Tehdit Modellemesi

İçerikler

Genel

Bu bölüm, bir penetrasyon testinin doğru bir şekilde yürütülmesi için bir tehdit modelleme yaklaşımını gerektiği gibi tanımlar. Standart belirli bir model kullanmaz, bunun yerine kullanılan modelin tehditlerin temsili, yetenekleri, test edilen kuruluşa göre nitelikleri ve aynı sonuçlarla gelecekteki testlere defalarca uygulanması açısından tutarlı olmasını gerektirir.

Standart, geleneksel tehdit modellemesinin iki temel unsuruna odaklanır - varlıklar ve saldırgan (tehdit topluluğu / ajan). Her biri sırasıyla ticari varlıklara ve iş süreçlerine, tehdit topluluklarına ve yeteneklerine ayrılmıştır.

En azından, dört elementin tümü her penetrasyon testinde açıkça tanımlanmalı ve belgelenmelidir.

Saldırgan tarafını modellenirken, tehdit topluluğunun üstünde (çoğunlukla semantiktir ve kuruluşun iş SWOT analizine geri bağlanabilir) ve yetenekleri (çoğunlukla teknik olan) ve motivasyon modellemesinin ek yönleri de sağlanmalıdır. Bu ek noktalar esasen hedefte bulunan farklı varlıkların değerini dikkate alır ve bunu edinme maliyeti ile birleştirilir. Tamamlayıcı bir model olarak, "ne-eğer" hakkında daha doğru bir görüş sağlamak için organizasyon için etki modellemesi de yapılmalıdır. Belirlenen varlıkların her birinin kayıp olayını çevreleyen senaryo. Bu, varlıkları "net" değerini, içsel değerini ve bir kayıp olayıyla ilişkili diğer dolaylı olarak maruz kalan maliyetleri dikkate almalıdır.

Herhangi bir penetrasyon testi katılımının tehdit modelleme aşaması hem testçiler hem de organizasyon için kritik öneme sahiptir. Kuruluşun risk iştahı ve önceliklendirmesi kadar netlik sağlar (hangi varlıklar diğerlerinden daha önemlidir? Topluluklar hangi tehdit diğerlerinden daha alakalıdır?). Ek olarak, test cihazının saldırganın araçlarını, tekniklerini, yeteneklerini, erişilebilirliğini ve genel profilini yakından taklit eden bir angajman sunmaya odaklanırken, kuruluşun içindeki gerçek hedeflerin ne olduğunu göz önünde bulundurur, böylece daha alakalı kontroller, süreçler ve altyapı, BT unsurlarının envanter listesinden ziyade teste tabi tutulur. Tehdit modeli, kuruluşun mümkün olduğunda test edilmesiyle koordineli olarak ve test cihazının organizasyon hakkında önceden herhangi bir bilgiye sahip olmadığı tam bir kara kutu durumunda bile, testçi, saldırganın hedef kuruluşla ilgili OSINT ile birlikte görüşüne dayalı bir tehdit modeli oluşturmalıdır.

Model açıkça belgelenmeli ve nihai raporun bir parçası olarak teslim edilmelidir, çünkü rapordaki bulgular, kuruluşa özgü daha doğru bir alaka düzeyi ve risk puanı oluşturmak için tehdit modelini referans alacaktır (genel bir teknik teknik olmaktan ziyade).

Yüksek seviyeli tehdit modelleme süreci

1. İlgili belgeleri toplayın
2. Birincil ve ikincil varlıkları tespit etmek ve kategorize etmek
3. Tehdit ve tehdit topluluklarını tanımlamak ve kategorize etmek
4. Birincil ve ikincil varlıklara karşı toplulukları haritalayın

Örnek

Bir PTES değerlendirmesi ışığında, dahili olarak barındırılan CRM uygulaması kapsamda olabilir. Arka uç veritabanında depolanan müşteri bilgileri, kapsamdaki uygulamaya doğrudan bağlı olduğu için kolayca tanımlanabilir bir birincil varlıktır. Ancak veritabanı sunucusunun teknik tasarımını inceleyerek, aynı arka uç veritabanı sunucusunda depolanan İK veritabanının ikincil bir varlık olduğu da tespit edilebilir. Bir saldırgan, çalışan bilgilerini elde etmek için CRM uygulamasını bir basamak olarak kullanabilir. Temel bir tehdit modelleme uygulamasında, bazı tehdit toplulukları CRM uygulamasına haritalandırıldığında alakalı olarak tanımlanabilir, ancak ikincil varlıkları belirleyerek tehdit manzarası aniden değişir.

