Bilgi Sistemleri Sızma Testleri Usul ve Esasları

1) **Amaç:** Sızma testlerinin amacı, Kurum Kuruluş ve Ortaklıkların bilgi sistemlerinde tespit edilen açıklıkların ve zafiyetlerin kullanılmasıyla sistemlere sızma girişimlerinin önceden tespit edilmesi ve düzeltilmesidir.
2) **Kapsam:** Sızma testleri kapsamında gerçekleştirilecek testler asgari olarak aşağıdaki başlıkları kapsar:
   a. İletişim Altyapısı ve Aktif Cihazlar
   b. DNS Servisleri
   c. Etki Alanı ve Kullanıcı Bilgisayarları
   ç. E-posta Servisleri
   d. Veritabanı Sistemleri
   e. Web Uygulamaları
   f. Mobil Uygulamalar
   g. Kablosuz Ağ Sistemleri
   ğ. Dağıtık Servis Dışı Bırakma Testleri
   h. Sosyal Mühendislik Testleri
3) **Metodoloji:** Sızma testleri, aşağıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek testlerden oluşur. Testler, sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder. Bu testler sonrası saptanan açıklık ve bulgular, Kapsam bölümünde belirtilen ve ilişkili olduğu her bir başlık altında ayrıntılı olarak incelenerek raporlanır. Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklık ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilir ve bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgular da raporlanır. Bulgular, **"Bulgu Önem Dereceleri"** bölümünde yer verilen dereceler kullanılarak **"Bulgu Formatı"** bölümünde tariflenen formata uygun olacak şekilde sunulur. Bu kapsamda bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmaz. Varlık değerlendirmesi yapmak ve varlıkların önem derecelerine göre aksiyon almak Kurum, Kuruluş ve Ortaklıkların sorumluluğundadır. Sızma testleri gerçekleştirilirken, Kurum, Kuruluş ve Ortaklıklar faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol açabilecek tüm testler Kurum, Kuruluş ve Ortaklıklar ile koordineli bir şekilde planlanarak gerçekleştirilir.

a. Testlerin Gerçekleştirileceği Erişim Noktaları

Sızma testlerinin gerçekleştirileceği asgari erişim noktaları aşağıda tanımlanmaktadır. Bu noktalardan sisteme erişildikten sonra, sızma testleri gerçekleştirilir.

i. İnternet: Kurum, Kuruluş ve Ortaklıkların internet üzerinden erişilebilen tüm sunucu ve servislerine İnternet üzerinden erişilerek sızma testleri gerçekleştirilir ve devamında ve detaylı sızma testleri uygulanır.

ii. Kurum, Kuruluş ve Ortaklıklar iç ağı: Kurum, Kuruluş ve Ortaklıkların iç ağında yer alan ve test kapsamında ele alınan sunuculara Kurum, Kuruluş ve Ortaklıklar iç ağı üzerinden erişilerek sızma testleri gerçekleştirilir. Ağ ve ağ trafiği üzerinde gerçekleştirilecek testler için de bu ağ kullanılır ve testi gerçekleştirecek şahıslara kullanımı en yaygın olan çalışan bilgisayarı profilinde bilgisayarlar sağlanır.

b. Testlerin Gerçekleştirileceği Kullanıcı Profilleri

Sızma testlerinin sağlıklı bir şekilde gerçekleştirilebilmesi ve testlerin gerçek hayata uygun olması için, yukarıda tanımlanan erişim noktalarına bu ortamların doğasına uyacak şekilde aşağıdaki kullanıcı profilleri ile sızma testleri gerçekleştirilir.

i. Anonim kullanıcı profili: İnternet üzerinden, Kurum, Kuruluş ve Ortaklıkların web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Kurum, Kuruluş ve Ortaklıklara ait web uygulamalarının üyesi olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

ii. Kurum, Kuruluş ve Ortaklıklar müşterisi profili: İnternet üzerinden, Kurum, Kuruluş ve Ortaklıklar'ın web servislerine erişebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. İnternet üzerinde Kurum, Kuruluş ve Ortaklıklara ait web uygulamalarının üyesi olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

iii. Kurum, Kuruluş ve Ortaklıklar çalışanı profili: Kurum, Kuruluş ve Ortaklıklar personelinin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır. Kurum, Kuruluş ve Ortaklıklar çalışanı profili ile gerçekleştirilecek testlerde, Kurum, Kuruluş ve

Ortaklıklarda çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici(local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilir. Kurum, Kuruluş ve Ortaklıklar çalışanı profili ile yapılan testlerde, testi yapan kişi/kuruluşa Kurum, Kuruluş ve Ortaklıklar tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilmelidir.

iv. Diğer kullanıcı profilleri: Sızma testlerinin, yukarıda tanımlanan diğer dört kullanıcı profiline uymayan bir kullanıcı profili ile gerçekleştirilmesi durumunda, kullanılan her bir profil için tanımlanan hak ve yetkiler bu başlık altında açıkça ifade edilir.

