BATMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı

Kurumsal Siber Güvenlik Rehberi

Batman Üniversitesi

Kurumsal Siber Güvenlik Rehberi

I. Siber Güvenlik Birimi :

Siber Olaylara Müdahale Ekiplerinin kurulması kararı Bakanlar Kurulu tarafından alınmıştır. Kurumların siber saldırılardan zarar görmesini engellemeyi ve Bilgi Güvenliklerinin alınmasına dönük koruyucu ve kollayıcı tedbirler alınmasını amaçlar. Siber Olaylara Müdahale Ekipleri; kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı; gerekli önlemleri alma veya aldırma, olay takip mekanizmasını oluşturma, kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler. SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar. Görevler ayrılığı prensibi gereği; Kurumsal SOME'nin, kurumun Bilgi İşlem Birimi (şube, daire, başkanlık vb.) altında ayrı bir birim olarak kurulması tavsiye edilir. SOME Birimi ve Bilgi İşlem sistem ve ağ birimlerinin görev, yetki ve sorumlulukları birbirinden farklıdır. SOME ekibi uygulama seviyesinde sisteme müdahale edebilir. Bilgi İşlem sistem ve ağ birimleri Siber Güvenlik Birimi alanlarına müdahale edemez. Bilgi İşlem Sistem Birimi sunucuları kurar ve bakımlarını yapar ancak Siber Güvenlik Birimi uygulama seviyesinde kayıt yönetimi, saldırı tespit, engelleme ve raporlama işini ve kurum sistem, ağ ve personelini siber saldırılardan korumakla yükümlüdür. Kurumlar, ilgili birime personel takviyesi yapmalıdır. Siber Güvenlik Biriminin başında en az lisans düzeyinde personel bulunmalıdır. Kurum dışı (vatandaşlar, diğer kurumlar, vb.) ve kurumdaki çalışanlara hizmet amacıyla yürütülen bilgi işlem birimi ağ ve sistem işletim faaliyetleri Kurumsal SOME'den ayrıdır. 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. Bu iki görev birbiri ile çatışan görevler olup bu görevleri yapan ekipler arasında "görevler ayrılığı" prensibinin uygulanması gerekir. Bu ilkenin tam anlamıyla uygulanabilmesi amacıyla Bilgi İşlem Biriminin sistem işletimi fonksiyonları ile Kurumsal SOME fonksiyonlarının farklı personel tarafından yapılması önem arz etmektedir.

1.1.Ulusal Siber Olaylara Müdahale Merkezi (USOM) Nedir?

Dünyada bilgi ve iletişim teknolojilerinin hızlı ve yaygın kullanımı ile siber ortam tehditlerinde sürekli artış görülmektedir. Ülkeler siber güvenliklerini sağlamak amacıyla idari, teknik ve hukuki alt yapılar hazırlamaktadırlar. Ülkemiz adına konunun önemi dikkate alınarak "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar" 20.10.2012 tarihli Resmi Gazete de Bakanlar Kurulu Kararı olarak yayınlanmıştır. Bu karar ile program, rapor, usul esas ve standartları onaylamak, uygulamak ve koordinasyonu sağlamak amacıyla "Siber Güvenlik Kurulu" oluşturulmuştur.

Siber Güvenlik Kurulu gerçekleştirdiği ilk toplantıda Ulusal Siber Güvenlik Stratejisi eylem planı kapsamında ülkemizde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması adına "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurularak faaliyetlerine başlamıştır. İnternet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyon USOM vasıtasıyla gerçekleştirilecektir.

Siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri de yapacak olan USOM, kritik sektörlere yönelik siber saldırıların önlenmesinde koordinasyonu sağlayacaktır.

SOME ise sektör ve kurum bazında kurulacak olan Siber Olaylara Müdahale Ekiplerinin kısaltmasıdır. Sektörel ve Kurumsal SOME olmak üzere iki farklı alanda mevcut olacaklardır. USOM ve SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde hayati önemi olan yapılardır. Bu yapıların koordineli ve daha etkin çalışabilmesi, işbirliği halinde olması ulusal siber güvenliğe çok büyük katkı sağlayacaktır.

