****

**Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı**

**TIBBİ CİHAZLARDA ALINMASI GEREKEN GÜVENLİK ÖNLEMLERİ DOKÜMANI V.1.0**

**HAZIRLAYAN**

Cihan Mehmet DOĞAN

(Sızma Testi Uzmanı)

**23.09.2019**

**İçindekiler**

[A. Biyomedikal ve Tıbbi Cihazlar için Genel Güvenlik Prosedürleri 4](#_Toc20068836)

[1) Hastanelerin Bilgi İşlem / Biyomedikal Birimleri Tarafından Takip Edilmesi Gereken Hususlar 4](#_Toc20068837)

[2) Tıbbi Cihaz Tedarik Planlaması Yapan Birimler Tarafından Dikkat Edilmesi Gereken Hususlar: 6](#_Toc20068838)

## **Biyomedikal ve Tıbbi Cihazlar için Genel Güvenlik Prosedürleri**

## **Hastanelerin Bilgi İşlem / Biyomedikal Birimleri Tarafından Takip Edilmesi Gereken Hususlar**

**a.** Tıbbi cihazlara fiziksel erişim sadece yetkili kişiler ile sınırlandırılır. Cihazların çalınmasını, kurcalanmasını engelleyebilmek için düzenli olarak güvenlik kontrolleri yapılır.

b. Tıbbi cihaz envanteri çıkarılır. Cihazlara ait temel bilgiler tespit edilerek kullanıldığı yer ile birlikte kayıt altına alınır.

c. Tedarik safhasında bilgi güvenliği yapılandırma imkânı sağlayan cihazlar tercih edilir ve bu husus hazırlanacak tıbbi cihaz tedarik şartnamelerine konulur.

d. Cihaz yaşam döngüsü boyunca bilgi teknolojileri ile ilgili cihaz yapılandırma ihtiyaçları için üretici firma desteği alınır.

e. Tıbbi cihazların bağlı olduğu ağın geniş alan ağı çıkışına sınır güvenliğini sağlamak üzere güvenlik duvarı kurulur. Tıbbi cihazlar söz konusu güvenlik duvarı vasıtasıyla oluşturulan DMZ bölgelerine konumlandırılarak cihazlara dış ağdan yapılacak erişimler engellenir veya asgari düzeye indirilir

f. Kullanıcıların erişmek istedikleri web servis erişimleri HTTPS (TLS) üzerinden yapılmalıdır.

g. Aşağıdaki listesi olan portlar haricindeki portlar ya dış erişime komple kapatılmalı yada firewall arkasında erişimi kontrolüne tabi tutulmalıdır. Aşağıda listesi verilen portlara erişim kısıtlanmalı ve firewall üzerinden belirli cihazların ve kişilerin erişimine izin sağlanmalıdır.

|  |
| --- |
| 80 – IIS – HTTP |
| 104 – DCOM |
| 139 – Drive Sharing |
| 190 – DCOM |
| 210 – DirectView Service Access |
| 220 – DirectView Service Access |
| 443 – HTTPS (secure tunnel) |
| 623 – Security Listener |
| 1433 – SQL |
| 2761 – DCOM |
| 2762 – DCOM |
| 4190 – DirectView Application |
| 4191 – DirectView Application |
| 5040 – DICOM PrintSCP |
| 5041 – PACS Push Connection |
| 11112 – DCOM |
| 12207 – DirectView Application |
| 14626 – DirectView Application |
| 58431 – RIG/RDET |
| * Tüm UDP portlarının erişimine (özellikle aşağıdaki liste) firewall üzerinden belirli IP’lere izin verilmelidir.
 |
| 123 – NTP |
| 137 – NetBIOS |
| 138 – NetBIOS |

ğ. Sağlık hizmet sunucusunun sınır güvenliğini sağlayan bir güvenlik duvarı yok ise tıbbi cihazlar ayrı bir VLAN’a (veya VLAN’lara) konulur. Ağ cihazlarının sağladığı imkânlar çerçevesinde dış ağdan yapılacak erişimler engellenir veya asgari düzeye indirilir.

h. Yerel alan ağının VLAN’lara bölünerek yönetilmesi, VLAN’lar için ACL’ler oluşturularak trafiğin yönetilmesi; tıbbi cihazlar için iç ağdan kaynaklanabilecek (bilinçli veya bilinçsiz) tehlikeleri önemli ölçüde azaltır.

ı. PACS cihazları gibi doğrudan uzak erişimi olan servisleri olan cihazların servisleri erişim kontrollü hale getirilmelidir.

i. İşletim sistemi kullanıcı hesaplarının sayısı sınırlandırılmalıdır. Misafir hesabı devre dışı bırakılmalı ve Yönetici hesabı yeniden adlandırılmalıdır (Windows Sunucular için)

j. İşletim Sistemi kullanıcılarında güvenli parolalar kullanılmalıdır.

k. SQL Server veritabanı oturum açma, yerel olarak veya ağ üzerinden MS Windows kimlik bilgileri veya SQL Server kimlik bilgileri gerektirmelidir.

l. İz kaydı üretme imkânı olan tıbbi cihazların iz kayıtları sadece yerel cihazda değil merkezi bir iz kaydı saklama sunucusuna da aktarılmak suretiyle saklanır.

