KİŞİSEL, KURUMSAL VE ULUSAL BİLGİ GÜVENLİĞİ FARKINDALIĞI ÜZERİNE BİR İNCELEME

S.E. Erol, E.B. Ceyhan ve Ş. Sağıroğlu

***Özet*—Bilgi sistemleri son yıllarda kamu ve özel sektörün en fazla yatırım yaptığı alanlardan biri olarak göze çarpmaktadır. Kritik altyapı sistemleri olarak kabul edilen altyapılar (elektrik, su, telekomünikasyon, bankacılık vb.) da dahil olmak üzere hayatın hemen her alanı bilişim sistemleri ile yönetilmektedir. Bu gelişmeler siber saldırıların da hızla artmasına ve çok farklı yöntemlerle uygulanmasına ortam sağlamaktadır. Bilgi sistemlerinin güvenliğinin sağlanabilmesinde en önemli unsur insandır ve ancak insanların bilgi güvenliği farkındalığının yükseltilmesi ile bilgi sistemlerinde güvenlikten söz edilebilir. Bu çalışmada öncelikle saldırganın bir sonraki adımının tahmin edilebilmesi için bir siber saldırı yaşam döngüsü ortaya konulmuştur. Tahmin edilen saldırıların ulusal, kurumsal ve kişisel düzeyde önlenebilmesi için ise bilgi güvenliği farkındalık döngüsü dinamik bir süreç olarak ortaya konulmuş ve örnek olaylar kapsamında değerlendirilmiştir.**

***Abstract*— Information systems have been developed in last years and public/private companies have been investing on much in this area. Especially, critical infrastructures that are affecting public life such as banking, barage systems, hydroelectric plant systems, telecomunication systems etc. are managing by information systems. This type of management systems allow hackers to reach and damage critical infrastructures so the number of cyber attacks increasing in this area. To defend information systems from hackers the most important component is human being. To be able to secure information systems all people should have high security awareness. In this paper firstly, cyber attack life cycle modelled to be able to predict attackers next step. Then, an information security awareness cycle modelled and evaluated with examples to prevent attacks that can be effective in national, institutional and personel level security.**

Anahtar Kelimeler—bilgi güvenliği; farkındalık; bilgi; siber saldırı; bilgi güvenliği farkındalık döngüsü; siber saldırı yaşam döngüsü; güvenlik.

Keywords—information security; awareness; information; information security awareness cycle; cyber attack life cycle; cyber attack; security.

I. GİRİŞ

Günümüzde bilgi teknoloji sistemlerinin bilgiye her yerden ve merkezi olarak erişimi mümkün kılmasından dolayı bilgi sistemleri hayatın tüm alanlarında etkin olarak kullanılmaktadır. Günümüzde e-devlet uygulamalarının da kullanıma sunulması ile resmi işlemlerden yasal işlemlere, eğlenceden eğitime kadar bir çok alanda bilgi teknolojileri gündelik hayat içerisinde kendisine yer edinmiştir.

Bu denli hızlı gelişen bilgi teknoloji sistemlerinin gelişimine ve tanımlarına göz attığımızda öneminin her geçen gün arttığı görülmektedir. Özellikle sistemlerin birbirine bağımlılığının artmasıyla iş dünyası ve kamu hayatı hızla artan sayılarda ve çok çeşitli saldırılara maruz kalmaktadır. Bilginin basılı, elektronik ortamda, tabelalarda, konuşmalarda vb. birçok şekilde bulunması, bilgi paylaşımlarının yaygınlaşması ve farklı bir çok yöntem ile gerçekleştirilmesi saldırıların yöntem ve çeşitliliğinin artmasına da imkan sağlamaktadır. Verinin paylaşımı ve sürekli erişime açık olması nedeniyle bilginin gönderen kaynaktan alıcıya kadar gizlilik içerisinde, bozulmadan, yok edilmeden, değiştirilmeden, başkaları tarafından ele geçirilmeden ve bütünlüğü sağlanmış bir şekilde iletilmesi bilgi güvenliğinin sağlanması için temel kriterlerdir. Kamu hayatını düzenleyen sistemler açısından bakıldığında bu kriterlerin önemi çok daha açık bir biçimde karşımıza çıkmaktadır.

Dünyada giderek yaygınlaşan e-devlet uygulamaları ve gelişen web ortamı dünyayı çok hızlı bir dönüşümden geçirmektedir. Bu yaklaşımların yaygınlaşması siber ortamdaki saldırganların motivasyonlarını da yükseltmiştir. Genel olarak politik, ticari ve bireysel olarak sınıflandırılan motivasyonlar siber ortamın sağladığı erişim imkanlarıyla da birleşerek siber saldırının sınırlarını yok etmiştir. Dünyanın herhangi bir bölgesinden başka bir bölgeye çok düşük maliyet ve tanınmazlık perdesinin arkasına sığınarak saldırılar yapmak ve ülke veya ticari kurumları zarara uğratmak günümüzde mümkün hale gelmiştir. İnternet ortamının getirdiği faydaların yanı sıra dış tehdit kavramı da oldukça yaygınlaşmıştır. Kritik bilgi altyapısına sahip SCADA sistemlerini etkileyen olayların 2001 öncesi %50'si kullanıcı hatası olarak etiketlenmiş ve sadece %29'u dış etkilere bağlanmıştır. 2004 yılında, bu oranlar aniden değişmiş ve %66 dış olaylar ve %22 kaza olarak rakamlar değişmiştir [1].

Günümüzde saldırılar ve saldırganların yöntemleri çok çeşitlenmiştir. Dolayısıyla takip etmek neredeyse imkansız hale gelmiştir. Ancak bilginin değerinin her geçen gün daha da artması ve sistemlerde oluşan hasarların giderilmesi maliyetlerinin koruma maliyetlerinden çok daha yüksek olması sebebiyle kurumlar ve kişiler bilgi güvenliğine dikkatlerini yöneltmişlerdir. Bu çalışmada bilgi güvenliği farkındalığının davranışa dönüştürülebilmesi için siber saldırı yaşam döngüsü ve bilgi güvenliği farkındalık döngüsü modellenerek dinamik süreçler olarak ortaya konulmuştur. Tekrarlayan ve birbirini izleyen adımlardan oluşan bu döngülerin anlaşılabilmesi ve içselleştirilebilmesi için öncelikli olarak bilgi ve bilgi güvenliği kavramları, siber saldırı yaşam süreci ve sınıflandırılması, bilgi güvenliği tehditleri açıklanmış, bilgi güvenliği farkındalığının eksik olması durumunda ortaya çıkan kişisel, kurumsal ve ulusal bilgi güvenliği ihlallerine ilişkin örnek olay değerlendirmeleri yapılarak bilgi güvenliği farkındalık döngüsünün önemi ortaya konulmuştur.

II. BİLGİ VE BİLGİ GÜVENLİĞİ KAVRAMLARI

Bilgi; fiziksel veya sanal ortamlarda yer alan, hayatımızı kolaylaştırma, düzenlenme, saklanabilme ve çeşitli iletişim araçları vasıtasıyla hedeflenen alıcılara iletilme özelliklerine sahip anlamlı, işlenmiş veriler bütünü [2] olarak tanımlanmaktadır. ISO-IEC 17979'da bilgi, iş dünyasının önemli varlıklarından biri olarak, kurumun iş yaşamını devam ettirmesi için korunması gereken varlıklardan biri olarak tanımlanmıştır. Özellikle sistemlerin birbirine bağımlılığının artmasıyla iş dünyasında hızla artan sayılarda ve çok çeşitli saldırılara maruz kalmaktadır. Yine ISO-IEC 17979'da bilginin filmlerden konuşmalara kadar bir çok farklı şekilde bulunabileceği, paylaşım ya da depolanma yöntemi gözetilmeksizin her zaman uygun şekilde korunması gerektiği belirtilmiştir. Bilgi güvenliğinin kamu ve özel sektör arasında yoğun veri alış verişi olmasının bilgiye erişimde kontrolleri zorlaştırdığı, bilginin kamu, özel sektör ve kritik altyapılar için çok önemli olduğu aktarılmıştır. Literatürde bilgi güvenliği bilginin bir varlık olarak doğru teknoloji ile doğru amaç ve yöntemler kullanılarak tüm platfomlarda başkaları tarafından elde edilmesinin engellenmesi, oluşabilecek zararlardan korunması [3], sayısal ortamda bilgilerin saklanması ve iletilmesi esnasında güvenliğin sağlanabilmesi için bilginin güvenli bir ortamda işlenmesine yönelik yapılan tüm çalışmalar [2] gibi ifadelerle tanımlanmaktadır. Genel bir değerlendirme yapıldığında; gizlilik, bütünlük, erişebilirlik ve önceden tahmin edip önlem alma kavramlarının ortak paydalar olduğu görülmektedir. Verinin paylaşımı ve sürekli erişime açık olması bilginin gönderen kaynaktan alıcıya kadar gizlilik içerisinde, bozulmadan, yok edilmeden, değiştirilmeden, başkaları tarafından ele geçirilmeden ve bütünlüğü sağlanmış bir şekilde iletilmesi çok büyük önem arz etmektedir. Bu şartların sağlanabilmesi için ise ortaya çıkabilecek tehditlerin önceden tespit edilerek önlemlerinin alınması gerekmektedir.

