BANKACILIK DÜZENLEME VE DENETLEME KURUMU
(Bilgi Yönetimi Dairesi)

Sayı: B.02.1.BDK.0.77.00.00/010.06.02-1 24.07.2012

Konu: Bilgi Sistemlerine İlişkin Sızma Testleri

GENELGE
BSD.2012/1

"Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" (Tebliğ) ile banka bilgi sistemlerinin maruz kalabileceği risklerin ve güvenlik açıklarının yönetimini de kapsayacak şekilde, bankaların faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetiminde esas alınacak asgari usul ve esaslar düzenlenmiştir.

Tebliğ'in "Bilgi Sistemlerine İlişkin Risk Yönetimi" başlıklı ikinci kısım birinci bölümünün "Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi" başlıklı 7 nci maddesinin üçüncü fıkrası (ç) bendinde ifade edilen

> *"Bilgi sistemlerinin güvenilirliğinin ve tutarlılığının düzenli olarak incelenmesini sağlayacak süreçler tesis edilir. Bu çerçevede güvenlik ile ilgili hükümlerin gereklerinin yerine getirilmesi hususunda herhangi bir icrai görevi bulunmayan bağımsız ekiplere düzenli aralıklarla sızma testleri yaptırılır. Güvenlik alanındaki güncel gelişmeler ve yeni açıklar takip edilir, gerekli yazılım güncellemeleri yapılır, gerekli yamalar uygulanır."*

hükmü ile sızma testleri bankacılık sektörü için zorunlu hale getirilmiştir.

Bilgi sistemlerine yönelik olarak elektronik ortamda gerçekleştirilebilecek saldırı türlerinin de hızlı bir değişim ve gelişim göstermesi nedeniyle 27.01.2011 tarih ve 4022 sayılı Bankacılık Düzenleme ve Denetleme Kurulu Kararı ile Tebliğ'in söz konusu 7 nci maddesinin üçüncü fıkrasının (ç) bendinde yer alan hüküm ile zorunlu kılınan ve düzenli aralıklarla yapılması istenilen sızma testinin sıklığının yılda en az bir defa yapılması şeklinde belirlenmesine karar verilmiştir.

Tebliğ'in 7 nci maddesinin üçüncü fıkrasının (ç) bendi uyarınca, 2012 yılından itibaren sızma testlerinin yaptırılmasında işbu Genelge ile çerçevesi çizilen usul ve esaslar dikkate alınır.

1) Amaç

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.

Atatürk Bulvarı No:191 Kavaklıdere 06680 ANKARA Tel: (312) 455 67 80 Faks: (312) 424 17 49
İnternet adresi: www.bddk.org.tr

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 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) ATM Sistemleri
h) Dağıtık Servis Dışı Bırakma Testleri
i) Sosyal Mühendislik Testleri

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. Temel sızma testleri sonrası saptanan açıklık ve bulgular, 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 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 koordineli bir şekilde planlanarak 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 İnternet 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 bilgisayarı profilinde bilgisayarlar sağlanır.

iii. **Şube ağı:** Bankanın yönlendirmesi ile belirlenecek bir şubenin sahip olduğu ağ altyapısına erişim sağlanarak bu şubede bulunan sistemler, ağ altyapısı, ağ

Atatürk Bulvarı No:191 Kavaklıdere 06680 ANKARA Tel: (312) 455 67 80 Faks: (312) 424 17 49
İnternet adresi: www.bddk.org.tr

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 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. **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 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.

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

Atatürk Bulvarı No:191 Kavaklıdere 06680 ANKARA Tel: (312) 455 67 80 Faks: (312) 424 17 49
İnternet adresi: www.bddk.org.tr

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.

3.4) Temel Sızma Testleri

i. **İnternet üzerinden gerçekleştirilecek temel sızma testleri:** Banka ağından bağımsız bir lokasyondan, bankanın internet üzerinde sahip olduğu IP 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:

- 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 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 gerçekleştirilmelisi
- 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. Detaylı sızma testlerine ilişkin usul ve esasları belirlemeye Bilgi Yönetimi Daire Başkanlığının bağlı olduğu Başkan Yardımcılığı yetkilidir.

Atatürk Bulvarı No:191 Kavaklıdere 06680 ANKARA Tel: (312) 455 67 80 Faks: (312) 424 17 49
İnternet adresi: www.bddk.org.tr

4) Sızma Testlerini Gerçekleştirilecek Kuruluşların Seçimi

Sızma testlerinin bir dış hizmet şeklinde alınması durumunda, sızma testi kuruluşlarının seçiminde ve bu kuruluşlar ile bankalar arasında imzalanacak sözleşmelerde Tebliğ'in "Bilgi Sistemlerine İlişkin Destek Hizmeti Alımı Sürecinin Yönetimi" başlıklı 8 inci maddesinde yer alan hükümler dikkate alınır.

5) Sızma Testi Sonuçlarının Takibi

Bankalar, 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, banka yönetim kurullarınca onaylanan ve bu bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planı çerçevesinde takip eder. Sızma testleri sonucu ortaya çıkan tespitler, aynı zamanda bankaların teftiş kurullarının iç denetim planına da dâhil edilir. Sızma testi raporları, tamamlanmasını müteakip bir ay içinde, elektronik ortamda, 17/02/2010 tarih ve BSD.2010/1 sayılı Genelgede tanımlanan Bağımsız Denetim Takip Sistemine(BADES) yüklenir. Bu kapsamda gerek duyulacak hususlara ilişkin ilave açıklamalar Bilgi Yönetimi Daire Başkanlığı tarafından yapılır.

Tebliğ olunur.

Mukim ÖZTEKİN
Başkan

EKLER:
1- Bulgu Önem Dereceleri(1 sayfa)
2- Bulgu Formatı(1 sayfa)

Atatürk Bulvarı No:191 Kavaklıdere 06680 ANKARA Tel: (312) 455 67 80 Faks: (312) 424 17 49
İnternet adresi: www.bddk.org.tr

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 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 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	*"3.1 Testlerin Gerçekleştirileceği Erişim Noktaları" bölümünde yer verilen testin gerçekleştirildiği erişim noktası*
Kullanıcı Profili	*"3.2 Testlerin Gerçekleştirileceği Kullanıcı Profilleri" bölümünde yer verilen testin gerçekleştirildiği kullanıcı profili*
Bulgunun Tespit Edildiği Bileşen/Bileşenler[1]	*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*

[1] *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.*