m. Tıbbi cihazlar tarafından üretilen iz kayıtları, (varsa) Merkezi Kayıt ve Olay Yönetim Sistemi (SIEM) vasıtasıyla diğer sistemler tarafından üretilen iz kayıtları ile ilişkilendirilir ve gerekli analizler yapılır.

n. Tıbbi cihazların düzgün bir şekilde yapılandırıldıklarından emin olmak ve güncelliğini yitirmiş yazılımlardan kaynaklanan tehlikelerin hedefi haline gelmeyeceklerine garanti altına alabilmek için düzenli olarak zafiyet taramaları yapılır. Tespit edilen açıklıklar üretici firmalardan da destek alınmak suretiyle giderilir.

o. Tıbbi cihazlar genellikle en fazla bir ya da birkaç tane bilgisayar ile haberleşme ihtiyacı duyarlar. Sahte DNS ile ilgili ataklardan korunmak maksadıyla, bağlanılacak sunucu ve/veya terminallerin isim ve IP adresleri tıbbi cihazların “host” dosyalarına yazılarak cihazın DNS bağlantıları kesilir.

ö. Cihazın ağ bağlantısı yapılmadan önce mutlaka varsayılan değer bilgileri (device host name, admin, user, supervisor vb.) değiştirilir. Parola vb. bilgileri cihazların yazılımları içine değiştirilemez bir şekilde gömülü cihazlar kesinlikle kullanılmaz.

p. Cihazlara hesap kilitleme ilkesi uygulanır. Ardı ardına üç defadan fazla hatalı giriş halinde, hesaplar kilitlenir veya belirlenecek bir süre için askıya alınır.

r. Cihazlar, verilerin sadece güvenli bir format ve en güncel SSH versiyonu vb. güvenli iletişim protokolleri aracılığı ile gönderilmesini mümkün kılacak şekilde yapılandırılır. FTP, Telnet veya http gibi güvenli olmayan iletişim protokolleri yerine HTTPS, SFTP protokolü kullanılır. Güvenli olmayan ağ protokolleri devre dışı bırakılır.

s. Cihazın bellenimi (firmware) ve önemli konfigürasyon bilgileri harici olarak yedeklenir.

ş. Cihazın belleğindeki veriler mümkün ise şifreli olarak muhafaza edilir.

t. Yönetici hesabı ve kullanıcı hesapları ayrılır. Mümkün ise ağ üzerinden yönetici hesabı ile cihaza erişim yapılması engellenir.

u. Güncelleme mekanizmaları oluşturulur. İşletim sistemleri de dâhil cihaz üzerindeki yazılımlar güncel halde tutulur.

ü. Cihaz üzerindeki kullanılmayan servisler, arayüzler, yazılımsal veya mümkün olmuyorsa donanımsal olarak kapatılır.

v. Tıbbi cihazlara uzaktan erişim yapmaya yetkili personelin kimlikleri belirlenir, bu personel ile kişisel gizlik sözleşmesi imzalanır. Uzak bağlantılar için güvenli erişim yöntemleri kullanılır.

y. Tıbbi cihazlara uzaktan müdahalede bulunan firma çalışanlarına gizlilik sözleşmesi yapılır.

z. Tıbbi cihazların işletim sistemleri destekliyorsa ve bu cihazların işleyişini etkilemiyorsa anti-virüs, endpoint security gibi programların kurulması gerekmektedir.

## **Tıbbi Cihaz Tedarik Planlaması Yapan Birimler Tarafından Dikkat Edilmesi Gereken Hususlar:**

a.Mevcut tıbbi cihazlar, siber güvenlik yetenekleri yönüyle incelenir ve iyileştirmek için bir strateji uygulanır.

b. Tıbbi cihazlardaki yazılım ve donanım güncelleme işlemleri için üretici firma veya yetkili temsilcilerinin desteği alınır.

c. Yeni tıbbi cihaz tedariklerinde siber güvenlik konusu, mutlaka göz önünde bulundurulur. Üreticilerin ve cihazların siber güvenlik konusundaki yetenekleri araştırılır. Kurumsal bilgi güvenliği politikalarının uygulanamayacağı cihazlar tedarik edilmez.

d. Envanterde yer alan ve siber güvenlik tedbirleri uygulanamayan cihazların yenilenmesi veya ağ bağlantısı ihtiyacı olmayan yerlerde kullanılması için planlama yapılır.

e. Yeni yapılacak tıbbi cihaz bakım ve onarım sözleşmelerine; yazılım/donanım güncellemelerinin yapılması, sıkılaştırma işlemleri ile ilgili hususlar da eklenir.

f. Tıbbi cihazlarda siber güvenliğin sağlanması için bilgi işlem ve biyomedikal birimlerinden oluşan ekipler kurulur. Biyomedikal birimlerde görev yapan personelin bilgi teknolojileri/siber güvenlik konularında eğitim alması için gerekli tedbirler alınır.

g. Tıbbi cihazlar, üreticilerinin öngördüğü kullanım amacı ve varsa kullanım kılavuzunda belirtilen öneriler dikkate alınarak kullanılır.

h. Tıbbi cihazların güvenli kullanımını sağlamak için üreticinin öngördüğü hususlar dikkate alınarak gerekli eğitimler yapılır.