T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

KamuNet

KamuNet (Kamu Sanal Ağı); kamu kurum ve kuruluşları tarafından içerik güvenliği sağlanan veri iletişiminin, kurumlar arası internete kapalı olan daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi ve oluşturulması, planlanan ortak veri merkezi/merkezlerinin dâhil edilmesi amacıyla oluşturulmuştur.

KamuNet Ağı kurulmasına ilişkin KamuNet İşbirliği Protokolü Bakanlığımız / Haberleşme Genel Müdürlüğümüz ile Türk Telekomünikasyon A.Ş. arasında imzalanmıştır.

KamuNet Ağı'na Dahil Olmak İçin Asgari Güvenlik Gereksinimleri

Her kamu kurumunda siber güvenlik risklerinin minimuma indirilebilmesi ve KamuNet ağının olumsuz etkilenmemesi için teknoloji bağımsız olarak aşağıdaki süreçlerin uygulanması gerekmektedir;

1. Bilgi Güvenliği Yönetim Sistemi (BGYS) kurularak tüm süreçler ile ilgili siber güvenlik politikaları ve prosedürleri oluşturulmalı (ISO 27001 standardına uyumlu hale getirilmeli),
2. Kurum çalışanlarının farkındalığının arttırılması amacıyla tüm çalışanlara siber güvenlik farkındalığı ile ilgili bilgilendirme, eğitimler verilmeli,
3. Kurum içerisinde ilgili süreçlerden sorumlu yetkin bir ekip oluşturulmalı,

4. Kurum kontrolünde, sunucu ve istemci (client) ağlarında internet üzerinden ve yerel ağ içerisinden düzenli zafiyet taramaları yapılarak var olan zafiyetler tespit edilip gerekli önlemlerin alınması için çalışmalar yapılmalı,

5. KamuNet Ağı için kurum içi envanter ve topoloji oluşturulmalı ve güncel tutulmalı,

6. Kuruma ait kritik sistemler üzerinde sızma/penetrasyon testleri yapılıp tespit edilen açıklıkların giderilmesi için çalışmalar yapılmalı,

7. Kritik sistemlere ait loglar sürekli gözden geçirilerek bir anomali olup olmadığı incelenmeli,

8. Süreçlerin (27001 Bilgi Güvenliği, sızma/penetrasyon testleri vb) yeterince uygulanıp uygulanmadığının kontrolü için düzenli aralıklar ile denetimler gerçekleştirilmeli,

9. Maksimum güvenlikli ideal çözümün sağlanabilmesi için kurum içerisinde aşağıdaki şekilde görülebileceği gibi sunucu ve istemci (client) ağları ayrılmalı,

10. Sunucu ve istemci (client) ağlarının birbirine erişiminde mutlaka FW, IPS, içerik filtreleme ve antivirüs gibi fonksiyonların bir arada olduğu UTM vb. ya da bu fonksiyonların ayrı ayrı olduğu cihazlar kullanılarak bir güvenlik katmanı oluşturulmalı,

11. KamuNet ağına dahil olacak kamu kurumları KamuNet ağından gelebilecek tehditlere karşı kendilerini korumak için de UTM vb. cihaz kullanmalı,

12. Kamu kurumlarının hizmet olarak verdiği, internete açık servislerinin (web vb.) bulunması halinde bu servislerden gelen saldırıların KamuNet ağını olumsuz etkilememesi için DDoS ataklarını önleyen hizmetlerden faydalanılmalı,

13. İstemci (Client) ağı içerisinde Dizin Hizmeti kullanılmalı ve her bir kullanıcı bilgisayarı Dizin Hizmeti'ne dahil edilmeli,

14. Dizin Hizmeti üzerinde kullanıcı bilgisayarlarının KamuNet ağını olumsuz etkilememesi için Anti-Virüs sisteminin, işletim sistemi güncelleme durumları takip edilmeli,

