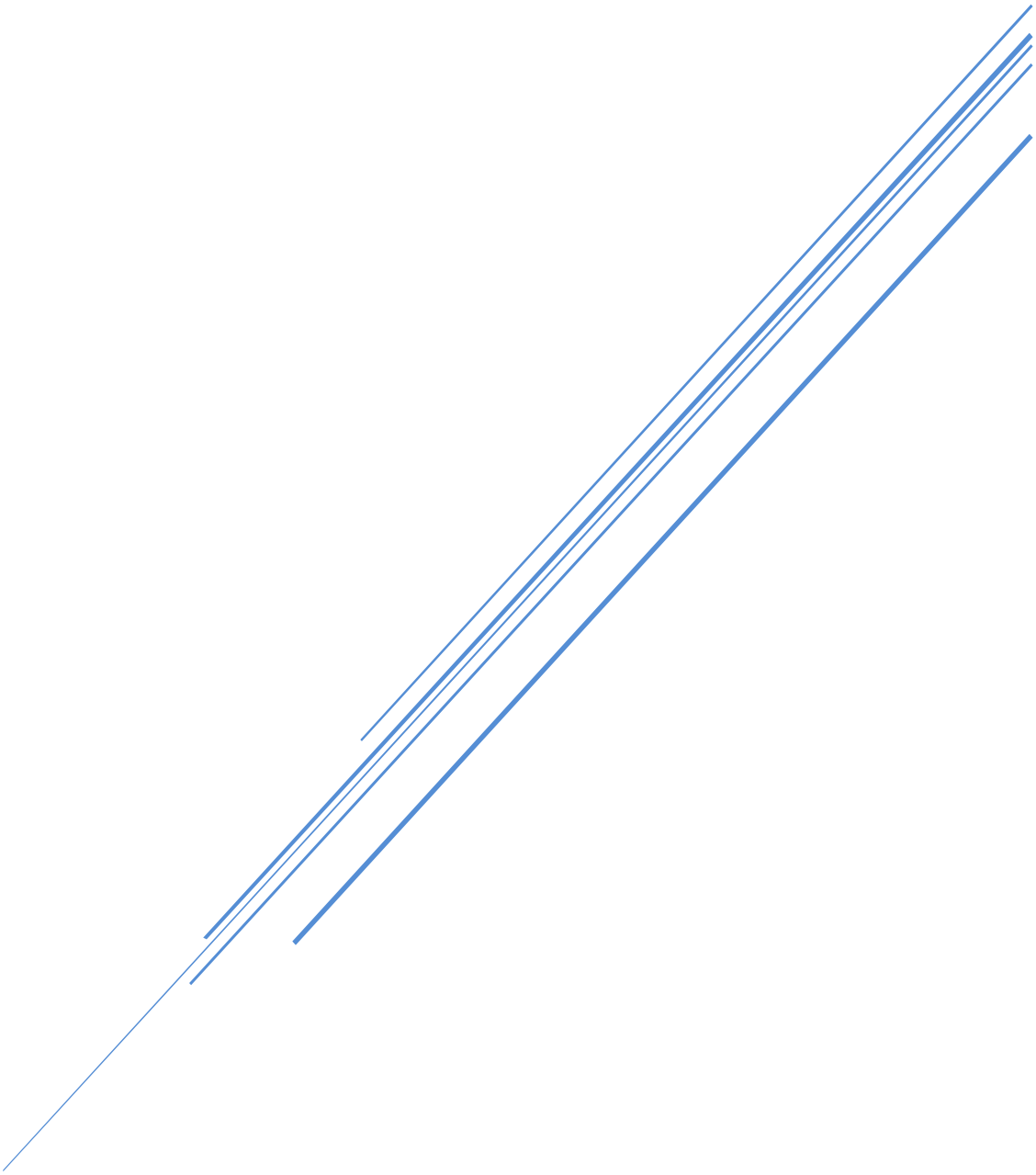
SIFIR GÜVEN (ZERO TRUST)

Öner Ziya Baş



Şubat 2022

İÇİNDEKİLER

1. Giriş 2

2. Sıfır Güven Nedir? 3

3. Sıfır Güven Teorik Model 5

4. Sıfır Güven İlkeleri 7

5. Sıfır Güven Mimarisinin Mantıksal Bileşenleri 9

6. Sıfır Güven Mimarisi Yaklaşımları 11

- **Gelişmiş Kimlik Yönetimine Sahip Sıfır Güven Mimarisi** 11
- **Mikro Segmentasyonlu Sıfır Güven Mimarisi** 11
- **Yazılım Tanımlı Ağ Çevreleriyle Sıfır Güven Mimarisi** 12

7. Sıfır Güven Mimarisi ile İlişkili Tehditler 13

8. Sonuç 15

9. Kısaltmalar 16

10. Kaynakça 17

1. Giriş

İşletmelerin bilişim altyapıları gün geçtikçe daha karmaşık hale geliyor. Tek bir işletme içinde birden fazla ağ, farklı bölgelerden mobil kullanıcılar, bulut hizmetleri, kendi altyapısına sahip uzak ofisler ve kendi cihazını kullanan kullanıcılar olabilir. Bu karmaşıklık eski güvenlik yöntemlerin yeterli olmadığını açıkça göstermektedir. Artık korunması gereken birçok çevre olduğundan saldırganlar bu çevrelerden birini ihlal ettiğinde yanal hareketlerle kritik bilgilere erişebilecektir.