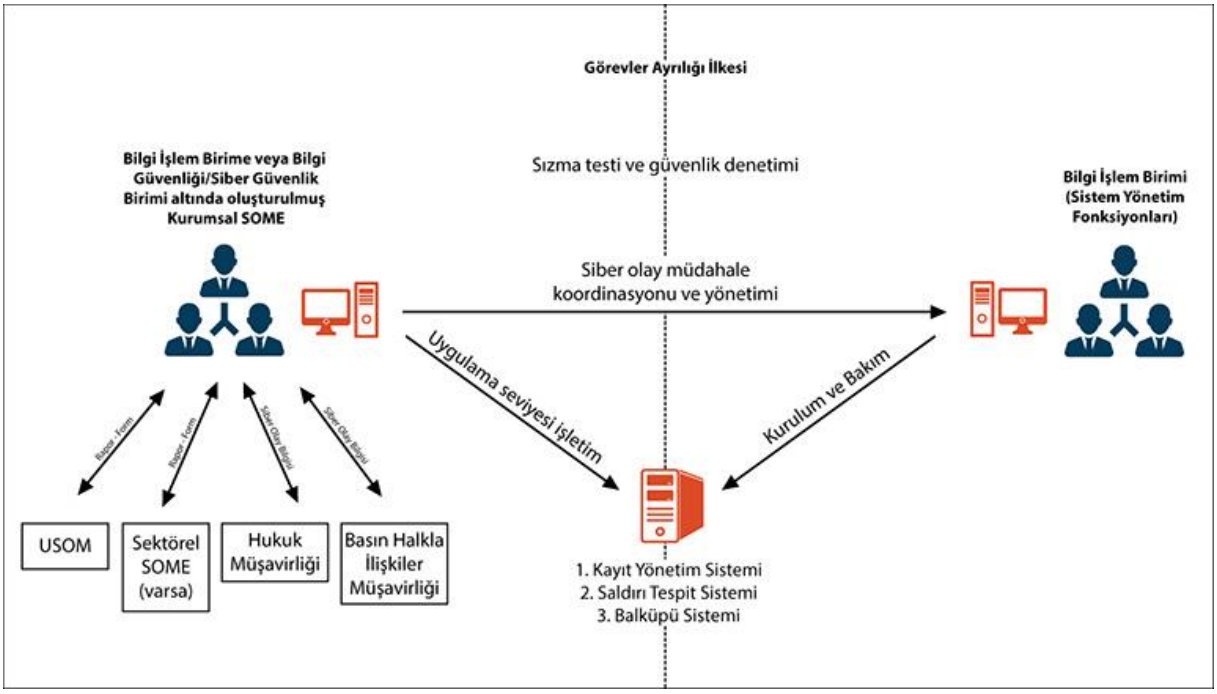
1.2.Kurumsal SOME Kurulumu Hakkında

Kurumsal SOME'ler Bakanlıkların bünyesinde, hizmet gereklerine göre, Bakanlık birimlerini, bağlı, ilgili ve ilişkili kurumlarını kapsayacak şekilde kurulur. Ancak Bakanlık koordinesinde Bakanlık birimleri, bağlı, ilgili ve ilişkili kurum ve kuruluşları altyapılarının önem ve büyüklüğüne göre kendi bünyelerinde bir kurumsal SOME kurabilirler. Kurumsal SOME'lerin kuruluşunun eşgüdümü Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yürütülür.

SOME'lerin nasıl yapılandırılacağı, hangi birim içinde çalışacağı, kurumun diğer birimleri ile ilişkileri, bilişim ve endüstriyel kontrol sistemlerinin yapısı da dikkate alınarak ilgili Bakanlık veya kurum tarafından belirlenir. SOME'nin kurulumu kurum içerisinde uygun yöntem ile duyurulur.

1.3.Kurumsal SOME'lerin Görev ve Sorumlulukları

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. Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar. Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini varsa birlikte çalıştığı sektörel SOME ile eşgüdüm içerisinde yürütürler. Durumdan gecikmeksizin USOM'u haberdar ederler. Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar. Bunun mümkün olmaması halinde varsa birlikte çalıştığı sektörel SOME'den ve/veya USOM'dan yardım talebinde bulunabilirler. Kurumsal SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler. Kurumsal SOME'ler kurumlarına yapılan siber olayları raporlar ve gecikmeksizin USOM ve birlikte çalıştığı sektörel SOME'ye bildirirler. Kurumsal SOME'ler USOM ve/veya birlikte çalıştığı sektörel SOME tarafından iletilen siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak kurumlarında gerekli tedbirleri alırlar. Kurumsal SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler. Siber Güvenlik Birimi USOM, Sektörel SOME, Hukuk Müşavirliği ve Basın Halkla İlişkiler Müşavirliği ile siber olaylar konusunda iletişim halinde olmalıdır. Kurum dışı (vatandaşlar, diğer kurumlar, vb.) ve kurumdaki çalışanlara hizmet amacıyla yürütülen bilgi işlem birimi ağ ve sistem işletim faaliyetleri Kurumsal SOME'den ayrıdır. 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. Bu iki görev birbiri ile çatışan görevler olup bu görevleri yapan ekipler arasında "görevler ayrılığı" prensibinin uygulanması gerekir. Bu ilkenin tam anlamıyla uygulanabilmesi amacıyla Bilgi İşlem Biriminin sistem işletimi fonksiyonları ile Kurumsal SOME fonksiyonlarının farklı personel tarafından yapılması önem arz etmektedir. Kurumsal SOME'nin kurum içi ve kurum dışı paydaşları aşağıdaki grafikte gösterilmiştir.



Bir Kurumsal SOME siber olay öncesi, esnası ve sonrasında, siber güvenliği yönetmek amacıyla USOM, Sektörel SOME, hukuk müşavirliği, basın ve halkla ilişkiler müşavirliği ve Bilgi İşlem Birimi ile birlikte çalışır. Kurumsal SOME, kayıt yönetim sisteminin sahibidir. Saldırı tespit sistemi, Güvenlik duvarı ve kurulu ise balküpü sisteminin uygulama seviyesi işletimi ile ilgili olarak ise politikaların belirlenmesini sağlar. Kurumsal SOME, siber olay öncesinde sızma testi yaptırır, siber olay sırasında olay müdahaleyi yönetir ve Bilgi İşlem Birimindeki ilgili personeli koordine eder. USOM ve/veya Sektörel SOME'ye siber olay ile ilgili rapor veya form gönderir. Kurum bünyesindeki hukuk müşavirliği ile basın ve halkla ilişkiler müşavirliğine yaşanan siber olay ile ilgili bilgi notu hazırlar. Kurulacak olan Kurumsal SOME için hâlihazırda bilgi işlem bünyesinde görev yapan personelin SOME kurulumunun ilk aşamasında ikiz görevli olarak görevlendirilebileceği, ancak nihai hedef olarak ayrı bir uzmanlık gerektiren bu konuda ayrı bir personel istihdamı yapılmasının uygun olacağı değerlendirilmektedir.

1.4. *Kurumsal ve Sektörel SOME'lerin yapısı*

SOME'lerin Bakanlık ve diğer kurumlar içinde nasıl yapılandırılacağı, hangi birim içinde çalışacağı, Bakanlığın veya kurumun diğer birimleri ile ilişkileri, bilişim ve endüstriyel kontrol sistemlerinin yapısı da dikkate alınarak ilgili Bakanlık veya kurum tarafından belirlenir ve kurum içerisinde uygun yöntem ile duyurulur. SOME'ler kurumların bilişim ve endüstriyel kontrol sistemlerinin büyüklük ve kritikliği dikkate alınarak meydana gelebilecek siber olaya müdahale edebilecek yeterlilikte personel ve teçhizatla desteklenirler. SOME'ler; bilgi güvenliği, bilişim ağları, yazılım ve sistem uzmanlığı gibi alanlarda bilgili ve tecrübeli personel öncelikli olmak üzere ilgili bakanlık ve kurumların belirleyeceği personelden teşkil edilir. SOME'ler siber olaylara imkânları dâhilinde 7/24 esasına göre müdahale ederler. SOME'ler, ilgili kurumların teşkilat yapılarına ve hizmet gereklerine göre farklı birim personelinden oluşturulabilir.