Kamu hayatını düzenleyen sistemlere kişisel, kurumsal ve ulusal bilgi güvenliği açısından bakıldığında bilgi güvenliğinin günümüzde hangi noktalara ulaşabildiğini görmek mümkündür. Estonya'nın 26 Nisan 2007'de Bronz Asker heykelini kaldırmasıyla dünyada siber savaş kavramı bir gerçekliğe dönüşmüş ve Rusya yanlısı gruplar tarafından gerçekleştirilen DoS saldırılarıyla Estonya Hükümeti, kamu kurumları ve bankacılık hizmetlerine ait bir çok internet sitesi hizmet dışı kalmıştır. Estonya konuyu NATO'nun gündemine taşımış, dünya bir savaşın eşiğine gelmiştir. Benzer olarak Rusya Gürcistan ile savaşırken eş zamanlı olarak siber saldırıları da başlatmış ve Gürcistan devlet kurumlarının bilgi sistemlerini uzun süre erişilemez hale getirmiş ve zarara uğratmıştır [4].

Türkiye'de halihazırda Gürcistan ve Estonya örneklerinde belirtilen uluslar arası ölçeklerde bir siber saldırı yaşanmamış olmasına karşın, UYAP'ta henüz yargılaması başlamamış gizli bir kovuşturmaya ilişkin verilerin deşifre olması durumunda kararlara tesir edecek delillerin karartılması, zanlıların kaçması gibi sonuçlar doğurabileceği, ya da askeri bir bilgi sisteminden harekata ait bilgilerin sızdırılması veya değiştirilmesi gibi senaryolar değerlendirildiğinde sonuçlarının çok vahim seviyelerde olabileceği açıktır.

Bahsedilen risklerin varlığı, ortaya çıkardığı dezavantajların yanı sıra kurumların varlıklarını gözden geçirip açıklıklarına yönelik önlemler üzerinde düşünmesine ve tedbirler almaya yönelik çalışmalara başlamasına sebep olmuş, kurumların bilgi sistemlerine yönelik farkındalığın artması sürecini de hızlandırmıştır.

III. BİLGİ GÜVENLİĞİ FARKINDALIĞI KAVRAMSAL DEĞERLENDİRME

Bilgi güvenliği farkındalığı kişisel ya da kurumsal güvenliğin sağlanabilmesi için bilgi güvenliğine yönelik tehditlerin ve sonucunda oluşabilecek durumların kavranmasıdır. Bu farkındalık sayesinde kullanıcıların karşısına çıkan kötücül uygulamalara, linklere ve yazılımlara karşı davranışlarında bilinçli bir tutum sergileyerek saldırganların bilgi sızıntısı yapmasına ya da kullanıcının kendini zorda bırakabileceği, veri, itibar kaybedebileceği durumlara karşı kendini korumasıdır. Bir başka deyişle bireylerin bilgi güvenliğinin ne olduğunu ve neden önemli olduğunu bilmeleri teknolojik tüm önlemlere rağmen insanın bilgi güvenliğinin en uç noktasında bulunduğunun kavranması açısından önemlidir.

Kurumlarda çalışanların kurumun bilgi güvenliği politikalarına uyumluluğu önemli bir sosyo-organizasyonel kaynak olarak ortaya çıkmıştır [5,6]. Çünkü çalışanlar bilgi güvenliği konusunda en zayıf halkadır [7,8]. Benzer şekilde internet, akıllı cihaz vb. kullanımlarında da kişi ancak bilgi seviyesi ile orantılı şekilde önlemler alabilir. E-devlet uygulamalarının getirisi olarak ulusal sistemler de artık dış tehditlere açık hale gelmiştir. Tehditlerin kişisel, kurumsal ve ulusal bilgi varlıklarını hedef alacak şekilde farklılıklar göstermesi, bilgi güvenliği farkındalığının 3 ana başlık altında değerlendirilmesini gerektirmektedir. Tüm başlıkların da hedef kitlesi insan olmasına rağmen izlenmesi gereken yol ve yöntemler ciddi anlamda farklılaşmaktadır.

Kurumların uzun yıllar yoğun çaba ve emek harcayarak sahip oldukları en değerli varlıkları olan bilginin, güvenliğin temel bileşenleri olan; gizlilik, bütünlük ve erişilebilirliğinin sağlanması için etkin bir şekilde korunması gerekmektedir. Kurumsal düzeyde bilgi güvenliği, kurumun sahip olduğu ürün ya da sunduğu hizmetin devamlılığının sağlanabilmesi için bilgi varlıklarının muhtemel saldırı ve tehditlere karşı korunması olarak ifade edilmektedir [9]. Bilgi varlıklarının bahse konu tehditlere karşı güvenliğinin sağlanabilmesi için üç temel sürecin bütüncül bir yaklaşımla uygulanması gerekmektedir [2]. Bu süreçlerden ilki, planlama, strateji ve politikaları kapsayan yönetsel süreç, ikincisi, virüsten koruma, yedekleme gibi teknik işlemleri kapsayan teknolojik önlem süreci, üçüncüsü ise kullanıcı eğitimlerini kapsayan bilgi güvenliği farkındalık sürecidir. Kurumlarda sistematik bir yaklaşımla bilgi güvenliği sağlanamadığı durumlarda kurumun saygınlığını kaybetmesi, borçlanması ve maddi zarara uğraması gibi sonuçlar ortaya çıkabilmektedir [10].

Kurumlarda çalışanların bilgi güvenliği farkındalığı, etkili bilgi güvenliği yönetim sistemlerinin çok önemli bir parçasıdır [11]. Kişisel ve kurumsal bilgi güvenliği olarak iki ana başlık altında yapılan değerlendirme sonrasında kurumlarda bilgi güvenliği farkındalığı da kendi içinde genel farkındalık ve bilgi güvenliği politikaları farkındalığı olarak ele alınabilir [12]. Genel bilgi güvenliği, bir çalışanın bilgi güvenliği konusunda temel bilgiler ve potansiyel problemler ve bunların etkileri hakkında fikir sahibi olmasıdır. Bilgi güvenliği politikası farkındalığı ise çalışanın kurumun güvenlik politikasını bilmesi, politika içinde yer alan gereksinimleri ve hedeflerini anlamasıdır [12]. Örnek olarak; çalışanlar parolalarının güvenli olması gerektiğini bilebilirler ancak kurumsal olarak parola belirleme ve yönetim

politikalarını ve nasıl uygulayacakları konusunda bilgi eksiklikleri olabilir. Bu durumda politikaların eyleme dönüştürülmesi yönünde eksiklik olduğu görülmektedir. Kurumsal bilgi güvenliğini arttırmak amacıyla verilen eğitimlerde, kurumların en değerli varlığı olan bilginin korunması konusunda kurum çalışanları ve bilgi etkileşiminde bulundukları kişilerin de sorumluluklarını anlamaları hedeflenmelidir [13]. Bir kurumda çalışan bireylerin düzenli olarak farkındalık eğitimleri almaları gerektiği ISO 27001:2005 standardında da Ek A 8.2.2 maddesinde, Bilgi Güvenliği Farkındalığı Eğitimi ve Öğretimi başlığı altında, "Kuruluştaki tüm çalışanlar ve ilgili olan yükleniciler ve üçüncü taraf kullanıcılar, kendi iş fonksiyonları ile ilgili kurumsal politikalar ve prosedürler hakkında gerekli farkındalık eğitimini düzenli olarak almalıdırlar." [14] şeklinde belirtilmektedir.