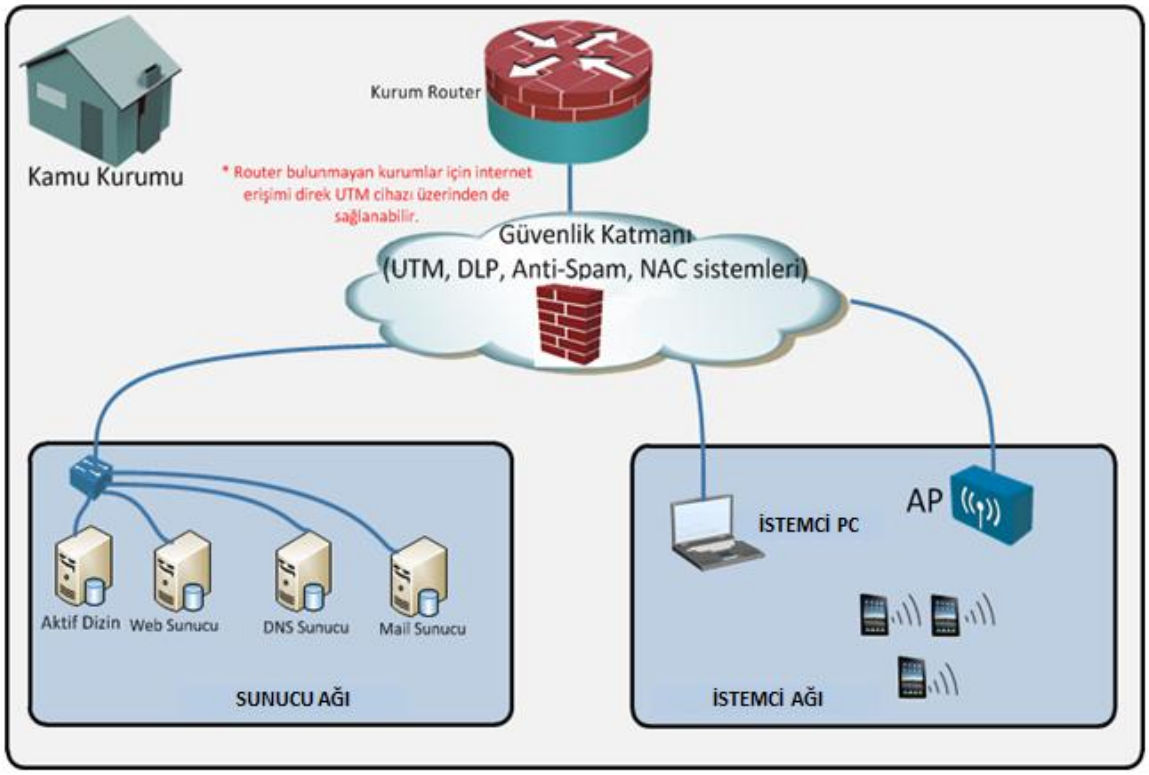
15. KamuNet ağına dahil olacak her bir cihazda (bilgisayar, sunucu vb.) virüsler, solucanlar, truva atları ve casus yazılımlar vb. gibi zarar verebilecek yazılımları saptama, silme işlevlerini yapabilecek, sürekli aktif halde çalışan ve güncellenmesi gereken son kullanıcı güvenlik yazılımlarını kurulu bulundurmalı,

16. KamuNet ağını olumsuz etkilememesi için Dizin Hizmeti üzerinde kullanılabilecek programlar belirlenmeli ve kullanıcıların kurup kaldırmaya izinli programlar sınırlandırılmalı,

17. KamuNet ağını olumsuz etkilememesi için NAC (Network Access Controller) çözümleri ile kullanıcıların yapılandırmasının güvenli olup olmadığı kontrol edilerek kendi ağlarına alınmaları sağlanmalı,

18. Kamu kurumları, KamuNET ağında bilgi görmesi gereken prensibine göre sadece ilgili kurumlar ile veri paylaşmalı ve ilgisiz kurumların bilgiye erişimi kısıtlanmalı,

19. KamuNet ağını olumsuz etkilememesi için kablosuz erişimi sağlayan modem veya Access Point'lerin yazılımları güncel tutulmalı, bu cihazların Dizin Hizmeti ile entegrasyonu yapılmalı,
20. Sunucuların bulunduğu sistem odaları güncel ISO 27001 standardına uygun olmalı, giriş ve çıkışlar kontrol altında tutulmalı ve yetkilendirme yapılmalı,
21. Sunucuların yedekleri buldurulmalı,
22. Sunucular üzerindeki gereksiz uygulamalar ve servisler mutlaka kapatılmalı,
23. Sunucular üzerindeki işletim sistemleri ve uygulama yazılımları güncel tutulmalıdır.



Şekil: Asgari Güvenlikli Çözüm