SİBER SAVUNMA TATBİKATLARI: PLANLAMA, UYGULAMA VE DEĞERLENDİRME

Ensar Şeker
NATO CCD COE
ensar.seker@ccdcoe.org

ÖZET

Siber savunma tatbikatları, siber güvenlik bilinirliliğini arttırmak, siber alanda meydana gelebilecek olası farklı senaryolarda nasıl hareket edilmesi gerektiği konusunda gerekli ortamın oluşturulması, ve konuyla ilgili uzmanların uygulamalı olarak eğitimleri açısından bakıldığında çok önemli bir araçtır. Söz konusu tatbikatlar siber alanda alınabilecek önlemler konusunda karar vericilere ve bu alan için geliştirilebilecek araçlar, teknikler ve prosedürler konusunda siber savunma ile görevli veya ilgili kurum, kuruluş, ve personele de fikirler verebilmektedir. Siber savunma tatbikatlarında gerçeğe en yakın şekilde oluşturulan senaryolarla özellikle siber saldırılar ile karşı karşıya iken özellikle stres altında en iyi kararları verebilme ve takım olarak koordineli hareket edebilmenin zorunluluğunu beraberinde getirerek çok önemli katkılar sağlamaktadır. Bu makalenin amacı uluslararası siber savunma tatbikatları göz önünde bulundurularak ve karşılaştırılarak bu tatbikatların planlama, uygulama ve değerlendirme aşamalarını ortaya koyarak konuyu bilimsel açıdan ele almaktır. Çalışmanın bir diğer amacı ise söz konusu süreçler her ne kadar yapılması planlanan tatbikatın hedef kitlesine göre farklılıklar arz etse de, türüne bakılmaksızın genel bir siber savunma tatbikatında olması gerekli süreçleri de ortaya koyabilmektir.

Anahtar Kelimeler: Siber savunma, siber tatbikat, siber tehdit, siber güvenlik.

CYBER DEFENSE DRILLS : PLANNING, IMPLEMENTATION AND EVALUATIONS

ABSTRACT

Cyber defense exercises are a very important tool when it comes to increasing the awareness of cyber security, creating the necessary environment for how to act in different scenarios that could lead to the cyber field, and looking at the practical training of the relevant experts. The exercises can give ideas to the decision makers about the measures that can be taken in the cyber area and to the officials, institutions, organizations and staff responsible for the cyber defense on the tools, techniques and procedures that can be developed for this field. In the cyber defense exercises, especially in the face of the cyber attacks with the scenarios that are created in the closest to reality, it provides very important contributions by bringing together the necessity of making the best decisions under stress and coordinated movement as a team. The objective of this article is to address the issue from a scientific point of view by setting out the stages of planning, implementation and evaluation of these exercises, taking into account and comparing international firefighting exercises. Another aim of the work is to be able to reveal the necessary processes that are required to be a general fat burning exercise, regardless of the type, although the processes involved vary according to the target mass of the planned exercise.

Keywords: Cyber defense, cyber exercise, cyber threat, cyber security.

I. GİRİŞ (INTRUDUCTION)

Siber alan kara, deniz, hava ve uzaydan sonra beşinci savaş alanı olarak kabul edildiğinden beri özellikle ulusal güvenlik açısından kritik derecede önem arz etmeye başlamıştır. Siber saldırıların anonim olarak gerçekleştirilebilmesi, reddedilebilirliği ve diğer alanlara nispeten gerçekleştirilen faaliyetlerin daha düşük maliyetlerde olması, bu saldırıları son zamanlarda daha popüler hale getirmiştir. Öyle ki ülkeler, basit seviyede gerçekleştirilen siber saldırılar bir kenara, çok ileri seviyede teknoloji ve sofistike düzeyde siber silahlar geliştirmeye ve kullanmaya başlamışlardır.

Ulusal güvenliğin ayrılmaz bir parçası haline gelen siber saldırılara karşı ülkeler, kritik alt yapılarla, kamunun ve toplumun dijital güvenliğini koruma altına alabilmek adına, siber savunma komutanlıkları, ulusal siber olaylara müdahale ekipleri ve diğer bilgi güvenliği merkezleri gibi otoriteleri kurmaya ve

yaygınlaştırmaya, yine bu sebeple ulusal siber güvenlik stratejileri geliştirmeye ve uygulamaya koymaya başlamışlardır.

Siber savunma konusunda kurum, kuruluş yada ülkelerin teknik kapasitelerini test etme, gerekli bilinçlendirmeyi ve eğitimleri sağlaması açısından siber savunma tatbikatları çok önemli rol oynamaya ve tüm dünya genelinde yaygınlık kazanmaya başlamıştır. Siber savunma tatbikatlarının başlıca amaçları arasında [1, 2, 3, 4];

- Ulusal bazda meydana gelebilecek siber saldırılara karşı ortak ve koordineli, teknik ve stratejik hareket kabiliyetini test etme ve geliştirebilme,
- Uluslararası bazda meydana gelebilecek siber saldırılara karşı ortak ve koordineli, teknik ve stratejik hareket kabiliyetini test etme ve geliştirebilme,
- Siber güvenlik yetenekleri ile devamlılık ve süreklilik süreçlerini test etme ve geliştirebilme, ve
- Siber savunma alanında kamu ve özel sektör arasında işbirliği ve koordinasyonu güçlendirme

sayılabilir.

İlerleyen bölümlerde dünya genelinde siber savunma tatbikatları, bu tatbikatların süreçleri, türleri ve katkıları güncel senaryo ve örneklerle incelenmiştir.

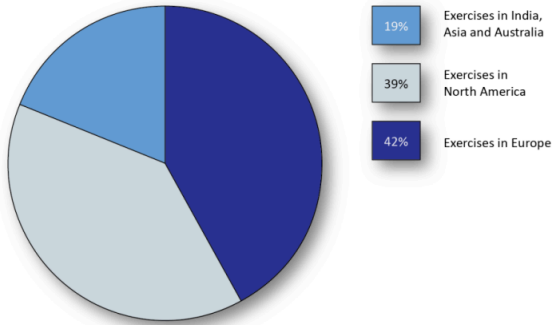
Söz konusu tatbikatlar planlama aşamasından uygulama ve nihai olarak değerlendirme aşamasına kadar hem tatbikat planlayıcılarına hem de katılımcılarına konuyla ilgili önemli katkılar sağlamaktadır. Tatbikat ile ilgili bu süreçlerin incelenmesi gerçekte planlamak istenen siber savunma mekanizmaları için de fikir verebilmektedir.

