Hata : başa çıkma, saptama ve kaydetme

Amaç

Endiüstrilerin çoğu aşağıdaki türden yasal kurallara gerek duyar :

- saptanabilir – kullanıcı konum veya dengesini etkileyen bütün etkinlikler izlenir.
- izlenebilir – uygulamanın her aşamasında oluşan etkinliği saptamak mümkündür.
- bütünleşebilir – yerelde veya sunucudaki kullanıcılar, kayıtların üzerine yeni bilgi yazamaz ve kayıtları tahrif edemez.

Çok iyi yazılmış uygulamalar, ikili amaçlı kayıt yapacak ve saptama ve izleme için etkinlik izleme işlemlerini gerçekleştirecek ve böylece fazla çaba harcamadan kayıt işlemi yapmak ve sisteme erişim kolaylaşacaktır.

Etkilenen ortamlar

hepsi.

Ilgili COBIT başlıkları

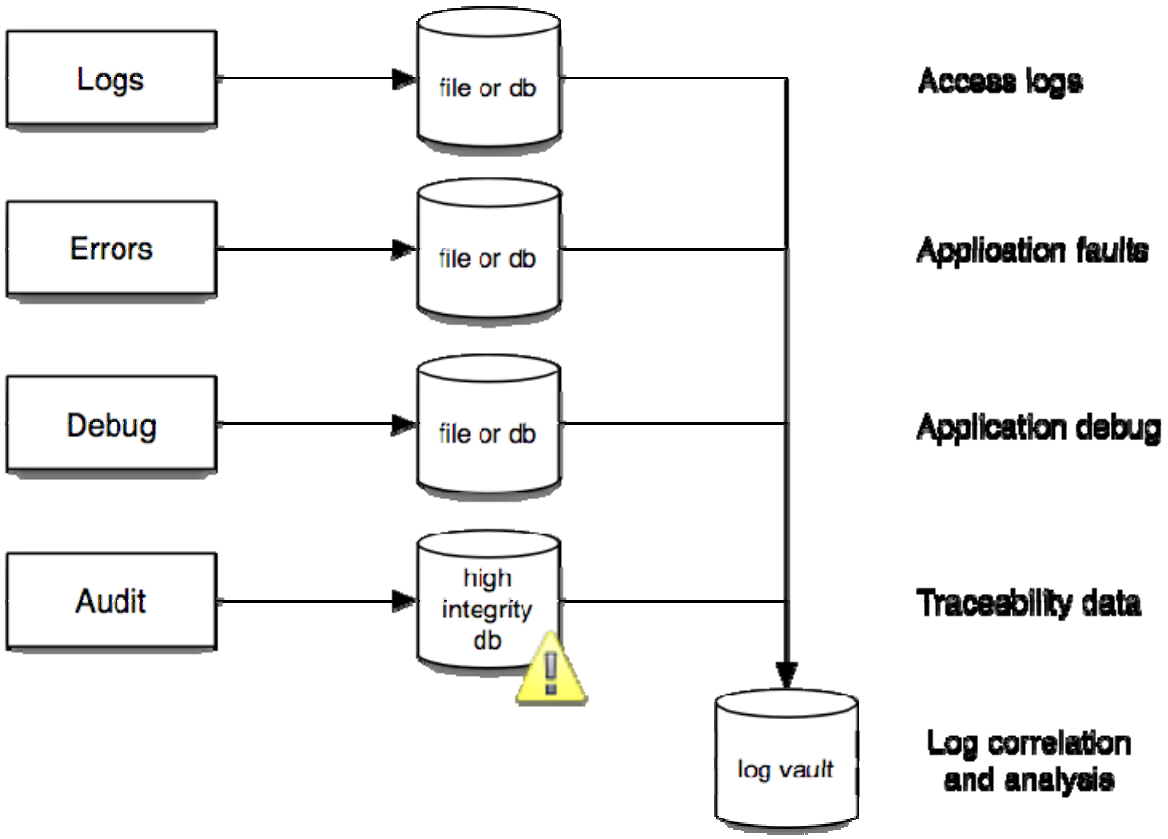
DS11 – veri işleme – bütün bölümler, özellikle aşağıdakiler gözden geçirilmelidir:

