****

**T.C.**

**ATATÜRK ÜNİVERSİTESİ**

**Mühendislik Fakültesi**

**Bilgisayar Mühendisliği**

**DERSİN ADI**

**BMS-302 Bilgisayar-Bilgi Güvenliği ve Yönetimi**

**ÖDEV KONUSU**

**Yaygın Sistem Tasarımı Kusurları ve Güvenlik Sorunları**

**Fiziksel Güvenlik: Kıvrımlı Erişim ve Katmanlı Savunma**

**Öğrencinin Adı**

**Mücahit ÖZGÜN**

**150707021**

**Dersin Öğretim Görevlisi**

**Prof. Dr. Abdulsamet HAŞILOĞLU**

**İÇİNDEKİLER**

1. Giriş
2. Güçsüz Kısıtlamalar
3. Karmaşa
4. Eksik Parametre Kontrolü
   1. Eksik Parametre Kontrolü Uygulaması
5. Eksik Hata İşleme
6. Kullanım Süresi
   1. Kontrol Süresi
7. Etkin Olmayan Ciltleme
8. Kontrollerin Yetersiz Granülerliği
9. Gratuitous İşlevselliği
10. Kaçış Mekanizmaları
11. Aşırı Ayrıcalık
12. Ayrıcalıklı Durum
    1. Ayrıcalıklı Durum Başarısızlığı
13. Güvensiz Varsayılanlar
14. Uygulama Kontrolleri
    1. Uygulama Kontrollerine Özel Güven
15. Öneriler
16. Fiziksel Güvenlik: Kıvrımlı Erişim ve Katmanlı Savunma
17. Fiziksel Güvenliği Yaklaşımı
18. Fiziksel Güvenlik Psikolojisi
19. Tesis Fiziksel Güvenlik
    1. Tesis Sınıflandırması
    2. Tesis lokasyonu
    3. Fasite Tehditleri ve Kontrolleri
    4. Doğal Tehditler
    5. İnsan Yapımı Tehditler
    6. Çevresel Tehditler
    7. Tesis Koruma Stratejisi
       1. Zoning
20. Bilgi Sistemleri Fiziksel Güvenlik
    1. Bilgi Sistemi Sınıflandırması
    2. Bilgi Sistemleri Fiziksel Tehditler ve Kontroller ve farkındalık Eğitimi
21. Kaynakça
22. **GİRİŞ**

Bu bölüm, uygulama ve sistem tasarımındaki yaygın hataların çoğunu tanımlar ve açıklar. Bu hataların sonuçlarını açıklar ve onlardan kaçınmak için önerilerde bulunur. Zorlanmamış kısıtlamalar, karmaşıklık, eksik parametre kontrolü ve hata yönetimi, basit işlevsellik, kaçış mekanizmaları ve güvenli olmayan işlem yapar. Turing Ödülünü kabul ettiğinde Ken Thompson bize bir program yazmazsa, biri tamamen ona güvenemez. Çoğu kişi, bir program yazmanın faydalı olsa bile yararlı olabileceğini fark eder. Yani, en yetenekli ve motive programcılar bile hatalar yapar. Öte yandan, birinin kullandığı her programı yazmak zorunda olsaydı, bilgisayarlar çok kullanışlı olmazdı. Güvenilir kod yazmayı ve tanımayı öğrenmek önemlidir. Tarihsel olarak, bilgisayar güvenlik topluluğu dış kaynaklı kontrollere güvenmeyi tercih etmiştir. Uygulama. Topluluk, bu kontrollerin daha güvenilir, etkili ve verimli olduğuna inanıyordu. Onlar daha güvenilir olduğu düşünülüyor çünkü daha az insanın kendileri üzerinde etkisi var ve bu insanlar daha uzak uygulamadan. Bypass' a daha dayanıklı oldukları için daha etkili oldukları düşünülmektedir. Onlar daha verimli oldukları düşünülmektedir, çünkü bunlar arasında çalışırlar ve birkaç uygulama tarafından paylaşılırlar. Bununla birlikte, uygulama kontrolleri her zaman önemli olmuştur. Ancak, modern sistemlerde, uygulama kontrollerine güven daha da artar. Uygulama oluşturucu, programının çalışacağı çevre hakkında bir fikre sahip olsa da, bunu belirleme yeteneği ve kontrol çok düşük olabilir. Aslında, uygulamaların crossplatform dillerinde yazılması giderek daha yaygındır. Bu diller yazarın programında çalışıp çalışmayacağını bilmesini zorlaştırır. Tarihsel olarak, biri uygulamayı dış müdahale veya kirlenmeden korumak için çevreye güveniyordu; Modern sistemlerde, kendisini trafikten korumak için uygulamaya güvenmek gerekir. Dağıtık sistemlerde, çevresel kontroller geleneksel sistemlerden çok daha az güvenilirdir. Söylemek değil, yaygınlaştı. Rutin, uygulamalar tarafından kirletilecek sistemler için. Sektörün hızlı büyümesi sınırlı tecrübeye sahip kişilerin birçok program yazdığını göstermektedir. Çevre ve girdiler uyumlu olduğunda iyi işleyen kod yazmaları için yeterince zordur beklentilerine göre, değilken daha az. Uygulamalardaki kontrollerin geçmişi çok iyi olmamıştır. Piyasa için programlar yapılmış olmasına rağmen oldukça iyi, bir girişim için özel olarak yapılmış olanlar genellikle felakettir. Daha kötüsü, aynı hata türleri, 20 yıl önce görüldüğü gibi kendini gösterir.

Bu bölüm, bazı daha yaygın hataların bazılarını ve bunların çözümlerini ümit ederek açıklar ve tartışır. Gelecekte daha güvenilir programlar olacak. Her ne kadar göstermek için bazı çizimler kullanılsa da, bu hataların nasıl kötüye kullanılması, okuyucudan hataların çoğunun akılda tutulması gerektiği sorulur.

1. **GÜÇSÜZ KISITLAMALAR**

Hesaplamanın ilk günlerinde, program yazarlarının kullanıcılardan gelen hata raporlarına yanıt vermesi alışılmadık bir durum değildi. Programı değiştirmek yerine belgeleri değiştirerek yapılırdı. Programı düzeltmek yerine, aksi halde meşru olan girdilerin belirli bir kombinasyonu programın başarısız olmasına neden olmaz, programcılar “Bu giriş kombinasyonunu girmeyin, çünkü aşağıdakilere neden olabilir; öngörülemeyen sonuçlar. “ Genellikle, bu sonuçlar o kadar tahmin edilemezdi ki, yıkıcı olsalar bile sömürülmezdi. Her zaman ve sonra, sonuç kötü amaçlı amaçlar için sömürülebilecek bir sonuçtu. Bir uygulamanın doğru davranışının sağlanan girdiye bağlı olması alışılmadık değildir. Bazen programın doğru girişi sağlamak için kullanıcıya bağlı olması. Program kullanıcıya yapmasını söyleyebilir ve yapılmaması gereken B. Bunu yaptıktan sonra, program kullanıcının her zaman söylediği gibi yapacağı gibi davranır. İçin. Örneğin, programcı, alfa karakterleri sayısal olarak belirtilen belirli bir alana koymanın farkında olabilir. Programın başarısız olmasına neden olabilir. Programcı, ekrana veya ekrana bir uyarı bile verebilir. Bu alana yalnızca sayısal karakterler koyun.” yazan belgeler. Programcının yaptığı şey bu değildir. Verileri kontrol edin veya alfa verilerinin hataya neden olmayacağı şekilde girişi sınırlayın. Tabii ki, pratikte, nadiren uygulamanın başarısız olmasına neden olan tek bir girdidir. Daha sık, belirli bir nadiren bile olsa, arızaya sebep olan girdilerin kombinasyonu. Programcıya bu kadar nadir gibi görünüyor birleşim asla gerçekleşmeyecek ve programlanmaya değmez.

1. **KARMAŞA**

Karmaşıklık kendi başına bir hata değildir. Ancak, bilgisayardaki her zaman birincil hata kaynaklarından biri olmuştur. Programları. Karmaşıklık bazı hatalara neden olur ve kötülüğü maskelemek için kullanılabilir. Sadelik, anlayışı maksimuma çıkarır ve kötülüğü ortaya çıkarır. Bir programın kapsamını sınırlamak, karmaşıklığını sınırlamak ve bunu sağlamak için yeterli değildir niyeti açıktır. Bir program kapsamını ne kadar fazla sınırlarsa, yaptığı şey o kadar açık olacaktır. Üzerinde öte yandan, bir tanesi tüm programların kapsamını ne kadar fazla sınırlarsa, o kadar fazla program o kadar sona erer. İnsanoğlu karmaşık şeyleri daha iyi ve daha basit hale getirerek onların anlayışını geliştirir. Parçalar. Bir bilgisayar programının atomik birimi bir talimattır. Programlama hakkında düşünmenin bir yolu bir programı atomik talimatlarına bölme sanatıdır. Biri tüm programları bire düşürmekseler birine talimat verildiğinde, o zaman tüm programlar basit ve anlaşılması kolay olacaktır, ancak birçok program olacaktır ve aralarındaki ilişkiyi anlamak karmaşık ve zor olurdu. Büyük programlar mutlaka kısa programlardan daha karmaşık olmayabilir. Ancak, bir kural olarak, daha büyük bir program, anlamak daha zor. Bir bilgisayarın boyutuna veya kapsamına bağlı bir üst kısım var bir insan tarafından anlaşılabilecek bir program. Programın boyutu arttıkça, Bunu anlayabilen insanlar sıfıra yaklaşır ve bu anlayış için gereken sürenin uzunluğu sonsuzluğa yaklaşır. Biri tam olarak bu geçişin nerede olduğunu söyleyemese de, değil gerekli. Bu noktaya ulaşmadan çok önce, program modülleri yararlı işler yapacak kadar büyük olabilir. Mesele, programların yararlı işler yapacak kadar büyük ve yeterince küçük olacak bir dengeye oturtulması. Kolayca anlaşılmak. Konfor bölgesi, 10 ile 50 arasında fiil ve biri arasında olmalıdır tam işlev ve bir sayfa.

