1. AMAÇ

T.C. Sağlık Bakanlığı Zonguldak İSM Bağlı Birimleri ve Sağlık Tesisleri bünyesinde bulunan tüm sistemlerin güvenlik ilke ve koşullarının tanımlanması amaçlanmaktadır.

2. KAPSAM

T.C. Sağlık Bakanlığı Zonguldak İSM, Bağlı Birimleri ve Sağlık Tesisleri bünyesinde bulunan tüm bilgi sistemlerini ve bunlardan sorumlu tüm personeli kapsamaktadır.

3. UYGULAMA

3.1. Yazılım Geliştirme Güvenliği

3.1.1. Kurum Üst Yönetimi tarafından sadece uygun görülen yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olunur.

3.1.2. Uygulama yazılımlarının kurum içerisinde mi hazırlanacağı yoksa satın mı alınacağının belirlenmesi Kurum Üst Yönetimi tarafından tanımlanır.

3.1.3. Yeni alınmış veya revize edilmiş bütün yazılımlar ile hazırlanan sistemler mevcut politikalar dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilir.

3.1.4. Eski sistemlerdeki veriler tamamen veya ihtiyaca yönelik şekilde, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılır ve\veya uygun şekilde saklanır.

3.2. Veritabanı Güvenliği

3.2.1. Veri tabanı sistemleri envanteri dokümante edilir ve bu envanterden sorumlu personel tanımlanır.

3.2.2. Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilir.

3.2.3. Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulur, yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli olarak alınması kontrol altında tutulur.

3.2.4. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulur.

3.2.5. Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilir.

3.2.6. Veri tabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak uygun şekilde muhafaza edilir.

3.2.7. En üst düzey veri tabanı yöneticiliği sadece İstatistik ve Bilgi İşlem Birimi tarafından yetkilendirilmiş kullanıcılara verilir.

3.2.8. Bütün şifreler düzenli aralıklarla değiştirilir. Şifre belirleme konusunda "Parola Güvenliği Politikası" esas alınır.

3.3. Sunucu ve Sistem Güvenliği

3.3.1. İş sürekliliği ve acil durum planlaması için iletişim yöntemleri tanımlanır ve yazılı hale getirilir. Acil durumlarda erişilmesi gereken kişilerin irtibat numaraları ilgili personelin kolayca ulaşabileceği bir şekilde bulundurulur.

3.3.2. Yeni teknolojileri, uygulamaları, tehdit veya açıklıkları takip etmek için dernek, forum siteleri, e-Posta grupları gibi özel ilgi grupları belirlenir ve ilgili personel tarafından takip edilir. USOM tarafından yayımlanan https://www.usom.gov.tr/tehdit.html adresinden yaygın kullanılan yazılım ve donanımlarla ilgili güvenlik bildirimleri takip edilebilir. Aynı şekilde Bakanlığımız BGYS ve SOME birimleri tarafından yayımlanan https://bilgiguvenligi.saglik.gov.tr ve https://some.saglik.gov.tr adreslerinden güvenlik haberleri takip edilir.

3.3.3. Sistem yöneticisine sistem ile ilgili genel ve tam bir bakış açısı sağlayabilmesi açısından sistemdeki işletim sistemi, yüklü servisler, kaç sunucu (sanal ve fiziksel) olduğunu gösteren varlık envanter listesi oluşturulur. Sistemde bulunan her varlığa mutlaka bir sahip atanır. Hazırlanan varlık envanter listesi sadece ilgili personelin erişebileceği bir şekilde saklanır.

3.3.4. Varlık envanter listesinde sunucuların isimleri, IP adresleri, yeri, ana görevi, üzerinde çalışan uygulamalar, sahibi; işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personelin isimleri ve telefon numaraları gibi sıklıkla ihtiyaç duyulan bilgiler yer alır.

