Politika Sistemleri (Yapıları)

Genel Bakış

Güvenli uygulamalar kendi kendilerine olmazlar – "güvenli uygulamalar üretecekleri" kararını alan organizasyonlar güvenli uygulamalar üretirler. OWASP, belli bir yaklaşımı kullandırmaya zorlamak veya organizasyonları, kendilerini ilgilendirmeyen kanunlara uymak zorunda bırakmak niyetinde değildir, kaldı ki her organizasyon farklıdır.

Ama, güvenli bir uygulama için, en azından aşağıdakiler gereklidir.

- Güvenliği savunan (destekleyen) organizasyon yönetimi
- Ulusal standartlara dayanarak üretilmiş yazılı bilgi güvenliği politikası
- Yeterli ve yerinde kontrol noktaları ve aktiviteleri barındıran bir geliştirme metodolojisi
- Güvenli dağıtım ve yapılandırma yönetimi

OWASP Kılavuzu 2.0'dak kontrollerden bir çoğu, COBIT gibi ulusal standartlar veya kontrol sistemlerinden esinlenmiştir. Tipik olarak, OWASP'tan şeçilen kontroller, ilgili ISO 17799 ve COBIT kontrollerini sağlar.

Yönetimde Güvenlik Kararlılığı

Yüksek kademelerinde güvenlik bilinci olan organizasyonlar genellikle temel bilgi güvenliği prensiplerine uygun uygulamalar üretirler. Bu durum, gelişigüzel "muhtemelen güvenli (ama büyük ihtimalle değil)" ile "gerçekten güvenli" arasındaki yolda, birçok adımdan ilkidir.

Yönetim bilinci olmayan veya güvenliğe önem vermeyen organizasyonlarda, çok büyük olasılıkla güvensiz uygulamalar üretirler. Her güvenli organizasyon bilgi güvenliği politikalarında kendi risk anlayışlarını belirtir, böylece hangi risklerin kabul edildiği, yok edileceği veya birilerine görev olarak verileceği işini kolaylaştırır.

Güvensiz organizasyonlar bu anlayışın nerde belirlendiğini bilmezler ve bu sebeple projeler güvensiz organizasyon seçim kontrolleri tarafından çalıştırıldığında, ya yanlış ya da eksik kontroller gerçeklenecektir. Bir çay demi yokeden mutfak lavabosu da dahil olmak üzere bütün kontrollerin büyük maliyetlerle gerçeklendiği az sayıda örnekle karşılaşılmıştır.

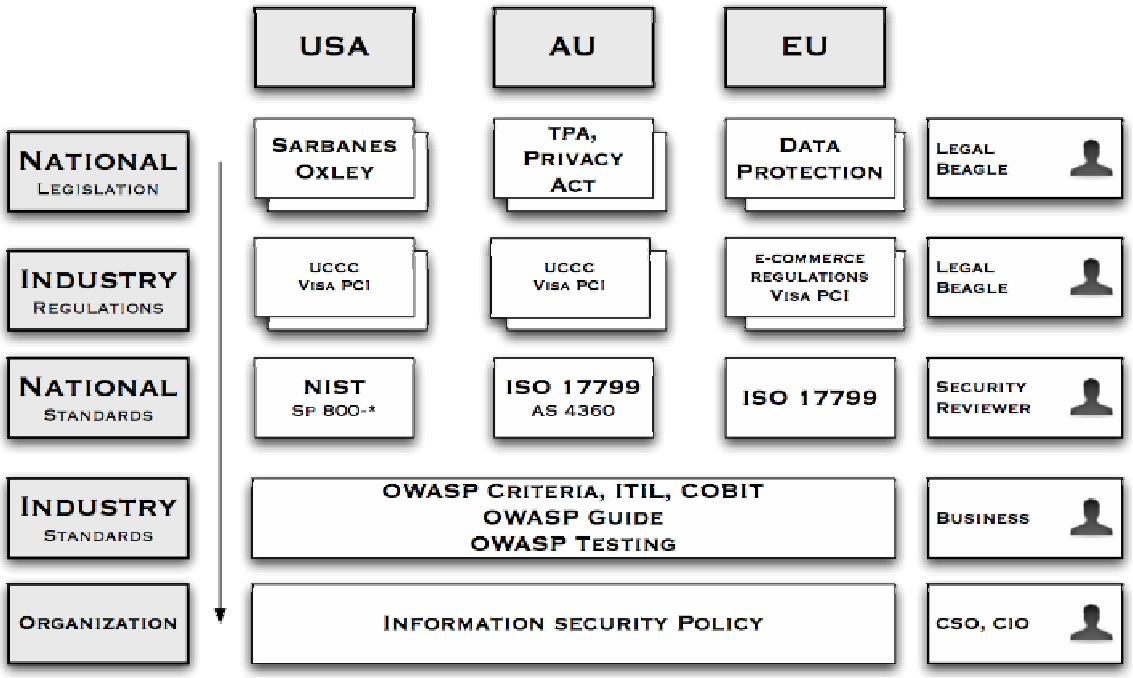
Organizasyonlardan bir çoğu bilgi güvenliği politikalarını ISO 17799'dan veya ABD'de iseler COBIT'ten veya arada sırada her ikisinden veya diğer başka standartlardan üretirler. Güvenlik politikaları dokümanını üretmenin belirli ve hızlı bir şekli olmasa da, genel olarak;

