mantıksal olarak Güvenli hale getirmek için 802.1x kullanın , Tüm tesisler için sıkı erişim kontrolünü zorunlu kılın , Tüm kullanılmayanları devre dışı bırakın parola kurtarma ve AP konsolu / USB Bağlantı Noktaları dahil yönetim erişimini kontrol edin , uygulamanın kullanılmayan protokollerini (icmp , echo , ip kaynağı , yönlendirme , arp proksi) devre dışı bırakma ve ayrıca kullanılmayan fiziksel bağlantı noktalarını devre dışı bırakma , kullanılmayan bağlantı noktalarını bir kara delik vlan'a devre dışı bırakma veya atama.

Eşler Arası ve Köprülü İletişimin Kontrolü ;

Düşük (Minumum yapılandırma) ; Ağdaki tüketici cihazlarının kullanımını izleyin , tüm ssid'lerde istasyonlar arası engellemeyi etkinleştirin , mdns'yi devre dışı bırakın , uç noktalarda reklamları " advertisements " devre dışı bırakın , unpnp'yi devre dışı bırakın.

Orta ; Onaylanmış ağlarda Tüketici Cihazlarının kullanımını kısıtlayın / yönetin , kuruluşa ait cihazlara sahip ağlarda mdns ve bonjour desteğini devre dışı bırakın , kuruluş yönetimi uç noktalarında destek mdns ve Bonjour'u devre dışı bırakın, upnp'li cihazlara izin vermeyin.

Yüksek ; ağlarda tüketici cihazlarını reddet , uç noktalarda arayüz köprülemeyi devre dışı bırak , ek uç nokta ve ağ sağlamlaştırma kılavuzunu takip et.

Güvenlik İzleme , Hileli Algılama ve WIPS ; Her güvenli mimari , güvenlik izleme , uyarı ve raporlama gerektirmektedir. Kablosuz ağlar istisna değildir. Kablosuz erişim ortamı sayesinde , kablosuz muhtemelen diğer sistemlerden daha yüksek derecede bir izleme gerektirir.

SSID'leri Gizlemeye veya Gizlemeye İlişkin Hususlar ; Konu Wi-Fi SSID'lerini gizlemeye gelince , 802.11 WLAN protokollerini tam olarak anlamayan güvenlik meraklıları tarafından internette bazı yetersiz tavsiyeler verilmektedir. Konut ve kurumsal Wi-Fi ürünlerinde , SSID yayınlamama , SSID gizleme , SSID gizlemeyi etkinleştirme seçeneği genelde mevcuttur. Bu ayarın tek yaptığı , AP'ye yalnızca SSID'nin açık adını içerdiğinde 802.11 araştırma isteğini yanıtlamasını söylemektir. Aksi takdirde , varsayılan davranış , AP'nin işaretçilerinin SSID adını içermesidir. İşlevsel olarak , SSID adı , kullanıcının kullanılabilir ağlar listesinde gördüğü addır. SSID gizliyse , işaret hala mevcuttur. Sadece ağ adını içermezler. Saldırgana karşı sıfır ek güvenlik sağlar ve kuruluşun duvarlarının dışında kullanılabilecek mobil uç noktalara ek güvenlik açıkları getirir. Meşru bir istemcinin gizli SSID'ye bağlanması gerektiğinde , dünyaya kimi aradığını duyurmak zorunda kalır.

Uç noktalar , gizli ağlara bağlanacak şekilde yapılandırılabilir. Ağ adı girilmelidir ve çoğu platformda büyük / küçük harf duyarlıdır.

SSID'yi gizlemenin , istemciler için kullanılabilirlik ve bağlanabilirlik üzerinde başka etkileri vardır ve dikkate alınması gerekenlerin tam listesi şöyledir ; SSID'yi gizlemek sadece ağ adını işaretçilerden kaldırır , saldırgan , temel saldırılarla SSID adını kolayca alabilir. Apple iOS aygıtları da dahil olmak üzere birçok istemcinin ilişkilendirme sürecinde ek gecikmeye neden olur. Diğer cihazlar güvenilmez davranıyor veya gizli SSID'lere hiç bağlanamıyor. SSID'leri gizlemek , gürültüyü veya havadaki trafiği azaltmaz. Kuruluşun dışında kurumsal SSID'yi aktif olarak araştıran mobil istemciler tarafından ek risk ortaya çıkar.

Bir veya daha fazla SSID'yi gizlemenin mantıklı olduğu bazı durumlar vardır. Öncelikle , kuruluşun fiziksel sınırları içinde kalan uç noktalara hizmet eden ağlar için karmaşık ortamda anlamlıdır.

Bu nedenle , SSID'yi gizlemek için en iyi uygulamalar şöyledir ; Kuruluşun fiziksel sınırları dışında seyahat eden mobil istemcilere hizmet veren ağlar için SSID'leri gizlemeyiniz. Fiziksel olarak kuruluşun sınırları içinde kalan uç noktalara hizmet eden ve kullanıcılardan bağlantı girişimini veya kazara bağlanmayı önlemek için gizlenmesi tercih edilen ağlar için SSID'leri gizleyiniz. Güvenlik mekanizması olarak SSID'leri gizlemeyiniz.

SSID'leri gizlemenin iki yaygın kullanım durumu arasında hastaneler ve imalat yerleri yer alır. Hastanelerde , klinik sistemler için binada kalan ve insan müdahalesiyle bağlanmayan bir veya daha fazla ağa sahiptir. Ağı içinden seçmesi gereken dizüstü bilgisayarı olan kullanıcı değil , önceden sağlanan IoT tipi bir cihazdır. Depo , imalat ve perakendede de gizlenebilecek çeşitli el tipi tarayıcılar , iletişim cihazları ve envanter yönetim sistemleri bulunur. Juniper Mist ve Aruba'da SSID'leri gizlemeye yönelik ayar örneklerini inceleyebilirsiniz.