Kurumsal bilgi güvenliği farkındalığı daha çok kurumun standart ve politikalarının kullanıcılara öğretilmesi ve ortaya çıkabilecek riskli durumlar ve karşılaşılan tehditlere yönelik olarak yapılması gerekenlerin üzerinde durularak gerçekleştirilebilmektedir. Ancak, kişisel bilgi güvenliği farkındalığı denildiğinde internet ortamına çıkılan andan itibaren her türlü tehdit kapsam alanına girmektedir. Genelde kurum çalışanları bir şekilde denetleme, belge imzalatma gibi uygulamalar ile güvenliğe ilişkin en azından fikir sahibi olmaktadır. Ancak, internet ve bilgisayarı kullanan her bir birey için kişisel bilgi güvenliği farkındalık eğitimleri kesinlikle verilmelidir. Özellikle sosyal paylaşım sitelerini (facebook, twitter, blogger, linkedin vb.) kullanan insanlar kendi istekleriyle farkında olmadan iş bilgileri, kişisel bilgiler gibi özel bilgileri internet ortamında herkesin erişebileceği şekilde paylaşmaktadır. Bu durum bilgisayar korsanlarına sosyal mühendislik yöntemlerini de kullanarak dolandırıcılık gibi suç faaliyetlerini gerçekleştirmelerine olanak sağlamaktadır.

Ulusal bilgi güvenliği ise Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısında; "Ulusal güvenliği ilgilendiren, yetkisiz ellere geçtiği taktirde devletin güvenliğini tehlikeye sokabilecek veya devlet aleyhine kullanılabilecek her türlü bilgiyi, üretim, kullanım ,işlenme saklanma, nakledilme ve imha sırasında yetkisiz kişilerin erişimine ve olası her türlü fiziksel ve elektronik müdahaleye karşı korumaya; bilgiye erişim ve kullanıma ait usulleri açık şekilde belirlemeye ve bilgiyi gerektiğinde hazır bulundurmaya yönelik tedbirler [15]" olarak tanımlanmıştır. Genel olarak değerlendirildiğinde en büyük tehdit kişisel bilgi güvenliğine yönelik olarak gerçekleşmektedir. Farkındalık seviyesi arttıkça tehdit miktarı da azalmakta, ancak tehditin gerçekleşmesi durumunda ortaya çıkan kayıp ters orantılı olarak artmaktadır. Bu nedenle kritik altyapılara, ülkenin ulusal güvenliğini ilgilendiren alanlarda yapılacak bir saldırı kaotik bir ortama sebep olacak olmasından dolayı dikkatle ele alınmalı ve en üst seviyede önlemler alınmalıdır.

Sosyal mühendislik saldırılarının odak noktasında insan vardır. Saldırganlar tarafından sistem güvenlik önlemleri aşılamadığı zaman en etkili yol sosyal mühendislik saldırıları ile erişim hakkı elde etme yöntemleri olmaktadır. Sosyal mühendislik saldırılarındaki başarı riskini indirgemenin en önemli yolu kişilerin bu konudaki farkındalığını, bilgi ve becerisini artırmaktır.

Kişisel, kurumsal ya da ulusal seviyede bilgi güvenliği farkındalığı oluşturabilmek için sistematik bir döngü dahilinde hareket edilmelidir. Bu döngü insanların davranışlarında değişiklik oluşturmalıdır. Dijle'nin Türkiye'de eğitimli insanların bilişim suçlarına yaklaşımına ilişkin yaptığı bir çalışmada, yazılımlar aracılığıyla verilerinin çalındığını düşünen kullanıcı sayısı %51,7 iken, açıklıklara ilişkin firmalar tarafından yapılan güncellemelerin kullanılamadığı ve savunmasız bir ortamı meydana getiren lisanssız yazılım kullanım oranı %75 olarak ortaya konulmuştur [16]. Farkındalık seviyesi ile davranışın ayrı yönlerde hareket edebildiği göz önüne alındığında farkındalık üzerine yapılan eğitim ve çalışmalarda davranış değişikliği hedeflenmelidir. Davranış değişikliği ise ancak tekrarlayan ve dinamik bir döngü ile güvenlik kültürü olarak kullanıcılar tarafından içselleştirilebilir.

Şekil 1'de gösterilen bilgi güvenliği farkındalık döngüsü doğrultusunda kullanıcılar öncelikle karşılaşabilecekleri tehditlere ilişkin bilgi sahibi olarak tehditlerin yeteneklerini kavramalıdır. Dönemsel olarak ortaya çıkan ya da sanal ortamda sürekli var olan tehditlerden kendisine karşı harekete geçebileceğini değerlendirdikleri tespit edilerek, bilgi varlıklarını koruyabilmek adına bu tehditlerden korunma yöntemlerini öğrenmeli ve en uygun olanını seçerek uygulamalıdır. Tehditin alınan korunma önlemlerine rağmen gerçekleşmesi durumunda kullanılan cihaz ve bilişim ortamı üzerinde nasıl etkiler bırakacağı, kötücül ortamı ve oluşturduğu hasarı nasıl saptayacaklarını bilmeli ve hangi düzeltici işlemleri uygulamaları gerektiği konusunda deneyim sahibi olmalıdırlar. Bu adımdan itibaren olası saldırılarda zarara uğramamak için güncel olası tehditler sürekli olarak izlenmelidir. Ancak bu şekilde dinamik bir farkındalık döngüsünü içselleştiren kullanıcıların sahip olduğu bilgi güvenliği farkındalık seviyesinin davranışlarını şekillendirilebileceği değerlendirilmektedir. Aksi taktirde edinilen bilgi ve tecrübeler kalıcı olmayacak, kısa bir süre sonra yeni tehditlerle beraber bilgi güvenliği ihlalleri ortaya çıkacaktır.

Şekil 1: Bilgi Güvenliği Farkındalık Döngüsü

Bilgi güvenliği farkındalığına ilişkin bir diğer önemli konu eğitimlerin genel kapsamlı yapılmamasıdır. Ağırlıklı olarak teknik, bilgi sistemlerinde çalışan personelin eğitilmesinin bilgi güvenliği açısından yeterli olduğu düşünülmektedir. Ancak bilgi sistemleri ile ilgili görevlerde çalışan kişilerde görevleri gereği farkındalık seviyesinin daha yüksek olduğu ortaya konulmuştur [17]. Bu nedenle bilgi sistemleri ile alakalı olmayan personelin daha çok risk altında olduğu, çalıştığı kurum ve birimle alakalı olarak da kurumsal ya da ulusal seviyede bilgi güvenliği için bir tehdit unsuru olabileceği de göz önünde bulundurulmalıdır.

IV. TEHDİTLERİ ANLAMAK: SİBER SALDIRI YAŞAM SÜRECİ VE SALDIRI SINIFLANDIRMASI

Kullanıcı ya da çalışanların bilgi güvenliği farkındalığının arttırılabilmesi için saldırıların hangi kaynaklar tarafından gerçekleştirildiği, bir saldırının hangi adımlardan oluştuğu, saldırıların türleri ve tasniflendirilmesi ile ilgili genel bilgi birikimi oluşturulmalıdır. Her ne kadar teknik personel kadar konuyu kavrayamasalar da içerik olarak neler olduğunu anımsayabilecekleri bilgi birikimine sahip olmalıdırlar. Günümüzde siber saldırılar sistemlerin sahip olduğu bilgi varlıklarının öneminin ve miktarının artmasıyla kabuk değiştirmiştir. Yabancı devletler, terörist gruplar, endüstriyel siber casuslar ve organize siber suçlular, siber eylemciler (Hacktivist), bilgisayar korsanları (Hackers) saldırılara kaynak teşkil etmektedir [18]. Saldırı ve tehditlerin artmasına paralel olarak güvenlik önlemleri de artmakta, sistemlere erişim eskiye nazaran takım çalışması ve karmaşık bilgilerin çözülmesine yönelik işlemlerle gerçekleştirilmektedir. Sisteme erişimin zorlaşması saldırganların sistematik bir yöntem izlemesini de gerektirmektedir. Tehditleri anlamak ancak siber saldırılar gerçekleştirilirken kullanılan metotların ve adımların anlaşılması ile mümkün olabilir. Bu kapsamda 6 adımlı siber saldırı yaşam süreci sistematik yaklaşımları tanımlayan ve en doğru ifade eden sınıflandırmalardan biri olarak karşımıza çıkmakta ve uygulanmaktadır [19]. Bu süreç sonucunda saldırganlar kazanç elde etmekte ve bir sonraki hedefi belirlemek için harekete geçmektedirler. Bu sayede siber saldırılar Şekil 2'de görülen dinamik bir döngüye dönüşmekte bu da saldırıların sürekli olarak kendini yenilemesini ve geliştirmesini sağlamaktadır.

