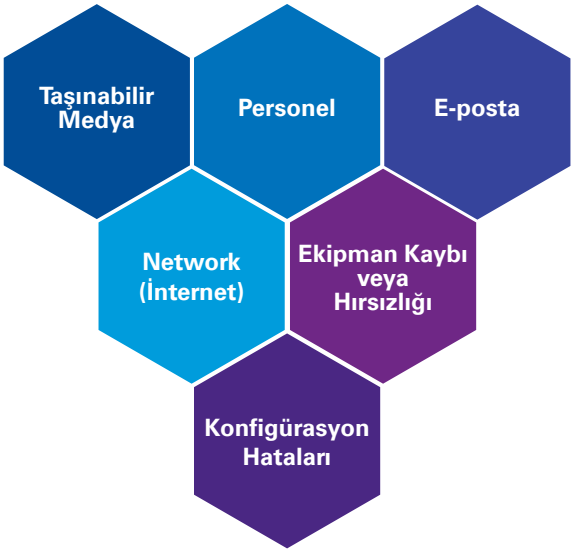
KPMG

Siber Suistimal İnceleme Hizmetleri

Siber saldırıya uğramanız durumunda sistemlerinizde ayrıştırılmayı bekleyen pek çok delil bulunacaktır. KPMG'nin Siber Suistimal İnceleme Hizmetleri için belirlemiş olduğu yaklaşım ve uzman kadrosu ile olası bir saldırının kaynağını belirleyip, saldırılara karşı hazır olup, doğru tepkiyi verebilirsiniz.

Siber saldırı kaynakları

Hem profesyonel hem de kişisel amaçlar için dijital teknolojinin gittikçe yaygınlaşması, veri kaynaklarının çoğalmasına yol açmıştır. Bir ofis gibi bir fiziksel alan incelenip olası veri kaynakları tanınabilmelidir. Bazen, birincil bir veri kaynağından veri toplamak mümkün olmamaktadır. Ağ etkinliği ve trafiği bilgisi bir İnternet Servis Sağlayıcısı (ISP) tarafından da kaydedilebilmektedir. Bu nedenle her veri kaynağının sahibi ve bunun veri toplama üzerindeki etkisi göz önünde bulundurularak ve aynı verilerin bir kısmını veya tümünü içerebilecek alternatif veri kaynaklarının farkında olunarak erişilemeyen kaynaklar yerine var olan kaynaklar etkin bir şekilde kullanılmalıdır.



Hizmetimiz size nasıl fayda sağlar?

Operasyonel sorun giderme: Pek çok suistimal sorgulama uygulaması ve tekniği operasyonel süreçlere uygulanabilir. Örneğin; yanlış konfigüre edilmiş fiziksel veya sanal olarak yerleştirilmiş sunucunun bulunması ve uygulama üzerindeki fonksiyon bir problemin çözülmesi gibi.

Denetim izi izleme: Çeşitli uygulamalar ve teknikler log görüntülemesi kapsamında logların analiz edilmesi ve çoklu sistemlerde logların birbiri ile ilişki kurmasına yardımcı olur. Bu sayede olay yönetimi, denetleme süreçleri ve prosedürlerin ihlali konularında destek olur.

Veri kurtarma: Yanlışlıkla veya bilerek silinen veya başka şekillerde değiştirilmiş veriler de dahil olmak üzere kayıp verileri sistemlerden kurtarabilecek birçok araç bulunmaktadır. Geri kazanılabilecek veri miktarı, duruma göre değişmektedir.

Veri toplama: Bazı kuruluşlar, yeniden yerleştirilen veya kullanımdan kaldırılan ana makinelerden veri edinmek için suistimal soruşturması araçlarını kullanmaktadır. Örneğin, bir kullanıcı bir kuruluştan ayrıldığında, kullanıcıların iş istasyonundan gelen veriler gelecekte ihtiyaç duyulması durumunda edinilebilir ve depolanabilir. Daha sonra, iş istasyonları medyası, tüm orijinal kullanıcı verilerini kaldırmak için sterilize edilebilir.

Durum tespiti / Yasal uygunluk: Mevcut ve gelişmekte olan düzenlemeler, hassas bilgilerin korunması ve denetim amacıyla belirli kayıtların muhafaza edilmesi için birçok organizasyon gerektirir. Ayrıca, korunan bilgiler diğer taraflara maruz kaldığında, kuruluşların diğer kuruluşları veya etkilenen kişileri bilgilendirmeleri istenebilir. Söz konusu inceleme kuruluşların durum tespiti yapmasına ve bu gereklilikleri yerine getirmesine yardımcı olabilir.