İşte bu karmaşıklık, siber güvenlik için "Sıfır Güven" (Zero Trust) olarak bilinen yeni bir modelin geliştirilmesine yol açmıştır. Sıfır Güven bir ürün veya bir teknoloji değildir, bir yaklaşımdır. Bu yaklaşım öncelikle veri ve hizmet korumasına odaklanır, ancak tüm kurumsal varlıkları (cihazlar, uygulamalar, sanal ve bulut bileşenleri) ve konuları (son kullanıcılar, kaynaklardan bilgi isteyen botlar) içerecek şekilde genişletilebilir ve genişletilmelidir.

Sıfır Güven yaklaşımı kuruma ait bir ortamda bir saldırganın bulunduğunu ve bu ortamın diğer ortamlardan daha farklı olmadığını, daha güvenilir olmadığını varsayar. Böylece bu varsayım işletmenin sürekli olarak risk altında olduğunu, bunların sürekli olarak analiz edilmesi gerektiğini ve analiz sonucu oluşan riskleri azaltmak için gerekli önlemlerin alınmasını sağlar. Koruma genellikle kaynaklara erişimi en aza indirgemeyi (yetkilendirme, tam zamanında erişim, doğrulama vb) içerir.

Sıfır Güven, "Asla güvenme, her zaman doğrula" tasarım ilkesi üzerine kurulmuş modern bir güvenlik modelidir. Bir kurumun ağının içinde veya dışında olmalarına bakılmaksızın tüm cihazların ve kullanıcıların kimliklerinin doğrulanmasını, yetkilendirilmesini ve erişim verilmeden önce düzenli olarak doğrulanmasını gerektirir.

Kısacası Sıfır Güven, "Doğrulanana kadar kimseye güvenmeyin" der.

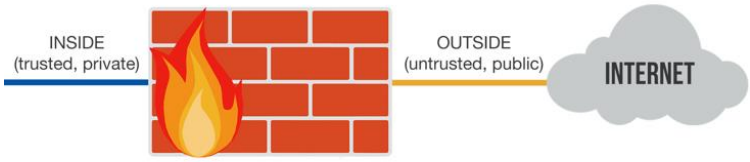
Sıfır Güven tek bir mimariden oluşmaz. Günümüzde birçok kurum kurumsal altyapısında Sıfır Güven Mimarisi unsurlarına sahiptir. Sıfır Güven Mimarisi "erişim ihtiyacı", "sürekli doğrulama" ve "minimum erişim verme" üzerine odaklanır. Ortak amaç veri ihlallerini önlemek ve içerideki yanal hareketi sınırlandırmaktır.

2. Sıfır Güven Nedir?

Sıfır Güveni destekleyen kavramların çoğunun yeni olmamasına rağmen Zero Trust konsepti ilk olarak 2010 yılında Forrester Research analisti John Kindervag tarafından "No More Chewy Centers, Introducing The Zero Trust Model Of Information Security" başlıklı bir raporda tanıtıldı. [1] Geleneksel ağ tasarımlarına duyulan güven ile ilgili yaygın sorunların listelendiği raporun yayınlanmasından birkaç yıl sonra Google, ağlarında Zero Trust güvenliğini uyguladığını duyurdu ve bu da teknoloji topluluğu içinde benimsenmeye yönelik artan bir ilgiye yol açtı.

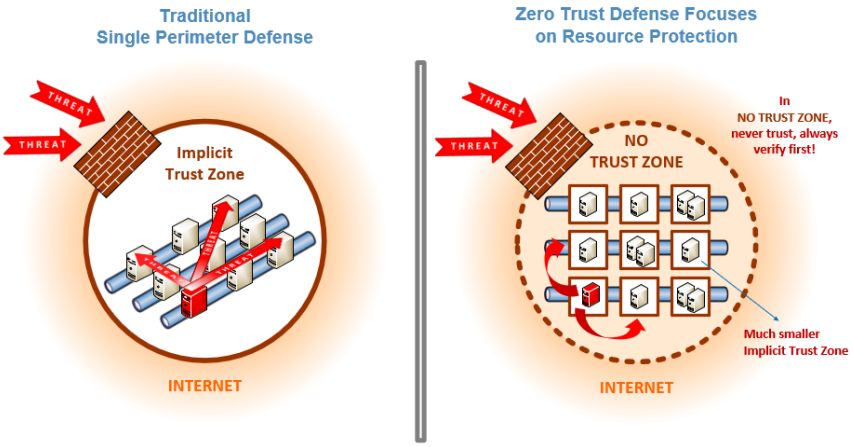
Çoğu geleneksel yaklaşım "güven ama doğrula" şeklindeyken, Sıfır Güven yaklaşımı "asla güvenme, her zaman doğrula" şeklinde açıklanabilir. Forrester, çoğu güvenlik uzmanının çok fazla güvendiğini ancak çok az doğruladığını tespit etmiştir. Varsayılan olarak insanlara güveniliyor, ancak doğrulamayı gerçekleştirmek zor olduğundan bu yapılmıyor.