Şekil 2 : Siber Saldırı Yaşam Döngüsü

Günümüzde Şekil 2'de belirtilen saldırı adımlarının gerçekleştirilebilmesine olanak sağlayan bir çok araç bulunmaktadır. Dolayısıyla artık çok yüksek bilgi seviyesinde olmayan kişiler bile rahatlıkla hedef sistemlere saldırı gerçekleştirebilmektedir.

Siber saldırı yaşam sürecinin ilk iki adımını, çoğu zaman iç içe geçen bilgi toplama ve keşif oluşturmaktadır. Saldırganlar, sistemlere sızabilmek için Host Sweep ve port tarama yöntemlerini kullanırlar. TCP Echo, UDP Echo, ICMP Sweep ile bir ağda bulunan hostları belirlenirken; port tarama atakları ise, açık portların belirlenerek servisler üzerinden saldırı yapılmasına imkan tanır [20].

Açık kaynak kodlu araçlarla kolaylıkla port taraması yapılabilmektedir. NMAP bir çok farklı port tarama tekniğini tek komutla yapmaya imkan tanımaktadır. Port tarama dışında sosyal mühendislik, whois sorguları, pasif saldırılar(ağa yerleşerek trafiğin izlenmesi, ağ topolojisinin çıkarılması vb.), ping okuma, google hacking, shodan gibi arama motorları bilgi toplama ve keşif için etkin olarak kullanılmaktadır.

Zafiyetlerin taranması adımında ise sistemin açıklıklarının bulunmasına yönelik uygulamalar yapılmaktadır. Açıklık; istemeden/kazayla başlatılabilen ya da bilerek suistimal edilebilen zaaflar [21] ya da "bir varlığı tehditlere karşı korumasız hale getiren her türlü unsur (sistem bileşenlerinden, güvenlik politika ve prosedürlerinin yokluğundan, yetersizliğinden veya uygulanmayışından, eksik veya hatalı sistem tasarım ve uygulamalarından, organizasyon yapısı, yönetici ve çalışanların bilgi birikimi ve tutumundan kaynaklı nedenler)" olarak tanımlanmaktadır [22].

Saldırı yaşam sürecinin zafiyet tarama, açıklıkları istismar etme ve sistemin ele geçirilmesi adımlarının içeriğini oluşturan saldırıların, genel olarak 5 ana başlık altında sınıflandırıldığı görülmektedir. Bunlar [23];

1) Amaca dayalı saldırılar: Keşif saldırısı, erişim saldırısı ve servisin engellenmesi saldırısı olarak 3 kategoride toplanmıştır.

2) Yasal sınıflandırma: Siber suç, siber casusluk, siber terörizm ve siber savaş olarak 4 kategoride toplanmıştır.

3) Dahil olma şiddetine göre: Aktif ve pasif saldırılar olmak üzere 2 kategoride toplanmıştır.

4) Kapsama göre: Kötü niyetli büyük ölçekli ve iyi niyetli küçük ölçekli olarak 2 kategoride toplanmıştır.

5) Ağ türüne göre: Mobil adhoc ağları ve kablosuz sensör ağları olarak 2 grupta kategorize edilmiştir.

Sisteme erişime imkan sağlayan açıklıklar KALI benzeri araçlar kullanılarak ya da manuel olarak tespit edilebilmektedir. Bu adımı takiben sistemin açıklıkları istismar edilerek hedeflenen verilerin elde edilmesine ve sistemin ele geçirilmesine yönelik işlemler gerçekleştirilir. Örneğin, web sitelerindeki kodun açıklıklarından faydalanarak kullanıcı girdilerinden anlamlı komutlar türeterek bilgi sızdırma olarak tanımlanan SQL enjekte yapılabilir.

Bir saldırının son adımı ise, sistemde yer alan saldırıya ilişkin izlerinin silinmesidir. Bir ağa sızmayı başaran saldırgan, elde ettiği bilgiler ya da sisteme verdiği zararlar anlaşıldığında kendisine ulaşılmasını engellemek için sisteme bıraktığı izleri silmek isteyecektir.

Tüm bu saldırı adımları uygulanarak dışarıdan yapılan saldırıların yanı sıra insider olarak tanımlanan iç saldırılar da gerçekleşebilmektedir. İçeriden gelen saldırıların bir kısmı aslında kötü niyetli olmayan ancak bilgisayarına zararlı yazılım bulaşmış masum kullanıcılardan kaynaklanırken, kötü niyetli saldırıların %80'inin ise sistemde görevli teknik personel tarafından yapıldığı gözlemlenmiştir [24].

V. ÖNEMLİ TEHDİTLER

Saldırı yaşam süreci ve bu sürecin adımlarında gerçekleştirilen işlemlerin ardından kullanıcı ve çalışanların kurumsal ve kişisel bilgi güvenliğine etkin katılan bir unsur olabilmeleri için öncelikle bütün tehditleri olmasa da en azından genel geçer ve yaygın olan tehditler konusunda bilgi

sahibi olmaları gerekmektedir. Bu tehditler alt başlıklar halinde verilmiştir.

A. Hizmet Dışı Bırakma Saldırıları (DoS/DDoS, Botnet)

Siber savaşın en etkili ve en verimli yöntemlerinden birisi Dağıtık Hizmet Aksattırma (DDOS/DOS) ataklarıdır. Bu saldırıda bilgi güvenliğinin özelliklerinden biri olan "erişilebilirlik" hedef alınmaktadır. Bu saldırı sonucu sadece bilgi, para, zaman kaybı değil bazen daha önemli olabilecek itibar kaybı ortaya çıkmaktadır [25]. Bu saldırıda amaç, hedef sisteme cevap veremeyeceği miktarda fazla istek göndererek, bant genişliği, CPU zamanı veya disk alanı gibi kaynakların tüketilmesi ya da yapılandırma bilgileri ile fiziksel ağ bileşenlerinin bozulmasıdır. Dağıtık hizmet engelleme (DDoS, Distributed Denial of Service) saldırılarında ise DoS saldırılarından farklı olarak botnetler kullanılmaktadır. Botnet, yönetici tarafından kontrol edilen savunmasız sistemler, köle bilgisayarlar olarak tanımlanmaktadır. Köle bilgisayarlar vasıtasıyla farklı konumlarda bulunan kaynaklardan tek bir hedef sisteme istekler gönderilmektedir. Kullanılan botnetin büyüklüğüne göre çok büyük ve iyi bağlantılı web sayfalarının bile hizmetlerinin engellenmesi mümkündür [26]. Bunun örneklerini şu ana kadar gerçekleşen iki büyük DDOS saldırında görmekteyiz. Şimdiye kadar tespit edilen en büyük DDoS saldırısı Apple Daily ve PopVote sitelerine 500 gbps trafik ve saniyede 250 milyon DNS sorgusu ile yapılmıştır. İkinci DDoS saldırısı ise NTP kullanılarak gerçekleştirilmiştir. ABD ve Avrupa'yı hedef alan bu saldırıda 400 Gbps seviyesinde bir zirve yakalamıştır [27].

DDoS ile mücadele edebilmek için öncellikle teknik altyapılar ön planda olsa da kurumsal düzeyde oluşturulan güvenlik politikaları ve yapılan risk analizleri sayesinde bu saldırıların önlenmesi mümkün olabilmektedir. İlave olarak ağ üzerindeki bütün cihazlar dikkate alınmalı, zaman ve kaynak tüketen fonksiyonlar belirlenmeli ve gerçek DoS saldırılarına benzer ortam oluşturularak, ağ test edilmelidir. DDoS saldırısına karşı alınabilecek proaktif önlemler şu şekilde sıralanabilir [28]:

- Kullanılmayan servisler kapatılmalı,
- IDS imzası oluşturulmalı,
- DNS zaman aşımı kısa tutulmalı,
- ISS ile irtibata geçilerek ek bant genişliği talebinde bulunulmalı,
- Statik web sayfası kopyası bulunmalı,
- IP ve portu paket özelliklerine göre aktif edebilme, engelleyebilme veya kapatabilme özelliği bulunmalı,
- Default TCP timeout değerlerinin yüksek olması nedeniyle bu değer 1/10 a düşürülmeli veya oturum dolmaya başladıkça timeout değerleri otomatik azaltılabilmeli,
- Bir IP adresinden örneğin 500'den fazla istek geldiyse engelenecekler listesine eklenebilmeli ve IP adresine ait oturum tablosu boşaltılmalı,
- Yasal trafik geçirmiş IP adresine göre beyaz liste/kara liste uygulanmalı,
- Ülkelerin IP bloklarına göre erişim izni verilmeli, (Örneğin 20-30 farklı ülkeden DDos saldırısı ile karşılaşıldığında sadece Türkiye kaynaklı servis sağlayıcılarına giriş izni verilebilir)
- DNS round robin ve TTL değerleriyle oynama yaparak engelleme yapılmalı,
- Sniffer kullanılmalıdır.

