OWASP

Güvenli Tıbbi Cihaz Kurulum Standardı

Christopher Frenz

Türkçe'ye Çeviren

Erdal YILDIZ

Versiyon 1.0 20.03.2017

Giriş

Günümüzde elektronik tıbbi kayıt sistemlerinin her geçen gün daha da çoğalması ve ağ destekli tıbbi cihazların kullanımının giderek yaygınlaşması sayesinde, hastaneler ve diğer sağlık tesisleri bugüne dek hiç olmadığı kadar birbirlerine bağlı olarak çalışmaktadır. Sürekli artan bu karşılıklı bağlılık içinde çalışma durumu, hasta bakımında kalite ve verimliliği olumlu yönde etkilese de, olası bazı güvenlik sorunlarını da beraberinde getirmektedir. Çoğu tıbbi cihazın yazılım sürümünün yükseltilmesi ya da yenisi ile değiştirilmesi son derece maliyetli bir iştir ve bu eski cihazlar birçok sağlık tesisinde yaygın olarak kullanılmaktadır. Ayrıca, çoğu tıbbi cihaz tasarlanırken esas olarak hastanın güvenliği ve hayat kurtarma fonksiyonları göz önünde bulundurulmuş, bu cihazların siber güvenliğine ise maalesef neredeyse yok denecek kadar az önem verilmiştir. Bu eğilim, hem kısa bir süre önce FDA'nın (Amerikan Gıda ve İlaç Dairesi) bu konu hakkında yayınladığı dokümanlarda, hem de birçok tıbbi cihazın güvenlik açıkları ile dolu olduğunu ispatlayan sayısız güvenlik araştırması/çalışması sayesinde açığa çıkartılmıştır. Hastanelerdeki bu tür ağ destekli tıbbi cihazların kurulumu yapılırken, genellikle güvenlik kavramı göz ardı edilmektedir ki bu da güvenlik meselesini zaman içinde daha da zora sokmaktadır. Günümüzde, bir alt grubunun da tıbbi cihazlar olduğu "IoT cihazları"nı (bir ağa kablosuz olarak bağlanabilen ve veri transferi yapabilen her tür standart dışı bilgisayara verilen ad) hedef alan "botnet"ler (çok sayıda bilgisayarın bir IP adresine saldırması) ve "kötü amaçlı yazılımlar"da meydana gelen patlama ile birlikte, tıbbi cihazların kurulumunda güvenlik kriteri hiç olmadığı kadar hayati bir önem kazanmıştır. Bu doküman, sağlık tesislerindeki tıbbi cihazların güvenli bir şekilde kurulumuna çok kapsamlı bir rehber niteliği taşımaktadır.

Satın Alma Kontrolleri

Sağlık hizmeti veren bir ortamda güvenliği muhafaza etmenin en iyi yollarından bir tanesi, bu ortamda sadece makul güvenlik tedbirlerine sahip tıbbi cihazların kullanıldığına emin olup, böylece güvenlik açığı oluşmasını engellemek için önceden önlemler almaktır.

Güvenlik Denetimi/Değerlendirmesi

Herhangi bir tıbbi cihaz satın alınmadan veya bir ağa bağlanmadan önce, cihazın söz konusu kurumun kendi kurumsal güvenlik standartları (cihaz parola ilkesi, hesap kilitleme ilkesi ve kurumun çok önemli saydığı diğer güvenlik kontrolleri ile uyumu) ile karşılaştırılmalı ve standartları karşılayıp karşılayamayacağına dair iyi bir karar verilmelidir.

Gizlilik Denetimi/Değerlendirmesi

Aynı şekilde, herhangi bir sistemi satın alıp kullanmadan önce, cihazın hasta ile ilgili verileri kurumsal ilkeler doğrultusunda toplama, depolama ve aktarma için gerekli güvenlik kontrollerine sahip olduğunu garanti altına almak adına bir gizlilik değerlendirmesi yapılmalıdır. Uygulanabildiği yerde, "Dizayn Gizlilik İlkesi (Privacy by Design)" mantığı ile tasarlanmış çözümler tercih edilmelidir.

(https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).

