**T.C.**
**ADNAN MENDERES ÜNİVERSİTESİ**
**YÖNETİM BİLİŞİM SİSTEMLERİ LİSANS PROGRAMI**

# ÜNİVERSİTE ÖĞRENCİLERİNİN SİBER GÜVENLİK BİLGİLERİNİN ANKET YOLUYLA ANALİZ EDİLMESİ VE FARKINDALIK EĞİTİMİ HAZIRLANMASI

**ENES ÖZKAN**

**BİTİRME ÇALIŞMASI**

**DANIŞMAN**
**Dr. Öğr. Üyesi Asil ALKAYA**

**AYDIN–2022**

# İÇİNDEKİLER

# ÖZET

# ÜNİVERSİTE ÖĞRENCİLERİNİN SİBER GÜVENLİK BİLGİLERİNİN ANKET YOLUYLA ANALİZ EDİLMESİ VE FARKINDALIK EĞİTİMİ HAZIRLANMASI

**Özkan E. Adnan Menderes Üniversitesi Yönetim Bilişim Sistemleri Lisans Çalışması, Aydın, 2022.**

Üniversite öğrencileri, Jenerasyonları ve bulundukları konum sebebi ile Siber Güvenlik kavramında toplum bazında en çok bilgi sahibi olması gereken toplumdur. Sebeplerin en başında Toplu ortamlarda (Ağlarda) sürekli bulunmaları, Kullandıkları Cihazların genelde yeni teknoloji olması söylenebilir. Bu Çalışmada Onların Bilgi düzeylerinin analiz edilmesi ve gerekli konularda farkındalık eğitimi verilmesi amaçlanmıştır.

**Anahtar Kelimeler:** Siber Güvenlik, Üniversite, Ağ, Toplum, Teknoloji, İnternet.

## ABSTRACT

# ÜNİVERSİTE ÖĞRENCİLERİNİN SİBER GÜVENLİK BİLGİLERİNİN ANKET YOLUYLA ANALİZ EDİLMESİ VE FARKINDALIK EĞİTİMİ HAZIRLANMASI

Due to their generation and status, University Students are the society that should have the most information on the concept of Cyber Security on the basis of society. Because They Are Exact connected of Networks All the time and their Devices usually are New Technologies. In this study,It is aim at analyze their knowledge level via survey and According the Results educate them about Cyber Awareness.



**Keywords**: Cyber Security, University, Network, Society, Technology, Internet.

# 1. GİRİŞ

Siber Güvenlik Günümüz Çağının En Önemli konularından biridir Şüphesiz. Bunun Sebebinin temelinde ” Teknolojiyi İlerletmek ve Onu Korumak” felsefesi yatıyor. Mesela Akıllı Ocaklarımızın Biz uyurken Evi yakacak kadar Yüksek derecelerde Uzun Saatler Çalışmasını İstemeyiz. Daha Basit bir örnek vermek gerekirse Cep Telefonlarımızdaki Özel Bilgileri bir anda Halka açık ortamda görmek bizi pek memnun etmez. İşte tam bu yüzden Siber Güvenlik, Teknoloji var oldukça hep Çok önemli olmaya devam edecek.

Üniversitelere Temelde Gelişmiş Eğitim Kurumlarıda diyebiliriz. İçerisinde Kayıtlı Elli Bin den fazla Öğrenci ve Öğretim Görevlisi barındırırlar Bu Öğrencilerin ve Öğretmenlerin Kimlikteki Bilgilerinin Tamamı Üniversite Veritabanlarında Bulunur. Sadece bu bilgi bile Kötü Niyetli insanların Üniversite Ağlarına neden sızmak istediklerini açıklar. Bu Yüzden Üniversite Toplumları Siber Güvenlik Konusunda Ortalama Bilgi Düzeyinin Çok üzerinde bilgiye sahip olmalıdır. Örneğin Her Gördüğü Link’e Tıklamamalı veya Her Aplikasyon ve Uygulamaları Cihazlarına İndirip Çalıştırmamalılar.

## 1.1. İnternetin Ortaya Çıkışı ve Gelişimi

Bilgisayarın taşınabilir hale gelmesi ve internete erişimin yaygınlaşmasıyla birlikte 21. yüzyılda dünyaya bunların şekillendireceği belli olmuştu. Bireyler arasında coğrafi mesafeler azalır ve iletişim alışkanlıkları değişirken, yeni teknolojiler sağladıkları imkânların yanı sıra beklenmedik problemlere de sebep olabilmektedirler. İnternet bunun en güzel örneklerinden birisidir. İletişim, haberleşme ve paylaşma alanı olarak ortaya çıkan internet, aynı zamanda dünya üzerindeki mesafeleri kaldırarak aynı düşünceyi, hobiyi, inancı, merakı, ideali paylaşan insanları bir araya getirmiştir. Öte yandan internetin Çin’de yaşayan bir insanın Güney Afrika’daki insanların durumundan, ekonomik problemlerinden ve devlet ilişkilerinden haberdar olmasını sağlayarak dünya vatandaşlığı yönünde adım atılmasını sağladığını söylemek de abartı olmayacaktır. Üstelik bilgisayar teknolojisinin hızla gelişmesi internetin yayılmasını günden güne daha da arttırmaktadır. İnternetin temel unsurları bilgisayar,

kullanıcı ve ağdır. Bilgisayar teknolojisinin gelişmesi ve değişimi ağ teknolojisinin yeteneklerini de arttırmaktadır. Bilgisayar teknolojisinin ilk geliştiği yıllarda ana bilgisayara ancak tek bilgisayarın erişimi söz konusuydu. İki bilgisayarın aynı anda ana bilgisayara erişimi için gereken işlemci ve iletişim protokollerinin gelişmesiyle ağ kavramı ortaya çıktı. Zamanla dosya aktarım protokolü (File Transfer Protocol - FTP) ve aktarım denetim protokolünün (Transmission Control Protocol - TCP) gelişmesiyle birlikte çok sayıda kullanıcı, sunucu bilgisayara bağlanabilir hale geldi.

Günümüzde telsiz iletişim (wireless communication) teknolojisinin gelişmesi ve akıllı telefon ve tabletler ile geniş kullanım alanları bulması ağ teknolojisinin önemini daha da arttırmıştır. Benzer şekilde sistemin esnekliği de politik ortamın elverdiği ölçüde büyüdü ve gelişti. Soğuk Savaş yıllarında ABD ile müttefiki ülkeler arasında teknoloji ve bilgisayar kullanımı hızla artarken, AB'nin uyguladığı ithalat rejimi CoCoM (Coordinating Committee for Multilateral Export Controls) kuralları gereği Varşova Paktı ülkelerine nükleer silahların yönlendirilmesi ve hedef sistemleri için kullanılabileceği gerekçesiyle bilişim sistemlerinin satılmasını engelliyordu. Soğuk Savaşın bitmesiyle birlikte o döneme ait yasaklar da uygulamadan kalkınca, sivilleşen ve genel kullanıma açılan internetin kullanıcı sayısı bir anda arttı. 2011'te yapılan ölçümlerde 2.267.233.742 kişinin internete girdiği tespit edildi. Bu artışla birlikte dijital verilerin aktığı ve veri işleyen bütün cihazların bağlanabildiği bir sanal dünya oluştu. Foucault'un dediği gibi gücü oluşturabilecek bilgilerin aktığı bu alan kısa sürede güvenlik problemleriyle anılır hale geldi.

Siber uzayın oluşmasıyla ortaya çıkan güvenlik sorunlarının sadece bilgisayar mühendislerinin ya da ağ uzmanlarının çözebileceği teknik içerikli problemler olmadığı da kısa sürede anlaşıldı. Siber uzayın gelişmesiyle birlikte sosyal gerçekliğin en önemli iki katmanı olan mekân ve zaman bağıntısı değişmeye başladı. Fiziksel uzaklıklar ve bilgi aktarımı için gereken zaman internetin oluşturduğu hızla kısaldı. Bu yeti kısa sürede ekonomik, politik ve askeri alanlarda kullanılmaya başlandı. Bankalar, borsalar ve her türlü ticari yapı, yeni teknolojiyi kullanarak daha geniş alanda hizmet vermeye başladı. Devletler de küçük ölçekte altyapı hizmetlerinin dağıtımında, makro ölçekte ise dış misyonlarıyla iletişimden diplomasiye, istihbaratî bilgi toplamada savunma teknolojilerine kadar geniş bir çerçevede bilgi teknolojisi ve siber uzayın imkânlarından yararlanmaya başladılar. Bilişim teknolojisinin bu herkesi birbirine bağlayan ağ yapısı dikey kurumsal hiyerarşiyi de azalttı. Böylece yöneticilerin her düzeydeki personellerine erişebilmeleri kolaylaştı. Toplumsal

düzeyden bakıldığında artık insanların bilgi alışverişinde bulunmalarının ağla bağlanmış bilişim sistemleri sayesinde daha kolay olduğunu görüyoruz.

Toplumsal bağlılığı bu derece farklılaşmış toplulukları Sanayii Devrimi döneminde oluşmaya başlamış algılarla yönetmenin kolay olmayacağı aşikârdır. Uluslararası ilişkilerin temel aktörlerinden olan devletler de bu topluluğu daha kolay yönetebilmek için hızla bilişim teknolojilerini kullanmaya başladılar. Fakat devlet sisteminin yavaş hareket eden yapısını bu teknolojik değişime uygun olarak yeniden yapılandırmak beklenenden zor oldu. Teknoloji birçok sahada devlet yönetiminin vatandaşlarıyla etkileşimini etkinleştirdi, devletin bilgiye ulaşımını hızlandırdı ve vatandaşları eskisine göre daha rahat şekilde kontrol etmesini sağladı. Fakat hızla genişleyen bu alan sistemlerin işlemez hale gelmesinden kayıtların silinmesine kadar birçok riski de beraberinde getirdi.

Gelişmiş ülkelerde bütün sektörlerin hizmetlerini siber uzaya taşımasıyla birlikte kritik öneme sahip bilgiler telefon hatlarından, eşeksenel kablolarından, fiber optik kablolardan ve elektro-manyetik dalgalar üzerinden akmaya başladı. Kendine fayda sağlamak isteyen kişiler, gruplar ve organizasyonlar bu bilgilere erişerek ya da hizmeti durdurarak güçlerini arttırmak istediler. Yine de siber uzayda gerçekleşen güvenlik problemlerinde çoğunlukla internetin coğrafi mekândan nispeten bağımsız olma özelliği kullanılmaktadır. Bu yüzden siber güvenlik olayları sıklıkla ulus-devlet sınırlarının ötesine geçerek uluslararası işbirliğini zorunlu hale getirmektedir. Bir taraftan devletler ulusal ve uluslararası seviyede farklı tedbirler almanın güvenlikleri için gerekli olduğunu hissederken, diğer taraftan siber saldırıların savaşa dönüşebileceği endişesi ve çıkabilecek bir dünya savaşının siber uzayda yaşanması ihtimali uluslararası politikayı da şekillendirmektedir.Öte yandan ulusal güvenliklerini sağlamak için siber uzaydaki gelişmelere odaklanan birçok devletin çıkaracağı kanunlar ile belirleyecekleri politik tavırlar siber uzayın gelişiminin de yönünü belirleyecektir.

## 1.2. ARPANET ve İnternetin temeli

İnternet yakın zamanda dünyanın kullanımına açılmış ve hızlı yayılmış olsa bile temelleri Soğuk Savaş yıllarında atılmış bir ağ sistemidir. O tarihten bu yana işleyişten kullanım şekline kadar birçok konuda değişimler yaşandı. Bugün güvenlik rekabetinin parçası olarak gelişen siber uzay, devletlerin ve grupların güç yarışını sürdürdükleri bir alana dönüştü.

4 Ekim 1957'de SSCB'nin dünya yörüngesine ilk yapay uyduyu yerleştirmesi ve ardından 3 Kasım'da bu sefer canlı bir köpekle birlikte Sputnik II'yi uzaya göndermesi, o güne kadar iki kutuplu dünyada yaşanan rekabette lider konumda olduğunu düşünen ABD'nin ilk defa nükleer tehdidi hissetmesine sebep oldu. ABD Başkanı Eisenhower'ın Bilim Başdanışmanı James Killian'ın belirttiği gibi, Sputnik sonrasında "Amerikan bilimine, teknolojisine ve eğitimine itimadın aniden buharlaştığını" gören yönetim Şubat 1958'de ABD'nin rekabet gücünü geliştirmeye katkı yapması için İleri Araştırma Projeleri Ajansı'nı ( Advanced Research Projects Agency – ARPA) kurdu. Ajansın en önemli görevi Sovyetler Birliği'nin ispatlanmış teknolojik üstünlüğünü alt etmekti.

ABD'nin milli güvenliğini sağlamak için farklı branşlarda araştırmalar yapan bilim insanlarını şemsiyesi altına alan ARPA'daki projeler uzay araştırmalarının yanı sıra balistik füze savunması, dünya üzerinde nükleer test yapılan coğrafi noktaların saptanması gibi konuları da içeriyordu. ARPA'nın ilk bilgisayara yönelik çalışmaları ise teknolojinin gelişimiyle ilişkilidir. O dönemde bilgisayar işlemcilerinin çok sayıda kullanıcının bilgisayar sistemine girişini desteklememesi araştırmaların zaman almasına ve işlemlerin gereken hızda yürütülmesine engel oluyordu. Fakat işlemci teknolojisinin gelişmesiyle birlikte çoklu kullanıcının ana bilgisayara bağlanabilmesi konusu tartışılmaya başlandı. Böylece uzay çalışmalarına katkı yapabilecek bilim insanlarını tek bir ağda buluşturmanın teknik alt yapısı da hazırlandı. 1958'de kurulan NASA'nınihtiyaç duyduğu kritik araştırmacı kitlesini oluşturmak için 1962 'de oluşturulan İleri Araştırma Projeleri Ajansı Ağı (Advanced Research Projects Agency Network - ARPANET ) ABD'nin ihtiyaç duyduğu gelişme ortamını sağladı. Küba füze kriziyle birlikte bütün Kuzey Amerika'nın vurabilecek hale gelmesi ve SSCB'nin füze teknolojisini denizaltılara yerleştirecek kapasiteye ulaşmasıyla ABD güvenlik politikasında "Karşılıklı Kesin İmha" kavramı (Mutually Assured Destruction - MAD) yoğun şekilde gündeme geldi.

MAD'in yanısıra tartışılan diğer bir konuda nükleer bir saldırı sonrasında iletişim hatlarının çalışmasını sağlamaktı. ARPANET'in saldırılardan etkilenmemesi için neler yapılması gerektiği tartışmalarında Rand'dan Paul Baran "fiziksel saldırı sonrasında kalan en büyük grupla elektrik bağlantısı sağlayarak" iletişimi sürdürebilecek bir ağ yapısını tartışmaya açtı. Baran'ın önerdiği merkezi olmayan ve dağıtık çalışan ağlar kavramı üzerine yapılan tartışmalar sonrasında altyapı buna göre düzenlendi. 1970'lerde internetin temeli olan askeri nitelikli ARPANET, ABD'nin müttefiklerinde gelişmeye başlayan ağ sistemleriyle

(İngiltere'deki Ulusal Fizik Laboratuvarındaki (National Physical Laboratory) ticari ağ ve Fransa'daki araştırma ağı olan Cyclades) birleştirildi.

