****

**Siber Olaylara Müdahale (SOME) Birimi**

**PACS SİSTEMLERİNDE ALINACAK GÜVENLİK ÖNLEMLERİ DOKÜMANI v.1.0**

**HAZIRLAYAN**

Cihan Mehmet DOĞAN

(Sızma Testi Uzmanı)

**26.09.2019**

**ÖZET**

Hastanelerimizin görüntüleme ile alakalı birimleri ve laboratuvar sonuç görüntüleme aktarma gibi birçok alanda kullanılan PACS (Picture Archiving and Communication System), cihazlarına ait dünya genelinde PACS cihazlarının standart olarak kullandığı DICOM (Digital Imaging and Communications in Medicine) protokolünün hatalı yapılandırılmasından kaynaklı kritik düzeyde bir güvenlik zafiyeti olduğu global güvenlik istihbarat raporlarına yansımış durumdadır. Yazının ilerleyen kısmında DICOM protokolü ve PACS cihazlarına kısaca değinip sorumluluk alanımızdaki PACS cihazlarında bazı sıkılaştırma önlemlerini uygulamanız sizlerden beklenecektir.

DICOM tıpta dijital görüntüleme ve iletişimi protokolü anlamına gelmektedir. Dijital tıbbi görüntülerin ve diğer ilgili dijital verilerin değişmesi ve depolanması ile ilgili uluslararası bir standarttır.

DICOM standardı, hem dijital tıbbi görüntülerin ve ilgili dijital verilerin depolanması için kullanılacak formatları hem de tıbbi görüntüleme iş akışında yararlı olan çeşitli iletişim servislerini uygulamak için kabul edilecek protokolleri kapsar. Bu protokol standardı sayesinde amaçlanan hedef, ilgili tüm aktörler bu standarda uyduğu sürece cihazlar arasında farklı tedarikçilerin cihazlarının birlikte çalışabilirliğini sağlamaktır. Örneğin A tedarikçisinin mamografi cihazındaki dijital veriyi bu protokol sayesinde B tedarikçisinin dijital arşiv dosyasına gönderebilecektir. D tedarikçisinin cihazı ise bu arşivdeki dijital veriyi alıp işleyerek başka bir amaçla kullanıcılara sunabilecektir.

Günümüzde DICOM protokolü, tüm büyük üreticilerin dijital tıbbi görüntüleme sistemlerinin büyük çoğunluğu, kamu ve özel hastaneler, tanı merkezleri ve farklı boyutlardaki analiz laboratuvarları dahil olmak üzere tıbbi kuruluşlar tarafından geniş çapta kabul edilmiştir.

PACS (Picture Archiving and Communication System), Resim Arşivleme ve İletişim Sistemi anlamına gelir. Genel olarak tıbbi görüntüleri ve ilgili verileri DICOM uyumlu bir şekilde yöneten tüm sistem olarak tanımlanabilir.

Değişik görüntüleme kaynaklarından gelen hasta ile ilgili imajların bilgisayar ve network ağıyla haberleşmesini sağlayan, yükleyen ve görüntüleyen sistemdir.

PACS aşağıdaki fonksiyonları içerir:

• Radyolojik görüntülerin dijital olarak taşınması:

–Farklı modalitilerden görüntü alma (MRI, CT, X-Ray ) ve bunları görüntüleme, arşivleme ve transmisyon için hazırlar.

–PACS network’u ile imajların taşınmasını içerir.

• Radyolojik görüntülerin dijital olarak görüntülenmesi:

–PACS istasyonlarında dijital görüntülenme ile tanı koyma ve klinik ve klinikler arası incelemeyi içerir.

• Radyolojik görüntüleri dijital olarak arşivleme:

–Gelecekte alınmak istenen dijital görüntüler arşivlenir.

• Klinik sistemlerle ara bağlantı:

–Klinik sistemlerin ve ulaşılacak raporların modalite bilgileri ve Hastane İnformasyon Sistemi ile onaylanmasını sağlar.