3.3.5. Sunuculara ve uygulamalara erişim sağlayan kullanıcıların erişim hakları, erişimlerin iptal edilmesi veya erişim yetkisinin değiştirilmesi gibi kuralların tanımlandığı erişim yetki ve kontrol matrisleri oluşturulmuştur.

3.3.6. Sunucularda zorunlu kalmadıkça "administrator" ve "root" gibi genel sistem hesapları kullanılmaz.

3.3.7. Sunuculara yapılan erişimlerin raporlanması, mesai saati dışındaki erişimlerin işaretlenmesi gibi detaylar gözlenir. Kullanıcılara olması gerekenden fazla yetki tanımlanmaz.

3.3.8. Sunucularda açılan oturumlar için kurallar tanımlanır. Sunuculara ve uygulamalara yapılan başarılı ve başarısız girişimlerin kayıtları tutulur. Kaba kuvvet ataklarına engel olmak maksadıyla sunuculara 5 (beş) başarısız oturum açma denemesi yapıldığında ilgili hesap belirlenecek bir süre boyunca askıya alınır.

3.3.9. Sunucularda oturum açmış kullanıcı hesapları ile herhangi bir işlem yapılmadığı takdirde 10 (on) dakika sonra ekran kilitlenir ve ilgili kullanıcının oturum açma ekranına düşmesi sağlanır. 1 (bir) saat boyunca işlem yapılmadığı takdirde, ilgili kullanıcının oturumu otomatik olarak sonlandırılır.

3.3.10. Sunucuda varsayılan yönetici adı (administrator) değiştirilir. Bir sunucuda mümkün olduğu kadar az sayıda kullanıcı hesabı bulundurulur ve gereksiz hesap açılmaz. Güvenlik amacıyla başkaca bir zorunluluk yok ise misafir (Guest) hesabı kapalı olarak tutulur. Misafir (Guest) ve yönetici (Administrator) hesaplarının isimleri değiştirilir. Açılmış fakat kullanılmayan kullanıcı hesapları kapalı duruma (disabled) getirilir veya silinir.

3.3.11. Sunucuların güvenliğini sağlayabilmek için kullanılmayan uygulamalar veya servisler kapatılır. Gerekli servis ve hizmetler dışında başka bir servis çalıştırılmaz.

3.3.12. Sunuculara güvenli bağlantı yapılacak ise SSL sertifikası yüklenir. Sunuculara SSH bağlantısı yapılacak ise kullanılan anahtarlar belirli aralıklarla değiştirilir.

3.3.13. Sertifika kullanım süresi, son kullanım süresi yaklaşan sertifikaların takibi gibi işlemler hazırlanacak bir sertifika takip listesi vasıtasıyla takip edilir.

3.3.14. BIOS güncellemeleri takip edilir. Sunucuların BIOS ayarlarının girişi parola ile korunur. Sunucuların varsayılan olarak CD-ROM, DVD-ROM veya flash disk gibi harici kaynaklardan başlatılması engellenir.

3.3.15. Sunucuda depolanan veriler, işletim sisteminin çalıştığı disk bölümünden farklı bir disk bölümünde tutulur.

3.3.16. Sunucuların arka planda çalışan servisleri ile birlikte o servislerinde kullandığı portlar kontrol edilir. Gereksiz portlar kapatılır. Mümkün olduğu surette uygulamaların varsayılan portları değiştirilir.

3.3.17. Güvenlik testleri yapılarak sunucular ve sistem ile ilgili açıklıklar tespit edilir. Tespit edilen açılıkların kapatılması sağlanır. (Sunucuda Windows işletim sistemi kullanıyor ise “Netstat –an”, Linux işletim sistemi kullanıyor ise “Netstat –tulp” komutu ile açık veya kullanılan portlar listelenerek kontrol edilebilir.)