1.5. *SOME'lerin USOM'la ilişkisi*

SOME'lerin USOM ile ilişkilerini varsa birlikte çalıştıkları sektörel SOME'ler üzerinden yürütmesi esastır. Birlikte çalıştıkları bir sektörel SOME olmayan kurumsal SOME'ler, faaliyetlerini doğrudan USOM ile koordineli yürütürler. Siber olaylar ile ilgili olarak diğer ülkelerin eşdeğer makamları ve uluslararası kuruluşlarla işbirliği USOM tarafından yerine getirilir. USOM gerekli gördüğü durumlarda kurumsal SOME'ler ve sektörel SOME'ler ile doğrudan çalışma yürütebilir.

Kurumsal/Sektörel SOME'ler siber olayların tespiti, önlenmesi, zararlarının en aza indirilmesi gibi konularda USOM tarafından geliştirilen veya yürütülen projelerin gerçekleştirilmesinde USOM ile işbirliği içerisinde hareket ederler.

1.6.*SOME Personeli için Tavsiye Edilen Eğitimler*

Eğitimler, Kurumsal SOME personelinin sistemli bir şekilde kayıt analizi ve yönetimi yapabilmesi, Kurumun bilgi sistemlerindeki önemli güvenlik açıklıklarını tespit edebilmesi ve siber olay müdahale koordinasyonu yapabilmesi için gerekli olan temel yetkinlikleri vermeyi hedeflemektedir.

Açıklık analizi başlığı altında bulunan eğitimler ile Kurumsal SOME personelinin bir siber olay gerçekleşmeden önce sistemlerindeki önemli açıklıkları tespit etmesi ve karşı önlem uygulamasını koordine etmesi için gerekli yetenekleri kazanması sağlanacaktır.
Kayıt yönetimi başlığı altında bulunan eğitimler ile Kurumsal SOME personelinin sistemdeki kayıtları takip edebilmesi ve sistemler ile ilgili durumsal farkındalık kazanabilmesi sağlanacaktır.
Siber olay müdahale alt başlığında bulunan eğitimler ile bir siber olay gerçekleştiğinde Kurumsal SOME personelinde bulunması gereken temel teknik yetenekler ile siber olay müdahale koordinasyonu yeteneği kazanılmış olacaktır.
Bilgi güvenliği yönetimi başlığı altındaki eğitimler ile bilgi güvenliğinin/siber güvenliğin bir sonuç değil, bir süreç olduğu ve bu sürecin sağlıklı işlemesi için nelerin yapılması gerektiği kavratılacaktır. Siber suç işlendiğinde delillerin geçerliliğinin bozulmaması için alınacak tedbirler belirtilecektir.

1.7.*Siber Olayda SOME'nin Rol ve Sorumlulukları*

Kurumsal SOME'lerin siber olay öncesi, siber olay esnası ve siber olay sonrasındaki temel görev ve sorumlulukları olarak üç bölüme ayrılmıştır. Kurumsal SOME'ler görev ve sorumluluklarını yerine getirirken, Sektörel SOME'ler veya USOM ile koordinasyon ve iletişim içerisinde bulunurlar. Ayrıca faaliyetleri kapsamında USOM, **Sektörel SOME** ve kurum üst yönetimini ilgilendiren rapor ve formlar oluştururlar. Oluşturulan bu dokümanların güvenli şekilde iletilmesi ve muhafaza edilmesi için gerekli düzenlemeleri sağlar.