Satış Sonrası Destek

Satın alınan her tıbbi cihaz, satıcı tarafından sadece belirli bir süre için desteklenebilecektir. Her türlü güvenlik açığının onarılmasının sistemin genel güvenliğini sağlamaktaki kritik önemi göz önünde bulundurulduğunda, cihazı satan firmanın o cihazın yazılımı ile ilgili ne tür bir destek sağlayacağına, piyasaya ne kadar sıklıkla yama (patch) süreceğine ve bu desteği toplam kaç yıl boyunca vermeye devam edeceklerine özel olarak dikkat edilmelidir. Çoğu tıbbi cihazın uzun yıllar boyunca aktif olarak kullanılacağı düşünüldüğünde, sistemin de uzun yıllar boyunca bakım onarım desteği olması, satın alma kararı verme aşamasında güvenlik meselesi ile ilgili en kritik değerlendirme noktası olmalıdır. Ve dolayısıyla, bu endişe satıcılar ile de açıkça paylaşılmalıdır.

Sınır Güvenlik Sistemleri

Tıbbi cihazların, mümkün olduğunca, harici olan herhangi bir şeye erişimi engellenmelidir. Ancak sunucuların güncellenmesi, makinalardaki tıbbi kayıt sistemlerinin buluta 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.

Güvenlik Duvarları

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.

Saldırı Tespit Sistemi

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.

Proxy Sunucular/Web Filtreleri

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 karşı tarama 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. Tüm bunlara ek olarak, birçok Proxy cihazının SSL ayırma (SSL stripping) yeteneği de bulunmakta ve bu özellik kurumsal Veri Kaybı Önleme (DLP-Data Loss Prevention) Sisteminin bir parçası olarak da kullanılmaktadır. DLP sistemlerinin, bir şekilde internet erişimi gerektiren tıbbi cihazlarda kullanımı kesinlikle tavsiye edilmektedir ama normal şartlarda, bir dış varlığa kişisel sağlık verisi veya kişiyi ayırt etmeye yarayan diğer veriler gönderilirken, DLP kullanılmaz.

Ağ Güvenlik Kontrolleri

Ağ Segmentasyonu/Bölütlemesi

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 segmenti/bölütü (VLAN) olmalıdır. Diğer tüm iletişimler sınırlandırılmalıdırlar. VLAN'lardaki trafiği kontrol altında tutmak için kullanılan ağ segmentasyonu, 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.

İç/Dâhili Ağ Güvenlik Duvarı

İç/dâhili ağ güvenlik duvarları, hem ağ segmentasyonunu iyileştirmek için hem de bu tıbbi cihazların çalışabilmeleri için etkileşim halinde olmaları gereken iç ve dış sistemler ile olan iletişimini daha da fazla kısıtlamak amacıyla kullanılabilir. Güvenlik duvarları, özellikle de yeni nesil modeller, çok daha derin seviyelerdeki trafiği denetleyebilme özelliklerinden dolayı, anahtarlardaki ACL'lerden farklı olarak trafiği daha iyi takip altında tutabilirler ve gerektiğinde kısıtlayabilirler. İç ağ güvenlik duvarları ayrıca MR makinesi gibi tek başına olmasının şart olduğu, ancak bir tek cihazın tamamen ayrı bir fiziksel ağ altyapısını almaya yeterli olamayacağı tek kullanımlık kullanılan cihazları korumak için de çok faydalıdır. İç ağ güvenlik duvarları, tıbbi cihazlar ile iletişim açısından da sıfır-güvenilirlik modeli geliştirilmesini destekler.

İç Ağ Saldırı Tespit Sistemi

Tıbbi cihazlarda de dâhil olmak üzere, ağ segmentlerinden/bölütlerinden akan trafik bir iç ağ saldırı tespit sistemine yönlendirilebilirse; varsayılan kullanıcı giriş bilgilerini, zararlı yazılımları yöneten komuta ve kontrol IP'lerine bağlanmak için yapılan girişimleri ve tıbbi cihazlara yapılabilecek bir saldırıyı gösteren, farklı tiplerdeki ağ trafiğini saptamak için imzalar oluşturulabilir. İç ağ saldırı tespit sistemi, fonksiyonu açısından sınır güvenlik sistemlerinde kullanılan saldırı tespit sistemine benzer olmakla beraber, iç ağda yer alan riskli bir uç cihazın diğer tıbbi cihazlara herhangi bir saldırı başlatmak amacıyla kullanılabileceğini de dikkate alır.

