Derinlemesine Güvenlik Stratejisi

Siber Güvenlik Vulnerability

El Kitabı

İçindekiler

I. Giriş

Hoş Geldiniz

CRR Kaynak Kılavuzu serisine hoş geldiniz. Bu belge, İç Güvenlik Bakanlığı'nın (DHS) Siber Güvenlik Değerlendirme Programı (CSEP) tarafından kurumların bir Siber Esneklik İncelemesi (CRR) sırasında iyileştirmeye yönelik hususlar olarak tanımlanan uygulamaları uygulamalarına yardımcı olmak için geliştirilen 10 kaynak kılavuzdan biridir. [1] CRR, bir organizasyonun BT operasyonlarına özgü *operasyonel esnekliğinin anlaşılmasını ve nitel ölçümünü yakalayan, görüşmeye dayalı bir değerlendirmedir.* Operasyonel esneklik, kuruluşun temel operasyonel kapasitelerini etkileyen risklere uyum sağlama yeteneğidir. [2] Ayrıca, kuruluşun normal operasyonlar sırasında ve operasyonel stres ve kriz zamanlarında kritik hizmetlere ve ilgili varlıklara yönelik operasyonel riskleri yönetme yeteneğini de vurgular. Kılavuzlar, bir CRR'ye katılan kuruluşlar için geliştirilmiştir, ancak kritik BT hizmetleri için operasyonel esneklik yeteneklerini uygulamak veya olgunlaştırmak isteyen tüm kuruluşlar bu kılavuzları yararlı bulacaktır.

CRR Kaynak Kılavuzu serisinin kapsadığı 10 alan şunlardır:

1. Varlık Yönetimi
2. Kontrol Yönetimi
3. Yapılandırma ve Değişiklik Yönetimi
4. **Güvenlik Açığı Yönetimi** ⇦ ***Bu kılavuz***
5. Olay Yönetimi
6. Hizmet Sürekliliği Yönetimi
7. Risk yönetimi
8. Dış Bağımlılıklar Yönetimi
9. Eğitim ve Farkındalık
10. Durumsal farkındalık

CRR'nin amacı, kuruluşların temel siber güvenlik uygulamalarının performansını ölçmesine izin vermektir. DHS, 2011'de CRR'yi tanıttı. 2014'te DHS, kritik altyapı siber güvenliğinin geliştirilmesine yardımcı olmak ve Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) Siber Güvenlik Çerçevesi (CSF). NIST CSF, kuruluşlar için ortak bir sınıflandırma ve mekanizma sağlar.

1. mevcut siber güvenlik duruşlarını tanımlayın
2. siber güvenlik için hedef durumlarını tanımlayın
3. Sürekli ve tekrarlanabilir bir süreç bağlamında iyileştirme fırsatlarını belirlemek ve önceliklendirmek
4. hedef duruma doğru ilerlemeyi değerlendirmek
5. siber güvenlik riski hakkında iç ve dış paydaşlar arasında iletişim kurmak

CRR Öz-Değerlendirme Paketi, CRR'de ölçülen uygulamaların NIST CSF kriterleriyle korelasyonunu içerir. Bir kuruluş, NIST CSF ile uyumluluğunu yaklaşık olarak tahmin etmek için CRR'nin çıktısını kullanabilir. CRR ve NIST CSF'nin farklı uygulama kataloglarına dayandığını belirtmek önemlidir. Sonuç olarak, bir kuruluşun CRR uygulamaları ve yeteneklerini yerine getirmesi, NIST CSF'deki karşılık gelen uygulama ve yeteneklerin altında kalabilir veya bunları aşabilir.

Bu serideki her kaynak kılavuzu aynı temel yapıya sahiptir, ancak her biri bağımsız olarak kullanılabilir. Her kılavuz, operasyonel esneklik yeteneklerinin uygulanmasını ve yürütülmesini destekleyen planların ve yapıların geliştirilmesine odaklanır. Birden fazla kaynak kılavuzu kullanan kuruluşlar, benimseme yaklaşımlarını optimize etmek için tamamlayıcı materyallerden ve önerilerden yararlanabilecektir. Örneğin, bu kılavuz, odaklanmış ve

tanımlanmış bir güvenlik açığı yönetimi sürecini gerçekleştirme sürecini açıklar. Bu sürecin gelişimi, bir kontrol yönetimi sürecinde öğrenilen ve geliştirilen bilgilerle bilgilendirilebilir. Güvenlik açığı sürecinin çıktıları, bir risk yönetimi sürecinin temel bileşenleridir.

Her kılavuz, bilgilerini çeşitli kaynaklarda açıklanan en iyi uygulamalardan, ancak öncelikle CERT ® [1]Esneklik Yönetim Modelinden (CERT ® -RMM) alır. [3] CERT-RMM, Carnegie Mellon'un CERT Bölümü tarafından geliştirilen, operasyonel esnekliği yönetmeye ve geliştirmeye yönelik bir olgunluk modelidir.
Üniversitenin Yazılım Mühendisliği Enstitüsü (SEI). Bu modelin amacı

- operasyonel esneklik faaliyetlerinin uygulanmasına ve yönetimine rehberlik eder
- kilit operasyonel risk yönetimi faaliyetlerini birleştirin
- yetenek seviyeleri aracılığıyla olgunluğu tanımlayın
- modele karşı olgunluk ölçümünü etkinleştir
- Bir kuruluşun operasyonel strese ve krize verdiği yanıtta güvenini artırmak

CERT-RMM, CRR'nin türetildiği çerçeveyi sağlar - başka bir deyişle, CRR yöntemi amaçlarını ve uygulamalarını CERT-RMM süreç alanlarına dayandırır.

Bu kılavuz bir güvenlik açığı yönetimi süreci oluşturma konusunda yardım arayan kuruluşlara yöneliktir. Açıklanan süreç alanları şunları içerir:

- bir güvenlik açığı analizi ve çözüm stratejisi geliştirmek
- bir güvenlik açığı yönetim planı geliştirmek
- bir güvenlik açığı bulma yeteneği geliştirme
- güvenlik açığı yönetimi faaliyetlerinin değerlendirilmesi
- maruz kalma yönetimi

Daha spesifik olarak bu kılavuz

- Okuyucuları güvenlik açığı yönetimi süreci hakkında eğitir ve bilgilendirir
- Bir güvenlik açığı yönetimi sürecine duyulan ihtiyaç konusunda ortak bir anlayışı teşvik eder
- Güvenlik açığı analizi ve çözümü ve güvenlik açığı yönetimi için temel uygulamaları tanımlar ve açıklar
- bu uygulamaları uygulamak isteyen kuruluşlara örnekler ve rehberlik sağlar Kılavuz aşağıdaki gibi yapılandırılmıştır:

I. Giriş— *CRR Kaynak Kılavuzu* serisini tanıtır ve bu belgelerin içeriğini ve yapısını açıklar.

II. Güvenlik Açığı Yönetimi—Açıklık yönetimi sürecine genel bir bakış sunar ve bazı temel terminolojiler oluşturur.

III. Bir Güvenlik Açığı Analizi ve Çözüm Stratejisi Tanımlayın—Uygun bir stratejinin içeriğini belirlemek için bir yaklaşım sağlar.

IV. Güvenlik Açığı Yönetimi için Bir Plan Geliştirin—Plan oluşturma sürecinin ana hatlarını verir ve planın kuruluşun ihtiyaçlarını karşılamasını sağlamaya yardımcı olmak için sorunları ve değerlendirmeleri tanımlar.

V. Güvenlik Açığı Analizi ve Çözüm Yeteneğinin Uygulanması—Planınızı, ekibinizi ve araçlarınızı kuruluşunuzu desteklemek üzere faaliyete geçirmeye yönelik bir yaklaşımı özetler.

VI. Yeteneği Değerlendirin ve Geliştirin—Kuruluşunuzun, kuruluşunuzla en ilgili olan bu güvenlik açıklarını keşfetme ve çözme ve planınızı buna göre ayarlama yeteneğini geliştirme sürecini özetler.

[1]CERT ® , Carnegie Mellon Üniversitesi'ne ait tescilli bir markadır.

VII. Sonuç—Daha fazla bilgi için ilgili kişileri ve referansları sağlar.

Ekler

A. Güvenlik Açığı Yönetimi Kaynakları

B. CRR/CERT-RMM Uygulaması/NIST CSF Alt Kategori Referansı

Kitle

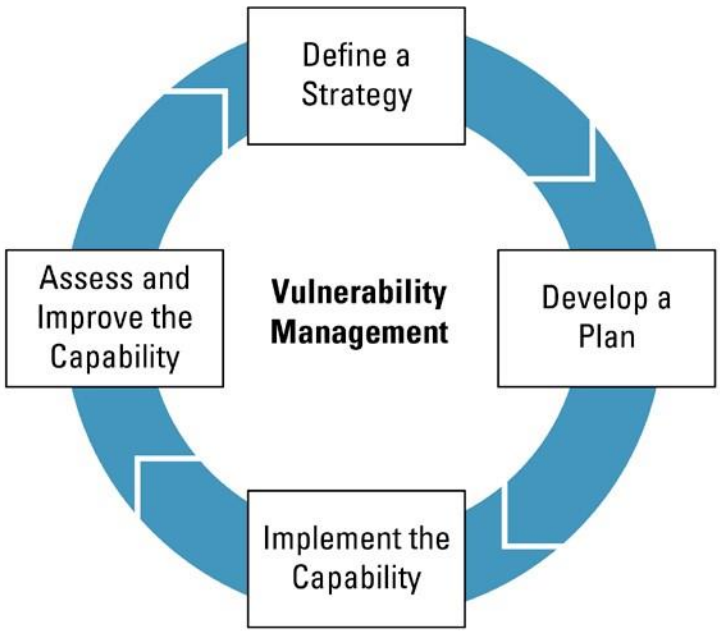
Bu kılavuzun ana hedef kitlesi, bir kuruluşun siber dayanıklılığını etkileyen hem siber hem de fiziksel güvenlik açıklarının yönetiminden, analizinden ve düzenlenmesinden sorumlu kişilerdir. Bu, güvenlik açığı yönetimi için politikalar ve öncelikler oluşturmaktan sorumlu yöneticiler, yürütme kararlarını planlara dönüştürmekten sorumlu yöneticiler ve planlayıcılar ve planı uygulayan ve güvenlik açığı düzenlemesine katılan operasyon personelini içerir.

Bu kılavuzun kaynak belgeleri ve diğer ilgi çekici belgeler hakkında daha fazla bilgi edinmek için Ek A'ya bakın.

II. Güvenlik Açığı Yönetimi

genel bakış

Güvenlik Açığı Yönetimi alanı, kuruluşların kritik bir hizmetin işletim ortamındaki güvenlik açıklarını belirleme, analiz etme ve yönetme sürecine odaklanır. CRR kaynak kılavuzlarının tümü, bir alanı bir süreç ve aşamaları açısından tanımlamak için CERT-RMM'den türetilen ortak bir yaklaşımı benimser. Bu kılavuz, Şekil 1'de gösterildiği gibi güvenlik açığı yönetimi sürecini dört aşamaya böler:



Şekil 1: Güvenlik Açığı Yönetim Süreci Bu kılavuz,

güvenlik açıklarının kapsamlı bir tanımını kullanacaktır.

güvenlik açığı: *"[P]bir varlığı, varlığı, sistemi, ağı veya coğrafi alanı istismara açık veya belirli bir tehlikeye açık hale getiren fiziksel özellik veya operasyonel özellik." DHS Risk Sözlüğü, 2010 Sürümü* [4]

Güvenlik açıklarını tartışırken, bir tehdit (doğal veya insan yapımı) tarafından kullanılması durumunda bir varlığı (yani, tüm bir kuruluş veya onu oluşturan parçalardan herhangi biri) bir riske açık hale getiren özellik veya koşulu tartışıyoruz. CRR, kuruluşun belirli bir kritik hizmetine odaklanır. Hizmetin her yönü, hizmeti destekleyen çeşitli varlıklar açısından tartışılır. Hizmetteki bir güvenlik açığı, bir veya daha fazla varlığındaki bir güvenlik açığının sonucudur. Varlıklar insan, bilgi, teknoloji ve tesis kategorilerine ayrılır.

Güvenlik açığı yönetimi, kontrollerin uygun şekilde uygulanmasının ve risk yönetiminin planlanması ve belirlenmesinde kilit bir bileşendir. Güvenlik açığı yönetiminin siber dayanıklılık için merkezi olduğunu söylemek mantıklıdır. Diğer CRR etki alanlarının konuları, savunmasız koşullar hakkında bilgi sağlar (Varlık Yönetim, Konfigürasyon ve Değişiklik Yönetimi, Dış Bağımlılıklar Yönetimi ve Durumsal Farkındalık) veya hassas koşullara (Kontrol Yönetimi, Olay Yönetimi, Hizmet Sürekliliği Yönetimi, Risk Yönetimi ve Eğitim ve Farkındalık) yanıt verilmesini sağlar. Güvenlik açığı yönetimi, buna göre plan yapabilmesi için kuruluşun zayıflıklarını anlamasını sağlar.

Bir güvenlik açığının bir tehdit tarafından kullanılması, kuruluş için bir risk ile sonuçlanır. *Güvenlik açıklarının ne olduğundan, kuruluşun kesintiye karşı ne kadar savunmasız olduğu* veya bu güvenlik açığından yararlanmanın *etkisinin ne olduğu* tartışmasını genişletmek, güvenlik açığı yönetimi alanının ötesine geçerek bir risk yönetimi tartışmasına dönüşür. Gerçekleşmiş bir tehlikenin etkisini ölçmeye çalıştığımız yer risk yönetimidir. Bu bağlam, bu serinin *Risk Yönetimi Kaynak Kılavuzu* , Cilt 7'sinde daha kapsamlı olarak tartışılmaktadır . Bir kuruluşun güvenlik açıklarını çözmesi ve risk dağılımı büyük ölçüde örtüşür. Bu kaynak kılavuzu, güvenlik açıklarının analizini, sınıflandırmasını ve çözümünü netleştirmek için gereken risk yönetimi yönlerini tartışacaktır.

