**Atatürk Üniversitesi**
**Bilgisayar Bilimleri Araştırma ve Uygulama Merkezi**

# Siber Saldırılara Karşı Eylem Planı

*(DDOS Kapsamında)*

Siber Savunma Ar-Ge Birimi

Şubat 2020

# İÇİNDEKİLER

## AMAÇ ve GEREKÇE

Bu eylem planı, Atatürk Üniversitesi tarafından sağlanan çevrimiçi hizmetlere karşı üç farklı zamanda gerçekleştirilen siber saldırıların sonucunda oluşturulmuştur. Bu saldırılardan, 2019 yılı içerisinde gerçekleştirilen ikisi, BAUM SSAr-Ge birimi tarafından alınan güvenlik tedbirleriyle başarıyla sonlandırılmıştır.

2020 yılı Şubat ayında gerçekeleştirilen saldırı ise; 09.02 günü 21:00 sularında başlayarak 12.02 tarihine kadar sürmüştür. Bu aralıkta saldırı, zarar veremeyecek şekilde engellenmiştir. Ancak; 12.02.2020 tarihinde saldırganın, saldırı boyutunu yaklaşık 30 kat artırması (2GB/s -> 60GB/s) sonucunda, ULAKNET kapasitesi sature edilmiş ve BAUM tarafından alınabilecek tedbirler etkisiz bırakılmıştır.

Bu eylem planı, gelecekte maruz kalınabilecek siber saldırılara karşı gerçekleştirilecek eylemlerin tespitini sağlamak amacıyla SSAr-Ge birimi tarafından önerilmiştir.

Maruz kalınabilecek DDOS saldırıların, edinilen tecrübeler sonucunda iki kategoride incelenebileceği tespit edilmiştir.

1. Kategori: Bant Genişliğini Aşmayan Saldırılar
2. Kategori: Bant Genişliğinin Üzerindeki Saldırılar

Kategorizasyonun temel dayanağı, BAUM tarafından saldırılara karşı tedbir alabilme imkanıdır. Şöyle ki; 1. kategorideki (*bant genişliğini aşmayan*) saldırılara karşı BAUM tedbirler alabilmekte ve hizmetlerin sürdürebilirliğini sağlayabilmektedir. Önlemlerin ne şekilde alınabileceği sonraki bölümde açıklanmıştır.

2. kategoride yer alan (*bant genişliğinin üzerindeki*) saldırılara karşı önlemler ise kurumumuz internet sağlayıcısının yükümlüğündedir. BAUM tarafından gerçekleştirilecek hiçbir güvenlik tedbiri bu saldırılara karşı bir önleyici etki yapamaz.

12.02.2020 tarihinde başlayan ve 2. kategoride yer alan saldırı; kurumumuz internet hizmetlerini bir haftadan uzun süre kesintiye uğratmıştır. Saldırı, internet servis sağlayıcı kurum olan ULAKBİM tarafından tespit edildiği andan itibaren; bir üst sağlayıcı olan Vodafone tarafından güvenlik tedbirleri alınmıştır. Alınan tedbirler sonucunda siber saldırının kurumumuza ulaşması engellenmiş olsa da; aşağıdaki sorunlarla karşılaşılmıştır:

a. Hizmetlerimize yurt dışından erişim tamamen engellenmiştir
b. Hizmetlerin yurt içi erişimleri ciddi şekilde yavaşlamıştır
c. Alınan önlemlerin teknik detayları elde edilememiştir

d. Saldırının seyri, veri istatistiği hakkında bilgi edinilememiştir
e. e-Posta hizmeti ciddi kesintilere maruz kalmıştır
f. Vodafone üzerindeki tüm iletişim ULAKBİM üzerinden yürtülmüştür

Karşılaşılan bu sorunlara karşı Vodafone, ULAKBİM ile aralarında gerçekleştirdikleri sözleşmeye (eKap: 2017/459855) karşı yasal sorumluluğu başlığını yerine getirmiştir. Bu durum, sözleşmede yer alan "4. Madde: DDOS Saldırısı Koruma Hizmeti Teknik Özellikler" başlığının yeteri kadar detaylı olmadığı gerçeğini açıkça ortaya koymaktadır. Nitekim; sözleşmede, basit bir ifadeyle, "önlem alınacaktır" haricinde kayda değer bir detay yer almamaktadır.