Yüksek seviyeli modelleme araçları

Hedefleri tanımlamak ve saldırı vektörlerini haritalamak için çeşitli araçlar mevcuttur. Bunlar normalde iş varlıklarına (hangi sistemlerin hedefleneceğine) ve iş süreçlerine (onlara nasıl saldırır) odaklanır. Katılıma bağlı olarak, penetrasyon testi ekibi bu egzersizleri müşteriden hiçbir girdi olmadan gerçekleştirebilir; veya

müşteri paydaşlarının ilgi hedeflerini belirlemesiyle çok fazla zaman harcayabilirler. İşletme varlığı odağına sahip araçlar genellikle her bir potansiyel hedefin test etmek için ne kadar önemli olduğunu tanımlamak için nicel bir girdi gerektirir. Girişler, müşterinin CIO'su tarafından bir sistemin görev açısından kritik olduğu bir açıklama gibi niteliksel de olabilir. İş süreçlerine, bilgi akışlarına ve teknik mimariye odaklanan araçlar, potansiyel saldırı vektörlerini tanımlamak ve çoğunlukla başarılı olması muhtemel veya belirli bir hasım sınıfı tarafından kullanılması muhtemel olan seçimlerin kullanılması için kullanılır.

İş Varlığı Analizi

İş varlık analizi sırasında, tehdit modelleme egzersizinin bir parçası, tüm varlıklara ve kapsamda dahil edilen onları destekledikleri iş süreçleri üzerinde varlık merkezli bir görüş alınır. Toplanan belgeleri analiz ederek ve organizasyon içindeki ilgili personelle görüşerek, bir saldırgan tarafından hedef alınması muhtemel varlıkları, değerlerinin ne olduğunu ve (kısmi) kayıplarının ne olacağını belirleyebilir.

Örgütsel Veriler

Politikalar, Planlar ve Prosedürler

İç politikalar, planlar ve prosedürler, kuruluşun nasıl iş yaptığını tanımlar. Bu belgeler, bir kuruluşun ve bir şirketin çalışmasını sağlayan kritik iş süreçlerindeki kilit rolleri belirlemeye yardımcı olabileceğinden özellikle ilgi çekicidir.

Ürün Bilgileri (örneğin ticari sırlar, Ar-Ge verileri)

Ürünle ilgili bilgiler, herhangi bir patent, ticari sır, gelecek planları, kaynak kodu, ürün piyasası değerini, algoritmaları ve kuruluşun bu ürünün iş başarısının önemli bir faktörü olarak gördüğü diğer bilgileri doğrudan etkileyen destekleyici sistemleri içerir.

Pazarlama Bilgileri (planlar, yol haritaları vb.)

Promosyonlar, lansmanlar, ürün değişiklikleri, konumlandırma, ortaklıklar, 3. parti sağlayıcıları, organizasyon içindeki veya dışındaki faaliyetlerle ilgili iş planları için pazarlama planları. Ek olarak, ortakların, muhabirlerin, danışmanlık firmasının ayrıntıları ve bu tür kuruluşlarla yapılan herhangi bir yazışma gibi PR ile ilgili veriler de çok aranan bir hedef olarak kabul edilir.

Finansal Bilgiler (örneğin banka, kredi, özkaynak hesapları)

Finansal bilgi genellikle bir kuruluşun sahip olduğu en korunaklı bilgilerden bazılarıdır. Bu bilgiler, diğerlerinin yanı sıra banka hesap bilgilerini, kredi kartı hesap bilgilerini ve / veya kredi kartı numaralarını ve yatırım hesaplarını içerebilir.

Teknik Bilgiler

Organizasyon ve kuruluşun operasyonları hakkında teknik bilgiler, penetrasyon test cihazına benzersiz bir ilgi alanıdır. Bu tür bilgiler genellikle bir penetrasyon testinin sunulması beklenen değildir, ancak değerli bilgileri diğer alanlara besleyerek test sürecini kolaylaştırır; altyapı tasarımı bilgileri İstihbarat Toplama sürecine değerli veriler sağlayabilir.