Ağı Devre Dışı Bırak ayarı , SSID'nin etkin olmasını durdururken , gizleme ayarı yalnızca adı istemci görünümünden kaldırır.

İstemciler için DHCP Gerektirme ; Göz önünde bulundurulması gereken basit bir kontrol ise istemciler için DHCP gerektirmesidir. Günümüzde birçok ağ güvenliği ve profil oluşturma aracı , DHCP trafiğini (IP yardımcıları , ağ bağlantı noktaları , yayılma / yansıtma bağlantı noktaları aracılığıyla) görebilmeye güveniyor ve bunun tersine , DHCP'yi bozmak , saldırganın ağlara yetkisiz erişim elde etmesinin bir yoludur. Çoğu Wi-Fi ürünü , istemcileri DHCP kullanmaya zorlamak için ayar sunar ve kasıtlı olarak statik olarak yapılandırılmış istemcilere hizmet vermeyen ağlar için harika bir seçenektir. DHCP'nin istenmesi , yanlış yapılandırılmış uç noktalardan erişimin önlenmesine yardımcı olarak istemci bağlandığında kaynaklara erişmek için uygun ağ parametrelerine (IP adresi , ağ geçidi ve DNS sunucuları) sahip olmasını sağlar. Buradaki büyük uyarı , statik olarak yapılandırılmış IP adreslerine sahip birçok uç noktanın hala mevcut olmasıdır. Geleneksel uç noktalarda daha az yaygındır ve daha çok IoT cihazlarında veya üçüncü bir tarafça yönetilen geleneksel olmayan IP cihazlarında görülür. Sağlık ağlarında hemen hemen her zaman statik IP'lere sahip klinik cihaz alt kümesi vardır ve hastanenin , bunu değiştirmek için cihazlara ilişkin görüş veya yönetim erişimi olmayabilir. Mümkün olduğunda , tüm ağlar adresleme için DHCP'ye güvenmelidir. Statik bir IP gerekiyorsa , sunucuda DHCP rezervasyonu kullanmak en uygun yaklaşımdır.

İstemci Kimlik Bilgileri Paylaşımını ve Taşımayı Ele Alma ; Wi-Fi'nin en önemli güvenlik açıkları bulunmuştur ; segmentasyon , Bonjour ve diğer sıfır konf protokolleri , istemcilerden kimlik bilgilerinin taşınması ile sağlamlaştırma eksikliği , uç noktalar arasında kimlik bilgisi paylaşımına yönelik saldırılardır. Birçoğu iPhone , iPad ve iPod cihazlarında bulunan Apple Share Network Password işlevinden özel olarak bahseder. Bu seçenekle , ağ için parolaya (WPA2-Kişisel veya WPA3-Kişisel) sahip herhangi iOS kullanıcısı bunu başka iOS kullanıcısına kolayca taşıyabilir. Altyapı açısından , bunu önlemek ve izlemek için yapabileceğiniz hiçbir şey yoktur ; eş cihazlar , izlenmesi muhtemel olmayan Wi-Fi veya Bluetooth üzerinden iletişim kuruyor olabilir. Bu sadece Apple'a özgü bir sorun da değildir. Birçok platform , bir tür parola paylaşımı içerir. Android , kullanıcıların ekrandan taranabilen veya e-postayla gönderilebilen QR kodu aracılığıyla parola korumalı ağları paylaşmasına olanak tanır. Microsoft , genel erişim noktası parolalarını paylaşmak için tasarlanmış , çok tartışılan Wi-Fi Sense özelliğini tanıttığında da katıldı. Önerilen geçici çözümler ; mümkün olduğunda parola ağlarını kullanmamak veya yetkili uç noktalar için MAC adresi izin verilen listelerini etkinleştirmektir. MAC rastgeleleştirme gibi yeni satıcı gizlilik mekanizmaları , MAC adresi üzerinde filtreleme veya MAC Kimlik Doğrulama Baypas (MAB) ile 802.1X güvenli ağ kullanma girişimlerini daha da karmaşık hale getirir. Bu davranışı denetleme seçenekleri sınırlıdır ve güvenli ağ için denetimler , parola tabanlı (Kişisel) ağların kullanılmamasına dayanır. Tek kontrol bu olmakla birlikte , kimlik bilgisi paylaşımına karşı korunmaya yönelik ek notlar ve dikkate alınması gereken hususlar ; Cihazlar (Apple iOS gibi) farklı sahiplerin cihazları arasında paylaşımda bulunabilir. Cihazlar , ağ kimlik bilgilerini aynı sahibine ait diğer cihazlarla otomatik olarak eşitler (Apple için iCloud ve Android ve Microsoft için diğer eşitleme seçenekleri aracılığıyla). Ağ parolaları cihazlar arasında paylaşılıyorsa , kuruluşun bundan haberi olmayacaktır. Yönetilmeyen cihazlarda ağ parolası paylaşımını engellemenin bir yolu yoktur. Ağ parolası paylaşımı , Apple aygıtları için AirDrop ayarları aracılığıyla MDM'li şirket tarafından yönetilen aygıtlarda kontrol edilebilir. Ağ parolası paylaşımına karşı tek koruma , yönetilmeyen cihazlarla parola korumalı SSID'leri kullanmamaktır. Parola korumalı ağlar tam olarak bir kuruluşun kişisel ve BYOD aygıtları için tipik olarak kullanacağı şey olduğundan , son madde gerçekten önemlidir.