B. SQL Enjekte Saldırıları

SQL enjekte açıklıkları web uygulamaları için en ciddi tehdit olarak tanımlanmaktadır. SQL enjekte açığı bulunan web uygulamaları saldırgana uygulamanın tüm veri tabanına erişim imkanı verir [29]. Bu veri tabanlarında kullanıcıların ve tüketicilerin çok hassas bilgileri yer almaktadır ve güvenlik ihlallerinde bu bilgiler çalınma, ifşa edilme, satılma veya dolandırıcılık amacıyla kullanılabilmektedir.

C. Sazan Avlama (Phishing) Saldırıları

Kimlik hırsızlığı olarak adlandırılan bu yöntem, banka, telekomünikasyon şirketleri gibi resmi bir kaynaktan geldiği izlenimi verilerek hazırlanmış e-postalar aracılığıyla kişisel bilgilerin elde edilmesi olarak tanımlanmaktadır. Sosyal mühendisliğin hareket alanında yer alan bu saldırı tipinde kullanıcı farkında olmadan kişisel bilgilerini kötü niyetli kişilere göndermekte ve sonrasında bu bilgiler kullanılarak gerçekleştirilen saldırılara maruz kalmaktadır [3]. Bu saldırı tipine karşı kişisel bilgi güvenliği farkındalık seviyesinin arttırılması ve dikkat en önemli silahlardır.

Ç. XSS Saldırıları

Kullanıcının veri girişi yapabileceği alanlarda genelde javascript kodları kullanılarak zararlı kod gönderilmesiyle yapılan saldırı türüdür [30]. XSS saldırıları günümüzde hakerlar tarafından web uygulamalarına sızmak için en fazla kullanılan saldırı türlerinden biridir. XSS saldırılarında saldırganın amacı, kullanıcının çerez bilgilerinin veya web sitesi tarafından kullanıcının kimlik doğrulamasının yapılmasına imkan sağlayan hassas bilgilerin çalınmasıdır [31]. Tablo 1'de web ortamında her dört saldırıdan birinin XSS saldırısı olduğu SQL injection saldırısının % 7 olduğu görünmektedir.

TABLO I
2013 YILI WEB UYGULAMA SALDIRILARI [32]

Saldırı Türü	Yüzde
XSS	25
Bilgi Sızdırma	23
Kimlik Doğrulama/Yetkilendirme	15
Oturum Yönetimi	13
SQL Enjekte	7
CSRF	6
Diğer	11

D. Zararlı Yazılımlar

Kötücül yazılımlar bulaştığı bilgisayar sistemindeki donanıma ve dosyalara zarar veren, yazılımların ayarlarını değiştiren, bilgisayardaki verileri izinsiz olarak başka kişilere gönderen veya bilgisayarı yabancı kişilerin erişimine açan istenmeyen zararlı yazılımlardır. En genel kötücül yazılımlar; Virüsler, solucanlar (worm), Truva atları (Trojan horse), arka kapılar (backdoor), mesaj sağanakları (spam), kök kullanıcı takımları (rootkit), korunmasızlık sömürücüleri (exploit), klavye dinleme sistemleri (keylogger), görüntü yakalama

sistemleri (screen logger), tarayıcı soyma (browser hijacking) ve casus yazılımlar (spyware) olarak belirtilebilir [33].

E. Sosyal Mühendislik

Günümüzde bilgi teknolojilerindeki hızlı ilerlemeye paralel olarak güvenlik alanında da teknolojik olarak kullanıcıyı koruyan uygulama ve donanımlar geliştirilmekte, kullanıcılar bilgi güvenliği eğitimleri ile bilinçli hale getirilmeye çalışılmaktadır. Bu noktada saldırganların başarıya ulaşmak için başvurdukları etkili yöntemlerden biri olarak sosyal mühendislik karşımıza çıkmaktadır. Sosyal mühendislik saldırıları, saldırganların isteklerini gerçekleştirmek için insan davranışları ve iletişimlerindeki açıklıkları kullanması [34, 35] ya da kullanıcıların normalde paylaşmayacağı kişisel verilerini kendiliğinden vermelerini sağlamak [36] olarak tanımlanmaktadır. Bu saldırıların en önemli riskleri oluşturduğu ve diğer bilinen saldırılara göre kontrolünün daha zor olduğu değerlendirilmektedir [37]. Bu saldırı türünün önlenebilmesi için kurumsal olarak güvenlik politikalarında düzenlemeler yapılmalı, eğitimlerde kullanıcılara anlatılmalı ve olay gerçekleştiğinde müdahale yöntemlerine yönelik önlemler alınması gerekmektedir.

En sık kullamılan sosyal mühendislik yöntemleri şunlardır:

- Karşı tarafı, güvenilir bir kaynak olduğuna inandırmak,
- Hedef sistemin atıklarını (çöpler, eski donanımlar vb.) bilgi bulmak maksadıyla karıştırmak,
- Ortak tanıdıklar vasıtasıyla yakınlık kurmak,
- Başkasını taklit ederek aldatmak (özellikle telefonda),
- Gizlice, düzmece, zor bir durum oluşturarak yardım ediyormuş izlenimi vermek.

Kurumsal düzeyde sosyal mühendislik saldırılarına karşı sistemin en zayıf halkası olan insanın eğitilerek hata payını en aza indirmek için bazı tedbirler alınabilir. Bu tedbilerin alınmasında amaç insan unsurunun;

- Bilgisini (İnsanlar ne biliyor)
- Tavırlarını (İnsanlar ne düşünüyor)
- Davranışlarını (İnsanlar ne yapıyor) değiştirebilmek ve geliştirebilmek [38] olmalıdır.

VI. BİLGİ GÜVENLİĞİNİN KURUMSAL VE KİŞİSEL OLARAK ÖNEMİ VE ÖRNEK OLAY DEĞERLENDİRMELERİ

Bilgi güvenliği farkındalığı oluşturulması kapsamında en önemli adımlardan biri de dünyada ve ülkedeki güncel gelişmelerin takip edilmesidir. Böylelikle kullanıcılar değişen ve gelişen teknolojik ortamda gerçekleşen saldırılar hakkında bilgi sahibi olarak, bu saldırılardan dersler çıkarmalı ve kendi bilgi sistemleri ya da cihazlarında saldırılara maruz kaldığında korunabilmeli ya da en az zararla kurtulabilmelidir. Bu kapsamda ulusal, kurumsal ve kişisel olarak farkındalık yaşam döngüsünün ihlal edilmesi sonucunda ortaya çıkan örnek saldırılar ve değerlendirmeler sunulmuştur.

A. Stuxnet

İran'ın Buşehr ve Natanz'da konuşlu nükleer tesislerinde gerçekleştirilen nükleer çalışmalarını sekteye uğratmak amacıyla ABD ve İsrail tarafından oluşturulduğu düşünülen, Haziran 2010'da tespit edilen solucan yazılımdır. Dış dünyaya kapalı sistemlerin ve endüstriyel kontrol sistemlerinin de tamamen güvende olmadığını, çeşitli saldırı yöntemleri kullanılarak bu sistemlerin de zarara uğratılabileceğini gösterdiğinden büyük yankı uyandırmıştır. Bu solucan İran'da 62.867 bilgisayara bulaşmış ve bunun için herhangi bir ağa gereksinim duymamıştır [39]. Bu örnekte ulusal düzeyde bir saldırı ile karşılaşılmıştır. Genel anlamda bilgi güvenliği farkındalık süreci doğrultusunda değerlendirildiğinde sistemin değerinin farkında olunduğu bu doğrultuda kapalı bir sistem kurularak bir çok saldırının doğrudan devre dışı bırakıldığı, tehditleri izleme ve anlama adımlarının gerçekleştirildiği görülmektedir. Bu saldırının usb bellek, cd, dvd veya başka harici cihazlarla yayıldığı düşünülmektedir. Kullanıcının harici cihazı sistemde kullanması, sistem yöneticilerinin harici cihazın kullanımına izin vermesi ve sistemin zararlı yazılımı tespit edecek güvenlik yazılımlarına sahip olmaması korunma yöntemlerinin uygulanması adımında yaşanan aksaklıklar olarak karşımıza çıkmaktadır. Solucanın sisteme dahil oluşuna ilişkin, bir çalışanın bedava aldığı veya yerde bulduğu bir usb belleği bilgisayarına takmasıyla başladığı düşünceleri bulunmaktadır. Bu örnek korunma yöntemleri öğrenmenin tek başına yeterli olmadığı, bilginin davranışa dönüştürülerek uygulanmadığı takdirde sistemin güvenliğini tehlikeye attığını göstermesi dolayısıyla son derece güzel bir örnektir.