Böylece uluslararası bilgisayar ağlarının oluşumuyla internetin (International Network of Computer Networks - Bilgisayar Ağlarının Uluslararası ağı) nüvesi ortaya çıktı. Bilgisayar ağlarının hızla büyümesi yeni teknoloji merakını arttırırken, 1971'de ARPA'nin ileri teknolojiler sahasındaki ortaklarından birisi olan BBN Technologies'da çalışan Bob Thomas ilk kendini çoğaltan (self-replicating) programı yazdı. Creeper adını verdiği programı TENEX işletim sistemiyle çalışan DEC PDP-10 bilgisayarlarına yükledi.

Creeper kısa sürede ARPANET'te hızla yayılmaya başladı. Program bulaştığı bilgisayarlarda "I'm the creeper, catch me if you can!" mesajını ekrana yazıyordu. Problem anlaşıldıktan sonra Creeper'ı silmek üzere Reaper adında bir program yazıldı. Böylece ARPANET sisteminde ortaya çıkan ilk "solucan" (worm) siber güvenliğe yönelik oluşacak gelecek tehditlerin ilk işaretçisi oldu. ARPANET dâhil olmak üzere birçok sunucunun birbirine bağlandığı sistemde kullanıcı sayısı hızla artmaktaydı. Kullanıcıların sunucular üzerinden dosya değişimi için gerekli olan dosya aktarım protokolünün (File Transfer Protocol - FTP) geliştirilmesiyle birlikte gizli ya da anonim dosyalar üzerinde ortak çalışabilme imkânı da arttı. Fakat kullanıcıların bilgisayarlarının birbiriyle haberleşebilmesi için geliştirilen paket değişim protokolü (Packet Switching Protocol) az sayıda bilgisayarda problem oluşturmazken, kullanıcı sayısı arttıkça iletişim de aksıyordu. Bu sorun, düğümler arasında dosyaları aktarırken önce paketlere bölen ve adrese ulaştığında parçaları birleştirilerek yeniden oluşturan gönderim kontrol protokolü (Transmission Control Protocol-TCP) sayesinde aşıldı ve iletişim daha da hızlandı.

Kısa bir süre sonra İngiltere Kraliçesi II. Elizabeth 26 Mart 1976'da Kraliyet Sinyal ve Radar Kurumu'ndan ilk elektronik postayı atarak, iletişimi yeni bir seviyeye taşıdı. Fakat internetin haberleşme ve dosya paylaşımındaki ayrıcalığından hala sınırlı sayıda kişi faydalanabiliyordu. Bu durumu değiştirecek olan kişisel bilgisayarların ilk prototipinin 1970'te elektronik parçaları kendin yap projesi (DIY- Do it yourself) olarak piyasaya çıktığında beklenenden fazla ilgi gördü. 1975'de "kişisel bilgisayar" terimi ilk defa kullanıldığında Altair 8800 birçok evde yerini almıştı. Eylül 1975'de piyasaya çıkan IBM 5100'le birlikte kullanıcıların artmasıyla bilgisayar ve ağ kültürü daha da gelişti. Bilgisayar satışlarının artışını takiben bir bilgisayar firmasının tanıtacağı yeni ürün için davet mektubunu genel ağa göndermesiyle birlikte ilk spam mesajı da gönderilmiş oldu.

### 1.3. Soğuk Savaşın Sonu ve Siber Uzay

1980'lere geldiğimizde bilgisayarların artışıyla birlikte ağlara katılım da artmıştı. 27 Ekim 1980'de ARPANET, durum mesajlarına (status message) bulaşan virüs sebebiyle 72 saatliğine durdu.ARPANET ve ağların kullanıcı kitlesinin artması gerçek dünyayı dolaylı da olsa etkileyebilecek dijital bir alan oluşmasını sağlamış, alan genişlerken güvenlik teorisinin temellerinden birisi olan risk kavramı da İnternet bağlantılı olarak tartışılmaya başlamıştı. ARPANET eskiden kontrolün yüksek olduğu bir alan iken, büyüyüp genişledikçe, ağa yönelik tehditler ve riskler de artmaya başlamıştı.

Artık sistem kendi dinamikleri yanında kullanıcıların müdahalelerine de açık hale gelmişti. 1982'de bilim kurgu yazarı William Gibson, Burning Chrome başlıklı eserinde bu yeni gelişen siber alan için "siber uzay" kavramını kullandı. 1984'de yazdığı Neuromancer romanında kavramı daha da detaylandırarak, siber uzayı "milyarlarca meşru kullanıcı tarafından her gün tecrübe edilen uzlaşılmış bir halüsinasyon" ve "tasavvur edilemez karmaşa" şeklinde tanımladı. Gibson'un ifadeleri geleceğe ait önemli işaretler taşıyordu. 1982'de ABD Savunma Bakanlığı ARPANET'teki tehditlerin artması üzerine, ABD askeri verilerini taşıyacak ayrı bir ağ oluşturmaya karar verdi. Böylece Aralık 1982'de ARPANET ve MILNET olarak iki ayrı ağ ortaya çıktı. ARPANET sivil araştırmalar için kullanılmaya devam ederken, MILNET sadece askeri amaçla kullanılır hale geldi.

Böylece sivil siber uzayın temelleri atıldı. Siber uzayı ve dinamiklerini anlamak siber güvenlik konusundaki gelişmeleri daha net anlamamızı sağlayacaktır. Siber uzayı tanımlamak için yola çıkanlar için farklı teknolojik özelliklere odaklanmaktadır. Araştırmacılardan birçoğu sadece internet ortamına bu ismin verilmesinin uygun olduğunu düşünmektedir. Hâlbuki siber uzay bütün bilişim sistemlerini ve kullanıcıları içine alan bir evrendir. En genel anlamda, insanların birbirine bağlı bilişim sistemleriyle etkileştiği ve birbirine bağlı bilişim sistemlerinin birbirleri arasında ya da insanlarla iletişim içinde olduğu fiziksel olmayan alana siber uzay diyebiliriz. Bu alanı paylaşan aktörler ile ve unsurların çokluğu ve bütün katılımcıları tanımda belirtme endişesi bütün tanımları biraz eksik bırakmaktadır. Fakat siber uzayı oluşturan katmanları açıklamak tanımların eksikliğini tamamlayacak ve alanın özelliklerini net bir şekilde ortaya koyacaktır.

### 1.4. Fiziksel Katman

Reel ve fiziksel dünyadaki donanım ile insanlar ve varlıklar siber uzayın oluşmasını sağlamaktadır. Siber uzayın değeri fiziksel dünya ile ne kadar etkileştiğine bağlı olarak değişmektedir. Fiziksel katmanın ana unsurunu kullanılan teknoloji oluşturmaktadır. Bilgisayarın ana kartı (main board), işlemcisi (central processing unit), hafızası (random-access memory), diski (hard disk) ve diğer ekipmanlarından oluşan bir ünitenin yanı sıra, diğer ağlarla bağlantısını sağlayan bir ethernet kartı ve kablolara ihtiyaç duyulmaktadır. Bir ağın diğer ağlarla iletişimini sağlayan yönlendirici (router) ve diğer ekipmanlara da ihtiyaç vardır. Fiziksel alandaki bu ekipmanların varlığı olmaksızın siber uzayın varlığı şimdilik söz konusu değildir.

Siber uzay'ın fiziksel varlığının sadece bilgisayar ekipmanlarından oluştuğunu düşünmek de yeterli olmayacaktır. Ayrıca akıllı telefonlar, oyun konsolları, televizyon sistemleri, uydu alıcıları gibi ağ ortamında iletişim kuran bütün elektronik aletler de bu ortamdadır. Öte yandan ülkelerin temel altyapılarının işleyişi için gerekli olan kritik alt yapı ile ülkelerin birbirleriyle bağlantı içinde olmasını sağlayan internet omurgası (backbone) da bu iletişimin devamlılığı için esastır. Herhangi kopma ya da kesilme iletişimi kesintiye uğratır ve o ülkenin internete erişimini genel olarak ortadan kaldırır. Bu tür durumlarda siber uzaya erişim ancak yedek hatlarla ya da uydu üzerinden sağlanabilir. Ülkelerin internet çıkışlarının kontrol altına alınması çabasıyla ilgili olarak üç farklı örnek vermek mümkündür.

İlk örnek olarak, 2010'da ABD'de Senatör Joseph Lieberman ve Susan Collins tarafından hazırlanan ve Amerikan Başkanına herhangi bir tehlike anında interneti kapatma yetkisi tanıyan "Siber Uzayın Milli Değer Olarak Korunması Kanun Taslağı" verilebilir. Bu tehlike anları "Milli Siber Acil Durumları" (National Cyber Emergency) olarak tanımlanmıştı. Bu konu tartışılırken siber saldırılara kinetik saldırıyla cevap verilebileceği de gündemi gelmişti. Böyle bir bakış açısının yaratacağı problemleri tartışan OECD raporu siber güvenliğe askeri yaklaşımların hata olacağını belirterek, bölgesel internet kapatma sistemlerinin beklenmeyen sonuçlar doğurma ihtimali üzerinde durmuştur. İnternetin tehlike anında kapatılması fikrinin ABD'de tartışıldığı o günlerde Tunus'ta başlayan halk hareketi Mısır'a sıçramış, halk internet üzerinden sosyal medyayı kullanarak kitlesel organizasyonlar yapmaya başlamıştı. Dönemin Cumhurbaşkanı Hüsnü Mübarek halk hareketini önleyebilmek için Mısır'ın internete erişimini kesme yoluna gitti. 25 Ocak'ta twitter'ın sunucusuna erişimin engellenmesiyle başlayan hamle, 26 Ocak'ta Facebook'un ve 27 Ocak'ta da Blackberry servisinin

engellenmesiyle devam etti. Her ne kadar engellemeler twitter kullanımını azaltmayı başardıysa da Mısırlı twitter kullanıcıları yurtdışındaki arkadaşları vasıtasıyla mesajlarını dünyaya iletmeye devam ettiler. Yine 2010 Haziran'da VirusBlokAda isimli virüs temizleme programı üreticisi MS Windows işletim sistemlerini ve Siemens endüstriyel yazılımlarını etkileyen bir bilgisayar solucanının (Stuxnet) bulunduğunu açıkladılar. Kimin tarafından yazıldığı hala bilinmeyen solucanın hedefi Siemens Programlanabilir Mantıksal Denetleyicileriydi. Saldırı sonrasında yapılan değerlendirmelerde en çok zararı İran'daki nükleer tesislerin aldığı belirlendi. Birçok saldırı metodunun birleşimi ve açıklar kullanılarak hazırlanan bu solucan, İran nükleer tesislerinin üretim hedeflerini geciktirmişti. İran, nükleer tesislerine yapılan bu saldırı sonrasında kendine ait temiz bir intranet kurarak internet bağlantısını sınırlamayı planlamaya başladı. Görüldüğü gibi ülkelerin internet erişimini sağlayan altyapı zaman zaman politik kararlar tarafından şekillendirilebilmektedir. Tehdit ve güvenlik hissi ise internet kullanımını etkilemektedir.

### 1.5. Kodlar Katmanı ve Yazılım

Siber uzayın varlığını fiziksel alandan sanallığa yaklaştıran katmanlardan birisi de kodlar katmanıdır. Bütün fiziksel katman unsurları (anakartlar, işlemciler, RAM'ler, diskler) ancak kodlarla kullanılır hale gelmektedir. "Doğru – Yanlış" ya da "1 – 0" düzleminde oluşan programlama dilleri sayesinde işlemcinin nasıl çalışacağı belirlenmektedir. Bütün donanım ekipmanlarının bütünlük içinde yürütülerek, verilen komutlara cevap vermesini sağlayan temel platform olan işletim sistemleri bilgisayar donanımlarının gelişmesine bağlı olarak gelişmiştir. 1960'lı yıllarda bir oda büyüklüğünde olan bilgisayar donanımlarına ancak sınırlı sayıda erişim sağlanırken, 1980'li yıllarda taşınabilir bilgisayarlar kullanılmaya başlanmıştır. Günümüzde ise akıllı telefonların, televizyonların ve çeşitli multimedya platformlarının çalıştırılması için gelişmiş işletim sistemleri kullanılmaktadır. 1975'de kurulan Microsoft'un Windows işletim sistemi dünya üzerinde %50'nin üzerindeki pazar payıyla bilgisayarlarda en çok kullanılan işletim sistemidir. Bu rakamı Linux işletim sistemleri ve Unix tabanlı Mac OS X işletim sistemi takip etmektedir. İşletim sistemlerinin ardından internetteki içeriğe erişmemizi sağlayan kodlar gelmektedir. İnternetin temel taşını oluşturan web sayfaları da kodlar sayesinde hazırlanmaktadır. Günümüzde kullanıcılar daha fazla etkileşim kurabilmek için web içeriğinin programlanmasında Phyton, Ruby, Perl, PHP, ASP.NET, Java gibi diller kullanmaktadırlar. Kodlama içeriğinin yoğun olduğu bu tür platformlarda, internet üzerinden

başkaları tarafından yazılmış kodları kopyalayarak kullanan programcılar için sitelerinin kısa sürede bilgisayar korsanları tarafından ele geçirilme riski vardır. Ayrıca programlama dillerini yorumlayan platformların güncellenmemesiyle oluşan güvenlik zafiyetlerine de sıkça rastlanılmaktadır. Görüldüğü gibi birçok bileşenin kontrol edilmesiyle oluşan siber güvenlik, en başta insan unsuru olmak üzere en küçük hatalardan etkilenmektedir.

### 1.6. İçerik Katmanı

İçerik katmanı öncesinde belirtilen bütün katmanlar aslında bir çerçeve katman oluşturmaktadır.

Fiziksel ve kodlar katmanı olmadan içeriğin internet üzerinde sunulabilmesi mümkün değildir. Fakat içerik ve onun içerdiği mesaj olmadan da interneti oluşturan diğer katmanların anlamı zayıflayacaktır. İçerik katmanıyla internet paylaşılan, taraf olunan ve eleştirilen bir ortaklık oluşturmaktadır. İçerik katmanı sadece mesaj ileten bir medya olmanın ötesinde finansal işlemlere ait verilerin tutulduğu, ülkelerin stratejik bilgilerinin depolandığı, hastanelerdeki hastaların tıbbi bilgilerinin tutulduğu bir ortamdır. Fakat içeriklerin çeşitliliği ve benzerliği hiyerarşik bir düzenleme yapılması gerekliliğini değiştirmemektedir. Farklı kurumlarda yönetimler çalışanlarına özgürce kurumun ağına bağlanabilme izni verirken, yine aynı çalışanların ağdaki bütün verilere erişmelerine müsaade etmez. Bilgi güvenliğini sağlamak isteyen kurumlar kendi çalışanları için hiyerarşiler oluşturmak zorundadırlar.