3.3.18. Sunucu işletim sistemleri, güvenlik açıklarına karşı güncel tutulur.

3.3.19. Etki alanındaki sunucu ve istemci bilgisayarların yama yönetiminin merkezi bir sunucu üzerinden otomatik olarak yapılması için gerekli olan sistem tesis edilir. Bu amaçla üreticiler tarafından yayımlanan yamalar merkezi bir sunucuya çekilir ve bu sunucu vasıtası ile diğer bilgisayarlara dağıtımı yapılır.

3.3.20. Mutlaka zorunlu değil ise sunucuların internete erişimleri kapatılır.

3.3.21. Sistem kaynaklarının uygun seviyede planlanması, sürdürülebilmesi ve etkin kullanılabilmesi için kapasite yönetimi yapılır. Kapasite yönetim planları uyarınca sunucuların performans gereklilikleri belirlenir. Sistemde belli aralıklarla disk birleştirmesi (defragment) ve disk temizlemesi yapılır. Yasal bulundurma süresi dolan veya sistem tarafından geçici olarak yaratılan dosyalar silinir. Disklerin doluluğu, ram ve işlemci kullanımı ve bunlara ilişkin kullanım parametreleri kontrol edilir.

3.3.22. Kullanıcıların bilgisayarlarının saat ve tarih ayarlarını değiştirmesi engellenir.

3.3.23. Virüs vb. zararlı yazılımlardan korunmak ve kurumsal bilgilerin kurum dışına sızmasını engellemek amacıyla gerekiyorsa USB bellek gibi taşınabilir cihazların kullanımı engellenir.

3.3.24. Kullanıcıların ".exe/.bat" gibi çalıştırabilir dosyaları çalıştırmaları engellenir.

3.3.25. Kullanıcıların kısa yolu olmayan uygulamaları açmalarını önlemek için komut satırı olarak da bilinen ve Windows işletim sistemli cihazlarda yer alan DOS tabanlı konsola (cmd) erişimleri engellenir.

3.3.26. Kullanıcıların DNS adreslerini değiştirmeleri engellenir.

3.3.27. Sunucuda paylaşıma açılmış klasörlerde izin verilen kullanıcı ve gruplar kontrol edilir. Kullanıcılara, gruplara verilen izinler ve kullanıcıların baskın izin seçeneğini nerden aldığı incelenir. Herkes (everyone) isimli kullanıcı grubuna izin atanmaz. İzinler kullanıcılardan ziyade gruplara verilir. Kullanıcıların bilgisayarlarını günlük işlerini yapmalarını sağlayacak seviyede en az yetki ile çalıştırmaları sağlanır. Aynı izinlere sahip olması gereken kullanıcılar bir grupta toplanır

3.3.28. Sunucularda yapılan işlemlerin iz kayıtlarına erişmek için olay günlükleri (event logs) tutulur.

3.3.29. Sunucu ve sistem güvenliğini sağlayabilmek için lisanslı yazılımlar kullanılır. Kurumun yazılım lisans varlıklarının sayısı, bu lisanların hangilerinin aktif kullanıldığı, kullanılmayan lisansların bilgisinin tutulması gibi ayrıntıları içeren listeleme ile aktif lisans yönetimi yapılır.

3.3.30. Tüm bilgisayarlar lisanslı anti-virüs yazılımı ile korunur. Anti-virüs yazılımının virüs veritabanı güncel tutulur.

3.3.31. Sunucuların fiziksel güvenliğini sağlamaya yönelik tedbirler alınır. Sunucu odası dışında sunucu bulundurulmaz. Sunucu/Sistem odalarına yapılan giriş çıkışlar kontrol edilir, giriş çıkışları kayıtları tutulur.

3.3.32. Sunucuların üretici tarafından tavsiye edilen/teknik dokümanlarında belirtilen süreler dikkate alınarak yıllık bakım planları hazırlanır. Bakımlar yetkili uzmanlar tarafından yapılır ve kayıt altına alınır.