Güvenlik açığı yönetimi süreci sırasında, kuruluş, kontroller için gereksinimler ve kriterler geliştirmesine yol açan güvenlik açıklarını sıklıkla keşfedebilir. Kontrol yönetimi süreci sırasında kuruluş, bir tehlikenin etkisini azaltan kontrolleri geliştirir, uygular ve iyileştirir. *Kontroller _*
Yönetim Kaynak Kılavuzu , bu serinin 2. Ciltinde, bir tehlikenin etkisini azaltan kontroller anlatılmaktadır.

Güvenlik açığı yönetimi, öncelikle kurumsal eğilimi anlama sürecidir. Kontrollerin ve risk yönetiminin uygun şekilde uygulanmasının planlanmasında ve belirlenmesinde kilit bir bileşendir. Bu serinin Kontrol Yönetimi Kaynak Kılavuzu, Cilt 2'sine bakın. Varlıklar için kontrollerin nasıl tanımlanacağı konusunda daha ayrıntılı rehberlik için CERT-RMM'deki Kontrol Yönetimi (CTRL) süreç alanına da bakın. [5]

Bu kılavuz, güvenlik açığı yönetimi sürecindeki adımların her birini ayrıntılı olarak açıklar.

Bir Güvenlik Açığı Analizi ve Çözüm Stratejisi Tanımlayın

Bir yetenek geliştirmenin ilk aşaması, organizasyonun hedeflerine ulaşmak için bir strateji tanımlamaktır. Strateji, güvenlik açığı yönetimi sürecini kuruluşun gereksinimlerine ve kritik başarı faktörlerine göre ayarlar. Stratejinin tanımlanması, ilk katılım stratejisini oluşturan bir faaliyet olan tüm paydaşlardan girdi ve destek toplamayı içerir.

Bu kılavuz, yukarıda açıklandığı gibi güvenlik açığı yönetimi programını uygulayan bir strateji geliştirmeye yönelik ayrı adımları ortaya koymaktadır:

- Güvenlik açığı yönetiminin kapsamını belirleyin.
- Onaylanmış güvenlik açığı değerlendirmesi yöntemlerini belirleyin.

- Faaliyetleri kaynaklayın.

Güvenlik Açığı Yönetimi için Bir Plan Geliştirin

Strateji, güvenlik açığı yönetim ekipleri için kurallar ve yönergeler içeren bir plana dönüştürülmelidir. Kendilerinden ne beklendiğini ve sahip oldukları kaynakları nasıl kullanacaklarını anlamaları gerekir. Planlama aşaması aşağıdaki adımlardan oluşur:

- Planı tanımlayın ve belgeleyin.
- Etkililik ölçütlerini tanımlayın.
- Eğitim gereksinimlerini tanımlayın.
- Stratejiyle uyumlu araçları belirleyin.
- Güvenlik açığı bilgilerinin kaynaklarını belirleyin.
- Rolleri ve sorumlulukları tanımlayın.
- Paydaşları dahil edin.
- Bir plan revizyon süreci geliştirin.

Güvenlik Açığı Analizi ve Çözüm Yeteneğini Uygulayın

Sürecin bu aşamasında kuruluş, zafiyet yönetim planını fiilen uygular ve zafiyet analizi ve çözümleme faaliyetlerini yürütür. Önceki aşamalarda tanımlanan metodolojileri, araçları ve kaynakları kullanır ve planda kararlaştırılan zaman dilimlerine dayalı olarak kuruluşun güvenlik açığına maruz kalmasını azaltır. Güvenlik açığı analizi ve çözümleme performansı boyunca kuruluş, güvenlik açığının izlenmesini, iyileştirme bilgilerinin toplanmasını ve uygun olduğunda risk yönetimi sürecinin devreye alınmasını sağlamak için adımlar atar.

Güvenlik açığı yönetim planının uygulanmasındaki temel adımlar şunlardır:

- Eğitim sağlayın.
- Güvenlik açığı değerlendirme faaliyetlerini yürütün.
- Keşfedilen güvenlik açıklarını kaydedin.
- Güvenlik açıklarını kategorilere ayırın ve önceliklendirin.
- Keşfedilen güvenlik açıklarına maruz kalmayı yönetin.
- Güvenlik açığı eğilimlerinin etkinliğini belirleyin.
- Kök nedenleri analiz edin.

Yeteneği Değerlendirin ve Geliştirin

Güvenlik açığı yönetimi, bir kuruluşun iki özel yeteneği anlamasını ve değerlendirmesini gerektirir: güvenlik açıklarının keşfi ve ilgili güvenlik açıklarının analizi. Keşif yeteneği, kritik hizmetlerin varlıklarını ve ilgili süreçlerini değerlendirmek için uzmanlığı gerektirir. Kuruluş ayrıca keşif yeteneğinin kuruluşun uygun şekilde kapsamlı bir bölümünü kapsadığından emin olmalıdır. Analiz, güvenlik açığının kapsamını ve bunun kuruluş ve kritik hizmetleri üzerindeki beklenen etkisini belirleme yeteneğidir. Genel güvenlik açığı yönetimi yeteneğinin değerlendirilmesi, hem analizin hem de keşfin kuruluşun ihtiyaçlarını karşılamasını sağlar.

Aşağıdakiler, güvenlik açığı yönetiminin değerlendirilmesinde ve iyileştirilmesinde temel temel adımlardır:

- Programın durumunu belirleyin.
- Program bilgilerini toplayın ve analiz edin.
- Yeteneği geliştirin.

Halihazırda güvenlik açığı yönetim planlarına sahip olan kuruluşlar, bunları değerlendirmek ve geliştirmek için bu kaynak kılavuzunu kullanabilir.

III. Bir Güvenlik Açığı Analizi ve Çözüm Stratejisi Tanımlayın

Sen başlamadan önce

Aşağıdaki kontrol listesi, bir güvenlik açığı analizi ve çözüm stratejisi oluşturmaya başlamadan önce tamamlamanız gereken görevleri ve toplamanız gereken bilgileri özetlemektedir.

	Giriş	Rehberlik
✓	Kapsam belirleme beyanı	• Değerlendirilecek ve izlenecek varlıkları ve hizmetleri belirleyin. • İlgili alanları içeren operasyonel ortamı belirleyin. • Hedefleri tanımlayın.
✓	Paydaşları belirleyin	Paydaşların listesi, kapsam belirleme beyanıyla uyumlu olmalı ve tüm uygun dahili ve harici varlıkları içermelidir. Potansiyel adaylar şunları içerir: • yönetici ve üst düzey yönetim • iş kollarının başkanları, özellikle kritik hizmet sahipleri • bilgi Teknolojisi • yasal • Yönetim Kurulu • teknoloji satıcıları • düzenleyiciler ve denetçiler • uyum personeli
✓	Düzenleyici ve diğer yasal gereksinimleri tanımlayın.	Bu belgeler, güvenlik açığı yönetiminin performansı için gereksinimleri sağlar. Bunlar gereklidir, ancak nadiren yeterlidir. Belgeler, strateji belgelenirken referans olarak mevcut olmalıdır. • İlgili düzenleyici gereksinimleri edinin. • Hizmet düzeyi anlaşmaları edinin. • Diğer tüm yasal yükümlülükleri alın.
✓	Paydaş yatırımı	Paydaşlar, stratejiye bağlı kalma ve stratejiyi destekleme niyetlerini kabul etmelidir.
✓	Yönetim katılımı	• Bütçeleme desteğini tanımlayan yönetimden onay • İç politika gereksinimlerine uyumu tanımlayan yönetimden alınan onay • Güvenlik açığı verilerinin toplanması ve dağıtılması faaliyetlerini, belirlenen dayanıklılık ihtiyaçları ve hedefleri ile uyumlu hale getirmek

Adım 1. Zafiyet yönetiminin kapsamını belirleyin.

Bir kuruluşun hizmetlerini ve ilgili siber varlıkları etkileyen güvenlik açıkları geniş ve çeşitlidir. Adım 1, güvenlik açığı yönetimi süreci için anahtar tanımlama etkinliğidir. Kuruluşun yetenekleri ve ilgi alanları için uygun kapsamı ana hatlarıyla belirtir. Kuruluş, hangi varlıkların ve hizmetlerin değerlendirilmesi gerektiğine ve bu değerlendirmenin ne kadar kapsamlı olması gerektiğine karar verdiği yerdir.

Siber dayanıklılık tartışmaları genellikle yalnızca sanal ortamlara miyop bir odaklanmadan muzdariptir. Fiziksel tehditler, siber varlıkların fiziksel hizmetleri ve varlıkları etkilediği gibi siber varlıkları da etkiler. Hizmetinizin güvenlik açığını değerlendirirken, CRR, siber bileşenlerin kritik hizmetler üzerindeki etkisiyle ilgilenir. Ancak, bu siber bileşenlere yönelik tehdit, siber olmayan faaliyetler veya güvenlik açıklarının sonucu olabilir. Siber güvenlik açıklarına karşı hafifletmeler ve çözümler de siber olmayan çözümler gerektirebilir. Bu tür güvenlik açıkları, güvenli olmayan sunucu odaları, su baskınları, personelin çalışma kapasitesi ve sistemin siber operasyonlarına ve ilgili hizmetlere özgü olmayan diğer güvenlik açıklarını içerir.

"Teknik zafiyetlerin belirlenmesi ve giderilmesi, operasyonel riskin azaltılmasına yönelik araçlardır, ancak risk yönetimi faaliyetlerini tam olarak oluşturmazlar." CERT-RMM [6]

A. **Değerlendirilecek ve izlenecek aday varlıkları ve hizmetleri belgeleyin.** Bu aktivitede, organizasyon öncelikle değerlendirme için tüm olası adayları belgelemeye odaklanmıştır. Kaynak kısıtlamaları, daha sonraki adımlarda belirlenecek olan, kuruluşun gerçekten başarabileceği değerlendirme ve izlemeyi etkileyecektir. Paydaşlardan kritik hizmetleri ve ilgi alanları ile ilgili girdileri istenmelidir.
   - Tüm paydaş varlıkları ve hizmetleri temsil ediliyor mu?
   - Paydaş varlıklarının ve hizmetlerinin kritikliğini tanımlayın.

B. **Analiz ve izleme için operasyonel ortamı belirleyin.** Operasyonel ortam, izlenen varlıkların maruz kaldığı risk türlerini tanımlar. Maruziyetler, varlığın oluşturduğu tehditlerin veya bu varlıktaki bir güvenlik açığının bir sonucu olarak kuruluşa yönelik tehditlerin tanımlarıdır. Çevre, en büyük endişe kaynağı olan tehditlere maruz kalmalarla tanımlanmalıdır.
   - Hem siber hem de siber olmayan güvenlik açıklarını ayrıntılandırın.
     - Varlık fiziksel veya siber tehditlerden etkilenebilir mi?
     - Bu tehditler, varlığın siber dayanıklılıktaki işlevini veya rolünü etkiler mi?
   - Hizmetlerinin ve varlıklarının operasyonel ortamındaki güvenlik açıklarına ilişkin paydaş girdisi elde edin.
   - Gerektiğinde üçüncü taraf tehdit değerlendirmesini edinin. Kuruluş, operasyonel ortamının tüm yönlerini ele alacak uzmanlığa sahip olmayabilir.

Tablo 1: Maruziyet Örnekleriyle Eşlenen Varlık Türleri

Varlık türü	Kapsam Örneği
İnsanlar	Çalışan güveni ve güvenilirliği
Bilgi	Ödeme bilgileri erişilebilirliği ve dağıtımı
teknoloji	Veritabanı kullanılabilirliği
Tesisler	Çevre sistemleri kullanılabilirliği

Adım 2. Onaylı güvenlik açığı değerlendirmesi yöntemlerini belirleyin.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 1: Zafiyet analizi ve çözümleme faaliyetleri için hazırlık yapılır.	
2. Varlıklardaki güvenlik açıklarını belirlemek için kullanılan standart bir araç ve/veya yöntem seti var mı? [VAR: SG1.SP2]	**DE.CM** : Siber güvenlik olaylarını belirlemek ve koruyucu önlemlerin etkinliğini doğrulamak için bilgi sistemi ve varlıklar ayrı aralıklarla izlenir.
Hedef 2: Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
1. Güvenlik açığı bilgilerinin kaynakları belirlendi mi? [VAR: SG2.SP1]	**ID.RA-2:** Bilgi paylaşım forumlarından ve kaynaklarından tehdit ve zafiyet bilgisi alınır.

Güvenlik açığı değerlendirmeleri, paydaş ve yönetim desteğine ihtiyaç duyar. Belirli yöntemler, hem operasyonel hem de yasal olarak iyice anlaşılmalı ve dikkatlice planlanmalıdır. Penetrasyon testi (fiziksel ve sanal) kanun uygulayıcılara veya hatta bir kuruluşun kendi güvenlik gücüne zarar verebilir. Seçilen değerlendirme yöntemleri, uygun paydaşlar tarafından netleştirilmelidir. Yöntemler, yasal otorite ve operasyonel paydaşlar tarafından gözden geçirilmelidir.

A. **Yönetmeliğin gerektirdiği yöntemleri belirler.** Kuruluşun endüstri düzenlemelerine bağlı olması muhtemeldir. Ödeme Kartı Sektörü (PCI) Veri Güvenliği Standardı (DSS) veya Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) gibi ilgili düzenlemelerin gerekliliklerini gözden geçirin. PCI DSS gibi bazı düzenlemeler, onaylı satıcılar tarafından güvenlik açığı değerlendirmelerinin yapılmasını gerektirir. Güvenlik açığı analizi ve çözüm planı, yönetmeliğin gerekliliklerini hesaba katmalıdır.