Her kullanıcının ağ üzerindeki bütün belgelere istediği şekilde erişmesi kritik bilgileri tehdit eder. Veri hiyerarşisi mantığı günümüzde kullanılan birçok işletim sisteminde uygulanmaktadır. Böylece sistem ve güvenliği hakkında bilgi sahibi olmayan kullanıcıların sistemin tamamını tehlikeye atmasının önüne geçilmeye çalışılmaktadır. Öte yandan pratik, gündelik ve geçici sebeplerle veri erişimi hiyerarşisinin kaldırılmaya çalışıldığı ve bunun da bilgi güvenliği sorunlarına yol açtığı durumları sıkça görmek mümkündür. Örneğin bir bürokratın üst seviyede yöneticisinin istediği verileri temin etmek için kişisel bağlantılarla erişilmemesi gereken verileri paylaşıma açtırması yoluyla bilgi sızıntısı olabilmektedir. Kurumsal içerik katmanı ve sınırları dışında internet ortamında da kontrol dışı gelişen sınırlamalar olabilmektedir.

Örneğin internet üzerindeki içeriklere erişmek için web sayfalarının adresleri dışında arama motorları kullanılmaktadır. Bu da aslında araştırılan konunun anahtar kelimelerini bir arama

motoruna yazarak onun gösterdiği linklerin takip edilmesi anlamına gelir. Bu da internetin sınırının tercih edilen arama motorunun çerçevesi olduğunu göstermektedir. Günümüzde arama motorları sanıldığı kadar apolitik ve bağımsız hareket edememektedir. Örneğin Google sunucu çiftliklerinin yer aldığı ülke olan ABD, ülke güvenliği için koyduğu sınırları dikkate alarak belirli sitelerin isimlerinin arama sonuçlarından çıkarılmasını sağlamaktadır. Google'ın indekslediği web sayfa sayısının tüm internet göz önüne alındığında %0.004'den %12'ye kadar bir aralıkta olduğunu söyleyen farklı kaynaklar bulunmaktadır. Bu durumda internet içeriğine erişimin özgürce gerçekleştiğini söylemek mümkün değildir.

### 1.7. Gelişen Hacker Kültürü

ARPANET genişlemesi ve nükleer füzelerin bilgisayarla ateşlenmesi fikri, varolan politik gündemle ilişkilendirilmiştir. İki unsur arasındaki bağlantı, 1983'de vizyona giren, Lawrence Lasker ve Walter F. Parkes tarafından yazılan Savaş Oyunları (War Games) isimli filmde nükleer gerginlikte bilgisayarın nasıl rol aldığını göstererek ortaya koyulmuştu.

Filmde notlarını değiştirmek üzere okulun bilgisayarına girmek için uğraşan hacker David Lightman eriştiği bilgisayardaki oyunun daha önce oynadıklarından farklı olduğunu görür. Lightman'ın girdiği bilgisayar nükleer füzeleri kontrol etmek üzere geliştirilmiş bir sistemdir. Görevli kişilerin nükleer füzeleri ateşlerken anahtarı çevirmekte tereddüt etmeleri üzerine özel olarak hazırlanmış NORAD (North American Aerospace Defense Command - Kuzey Amerika Hava Sahası Savunma Komutanlığı) isimli bir bilgisayar bu misyonla görevlendirilmişti. Bilgisayar'ın içindeki WOPR (War Operation Plan Response) programı muhtemel SSCB nükleer saldırısını simüle etmekteydi ve simülasyon programı nükleer saldırı senaryosuna cevap verecek şekilde kurgulanmıştı. Filmde Lightman'ın bilgisayara izinsiz olarak erişirken başlattığı programın ve simülasyon modülünün gerçek hayatta etkili olduğunu fark etmesi üzerine olaylar gelişmeye başlar.

Çok sayıda insan tarafından izlenen bu film sayesinde siber uzay ve güvenliği kavramları yaygınlaşmıştır. Filmde sıkça kullanılan hacker kavramı da toplumda popülerlik kazanmıştır. War Games filmi ABD'de hacker kültürünün yaygınlaşmasına da sebep oldu. Milwaukee, Wisconsin'in telefon kodunu (414s) kendilerine isim olarak seçen 16-22 yaşları arasındaki altı gençten oluşan bir hacker grubu aniden şöhret oldu. 414s ismiyle bilinen bu grup, nükleer çalışmalarıyla ünlü New Mexico'daki Los Alamos Ulusal Laboratuvarına, 10.000 hastanın tedavi edildiği New York'taki Memorial Sloan-Kettering Kanser Merkezine, Los Angeles'ta

bir bankaya ve Milwaukee bölgesindeki birçok okulun bilgisayarına izinsiz olarak erişmeyi başardı. Federal İnceleme Bürosu'nun (FBI) üç yıllık takibiyle 1984'te yakalanarak mahkûm edilen grubun saldırılarının en önemli sonucu ABD'nin bilgisayar korsanlığı hakkında yasal düzenleme yapmaya yönelmesidir. Özellikle 1984'deki Computer Fraud and Abuse Act 18 USC 1030 (Bilgisayar Sahtekârlığı ve Suiistimali Yasası) bu konuda atılan en önemli adımlardan birisidir.

Yasada özellikle adaletin yönetimi, ulusal savunma ya da ulusal güvenlik için kullanılan Birleşik Devletler hükümetine ait bilgisayarların güvenliği konusunun altı çizilmişti. Saldırıların ortaya koyduğu diğer bir nokta da hangi eylemlerin bilgisayar korsanlığı sayılacağı, hangilerinin sayılamayacağının netleştirilmiş olmasıdır. 1980'li yıllardan itibaren ABD'de ortaya çıkan hacker kültürü kısa sürede dünyaya yayılarak, tecrübelerin paylaşıldığı güçlü bir ağ haline gelmiştir. Bir tanıma göre hacker "aklını zorlamak (sınamak) için bilgisayarlarla uğraşan kişidir." Diğer bir tanım da hackerların, "sistemlerin detaylarını öğrenmekten hoşlanan ve bir sistemde çalışmak için gereken asgari bilgiyi edinenlerin tersine sistemle yapabileceklerini öğrenerek onun kapasitesini zorlamayı sevenler" olduğunu vurgulamaktadır. 1950'lerde gelişmeyen başlayan Hippi hareketi ile açık kaynaklı programlar arasında önemli bir bağlantı vardır. Hippilerin yerleşmiş değerlere ve kontrole karşı duruşu bilgisayar temelli teknolojinin felsefesini de inşa etmiştir. Massachusetts Institute of Technology laboratuvarlarında gelişen felsefede programcılar ya da Steven Levy'in ifadesiyle hacker programlar geliştirip bunların kodlarını arkadaşlarının kullanımı için paylaşırlardı. İhtiyaç duyan programcılar da yazılan kodları geliştirip kendi ihtiyaçlarına göre düzenledi.

Tamamen kişisel tercihlerle ve özgürce paylaşımlar yapılırdı. Burada paylaşımın arkasındaki açık kaynak felsefesi öne çıkmaktaydı. Hippilerin de benzer felsefeye sahip olmaları bu hareketin hackerlar tarafından desteklenmesini sağladı Teknolojiye ve onun sağladığı bilgi kaynaklarına herkes tarafından erişimin sağlanması için ortak hareket etmenin ilk örneklerinden birisi California Berkeley'deki Leopold Plak şirketine halkın genel kullanımı için konulan bilgisayardı. Böylece üniversitelerin dışına doğru dürüst çıkmamış kaynaklar halkın kullanımına sunulmuştur. Bu dönemde şekillenen hacker felsefesinin altı temel şartı oluşmuştur:

1) Bilgisayarlara ya da dünyanın nasıl işlediğini öğrenmemize yardım edecek her şey kontrolsüz paylaşılmalı ve problemin üzerinde çalışılabilmesi için hep erişilebilir olmalıdır: Hackerlar kendi alanlarını sadece bilgisayarlar ve siber dünya ile sınırlı görmeyip, dünya

algılarını değiştirebilecek bütün kaynakların sınırsızca paylaşılması gerektiğini belirtmektedirler. Bu konuda sınırlama getirmeye çalışan bütün güçlerin ortadan kaldırılacağı da ima edilmektedir. Hackerlara göre bir konunun anlaşılabilmesi için bütünün onu oluşturan küçük parçalara ayrılması gereklidir. Bu bir programın hatalarının giderilmesi (debugging) ya da bir donanımın içinin incelemesi olarak da anlaşılabilir. Günümüzde sıkça kullanılan tersine tasarım (reverse engineering) yöntemi de bir mekanizmanın nasıl çalıştığını anlamak için çokça tercih ettikleri yollardan biridir.

2) Üretilmiş bilginin ulaşılabilir olmasının yaratıcılığı arttırdığını düşünen hackerler bütün bilgilerin ücretsiz olmasını savunurlar. Daha önceden yazılmış bir programın tekrar kodlanmasını emek israfı olarak görürler. Bir programın herkese açık olması halinde, başka programcılar tarafından ihtiyaçlarına göre daha kullanışlı hale getirebilecektir. Böylece herkesin kendi programı olması yerine, herkesin kullanabileceği en iyi programa ulaşılabilecektir. Hackerlara göre bilgi akışına izin veren her sistem bundan faydalanır. Bilgilerin özgür (free) olması bugün açık kaynak kodlu programların oluşmasını sağlayan temel anlayıştır. Hackerlar bilgi paylaşımını sağlamak amacıyla teknolojik gelişmeleri sürekli olarak takip ederek, bu teorik bilgilerini capture the flag (bayrağı ele geçir) yarışmalarıyla pratiğe dökerler. Bu yarışmalar sırasında özel olarak dizayn edilmiş ekipmanlarla, belirlenmiş zaman diliminde hackerlar ele geçirmeleri gereken hedefe ulaşmaya çalışırlar. Bazı düzenlemelerde katılımcıların sosyal becerilerini kullanarak istenilen bilgilere ulaşıp ulaşamayacakları da sınanır.

3) Otorite'ye güvenmemek ve adem-i merkeziyeti teşvik etmek: "Serbest bilgi değişimini teşvik etmek için hackerlarla bilgi arasında ya da donanım arasında, sınırların ve engellerin olmadığı açık sisteme sahip olunmalıdır." Hackerlara göre merkezi otorite kendini bürokrasi olarak ortaya koyar. Bu yüzden bürokrasinin hâkim olduğu şirketler ve üniversitelerin dürtülerini öldürdüğünü düşünürler. Bürokrasiye karşı tutumları günümüzde devlet kurumlarına ve onun sistemlerine yapılan saldırıların sebebini net olarak açıklamaktadır.

4) Hackerlar yaptıkları eylemlere göre değerlendirilmelidir; diploma, yaş, ırk ve ünvan gibi kriterlere göre değil: Hackerlar için iyi eğitimin sınıfta alınması gerekmez. Günümüzde internetin geniş kitlelere yayılmış olması bir çok insanın hacker olmak için gereken nitelikli bilgiye kolayca ulaşmasını sağlamaktadır. Örgün eğitim içinde olan ya da olmayan, bilgisayar konusunda sistemli eğitim alan ya da almayan herkes hacker olma şansına sahiptir. Siber güvenliğin bu önemli aktörlerinin dünyasında kişilerin başarısı yaptıkları eylemlerle ölçülür.

Siber uzayda takma isim kullandıkları için gündelik yaşamlarında hangi yaş, eğitim, ırk ve dil grubuna ait olduklarını tahmin etmek kolay değildir.

5) Bilgisayarda sanat ve güzellikler yapabileceğine inanan Hackerlar ellerindeki aracı daha iyi ve kullanışlı hale getirme felsefesine kendilerini adamıştır. Steven Raymond hackerların en azından Python, C/C++, Java, Perl ve LISP gibi programlama dillerini bilmeleri gerektiğini belirtilmektedir. Onlara göre programlarken kullandıkları betiğin sadeliği ve kısalığı bir tür bilgisayar ortamında icra edilmiş sanattır. Yazılımın kodları hackerın düşünce yapısının göstergesidir. Zira yalın yazılmış kodlar sayesinde bilgisayar işlemcileri (CPU) daha az çalışmakta böylece az enerji ile çok iş yapılabilmektedir.

6) Bilgisayarlar hayatınızı daha da güzelleştirebilir. Bilgisayarlar sadece hackerlara değil, diğer insanlara da büyük imkânlar sunmaktadır. Günümüzde kolaylıkla elde edilen birçok donanım ve yazılım hackerların katkıda bulunduğu süreçle geliştirilmiştir. Örneğin hackerlar açık kaynak kodlu yazılımları desteklemekte ve bunların kullanılmasını teşvik etmektedirler. Unix benzeri özgür bir program projesinin kurucusu Richard Stallman'dan Linux'un ilk çekirdeğini (kernel) yazan Linus Torvalds'a kadar, bir çok hacker bunu gerçekleştirmeye çalışmıştır. 1975'te yazılmaya başlayan hacker manifestosu zamanla değişerek gelişmiştir. 2004'te yayınlanan yeni bir manifesto eğitimden bilgiye, sınıf olgusundan üretime kadar birçok konuda hackerların algılarını aktarmıştır. Yeni manifestodaki şu ifade konuyu net bir şekilde ifade etmektedir: "bir hack sanal'a dokunur ve gerçeği değiştirir.

Özünde bir hareketin hack sayılabilmesi için yenilik, stil ve teknik uzmanlıkla dolu olması beklenir." Bu sadece bilgisayarla ilgili değildir. Eric S. Raymond'un ifadesiyle, " Yazılımdan başka şeylere (elektronik ve müzik) de hacker davranışını uygulayan insanlar var. Aslında herhangi bir bilim dalının veya sanatın en yüksek seviyelerinde onu bulabilirsiniz."

Günümüzde hacker felsefesinden farklılaşan motivasyonlarla bilgisayar veya ağ sistemlerine zarar veren kişiler için farklı terimler kullanılmaya başlanmıştır. Hackerlar yeni yollar ve yöntemler ortaya koymakla tanınırlar. Bu anlamda hackerlardan ilk ayrışanlar Cracker'lardır. Bu bilgisayarların güvenlik kontrollerini kendine menfaat sağlamak amacıyla ve suç motivasyonuyla aşan kişi ya da kişilere verilen isimdir.

Ne var ki, hackerlar ile crackerlar arasındaki netliğin zaman zaman kaybolduğu da ortadadır. Türkçe'de bu iki kavramı karşılayabilecek ve ayırabilecek kabul görmüş karşılıklar yoktur. Hacker kavramı için "üstad" kelimesini kullanan çevirileri görmek mümkün iken, cracker için

"bilgisayar korsanı" tabiri kullanılmaktadır. Öte yandan hem hackerlar hem de crackerlar odak hedefli çalışırlar. Hedefin niteliği ve ne derece meydan okuyucu olduğu bu iki grubu teşvik eden en önemli unsurdur. Hackerlar iş gereği ya da kendilerine buyrulan bir hedefe ulaşmayı genelde sıkıcı bulurlar. Eğer gerekli motivasyon sağlanırsa zaman sınırlaması onlar için anlamsız hale gelir. Bu davranış biçimleri onları siber güvenlik için çalışanlara göre daha avantajlı hale getirmektedir. Siber güvenliğin önemli aktörleri haline gelen hackerlar/crackerlar devletlerin de ilgisini çekmiştir.

Siber casusluktan istihbarata, güvenlikten siber suçlara kadar birçok alanda yönetime destek verebileceklerini düşündükleri bu kişilerle birlikte çalışma anlayışı pek çok devlette ortaya çıkmıştır. Fakat hem hacker/cracker felsefesinin devlet bürokrasisi içinde çalışmayı kabul etmemesi, hem de ekonomik imkanların özel şirketler kadar geniş olmaması bu işbirliği arayışlarını sınırlamaktadır. Bu nedenle devletler siber güvenliklerini sağlayabilmek için daha çok farklı donanım ve yazılım önlemleri almaktadır. Çalışanlarına sürekli eğitim vermekte ve sık sık tatbikatlar yapmaktadır. Bunların yanısıra özel firmalardan aldıkları desteklerle kendi sistemlerine yaptırdıkları penetrasyon testleriyle muhtemel zayıflıklarını bularak kapattıkları da bilinmektedir.