II. DÜNYA'DA SİBER SAVUNMA TATBİKATLARI (CYBER DEFENCE DRILLS IN THE WORLD)

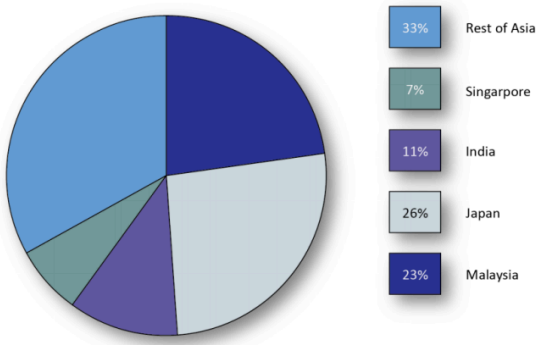
Siber savunma tatbikatları alanında en büyük oyuncuların başında Avrupa gelmektedir. Geçtiğimiz senelerde dünya genelinde gerçekleştirilen siber savunma tatbikatlarının yüzde 42'si Şekil 1'de de görülebileceği üzere Avrupa kıtasında gerçekleştirilmiştir.

Siber Savunma Tatbikatları alanında en az Avrupa kadar önemli bir diğer aktör özellikle ABD'nin başını çektiği Kuzey Amerika kıtasıdır. Bunların içinde Japonya, Malezya, Hindistan, ve Singapur'un başı çektiği Asya ve sonra Avusturalya takip etmektedir.

Şekil 2'de Asya kıtasında gerçekleştirilen siber savunma tatbikatlarının güncel dağılımı Şekil 2'deki gibidir. Asya kıtasında Japonya'dan sonra özellikle Malezya'nın son yıllarda bu alana yapmış olduğu yatırımlarla ikinci sıraya yükselmesi dikkat çekicidir. Japonya ve Malezya'nın oranları her ne kadar birbirine yakın olsa da Japonya'nın Malezya'dan çok daha uzun süredir siber savunma tatbikatlarına ağırlık verdiği ve dolayısı ile Malezya'dansa bu alanda çok daha fazla tecrübeye sahip olduğu muhakkaktır [5].



Şekil 1. Siber Savunma Tatbikatlarının Dünya Genelinde Dağılımı [5]



Şekil 2. Siber Savunma Tatbikatlarının Asya Genelinde Dağılımı [5]

Uluslararası boyutta gerçekleştirilen birkaç siber savunma tatbikatına örnek olarak Locked Shields, Cyber Coalition, Cyber Europe u verebiliriz.

- *Locked Shields:* Locked Shields (Kilitli Kalkan) siber savunma tatbikatı, merkezi Talin, Estonya'da bulunan NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (NATO CCD COE) tarafından yıllık organize edilmekte ve dünyanın en geniş katılımlı ve birçok otoriteye göre en karmaşık ve ileri teknolojilerine sahip siber savunma tatbikatı olarak kabul edilmektedir. 2017 Locked Shields tatbikatına, tüm dünya genelinden 900'den fazla siber güvenlik uzmanı dahil olmuş olup, 20 ülkenin ulusal takımı katılım sağlamıştır. 3000'den fazla sanal sistemin yer aldığı tatbikatta ulusal takımlara (mavi takımlara) kırmızı takım tarafından 2500'den fazla saldırı gerçekleştirilmiştir. Yeni gelişen bilişim teknolojilerini adapte etme konusu da başarılı bir rota izleyen Locked Shields siber savunma tatbikatları, 2017 yılında diğer yıllardaki

tatbikatlardan farklı olarak akıllı şebeke sistemleri, hava üssü yakıt tesis sistemleri, dron kontrol sistemlerini de senaryolara dahil etmiş ve mavi takımların sorumlulukları arasına diğer sistemlerin yanında bu özel sistemlere eklenmiştir [6].

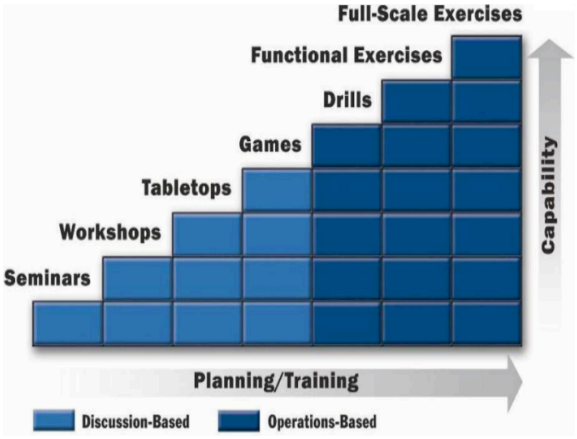
- *Cyber Coalition:* Cyber Coalition (Siber Koalisyon) siber savunma tatbikatı, NATO tarafından yıllık olarak organize edilmektedir. Üç günlük süren etkinliğe, NATO üyesi ve ittifak ülkelerden katılım gerçekleşmektedir. 2016 yılı Aralık ayında gerçekleşen tatbikata 700'den fazla siber savunma ve hukuk uzmanı, hükümet yetkilileri, subay, akademisyen ve endüstri temsilcileri katılım göstermiştir. Tatbikatta, Cezayir, Avusturya, Finlandiya, İrlanda, Japonya ve İsveç gibi NATO üyesi olmayan ülkelerin temsilcileri gibi Avrupa Birliği'nden siber savunma personeli de yer almıştır [7].
- *Cyber Europe:* Cyber Europe (Siber Avrupa) bir Avrupa Birliği kurumu olan ENISA (European Union Agency for Network and Information Security) tarafından 2 yılda bir Avrupa Birliği üyesi ülkeler için düzenlenmektedir. Locked Shields ve Cyber Coalition gibi askeri temelli tatbikatlardan farklı olarak sivil bir otorite tarafından organize edilmektedir. 2016 yılında gerçekleştirilen tatbikata 28 Avrupa Birliği üye ülkesi ve Avrupa Birliği üyesi olmamasına rağmen 2 EFTA (the European Free Trade Association) üyesi ülke dahil olmuştur [8].