- Eğer bir çok ülkede halka açık ticaret yapıyorsanız, bir bilgi güvenliği politikanız olmalıdır
- Eğer ABD'de halka açık ticaret yapıyorsanız, genellikle COBIT kontrolleri anlamına gelen SOX taleplerine uygun bilgi güvenliği politikanız olmalıdır.
- Eğer özel olarak tutulmuşsanız, ama birkaç çalışanınız veya kod yazarınız varsa muhtemelen bir bilgi güvenliği politikasına ihtiyacınız vardır.
- Tipik organizasyonlardan olmayan popüler FOSS projelerinin de bir bilgi güvenliği politikası olmalıdır.

COBIT veya ISO 17799'dan veya herhangi bir diğer bilgi güvenliği standardlarından kontrolleri karıştırmak veya birbirine uydurmak tamamen mümkündür, standardlar kendi aralarında çok nadiren çatışırlar. Üretim metodu bazen zor olabilir – eğer sertifikalı bir politikaya ihtiyacınız varsa, bu iş için vasıflı bir firma ile anlaşmanız gerekecektir.

Yapı Tablosunda OWASP'ın Yeri

Aşağıdaki diyagram OWASP'ın nereye oturduğunu gösterir (eğer yoksa, kendi ülkenizi ve ülkenizin kanunları, düzenlemeleri ve standardları ile değiştirin):



Organizasyonlar, ilgili ulusal kanunlar, endüstriyel düzenlemeler, ticari anlaşmalar ve yardımcı en iyi uygulamalar kılavuzlarının (OWASP gibi) gösterdiği şekilde bilgi güvenliği politikalarını kurmalıdırlar. Bütün ilgili kanunları ve düzenlemeleri küçük bir diyagrama sığdırmak imkansız olduğundan, bütün ilgili kanunlar, standardlar, düzenlemeler ve kılavuzların eksik olduğunu farzetmelisiniz – hangilerinin, organizasyonunuzu, müşterilerinizi (uygulanabildikçe) ve uygulamanızın nerede üretime konacağı konularını etkileyeceğini bulmalısınız.

IANAL: OWASP yetkili bir yasal tavsiye kaynağı değildir; kendi yasal tavsiyenizi aramalısınız.

COBIT

COBIT, dört alan etrafında biçimlendirilmiş popüler bir risk yönetim yapısıdır.

- Planlama ve organizasyon
- Edinim ve gerçekleştirme
- Teslim ve destek
- İzleme

Bütün dört alanın da 13 üst düzey, DS5 *Ensure Systems Security* gibi, amaçları vardır. Her üst düzey amacın da bir kaç detaylı amaçları, 5.2 *Identification, Authentication, and Access*, vardır. Amaçlar, her organizasyon için farklı olabilecek

değişik metotlar ile yerine getirilebilir. COBIT tipik olarak bir SOX kontrol yapısı veya ISO 17799 kontrollerini tamamlayıcı olarak kullanılır. OWASP, aslında COBIT'in yönetim ve iş riskleri özellikleri üzerinde durmaz. Eğer COBIT'i uyguluyorsanız, OWASP, sistem geliştirme riskleri için ve özel yapım veya satın alabileceğiniz uygulamaların COBIT kontrolleri ile uygunluğunu saptamak için harika bir başlangıçtır. Ama OWASP bir COBIT uygunluğu sihirli değneği değildir.