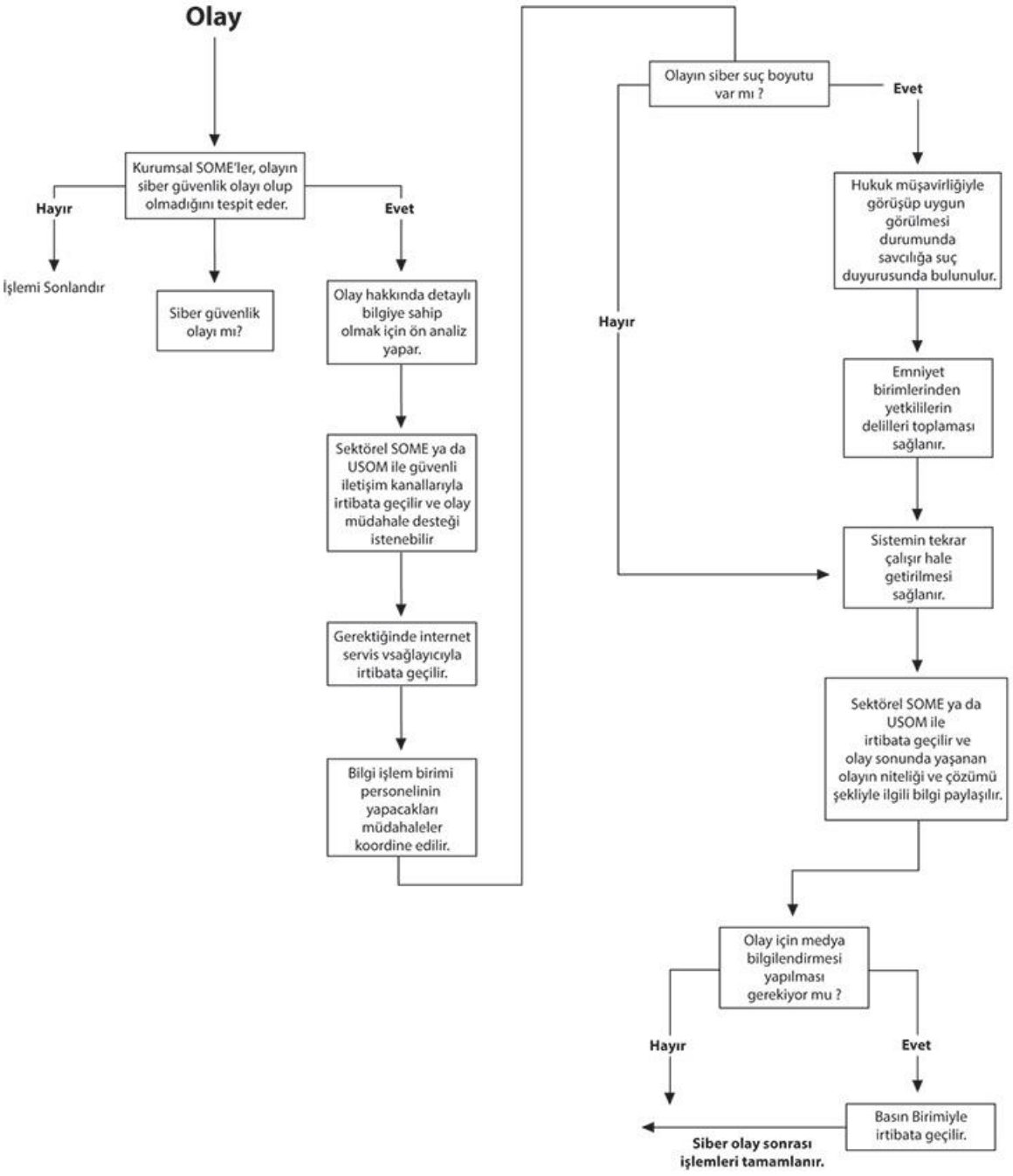
Kurumsal SOME'lerin oluşturabileceği dokümanlar, bu dokümanları hangi paydaşlarla paylaşabileceği ve oluşturma periyotları, talep edilen dokümanların sayısına, tipine, içeriğine, detay seviyesine ve gönderim periyoduna USOM ve varsa Sektörel SOME karar verecektir. Ayrıca Kurum üst yönetimi de Kurumsal SOME'den farklı tiplerde dokümanlar talep edebilir. SOME çalışanları Kurumsal SOME'nin kurulduğu yere bağlı olarak bilgi işlem yöneticisine veya bilgi güvenliği/siber güvenlik birimi yöneticisine bağlıdır; Kurumsal SOME personeli arasında hiyerarşik yapılanma şart değildir. Yurt dışı bağlantılı siber olaylar için USOM'la iletişime geçilmesi, siber olayların USOM üzerinden çözüme kavuşturulması tavsiye edilir. Ayrıca yurt dışı temsilciliği olan kurumlarda yaşanacak siber olaylarda da aynı şekilde USOM'la iletişime geçilmesi tavsiye edilir.

Siber Olay Öncesi

Kurumda bir siber olayın yaşanmadığı veya gerçekleşmediği durumda Kurumsal SOME'ler, kurum içi farkındalık çalışmalarının gerçekleştirilmesi, kurumsal bilgi sistemleri sızma testlerinin yapılması / yaptırılması ve kayıtların düzenli olarak incelenmesi çalışmalarını yaparlar.

Siber Olay Esnası

Kurumda herhangi bir siber durum da SOME'ler öncelikle bir olayın siber olay olup olmadığı değerlendirirler. Eğer bir siber olaysa, olay hakkında detaylı bilgiye sahip olmak için ön analiz yapılır. Bu aşamada Sektörel SOME ya da USOM ile güvenli iletişim kanallarıyla irtibata geçilir ve olay müdahale desteği istenebilir. Ayrıca gerektiğinde internet servis sağlayıcıyla da irtibata geçilir. Bilgi işlem birimi personelinin yapacakları müdahaleler koordine edildikten sonra siber olayın, bir siber suç boyutunun olup olmadığına karar verilir. Hukuk müşavirliğiyle görüşüp uygun görülmesi durumunda savcılığa suç duyurusunda bulunulur ve emniyet birimlerinden yetkililerin delilleri toplaması sağlanır. Daha sonra sistemin tekrar çalışır hale getirilmesi sağlanır. Sektörel SOME ya da USOM ile önceden belirlenen iletişim kanalı üzerinden iletişime geçilir ve olay sonunda yaşanan olayın niteliği ve çözümü şekliyle ilgili bilgi paylaşılır. Siber olay için medya bilgilendirmesi yapılması gerekiyorsa Basın ve Halka İlişkiler Birimi'yle irtibata geçilir.



Siber Olay Esnasında Yapılması Gereken İşlemler Grafiği

Siber Olay Sonrası

Bir siber olay gerçekleştikten ve olaya müdahale edildikten sonra Kurumsal SOME'ler aşağıdaki görevleri icra ederler:

1. Siber Olay Bildiririmleri ve kayıt altına alınır.
2. Olaydan çıkarılan dersler kayıt altına alınır.
3. Olayla ilgili olarak gerçekleştirilebilecek düzeltici / önleyici faaliyetlere ilişkin öneriler kurum yönetimine arz edilir. Siber olayların türleri, miktarları ve maliyetleri ölçülüp izlenir.

II. Siber Güvenlik Temelleri:

1. Terimler:

Siber Güvenlik: Siber ortamda; kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür.

Siber Saldırı: Hedef seçilen şahıs, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır.

Siber Savaş: Aynı saldırıların ülke veya ülkelere yönelik yapılmasıdır. Siber savaşta hedef ülkelerin güvenlik, sağlık, enerji, haberleşme, su ve kanalizasyon, bankacılık ve kamu hizmetleri gibi kritik altyapıları saldırı alanı olarak seçilmektedir.