Ağ güvenliğinin önemli sorunlarından biri, ağın bazı alanlarının varsayılan olarak güvenilir kabul edilmesidir. Güvenlik duvarı (firewall) gibi hemen hemen her güvenlik aygıtı, "güvenilmeyen" etiketli en az bir bağlantı noktası ve "güvenilir" etiketli başka bir bağlantı noktasıyla birlikte gelir.



Şekil 1: Güvenilir ve güvenilmeyen bağlantı noktası [2]

Günümüzde, internet bağlantısı "güvenilmeyen" bağlantı noktasına mı yoksa "güvenilir" bağlantı noktasına mı bağlanıyor? Aynı şekilde iç ağ "güvenilmeyen" bağlantı noktasına mı yoksa "güvenilir" bağlantı noktasına mı bağlanıyor? Burada yer alan sorunlardan biri, iç ağdaki varlıkların varsayılan olarak güvenilir varlıklar olarak görülmesi ve ağ içinde yetkisiz yanal hareket ederek tehdit oluşturmasıdır. Rapor, içeridekilerin de kötü niyetli olabileceğinin ve her zaman güvenilmez olarak ele alınması gerektiğinin altını çizmektedir. Sıfır Güvenin basit ilkesi, ağ trafiğine göre güveni belirlemek mümkün olmadığı için, tüm trafiğin güvenilmez bir şekilde ele alınması gerektiğidir.



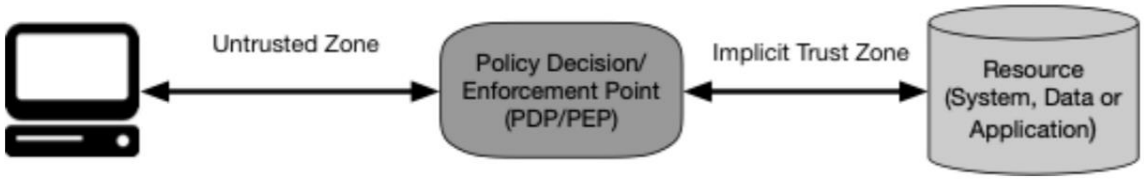
Şekil 2: Doğu-Batı trafiğine karşı savunmasız olan geleneksel güvenlik duvarıyla korunan bir ağ ile Sıfır Güven Mimarisine sahip bir ağ arasındaki fark [3]

Sıfır Güven yaklaşımı, sadece ağın içinde ve dışında tehditlerin bulunduğunu kabul etmekle kalmaz, aynı zamanda bir ihlalin kaçınılmaz olduğunu (veya muhtemelen zaten meydana geldiğini) varsayar. Bu yüzden, sürekli olarak kötü amaçlı etkinliği izler ve kullanıcı erişimini yalnızca işi yapmak için gerekli olanla sınırlar. Bu, kullanıcıların (potansiyel kötü aktörler dahil) ağda yanal olarak hareket etmesini ve sınırlandırılmamış herhangi bir veriye erişmesini engeller.

Amerika Birleşik Devletleri federal devletinin Ulusal Standartlar ve Teknoloji Enstitüsü olan NIST (National Institute of Standards and Technology) Ağustos 2020'de, Sıfır Güven Mimarisinin soyut bir tanımını, dağıtım modellerini ve siber güvenlik yaklaşımı için kullanım senaryolarını özetleyen Özel Yayın 800-207'yi yayınladı. [4] Yayın, Sıfır Güvenin gerçekte ne anlama geldiği konusunda ihtiyaç duyulan netliği sağlıyor.

3. Sıfır Güven Teorik Model

Sıfır Güven'in teorik modelinde, erişim “Güvenilmeyen (Untrusted)” ve “Örtülü Güven (Implicit Trust)” bölgelerine ayrılır.



Şekil 3: Sıfır Güven Erişimi [5]

Güvenilmeyen Bölge, oturumların kimliği doğrulanmayan ve bu nedenle güvenilmeyen olarak kabul edilen alandır. Örtülü Güven Bölgesi, tüm varlıkların güvenildiği alanı temsil eder. Sıfır Güven erişimi, güvenilmeyen bir ortamdaki bir öznenin, kimlik doğrulama ve yetkilendirmeye dayalı olarak kaynaklara erişmesine izin verir, ancak bu karar, politika karar noktası / politika uygulama noktası (PDP/PEP) tarafından yapılır.