- Altyapı Tasarım Bilgileri

Altyapı tasarımı ile ilgili bilgiler, organizasyonu yürütmek için kullanılan tüm temel teknolojiler ve tesislerle ilgilidir. Yapı planları, teknik kablolama ve bağlantı diyagramları, bilgi işlem ekipmanları / ağ tasarımları ve uygulama seviyesi veri işleme, altyapı tasarımları olarak kabul edilir.

- Sistem Yapılandırma Bilgileri

Sistem yapılandırma bilgileri yapılandırma temel dokümantasyon, yapılandırma kontrol listeleri ve sertleştirme prosedürleri, grup politikası bilgileri, işletim sistemi görüntüleri, yazılım envanterleri vb. içerir. Bu bilgiler, güvenlik açıklarının keşfine yardımcı olabilir (konfis hataları veya modası geçmiş yazılım kurulumları bilgisi ile olduğu gibi).

- Kullanıcı Hesabı Kimlik Bilgileri

Kullanıcı hesabı kimlik bilgileri, doğrulamak için bir araç var olduğu sürece, ayrıcalıklı olmayan bir düzeyde bilgi sistemine erişimi kolaylaştırmaya yardımcı olur (örneğin. VPN, web portalı vb.).

- Ayrıcalıklı Kullanıcı Hesabı Kimlik Bilgileri

Ayrıcalıklı kullanıcı hesabı kimlik bilgileri, doğrulamanın bir yolu olduğu sürece, yüksek bir erişim seviyesinde, bilgi sistemine erişimi kolaylaştırmaya yardımcı olur (örneğin. VPN, web portalı vb.). Ayrıcalıklı kullanıcı hesabı kimlik bilgilerinin alınması genellikle test edilen bilgi sisteminin tehlikeye girmesine neden olur.

Çalışan Verileri

Burada çalışan verileri, bir saldırgan tarafından bir onaycı tarafından elde edilen veya tehlikeye girebilecek herhangi bir verinin sağlanması gibi analiz edilmektedir. Bu tür verilerin kaybına veya maruziyetine para cezaları veren bazı uyumlara uymak zorunda olan kuruluşlar, bu tür doğrudan bir kayıp etkisi için bariz adaylardır. Ayrıca, çalışanları kritik varlıklar olarak kabul edilebilecek kuruluşlar da bu tür incelemelere tabi tutulabilir (özel hükümet organları, uzmanlaşmış ticari sırla ilgili çalışanlar / departmanlar vb.) Aşağıdaki liste, tehdit modellemesi için iş varlıkları olarak kabul edilebilecek kişisel verilerin bilgi alanlarına örnekler sunar.

- Ulusal Kimlik Numaraları (SSN'ler vb.)
- Kişisel Olarak Tanımlanabilir Bilgiler (PII)
- Korumalı Sağlık Bilgileri (PHI)
- Finansal Bilgiler (örneğin banka, kredi hesapları)

Müşteri Verileri

Çalışan verileri gibi, müşteri verileri, bu tür bilgiler kuruluşa doğrudan / dolaylı bir zarara neden olacağında tehdit modelleme sürecinde bir iş varlığı olarak kabul edilir. Düzenleyici / uyum ihtiyacının (para cezalarına göre) üzerine, bu tür veriler dolandırıcılık yapmak için kullanılabildiğinde, kuruluşun dolandırıcılıkla ilgili kayıplar için sorumlu tutulabileceği veya dava edilebileceği (dolandırıcılığın gerçekleşmesini sağlayan müşteri bilgilerini kaybetmeye dayanarak) burada ek bir faktör devreye girer. Aşağıdaki liste, ilgili müşteri verilerini tutabilecek ve tehdit modellemesi uğruna iş varlıkları olarak kabul edilmesi gereken bu tür bilgi alemlerinin örneklerini sunar.