DS11.4 kaynak verileri hata başa çıkma işlemleri

DS11.8 veriler giriş hata başa çıkma işlemleri

Tanımlama

hata başa çıkma, hata ayıklama mesajları, saptama ve kaydetme aynı başlık altında yeralır: bır uygulama içinde olup bitenleri izleme:



En iyi uygulamalar

- sistemden düşmeye karşı korunmalı – açık konumda yapın
- Ikili amaçlı kayıtlar
- Saptama kayıtları yasal olarak koruma altındadır – kayıtarı koruyun
- Raporlar ve arama loglarının sadece-okuma kopyası veya ikinci bir tam kopyasını almak

Hata başa çıkma

hata başa çıkma iki formda olur: yapılandırılmış harici başa çıkma ve fonksiyonel hata kontrolü. yapılandırılmış harici başa çıkma kodu %100 oranında geri kazanmak mümkün olduğu için her zaman tercih edilir. PHP 4 gibi fonksiyonel diller hariciliği olmadığı için bütün hataların %100 oranında geri kazanımı çok zordur. 100% hata içeren kodlar fazlasıyla gereksizdir ve okunması zordur ve güç algılanan kusurların yanısıra,

yapılandırılmış harici başa çıkma kodunun kendisi hatalar içerir. Saldırganlar hata mesajlarını görmeyü sever çünkü bir sonraki saldırı için gereken bilgiye sızabilirler veya ilgili bilgiye ulaşabilirler. Web uygulama yapılandırılmış harici başa çıkma işlemi ise nadiren sızma testine karşı koyacak güçtedir.

Uygulamalar her zaman sistemden düşmeye karşı korunmalı olmalıdır. Uygulama bilinmeyen bir konuma düşerse saldırganın izinsiz işlevselliğe erişimi söz konusu olabilir veya saldırgan veri yaratma, değiştirme ve bozma işlemlerini yapabilir

sistemden düşmeye karşı korunmalı

- Uygulamanın ölümcül hata ile başa çıkma sistemini sınayın.
- sistemden düşmeye karşı korunmalı mı ? öyle ise, nasıl ?
- ölümcül hata ile başa çıkma sistemi yeterince sık devreye giriyor mu ?
- olmakta olan işlemlere ve geçici verilere ne olur ?

kusur giderme hataları

- üretim kodu kusur giderme/hata ile başa çıkma sistemleri ve mesajları içerir mi ?
- dil etkin ön-işlem veya derleme olmaksızın çalışan bir metin dili ise, browserda kusur giderme etiketini çalışır hale getirmek mümkün müdür ?
- kusur giderme mesajları özel bilgilere veya bir sonraki saldırının başarıı olmasına neden olacak bilgiye sızmaya neden olur mu ?

hariç tutma işlemi

- yapılandırılmış harici başa çıkma sistemleri kodunu ({} catch {} vs.yi deneyin) veya fonksiyon-bazlı hata ile başa çıkma işlemlerini kullanır mı ?
- kod fonksiyon-bazlı hata ile başa çıkma işlemlerini kullanırsa, geri dönen her değeri kontrol eder ve hata ile doğru dürüst başa çıkabilir mi ?
- Would fuzz injection against the average interface fail? Ha ???

Fonksiyonel deri dönüş değerleri

Birçok dil hatayı geri dönüş değeri ile gösterir. Örnek :

```
$query = mysql_query(“SELECT * FROM table WHERE id=4”, $conn);
```

```
if ( $query === false ) {
            // error
}
```

- Bütün fonksiyonel hatalar kontrol edildi mi ? edilmediyse, ne gibi bir yanlışlık olabilir ?

Ayrıntılı hata mesajları

Ayrıntılı hata mesajları saldırgana kullanışlı bilgilerle dolu bir kaynak sunar.

