KKTC MERKEZ BANKASI

SIZMA TESTLERİ GENELGESİ

(Genelge No: 2015/01)

Mart-2015

BANKACILIK DÜZENLEME VE GÖZETİM MÜDÜRLÜĞÜ

İçindekiler

SIZMA TESTLERİ GENELGESİ

(Genelge No: 2015/01)

Giriş

İşbu Genelge 39/2001 Sayılı Bankalar Yasasının 15'inci maddesinin (3)'üncü fıkrası altında 18 Aralık 2014 tarih ve 258 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren "Bankalarda İç Denetim, Risk Yönetimi, İç Kontrol ve Yönetim Sistemleri Tebliği'nin" 11'inci maddesinin (3)'üncü fıkrası (E) bendi (a) alt bendi uyarınca düzenlenmiş olup, Bankamız Yönetim Kurulunun 30 Mart 2015 tarih ve 902 sayılı kararı ile onaylanmıştır. 2015/01 sayılı Genelge 8 Nisan 2015 tarihinde yürürlüğe girer.

1 Amaç

Sızma (Penetrasyon) Testi, bankaların bilgi sistemlerini oluşturan altyapı, donanım, yazılım ve uygulamalara bir saldırganın izlemesi öngörülen yöntemler kullanılarak yapılan saldırı ve müdahaleler sonucunda güvenlik açıklarının tespit edilip bu zafiyetlerin kullanılarak sistemlere sızılmaya çalışılması, bu açıkların nelere sebep olabileceğinin incelenmesi ve sonuçların raporlanmasıdır.

Sızma testlerinin amacı, banka bilgi sistemlerinde yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilmesi ve düzeltilmesidir.

2 Kapsam

Sızma testleri, temel sızma testleri ile bu testler sonrası uygulanacak detaylı sızma testlerinden oluşur. Sızma testleri kapsamında gerçekleştirilecek testler asgari olarak aşağıdaki başlıkları kapsamalıdır:

a) İletişim Altyapısı ve Aktif Cihazlar

b) DNS (Domain Name System) 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) ATM (Automated Teller Machine) Sistemleri

h) Sosyal Mühendislik Testleri

Bankalar, isteğe bağlı olarak yukarıdaki konulara ek olarak Dağıtık Servis Dışı Bırakma Testlerini de kapsam dâhiline alabilirler.

3 Metodoloji

Sızma testleri, aşağıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek temel sızma testleri ve detaylı sızma testlerinden oluşur.

Temel sızma testleri: Sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder.

Detaylı sızma testleri: Temel sızma testleri sonrası saptanan açıklık ve bulgular, bu dokümanın "Kapsam" bölümünde belirtilen ve ilişkili olduğu her bir başlık altında, detaylı sızma testlerinin gerçekleştirilmesi suretiyle 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, Ek-1'de yer verilen bulgu önem dereceleri kullanılarak Ek-2'de yer verilen bulgu formatına uygun olacak şekilde ilgili testi yapan kuruluş tarafından testi yaptıran bankaya sunulur. Bu kapsamda bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmaz. Varlık değerlendirmesi yapmak ve varlıkların önem derecelerine göre aksiyon almak bankaların sorumluluğundadır.

Sızma testleri gerçekleştirilirken, banka faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol açabilecek tüm testler banka ile koordine edilerek planlı bir şekilde gerçekleştirilir.

3.1 Testlerin Gerçekleştirileceği Erişim Noktaları

Sızma testlerinin gerçekleştirileceği asgari erişim noktaları aşağıda tanımlanmaktadır. Bu noktalardan sisteme erişildikten sonra, temel sızma testleri gerçekleştirilmeli ve sonrasında detaylı sızma testleri uygulanmalıdır.

i. İnternet: Bankanın internet üzerinden erişilebilen tüm sunucu ve servislerine internet üzerinden erişilerek sızma testleri gerçekleştirilir.

ii. Banka iç ağı: Bankanın iç ağında yer alan ve test kapsamında ele alınan sunuculara banka 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 profilindeki bilgisayarlar sağlanır.

iii. Şube ağı: Bankanın yönlendirmesi ile belirlenecek ve ülkemizde bulunan en az bir şubenin sahip olduğu ağ altyapısına erişim sağlanarak bu şubede bulunan sistemler, ağ altyapısı, ağ trafiği ve şube üzerinden erişilebilen

diğer sistemler sızma testlerine tabi tutulur. Testi gerçekleştirecek şahıslara, şube çalışanlarının kullanmış olduğu bilgisayarlar ile aynı profilde bilgisayarlar sağlanır.

