RAPORLAMA

NEDEN RAPORLAMA YAPILIR?

Günümüz dünyasında kurumlar kendi bünyelerindeki sistemlere ve ağların dışarıdan veya içerinden gelebilecek siber saldırılara karşı zayıflığını ölçmek, potansiyel tehlike ve tehditleri anlamak ve gerekli önlemleri almak zorundadırlar. Bu sebeple siber saldırı sonrası raporlama siber saldırı yapan beyaz şapkalı hackerlerin en önem verdiği kısımdır.

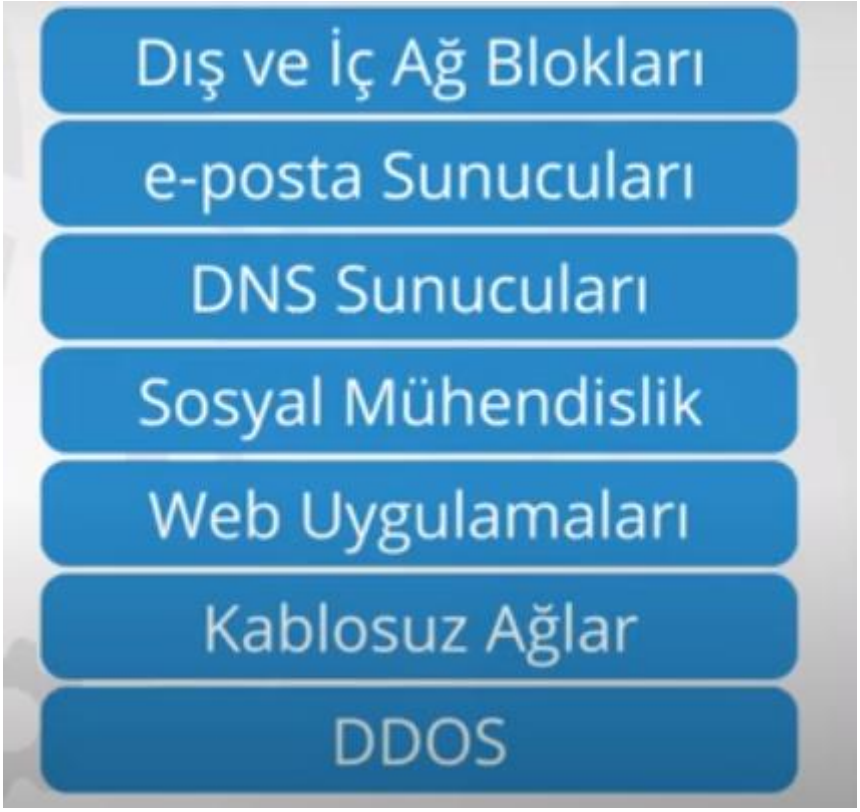
Sızma testi raporlarının amacı sızma testi yapılan kuruma bilgi vermek olduğundan ve saldırı yapılan kurumun kritik bilgi içerdiğinden dolayı sızma testinin raporları oldukça gizli olduğunu unutmamalıyız. Sızma testi yapılmadan önce rapor içeriği kurum ve sızma testi yapan ekip tarafından belirlenerek gizlilik sözleşmesi imzalanır

Raporun Giriş Bölümü

Raporun giriş kısmında sızma testi tarihi, hangi kuruma yapıldığı, sızma testi süreci takvimi ve genel test adımları gibi bilgiler yer alır. Bu kısım raporun içeriğinden kısaca bahseder ve rapor başlığı gibi açıklamaları barındırır.

Sızma Testinin Kapsamı

Bu kısımda gerçekleştirilen testlere yönelik bilgiler ve kuruma yapılan sızma testi çeşitleri detaylandırılır.



Sızma Testi Özeti

Test sonuçlarının genel özeti bulunduğu kısımdır. Çalışmalar sonucunda acil kritik, yüksek, orta gibi seviyeler belirlenerek güvenlik açıkları sınıflandırılır ve burada listelenir. Sızma testinde yapılan işlemlerden ve yöntemlerden bahsedilir. Risk seviyesi ve kapsam tablosu kullanılabilir. Diğer durumlarla karşılaştırma yapılarak grafik, tablo gibi görseller kullanılırsa raporun daha iyi anlaşılması sağlanabilir.

Raporlama Yöntemleri

Herhangi bir sistemin güvenlik ölçüm çalışması yapılırken uluslararası standartlardan faydalanmak gerekir.

ISO 27001, HIPPA gibi yönetmelikler gerçekleştirilen testler ile uyumlu olmalıdır.

Tanımlar ve Güvenlik Seviyeleri

Erişim noktaları dış ve iç olarak ikiye ayrılabilir.

Kullanıcı profilleri de kurum yapısına göre değişkenlik gösterebilir. Anonim bir kişi kurum içinden bir profil veya kurum müşterisi profili bunlara örnek verilebilir.

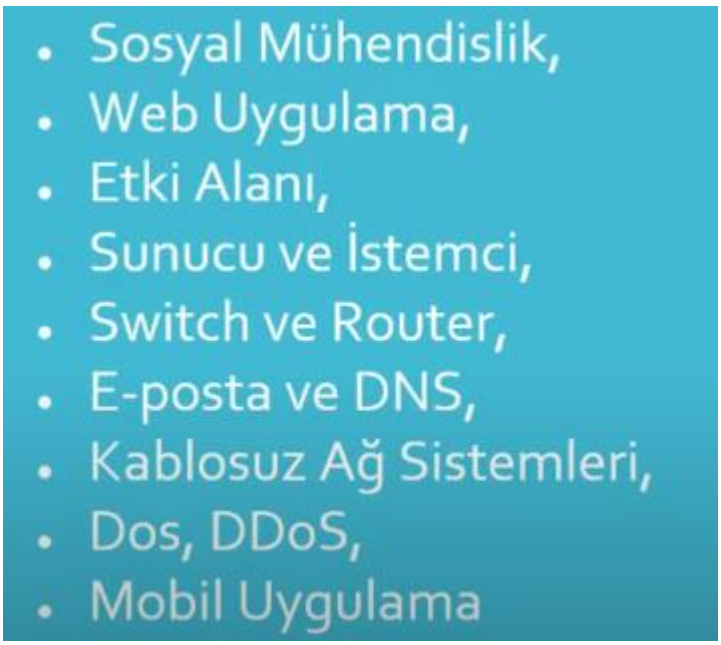
Risk seviyelendirme de PCI DSS güvenlik prosedüründe ki 5 seviye örnek olarak kullanılabilir.

Uygulanan Testler ve Sonuçları

Sızma testi raporlaması 2'ye ayrılır:

Hedef bazlı raporlama da her bir açıklık tek tek ele alınarak açıklanır ve detaylandırılır.

Bileşen bazlı raporlamada ise zafiyetler kategoriye ayrılır ve aynı kategoriler aynı başlık altında incelenirler. Bileşen bazlı raporlama için sızma testi sonucu yazılırken güvenlik testleri kategorize edilmesi:



En kritik öneme sahip bilgiler ve detaylar bu kısımda verilir. Eğer hedef bazlı raporlama yöntemi seçilirse bulunan her bir zayıflık listelenir ve sırasıyla risk ve tespit yöntemleri açıklanır.

KAYNAKÇA

Bilgeiş “Sızma Testine Giriş” eğitimi.