III. SİBER SAVUNMA TATBİKATLARI TAKSONOMİSİ (CYBER DEFENSE EXERCISE TAXONOMY)

Siber savunma tatbikatları çeşitli formlarda gerçekleştirilebilmektedir. Elde edilmek istenen veri setine göre, bu tatbikat türleri farklılık göstermektedir. Bununla birlikte söz konusu farklılıklar uluslararası bir standart olan ISO 22398'den gelen parametrelere dayanmaktadır. Siber savunma tatbikatlarını amaçları doğrultusunda karakterize edilebilir. Bunu yaparken, aşağıdaki dört kategoriyi takip ederek bunları sınıflandırmak mümkündür [9].

1. Siber yeteneklerin geliştirilmesi.
2. Bireylerin, organizasyonların ve sistemlerin siber yeteneklerinin değerlendirilmesi.
3. Bilgi, yetenek, dayanıklılık ve/veya teknik kapasitenin ölçülmesi.
4. Katılımcıları eğitilmesi ve bilgi, anlama ve beceri kazanma fırsatının sağlanması.

Oluşturulabilecek tüm farklı tatbikat türlerine (CTF, discussion based game, simulation, workshop, drills, seminar) karşın, siber savunma tatbikatları temelde 3 kategoriye ayrılabilir [11].



Şekil 3. Türlerine göre Siber Savunma Tatbikatları [10]

1. *Masa Üstü (Table Top) Tatbikatlar:* Tüm senaryo/alt senaryolar, enjeksiyonlar ile kırmızı takım saldırıları tatbikat öncesinde yazılmıştır ve hazırdır. Çoğu durumda tatbikat planlayıcıları ve oyuncuları bir masaya oturup tatbikatı uyguladığından bu tür tatbikatlar masa üstü tatbikatları adını almıştır. Masa üstü tatbikatları oldukça sınırlı sayıda bir eğitim kitlesine ve çok iyi tanımlanmış amaçlara sahip olmalıdır [12]. Diğer tatbikat türlerine göre daha hızlı ve kısa sürede planlanabildiği gibi uygulama süreci de nispeten daha kolaydır.
2. *Karma (Hybrid) Tatbikatlar:* Tatbikat senaryo/altsenaryolar ve enjeksiyonlar önceden yazılmış fakat kırmızı takım saldırılarını tatbikat sırasında canlı olarak ifa etmektedir. Tatbikat planlayıcıları, gerçek olayları önceden belirlenmiş hedeflere göre uygulayan bir kırmızı takım ile birlikte tatbikatı gerçekleştirirler [13].
3. *Tam Canlı (Full Live) Tatbikatlar:* Bu tür tatbikatlarda her ne kadar ana senaryo ve bazı alt senaryolar önceden hazırlanmış olsa da takımların gidişatı ve stratejilerine göre ilgili takımlarca (genellikle beyaz takım) anlık senaryolar ve enjeksiyonlar geliştirilmekte, kırmızı takım ise mavi takımın savunma kapasitesi ve durumuna göre yeni saldırı stratejileri üretmektedir. Diğer siber savunma tatbikatlarına göre planlama süreci çok daha uzun bununla birlikte gerçek hayatta meydana gelebilecek senaryolara göre daha gerçekçidir [14].

IV. SİBER SAVUNMA TATBİKATLARI YAŞAM DÖNGÜSÜ (CYBER DEFENSE EXERCISE LIFE CYCLE)

Bir siber savunma tatbikatı için genel olarak yaşam döngüsü şu dört aşamadan oluşmaktadır [15];

1. Tanımlama: Katılımcı profilini tanıma ve oluşturma, tatbikat türü ve büyüklüğünü belirleme,

mevcut senaryo opsiyonlarını değerlendirme gibi konuları içerir.

2. Planlama: Finansal kaynakların temin edilmesi, tatbikat takvim ve yerinin ayarlanması, rollerin dağıtılması ve gerçekçi bir senaryonun oluşturulması, tatbikat materyallerinin hazırlanması, tatbikatta görev alacak kişilerin ve takımların görevleri ile ilgili bilgilendirilmesi ve eğitilmesi, medya politikasının belirlenmesi, gözlemci ve medya mensuplarının davet edilmesi konularını içerir.

3. Uygulama: Tatbikatın belirlenen çerçeve ve kurallar içinde en düzgün şekilde tatbik edilmesi, senaryo ve enjeksiyonların belirlenen sıraya göre uygulanması, meydana gelebilecek aksaklık ve sorunların en kısa ve hızlı bir biçimde çözüme kavuşturulması, katılımcıların gözlemlenmesi ve katılımcıların karar ve aktivitelerinin not alınması, değerlendirme aşamasını desteklemek amacıyla anket ve soruların katılımcılara yönetilmesi gibi konuları içerir.

4. Değerlendirme: Değerlendirmeyi yapacak bir grubun oluşturulmasını, katılımcılar tarafından cevaplanan anket ve soruların toplanıp, değerlendirilmesini, tatbikatta görev alanlardan gerekli bilgilerin toplanmasını, medya ve umuma sunulacak dokümanların hazırlanmasını, değerlendirmeler sonucu katılımcılarla paylaşılacak raporların hazırlanması konularını içerir. Siber Savunma Tatbikatı Yaşam Döngüsü detayı [13] nolu kaynakta verilmiştir.

IV. PLANLAMA (PLANNING)

Tatbikat planlama süreci, katılımcılar, tatbikat senaryosu/alt senaryoları, enjeksiyonları, tatbikat ortamının hazırlanması ile birlikte, tatbikatın olağan seyrinde yürütme düzenini belirler. Tatbikat uygulaması ve senaryolar, katılımcı gruba ve spesifik olarak gerçekleştirilmesi istenilen hedeflere göre çeşitlilik göstermektedir. Farklı tatbikat türlerini ve her birinin yerine getirdiği hedefleri anlamak, tatbikatın gerçekçiliğini ve etkinliğini artıracaktır.