Bir programın karmaşıklığının bir başka ölçüsü, programın içinden geçen toplam yol sayısıdır. Basit bir program üstündeki girişinden altındaki çıkışına kadar bir yolu vardır. Birkaç program bu şekilde görünüyor; çoğu olacak bazı yinelemeli döngüler içlerinde. Bununla birlikte, toplam yol sayısı düşük seviyelerde olduğu gibi hala numaralandırılabilir.

AU1997\_Frame\_Ch126 Sayfa 1548 14 Kasım 2003 Cuma 06:03

Genel Sistem Tasarım Hataları ve Güvenlik Sorunları 1549 bu döngüler sadece sıra ile birbirlerini takip ettikleri veya kucakladıkları ancak geçmedikleri sürece. Yollar başladığında çapraz, toplam olası yol sayısı hızla artar. Sadece anlamak daha zor hale gelmez. Her bir yol ne yaparsa, bir yolun kullanılıp kullanılmadığını (yani gerekli olup olmadığını) bilmek zorlaşır.

1. **EKSİK PARAMETRE KONTROLÜ**
   1. **Eksik Parametre Kontrolü Uygulaması**

Girdi parametrelerinin kontrol edilmemesi, Birinci Günden bu yana uygulama hatalarına neden oldu. Modern sistemlerde uzunluğu kontrol etmeme büyük bir güvenlik açığıdır. Her ne kadar modern veri tabanlarının uzunluğu çok hassas olmasa da, çoğu sistem giriş uzunluğuna bir dereceye kadar duyarlıdır. Yakın tarihli bir saldırı, e-posta ekinin 64 KB’den uzun bir ad vermesini içeriyordu. Empoze etmek yerine isteğe bağlı bir kısıtlama olarak, tasarımcı, uzunluğun dinamik olarak atanacağını belirtmişti. Altında uzunluklarda64 KB, program iyi çalıştı; Bunun üzerindeki uzunluklarda, giriş program talimatlarını kapladı. Ne programcı, derleyici veya test cihazı böyle bir uzunlukta ne olacağını sormadı. En az iki ayrı işlevin uygulamaları bu şekilde başarısız oldu. Evet, dışarıda gerçekten bu şekilde stres yaratan insanlar var. Biri bunu savunabilir64 KB' den büyük bir dosya adı olup olmadığını kontrol etmeniz gerekmez. Çoğu dosya sistemi kabul etmedi bile böyle bir uzunluk. Neden biri böyle bir şey yapsın ki? Cevap, sömürülebilir bir başarısızlığa neden olup olmayacağını görmektir; Cevap, olduğu gibi. UNIX için pek çok derleyici, programcının arabellek boyutunu uygulama sırasında statik olarak tahsis etmesine izin verir saati. Bu, böyle bir aşırı çalışmayı daha olası kılar ancak performansı artırır. Tamponun dinamik tahsisi kazara aşırı yüklenmeye karşı koyma olasılığı daha yüksektir, ancak kasıtlı olarak aşırı uzun süre kullanan saldırılara karşı kanıt değildir veri alanları. Bu saldırılar genel olarak “arabellek taşması” saldırıları olarak bilinir. Bu sınıftan sonra on yıldan fazla sorun tespit edildi, savunmasız programlar çoğalmaya devam ediyor. Uzunluğa ek olarak, kodu, veri türünü, biçimini, aralığını ve geçersiz karakterleri kontrol etmek gerekir. çok bilgisayarlar birden fazla kod türünü tanır (örneğin, sayısal, alfabetik, ASCII, onaltılık veya ikili).Sık sık, bunlardan biri diğerinde kodlanabilir. Örneğin, bir ikili numara her ikisine de girilebilir. Sayısal veya alfa numerik bir alan. Uygulama programı, kod değerlerinin her ikisinde de yasal olmasını sağlamalıdır kod setleri - giriş ve ekran seti ve depolama seti. Modern veri tabanı yöneticilerinin çok bağışlayıcı, programın çalışmaya devam ettiği gerçeği verilerin doğru olduğu anlamına gelmeyebilir. Veri tipleri (örneğin, alfa, tarih, para birimi) de kontrol edilmelidir. Uygulamanın kendisi ve diğer programlar veriler üzerinde çalışmak tarihlerin ve para birimi biçimlerinin doğruluğuna çok hassas olabilir. Doğru olan veri Kod ve veri türüne göre hala geçerli olmayabilir. Örneğin, ölüm tarihinden sonra olan bir doğum tarihi geçerli bir veri türü olmasına rağmen geçerli değil.

1. **EKSİK HATA İŞLEME**

Parametre kontrol problemiyle yakından ilişkili olarak hata işlemeyle ilgilidir. Çalışan dolandırıcılık sayısı Kökleri, doğru şekilde ele alınmamış masum hatalarda bulunur. Çalışan masum bir hata yapar; hiçbir şey olmuyor. Çalışan zarfı iter; hala hiçbir şey. Çalışan üzerinde şafak başlar hatayı kendi yararına yapabilirdi - ve yine de hiçbir şey olmayacaktı. Geleneksel uygulamalarda ve ortamlarda, bu tür koşullar yeterince tehlikeliydi. Ancak, onlar vardı Çalışanlar tarafından görülmesi en muhtemeldir. Bazı çalışanlar durumu rapor edebilir. Modern ağda, öbür şartların tüm dünyaya görünmesi olağandışı değildir. Görebilen nüfus arttıkça sistem veya uygulama, daha fazla saldırı yaşanması muhtemeldir. Bir saldırgan ne kadar çok hedef görürse o kadar çok büyük olasılıkla başarılı olması, özellikle de saldırısını otomatikleştirebilmesi durumunda. Hatalar üzerine yüklendiğinde, sistemlerin veya uygulamaların olağandışı şekilde başarısız olması olağandışı değildir. Programcılar, programın ilk hatayı bile doğru şekilde işlemesini sağlamak için programlayamaz veya test edemezler, başarılı olanlar için çok daha az. Saldırganlar, diğer taraftan, sömürülebilir koşullar yaratmaya çalışıyor; onlar Her türlü hatalı girişleri deneyecek ve daha sonra bu hataların üstüne daha fazla hata göndereceksiniz. Bu tür bir saldırı olmasına rağmen Hiç bir zarar vermeyebilir, bazen bir hataya neden olabilir ve bazen bir istismara neden olabilir şart. Yukarıdaki gibi, saldırganlar kendi zamanlarını ucuza değerlendirebilir, saldırılarını otomatikleştirebilir ve çok sabırlı.

1. **KULLANIM SÜRESİ**
   1. **KONTROL SÜRESİ**

Son zamanlarda, bir Web posta servisi uygulaması kullanıcısı, Gelen Kutusunu “yer imlerine ekleyebileceğini” ve kapatmadan ve yeniden başlattıktan sonra bile, tekrar oturum açmadan doğrudan gelecekte. Cuma öğleden sonra, kullanıcı bunu bazı arkadaşlarına işaret etti. Cumartesiye kadar, başka bir kullanıcı tanıdı bu çalışmayı yapan şeylerden birinin onaltılık olarak kodlanmış kullanıcı tanımlayıcısının (UID) olduğu; Gelen Kutusu sayfasının evrensel kayıt bulucusuna (URL) dahil edilmiştir. Bu kullanıcı ne olacağını merak etti başka birinin UID' si de aynı şekilde kodlanmış ve URL’ye girmiştir. Okuyucu şaşırmamalı İse yaradığını öğrenmek için. Pazar günü, birileri ASCII’de kodlanmış keyfi bir UID’ yi almak için bir sayfa yazmış, onaltılığa dönüştürün ve doğrudan herhangi bir kullanıcının Gelen Kutusuna gidin. Pazartesi sabahı başvuru yapıldı aşağı çekilmiş. Programcı, kullanıcının URL’sinin URL’sini söylemeden önce oturum açmaya davet edildiğine güvenmiştir. Gelen kutusu. Yani, programcı kontrol zamanı ile kullanım zamanı arasındaki ilişkiye dayanıyordu. Programcı, kontrol edilen bir koşulun doğru olmaya devam ettiğini varsayar. Bu özel durumda, Kararın sonucu, hem tekrar hem de girişime açık olan URL’de saklandı. Sevmek Burada tartışılan sorunların çoğu, bu ilk 30 yıl önce belgelenmiştir. Şimdi hikaye başka bir eski sorunu göstermeye başlıyor.