PDP/PEP, erişim talebinde bulunanın özgün olduğunu ve isteğin geçerli olduğunu tespit edebilmeli ve sonrasında kaynağa erişmesine izin vermek için gereken kuralları işlemelidir.

Kurallara örnek olarak şunlar verilebilir: [6]

- Bu benzersiz istek için öznenin kimliğine ilişkin güven düzeyi nedir?
- Öznenin kimliğine olan güven düzeyi dikkate alındığında kaynağa erişime izin veriliyor mu?
- İstek için kullanılan cihaz uygun güvenlik duruşuna sahip mi?
- Göz önünde bulundurulması gereken ve güven düzeyini değiştiren başka faktörler var mı? (örn. zaman, öznenin yeri, öznenin güvenlik durumu)

Doğrulama süreci Sıfır Güven yaklaşımının kilit yönlerinden biridir. Bir kaynağa yönelik her erişim talebi, erişime izin verilmeden önce, geçerli erişim ilkelerine ve kimlik bilgileri, cihaz, uygulama ve hizmetin yanı sıra diğer gözlemlenebilir davranış ve çevresel niteliklere dayalı olarak dinamik olarak ve gerçek zamanlı olarak kapsamlı bir şekilde

değerlendirilmelidir. Örneğin, bir personel üyesi veya yüklenici, hatta bir misafir kullanıcı doğrulanabilir ve belirli bir kaynağa erişim izni verilebilir, ancak yine de Sıfır Güven zorlamalı bir ortamda başka bir kaynağa erişmek için yeniden doğrulanmaları gerekir. Bu sürekli inceleme, temelde herhangi bir Sıfır Güven çözümünün özü olan, ağ ortamlarında güvenliği ihlal edilmiş sistemlerden yayılan kötü aktörlerin yanal hareketini önleyen güvenlik kontrol mekanizmasıdır. [7]

Sıfır Güven kavramını uygulamak için genel hedef, Örtülü Güven Bölgesini mümkün olduğunca küçük tutmaktır, bu da pratikte güvenilen varlıkların sayısını en aza indirmek anlamına gelir. Bunu yapabilmenin yolu ise politika kararlarının kaynaklara daha yakın olan konumda verilmesidir.

Bu nedenle, her kurum kaynak erişimi için dinamik risk tabanlı politikalar geliştirmeli ve sürdürmelidir.

4. Sıfır Güven İlkeleri

NIST tarafından hazırlanan Sıfır Güven Mimarisi "Özel Yayın 800-207", kullanıcı erişimini ve veri yönetimini düzenleyen aşağıdaki Sıfır Güven temel ilkelerine bağlı kalarak tasarlanmış ve dağıtılmıştır:

- Tüm veri kaynakları ve bilgi işlem hizmetleri kaynak olarak kabul edilir. Bunlar IOT cihazları, kişisel olarak sahip olunan cihazlar, SaaS uygulamaları vb. olabilir.
- Ağ konumundan bağımsız olarak gerçekleşen tüm iletişim güvenlidir. Ağ konumu tek başına güven anlamına gelmez. Kuruma ait ağ altyapısında bulunan varlıklardan gelen erişim istekleri ile şirket dışı ağdan gelen erişim istekleri aynı güvenlik gereksinimlerini karşılamalıdır. Tüm iletişim gizliliği ve bütünlüğü koruyacak şekilde mümkün olan en yüksek güvenlik düzeyinde yapılmalıdır.
- Kurumsal kaynaklara erişim, oturum bazında verilir. Erişim verilmeden önce istekte bulunana olan güven değerlendirilir. Erişim ayrıca görevi tamamlamak için gereken en az ayrıcalıkla verilmelidir. Başka bir oturum gerekiyorsa güven tekrar değerlendirilir.
- Kaynaklara erişim, istemci kimliğinin, uygulamanın/hizmetin ve istekte bulunan varlığın gözlemlenebilir durumu da dahil olmak üzere dinamik ilke tarafından belirlenir. İlke diğer davranışsal ve çevresel öznitelikleri içerebilir. Sıfır Güven için, istemci kimliğiyle birlikte, yüklenen yazılım sürümleri, ağ konumu, isteğin saati/tarihi, önceden gözlemlenen davranış ve yüklenen kimlik bilgileri gibi öznitelikler kontrol edilir ancak bunlarla sınırlı değildir. Bir kurum, hangi kaynaklara sahip olduğunu, üyelerinin kim olduğunu ve bu üyelerin hangi kaynaklara ihtiyacı olduğunu tanımlayarak kaynakları korur.
- Kurum, sahip olunan ve ilişkili tüm varlıkların bütünlüğünü ve güvenlik duruşunu izler ve ölçer. Hiçbir varlığa güvenilmez. Kurum, bir kaynak isteğini değerlendirirken varlığın güvenlik duruşunu değerlendirir. Sıfır Güven Mimarisini uygulayan bir kurum, cihazların ve uygulamaların durumunu izlemek için sürekli bir tanılama ve azaltma (CDM) veya benzeri bir sistem kurmalı ve gerektiğinde düzeltmeleri uygulamalıdır. İstekte bulunan bir cihazda kurum

tarafından yönetilmeyen bir güvenlik açığı tespit edilirse, kaynaklara erişimi reddetmek gibi farklı şekilde ele alınabilir.