B. Operasyonel gereksinimleri karşılamak için gerekli yöntemleri belirleyin. Yöntemler, güvenlik açığı değerlendirmesi kapsamına göre belirlenen güvenlik açıklarını, hizmetleri ve ilgili varlıkları ele almalıdır (1. Adımda oluşturulmuştur). Kuruluş şunları sormalıdır:

- Aday yöntemler kapsam dahilindeki güvenlik açıkları hakkında bilgi üretiyor mu?
- Seçilen yöntemler, beklenmeyen güvenlik açıklarının keşfedilmesini sağlıyor mu?

Metodoloji hizmet üzerindeki etkiye odaklanırsa, hizmeti destekleyen varlıkların ayrıntılı bir ayrıştırması, her bir varlığın hizmeti ne sağladığını vurgulayacaktır. Bu bilgi ve paydaşlardan gelen girdilerle kuruluş, hizmeti etkileyebilecek olayları keşfetme ve daha iyi önceliklendirme olasılığını artırır.

C. Yasal sonuçları belirleyin .

- Kuruluşun belirlenen yöntemleri uygulayabilmesi için yasal gereklilikler nelerdir?
- Belirlenen yöntemleri üçüncü kişilerin kullanabilmesi için yasal gereklilikler nelerdir?

Ç. Aday yöntemlerin dayattığı etkiyi belirleyin. Bazı yöntemler, savunulamaz operasyonel etki yaratabilir. Güvenlik açığı bulma yöntemleri, sistemin çalışmama süresine neden olabilir veya personelin iş performansını olumsuz etkileyebilir.

- Yasal kısıtlamalarla kısıtlanmış yöntemleri tanımlayın.
- Operasyonel kısıtlamalarla kısıtlanmış yöntemleri tanımlayın.
- Belirlenen kısıtlamalara göre yöntem seçimini tanımlayın.

D. Kullanılacak yöntemleri seçin . Kriterleri belirledikten sonra, kuruluşa operasyonel gereksinimi, operasyonel performans kısıtlamalarını, yasal sorumluluğu ve etkiyi karşılayan bir yöntem seçeneği bırakılmalıdır.

Adım 3. Faaliyetleri kaynaklayın.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 1 – Zafiyet analizi ve çözümleme faaliyetleri için hazırlık yapılır.	
1. Bir zafiyet analizi ve çözüm stratejisi geliştirildi mi? [VAR: SG1.SP2]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır

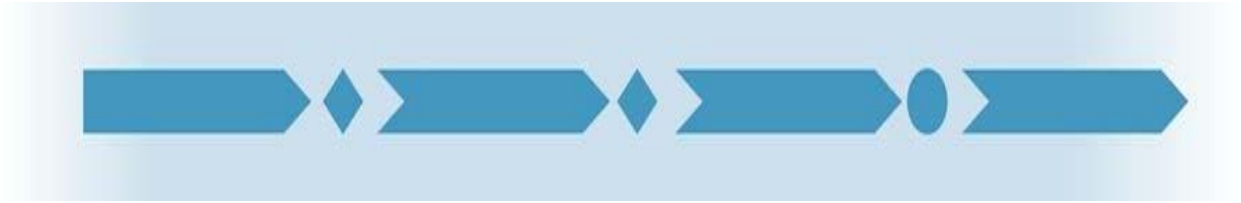
Kaynak, personel alımını içerir. Paydaşlar, güvenlik açığıyla ilgili işlevlerin yetkilendirilmesinde ve performansında rol oynayabilir. Geliştiricilerin kendi makinelerini taramaları ve sonuçları analiz için güvenlik açığı yönetimi ekibine sağlamaları gerekebilir. Sunucu odası kapılarının dolu olmadığı zamanlarda kilitli olduğunun kontrol edilmesinden personel sorumlu olabilir. Tüm bina sakinlerinin uygun şekilde rozetlerinin alınmasını sağlamaktan herkes sorumlu olabilir. Bu faaliyetlerden bazıları finansal veya personel taahhüdü gerektirebilir. Yönetim de dahil olmak üzere paydaşlar, güvenlik açığı yönetimini desteklemeyi taahhüt etmelidir. Kuruluş, planın geliştirilmesi sırasında rolleri ve sorumlulukları belirleyecektir (bkz. Bölüm IV, Adım 6).

A. Paydaş kaynak sorumluluğunu belirleyin. Menfaat sahipleri, yetkilendirmede rolü olduğu belirlenen kişiler ile varlıkların bulunduğu birimlerin üst düzey yönetici ve yöneticilerini içerir. İyileştirme ihtiyacını ve düzeltici eylemler için ilgili zaman çerçevelerini anlamalı ve kabul etmelidirler. Bu eylemler, birimlerinin normal iş işleyişinde aksamalara neden olabilir. Faaliyetler üzerindeki etkileri anlaşılmalı ve paydaşlara endişelerini dile getirme fırsatı verilmelidir.

B. Bir bütçe tanımlayın. Bir bütçe tanımlarken, kuruluşun kapsamı yeniden ele alması gerekebilir. Bütçe nihai olarak kapasiteyi tanımlayacak ve öncelikleri büyük ölçüde etkileyecektir. Bütçe kısıtlamaları yetenekleri sınırlayabilir.

Bölüm III'ün Çıktısı

	Çıktı	Rehberlik
✓	Kapsam tanımı	Kapsam, operasyonel kısıtlamaları ve kuruluşun yeteneklerini ve ilgili alanlarını açıkça tanımlamalıdır.
✓	Belgelenmiş güvenlik açığı analizi ve çözüm stratejisi	Strateji tanımının sonuçları, süreç planının gelişimini bilgilendirebilmeleri için açıkça belgelenmiştir.
✓	Güvenlik açığı analizi ve çözüm planı çerçevesi	Strateji, geliştirilecek süreç planı için çerçeve yapısını tanımlamıştır. Plan için tüm başlangıç gereksinimleri belirlenmelidir. Kuruluş artık plandaki rolleri ve sorumlulukları tanımlamaya hazırdır.
✓	Paydaşların temsili ve yatırımı	Tüm paydaşların rolü ve arayüzü açıkça tanımlanmıştır ve tüm taraflar taahhüt etmiştir.
✓	Yönetimin temsili ve yatırımı	Yönetim bu süreçte paydaş rolünü üstlenmiştir.
✓	Bütçe taslağı	Bütçe, hem önceliklerin hem de yeteneklerin oluşturulmasına rehberlik edecektir.



IV. Güvenlik Açığı Yönetimi için Bir Plan Geliştirin

başlamadan önce

Aşağıdaki kontrol listesi, tamamlamanız gereken görevleri ve güvenlik açığı yönetimini planlamaya başlamadan önce toplamanız gereken bilgileri özetlemektedir.

	Giriş	Rehberlik
✓	Güvenlik açığı yönetimi stratejisi	Strateji, Bölüm III'te geliştirilmiştir ve güvenlik açığı yönetim planının temelini oluşturur.
✓	Paydaşların listesi	Paydaşların, güvenlik açığı yönetimi ihtiyacını anlamaları ve iyileştirme zaman çerçevelerini kabul etmeleri gerekir. Potansiyel adaylar şunları içerir: • yönetici ve üst düzey yönetim • iş kollarının başkanları, özellikle kritik hizmet sahipleri • bilgi Teknolojisi • yasal • Yönetim Kurulu • teknoloji satıcıları • düzenleyiciler ve denetçiler • uyum personeli
✓	Yönetim desteği	Üst yönetim, bir güvenlik açığı yönetim programının oluşturulmasını onaylar, bütçeler atar ve planın süreçlerini ve işleyişini uygular.
✓	Güvenlik açığı için bütçe yönetmek	Bütçe, güvenlik açıklarının belirlenmesini sağlar. Kurum içinde uzmanlık geliştirmek veya bir hizmeti kullanmak için yapılan ödünler, program ve becerilerin bakımı gibi uzun vadeli maliyetlerle birlikte düşünülmelidir.

Adım 1. Planı tanımlayın ve belgeleyin.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 1 – Zafiyet analizi ve çözümleme faaliyetleri için hazırlık yapılır.	
1. Bir zafiyet analizi ve çözüm stratejisi geliştirildi mi? [VAR: SG1.SP2]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır
2. Varlıklardaki güvenlik açıklarını belirlemek için kullanılan standart bir araç ve/veya yöntem seti var mı? [VAR: SG1.SP2]	**DE.CM** : Siber güvenlik olaylarını belirlemek ve koruyucu önlemlerin etkinliğini doğrulamak için bilgi sistemi ve varlıklar ayrı aralıklarla izlenir.
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
1. Güvenlik açığı bilgilerinin kaynakları belirlendi mi? [VAR: SG2.SP1]	**ID.RA-2:** Bilgi paylaşım forumlarından ve kaynaklarından tehdit ve zafiyet bilgisi alınır.
6. Güvenlik açıkları ve bunların çözümleriyle ilgili bilgileri kaydetmek için bir havuz kullanılıyor mu? [VAR: SG2.SP2]	**ID.RA-1:** Varlık güvenlik açıkları belirlenir ve belgelenir **PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır

Bu adım, güvenlik açığı yönetimi için geliştirilen stratejiyi alır ve bunu uygulamak için bir plan oluşturur. Strateji yönü sağlar ve plan ayrıntıları tanımlar. Örneğin, strateji, tüm varlıklar üzerinde güvenlik açığı taramasının

gerçekleştirileceğini gösterebilir. Plan, bunun nasıl gerçekleştirileceğini detaylandıracaktır, çünkü her şeyi bir kerede taramak pratik olmayabilir. Farklı varlık türleri, büyük olasılıkla, plan hedeflerini karşılamak için farklı araçlar ve teknikler gerektirecektir. Örneğin, teknoloji için bir ağ güvenlik açığı tarayıcısı kullanılabilir, tesisler için bir güvenlik görevlisi kullanılabilir ve insanlar için periyodik arka plan kontrolleri kullanılabilir.

A. Güvenlik açığı yönetim ekibini oluşturun. Zafiyet yönetimi planının, organizasyonun farklı işletim birimlerinden gelen girdilerden faydalanması gerekebilir. Örneğin, belirli bir ürüne yama uygulamayla ilgili gereksinimleri anlamak için veri güvenliği ekibinin sunucu ekibinden girdilere ihtiyacı olacaktır. Benzer şekilde, fiziksel güvenlik ekibi, fiziksel varlıkların nasıl güvence altına alınacağına ilişkin girdiler sağlar.

B. Risk yönetimi ile koordineli olun. Güvenlik açıkları kuruluş için bir risk oluşturur. Zafiyet yönetimi ekibi, süreçlerinin birbirleriyle bağlantılı olarak ne zaman yürütülmesi gerektiğini belirlemek için risk yönetimi ekibi ile koordineli olmalıdır.

C. Standart iyileştirme zaman çizelgelerini tanımlayın. Bir güvenlik açığının nasıl sınıflandırılacağı için kritik-yüksek-orta-düşük gibi bir güvenlik açığı sınıflandırma ölçeği tanımlanmalıdır. Bu ölçeğin her düzeyiyle ilişkili olarak, kuruluşun keşfedilen bir güvenlik açığının var olmasına kaç gün izin verebileceğini tanımlayan bir düzeltme zaman çerçevesi olmalıdır.

Ç. Güvenlik açıklarının nasıl belgelenmesi gerektiğini tanımlayın. İdeal olarak, keşfedilen tüm güvenlik açıkları merkezi bir havuza yerleştirilmelidir. Bu, iyileştirme çabalarının izlenmesini kolaylaştıracak ve geçmişle ilgili bilgiler sağlayacaktır. Ek olarak, bilgiler etkinliği ölçmenin bir parçası olarak kullanılabilir.

D. İstisnaların nasıl ele alınması gerektiğini tanımlayın. Bazen, belirli bir güvenlik açığı zamanında çözülemez. Plan, risk yönetimi sürecini kullanarak bir risk oluşturmak gibi bu durumların nasıl ele alınacağını ve standart iyileştirme zaman çizelgelerini aşma kararına hangi düzeyde yönetimin dahil edilmesi gerektiğini tanımlamalıdır.

E. Periyodik aktiviteleri tanımlar. Genel olarak, güvenlik açıkları yalnızca ortamda bir değişiklik meydana geldiğinde ortaya çıkar. Bu hem fiziksel hem de siber güvenlik açıkları için geçerlidir. Güvenlik açığı yönetimi faaliyetlerinin periyodikliği, değişiklik yönetimi ve bilgi farkındalığı zaman çerçevelerini hesaba katmalıdır. Tablo 2, her varlık türü için örnek periyodik güvenlik açığı yönetimi etkinliklerini vermektedir.

Tablo 2: Varlık Türleri için Örnek Periyodik Güvenlik Açığı Yönetimi Faaliyetleri

Varlık türü	Örnek Periyodik Faaliyetler
İnsanlar	Temiz masa kontrolleri, yeniden soruşturmalar, bilgi farkındalığı faaliyetleri
Bilgi	İlgili bilgiler için izleme kaynakları (ör. e-posta, Twitter)
teknoloji	Tarama, değişiklik yönetimi
Tesisler	Gezici gardiyanlar tarafından güvenlik kontrolleri

F. Proaktif faaliyetleri tanımlayın. Posta listelerini, Twitter'ı, blogları ve benzeri bilgi varlıklarını izlemek reaktif bir aktivitedir. Tarama ve sızma testleri ise proaktif faaliyetlerdir ve programlanması gerekir. Plan, bu faaliyetlerin ne sıklıkta ve çevrenin hangi kısımlarında gerçekleştirildiğini detaylandırmalıdır. Kuruluş, tarama yaparken aşağıdakileri dikkate almalıdır:

- güvenlik duvarı kuralları olan veya olmayan
- dahili veya internet tarama kaynağı
- tarama seviyesi
- kurum içi veya üçüncü taraf tarama

Kuruluşlar, aşağıdaki örneklerde olduğu gibi, teknoloji dışı varlıklardaki güvenlik açıklarını keşfetmek için proaktif faaliyetler de yürütebilir:

- tesisler ○ Günün sonunda sunucu odası kapısı kilitli mi?
  - Giriş ve çıkış günlükleri dengeleniyor mu?
  - Yangın söndürme sistemlerinin bakımı gerektiği gibi yapılıyor mu?
- insanlar
  - İş davranışlarında bir değişiklik oldu mu? Ö Kişisel yaşamlarında (örneğin, finans) bir değişiklik oldu mu?

