EK-1

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Olumlu Görüş

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ..... A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

[Bağımsız denetim kuruluşuGörüşü]

Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin

Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-2

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Şartlı Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ..... A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Bağımsız denetim faaliyetine getirilen sınırlandırma ve bu nedenle denetlenemeyen süreçler, uygulamalar, kontroller; denetlenenin bilgi sistemleri üzerinde tespit edilen önemli kontrol eksiklikleri ve bu kontrol eksikliklerinin denetlenenin bilgi sistemlerinin bütününü veya büyük bir kısmını etkilememesine ilişkin görüşüne esas neden ve gerekçeler)

[Bağımsız denetim kuruluşuGörüşü]
Görüşümüze göre, yukarıda *(....ncı paragrafta)* açıklanan *husus(lar) nedeniyle,* denetlenenin bilgi sistemleri üzerinde bu *hususun/hususların* muhtemel etkileri haricinde bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin

Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-3

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Olumsuz Görüş

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ..... A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetlenenin bilgi sistemleri üzerindeki kontrollerin etkin, yeterli veya uyumlu bulunmama sebepleri)

[Bağımsız denetim kuruluşuGörüşü]

Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmemiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin

Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-4

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Görüşten Kaçınma

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ..... A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetçinin görüş bildirmemesinin nedenleri)

[Bağımsız denetim kuruluşuGörüşü]

Yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle ..... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde tesis edilen kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş bildirmiyoruz.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin

Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-5

Bilgi Sistemleri Sızma Testleri Usul ve Esasları

1) AMAÇ

Sızma testlerinin amacı, kuruluş bilgi sistemlerinde gizlilik, bütünlük ve erişilebilirlik açısından güvenlik açıklarının istismar edilmeden önce 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
d) E-posta Servisleri
e) Veritabanı Sistemleri
f) Web Uygulamaları
g) Mobil Uygulamalar
h) Bulut Sistemleri
i) Kablosuz Ağ Sistemleri
j) ATM, kiosk, vb. istemleri
k) Dağıtık Servis Dışı Bırakma (DDoS) Testleri
l) Sosyal Mühendislik Testleri

3) METODOLOJİ

Sızma testleri, aşağıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek testlerden oluşur. Testler, sistem tespiti, servis tespiti ve zafiyet taraması/araştırması adımları ile başlar ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder. Bu testler sonucunda saptanan açıklar ve bulgular, Kapsam bölümünde belirtilen ilişkili her bir başlık altında ayrıntılı olarak incelenerek raporlanır. Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklar ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklar açısından da değerlendirilir ve bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklar ve bulgular da raporlanır. Bulgular, "**Bulgu Önem Dereceleri**" bölümünde yer verilen bulgu önem dereceleri 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 kuruluşların sorumluluğundadır.

Sızma testleri gerçekleştirilirken, kuruluş faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol açabilecek tüm testler kuruluş 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**: Kuruluşun internet üzerinden erişilebilen tüm sunucu ve servislerine İnternet üzerinden erişilerek sızma testleri gerçekleştirilir.
ii. **Kuruluş iç ağı**: Kuruluşun iç ağında yer alan ve test kapsamında ele alınan sunuculara kuruluş 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**: Kuruluş şube kullanıyorsa, kuruluşun yönlendirmesi ile belirlenecek 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.
iv. **Temsilci bağlantısı**: Kuruluş temsilci kullanıyorsa, kuruluşun yönlendirmesi ile belirlenecek bir temsilciye bağlantı sağlanarak bu temsilcinin kuruluşa bağlantıda kullandığı giriş noktaları sızma testlerine tabi tutulur. Testi gerçekleştirecek şahıslara, temsilcinin bağlantıda kullandığı aynı profilde ortam sağlanır.
v. **Dış hizmet sağlayıcının bağlantısı:** Dış hizmet sağlayıcının kuruluşun bilgi sistemlerine uzaktan bağlantıda kullandığı giriş noktaları sızma testine tabi tutulur. Testi gerçekleştirecek şahıslara, dış hizmet sağlayıcının bağlantıda kullandığı aynı profilde ortam 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, kuruluşun web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Kuruluşa 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. **Kuruluş müşterisi profili**: İnternet üzerinden, Kuruluşun web servislerine erişebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. İnternet üzerinde kuruluşa 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. **Kuruluş misafiri profili**: Kuruluşu ziyaret eden kişilerin misafir ağında oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
iv. **Kuruluş personel profili**: Kuruluş 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. Kuruluş personeli profili ile gerçekleştirilecek testlerde, kuruluş çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici (*ing.* local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilir. Kuruluş personeli profili ile yapılan testlerde, testi yapan kişi/kuruluşa kuruluş 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.

c) Sistem Tespiti, Servis Tespiti ve Açıklık Taraması

Sızma testleri aşağıda tanımlanan sistem tespiti, servis tespiti ve zafiyet taraması/araştırması adımları ile başlar. Sistem tespiti, servis tespiti ve zafiyet 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**: Kuruluş bilgi sistemlerinde yer alan varlıkların port taramasının gerçekleştirildiği ve dış dünyaya/genel erişime açık olan portların sunduğu servislerin tespit edilmeye çalışıldığı adımdır.
iii. **Zafiyet taraması/araştırması**: Kuruluşun bilgi sistemleri unsurları ve bunların sunduğu servislerin zafiyet tarayıcıları ile güncel açıklara karşı tarandığı ve muhtemel güvenlik açıklarının belirlenmeye çalışıldığı adımdır. Bu adımda ayrıca, tespit edilen muhtemel açıklar için güvenlik açıkları veritabanları gibi kaynaklar kullanılarak bu açıkların bilgi sistemleri unsurlarına ve bu unsurların etkileşimde olduğu sistemlere güvenlik açısından etkileri araştırılır.

d) Sızma Testleri

i. **İnternet üzerinden gerçekleştirilecek sızma testleri**: Kuruluş ağından bağımsız bir yerleşkeden, kuruluşun internet üzerinde sahip olduğu IP ağı taranarak sistem tespiti, servis tespiti ve zafiyet taraması adımları gerçekleştirilir.
ii. **Kuruluş iç ağından gerçekleştirilecek sızma testleri:** Kuruluşun iç ağında sistem tespiti, servis tespiti ve zafiyet taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:
   - Kuruluş 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
   - Kuruluş 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. **Kuruluş şube ağından gerçekleştirilecek sızma testleri:** Kuruluş, şube kullanıyorsa, şube ağında sistem tespiti, servis tespiti ve zafiyet 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

iv. **Temsilcinin bağlantısında gerçekleştirilecek sızma testleri:** Temsilcinin kuruluşa gerçekleştirdiği bağlantı ve giriş noktalarından kaynaklanabilecek tehditlerin incelenmesi sağlanır.

v. **Dış hizmet sağlayıcının bağlantısında gerçekleştirilecek sızma testleri:** Dış hizmet sağlayıcının kuruluşun bilgi sistemlerine uzaktan erişim için kullandığı bağlantı ve giriş noktalarından kaynaklanabilecek tehditlerin incelenmesi sağlanır.

4) BULGU ÖNEM DERECELERİ

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 gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklardır.
Kritik	Nitelikli saldırgan tarafından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklardır.
Yüksek	Kuruluş 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 açıklardır.
Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

5) BULGU FORMATI

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, *"4. Bulgu Önem Dereceleri"* bölümünde verilen önem derecesi
Etkisi	Bulguda yer verilen açığın/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 Bilgi Sistemi Unsuru/Unsurları	Bulgunun tespit edildiği bilgi sistemleri unsurunu 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