Principles of Security

Task 1 Introduction (Giriş)

Aşağıdaki oda, bilgi güvenliğinin bazı temel ilkelerini ana hatlarıyla açıklayacaktır. Verileri ve sistemleri korumak için kullanılan çerçevelerden, verileri tam olarak neyin güvenli kıldığına dair unsurlara kadar.

Bu oda boyunca tartışılan önlemler, çerçeveler ve protokollerin hepsi "Derinlemesine Savunma "da küçük bir rol oynamaktadır.

Derinlemesine Savunma, çoklu katmanların bir kuruluşun güvenlik çevresinde yedeklilik sağlayacağı umuduyla bir kuruluşun sistemleri ve verileri için çok çeşitli güvenlik katmanlarının kullanılmasıdır.

Devam edelim!

Görev 2 The CIA Triad (CIA Üçlüsü)

CIA üçlüsü, bir güvenlik politikası oluşturulurken göz önünde bulundurulan bir bilgi güvenliği modelidir. Bu model 1998 yılında kullanılmaya başlanmasına kadar uzanan geniş bir geçmişe sahiptir.

Bu tarihçenin nedeni, bilgi güvenliğinin (bilgi güvenliği) siber güvenlikle başlamaması ve/veya bitmemesi, bunun yerine dosyalama, kayıt saklama vb. senaryolar için geçerli olmasıdır.

Üç bölümden oluşmaktadır: Gizlilik, Bütünlük ve Kullanılabilirlik (CIA), bu model günümüzde hızla bir endüstri standardı haline gelmiştir. Bu model, uygulandığı verinin değerini ve buna bağlı olarak işletmenin ihtiyaç duyduğu ilgiyi belirlemeye yardımcı olmalıdır.

CIA üçlüsü, ayrı ayrı bölümlere sahip olduğunuz geleneksel bir modelden farklıdır; bunun yerine sürekli bir döngüdür. CIA üçlüsünün üç unsuru tartışmalı bir şekilde örtüşebilirken, sadece bir unsur bile karşılanmazsa, diğer ikisi işe yaramaz hale

gelir (ateş üçgenine benzer). Eğer bir güvenlik politikası bu üç bölüme cevap vermiyorsa, nadiren etkili bir güvenlik politikasıdır.

CIA üçlüsünün üç unsuru tartışmasız bir şekilde kendini açıklıyor olsa da, bunları inceleyelim ve siber güvenlik bağlamına oturtalım.

Confidentiality (Gizlilik)

Bu unsur, verilerin yetkisiz erişime ve kötüye kullanıma karşı korunmasıdır. Kuruluşlar her zaman sistemlerinde saklanan bir tür hassas veriye sahip olacaktır. Gizliliği sağlamak, bu verileri amaçlanmadığı taraflardan korumaktır.

Bunun için birçok gerçek dünya örneği vardır, örneğin çalışan kayıtları ve muhasebe belgeleri hassas olarak kabul edilecektir. Gizlilik, yalnızca İK yöneticilerinin çalışan kayıtlarına erişmesi, inceleme ve sıkı erişim kontrollerinin mevcut olması anlamında sağlanacaktır. Muhasebe kayıtları daha az değerli (ve dolayısıyla daha az hassas) olduğundan, bu belgeler için o kadar sıkı erişim kontrolleri uygulanmayacaktır. Ya da örneğin, bir hassasiyet sınıflandırma sistemi kullanan hükümetler (çok gizli, gizli, sınıflandırılmamış)

Integrity (Bütünlük)

Bütünlüğün CIA üçlüsü unsuru, yetkilendirilmiş değişiklikler yapılmadığı sürece bilginin doğru ve tutarlı tutulması durumudur. Bilginin dikkatsiz erişim ve kullanım, bilgi sistemindeki hatalar veya yetkisiz erişim ve kullanım nedeniyle değişmesi mümkündür. CIA üçlüsünde bütünlük, bilgide değişiklik içermeyen depolama, iletim ve kullanım sırasında bilgi değişmeden kaldığında korunur. Verilerin yetkisiz kişiler tarafından değiştirilemeyeceğinden emin olmak için adımlar atılmalıdır (örneğin, gizlilik ihlali).