Hizmet Yaklaşımımız

KPMG Siber Suistimal İnceleme hizmet çerçevesini üç ana başlıkta değerlendirmektedir:

Veri Toplama

- Olası veri kaynaklarının (en yaygın veri kaynakları; masaüstü bilgisayarları, sunucular, ağ depolama aygıtları ve dizüstü bilgisayar) veri bütünlüğünün sağlanması için oluşturulmuş prosedürlerin takip edilerek belirlenmesi.
- Veri toplama planının oluşturulması, verinin toplanması ve toplanan verinin bütünlüğünün kontrol edilmesi.
- Olay yönetimi ekibi ile olası bir durumda birlikte çalışılması.

İnceleme ve Analiz

- Otomatik ve manuel yollarla toplanan verilerin bütünlüğü korunarak suistimal kapsamında inceleme yapılması.
- Yasal olarak geçerli yöntemler ve metotlar ile toplanan verilerin sonuçlarının analiz edilmesi.
- Sonuca ulaşmak için doğru metodolojinin belirlenmesi.

Raporlama

- Analizlerin raporlanması.
- Rapor içerisinde kullanılan uygulama ve prosedürlerin neden seçildiğinin açıklanması.
- Suistimal sürecinde geliştirilecek alanların belirlenmesi
- Rapor içeriğinde yer alacak bilgilerin doğru bir şekilde belirlenmesi
- Çalışma sonucunda alınacak aksiyonların tanımlanması
- Belirli periyotlar dahilinde prosedürlerin gözden geçirilmesi

Söz konusu hizmet çerçevesinde aşağıdaki çalışmalar gerçekleştirilir;

I. Verinin Toplanması:

I.I Sürecin ilk aşaması, verilerin bütünlüğünü koruyan yönergeleri ve prosedürleri izlerken, olası kaynaklardan veriyi tanımlamak, etiketlemek ve kaydetmektir.
- Olası Değer Belirleme
- Volatilite
- Harcanacak Eforun Belirlenmesi

I.II Veri Bütünlüğünün Doğrulanması

II. İnceleme ve Analiz:

II.I Dosya lokasyonlarının tespit edilmesi
II.II Verinin çıkartılması ve analiz edilmesi
- Firewall-Proxy-DNS loğları
- DHCP-Web Uygulamaları loğları
- IDS/IPS logları

III. Raporlama:

III.I Alternatif Açıklamalar
III.II İzleyici Bakış Açısı
III.III Alınması Gereken Aksiyon Bilgisi

Nasıl Önleyebilirsiniz?

- Siber suistimal inceleme süreçleri tutarlı bir süreç kullanarak gerçekleştirilmelidir.
- Analistler olası veri kaynakları aralığının farkında olmalıdır.
- Kuruluşlar yararlı verilerin toplanmasında proaktif olmalıdır.
- Analistler standart bir işlem kullanarak veri toplama yapmalıdır.
- Analistler, verileri incelemek için metodik bir yaklaşım kullanmalıdır.
- Analistler süreçlerini ve uygulamalarını gözden geçirmelidir.

İletişim:

Ümit Yalçın Şen
Siber Güvenlik Hizmetleri Lideri,
Şirket Ortağı
umitsen@kpmg.com

Oytun Önder
Usulsüzlük Önleme,
İnceleme, Ticari Uyuşmazlık
ve Uyum Danışmanlığı,
Şirket Ortağı
oonder@kpmg.com

Sezgin Topçu
Bilgi Teknolojileri Danışmanlığı,
Şirket Ortağı
stopcu@kpmg.com

İstanbul
İş Kuleleri Kule 3 Kat 1-9
34330 Levent İstanbul
T : +90 212 316 6000

Ankara
The Paragon İş Merkezi Kızılırmak Mah. Ufuk
Üniversitesi Cad. 1445 Sok. No:2 Kat:13
Çukurambar 06550 Ankara
T: +90 312 491 7231

İzmir
Folkart Towers Adalet Mah. Manas Bulvarı
No:39 B Kule Kat: 35 Bayraklı 35530 İzmir
T : +90 232 464 2045

Bursa
İnallar Cadde Plaza, Balat Mahallesi Mudanya
Yolu Sanayi Caddesi No: 435 K:5
D:19-20 Nilüfer
T : +90 232 464 2045

kpmg.com.tr
kpmgvergi.com