### 1.8. Siber Saldırının Yeni Boyutları

Siber güvenlik dünyasındaki tehditlerin çoğunluğu birden fazla değişkenle ortaya çıkar. Tehdidin çok boyutluluğu savunma için de benzer bir yaklaşımı zorunlu kılmaktadır. Her ne kadar hamleler gizlilik gerektirse de, gelişmiş ağ güvenlik çözümleri ortaklıkların kurulmasına ihtiyaç duymaktadır. Özellikle servis dışı bırakma (DOS- Denial of Service) yaygın olarak yapılan saldırılardan birisidir. Herhangi bir grup saldırganın farklı yerlerden yapılan saldırı türüne dağıtık servis dışı bırakma (DDOS - Distributed Denial of Service) ismi verilmektedir. Servis dışı bırakma saldırısı adından da anlaşılacağı gibi hizmet veren sunucu bilgisayarın verdiği servisi yerine getiremez hale gelmesidir. Bazı durumlarda hizmet durmaz ama o kadar yavaşlar ki, sunulan hizmetin niteliği açısından anlamsız hale gelir. Servis dışı bırakma saldırısında sunucu bilgisayarın ağ kaynakları tüketilmeye çalışılır. Bu saldırılar sırasında sunucu bilgisayarın bellek ve işlemci gücü de önemli rol oynar. DOS saldırıların farklı çeşitleri vardır. Dağıtık olsun ya da olmasın saldırılarda değiştirilmiş (spoof) IP numaralarıyla saldırıların yapılması mümkündür. Günümüzde

bireysel saldırıların yanı sıra grup halinde saldırılar da sıkça görülmektedir. Grup halinde saldırılar farklı yöntemlerle yapılabilir. Gönüllü grupların katılımıyla büyük katılımcıları organize eden Anonymous saldırıları bu türe örnek olabilir.

Ayrıca bu tür saldırıları gerçekleştirmek için kullanılan botnet'ler de siber dünyanın önemli tehditlerinden birisidir. Botnetler organize edilmiş saldırıya ya da verilen emiri yerine getirmeye planlanmış sistemlerdir. Botnet'ler "bot master" adı verilen kişiler tarafından kurulurlar. Bot masterlar yazdıkları program ya da web sayfaları aracılığıyla zararlı yazılımlarını farklı bilgisayarlara yayarlar. Bu yazılımları kullanmaya başlayan bilgisayarlar farkında olmadan botnet içine dâhil olurlar.

Bot master'ın emirini bekleyen bu bilgisayarlara "zombi" ismi verilir. Botnetler genişliklerine göre farklı sunucu alternatifleriyle yönetilirler. Botnetler bilgi çalmaktan spame, siber şantajdan kanundışı eylemler için dosya aktarımına ve reklam servislerinden gelir elde etmeye kadar farklı alanlarda kullanılabilir. Yetenekleri ve sınırları bu kadar geniş olan bu siber ordu organize suç örgütleri tarafından da sıkça kullanılmaktadır.

Takip edilmesi ve bulunması zor olan bu sistemde, genelde yakalananların masum zombi bilgisayar sahipleri olması hukuk sistemlerini ve polis örgütlerini zora sokmaktadır. Son zamanlarda botnetlerin hızlıca pazarlanan bir meta halini geldiğini ve botnet sahiplerinin ellerindeki gücü isteyenlere belirli bir ücret karşılığında kiraladıklarını görüyoruz. Bu da güvenlik güçlerinin işlerini daha da zorlaştırıyor. Gürcistan saldırısından bu yana siber güvenlik sahasında ortaya çıkan en büyük gelişme Stuxnet'tir. Haziran 2010'da ortaya çıkan bu bilgisayar solucanı hem yayılma tarzı, hem de politik olarak kullanılış şekliyle dikkati çekmiştir. Stuxnet'in en önemli özelliği spesifik olarak bir anakartı (PLC) hedef alacak şekilde programlanmış olmasıdır. Microsoft Windows işletim sistemleri aracılığıyla yayılan bu solucan, Siemens'in S7 300 modüllerini hedef almaktaydı. Hackerlar tarafından spesifik olarak bir endüstriyel PLC'ye (Programlanabilir Kontrol Cihazı) ve SCADA'ya (Supervisory Control and Data Acquisition - İzleme, Kontrol ve Veri Toplama Sistemi) yönelik saldırı çok sık görülen bir uygulama değildir. Stuxnet'in Microsoft Windows sistemlerindeki ilk gün açığını (Zero Day Exploit) kullandığı, saldırı sonrasında yapılan çalışmalarla ortaya çıktı.

İlk gün açığı yazılımların piyasa çıkarılması sonrasında belirlenen zayıf noktalardır. Bu tip açıklardan genelde iki şekilde haberdar olunur; ya firmalar açığı ilan ederler ya da firmanın bile haberi yokken hackerlar tarafından bulunarak internette çeşitli forumlarda açıklanması sayesinde yayılır. İnternet üzerinde bu açıkları pazarlayan hackerlar olduğu gibi, yazılım üreticisi firmalar da açıkları bulan kişilere belirli miktarlarda ödemeler yaparak, açıklar bir soruna dönüşmeden bilgi sahibi olmaya ve sorunu gidermeye çalışırlar. Stuxnet saldırısında dikkat çeken bir husus, Siemens PLC'lere ulaşmak için MS Windows sistemlerin açığını kullanan solucanın hedefine ulaşıncaya kadar eriştiği hiç bir bilgisayara zarar vermemiş olmasıdır. Esasında zarar vermemesi solucanın ömrünü ve hedefe ulaşabilme yüzdesini de yükseltmiştir. Stuxnet'in görevini yerine getirebilmek için çalıntı dijital imzaları kullanması da bundan önceki örneklerde görülmemiş bir uygulamaydı. Solucan Siemens karta ulaştığında bağlı bulunduğu motorun çalışma hızını farklı aralıklarla değiştirecek şekilde makinaya müdahale etmiştir. Saldırılardan zarar gören ülkeler arasında İran (%58.85) ve Endonezya (%18.22) ilk sıraları alırken, Hindistan, Azerbaycan, Amerika Birleşik Devletleri, Pakistan da listede yer almıştır. Solucanın yazılışı ve gerektirdiği teknik birikim açısından sınırlı sayıda programcının yazabileceği belirtilen saldırıyı kimin yaptığı konusunda bir çok spekülasyon yapıldı.

Saldırılan ülkenin İran olması ve nükleer zenginleştirme faaliyetlerini geciktirmesi hasebiyle Stuxnet'i kimin yazdığı yönünde tahminlerde bulunmak mümkün olabilir.85 Fakat bunu kesin kanıtlarla ortaya koymak sanıldığı kadar kolay değildir Stuxnet'in bulunmasından kısa bir süre sonra 1 Eylül 2011'te Duqu isimli Trojan Budapeşte Teknoloji ve Ekonomi Üniversitesi tarafından kamuoyuna duyuruldu. Duqu'nun bir çok özelliğinin Stuxnetle aynı olması, Stuxnet'in kernel'ine ulaşabilen kişi(ler) tarafından yazıldığının iddia edilmesine sebep oldu. Temelde benzerliklerin fazla olması bu kanaati oluşturmuştu.

Fakat Duqu'nun temel görevi endüstriyel kontrol sistemleri hakkında istihbarat toplamaktı. Bunu gerçekleştirebilmek için şifreleri kopyalıyor, belirli işlemlerin nasıl yapıldığını anlamak için ekran görüntüsü alıyor, bir çok dokümanı çalıyordu Duqu'nun siber casusluk olarak kullanımı ile ilgili tartışmalar sürerken, İran Ulusal Bilgisayar Acil Müdahale Ekibi (CERT-Computer Emergency Response Team) Maher tarafından 28 Mayıs 2012'te bir Flame Malware (kötücül yazılım) bulunduğu açıklandı. Alışılmışın tersine bu yazılım 20 megabit ağırlıktaydı ve sadece istihbarat toplamak üzere olduğu her

haliyle belliydi. Yerel ağlarla ve USB bağlantısıyla yayılabilen solucanın 1000 kadar bilgisayara bulaştığı tahmin ediliyordu. Bu kötücül yazılım (malware) yerleştiği bilgisayardaki her türlü sesi, ekran görüntüsünü ve klavyede yazılan her şeyi kayıt edebilmesinin yanı sıra, ağ trafiğini takip ettiği ve Skype konuşmalarını da kaydettiği belirtildi. Girdiği bilgisayarda bluetooth'u etkin hale getirebilen solucan, çevredeki bluetooth'u açık cihazların listesini oluşturmaktaydı. Özellikle AutoCAD çizimleri, PDF ve metin formatındaki dosyaları topladığı, hatta Arapça ve İbranice metinleri analiz edebildiği ve bu dökümanlara ait yer etiketi (geotagging) var ise bunları da topladığı iddia edilmiştir. i 2012'de Flame'in benzer özelliklerini taşıyan bir başka kötücül yazılım daha bulundu.

Gauss adı verilen yazılım özellikle Lübnan'daki bankaların sunucularında ortaya çıktı. Bu yazılım da, Flame'e benzer şekilde farklı internet programlarında kullanıcı adlarını ve şifreleri çalabilmekteydi. Ayrıca ağ bağlantı bilgilerini, işlemlerini, dosya dizinlerini toplamaktaydı. Yerleştiği bilgisayarın BIOS, CMOS ve RAM bilgilerini kaydetmekteydi. Bulaştığı bilgisayarlara takılan USB'lere yerleşerek başka bilgisayarları etkileme kapasitesine de sahipti. Bütün sahip olduğu bilgileri komuta kontrol sunucusunda görebilmekte ve ilave modülleri indirerek kapasitesini arttırabilmekteydi.

### 1.9. Türkiye'de Siber Güvenlik

NATO'nun bütün üyelerinin siber kabiliyetlerini arttırma ve ortak bir düzlemde çalışabilir hale getirme çabaları, Türkiye'nin siber güvenlik konusundaki çalışmalara hız verdi. Türkiye'de yetkililer uzunca bir süre siber tehditleri sadece siber suç seviyesinde değerlendirdi. Hatta önemli güvenlik kurumlarına yapılan saldırılar terörle mücadele çerçevesinde ele alındı. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (Tübitak) bünyesinde kurulan birimler ve ulusal bilgi güvenliği kapısıyla devlet kurumlarındaki siber güvenlik bilinci arttırılmaya çalışıldı. 27 Ekim 2010'da toplanan Milli Güvenlik Kurulu'nda siber tehditler tartışılarak, Milli Güvenlik Siyaset Belgesi'ne girmesine karar verildiği ilan edildi. 25-28 Ocak 2011'de Tübitak ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) ortaklığıyla I. Ulusal Siber Güvenlik Tatbikatı icra edildi. Tatbikat sonrası yayınlanan rapordaki bulgular Türkiye'nin siber saldırılara açık olduğunu ve konunun kamu kuruluşlarında yeterince ciddiye alınmadığını ortaya çıkardı.

2011'de Emniyet Genel Müdürlüğü'nde Bakanlar Kurulu kararıyla Bilişim Suçlarıyla Mücadele Daire Başkanlığı kuruldu. Bu dönemde mahkeme kararlarıyla Youtube ve Blogspot gibi sayfalara erişimin yasaklanmasını protesto etmek için Anonymous grubunun İçişleri Bakanlığı'ndan Büyük Millet Meclisi'ne kadar 20 farklı kuruma saldırması tehditin ne derece büyüdüğünün yakından farkedilmesini sağladı.

Öte yandan Redhack isimli grubun 2012'de Ankara Emniyet Müdürlüğü, İçişleri Bakanlığı, Dışişleri Bakanlığı ve Kara Kuvvetleri Komutanlığı da dahil olmak üzere birçok kamu kuruluşuna yaptığı saldırılar ve bu saldırıların medyada yer bulması, Türkiye'de siber tehdit algısının oluşmasını hızlandı. Bunun üzerine 20 Ekim 2012'de toplanan Bakanlar Kurulu, ''Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar''ı onayladı. Bu kararda siber güvenlik kurulunun Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığınca oluşturulmasına karar verildi. Ulaştırma, Denizcilik ve Haberleşme Bakanı başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği müsteşarı, Milli İstihbarat Teşkilatı müsteşarı, Genelkurmay Başkanlığı Muhabere, Elektronik ve Bilgi Sistemleri başkanı, Bilgi Teknolojileri ve İletişim Kurumu başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu başkanı, Mali Suçları Araştırma Kurulu başkanı, Telekomünikasyon İletişim başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmasına karar verildi. Bu kurulun görevi "kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasları düzenlemek" olarak belirlenmiştir.

Siber Güvenlik Kurulu'nun toplantıları sonrasında Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 18.2.2013 tarihli ve 412 sayılı yazısı üzerine, Bakanlar Kurulu'nun 25.3.2013'de onayıyla, 20 Haziran 2013'de Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 4890 sayılı Resmi Gazete'de yayınlandı. Stratejik yaklaşımında nispeten zayıflıklar bulunan belgede Eylem Planı'nın detaylandırıldığı görülmektedir. Ulusal siber güvenlik strateji eylemlerini şöyle sıralamaktadır:

1. Yasal düzenlemelerin yapılması,

2. Adli süreçlere yardımcı olacak çalışmaların yürütülmesi,

3. Ulusal siber olaylara müdahale organizasyonunun oluşturulması,

4. Ulusal siber güvenlik altyapısının güçlendirilmesi,

5. Siber güvenlik alanında insan kaynağının yetiştirilmesi ve bilinçlendirme faaliyetleri,

6. Siber güvenlikte yerli teknolojilerin geliştirilmesi,

7. Ulusal güvenlik mekanizmanlarının kapsamının genişletilmesi.

Siber güvenlik eylem planının sonunda stratejik eylemlerin uygulanması için oluşturulan detaylı bir takvim yer almaktadır Siber güvenlik için gerekli olan hamlelerin detaylı olarak listelendiği bu eylem planı teorikte optimum düzeyde olsa da pratik de uygulanabilirlik sorunlarına sahiptir.

Siber Güvenlik eylem planında yer alan işlemlerin küçük kısmının bile tamamlanmasının, Türkiye'nin siber güvenlik altyapısı için büyük bir katkı sağlayacağı açıktır. Türkiye planladığı siber güvenlik eylemlerini gereği gibi yerine getirmeyi başarırsa, NATO'nun istediği siber savunma seviyesine de yaklaşmış olacaktır.