Bütünlüğü sağlamak için birçok savunma mekanizması devreye sokulabilir. Erişim kontrolü ve titiz kimlik doğrulama, yetkili kullanıcıların yetkisiz değişiklikler yapmasını önlemeye yardımcı olabilir. Karma doğrulamalar ve dijital imzalar, işlemlerin gerçek olmasını ve dosyaların değiştirilmemesini veya bozulmamasını sağlamaya yardımcı olabilir.

Availability (Kullanılabilirlik)

Verilerin faydalı olabilmesi için kullanıcı tarafından kullanılabilir ve erişilebilir olması gerekir.

Kullanılabilirlik çoğu zaman bir kuruluş için önemli bir ölçüttür. Örneğin, web sitelerinde veya sistemlerinde %99,99 çalışma süresine sahip olmak (bu Hizmet Seviyesi Anlaşmalarında belirtilmiştir). Bir sistem kullanılamadığında, genellikle kuruluşların itibarına zarar verir ve mali kayıplara yol açar. Kullanılabilirlik, aşağıdakiler de dahil olmak üzere birçok unsurun bir araya gelmesiyle elde edilir:

Bilgi teknolojisi sunucuları için güvenilir ve iyi test edilmiş donanımlara sahip olmak (örn. saygın sunucular)

Birincil sistemin arızalanması durumunda yedek teknoloji ve hizmetlere sahip olmak

Teknolojiyi ve hizmetleri saldırılara karşı korumak için uzman güvenlik protokolleri uygulamak

soru⇒ CIA üçlüsünün hangi unsuru verilerin yetkisiz kişiler tarafından değiştirilememesini sağlar?

cevap⇒ **integrity**

soru ⇒ CIA üçlüsünün hangi unsuru verilerin kullanılabilir olmasını sağlar?

cevap ⇒ **availability**

soru ⇒ CIA üçlüsünün hangi unsuru verilere yalnızca yetkili kişiler tarafından erişilmesini sağlar?

cevap ⇒ **confidentiality**

Task 3 Principles of Privileges (Ayrıcalıkların İlkeleri)

Bireylerin bir bilgi teknolojisi sistemine ihtiyaç duydukları çeşitli erişim düzeylerini yönetmek ve doğru bir şekilde tanımlamak hayati önem taşımaktadır.

Bireylere verilen erişim seviyeleri iki temel faktöre göre belirlenir:

Bireyin kurum içindeki rolü/işlevi

Sistemde depolanan bilgilerin hassasiyeti

Bireylerin erişim haklarını atamak ve yönetmek için iki temel kavram kullanılır: Ayrıcalıklı Kimlik Yönetimi (PIM) ve Ayrıcalıklı Erişim Yönetimi (ya da kısaca PAM).

Başlangıçta bu iki kavram örtüşüyor gibi görünebilir; ancak birbirlerinden farklıdırlar. PIM, bir kullanıcının bir kuruluş içindeki rolünü bir sistem üzerindeki erişim rolüne çevirmek için kullanılır. PAM ise diğer şeylerin yanı sıra bir sistemin erişim rolünün sahip olduğu ayrıcalıkların yönetimidir.

Ayrıcalık ve erişim kontrollerini tartışırken esas olan en az ayrıcalık ilkesidir. Basitçe, kullanıcılara en az miktarda ve yalnızca görevlerini yerine getirmeleri için kesinlikle gerekli olan ayrıcalıklar verilmelidir. Diğer insanlar, insanların yazdıklarına güvenebilmelidir.

soru ⇒ "PIM" kısaltması ne anlama geliyor?

cevap ⇒ **Privileged Identity Management**

soru ⇒ "PAM" kısaltması ne anlama geliyor?

cevap ⇒ **Privileged Access Management**

soru⇒ Bir sistem erişim rolünün sahip olduğu ayrıcalıkları yönetmek isteseydiniz hangi metodolojiyi kullanırdınız?