Syslog Sunucuları

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 aktarılması kritik önem taşımaktadır.

İz Bilgisi Görüntüleme ve Analiz Sistemleri

Yukarıda bahsedilen kontrole bağlı olarak, toplanan iz bilgileri üzerinde Bilgi Güvenliği Tehdit ve Olay Yönetimi (SIEM-Security Information and Event Management) araçları kullanılmak suretiyle analiz edilmelidir. Örneğin, bir cihaza giriş yapmaya çalışırken çok fazla sayıda hata oluştuysa, ya da tam tersi, çok sayıda cihaza hiç problem yaşamadan sayısız defa başarılı bir şekilde giriş yapılabildiyse (planlı bakımın dışında), bu durum IoT cihazları için yazılmış "Mirai" virüsünden kaynaklanan bir saldırının habercisi olabilir.

Güvenlik Açığı Taraması

Tıbbi cihazların düzgün bir şekilde yapılandırıldıklarına emin olmak ve güncelliğini yitirmiş yazılımlar yüzünden bu cihazların tehlikelerin hedefi haline gelmeyeceklerine garanti altına alabilmek için düzenli olarak taramadan geçirilmeleri gerekmektedir. Dolayısı ile tıbbi cihazlar, kurumun daha kapsamlı olarak kullanmakta olduğu Güvenlik Açığı Yönetimi programına dahil edilmelidir. Bütün IoT cihazlar ve onların tüm teknolojik özellikleri, eskiden beri kullanıla gelmekte olan güvenlik açığı tarayıcıları tarafından taranamayabilir. Özel bir tarayıcı kullanmak gerekebilir. Hatta özel bir tarayıcı kullanılsa bile, IoT cihazların o kadar çok değişik çeşitleri var ki aşağıda "cihaz güvenliği" bölümünde de anlatılacağı üzere, bazı durumlarda manuel olarak "uyum denetimi" yapmak gerekebilir.

Sahte DNS'lerden Kaçınma

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.

Cihaz Güvenlik Kontrolleri

Ağ destekli herhangi bir tıbbi cihazı korumak için gerekli olan en kritik kontrol mekanizmalarından bazılarının, cihazın kendi içinde uygulanması gerekmektedir. Bunlar, bu tür kontrollerde fayda sağlayacağına inanılan, şiddetle tavsiye edilen konfigürasyonlardır. Tüm cihazlar aşağıda sıralanan kontrolleri desteklemeyecektir, ancak bir cihazı satın almadan önce gerekli güvenlik denetimleri yapılmalı ve bu tür kusurlar tespit edilmiş olmalıdır.

Varsayılan Uygulama Ayarlarını Değiştirme Bilgileri

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.

Hesap Kilidi

Eğer cihaza bir “sözlük saldırısı” veya “kaba kuvvet saldırısı” ile hücum etmek kolay ise, bu durumda varolan 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.

Verilerin Güvenli Bir Şekilde Taşınması

Cihazlar, verilerin sadece güvenli bir format ve SSH gibi güvenli iletişim protokolleri aracılığı ile gönderilmesini mümkün kılacak şekilde yapılandırılmalıdır. Ayrıca, telnet ve http gibi güvenli olmayan iletişim protokolleri yerine https kullanılmalıdır. Güvenli olmayan ağ protokolleri mümkün oldukça devre dışı bırakılmalıdır.

Bellenim ve Yazılımların Yedeklenmesi

Bir cihaz risk altında olduğunda veya başka türlü yazılım problemleri ile karşılaşıldığında, bu cihazın bellenim veya yazılım programlarının bir yedeğinin bulunması cihazın bir an evvel tekrar çalışır duruma getirilebilmesi açısından kritik bir önem taşımaktadır. Personel değişik tipteki cihazların desteklediği yazılım programlarını yüklemek ve gerektiğinde yeniden yüklemek konusunda eğitilmiş ve yetkin kişiler olmalıdır.

