	GÜVENLİK AÇIKLARINI TESPİT ETME PROSEDÜRÜ	Doküman No	PR.011
		Yayın Tarihi	05.05.2023
		Revizyon No	0
		Revizyon Tarihi	0
		Toplam Sayfa Sayısı	5

İÇİNDEKİLER

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

1 AMAÇ

Bu prosedürü amacı; EGE ÜNİVERSİTESİ HASTANESİ sorumluluğunda bulunan bilgi kaynaklarının bütünlüğünü ve gizliliğini sağlamak, firmanın güvenlik politikalarına uyumunu kontrol etmek, sistemlerin güvenlik açıklarını tespit etmek, kullanıcıların veya sistemin aktivitelerini kontrol etmek amacıyla yapılan çalışmalara ilişkin esasları ve adımları tanımlamaktır.

2 KAPSAM

EGE ÜNİVERSİTESİ HASTANESİ içerisinde yapılan güvenlik açıklarını tespit etme faaliyetleri bu prosedür kapsamındadır. Ayrıca güvenlik açıklığına neden olabilecek süreçlerle ilgili iyileştirme kapsamı da bu prosedür kapsamında değerlendirilir.

3 TANIMLAR ve KISALTMALAR

-

4 SORUMLULAR

Bu prosedürün hazırlanmasından BGYS Yönetim Temsilcisi sorumludur. Prosedürün uygulanmasından genel sorumlu BGYS Yönetim Temsilcisidir. Bunun dışında özel olarak sorumluluğu bulunan roller prosedürün uygulama adımlarında verilmiştir.

5 UYGULAMA

EGE ÜNİVERSİTESİ HASTANESİ bünyesinde uygulanan BGYS yönetim sistemi kapsamında genel olarak bilgi güvenliği problemleri gözlemlenmekte ve gerekli durumda aksiyon alınmaktadır.

Ancak sistematik olarak yapılan güvenlik açıklıklarını tespit etme çalışmaları iki başlık altında değerlendirilir.

- Ağ ve Sistem Açıklarını Tespit Etme
- Uygulama Açıklıklarını Tespit Etme

5.1 AĞ VE SİSTEM AÇIKLARINI TESPİT ETME

Ağ ve sistem açıklıklarını tespit etmek amacıyla 1 yılı geçmeyen periyotlarla EGE ÜNİVERSİTESİ HASTANESİ ağ ve sistem altyapısına sızma testi uygulanır. Aynı şekilde uygulamalar içinde projeleri ilk kez devralmadan önce ve yine en fazla 6 ayda bir çalışan uygulama sistemlerinde sızma testleri gerçekleştirilir.

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

Sızma testleri hem iç kaynaklı hem de dış kaynaklı olmalıdır. Firma dışı sızma testleri yılda 1 kapsayıcı şekilde olmalıdır.

Üst yönetimin uygun görmesi durumunda daha sık aralıklarla ve periyodik takvimleri beklemeden sızma testleri yapılabilir.

Sızma testleri, firma dışından bu alanda hizmet sağlayan uzman firma veya kişiler tarafından yapılır.

Sızma testi sürecinde aşağıdaki adımlar izlenir:

- Genel Müdür, BGYS Yöneticisi tarafından veya görevlendirilmiş bir kişi tarafından sızma testini gerçekleştirmek için uzman firma veya kişi(ler) araştırması yapılır.
- Uygun olduğu düşünülen adaylar firmaya davet edilir veya telefon ile iletişim sağlanır.
- Adayların yetkinliklerini değerlendirmek için; referansları, sahip oldukları sertifikalar, eğitim geçmişleri, sektör tecrübeleri gibi parametreler sorgulanır.
- Adaylar veya kurumlar arasından birine karar verilir.
- Sızma testi yapacak firma ve adayı kapsayan bir gizlilik sözleşmesi yapılır.
- Sızma testi yapacak kişi ile test öncesi planlama toplantıları yapılır.
- Sızma testinin kapsamı belirlenir.
- Sızma testi için gerekli bilgi altyapısı sağlanır.

Bu kapsamda ihtiyaç durumuna göre aşağıdaki bilgi ve imkânlar ilgili test uzmanına sağlanabilir:

  - Bilgisayar veya ağ cihazlarına yapılan kullanıcı ve/veya sistem seviyeli erişim bilgileri.
  - Çalışma alanlarına erişim (ofisler, bilgi depolama alanları vs).
  - İletişim ağının trafiğini etkileşimli olarak gözlemleme ve loglama imkanı.

- Sızma testi sürecinde firmanın sunduğu kritik servislerin zarar görmemesi için gerekli tedbirler alınır.
- Sızma testinin zaman planlaması yapılır.
- Belirlenen plan kapsamında sızma testi gerçekleştirilir.
- Test sonunda testi gerçekleştiren kişi tarafından bir rapor hazırlanarak yapılan testin sonuçları Daire Başkanı ve BGYS Yöneticisi'ne sunulur..
- Raporun tespit edilen her bir probleme ilişkin en az aşağıdaki detayları içermesi gerekir:
  - Problem İsmi
  - Problemin Tanımı
  - Problemin Etkisi

- Risk Seviyesi
- Problem Sınıfı (Gizlilik, Bütünlük, Erişilebilirlik)
- Problemi kullanabilecek tehdit noktaları
- Kısa Vadeli Çözüm Yöntemi ve Aksiyonlar (devre dışı bırakma vb.)

- Tespit edilen zafiyetler kapsamında gerekli faaliyetlerin gerçekleştirilmesi BGYS Yöneticisi koordinasyonunda gerçekleştirilir.

5.2 UYGULAMA AÇIKLIKLARINI TESPİT ETME

EGE ÜNİVERSİTESİ HASTANESİ Bilgi İşlem Daire Başkanlığı bünyesinde geliştirilen uygulamalar "Güvenli Yazılım Geliştirme ve Destek Prosedürü" kapsamında geliştirilir. Bu prosedür kapsamında Yazılım Geliştirme Grubu içerisinde yer alan uzman personeller tarafından geliştirme sürecinde güvenlik açıklarını tespit etmek için test ve analizler yapılır.

Eğer dış kaynaklı test hizmeti alınacaksa izlenen süreç, Ağ ve Sistem Açıklarını Tespit Etme süreci ile aynıdır.

Uygulama açıklıklarını tespit etme sürecinde minimum aşağıdaki açıklıkların kontrolü yapılır:

- Yanlış transaction kullanımı
- Biçim kelimesi problemleri
- Sayı taşmaları (Buffer Overflow)
- SQL sokuşturma
- Komut sokuşturma
- Hataların ele alınmaması
- İstisnaların ele alınmaması
- Çapraz site betikleri
- URL bazlı veri girdisi
- Uygunsuz SSL kullanımı
- Zayıf şifre yapıları
- Güvensiz veri saklama
- Veri sızıntısı
- Uygunsuz dosya erişimi (veri kaybı)
- Yetkilendirilmemiş anahtar değişimleri

6 İLGİLİ DOKÜMANLAR

- PR.018 - GÜVENLİ YAZILIM GELİŞTİRME VE DESTEK PROSEDÜRÜ
- FRM.012 GİZLİLİK SÖZLEŞMESİ