Tehlikeye açık olup olmadığınızı saptama

- Ayrıntılı hata mesajları açık mı ?
- Ayrıntılı hata mesajları bir sonraki saldırıda kullanılmaya veya özel bilgi sızdırmaya izin verir mi ?
- Browser hata mesajlarını toplar mı ?

Kendinizi koruma

Uygulamanızın 'güvenli mod' da olduğundan emin olun ki beklenmedik bir hata oluşursa size geri dönebilsin. Herşey devredışı kalırsa, kullanıcıyı sistemden çıkarın ve browser penceresini kapatın.

Üretim kodu hata giderme mesajları içermemelidir. Içerirse, hata giderme işlemi dosya düzeltme veya konfügirasyonu işlemleri sunucu tarafından devreye sokulmalıdır. Özellikle hata giderme, uygulama içinden devreye sokulmamalıdır.

Dil yapılandırılmış harici başa çıkma işlemine sahipse (yani try {} catch {}), işlevsel hata gidermeye refere olarak kullanılmalıdır.

Uygulama işlevsel hata gidermeyi uygularsa, kullanımı doğrudan ve ayrıntılı olmalıdır.

Özel bilgi sızdırma veya yığın izleme gibi ayrıntılı hata mesajları kullanıcıya kesinlikle ulaştırılmamalıdır. Onun yerine jenerik hata mesajı kullanılmalıdır. Bu, HTTP konum cevap kodlarını içerir (yani 404 veya 500 iç sunucu hatası).

kayıt

nereye kayıtlama ?

kayıtlar kayıt dosyasına yazılmalıdır. Böylece kayıt dosyası niteliklerine sadece yeni bilgiler yazılır (ya eskilerin üzerine ya da eskileri silerek yapılamaz). Fazladan güvenlik sağlamak için, kayıtlar bir kez yaz/CD-R gibi bir çok cihazı oku'ya da kayıt yapılmalıdır.

Kayıt dosyalarının kopyaları hacım ve boyuta bağlı olarak (günlük, aylık, yıllık vs) düzenli aralıklarla yapılmalıdır. Genel adlandırma konvensiyonu kayıtlara göre ayarlanmalıdır, bu index işlemini kolaylaştırır. Kayıtım hala etkin olduğunu doğrulama çoğu kere gözden kaçar, ve basit bir cron işi ile bu iş çözümlenebilir.

Verilerin yeniden yazılmadığından emin olun.

Kayıt dosyaları kopyalandıktan sonra sabit depoya aktarılır ve organizasyonun bütün yedekleme stratejisiyle birleştirilir.

Kayıt dosyaları ve ortam silinmeli ve sistemden uzaklaştırılmalıdır. Ayrıca organizasyonun kesme ve güvenle ortamdan uzaklaştırma planına uygun olmalıdır. Raporlar düzenli olarak alınmalıdır, raporlara hata raporları dahil olmalıdır.

Yedeklenmiş olsa bile kayıtların güvenle korunduğundan ve güzli tutulduğundan emin olun.

Başa çıkma

Kayıtlar gerçek zamanlı saldırı saptama ve performans ve sistem izleme araçlarına beslenebilir. Analiz sırasında manipulasyon ve silme işlemi yapılmaz.

Genel kusur giderme

Kayıtlar güvenlikle ilgili olsun olmasın, bir sorundan sonra yeniden yapılanma açısından önemlidir. Yeniden yapılandırma güvenlik yetkilisinin saldırganın bütün etkinliklerini görmesini sağlar ve geri kazanım işlemini hızlandırır.

Forensik kanıt

Kayıtlar zaman zaman yasal işlemlerde kanıt olarak kullanılabilir. Bu durumda, kayıt verileriyle aktüel başa çıkma önemlidir.

Saldırı saptama

Kayıtlar çoğu kere sadece şüpheli davranışı kaydeder. Bu nedenle de kayıtlar bazen saldırı saptama sistemlerine gerçek-zamanlı olarak kaydolur.

Geçerliliğin kanıtlanması

Uygulama geliştiriciler bazen uygulamalarının diledikleri gibi çalıştığını göstermek için kayıt tutarlar.