# 2. GENEL BİLGİLER

## 2.1. Siber Korsanlar(Hackers)

Siber uzayda saldırı gerçekleştirmek isteyen kişilere siber korsanlar denir. Siber korsanlar niteliklerine ve amaçlarına göre Beyaz Şapkalılar, Siyah Şapkalılar ve Gri Şapkalılar olmak üzere üçe ayrılırlar. Beyaz şapkalı korsanların amacı zarar vermek değildir. Buldukları açıklıkları bildirerek, sistem ve yazılım sorumlularına destek olurlar. Bunlar iyi niyetli kişilerdir. Siyah şapkalı korsanlar ise güvenlik sistemlerini izinsiz olarak aşarak bilgi hırsızlığı, menfaat sağlama, dolandırıcılık, terörizm, bilinçli yıkım gibi zarar verici faaliyetlerde bulunurlar. Gri şapkalı korsanlar ise siyah şapkalı ve beyaz şapkalı arasında melezdir. Sistemin güvenliğini test etme iznine sahip olmasalar bile, herhangi bir sisteme sızabilir ancak sisteme zarar vermezler.

### 2.1.1. **Kötü Niyetli Yazılımlar**

Genel olarak tüm kötücül yazılımlar; yaşam döngüsü, kendi kendini çoğaltma, özerklik, bulaşma mekanizması, ayrık veya virüs özelliği taşıma, korunma mekanizması açısından farklı karakteristikler sergileyebilmektedir. Kötücül yazılımlar, yaşam döngüsünde her hangi bir aşamada farklı davranışlar sergileyebilecekleri gibi, kendi kendini çoğaltmayacak tek bir amaca yönelik çalışmakta; kullanıcının araya girmesine ihtiyaç duyabilecekleri gibi tamamen özerk bir yaklaşıma sahip olmakta; kötü niyetli kişiler tarafından bizzat elle hedef bilgisayar sistemine kurulabilmekte, kendisini saptayacak veya yok edecek korunma yapılarına karşı direnç gösterebilmekte, çeşitli taktiklerle bu tür programları atlatabilmektedir. En temel kötücül yazılımlar, gelişme süreçleri açısından karşılaşılan ilk kötücül yazılım olmaları dışında; belirgin karakteristik özellikleriyle bilgi ve bilgisayar güvenliğine karşı önemli tehditler içeren ve oldukça yaygın bir şekilde kullanıcıların maruz kaldığı yazılımlardır. Virüs, solucan, Truva atı ve mesaj sağanağı (spam) gibi kullanıcıların nispeten farkında olduğu türler dışında var olan diğer ana türler takip eden kısımda incelenmiştir.

#### 2.1.1.1 Bilgisayar Virüsleri (Computer Viruses)

Virüsler, en tehlikeli ve en eski kötücül yazılım olarak kabul edilmektedirler. Organizmalardaki hücrelere bulaşan küçük parçacıklar olarak tanımlanan biyolojik virüslerden esinlenerek adlandırılan bilgisayar virüsleri, kendi kopyalarını çalıştırılabilir diğer kodlara veya belgelere yerleştirilerek yayılan ve kendi kendine çoğalan programlardır. Ekranda rahatsız edici, çalışmaya kısa süreliğine de olsa mani olan mesajlar göstermek gibi zararsız sayılabilecek türlerinin de bulunmasına karşın, çoğu virüs programlarının, önemli dosyaları silmek veya konak (host) sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkileri bulunmaktadır. Bu virüsler, bilgisayar solucanının bir parçası olarak ağ üzerinden yayılabilir olmalarına rağmen yayılmak için ağ kaynaklarını kullanmazlar.

Bunun yerine disket, CD veya DVD gibi ortamlarla veya e-posta eklentileri ile hedef sistemlere bulaşırlar. Virüsleri diğer kötücül yazılımlardan ayıran en önemli özellik insan etkileşimine ihtiyaç duymasıdır. Virüs dâhilindeki kötücül kod mutlaka bir kullanıcı tarafından yürütülmelidir. Bir dosyanın açılmasıyla, bir e-postanın okunmasıyla, bir sistemi önyüklemesiyle (boot) veya virüs bulaşmış bir programı çalıştırması ile kullanıcı farkına varmadan virüsü yayar Virüsler yaygınlaştıkça virüs korunma programları da gelişmeye başlamış ve McAfee ve Symantec gibi firmaların öncülüğünü yaptığı virüs korunma programları, bilgisayar güvenlik sistemlerinin ayrılmaz parçası olmuştur. Bu firmalar, kötü niyetli kişiler tarafından geliştirilen "vahşi" (the wild) olarak tabir ettikleri virüslere karşı önlemler üretmek yanında; "hayvanat bahçesi" (zoo) ve "balçanağı" (honeypot) tabir ettikleri laboratuarlarında ileride çıkması muhtemel virüsler için de çeşitli çalışmalar yürütmektedirler.

Bilgisayar virüsleri;

- Dosya virüsleri
- Önyükleme (boot) virüsleri
- Makro virüsleri ve
- Betik (script)

virüsler olmak üzere dört sınıfta incelenebilirler. Dosya virüsleri, yayılmak için kendilerini çeşitli dizinlere kopyalayarak veya virütik kodlarını çalıştırılabilir dosyalara bulaştırarak, işletim sisteminde bulunan dosya sisteminde kullanan virüs türleridir. Önyükleme (boot) virüsleri, sabit disk veya disketin "Ana Önyükleme Kaydını" (Master Boot Record)

değiştirerek bilgisayarın her açılışında virütik kodun çalışmasını sağlayan virüslerdir. 26 Nisan 1986'da yaşanan Çernobil faciası üzerine Çernobil virüsü olarak adlandırılan ve bu tarihte bulaştığı konak sisteme zarar veren W95/CIH virüsü, önyükleme virüsleri arasında en çok tanınan ve oldukça zararlı virüslerden biridir [12]. Makro virüsleri, Microsoft Word ve Excel gibi güçlü makro desteği olan masaüstü programları kullanan ve bunlara ait belgelerin açılışında çalışan makrolar ile yayılan virüs türleridir.

Çalıştırılabilir dosyalar dışındaki dosyalara bulaşan ilk virüs olan WinWord/Concept ve Microsoft Excel çalışma sayfalarına bulaşan XM/Laroux, bu tür makro virüslerine örnek olarak verilebilir [5]. Betik (script) virüsleri, VB (Visual Basic), JavaScript, BAT (toplu işlem dosyası), PHP gibi betik dilleri kullanılarak yazılan virüslerdir. Bu virüsler ya diğer Windows veya Linux komut ve hizmet dosyalarına bulaşır ya da çok bileşenli virüslerin bir parçası olarak çalışırlar. Betik desteği olan ve zararsız gibi görünen HTML, Windows yardım (help) dosyaları, toplu işlem dosyaları ve Windows INF dosyaları, bu tür virüslerin yerleştiği dosyalar olarak karşımıza çıkabilir.

#### 2.1.1.2 Bilgisayar Solucanları (Computer Worms)

Bilgisayar virüslerine benzer bir yapıda olan solucanlar, virüsler gibi bir başka çalıştırılabilir programa kendisini iliştirmez veya bu programın parçası olmazlar. Solucanlar, yayılmak için başka bir programa veya virüslerde olduğu gibi insan etkileşimine ihtiyaç duymayan, kendi kendini çoğaltan bir yapı arz ederler. Bir solucanın yayılmasında kullandığı en yaygın yöntemler arasında, e-posta, FTP ve HTTP gibi İnternet hizmetleri bulunmaktadır. Solucanları yaymak için, hedef sistemdeki korunmasızlıklardan faydalanma veya kullanıcıların solucanları çalıştırabilmeleri için sosyal mühendislik yöntemlerini kullanma gibi yöntemler kullanılmaktadır. Solucanlar, başka dosyaları değiştirmezler; fakat etkin bir şekilde bellekte dururlar ve kendilerini kopyalarlar. Solucanlar otomatik olarak gerçekleştirilen ve genellikle kullanıcılara gözükmeyen işletim sistemi yapılarını kullanırlar.

Solucanların kontrol dışı çoğalmaları, sistem kaynaklarını aşırı kullandığında veya diğer işlemekte olan görevleri yavaşlattığında veya bu görevlerin sonlanmalarına neden olduğunda farkına varılabilir. Solucan ismi, 1975 yılında John Brunner tarafından yazılan "Shockwave Rider" (Şok Dalgası Binicisi) adında bir bilim kurgu romanında, bir bilgisayar ağı üzerinden

kendi kendini yayan bir programa verdiği isimden gelmektedir Bilgisayar solucanları; e-posta, IM (Internet Messaging), İnternet ve ağ solucanları olmak üzere dört grupta incelenebilir. E-posta solucanları, kötücül yazılımların en çok tercih ettikleri yayılma yöntemi olan e-postaları kullanmaktadır. Genellikle bir fotoğraf veya metin dosyası gibi tek bir eklenti içerecek şekilde gönderilen e-postaların içerisinde bulunurlar.

Kullanıcı eklentiyi çalıştırdığında solucan kendini başlatır ve konak makineye bulaşır. Solucanlar genellikle bulaştıkları makinede kullanıcının adres defterinden e-posta adreslerini toplar ve kendini bulduğu her bir adrese gönderir. "İnternet Mesajlaşma" (IM) Microsoft'un MSN Messenger, AOL'nın AIM, IRC, ICQ, KaZaA gibi yaygın mesajlaşma hizmetleri ve ağ paylaşımları IM solucanlarının yayılması için kullanılırlar. Hedeflenen hizmeti kullanan tüm kullanıcılara, solucan bulaşmış bir dosya veya solucanın kendisinin yer aldığı bir web sitesine yönelen İnternet bağlantısı gönderirler.

Bağlantıya tıklandığında solucan bilgisayara indirilir ve otomatik olarak çalışır. Solucan kendini konak makineye kurar ve kullanıcının haberleşme listesindeki tüm kullanıcılara aynı türde mesajlar göndererek kendini yaymaya devam eder. İnternet solucanları, sadece İnternet'e bağlı olan makinelere bulaşabilen solucanlardır. Bu tür solucanlar, İnternet üzerinde tarama yapar ve en son güvenlik güncellemelerini kurmamış olan, açık kapıları olan veya güvenlik duvarı olmayan korunmasız bilgisayarları bulmaya çalışırlar. Solucan böyle bir bilgisayar bulununca, kendini bu makineye kopyalar ve kendini kurar. W32/Blaster ve W32/Deloder bu tür solucanlara örnektir. Bir başka ilginç solucan türü olan ağ solucanları, paylaşılan bir klasöre, isimlerini faydalı veya ilginç gözükebilecek bir uygulama veya dosya ismine dönüştürerek kendilerini kopyalarlar.

Bu dosyaları çalıştıran kullanıcılar kendi bilgisayarlarına solucanı bulaştırmış olur. Çoğu solucan tek tip işletim sisteminde çalışacak şekilde geliştirilmektedir. Fakat çok yakın zamanda Windows, Linux, Solaris, BSD ve diğer işletim sistemlerinde çalışabilecek şekilde bir "savaş başlığı" içeren süper solucanlar ortaya çıkacaktır.

## 2.2. Saldırı Yöntemleri

### 2.2.1. Oltalama (Phishing)

Phishing, dolandırıcıların rastgele kullanıcı hesaplarına e-mail gönderdikleri bir çevrimiçi saldırı türüdür. E-postalar, bilinen web sitelerinden veya kullanıcının bankasından, kredi kartı şirketinden, e-posta veya internet hizmeti sağlayıcısından gönderilmiş gibi gözükür. Genellikle hesapları güncelleyebilmek için kredi kartı numarası veya şifre gibi kişisel bilgiler sorulur. Bu e-postalarda kullanıcıları bir başka web sitesine yönlendiren URL bağlantısı yer alır. Bu site aslında ya sahte ya da değiştirilmiş bir web sitesidir. Kullanıcılardan da bu siteye gittiklerinde phishing saldırısını yapan kişiye iletilmek üzere kişisel bilgilerini girmeleri istenir.

Phishing, genelde bir kişinin şifresini veya kredi kartı bilgilerini öğrenmek amacıyla kullanılır. Bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilir. Phishing saldırıları için bankalar, sosyal paylaşım siteleri, e-posta servisleri, online oyunlar vb. sahte web sayfaları hazırlanmaktır. Burada bilgisayar kullanıcısından kimlik bilgileri, kart numarası, şifresi vb. istenir. E-posta mesajındaki ve sahte sitedeki talepleri dikkate alan kullanıcıların bilgileri çalınır.

Tam bir aldatmacadır. Saldıran kişi bir “yem” hazırlar ve bu yeme “balıkların” takılmasını bekler. Büyük kayıplar yaşanmaması için bu tür sahtekarlıklara karşı bilinçli olmak gerekmektedir.

Bu yazının amacı da zaten bu bilinci yaratarak teknoloji kullanan insanların zarar görmesini engellemektedir.

Phishing saldırılarıyla nelerin çalınması amaçlanıyor ?

Phishing yöntemi kullanarak bilgisayar kullanıcılarını kandıran saldırganlar genellikle aşağıdaki bilgilere erişmeyi hedeflemektedirler.

- Kullanıcı hesap numaraları
- Kullanıcı şifreleri ve parolaları
- Kredi kartı numaraları
- İnternet bankacılığında kullanılan kullanıcı kodu ve şifreleri vb.

- E-Posta ile Phishing
- E-posta yöntemini kullanan dolandırıcılar burada da kullanıcıları farklı şekillerde aldatma yoluna giderler.

a) E-postanıza devamlı temas halinde olduğunuz kuruluşlardan gönderiliyormuş izlenimi verilen sahte bir e-posta gönderiliyor. Bu e-postalarda kullanıcıya kurumun web sitesine gitmesinin gerektiği, şifresinin süresinin dolduğu söylenir ve altta o sayfaya yönlendirileceği bir link (bağlantı) verilir. Dolandırıcı daha önceden hazırladığı ve kuruluşun sitesinin aynısı veya benzeri olan bu siteye kullanıcıyı getirdikten sonra, ondan şifreyi girmesini ister. Dolandırıcı bu şifreyi kullanarak internet aracılığı ile para transferi, e-ticaret, sizin adınıza bağış toplama, reklam gönderme, çok sayıda spam mesaj gönderme vb. işler yapabilir.

b) Bazı e-postalarda ise; bir yarışma düzenlendiği ve bu yarışmaya katılması teklif edilen kullanıcılara ödül olarak bir ürün kazandıkları ancak gerekli kişisel bilgileri vermeleri gerektiği söylenir. Bu gibi durumlarda bilgilerini veren kullanıcının tüm bilgileri dolandırıcının eline geçer.

c) Bir başka kullanılan teknikte ise; gelen e-postada müşteriye kişisel bilgilerini güncellemesi gerektiği, tüm bilgileri tekrar girmesi bunun kendileri açısından daha iyi hizmet verebilmeleri için gerekli olduğu söylenir.

d) Bir başka teknikte ise; gelen e-postada kullanıcının e-posta kotasının dolduğu, eğer bilgilerini güncellemezse hesabının kapatılacağı söylenir.

e) Son zamanlarda bazı bankaların başlatmış oldukları ve cep telefonları ile para transferine imkân veren sistem kullanılarak banka müşterilerine sanki kendi hesaplarına para gönderilmiş veya alınmış gibi gösterilip sahte banka sitesi linki (bağlantı yolu) verilerek bu paranın tahsil edilebilmesi için bilgi güncelleştirmesi istendiği bilinmektedir.

Phishing amaçlı gönderilen e-postalar ve sahte web siteleri nasıl tespit edilir?

E-posta tanınmış yasal bir e-ticaret sitesinden, finansal kurumdan, e-posta sağlayıcısından, internet hizmet sağlayıcısından mı geliyor?