• Tekrar film basımı/üretme:

–Hastalar için tekrar dijital imajların basımını içerir.

**PACS Cihazların Bulunduğu Ağlarda Alınması Gereken Önlemler**

Tıbbi cihazların, mümkün olduğunca, harici olan herhangi bir şeye erişimi engellenmelidir. Ancak sunucuların güncellenmesi, makinalardaki tıbbi kayıt sistemlerinin başka bir alana depolanması için veri transferi yapılması veya değerlendirme yapılması için üçüncü şahıslara veri transferi yapılması (örneğin, radyolojik işlemlerde uzaktan raporlama hizmeti) gibi ihtiyaçların doğma olasılığından dolayı bunun kesinlikle mümkün olamayacağı durumlar da ortaya çıkabilir. Bu kontroller, tıbbi cihazlar ile dış kaynaklar ve hizmetler arasındaki bilgi akışını kontrol altında tutmak amacı ile tasarlanmaktadır.

**1) Authentication, Authorization, and Accounting (AAA) Politikasının Uygulanması**

Authentication: Cihazlara erişim yapanların Kimlik doğrulanması işlemidir.

Authorization: Kimlik doğrulanmasından geçen kullanıcıya verilecek yetkileri ifade eder. Mutlaka harici bir sunucu tarafından gerçekleştirilmesi gerekir.

Accounting: Kimliği doğrulanıp yetkisi verilen kullanıcının neler yaptığının kayıt altına alınmasıdır. (Log tutma)

Bu 3’lü politikanın uygulanması gerekmektedir.

**2) Application Entity Title (AE) Başlıklarının Detaylı Yapılandırılması**

Rastgele AET başlıklarıyla gelen isteklerin kabul edilmemesi gerekmektedir.



**3) PACS Cihazları Üzerinde Dışarıdan Bağlanmak Suretiyle Çeşitli İşlemler Yapması Gereken Firmalar, Kurumlar, Kişiler Bu Bağlantılarını Belirli Bir SSL VPN Üzerinden Bağlanarak Yapmalıdırlar.**

**4) PACS Sunucuların Erişimi Güvenlik Duvarları ile Sınırlandırılmalı ve erişim sadece izin verilen IP adresleri Üzerinden Yapılmalıdır.**

(Özellikle 104 NO’lu varsayılan DICOM port erişimi KAPATILMALIDIR!)

İç ve dış ağın birleştiği sınır noktalarına konulan güvenlik duvarları, tıbbi cihazlar ile dış kaynaklar arasındaki iletişimin tamamen engellenip engellenmediğine ya da sadece cihazın düzgün bir şekilde çalışması için gerekli olan iletişim ile kısıtlanıp kısıtlanmadığına emin olmak için çok önemli bir kontrol mekanizmasıdır. Bir tıbbi cihaz, internet üzerinden erişilebilir olduğu durumlarda, cihazın ayrı bir yönetimsel arayüzünün olmasına ve bu arayüze dışarıdan hiçbir şekilde erişim olmadığına emin olunmalıdır.

**5) PACS Cihazları İçin Ayrı Bir Ağ Segmentasyonu (VLAN) İşlemi Yapılmalı ve Mevcut İç Ağ Yapısından ACL (Access Listler) ile Ayrılmalıdır.**

Ağ segmentasyonu, bir ağa gönderilebilecek kötü amaçlı yazılımları ve diğer siber saldırıları önlemek ve bir bitiş noktası veya cihaz başarılı bir şekilde kurulduğunda oluşabilecek herhangi bir tehdidi kontrol altına almak açısından oldukça başarılı bir yöntemdir. Tıbbi cihazlar ve onların çalışabilmeleri için gerekli sistemler ile aralarındaki iletişimi kesebilmek için, tüm tıbbi cihazlar ayrı bir ağ bölümünde (VLAN) olmalıdır. Diğer tüm iletişimler sınırlandırılmalıdırlar. VLAN’lardaki trafiği kontrol altında tutmak için kullanılan ağ bölümlemesi, çoğu zaman VLAN’lar ve erişim kontrol listeleri (ACL) oluşturarak yapılmaktadır. Ama aynı zamanda, ağ segmentasyonu tamamen ayrı bir fiziksel ağ altyapısı kullanarak da yapılabilir ki bu altyapı aynı bölgede aynı tip yeni tıbbi cihazların kurulumunda da çok işe yarayacaktır.

