Revizyon İzleme Tablosu		
Rev. No	**Rev. Tarihi**	**Açıklama**
01	18.10.2022	Referanslar düzenlendi.

1. AMAÇ

Kurumumuzda VPN güvenliği için gerekli kuralları belirlemektir.

2. SORUMLULUKLAR

Bu talimatın uygulanmasından tüm VPN kullanıcıları sorumludur.

3. UYGULAMA

3.1. Fiziksel Güvenlik

- Cihaza fiziksel olarak erişebilen saldırgan cihazın kontrolünü rahatlıkla ele geçirebilir. Bu yüzden VPN cihazı, sadece yönetiminden sorumlu olan kişilerce erişilebilecek bir şekilde kilitlenerek veya başka bir şekilde güvenlik önlemi alınmış bir oda da bulundurulmalıdır. Cihazın manyetik kartla veya parmak iziyle girilebilen odalarda tutulması en güvenli yöntemdir.Güvenlik duvarı genel olarak internet hizmetleri için tasarlanmış hariç diğer tüm servislere erişimi reddedecek şekilde uygulanacaktır.
- Oda ayırmanın mümkün olmadığı yerlerde ise bu cihazlar özel kilitli dolaplarda tutulmalıdır.
- Kablolar tek tek etiketlenmeli ve kullanılmayan kablolar devre dışı bırakılmalıdır.
- Cihaz civarına güvenlik bilgileri (kullanıcı adı, şifre…) yapıştırılmamalı ve bu bilgiler gizli tutulmalıdır.
- Cihazı besleyen güç kaynağının bağlı olduğu prizin güvenliği de hizmetin sürekliliği açısından önemlidir. Bu yüzden güç kaynağının bağlı bulunduğu prizin fiziksel güvenliği de sağlanmış olmalıdır.
- Cihaza sürekli olarak güç sağlanabilmesi için UPS (Uninterupted Power Supply) kullanılmalıdır.
- Cihaza fiziksel olarak kimlerin ve ne zaman eriştiği gözlenmelidir.

3.2. Çalışma Koşulları

- Cihazın çalışması için gerekli havalandırma koşulları sağlanmalıdır. Özellikle cihazın bulunduğu oda da klima olması uygun çalışma sıcaklığını sağlamak açısından önemlidir.
- VPN cihazının bulunduğu odaya toz girmemeli ve toza neden olacak etkenler bulunmamalıdır.
- Cihazın bulunduğu oda da nem olmamalıdır

3.3. Kimlik Doğrulama

Bilgi Güvenliği politikaları Şifre Politikası uyarınca ilgili düzenlemeler bu politakaya göre yapılmalıdır.

3.4. Yetkilendirme

- Sistemde kayıtlı olan yapılandırma dosyası ile tanımlanan anahtarların tutulduğu dosyalara yetkisiz kişilerce erişim olmamalıdır. Bu dosyalara yönetici haricinde kişilerin erişimi olmamalıdır.
- Mümkün olduğunca az sayıda kullanıcı oluşturulmalıdır.
- Kullanıcılara işlerini yapabilecekleri en düşük seviyede yetki verilmelidir.
- Kullanıcıların genel bir kullanıcı adı ve parolayla sisteme girişine izin verilmemelidir.
- Yetkilendirme yapıldıktan sonra kullanıcıların sistem üzerindeki aktiviteleri izlenmeli ve kayıt altına alınmalıdır.

3.5. Anahtar Değişimi

VPN cihazı üzerinden sisteme erişmek isteyen istemcilerin erişime yetkili olup olmadığını belirlemek için VPN istemci ve VPN sunucu arasında anahtar değişimi yapılmaktadır. Bu işlem yapılırken aşağıdaki kimlik doğrulama mekanizmalarından biri uygulanır.

3.5.1. Manuel Anahtar Değişimi

VPN yapılandırmasının en basit yöntemidir. Bu yöntemde IKE hiçbir aşamada kullanılmaz. Doğrulama ve şifreleme anahtarları VPN uç noktalarına manuel olarak girilir. Manuel anahtarla kimlik doğrulama işlemi basitliğiyle birlikte bazı dezavantajları da beraberinde getirmektedir:

- Her zaman aynı anahtarlar kullanılır. Tekrarlama saldırılarına (reply attack) karşı korunmasızdır. Şifreli trafiği dinleyen yetkisiz bir kişi bu trafiği kaydederek daha sonra tekrar gönderebilir. Bu durumda VPN cihazı tekrarlama saldırısını algılayamaz. Böylece önemli bilgi yetkisiz kişilerin eline geçebilir. Bu yüzden manuel kimlik doğrulama yöntemi kullanılmamalıdır.
- Uç sayısı arttıkça, manuel kimlik doğrulama işlemi zorlaşmaktadır.

3.5.2. Paylaşımlı Anahtar Değişimi

Ön paylaşımlı anahtarlar VPN cihazı üzerinden sisteme erişebilmek için kullanıcılara verilen şifrelerdir. Bu kimlik doğrulama mekanizmasında sınırlı sayıda kullanıcı sisteme erişebilir. Çok geniş kullanıcı gruplarının bulunduğu bir yapıda yetersiz kalmaktadır. Uç nokta doğrulaması yaptığından tekrarlama saldırılarına karşı güvenlidir. Sayısal sertifikayla kimlik doğrulanmanın mümkün olmadığı yerlerde ön paylaşımlı anahtarla kimlik doğrulama tercih edilmelidir.

3.5.3. Sayısal Sertifika İle Anahtar Değişimi

Sayısal sertifikalar kullanıcıların sistemde var olduklarını gösteren bir çeşit elektronik belgelerdir. Bu belgeler kullanıcı bilgisayarında olabileceği gibi kullanıcılarda bulunan jetonlarda

(token) da bulunabilmektedir. Sayısal sertifikaların yönetimi Açık Anahtar Altyapısı (Public Key Infrastructure – PKI) ile yapılmaktadır. PKI, ön paylaşımlı anahtarlara oranla daha güçlü ve daha geniş bir kimlik doğrulama altyapısı sunmaktadır. Ancak daha pahalı ve karmaşık bir çözümdür. Uç sayısının artması sistemin performansını önemli ölçüde etkilemez. Sonuç olarak, ön paylaşımlı anahtarla kimlik doğrulama yerine sayısal sertifikayla kimlik doğrulama tavsiye edilmektedir. Çünkü ön paylaşımlı anahtar mekanizması, sayısal sertifika kullanımına göre daha zayıf bir mekanizmadır. Sertifika ile kimlik doğrulama işleminin kurulumu görece daha zor olmasına rağmen daha güvenlidir ve uzak bağlantılar için en güvenilir yöntem olan IKE Asıl mod (IKE Main mod) kullanır.

4. REFERANSLAR

- Ağ ve Erişim Güvenliği Politikası BGYS.PLT.02