KURUMSAL BULUT SİSTEMLERİ GÜVENLİĞİ İÇİN EN İYİ UYGULAMALAR

4 kısıma ayırabiliriz ; Buluta hazırlığı , ağ hazırlığı , sunucu hazırlığı , diğer hazırlıklar olmak üzere ayırabiliriz.

Bulut hazırlığı ; Bulut hizmeti sağlayıcısıyla devam etmeye karar verdiğinizde ve altyapınızı başlatmayı planladığınızda ilgilenmeniz gerekenler şöyledir ;

1-) MFA kurulmalı ve ROOT hesabı kullanılmamalıdır ; KÖK hesabının ortamımız üzerinde tam " full " izni olduğundan ve KÖK hesabının izinlerini sınırlayamadığımız için KÖK hesabının kullanılmasından kaçınarak IAM hesabına geçiniz.

2-) Bulut sertleştirme yönergelerini uygulayınız ; AWS , internet güvenliği için merkez tarafından geliştirilmiş harika sıkılaştırma yönergelerine sahiptir. Azure ve Google Cloud gibi diğer bulut ortamları için yığınlarına bağlı olarak takip edilebilecek en iyi güvenlik uygulamaları vardır. Her halükarda otomasyonu tercih ediniz. Terraform bunun için çok iyi bir seçim olacaktır.

3-) Çevrenizin değiştiğinin farkında olunuz ; Sunucu sayısı arttıkça , ortamın belirli bir süre içinde nasıl değiştiği konusunda çok az farkındalık sahibi olunabilir. AWS Config , AWS ortamı için harika bir araçtır. Splunk ile entegre edin ve kurulumunuz AWS için hazırdır.

4-) Bilinen uygulamalara yoğunlaşın ; İşler iyi şekilde test edildiğinde , aynı şeyleri tekrar geliştirmekten kaçınınız. AWS gibi bulut ortamlarında barındırılan birçok hizmet bulunur. AWS'de KMS , Config ve S3 bulunur. Birçok sistem yöneticisi RabbitMQ'yu mesaj aracıları olarak uygulamaktadır fakat bu sunucularda güvenlik özelliklerini ve yapılandırmayı devralmayı unutulmaktadır. Bu nedenle , SQS'yi doğrudan bulut sağlayıcısının güvenlik bölümünü yönettiği yerde kullanmak daha iyidir.

5-) Altyapıyı kod çözümü olarak kullanmaya çalışınız ; IAC çözümü aracılığıyla altyapı geliştirmeye ve dağıtmaya başladığınızda bize birçok fayda sağlayacaktır. Avantajlardan biri de onu çekme istekleriyle bütünleştirme yeteneğini içerir. Bir kişi IAC çözümü aracılığıyla altyapının bir yönünü değiştirmek istediğinde , kod birleştirilip dağıtılmadan önce çekme talebi göndermesi gerektiği anlamına gelir.

6-) CSP'nin paylaşılan güvenlik sorumluluğu modelini anlamak ; Bulut ortamında belirli yönler CSP tarafından yönetilerek belirli yönler kullanıcının sorumluluğundadır. Bu nedenle , paylaşılan sorumluluk modelini anlamak çok önemlidir. Hangi CSP'yi kullanırsanız kullanın , CSP'nin ne olduğunu ve tüketicinin sorumluluğunun ne olduğunu anlamanız gereklidir.

Ağ hazırlığı ; Ağla ilgili tasarım ve uygulama parametreleri hakkında genel bakış sağlayacak olursak ;

1-) Optimum güvenlik duvarı kuralları bizler için zorunluluktur ; Bu çok önemlidir. Güvenlik duvarını yapılandırırken her zaman hem INBOUND hem de OUTBOUND güvenlik duvarı kurallarını uygulayınız. Bu , ihlal durumunda size çok şey kazandırabilir.