- Ulusal Tanımlama Sayıları (SSN'ler, vb.)
- Kişisel Olarak Tanımlanabilir Bilgiler (PII)
- Korumalı Sağlık Bilgileri (PHI)

- Finansal Hesaplar (örneğin banka, kredi, özkaynak hesapları)
- Tedarikçi Verileri

Kuruluş için kritik olarak kabul edilen tedarikçilerle ilgili bilgiler (kritik bileşen üreticileri, ticari bir sırrın parçası olabilecek tedarikçilerle yapılan anlaşmalar, tedarik edilen bileşenlerin maliyet analizi) ve tedarikçileri aracılığıyla kuruluşun iş operasyonlarını etkilemek için kullanılabilecek herhangi bir veri bir iş varlığı olarak kabul edilir.

- Ortak Verileri
- "Bulut" Hizmet Hesabı Bilgileri

İnsan Varlıkları

Bir organizasyondaki insan varlıklarını tanımlarken, bağlamın bu tür varlıkların örgütü tehlikeye atmak için daha büyük bir çabanın parçası olduğunu hatırlamak zorundayız. Bu nedenle, ticari varlıklar olarak tanımlanan insan varlıkları, bilgiyi ifşa etmek için kaldıraçlanabilecek, organizasyonu olumsuz yönde etkileyecek kararlar veya eylemler yapmak için manipüle edilebilen veya bir saldırganın daha fazla taviz vermesini sağlayan varlıklardır. İnsan varlıkları mutlaka kurumsal hiyerarşi içinde en yüksek değildir, ancak daha önce tanımlanmış ticari varlıklarla ilgili olan veya bu tür varlıklara erişimi sağlamak için pozisyonlarda olan daha sık kilit personeldir. Bu liste, normalde sınırlı şirket varlıklarına erişimle ilişkili olmayan çalışanları da içerebilir, ancak güvenlik veya prosedürün ihlalini kolaylaştıran bir şirkete fiziksel erişim sağlayacak bir konumda olabilir. Aşağıdaki liste, bu tür varlıkların bazı örneklerini sağlar ve test edilen kuruluşa uyarlanmalıdır.

- Yönetici Yönetimi
- Yönetici Asistanları
- Orta Yönetim
- İdari Asistanlar
- Teknik/Takım Liderleri
- Mühendisler
- Teknisyenler
- İnsan Kaynakları

İş Süreci Analizi

Bir iş para kazanmazsa bir iş değildir. Bunun olma şekli, onları geliştirmek ve katma değer yaratmak için çeşitli süreçlerden geçen ham malların veya bilginin incelenmesidir. Bu da gelir elde ediyor. İş süreçleri ve onları destekleyen varlıklar (insanlar, teknoloji, para) değer zincirleri oluşturur. Bu süreçleri haritalandırarak, kritik olmayan kritik süreçleri belirleyerek ve sonunda kusurları tespit ederek, işin nasıl çalıştığını, onları neyin para kazandırdığını ve sonunda belirli tehdit topluluklarının para kaybetmelerini sağlayabileceğini anlayabiliyoruz.

İş süreci analizinde kritik iş süreçleri ile kritik olmayan süreçler arasında ayrım yaparız. Her kategori için analiz aynıdır ve aynı unsurları dikkate alır. Temel fark, kritik bir iş sürecinden gelen tehdidin kritik olmayan bir iş sürecinin aksine atanmasıdır. Bununla birlikte, birkaç kritik olmayan iş sürecinin birliğinin, bir element / süreç içinde esasen kritik bir kusur oluşturan bir senaryoda birleştirilebileceğini hatırlamak zorunludur. Bu tür tehdit senaryoları da bu aşamada tanımlanmalı ve penetrasyon testinde daha sonra kullanılmak üzere haritalanmalıdır.

Teknik altyapı destek süreci

İş süreçleri genellikle BT altyapısı tarafından desteklendiğinden (bilgisayar ağları, işleme gücü, bilgi girmek ve iş sürecini yönetmek için PC'ler vb. ...) tarafından desteklendiğinden, tüm bu unsurların tanımlanması ve haritalandırılması gerekir. Bu tür haritalama, tehdit modelini güvenlik açığı haritalama ve sömürüye çevirirken süreçte daha sonra kullanılacak kadar açık olmalıdır.

Bilgi varlıkları destek süreci

Teknik altyapının aksine, bilgi varlıkları, kuruluşta referans olarak veya destek materyali (karar verme, yasal, pazarlama vb.) olarak kullanılan mevcut bilgi dayanaklarıdır. Bu tür varlıklar genellikle iş sürecinde zaten tanımlanmıştır ve teknik altyapının yanı sıra bilgi varlıklarını kendileri destekleyen herhangi bir ek teknik altyapı ile birlikte haritalanmalıdır.

