ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ

Kurumsal Siber Olay Müdahale Rehberi

1. Amaç

Bu rehber, 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete 'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ kapsamında Ankara Sosyal Bilimler Üniversitesi bünyesinde Kurumsal SOME kurma sorumluluğunu düzenlemeyi amaçlamıştır.

2. Kapsam

Ankara Sosyal Bilimler Üniversitesi bünyesinde kurulan kurumsal SOME biriminin sorumlulukları, hedefleri ve işleyiş şekli bu dokumanda sunulmaktadır.

3. Ulusal Siber Olaylara Müdahale Organizasyonu (USOM)

20/10/2012 tarih ve 28447 sayılı Resmi Gazete 'de yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince 20/06/2013 tarih ve 28683 sayılı Resmi Gazete 'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı ile "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" kapsamında, Ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel siber saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 27/05/2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur.

Ayrıca 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME) oluşturulmuştur. USOM ve SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları öncelemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde hayati önemi olan yapılardır. USOM ile Kurumsal SOME'nin koordineli çalışması ve işbirliği halinde olması ulusal siber güvenliğimize katkı sağlamaktadır.

4. Kurumsal SOME Ekibinin Oluşturulması

22 Mayıs 2013 Tarihli 2013/278 Sayılı Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esasları ile kamu kurumlarının yükümlü tutulduğu süreçlerin yürütülebilmesi için tablo 1 de belirlenen haliyle üniversitemiz bünyesinde kurumsal SOME ekibi kurulmuştur.

Organizasyon	Kurulduğu Kurum/Kuruluş	Hizmet Alanı
USOM	BTK / Telekomünikasyon İletişim Başkanlığı (TİB)	Ulusal Siber Ortam
Sektörel SOME	• Kritik sektörü düzenleyici ve denetleyici kurumlar • Düzenleyici ve denetleyici kurumlar	Kritik altyapı sektörü

	kuruluncaya kadar ilgili bakanlık	
Kurumsal SOME	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumların siber ortamı

Tablo 1. Hizmet Alanları

Ekip Bilgi İşlem Daire Başkanlığı bünyesinde görev yapan ve siber olaylara karşı tepki verebilecek personelden oluşturulmuştur. Ekip Ulusal siber olaylarla mücadele merkezi tarafından oluşturulan SOME İletişim platformu üzerinden yetkilendirilmekte ve güncellenmektedir.

5. Kurumsal SOME Ekibinin Görev ve Sorumlulukları

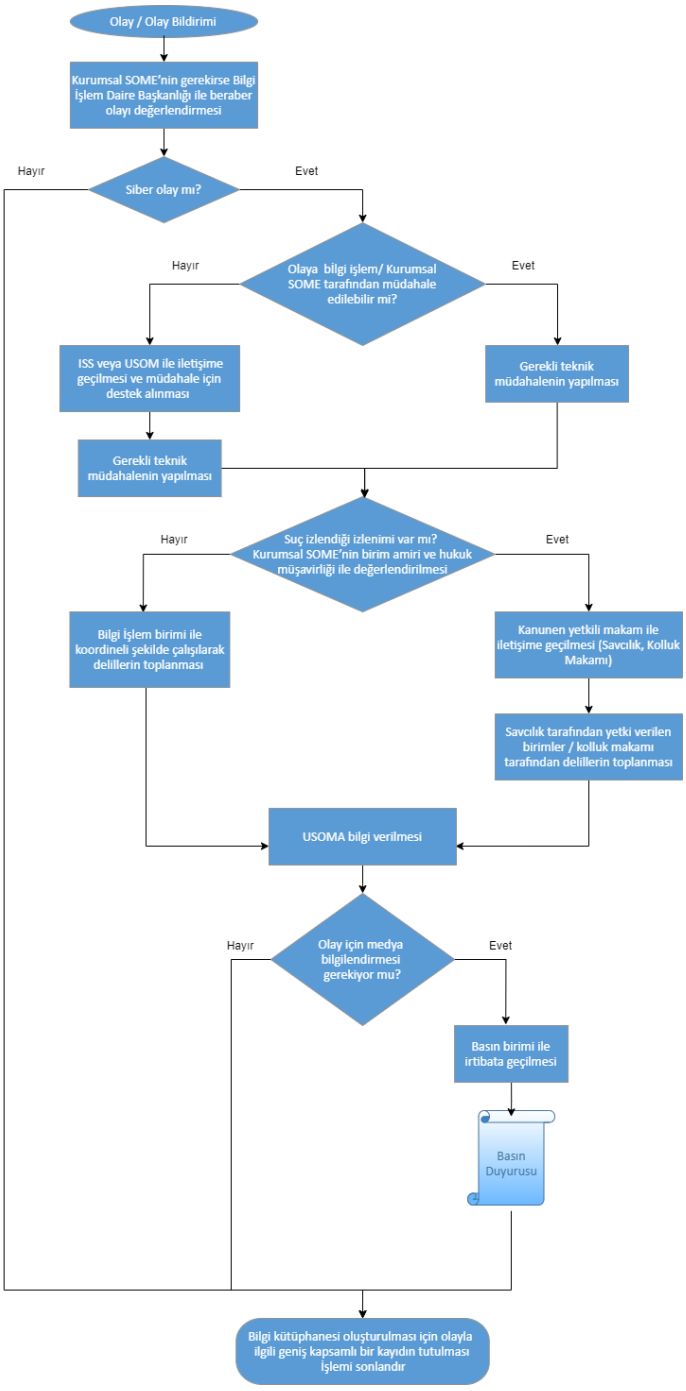
Kurum dışı (vatandaşlar, diğer kurumlar, vb.) ve kurumdaki çalışanlara hizmet amacıyla yürütülen bilgi işlem birimi ağ ve sistem işletim faaliyetleri Kurumsal SOME'den ayrı ele alınmaktadır. Bilgi işlem ekibi tarafından gerçekleştirilen faaliyetlerin hedefi ağ ve sistem sürekliliğini sağlamak ve kurumsal siber güvenlik politikalarını uygulamaktır.

