KLVZ-EK-21 OLAY BİLDİRİM VE MÜDAHALE FORMU

|  |
| --- |
| **OLAY BİLDİRİM BÖLÜMÜ** |
| 1. **Bildirimi yapan birim:** |
| 1. **Bildirimi yapan personelin**   **Ad, Soyadı :**  **Unvan/Birim :**  **Telefon :**  **e-Posta :** |
| 1. **Olay türü:**  |  |  | | --- | --- | | □ Servis Dışı Bırakma Saldırısı (DoS/DDoS) | □ Web Uygulamaları Güvenlik İhlalleri | | □ Bilgi Sızdırma (Data Leakage)  □ Zararlı Yazılım (Malware)  □ Dolandırıcılık (Fraud)  □ Port Tarama  □ Veritabanı Saldırısı  □ Diğer (Lütfen açıklayınız): | □ Sosyal Mühendislik  □ Veri Kaybı/ Veri İfşası  □ Zararlı Elektronik Posta(Spam)  □ Parola Ele Geçirme | | □ Taşınır Cihaz Kaybı | | □ Kimlik Taklidi  □ Oltalama (Phishing)  □ Kişisel Bilgilerin Kötüye Kullanımı | |  | |
| 1. **Olay sistem kesintisine sebep oldu mu?**  □ Evet □ Hayır |
| 1. **Olayın:**   **Tahmini başlangıç zamanı**  Tarih : ……………….. Saat : ………………..  **Tespit edildiği zaman**  Tarih : ……………….. Saat : ……………….. |
| 1. **Eklemek istedikleriniz:** |

|  |
| --- |
| **OLAY MÜDAHALE BÖLÜMÜ** |
| **Dikkat: Bu kısım Bilgi Güvenliği /SOME Olay Müdahale Ekibi tarafından doldurulur.** |
| 1. **Siber olaylara ait iz (log) kayıtları tespit edildi mi?**   □ Hayır  □ Evet  **Kaynak IP** : **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Hedef IP** : **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Port** : **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Diğer**  : **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| 1. **Olayın etkisini azaltıcı ilk önlemler:** |
| 1. **Olayın muhtemel sebepleri:** |
| 1. **Olayın tekrarlanmaması için alınan önlemler:** |
| 1. **Tahmini Olay Maliyeti** |
| 1. **Eklemek istedikleriniz:** |