İnsan varlıkları süreci destekliyor

İş sürecine dahil olan İK'nın tanımlanması, süreç analizinin kendisi ile birlikte yapılmalıdır (belirlenmiş olsun ya da olmasın) ve herhangi bir tür katılımı olan her kişi (belirli bir bilgi varlığı veya teknik bir altyapı unsuru ile ilgili olmasa bile) bu süreçte belgelenmeli ve haritalanmalıdır. Bu tür İK varlıkları genellikle bir onay alt sürecinin, bir doğrulama alt sürecinin veya hatta bir referansın (yasal tavsiye gibi) bir parçasıdır. Bu tür varlıklar (özellikle bilgi varlıkları veya teknik altyapı ile hiçbir ilişkisi olmayanlar) daha sonra doğada teknik olandan daha sosyal olan vektörlere saldırmak için haritalanacaktır.

3. taraf entegrasyonu ve/veya süreç kullanımı

Süreci destekleyen insan varlıklarına benzer şekilde, iş süreciyle herhangi bir ilgisi olan herhangi bir 3. taraf da haritalandırılmalıdır. Bu kategori, hem insan varlıklarını hem de bilgi / teknik olanları (saaS sağlayıcısı gibi) içerebileceği için haritalanması zor olabilir.

Tehdit Ajanları/Topluluk Analizi

İlgili tehdit topluluklarını ve ajanlarını tanımlarken, tehdidin net bir şekilde tanımlanması, konumdaki konum (iç / dış kuruluş) açısından sağlanmalıdır; konumdaki belirli topluluk ve belirli ajan / topluluk için bir yetenek / motive profili oluşturmaya yardımcı olacak herhangi bir ek ilgili bilgi. Mümkün olduğunda, belirli ajanlar tanımlanmalıdır. Aksi takdirde, herhangi bir destekleyici materyal ve istihbaratla birlikte daha genel bir topluluk özetlenmelidir. Tehdit ajanı/topluluk sınıflandırmalarının bazı örnekleri şunlardır:

İç	Dış
Çalışanlar	İş Ortakları
Yönetim (yönetim, orta)	Rakipler
Yöneticiler (ağ, sistem, sunucu)	Müteahhitler
Geliştiriciler	Tedarikçiler
Mühendisler	Ulus Devletleri
Teknisyenler	Organize Suç
Yükleniciler (aşırı kullanıcılarıyla)	Hacktivistler
Genel kullanıcı topluluğu	Senaryo Kiddies (rektici / rastgele hackleme)
Uzaktan Destek	

Çalışanlar

Doğrudan şirket için yarı zamanlı veya tam zamanlı bir sözleşme kapsamında çalışanlar. Genel olarak, çoğu şirkete güvendiği için ciddi bir tehdit oluşturuyorlar. Geçimini sağlamak ve iyi muamele gördüklerini varsayarsak, şirketi incitmek yerine korumaya meyillidir. Çoğu zaman veri kaybı olaylarına veya kazara uzlaşmaya karışır. İçeri Yabancılar tarafından izinsiz girişlere yardımcı olmak için motive edilebilirler veya kendi başlarına (örneğin haydut tüccarlar) kötü niyetli eylemlerde bulunabilirler. Beceri seviyesi değişse de genellikle düşük olur Ortadan ortaya.

Yönetim (İcracı, orta)

Doğrudan şirket için yukarıda açıklandığı gibi çalışanlar. Şirket içindeki konumları ve işlevleri göz önüne alındığında, çoğu zaman ayrıcalıklı bilgilere erişebilir ve

Tehdit Yeteneği Analizi

Bir tehdit topluluğu tespit edildikten sonra, söz konusu topluluğun yetenekleri, böyle bir topluluğun / ajanın organizasyona başarılı bir şekilde hareket etme ve onu tehlikeye atma olasılığını yansıtan doğru bir tehdit modeli oluşturmak için de analiz edilmelidir. Bu analiz hem teknik bir analiz hem de bir fırsat analizi (uygulanabilir durumlarda) gerektirir.