Cihaz Konfigürasyonlarının Yedeklenmesi

Bir cihazı çalıştırmak için kullanılan yazılım programı veya bellenime ek olarak, o cihazın ağınızda düzgün bir şekilde çalışmasını sağlamak için büyük ihtimal ile bir de özel yapılandırma yapmak gerekecektir. Değişiklikler oldukça bu özel ayarları yedeklemiş olmak, cihazın en kısa zamanda tekrar çalışır duruma gelmesini sağlayacaktır.

Giriş (Baseline) Konfigürasyonu

Yukarıda anlatılan kontroller ile ilişkili olarak, her cihazın klinik işlevselliğini ve güvenliğini garantiye almak üzere, her bir cihazın tek tek temel giriş ayarlarının yapılması gerekmektedir. Spesifik bir cihaza ait yedek kurulumların olmaması veya bulunamaması halinde, giriş konfigürasyonları , bu spesifik cihazın kurumsal güvenlik prensipleri ile uyumlu bir şekilde tekrar çalıştırılabileceği şekilde değiştirilebilir.

Belleğe Şifre Koymak

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.

Farklı Kullanıcı Hesapları

Farklı yönetici hesapları ve kullanıcı hesapları olmalıdır. İdeal olanı, yönetici hesabı yönetim arayüzüne bağlı olmalı ve bu arayüze internet üzerinden erişim engellenmeli veya kısıtlanmalıdır.

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.

Güncelleme Mekanizmaları

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.

Uyumluluğun İzlenmesi

Zaman içinde tüm sistemlerde değişiklikler yapılır ve uygulanan güncellemeler yüzünden cihazlarda yeni değişiklikler yapılması gerekebilir. Bu güncellemelerin ve diğer değişikliklerin, cihazdaki yapılanmalar ile giriş (baseline) ayarlamaları ve kurumsal güvenlik ilkeleri arasında bir istikrar sağlayıp sağlamadığına emin olmak için rutin olarak uyumluluk gözlemi yapılmalıdır.

Fiziksel Güvenlik

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

Varlık Yönetimi

Hangi cihazın nerede olduğunu takip etmek ve hangi yazılımı/donanımı kullandığını bilmek, olası bir hadisenin kapsamını önceden belirleyebilmek için paha biçilemez bir bilgi kaynağıdır. Bu bilgiler aynı zamanda, yaşanan bir probleme çözüm üretme aşamasında da son derece kıymetlidir.

Arayüz ve Merkezi Birim Güvenliği

Tıbbi cihazları kontrol eden merkezi birimler veya kontrol bilgisayarlarında saklanan verilere erişim ve elektronik tıbbi kayıt sistemine veri transfer etmek üzere, söz konusu cihazlara bir, hatta kimi zaman daha fazla sayıda bilgisayar bağlanması oldukça sıkça görülen bir durumdur. Tüm bu cihazlar genellikle aynı sistem üzerinde yer alırlar. Aşağıdaki güvenlik kontrolleri bu sistemler ile ilgilidir. Arayüz sistemleri ise tıbbi cihaz ağı ile kurumun esas yerel alan ağındaki sistemlerin birleştikleri noktalar oldukları içinarayüz güvenliğini sağlamak da büyük bir önem arz etmektedir.

İşletim Sistemini Sıkılaştırma

Bu elinizdeki rehber sizi özel olarak tıbbi cihazlar konusunda aydınlatmak için hazırlandığından dolayı, burada işletim sistemi sıkılaştırma tekniklerinin ince detaylarına değil de gereksiz hizmetlerin kaldırılması, şifre koruma, antivirüs yazılımı kurulumu, ve çok yaygın olarak kullanılan diğer bazı işletim sistemi sıkılaştırma tekniklerine değineceğiz. Kendi özel işletim sisteminizle ilgili daha detaylı bilgi alabilmek için lütfen bir danışmana başvurunuz.

Şifreli Veri Aktarımı

Tıbbi cihazların kendilerinde olduğu gibi, merkezi birimler ve arayüz sistemleri de veri göndermek ve almak için kullanılır. Dolayısı ile bu sistemlere de “cihaz kurulumu bölümünde” bahsedilen güvenlik konfigürasyonları yapılmalıdır.