1. **ETKİN OLMAYAN CİLTLEME**

Burada problem etkisiz bağlanma olarak tanımlanabilir. Programcı, kullanıcının kimliğini doğruladı.

Sunucu, sonucu istemcide depolar. Başka bir deyişle, programcı ayrıcalıklı devleti bir yerde saklar. Güvenemediği ve tekrar oynamaya açık olduğu yer. İstemci / sunucu sistemleri bu hatayı davet ediyor gibi görünüyor. Resmi istemci / sunucu paradigmasında, sunucular vatansızdır. Yani, bir müşteriden bir sunucuya bir talep atomiktir; istemci bir istek yapar, sunucu cevaplar ve sonra öyle yaptığını unutur. Sunucuların durumu hatırladığı ölçüde, hizmet reddi saldırılarına karşı savunmasız kalırlar. Böyle bir saldırı Syn Flood Attack olarak adlandırılır. Saldırgan bir TCP oturumu ister. Kurban isteği kabul ettiren saldırganın oturumu tamamlamasını ve kullanmasını bekler. Bunun yerine, saldırgan başka bir oturum daha ister. Kurban sistemi, tükenene kadar yeni oturumlara kaynak ayırmaya devam ediyor. Sunucu, istemcilerin sayısını tahmin edemediğinden, güvenli bir şekilde birden fazla kişiye kaynak tahsis edemez. Bir seferde bir müşteri. Bu nedenle, tüm uygulama durumları istemcilerde depolanmalıdır. Bu konuda zorluk daha sonra, kullanıcı tarafındaki veya diğer Aynı sistem Sunucu, bu durumun kaydedilmesi, çoğaltılması ve yeniden oynatılmasına açık hale gelir. Bu nedenle, en azından devletin imtiyazlı olduğu ölçüde, bu şekilde kaydedilmesi esastır. Ayrıcalığı ve sunucuyu korumak. Müşterinin durumu korumak için güvenemeyeceği için, koruma gizli kodlara güvenmek zorundadır.

1. **KONTROLLERİN YETERSİZ GRANÜRLERLİĞİ**

Yöneticiler genellikle bir kullanıcıya istediklerinden daha fazla yetki vermeleri gerektiğini veya kullanıcının ihtiyaç duyduklarından fazlasını bulmaları gerektiğini fark ederler. Sistem veya uygulama tarafından sağlanan kontroller veya nesneler yeterince granül değildir. Başka bir şekilde, olağan ve normal görev ayrımını uygulayamazlar. Örneğin, atamak isteyebilirler hesap kurabilenlerin bu hesaplara karşı faaliyet yürütemeyeceği şekilde görevleri, ve tersine. Ancak, uygulama tasarımı her iki özelliği de aynı nesneye koyarsa (ve alternatif kontrol), o zaman her iki birey de yönetimin düşündüğünden daha fazla takdir yetkisine sahip olacaktır. Alışılmadık değil tüm yeteneklerin tek bir nesneye toplandığı uygulamaları görmek için.

1. **GRATUİTOUS İŞLEVSELLİĞİ**

İlgili ancak daha da kötüsü bir tasarım veya uygulama hatası, işlevsellik uygulamasına dahil edilmesidir. Bu kullanım amacı veya uygulama için doğal değildir veya gerekli değildir. Çünkü güvenlik sisteme bağlı olabilir sadece amaçlananı yapmak, bu büyük bir hata ve sorunların kaynağıdır. Bu tür bir işlevselliğin varlığında,AU1997\_Frame\_Ch126 Sayfa 1550 14 Kasım 2003, Cuma 06:03Genel Sistem Tasarım Hataları ve Güvenlik Sorunları 1551yalnızca kullanıcının yalnızca uygun uygulama ayrıcalıklarına sahip olmasını sağlamak değil, aynı zamanda kullanıcı tamamen alakasız bir şey alamaz. Son zamanlarda, bir E-ticaret Web sunucusu uygulamasının uygulayıcısı düşünülemez olanı yaptı; o okudu dokümantasyon. Yazılımın herhangi birini görüntülemek, kopyalamak veya düzenlemek için kullanılabilecek bir komut dosyası içerdiğini buldu. Sunucuya görünür olan veri nesnesi. Komut dosyası, bilgisayara bağlı herhangi bir tarayıcıdan başlatılabilir. Sunucusu. Bu senaryonun kullanımı için gerekli olmadığını kabul etti. Daha da kötüsü, onun sistemindeki varlığı onu ortaya koydu risk; Senaryonun ismini bilen herkes onun sisteminden faydalanabilir. Diğer tüm kullanıcıların olduğunu fark etti.

Uygulama bu komut dosyasının adını biliyordu. Ne kadarını görmek için Net’te bulunan sunucuları aramaya karar verildi. Bu betiğin kopyaları bulunamadı. 100 yaşına geldiğinde saymayı bıraktığı bildirildi. Bunun bir biçimi, programın asıl amacı için tasarlanan kancaları, iskeleleri ya da araçları bırakmaktır. Test amaçlı Bir diğeri ise programın yazarını programdan atlamak için izin veren arka kapıların kullanılmasıdır. Kontrolleri. Yine bir diğeri, başvuru ile ilgili olmayan kamu hizmetlerinin dahil edilmesidir. Daha başarılı ve hassas uygulama, başkaları tarafından keşfedilme ve sömürülme potansiyeli daha yüksek. Daha fazla kopya Kullanılan programın sorunu ne kadar büyükse çözüm de o kadar zor olur. Ücretsiz bir işlevselliğin çok ciddi bir formu bir kaçış mekanizmasıdır.

1. **KAÇIŞ MEKANİZMALARI**

İlgili ancak daha da kötüsü bir tasarım veya uygulama hatası, işlevsellik uygulamasına dahil edilmesidir. Bu kullanım amacı veya uygulama için doğal değildir veya gerekli değildir. Çünkü güvenlik sisteme bağlı olabilir sadece amaçlananı yapmak, bu büyük bir hata ve sorunların kaynağıdır. Bu tür bir işlevselliğin varlığında,AU1997\_Frame\_Ch126 Sayfa 1550 14 Kasım 2003, Cuma 06:03Genel Sistem Tasarım Hataları ve Güvenlik Sorunları 1551yalnızca kullanıcının yalnızca uygun uygulama ayrıcalıklarına sahip olmasını sağlamak değil, aynı zamanda kullanıcı tamamen alakasız bir şey alamaz. Son zamanlarda, bir E-ticaret Web sunucusu uygulamasının uygulayıcısı düşünülemez olanı yaptı; o okudu dokümantasyon. Yazılımın herhangi birini görüntülemek, kopyalamak veya düzenlemek için kullanılabilecek bir komut dosyası içerdiğini buldu. Sunucuya görünür olan veri nesnesi. Komut dosyası, bilgisayara bağlı herhangi bir tarayıcıdan başlatılabilir. Sunucusu. Bu senaryonun kullanımı için gerekli olmadığını kabul etti. Daha da kötüsü, onun sistemindeki varlığı onu ortaya koydu risk; Senaryonun ismini bilen herkes onun sisteminden faydalanabilir. Diğer tüm kullanıcıların olduğunu fark etti. Uygulama bu komut dosyasının adını biliyordu. Ne kadarını görmek için Net’te bulunan sunucuları aramaya karar verildi. Bu betiğin kopyaları bulunamadı. 100 yaşına geldiğinde saymayı bıraktığı bildirildi. Bunun bir biçimi, programın asıl amacı için tasarlanan kancaları, iskeleleri ya da araçları bırakmaktır. Test amaçlı Bir diğeri ise programın yazarını programdan atlamak için izin veren arka kapıların kullanılmasıdır. Kontrolleri. Yine bir diğeri, başvuru ile ilgili olmayan kamu hizmetlerinin dahil edilmesidir. Daha başarılı ve hassas uygulama, başkaları tarafından keşfedilme ve sömürülme potansiyeli daha yüksek. Daha fazla kopya, Kullanılan programın sorunu ne kadar büyükse çözüm de o kadar zor olur. Ücretsiz bir işlevselliğin çok ciddi bir formu bir kaçış mekanizmasıdır.

1. **AŞIRI AYRICALIK**

IBM AS / 400 gibi birçok çok kullanıcılı, çok uygulamalı sistemler ve UNIX'in çoğu uygulaması bir programın atananların dışındaki ayrıcalık ve yeteneklerle çalışmasına izin verecek bir mekanizma içerir kullanıcıya Kavram, böyle bir yeteneğin erişim kontrolü sağlamak için kullanılabileceği görülüyor. Veri nesnesine tam erişim ile sağlanacak olandan daha küçük ve daha kısıtlayıcıdır. Rağmen yapamam erişim nesnesi A, kullanıcının A nesnesine erişmek için ayrıcalıklı bir programa erişebileceği ancak kullanıcıya yalnızca A nesnesinin belirli bir alt kümesini gösterirdi.