Dökümanda ne zaman bir COBIT amacı bir OWASP kontrolü tarafından sağlansa, sizi ilgili bölüme yönlendirecek "COBIT XXyz.z" bilgisini göreceksiniz. Bu tür controller her uygulamanın parçası olmalıdır.

COBIT hakkında daha fazla bilgi için lütfen http://www.isaca.org/ adresini ziyaret edin.

ISO 17799

ISO 17799, direk olarak AS / NZS 4444 ve BS 7799 standardlarından türetilmiş risk tabanlı bir Bilgi Güvenliği Yönetimi yapısıdır. Uluslararası bir standard olup, daha fazla ABD dışındaki organizasyonlarda kullanılır. Nadiren de, ABD organizasyonları da ISO 17799 kullanırlar, özellikle ABD dışında yan kuruluşları varsa. ISO 17799 tarihi, 1990'ların başlarına kadar gider ve bazı kontrol elemanları o tarihi yansıtır – mesela yönetim arayüzlerinin "tanımlayıcı portlar" olarak tanımlanması.

ISO 17799 kullanan organizasyonlar geniş bir ISO 17999 kontrol yelpazesini seçip, gerçekleştirirken, (diğerleri arasında özellikle Systems Development bölümündekiler) OWASP'ı detaylı bir kılavuz olarak kullanabilirler. OWASP kontrolleri tarafından bir ISO 17799 elemanı gerçekleştirildiği yerde, sizi ilgili ISO 17799 bölümüne yönlendirecek "ISO 17799 X.y.z" bilgisi göreceksiniz. Bu tür kontroller bütün uygulamaların bir parçası olmalıdır.

), or British Standards International (http://www.bsi-global.com/).

ISO 17799 hakkında daha fazla bilgi için, lütfen http://www.iso17799software.com/ ve Standards Australia (http://www.standards.com.au/), Standards New Zealand (http://www.standards.co.nz/), veya British Standards International (http://www.bsi-global.com/) gibi ilgili standard bünyelerini ziyaret ediniz.

Sarbanes-Oxley

Bir çok ABD organizasyonlarının OWASP kontrollerini uygulamalarının ana motivasyonu devam eden Sarbanes-Oxley uyumu için yardım etmesidir. Eğer bir organizasyon bu kitaptaki her kontrolü takip ederse, bu organizasyona SOX uyumu vermeyecektir. Kılavuz, uygulama iyileştirmesi (?) ve lokal (?) geliştirmelerinde, daha geniş bir uyumluluk programının parçası olarak, uygun bir kontrol olarak kullanılabilir.

Ama, SOX uyumluluğu çoğu kez, kaynak sıkıntısı çeken IT yöneticileri tarafından uzun ve ihmal edilmiş güvenlik kontrollerinin üzerlerini örtmek için kullanılır, bu yüzden SOX'un tam olarak ne istediğini anlamak önemlidir. SOX'un özeti olarak AICPA'nın http://www.aicpa.org/info/sarbanes_oxley_summary.htm web sitesindeki bölüm 404 der ki:

> Bölüm 404: Dahili Kontrollerin Yönetimsel Değerlendirmesi
>
> Yayımcının her yıllık raporu "dahili kontrol raporu" içermesi ve bu raporun:
>
> 1) Finansal raporlama için yönetimin yeterli bir dahili kontrol yapısı kurması ve yönetmesi sorumluluğunu belirtir
> 2) Yayımcının mali yılının sonunda, dahili kontrol yapısının etkisinin ve finansal rapor için yayımcı prosedürlerinin bir değerlendirmesini içerir.

Bu, temel olarak yönetimin, dahili **finansal** kontrol yapılarını ve prosedürlerini kurması ve yönetmesi ve kontrollerin etkili olduklarını yıllık olarak değerlendirmesi gerektiğini söyler. Finans artık hesap defterlerindeki çift kayıtlar ile tutulmadığından, "SOX uyumluluğu" çoğu kez IT anlamına gelecek şekilde kullanılır.

Kılavuz, sadece finansal raporlama amaçları için değil uygulamalar için etkili kontrolleri sağlayarak SOX uyumluluğuna yardım eder. Organizasyonların, OWASP kontrollerini kullandıklarını iddia eden ürünleri almalarına ve organizasyonların, özel yazılım firmalarına güvenli yazılım üretmeleri için OWASP kontrollerini kullanmaları gerektiğini bildirmelerine yardım eder.