Adım 2. Etkililik ölçütlerini tanımlayın.

Kuruluşun zafiyet yönetimi faaliyetlerini ne kadar iyi gerçekleştirdiğini anlamak için kuruluş bunların etkinliğini ölçmelidir. Planlama ekibi, etkinliğin nasıl ölçüleceğini, herhangi bir raporlama gereksinimlerini ve gerekli süreçleri ve araçları belirlemelidir.

Adım 3. Eğitim gereksinimlerini tanımlayın.

Güvenlik açığı yönetiminin gereksinimlerinin karşılanması iki tür eğitim gerektirebilir: son kullanıcı eğitimi ve uygulayıcı eğitimi. Bu serinin *Eğitim ve Farkındalık Kaynak Kılavuzu* , Cilt 9'u, kuruluşun bu eğitimi nasıl tanımlaması, yürütmesi ve değerlendirmesi gerektiğini ayrıntılarıyla anlatmaktadır.

A. Son kullanıcı eğitimini tanımlayın. Kuruluş, güvenlik açığı yönetimi stratejisi kapsamında, bir olayın kaynağı olma olasılığını azaltmak için genel çalışan nüfusunun özel eğitim alması gerektiğine karar vermiş olabilir. Zafiyet yönetimiyle ilgili eğitim, diğer şeylerin yanı sıra aşağıdakileri ele alabilir: • kimlik avı saldırıları • güvenli sörf

B. Uygulayıcıları eğitin. Bu eğitim, zafiyet yönetiminden sorumlu personeli, organizasyonun yöntem ve araçları konusunda eğitmeye odaklanmaktadır. Bu içerebilir

- onaylanan araçlar nasıl kullanılır
- Nasıl izlendikleri, düzeltme için zaman çerçeveleri ve diğerleri dahil olmak üzere güvenlik açığı yönetimi prosedürleri
- Görev ve Sorumluluklar
- sertifikalar

Uygulayıcılar organizasyonun farklı alanlarına yayılabilir. Örneğin, yöneticiler ve insan kaynakları personeli, insan varlıkları için güvenlik açığı bilgilerinin izlenmesinden sorumlu olabilirken, tesislerden site güvenliği sorumlu olabilir.

Adım 4. Stratejiyle uyumlu araçları belirleyin.

Bu adımda kuruluş, strateji tarafından belirtilen yöntemleri uygulamak için hangi araçları kullanması gerektiğini belirler. Bazı metodolojiler, kapsamlı bir değerlendirme yapmak için birden fazla araç gerektirebilir.

A. Aday araçları belirleyin. Her metodolojinin ihtiyaçlarını karşılamak için hangi araçların veya hizmetlerin kullanılabileceğini araştırın.

B. Test araçları. Değerlendirmek ortam için uygun olup olmadıklarını belirlemek için aday araçların veya hizmetlerin her biri. Belirlenmesi gereken önemli bir gerçek, aracın tüm ihtiyaçları karşılayıp karşılamadığı veya boşlukları doldurmak için başka bir araca ihtiyaç olup olmadığıdır.

C. Yetkili takım listesini yayınlayın. Kuruluş içindeki herkesin, hangi araçları kullanmasına izin verildiğini belirleyebilmesi için, nihai araç listesi yayınlanmalıdır.

Ç. İstisna sürecini tanımlayın. Değişen durumlar, yeni bir güvenlik açığını doğrulamak veya olay müdahalesine yardımcı olmak gibi kritik bir ihtiyacı karşılamak için yeni bir aracın kullanılmasını gerektirebilir. Kuruluş, belirli bir süre için yeni bir aracın kullanımına izin vermek için bir süreç tanımlamalıdır.

D. Yönetmek periyodik incelemeler Kuruluşun ihtiyaçlarını karşılamaya devam edip etmediklerini belirlemek için araçları periyodik olarak gözden geçirin. Aynı şekilde, mevcut bir araçtan daha iyi bir çözüm sağlayabilecek yeni araçları ve hizmetleri inceleyin.

Adım 5. Güvenlik açığı bilgilerinin kaynaklarını belirleyin.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
1. Güvenlik açığı bilgilerinin kaynakları belirlendi mi? [VAR: SG2.SP1]	**ID.RA-2:** Bilgi paylaşım forumlarından ve kaynaklarından tehdit ve zafiyet bilgisi alınır.

İyi güvenlik açığı bilgisi kaynakları, kuruluşu korumak için gereklidir. Bu bilgilerin birçok kaynağı vardır (aşağıdaki B Bölümünde Tablo 3'e bakınız) ve özellikle değişken varlık türleri nedeniyle tek bir kaynak büyük olasılıkla yeterli olmayacaktır. Kuruluş, hangilerinin ihtiyaçlarına ve kaynaklarına en uygun olduğunu değerlendirmeye ihtiyaç duyacaktır.

A. Kullanımdaki varlıkları tanımlayın. Bir kuruluşun hangi güvenlik açığı bilgilerine ihtiyaç duyduğunu anlamak için hangi varlıkların kullanımda olduğunu bilmesi gerekir. Bu bilgi, ilgili varlık türü için varlık envanterlerinden elde edilebilir. Güvenlik açıklarından bahsederken, siber alandaki çoğu insan hemen BT altyapılarının donanım ve yazılım bileşenlerini düşünür. Ancak, insanlar ve teknolojiyi, bilgiyi ve insanları barındıran tesisler gibi diğer varlıklar da savunmasızdır.

Varlık yönetimi uygulamalarıyla ilgili yardım için bu serinin Varlık Yönetimi Kılavuzu, Cilt 1'e bakın.

Teknoloji varlıkları için aşağıdaki bilgilere ihtiyaç duyulacaktır:

- donanım için model numaraları
- yazılım için sürüm numaraları
- bileşenin konumu

İdeal olarak, kuruluş bu bilgileri, belirli bir güvenlik açığıyla ilgili düzeltici eylemleri gerçekleştirirken ihtiyaç duyacağı bir varlık veritabanında saklayacaktır.

Teknoloji varlıklarını belirlerken sadece ortamdaki iş istasyonuna ve sunuculara odaklanmayın. Ayrıca kullanımda olan güvenlik duvarları, yönlendiriciler, anahtarlar ve yük dengeleyiciler gibi BT altyapısı bileşenlerini de içerir.

B. Güvenlik açığı bilgilerinin kaynaklarını belirleyin. Elinde izlenecek benzersiz varlıkların listesi ile kuruluş, her bir varlık için güvenlik açığı bilgilerinin kaynaklarını belirlemelidir. Tablo 3, bazı potansiyel kaynakları tanımlar ve belirli bir öğeyle ilgili güvenlik açığı bilgilerinin internette aranması, diğerlerini ortaya çıkarabilir.

Tablo 3: Güvenlik Açığı Bilgilerinin Kaynakları

Kaynak	Bilgi
Satıcılar	Satıcılar ve özellikle teknoloji satıcıları, genellikle güvenlik açıkları için yamalar ile birlikte tavsiyeler sağlar.

Posta listeleri	Bugtraq ve Tam Açıklama gibi listeler, geniş bir ürün yelpazesi hakkında güvenlik açığı bilgileri sağlar, ancak bunun sonucunda e-posta hacmi oldukça fazladır.
Bölümü vatan Güvenlik (DHS)	US-CERT ve ICS-CERT, BT varlıkları için güvenlik tavsiyeleri sağlar. DHS ayrıca bölgesel PSA (Koruyucu Güvenlik Danışmanı) programı aracılığıyla yerinde tesis denetimleri sağlar.
Bilgi Paylaşım ve Analiz Merkezleri (ISAC'ler)	Belirli sektörlere odaklanan ve üyelerine sektöre göre uyarlanmış tavsiyeler ve tehdit uyarıları gibi çeşitli hizmetler sunan çeşitli ISAC'ler vardır.
Kullanıcı Grupları	Belirli bir ürün için kullanıcı grupları, o üründeki tehditler ve güvenlik açıkları hakkında da bilgi sağlayabilir. Kullanıcı grupları genellikle bir posta listesi aracılığıyla iletişim kurar ve her zaman güvenlikle ilgili bilgiler içermeyebilir. Ancak, birisinin destek nedenleriyle listeyi izlemesi, bir güvenlik danışma belgesine bakması ve onu güvenlik açığı yönetiminin ekibinin dikkatine sunması muhtemeldir.
Kızılötesi	Federal Soruşturma Bürosu (FBI), incelenmiş üyelerine mevcut tehditler hakkında bilgi sağlayan ve kaynak bilgileri ve kullanılan metodolojiler gibi bilgileri içeren InfraGard programını yürütür.
heyecan	Twitter'ın izlenmesi, belirli bir konumu veya bir bütün olarak kuruluşu etkileyebilecek faaliyetler hakkında bilgi sağlayabilir.
Güvenlik Servisi	Yönetilen Güvenlik Hizmeti (MSS) satıcıları, özel öneriler ve güvenlik açığı taraması gibi güvenlik açığıyla ilgili hizmetleri bir ücret karşılığında sağlar.

Dış kaynaklar, belirli bir varlığa özgü güvenlik açıkları hakkında bilgi sağlayabilirken, bir teknoloji varlığının yanlış yapılandırılmasından veya insan varlıklarının eğitimindeki bir başarısızlıktan kaynaklanan güvenlik açıklarını ortaya çıkaramazlar. Kuruluş, bu zayıflıkları belirlemek için araçlar kullanmaya karar verebilir. Örneğin, bir güvenlik açığı tarayıcısı veya bir sızma testi, teknoloji varlıklarına karşı periyodik olarak çalıştırılabilir. Aynı şekilde, eğitim sorunlarını değerlendirmek için kuruluş, çalışanlarına kimin tıkladığını görmek için periyodik olarak sahte kimlik avı e-postaları gönderebilir.

Bazı güvenlik açığı bilgisi kaynakları, kuruluşun içinde olabilir. Yöneticiler ve insan kaynakları personeli, diğer çalışanlarda kötü niyetli eylemleri gösterebilecek anormal davranışlar gözlemleyebilir. Çalışanların periyodik özgeçmiş kontrolleri başka bir bilgi kaynağı olabilir.

Tesis varlıkları için kuruluş, yerinde operasyonları etkileyebilecek olaylar hakkında hava durumu tahminleri gibi diğer bilgi kaynaklarını dikkate almalıdır.

Adım 6. Rolleri ve sorumlulukları tanımlayın.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
6. Güvenlik açıkları ve bunların çözümleriyle ilgili bilgileri kaydetmek için bir havuz kullanılıyor mu? [VAR: SG2.SP2]	**ID.RA-1:** Varlık güvenlik açıkları belirlenir ve belgelenir **PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır

Bu adımla kuruluş, güvenlik açığı yönetimi için bir plan geliştirmeyi neredeyse tamamlamıştır: bilgi kaynakları belirlenmiş ve kullanılacak araçlar seti tanımlanmıştır. Kuruluş şimdi planı kimin yürütmesi gerektiğini ve sorumluluklarının neler olduğunu belirlemelidir. Planlama ekibi, zafiyet yönetimi işlevlerini yerine getirmekle görevlendirilecek kuruluşun birimlerini veya bireylerini belirleyecek ve bunları aşağıdaki rollere atayacaktır.

A. **İzleme rolleri.** Bu personel, çeşitli güvenlik açığı bilgilerinin izlenmesinden ve uygun önlemin alınmasından sorumludur. İzleme rolleri şu kişilere atanmalıdır : güvenlik açıklarının kuruluşla olan ilişkisini analiz etmek
   - güvenlik açığı bilgilerini güvenlik açığı deposuna kaydedin
   - düzeltme ekibini uyar

B. İyileştirme rolleri. Kuruluşun farklı bölümlerinden personelin aşağıdaki gibi sorumlulukları olabilir:

- Yamaların kuruluş üzerindeki etkisini analiz edin
- hiçbiri mevcut değilse, güvenlik açığı için şirket içi geçici çözümler geliştirin
- Muhtemelen değişiklik yönetimi yoluyla değişiklikleri yapmak için yetki kazanın (bu serinin Konfigürasyon ve Değişiklik Yönetimi Kaynak Kılavuzu, Cilt 3'e bakın)
- Güvenlik açığının tanımlanmış eşikleri aşarak açık kalması gerekiyorsa risk yönetimi sürecini başlat

C. Yetkilendirme rolleri. Bu roldeki personel, çevrelerini anlamaktan sorumludur ve herhangi bir olumsuz etki olup olmadığını belirlemek için düzeltici eylemleri gözden geçirmelidir. Değişim yönetimi sürecinin bir parçasıdırlar ve buna göre hareket ederler. Derhal ele alınması gereken düzeltici eylemleri ele almak için bir acil durum değişiklik talebi süreci mevcut olmalıdır.

Adım 7. Paydaşların katılımını sağlayın.

Paydaşlar, 6. Adımda tanımlanan yetkilendirme rolüne sahip olanları ve varlıkların bulunduğu birimlerin üst düzey yöneticilerini ve yöneticilerini içerir. Güvenlik açığı yönetimi yalnızca BT işlevleriyle sınırlandırılamayacağından, kuruluşun, planın gereksinimlerine bağlı olarak diğerlerine ek olarak fiziksel güvenlik ve insan kaynakları departmanlarındaki paydaşları belirlemesi gerekebilir.

