1- SORUMLULAR

Bu talimatın uygulamasından Some(Siber Olaylara Müdahale Ekibi) Birim Sorumlusu sorumludur.

2. TANIMLAR

MAC adresi: Bilgisayar ethernet kartı fiziksel adresi

3. UYGULAMA

- İz kaydının alınması gereken sistemlerin (fiziksel ortam kayıtları ve sanal ortam kayıtları) iz kayıtlarının alınmasını sağla.
    - **Fiziksel ortam kayıtları:**
        - Kritik Bilişim sistemleri odaları giriş-çıkış kayıtları,
        - Kritik Bilişim sistemleri odaları giriş-çıkış kamera kayıtları,
        - Çalışma ortamları giriş-çıkış kayıtları,
        - Çalışma ortamları giriş-çıkış kamera kayıtları.
    - **Sanal ortam kayıtları:**
        - Güvenlik duvarları,
        - Antivirüs yazılımları,
        - Saldırı tespit/önleme sistemleri,
        - Yönlendiriciler ve anahtarlama cihazları,
        - Sunucular,
        - İş uygulamaları (Kritik Kurumsal projeler),
        - Veri tabanları,
        - Sanal özel ağ sistemleri
- İz kayıtlarında bulunması gereken aşağıda sıralanan asgari niteliklerin bulunmasını sağla.
    - Kaydı Oluşturan Sistem
    - Kaydın Oluşturulma Zamanı (Tarih, saat, zaman dilimi)
    - Kaydı Oluşturan Olay
    - Kaydın İlişkili Olduğu Kişi (IP-Port bilgisi, MAC adresi, işlemi yapan tekil kullanıcı adı veya sistemin adı)

- İz kayıtlarının güvenliğini gizlilik, bütünlük ve erişilebilirlik ögeleri göz önünde bulundur.
    - Gizlilik
        - Siber olaylara ilişkin tutulan iz kayıtlarına, “bilinmesi gerektiği kadar” (need to know) prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabiliyor olmasını sağla.
        - Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemlerini yapılandır.
        - Kayıt üreten ortamlarla iz kayıtları saklama merkezleri arasında teknik imkânlar dâhilinde trafiğin şifreli olarak transfer edilmesini sağla.
    - Bütünlük
        - İz kayıtlarını tek yönlü kriptografik özet değerleri (hash) hesaplat ve iz kayıtlarını güvenli ortamlarda sakla.
        - Siber olaylara ilişkin iz kayıtlarının saklanması için kurulacak yapının kayıtları, olayların olduğu sistem dışında merkezi bir sunucuda saklamalıdır.

- Kurum kritik olaylarını belirlemelidir. Kritik olayların iz kayıtlarının merkezi sunucuya anlık olarak (olay oluştuğu zaman) gönderilmesi, kritik olmayan olayların iz kayıtlarının da kurumun belirlediği aralıklarda merkezi sunucuya iletilmesini sağla.
- Kritik sistemlerde oluşan iz kayıtlarını eş zamanlı olarak merkezi sunucularda yedekle, silinmelerine ve değiştirilmelerine izin verilmemesini sağla.
- Merkezi iz kaydı sunucuların sadece yeni iz kayıtlarının saklanması için fonksiyonlar içermesi, iz kayıtlarının silinmesi/değiştirilmesi amaçlı erişimlere kapalı olmasını sağla.

o Erişilebilirlik
- İz kayıtlarının periyodik olarak yedeklenmesini ve yedeklerin uygun şekilde muhafaza edilmesini sağla.

- Önceden belirlenmiş İz Kayıtlarının Yönetimi ile ilgili roller doğrultusunda aşağıda belirlenen kişiler sorumluluklarının gereğini yerine getirirler. İz kayıtlarının yönetimi; iz kayıtlarının üretilmesi, transfer edilmesi, depolanması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi aşamalarını kapsar. Bu süreçlerde sistem, veri tabanı, ağ ve güvenlik yöneticileri, Siber Olaylara Müdahale Ekipleri (SOME), yazılım geliştiriciler ve denetçilere ait görev ve sorumluluklar belirlenmiştir.

- **İz Kayıtlarının Saklanma Süresi**
  - İz kayıtlarının saklanma süresi belirlenmesinde, iz kayıtlarından sağlanacak fayda, saklama maliyeti ve ilgili iz kaydının kritikliği parametreleri göz önünde bulundurulmalıdır.
  - İz kayıtlarını bu bilgiler ışığında asgari olarak 1 yıl süre ile sakla.

- **Ortak Zaman Sunucusu Kullanımı**
  - Kayıtların toplandığı bütün sistemlerin aynı zaman değerine sahip olması gerekmektedir.
  - Bütün sistemlerin zamanlarının aynı yapılması işlemi için Ağ Zaman Protokolü (NTP-Network Time Protocol) sunucusunun kurulmasını sağla, kayıt üreten farklı sistemlerin zamanlarını bu sunucu ile senkronize etmesini sağla.

- **Merkezi İz Kayıtları Yönetiminin Sağlanması**

Yukarıda asgari nitelikleri belirtilen iz kayıtlarının daha etkin, verimli ve güvenli bir şekilde toplanması, ilişkilendirilmesi, arşivlenmesi, raporlanması amacıyla Merkezi İz Kayıtları Yönetimi Mekanizmalarını devreye al