Siber güvenlik zaafları ülkelerin fiziksel savaşlardan daha fazla zarar görmelerine sebep olabilmektedir. Ülkeler siber güvenliklerini sağlamak için stratejiler ve politikalar belirlemektedir. G8 ülkelerinden birinin devlet başkanının şu sözleri siber güveliğin önemini vurgulamaktadır: “ 19. yy da ulusal güvenliğimizi korumak için deniz ve hava güvenliğimizi sağlamak zorundayken 21. yy da kamu kurum ve kuruluşlarımız ile işletmelerimizin sanal dünyadaki güvenliğini sağlamak zorundayız.

Ülkelerin kurum ve kuruluşlarına yönelik siber saldırıların, sanal dünya ağının çok geniş kitlelere ulaştığı ve kullanıldığı tespiti dikkate alındığında herhangi bir kaynaktan gelebileceği görülmektedir. Bu durum evrensel kuralların uygulanmasını zorunlu kılmaktadır. Siber güvenlik yaklaşımları belirlenirken dikkate alınan bazı unsurlar; Ulusal politika ve stratejinin belirlenmesi, yasal çerçevenin oluşturulması, teknik tedbirlerin alınması, bütün sistem, şebeke ve alt yapıların birbiriyle bağlantılı olduğu, her birinin güvenliğinin sağlanmadan tam bir güvenlikten bahsedilmeyeceği unutulmamalıdır. Teknolojinin sürekli gelişmesi siber tehdit araçlarının da değişmesine neden olmaktadır. Bu nedenle, uygulama geliştirici teknik personel, yönetim birimleri, hukukçular ve kanun koyucuların teknolojiyi yakından takip ederek bilgi

birikimlerini geliştirmeleri gereklidir. En zayıf halka olan son kullanıcıların siber tehdit araçları ve korunma yolları konusunda bilgilendirilmesi gerekmektedir. Siber saldırıların yol açmış olduğu maddi ve manevi zararlar tehlikenin boyutunu anlamak açısından önem arz etmektedir. 2007 yılında Estonya'ya gerçekleştirilen siber saldırı, 2010 yılında Çin'de Google ve diğer sitelere yapılan Aurora kod adlı saldırılar, 2008'de Microsoft ürünlerini hedef alan Conficker adındaki solucan, İran nükleer programını hedef alan Stuxnet solucanı ve 2014 Amerika firması SONY'yi hedef alan ciddi boyutlarda zarara yol açan siber saldırılar saldırıların her kesimi, her ülkeyi, her kurumu hedef alabileceğini ortaya çıkarmıştır.

Siber güvenliği sağlarken göz önünde bulundurulması gereken tespitler:

- Temel hak ve hürriyetler korunmalıdır.
- Demokratik toplum düzeninin gereklerine uyulmalıdır.
- Ölçülülük esası temel alınmalıdır.
- Güvenlik politikası kısıtlayıcı olmaktan ziyade koruyucu olmalıdır.
- Güvenlik politikaları sonuçlarından etkilenecek kişilerle istişare ile oluşturulmalıdır.
- Genel bir yaklaşımla idari, teknik, hukuki, ekonomik, politik ve sosyal parametreleriyle ele alınmalıdır.
- Politikaların, kurum ve kuruluşların özgün yapısına uygun olarak, ihtiyaçlara yönelik olarak hazırlanması.
- Diğer ülke mevzuatlarının göz önünde bulundurulması.
- Ulusal ve uluslararası işbirliğini esas alınması.
- Özel hayatın gizliliği prensibine uygun olarak izleme ve kollamanın yapılması.
- İstatistiki verilerin kullanımı gereksinimi ortaya çıktığında son kullanıcıların onayı ile verilerinin kullanılması ve ifşa, teşhir, zan altında bırakma gibi mağduriyet yaratacak eylemlerden kaçınılması gerekmektedir.
- Kurumsal kimliğe bağımlı olarak stratejiler geliştirilmelidir.
- Ulusal politikalar ve stratejiler göz önünde tutularak tedbirler alınmalıdır.

Siber Saldırılara karşı koruma sağlarken referans alınabilecek kurallar şunlardır:

- Bölgesellik kuralı: Kurum ve kuruluşlar her türlü siber saldırı durumunu karşı yerel tedbir almak ve güvenlik politikaları belirlemekle mükelleftir.
- Sorumluluk Kuralı: Kurum ve kuruluşlar, Bilgi İşlem sistemlerine yapılan her türlü saldırıyı önleyici tedbirler alma sorumluluğuna sahiptir.
- İşbirliği Kuralı: Kurum ve kuruluşlar siber saldırıları bertaraf etmek için kurumsal ve sektörel somelerle güvenlik temelli politikalar oluşturmak, önleyici tedbirler almak ve destekleyici eylemlerde bulunma gibi yollara başvurmalıdırlar.
- Öz-Savunma Kuralı: Kurum ve kuruluşlar kendilerine tehdit olarak gördükleri hedeflere önleyici tedbir alabilirler.
- Veri Koruma Kuralı: Bir bireyin ağ üzerinde bulunan herhangi bir verisi AB'nin Veri Koruma Yönergesine göre kişisel veri kabul edilmiştir. Bu bakımdan bir kişinin ağ

üzerindeki IP adresi yasa dışı yollardan elde edilirse hukuki olarak delil kabul edilmez. Bireyin bilgilerini konumlandırdığı platformun kullanım hakları sözleşmesinde geçmesi dışında farklı yerlerde kullanılması, paylaşılması, istatistiki amaçlı kullanılması legal değildir. Bireyin verileri şayet başka bir ülkenin sanal platformlarında olsa bile verilerin orada korunması zorunludur. Verilerin kullanımı gibi suistimal durumlarında ilgili bireyin özel hayatının korunması gibi koruyucu mevzuatlar devreye girer.