B. Rusya Kaynaklı Sitenin Kamera Kayıtlarını İzinsiz Yayınlaması

Kasım 2014 tarihinde çıkan bir habere göre Rusya kaynaklı bir internet sitesi dünyanın 250 noktasında bulunan evlerdeki kameraların görüntülerini canlı yayınlamaktadır. Habere göre bu siteye girenler, sadece Türkiye'de ev, bebek odaları, hastane ve devlet daireleri de dahil çeşitli yerlere kurulan 170 kameranın canlı görüntülerini izleyebilmekte ve kamera sahiplerinin bu durumdan haberleri bulunmamaktadır [40]. Bu duruma sebep olarak insanların kamera ilk kurulduğunda otomatik belirlenen default şifreleri değiştirmedikleri dolayısıyla hakerların sistemlere kolayca erişebildiği tahmin edilmektedir. Şifrelerin ya boş bırakıldığı ya da "12345678", "0000000", "88888888" gibi şifreler olduğu görülmektedir. Yaşanan bu durum bilgi güvenliği farkındalık döngüsü kapsamında değerlendirildiğinde kullanıcıların tehditleri izleme ve anlama adımlarında eksiklik gösterdiği görülmektedir. Kişilerde evlerinde bulunan kamera sisteminin özel hayatlarına ilişkin bilgileri deşifre edebileceğine ve saldırganların öncelikle standart şifreleri deneyeceğine yönelik bilgi eksikliği olduğu görülmektedir. Bu ve benzeri bilgi güvenliği ihlalleri ile karşılaşmamak için default şifreler ürün/sistemler kullanılmaya başlamadan önce değiştirilmeli, hatırlanması kolay tahmin edilmesi zor parolalar tercih edilmelidir.

C. Cryptolocker Virüsü

2015 yılında da dünyada ve ülkemizde fidye yazılımları olarak da adlandırılan "cryptolocker" virüsü gündemdeki yerini korumuştur. Bu virüs TTNET tarafından gönderildiği izlenimi verilen bir e-posta ile kullanıcılara ulaştırılmaktadır. Fatura meblağının yüksek olması gibi insan zaafiyetlerinin de kullanıldığı e-postada ekli olan fatura dokümanı PDF dosyası

ikonuna sahip olmasına rağmen .exe uzantısına sahiptir. Faturayı görüntülemek amacıyla .exe uzantılı dosyanın çalıştırılmasıyla zararlı yazılım aktif hale gelmekte ve kullanıcının bilgisayarındaki tüm dokümanları şifreleyerek kullanılamaz hale getirmektedir. Şifrenin anahtarı karşılığında kullanıcıdan veya kurumdan hatırı sayılır miktarda para talep edilmektedir. Günümüzde internetin yaygınlaşması ile bir çok insan bu virüsten haberdar olmuştur. Ancak çok sayıda insan dokümanlarının şifrelenmesine engel olamamıştır. Bu örnekte bilgi güvenliği farkındalık döngüsünün tehditleri izleme ve anlama adımlarının gerçekleştirildiği, ancak korunma yöntemlerini öğrenme adımında eksiklik olduğu değerlendirilmektedir. Kullanıcının sahte e-postanın uzantısının kontrol edilerek tıklamaması yeterli olabilecekken cyrptolocker virüsü bilgi eksikliği dolayısıyla kişisel bilgisayarlarda çok etkili olmuştur [41]. Farkındalık dögüsünün etkin olarak kullanıldığı kurumsal bilgisayarlarda belirli uzantıdaki dosyaların erişime kapatılması nedeniyle korunma yöntemleri iyi uygulanmış ve güvenlik ihlallerinin yaşanılmasının önüne geçilmiştir.

Şekil 3: Cyrptolocker Virüsü için Kullanılan E-Posta Örneği [41]

Şekil 3'te gönderen adrese dikkatli bakıldığında e-postanın TTNET'ten gelmediği görülmektedir. Ayrıca ekteki dosyada .exe uzantılı dosya olması yine şüphe ile bakılması gereken bir durumdur. Fatura meblağının da normalden yüksek olması dikkati çekmesi gereken konulardan birisidir. Cyrptolocker virüsü kurumsal ve kişisel alanda etkili olmuş, ancak kurumsal anlamda başarılı olamamıştır.

Ç. Ankara'da Tapu Bigilerinin Sızdırılması

Ankara'da 1 milyon 568 bin kişinin tapu bilgileri çalınmıştır. Bir emlakçı tarafından bir vatandaşa ilişkin tüm bilgilerin söylenmesi üzerine ortaya çıkmıştır. Organize Suçlarla Mücadele polisi, vatandaşın tapu bilgilerini çalarak 500 TL karşılığında satan suçluları gözaltına almıştır. Bilginin içerden sızdırıldığı tahmin edilmektedir. Bu olayda milyonlarca insanın bilgilerinin sızdırılmasına sebep olan ana unsurun güvenlik eksiklikleri olduğu değerlendirilmektedir [42]. Bilgi güvenliği farkındalık döngüsünün tehditleri anlamak adımında yaşanan eksiklik dolayısıyla bu durumla karşılaşıldığı değerlendirilmektedir. Tapu bilgilerinin siber saldırı yaşam döngüsünün kazanç adımında etkin olarak kullanabileceği bir veri olması nedeniyle tehdit altında olduğu tam olarak tespit edilememiş dolayısıyla farkındalık döngüsünün takip eden adımları da uygulanmamıştır. Bu örnekte çözüm olarak işlenen bilgi önemine göre tasnif edilmeli ve her bir veri uygun seviyede güvenlik önlemleri ile korunmalıdır.

D. TEİAŞ Kurumuna Siber Saldırı

15 Kasım 2014 tarihinde Türkiye'nin kritik altyapılarından biri olan TEİAŞ kurumu siber saldırıya uğramış ve bu durum bir paylaşım sitesinde paylaşılarak kurumun prestiji sarsılmıştır. Bir müdür yardımcısının şifreleri çalınarak sisteme yönetici yetkisiyle girilmiştir. Bu saldırı çalışanların daima sosyal mühendislik saldırısına maruz kalabileceğini göstermiştir. Bu nedenle çalışanların özellikle kişisel bilgilerini paylaşmamaları, sosyal ağlarda kullandıkları şifreleri ve e-posta adreslerini iş yerinde kullanmamaları gerekmektedir. Ayrıca donanımsal olarak da bazı güvenlik zafiyetleri olduğu yapılan araştırma sonucu ortaya çıkmıştır [43]. Bu örnekte kişisel bilgi güvenliği farkındalık eksikliğinin kurumsal sonuçlar doğurduğu görülmektedir. Dolayısıyla kurumların bilgi güvenliğinden söz edebilmesi için çalışanlarının kişisel bilgi güvenliği farkındalık seviyesinin de yüksek olması gerekmektedir. Farkındalık döngüsü kapsamında değerlendirildiğinde kişisel ve kurumsal olarak sisteme uzaktan erişimin bir sorun sahası yaratabileceği ve yetkilendirme seviyelerinin iyi değerlendirilerek uygun önlemlerin alınmadığı, dolayısıyla tehditleri anlama adımında eksiklikler olduğu değerlendirilmektedir.