- Tüm kaynak kimlik doğrulaması ve yetkilendirmesi dinamiktir ve erişime izin verilmeden önce zorunlu olarak kesinlikle uygulanır. Sürekli olarak erişim doğrulanmalı, tehditler taranmalı ve değerlendirilmeli, iletişime olan güven uyarlanmalı ve güven sürekli olarak yeniden değerlendirmelidir. Sıfır Güven Mimarisini uygulayan bir kurumun çok faktörlü kimlik doğrulaması (MFA) dahil, kimlik, kimlik doğrulama ve erişim yönetimi (ICAM) ve varlık yönetim sistemlerine sahip olması beklenir.
- Kurum, varlıkların mevcut durumu, ağ altyapısı ve iletişim hakkında mümkün olduğunca fazla bilgi toplar ve bunu güvenlik duruşunu iyileştirmek için kullanır. Bu, politika oluşturma ve yürütmeyi iyileştirmeye yardımcı olacaktır.

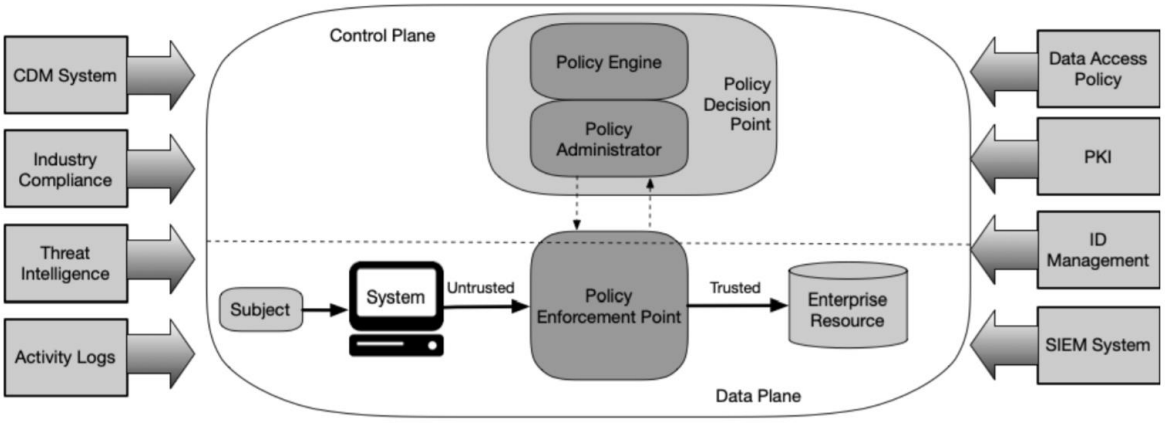
5. Sıfır Güven Mimarisinin Mantıksal Bileşenleri

Bir kurumda Sıfır Güven Mimarisinin dağıtımını oluşturan çok sayıda mantıksal bileşen vardır. Bu bileşenler, şirket içi bir hizmet olarak veya bulut tabanlı bir hizmet aracılığıyla çalıştırılabilir. Şekil 4' teki kavramsal çerçeve modeli, bileşenler ve bunların etkileşimleri arasındaki temel ilişkiyi göstermektedir. Şekil, mantıksal bileşenleri ve bunların etkileşimlerini gösteren ideal bir modeli tasvir eder.

Sıfır Güven Mimarisinin mantıksal bileşenleri, iletişim kurmak için ayrı bir kontrol düzlemi kullanırken, uygulama verileri başka bir veri düzleminde iletilir.

İki ayrı ağ düzlemi: [8]

- Kontrol Düzlemi: Sıfır Güven bileşenleri tarafından ağı kurmak ve yönetmek için kullanılır.
- Veri Düzlemi: İş süreçleri için uygulamalar tarafından kullanılır.



Şekil 4: Sıfır Güven Mantıksal Bileşenleri [9]

İlke motoru (Policy Engine), bir kullanıcının kurumsal ilkelere dayalı kararla her bir kaynağa erişmesine izin verir. İlke motoru, kullanıcının bir kaynağa erişmesine izin verilip verilmediğini ve gereken kimlik doğrulama bilgilerinin yürütülüp oluşturulmayacağını belirlediğinde, ilke yöneticisi (Policy Administrator) ilke motoruna bağlanır.

İlke uygulama noktası (Policy Enforcement Point), kullanıcılar ve kaynaklar arasındaki bağlantıları yönetir. Görevi, ikisi arasındaki sürekli erişimi izlemek ve belirlemektir.