**6) Eğer Ağda Bir Saldırı Tespit Sistemi (IDS/IPS) Mevcutsa Bu Cihazların Bulunduğu VLAN Yapılacak Yetkisiz Erişimleri ve Servis Dışı Bırakma Saldırılarını Engelleyin.**

Sınır noktalarına konulacak Saldırı Tespit Sistemleri, hem dışarıdaki gruplardan gelen yetkisiz erişim teşebbüslerini, hem de (botnetler ve zararlı yazılımların yayılmasının kontrolünü yapan) komuta kontrol sistemlerine ve fidye yazılım anahtar üretimi yapan sitelere giden bilgi trafiğini tespit etmektedirler. Dolayısı ile kurulacak bir Saldırı Tespit Sistemi, bir saldırı teşebbüsünü erkenden haber verme veya ağ destekli bir cihazın sorunsuz bir şekilde çalıştırılmasını sağlama potansiyeli açısından faydalı olabilirler.

İletişim alanında, dış kaynaklar ile http ve/veya https üzerinden iletişim kuran cihazlar için bir Proxy sunucu veya web filtreleme uygulaması kullanıldığı takdirde, güvenlik duvarlarının yapabildiğinden çok daha sıkı kontrol sağlanabilir. Ayrıca çoğu proxy sunucunun, web trafiğini olası virüslere karşıt arama özelliği de bulunmaktadır. Proxy sunucularda, iç ağdaki uç cihazlarda kullanılandan farklı bir anti virüs (AV) motoru kullanılması halinde, kötü amaçlı yazılım vektörünün tespit edilebilmesi şansını artıracaktır.

**7) PACS cihazlarına özgü Query Retriwe özelliği kapatılmalıdır (C-GET ve C-MOVE özelliği).** Örneğin ücretsiz olarak kullanılan Open Source Microdicom programı kapatılarak kendine has PACS özellikleri belirlenerek doğrulamalar yazılım tarafında belirlenen PACS programlarına izin verilebilir. Yazılımsal olarak bir erişim ID’Sİ belirlenebilir.

**8) PACS Sunuculara Erişim Loglarının Kaydedilmesi**

Mümkün olduğunca, tıbbi cihazlardaki iz bilgileri (log) sadece cihazın kendisinde depolanmamalı, cihazı etkileyen olayların toplanabilmesi ve analiz edilebilmesi için aynı zamanda tamamen ayrı bir syslog sunucusuna da aktarılmalıdır. Tıbbi cihazın kendisinin artık güvenilir olmayabileceği veya cihazda kayıtlı olan veri günlüğünün bir güvenlik probleminden dolayı artık ulaşılamaz olabileceği durumlara karşı bir önlem olarak, bilgilerin tamamen farklı bir syslog sunucusuna ya da SIEM ürününe aktarılması kritik önem taşımaktadır.

**9) Sahte DNS’lerden Kaçınma için PACS Vlanına Özgü DNS Server Kullanma**

Düzgün bir şekilde çalışması için DNS sunucusu bağlantısı ihtiyacı olan tıbbi cihazlar büyük ihtimalle sınırlı sayıda adres ihtiyacı duymaktadır. Bir tıbbi cihazın kurulum güvenliği, bu cihazların düzgün performans gösterebilmesi için gerekli olan sınırlı sayıdaki IP adresinde ortaya çıkacak problemlere çözüm üretebilen, o spesifik cihaza özel DNS sunucuları oluşturarak iyileştirilebilir. Diğer tüm DNS istekleri yok edilebilir.