Bununla birlikte, uygulamada, başvurunun ayrıcalıklarla çalışmasına izin vermek için sıklıkla kullanılır. Programcı hatta sistem yöneticisi olanlar. Bu tür kullanımın bir zorluğu, kullanıcı yönettiğinde ortaya çıkar uygulamadan işletim sistemine kaçmak, ancak daha ayrıcalıklı durumu korumak. Başka biri kendini gösterir başlatılan bir işlem, alt sistem veya arka plan programı aşırı ayrıcalıkla çalıştığında. Örneğin, posta servisi amaç için oluşturulmuş bir profil yerine, sistem yöneticisinin ayrıcalıklarına sahip olacak şekilde kurulmalıdır. Bu uygulamanın kontrolünü ele geçiren, örneğin arabellek taşması veya kaçış mekanizmasıyla saldırgan, şimdi sistemi, yalnızca uygulamanın veya kullanıcının sahiplerinin gerektirdiği ayrıcalıklarla değil, aynı zamanda Sistem yöneticisi olanlar. Biri, kusurlu bir programın aşırı imtiyazlı böyle bir tesadüfün muhtemel olmadığını iddia edebilir. Bununla birlikte, deneyim bunun sadece olası değil aynı zamanda yaygın olduğunu da göstermektedir. Bir daha iddia edebilir uygulama programcısının bu sorunun sadece bir kısmına neden olduğunu; geri kalanı ise sorumluluğundadır. Sistem programcısı veya sistem yöneticisi. Bununla birlikte, uygulamada, Programın tamamen ayrıcalıklı olması ve ayrıcalıkların istendiği şekilde uygulama programına verilmesi.

1. **AYRICALIKLI DURUM**

**11.1. Ayrıcalıklı Durum Başarısızlığı**

Uygulama programları, genellikle tamamen kontrol dışındaki nedenlerden dolayı, programcılarının programlarında başarısız olur veya kullanıcılarının. Kural olarak, bu tür başarısızlıklar nispeten iyi huyludur. Bazen, başarısızlık verilerini ortaya çıkarır veya çevreleri. Olası arıza modalarını karşılaştırarak bunu anlamak en kolay yoldur. Güvenlik açısından Bir uygulamanın başarısızlığa uğramasının en güvenli hali, sistemin durmasıdır. Elbette, bu aynı zamanda en azını bırakan durumdur. Kullanıcı ve sistem ve uygulama yönetimi için seçenekler. Sistemi yeniden başlatmak zorunda kalacaklar,AU1997\_Frame\_Ch126 Sayfa 1552 14 Kasım 2003, Cuma 06:03Genel Sistem Tasarım Hataları ve Güvenlik Sorunları 1553yeniden yükleyin ve uygulamayı yeniden başlatın. Bu en güvenli durum olsa da, en düşük durum olan devlet olmayabilir. İyileşme zamanı. Sistem operatörleri çoğu zaman başarısızlığa uğramak için uzun süreden fazla bir sürede iyileşme için kısa süreye değer verir. Alternatif olarak, uygulama oturum açmak için başarısız olabilir. Yıllarca, bu seçim için başarısızlık moduydu. Çok kullanıcılı, zamanın çok uygulamalı sistemleri. Kullanıcının çare, oturum açıp başlatmaktı. Tekrar uygulama. Bu güvenli ve oldukça düzenliydi. Windows ve UNIX gibi daha modern sistemlerde, uygulamanın başarısız olması tercih edilen başarısızlık modudur. İşletim sistemine. Tek kullanıcılı, çoklu uygulama sistemlerinde bu oldukça güvenli ve düzenlidir. İzin verir. Uygulamayı ve verileri kurtarmak için işletim sistemini kullanmak için kullanıcı. Bununla birlikte, çok kullanıcılı, çok uygulamalı sistemlerde hala yaygın olmasına rağmen, bu arıza modu daha tehlikelidir. Nitekim çökmesini çok güvensiz uygulamalar, yalnızca uygulama sistemleri olması amaçlanan saldırı sistemleri için tercih edilen bir yöntem haline gelmiştir. Uygulamanın çökmesine neden olur ve saldırgan işletim sistemine bakarken kendini bulabilir (komut işlemcisi veya uygulamayı başlatan kişinin kimliğine ve imtiyazlarına sahip grafiksel kullanıcı arayüzü [GUI]).

En kötü durumda, bu kişi sistem yöneticisidir.

1. **GÜVENSİZ VARSAYILANLAR**

Uygun kontrollere sahip uygulamalar bile, genellikle bu kontrollerin güvensiz ayarlarına varsayılandır. Demek ki, uygulama ilk yüklendiğinde ve yükleme yapan kullanıcı bir şeyleri değiştirinceye kadar, sistem güvenli olmayabilir yapılandırdı. Yaygın bir örnek denetim izleridir. Uygulamaya, yaptıklarını ve gördüklerini kaydedip kaydetmediği konusunda yönetim kontrol edilebilir. Ancak, kutunun dışında ve yönetimin müdahalesinden önce dergiler varsayılan olarak “kapalı” dır. Benzer şekilde, yönetime şifre uzunluğunun kontrolü de verilebilir. Tekrar dışarı kutunun içinde, şifre uzunluğu varsayılan olarak sıfır olabilir. Bir sistemin neden güvenli olmayan şartlar için varsayılan olarak ayarlanması gerektiğine dair her türlü iyi bahane vardır. Bunlar genellikle kurulum kolaylığı ile ilgilidir. Bunun nedeni, sistem güvenli ayarları başlatırsa, prosedür, tek çare kurulumunu iptal edip başlatmak olan bir kilitlenme durumuna neden olabilir bitti. Zorluk, sistem kurulduktan ve çalıştıktan sonra, kurucunun genellikle herhangi bir şeyi yapmak için isteksiz olmasıdır. Onunla karışabilecek değişiklikler. Bazı durumlarda, tasarımcıların veya programcıların güvenli varsayılan değerlerin ne olduğunu bilmesi mümkün değildir. Çevreyi veya uygulamayı bilmiyorlar. Öte yandan, kullanıcılar kontrolleri anlayamayabilir. Eğer kontroller karmaşıksa ve ince şekillerde etkileşime girerse, bu durum daha da kötüleşebilir. Bir sistem için bir kontrol vardı kullanıcıların şifrelerini maksimum ömürde değiştirmelerini sağlamak. Yapabilmesi için ayrı bir kontrolü vardı. Kendisiyle değiştirilemez. Bu kontrolün çalışmasını sağlamak için, minimum ömrünü belirlemek üzere üçüncü bir kontrol vardı. Parola. Bu kontrollerin etkileşimini anlamak için büyük miktarda özel bilgi gerekiyordu ve etkili kullanımları.

1. **UYGULAMA KONTROLLERİ**

**13.1. Uygulama Kontrollerine Özel Güven**

Uygulama tasarımcısı sık sık uygulama programı denetimlerine, dosya sistemine güvenip güvenmeyeceğine karar verirden etimler, veri tabanı yöneticisi denetimleri veya bunların bir kombinasyonu. Uygulama programcıları bazen güveniyor münhasıran uygulama programındaki kontroller üzerinde. Bunun bir avantajı, kayıt yaptırmaya gerek kalmamasıdır. Kullanıcı, dosya sistemine veya veri tabanı yöneticisine veya kullanıcının bu sistemlere ayrıcalıklarını ve sınırlamalarını tanımlamak için kullanılır. Bununla birlikte, uygulama bu sistemlere sıkıca bağlı değilse, ya ortak bir işletim sistemi ya da şifreleme, bir güvenlik açığı ortaya çıkar. Kullanıcının veya saldırganın dosya sistemine erişmesi veya doğrudan veri tabanı yöneticisi. Yani, uygulama kontrollerini atlamak mümkündür. Bu sorun genellikle ortaya çıkar Uygulama tek sistemli bir ortamda geliştirildiğinde, başvuru ve dosya servisi veya verit abanı yöneticisi tek bir işletim sistemi altında çalışır ve daha sonra dağıtılır. Veri tabanı yöneticisinin kontrollerinin uygulamadakilerden daha güvenilir olduğunu unutmayın. Kontrol daha lokalizedir ve kullanıcı tarafından girişimden veya bypasstan korunur. Diğer yandan, kullanıcının veri tabanı yöneticisine kayıtlı olmasını ve erişim kontrol kurallarının yönetilmesini gerektirir. Bypass kontrolündeki bu güvenlik açığı diğer bağlamlarda da ortaya çıkmaktadır. Örneğin, kontroller atlanabilir dosya sisteminden ziyade işletim sisteminde erişim kontrolü olan tek kullanıcılı, çok uygulamalı sistemler. Saldırgan, tamamen ayrıcalıklı olduğu kendi işletim sistemini getirir ve bunu yerine ayrıcalıklarının olmadığı işletim sistemi.