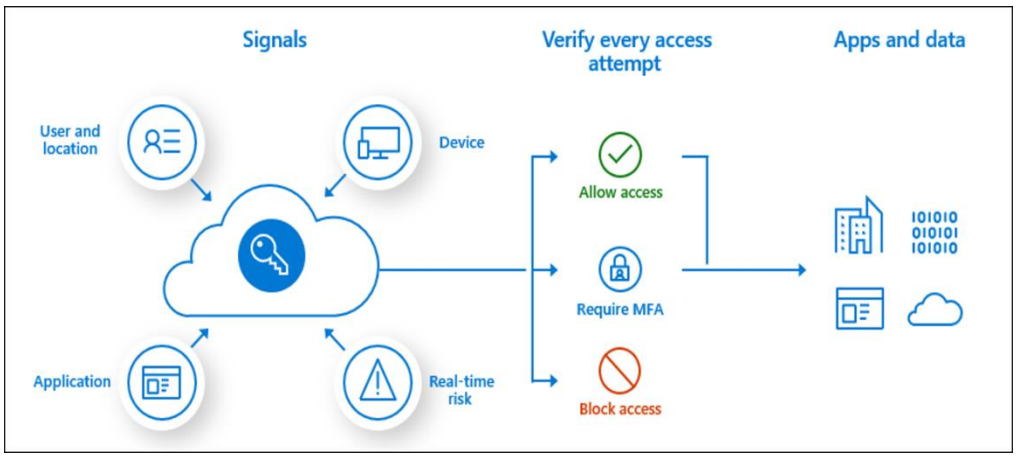
Bu çerçeve aynı zamanda Sürekli tanılama ve azaltma sistemi (CDM System), Sektör uyumluluk sistemi (Industry Compliance), Tehdit istihbaratı (Threat Intelligence), Etkinlik günlükleri (Activity Logs), Veri erişim ilkeleri (Data Access Policy, Kurumsal ortak anahtar altyapısı (PKI), kimlik yönetim sistemi (ID Management), Güvenlik bilgileri ve olay yönetimi sistemi (SIEM System) dahil olmak üzere tamamlayıcı bileşenlerin nasıl entegre edildiğini ortaya koymaktadır.

6. Sıfır Güven Mimarisi Yaklaşımları

Kurumlar, iş akışlarına yönelik Sıfır Güven Mimarisini uygulamak için çeşitli yollar seçebilir. Politikalar ve bileşenler, iş hedeflerine ve kültürüne bağlı olarak kurumdan kuruma değişiklik gösterebilir. Farklılaşmaya rağmen, tüm yaklaşımlar Sıfır Güven'in tüm ilkelerine uyumu sağlar. [10]

- **Gelişmiş Kimlik Yönetimine Sahip Sıfır Güven Mimarisi**

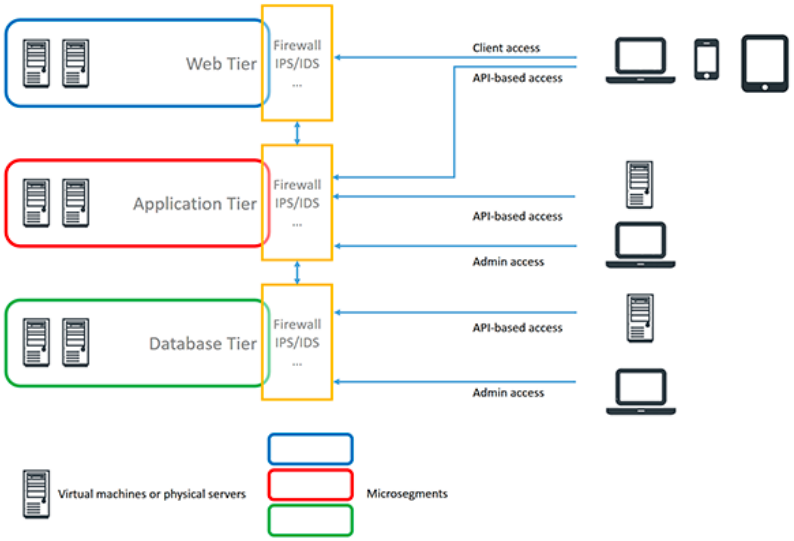
Bu seçenek, aktörün kimliğini politika yapımında önemli bir faktör haline getirir. Her kurumsal kaynak için erişim koşullarını, kaynağa erişen kullanıcı veya sistemin kimliğine ve atanan özniteliklerine göre tanımlarsınız. Ana gereksinim, her kullanıcıya veya sisteme, gereksiz sistemlere erişim vermeden kaynaklara uygun erişim sağlamaktır.