Kullanılan araçların analizi

Tehdit topluluğu / acentesi için mevcut olduğu bilinen herhangi bir araç burada dahil edilmelidir. Ek olarak, serbestçe mevcut olabilecek araçlar, onları potansiyellerine göre kullanabilmek için gereken gerekli beceri seviyesi için analiz edilmeli ve tehdit kabiliyetinde haritalanmalıdır.

İlgili istismarlara/ücretli araçlara uygunluk

Tehdit topluluğu / acentesi, organizasyonla ilgili çevre için istismar elde etme veya geliştirme yeteneği açısından analiz edilmelidir. Ek olarak, bu tür istismarlara / maaş yüklerine 3'üncü taraflar, iş ortakları veya yeraltı toplulukları aracılığıyla erişilebilirlik de bu analizde dikkate alınmalıdır.

İletişim mekanizmaları

Tehdit ajanı/topluluğu için mevcut iletişim mekanizmalarının bir analizi, bir kuruluşa yönelik saldırıların karmaşıklığını değerlendirmek için yapılmalıdır. Bu iletişim mekanizmaları, şifreleme gibi basit ve açık bir şekilde mevcut teknolojilerden, kurşun geçirmez barındırma, bırakma sitelerinin kullanımı ve saldırı veya maskeli bilgi vermek için bilinen veya bilinmeyen botnetlerin kullanımı gibi uzman araçlara ve hizmetlere kadar uzanır. Örneğin, testin bir parçası olarak, bir organizasyon için genel saldırı yüzeyinin dışarıdan ne olduğunu görmek için test ediyoruz. Bununla birlikte, genellikle zaman kaçırılan başka bir bileşen vardır. Sömürü sonrası ne tür tehditler var olabilir? Bu, sızdırmazlık kanallarını tespit etme bağlamına girer. Tesadüfen, penetrasyon test cihazları, günümüzün modern kötü amaçlı yazılımlarının komuta ve kontrol kanallarını tespit etmek için bir organizasyon yeteneğini test etmek için benzersiz bir konuma sahiptir. Bu kapsam olduğunda, test cihazının C2'yi gizlemek için kullanılan bulanıklık seviyesini artıran bir dizi kötü amaçlı yazılım örneği oluşturmasını öneririz. Amaç, kolayca tespit edilen kötü amaçlı yazılımlar oluşturmak, ardından tespitin artık gerçekleşmediği noktaya gizlenmeyi arttırmaktır.

Erişilebilirlik

Tehdit aktörü yetenek analizindeki son unsur, organizasyona ve / veya söz konusu belirli varlıklara erişilebilirlikleridir. Erişilebilirlik analizinde faktoring yaparken yukarıda tasvir edilen profili tamamlamak, penetrasyon testinin kuruluşun riskiyle ilgili net senaryolar oluşturmasını sağlayacaktır.

Motivasyon Modellemesi

Daha fazla analiz için tehdit ajanlarının / toplulukların olası motivasyonu belirtilmelidir. Saldırganların motivasyonları, Anonymous ve Antisec gibi grupların hacktivism markalı saldırılarındaki artışla görülebileceği gibi sürekli değişiyor. Her organizasyona ve / veya dikey pazara dayalı benzersiz motivasyonlarda ince farklılıklar olacaktır, bazı ortak motivasyonlar şunları içerir:

- Kâr (doğrudan veya dolaylı)
- Hacktivizm
- Doğrudan kin
- Eğlence / İtibar
- Ortak / bağlantılı sistemlere daha fazla erişim

Karşılaştırılabilir Kuruluşların ele geçirildiğine dair ilgili haberleri bulmak

Tam bir tehdit modeli sağlamak için, aynı endüstri dikeyindeki diğer kuruluşlara bir karşılaştırma sağlanmalıdır. Bu karşılaştırma, bu tür kuruluşlarla ilgili herhangi bir olayı veya haberi ve karşılaştıkları zorlukları içermelidir. Böyle bir karşılaştırma, tehdit modelini doğrulamak ve kuruluşun kendisini karşılaştırması için bir temel oluşturmak için kullanılır (bu kamuya açık bilginin yalnızca gerçek tehditlerin ve olayların bir kısmını temsil ettiğini hesaba katmak).