1. **ÖNERİLER**

Uygulamalar oluşturulurken ve sahnelenirken aşağıdaki önerilere dikkat edilmelidir. Bağlı kalarak Bu öneriler, programcı ve uygulama yöneticisi, belirtilen hataların çoğundan kaçınabilir bu bölümde.

1. Güvenilen tüm kısıtlamaları uygulayın.

2. Tüm parametreleri kontrol edip istenen uzunluk ve kod türüyle sınırlandırın.

3. Kısa ve basit programları ve program modüllerini tercih edin. Sadece bir giriş noktası olan programları tercih et üstte veya başında ve altta veya sonunda yalnızca bir çıkış.

4. Hem parametre kontrolü hem de hata düzeltmesi için iyi test edilmiş genel rutinlere güvenmeyi tercih edin. Veritabanı istemcisi ile birlikte verilen rutinlerin kullanımını düşünün. Parametre kontrolü ve hata düzeltme kod tasarlamak, yazmak ve test etmek zordur. En iyi master programlayıcılarına atanır.

5. Uygulamaların mümkün olan en güvenli duruma getirilememesi. Arızalı çok kullanıcılı uygulamaları durdurmak veya oturum açmak için tercih edin uygulamanın yeni bir örneğine. Arızalı tek kullanıcılı uygulamaları bir tek kullanıcılı işletimde tercih et sistemi.

6. Uygulamaları mümkün olan en az ayrıcalıkla sınırlandırın. Kullanıcının ayrıcalıklarını tercih et. Aksi takdirde, bir

Sınırlı profil oluşturuldu ve yalnızca amaç için kullanıldı. Asla bir sistem genelinde bir uygulama ayrıcalıkları vermeyin.(Çünkü programcı, uygulamanın çalışabileceği ortamı öngöremez ve sistem yöneticisi riskleri anlayamayabilir, bu kuralın istisnaları son derece tehlikelidir.)

7. Kontrol bypasslarına karşı koymak için uygulamaları baştan sona bağlayın. Güvenilir bir tek sistemli ortamı tercih edin.

Aksi takdirde, güvenilir bir yol kullanın (örneğin, özel yerel bağlantı, uçtan uca şifreleme veya ikisinin hazırlanmış kombinasyonu).

8. Bir uygulama kullanıcısının ayrıcalıklarına, yalnızca uygulamanın kullanımı için gerekli olan işlevselliği dahil edin. Başvuruyu kolaylaştırmak için ayrı yetkilendirme gerektiren birden çok nesneye ayırmayı düşünün birden fazla kullanıcıyı hassas görevlere dahil etmek.

9. Kontroller güvenli ayarlara varsayılan olmalıdır. Kontrollerin karmaşık olduğu veya ince yollarla etkileşime girdiği durumlarda, komut dosyaları (“sihirbazlar”) veya profiller sağlayın.

10. Verilere yakın lokalize kontrolleri tercih edin (örneğin, uygulamaya dosya sistemi, dosya yöneticisi sistemi).

11. Kodun bütünlüğünü doğrulamak ve kontrollerin atlanmasına karşı koymak için şifreleme tekniklerini kullanın.

12. Kurcalamaya karşı korumalı ambalajda bilinen ve güvenilir kaynaklardan gelen uygulamaları ve diğer programları tercih edin.

1. **NOT**

1. George Santayana, Reason in Common Sense

1. **FİZİKSEL GÜVENLİK: KIVRIMLI ERİŞİM VE KATMANLI SAVUNMA**

Fiziksel güvenlik, bir şeyin emniyetini ve maddi varlığını sağlamak için alınan önlemler olarak tanımlanabilir. Veya hırsızlığa, casusluğa, sabotaj veya zarara karşı birisi olabilir. Bilgi güvenliği bağlamında bu, bilgi, ürünler ve insanlar hakkında. Fiziksel güvenlik en eski koruma şeklidir. Yıllardır insanlar kendilerini koruyorlardı. Zarar ve değerli eşyalarını hırsızlık veya imhadan kurtarır. Geçmişte, fiziksel güvenlik tüm koruma biriydi güvenlik olması gerekiyordu. Bununla birlikte, teknolojiyle, yalnızca fiziksel güvenlik etkili değildir. Bilgi Güvenliği hedefine ulaşmak için birçok farklı güvenlik katmanını dağıtan bir yaklaşımdır; dolayısıyla “güvenlik girişi Katmanlar. ”Hiçbir şeyin yüzde 100 güvenli olmadığı kabulü ile bilgi güvenliği derinliği kullanırken yüksek güvenlik formunu elde etmek için katmanlarının. Bu katmanlardan herhangi birindeki zayıflık, güvenliğe neden olacaktır. Kırmak. Fiziksel koruma, katmanlı bilgi güvenliği yaklaşımında ilk adımdır. Eğer mevcut değilse, zayıf veya yanlış uygulamalarda kullanıldığında, bilgi güvenliği başarısız olacaktır.

1. **FİZİKSEL GÜVENLİK YAKLAŞIMI**

Fiziksel güvenlik, sınırsız bir şekilde ele alınamayan sürekli bir süreçtir. Yaklaşım kuruluşun hedefleriyle tutarlı olmalı ve standartlara uygun olarak uygulanmalıdır. ve bilgi güvenliği politikasında belirtilen kurallar. Çünkü fiziksel güvenlik dünyasında çok az bir değişiklik var (en azından geri kalan kadar hızlı değil).bilgi güvenliği dâhilindeki kontroller), genellikle sıkıcı veya önemsiz olarak kabul edilir. Bu yanlış anlama, genellikle fiziksel güvenliğin ihmal edilmesine veya rastgele uygulanmasına neden olur. Genellikle, en büyük zayıflığı Herhangi bir bilgi güvenliği kontrolü, kontrolün kendisi değil, bir kontrolün yanlış uygulanmasıdır. Fiziksel güvenlik, diğer bilgi güvenliği ile aynı enerji, odak ve ciddiyetle ele alınmalıdır kontrol. Aslında, güvenlik kontrollerine tutarlı ve önceden belirlenmiş bir şekilde yaklaşılmalı ve uygulanmalıdır. Öngörülebilir, tekrarlanabilir ve etkili bilgi güvenliği sağlamak. Kilitler, korumalar, güvenlik kameraları ve kimlik kartları sadece fiziksel araç ve gereçlerdir. Güvenlik. Fiziksel güvenliği planlamak ve tasarlamak için aşağıdaki sorulara cevap verilmelidir:

• Neyi koruyorsun?

• Bilgilerin korunması (ekonomik, politik veya kamu güvenliği açısından) ne kadar önemlidir?

• Kimi koruyorsun ve onlar için daha önemli olan şey nedir? Gizlilik, bütünlük veya Kullanılabilirliği?

• Siz ve onu kimden koruyorsunuz?

Verilen, tüm yerlerin Fort Knox’un fiziksel güvenliğine (kim orada çalışmak ister?) İhtiyaç duymaz, fiziksel olarak

İnsanların önemi ve duyarlılığı ile orantılı olarak güvenlik uygulanmalı ve

18 Kasım 2003, Salı 10:03

1926 Bilgi Güvenliği Yönetimi El Kitabı

Korur. Bu bölümde, bilgi güvenliğindeki ortak tehditler ve güvenlik açıkları kaynaklı riskler tartışılmaktadır. ve ne kadar iyi fiziksel güvenlik bu riskleri ele almak için bir temel oluşturabilir.

1. **FİZİKSEL GÜVENLİK PSİKOLOJİSİ**

Fiziksel güvenliği planlarken ve tasarlarken, fiziksel olduğu kadar psikolojik olduğunu unutmayın. Psikolojik etkinin sahip olabileceği avantajları göz önünde bulundurmak önemlidir. Eğer biri fiziksel tasarlayabilirse Güvenlik, güvenliği yüksek oranda görünür kılacak şekilde (ayrıntıları korurken),Örgüt iyi bir şekilde korunuyor ve bu da tehdit edici bir faaliyet için daha az hedef haline geliyor. Bu dolaylı bir yoldur. Bu kuruma karşı suç işleme arzusunu ortadan kaldırır. Fiziksel güvenliğin etkinliği, olduğu gibi herhangi bir güvenlik kontrolü, fırsatın elimine edilmesiyle ölçülür; fiziksel güvenlik psikolojisi Arzu ortadan kaldırmak için ölçülür.

1. **TESİS FİZİKSEL GÜVENLİK**

Modern iş yerinin çeşitliliği genellikle evrensel, katı fiziksel güvenlik kurmanın pratik olmamasını sağlar. Standartları. Bununla birlikte, tam olarak ulaşmak için her yerde yeterli fiziksel güvenlik gereklidir. Güvenli ortam Bu bölüm, tesis türlerini, nasıl farklılık gösterdiklerini ve yaklaşma yollarını açıklamaktadır. Her biri için fiziksel güvenlik.

