BGYS POLİTİKASI

Politika Numarası	PLTK-25
Politika Tanımı	Kaydetme (Log Tutma) Politikası
Amaç ve İlkeler	**Bu politika,** log tutma süreçlerinin yönetimi ve log verilerinin doğru bir şekilde oluşturulması, kaydedilmesi, korunması ve işlenmesini sağlamak üzere oluşturulmuştur. Güvenlik tehditlerinin tespiti, sorun giderme süreçlerinin desteklenmesi ve yasal gerekliliklerin karşılanması amaçlanmaktadır. Tüm kuruluş çalışanlarını ve bilgi işlem sistemlerini kapsar. Log tutma süreçleri, bilgi işlem sistemlerinde, ağ altyapısında ve bulut hizmetlerinde uygulanır.
Sorumluluklar	**Bilgi İşlem Personeli:** Politikanın tasarımı, uygulanması ve yönetilmesinden sorumludur. Ayrıca, güncel mevzuat ve standartlara uygun olarak politikaların düzenli olarak gözden geçirilmesi ve güncellenmesi bu departmanın sorumluluğundadır. Sistem ve ağ yöneticileri, log tutma süreçlerinin uygulanması, sistemlerin düzenli olarak denetlenmesi ve izlenmesinden sorumludur. **Tüm çalışanlar:** Log tutma süreçlerine uymak, log verilerini yanlış kullanmamak ve güvenlik önlemlerine dikkat etmekle yükümlüdür.
Sapma ve Özel Durumlar	Sapmalar veya özel durumlarla karşılaşıldığında, ilgili departman veya yöneticilerle iletişime geçilmelidir. Bu durumlar, politikanın etkinliğini artırmak için incelenir ve gerekli düzeltici önlemler alınarak, uygun cezai yaptırımlar gerçekleştirilir.

UYGULAMA

Olay kayıtları, kullanıcı kimlikleri, sistem faaliyetleri, tarihler ve saatler gibi bilgileri içermelidir. Kayıtlar arasında, sistem erişim girişimleri, veri erişim girişimleri, yapılandırma değişiklikleri ve güvenlik olayları yer almalıdır.

Log kayıtları, sistemlerin güvenliği ve bütünlüğü için kritik öneme sahip olduğundan, bu kayıtların korunması ve izlenmesi süreci titizlikle yürütülmelidir. Yedekleme ve felaket kurtarma planları, log verilerinin kaybını önlemek ve sürekliliğini sağlamak için düzenli olarak test edilmelidir.

Kullanıcıların kendi etkinliklerine ilişkin kayıtları silme veya devre dışı bırakma izni bulunmamalıdır. Bu durum ayrıcalıklı erişim haklarına sahip olanlar da dahil olmak üzere tüm kullanıcılar için geçerli olmalıdır. Bu politika, log kayıtlarının doğru ve güvenilir kalmasını sağlamak ve potansiyel manipülasyonları önlemek amacıyla uygulanmaktadır.

Ayrıcalıklı kullanıcılar için hesap verebilirliği sürdürmek amacıyla, log kayıtlarını korumak ve gözden geçirmek için özel kontroller uygulanmalıdır. Bu kontroller, log bilgisinde yapılan değişiklikleri izlemek ve aşağıdaki durumlar gibi işletimle ilgili sorunlara karşı koruma sağlamak için tasarlanmalıdır;

- Kaydedilen mesaj türlerinde yapılan değişiklikler,
- Düzenlenen veya silinen log dosyaları,
- Log dosyası tutan depolama ortamının dolum seviyesi, olayların kaydedilmemesi veya geçmişte kaydedilen olayların üzerine yazılmasını önlemek için düzenli olarak izlenmelidir.

Bu kontrollerin uygulanması, log kayıtlarının güvenliğini ve bütünlüğünü sağlamak için kritik bir öneme sahiptir. Bu sayede, olası güvenlik tehditleri tespit edilebilir ve gerekli önlemler hızla alınabilir.

Logların Analizi

Bilgi güvenliği olaylarının analizi ve yorumlanması için muhtemel ihlal olayı göstergelerini belirleme aşamalarında yol göstermesi adına olağandışı etkinliklerin veya anormal davranışların tespit edilmesi sağlanmalıdır.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
06.02.2024	-	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

Log Analizi ve İzleme Süreçleri

Log analizi süreci aşağıdaki unsurları dikkate alarak gerçekleştirilmelidir;

- Uzmanlar tarafından gerekli becerilerin kullanımı
- Log analizi prosedürlerinin belirlenmesi ve uygulanması
- Güvenlik olaylarının gerekli niteliklerinin belirlenmesi
- Önceden belirlenmiş kuralların kullanımı ve istisnaların belirlenmesi
- Anormal etkinliklerin belirlenmesi için bilinen davranış kalıplarının ve standart ağ trafiğinin izlenmesi
- Trend analizi ve yapı analizinin sonuçlarının incelenmesi
- Mevcut tehdit istihbaratının göz önünde bulundurulması

Destekleyici İzleme Faaliyetleri

Log analizi, aşağıdaki izleme faaliyetleriyle desteklenmelidir;

- Korunan kaynaklara erişim için başarılı veya başarısız saldırıların gözden geçirilmesi
- Botnet komuta ve kontrol sunucularıyla ilişkili kötü amaçlı sunuculara giden ağ bağlantılarının belirlenmesi
- Olağandışı etkinlikler için hizmet sağlayıcılardan alınan kullanım raporlarının incelenmesi
- Fiziksel izleme olay loglarının dahil edilmesi
- Logların ilişkilendirilmesi ve analiz edilmesi

Log analizi ve güvenlik izleme süreçlerini desteklemek amacıyla Wazuh SIEM benzeri ürünler kullanılmalıdır. Ayrıca, endpoint security ürünleriyle de işletim sistemleri ve cihazların korunması sağlanmalıdır.