3.2 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, bankanın web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Bankaya 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. Banka müşterisi profili: İnternet üzerinden, bankanın web servislerine erişebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. İnternet üzerinde bankaya 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. Banka misafiri profili: Bankayı ziyaret eden kişilerin misafir ağında oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

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

v. Diğer kullanıcı profilleri: Sızma testlerinin, yukarıda tanımlanan diğer kullanıcı profillerine uymayan bir kullanıcı profili ile gerçekleştirilir. Kullanılan her bir profil için tanımlanan hak ve yetkiler bu başlık altında açıkça ifade edilir.

3.3 Sistem Tespiti, Servis Tespiti ve Açıklık Taraması

Temel 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: Banka 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: Bankanın 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 veri tabanları gibi kaynaklar kullanılarak bu açıklıkların bileşenlere ve bileşenlerin etkileşimde olduğu sistemlere güvenlik açısından, etkileri araştırılır.

3.4 Temel Sızma Testleri

i. İnternet üzerinden gerçekleştirilecek temel sızma testleri: Banka ağından bağımsız bir konumdan, bankanın internet üzerinde sahip olduğu IP-Internet Protocol ağı taranarak sistem tespiti, servis tespiti ve açıklık taraması adımları gerçekleştirilir.

ii. Banka iç ağından gerçekleştirilecek temel sızma testleri: Bankanın iç ağında sistem tespiti, servis tespiti ve açıklık taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:

- Banka 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,
- Banka yerel ağında araya girme teknikleri ile hassas 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,

iii. Banka şube ağından gerçekleştirilecek temel sızma testleri: Bankanın şube ağında sistem tespiti, servis tespiti ve açıklık taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:

- Şube yerel ağ haritasının tespiti,
- Şube yerel alan ağında zafiyet taraması yapılması,
- Şube yerel ağında araya girme teknikleri ile hassas bilgilerin elde edilmeye çalışılması,
- Ağ altyapısında bulunan aktif cihazların testlerinin gerçekleştirilmesi,
- Şube personelinin bilgisayarı üzerinden oluşturulabilecek tehditlerin incelenmesi,
- Elde edilen bilgiler ışığında şube ağından erişilebilen diğer sunucu ve sistemlere yönelik ele geçirme saldırılarının gerçekleştirilmesi.

3.5 Detaylı Sızma Testleri

Temel sızma testlerinin tamamlanması sonrası, "Kapsam" bölümünde belirtilen başlıkların her biri için detaylı sızma testleri gerçekleştirilir.

4 Sızma Testlerini Gerçekleştirecek Kuruluşların Seçimi

Sızma testleri dış hizmet alımı şeklinde bilgi güvenliği ve sızma testleri konusunda uzman çalışanları bulunan kuruluşlardan alınmalıdır. Sızma testini yapacak olan kişilerin ilgili kuruluşun kendi çalışanı olması gereklidir.

Banka, teste başlamadan önce sızma testini gerçekleştirecek kuruluş ile mutlaka **'Gizlilik Sözleşmesi'** imzalamak zorundadır. Eğer, teklif esnasında gizli niteliğinde olan bilgilerin paylaşımı söz konusu olacaksa, Gizlilik Sözleşmesinin teklif alınmadan önce yapılması gerekmektedir.

Banka, sızma testlerine başlamadan önce ilgili kuruluştan asgari aşağıdaki belgeleri temin etmelidir:

- Sızma testi yapacak olan kişilerin kuruluş çalışanı olduğunu gösteren belge,
- Sızma testinde görev alacak olan çalışanlarının özgeçmişleri ve sahip oldukları sertifikaları,
- Kuruluşun bilgi güvenliği ile ilgili sahip olduğu sertifikalar,
- Kuruluşun bilgi güvenliği ile ilgili üye olduğu kuruluşlar,
- Kuruluşun bilgi güvenliği hizmetleri ile ilgili kurumsal referansları,
- Kuruluşun "Kapsam" bölümündeki her bir başlığın sızma testleri sırasında kullanacağı uluslararası standartlar,
- Kuruluşun test sırasında kullanacağı araçların isimleri.