A. Amaçların Belirlenmesi

Bir siber tatbikat, izole edilmiş bir ağ üzerinde tek başına bir etkinlik olarak ya da operasyonel bir ağ üzerinde daha geniş bir eğitim tatbikatı olarak düzenlenebilir. Planlama süreçleri benzerdir. Tatbikat planlama süreci, tatbikatın amaç ve arzulanan sonuçlarının tanımlanmasıyla başlar. Açık hedefler olmadan, planlayıcılar anlamlı bir tatbikat tasarlayamazlar. Belirlenecek bu amaçlar planlayıcıların; katılımcıların, savaş ortamı olarak düzenlenen bir siber ortamında başarıyla çalışması ve siber tehditlere karşı savunma için gerekli yeteneklere sahip olup olmadığını belirlemek için tatbikat içindeki senaryoları açıkça yapılandırmalarını sağlar. Farklı organizasyonların, her tatbikat için bir başlangıç noktası oluşturmayı önemli hale getiren farklı rehber ilkeleri, araçları, taktikleri ve prosedürleri vardır.

- Tatbikat başlamadan önce katılımcılara sağlanan siber eğitimin etkililiğinin belirlenmesi,
- Tatbikat olay raporlarının etkinliğinin değerlendirilmesi ve tatbikat vasıtasıyla ortaya çıkarılan eksiklikleri gidermek için analiz kılavuzlarının hazırlanması,
- Tatbikat sırasında, katılımcıların zararlı faaliyetleri algılayıp gerekli karşılığı verebilme yeteneğinin değerlendirilmesi,
- Siber saldırıların operasyonel etkilerini belirleme ve bu saldırılar için gerekli kurtarma ve iyileştirme prosedürlerinin uygulama yeteneğinin değerlendirilmesi,
- Senaryo planlamasının ve uygulanmasının başarısının belirlenmesi,
- Siber güvenlik sistemlerindeki zayıflıkların açığa çıkarılması ve düzeltilmesi,
- Siber alanla ilgili politika ve prosedürlerdeki zayıflıkların açığa çıkarılması ve düzeltilmesi,
- Bir bilgi sistemini korumak ve zararlı saldırıların gerçekleştirildiği bir siber ortamda gerekli aktivitelerin gerçekleştirmesi için hangi donanımların veya yeteneklerin gerekli olduğunun belirlenmesi,
- Enjeksiyonların tatbikatın amaçlarını karşılayıp karşılamadığının belirlenmesi,
- Siber farkındalık, siber saldırılar karşısında hazır olma durumu ve koordinasyonun artırılması,
- Bilişim sistemlerinin siber saldırılar karşısında korunabilmesi ve gerekli önlemlerin alınarak en az zararla müdafaasına yönelik önceden hazırlanacak acil durum planlarının geliştirilmesi,

gibi maddeler genel olarak tüm siber savunma tatbikatları için belirlenen ortak hedeflerdir.

B. Planlama Süreci

Planlama süreci [10], aşağıda açıklanmıştır.

1) Ön Planlama Toplantısı (Initial Planning Meeting/Conference);

- Gereksinim ve koşulların belirlenmesi,
- Senaryo değişkenlerinin ve taslak senaryo tekliflerinin belirlenmesi,
- Gerekli bilgilerin toplanması ve tatbikat planlayıcıları arasında görev dağılımlarının yapılması,

konularını kapsamaktadır. Tatbikattan yaklaşık 6, 7 ay önce gerçekleşmektedir.

2) Ana Planlama Toplantısı (Main Planning Meeting/Conference);

- Personel, senaryo ve zaman çizelgesi geliştirme ve idari gereklilikler gibi lojistik ve örgütsel sorunları çözüme kavuşturulması,
- Tatbikatta kullanılacak tüm taslak belgelerin incelenip, değerlendirilmesi ve nihayete erdirilmesi,
- Nihai planlama aşamasının öncesinde isteklerin incelenmesi ve geliştirmesi,
- Tatbikatın amacına göre belirlenen görev, koşul ve standartların gözden geçirilmesi,

konularını kapsamaktadır. Tatbikattan yaklaşık 3, 4 ay önce gerçekleşmektedir.

3) Nihai Planlama Toplantısı (Final Planning Meeting/Conference);

Nihai plan toplantısı, tatbikat süreçlerini ve prosedürlerini gözden geçirmek için yapılan son toplantıdır. Bu toplantıdan sonra, tatbikatın tasarımı veya kapsamı veya destekleyici dokümantasyonu üzerinde önemli bir değişiklik yapılmamalıdır. Tatbikattan 3, 4 hafta önce gerçekleşmektedir.

4) Test Uygulaması (Test Run)

Test uygulaması, siber savunma tatbikatlarının teknik alt yapısını ve organizasyonla ilgili çıkması muhtemel sorunların tatbikat öncesinde test edilip değerlendirilmesine yönelik son hazırlık aşamasıdır. Test uygulamasında tatbikat için seçilen yerde tatbikat için kullanılacak tüm bilişim alt yapıları kurularak bu alt yapılar, tatbikat süreci sanki normal sürecinde işliyormuş gibi test edilip gözlemlenerek, tatbikat öncesi de olası muhtemel aksaklıkların önüne geçilmesi amaçlanmaktadır. Test uygulamasına mavi takımlar dışındaki tüm takımlardan katılım gerçekleşmektedir. Böylelikle tüm takımlar tatbikat öncesinde son durumlarını ve tatbikat işleyiş süreçlerini son kez gözden geçirme şansını elde etmiş olurlar. Test uygulaması tatbikattan bir hafta önce gerçekleşmektedir.

V. UYGULAMA (APPLICATION)

A. Takımlar

1) Mavi Takım

Bir kuruluşun bilgi sistemlerini yada tatbikat kapsamında oluşturulan sanal ortamları temsili saldırganlara (kırmızı takım) karşı güvenliğini sağlamakla ve savunmakla sorumlu grup ya da takımdır. Uluslararası siber savunma tatbikatlarında, mavi takımlar her bir katılımcı ülkenin kendi ülkesini temsilen oluşturduğu ulusal takımları ifade etmektedir. Mavi takım, simüle edilen saldırılara karşı;

1- verilen belli bir süre boyunca,
2- temsili savunma temelli ve operasyonel bağlamda,
3- nötr bir grup (genellikle beyaz takım) yardımıyla kurulan ve izlenen kurallara,

göre sorumlu olunan sisteme dayalı herhangi bir veri sızıntısını tanımlama ve bunları engelleme ile gizliliğin, bütünlüğün ve kullanılabilirliğin korunması üzerine dayalı savunma yapmalıdır.