- Kanun gerektirdiği için veya ilkeler gereğince
- Kayıtlar kullanıcının etkinliklerini izleyerek web uygulama sistemi ortamında bireysel sorumluluğunu ortaya koyar.

Ortak ilke veya yerel kanun, (örneğin) bütün uygulama bilgilerinin kaydedilmesini gerektirebilir. Bu kayıtlar silinmeden önce altı ay boyunca güvenli ve gizli olarak tutulmalıdır.

Yukarıdaki bilgiler farklı bütün motivasyonları göstermektedir ve farklı gereklilik ve stratejilerle sonuçlanır. Yani, bir sisteme veya uygulamaya kayıt mekanizması sunmadan önce gereklilikleri ve sonraki kullanımlarını bilmemiz gerekmektedir. Bunu bilmezsek, beklenmedik sonuçlarla karşılaşabiliriz.

Web uygulamasında kayıt mekanizmalarının tasarımı veya mümkün kılınmaması organizasyonun izinsiz erişimleri saptamadaki yeteneğini zayıflatır ve bu saldırıların başarılı olup olmadığını sorgulatır. En genel saldırı yöntemlerine, tasarım ve sunum hatalarının yanısıra bu bölümde mitigasyon stratejilerine de göz atacağız.

Kayıt mekanizmasının sunum öncesinde neden planlanması gerektiğine dair bir başka neden daha vardır. Bazı ülkelerde, ne tür kişisel bilgilerin sadece kayıtların değil o kayıtların nasıl analiz edileceğine de dair yasal belirlemeler vardır. Örneğin isviçrede firmalar çalışanlarının kişisel bilgilerini kayıt edemezler (internette ne yapıyorlar veya e-postada neler yazdıkları gibi). Bir firma çalışanının arama alışkanlıklarını kaydetmek isterse, planını önceden kişiye bildirmek zorundadır.

Bu da gizli kayıt veya isimsiz kayıtların sonradan isimlendirilmesi gereğini doğurur. Izinsiz kişi şahsi kayıtlara girerse (yasal olarak), işbirliği yasadışı olur. Dolayısıyla bir kaç yasal tuzağın mevcut olduğu akılda tutulmalıdır.

Kayıt türleri

Kayıtlar farklı türden veriler içerebilir. Kullanılan verilerin seçimi kayıt nedeni tarafından etkilenir. Bu bölüm farklı kayıt bilgileri ve neden kaydetmek isteyebileceğimiz hakkında bilgiler içermektedir.

Normalde kayıt özellikleri saat, işlemin sahibi, işlemin başlaması, olayın ayrıntılı tanımı gibi bilgilerdir. Aşağıdakiler bir uygulamaya kayıt edilebilecek sistem olay türleridir. Belli bir uygulama ve sisteme bağlıdır ve kayıtlarda hangisinin kullanılacağına karar verilmesini gerektirir:

- Veri dosyasına erişimin okunması ve ne tür verinin okunduğu. Bu sadece verinin kimden ne zaman geldiği ve verinin okunup okunmadığını saptamaya izin verir.
- Veri kayıtlarının yazılması aynı zamanda nerede ve hangi modda yazıldığı anlamına da gelir. Bu, program veya verinin üzerine yazma olup olmadığını görmek için kullanılır.
- Herhangi bir veri karakteristiğinin, erişim kontrol izinleri veya etiketleri, veritabanı veya dosya sistemindeki yeri veya veri sahipliği dahil, modifikasyonu. Yöneticiler konfigürasyonların değişip değişmediğini saptayabilirler.
- Yönetim fonksiyonları ve üstüste gelmesine bakımaksızın konfigürasyondaki her türlü değişiklik (yönetim etkinlikleri, herhangi bir kullanıcının verilerini inceleme, kayıt uygulama veya iptali, vs.).
- Muhtelif hata giderme bilgileri etkinlik sırasında iptal edilebilir veya uygulamaya konabilir.
- Başarı/başarısızlık, kaynak veya fonksiyon yetkilendirme ve kullanıcı talebiyle yetkilendirme gibi her türlü yetkilendirme çabası (zaman dahil). Bu kayıtlara bakarak şifreyi saptayabiliriz. Bu türden kayıtlar, değişiklikleri saptayacak olan saldırı saptama sistemine beslenebilir.
- Herhangi bir verinin (obje) silinmesi. Zaman zaman uygulamalar, silme işlemini iptal etmek üzere bir tür versiyonlama gerektirebilir.
- Network haberleşmeleri (katılma, bağlanma, kabul etme, vs.). saldırı saptama sistemi bu bilgiyle port tarama ve aşırı saldırıları saptayabilir.
- Aşırı saldırıları ve tahmini saldırıları saptamaya yarayan bütün yetki etkinlikleri (sisteme giriş, sistemden çıkış, başarısız giriş, vs.).
-