Şekil 5: Gelişmiş Kimlik Yönetimi [11]

- **Mikro Segmentasyonlu Sıfır Güven Mimarisi**

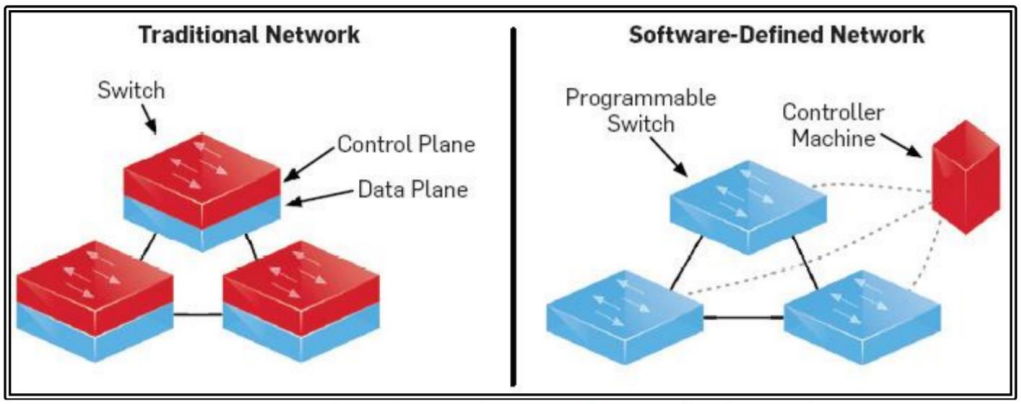
Bu seçenek, bireyleri veya kaynak gruplarını, segmentler arasında güvenli ağ geçitleriyle farklı ağ segmentlerine yerleştirerek Sıfır Güven uygular. Kuruluşlar, kaynak gruplarını koruyan bir ilke uygulama noktası (PEP) olarak hareket etmek için yönlendiriciler, anahtarlar, yeni nesil güvenlik duvarları (NGFW) veya yazılım aracıları gibi ağ ekipmanlarını kullanabilir.



Şekil 6: Mikro Segmentasyon [12]

- **Yazılım Tanımlı Ağ Çevreleriyle Sıfır Güven Mimarisi**

Bu seçenek, ağın kontrolünü merkezileştirerek ağın esnekliğini ve verimliliğini artırır. OSI modelinin 7. katmanında (uygulama katmanı) bir yer paylaşımlı ağdan yararlanır, ancak ağ yığınında daha aşağıda da olabilir. Bu yöntem Yazılım Tanımlı Çevre (SDP) olarak bilinir, çünkü genellikle ağların esnek, sanallaştırılmış cihazlar kullanılarak yönetildiği Yazılım Tanımlı Ağ (SDN) teknolojisinden yararlanır.



Şekil 7: Yazılım Tanımlı Ağ [13]

7. Sıfır Güven Mimarisi ile İlişkili Tehditler

Hiçbir kuruluş siber güvenlik riskini ortadan kaldıramaz. Mevcut siber güvenlik politikaları, kimlik ve erişim yönetimi, sürekli izleme ve genel siber hijyen ile tamamlandığında, uygun şekilde uygulanan ve bakımı yapılan bir Sıfır Güven Mimarisi, genel riski azaltabilir ve yaygın tehditlere karşı koruma sağlayabilir. Ancak bazı tehditler Sıfır Güven Mimarisi ile de ilişkilidir.

- Sıfır Güven Mimarisinin karar sürecinin bozulması: İlke Motoru (PE) ve İlke Yöneticisi' ndeki (PA) yanlış yapılandırmalar ve onaylanmamış değişiklikler kurumsal operasyonları kesintiye uğratabilir. Nasıl azaltılır? Tüm yapılandırma değişiklikleri günlüğe kaydedilmeli ve denetime tabi olmalıdır.
- Hizmet Reddi veya Ağ Bozulması: İlke Motoru ve İlke Yöneticisi (PA/PE), kaynaklara erişim için anahtar bileşen olduğundan, bir saldırgan PE/PA erişimini durdurabilir. İlke altyapısına veya ilke yöneticisi bileşenine ağdan erişilemezse tüm kuruluşun çalışması engellenebilir. Nasıl azaltılır? İlke zorlaması, uygun şekilde güvenli bir bulut ortamında veya birden çok konumda bulunabilir.
- Çalınan Kimlik Bilgileri/İçeriden Tehdit: Saldırganların birincil hedefi, değerli hesapların kimlik bilgilerini ele geçirmek olacaktır. Kimlik bilgilerini elde etmek için sosyal mühendislik veya çoklu saldırılar kullanabilirler. "Değerli hesap" saldırganın motivasyonuna göre farklı anlamlara gelebilir. Örneğin, kurumsal yönetici hesapları değerli olabilir, ancak finansal kazançla ilgilenen saldırganlar, eşit değerdeki finansal veya ödeme kaynaklarına erişimi olan hesapları göz önünde bulundurabilir. Nasıl azaltılır? Erişim istekleri için MFA'nın uygulanması, güvenliği ihlal edilmiş bir hesaptan bilgi kaybı riskini azaltabilir.
- Ağda Görünürlük: Tüm paketler denetlenip günlüğe kaydedilse bile, trafiğin bir kısmı, şifreli trafik dahil olmak üzere katman 3 ağ analiz araçlarına karşı yetersiz kalacaktır. Nasıl azaltılır? Şifreli trafiği analiz etmek için makine öğrenimi teknikleri kullanılabilir.
- Sistem ve Ağ Bilgilerinin Depolanması: Adli veriler, izleme verileri, ağ diyagramları, yapılandırma dosyaları daha sonra analiz edilmek üzere saklanırsa,

saldırganlar bu verileri hedef alabilir. Nasıl azaltılır? Yetkisiz erişimi ve girişimi önlemek için gereken önlemler alınmalıdır.