Banka, sızma testlerini hangi kuruluşa yaptıracağına politikasını ve mevzuatı çerçevesinde belirler. Bu konuda **tüm sorumluluk banka yönetimine aittir**.

5 Sızma Testi Sonuçlarının Takibi

Sızma testi sonucunda testi yapan kuruluş tarafından bankaya tüm bulguları içeren sonuç raporu teslim edilmelidir. Banka, sonuç raporu tarihinden itibaren en geç yedi iş günü içerisinde, yapılan sızma testi ile ilgili özet bilgileri içeren Ek-3'teki Sızma Testi Sonuç Bildirim Formu'nu doldurarak bir kapak yazısı ile birlikte Merkez Bankasına hem matbu hem de elektronik ortamda bildirmelidir.

Banka, sızma testleri sonucu tespit edilen bulguların en kısa sürede giderilmesini hedefleyen bir 'Aksiyon Planı' hazırlamalıdır. Söz konusu Aksiyon Planı için Ek-4'deki 'Sızma Testi Sonuçları Aksiyon Planı Bildirim Formu' kullanılmalı, ilgili formdaki Bulgu Takip Çizelgesi'ne "Acil", "Kritik" ve "Yüksek" önem derecesine sahip bulguların bilgileri yazılmalı ve Yönetim Kurulu tarafından onaylanarak her çeyrek sonunda Merkez Bankasına hem matbu hem de elektronik ortamda bildirilmelidir. "Orta" ve "Düşük" önem derecesine sahip bulgular Bankanın kendi güvenlik politikasına uygun olarak takip edilmelidir.

Sızma testleri sonucu ortaya çıkan tespitlerin, bankaların iç denetim birimlerinin denetim planına dâhil edilmesi şarttır.

6 Sızma Testini Uygulama Dönemleri

Sızma testleri banka tarafından düzenli olarak on iki ayda en az bir defa yaptırılmalıdır. Ayrıca bankanın yeni hizmete girecek olan sistem ve uygulamalar için işletime alma öncesinde sızma testleri yaptırması şarttır.

Ek-1: 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 banka dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Kritik:	Nitelikli saldırgan tarafından banka dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Yüksek:	Banka 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 teknik yazındaki (literatürdeki) en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

Ek-2: Bulgu Formatı

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

Bulgu Referans No:		Rapordaki her bulguya tekil olarak niteleyen harf/rakam dizisi
Bulgu Adı:		Bulguyu özet olarak ifade eden tanımlayıcı isim.
Önem Derecesi:		Bulgunun önem derecesi.
Etkisi:		Bulguda yer verilen açıklığın/eksikliğin kötüye kullanılması durumunda oluşabilecek potansiyel sonuç.
Erişim Noktası:		"Testlerin Gerçekleştirileceği Erişim Noktaları" bölümünde yer verilen testin gerçekleştirildiği erişim noktası.
Kullanıcı Profili:		"Testlerin Gerçekleştirileceği Kullanıcı Profilleri" bölümünde yer verilen testin gerçekleştirildiği kullanıcı profili.
Bulgunun Tespit Edildiği Bileşen/Bileşenler:		Bulgunun tespit edildiği bileşeni niteleyen IP (Internet Protocol) Numarası, URL (Uniform Resource Locator), 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.

Not: Kapsam bölümünde belirtilen her bir başlık altında aynı bulgunun aynı önem derecesi ile birden fazla bileşende tespit edilmesi durumunda, yeni bulgu referansı verilmeden bulgunun tespit edildiği tüm bileşenler aynı bulgu altında sıralanır.

Ek-3: Sızma Testi Sonuç Bildirim Formu

<table>
<tr><th colspan="2">SIZMA TESTİ SONUÇ BİLDİRİM FORMU</th></tr>
<tr><td>Banka Adı:</td><td></td></tr>
<tr><td>Bankanın Sızma Testi Baş Sorumlusu:</td><td></td></tr>
<tr><td>Sızma Testinin Ait Olduğu Takvim Yılı:</td><td></td></tr>
<tr><td>Sızma Testini Yapan Kuruluşun Unvanı:</td><td></td></tr>
<tr><td>Kuruluşun Sızma Testi Baş Sorumlusu:</td><td></td></tr>
<tr><td>Kuruluşun Sızma Testinde Görev Alan Çalışanları:</td><td></td></tr>
<tr><td>Sızma Testi Sonuç Raporu Tarihi:</td><td></td></tr>
<tr><td>Önem Derecesine Göre Bulgu Sayıları:</td><td>
<table>
<tr><td>Acil:</td><td></td></tr>
<tr><td>Kritik:</td><td></td></tr>
<tr><td>Yüksek:</td><td></td></tr>
<tr><td>Orta:</td><td></td></tr>
<tr><td>Düşük:</td><td></td></tr>
</table>
</td></tr>
</table>

