1.AMAÇ

Bu prosedür, Birimimiz Bilgi Güvenliği Yönetim Sistemi kapsamında bilgi ve yazılım bütünlüğünün korunması için kötü niyetli yazılımın girişini tespit edecek ve önleyecek tedbirleri tanımlamak amacı ile hazırlanmıştır.

2.SORUMLULUKLAR

Bu prosedür, Birimimiz BGYS Yöneticisi sorumluluğundadır.

3.UYGULAMA

Kötü niyetli yazılımlara karşı aşağıdaki yöntemler kullanılır.

- Güvenlik Duvarları Cihazları
- Atak Tespit ve Önleme Cihazları(IPS/IDS)
- Yük Dengeleme Cihazları
- İçerik Filtreleme Cihazları
- Antivirüs/Antispam Sunucu

3.1. Güvenlik Duvarları Cihazları

Güvenlik duvarları kurulduğu konumda gelen ve giden ağ trafiğini kontrol ederek bağlı olduğu ağa ya da ağdaki diğer bilişim cihazlarına yetkisiz veya istenmeyen kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır. Ağdaki katmanlar arası ve alt ağlar arası ya da sunucular arasındaki erişim yetkileri bu cihazlar üzerinden yapılır. Lokal ağ (LAN, Wireless LAN vs.) ve internet(WAN) arasındaki erişim ve güvenlik politikaları bu cihazlar üzerinden kontrol edilir. Erişim protokolleri, servisler, TCP/IP katmanında erişim yetkileri bu cihazlar sayesinde yönetilir.

3.2. Atak Tespit ve Önleme Cihazları(IPS/IDS)

IDS: Intrusion Detection Systems-Atak Tespit Sistemleri: Kötü niyetli ağ hareket ve bağlantılarının tespiti için kullanılan sistemdir. Amacı tanımlama ve loglamadır.

IPS: Intrusion Prevention Systems-Atak Önleme Sistemleri: Kötü niyetli ağ hareket ve bağlantılarının önlenmesi için kullanılan sistemdir. Amacı kötü niyetli ağ hareketlerinin önlenmesidir.

Bu sistemler güvenlik duvarı cihazlarının içinde tümleşik yazılımlardır.

3.3. Yük Dengeleme Cihazları

Yük dengeleme bir işi iki ve daha fazla kaynak arasında paylaştırma teknolojisidir. Yük dengeleme kullanılan birden fazla bileşen ile yedekliliği sağlar. Sunucular üzerindeki trafiği azaltıp dengeli olarak dağıtarak sunucuların ve üzerlerindeki servislerin güvenliğine katkı sağlar.

3.4. İçerik Filtreleme Cihazları

Web, eposta ve dosya transferleri trafiğini yönetir, belirlenen politikalar sayesinde bu trafiğin güvenliğini sağlar. Zararlı içeriğe sahip web sitelerin erişimleri, e-posta trafiğini tehdit edecek spam, virüs, solucan, trojan vs. gibi içerikleri, kurum için gizlilik önemi taşıyan dosyaların kurum dışına web ya da e-posta yoluyla çıkarılmasını yasaklayan, bunları loglayan ve raporlayan, kısacası yöneten sistemdir.

3.5 Antivirüs/Antispam Sunucuları

Antivirüs/Antispam sunucuları kurulu olduğu ağ üzerinde, o ağa bağlı olan uçlarda otomatik olarak son çıkmış olan virüslere ve ajanlara karşı savunma sistemi oluşturur. Kullanıcı bilgisayarlarına agent yükleyerek kullanıcı bilgisayarlarını ve sunucuları koruma altına alır.

Sistem gerçek zamanlı koruma yaparak ajanların veya virüslerin sisteme ulaşmalarını engeller. Ayrıca zamanlama ayarı yapılarak belirli dönemlerde veya manuel olarak virüs ve ajan kontrolleri yapılabilir. Bunlarların yanında yine zaman ayarı yapılarak ve manuel olarak internet üzerinden program güncellenir ve yeni çıkan virüs ve ajanların bilgileri yenilenir.

Sistem karantina özelliği sayesinde bulunan virüsleri veya virüslü olduğu düşünülen belgeleri karantinaya alarak virüsün yayılmasını engellerken, ileride virüsü temizlemeye

uygun yöntem geliştirildiğinde dosyayı virüsten temizleyip tekrar kullanıma sunar.

Antivirüs yazılımı ile her bilgisayar düzenli olarak taranır.