Olay Kaydı Politikası

Seviye Tespiti

Önem Seviyesi	Belirtiler	Örnekler
Seviye 1 - Kritik	• Çok sayıda hedefin etkilenmesi • Servis kesintisine sebep olması • Olaya sebep trafiğin devam etmesi	• UlakNET omurga cihazlarının çalışmasını engelleyen trafikler • Devam eden DdoS saldırısı • Devam eden sızma çabası
Seviye 2 - Ciddi	• Belirli bir hedef grubunun etkilenmesi • Servis yavaşlamasına sebep olması • Olaya sebep trafiğin devamı	• Erişime açık sunucu tesbiti • Relay 'e açık e-posta sunucusu • Devam eden port taraması
Seviye 3 - Orta	• Sınırlı sayıda hedefin etkilenmesi • Olaya sebep olan trafiğin kesilmiş ancak tekrar başlaması çok muhtemel olması	• Copyright uyarısı
Seviye 4 - Düşük	• Çok az sayıda hedefin etkilenmesi • Olaya sebep olan trafiğin kesilmiş olması	• Istenmeyen e-posta • Virus sebepli tarama
Seviye 5 - Özel	• Ulak-CSIRT üyeleri tarafından diğer seviyelerle sınıflandırılamayan olaylar	• Süreli adli yazı ile kullanıcı bilgi talebi

***** Her bir olay kaydı için seviye tespiti ULAK-CSIRT tarafından yapılacak ve olay kaydı bildirim e-postasında olay detayları ile beraber ilgili kuruma iletilecektir.

Seviye Süreleri

Önem Seviyesi	İlk Tepki Süresi *	Olay Çözümü Süresi
Seviye 1	1/2 Saat	1 saat
Seviye 2	1 saat	4 saat
Seviye 3	4 saat	24 saat
Seviye 4	12 saat	48 saat
Seviye 5	Olaya özel belirlenecektir	Olaya özel belirlenecektir

***** İlk Tepki Süresi; olay kaydının açılmasından olay üzerinde çalışmalara başlanıldığına dair bilgilendirmenin yapılmasına kadar geçen zamandır. Bilgilendirme, olay bildirimi e-postasında belirtilen web sayfası bağlantısı kullanılarak yapılmalıdır.

Yaptırımlar

Önem Seviyesi	İlk Tepki Süresinin Aşılması Durumu	Çözüme Ulaşılamaması Durumu
Seviye I - Kritik	Tepki süresi sonunda otomatik tekrar bildirim ve ilgili Ulak-CSIRT üyesi tarafından telefonla bildirim ile tepki süresinin yarısı kadar zaman tanıma*	Erişim engellenmesi (NAT benzeri uygulamalar sebebiyle uç trafiğinin tamamen etkilenecek olması durumu dahil)
Seviye II - Ciddi	Tepki süresi sonunda otomatik tekrar bildirim ve ilgili Ulak-CSIRT üyesi tarafından telefonla bildirim ile tepki süresinin yarısı kadar zaman tanıma*	Erişim engellenmesi (NAT benzeri durumlarda uç yöneticisi ile iletişime geçerek çözüm süresinin yarısı kadar daha zaman tanıma)**
Seviye III - Orta	Tepki süresi sonunda otomatik tekrar bildirim ile tepki süresi kadar zaman tanıma*	Çözüm süresi sonunda otomatik tekrar bildirim ile çözüm süresinin yarısı kadar zaman tanıma **
Seviye IV - Düşük	Tepki süresi sonunda otomatik tekrar bildirim*	Çözüm süresi sonunda otomatik tekrar bildirim ile çözüm süresi kadar zaman tanıma **
Seviye V - Özel	Olaya özel belirlenecektir	Olaya özel belirlenecektir

* Sürenin bitiminde olay çözümü süresi aşılana dek bir işlem yapılmayacaktır.
** Ek süre bitiminde erişim engellenmesi yapılacaktır.