Son zamanlarda siber savunmanın ulusal ve uluslararası hukuk ve politikalar, medya, ulusal güvenlik stratejilerinin de bir parçası olması nedeniyle siber savunma tatbikatları da bu bağlamda dizayn edilmeye başlamış ve mavi takım tarafından sadece teknik savunma yapılması siber savunma kapsamında yeterli görülmemeye başlanmıştır. Bu nedenle özellikle uluslararası siber savunma tatbikatlarına teknik senaryolara ek olarak hukuk, politika, strateji ve medya senaryoları da dahil edilmeye başlanmış, dolayısı ile mavi takımın bu konulardaki sorumlulukları da artırılmıştır.

Mavi takımın sorumlulukları arasında angajman kuralları çerçevesinde [1, 2, 3, 4], yürürlükteki kanunlara ve yönetmeliklere her zaman uyulması zorunluluk arz etmekte ve takım üyeleri tarafından alınan yada gerçekleştirilen herhangi bir yasadışı işlem kabul edilemez olarak görülmektedir. Dolayısı ile simülasyon ortamında dahi olsa mavi takım tarafından gerçekleştirilen tüm eylem ve kararların mevcut kanun ve yönetmelikler göz ardı edilmeden gerçekleştirilmesi oldukça önemlidir.

Angajman kuralları içerisindeki bir diğer net kural, mavi takım tarafından kırmızı takıma, diğer mavi takımlara yada tatbikat sanal sistemlerinin alt yapılarına hiçbir şekilde saldırı yapılamamasıdır.

Mavi takım üyeleri, istenildiğinde kendi operasyonel güvenliklerine zarar vermeyecek doğru bilgileri vermelidir.

Mavi takım, tatbikat ortamı ile ilgili meydana gelen teknik sorunlarla alakalı bildirim ve taleplerini kendileri için tasarlanan web sayfası üzerinden bu konu ile sorumlu bulunan yeşil takıma iletilebilmelidir. Yeşil takım kendisine iletilen bu teknik sorunları makul olan en kısa sürede çözüme kavuşturmakla mesuldür.

Takım tarafından yapılacak tüm raporlamaların takım içindeki komuta zinciri üzerinden yapılması önemlidir.

Mavi takıma kendi araçlarını ve yazılım ürünlerini kullanma izni verilmektedir, ancak bu ürünlerin lisanslı yasal kopyalarının olması konusunda tüm sorumluluk bu takıma aittir.

'Blonde user' olarak adlandırılan ve bilinçsiz kullanıcıları temsil eden ve mavi takımların sistemlerini kullanıp, gönderilen zararlı eposta ve dosyaları açıp, zararlı linkleri bilinçsizce tıklayan bu kullanıcıların yada bu kullanıcıların kullandığı hizmet ve sistemlerin mavi takımlar tarafından engellenmesi angajman kurallarına aykırıdır. Ayrıca bu kullanıcılar

tarafından mavi takıma gönderilen, kullandıkları sistemlerle alakalı teknik sorunlarla ilgili gönderdikleri taleplerin mavi takım tarafından en kısa süre içerisinde çözüme kavuşturulması beklenmektedir.

Mavi takımlara tatbikat öncesinde, tatbikat ortamı ile kullanacakları sistemlere yönelik ön bilgi aktarabilmek amacıyla internet üzerinden yapılan seminerlerle bilgi aktarımı yapılmaktadır.

2) Kırmızı Takım

Kırmızı takımın amacı, tatbikata katılan tüm mavi takımlara eşit derecede dengeli siber saldırılar gerçekleştirmektir. Bunun için kırmızı takım önceden tanımlanmış bir senaryoyu izlemekle birlikte, mavi takımın sistemlerinde daha önceden oluşturulan güvenlik açıklarını kullanma iznine sahiptir. Kırmızı takım tarafından gerçekleştirilen başarılı saldırılar, saldırının başarıyla yapıldığı mavi takımın eksi puan almasına yol açar. Kırmızı takım ve beyaz takım yakın işbirliği içerisinde çalışmak durumundadır. Kırmızı takım, tatbikat planına göre hareket ederken, her zaman beyaz takım tarafından verilen talimatlara da uymak zorundadır. Kırmızı takımın tatbikat alt yapı sistemlerine yada yeşil takım tarafından kullanılan servislere saldırması kesinlikle yasaktır. Kırmızı Takım tarafından gerçekleştirilecek tüm saldırıların tatbikat ortamının içinde kalması zorunludur. Buna sosyal mühendislik saldırıları da dahildir.

3) Yeşil Takım

Yeşil takım tatbikat altyapısını hazırlamak ve tatbikat boyunca işlevselliğini korumakla sorumlu olan takımdır. Bu altyapılar yönetimsel bilgisayar düğümlerini tasarlama, kurma ve yönetme, sanallaştırma platformu, depolama, çekirdek ağ oluşturma gibi sistemlerle birlikte mavi takımların tatbikat sırasında savunmak zorunda oldukları sistemleri de kapsamaktadır. Söz konusu sistemlerin fonksiyonlarının tatbikat süresince sağlıklı bir şekilde çalışılabilirliğini sağlayabilmek adına mavi takımlar tarafından teknik sorunların çözümüne yönelik gönderilen taleplerin makul bir süre içerisinde yeşil takım tarafından çözüme kavuşturulması beklenmektedir.

4) Sarı Takım

Sarı takımın rolü, tatbikat sırasında tatbikatla ilgili başta beyaz takıma ve sonra tüm katılımcılara durumsal farkındalık sağlamaktır. Sarı takım için ana bilgi kaynakları, mavi takımlar tarafından sağlanan ara raporlar, kırmızı takım üyelerinden gelen saldırı kampanyalarının durumu ilgili raporlar ve sistem tarafından sağlanan raporlardır. Beyaz takım liderlerine ve mavi takımlara düzenli olarak öne çıkan güncellemeler sarı takım tarafından sağlanmaktadır.

