T.C. İÇİŞLERİ BAKANLIĞI
TAŞRA TEŞKİLATLARI
BİLGİ SİSTEMLERİ GÜVENLİK VE İŞLETME STANDARTLARI

İçindekiler

1. GENEL HÜKÜMLER

Amaç: Bu standartlaştırma bildirisinin amacı, İçişleri Bakanlığı Taşra Teşkilatları bilgi sistemlerindeki iç ve dış güvenlik tehditlerine karşı gerekli tedbirleri temin etmek, sistemlerden ve ağ kaynaklarından en verimli şekilde yararlanmak ve iletişim ağının amacına uygun olarak kullanılmasını sağlamak üzere sistem kullanımı ve güvenliğine yönelik genel kuralları belirlemektir.

Kapsam: Bu standartlaştırma bildirisi, İçişleri Bakanlığı Taşra Teşkilatları bilgi sistemlerini kullanan tüm personel ile kendilerine herhangi bir nedenle bilgi işlem sistemlerini kullanma yetkisi verilen paydaş ve konukların bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

2. BİLİŞİM SİSTEMLERİ GENEL KULLANIM POLİTİKALARI

a. Bilgi Sistemleri Yönetimi Politikaları

1. Birim içerisinde bulunan tüm bilgisayarların Domain yapısına dahil edilmesi gerekmektedir.
2. Domain bilgisayarlarının açılması için kullanılacak olan kullanıcı adları için şifre politikası uygulanmalıdır.
3. Domain Sunucusuna erişim hakkı yalnızca Bilgi İşlem Müdürlükleri tarafından konfigüre edilmelidir.
4. Bilgi Güvenliği ve iş sürekliliğinin sağlanması açısından sunucu bilgileri ve konfigürasyonları sadece Bilgi İşlem Müdürlüğünün erişebileceği ortak veri tabanında saklanmalıdır.
5. Bilgi İşlem Müdürlüğünün onayı alınmadan herhangi bir sunucu barındırılmamalı ve tüm sunucuların kontrolü ve yönetimi Bilgi İşlem Müdürlükleri tarafından yapılmalıdır.
6. Bilgisayarlarda bulunan kaynaklar paylaşıma açılmamalıdır. Group Policy'ler ile bu kurallar düzenlenmelidir.
7. Tüm sunucu ve son kullanıcı bilgisayarlarının konfigürasyonlarının Bilgi İşlem Müdürlükleri tarafından yapılması gerekmektedir.
8. Bilgi işlem personeli haricinde hiç kimse bilgisayarlarda program kurulumu yapmamalıdır.
9. Bilgi işlem personeli haricinde hiç kimse bilgisayarın iç kısmını açmamalı ve yeni donanım ekleyip çıkarmamalıdır.
10. Firma personellerinin işlem yapması gerektiği zaman Bilgi İşlem personelinin nezaretinde işlem yapması sağlanmalıdır.
11. Yedeklemelerin düzenli olarak yapılması sağlanmalı ve yedekler kilitli olarak muhafaza edilmelidir.
12. Virüs programlarının ve işletim sistemlerinin güncelliği sürekli olarak kontrol edilmelidir.
13. Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılmalıdır.
14. Sistem Odasına yalnızca Bilgi İşlem personellerinin girme izinleri olacak şekilde fiziksel güvenlik sağlanmalıdır.
15. Sunucu ve bilgisayarlara uzaktan bağlantı için sadece Bilgi İşlem Dairesi Başkanlığı personeline izin verilmesi bunun dışında kimseye yetki verilmemesi gerekmektedir. Firmalar aracılığıyla alınacak desteklerin Bilgi İşlem personeli nezaretinde yerinde olacak şekilde yaptırılması sağlanmalıdır.
16. Kurum internet sitelerinde "Tasnif Dışı" ve kamuya açık bilgiler dışında doküman paylaşımı yapılmamalıdır.
17. Birimlerden ayrılan hizmet alımı, işçi, sözleşmeli 4C ve kurum dışı personel kayıtlarının e-İçişleri üzerinden ilişik kesme işlemleri Bilgi İşlem Müdürlükleri tarafından yapılmalıdır.