Paydaş sorumlulukları şunları içerir:

- birimlerinin özel gereksinimleri hakkında girdi sağlamak
- güvenlik açığı yönetim planını ilgili ekiplerine savunmak • düzeltme zaman dilimlerini kabul etmek

Adım 8. Bir plan revizyon süreci geliştirin.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
2. Bu kaynaklardan alınan bilgiler güncel tutuluyor mu? [VAR: SG2.SP1]	**DE.DP-5:** Algılama süreçleri sürekli iyileştiriliyor **ID.RA-2:** Bilgi paylaşım forumlarından ve kaynaklarından tehdit ve zafiyet bilgisi alınır. **PR.IP-7** : Koruma süreçleri sürekli iyileştirilmektedir

Herhangi bir iyi planın etrafındaki ortam değiştikçe değişmesi gerekir. Kuruluşlar, kuruluşun ihtiyaçlarını karşılayıp karşılamadığını belirlemek için güvenlik açığı yönetim planlarını en az yılda bir kez gözden geçirmelidir.

A. Değişikliklerin olup olmadığını belirleyin. Planın güncellenmesi gerekip gerekmediğini belirlemek için, son plan incelemesinden bu yana kuruluşa ne olduğunu gözden geçirin. Dikkate alınması gereken bazı sorular:

- Kuruluşa yeni teknoloji tanıtıldı mı?
- Organizasyona yeni tesisler eklendi veya çıkarıldı mı?
- Kuruluş başka kuruluşlar satın aldı mı?
- Kuruluşun herhangi bir bileşeni kuruluştan çıkarıldı mı?
- Güvenlik açıklarını tespit etmek için yeni metodolojiler tanıtıldı mı?
- Yeni insanlar eklendi mi, kaldırıldı mı veya dış kaynaklı mı?

Bu sorulardan herhangi birine *evet* yanıtı, planın daha derinlemesine incelenmesinin garanti edildiğini gösterir.

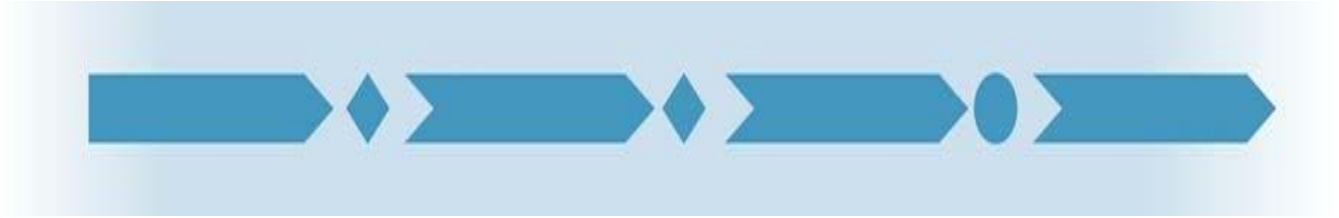
B. Değişiklikleri gözden geçirin. Değişikliğin organizasyon üzerindeki etkisini belirleyin ve planda uygun değişiklikleri yapın.

C. Gerekirse araç setini güncelleyin. Plandaki değişiklik, güvenlik açıklarını tespit etmek için kullanılan araçlarda bir güncelleme gerektirebilir.

Ç. Güvenlik açığı bilgilerinin kaynaklarını güncelleyin. Bir değişiklik kuruluşa yeni bir şey (tesisler, teknoloji vb.) getirdiyse, kuruluşun yeni varlık için bir güvenlik açığı bilgisi kaynağı belirlemesi zorunludur. Büyük olasılıkla, yeni varlığın satıcısıyla yakın zamanda bir ilişki kurulmuş olacaktır ve satıcı, birincil bilgi kaynağı olacaktır. Ancak kuruluş, kullanıcı grupları gibi diğer kaynakları da dikkate almak isteyebilir. Ek olarak, mevcut bilgi kaynaklarından herhangi biri, gönderdiklerini bir profile göre uyarlıyorsa, güncellenmesi de gerekir.

Bölüm IV'ün Çıktısı

	Çıktı	Rehberlik
✓	Güvenlik açığı yönetim planı	Paydaşların katılımını sağlayın ve hepsinin keşif ve iyileştirme için zaman çerçeveleri üzerinde anlaşmasını sağlayın. Roller ve sorumlulukların atandığından ve tanımlandığından emin olun.
✓	Güvenlik açığı yönetimi süreci	Farklı varlıkların farklı süreç belgeleri olacaktır. Tüm süreç belgelerinde tutarlılık ve entegrasyon sağlayın.
✓	Onaylı araçların listesi	Listeyi herkesin kullanımına açın ve yeni araçların kullanım sürecini tanımlayın.
✓	Güvenlik açığı bilgisi kaynaklarının listesi	Ortamda neyin risk altında olduğunu anlamak, kuruluşun uygun güvenlik açığı bilgisi kaynaklarını belirleyebilmesi için çok önemlidir.
✓	Güvenlik açığı yönetimi revizyon süreci	Değişim gerçekleşir ve organizasyonun planın çeşitli bileşenlerini güncellemek için bir sürece ihtiyacı vardır.



V. Güvenlik Açığı Analizi ve Çözüm Yeteneğini Uygulayın

Sen başlamadan önce

Aşağıdaki kontrol listesi, tamamlamanız gereken görevleri ve güvenlik açığı analizi ve çözümleme yeteneğini uygulamaya başlamadan önce toplamanız gereken bilgileri özetlemektedir.

	Giriş	Rehberlik
✓	güvenlik açığı Yönetim planı	Paydaşların katılımını sağlayın ve hepsinin keşif ve iyileştirme için zaman çerçeveleri üzerinde anlaşmasını sağlayın. Rol ve sorumlulukların kabul edildiğinden emin olun.
✓	güvenlik açığı Yönetim süreci	Farklı varlıkların farklı süreç belgeleri olacaktır. Tüm süreç belgelerinde tutarlılık ve entegrasyon sağlayın.
✓	Güvenlik açığı bilgisi kaynaklarının listesi	Kaynak bilgileri, güvenlik açığı yönetim ekibine süreci başlatmak için neyi izlemeleri gerektiğini söyler.
✓	Rol ve sorumlulukların tanımı	Herkes, güvenlik açıklarının ele alınmasıyla ilgili olarak kendilerinden ne beklendiğini anlamalıdır.
✓	Onaylı araçlar listesi	Ekip, ortamdaki güvenlik açıklarının düzenini keşfetmek, izlemek ve belirlemek için bu listedeki test edilmiş ve onaylanmış araçları kullanır.

Adım 1. Eğitim sağlayın.

Kuruluş, süreci yürüten personelin, sürecin kendisi ve planlanan görevler hakkında tam olarak eğitilmesini sağlamalıdır. Personel, tanımlanan görevleri uygun şekilde yürütecek becerilere sahip olmalıdır. Bireylerin belirli araçları, teknikleri ve metodolojileri kullanmak için eğitilmesi gerekir. Rollerini, paydaşların rollerini, tüm üçüncü taraf varlıklarını ve iş akışını anlamaları gerekir. Eğitim, kilit karar noktalarını ve operasyonel kısıtlamaları vurgulamalıdır.

Bu serinin Eğitim ve Farkındalık Kılavuzu, Cilt 9'a bakın.

A. Personeli süreç hakkında eğitin. Güvenlik açığı yönetiminde yer alan tüm personel, görevleriyle ilgili süreçleri anlamalıdır. Tutarlı bir yaklaşım sağlamak için değişim yönetimi gibi diğer süreçlerle karşılıklı ilişkilerin anlaşılması vurgulanmalıdır.

B. Personeli görevlerle ilgili eğitin. Sürece ek olarak, personelin görevlerinin ne olduğunu ve geliştirilen plana göre bunları nasıl gerçekleştireceklerini anlamaları gerekir.

Adım 2. Güvenlik açığı değerlendirme faaliyetlerini yürütün.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
3. Güvenlik açıkları aktif olarak keşfediliyor mu? [VAR: SG2.SP2]	**DE.CM-8:** Güvenlik açığı taramaları yapılıyor **ID.RA-1:** Varlık güvenlik açıkları belirlenir ve belgelenir

Bu adım, kuruluştaki mevcut güvenlik açıklarını keşfetmek için güvenlik açığı değerlendirme faaliyetlerinin yürütülmesini gerektirir. Daha önce tartışıldığı gibi, değerlendirme yöntemleri bilgi, teknoloji, insanlar ve tesisler dahil olmak üzere kritik hizmeti destekleyen her türlü varlığı ele almalıdır. Fiziksel güvenlik denetimleri, çevresel kontrol kontrolleri (HVAC, yangın söndürme), kurumsal tehdit değerlendirmeleri ve siber güvenlik açığı tarayıcıları, kapsamlı bir kurumsal güvenlik açığı değerlendirmesinin temel bileşenleridir.

A. Güvenlik açığı taramaları yürütün. Tarama kurum içinde yapılabilir veya üçüncü bir tarafa ihale edilebilir. Kuruluş personelinin yeteneklerini belirleyin ve gerektiğinde dış yardımla destekleyin. Teknik olarak yetenekli kurum içi ekipler her zaman mevcut olmayabilir; iyileştirme ile meşgul olabilirler veya paydaşlarla birlikte çalışabilirler.

B. Güvenlik açığı değerlendirmelerini yürütün. Sızma testleri olarak da bilinen güvenlik açığı değerlendirmeleri, bir tarayıcıdan daha fazla derinlikte test eder. Bunlar, denetimlerden veya taramalardan daha kapsamlıdır ve genellikle sistemlere yönelik fiziksel güvenlik açıklarını içerir. Daha kapsamlı oldukları ve otomatikleştirilemedikleri için, güvenlik açığı değerlendirmeleri genellikle kuruluşun kullandığı tüm varlıklarda gerçekleştirilmez ve belirli bir örnek için uyarlanmalıdır.

Sızma testleri (veya kalem testleri), üçüncü taraf test cihazlarının normalde sahip olamayacakları varlıklara erişim elde etmek için genellikle kuruluşun personeli ile rekabet etmesi bakımından zıttır. Kuruluş, sızma testini paydaşlarla önceden görüşmeli ve ilgili herkes bunun öğrenme hedefiyle güvenli bir etkinlik olduğunu anlamalıdır. Sızma test cihazlarını yenmeye veya testin kendisini oynamaya odaklanmak organizasyona fayda sağlamayacaktır (ancak izinsiz giriş müdahale ekibinin moralini artırabilir). Bunun yerine, güvenlik açığı yönetimi ekibi, sızma testini günlük operasyonlarının güçlü ve zayıf yönlerini öğrenmek için bir fırsat olarak görmelidir.

Adım 3. Keşfedilen güvenlik açıklarını kaydedin.

Güvenlik açıkları bir güvenlik açığı deposuna kaydedilmelidir. Bu, kuruluşların güvenlik açığı yönetimine yapılandırılmış ve izlenebilir bir şekilde yaklaşmasını sağlar. Keşfedilen güvenlik açıkları, yalnızca kuruluşun mevcut duruşunu sağlamlaştırmak için değil, aynı zamanda operasyonlarda organizasyonel değişiklikleri planlamak için de faydalıdır. Güvenlik açıklarına ilişkin veriler de dahil olmak üzere geçmiş veriler, bir mimari değişikliğin uygulanmasında belirleyici bir faktör olabilir.

A. Güvenlik açığını depoda oturum açın. Güvenlik açığının kapanmaya kadar takip edildiğinden emin olmak için bir havuzda oturum açılmalıdır. Kuruluşun havuza kaydetmek isteyebileceği bazı alanlar şunlardır:

- keşif tarihi ve saati
- etkilenen varlıklar
- öncelik
- sınıflandırma
- kaynak
- sahip

- analiz notları
- şu anki durum
- kapanış tarihi ve saati

B. Deponun erişim kontrolünü sağlayın. Bu bilgilerin son derece hassas olduğunu unutmayın: temel olarak kuruluşun maruz kaldığı risklerin bir yol haritasıdır. Bu bilgiyi uygun şekilde ele alın. Depoya erişimi, bu bilgileri bilmesi gereken kişilerle sınırlayın: öncelikle güvenlik açığı yönetim ekibi ve yönetimi, ancak muhtemelen risk yönetimi ekibinden de personel.

Adım 4. Güvenlik açıklarını kategorilere ayırın ve önceliklendirin.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
4. Güvenlik açıkları kategorize edilip önceliklendiriliyor mu? [VAR: SG2.SP3]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır
5. Kuruluşla alaka düzeyini belirlemek için güvenlik açıkları analiz ediliyor mu? [VAR: SG2.SP3]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır
Hedef 3 - Belirlenen güvenlik açıklarına maruz kalma yönetilir.	
1. Belirlenen güvenlik açıklarına maruz kalmayı yönetmek için önlemler alınıyor mu? [VAR: SG3.SP1]	**RS.MI-3:** Yeni tanımlanan güvenlik açıkları azaltılır veya kabul edilen riskler olarak belgelenir
3. Çözümlenmemiş güvenlik açıklarının durumu izleniyor mu? [VAR: SG3.SP1]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır

Bu adımda kuruluş, güvenlik açığı keşfi bulgularıyla ilişkisini belirler. Bulgular kritik hizmetleri etkiliyor mu? etkisi nedir? Bulgular arasında herhangi bir ilişki var mı? Bu, güvenlik açıklarının analizindeki ilk adımdır.

Analiz, güvenlik açıklarının karakterizasyonuna ve bunların nasıl düzeltileceğine odaklanmalıdır.

A. Alaka düzeyi için analiz edin. Güvenlik açığı kuruluşun operasyonlarıyla ilgili mi? Bilgi kanalları, sızma testi ekipleri (dahili ve üçüncü taraf) ve güvenlik açığı keşif araçları, çok sayıda bilgi üretecektir. Yalnızca kuruluşun kullanmadığı varlıkları etkileyen bu bulgular göz ardı edilebilir, ancak kuruluşta değişiklik planlanırken referans olması için muhafaza edilmelidir. Bir teknolojinin güvenlik açığı oranı yüksekse, kuruluş, iyileştirme iş yükünden ve ilgili maliyetlerden kaçınmak için farklı bir teknoloji seçmeye karar verebilir.

