BGYS POLİTİKASI

Politika Numarası	PLTK-30
Politika Tanımı	Siber Saldırı Politikası
Amaç ve İlkeler	**Bu politika,** Kayalar Şirketi'nin bilgi sistemlerini ve verilerini siber saldırılara karşı korumayı hedefler. Bu politika, siber saldırıları tespit etme, önleme, yanıtlama ve iyileştirme için bir çerçeve sunar ve Kayalar Şirketi'nin tüm bilgi sistemlerini, ağlarını ve kaynaklarını kapsar.
Sorumluluklar	**Yönetim:** Siber güvenlik konusunda liderlik sağlar, politikaları belirler, güvenlikle ilgili kaynakları tahsis eder ve sürekli iyileştirme sürecini destekler. **Bilgi İşlem Personeli:** Bilgi güvenliği ekibi, siber güvenlik politikalarını uygulamak, sistemlerin güvenliğini izlemek, tehditleri değerlendirmek ve siber saldırılara karşı koruma sağlamakla sorumludur. **Tüm Çalışanlar:** Bilgi güvenliği politikalarına uymakla ve güvenlikle ilgili riskleri rapor etmekle sorumludur.
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, kusurlu bir çalışan olması durumunda uygun cezai yaptırımlar gerçekleştirilir.

UYGULAMA

Siber saldırı, bilgi sistemlerine yetkisiz erişim, veri ihlali, hizmet kesintisi veya sistemlerin zarar görmesi gibi herhangi bir zararlı etkinliği içermektedir.

Siber saldırının önlenmesi ve korunma amacıyla;

- Bilgi sistemlerinin güvenliğini sağlamak için güvenlik duvarları, yazılımlar ve yamalar gibi koruyucu önlemler alınmalıdır.
- Güvenlik politikaları ve prosedürleri düzenli olarak gözden geçirilip güncellenmelidir.
- Hassas veriler şifrelenip düzenli yedeklemeler yapılmalıdır.

Tespit ve izleme kapsamında;

- Ağ ve sistem günlükleri düzenli olarak izlenip ve analiz edilmelidir.
- Saldırı tespit edildiğinde, etkilenen sistemler hemen izole edilmeli ve saldırı türüne uygun önlemler alınmalıdır.
- Otomatik izleme sistemleri kullanılarak anomaliler ve potansiyel saldırı işaretleri tespit edilmelidir.
- Saldırı kayıtları derhal incelenmeli ve saldırının boyutu ve etkisi değerlendirilmelidir.
- Tespit ve izleme sonuçları düzenli olarak raporlanıp değerlendirilmelidir.

Siber saldırıya yanıt olarak;

- Olay yanıt ekipleri oluşturulmalı ve siber saldırılara hızlı yanıt verme kapasitesi geliştirilmelidir.
- Uygun yanıt stratejileri belirlenip uygulanmalı, saldırıların etkileri minimize edilmeli ve normal işletme faaliyetleri en kısa sürede yeniden başlatılmalıdır.
- Saldırıdan etkilenen çalışanlar ve dış paydaşlar derhal bilgilendirilmeli ve gerekli önlemler alınmalıdır.
- Kriz iletişim planları oluşturularak saldırı sonrası iyileştirme süreci başlatılmalıdır.

Saldırı Sonrası İyileştirme için;

- Saldırı sonrası inceleme ve analiz yapılmalı, zayıf noktalar belirlenmeli ve iyileştirme planları oluşturulmalıdır.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
08.02.2024	-	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

- Gerekli güvenlik yamaları ve düzeltmeler yapılmalı, sistemlerin güvenliği sağlanmalı ve benzer saldırıların önlenmesi için önleyici tedbirler alınmalıdır.
- İyileştirme planları uygulanmalı ve siber güvenlik önlemleri güçlendirilmelidir.
- Saldırılardan dersler çıkarılıp gelecekte benzer saldırıların önlenmesi için sürekli olarak iyileştirme yapılmalıdır.