5) Beyaz Takım

Beyaz takım, tatbikat hazırlama ve yürütme sırasında kontrol etme sorumluluğuna sahiptir. Beyaz takım, talim hedefleri, senaryo, kırmızı takım için üst seviye hedefleri, yasal enjeksiyonları, kuralları, medya hazırlıklarını ve iletişim planlarını belirler. Yürütme sırasında beyaz takım, farklı aşamaların ne zaman başlayacaklarını, kırmızı takımın kampanyasının yürütülmesinin denetlenmesi ve puanlama ile ilgili konularda karar vererek tatbikatın kontrolünü sağlar. Yönetim, blonde kullanıcılar, enjeksiyonlar, puanlama ve medya simülasyonu da beyaz takımın sorumlulukları arasındadır.

B. Senaryo

Tatbikat sonrası arzulanan sonuçlar yada çıktılar her bir tatbikat için farklılık gösterir, ancak bu çıktılar her zaman katılımcılara siber tehdit yöntemlerini göstermek ve tatbikat hedeflerini karşılamak için kullanılan talim programlarının ve araçlarının başarısını değerlendirmek için gerçekçi bir senaryo sunmak etrafında döner. Tatbikat çıktıları, farkındalık yaratmayı ve çeşitli siber tehditlere karşı aktiviteleri planlamasını ve değerlendirilmesini amaçlamalıdır ve bu senaryolar tatbikatın ana hedefleri çevresinde dönmelidir.

Geçmiş senelerde gerçekleştirilen bir uluslararası siber savunma tatbikatının örnek senaryosu şöyledir; X ülkesi, Afrika'nın batı yakasında bulunan bir ada cumhuriyeti olup ülkede, üyesi olduğu uluslararası bir organizasyonun koalisyon gücü bulunmaktadır. Adanın büyüklüğü İrlanda ile karşılaştırılabilir iken, iklim ve manzara Fas'a daha yakındır. Yoksul bir ülke olan X Cumhuriyeti'nin yerel altyapısı, ve özellikle sanitasyon, iletişim, tıbbi hizmetler ve eğitim oldukça yetersiz ve kötü bir durumdadır. Örneğin, ülke, dünyanın geri kalanıyla güvensiz bir internet bağlantısına sahipken ve bağlantının bant genişliği ise düşüktür. Ülke içinde bağlantı, çok sayıda ücretsiz (ve anonim) kablosuz ağlardan yararlanan şehir merkezleriyle sınırlıdır. Ülkenin, USOM (Ulusal Siber Olaylara Müdahale) ekibi ya da bilişim sistemlerini korumaya yönelik kolluk kuvvetleri bulunmamaktadır. Bu, çoğu uluslararası aktörü pahalı uydu bağlantısına veya yerel olarak çalıştırılan sistemleri kurmaya ve kullanmaya zorlamaktadır.

X Cumhuriyeti, yıllardır komşusu olan ve uluslararası toplum tarafından anti demokratik uygulamaları hayata geçiren bir yönetime sahip olduğu eleştirilerine muhatap olan Y ülkesi ile diplomatik çatışma içerisinde bulunmaktadır. Uzun zamandır X Cumhuriyeti, Y ülkesi kaynaklı olduğu tahmin siber saldırılara maruz kalmaktadır. X Cumhuriyeti ve Y ülkesi arasında en son yaşanan diplomatik krizin hemen akabinde, X Cumhuriyeti'nin Hava Kuvvetleri üssüne siber saldırılar gerçekleştirilmeye başlanmış ve bir takım gizlilik dereceli bilgi ve belgeler çalınmıştır. Mavi takımın görevi uluslararası koalisyonun bir parçası olarak, X Cumhuriyeti'nin Hava Kuvvetleri üssünde

bulunan bilgi işlem cihazları üzerinde gerekli analizleri yaparak raporlamak ve mevcut devam eden saldırılar yada muhtemel yapılması planlanan başka siber saldırıları önlemek adına gerekli tedbirleri almaktır.

Mavi takım, tatbikat boyunca sonradan dahil olacak hukuk, medya, ve strateji tabanlı alt senaryolar ve enjeksiyonları da dikkate alarak daha önce hiç tanıdık olmadığı bir bilişim sistemde kendisine verilen görevleri, belirlenen kuralların dışına çıkmadan yerine getirmeye çalışmalıdır.

C. Puanlama

Puanlama, siber savunma tatbikatları için en sıkıntılı konulardan bir tanesidir. Yapılan puanlama sistemleri her ne kadar standartlaştırılmaya çalışılırsa çalışılsın, genelde beyaz takımın kararları doğrultusunda, zaman zaman yine inisiyatiflere dayanarak puanlamalar yapıldığından mavi takımlardan her zaman itirazlar gelme ihtimali oldukça yükseltir. Bu nedenle özellikle uluslararası boyutta düzenlenen birçok siber savunma tatbikatı yarışma ortamı yaratarak değil, mevcut tatbikat sonuçlarına göre dersler çıkarılıp, bu konuyla ilgili gerekli tedbirlerin alınmasının asıl amaç olduğunu ileri sürerek puanlama sistemine karşı çıkmıştır. Avrupa Birliği tarafından düzenlenen Siber Avrupa puanlama sistemini kullanmayan tatbikatlara örnek gösterilebilir. Bununla birlikte, puanlama sisteminin bu tür tatbikatlarda kullanılmasının katılımcılar için birer motivasyon aracı olarak görüldüğü ve katılımcılar arası oluşan pozitif rekabetin daha başarılı sonuçlara ulaşma konusunda daha büyük bir itici güç olduğu NATO CCD COE tarafından organize edilen Locked Shields siber savunma tatbikatlarında gözlemlenmiştir.