B. Sorumluluğu belirleyin. Güvenlik açığı yönetim ekibi, güvenlik açıklarını keşfedebilir, ancak genellikle bunların azaltılmasından veya çözülmesinden sorumlu değildir. Güvenlik açığı ekibinin uygun paydaşları bilgilendirmesi gerekecektir. Güvenlik açıklarının uygun şekilde düzenlenmesi, önceliklendirme ve planlama için paydaşlarla koordinasyon gerektirir.

C. Öncelik ver. Güvenlik açıklarını önceliklendirirken, güvenlik açığı ekibi, risk yönetimi ekibi ile koordineli olmalıdır. Bazı kuruluşlarda zafiyet ve risk yönetimi ekipleri aynı personelden oluşabilir. Bu ekipler birleştirildiğinde, güvenlik açıklarının izlenmesi, sınıflandırılması ve önceliklendirilmesi genellikle eşdeğer risk süreçlerinde birleştirilir.

Bir güvenlik açığının önem derecesi, genellikle önceliklendirme için kullanılır, çünkü yüksekler genellikle düşüklerden daha hızlı yamalanır. Bazı güvenlik açığı bilgileri kaynakları (bazı örnekler için Tablo 4'e bakın) önem dereceleri atayabilirken diğerleri vermez. Ne olursa olsun, kuruluş kendisine bir önem derecesi derecesinin neyi gösterebileceğini ve kuruluş için ne anlama geldiğini sormalıdır. Örneğin, iki dahili varlık üzerindeki yüksek önem düzeyine sahip bir güvenlik açığı, tüm dışa dönük varlıkları etkileyen bir güvenlik açığı kadar kritik olmayabilir. Bilgi kaynağının seçtiği önem derecesi, kuruluşun güvenlik açığını nasıl

gördüğüyle eşleşmeyebilir ve kuruluşun önem derecesini ayarlaması gerekir. Güvenlik açığının niteliğine bağlı olarak, kuruluş genelinde aynı önem derecesine sahip olmayabilir. Kuruluş, zafiyet yönetimi stratejisinde tanımlanan metodolojiyi kullanarak, kuruluşun mimarisi ve operasyonlarıyla ilgili olarak zafiyetin önceliğini değerlendirmelidir.

Tablo 4: Önceliklendirme ve Önem Derecesi Kılavuzunun Örnek Kaynakları

Kaynak	Referans
CVSS	http://nvd.nist.gov/cvss.cfm
DISA Güvenlik Teknik Uygulama Kılavuzları	http://iase.disa.mil/stig/
Satıcılar	
Adobe	http://helpx.adobe.com/security/severity-ratings.html
Microsoft	http://technet.microsoft.com/en-us/security/gg309177.aspx
Kırmızı şapka	https://access.redhat.com/site/security/updates/classification/

Adım 5. Keşfedilen güvenlik açıklarına maruz kalmayı yönetin.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
5. Kuruluşla alaka düzeyini belirlemek için güvenlik açıkları analiz ediliyor mu? [VAR: SG2.SP3]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır
6. Güvenlik açıkları ve bunların çözümleriyle ilgili bilgileri kaydetmek için bir havuz kullanılıyor mu? [VAR: SG2.SP2]	**ID.RA-1:** Varlık güvenlik açıkları belirlenir ve belgelenir **PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır
Hedef 3 - Belirlenen güvenlik açıklarına maruz kalma yönetilir.	
1. Belirlenen güvenlik açıklarına maruz kalmayı yönetmek için önlemler alınıyor mu? [VAR: SG3.SP1]	**RS.MI-3:** Yeni tanımlanan güvenlik açıkları azaltılır veya kabul edilen riskler olarak belgelenir

Artık kuruluş, güvenlik açığının alakalı olduğunu belirlediğine ve ona bir öncelik derecesi atadığına göre, açıklığını azaltmak için harekete geçer. Ortak risk eğilimleri, operasyonel riski kabul etmek, önlemek, azaltmak veya transfer etmektir.

A. Elden çıkarma metodolojisini belirleyin. Elden çıkarma eylemi, varlığın niteliğine ve güvenlik açığı bilgilerinin kaynağına göre değişir.

- *Satıcı tarafından sağlanan çözümü edinin.* Satıcılar, ürünlerindeki bir güvenlik açığından haberdar olduklarında, güvenlik açığını ortadan kaldırmak için değişiklikler yapacaklardır. Bilgi teknolojisi sistemleri için bu değişikliklere yamalar denir.
- *Yapılandırmayı değiştirin.* Bazı durumlarda, düzeltici eylemler, güvenlik açığını ortadan kaldırmak için varlığın yapılandırmasını değiştirmek olabilir. Bir ağ güvenlik taraması, kullanılmayan bir hizmet ortaya çıkarırsa,

  Çözüm, hizmeti kapatmak olabilir. Fiziksel bir erişim güvenlik açığı için, birinin varlığa nasıl ulaştığını değiştirmek çözüm olabilir.
- *Geçici çözümü uygulayın.* Güvenlik açığını ortadan kaldıracak herhangi bir yama veya yapılandırma seçeneği yoksa, riski azaltmanın başka bir yöntemi de ortama güvenlik açığından yararlanılmasını engelleyebilecek denetimler yerleştirmektir.
- *Riski kabul edin.* Güvenlik açığı riskinin en azından bir kısmını hafifletmek için pratik veya uygun maliyetli bir yöntem yoksa, riski tanımlamak ve açık bırakmak için kabul görmek için risk yönetimi süreci başlatılmalıdır.

B. Test düzeni. Kuruluş, operasyonel ortam üzerindeki etkisini belirlemek için genel dağıtımdan önce seçilen eğilimi test etmelidir. Bu özellikle teknoloji çözümleri için geçerlidir, ancak herhangi bir değişiklik için de geçerlidir. Örneğin, park yeri için bir giriş kontrol kapısının dikilmesi, istemeden araçların yola geri çekilmesine neden olabilir. Çoğu durumda, değişiklik yönetimi süreci bu adımı zorunlu kılacaktır.

C. Elden çıkarma yöntemini dağıtın. Test edilen elden çıkarma yöntemi şimdi, güvenlik açığının önceliği için hedeflenen zaman dilimleri kullanılarak ortama dağıtılmalıdır. Değişiklik yönetimi sisteminin kullanılması, değişikliği yapmak için gereken zamanlama ve onaylara izin vermek için teşvik edilir. Bazı durumlarda, düzenlemeyi gerçekleştiren ekipler, güvenlik açığını yöneten ekipten farklı olabilir. Örneğin, Windows güvenlik açıklarının yamalanması sunucu ve iş istasyonu ekipleri tarafından gerçekleştirilebilir, ancak güvenlik açığının yönetimi bilgi güvenliği ekibi tarafından gerçekleştirilebilir.

Ç. Çözünürlük için takip edin. Tüm düzeltici eylemler, kuruluşun ortamında güvenlik açığı için seçilen değerlendirme metodolojisi uygulanana kadar güvenlik açığı yönetimi havuzunda izlenmelidir. Bir değerlendirme dağıtımı ertelenirse ve güvenlik açığının çözüm için hedeflenen zaman çerçevesini kaçıracaksa, planla birlikte geliştirilen özel durum süreci başlatılmalıdır. Kuruluşlar, kararın neden olduğu anormal etkileri, çözümleriyle birlikte depoya not etmelidir. Kuruluş bir değişiklik yönetimi aracı kullanıyorsa, girişlerinin her biri güvenlik açığı havuzundaki ilgili girişe atıfta bulunmalıdır ve bunun tersi de geçerlidir. Bu, bir sonraki adımı kolaylaştıracaktır.

Elden çıkarma etkinliği yalnızca bir geçici çözümse, kuruluş, satıcı tarafından sağlanan bir çözümün kullanılabilirliğini izlemeye devam etmelidir. Mevcut olduğunda, bu "Keşfedilen güvenlik açıklarına maruz kalmayı yönet" adımı bütünüyle tekrarlanmalıdır.

Adım 6. Zafiyet eğilimlerinin etkinliğini belirleyin.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
6. Güvenlik açıkları ve bunların çözümleriyle ilgili bilgileri kaydetmek için bir havuz kullanılıyor mu? [VAR: SG2.SP2]	**ID.RA-1:** Varlık güvenlik açıkları belirlenir ve belgelenir **PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır
Hedef 3 - Belirlenen güvenlik açıklarına maruz kalma yönetilir.	
2. Güvenlik açığı azaltmanın etkinliği gözden geçiriliyor mu? [VAR: SG3.SP1]	**DE.DP-5:** Algılama süreçleri sürekli iyileştiriliyor **PR.IP-7:** Koruma süreçleri sürekli iyileştirilmektedir **RS.IM:** Organizasyonel müdahale faaliyetleri, mevcut ve önceki tespit/yanıt faaliyetlerinden öğrenilen derslerin dahil edilmesiyle geliştirilir.

Kuruluş, güvenlik açığının düzenini belirledikten sonra, eğilimin hedeflerine ulaşıp ulaşmadığını belirlemelidir. Güvenlik açığı riskinin azaltılıp azaltılmadığını veya kaldırılıp kaldırılmadığını anlamak önemlidir. Güvenlik açığının nasıl keşfedildiğine bağlı olarak kuruluş, güvenlik açığının düzenini doğrulamak için keşif yöntemini tekrarlayabilir. Örneğin, bir ağ tarayıcısı veya sızma testi güvenlik açığını keşfettiyse, testin ilgili bölümünün yeniden çalıştırılması, iyileştirme çabalarının nasıl sonuç verdiğini gösterecektir.

A. Elden çıkarma çabalarını değerlendirin. Kuruluş, eğilimlerin doğru bir şekilde uygulandığını doğrulamak için testler yapmalıdır. Bu testler, iyileştirme çabalarının herhangi bir sorun yaşayıp yaşamadığını veya herhangi bir soruna neden olup olmadığını değerlendirmeli ve eylemlerin belirlenen güvenlik açıklarını ele alıp almadığını belirlemelidir. Bileşenlerin sayısına bağlı olarak, bunu yapmak için otomatik yöntemler yoksa, elden çıkarmanın tamamlandığını kontrol etmek gerekebilir. Bu durumda, yönetim, planda belgelenmesi gereken, ilgili popülasyonu temsil eden sistemlerin örnek yüzdesi üzerinde anlaşmalıdır.

Otomatikleştirilmiş araçlar veya onu güncel tutan yöntemler varsa, olası bir bilgi kaynağı varlık envanteri olabilir.

B. Güvenlik açığı deposunu güncelleyin. Güvenlik açığı ekibi, değerlendirme bulgularıyla veri havuzunu güncellemelidir.

C. Elden çıkarma işlemini gerektiği kadar tekrarlayın. Etkililik testinin bulguları, tasarrufların riski azaltmadığını gösteriyorsa, daha etkili bir tasarruf stratejisi belirlemek için, "Keşfedilen güvenlik açıklarına maruz kalmayı yönetin" Adım 5'te süreç yeniden başlatılmalıdır.

Adım 7. Kök nedenleri analiz edin.

CRR Hedefi ve Uygulaması [CERT-RMM Referansı]	NIST CSF Kategorisi/ Alt Kategorisi
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	
5. Kuruluşla alaka düzeyini belirlemek için güvenlik açıkları analiz ediliyor mu? [VAR: SG2.SP3]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır
6. Güvenlik açıkları ve bunların çözümleriyle ilgili bilgileri kaydetmek için bir havuz kullanılıyor mu? [VAR: SG2.SP2]	**ID.RA-1:** Varlık güvenlik açıkları belirlenir ve belgelenir **PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır
Hedef 3 - Belirlenen güvenlik açıklarına maruz kalma yönetilir.	
1. Belirlenen güvenlik açıklarına maruz kalmayı yönetmek için önlemler alınıyor mu? [VAR: SG3.SP1]	**RS.MI-3:** Yeni tanımlanan güvenlik açıkları azaltılır veya kabul edilen riskler olarak belgelenir
Hedef 4 – Güvenlik açıklarının temel nedenleri ele alınmaktadır.	
1. Güvenlik açıklarının altında yatan nedenler (kök neden analizi veya başka yollarla) tanımlandı ve ele alındı mı? [VAR: SG4.SP1]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır **RS.IM:** Organizasyonel müdahale faaliyetleri, mevcut ve önceki tespit/yanıt faaliyetlerinden öğrenilen derslerin dahil edilmesiyle geliştirilir.

Kök neden analizi (RCA), bir olayın neden meydana geldiğine dair daha derin bir anlayış kazanmak için bir mekanizmadır. Bu anlayıştan yola çıkarak, bu eylemin yeniden gerçekleşmesini düzeltmek ve potansiyel olarak önlemek için bir araç geliştirilebilir. Güvenlik açığı yönetimi için, güvenlik açıkları üzerinde RCA yapmak, kuruluşun tekrarlanan güvenlik açıklarını önlemesini sağlar.

Bazı güvenlik açıkları, bir RCA'dan yararlanmayabilecek, kuruluşun kontrolü dışındadır. Keşfedilen her güvenlik açığı RCA için dikkate alınmalıdır, ancak bir varlık için alternatif satıcılar gibi doğal bilgiler, düzeltici eylem için düşünülebilir.

RCA gerçekleştirmenin birincil nedeni, güvenlik açığının tekrar oluşmasını önlemektir. RCA'ların bir maliyeti vardır, ancak bir güvenlik açığının ilk ortaya çıkışında bir RCA yürütmek, daha fazla maliyete neden olabilecek ve kötüye kullanılması durumunda potansiyel olarak bir olaya yol açabilecek gelecekteki oluşumları önleyebilir.