- Bakım Kuralı: AB'nin Veri Koruma Yönergesine göre, kişiler ağ üzerinden ya da yasal olmayan yollarla erişime karşı verilerin yanlışlıkla veya kasıtlı olarak yok edilmesine, değiştirilmesine, yetkisiz kişilere açıklanmasını önlemek amacıyla her türlü teknik ve operasyonel önlemi almakla sorumludur. Aynı şekilde Avrupa Konseyi Sözleşmesi'nde kişilerin verilerini her türlü veri kaybı, yetkisiz kişilerin erişimi ve verilerin üçüncü kişilere açıklanması ile değiştirilmesini önlemek amacıyla gerekli önlemleri alması zorunluluğu hükmü bulunmaktadır.
- Erken Uyarı Kuralı: Olası saldırı durumlarında hiyerarşik olarak ilgili kesimlere tedbir amaçlı erken uyarıda bulunmak gerekmektedir. Servis sağlayıcılar her türlü teknik ve organizasyonel önlemleri almak, Siber güvenlik birimi son kullanıcıları bilgilendirmek ve önleyici tedbir almakla mükelleftir. Bireylerin yaşam, güvenlik ve refahına yönelik tehditler hakkında bilgi alma hakkı vardır. Bu önleyici tedbir alma ve kamu bilincini artırma yönünde katkı sağlayacaktır.

III. Siber Güvenlik Analizi:

Kurum kendisine özel Güvenlik Riski Analizini yapmalıdır. Bilgi sistemine dönük herhangi bir saldırıyı önleyici tedbir almanın temel koşulu risk analizi sonucu kalabileceği saldırıları öngörebilmekten geçmektedir. Yapılan incelemelerde siber saldırıların her geçen yıl artış gösterdiği tespit edilmiştir. Bu nedenle yapılacak risk analizleri:

- Sistem, ağ ve bilgi yönetimini geliştirmek,
- Birincil derecede önemli sistemlerin, belgelerin ve servislerin izlenmesi ile korunması gibi tedbirler almada,
- Siber saldırılara karşı etkin bilgi güvenliği sağlamak,
- Organizasyonel anlamda pratik politikalar belirlenmesinde,
- İleriki süreçler için değerli veri analizlerinin yapılmasında,

Önemli rol oynamaktadır.

Sistemlerin uğrayabileceği siber saldırıları bertaraf etmede kullanılabilecek yöntemler:

- Sistemlere Erişimin kontrollü yapılmasını sağlamak. Şifre tanımlamaya dayalı sistemler, akıllı kart geçiş sistemleri kullanmak kimlik doğrulamada kullanılabilir.

- Şifre kullanımının kompleks yapıda kullanılması gerekmektedir. Yazılımsal erişimlerin her seviyesinde kontrollü şekilde güçlendirilmiş şifre algoritmaları kullanılmalıdır.
- Sistemlerin siber saldırılara karşı korunmasında kullanılabilecek saldırı tespit sistemi (IDS), Güvenlik Duvarı, Anti Bot, Anti Spam gibi önleyici tedbirler alınmalıdır.
- Servislerin güvenliği kapsamında ise kullanılan veri tabanları gibi yazılımların sağlam güvenlik şifreleri ve protokolleriyle korumaya alınmış olması gerekmektedir. Sistem config dosyaları güncel olarak yedeklenmelidir.
- Kurum sistem ve ağ alt yapısı birincil olarak fiziksel saldırı etkenlerine maruz kalmaması için tesis güvenliği, sistem odası güvenliği, kurum güvenliği, giriş çıkış kontrolü gibi tedbirler alınmalıdır.

Güvenlik Açığı kaynaklı Saldırılar:

- Sıfır gün saldırıları: Genellikle kötü niyetli korsanlar tarafından keşfedilen açığın, yama tarihinden önce kullanıldığı saldırılardır.
- Sözde sıfır gün saldırısı: Piyasaya sürülen yamanın sisteme eklenmesi kaynaklı saldırılardır.
- Olası sözde sıfır gün saldırısı: Bu saldırı tipinde düzeltme yayınlanmış ama saldırıya uğrama olasılığı hala gündemdedir.
- Saldırı olasılığı: Sistem açığının bulunmuş, ilgili yamanın hazırlanmış fakat dağıtımının yeterli yapılamadığı durumlarda gerçekleşme ihtimali olan saldırı tipidir.

Siber savunmanın temel unsuru tehdit seviyelerine göre güvenlik politikaları oluşturmaktır. Siber tehditlere karşı kurumun misyonu belirlenmeli, belirlemeler yapıldıktan sonra ise bu misyon doğrultusunda önlemler alınmalıdır. Bu önlemler: görev dağılımlarının yapılması, strateji planı oluşturulması, güvenlik yatırımlarının yapılmasıdır. Siber saldırılar yapılış şekline göre farklı kategorilere ayrılabilirler. Veri hırsızlığı, dolandırıcılık, sabotaj, hizmet alınmasını aksatma, casusluk, dinleme, izleme, prestij sarsıcı saldırılar ve benzeri olabilmektedir.

Bu saldırılar yapılırken; truva atı, virüs, klavye dinleme, casus yazılımlar kullanma, spam postalar, güvenlik açıkları zafiyetleri gibi yollarla verileri elde etme, değiştirme, yok etme gibi yollara başvurulabilir. Bu saldırı tipleri yazılım destekli olabileceği gibi donanımsal destekli de olabilir. Klavyeye entegre edilen dinleme cihazları gibi aksesuarlarla tüm şifreleriniz, dosya isimleriniz, dosya içerikleriniz gibi verilerinizi çaldırabilirsiniz. Saldırıların kolay yapılabildiği ortamlarda siber saldırıları zaaflarındandır. Güvensiz ağ alt yapısına sahip ortamlar kullanıcıların mağduriyetine sebep olabilmektedir. Havaalanı, otogar, park ve cafeler gibi herkesin kullanımına açık kablosuz bağlantılardan bankacılık işlemleri yapmak, man in the middle yöntemiyle araya giren şahıslar tarafından zayıf güvenlik protokolleri ile korunan ağ yüzünden maddi manevi zararlar doğabilmektedir. Sosyal mühendislik dediğimiz yolla kurbanlar kendi sistemlerinin, bilgisayarlarının ya da kullanmış oldukları servislerin şifrelerini kötü amaçla kullanabilecek kimselere kaptırabilmektedirler. Burada tahmin yoluyla şifre bulma, kişinin hobileri, doğum yeri ve tarihi, tuttuğu takım, il plaka kodu gibi isim ve rakamları