**18.1. Tesis Sınıflandırılması**

Tesisler aşağıdaki genel sınıflandırmalardan birine ayrılabilir:

• Sahip olunan tesis. Sahip olunan tesisler muhtemelen fiziksel güvenliği sağlamak için en basit yapıdır. Tam idari kontrole sahip olan işgalciden dolayı güvenlik yönetimi kolaylığı doğasındadır tesisin üzerinden. Bu, herhangi bir tür fiziksel güvenlik kontrolünü uygulamak için esnekliğin Herhangi bir şekilde, mal sahibi / mülk sahibi koruma hedeflerini gerçekleştireceğini düşünüyor. Bir ana çöküşü sahip olunan tesis, fiziksel güvenlik arızalandığında mal sahibinin / sahibinin tamamen sorumluluk alması gerektiğidir. bir sahip olunan bir tesise güzel bir örnek büyük bir şirket merkezidir.

• Sahipsiz tesis. Sahipsiz tesisler fiziksel olarak korunma konusunda biraz daha zor olabilir. İşgalci ve mal sahibi, kendileri içind sorumluluktan sorumlu olacak kendi sorumluluk listelerine sahip olacaktır. Güvenlik başarısız. Örneğin, bir su borusu patlar ve bir bilgisayar odasını taşarsa, yolcu alabilir mal sahibinin yeterli bir şekilde bakmadığı tespit edilirse tazminattan sorumlu olan mal sahibi tesisat. Bu durumda, sahiplenmemiş tesisler, başarısız olan fiziksel durumlar için yasal başvurunun avantajını sunabilir güvenlik. Sahipsiz tesislere örnek olarak, binada yaşayan bir kiracıdır, ancak mülk sahibi değildir.

• Paylaşılan tesis. Paylaşılan tesisler, muhtemelen işgal edilebilecek tesislerin en çeşitliliği ve tehdididir, ancak yapıların çoğunu açıklarlar. Bu tesisler, bazı işgalcilerin muhtemelen rakip oldukları. Çünkü tesis herkese eşit erişim sağlamalıdır.yolcular (belirli bölgelerde), fiziksel güvenlik çok zorlaşır. İyi paylaşılan örnekler tesisler birden fazla yolcu, merkez ofisler ve eş merkezler ile sahipsiz tesisler olabilir. Tesisleri sınıflandırırken, risk azaltma stratejisinin geliştirilmesinde ilk adım atılmaktadır. Belirli tesislerin doğasında olabilecek tehditleri anlayarak, riskler. Bazı tesisler birden fazla sınıflandırma tanımına uyabileceğinden, bir kişi kesin olarak bu sınıflandırma şemasına uyma. O zaman bunun farkında olması gereken, herhangi bir yeni içsel güç ve bu melez sınıfların yaratabileceği zayıflıklar.

**18.2. Tesis Lokasyonu**

Sadece birinin ne tür bir tesisi işgal ettiğiyle değil, aynı zamanda bulunduğu yerle de ilgilenmesi gerekir. Belirli yerleşim diğerinden daha fazla tehdit barındırabilir. Aşağıda, ne zaman dikkate alınması gereken konum tabanlı bazı tehditler bulunmaktadır. Tesis için bir alan seçmek:

• Suç, isyan ve terörle ilgili güvenlik açığı. Tesisin konumu bu faaliyetlerin sıkça kullanıldığı bir bölgedeyse her yer için araştırma suçu ve terör istatistikleri düşünülüyor.,18 Kasım 2003, Salı 10:03

Fiziksel Güvenlik: Bilgi Güvenliği Vakfı

Fiziksel güvenliğin ihlal edilme olasılığı artar. Örneğin, sık sık gösteriler veya isyanlar

Bir tesis yakınında, bölgeyi tehdit edebilecek rastgele şiddet olaylarına (örneğin, yangınlar, suç, vb.) girebilir. Tesis, çalışanları ve muhtemelen müşterileri. Bilgi güvenliğinde bile, koruma ve

İnsanların güvenliği her zaman her şeyden önce gelmelidir.

• Bitişik binalar ve işletmeler. Bu konu, daha önce tartışılan tesislerin sınıflandırılması ile ilgilidir.(özellikle ortak tesisler) ve önceki suç ve isyan güvenlik açığı sorunu. Bu iyi bir uygulama birinin komşusunun kim olduğunu ve ne yaptıklarını bilmek. Örneğin, bir şirket bulmak istemeyebilir. Rakiplerin, nükleer santrallerin veya otoyol veya tren yollarının yanındaki veri merkezi. Tehlikeli kimyasal taşıma. Ayrıca, bu endişeler bağlı binalar hakkında akla geliyor. Ar fiziksel güvenlik kontrolleri sizinki kadar güçlü mü? Birisi içeri girerse tesise girebilir mi? Bitişik bir bina? Peki ya çatı? Bunların hepsi ne zaman birinin aklında ön planda olmalı, Bir yer seçmek.

• Acil destek desteği. Bu sadece acil destek almasının zamanı (yani, Ateş, Polis ve sağlık personeli) tesise ulaşmak için. Sürüş mesafesini ve mesafesini bilin(en yoğun trafik sırasında) acil destek merkezlerinden tesise. Bu bilgi sağlar yalnızca tespit ve caydıracak değil, aynı zamanda geciktirecek ve acil destek gelene kadar hasarı veya hasarı en aza indirir.

• Çevresel destek. Çevresel destek, tesise hizmet eden temiz hava, su ve güçtür.

Konumun tüm bu alanlarda büyüme için yer açtığından emin olun. Özellikle, yüksek kullanılabilirlik için tesislerinde iki ayrı elektrik şebekesinden çekilecek yerleri arayın.

• Doğal afetlere karşı güvenlik açığı. Doğal desenler için yerel jeolojik ve hava durumu istatistiklerini kontrol eden son 100 yıldır tercih edilen yerlerde felaketler. Verilen, doğal afetler tahmin edilemez ya da tamamen kaçınılması, ancak böyle felaketlerin olduğu bir yer seçerek etkilerini en aza indirgemek gerçekleşmesi daha az olası.

**18.3. Fasite Tehditleri ve Kontrolleri**

Bir önceki tartışmaya göre, belirli konumların nasıl daha fazla veya daha az tehdit oluşturabileceğini görüyoruz. Ne takip ediyor işte temel biçimlerindeki tehdit ve kontrollerin listesi. Bu, birinin bir tehdidi ortadan kaldırabileceğini göstermek içindir kökünden biri, birkaç kişiyi aynı anda etkili bir şekilde ortadan kaldırabilir. Ancak bunun tersi de dikkat edin

Bir tehdit diğerini gösterdiğinde olabilir. Kontroller doğada basit ve basit, ancak Kontrollerin, bir bütün olarak, verilen bir tehdide caydırması, tespit edilmesi, geciktirilmesi ve tepki vermesi gerektiğine dikkat edin.

**18.4. Doğal Tehditler**

İyi fiziksel güvenlik bazı tehditlere karşı psikolojik bir avantaja sahiptir. Ne yazık ki, doğal tehditler onlardan biri değil. Bu tehdit caydırılamaz veya caydırılamaz. Bir anda veya başka, Tabiat Ana tesisi tehdit ediyor. Tek seçenek, etkiyi en aza indirecek ve hızlı düzelme. Doğal tehditler ve kontrollerinin bazıları şunlardır:

• Yangın aşağıdaki risklere neden olur:

- Sıcaklık

- Duman

- Söndürme maddesi (örneğin, yangın söndürücüler ve su) hasar

• Yangın kontrolleri şunları içerir:

- Duman detektörlerini ekipmanın yakınına kurmak

- Yangın söndürücülerin kurulması ve çalışanların uygun kullanımları için eğitilmesi

- Bilgi sistemlerinin yakınında gazlı (likit olmayan) söndürme sistemlerinin kullanılması

- Düzenli yangın tahliye tatbikatları yapılması

- Tüm yedekleme ortamlarını saha dışında saklamak (bağlı bir üçüncü tarafla)

- Bir felaket kurtarma planının geliştirilmesi ve uygulanması

• Şiddetli Hava Koşulları aşağıdaki risklere neden olur:

- Şimşek

AU1997\_Frame\_Ch158 Sayfa 1927 18 Kasım 2003 Salı 10:03

1928 Bilgi Güvenliği Yönetimi El Kitabı

- Ağır rüzgarlar

- Dolu

- Su baskını

• Şiddetli hava kontrolleri şunları içerir:

- Hava koşullarının izlenmesi

- Ekipmanı hava koşullarına dayanıklı ve güçlü rüzgarlara dayanabilecek alanlarda tutmak

• Ekipmanın doğru şekilde topraklandığından emin olun

- Dalgalanma bastırıcıları ve kesintisiz güç kaynaklarını (UPS) veya dizel jeneratörleri takma

- Yükseltilmiş döşeme montajı

- Düzenli hava tahliye tatbikatları yapılması

- Tüm yedekleme ortamlarını saha dışında saklamak (bağlı bir üçüncü tarafla)

- Bir felaket kurtarma planının geliştirilmesi ve uygulanması

• Depremler, diğer doğal afetleri teşvik etme kabiliyetleri nedeniyle özellikle tehlikelidir.

yangınlar. Deprem kaynaklı yangınların teminatlı hasarına ek olarak, bazı ek riskler şunlardır:

- Acil durum ajanslarından sınırlı cevap veya cevap yok

- Tesislerde ve bilgi sistemlerinde kalıcı yapısal fiziksel hasar

- Geçersiz kılma tehdidi kontrolleri (örneğin, yangın söndürme özelliğini devre dışı bırakır)

- Personel tahliyesi sınırlı

• Deprem kontrolleri şunları içerir:

- Bilgi sistemleri ekipmanını yüksek yüzeylerden uzak tutmak (doğru montaj olmadan)

- Bilgi sistemleri ekipmanını cam pencerelerden uzak tutmak

- Ekipman ve altyapı üzerine depreme dayanıklı veya anti vibrasyon cihazları kurmak

- Rutin deprem tatbikatlarının yapılması

- Tüm yedekleme ortamlarını saha dışında saklamak (bağlı bir üçüncü tarafla)

- Bir felaket kurtarma planının geliştirilmesi ve uygulanması

Doğal tehditler her zaman yukarıda sıralanan dramatik olaylar değildir. Genellikle çok daha ince olabilirler ve öngörülemeyen şekli. Buna bir örnek, zaman içinde kuru ısıya, neme ve hafif rüzgarlara maruz kalmadır. Bu daha az şiddetli tehditler derhal alarm vermeyebilir, ancak potansiyellerinin farkında olmalı

etki.

