SİBER OLAYLARA MÜDAHALE POLİTİKASI

Politika Adı:	SİBER OLAYLARA MÜDAHALE POLİTİKASI
Doküman Kodu:	BGYS.P.T.013.ATABAUM.IT
Doküman Sahibi:	BGYS Yöneticisi
Doküman Onay Tarihi:	05/12/2021
Gizlilik Sınıfı:	İç Kullanım

İçindekiler

AMAÇ:

Bu Politika, Kuruluş Kurum Bilgi varlıklarının Gizlilik, Bütünlük ve Erişilebilirliğini bozabilecek bir Siber Olay Meydana gelmesi durumunda yapılması gereken kuralları tanımlamaktadır.

KAPSAM:

Bu Politika, Kuruluş ve Kuruluş ile ilişkili Dijital Bilgi Varlıkları ve bu varlıklar ile ilişkili altyapı bileşenlerini kapsamaktadır.

POLİTİKA MADDELERİ:

1. Bu Politika Kapsamında belirlenen Güncel "Siber Olay Tipleri" SİBER OLAYLARA MÜDAHALE TABLOSU'nda yer almaktadır.
2. Olay tipleri SİBER OLAYLARA MÜDAHALE TABLOSU işlenir. Buradan amaç güncel saldırı metotlarının takip edilebilmesidir.
3. Ayrıca TEHDİT VE ZAYIFLIK VERİTABANI içerisindeki SİBER RİSKLER de dikkate alınarak SİBER OLAYLARA MÜDAHALE TABLOSU güncel tehdit vektörleri eklenebilir.
4. Siber Saldırılardan etkilenecek Bilgi Varlıkları belirlenmelidir,
5. Her bir saldırı tipi ve Bilgi varlığı için yanıt verecek ekip üyeleri SİBER OLAYLARA MÜDAHALE TABLOSU'nda "Olay Müdahale Sorumlusuna" kaydedilir. Böylelikle Olay Tipinden uzman personelin, Bilgi varlığından ilgili varlık sahibinin bulunması sağlanır.
6. Siber Olaya Müdahale Personelinin iletişim (İş veya Cep Telefonu, E-mail) bilgisi SİBER OLAYLARA MÜDAHALE TABLOSU'na girilir. Bu belirleme işlemi VARLIK ENVANTER LİSTESİ dikkate alınarak yapılır.
7. Her bir saldırı Kuruluşa olan etkisine göre seviyelendirilmiştir. Bu seviyeler;
    a. ÇOK YÜKSEK (Kuruluş Sistemlerinin tamamını etkileyen olaylar),
    b. YÜKSEK (Kuruluş en az bir Departmanını veya önemli sistemlerini etkileyen olaylar),
    c. DÜŞÜK (Bir personel veya alt servis ile sınırlı kalan olaylar),
    d. ÇOK DÜŞÜK (Bir personel ile sınırlı kalan olaylar).
8. Her bir saldırı tipinin işaret ettiği riskler VARLIK ENVANTER LİSTESİ üzerinden analiz edilmiş ve risk sahipleri atanmıştır,
9. Olay tipine bağlı bir saldırı meydana gelmesi durumunda;
    a. Saldırıyı Kimlerin hangi araçları kullanarak tespit edeceği,

b. Saldırıya İlk Müdahaleyi Kimlerin yapacağı,
c. Saldırıya İlk Müdahalesinde Ne Yapılacağı,
d. Saldırı Sonrası Olayların Nasıl Kayıt Altına alınacağı,
e. Saldırı Sonrası Uğranılan Zararın tespiti, Saldırının kök nedeni, Alınacak Kontrolleri ve Kontrollerin Performans ölçümünü Kimin belirleyeceği doküman haline getirilecektir.

10. Saldırı ilgili taraflara, Yasalar, Sözleşmeler dikkate alınarak bildirilir.
11. Tüm Saldırı Türleri için Örnek Senaryo ve Tatbikat Çalışması SİBER OLAYLARA MÜDAHALE TABLOSU'ndaki ilgili personel/ler tarafından gerçekleştirilir,
12. Ağ yapısının bilinmesi ve ilgili manevraların yapılabilmesi için güncel Ağ topolojisinin basılı hali olaya müdahale edecek ilgililerin ulaşabileceği bir konumda tutulur,
13. Siber Saldırı Tipleri Saldırı Meydana geldiğinde ve Yılda en az bir BGYS TAKVİMİ olmak üzere gözden geçirilerek ihtiyaç duyulması durumunda Saldırı Tipi ve Alt Süreçler güncellenir.
14. Ayrıca BİLGİ GÜVENLİĞİ İHLAL YÖNETİM PROSEDÜRÜ dikkate alınır.

YAPTIRIM:
Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenlik Kurulu ve ilgili Yöneticinin onaylarıyla BİLGİ GÜVENLİĞİ YAPTIRIMLARI DOKÜMANINDA belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

İLGİLİ REFERANS DOKÜMANLAR VE KONTROL MADDELERİ:
REFERANS VERİLEN:

REFERANS ALINAN:

1. A.16.1.1 | İlişkili Kontroller: A.16.1.1
2. A.16.1.2 | İlişkili Kontroller: A.16.1.2
3. A.16.1.3 | İlişkili Kontroller: A.16.1.3
4. A.16.1.4 | İlişkili Kontroller: A.16.1.4
5. A.16.1.5 | İlişkili Kontroller: A.16.1.5
6. A.16.1.6 | İlişkili Kontroller: A.16.1.6
7. A.16.1.7 | İlişkili Kontroller: A.16.1.7

Bu sayfa son olarak 5 Aralık 2021 tarihinde ve 11.49 saatinde düzenlenmiştir.