kullanarak şifre ele geçirilir. Bu saldırı tipini önlemede siber saldırıların doğurduğu mağduriyetlerin toplum tarafından bilinmesi ve bilinçli olunması yoluyla önlemler alınabilir. DOS (Denial of Service) ve DDOS (Distributed Denial of Servisi) gibi siber saldırı tipinde ise tamamıyla sistemi hedef alır, servislerin hizmetlerini durdurma yoluyla prestij kaybına yol açma şeklinde yapılmaktadır. Bu saldırlar bilginin erişebilirlik kuralını hedef alır; sistemi, sunucu ya da uygulamanın cevaplayabileceğinden fazla sayıda istek göndererek sistemi durdurma noktasına getirir. Yazılım tarafında dikkat edilmesi gereken en önemli açık ise SQL enjeksiyonudur. Bu saldırı tipinde veri tabanında yapılan sorgulama işlemi hedef alınır. HTML Enjeksiyonu yöntemi ile oturum ve çerez hırsızlığı yapılıp, saldırganın amaçlarına hizmet edecek şekilde kullanılmasıdır. Programcıların kodlama esnasında yaptığı hatalar açıklara sebep olmaktadır.

IV. Kurumsal Ağ ve Sistem Alt Yapısının Korunması:

1. Alt Yapısının Korunmasına Dönük tedbirler:

1.1. Ağ alt yapısındaki tüm cihazlar belli bir topoloji temel alınarak konumlandırılmış olmalıdır. Siber saldırı esnasında fiziksel olarak aktif cihaza erişim sağlamak açısından önemlidir.

1.2. Ağ alt yapısındaki tüm cihazların kablolarında etiketlendirme yapılmış olmalıdır. Dağınıklığın giderilmesi ve belli bir düzenin tutturulması personel bağımsız müdahaleyi kolaylaştırır ve zamandan kazanç sağlar.

1.3.Tüm aktif cihazların konfig dosyalarının yedekleri düzenli olarak alınmalıdır. Bu yedekler birey bağımsız belli sunucularda barındırılmalıdır.

1.4. Tüm aktif cihazlarda kullanılan parolaların rakam, harf ve özel karakterlerden oluşan karma yapıda olması önemlidir.

1.5. Mümkün ise en geç üç ayda bir parolalar değiştirilmelidir.

1.6. Cihaz erişimlerinin Telnet yerine güvenli erişim protokolleri destekleyen Secure Shell (SSH) üzerinden yapılması.

1.7. Simple Network Management Protokol (SNMP) genel isimlerinin (Community Name) default gelenlerin dışında farklı isimlendirilmesi. Tuhaftır; çalışmalar esnasında denk geldim, Neutron marka kameraların default kullanıcı adları 666666, default passwordleri ise 666666 idi. Tüm üreticiler bir problem olması durumunda aktif cihazlarına erişim yapabilmek adına bu şekilde default şifreler yaratabiliyorlar. Siber saldırıyı yapacak kişiler sosyal mühendislikte ilk olarak bu yöntemlere başvurmaktadır.

1.8. Simple Network Management protokolünün minimum Version 2 seviyesinde olması güvenlik için gereklidir.

1.9. TCP Dump, MRTG, CACTİ gibi 3rd parti yazılımlarla trafiğin izlenmesi zombi saldırılarının tespiti, kirli trafiğin izlenmesi ve loop gibi internet trafiğini kısıtlayan uygulamaları takip etmeyi kolaylaştırmaktadır. Kullanılması ciddi katkılar sunacaktır.

1.10. Netflow, Sflow gibi yazılımlarla layer 4 seviyesinde trafiğin izlenmesi kirli trafiği önlemede yardımcı olacaktır.

1.11. Tüm aktif cihazlara erişecek son kullanıcıların IP adreslerinin cihazlar üzerindeki ACL ile belirlenmesi gerekmektedir.

1.12. Kenar switchler üzerinde DHCP Snooping ve ARP (Address Resolution Protokol) Protect gibi koruyucu protokollerle desteklenmelidir.

1.13. Tüm sahada Port Security gibi dışardan ağa cihaz bağlanmasını kısıtlayacak protokollerin uygulanması gerekmektedir.

1.14. Mümkün olduğu sürece dışardan müdahaleye açık bırakmamak için aktif cihazlardaki Telnet ve http/s servislerinin devre dışı bırakılması gerekmektedir.

1.15. Ağ da anti bot, anti virüs, anti spam gibi koruyucu yazılımlar güvenlik duvarının destekleyici olarak bulunmalıdır.

1.16. Saldırı Tespit Servislerinin kullanılması suretiyle DoS ve DDoS gibi saldırılar için ağ trafiğinin kısıtlanması gibi önlemler alınmalıdır. Ya da saldırıların yapıldığı portların geçici olarak devre dışı bırakılması sağlanmalıdır.

1.17. Kurum ağında odalarda ayrıca switch access point gibi cihazların kullanımı engellenmelidir. Özellikle dhcp snooping engelleme yapılmalıdır. DHCP için ip kiralama süresi ideal olarak 8 ile 24 saat arasında tutulmalıdır.

1.18. LAN ve WAN Flood Tespit, AntiSpoof servisleri aktif olarak kullanılmalıdır.

1.19. 5651 yasasının gereksinimlerinin karşılanması amacıyla MAC-IP eşleştirme, kayıt alma gibi servisler aktif olarak kullanılmalıdır.

1.20. Web filtreleme, Sayfa Yasaklama, URL ve Uzantı Filtreleme yoluyla web üzerindeki trafik kontrollü yapılması sağlanmalıdır.

1.21. Güvenlik Duvarının aktif olarak çalışması sağlanmalıdır. Saldırı Tespit servisleri aktif olarak çalışmalıdır.

1.22. E-Posta Sunucuları ve istemci makinelerine anti virüs yazılımları yüklenmeli ve devamlı güncellemeleri yapılmalıdır.