BAUM, süreç içerisinde USOM (Ulusal Siber Olaylara Müdahale Merkezi), diğer üniversiteler ve saldırılara karşı tecrübe sahibi çözüm ortakları ile görüşerek; belirtilen sorunlara karşı önerilerini, etki mekanizmaları olan ULAKBİM veya Vodafone'a kabul ettirmek bir yana; saldırı istatisiklerini almak bile günlerce sürmüştür.

Bu doküman, belirtilen sorunların tekrar yaşanmaması için alınabilecek tedbir önerileri sunmayı amaçlamaktadır.

## 1. Kategori: Bant Genişliğini Aşmayan Saldırılar

Her iki kategorideki saldırı, gerçekleştirilme biçimleri açısından aynı olmakla birlikte; 1. kategoride yaklaşık 40.000 saldırı/saniye istek gelmesine karşın; 2. kategoride bu değer, milyonlarla ifade edilmektedir.

2. kategori için alınacak önlemler, 1. kategoride için de koruma sağlayacaktır.

Bu kategoride alınabilecek önlemler:

a. DDOS koruma cihazı alınması
b. Siber güvenlik uzmanı istihdam edilmesi
c. SUNGUR projesinin hayata geçirilmesi

### 1.a. DDOS koruma cihazı alınması

Günümüzde DDOS saldırılarına karşı güvenlik sağlaması amacıyla cihazlar hem yerli firmalar tarafından hem de yurt dışı menşeili olarak üretilmektedir. Bu tür genellikle internet servis sağlayıcılar tarafından kullanılmaktadır.

***Avantajlar:*** Kolay kullanım, yalnızca ürün kullanım eğitimi gerektirmesi
***Dezavantajlar:*** Yüksek maliyet
₺ 500.000 – yerli çözüm (FortiDDoS)
$ 5.000.000 – yurt dışı menşeili (Armor, 10Gb/s)

*Bu başlık altında incelenen yurt dışı menşeili ürünler, ulusal siber güvenlik politikamız ile uyuşmamaktadır. 10.02.2020 tarihinde Cumhurbaşkanımız Recep Tayyip Erdoğan USOM genel merkezi açılışında, "Veri güvenliğini yabancı çözümlerle sağlamaya çalışmak sınır güvenliğini yabancı askerlere emanet etmekle eşdeğerdir."[1] İfadesini kullanmıştır. Ayrıca; bu açıklamanın kurumumuza yapılan saldırının başlangıcı ile aynı gün yapılmış olması dikkat çekicidir.*

### 1.b. Siber güvelik uzmanı istihdam edilmesi

Düşük bant genişliğinde gerçekleştirilen DDOS saldırıları, mevcut güvenlik duvarı üzerinde gerçekleştirilecek IP kısıtlamaları ile önlenebilmektedir. Saldırganların belirlenmesi için

[1]: https://www.iletisim.gov.tr/turkce/haberler/detay/cumhurbaskani-erdogan-ulkemizi-siber-guvenlikte-dunya-capinda-bir-marka-haline-donusturecegiz

tecrübeli bir Siber Güvenlik Uzmanı istihdam edilmesi ve güvenlik duvarı üzerinde yapılacak değişiklikler ile bu tür saldırılar önlenebilir.

| | |
|---|---|
| ***Avantajlar:*** | Düşük maliyet ( yaklaşık ₺100.000/yıl ) |
| ***Dezavantajlar:*** | İstihdam edilecek personelin alım koşulları |
| | Piyasa maaşlarının kamu kurumlarından yüksek olması |
| | Personele bağımlılık |

*Bu başlığın geçerli politika olarak belirlenmesi halinde; sürdürülebilirlik için, planlanmış eğitim programlarıyla yeni personel yetiştirilmesi, 2. ve 3. yedek personelin mevcut olması, faydalı olacaktır.*
*Maliyet karşılaştırması açısından, ilk madde kapsamında alınabilecek bir cihazın 5 yıl sonrasında halen daha etkin koruma sağlaması beklenemez. Ayrıca; kurumun piyasadaki mevcut maaş şartlarına yaklaşması açısından istihdam edeceği personeli mümkün olabildiğince desteklemesi önerimizdir.*