**18.5. İnsan Yapımı Tehditler**

İnsan Yapımı Tehditler

İkinci tehdit sınıfına insan yapımı denir. Bu tür bir tehdit genellikle en dinamik ve en zor olanıdır, insan doğasında bağları nedeniyle. Bu, insan yapımı tehditlere neden olan üç motive edici ajanın, kötülük, fırsat ve kaza sonucu ortaya çıkan bir sonuçtan çıkarılmıştır. İnsan kaynaklı tehditler ve bazı kontroller

Dahil etmek:

• Hırsızlık / dolandırıcılık aşağıdaki risklere neden olur:

- Bilgi sistemleri yeteneklerinin azaltılması veya kaybı

- Hassas bilgi veya ticari sır kaybı

- Gelir kaybı

• Hırsızlık / dolandırıcılık kontrolleri şunları içerir:

- Tesisin izlendiğini ve terk edildiğinde kişilerin denetlenebileceğini belirten işaretler gönderildi.

tesise girmek

- Görünür kapalı devre televizyon kameraları (CC TV'ler)

- Güvenlik ve güvenlik bilinçli çalışanlar

- Kimlik rozetleri

- Muhafızlar

- Yer işaretleri kullanımının en aza indirilmesi

- Rutin denetimler

- İyi stok kontrol uygulamaları

- İyi kilit ve temel uygulamalar

- Sigorta

18 Kasım 2003, Salı 10:03

Fiziksel Güvenlik: Bilgi Güvenliği Vakfı

- Görevlerin ayrılması / iş rotasyonu

- Çalışan işe alma / işten çıkarma uygulamaları

• Casusluk aşağıdaki risklere neden olur:

- Hassas bilgi veya ticari sır kaybı

- Rekabet avantajı kaybı

- Gelir kaybı

• Casusluk kontrolleri şunları içerir:

- Tesisin izlendiğini ve terk edildiğinde kişilerin denetlenebileceğini belirten işaretler gönderildi.

tesise girmek

- Görünür kapalı devre televizyon kameraları (CC TV’ler)

- Güvenlik ve güvenlik bilinçli çalışanlar

- Kimlik rozetleri

- Yer işaretleri kullanımının en aza indirilmesi

- Muhafızlar

- Çalışan işe alma / işten çıkarma uygulamaları

- Görevlerin ayrılması / iş rotasyonu

- Rutin denetimler

• Sabotaj aşağıdaki risklere neden olur:

- Bilgi sistemleri yeteneklerinin azaltılması veya kaybı

- Hassas bilgi veya ticari sır kaybı

- Gelir kaybı

• Sabotaj kontrolleri şunları içerir:

- Tesisin izlendiğini ve terk edildiğinde kişilerin denetlenebileceğini belirten işaretler gönderildi.

tesise girmek

- Görünür kapalı devre televizyon kameraları (CC TV’ler)

- Güvenlik ve güvenlik bilinçli çalışanlar

- Yer işaretleri kullanımının en aza indirilmesi

- Kimlik rozetleri

- Muhafızlar

- Sigorta

- Görevlerin ayrılması / iş rotasyonu

• İşyerinde şiddet aşağıdaki risklere neden olmaktadır:

- Çalışanlara zarar veya ölüm

- Verimlilik kaybı

- Gelir kaybı

• İşyerinde şiddet kontrolleri şunları içerir:

- Tesisin izlendiğini ve terk edildiğinde kişilerin denetlenebileceğini belirten işaretler gönderildi.

tesise girmek

- Görünür kapalı devre televizyon kameraları (CC TV’ler)

- Güvenlik ve güvenlik bilinçli çalışanlar

- Uyarı işaretlerinin farkındalığı

- Muhafızlar

- Çalışan işe alma / işten çıkarma uygulamaları

İnsan aklının ustalığı ve uyarlanabilir doğası insan yapımı tehditlerin kontrolünü zorlaştırıyor. Bir Kuruluş, koruma programı ile ilgili rutin değerlendirmeler yaparak dikkatli davranmalıdır. Bu tehditlere karşı uygulanan kontroller.

**18.6. Çevresel Tehditler**

Üçüncü tehdit sınıfı, çevresel tehditler olarak etiketlenmiştir. Çevresel kontroller operasyon için önemlidir ve bilgilerin ve sistemlerin korunması. Temiz hava, su, güç ve güvenilir iklim kontrolleri olmadan,

bilgi sistemleri tutarsız performansa veya tamamen başarısızlığa uğrayabilir.

18 Kasım 2003, Salı 10:03

1930 Bilgi Güvenliği Yönetimi El Kitabı

• İklim yetersizliği aşağıdaki risklere neden olur:

- Ekipman ve altyapı arızası veya aşırı ısınmanın başarısız olması

- Depolama / yedekleme medyasında hasar

- Hassas ekipman bileşenlerinde hasar

• İklim kontrolleri şunları içerir:

- Bilgi sistemleri ekipmanlarının sıcaklıklarının izlenmesi

- Bilgi sistemleri içeren tüm odaları makul sıcaklıklarda tutmak (60 -

75 ° F veya 10 ila 25 ° C)

- Nem seviyelerini yüzde 20 ila 70 arasında tutmak

- Bilgi sistemi donanımı bulunan odalarda gereksiz ışıkların kapatılması

- Klima kontrol sisteminin rutin koruyucu bakım ve denetimlerinin yapılması

- Tüm yedekleme ortamlarını saha dışında saklamak (bağlı bir üçüncü tarafla)

- Bir felaket kurtarma planının geliştirilmesi ve uygulanması

• Su ve sıvı kaçağı aşağıdaki risklere neden olur:

- Suya veya diğer sıvı türlerine aşırı derecede maruz kalmaktan kaynaklanan ekipman ve altyapı arızası

- Depolama / yedekleme medyasında hasar ve kritik basılı kopya bilgileri

- Kritik ekipman bileşenlerinde hasar

• Su ve sıvı kaçağı kontrolleri şunları içerir:

- Cihazın yakınında sıvı geçirmez kapak bulundurma

- Kritik bilgileri barındıran odalara drenaj, su dedektörü ve yükseltilmiş döşeme montajı

sistem donanımları

- Tesisatın rutin denetimlerinin yapılması

- Bilgi sistemlerinin yakınında gaz veya kuru boru söndürme sistemlerinin kullanılması

- Tüm yedekleme ortamlarını saha dışında saklamak (bağlı bir üçüncü tarafla)

- Bir felaket kurtarma planının geliştirilmesi ve uygulanması

• Elektrik kesintisi aşağıdaki risklere neden olur:

- Kritik ekipman bileşenlerinde hasar

- Yazılım ve depolama / yedekleme medyasında hasar

- İklim kontrolünün kaybı

- Fiziksel erişim kontrollerinin ve izleme cihazlarının kaybı (yani, gözetleme kameraları, kapı alarmları, Kimlik /

kart okuyucular)

• Elektrik kesintisi kontrolleri şunları içerir:

- Kesintisiz güç kaynaklarını (UPS) veya dizel jeneratörleri kurmak ve test etmek

- Dalgalanma bastırıcıların kullanılması

- Gerilim yükselmelerini kontrol etmek için elektrik hattı filtrelerinin takılması

- Statik korumaların ve uygun olan yerlerde anti statik halıların kullanılması

- Tüm ekipmanın doğru şekilde topraklandığından emin olun

- Devre kutuları ve kabloların düzenli olarak kontrol edilmesi

- İki ayrı şebekeden güç çekmek (mümkünse)

- Tüm yedekleme ortamlarını saha dışında saklamak (bağlı bir üçüncü tarafla)

- Bir felaket kurtarma planının geliştirilmesi ve uygulanması

Çevresel başarısızlık, kendi başına, bilgi sistemlerinde ciddi hasara neden olabilecek bir tehdittir.