Kişisel bilgilerinizi vermeniz mi isteniyor?

E-postada ya da web sitesinde yazım veya dilbilgisi hataları var mı?

E-posta ya da yönlendirildiğiniz web sitesi, sizden yanıt alabilmek için duygusal veya heyecan verici bazı sözler kullanıyor mu?

Eğer e-postadaki bir bağlantı (link) aracılığıyla bir web sitesine yönlendirilmişseniz, tarayıcının (browser) üst kısmında yazan URL ile ziyaret ettiğinizi düşündüğünüz yasal şirketin URL adresi birbirine uyuyor mu?

Phishing saldırısına hedef olduysanız neler yapmalısınız ?

Eğer saldırı yasal bir şirketle ilişkiliyse (yani phishing saldırısında gönderilen e-posta tanınmış bir e-ticaret sitesinden, finansal kurumdan, e-mail sağlayıcısından, internet hizmet sağlayıcısından geliyorsa) bu saldırıyı ilgili şirkete bildirin. Böylece, ilgili kuruma sahte web sitesini kapatma ve saldırganın izini sürmesini sağlamak için yardımcı olabilirsiniz.

E-posta hesabımın şifresi ele geçirildiğinde ne olur?

Gönderilecek mesajın görünen ismi, sizin isminiz yerine genellikle başka bir isimle değiştirilir.

Mesajın sonuna eklenecek olan imza metni değiştirilir.

Hesabınızda bulunan veya size sonradan gelecek olan mesajlar saldırgana yönlendirilir ve sizdeki kopyası silinir.

Hesabınızdaki mesajların tümü silinebilir.

Çevrimiçi dolandırıcılıktan korunmanın yolları

E-posta hesabınız için kullandığınız şifre, diğer hesaplarınızdaki şifrelerden farklı olmalıdır.

Kişisel bilgilerinizi isteyen e-postalara yanıt vermeyin.

Gelen e-postanın kimden geldiğinden emin değilseniz dikkate almayınız. Unutmayın hiç bir kurum veya kuruluş e-posta yoluyla sizden kişisel bilgilerinizi istemez.

ÇALIŞTIĞINIZ KURUM SİZE ASLA KİŞİSEL BİLGİLERİNİZ VEYA ŞİFRENİZİ SORAN E-POSTA GÖNDERMEZ.

Şüpheli gördüğünüz e-postalardaki URL linklerini tıklamayın.

E-posta mesajlarındaki kısaltılmış URL linklerine ( bit.ly,ow.ly, tinyurl.com, is.gd, goo.gl, tiny.cc, cli.gs vb.) kesinlikle tıklamayın.

Şüpheli veya bilmediğiniz web sitelerine kişisel bilgilerinizi vermeyin.

Kişisel bilgilerinizi girmek için banka, kredi kartı ve servis sağlayıcılarının web sitelerini ziyaret ettiğinizde, web sitesinin URL'sini internet tarayıcınıza doğrudan yazın.

Güvenli olan sitelerde bile çevrimiçi olarak bir formu doldurmadan önce, sitenin üçüncü kişilerle bu bilgileri paylaşıp paylaşmadığını belirten gizlilik anlaşmasının olup olmadığını kontrol edin.

Antispyware ve antivirüs programları kullanın.

Yasal olmayan veya kaynağı belirsiz yazılımları yüklemeyin ve çalıştırmayın.

Kredi kartı numaraları, kişisel bilgiler, e-posta dahil her türlü şifre hiç bir zaman e-posta ile açıkça yollanmamalıdır. Bir e-posta teknik olarak gideceği yere varana kadar birçok noktadan geçmektedir. Bu noktalarda e-postaların içeriğinin "dinlenmesi" her zaman mümkündür.

Özellikle Kablosuz Internet'in kullanıldığı alanlarda mecbur kalınmadıkça banka gibi yerlere girilmemeli, kredi kartı, şifre vs. ile ilgili işlemler yapılmamalıdır. Havadaki sinyaller üçüncü şahıslar tarafından dinlenebilir. Sinyaller şifreli dahi olsa unutulmamalıdır ki tüm şifreleme yöntemleri sadece kırılıncaya kadar güvenlidir.

Bu tip saldırılara karşı korunmanın en etkili yolu,bu konuda bilinçli ve bilgili olmaktır.

### 2.2.2. Kimlik Sahteciliği (Spoofing)

Saldırgan, güvenilir bir kişiyi veya varlığı taklit eder. IP, ARP ve DNS sahteciliği olarak isimlendirilen türleri vardır. IP sahteciliğinde, saldırgan başkasının IP adresini kullanarak kendini gizler. Günümüzde daha çok DDOS saldırılarında kullanıldığından bahsedilmiştir.

### 2.2.3. Ortadaki Adam (Man In The Middle)

Ortadaki Adam (MitM) Saldırısı Nedir? sorusu büyük veri ihlallerine neden olabilen ciddi siber saldırılara karşı hazırlıklı olmanızı sağlayabilir.Adından da anlaşılacağı gibi, ortadaki

adam (Man In The Middle) saldırısı, kötü niyetli birinin iki taraf arasındaki iletişime gizlice dahil olduğu en eski siber saldırı türüdür.

MITM, kurban tarafından iletilen verilerin okunmasına hatta değiştirilmesine olanak tanır. Saldırgan kendi bilgisayarı ile kurbanın bilgisayarı arasında oluşturduğu gizli, sözde, sahte bir bağlantı sayesinde bunu başarır.

MITM saldırısının amacı, kişisel verileri, şifreleri, banka bilgilerini ele geçirmek veya taraflardan birini taklit etmektir. Bu eylemler, ne yazık ki oturum açma bilgilerinin değiştirilmesini veya bir para transferinin başlatılmasını içerebilir. Örneğin, bankacılık işlemlerinde bir saldırgan, bir kullanıcının transfer yaptığını görebilir ve hedef hesap numarasını veya gönderilen tutarı değiştirebilir.

Bazen ortadaki adama, ortadaki maymun (monkey in the middle), ortadaki canavar (monster in the middle), ortadaki makine (machine in the middle) veya ortadaki kişi (person in the middle) de denir.

Artan iş mobilitesi, açık Wi-Fi kullanımı ve savunmasız IoT cihazlarının yaygınlaşması MitM saldırılarının artmasına yol açan gelişmeler olarak sıralanabilir. Kablosuz ağların benimsenmesini saldırganlar veri çalmak ve kuruluşlara sızmak için bir fırsat olarak görmektedir. Son birkaç yılda Nesnelerin İnterneti (IoT) cihazlarının kullanımının önemli ölçüde artması, henüz yeterli güvenlik standartlarına sahip olmayan bu cihazları MitM saldırılarına karşı savunmasız kılmaktadır. Saldırganlar, diğer teknikleri uygulayabilmek için IoT cihazlarını şirketlerin ağına girmenin bir yolu olarak kullanmaktadır.

MitM Neden Tehlikeli?

Saldırganların, ara sunucular oluşturarak, kurbanların bir iletişimde gerçek tarafla konuştuklarına inanmasını sağlayabildiği bu saldırı türü genellikle bireyleri hedef alsa da işletmeler ve büyük kuruluşlar için de önemli endişe kaynağıdır. Bilgisayar korsanları; ortak bir erişim noktasını, mesajlaşma hizmetlerini, dosya depolama sistemlerini veya uzaktan çalışma uygulamalarını işletmelerin ağlarına giriş yolu olarak kullanılabilmektedir.

Genellikle casusluk veya finansal kazanç elde etme amacıyla kullanılan man-in-the-middle sadırıları, iş süreçlerine zarar vermek ve kurbanlar açısından kaos yaratmak için de gerçekleştirilir. Saldırganlar, kötü amaçlı yazılımların kurbanların mobil cihazlarına gönderilmesini sağlayabilir, trafiği şifreleyemedikleri göz önüne alındığında, mobil cihazlar bu senaryoya duyarlıdır.

Ayrıca bir MitM saldırısında virüslü bilgisayarlara yasal olmayan SSL sertifikaları yüklenebilir ve kurbanın cihazından ekran görüntüleri alınabilir.

Ortadaki Adam Saldırısı Nasıl Gerçekleştirilir?

Gizli bir dinleme sayılan, gerçek zamanlı konuşmaları ve veri aktarımını açığa çıkaran ortadaki adam saldırıları bir tür oturum kaçırmadır ve Sidejacking, Evil Twin, sniffing gibi formlara bürünür.

Sniffing'de saldırgan, verilere müdahale etmek için bir yazılım kullanır. Saldırganların bilgisayarlara enjekte ettiği kötü amaçlı yazılım kendisini otomatik olarak tarayıcıya yükleyebilir. Sidejacking oturum açma bilgilerini çalmaya ve bir kullanıcı oturumunu ele geçirmeye odaklanır. Evil Twin'de ise saldırgan meşru bir Wi-Fi ağını çoğaltarak gerçek ağda oturum açtığına inanan kullanıcıların verilerini ele geçirir. Siber korsanların, kullanıcı ağına müdahale amacıyla kullandıkları en yaygın yöntemlerden biri kötü niyetli Wi-Fi erişim noktalarını ücretsiz olarak halka açık hale getirmektir.

MITM saldırıları genellikle iki aşamadan oluşur: müdahale (Interception) ve şifre çözme (Decryption). Müdahale aşamasında, siber suçlular, bir Wi-Fi yönlendirici aracılığıyla ya da alan adı sistemi (DNS) sunucularını manipüle etmek gibi yollarla erişim elde ettikleri ağda güvenlik açıklarını ve olası giriş noktalarını bulmaya çalışır.

MITM saldırılarının ikinci aşaması olan şifre çözme, çalınan verilerin şifresinin çözülerek siber suçlular tarafından anlaşılır hale getirilmesini kapsar. Şifresi çözülen veriler; kimlik hırsızlığı, yetkisiz satın almalar veya dolandırıcılık amaçlı banka faaliyetlerinde kullanılabilir.

### 2.2.4. Kimlik Doğrulama (Authentication Hacking)

Kimlik doğrulama, web uygulamalarının güvenliğinde kritik bir rol oynar. Saldırgan, bilinen ve geçerli bir kullanıcı olduğunu kanıtlayarak sisteme girdiğinde, yönetici ayrıcalığına erişebilir. Oltalama, basit şifreler, sistem açıkları, sosyal ilişkiler vb. yöntemlerle şifrelerin ele geçirilmesidir. Sistemde istenmeyen durumların oluşmasına sebep olabildiğine değinilmiştir. Basit şifreler kaba kuvvet (brute force) atakları ile çözülebilir. Yetkili kullanıcı şifrelerinin çeşitli yöntemlerle ele geçirilmesi için ortam oluşturulmaması gerektiğinden bahsedilmiştir.

### 2.2.5. DDOS Saldırısı (Distributed Denial of Service)

Servisleri çalışamaz duruma getiren bir yöntemdir. Bilgisayarlara bulaştırılmış kötü amaçlı yazılımlar kullanılarak hedefe kaldırabileceğinden fazla istekler göndererek, hizmet durma noktasına getirilir. DDOS saldırılarına çeşitli çözümler üretilse de tam anlamıyla korunma

yöntemleri yoktur. Uluslararası bilgisayar korsanlarının hedefi haline gelecek durumlardan uzak durmak gerekir. Sınav döneminde veya başvuru dönemlerinde sistemler hizmet veremez duruma getirildiğinde itibar kaybı, iş ve işlemlerde gecikmelere neden olunduğundan bahsedilmiştir.

### 2.2.6. Enjeksiyon (Injection)

Web gibi dış dünyaya açık uygulamalar, dış kullanıcılara güvenlik önlemlerini kırmak, sistemlerin açıklarını tespit ve istismar için ortam sunmaktadır. Ayrıca bu sistemler optimize çalışmak için çeşitli servisler ve uygulamalarla ile veri alışverişinde bulunurlar. Bunu yaparken de yetkilendirme kullanırlar. Bu sunuculardan biri ele geçirildiğinde diğer sistemlerde risk altına girer. Enjeksiyon saldırıları, kullanıcı adı ve parola bilmeden bir uygulamada oturum açmak, aynı zamanda özel, gizli veya hassas bilgileri ortaya çıkarmak veya hatta tüm sunucuyu ele geçirmek için kullanılabilir. Bu saldırılar yalnızca web uygulamaları için değil, verileri bu uygulamalarda ve diğer bağlı uygulama ve hizmetlerde bulunan kullanıcılar için de bir tehdit olduğundan bahsedilmiştir.

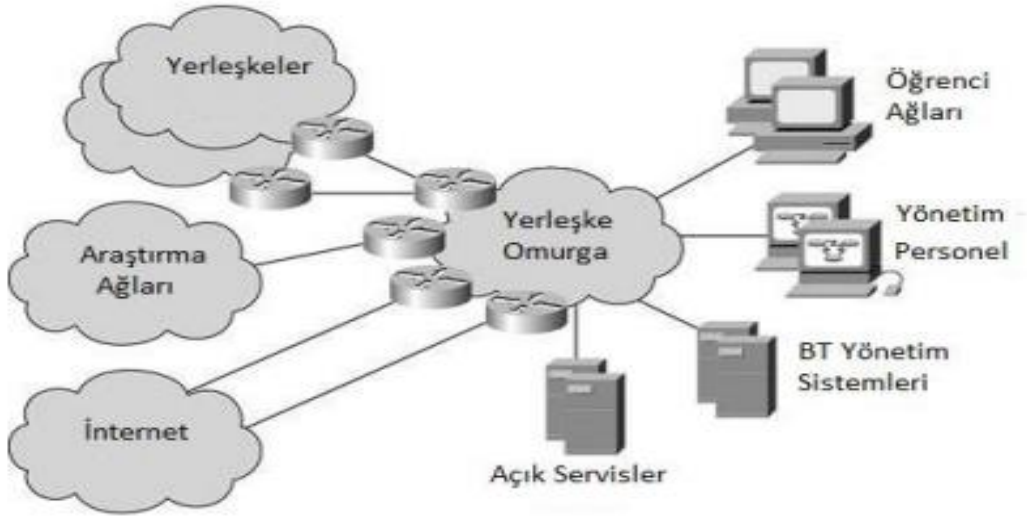
**Injection (Enjeksiyon) için alınabilecek tedbir kapsamları**

- Veri tabanında bulunan tablo ve tablo alanı isimlerinin kolay tahmin edilebilecek şekilde olmaması gerekir.
- Web formlarında parametrik sorguların kullanılması tercih edilmelidir.
- Web formlarındaki giriş kontrollerine veri girişi
- yapılırken bu verilerin doğrulanması, girdi uzunluğunun kontrol edilmesi önemlidir.
- Web formlarında kullanılan ve veri tabanında bir kayıt satırını temsil eden sayısal değerler için (QueryString değeri) formlar arası geçişlerde bu değerlerin sayısal değer olup olmadığının kontrol edilmesi gerekir.
- SQL tabanlı web uygulamalarında kullanıcı, veri girişi yaptıktan sonra veri tabanına gönderilen SQL sorgusu karakterlerinde arama yaptırılarak tehlikeli karakterleri, replace vb. komutlarla SQL Sunucuda hataya yol açmayacak şekilde zararsız karakterlere çevrilmelidir.
- SQL sunucuda oluşacak hataların web formlarında görüntülenmesi engellenmelidir.