2-) Güvenlik duvarı gerekçe belgesi bulundurunuz ; Birkaç ay sonra güvenlik duvarı kurallarına bakıldığında , bu kuralın neden ilk başta uygulandığını hatırlamayabilirler. Güvenlik duvarı doğrulama belgesi olmadan , her kuralın açıklamasına bakmak zordur ve yeni güvenlik mühendisi katılırsa , belirli bir kuralın neden mevcut olduğu hakkında hiçbir fikri olmayacaktır.

3-) Bastion / VPN'iniz olsun ; Her zaman mimarinizin bir Bastion veya VPN çözümü olduğundan emin olunuz. Hiçbir ortam gerekmedikçe internete açık olmamalıdır. OpenVPN , uygulanması basit ve etkili çözüm olan harika bir araçtır. Bastion işlevi , SSH Anahtar iletme yaklaşımıyla da uygulanabilir.

4-) IPS'in önemi ; IPS'yi doğrudan bulutta uygulamak zorlu bir iştir ve bu nedenle her host bilgisayarda aracı tabanlı yaklaşımı izlememiz gerekir. Deep Security , uygulamak isteyebileceğiniz IPS için güzel ücretli çözümdür.

5-) DDoS'a hazırlıklı olunuz ; Ortamınızı DDoS saldırılarına karşı koruyabilecek yerinde çözümler olmalıdır. Birçok kuruluş , özel performans sunan AWS Shield gibi çeşitli hizmetlerin yanı sıra DDoS koruması sunan CDN'yi uygular. Ana bilgisayar düzeyinde , yatay ölçeklendirme , TCP SYN tanımlama bilgileri ve IP başına istek hızı sınırlaması , bu tür saldırılar sırasında yardımcı olabilecek yaklaşımlardan bazılarıdır.

6-) Web uygulaması güvenlik duvarına sahip olmak ; Geleneksel güvenlik duvarı ve IPS , web uygulaması düzeyindeki saldırılara karşı yardımcı olmazlar. Bu nedenle de günümüzde organizasyonlarda WAF'ı uygulamak bir zorunluluktur. AWS WAF , Naxsi ve ModSecurity kullanılabilecek araçlardan bazılarıdır. Çeşitli CDN sağlayıcıları , kullanabileceğiniz kendi WAF çözümlerini sunar.

7-) SSL / TLS sertifikalarının savunmasız olmadığını doğrulayınız ; Zayıf hash algoritmaya veya diğer bazı algoritmalara sahip sertifikalar , gizlilik , bütünlük için genel riskler sağlar. Dağıtılan SSL / TLS sertifikanızın puanını doğrulamak ve neyin eksik olduğunu bulmak için Qualys SSL laboratuvarları gibi çevrimiçi araçları kullanınız.

Sunucu hazırlığı ; Ortamınızda konuşlandırılacak olan sunucularda uygulanması gereken güvenlik mekanizmalarını ele alacak olursak ;

1-) SSH parola doğrulaması sadece anahtar tabanlı doğrulamadır ; Asla SSH parola tabanlı kimlik doğrulamayı kullanmayınız. Her zaman anahtar tabanlı kimlik doğrulamayı kullanınız.

2-) Denetimin Önemi ; Sunucuda neler olduğu ve değişiklikleri kimin yaptığı konusunda keskin bir farkındalığa sahip olunmalıdır. AuditD , bize ayrıntılı görünürlük sağlayabilen harika arka plan programıdır. Sunucu ortamınızda AuditD'yi uyguladığınızdan ve yapılandırdığınızdan emin olun.

3-) Dosya bütünlüğü izleme ; Sunucunun ayrılmaz bir parçası olarak FIM , sunucu güvenliğinin çok önemli bir parçasıdır. Sunucu herhangi bir ortamda (dev , hazırlama ve prod) dağıtıma başlamadan önce tüm dosyalar ve binary dosyalar için temel hash oluşturulmalıdır. OSSEC , FIM'i oldukça iyi yapan harika bir araçtır.