3.3.33. Sunucuların erişilebilirlik (availability) seviyesini artırmak için herhangi bir sunucunun çalışmaması durumunda diğer bir sunucunun onun yerine amaçlanan şekilde çalışmasını sağlayacak kümelenmiş (cluster) mimari yapıda yapılandırılması gerekir. Yüksek maliyet ya da yönetimsel zorluklar nedeni ile sunucular kümelenmiş yapıda tesis edilemiyorsa en azından disklerin kümelenmiş olarak yapılandırılması tavsiye edilir.

3.4. Ağ Güvenliği

3.4.1. Güvenlik ve ağ cihazlarında yönetici olarak erişim yetkisine sahip olan kullanıcılar yazılı olarak tanımlanır. Bu erişim yetkisine sahip kullanıcı hesaplarındaki değişiklikler kontrol edilir. Sistemler üzerinde ortak erişim yetkisi olan hesaplar açılmaz. Sahibi bilinmeyen hesaplar kaldırılır.

3.4.2. Güvenlik duvarları, ana omurga cihazları gibi kritik sistemlere yapılacak erişimler için yerel kullanıcılar yerine ikincil bir kimlik doğrulamasının kullanılması tavsiye edilir.

3.4.3. Güvenlik ve ağ cihazları için varlık envanter listesi oluşturulur. Listede cihaz/ürünün adı, marka ve modeli, kullanım maksadı, IP ve MAC adresi, bulunduğu yer, sorumlusu gibi bilgiler yer alır.

3.4.4. Güvenlik ve ağ cihazlarının gösterildiği "ağ mimarisi krokisi" hazırlanır. Hazırlanan kroki, sadece ilgili personelin görebileceği bir şekilde saklanır. Güvenlik ve ağ mimarisinde değişiklik yapıldığı zaman kroki de güncellenir.

3.4.5. Sistemi etkileyecek bir çalışma yapılması gerekiyorsa mesai saati dışında yapılır. Bu çalışmadan etkilenecek kurum/firma ya da kişilere bilgi verilir.

3.4.6. Kablosuz ağlara giriş yapan tüm kullanıcılar sisteme kimlik tanımlı olarak kaydedilmelidir. Kimlik doğrulamasında bağlantı yapacak kullanıcının kimlik bilgileri ve ne kadar süre ağda kalacağı gibi bilgiler alınır. 5651 sayılı Kanun ve Bakanlık BGYS politikaları uyarınca, ağa dâhil olan tüm kullanıcılar kaydedilir ve bu bilgiler belirlenen süreler boyunca saklanır.

3.4.7. Telnet gibi güvensiz bağlantılara izin verilmez. SSH protokolünü kullanan bağlantılarda SSH Ver2 kullanılır.

3.4.8. İhtiyaç olmayan tüm portlar kapatılır. Dışarıdan tarama yapıldığında portların durumunun açık olarak görülmemesi için gerekli tedbirler alınır. Kurum web sayfaları, laboratuvar sonuç sorgulama sayfası gibi uygulamalarca kullanılan 80 ve 443 dışındaki portlar kullanıma kapatılır.

3.4.9. Güvenlik duvarı ve ağ cihazları için kontrol listeleri (ACL, güvenlik ürünleri erişim kısıtlaması vb.) tanımlanır.

3.4.10. Güvenlik ve ağ cihazlarının fiziksel güvenliğini sağlamak için gerekli tedbirler alınır.

3.4.11. Güvenlik ve ağ cihazlarının yazılım güvenliğini sağlamaya yönelik tedbirler alınır. Cihazlar ilk kurulduğunda varsayılan olarak atanmış olan kullanıcı adı ve parolalar değiştirilir. Parolalar, Bilgi Güvenliği Parola Politikası kapsamındaki güçlü parola ilkeleri esaslarına göre oluşturur.