Ancak, doğal veya insan yapımı tehditlerle de kendini gösterir. Bu nedenle, yaklaşmak önemlidir. Tüm tehditler derinlemesine savunma olan katmanlı bir yaklaşımla. Bu sadece kontrollerin çoğu kapsamasını sağlar tehditlerin arasında, ancak bu kontrollerin kapsamları dâhilinde de eksiksiz oldukları.

**18.7. Tesis Koruma Stratejisi**

Fiziksel koruma için genel bir strateji geliştirmek, iyi sonuçlara ulaşmak için atılan birçok adımdan biridir. Bilgi Güvenliği. Birinin koruma stratejisi birçok prensipten oluşacak ve odaklanmalıdır Bilgilerin gizliliğinin, bütünlüğünün veya erişilebilirliğinin daha büyük önemi olup olmadığı. İmar stratejisi

Verimli ve etkili fiziksel bilgi koruması için bir temel oluşturmak için kullanılabilir.

**18.7.1. Zoning**

İmar, yeni bir kavram değildir. Geleneksel olarak, imar, yangın algılama alarmlarını kurmak için kullanılan bir işlemi ifade eder. Gizli duman veya ateş yerlerini belirlemek (tavan üstü, zemin altı vb.). Ayrıca, denilen bir kavram iki veya daha fazla alarmın istenmesini gerektirerek yanlış alarmların azaltılmasını sağlayan çapraz bölgeleme kullanılmıştır. İmar, en detaylı güvenlik modeline en basitini sağlamak için yeterince esnektir. Bu nedenle, biri diğer tüm fiziksel güvenlik kontrollerini bu konsepte uygulayabilir (örneğin, hareket detektörleri, fiziksel izinsiz giriş algılama alarmları, CCTV'ler vb.) En büyük avantaj, rol tabanlı erişim kontrolü modelleridir. Rol bazında erişim kontrol programları, kullanıcılara göre sistemlere, bilgilere ve fiziksel alanlara erişim organizasyondaki rolü. Sergi 158.1, rol tabanlı erişim kontrolü için imar kullanımının temel bir örneğini göstermektedir. Bu örnekte, Bölgeler 1 ila 4, 4 arasında en kısıtlayıcı etiketlidir. Bu tesiste, her çalışanın erişimi var 1, 2 ve 3; Bununla birlikte, Bilgi Teknolojileri Direktörü, BT personeli ve Güvenlik Yöneticisi, erişime sahiptir. rolleri nedeniyle 1, 2, 3 ve 4 bölgelerine. Güvenliğin doğal ilerleyişi açıktır; Bir daha ileriye doğru hareket ettikçe bölgeler daha kısıtlayıcı hale gelir tesis (soldan sağa). Bu alıştırma tamamlandıktan sonra, bir sonraki adım kontrolleri belirlemek olacaktır. Bu, erişim kontrol bölgelerini desteklemek için yerine konulmalıdır. Sonun daha kısıtlayıcı olduğunu unutmayın. Kontroller daha güçlü ve daha güvenilir olmalıdır. Fiziksel erişim denetimlerini, rol tabanlı modelleri ve bölgeleri birleştirerek, kapsamlı bir bilgi ve varlıklarını fiziksel olarak korumak için merkezi sistem. İmar çok önemli bir parçası olabilir birinin bilgi güvenliği stratejisi. Bununla birlikte, bir imar egzersizi yapmadan önce bir risk analizi yaptı (bir kişinin varlıklarına yönelik tehditleri ve kırılganlıklarını anlamak için) ve risk azaltma stratejisi. Ancak o zaman imar, bir kuruluşun yapabileceği sağlam bir temel oluşturacaktır. Bilgi güvenliği hedeflerine ulaşmaktılar.

1. **BİLGİ SİSTEMLERİ FİZİKSEL GÜVENLİK**

Fiziksel güvenliğin ikinci kısmı, bilgi sistemlerinin fiziksel korunmasıdır. Tartışıldığı gibi, koruma katmanlar halinde gelmelidir. Bir kuruluşun bilgisayarlarından yalnızca birinin fiziksel bütünlüğü tehlikeye girerse, bilgi güvenliği risk altında olabilir. Birisi bir yetkisiz fiziksel erişim kazanmak için bilgisayar, bu kişi bilgisayardaki tüm bilgilere ve muhtemelen herhangi birisine erişebilir bilgisayarın bağlı olduğu diğer kaynaklar (dosya sunucuları, ana bilgisayarlar ve e-posta dahil).

**19.1. Bilgi Sistemleri Sınıflandırılması**

Bilgi sistemleri üç tipe ayrılabilir:

1. Sunucular / ana bilgisayarlar: Genellikle fiziksel olarak en güvenli sistemler sınıfı. Bu ortak kaynaklanmaktadır

Bunları bir çeşit erişim ve çevre kontrolü olan bir yere yerleştirme uygulaması. olmasına rağmen. Bu sınıf en fiziksel olarak güvenli olabilir, genel güvenliği fiziksel güvenliğe bağlıdır. İş istasyonlarının ve bunlara erişen taşınabilir cihazların listesi.

2. İş İstasyonları: Genellikle bir tesisin daha açık veya erişilebilir alanlarına yerleştirilir. Kullanılabilirliği nedeniyle iş yerinde, iş istasyonları dikkatsizce kullanılırsa fiziksel güvenlik sorunlarına eğilimli olabilir.

3. Taşınabilir cihazlar: Bir kuruluşun güvenlik kabusu olabilir. Dizüstü ve PDA ihraç etmeme rağmen çalışanlar bir kuruluşta esneklik ve üretkenliği kolaylaştırır, bununla birlikte birkaç ciddi risk oluşturur fiziksel güvenlik ile ilgili olarak. Şirketin dahili bilgi sistemlerine erişen kullanıcılar herhangi bir yerde, bu cihazlardan birinin fiziksel güvenliğinin ihlal edilmesi bir kuruluşun bilgi güvenliğine zarar verir. Bu sınıfa çok özen gösterilmelidir.

**19.2. Bilgi Sistemleri Fiziksel Tehditler ve Kontroller ve Farkındalık Eğitimi**

Bilgi sistemlerinin sınıflandırılması, hangi tehditlerin hangi sistemler için daha büyük bir risk oluşturduğunun belirlenmesine yardımcı olur. Bu kontrolleri uygulamak için bir rehber sağlar. Muhtemelen en büyük bilgi sistemleri için tehdit kullanıcı. Herhangi bir kullanıcı, fiziksel olarak bilgisayarlarını korumada gerekli özen göstermediği takdirde aklınızda bulundurun. Varlıklar, hemen hemen tüm kontroller etkisiz hale gelir ve cihazı savunmasız bırakır. Bu bölüm, ana hatları

Bilgi sistemleri için temel tehdit ve kontroller.

• Kayıp / hırsızlık / imha aşağıdaki riskleri taşır:

- Hassas bilgi veya ticari sır kaybı

- Verimlilik kaybı

- Gelir kaybı

• Kayıp / hırsızlık / imha kontrolleri şunları içerir:

- Cihazlar için fiziksel kilitler

- Cihazları işaretleme ve etiketleme

- Yer işaretlerinin kullanımını en aza indirin

- Hassas bilgi depolama için şifreleme

- Hassas bilgi için veri sınıflandırma ve teslim prosedürleri

- Sigorta

- Farkındalık eğitimi

- Görünür kapalı devre televizyon kameraları (CC TV'ler)

- Muhafızlar

- Alarm sistemleri

- Rutin denetimler

• İzinsiz erişim aşağıdaki riskleri doğurur:

- Hassas bilgi veya ticari sır kaybı

- Bilgi kurcalama

- Kötü amaçlı yazılım

- Gelir kaybı

• İzinsiz giriş kontrolleri şunları içerir:

- Kilitleme konsolları

- İyi şifre uygulamaları

18 Kasım 2003, Salı 10:03

Fiziksel Güvenlik: Bilgi Güvenliği Vakfı

- Farkındalık eğitimi

- Hassas bilgi için veri sınıflandırma ve teslim prosedürleri

- Yer işaretleri kullanımının en aza indirilmesi

- Görünür kapalı devre televizyon kameraları (CC TV’ler)

- Hassas bilgi depolama için şifreleme

- Güçlü kimlik doğrulama ve erişim kontrolleri

1. **KAYNAKÇA**

1. Fennelly, Lawrence J. et al., Effective Physical Security, Second Edition, Butterworth-Heinemann, 1997.

2. Fites, P. and Kratz, M.P.J., Information Systems Security: A Practitioner’s Reference, International Thomson Computer Press, 1996.

3. Tipton, Harold and Krause, Micki, Eds., Information Security Management Handbook, 4th edition, Auerbach Publications, 2000.

4. Department of Education, National Center for Education Statistics, Protecting Your System: Physical Security (online), 1998. Available from World <http://nces.ed.gov/pubs98/safetech/chapter5.html>.

5. Tipton, Harold and Krause, Micki, Eds., Information Security Management Handbook, Auberbach Publications, 1999.

6. Linux Documentation Project, Security How-To: Physical Security (online). Available http://www.linuxdoc.org/HOWTO/Security-HOWTO-3.html.