A. Kök neden analizi yapın. Kuruluş, neden var olduğunu belirlemek için güvenlik açığını analiz etmelidir. Bazı olası nedenler

- satıcı sorunu
- yanlış yapılandırma
- politika veya prosedürleri takip etmemek
- zayıf yazılım tasarımı
- uygunsuz eğitim
- operasyonel karmaşıklık

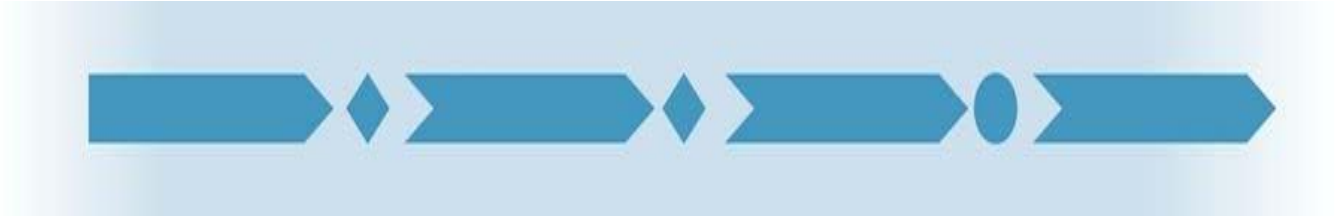
B. Kök nedeni ele almak için düzeltici eylemler geliştirin. Nedene bağlı olarak kuruluş, belirli bir güvenlik açığının gelecekte ortaya çıkma olasılığını azaltmak için düzeltici bir eylem geliştirmelidir. Şirket içinde geliştirilen uygulama yazılımının, üretime geçmeden önce güvenlik açıkları açısından test edilmesi veya personelin güvenli kodlama teknikleri konusunda eğitilmesi gerekebilir. Bir tesis güvenlik açığının RCA'sı, diğer sitelerin aynı sorunu yaşamasını önlemek için mimari değişiklikler önerebilir.

C. **Güvenlik açığı deposunu güncelleyin.** Güvenlik açıklarıyla ilgili tüm eylemlerde olduğu gibi, kuruluş, güvenlik açığının depodaki kaydını, nedeni ve alınan düzeltici eylemlerle güncellemelidir. Bu, bir sonraki aşamada yardımcı olacaktır.

Ç. **Düzeltici faaliyetlerin etkisini izleyin.** Kuruluş düzeltici önlemleri aldıktan sonra, depoyu sorgulayarak veya taramalar gibi algılama etkinliklerini yeniden çalıştırarak güvenlik açığının ek örneklerini izlemelidir. Güvenlik açığının ek örnekleri, ek düzeltici eylemler gerektirebilecek bir temel nedenin ele alınmadığını gösterebilir.

Bölüm V'nin Çıktısı

	Çıktı	Rehberlik
✓	Güvenlik açığı önceliklendirme yönergeleri	Güvenlik açıklarının bulundukları ortama göre önceliklendirilmesi gerekir.
✓	Güvenlik açığı analizi	Her bir güvenlik açığı keşfedildikçe, kuruluşla ilgili olup olmadığını belirlemek için analiz edilir. Eğer öyleyse, kategorize edilir, önceliklendirilir, günlüğe kaydedilir ve bir azaltma stratejisi geliştirilir.
✓	Öncelikli güvenlik açıkları ve düzenleme deposu	Güvenlik açıklarını izlemek ve gerçekleştirilen eylemlerin geçmiş kaydını tutmak için bir havuz şiddetle tavsiye edilir. Daha sonra, daha önce ne yapıldığını anlamak için yeni güvenlik açıkları keşfedildiğinde sorgulanabilir.
✓	Güvenlik açıklarının kaynaklarının analizi	Bir güvenlik açığının neden oluştuğunu anlamak için kök neden analizini kullanmak, kuruluşa gelecekte benzer bir güvenlik açığını önleyebilecek değişiklikler yapma fırsatı verir.
✓	Güvenlik açığı düzenleme yeteneklerinin analizi	Güvenlik açıklarının düzenini izlemek, kuruluşa yalnızca güvenlik açıklarının doğru bir şekilde ele alındığına dair güven vermekle kalmaz, aynı zamanda sürecin nasıl iyileştirileceğini öğrenme fırsatları da sunar.



VI. Yeteneği Değerlendirin ve Geliştirin

Sen başlamadan önce

Aşağıdaki kontrol listesi, tamamlamanız gereken görevleri ve yeteneği değerlendirmeye ve geliştirmeye başlamadan önce toplamanız gereken bilgileri özetlemektedir.

	Giriş	Rehberlik
✓	Güvenlik açığı yönetimi stratejisi	• Stratejide tanımlanan rehberliği ve gereksinimleri toplayın.
✓	Belirlenen paydaşların listesi	• Güvenlik açığı bilgilerinin tüketicilerini belirleyin. • Keşfedilen güvenlik açıklarından etkilenebilecek kişileri belirleyin.
✓	Yerleşik iyileştirme önlemleri	• Program sonuçlarını belirtilen hedeflere karşı ölçün. • Eyleme geçirilebilir bilginin ne olduğunu belirleyin. • Gerekli türev metriklerini belirleyin.
✓	Yerleşik izleme programı	• Belirlenen önlemleri uygun aralıklarla toplamak için bir araç oluşturun.

Adım 1. Programın durumunu belirleyin.

Kuruluş, güvenlik açığı yönetimi programında iyileştirmeler yapmadan önce, programın mevcut performans durumunu belirlemelidir. Bu belgenin Ek B'sinde yer alan CRR sorularının kendisi iyi bir referans noktasıdır. Kuruluş, CRR sorularını yanıtlamakta zorlanıyorsa, bu, kuruluşun programın durumu hakkında daha fazla bilgiye ihtiyaç duyduğunun iyi bir göstergesidir.

A. Paydaşlarla stratejiyi gözden geçirin.
- İlgili tüm paydaşlar temsil ediliyor mu?

B. Her bir paydaşın neye ihtiyacı olduğunu belirleyin.
- Süreç uygun iş ürünlerini etkiliyor mu?
- Hangi bilgiler doğrudan paydaş süreçlerini etkiler?
- Paydaşlar bilgileri nasıl kullanıyor?

C. Mevcut sürecin ne sağladığını belirleyin.
- Süreç uygun iş ürünlerini sağlıyor mu?
- Kuruluş tüm CRR sorularını yanıtlayabiliyor mu?
- Hangi bilgiler eksik?

Adım 2. Program bilgilerini toplayın ve analiz edin.

Önceki adım, programın amaçlandığı gibi çalıştığından emin olmak için programın durumunu değerlendirdi; bu adım, kuruluş genelinde güvenlik açıklarını azaltma hedefine gerçekten ulaşıp ulaşmadığını belirlemek için programın çıktılarını değerlendirir.

A. İlgili tüm çalışma ürünlerini, ilkelerini ve kılavuzluğunu toplayın.

- Süreç çıktılarını toplayın.
- İşlem politikasını toplayın.
- Süreç planını toplayın.
- Süreç stratejisini toplayın.
- Standartları ve yönergeleri toplayın.
- Paydaşların ve dış bağımlılıkların listesini toplayın.
- Etkililik ölçütlerine ilişkin tüm raporları derleyin.
- Gözden geçirme faaliyet programını toplayın. Bu, sürecin kendisinin gözden geçirilmesinin periyodikliğini belirleyen programdır.
- Yönetime yönelik raporlar da dahil olmak üzere paydaşlara örnek raporlar toplayın.
- Güvenlik açığı yönetimi için kurumsal standartları toplayın.

B. Etkililik ölçütlerini analiz edin.

- Etkililik ölçütleri, sürecin gerekli yönlerini ele alıyor mu?
- Etkililik ölçüleri kritik hizmetle uyumlu mu?
- Etkililik ölçütleri, iş ürünleri hakkında eyleme geçirilebilir bilgiler veriyor mu?

C. Toplanan ürünleri etkinlik ölçülerine karşı analiz edin.

- İş ürünleri, paydaşlar tarafından eyleme geçirilebilir bilgiler sağlıyor mu?
- Paydaşlar sürece bağlı mı?
- Güvenlik açığı bilgilerinin kaynakları hala güncel mi?

Ç. Etkililik ölçütlerini karşılamama riskini belirleyin. Burada güvenlik açığı yönetim ekibi, risk ölçümü etrafındaki parametreleri anlamak için risk analiz ekibiyle birlikte çalışmalıdır. Değerlendirilen güvenlik açıklarına olası yanıtlardan en iyi ve en kötü durum örneklerini belirleyin. En iyi ve en kötü durumlara verilen tepkiler arasındaki fark küçükse, etkinlik ölçütlerini karşılama çabası harcamaya değmeyebilir. Böyle bir durumda, kuruluş etkinlik ölçütlerini yeniden ele almalıdır. Etkililik ölçüleri, operasyonel gereksinimler ve etki ile tanımlanmalıdır.

Adım 3. Yeteneği geliştirin.

İyileştirme, sürecin analizi sırasında bulunan eksikliklerin giderilmesi eylemidir. Uygun şekilde tanımlanmış bir süreç, istenen hedeflere verimli ve etkili bir şekilde ulaşır. Organizasyon, planlama sürecinde arzu edilen etkinliğini tanımlamış olacaktır. Adım 2'de gerçekleştirilen analiz, sürecin etkinliğini anlamak için bir temel oluşturur. Kuruluş, yeteneğinin etkinlik ölçütlerini ne kadar iyi karşıladığını anladıktan sonra, ölçülerin ihtiyaçlarını ne kadar iyi karşıladığını ele alır.

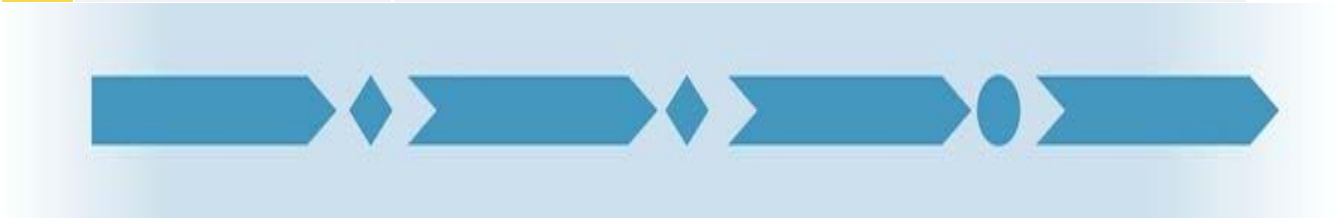
A. Etkinlik ölçütleri tarafından tanımlanan süreçteki eksiklikleri ele alın.

- Ölçümlerden birinin metriği negatifse, bu süreç hakkında ne anlama gelir?
- Eksiklik, sürecin güvenlik açıklarını azaltma yeteneğini etkiler mi? güvenlik açıklarını keşfetmek? paydaşları dahil etmek?
- Bu eksiklik nasıl giderilir? Eksikliği gidermek için süreç nasıl değiştirilmelidir?

Yeteneği geliştirmek yinelemelidir. Bir bütün olarak yetenek, kuruluş süreci her gelişim aşamasında değerlendirdiğinde ve geliştirdiğinde gelişir. Kuruluşun sürecin bu bölümüne ne kadar yatırım yapacağı, iyileştirmesi gereken bilgi miktarına bağlıdır. Genç süreçler için kuruluş, daha hızlı ve kolay bir şekilde daha kaba bilgiler toplayabilir ve daha hızlı ve daha tanınabilir değişiklikler sağlayabilir. Daha olgun bir süreçte, değişiklikler belirsizdir ve uygun ölçümleri yapmak ve bunları daha incelikli iyileştirmelerle ilişkilendirmek için daha olgun bir iyileştirme süreci gerektirir.

Bölüm VI'nın Çıktısı

	Çıktı	Rehberlik
✓	Değerlendirme raporu	• Aşağıda sunulan konuları detaylandırın
✓	Varlık kapsamındaki boşluklar	• Mevcut güvenlik açığı yönetim planı kapsamında olmayan varlıkların listesi
✓	Hizmet kapsamındaki boşluklar	• Mevcut güvenlik açığı yönetim planı kapsamında olmayan hizmetlerin listesi
✓	Keşfedilmemiş güvenlik açıklarından kaynaklanan riskler	• Varlık veya hizmet kapsamındaki boşluklardan beklenen etkiler
✓	Yanlış analizden kaynaklanan riskler	• Hizmetin yetersiz anlaşılmasından, varlıkların rollerinin yetersiz anlaşılmasından veya sistemik ilişkilerden kaynaklanan analizlerin etkileri
✓	Kontrollerin etkinliği hakkında rapor	• Kontrollerin (mevcut ve önerilen) keşfedilen güvenlik açıkları üzerindeki etkisini tartışır
✓	Önerilen süreç değişiklikleri	• Bulguları ve bunların operasyonlarla ilişkisini tartışır; yeniden hizalama, yetenek değişiklikleri ve kapasite ayarlamaları için önerileri belgeler



VII. Çözüm

Devam eden bir güvenlik açığı yönetim programı oluşturmak ve desteklemek, bir kuruluşun güvenlik açığı keşfi, analizi ve çözümleme yeteneğinin etkinliğini değerlendirmesine olanak tanır ve diğer yönetim etki alanlarına rehberlik eden bilgiler sağlar. Güvenlik açığı yönetimi programı, kuruluşun kritik hizmetlerine ilişkin kapsamlı bir anlayışa sahip olmasını, paydaşlarına karşı sorumluluğunu yerine getirmesini ve ulusal kritik altyapıya katkıda bulunmasını sağlamaya yardımcı olur.