karmaşa

Güvenlik hatalarının giriş bilgileri ile bir hata kaydı yazmasını bilinçli olarak istemek (karmaşa) ve böylece başarılı bir saldırının suç dışı kalmasını sağlamak. Yönetici veya kayıt ayrıştırıcı kayıtları gözden geçirdiğinde, kayıt girişleri kapasitesini, ‘samanlıkta iğne arama’ olarak tanımlamak yerine hizmet reddi olarak özetleyecektir.

Kendinizi koruma

Uygulamalar genelde kayıt etkinliği yaratma kapasitesi olan fonksiyonlara engellenmemiş bir rota sundukları için bu oldukça zordur. bir kaç saldırı sonrası saldırganın çekinmesini sağlayacak akıllı bir araç veya uygulama elemanı konuşlandırabilirseniz, o zaman anlamlı olacaktır. Bu olmazsa, hata kaydı aracı etkiliğin tekrarı temelindeyse veya örneğin aynı kaynaktan doğmuşsa, bu, karmaşayı azaltabilir. Ayrıca kayıt görüntüleyici sadece zaman bazında değil ciddiyet seviyesine göre olayları gösterebilirse, bu kullanışlı olacaktır.

Iz kaybettirme

Asıl mükafat ise, pürüzlü bu yolda kayıt girişlerini silen veya manipule eden, 'sanki hiç böyle birşey olmamış gibi' davranan yarışmacıya gider. Rootkitlerin konuşlandırılması ve saldırı, saldırgana, bilinen kayıt dosyalarının manipulasyonunu otomatikleştirebilen veya destekleyebilen uzman araçları kullanma şansı tanır. Çoğu kez kayıt dosyaları kök/yönetim yetkilerine sahip kullanıcılarca veya kanıtlanmış kayıt manipulasyon uygulamalarınca manipule edilebilir. Genel kural olarak,saldırgan izini belli etmeden uzu süre saklayabileceği için, kayıt mekanizmaları manipulasyonu pürüzlü seviyede engellemeyi amaçlar. Basit soru şudur : saldırgan ile anlaşmaya varırsanız, kayıt dosyanız çok büyük veya küçükse saldırı daha mı belirgin olacak yoksa her zamanki kayıtlar gibi mi olacak ?

Kendinizi koruma

Kayıt dosyalarını en yüksek güvenlik korumaya alın ve işler yolunda gitmediğinde etkin bir 'kara kutu' kayıtedicinin devreye gireceğinden emin olun. Bu aşağıdakileri içerir :

Uygulamalar yönetici ile veya kök-seviyesi öncelikleriyle çalıştırılmamalıdır. bu, süper kullanıcılar sisteme tam erişim hakkına sahip olduğu için kayıt dosyası manipulasyonun başarılı olmasının ana nedenidir. Uygulama kullanıcısının izini kaybettirmekten kayıt dosyasını manipule etmeye kadar, önceliklerini engellemede başka güvenlik tabakaları olacak mıdır ?