cevap⇒ **PAM**

soru ⇒ Bir kullanıcının bir kuruluştaki rolüne/sorumluluklarına dayalı bir sistem rolü oluşturmak isterseniz, bu hangi metodolojidir?

cevap⇒ **PIM**

Task 4 Security Models Continued (Güvenlik Modelleri Devamı)

Güvenlik modellerini daha fazla tartışmadan önce, CIA üçlüsünün üç unsurunu hatırlayalım: Gizlilik, Bütünlük ve Kullanılabilirlik. Bu unsurların ne olduğunu ve önemini daha önce ana hatlarıyla belirtmiştik. Ancak, bunu başarmanın resmi bir yolu vardır.

Bir güvenlik modeline göre, bilgi depolayan herhangi bir sistem veya teknoloji parçası bir bilgi sistemi olarak adlandırılır; bu görevde sistemlere ve cihazlara bu şekilde atıfta bulunacağız.

CIA üçlüsünün üç unsuruna ulaşmak için kullanılan bazı popüler ve etkili güvenlik modellerini inceleyelim.

Bell-La Padula Modeli

Gizliliği sağlamak için Bell-La Padula Modeli kullanılır. Bu modelin, kullanıldığı kurumun herkesin sorumluluklarının/rollerinin iyi tanımlandığı hiyerarşik bir yapıya sahip olması gibi birkaç varsayımı vardır.

Model, veri parçalarına (nesne olarak adlandırılır) kesinlikle bilinmesi gereken bir temelde erişim izni vererek çalışır. Bu model "yazmak yok, okumak yok" kuralını kullanır.

Avantajlar	Dezavantajlar
Bu modeldeki politikalar gerçek hayattaki kurum hiyerarşilerine uyarlanabilir (ve tersi de geçerlidir)	Bir kullanıcı bir nesneye erişemese bile, onun varlığından haberdar olacaktır -- yani bu açıdan gizli değildir.
Uygulanması ve anlaşılması basittir ve başarılı olduğu kanıtlanmıştır.	Model, kurum içinde büyük miktarda güvene dayanmaktadır.

Bell LaPadula Modeli, hükümet ve ordu gibi kuruluşlarda popülerdir. Bunun nedeni, kuruluşların üyelerinin halihazırda inceleme adı verilen bir süreçten geçtiğinin varsayılmasıdır. İnceleme, başvuru sahiplerinin geçmişlerinin incelenerek kurum için oluşturdukları riskin tespit edildiği bir tarama sürecidir. Bu nedenle, başarılı bir şekilde incelenen başvuru sahiplerinin güvenilir olduğu varsayılır - bu model de bu noktada devreye girer.

Biba Model

Biba modeli, CIA üçlüsünün bütünlüğü açısından Bell-La Padula modeline eşdeğerdir.

Bu model nesnelere (verilere) ve öznelere (kullanıcılara) "yukarı yazmak yok, aşağı okumak yok" şeklinde özetlenebilecek kuralı uygular. Bu kural, öznelerin kendi seviyelerinde veya altındaki nesnelere içerik oluşturabileceği veya yazabileceği, ancak yalnızca öznenin seviyesinin üzerindeki nesnelerin içeriğini okuyabileceği anlamına gelir.

Bu modelin bazı avantaj ve dezavantajlarını aşağıdaki tabloda karşılaştıralım:

Avantajlar	Dezavantajlar
Bu modelin uygulanması basittir.	Birçok erişim seviyesi ve nesne olacaktır. Güvenlik kontrolleri uygulanırken bazı şeyler kolayca gözden kaçabilir.

Bell-La Padula modelinin sınırlamalarını hem gizlilik hem de veri bütünlüğünü ele alarak çözer.	Genellikle işletme içinde gecikmelere neden olur. Örneğin, bu modelin uygulandığı bir hastanede bir doktor, bir hemşirenin tuttuğu notları okuyamaz.