E. Apple ICloud Skandalı

2014 yılında bazı yabancı ünlülerin hesaplarının heklenmesi sonucu kişisel özel fotoğrafları basına sızdırılmıştır. Bu olayda Apple şirketine sınırsız sayıda parola deneme imkanı sunduğu ve fotoğrafların silinmesine rağmen hesaplarda tutulduğu gibi gerekçelerle dava açılmıştır. Fakat bu vakada diğer bir zafiyet yine kullanıcıların zayıf parola kullanması sonucu sözlük saldırı ile parolalarının kırılabilmesidir. Bir kez daha bilgi güvenliği farkındalık eksikliği sonucu kullanıcılar prestij ve manevi yönden ağır zarara uğraşmıştır [44]. Günümüzde en çok üzerinde durulan ve vurgulanan konuların başında parola güvenliği gelmektedir. Bu ve benzeri saldırılardan kişisel anlamda korunabilmek için parolaların belirlenmesi konusunda karakter sayısı, kombinasyon ve tüm hesaplar için farklı parolalar belirlenmesi hususlarına dikkat edilmeli, periyodik olarak parolalar değiştirilmelidir. Kurumsal bazda güvenliğin sağlanabilmesi için fazla sayıda parola girişi önlenmelidir. Kullanıcıların parola belirlemesi esnasında uyulacak politikalar belirlenerek kullanıcıların politikaya uygun parola belirlemesi zorunlu kılınmalıdır. Bu olay kurumsal ve kişisel bilgi güvenliği kavramlarının iç içe geçtiği bir örnek gibi görünse de farkındalık döngüsünde yer alan korunma yöntemlerinin uygulanması adımında firmanın etkin önlemleri alması durumunda kullanıcıların hata yapmasının da önüne geçebileceği ve bilgi güvenliği ihlallerinin gerçekleşmesini önleyebileceği değerlendirilmektedir.

F. HSBC Bankasına Siber Saldırı

13 Kasım 2014 tarihinde HSBC bankası 2.7 milyon kullanıcısının kullanıcısının kredi kartı ve banka kartı bilgilerinin çalındığını duyurmuştur. İlk kez bir banka siber saldırıya uğradığını kamuoyuyla paylaşmıştır. Bu olayın detayları hakkında fazla bilgi bulunmamasına rağmen, üçüncü parti yazılımların kullanımından kaynaklanan zafiyetlerin sebep olduğu konusunda teyit edilmemiş bilgiler bulunmaktadır. Bu yüzden eldeki zayıf bilgiler ışığında saldırının bireysel kullanıcı hatalarından çok kurumsal politikalardaki eksiklik veya hatalardan kaynaklandığı söylenebilir [45]. Dolayısıyla farkındalık döngüsünün

korunma yöntemlerinin uygulanması adımında eksiklikler olduğu görülmektedir.

Örnekler genel olarak değerlendirildiğinde bilgi güvenliğinin %100 sağlanmasının mümkün olmadığı bir gerçeklik olarak karşımıza çıkmaktadır. Bilgi güvenliği farkındalık döngüsünün içselleştirilmesi durumunda kişiler tehditleri izleme, anlama ve korunma yöntemlerini öğrenerek uygulama adımlarını gerçekleştirme konusunda daha başarılı olacaktır. Ancak gene de saldırılar gerçekleşecek ve kişiler zarar görebilecektir. Bahse konu adımların etkinlikle uygulanmasına rağmen ortaya çıkan siber saldırılarda zararın asgari düzeyde tutulabilmesi için kişiler döngünün bir sonraki adımı olan saldırıların etkilerini giderme yönünde harekete geçmelidir. Siber saldırıların bir yaşam döngüsü olduğu göz önüne alındığında değişim ve dönüşüm geçirerek tekrar karşımıza çıkacağı unutulmamalıdır. Bir sonraki saldırı öncesinde tehditler izlenerek proaktif önlemler alınmalıdır.

VII. SONUÇ VE GELECEK ÇALIŞMA

Kurumlar tarafından bilgi güvenliği farkındalığı ancak iyi hazırlanmış ve etkin kullanılan bir bilgi güvenliği yönetim sistemi kurulduktan sonra etkili olacaktır. Aksi takdirde bilgi güvenliğinin bir diğer sorun sahası olan sistemsel ve teknolojik eksiklikler sebebiyle saldırılar ve bilgi sızıntıları meydana gelecektir. Bilgi güvenliği yönetim sistemleri içeriğinde yer alan standart ve politikaların kurum dinamiklerini de göz önüne alacak şekilde oluşturulması ve yönetim kademesi tarafından uygulanması aşamasında destek görmesi büyük öneme sahiptir.

Teknolojik ve yönetsel açıklıkların giderilmesini takiben bilgi güvenliğinin yumuşak karnı olan insan faktörü üzerine yoğunlaşılmalıdır. Bu doğrultuda kullanıcı ve çalışanların etkin bilgi sistemi ve cihaz kullanımı sağlanarak bilgi güvenliği farkındalığını kaybetmeyecekleri şekilde eğitim ve bilgilendirme faaliyetlerine tabi tutulmaları gerekmektedir. Aksi takdirde yapılan yatırımlar küçük hatalar nedeniyle çok büyük maddi zarar ve itibar kaybına sebep olarak kaynakların etkin kullanımını engellemektedir. Buna rağmen verilen eğitimlerin ve sağlanan farkındalığın ortaya çıkan yeni gelişmeler ile tamamen geçersiz ya da yetersiz hale gelebileceği unutulmamalıdır.

Günümüzde farkındalık eğitimleri dönemsel olarak kullanıcıların bilgilerini tazelemektedir. Ancak saldırıların yaşadığı dönüşüm ve gelişim çoğu zaman iki eğitim arasındaki zamandan çok daha hızlıdır. Dolayısıyla kullanıcı bir önceki gün aldığı eğitime rağmen ertesi gün hiç duyulmamış bir saldırının kurbanı olabilir. İşte bu noktada çoğu zaman sosyal mühendislik saldırılarına hareket noktası oluşturduğu için sıklıkla eleştirilen sosyal medya ve mobil uygulamalar bir fırsata dönüştürülmelidir. Farkındalık kavramı kullanıcılara planlanan eğitimlerden ziyade günlük hayatta yaptıkları işlemlerin içerisine entegre olarak sunulmalıdır. Bu kapsamda ülkemizde de bir hareketlilik söz konusudur. Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalı Yüksek Lisans öğrencileri tarafından www.guvenlikicinbirdakika.org alan adı ile bir sosyal sorumluluk projesi başlatılmış ve sosyal medya üzerinden bir dakikalık spotlarla insanların bilgi güvenliği konuları ile etkileşim içerisinde tutulmasına yönelik yayınlar yapılmaktadır. Bu ve benzeri çalışmalar arttırıldığı taktirde kullanıcılar gündelik yaşamlarının içinde bilgiye, istediği zaman ve hızlı bir şekilde erişim sağlayabilecek ve farkındalık kavramı dinamiklik kazanacaktır.

Günümüzde bilgi güvenliği ihlallerinin büyük bir bölümü eğitimlerle, deneyimlerle kazanılan farkındalık seviyesine uygun olarak davranılmamasından kaynaklanmaktadır. Farkındalık sahibi olmanın ancak davranışlarda değişiklik yapıldığında güvenlik konusunda fayda sağlayacağı unutulmamalıdır. Bu da ancak siber saldırı yaşam döngüsü ve bilgi güvenliği farkındalık döngüsünün içselleştirilmesi ile sağlanabilecektir. Ancak bu sayede saldırganın davranışsal olarak nasıl bir yol izleyeceği tespit edilerek, bu yolda saldırganı engellemek için gerekli önlemler alınabilecektir.

Türkiye'nin 1994 yılında tanıştığı internet şuan bir çok kurumsal işlemlerin gerçekleştirildiği bir platforma dönüşmüştür. Bu nedenle kurumlar tarafından son 10 yıldır CIO (Chief Information Officer) adında pozisyonlar oluşturarak hem bilgi sistemlerini yapılandıran ve mevcut operasyonlara entegre eden ve hem de bilgi sistemleri ile ilgili güvenlik ve farkındalığı yöneten ve direk CEO ile çalışan pozisyonlar açılmıştır. Bilgi güvenliği ile ilgili olarak bahse konu yönetimsel düzenlemelerin dışında dünya genelinde iki yönlü bir çalışma hızla sürdürülmektedir. Bilgi güvenliği kavramına ilişkin kanuni düzenlemeler, standartlar ve iş birlikleri çalışmaların bir yönünü oluştururken diğer yandan da teknolojik olarak güvenliğin sağlanmasına yönelik çalışmalar sürdürülmektedir. Tüm bu çalışmalara rağmen bilgi güvenliğinde açıklıklar, saldırılar, istismarlar artarak sürmektedir. Bilgi güvenliği riskleri insan faktörü olayın içine dahil olduğu andan itibaren tekrar ortaya çıkmaktadır. Bunun en temel nedeni güvenlik tehditleri için birçok donanımsal ve yazılımsal yatırımlar yapılmakla birlikte zaman zaman insana yatırım yapılmasının unutulmasıdır. Eğitimler, yayınlar ve sosyal medya yolu ile insanlar bilinçlendirilmeli, bilgileri içselleştirilmeleri ve öğrendiklerini uygulamaları sağlanmalıdır.