### 1.c. SUNGUR projesinin hayata geçirilmesi

SSAr-Ge birimi tarafından planlanan, prototip olarak üretilerek BAUM ağ trafiğin üzerine yerleştirilen SUNGUR projesi, bir kutu çözüm önerisi sunmaktadır. Prototip cihaz, veri trafiğini kontrol edebilmekte ve planlanan yapay zeka algoritması için hazır halde bekletmektedir. Projenin yeterli kaynaklara ulaşması halinde, 1.a. maddesinde sunulan bir cihaz ortaya koyulabilir.

| | |
|---|---|
| ***Avantajlar:*** | Ar-Ge Faaliyeti |
| | Yüksek katma değer |
| | Ulusal çıkarlara katkı |
| | Ticari faaliyete dönüşebilme potansiyeli |
| ***Dezavantajlar:*** | - |
| ***Gereksinimler:*** | Tam zamanlı çalışma ile yaklaşık 6 ay sürecek istihdam/görevlendirme |
| | Nihai ürün için yaklaşık ₺200bin fon |

*Bu tür yüksek endüstriyelleşme potansiyeline sahip Ar-Ge faaliyetlerinin desteklenmesinin, ASELSAN, ROKETSAN, HAVELSAN gibi başarılı rol modeller örnek alınarak personel-paydaş şekline yapılması önerimizdir. Bu yöntemde ticarileşen ürünün getirisi ciddi bir motivasyon faktörü olacaktır.*

## 2. Kategori: Bant Genişliğinin Üzerindeki Saldırılar

Bu tür saldırılar müdahale edilebilirliği açısından ilk kategoriden farklıdır. İlk kategorideki saldırılarda kurumun elinde yönetim ve gözetim imkanı varken; bu tür saldırılarda üst kuruluşlardan bilgi bekleme modundadır. Bu dokümanın Amaç ve Gerekçe başlığı altında belirtilen tüm sorunların temel nedeni budur.

Çözüm önerilerini belirtmeden önce; karşılaşılan sorunları, gereksinimlerle birlikte tekrar belirtecek olursak:

| *Karşılaşılan Sorun* | *Gereksinim* |
|---|---|
| • *Hizmetlerimize yurt dışından erişim tamamen engellenmiştir* | Önleme politikasının "yurt dışından tüm girişleri engelle" değil; "saldırganları engelle" şeklinde belirlenmesi |
| • *Hizmetlerin yurt içi erişimleri ciddi şekilde yavaşlamıştır* | Tüm trafik paketlerinin incelenmesi yerine; IP toplama ve toplanan IP'leri engelleme şeklinde periyodik uygulamaya dönüştürülmesi |
| • *Alınan önlemlerin teknik detayları elde edilememiştir*<br>• *Saldırının seyri, veri istatistiği hakkında bilgi edinilememiştir*<br>• *e-Posta hizmeti ciddi kesintilere maruz kalmıştır*<br>• *Vodafone üzerindeki tüm iletişim ULAKBİM üzerinden yürütülmüştür* | ULAKBİM'in ihalesinde yayınladığı teknik şartnamenin kapsamının genişletilmesi |

İnternet servis sağlayıcı kapsamında gerekli teknik şartname düzenlemeleri yapıldıktan sonra; kurumumuz tarafından diğer gereksinimleri karşılayabilmesi için aşağıdaki çözümler uygulanabilir:

a. Üst internet sağlayıcı kutu çözümleri
b. Bulut üzerinden trafik geçirilmesi
c. 3. Taraf hizmet alımı
d. Yedek internet hattı alınması

## 2.a. Üst internet sağlayıcı kutu çözümleri

Üst internet sağlayıcı (2020 yılı için Vodafone) tarafından sağlanan güvenlik duvarı uzantısının kurumumuza konuşlandırılması sonucunda; normal trafik periyodik aralıklarda izlenilerek saldırıların tespiti sağlanabilir.