Kurumsal SOME'nin görevi ise kurumsal siber güvenliğe ilişkin politikaları belirlemek, uygulanıp uygulanmadıklarını izlemek, olaylardan sonra yetkili makamlarla iletişime geçmek, delil, kayıt vb. veriyi yetkili makamlara aktarmak ve müdahalenin yapılmasına yardımcı olmaktır. Ayrıca Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler. Bu iş tanımlarının yanı sıra Kurumsal SOME aşağıdaki görevleri ifa etmekle yükümlüdürler.

- Kurum içi farkındalık çalışmalarının gerçekleştirilmesi, kurumsal bilişim sistemleri sızma testlerinin yapılması / yaptırılması ve kayıtların düzenli olarak incelenmesi çalışmalarının yapılması.
- Siber olay öncesi, esnası ve sonrasındaki görev ve sorumlulukları ile kurumun diğer birimlerle ilişkilerin düzenlenmesi, siber olay yönetim talimatlarının (siber olay müdahale, siber olay bildirim süreci vb.) hazırlanması.
- Ulusal Siber Güvenlik Tatbikatı başta olmak üzere tatbikatlara ve USOM tarafından önerilen/düzenlenen toplantı ve etkinliklere katılım sağlanması.
- Güvenlik ürünlerinin (saldırı tespit sistemi, güvenlik duvarı, balküpü sistemi vb.) belirlenmesi sürecinde bilgi işlem birimine destek verilmesi.
- Güvenlik ürünlerinin uygulama seviyesi işletimi ile ilgili politikaların bilgi işlem ile koordineli şekilde belirlenmesi.
- Siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneriler sunulması.
- Siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini yürütülmesi.
- Bir siber olayla karşılaştıklarında, USOM'a bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışılması, bunun mümkün olmaması halinde USOM'dan yardım talebinde bulunulması.

- Siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaşıldığında gecikmeksizin durumun kanunen yetkili makamlara bildirilmesi.
- Kurumlarına yapılan siber olayların raporlanması ve gecikmeksizin USOM'a bildirilmesi.
- USOM tarafından iletilen siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak kurumlarında gerekli tedbirlerin alınması.

Kurumsal SOME'ler tüm bu görevleri Şekil 1'de yer alan akış diyagramına göre icra ederler. Bu görevleri sorunsuz bir şekilde ifa edebilmek için Kurumsal SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek USOM'a bildirirler. USOM, Hukuk Müşavirliği ve Basın Halkla İlişkiler Birimi ile siber olaylar konusunda iletişim halinde olmalıdırlar.



Şekil 1. SOME İş Akış Diyagramı

6. Siber Olay Bildirim Yöntemleri

Ankara Sosyal Bilimler Üniversitesi bünyesinde kurulan Kurumsal SOME ekibi kurumu ilgilendiren siber olaylarla ilgili olarak tüm paydaşlardan istihbarat toplamakta ve kendi içinde yaptığı tahkikler sonucunda gerekli durumları USOM a bildirmektedir.

- **Kurumsal SOME'ye Yapılan Bildirimler**

Kurumsal SOME, paydaşlarından istihbarat toplayabilmek için **asbusome@asbu.edu.tr** eposta adresi oluşturmuş ve bidb.asbu.edu.tr adresi içerisinde Kurumsal SOME başlığı altında paydaşlarla gerekli bilgilerin paylaşılmasını sağlamıştır.

- **Kurumsal SOME'ye USOM Tarafından Yapılan Bildirimler**

USOM, kurumsal SOME'lere istihbarat ağından edindiği bilgileri ve kendi analiz ettiği zafiyetlerle ilgili istihbaratı SOME İletişim platformu üzerinden ve/veya gerekliliğine göre gizlilik derecesi sınıflandırılmış resmi yazı ile göndermektedir. Kurumsal SOME, ilgili istihbarat için gerekli çalışmayı yaptıktan sonra USOM'a bilgilendirmenin yapıldığı aynı yöntem ile dönüş yapmaktadır.

- **Kurumsal SOME'nin Yapacağı Bildirimler**

Kurumsal SOME, paydaşlarından eposta adresi üzerinden topladığı istihbarat verilerini gerekli incelemelerden geçirdikten siber olay içeren bilgileri USOM'un oluşturduğu SOME İletişim platformu üzerinden USOM ile paylaşacaktır.