Biba modeli, bütünlüğün gizlilikten daha önemli olduğu kurumlarda veya durumlarda kullanılır. Örneğin, yazılım geliştirmede, geliştiricilerin yalnızca işleri için gerekli olan koda erişimleri olabilir. Veritabanları vb. gibi kritik bilgi parçalarına erişmeleri gerekmeyebilir.

soru ⇒ "Yukarıdan okunamaz, aşağıdan okunabilir" kuralını kullanan modelin adı nedir?(ipucu=Biçimlendirme: x Modeli Modele bağlı olarak hangi yönlerin yukarı/aşağı okunabileceğini anlamak için okların yönüne ve yanlarındaki metne bakın. Not: Bazı ders kitaplarında "yukarı okuma yok" ve "aşağı yazma yok" olarak tanımlanmaktadır.)

cevap ⇒ **The Bell-LaPadula Model**

soru ⇒ "Yukarı okuyabilir, aşağı okuyamaz" kuralını kullanan modelin adı nedir? (Biçimlendirme: x Modeli Modele bağlı olarak hangi yönlerin yukarı/aşağı okunabileceğini anlamak için okların yönüne ve yanlarındaki metne bakın. Not: Bazı ders kitaplarında bu durum "aşağı okuma yok" ve "yukarı yazma yok" olarak tanımlanmaktadır.)

cevap ⇒ **The Biba Model**

soru ⇒ Eğer bir ordu mensubu olsaydınız, hangi güvenlik modelini kullanırdınız? (Biçimlendirme: X Modeli)

cevap ⇒ **The Bell-LaPadula Model**

soru ⇒ Bir yazılım geliştiricisi olsaydınız, şirket belki de hangi güvenlik modelini kullanırdı? (Biçimlendirme: X Modeli)

cevap ⇒ **The Biba Model**

Task 5 Threat Modelling & Incident Response (Tehdit Modelleme ve Olay Müdahalesi)

Tehdit modellemesi, bir kuruluşun bilgi teknolojisi altyapısı ve hizmetlerinde yürürlükte olan güvenlik protokollerinin gözden geçirilmesi, iyileştirilmesi ve test edilmesi sürecidir.

Tehdit modelleme sürecinin kritik bir aşaması, bir uygulama veya sistemin karşılaşabileceği olası tehditleri, bir sistem veya uygulamanın savunmasız olabileceği güvenlik açıklarını belirlemektir.

Tehdit modelleme süreci, işyerlerinde çalışanlar ve müşteriler için yapılan risk değerlendirmesine çok benzer. İlkelerin hepsi geri döner:

Hazırlık

Tanımlama

Hafifletmeler

İnceleme

Bununla birlikte, özel bir ekiple sürekli inceleme ve tartışma gerektiren karmaşık bir süreçtir.
Etkili bir tehdit modeli şunları içerir:

Tehdit istihbaratı

Varlık tanımlama

Hafifletme yetenekleri

Risk değerlendirmesi

Bu konuda yardımcı olmak için STRIDE (Kimlik sahteciliği, Verilerle oynama, İnkar tehditleri, Bilgi ifşası, Hizmet reddi ve Ayrıcalıkların yükseltilmesi) ve PASTA (Saldırı Simülasyonu ve Tehdit Analizi Süreci) gibi çerçeveler vardır. STRIDE'ı aşağıda detaylandıralım. İki Microsoft güvenlik araştırmacısı tarafından 1999 yılında kaleme alınan STRIDE bugün hala geçerliliğini korumaktadır. STRIDE, aşağıdaki tabloda detaylandırdığım altı ana ilkeyi içermektedir:

Prensip	Açıklaması
Spoofing	Bu ilke, bir sisteme erişen isteklerin ve kullanıcıların kimliklerini doğrulamanızı gerektirir. Spoofing, kötü niyetli bir tarafın kendisini yanlışlıkla başka bir taraf olarak tanıtmasını içerir. Erişim anahtarları (API anahtarları gibi) veya şifreleme yoluyla imzalar bu tehdidin giderilmesine yardımcı olur.