***Avantajlar:*** Saldırının seyri, önlemler ve istatistikler kuruma anlık olarak geçecektir.

***Dezavantajlar:*** Hizmet sağlayıcının değişmesi durumunda güvenliğin devamı garanti edilemez.

*Bu çözüm önerisi, kısmi olarak, ULAKBİM tarafından teknik şartnameye eklenebilecek bir madde ile tüm akademik ağ paydaşlarına sağlanabilir. Üst hizmet sağlayıcının saldırıların anlık olarak bilgisini ve alınan çözüm önerilerini bir panel yardımıyla alt paydaşlara sunabilir; bizce sunmalıdır.*

## 2.b. Bulut üzerinden trafik geçirilmesi

Küresel ölçekte hizmet veren veri merkezi sağlayıcıları (Google Cloud, DigitalOcean, UpCloud vb. gibi) DDOS saldırılarına yüksek yatırımlar yapmaktadır. Kurumumuz çevrimiçi hizmetlerini, saldırı anlarında bu bulutlarda kuracağı dağıtık bir ağ üzerinden geçirerek temiz trafiği ULAKNET'e yönlendirebilir.

***Avantajlar:*** DDOS koruması için yatırım gerektirmez, düşük maliyetlidir

***Dezavantajlar:***

- Veri trafiği her ne kadar şifrelenerek okunması engellense de; yönetmelikte verinin yurt dışı üzerinden geçirilmesi hakkında belirgin bir çerçeve yoktur.
- Bulut üzerinde hesaplar kredi kartı kullanılarak açılacağı için, gerçek kişiliğin kim tarafından temsil edileceği belirlenmelidir
- Bulut hesapları firmaya ait bir kredi kartı üzerinden açılamaz. Bu durum firmanın, bulut hesabına; dolayısıyla veri trafiğine erişebilme imkanı sağlayacaktır

## 2.c. 3. Taraf hizmet alımı

DDOS saldırılarına karşı günümüzde en yaygın kullanıma sahip çözümlerden birisi de DNS yetkilerinin üçüncü taraf bir firmaya (CloudFlare) devredilerek; veri trafiğinin temizlenmesinin sağlanmasıdır. Bu çözüm, BAUM tarafından manuel olarak üretilmesi gereken 2.b. çözümünün hazır bir alternatifi olarak düşünülebilir.

***Avantajlar:*** Hızlı ve kesin çözüm
***Dezavantajlar:*** Yüksek maliyet ( $ 60.000/yıl )

*Bu çözümün yönetmeliğe uygunluğu tartışmalıdır. SSAr-Ge birimi olarak görüşümüz, veri trafiği şifrelendiği için herhangi bir risk barındırmadığıdır. Ancak; 1.a. maddesinde belirttiğimiz, "Ulusal çıkaralara uygunluk" açıklaması bu metod için de geçerlidir.*

## 2.d. Yedek internet hattı alınması

Saldırı altında, çevrimiçi hizmetlere kampüs dışından erişimlerde aksamalar yaşanmaktadır. Ayrıca bant genişliğinde yaşanan bu yoğunluk durumu; kampüs içerisindeki birimlerin internet bağlantıları da ciddi oranda etkilemektedir. Özellikle sağlık hizmeti veren kurumların erişimlerinin kısıtlanması telafisi mümkün olmayan sonuçlar ortaya çıkarabilir. Bu nedenle, üniversitenin yedek bir internet hattının bulunması önem arz etmektedir.

# SONUÇ ve ÖNERİLER

Siber Savunma Ar-Ge birimi olarak, 1.b., 1.c., 2.a. ve 2.d. maddelerinin desteklenmesini; 2.b. maddesinin ise kısmi olarak test edilmesini öneriyoruz. 2.b. maddesinin başarıya ulaşması halinde; BAUM düşük maliyetle ve geçici olarak, kendi kendine yeter vaziyette büyük çaptaki saldırılara karşı kendini koruyabilir.

Ayrıca; 2.b. maddesi için yapılan çalışmalar kapsamında edinilecek tecrübe içerisinde, bulut üzerinde (Google Cloud) yük dengeleme özellikleri de yer almaktadır. Bu özellikler Citrix gibi kutu çözümlere olan bağımlılığımızı düşük maliyetle ve çok daha profesyonel alternatiflerle değiştirmemize olanak verebilir.

SSAr-Ge birimi olarak, 10.02.2020 tarihinden itibaren yaşanan 2. kategorideki büyük saldırından alınacak en önemli sonucun; veri trafiği üzerindeki kontrol ve gözlem imkanlarının asla üçüncü bir tarafa verilmemesi gerektiğidir. Bu nedenle ULAKBİM, güvenlik paketi teknik şartnamesinde mutlaka kontol ve gözlem imkanının padaşlara sağlanması gerektiğini belirtmelidir.