Kayıt dosyalarını korumada erişim önceliklerinin sınırlayıcı olduğundan emin olmak, işletimlerin büyüklüğünü, kayıt dosyasını değiştirme ve okumaya karşı, azaltmak

Kayıt dosyalarının obje adlarını atadığından ve adların belirgin olmadığından ve dosya sisteminin güvenilir bir yerinde saklandığından emin olmak.

Kayıt dosyalarını herkese açık veya dikkatle gözden geçirilmiş teknikler kullanarak yazmak ve böylece kayıt dosyası manipulasyonu veya tersine mühendislik ile riski azaltmak.

Log dosyalarını sadece-okuma (etkinlik kayıt bütünlüğünün kritik öneme sahip olduğu) ortamına yazma.

Dijital parmak izi oluşturmada, hesaplanmış adresleme teknolojisinin kullanımı. Saldırgan kayıt dosyasını manipule ederse, dijital parmak izi uymayacak ve uyarı mesajı yollayacaktır.

Normal davranış modellerinin sabitlenebileceği misafir-tabanlı IDS teknolojisinin kullanımı

Saldırganın normal yollarla kayıt dosyasını güncelleme girişimleri, farklı bir durum yaratır ve bu sayede saldırı saptanarak engellenebilir.

Yanlış alarmlar

1966 yapımı klasik film ‘bir milyon çalmanın yolu’ veya Ezop’un masalı ‘yalancının mumu’ ndan yola çıkarak, tekrarlanan yanlış alarmlara karşı uyanık olmak gerekir. Bu tür uyarılar, saldırganın ‘güvenlik yöneticisinde teknolojinin hatalı olduğu ve düzeltilene dek güvenilir olmadığı gibi bir hisse kapılmasına neden olma’sı anlamına da gelebilir.

Kendinizi koruma

Bu tür saldırılara karşı uyanık olun ve her türlü güvenlik karşıtı etkinliği ciddiye alın, kayıt hatalarını yaratan nedenin köküne inin ve teknik bir problemden kaynaklandiğından emin olana kadar hataları gözardı etmekten kaçının.

Hizmetin reddi

Kayıt girişine neden olan ve onbin kere tekrarlanan talepler içeren bir uygulama, çok büyük bir kayıt dosyasına sahip olmanıza neden olacaktır ve güvenlik yetkilisi için problem yaratacaktır. Kayıt dosyalarına ayrılmış sabit bir kapasitenin söz konusu olduğu yerlerde, dosya dolunca bütün kaydetme işlemleri duracaktır ve saldırgan kayıtlama mekanizması hizmetini reddettirme şansını elde edecektir. Daha da kötüsü , maksimum

dosya kapasitesi belirlenmemişse, saldırgan bütün hard sürücü partitisyonunu dolduracak ve sistemin hizmete tümüyle kapanmasına neden olacaktır. bu, bugünün hard sürücülerinin giderek artan kapasitesi nedeniyle giderek daha az gerçekleşmektedir.

Kendinizi koruma

Bu türden saldırılara karşı ana korunma yöntemi kayıt dosyası kapasitesini ulaşılabilirin ötesinde bir kapasiteye ayarlamak, kayıt dosyasını işletim sistemi veya diğer kritik uygulamalardan farklı bir yere yerleştirmek, ya da en iyisi, kayıt dosyası kapasitesi ve/veya etkinliğine karşı ön-girişli bir tür sistem izleme uygulaması ve bu türden bir saldırı geliyorsa bir uyarı mesajı kullanmaktır.

İmha

Yukarıda sözü edilen hizmetin reddindeki senaryoda olduğu gibi, bir kayıt dosyası, dolduğunda geri gidip eski girdilerin üzerine yazıyorsa, saldırganın zararlı etkinlik potansiyeli var demektir.