c. *Sistem Tespiti, Servis Tespiti ve Açıklık Taraması*

Sızma testleri aşağıda tanımlanan sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar. Sistem tespiti, servis tespiti ve açıklık taraması/araştırması tüm bilgi sistemi varlıklarına uygulanır.

i. Sistem tespiti: Sunucu veya aktif/pasif ağ cihazlarının sistem/yapılandırma bilgilerinin tespit edilmeye çalışıldığı adımdır.

ii. Servis tespiti: Kurum, Kuruluş ve Ortaklıklar bilgi sistemlerinde yer alan varlıkların port taramasının gerçekleştirildiği ve dış dünyaya/genel erişime açık olan portların sunduğu servislerin tespit edilmeye çalışıldığı adımdır.

iii. Açıklık taraması/araştırması: Kurum, Kuruluş ve Ortaklıkların bileşenleri ve bu bileşenlerin sunduğu servislerin açıklık tarayıcıları ile güncel açıklıklara karşı tarandığı ve muhtemel güvenlik açıklıklarının belirlenmeye çalışıldığı adımdır. Bu adımda ayrıca, tespit edilen muhtemel açıklıklar için açıklık veritabanları gibi kaynaklar kullanılarak bu açıklıkların bileşenlere ve bileşenlerin etkileşimde olduğu sistemlere güvenlik açısından etkileri araştırılır.

d. *Sızma Testleri*

i. İnternet üzerinden gerçekleştirilecek temel sızma testleri: Kurum, Kuruluş ve Ortaklıklar ağından bağımsız bir lokasyondan, Kurum, Kuruluş ve Ortaklıklar'ın internet üzerinde sahip olduğu IP ağı taranarak sistem tespiti, servis tespiti ve açıklık taraması adımları gerçekleştirilir.

ii. Kurum, Kuruluş ve Ortaklıklar iç ağından gerçekleştirilecek sızma testleri: Kurum, Kuruluş ve Ortaklıkların iç ağında sistem tespiti, servis tespiti ve açıklık taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:

- Kurum yerel ağ haritası tespiti
- Belirlenen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin gerçekleştirilmesi
- Yerel alan ağı içerisinde zafiyet taraması yapılması
- Kurum yerel ağında araya girme teknikleri ile hassasiyet derecesi yüksek bilgilerin elde edilmeye çalışılması
- Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırılarının gerçekleştirilmesi
- Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılması

4) Sızma Testi Sonuçlarının Takibi

Kurum, Kuruluş ve Ortaklıklar, sızma testleri sonucu tespit edilen bulguları, bulguların önem derecelerini, birlikte oluşturabilecekleri riskleri, tespit edildiği varlıkların değerini ve sızma testi raporlarında yer alan önerileri dikkate alarak, Kurum, Kuruluş ve Ortaklıklar yönetim kurullarınca onaylanan ve bu bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planı çerçevesinde takip eder. Sızma testleri sonucu ortaya çıkan tespitler, gerekli görülmesi halinde Kurum, Kuruluş ve Ortaklıkların teftiş kurullarının iç denetim planına da dâhil edilir. Sızma testi raporları, tamamlanmasını müteakip bir ay içinde Kurula gönderilir.

Bulgu Önem Dereceleri

Bulgu önem dereceleri beş kategoride ele alınır. Acil, kritik, yüksek, orta ve düşük şeklinde olan bu kategorilere ilişkin açıklamalar aşağıda yer almaktadır:

Önem Derecesi	Açıklama
Acil	Niteliksiz saldırgan tarafından Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Kritik	Nitelikli saldırgan tarafından Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Yüksek	Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklıklardır.

Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

Bulgu Formatı

Kapsam bölümünde belirtilen başlıkların her biri altında raporlanacak bulguların sunuluş biçimi aşağıda yer almaktadır:

Bulgu Referans No	**Rapordaki her bulguyu tekil olarak niteleyen harf/rakam dizisi**
Bulgu Adı	Bulguyu özet olarak ifade eden tanımlayıcı isim
Önem Derecesi	Bulgunun, EK-1'de yer verilen önem derecesi
Etkisi	Bulguda yer verilen açıklığın/eksikliğin kötüye kullanılması durumunda oluşabilecek potansiyel sonuç
Erişim Noktası	"3.a Testlerin Gerçekleştirileceği Erişim Noktaları" bölümünde yer verilen testin gerçekleştirildiği erişim noktası
Kullanıcı Profili	"3.b Testlerin Gerçekleştirileceği Kullanıcı Profilleri" bölümünde yer verilen testin gerçekleştirildiği kullanıcı profili
Bulgunun Tespit Edildiği Bileşen/Bileşenler1	Bulgunun tespit edildiği bileşeni niteleyen IP Numarası, URL, Sistem, Servis, Sunucu veya Varlık adı gibi bilgiler
Bulgu Açıklaması	Bulgunun detaylı açıklaması
Çözüm Önerisi	Bulgunun giderilmesi için testi gerçekleştiren kuruluş tarafından yapılacak çözüm önerisi