Ama SOX bir bahane olarak kullanılmamalıdır. SOX kontrolleri, işinize yarayıp veya yaramayan aletler almak için değil, diğer bir Enron'u önlemek için gereklidirler.

Tezgah üztü aletler, eğitim, kod kontrolleri veya iş süreci değişiklikleri gibi bütün kontroller, ölçülebilen yararlara ve riski değerlendirebilme yetisine göre seçilmelidirler, kutucuklara tik atmak için değil.

Geliştirme Metodolojisi

Yüksek performanslı geliştirme iş yerleri bir geliştirme metodolojisi ve kod standardları belirlemişlerdir. Geliştirme metodolojisi tercihi seçmek basitçe birine sahip olmak kadar önemli değildir.

Gelişigüzel geliştirme, güvenli uygulamalar üretmek için yeterli yapıya sahip değildir. Güvenli kod üretmek isteyen organizasyonlar, her zaman amacı destekleyecek bir metodolojiye gereksinim duyarlar. Doğru metodolojiyi seçin – küçük takımlar asla, bir çok rolü belirleyen ağır metodolojileri seçmemelidirleri. Geniş takımlar kendi gereksinimlerine göre büyüklükte metodolojiler seçmelidirler.

Bir geliştirme metodolojisinde aranması gereken noktalar:

- Güçlü bir dizayn, test ve dokümantasyon anlayışı
- Güvenlik kontrollerinin (tehdit risk analizi, meslektaş denetimi, kod gözden geçirmeleri, vb.gibi) koyulabileceği yerler
- Organizasyonun büyüklüğüne ve olgunluğuna uygun
- Geçerli hata oranını düşürecek ve geliştiricinin verimliliğini geliştirecek potansiyele sahip olması

Kodlama Standardları

Metodolojiler kod standardları değillerdir; her iş yeri, olağan uygulamalarına göre ne kullanacağına karar vermek durumundadır veya en iyi uygulamalara göre belirlenmiş kanunlara uyarlar.

Değerlendirilecek yapılar:

- Yapısal yol göstermeler (mesela, “web katmanı veritabanını direk olarak çağırmaz”)
- En az seviyede dokümantasyon gereklidir
- Zorunlu test şartları
- En az seviyede kod içi yorumlar ve tercih edilen yorum stili
- Olağan dışı durum yönetiminin (exception handling) kullanımı
- Kontrol blokları akışının kullanımı (mesela, “Bütün şartlı akışların (conditional flows) açık ifade bloklarını (statement blocks) kullanması”)
- Tercih edilen değişkeni fonksiyon, sınıf ve tablo metot isimlendirilmesi
- Akıllı ve komplex kod yerine yönetebilir, açık kodu şeçin

Girinti (indent) stili ve sekmeler (tabbing) kutsal birer savaştır, ve güvenlik perspektifinden o kadar da önemli değildirler. Ama, artık 80x24 terminalleri kullanmadığımıza göre, düşey boşluk artık eskisi kadar önemli değildir. Girintiler ve sekmeler otomatik araçlar veya bir kod düzenleyicisi kullanılarak düzeltilebilir, bu nedenle bu konuda çok titiz olmayın.

Kaynak Kodu Kontrolü

Yüksek performanslı yazılım mühendisliği, ilgili testler ile birlikte, koda uygulanacak düzenli geliştirmeleri gerektirir. Bütün kodlar ve testler eski hallerine döndürülebilmeli ve versiyonlanmalıdırlar.

Bu dosyaları bir dosya sunucusuna kopyalamak ile olur ama bunun Subversion, CVS, SourceSafe, veya ClearCase gibi bir kaynak kodu revizyon aracı ile yapılması daha iyidir.

Gözden geçirilip ve düzeltilmiş bir koda neden testler uygulanır? Daha sonra yapılandırılmış kodlara (build) uygulanan testler ile önce yapılandırılmış kodlara uygulanan testler birbirlerinden farklıdırlar. Bir testin uygulanması gereken yapılandırılmış koda uygulanması hayati önem taşır.

Dökümanın Aslı : OWASP GUIDE 2.0.1

Çeviri : Bedirhan Urgun - bedirhan@webguvenligi.org