- Tescilli Veri Formatlarına veya Çözümlerine Güven: Sıfır Güven Mimarisi, erişim kararları almak için birkaç farklı veri kaynağına güvenir. Farklı standartların kullanılması tek bir sağlayıcıya güvenmeye yol açacaktır ve bu sağlayıcıda bir kesinti olursa, farklı bir sağlayıcıya geçiş daha yüksek maliyetli olacaktır. Nasıl azaltılır? 3. taraf satıcı risk değerlendirmesi, tedarik zinciri risk yönetimi.
- Sıfır Güven Mimarisi Yönetiminde Kişi Olmayan Varlıkların (NPE) Kullanımı: Herhangi bir insan müdahalesi olmadan düzenli olarak Sıfır Güven Mimarisi ile etkileşime giren otomatik yazılım ve yapay zekâ motorları tarafından kimlik doğrulama için API kullanımı. Yalnızca API anahtarlarını kullanırlar; Saldırgan aracıyla etkileşime girebilirse, aracı adına kötü amaçlı kod kullanabilir.

8. Sonuç

Bu çalışmada Sıfır Güven yaklaşımı incelenmiştir. Ortaya koyduğu zorluklara rağmen, Sıfır Güven yaklaşımı, veri hırsızlığına ve içeriden gelen tehditlere direnmek için ideal bir model olarak gözükmektedir.

Sıfır Güven güvenlik modelini uygulamak karmaşık ve uzun bir süreçtir. Ancak kurumların Sıfır Güven ilkelerinin tümünü aynı anda uygulamasına gerek yoktur. Kurumun tüm kaynaklarını tanımlama ve sınıflandırma, uygun bir kullanıcı doğrulama süreci uygulama ve yalnızca ayrıcalıklı kullanıcılara erişim verme gibi küçük adımlarla bu güven modelini uygulamaya başlayabilirler. Başlangıç noktası ne olursa olsun, Sıfır Güven güvenlik modeli, risk azaltma ve güvenlik kontrolü yoluyla kazanımlar sağlar.

Sıfır Güven yaklaşımı kurumların bugün karşılaştığı bazı önemli siber güvenlik sorunlarından korunmaya yardımcı olur, ancak Sıfır Güven Mimarisi ile ilgili tehditler göz ardı edilmemelidir. En iyi yaklaşım, modeli yeterince uygulayarak ve diğer siber güvenlik uygulamalarıyla entegre ederek güvenliği arttırmaktır.

9. Kısaltmalar

CDM: Continuous Diagnostics and Mitigations – Sürekli Tanılama ve Azaltma

ICAM: Identity, Credential and Access Management – Kimlik, Kimlik Doğrulama ve Erişim Yönetimi

MFA: Multi Factor Authentication – Çok Faktörlü Kimlik Doğrulama

NIST: National Institute of Standards and Technology – Ulusal Standartlar ve Teknoloji Enstitüsü

NPE: Non Person Entity – Kişi Olmayan Varlık

PA: Policy Administrator – İlke Yöneticisi

PE: Policy Engine – İlke Motoru

PEP: Policy Enforcement Point – İlke Uygulama Noktası

PDP: Policy Decision Point – İlke Kararı Noktası

PKI: Public Key Infrastructure – Ortak Anahtar Altyapısı

SDN: Software Defined Network – Yazılım Tanımlı Ağ

SDP: Software Defined Perimeter – Yazılım Tanımlı Çevre

10. Kaynakça

1. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf
2. https://www.kwtrain.com/blog/network-security-zones
3. https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify
4. https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207
5. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
6. https://www.linkedin.com/pulse/zero-trust-architecture-what-nist-sp-800-207-all-nidhin-jose/
7. https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207
8. https://csrc.nist.gov/CSRC/media/Presentations/zero-trust-architecture-101/images-media/Zero%20Trust%20Architecture%20101%20-%20Scott.pdf
9. https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207
10. https://www.hysolate.com/learn/zero-trust/zero-trust-architecture-3-approaches-and-4-best-practices/
11. https://devblogs.microsoft.com/azuregov/implementing-zero-trust-with-microsoft-azure-identity-and-access-management-1-of-6/
12. https://www.kuppingercole.com/blog/kuppinger/beyond-datacenter-micro-segmentation
13. https://digitalrepository.unm.edu/cgi/viewcontent.cgi?article=1013&context=ece_etds&httpsredir=1