D. Medya Aktivite Simülatörü

Medya simülatörü, tatbikat oyuncularının gerçek hayatta olduğu gibi medya ve sosyal medyayı görüntülemesine ve bunlarla etkileşime geçmesine izin verir. Tüm oyuncuların sosyal medya kullanımları için kendilerine mahsus şifreleri bulunmaktadır. Twitter, Facebook, TV, radyo, çevrimiçi haberler ve gazeteler gibi yayın organları olarak kullanılan tüm medya ve sosyal platformlardan canlı yayın imkanı simülator yardımıyla sağlanabilmektedir. Bu simülasyon ile senaryo gereği oluşturulan temsili ülkenin ve bu ülkede senaryoda yer alan kurum ve organizayonlara ait web sayfalarına da yer verilmektedir. Mavi takımlar, kırmızı takımlardan gelen saldırılara karşı gerekli tedbirleri almakla meşgullerken tıpkı gerçek yaşamda olduğu gibi işin medya boyutu ile ilgili de gereken adımları atmak durumundadırlar.

E. Enjeksiyonlar

Enjeksiyonlar; senaryo enjeksiyonları, medya oyunu, yasal oyun ve adli bilişim olmak üzere 4'e ayrılmaktadır.

1) Senaryo enjeksiyonları; *Haberlerin takip edilmesi, istihbaratların değerlendirilmesi, siber saldırıları gerçekleştirenlerle ve bu saldırılarla ilgili malumatların toplanıp ve raporların hazırlanması, suistimal bildirimi ve mavi takım sistemlerini kullanan sıradan kullanıcıların (blonde users) meydana getirdiği yada getirebileceği zayıflıklara karşı gerekli önlemleri almak ve bu kullanıcılardan gelen sorunların en kısa sürede çözümlerini sağlamak konularını içeren ve beyaz takım tarafından hazırlanan enjeksiyonları.*

2) Medya oyunu; *Daha önce de bahsedildiği üzere medya simülasyonunun amacı, gerçek dünyadan haberler ile tatbikatı medya ortamına taşımak ve kırmızı takımın faaliyetleri dışında geliştirilen enjeksiyonlarla mavi takımlara baskı yapmaktır. Haberlerde yer alan hikayelerde senaryo gereği oluşturulan ülke ile ilgili arka planda cereyan eden olaylarla hakkında bilgiler, devam eden siber olaylar hakkında raporlar, siber saldırılardan etkilenenlerden gelen yorumların yanı sıra yalan, değiştirilmiş, ve doğrulanmamış haberler de yer almaktadır.*

3) Hukuk Enjeksiyonları: *Mavi takımın senaryo gereği emir-komuta zincirinden gelen soruları cevaplayabilmesi derin yasal bilgilere sahip olmasına bağlıdır. Karışık hukuki meseleleri ele almak, yanlış ifadeleri ve yorumları çürütmek ve aynı zamanda meydana gelen siber saldırılarla alakalı açıklamaları konunun uzmanı olmayan kişilere anlaşılabilir kılmak amacıyla medya ile iletişim kurmak ve medyanın yayınladığı, yalan ve gerçeği yansıtmayan yada gerçeği çarpıtan haber ve analizlere hukuki bağlamda karşılık vermek yasal oyunun gereklilikleri arasındadır.*

4) Adli Bilişim: *Adli bilişim oyunu, meydana gelen siber saldırılarla alakalı adli bilişim raporu hazırlamaya ve yine bu saldırılarla alakalı kim, ne, ne zaman, nasıl ve neden sorularına cevap aramaya yöneliktir.*

VI. DEĞERLENDİRME (EVALUATION)

Siber savunma tatbikatlarının en önemli çıktılarından birisi Faaliyet Sonu Raporudur. Bu raporda, tatbikat sonrasında her bir mavi takım ile ayrı ayrı detaylı ve özel olarak sadece o takıma mahsus tatbikat performansının paylaşıldığı rapordan farklı olarak, tatbikatta yer alan senaryo ve alt senaryolar, enjeksiyonlar, tatbikat amaçları, katılımcılar, puanlama, teknik alt yapı, kırmızı takım tarafından gerçekleştirilen saldırılar (client-side, web, network), genel manada mavi takım tarafından yapılan savunmalar, bu savunmalardaki zayıflıklar, yapılan genel hatalar, tüm takım ve alt takımlardan gelen gözlem, tavsiye ve değerlendirmeleri içermektedir.

Ayrıca her bir mavi takım ile o takıma özel yapılan analizler, değerlendirmeler, tatbikat boyunca

gösterdikleri zafiyet ve zayıf oldukları noktalar, tavsiye ve önerileri içeren ayrı bir rapor da paylaşılmaktadır.

VII. SONUÇ VE GELECEK ÇALIŞMALAR (CONCLUSION AND FUTURE STUDIES)

Siber savunma tatbikatlarına verilen önem her geçen gün artmaktadır. Ülkelerin gerek ulusal bazda kendi siber savunma tatbikat platformlarını geliştirme ve uygulamasını yaygınlaştırma gerekse uluslararası arenada organize edilen siber savunma tatbikatlarına dahil olmaları ve bu tatbikatların planlama ve gelişimlerine daha yüksek bütçeli rakamlar ayırmaları ileride daha güçlü siber savunma sistemleri oluşturabilmeleri adına faydalı sonuçlar elde etmelerine katkılar sağlayabilecektir. Ulusal ve uluslararası alanda bu tatbikatlara ağırlık verilmesi bir yandan siber alandaki zayıf noktaların ortaya çıkarılması ve siber savunma bilincinin canlandırılmasına bir yandan da siber savunma ile ilgili konularda geliştiren tatbikatlara da entegre edilen teknolojilerin de takip edilebilmesi açısından yararlar sağlayacaktır.

Gelecek çalışmalar için daha önce de bahsedildiği gibi siber savunma tatbikatları için sorunlu bir konu olan puanlama sistemi ve bu sistemin standartlaştırılması ve daha adil puanlama sistemi geliştirilmesi üzerine teknik bir araç geliştirilecektir. Yine bahsedildiği gibi elektrik şebeke sistemleri ve dron kontrol sistemleri gibi yeni teknolojilerin siber savunma tatbikatlarına entegrasyonu oldukça kritik bir konudur. Bu özel sistemlerin tatbikatlara entegre edilmesinde mevcut sorunlar ve izlenmesi gerek metotlar gelecekte yapılacak bir başka çalışma konusudur.