Tampering (Kurcalama)	Bir sisteme veya uygulamaya kurcalamaya karşı önlemler sağlayarak, verilerin bütünlüğünü sağlamaya yardımcı olursunuz. Erişilen veriler bütünlüklü ve doğru tutulmalıdır. Örneğin, mağazalar gıda ürünleri üzerinde mühür kullanmaktadır.
Repudiation (Reddetme)	Bu ilke, bir sistem veya uygulamanın izlemesi için faaliyetlerin kaydedilmesi gibi hizmetlerin kullanımını belirler.
Information Disclosure (Bilgi Açıklaması)	Birden fazla kullanıcının bilgilerini işleyen uygulamaların veya hizmetlerin, yalnızca sahibiyle ilgili bilgileri gösterecek şekilde uygun şekilde yapılandırılması gerekir.
Denial of Service (Hizmet Reddi)	Birden fazla kullanıcının bilgilerini işleyen uygulamaların veya hizmetlerin, yalnızca sahibiyle ilgili bilgileri gösterecek şekilde uygun şekilde yapılandırılması gerekir.
Elevation of Privilege (Ayrıcalığın Yükseltilmesi)	Bu, bir uygulama veya hizmet için en kötü durum senaryosudur. Bu, bir kullanıcının yetkilerini daha yüksek bir seviyeye, yani bir yöneticiye yükseltebildiği anlamına gelir. Bu senaryo genellikle daha fazla istismara veya bilgi ifşasına yol açar.

Bir güvenlik ihlali olay olarak bilinir. Ve tüm titiz tehdit modellerine ve güvenli sistem tasarımlarına rağmen, olaylar meydana gelir. Tehdidi çözmek ve düzeltmek için yapılan eylemler Olay Müdahalesi (IR) olarak bilinir ve siber güvenlikte tam bir kariyer yoludur.

Olaylar aciliyet ve etki derecelendirmesi kullanılarak sınıflandırılır. Aciliyet, karşılaşılan saldırı türüne göre belirlenir; etki ise etkilenen sisteme ve bunun iş operasyonları üzerindeki etkisine göre belirlenir.

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5
Low	3	4	5

Bir olaya, sistemler ve/veya mevcut olay hakkında teknik bilgiye sahip çalışanlardan oluşan önceden düzenlenmiş bir grup olan Bilgisayar Güvenliği Olay

Müdahale Ekibi (CSIRT) tarafından müdahale edilir. Bir olayı başarılı bir şekilde çözmek için, bu adımlar genellikle aşağıdaki tabloda listelenen Olay Müdahalesinin altı aşaması olarak adlandırılır:

Eylem	Açıklaması
Preparation (Hazırlık)	Güvenlik olayıyla başa çıkmak için kaynaklarımız ve planlarımız var mı?
Identification (Tanımlama)	Müdahale edebilmemiz için tehdit ve tehdit aktörü doğru bir şekilde tanımlandı mı?
Containment (Sınırlama)	Diğer sistemlerin veya kullanıcıların etkilenmesini önlemek için tehdit/güvenlik olayı kontrol altına alınabilir mi?
Eradication (Eradikasyon)	Aktif tehdidi ortadan kaldırın.
Recovery (Kurtarma)	Olağan operasyonlara dönmek için etkilenen sistemlerin tam bir incelemesini gerçekleştirin.
Lessons Learned (Çıkarılan Dersler)	Bu olaydan ne öğrenilebilir? Örneğin, bir kimlik avı e-postasından kaynaklandıysa, çalışanlar kimlik avı e-postalarını tespit etmek için daha iyi eğitilmelidir.

soru ⇒ "Spoofing" hangi modelin ana hatlarını oluşturur?

cevap ⇒ **STRIDE**

soru ⇒ "IR" kısaltması ne anlama geliyor?

cevap ⇒ **Incident Response**

soru ⇒ Verilerin bütünlüğünü iyileştirmek için bir uygulamaya bazı önlemler eklemekle görevlendirildiniz, bu hangi STRIDE ilkesidir?

cevap ⇒ **Tampering**

soru ⇒ Bir saldırgan kuruluşunuzun güvenliğine sızdı ve verileri çaldı. Sizin göreviniz kuruluşu her zamanki gibi çalışır hale getirmektir. Bu hangi olay müdahale aşamasıdır?

cevap ⇒ **Recovery**