Gelecek çalışma olarak, ortaya konulan bilgi güvenliği farkındalık döngüsünün sosyal mühendislik, sazan avlama, zararlı yazılımlar gibi bilgi güvenliği tehditlerinin gerçekleşme süreçlerine uygun olarak test edilmesi ve elde edilecek bulgular doğrultusunda modelin geliştirilerek, güncel hayatta kullanılan uygulama ve araçlarla bütünleştirilmesine yönelik çalışmalar yapılmasının faydalı olacağı değerlendirilmektedir.

KAYNAKÇA

[1] Dumont, D., "Cyber Security Concerns of Supervisory Control and Data Acquisition (SCADA) Systems", IEEE HST 2010 Conference.

[2] G Öztemiz, S., Yılmaz, B. (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası*, 14 (1) syf. 87-100.

[3] Canbek, G., Sağıroğlu, Ş. (2006). Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri. Türkiye: Grafiker. syf. 168-169

[4] ALTUNDAL, Ö., F., "DdoS nedir?Ne değildir?, http://www.siberguvenlik.org.tr/makaleler/ddos-nedir-ne-degildir, Ağustos 2012.

[5] S. R.Boss, L. J. Kirsch, "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness,"in Proceedings of the 28th International Conference onInformation Systems, Montreal, Aralık 9-12, 2007.

[6] M. T.Siponen, S. Pahnila, A. Mahmood, "Employees' Adherenceto Information Security Policies: An Empirical Study," in New Approaches for Security, Privacy and Trust In Complex Environments, H. Venter, M. Eloff, L. Labuschagne, J.Eloff, and R. vonSolms, Boston: Springer, syf. 133-144, 2007.

[7] K. D. Mitnick, W., L., Simon, "The Art of Deception: Controlling the Human Element of Security", Indianapolis, IN:Wiley Publishing, Inc., 2002.

[8] M. Warkentin, R. Willison, 2009, "Behavioral and Policy Issues in Information Systems Security: The Insider Threat, "European Journal of Information Systems (18:2), syf. 101-105

[9] T., K., Bensghir, (2008). Kurumsal bilgi güvenliği yönetim süreci. URL: www.erzincan.edu.tr/userfiles/file/stratejidb/guvenlik.ppt. Son Erişim Tarihi: 27.03.2015.

[10] H. Cavusoglu, Raghunathan, "Economics of IT Security Management: Four Improvements to Current Security Practices" Communications of the Association for Information Systems (14), syf. 65-75, 2004

[11] H. Cavusoglu, J., Son I., Benbasat, "Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers," working paper,Sauder School of Business, University of British Columbia, 2009.

[12] B., Bulgurcu, H., Cavusoglu, I., Benbasat, "Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness1", MIS Quarterly Vol. 34 No. 3 pp. 523-548 / Eylül 2010

[13] E. Şahinaslan, A. Kantürk, Ö. Şahinaslan, E. Borandağ, "Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri", Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri 11-13 Şubat 2009 Harran Üniversitesi, Şanlıurfa

[14] TS ISO/IEC 27001, 2006, Syf. 17

[15] Internet: http://www.yasad.org.tr/hakkinda/Sayfa/ulusal-bilgi-guvenligi-kanun-tasarisi, son erişim tarihi: 04.08.2015

[16] Öğütçü, G.,"E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi.", Yüksek Lisans Tezi, 2010.

[17] Ilkan, M., Iscioglu, E., Egelioglu, F., Doganalp, A., "Information Security Awareness of Academic Staff Members: An Example of Eastern Mediterranean University School of Computing and Technology", 4th Information Security and Cryptology Conference, 2010

[18] İnternet: United States Computer Emergency Readiness Team "Control Systems Security Program(CSSP)" http://www.us-cert.gov/control_systems/csthreats.html (2011).

[19] Yiğit, T., Akyıldız, M., A., "Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi",2014

[20] Al-Jarrah, O., Arafat, A., "Network Intrusıon Detectıon System using Attack Behavior Classification" , 2014, 5th International Conference on Information and Communication Systems (ICICS).

[21] Stoneburner, G., Goguen, A., Feringa, A., "Risk Management Guide for Information Technology Systems","Recommendations of the National Institute of Standards and Technology", Special Publication 800-30, July 2002.

[22] Özbilen, A., "TCP / IP Tabanlı Dağıtık Endüstriyel Denetim Sistemlerinde Güvenlik ve Çözüm Önerileri", Ankara(2012).

[23] Uma, M., Padmavathi, G., "A Survey on Various Cyber Attacks and Their Classification", International Journal of Network Security, Vol.15, No.5, syf. 390-396, Eylül 2013.

[24] Garuba, M., Liu, C., Fraites, D., "Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems", 5th International Conference on Information Technology: New Generations, 2008.

[25] Zargar, S.T., Joshi J., Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communıcatıons Surveys & Tutorıals*, Vol. 15, No. 4.

[26] Canbek, G., Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Gazi Üniversitesi Politeknik Dergisi*, 9.3.

[27] İnternet: Largest Ever DDoS Cyber Attack Hits US and European Victims, URL: http://www.ibtimes.co.uk/largest-ever-ddos-cyber-attack-hits-us-european-victims-1435973. Son Erişim Tarihi: 27.03.2015.

[28] Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J., K. (2014). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters 51*, p: 1–7.

[29] Halfond W., G., Viegas, J., Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. *Proceedings of the IEEE International Symposium on Secure Software Engineering, Arlington, VA, USA.*

[30] Demirez, K. (2011). *Linux Backtrack 5*, Türkiye: Nirvana Yayınları.

[31] Klein, A. (2002). Cross Site Scripting Explained. URL: https://crypto.stanford.edu/cs155/papers/CSS.pdf

[32] *Application Vulnerability Trends Report 2014*. URL: https://www.trustwave.com/Resources/Library/Documents/Cenzic-Application-Vulnerability-Trends-2014/

[33] Çifci, H. (2012). *Her Yönüyle Siber Savaş.* Tübitak Popüler Bilim Kitapları, Ankara.

[34] Bircan, C. (2014). Sosyal Mühendislik Saldırıları. https://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html, Son Erişim tarihi: 27.02.2015)

[35] K. D. Mitnick and W. L. Simon, The art of deception: Controlling the human element of security: Wiley, 2001

[36] TÜBİTAK BİLGEM. Tehditler ve Korunma Yöntemleri. http://www.bilgimikoruyorum.org.tr/?b325_sosyal_muhendislik_saldirilarindan_korunmak, Son Erişim Tarihi: 27.02.2015.

[37] C. Hadnagy, Social engineering: The art of human hacking: Wiley, 2010

[38] Allam, S., Flowerday, S., V., Flowerday, E. (2014). Smartphone information security awareness:A victim of operational pressures. *Compute r s & security42*, 56 -65.

[39] İnternet: "Stuxnet". URL: http://tr.wikipedia.org/wiki/Stuxnet, Son Erişim Tarihi: 11.04.2015.

[40] İnternet: http://www.hurriyet.com.tr/dunya/27620170.asp. Son Erişim Tarihi: 11.04.2015.

[41] İnternet: http://www.hwp.com.tr/2014/12/17/dikkat-cryptolocker-virusu-bu-sefer-de-turk-telekom-faturasi-ile-geliyor/. Son Erişim Tarihi: 12.04.2015.

[42] İnternet: http://www.hurriyet.com.tr/gundem/27662013.asp. Son Erişim Tarihi: 12.04.2015.

[43] İnternet: "Enerji Bakanlığı: Borçlar silinmedi." URL: http://www.hurriyet.com.tr/gundem/27580556.asp. Son Erişim Tarihi: 12.04.2015.

[44] İnternet: "Apple'dan ilk açıklama". URL: http://www.milliyet.com.tr/unlulerin-ciplak-fotograflarina/dunya/detay/1934735/default.htm. Son Erişim Tarihi: 18.04.2015.

[45] İnternet:" HSBC Türkiye'ye Siber Saldırı Şoku!" URL: http://www.milliyet.com.tr/hsbc-turkiye-ye-siber-saldiri-bilisim-1969049/ Son Erişim Tarihi: 27.03.2015.

Salih Erdem Erol Lisans eğitimini Hava Harp Okulu Bilgisayar Mühendisliği Bölümünde tamamlamıştır. Gazi Üniversitesi Bilgi Güvenliği Mühendisliğinde yüksek lisans eğitimine devam etmektedir.

Eyüp Burak Ceyhan Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde araştırma görevlisidir.

Şeref Sağıroğlu Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürü ve Bilgisayar Mühendisliği Bölüm Başkanıdır.