4-) Zafiyet değerlendirmesi ; Her hafta keşfedilen ve açıklardan yararlanılan bir tür güvenlik açığı bulunmaktadır. Bu nedenle de güvenlik açıklarının sürekli değerlendirilmesi çok önemlidir. Nessus , oldukça iyi çalışan harika bir güvenlik açığı değerlendirme aracıdır. OpenSCAP'i açık kaynak alternatifi olarak kullanabilirsiniz.

5-) Yama yönetimi ; Sadece güvenlik açıklarını değerlendirmek yeterli değildir. Güvenlik açıklarını istismar edilmemeleri için düzeltmemiz gerekmektedir. SpaceWalk , merkezi yama yönetimi için harika bir araçtır.

6-) Merkezi Kimlik Doğrulama ; Merkezi kimlik doğrulamayı uygulamak , çok fazla kullanıcı ve sunucu olduğunda harika bir yöntemdir fakat bunun uygulanması ve bakımı için uzun bir zamana ihtiyacı vardır. Bunun operasyonel faydalara bağlı olarak düşünebilirsin. FreeIPA bu yaklaşım için harika bir araçtır. Destek verilen daha istikrarlı bir ürüne sahip olmak istiyorsanız tercih ettiğiniz araç Red Hat IDM ürünü olabilir.

7-) Merkezi log izleme çözümünü ; Birçok kuruluşun yüzlerce sunucusu vardır ve bu gibi durumlarda her sunucuya giriş yapmak ve güvenlik günlüklerine bakmak ideal bir çözüm değildir. Tüm sunuculardan gelen güvenlikle ilgili tüm günlükler , analiz edilebilecekleri merkezi günlük izleme sunucusunda alınmalıdır. ELK yığını veya Splunk gibi SIEM çözümü veya OSSIM gibi açık kaynaklı çözümler olabilir.

8-) Dockerizasyon ; Docker kullandığımızda , güvenlik yapılandırmaları ve güncellemeleri nedeniyle uygulamanın çökmesi konusunda endişelenmemize gerek olmadığı için genel yama yönetimi ve güvenlik yığını daha az karmaşık olacaktır. Böylece uygulamalar geliştirilip docker kapsayıcılarında çalışıyorsa hayatı çok daha kolay hale getirir.

9-) Sunucu sertleşmesi ; Sunucu sertleştirme anahtardır. Tüm sunucular , ortamınıza göre standart sertleştirme kurallarına sahip olmalıdır. CIS kıyaslamaları , kuralların katılaştırılması için harika bir başlangıç noktasıdır.

10-) İstenilen duruma ulaşmak ; İstenen durum yaklaşımı , çok az kuruluşun uyguladığı bir şeydir. Güvenlik ekibi , tüm yapılandırma dosyaları için istenen bir duruma sahip olmalıdır ve biri bunları değiştirse bile otomatik olarak istenen duruma geri dönecektir. Ansible pull bunu başarmak için harika bir yaklaşımdır.

11-) Daima net görüntü oluşturun ; Güvenlik ekibi , sertleştirme , FIM veya diğerleri gibi tüm güvenlik yığınlarını içeren net görüntü oluşturmalıdır. DevOps ekibi , sunucuları sadece güvenlik ekibi tarafından sağlanan altın görüntüden başlatmalıdır.

Diğer Hazırlıklar ; Diğer önemli hususlar şöyledir ;

1-) Single Sign On ; Kuruluşunuzun birden fazla dahili uygulaması varsa ve bu uygulama aralığı sekizden fazlaysa , SSO olasılığını göz önünde bulundurmalısınız. ADFS ile tasarlayabilir veya kurulumu oldukça kolay olan , AWS ve Gmail gibi diğer sağlayıcılarla birçok entegrasyona sahip olan Okta veya JumpCloud gibi SaaS çözümlerini kullanabiliriz.