1.23. Son kullanıcılarda sistem güncellemeleri belirli aralıklarla yapılmalıdır. Güvenlik yamalarının giderilmesi hususunda son kullanıcılar bilgilendirilmelidir.

1.24. Dış ve iç sistemler arasında güvenilir şifreli uygulamalar kullanılmalıdır. (VPN, SSH, Proxy..)

1.25. Mümkünse sistem servislerinin güvenliği için DMZ bölgeleri oluşturulmalıdır.

1.26. Taşınabilir sistemlerin; dizüstü bilgisayarlar, flaş sürücüler, harici hard diskler gibi aparatlar iç ağda kullanılmadan evvel anti virüs taramasından geçirilmesi konusunda son kullanıcılar bilgilendirilmelidir.

1.27. Tüm sunucular dış bağlantıya, uzak erişime kapatılmalıdır.

1.28. Sunuculara erişimde komplex şifreler kullanılmalıdır. Password, 1q2w3e, isimler, doğum tarihleri, plaka kodları kullanılmamalıdır.

1.29. Tüm sunucular üzerindeki yazılımların periyodik olarak güncellemesi yapılmalıdır.

1.30. Ağdaki tüm erişimlerde web, mail, pdks, yordam gibi sunucuların gereksinim duyduğu portlar dışında tüm portlar kapalı tutulmalıdır. Saldırı amaçlı kullanılabilmektedirler.

1.31. Kurumdaki yapılara fiziksel güvenlik testleri (Penetrasyon) uygulanmalı ve gerekiyorsa güçlendirilmelidir.

1.32. Mümkün olduğunca tüm sunucuların periyodik olarak sıcak yedekliliğini sağlamak, disaster uyumlu yapıyı kurmak ve güçlendirmek gerekmektedir.

1.33. Servislerde olumsuz bir durum ortaya çıkması durumuna karşılık aktif olarak kullanılabilecek şekilde yedek sunucuları oluşturmak gerekmektedir.

1.34. Web, mail, obs ve ebys gibi servislerin veri hırsızlığına karşı özel olarak korunması sağlanmalıdır.

1.35. Web duyuru ve güncellemelerine bakan tüm personellerin güvenli parola oluşturma, sosyal mühendislik gibi bilgi hırsızlığına karşı duyarlı olması konusunda bilinçlendirilmesi için seminerler vermek gerekmektedir. Ana sayfa duyuruları konusunda mümkün olduğunca az kişiye yetki vermek ve yetkiyi alan kişinin dikkatli davranması konusunda bilinçlendirilmesi gerekmektedir. Aksi halde kurum prestiji açısından çok problem yaratacak bir fotoğraf, duyuru ya da ilan çıkması muhtemeldir.

1.36. Siber güvenlik, sistem ve ağ birimlerinin karşılaştıkları saldırılar, sorunlar ve güncel konular ile ilgili bilgi paylaşımında bulunmaları için ortak mail hesabını aktif kullanmaları gerekmektedir.

1.37. USOM'dan gelen uyarı mailleri dikkate alınmalıdır. Yayınlanan ve duyurulan "Siber Güvenlik Bildirimlerinin" kurumsal kullanıcılara ve sistem yöneticilerine iletilmesi ve gereğinin yapılması sağlanmalıdır.

1.38. USOM tarafından güncel biçimde sunulan "Zararlı Bağlantıların" kurumsal güvenlik cihazlarına kural olarak eklenmesi gerekmektedir.

1.39. Siber olay öncesi ve sonrasında yapılması gerekenlere dair Kurumsal SOMElerin görev ve sorumlulukları dokümanının ilgili kısımlarının gereği yapılmalıdır.

1.40. Kurum bünyesinde mevcut kullanıcıların zombi olup olmadığının tespitinin yapılması, tespit edilememesi durumunda hafta sonu ve akşamları kurum internet trafiğinin kısıtlanması gibi tedbirlerin alınması gerekmektedir.

1.41. Olası siber saldırı durumunda USOM ile doğrudan 0312 586 53 05 veya iletisim@usom.gov.tr yolu ile iletişim kurulması gerekmektedir.

1.42. Olası iç ve dış siber saldırılara karşı risk analizi yapılarak gerekli önlemler alınmalıdır.

1.43. Olası bir siber saldırı durumunda kurum sistemlerinin hızlı biçimde ayağa kaldırılması için gerekli acil eylem planları hazırlanmalıdır.

1.44. Sistem odalarının yetkisiz girişlerin önlenmesi, güçlü şifrelerin belirlenmesi, sistem odalarında çalışma yapılacaksa yetkili personel nezaretinde yapılması gerekmektedir.

1.45. TÜBİTAK Ulakbim Abuse hesabı olan Olta'nın Kurumsal siber saldırılarının olay kayıtlarının incelenmesi ve giderilmesi amacıyla takip edilmesi gerekmektedir.

1.46. Mail yoluyla yapılan phishing, spam, dolandırıcılık gibi siber saldırıların önlenmesi için son kullanıcıların bilinçlendirilmesi çalışmaları sürekli olarak yapılmalıdır.

1.47. Son kullanıcıların karşılaşabilecekleri problemlerin giderilmesi ve sanal dünyadaki güvenlikleri konusunda bilinçlendirilmelerinin sağlanması amacıyla mail ve duyurular yoluyla bilgilendirilmeleri gerekmektedir.

1.48. Siber olay kayıtları Siber Güvenlik Klasörüne raporlanıp eklenmelidir.

1.49. Siber olay yaşanması durumunda olay iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu hazırlanır, üst yönetim, USOM ve ilgili birimlere iletilir.

1.50. Siber Güvenlik Ekibi olay müdahale esnasında bilişim sistemlerine yetkisiz erişim yapılmaması için gerekli tedbirleri alır, aldırır. Suç unsuruna rastlanması durumunda savcılık, kolluk makamlarına haber verilir.

Hafzullah İŞ