- Web uygulamalarında kullanılan veri tabanına yazma, okuma, silme gibi temel özelliklerin yalnızca bir yönetici tarafından yönetilmesi gerekir.
- Uygulamada web formlarına sorgu yazmak yerine, bu sorguları veri tabanı kısmında saklı yordam (Stored Procedure) olarak yazılması sağlanmalıdır.
- SQL enjeksiyon yönteminde kullanılabilecek sözcüklerin (select, insert, update vb.) bir fonksiyon ile filtrelenmesi olası sızmalara karşı bilgi verilmesini engeller.
- Veri tabanının kullanacak yöneticilerin yetkilendirilme işlemlerinde, sınırlı yetkilere sahip kullanıcı hesabı ile çalıştırılmasına büyük özen gösterilmelidir.
- Kullanılmayan saklı yordamların ve yönetici hesaplarının kaldırması gerekir.
- Sistem nesneleri için genel erişim verilmemeli, gerekirse kullanıcı bazında yetki verilmelidir.
- Web uygulaması ve veri tabanı sunucularının bulunduğu sistem, donanım veya yazılım tabanlı bir güvenlik duvarı ile saldırılara karşı muhafaza edilmelidir.
- Yukarıda belirtilen öneriler dikkate alındığında, veri tabanı kullanan web uygulamaları, büyük ölçüde SQL enjeksiyon saldırılarından korunmuş olacaktır.

# 3. AĞ ÇEŞİTLERİ

Kampüste Nasıl Bir Ağ Yapısına sahip olduğunu inceleyelim.




Şekil 1. Kampüs ağı
(Campus network)

En az iki cihazın birbiriyle iletişimde olması durumuna kısaca ağ diyoruz. Bir ağ oluşturmak için iki bilgisayar yetse bile binlerce hatta milyonlarca bilgisayar ile de ağ kurabiliriz. Peki ağ çeşitleri nelerdir? Ağ çeşitleri neden vardır?

## 3.1. Local Area Network (LAN-Yerel Alan Adı)

Yalnızca birkaç cihazın birbirine bağlanarak sınırlı bir alanda oluşturdukları ağ çeşididir. Buna sınıf içinde kurduğumuz ağı örnek verebiliriz. Bu ağda ağ kabloları, bilgisayarlar, kontrol cihazları yer alır. Genelde dosya paylaşımı veya yazıcı paylaşımı için kurarız.

## 3.2. Metropolitan Area Network ( MAN- Metropol Alan Ağı)

Geniş bir alan içerisinde kullandığımız ağ çeşididir. Mesela bir üniversite yerleşkesi içerisinde kullandığımız ağ buna örnektir. Veya bir mağazanın aynı şehir içindeki iki ofisinin bağlantısı MAN'dır. LAN ağlarından daha geniş bir alanı kapsar. Aslında birkaç LAN ağının birleşmesiyle de oluşur. MAN bir kamu kuruluşu veya özel bir kurum yönetir. Ama birden fazla grup veya şirket bağlıdır. Yerel ağların birbiriyle iletişimi için kurarız.

### 3.3. Wide Area Network (WAN- Geniş Alan Ağı)

Çok geniş alanlar içinde cihazların birbirine bağlanmasıyla oluşur. Buna örnek olarak bir bankanın Türkiye'deki tüm şubelerinin birbiri ile bağlantısını örnek veririz. Birçok tipte cihazı ve bir çok tipte alt ağı birbirine bağlar. Asıl amacı veri paylaşımıdır. Ama bu veri paylaşımının güvenli ve hızlı olması için de ağda bir çok cihaz bulunur.

Biraz LAN ağlara göre yavaştır. Çünkü kullanıcı sayısı çok çok fazladır. LAN ağlarda kullanıcı sayısı kısıtlıdır. Kapasitesi sınırlıdır. Fakar WAN ağlarında herhangi bir kısıtlama yoktur.

### 3.4. Virtual Private Network (VPN- Sanal Özel Ağ)

Adından da anlaşılacağı gibi özel bir ağ hattı oluşturulmuş gibi iletişim kurulur. Yani sanki size özel bir hat çekilmiş gibi veri paylaşımı yaparız. Bilgileriniz daha güvende olurlar. Çoğunluklar ticari işletmelerde güvenlik için tercih ederiz. Evinizden işyerinizdeki ağa bağlanmak için yine VPN'leri kullanırız.

### 3.5. Storage Area Network ( SAN- Depolama Alan Ağı)

İnternet kullanımının artmasıyla depolama sorunları da ortaya çıktı. Bu depolama ünitelerinin güvenliğini sağlamak ise ayrı bir sorun. Bu nedenle ana ağdan ayrı güvenlikli bir ağ oluşturma gereği ortaya çıktı. Bir şirket düşünün veya bir banka. Zaman geçtikçe veritabanında daha fazla bilgi oluşacağı için ayrı bir depolama ünitesi de gerekecektir. Fakat istenilen zamanlarda o bilgilere ağ üzerinden de erişmek gerekecektir. SAN ağları sayesinde bu sorunları çözmüş oluyoruz.

### 3.6. PAN (Personal Area Network - Kişisel Ağ Bağlantısı)

PAN kişisel cihazların birbiriyle bağlanması sonucu elde edilen kişisel ağdır. InfaRed (IR) ve BlueTooth (BT) günümüzde PAN ağlarında en çok kullanılan teknolojilerdir. BT 10 ile 200 metre arasında bağlantı sağlarken (700 kbps) IR ancak bir kaç metre içerisinde bağlantı sağlar (115 kbps). PAN bağlantısı sağlandığında PAN'ın parçası olan tüm etkin aygıtlar (cep telefonu, USB, fotoğraf makinesi, yazıcı gibi) ve bilgisayarlar arasında erişim sağlanır. Kişisel ağ bağlantısı, bilgisayar ile ağ dahilindeki diğer bilgisayar ve cihazlar arasında otomatik olarak bağlantı kurulmasını sağlar.

# 4. SİBER GÜVENLİK PRENSİPLERİ


## 4.1. Gizlilik

Gizlilik, bilginin yetkisiz kullanıcılar tarafından ele geçirilmesini önlemektir. Gizlilik, sadece kalıcı ortamlarda (disk, tape, vb.) değil aynı zamanda internet araçlığıyla iletilen gizli bilgiler içinde önem arz etmektedir.

## 4.2. Bütünlük

Veri bütünlüğü, veriyi bir kullanıcıdan gönderildiği gibi veriler üzerinde herhangi bir değişiklik yapılmadan bütünüyle diğer kullanıcıya iletilmesidir. Amaç veriyi bozulmadan, yeni veriler eklenmeden veya verilerin bazıları veya hepsi 6 silinmeden, tekrar edilmeden ve düzeni bozulmadan güvenli bir biçimde tutmak ve korumaktır.

## 4.3. Erişilebilirlik-Süreklilik

Erişilebilir prensibi bilgi veya veriye istenildiği zaman ulaşılabilir ve kullanılabilir olmasını sağlamaktadır. Süreklilik hizmetinin amacı, bilişim sistemlerini, dâhili ve harici her türlü tehditlere karşı korumaktır. Bu hizmet sayesinde, kullanıcılar, erişim yetkileri olan verilere,

istedikleri zaman ve güvenli bir şekilde ulaşabilmektedirler. Sistem sürekliliği, sadece kötü niyetli bir saldırı sonucu zarar görmez. Aynı zamanda Bilgisayar yazılımlarının çökmesi gibi yazılım hataları sonucu veya donanım sorunları, sistemin yanlış, bilinçsiz ve eğitimsiz kişilerin kullanması, bazı doğal olumsuzluklar(ısı, nem, topraklama eksikliği, yıldırım düşmesi) gibi etkenler de sistem sürekliliğini bozabilmektedir.

### 4.4. İzlenebilirlik

Bu prensip sistemde gelişen olayları, daha sonra incelemek için kayıt edilmesini sağlamaktadır. Bir sistemde olabilecek tehditlere örnek olarak, kullanıcılar şifrelerini kullanarak sisteme girmesi, bir web sayfası üzerinden e-posta göndermek veya almak verilebilmektedir. Kaydedilen olaylar incelendikten sonra gerçekleştirilecek analiz neticesinde, herhangi bir saldırı türü görüntülenirse veya saldırı olasılığı yüksek bir tehdit görülürse yöneticilerini uyarmak için alarm mesajları kurulabilir.

### 4.5. Kimlik Doğrulaması

Ağ güvenliği bakımından kimlik doğrulaması; kullanıcının gerçekten iddia da bulunan kişiyle aynı olup olmadığından emin olmaktır. Aynı zamanda, bir yazılım sisteminden yaralanırken şifrelerin kullanılması da bir kimlik sınamasıdır. Günümüzde kimlik doğrulaması, bilgisayar ağ ve sistemlerinin yanı sıra, fiziki sistemlerde de oldukça mühim bir hizmettir. Akıllı kartlara veya biometrik teknolojilere yönelik doğrulama yöntemleri kullanılmaktadır.

### 4.6. Güvenilirlik

Sistemin öngörülen davranışıyla alınan sonuç arasındaki tutarlılığıdır. Diğer bir deyişle güvenilirlik, sistemin yapmasını beklediğimiz şeyi tam olarak ne eksik ne de fazla yapmış olması ve çalıştırılmak istendiği her defada da hiç değişiklik göstermeden aynen davranmasıdır.

### 4.7. İnkâr Edememe

Burada veriyi gönderen ile alan arasındaki iletişim mesajlaşmada çıkabilecek sorunları ne gönderici ne de alıcı inkâr edebilir. Yani iki kullanıcı arasında bir bilgi alışverişi gerçekleşmişse ne gönderen alana bir ileti ilettiğini ne de alan almış olduğu bu iletiyi inkâr edemez. Genellikle gerçekliği olan işlemlerde kullanılmakta ve kullanıcıların aralarında meydana gelebilecek sorunları minimum seviyeye indirmeyi amaçlamaktadır.

### 4.8. Siber Güvenlik Kavramları

Siber güvenlik kavramlarını açık ve net bir şekilde anlayabilmek için çalışmanın bu bölümünde, siber, siber ortam/uzay, siber saldırı, siber suç, siber terörizm, siber casusluk, siber savunma, gibi bazı siber güvenlik kavramlarına yer verilmiştir.

### 4.9. Siber

Siber kelimesi "Cybernetics" sözcüğünün ön ekidir. Siber kelimesinin ayni anda bu kelimenin kısaltması olarak da kullanıldığı görülmektedir. Türkçede siber kelimesinin yerinde "bilişim" kelimesi kullanılmaktadır.

Türk Dil Kurumu ise bilişim kelimesini, "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik" şeklinde tanımlamaktadır (TDK).

### 4.10. Siber Ortam/Uzay

Siber Uzay kelimesini ilk defa, bilimkurgu yazarı William Gibson 1980'li yılların başında kullanmıştır. Siber ortam, topluma yararlı pek çok hizmet vermektedir, kamu ve özel sektörler, daha iyi hizmet verebilmek için siber ortam kullanmaktadırlar. 8 Siber ortam sunduğu yararlı hizmetlerin yanı sıra bazı kötü amaçlar için de kullanılabilmektedir.

*Siber Uzayın Bileşenleri*

| Siber Uzay | |
|---|---|
| Fiziksel Yapı | Sanal Yapı |
| • Sosyal elektronik cihazlar<br>• Akıllı telefonlar<br>• Akıllı nesneler<br>• Algılayıcılar / Duyargalar<br>• Uydu sistemleri<br>• İnternet / bilgisayar ağları | • İşletim sistemleri<br>• Veri tabanı yönetim sistemleri<br>• Yazılım ve kodlar ile üretilen, depolanan, iletilen ve çeşitli maksatlarla kullanılan her türlü veri ve bilgi |
| Diğer Varlıklar | |

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı ise siber uzayı şöyle tanımlamaktadır. "Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamdır" (T.C. UDHB, 2016).

# 5. BAZI ÜLKELERDE SİBER GÜVENLİK SİSTEMLERİ

Siber Güvenlik Sadece Kampüs içinde var olması gereken bir konu olmadığından dolayı Gelişmiş Ülkelerde nasıl Önlemler alındığını Öğrenmemiz gereklidir.

## 5.1. Amerika Birleşik Devletleri

Başka ülkelerin gerçekleştirdiği siber saldırıları bir savaş sebebi olarak algılayacak olduğunu belirten ABD, dünyaya sunduğu siber ortamı ve icat ettiği 5. boyut silah karşısında kendisini bile korumaya çalışmakta ve bu sebeple yeni güvenlik stratejileri geliştirmektedir.

ABD'nin siber güvenlikle ilgili ilk geniş ve kapsamlı belgesi 2003'te Beyaz Saray'ın yayınladığı Güvenli Siber Uzay (Secure Cyberspace) belgesidir. Bu belgede "siber güvenlik" terimi sadece 3 defa kullanılmakta ve siber güvenlik yerine çoğunlukla güvenli siber uzay veya siber alan kelimelerine yer verilmektedir.

Bu Yazının devamında, ulusal güvenliğin sağlanması için aşağıdaki adımların atılması gerektiği belirtilmiştir.

- Ulusal bir siber ortam güvenliğini sağlamak için karşılık sistemleri.
- Güvenlik tehdit ve zafiyetleri konusunda sistem geliştirme.
- Ulusal bir siber ortam güvenliği için tehdit ve güvenlik zafiyet savunma Sistemi.
- Ulusal bir siber uzay güvenliği için geliştirme ve farkındalık.
- Devletin siber uzayı sistemini güvence altına almak.
- Ulusal güvenlik ve uluslararası siber ortam güvenliği için işbirliği yapmak.

## 5.2. Almanya

Almanya'da bilgi güvenliği için başlatılan faaliyetler siber güvenlik terimi meydana gelmeden çok daha eskilere dayanmaktadır. İkinci Dünya Savaşı esnasında Nazi Almanya'nın kullandığı Enigma isimli aygıt, Alman askerleri arasında gizli bilgiler için şifre kullanılması ve bu şifreleri tekrar çözülmesi için yararlanılan ve aynı zamanda başka devletlerin iletişim bilgilerini de deşifre edebilen bu aygıt tarih sayfalarında kendine yer bulmuştur. Ülkenin siber

güvenlik stratejisini çoğunlukla Alman ordusu belirlemektedir. Fakat siber güvenliğin oldukça kapsamlı olması ve siber saldırıların nasıl, nerden gelebileceğinin ve hangi büyüklükte olduğu bilinmediğinden dolayı birçok uluslararası kuruluşla da iş birliği yapmaktadır. Ülkenin siber güvenlikle ilgili düzenlediği belgelere bakıldığında ilk defa 1989'da Ulusal Politika belgesi yayımlanmıştır. Daha sonra 2005'te Bilgi Güvenliği ve Kritik Altyapıların Korunması ile ilgili Ulusal Strateji Belgesi yürürlüğe konulmuştur. Bu belgeden sonra 2011'de yayımlanan Alman Ulusal Siber Güvenlik Stratejisi özellikle siber ortamdan gelebilecek risk ve tehditlere karşı koyabilmek için odaklanmıştır. Ülkenin siber güvenliğinin sağlanması için temel yapı olarak önemli katkılarda bulunan Alman Federal Bilgi Güvenliği Örgütünün birimleri ise siber güvenlik ile ilgili uzmanlaşan bir politika takip etmektedirler. Bu örgüt, Siber Güvenlik Dairesi, Kriptoloji Dairesi, Güvenli Elektronik İşlemler Sertifikasyon ve Standardizasyon Dairesi, Profesyonel Ağ Savunma Birimi gibi birimlerden oluşmaktadır.

