Sefine Log Politikası

Bu politikanın amacı; kurum bilişim varlıklarında gerçekleşen faaliyetlerin güvenli, bütünlüklü ve izlenebilir şekilde kayıt altına alınmasını, saklanmasını, korunmasını ve gerektiğinde analiz edilmesini sağlamaktır. TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve siber hijyen farkındalığı en iyi uygulamalarına uyumu destekler.

Log Üretimi ve Toplanması

Aşağıdaki logların üretilmesi zorunludur:

- Kimlik doğrulama (login/logout) kayıtları,
- Yetki değişiklikleri,
- Sistem başlangıç ve kapanma logları,
- Güvenlik olayları (IDS/IPS, firewall bloklamaları vb.),
- Uygulama hata logları,
- Erişim logları (dosya, veritabanı, API erişimleri),
- Konfigürasyon değişiklikleri,
- Ağ trafiği kayıtları,
- Kritik sunucu ve güvenlik cihazı logları,

Zaman Senkronizasyonu

- Tüm sistemler NTP kullanarak ortak zaman kaynağı ile senkronize edilir. Loglarda doğru zaman damgası bulunması zorunludur.

Log Aktarımı

- Loglar mümkün olduğunda bir SIEM veya merkezi log yönetim sistemine güvenli kanal (TLS/SSL) üzerinden aktarılmaktadır.
- Aktarım sırasında log bütünlüğü korunmaktadır.

Log Saklama Süresi

- Yasal süreç dahilinde loglar iki yıl boyunca saklanmaktadır.

Logların Bütünlüğü ve Güvenliği

- Log dosyaları yetkisiz değişikliği engelleyecek şekilde korunmaktadır.
- Loglara yalnızca yetkili personel erişebilmektedir.
- Loglar üzerinde değişiklik yapılması yasaktır.

Genel Müdür

Döküman No: SFN-PT-34, Yayım Tarihi: 17.11.2025 Revizyon Tarihi/No: 17.11.2025/00

Sefine Log Politikası

Log Analizi ve İzleme

- SIEM üzerinden gerçek zamanlı izleme yapılmaktadır.
- Şüpheli aktivitelerde otomatik alarm oluşturulmaktadır.
- Günlük log inceleme faaliyetleri gerçekleştirilmektedir.
- Kritik güvenlik olayları Olay Yönetimi Prosedürüne göre işlenir.
- Log analiz sonuçları düzenli raporlanmaktadır.

6698 Sayılı Kişisel Verilerin Korunumu Kanunu ve Gizlilik Gereksinimleri

- Loglar kişisel veri içeriyorsa KVKK'ya uygun şekilde işlenmektedir.
- Gereksiz kişisel veri içeren log üretimi engellenmektedir.
- Loglara erişim kayıt altına alınmaktadır.

Dış Hizmet Sağlayıcıları

Bulut veya dış kaynak hizmetlerinde sağlayıcılar:

- Log üretme ve saklama yükümlülüklerini yerine getirmektedir.
- İstendiğinde Sefine'ye erişim loglarını paylaşmaktadır,
- Logların gizliliğini ve bütünlüğünü sağlamalıdır.

Otomasyon ve Siber Hijyen Gereklilikleri

- Varsayılan log seviyeleri düşürülmez.
- Yönetici erişim logları daha hassas korunmaktadır.
- MFA olayları loglanmaktadır.
- Malware/EDR telemetrileri saklanmaktadır.
- Kritik sistem güncellemeleri ve patch dağıtımlarına ilişkin loglar tutulmaktadır.

Uyum ve Denetim

- Politikanın uygulanması düzenli iç denetimlerle kontrol edilir.
- Uyumsuzluklar düzeltilmek üzere ilgili yöneticilere raporlanır.
- Politika yılda en az bir kez gözden geçirilmektedir.

Genel Müdür

Döküman No: SFN-PT-34, Yayım Tarihi: 17.11.2025 Revizyon Tarihi/No: 17.11.2025/00