Bu özel sistemlerin tatbikatlara entegre edilmesinde mevcut sorunlar ve izlenmesi gereken metotlar gelecekte yapılacak bir başka çalışma konusudur.

KAYNAKLAR

[1] Cyber Defence Exercise Locked Shields 2013 – After Action Report, NATO CCD COE, Tallinn, 2013.

[2] Cyber Defence Exercise Locked Shields 2014 – After Action Report, NATO CCD COE, Tallinn, 2014.

[3] Cyber Defence Exercise Locked Shields 2015 – After Action Report, NATO CCD COE, Tallinn, 2015.

[4] Cyber Defence Exercise Locked Shields 2016 – After Action Report, NATO CCD COE, Tallinn, 2016.

[5] The 2015 Report on National and International Cyber Security Exercises, ENISA, 2015.

[6] Locked Shields 2017, NATO CCD COE, Retrieved from: https://ccdcoe.org/locked-shields-2017.html, 2017.

[7] Cyber Coalition 16: NATOs Largest Cyber Defence Exercise, NATO SHAPE, Retrieved from: https://www.shape.nato.int/2016/cyber-coalition-16-ends-natos-largest-cyber-defence-exercise, 2017.

[8] Cyber Europe 2016, Retreived from: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce-2016, 2017.

[9] Cyber Defense Exercises – Participant Information Package, ENISA, 2013.

[10] Introduction to Cyber Exercises, National Cyber Security, Division Cyber Exercise Program, DHS, 2003.

[11] N. Wilhelmson, T. Svensson, "Handbook for Planning, Running, and Evaluating Information Technology and Cyber Security Exercises", CATS, 2013.

[12] C. A. M. Forero, Tabletop Exercise For Cybersecurity Educational Training; Theoretical Grounding And Development, Master's Thesis, 2016.

[13] J. Kick, "Cyber Exercise Playbook", The MITRE Corp., 2014.

[14] Cyber-Exercises Analysis Report, ENISA. 2016.

[15] Good Practice Guide on National Exercises, ENISA, 2009.

[16] Joint Training Manual for the Armed Forces of the United States, Chairman of the Joint Chiefs of Staff Manual, 2012.

[17] 2016 - 2019 Ulusal Siber Guvenlik Stratejisi, T.C. UDHB, 2016.

[18] R. Kissel (Ed.), "Glossary of Key Information Security Terms", NIST, 2013.

[19] H. Watanbe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami. "Blockchain Contract: Securing a Blockchain Applied to Smart Contracts". IEEE International Conference on Consumer Electronics (ICCE), pp. 467-468, 2016.

[20] S. Singh and N. Singh. "Blockchain: Future of Financial and Cyber Security". IEEE 2nd International Conference on Contemporary Computing and Informatics (IC3I), pp. 463-467, 2016.

[21] SecureChain: A Blockchain Security Gateway for SDN. http://www.reply.com/en/content/securechain (Erişim Tarihi: 30.08.2017).

[22] N.B. Barnas. "Blockchains in National Defense: Trustworthy Systems in a Trustless World". A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Air University, 2016.

[23] K.J. O'Dwyer and D. Malone. "Bitcoin Mining and its Energy Footprint". 25th IET Irish Signals & Systems Conference and China - Ireland International Conference on Information and Communications Technologies (ISSC 2014 / CIICT 2014), 2014.

[24] The Bitcoin and Blockchain: Energy Hogs. https://theconversation.com/the-bitcoin-and-blockchain-energy-hogs-77761 (Erişim Tarihi: 30.08.2017).

[25] J. Poon and T. Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments". 2016. DRAFT Version 0.5.9.2. https://lightning.network/lightning-network-paper.pdf (Erişim Tarihi:30.08.2017).

[26] Could a Blockchain-based Electricity Network Change the Energy Market? https://www.theguardian.com/sustainable-business/2017/jul/13/could-a-blockchain-based-electricity-network-change-the-energy-market (Erişim Tarihi: 30.08.2017).

[27] Proof of Work vs Proof of Stake: Basic Mining Guide. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake (Erişim Tarihi: 30.08.2017).

TERMİNOLOJİ

Faaliyet Sonu İncelemesi (After Action Review – AAR) [16]: Proje yada faaliyetten sorumlu kişiler ve katılımcılar tarafından gerçekleştirilen faaliyet ile ilgili, ne olduğu, neden olduğu ve daha iyi nasıl yapılabileceği sorularına cevap olabilecek nitelikte, analiz amaçlı hazırlanan analitik gözden geçirmedir.

Faaliyet Sonu Raporu (After Action Report – AAR) [16]: Gerçekleştirilen faaliyet ile ilgili, faaliyeti gerçekleştirenler tarafından üstlenilen belirli bir hedef odaklı eylem dizisi üzerine geriye dönük analiz için hazırlanan rapordur.

Siber Güvenlik [17]: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade eder.

Ana Senaryo Etkinlik Listesi (Master Scenario Event List – MSEL) [16]: Belli çıktıları elde etmek amacıyla önceden yazılmış senaryolar bütünüdür.

Enjeksiyon [16]: Ana senaryo etkinlik listesinin bir parçası olarak yürütülen belirli bir etkinliği ifade eder.

Tatbikat [16]: Talim ve durum değerlendirme amaçlarıyla yürütülen, planlama, hazırlık ve uygulama aşamalarını içeren simüle edilmiş savaş anı ortamıdır.

Tatbikat Senaryosu [16]: Tatbikat ve talim hedeflerini başarmak için yeterli kapsam ve ayrıntıda olan stratejik ve operasyonel ortamı tanımlar.

Hotwash [18]: Tatbikatın hemen sonrasında görevli personel ve katıımcılarla yapılan bilgilendirme ve değerlendirmelerdir.

Angajman Kuralları (Rules of Engagement) [18]: Bilgi güvenliği testinin yürütülmesine ilişkin detaylı yönergeler ve kısıtlamaları ifade etmektedir. Angajman kuralları bir güvenlik testinin başlamasından önce oluşturulur ve test ekibine ek izinlere gerek kalmaksızın tanımlanmış faaliyetleri yürütme yetkisi verir.

Tehdit [17]: Bir kurumun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen bir olayın potansiyel nedenini ifade eder.