Form ile ilgili açıklamalar:

- Kuruluşun Sızma Testi Baş Sorumlusu: Kuruluşun sızma testi için belirlediği esas sorumlu kişinin (proje yöneticisi, koordinatör, vb.) adı soyadı ve kimlik numarası.
- Kuruluşun Sızma Testinde Görev Alan Çalışanları: Sızma testi sırasında görev alan kuruluş çalışanlarının adı soyadı ve kimlik numaraları.
- Önem Derecesine Göre Bulgu Sayıları: Sızma testi raporunda bulunan bulguların önem derecelerine göre toplam sayıları.
- Bankanın Sızma Testi Baş Sorumlusu: Bankanın en az genel müdür yardımcısı düzeyinde olan esas sorumlu yöneticisinin belirlenerek adı soyadı ve kimlik numarası.
- Formu biri en az genel müdür yardımcısı olmak şartıyla, iki konuyla yetkili kişinin açık isim belirtmek şartıyla bankayı temsil edecek şekilde imzalaması gerekmektedir.

Ek-4: Sızma Testi Sonuçları Aksiyon Planı Bildirim Formu

Yüksek, Kritik ve Acil önem derecesine sahip bulgular için doldurulacak olan bildirim formu aşağıdadır:

SIZMA TESTİ SONUÇLARI AKSİYON PLANI BİLDİRİM FORMU		
Sızma Testi Sonuç Raporu Tarihi:		
Aksiyon Planı Dönemi:		
Yönetim Kurulu Onay Tarihi:		
Yönetim Kurulu Onay Sayısı:		
Dönem Sonu İtibarıyla Bir Önceki Döneme Göre Tam Olarak Giderilen Bulgu Sayıları (Önem Derecesine Göre):	**Acil:**	
	Kritik:	
	Yüksek:	
Dönem Sonu İtibarıyla Tam Olarak Giderilemeyen Bulgu Sayıları (Önem Derecesine Göre):	**Acil:**	
	Kritik:	
	Yüksek:	

BULGU TAKİP ÇİZELGESİ

Bulgu Referans Numarası	Bulgu Adı	Önem Derecesi	Planlanan / Alınan Tedbirler	Planlanan / Gerçekleşen Başlangıç Tarihi	Planlanan / Gerçekleşen Bitiş Tarihi	Durumu

Form ile ilgili açıklamalar:

- Aksiyon Planı Dönemi: Planın hangi yıl ve kaçıncı çeyreğe ait olduğu bilgisi. Örnek 2015-1
- Yönetim Kurulu Onay Tarihi: Banka Yönetim Kurulu'nun Aksiyon Planı'nı onayladığı kararın tarihi.
- Yönetim Kurulu Onay Sayısı: Banka Yönetim Kurulu'nun Aksiyon Planı'nı onayladığı kararın sayı numarası.
- Formu biri en az genel müdür yardımcısı olmak şartıyla, iki konuyla yetkili kişinin açık isim belirtmek şartıyla bankayı temsil edecek şekilde imzalaması gerekmektedir.

Bulgu Takip Çizelgesi sütun açıklamaları:

- Bulgu Referans Numarası: Sızma testi sonuç raporundaki kuruluş tarafından belirlenen orijinal 'Bulgu Referans No' alanı.
- Planlanan/Alınan Tedbirler: Bulgunun giderilmesi amacıyla durumuna bağlı olarak alınması planlanan veya alınan tedbirler.
- Planlanan/Gerçekleşen Başlangıç Tarihi: Bulgunun giderilmesi amacıyla durumuna bağlı olarak planlanan veya gerçekleşen başlangıç tarihi.
- Planlanan/Gerçekleşen Bitiş Tarihi: Bulgunun giderilmesi amacıyla durumuna bağlı olarak planlanan veya gerçekleşen bitiş tarihi.
- Durumu: "Planlandı", "Devam Ediyor" veya "Tamamlandı" kelimelerinden uygun olanı.