Aşağıdaki belgeler kapsamlı program rehberliği sağlar:

- *NIST Özel Yayını SP 800-53* (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.80053r4.pdf), bilgi sistemleri için bir kontrol kataloğu sağlar.
- *NIST Özel Yayını SP 800-53A* (http://csrc.nist.gov/publications/nistpubs/800-53Arev1/sp800-53A-rev1-final.pdf), bilgi sistemleri üzerinde değerlendirme yapmak için kılavuzlar sağlar.
- *CERT-RMM [Caralli* 2010], CRR'nin temelidir ve uygulamaları oluşturmak için daha derinlemesine rehberlik içerir.

Siber Esneklik İncelemesi hakkında daha fazla bilgi için lütfen Siber Güvenlik Değerlendirme Programına CSE@hq.dhs.gov adresinden e-posta gönderin veya http://www.us-cert.gov/ccubedvp/self-service-crr adresini ziyaret edin.

Ek A. Güvenlik Açığı Yönetimi Kaynakları

Federal Finansal Kurumlar Sınav Konseyi (FFIEC) http://www.ffiec.gov/

- Bilgi Güvenliği Kitapçığı http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

Gartner (abonelik gerektirir)
http://www.gartner.com/technology/home.jsp

- *Zafiyet Değerlendirme Teknolojisi ve Zafiyet Yönetimi Uygulamaları* https://www.gartner.com/doc/2664022?pcp=itg ○ Güvenlik Açığı Değerlendirmesi için MarketScope https://www.gartner.com/doc/2586218?pcp=itg
  - Güvenlik Açığı Yönetimi ile BT Güvenliğini Artırın https://www.gartner.com/doc/480703

Forrester http://www.forrester.com/home/

- Güvenlik açığı yönetimi makaleleri, araçları ve şablonları (bazıları ücretlidir) http://www.forrester.com/search?tmtxt=vulnerability%20management&searchOption=10001&source=typed

FS-ISAC

- Siber İstihbarat Deposu https://www.fsisac.com/CyberIntelligenceRepository

HIPAA.com
http://www.hippa.com/

- Güvenlik Yönetimi Süreci: Risk Analizi-Ne Yapmalı ve Nasıl Yapılmalı [Risk ve zafiyet yönetimi] http://www.hipaa.com/2009/02/security-management-process-risk-analysis%E2%80%94what-to-doand-how-to-do-it/

Uluslararası Standardizasyon Örgütü (ISO) http://www.iso.org/iso/home.html

- ISO/IEC TR 20004:2012 Bilgi teknolojisi -- Güvenlik teknikleri -- ISO/IEC 15408 ve ISO/IEC 18045 (ücretli) kapsamında yazılım güvenlik açığı analizinin iyileştirilmesi http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50951 ○ ISO/IEC 30111:2013 Bilgi teknolojisi -- Güvenlik teknikleri -- Güvenlik açığı işleme süreçleri (ücret)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231
  - ISO/IEC 29147:2014 Bilgi teknolojisi -- Güvenlik teknikleri -- Güvenlik açığı ifşası (ücretli)
    http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45170

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) http://www.nist.gov/index.html

- NIST Bilgisayar Güvenliği Bölümü, Bilgisayar Güvenliği Kaynak Merkezi http://csrc.nist.gov/

- Ulusal Güvenlik Açığı Veritabanı http://www.nist.gov/itl/csd/stvm/nvd.cfm http://nvd.nist.gov/home.cfm
- NIST IR 7946 TASLAK CVSS Uygulama Kılavuzu
  http://csrc.nist.gov/publications/drafts/nistir-7946/draft_nistir_7946.pdf
- NIST NIST IR 7669 DRAFT Açık Güvenlik Açığı Değerlendirme Dili (OVAL) Doğrulama Programı Türetilmiş Test Gereksinimleri
  http://csrc.nist.gov/publications/drafts/nistir-7669/draft-nistir-7669.pdf
- NIST IR 7328 DRAFT Güvenlik Değerlendirmesi Sağlayıcı Gereksinimleri ve Müşteri Sorumluluklar: Federal Bilgi için Güvenlik Değerlendirmesi Kimlik Bilgilendirme Programı Oluşturma
  Sistemler
  http://csrc.nist.gov/publications/drafts/nistir-7328/NISTIR_7328-ipdraft.pdf
- SP 800-40 v.2.0 Yama ve Güvenlik Açığı Yönetim Programı Oluşturma
  http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
- NIST Yayın listesi http://csrc.nist.gov/publications/PubsFL.html

Ödeme Kartı Endüstrisi (PCI) Güvenlik Standartları Konseyi
https://www.pcisecuritystandards.org/index.php

- *Ödeme Kartı Endüstrisi (PCI) Veri Güvenliği Standardı, PCI DSS'de Gezinme – Gereksinimlerin Amacının Anlaşılması v.2.0* Bölüm 5 ve 6'ya bakın, *Bir Güvenlik Açığı Yönetim Programının Sürdürülmesi* https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf
- *Ödeme Kartı Endüstrisi (PCI) Veri Güvenliği Standardı – Güvenlik Tarama Prosedürleri* https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf
- *PCI Hızlı Başvuru Kılavuzu* https://www.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf
- PCI onaylı tarama satıcıları https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

AramaSağlıkIT
http://searchhealthit.techtarget.com/

- *En iyi güvenlik açığı yönetimi 2013* http://searchsecurity.techtarget.com/feature/Best-of-vulnerability-management-2013 Ö "Güvenlik açığı yönetimi programları: Güvenlik uzmanları için bir el kitabı"na erişin http://searchsecurity.techtarget.com/ehandbook/Vulnerability-management-programs-Ahandbook-for-security-pros

Yazılım Mühendisliği Enstitüsü, CERT Bölümü http://www.sei.cmu.edu/

- CERT Esneklik Yönetim Modeli http://www.cert.org/resilience/products-services/cert-rmm/index.cfm
- OCTAVE (Operasyonel Olarak Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi) http://www.cert.org/resilience/products-services/octave/index.cfm ○ CERT'de güvenlik açığı analizi konuları http://www.cert.org/blogs/blog_categories.cfm?getCat=Vulnerability%20Analysis
  - CERT'de güvenlik açığı bulma konuları
    http://www.cert.org/blogs/blog_categories.cfm?getCat=Vulnerability%20Discovery

Amerika Birleşik Devletleri Bilgisayar Acil Durum Hazırlık Ekibi (US-CERT)
http://www.us-cert.gov

- *Eyalet, Yerel, Kabile ve Bölgesel (SLTT) Hükümetler için Başlarken* http://www.us-cert.gov/ccubedvp/getting-started-sltt
- *Açıklardan Yararlanma ve Güvenlik Açığı Veritabanları* https://buildsecurityin.us-cert.gov/swa/resources/exploit-and-vulnerability-databases
- Analitik Araçlar ve Programlar http://www.us-cert.gov/government-users/tools-and-programs
  Ulusal Siber Farkındalık Sistemi https://www.us-cert.gov/ncas

Ek B. CRR/CERT-RMM Uygulaması/NIST CSF Alt Kategori Referansı

Tablo 5, NIST CSF Kategorileri/Alt Kategorileri için CRR Güvenlik Açığı Yönetimi Alanı hedefleri ve uygulama soruları ile bu kılavuzun bu soruları ele alan bölümlerine çapraz referanslar verir. Bu kılavuzun kullanıcıları, alıştırma sorularını yorumlama hakkında daha fazla bilgi için https://www.us-cert.gov/ccubedvp adresinde bulunan Kılavuzlu CRR Soru Setini incelemek isteyebilir. https://www.uscert.gov/ccubedvp adresinde bulunan NIST CSF, Kategori ve Alt Kategori ifadelerini yorumlamak için bilgilendirici referanslar da sağlar.

Tablo 5: Güvenlik Açığı Karşıtı CRR Hedefleri/Uygulamaları ve NIST CSF Kategorisi/Alt Kategorisinin Çapraz Referansı Yönetim Kaynak Kılavuzu

CRR Hedefi ve Uygulaması [CERT-RMM Referans]	NIST CSF Kategorisi/ Alt Kategorisi	Güvenlik Açığı Yönetimi Kaynak Kılavuzu Referansı
Hedef 1 – Zafiyet analizi ve çözümleme faaliyetleri için hazırlık yapılır.	-	-
1. Bir zafiyet analizi ve çözüm stratejisi geliştirildi mi? [VAR: SG1.SP2]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır	Bölüm III, Adım 3 Bölüm IV, Adım 1
2. Varlıklardaki güvenlik açıklarını belirlemek için kullanılan standart bir araç ve/veya yöntem seti var mı? [VAR: SG1.SP2]	**DE.CM** : Siber güvenlik olaylarını belirlemek ve koruyucu önlemlerin etkinliğini doğrulamak için bilgi sistemi ve varlıklar ayrı aralıklarla izlenir.	Bölüm III, Adım 2 Bölüm IV, Adım 1
Hedef 2 – Güvenlik açıklarını belirleme ve analiz etme süreci oluşturulur ve sürdürülür.	-	-
1. Güvenlik açığı bilgilerinin kaynakları belirlendi mi? [VAR: SG2.SP1]	**ID.RA-2:** Bilgi paylaşım forumlarından ve kaynaklarından tehdit ve zafiyet bilgisi alınır.	Bölüm III, Adım 2 Bölüm IV, Adım 1 Bölüm IV, Adım 5
2. Bu kaynaklardan alınan bilgiler güncel tutuluyor mu? [VAR: SG2.SP1]	**DE.DP-5:** Algılama süreçleri sürekli iyileştiriliyor **ID.RA-2:** Bilgi paylaşım forumlarından ve kaynaklarından tehdit ve zafiyet bilgisi alınır. **PR.IP-7** : Koruma süreçleri sürekli iyileştirilmektedir	Bölüm IV, Adım 8
3. Güvenlik açıkları aktif olarak keşfediliyor mu? [VAR: SG2.SP2]	**DE.CM-8:** Güvenlik açığı taramaları yapılıyor **ID.RA-1:** Varlık güvenlik açıkları belirlenir ve belgelenir	Bölüm V, Adım 2
4. Güvenlik açıkları kategorize edilip önceliklendiriliyor mu? [VAR: SG2.SP3]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır	Bölüm V, Adım 4
5. Kuruluşla alaka düzeyini belirlemek için güvenlik açıkları analiz ediliyor mu? [VAR: SG2.SP3]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır	Bölüm V, Adım 4 Bölüm V, Adım 5 Bölüm V, Adım 7
6. Güvenlik açıkları ve bunların çözümleriyle ilgili bilgileri kaydetmek için bir havuz kullanılıyor mu? [VAR: SG2.SP2]	**ID.RA-1:** Varlık güvenlik açıkları belirlenir ve belgelenir **PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır	Bölüm IV, Adım 1 Bölüm IV, Adım 6 Bölüm V, Adım 5 Bölüm V, Adım 6 Bölüm V, Adım 7
Hedef 3 - Belirlenen güvenlik açıklarına maruz kalma yönetilir.	-	-
1. Belirlenen güvenlik açıklarına maruz kalmayı yönetmek için önlemler alınıyor mu? [VAR: SG3.SP1]	**RS.MI-3:** Yeni tanımlanan güvenlik açıkları azaltılır veya kabul edilen riskler olarak belgelenir	Bölüm V, Adım 4 Bölüm V, Adım 5 Bölüm V, Adım 7
2. Güvenlik açığı azaltmanın etkinliği gözden geçiriliyor mu? [VAR: SG3.SP1]	**DE.DP-5:** Algılama süreçleri sürekli iyileştiriliyor **PR.IP-7:** Koruma süreçleri sürekli iyileştirilmektedir	Bölüm V, Adım 6

CRR Hedefi ve Uygulaması [CERT-RMM Referans]	NIST CSF Kategorisi/ Alt Kategorisi	Güvenlik Açığı Yönetimi Kaynak Kılavuzu Referansı
	RS.IM: Organizasyonel müdahale faaliyetleri, mevcut ve önceki tespit/yanıt faaliyetlerinden öğrenilen derslerin dahil edilmesiyle geliştirilir.	
3. Çözümlenmemiş güvenlik açıklarının durumu izleniyor mu? [VAR: SG3.SP1]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır	Bölüm V, Adım 4
Hedef 4 – Güvenlik açıklarının temel nedenleri ele alınmaktadır.	-	-
1. Güvenlik açıklarının altında yatan nedenler (kök neden analizi veya başka yollarla) tanımlandı ve ele alındı mı? [VAR: SG4.SP1]	**PR.IP-12:** Bir güvenlik açığı yönetim planı geliştirilir ve uygulanır **RS.IM:** Organizasyonel müdahale faaliyetleri, mevcut ve önceki tespit/yanıt faaliyetlerinden öğrenilen derslerin dahil edilmesiyle geliştirilir.	Bölüm V, Adım 7

son notlar

1 . *Siber Esneklik İncelemesi* hakkında daha fazla bilgi için lütfen Siber Güvenlik Değerlendirme Programına CSE@hq.dhs.gov adresinden e-posta gönderin.

2. *CERT-RMM* (Terimler Sözlüğü) [Caralli 2010]

3. Caralli, RA; Allen, JA; & White, DW *CERT ® Esneklik Yönetim Modeli: Operasyonel Esnekliği Yönetmek için Bir Olgunluk Modeli (CERT-RMM, Sürüm 1.1)* . Addison-Wesley Professional, 2010. CERT-RMM hakkında daha fazla bilgi için lütfen http://www.cert.org/resilience/products-services/cert-rmm/index.cfm adresini ziyaret edin.

4. Risk Yönlendirme Komitesi, İç Güvenlik Bakanlığı. *DHS Risk Sözlüğü – 2010 Sürümü.* İç Güvenlik Bakanlığı, 2010. http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

5. *CERT-RMM* . "Kontrol Yönetimi" (s. 241) [Caralli 2010].

6. *CERT-RMM* . "Güvenlik Açığı Analizi ve Çözümü" (s. 915) [Caralli 2010].