2-) MFA'ya sahip olma ; Çok faktörlü kimlik doğrulama , özellikle VPN ve AWS gibi giriş noktalarında bir zorunluluktur. Saldırganın çalınan kimlik bilgileriyle oturum açabileceği herhangi bir yer MFA tarafından desteklenmelidir.

3-) İş istasyonları için tam disk şifreleme şarttır ; Birçok geliştirici ve sistem yöneticisi , erişim / gizli anahtarların , özel anahtarların , kurumsal bulut için açık oturumların vb. kopyalarına sahiptir. Böyle bir durumda dizüstü bilgisayar çalınırsa , saldırgan tüm verileri kopyalayıp kullanabilir. LUKS gibi araçlarla tam disk şifrelemeye sahip olmak verilerin tehlikeye atılmamasını sağlar.

4-) Güvenlik yangın tatbikatları önemlidir ; Tüm kontrollerin çalıştığından emin olmanın tek yolu ; deneme tatbikatı yapmaktır. Bir ekip üyesinin herhangi bir rastgele sunucuda oturum açmasına ve ideal olarak alarm verecek bir şey yapmasına izin veriniz. Bunun nasıl işe yarayacağını kontrol ediniz. Çoğu zaman , sahte tatbikatlardan sonra , güvenlik aracısının kendisinin çalışmadığı veya e-posta işlevinin çalışmadığı görülür.

5-) En az ayrıcalık ilkesi ; Bir kullanıcının bulut konsolundan belirli bir sunucuya erişimi durdurması gerekiyorsa , sadece ona erişimi durdurma izni veriniz. Sunucuya tam erişim verilmesine gerek yoktur. Genelde eğilimdir çünkü koşullu rol yazmak biraz daha fazla zaman alır ve birçok çözüm mimarı bundan kaçınır.

6-) Konfigürasyon yönetim aracıyla otomatikleştirme ; Manuel olarak yapmak hataya açık ve zaman alıcıdır. Bir kez yazmak ve birden çok kez uygulamak iyi bir yaklaşımdır. Sunucu sağlamlaştırma , OSSEC'yi yapılandırma ve diğerleri gibi tüm kurallar , Ansible gibi yapılandırma yönetimi araçlarıyla otomatikleştirilmelidir.

7-) DNS özel bölgeleri yapınız ; AWS'ye çok özel bir durumdur. Birçok kuruluş , tüm kayıtları genel olarak barındırılan Route 53 bölgesinde oluşturur. Bu ideal bir yaklaşım değildir. openvpn.xxx.com gibi kayıtlara sahip olmak , saldırganın kuruluşunuzun OpenVPN kullandığını bilmesini sağlar.

8-) Log arşivi tutma ; Tüm günlükler merkezi depolama yerinde arşivlenmelidir. Glacier'a daha da taşınabilen S3 olabilir. Kuruluşunuzun güvenliği ihlal edilirse , bu günlükler tek kanıt olacaktır. Bu nedenle onu güvende tutmak daha iyi olacaktır. İdeal olarak , bir yıllık günlükler saklanmalıdır. Bu günlükler , sunucu günlüklerinden , ağ günlüklerinden CSP ile ilgili günlüklerinizin yanı sıra temel olarak geçmiş bir olayı yeniden yapılandırmanıza yardımcı olacak tüm günlüklere kadar değişebilir.

9-) Birinden sizi denetlemesini isteyin ; Tüm güvenlik uygulamalarına uysalar bile kimse güvende değildir. Ortamınızı denetlemesi için bir güvenlik denetçisi edinin, böylece uyguladığınız şeylerin ideal ve hedefe uygun olduğundan emin olabilirsiniz. İdeal olarak, bu asla olmaz. İyi bir güvenlik denetçisi her zaman boşluklarınızı paylaşacaktır. Sonuçta, bunun için para alıyorlar.