Mesaj Güvenliği – HL7 v3 Güvenlik Standartları

Arayüz sistemleri genellikle bir kurumun EHR, PACS ve diğer klinik sistemlerine veri transferi yapmak için kullanılırlar. Bunu başarmak için kullanılan standart format ise HL7 mesajlarıdır. HL7 mesaj alışverişi HL7 v3 standardı kullanılarak yapılmalıdır. Çünkü bu standart, HL7 standardının daha eski versiyonlarında bulunmayan bir güvenlik önlemi sağlamaktadır.

Güvenlik Testleri

Yanlış ayarlamalar/konfigürasyonlar ve güvenlik açıkları her yerde kol gezip dururken, dünyadaki hiçbir güvenlik kontrolü yüzde yüz güvenliği sağlayamaz. Güvenlik testleri, cihazlarınızın kendi içindeki ya da kurulumundaki kusurları ortaya çıkartmanıza yardımcı olacaktır. İleride tekrar aynı sorunları yaşamaktan, hatta belki de adli makamlara şikayet konusu olacak vakalar yaşamaktansa, bu tür problemlere hemen çözüm üretebilmek ya da daha yeterli bir kontrol mekanizması kullanabilmenin en iyi ve en akla yatkın yolu, güvenlik testi yapmaktır.

Penetrasyon Testi

Penetrasyon testi, cihazınızın ve ağ yapılandırmalarınızın /konfigürasyonlarınızın, ağınıza kurulumu yapılmış olan tıbbi cihazınıza yapılan saldırıları geri püskürtmekte ne kadar işe yaradığını değerlendirebilen etkili bir araçtır. Böylece, elde edilecek sonuçlar hem savunma mekanizmalarınızı güçlendirmek için kullanılabilir; hem de cihazda tespit edilen kusurlar üreticiye bildirilerek, firmanın piyasaya süreceği bir sonraki güncelleme sürümünde bu sıkıntılara bir çözüm üretmesi sağlanabilir.

Olay Müdahale

Bütün kurumlar eninde sonunda bir veya belki de daha fazla sayıda cihazda çeşitli riskler ve tehlikeler ile karşı karşıya gelirler. Profesyonelce hazırlanmış bir güvenlik kontrol programı olan kurumları, böyle bir programı olmayanlardan farklı kılan şey, onların bu tür tehditleri tespit etmekte, kontrol altına almakta ve yok etmekte ne kadar etkili olduklarıdır.

Olay Müdahale Planı

Kurumlar, olası sıkıntılar gerçeğe dönüşmeden önlem alınabilmesi maksadıyla, tıbbi cihazlarında yaşamaları muhtemel problemler ile nasıl başa çıkacaklarına dair detaylı planlar hazırlamalıdır. Planda; herhangi bir probleme nasıl müdahale edileceği; problemin tespiti, kontrol altına alınışı, ortadan kaldırılışı ve durumun iyileştirilmesi aşamalarında kimin hangi işten sorumlu olacağını bildiren hususlar ayrıntılı olarak yer almalıdır. Ayrıca gerektiğinde uygun ve etkin bir şekilde duruma müdahale edilebilmesi maksadıyla bütün personel önceden plan hakkında çok detaylı bilgilendirilmeli ve eğitilmelidir. Henüz böyle iyi bir plan yapmamış kurumlar için aşağıdaki bağlantı iyi bir bilgi kaynağı olabilir:

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Olay Müdahale Tatbikatı

Kurumlar, olay müdahale planlarının ne kadar etkin olduğunu ve ayrıca personelin olaylara müdahale etmek konusunda ne kadar yetkin olduklarını test edebilmek için kendi üretecekleri arıza senaryoları ile tatbikat yapmalıdırl. Bu tatbikatlar, sistemdeki güvenlik zafiyetlerini tespit etmenin yanı sıra, personele pratik yapma imkanı sağlayacak, ve böylelikle yapılan hatalardan ve edinilen tecrübelerden öğrenilecek dersler gelecekte kurumun güvenlik ile ilgili tutumunu iyileştirebilmek için kullanılacaktır.

Teşekkür

Tıbbi cihazlar ile ilgili verdiği bilgilerden dolayı Tony Alas'a teşekkürlerimizi sunarız.