3.4.12. Güvenlik ve ağ cihazları üzerindeki gereksiz ve kullanılmayan tüm servisler kaldırılır.

3.4.13. Cihazları kaba kuvvet saldırılarından korumak için 5 (beş) yanlış deneme sonrasında oturum belirli bir süre kilitlenecek şekilde ayarlama yapılır.

3.4.14. Doğru yapılandırılmış zaman damgası için cihazlar NTP sunucu ile senkronize olarak çalıştırılır.

3.4.15. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Kanunu uyarınca trafik bilgileri (iz kayıtları) kayıt altına alınmalıdır.

3.4.16. Saldırganların yerel ağda kendilerini ağ geçidi olarak tanımlayarak trafiği kendi üzerinden geçirerek bilgilere erişim sağlamasını önlemek için ağda kullanılan anahtarlarda “DHCP snooping” ve “arp inspection” özelliği aktif edilir.

3.4.17. Kurum ağı, IEEE 802.1x port bazlı kimlik doğrulama sistemine göre yapılandırılır. Port tabanlı kimlik doğrulama ile yerel ağların dinlenilmesi, istenmeyen erişimlerin ağa bağlanması engellenir.

3.4.18. Dış ağdan sunucular üzerindeki servislere, sunucu yönetim protokolleri (RDP, SSH) ile erişim engellenir. Sunucular, sadece belirli portlardan erişim sağlanacak şekilde yapılandırılır.

3.4.19. Kurum bünyesinde barındırılan ve hizmet veren uygulamalara HTTPS üzerinden bağlanılır.

3.4.20. Güncel atak metotlarından korunmak için saldırı tespit ve önleme sistemleri, ağ hizmetlerine erişim ilkelerinin belirlenmesi için güvenlik duvarı kullanılır.

3.4.21. Kurumsal kaynakların etkin olarak kullanılması, 5651 sayılı Kanun’dan kaynaklanan uyum zorunlulukları, veri güvenliğinin sağlanması, zararlı içerik ve yazılımlardan korunma vb. maksatlarla internet erişimi kısıtlamaları yapılabilir. Kısıtlama ile ilgili politikalar, kurumumuz bilgi güvenliği alt komisyonu tarafından belirlenir. Kısıtlama ile ilgili planlama yapılırken aşağıdaki hususlar dikkate alınır:

3.4.21.1. Basın yayın organlarını takip ederek idareye raporlamakla sorumlu personel haricindeki tüm personelin dizi, film ve TV erişimlerinin kapatılması,

3.4.21.2. Kurum sosyal medya hesaplarını yönetmekle sorumlu personel dışındaki tüm personelin Facebook, Twitter, İnstagram vb. uygulamalara erişimlerinin engellenmesi veya bant genişliği sınırlaması yapılması,

3.4.21.3. Youtube, Vimeo, Dailymotion gibi platformlarda erişimlerle ilgili olarak sadece ihtiyaç duyan personele izin verilmesi, bu yapılamıyorsa bu platformlara erişimlere bant genişliği sınırlaması yapılması önerilir.

3.5. Etki Alanı Kurulum ve Yönetimi

3.5.1. Yönetilebilirlik, ölçeklenebilirlik, genişletilebilirlik, güvenlik entegrasyonu, diğer etki alanları ile birlikte çalışabilme, güvenli kimlik doğrulama ve yetkilendirme, grup politikaları ile yönetim, DNS ve DHCP gibi servislerle birlikte çalışabilme gibi avantajları nedeniyle etki alanları kurulur ve işletilir.

3.5.2. Kurumumuzda etki alanına dâhil olan her kullanıcı için kullanıcı adı ve şifresi oluşturulur. Kullanıcı adı (ad.soyad) yapısında, şifresi ise kurumumuz bilgi güvenliği parola politikası doğrultusunda oluşturulur.

4. YAPTIRIM

Bilgi Güvenlik Politikalarının ve Prosedürlerinin ihlali durumunda Bilgi Güvenliği Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.