b. İnternet Erişim ve Kullanım Politikaları

1. Taşra teşkilatının bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvarı üzerinden internete çıkmalıdır.
2. Taşra teşkilatı cihazları üzerinde istenilmeyen ve sakıncalı siteler (cinsel içerik, oyun, kumar, şiddet, zararlı yazılım bulunduran vs.) yasaklanmalıdır.
3. Yaptığı işin niteliğine göre bazı kullanıcılara internete çıkışta özel haklar verilebilmelidir.
4. İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilemez ve indirilemez. Bu konuda gerekli önlemler Bilgi İşlem Müdürlükleri tarafından alınmalıdır.
5. Üçüncü şahısların internet erişimleri isteniyorsa misafir kablosuz ağı oluşturularak gerekli erişim sağlanır.
6. İnternet erişim kayıtları 5651 Sayılı Kanuna göre kayıt altına alınmalıdır.

c. Ağ Cihazları Güvenlik ve Yönetim Politikaları

1. Ağ bağlantıları Bilgi İşlem Şube Müdürlükleri tarafından düzenli olarak takip ve kontrol edilmelidir.
2. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde yapılandırılır, ihtiyaçlara göre Bilgi İşlem Şube Müdürlükleri tarafından serbest bırakılmalıdır.
3. İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.
4. Ağ yapısı VLAN gibi ayrı mantıksal alanlar oluşturularak tasarlanmalıdır.
5. Taşra teşkilatı iletişim ağına yönelik dokümantasyon (ağ adresleri, yapılandırma, tasarım bilgileri, vb.) hiçbir şekilde üçüncü kişiler ile paylaşılmaz ve bu kişilerin erişebileceği mantıksal ve fiziksel alanlarda saklanmaz.
6. Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.
7. Kurum içerisinden dışarıya erişilen tüm IP bilgileri için güvenlik duvarı üzerinde NAT/PAT dönüşümleri yapılmalıdır.
8. Cihazlara erişimde tanımlanan parolalar Bilgi Güvenliği Politikaları Yönergesi Parola Politikalarına uygun olmalıdır.
9. Kurumdan ilişiği kesilmiş veya görev yeri değişmiş kullanıcıların yetkileri alınmalıdır.
10. Ağ cihazlarına erişimler için IP kısıtları getirilir ve sadece Bilgi İşlem Şube Müdürlükleri tarafından erişilmelidir. Ağ cihazlarına erişimler güvenli kanallar (örn. SSH, IPSec, vb.) üzerinden yapılmalıdır.
11. Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanmamalıdır.
12. Ağ cihazları üzerinde kullanılmayan tüm servisler kapatılmalıdır.
13. İhtiyaç duyulduğu zaman erişim listeleri eklenebilmelidir.
14. Ağ cihazları üzerindeki tüm yapılandırma değişikliği ve yönetici hareketlerinin log kayıtları tutulmalıdır.
15. Tüm kritik servisler güvenlik duvarı arkasında sonlandırılmalı ve tüm trafik güvenlik duvarı tarafından onaylanmalıdır. Güvenlik duvarı üzerindeki tüm yetkisiz servisler engellenmeli ve alarm üretilmelidir.

16. Kablosuz Erişim Noktası cihazlarında güçlü bir şifreleme ve erişim kontrol sistemi kullanılır. Bunun için Wi-Fi Protected Access2 şifreleme kullanılır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.
17. Kablosuz Erişim Noktası cihazlarındaki firmware'ler düzenli olarak güncellenmelidir.
18. Varsayılan SSID isimleri kullanılamaz. SSID ayarı bilgisi içerisinde resmi isimler olmamalıdır.
19. Kablosuz internet kullanımında erişim kısıtlamaları uygulanmalıdır.

Esra DAKAK	Can CANAN	Yılmaz BERKTAŞ
Veritabanı Uzmanı	Mühendis	Mühendis