**10) Varsayılan Uygulama Ayarlarını Değiştirme**

Yakın geçmişte meydana gelen “Mirai” ve “Bashlight” saldırılarında da gördüğümüz üzere, varsayılan değer bilgilerinin varlığı, herhangi bir IoT cihazı bu tür saldırılar karşısında savunmasız bırakabilir ve tıbbi cihazlar için de aynı risk söz konusudur. Dolayısı ile bir cihazın ağ bağlantısı yapılmadan önce mutlaka varsayılan değer bilgileri değiştirilmelidir ve bilgileri sabit kodlu olan cihazlar kesinlikle kullanılmamalıdır. Varsayılanların yerine kullanılan hesap bilgileri kurumsal şifre ilkelerine uygun olmalıdır.

**11) Hesap Kilidi İlkesinin Uygulanması**

Eğer cihaza bir “sözlük saldırısı” veya “kaba kuvvet saldırısı” ile hücum etmek kolay ise, bu durumda var olan şifreyi değiştirmenin de bir anlamı yoktur. Hesap kilitleme yaparken, 3-5 kez oturum açma girişiminde bulunulduktan sonra o hesaba giriş yapmayı engelleyecek şekilde konfigüre edilmelidir /yapılandırılmalıdır.

**12) Yönetim Arayüzüne Erişimin Engellenmesi**

Yönetim arayüzü bir cihazın yönetimsel fonksiyonlarına erişime çok kolay izin verdiğinden dolayı, bir cihaz risk altındayken ona en büyük zararı verme potansiyeline sahip olan şey o cihazın yönetim arayüzüdür. Bu cihaz üzerinde herhangi bir değişiklik yapılacağı zaman, cihazla iletişim kurma izni sadece yetkili terminaller ile kısıtlanmalıdır.

**13) Düzenli Güncelleme ve Cihaz Ayar ve Veri Yedekleme Mekanizmalarının Kurulması**

Yeni yazılımı/donanımı ister otomatik olarak yüklenmiş isterse elle kurulum yapılmış olsun, tüm cihazları bir noktada güncellemek gerekmektedir. Tamir edilmeyen güvenlik açıklarını mümkün olduğunca en aza indirebilmek için hem dönem dönem ortaya çıkacak olan güncelleme ihtiyaçlarının belirlenebilmesi hem de tüm tıbbi cihazların rutin güncellemeleri yapılabilmesi amacıyla düzenekler devreye sokulmalıdır.

**14) Cihaz Belleklerinin Şifrelenmesi ve İletişiminin Şifreli Şekilde Yapılması**

Tıbbi cihazlar, bu cihazlarda saklanan kişisel sağlık verilerini ve kişiyi tanımlamada kullanılan diğer verilerin şifrelenmesini desteklemelidir. Cihazın çalınması veya yetkili olmayan bir kimsenin cihaza fiziksel erişimi durumunda bu özellik hemen aktive edilmelidir.

Yeni yazılımı/donanımı ister otomatik olarak yüklenmiş isterse elle kurulum yapılmış olsun, tüm cihazları bir noktada güncellemek gerekmektedir. Tamir edilmeyen güvenlik açıklarını mümkün olduğunca en aza indirebilmek için hem dönem dönem ortaya çıkacak olan güncelleme ihtiyaçlarının belirlenebilmesi hem de tüm tıbbi cihazların rutin güncellemeleri yapılabilmesi amacıyla düzenekler devreye sokulmalıdır.

**15) Fiziksel Güvenlik Önlemlerinin Uygulanması**

Tıbbi cihazlara fiziksel erişim sadece yetkili kişiler ile sınırlandırılmalı ve cihazın çalınmasını engelleyebilmek için düzenli olarak güvenlik kontrolü yapılmalıdır.