Herşey devre dışı kalırsa, o zaman saldırgan bu tür bir etkinliği yapma hakkına sahip olduğunu varsayarak bütün kayıt girişlerini temizleyip izini kaybettirebilir. Bu saldırı, kayıt dosyası yönetim programını çağırma ve kayıt temizleme şeklindedir, veya basitçe, kayıt güncellemelerini alan objeleri (bu obje çoğu kere uygulama tarafından kilitlenecektir) silmek daha kolay olabilir. Bu türden bir saldırı, kayıt dosyalarının düzenli olarak izlendiği varsayımıyla saldırıyı daha da belirgin hale getirecektir. Bu tür saldırılar, sistem yöneticileri ve yetkililerinin yapacak birşey olmadığını anlayıp paniğe kapılmalarına neden olma eğilimindedir.

Kendinizi koruma

yukarıda ifade edilen tekniklerini çoğunu uygulama bu saldırıya karşı iyi bir korunma sistemi yaratacaktır. Iki noktaya dikkat etmekte yarar vardir :

sistemin yönetici kullanıcıları kayıt dosyası yonetimi ve gözden geçirme işinde eğitilmiş olmalıdır. Kayıt dosyalarının ‘özel’ temizliği kesinlikle önerilmez ve mutlaka bir arşiv oluşturulmalıdır.kayıt dosyası defalarca temizlenebilir, bu, teknik bir sorunu çözmek ya da ileride gerekecek saptama çalışmaları için gerekecek etkinlikler tarihçesini silmek içindir.

Boş bir güvenlik kayıt dosyası forensik yetkililerine telefon etmeniz gerektiği anlamına gelmez. Zaman zaman güvenlik kayıtlama varsayılan ayar olarak seçilmemiş olabilir ve seçilip seçilmediğinden emin olmak sizi ilgilendirir. Ayrıca doğru ayrıntı seviyesinde kayıt yapıldığından emin olun ve hataları, 'normal' etkinlik olarak düşünülen, uygun oranda bir referans hattı ile karşılaştırarak değerlendirin.

Saptama izleri

Saptama izleri bir çok ülkede yasal olarak koruma altına alınmıştır. Tesadüfi ve bir nedene bağlı zararları ve tahrifatı engellemek için üst düzey bütünlük hedeflerine kayıt edilmeleri gerekir.

Tehlikeye açık olup olmadığınızı saptama

- Kayıtlar, kayıtlama hedefi ile host arasında sorunsuz bir şekilde transit ediliyor mu ?
- Kayıtların, kayıtlama etkinliğinden gözden geçirilişe kadarki sürede değişmesini engellemek üzere, bir HMAC'I, veya benzeri bir tahrifat kanıtlama mekanizması var mı ?
- Ilgili kayıtlar kovuşturmayı destekleyici, yasal olarak geçerli olacak şekilde, kolaylıkla elde edilebiliyor mu ?

Kendinizi koruma

- Sadece gerçekten önemli etkinlikleri saptayın—saptama izlerini uzun bir süre saklamanız ve hatalardan gidermeniz gerekir, aksi takdirde bilgi içeren mesajlar israf edilir.
- Kayıtları, uygun bir biçimde tek merkezden kaydedin ve birincil saptama izlerinin, özellikle ön taraftaki web sunucuları gibi tehlikeye açık sistemlerde yeralmadığından emin olun.
- Kayıtların, asıllarını değil, sadece kopyalarını gözden geçirin.
- Saptama kayıtlarının güvenilir sistemlere yollandığından emin olun.
- Üst düzeyde korunmalı sistemlerde, uzun vadeli ve güvenilir kayıt depoları oluştumak amacıyla sadece-bir-kez-yaz veya benzeri ortamları kullanın.
- Üst düzeyde korunmalı sistemler için kayıtlama mekanizmasında baştan-sona güvenin varolduğundan emin olun. Dünya yazılabilir kayıtları, ehliyetsiz kayıtlama araçları (SNMP tuzakları, syslog, vs.gibi), kovuşturma dışı olma açısından yasal olarak tehlikeye açıktır.

Ileri okuma

- Oracle saptama
  http://www.sans.org/atwork/description.php?cid=738
- IT güvenliğinde Sarbanes Oxley
  http://www.securityfocus.com/columnists/322

Dökümanın Aslı : OWASP GUIDE 2.0.1

Çeviri **:** Billur C. Yılmazyiğit - info@biledge.com