### 5.3. Çin

Çin siber güvenlik ve iletişim teknolojilerine 20. yüzyılın sonlarından, yani bu teknolojilerin ortaya çıktığından beri önem vermektedir. İlk önce 1986'da ekonomik bilgilerin yönetimi ile ilişkin küçük bir ekip kurulmuş ve 2001 yılına kadar etkin olarak görev yapmıştır. 2003'te ise siber güvenlikle ilgili Belge 27 isminde ilk sivil belge yayınlanmıştır. BİT'lerin artmasından dolayı ülkede, siber suç ve siber saldırılar çoğalmış ve siber güvenlik konusu bu ülkenin de öncelik verdiği bir konu olmuştur.

Çin'in siber güvenlik konusunda bakış açısı da başka ülkelerle hemen hemen aynıdır. Fakat tehditlere karşı ülkenin uyguladığı siber güvenlik yöntemi daha ulusal ve uluslararası platforma nispeten kapalı olduğundan dolayı batı ülkelerine göre farklılık göstermektedir. Bu ülkenin, başka ülkelerden farkı ise kendi ulusal siber ağlarını kullanarak ve dünyada yoğun olarak kullanılan birçok ağın kullanmasına yasak getirerek ya da kullanımını kısıtlayarak en etkili savunma sistemlerini geliştirmiş olmasıdır. Bu şekilde izlenen bir yöntem ülkeyi, siber güvenlik açısından batı ülkelerine göre daha güvenli kılmaktadır.

Çin bir yandan her alanda bilişim teknolojilerinin geliştirilmesini ve kullanılmasını önerirken, diğer yandan da temel bilgi ağlarının ve kritik alt yapılarının, güvenlik sistemlerini güçlendirilmesini göz önünde bulundurmuştur. Ülkenin siber güvenlik ve siber savunmasının sorumluluğu Halk Kurtuluş Ordusu (Peoples Liberation Army-PLA) tarafından sağlanmaktadır. Buna ek olarak, binlerce uzman personelden oluşan ve devlet tarafından desteklendiği düşünülen Çin 61398 nolu birliği 2006'dan beri faaliyet göstermektedir.

### 5.4. Estonya

Estonya, 2007 yılındaki siber saldırıdan sonra teknik ve teknik olmayan bir eğitim sisteminin kurulmasına önem vermeye başlamıştır. Siber güvenlik projelerinde Avusturya, Lüksemburg, Güney Kore ve NATO ile iş birliği yapan ülkelerde bu ulusal altyapının tamamen dijitalleştirilmesi ve korunması için araştırma ve geliştirme projelerini hızlandırmak atılan en büyük adımlardan biridir.

Estonya, NATO tarafından tanınan bir siber güvenlik kuruluşu olan CCDCOE'nin Kilitli Kalkan çalışmasını da sürdürmektedir (2019 yılında katılımcı ülke sayısı 30, katılımcı sayısı 1.200). Siber risk analizi ve bilgi güvenliği araştırmaları ile küresel siber güvenlik sistemine katkılar, dijital hizmetlerin ve kişisel verilerin korunması için alınan önlemler, siber kriz yönetimi araştırması ve askeri siber operasyonlarda elde ettiği başarı ile Estonya kısa sürede dünya lideri, Avrupa'nın sayılı ülkelerinden ve liderlerinden biri haline gelmiştir.

### 5.5. İngiltere

2009 yılında kraliçenin buyruğu üzerine Siber Güvenlik Stratejisi Birleşik Krallık Güvenlik/Güvenlik ve Siber Alanda Dayanıklılık (Cyber Security Strategy Of The United Kingdom Safety/Security And Resilience İn Cyber SpaceCSSUKS/SRCS) adlı ilk siber güvenlik strateji belgesi yayımlanmıştır. Bu belge hem şirketler hem de devlet ve vatandaşların siber tehditlerle karşı karşıya olduğu açıklamaktadır.

Devletin, şirketlerin ve halkın korunması gerektiğini vurgulayan bu belgede tüm siber suçlara karşı nasıl önlemler alınması gerektiğine dair açıklamalara yer verilmiştir. Aynı yılın Haziran ayında stratejik liderliği sağlamak ve Birleşik Krallık Siber Güvenlik Stratejisini geliştirmek ve koordine etmek amacıyla Siber Güvenlik Ofisi kurulmuştur. 2010 yılına gelindiğinde Siber Suç Stratejisi (Cyber Crime Strategy) belgesi yayımlanmıştır. Bu belgenin amacı 2009'da ki Siber Güvenlik Strateji politikasını koordine etmek ve uygulamak, siber güvenlik ofisinin diğer bölümler ve ajanslarla birlikte hareket etmesini sağlamak, özellikle gelişen tehditlere karşı hazırlıklı olmak için Siber Suç Stratejisinin geliştirilmesini ve Siber Güvenlik Ofisi çatısı altında gelişen işlemlere uyumlu olmasını sağlamaktır.

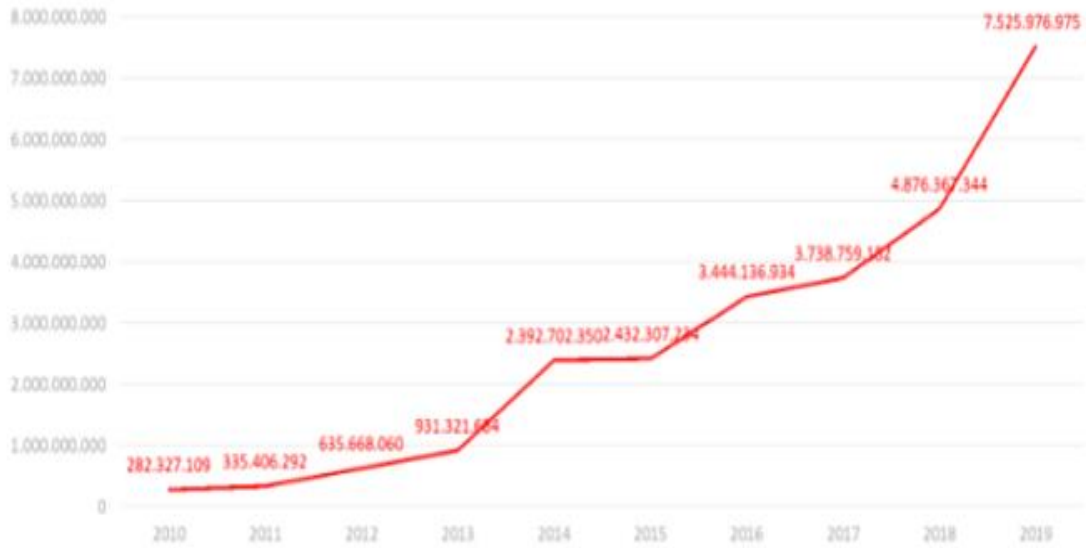
### 5.6. Singapur

Singapur'un siber güvenlik alanında başarılı ve yükselen ülkelerden biri haline gelmesinin önemli nedenlerinden biri hızlandırıcı projeler oluşturma ve küresel ortaklık projelerine katılma konusunda istikrarlı ve başarılı olmasıdır. Uluslararası ortaklıklarla programlara katılmak, Block71 (ICE71) ve erken aşama girişim fonu programlarını sürdürmek ve sahada düzenli olarak gösteri günleri düzenlemek, siber güvenlik alanında girişimcilik ekosistemine katkıda bulunan ülke tarafından yürütülen önemli faaliyetlerden biridir.

Bu faaliyetler dijital verilere de yansımaktadır. 2018'in sonu itibariyle, Singapur'un siber güvenlik endüstrisinin net varlıkları 500 milyon ABD dolarıydı. 2022 yılına kadar, Singapur'un siber güvenlik endüstrisinin beklenen değeri 1,1 milyar ABD dolarıdır. Singapur'da şu anda 105 siber güvenlik şirketi bulunmaktadır.

**Şekil 5.**

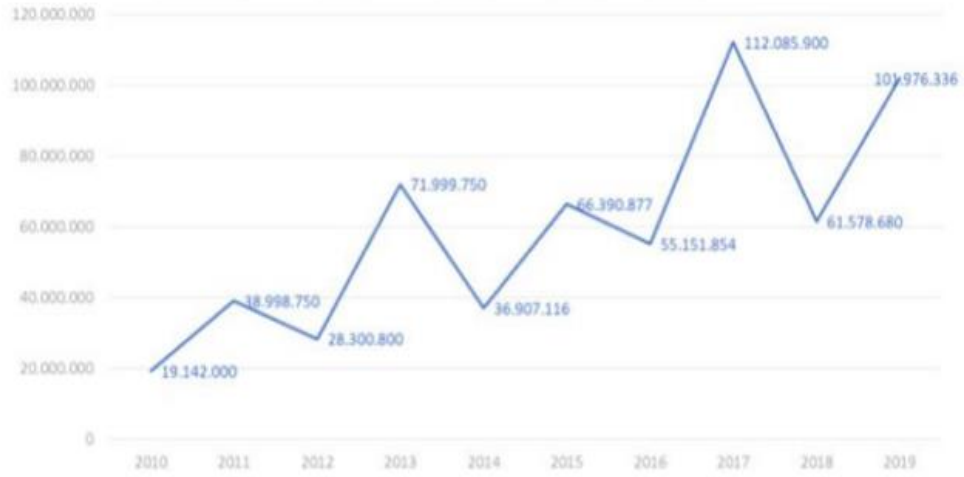
*Siber güvenlik girişimcilerine yapılan küresel yatırım*




Crunchbase verilerine göre siber güvenlik girişimcilerine yapılan küresel yatırım son 10 yılda katlanarak artmıştır (Şekil 5).

**Şekil 6.**

*Türkiye siber güvenlik alanındaki girişimcilere yapılmış olan yatırım*




Türkiye'de de 2017 yılından bu yana son 10 yılda siber güvenlik alanındaki girişimcilere yapılan yatırımların sayısında kendi içinde sıçramalar olduğu görülse de bu oran dünya ölçeğine kıyasla oldukça düşüktür (Şekil 6).

# 6. DÜNYADA YAŞANMIŞ SİBER SALDIRILAR

Siber Saldırıların Ciddiyetini Tam Olarak kavrayabilmek ve Korunmak İçin daha çok Çaba Göstermek için Aşağıda Dünyada Yaşanmış Siber Saldırılara Birkaç Örnek Verilmiştir.

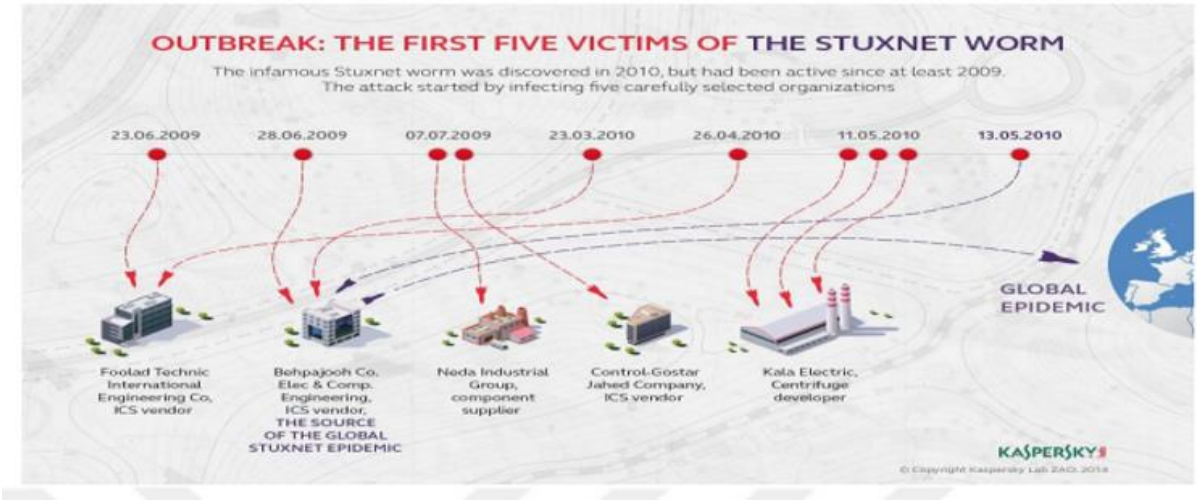
## 6.1. Stuxnet Saldırısı

İnsanlık tarihinde sabotaj amacıyla geliştirilen ve İran'ın nükleer santrallerini hedef alan ilk süper bilgisayar virüsü olan Stuxnet 21. yüzyılın en tehlikeli siber saldırıları arasında yer almıştır. Kötü amaçlı yazılım programlarının arasında en gelişmiş ve çözümlenmesi zor bir versiyon olan Stuxnet adındaki solucan (worm) virüsü 2010 yılında keşfedilmiştir. En karakteristik özelliği kendi kendini kopyalayabilmesi olan virüsün, içine yerleştiği ağı işlevsiz hale getirene kadar yayılabilmesi onun bir tür yazılım bombası olarak faaliyet göstermesine yol açmaktadır. Ayrıca uzaktaki bir bilgisayar ağını hedef alarak yapılan ilk büyük saldırı olmasıyla da büyük bir öneme sahiptir. Stuxnet saldırısı sonucunda siber terör düzeni ve kurallarında köklü değişimler yaşanarak süper bilgisayar virüsleri çağı başlamıştır.

Stuxnet en dar anlamıyla bir bilgisayar virüsü olarak tanımlansa da esasen uzaktaki bilgisayar sistemlerine sızması ve bunları istediği gibi yönlendirebilmesi amacıyla kodlanmış son derece karmaşık bir bilgisayar programıdır.

Kullanılan virüsün ile aynı adı taşıyan 'Stuxnet saldırısı' 2009 yılında ABD tarafından İran'da yer alan Natanz nükleer yakıt zenginleştirme tesislerini hedef almıştır. Gerçekleştirilen bu saldırılar neticesinde tesisteki çalışmaların uzaktan takibini sağlayan santrifüjlerden yaklaşık bin tanesi hasara uğratılarak faaliyetlerin durdurulmasına yol açmıştır. Uranyum zenginleştirme amacıyla kurulan bu tesisin yaklaşık beşte biri işlevsiz hale gelmiştir. Santrifüjleri yöneten SCADA sisteminin işleyişinin zarar görmesi büyük ölçüde verim kaybına yol açmıştır. Onarılması uzun zaman alacak bir tahribata neden olan bu olayın kısa vadeli de olsa fiziksel bir tahribata yol açtığı görülmektedir (Gümüşbaş, 2016: 185). Aşağıda Stuxnet virüsünün tahribat yarattığı ilk beş alan Şekil 7'de gösterilmiştir (Kaspersky.com).

*Stuxnet virüsünün tahribat yarattığı ilk beş alan*




Virüsün kaynağını tespit etmek amacıyla Kaspersky ve Amerikan yazılım şirketi Microsoft tarafından birlikte yürütülen araştırmaya ilerleyen süreçte Amerikan bilişim güvenlik şirketi Symantec de katılmıştır.

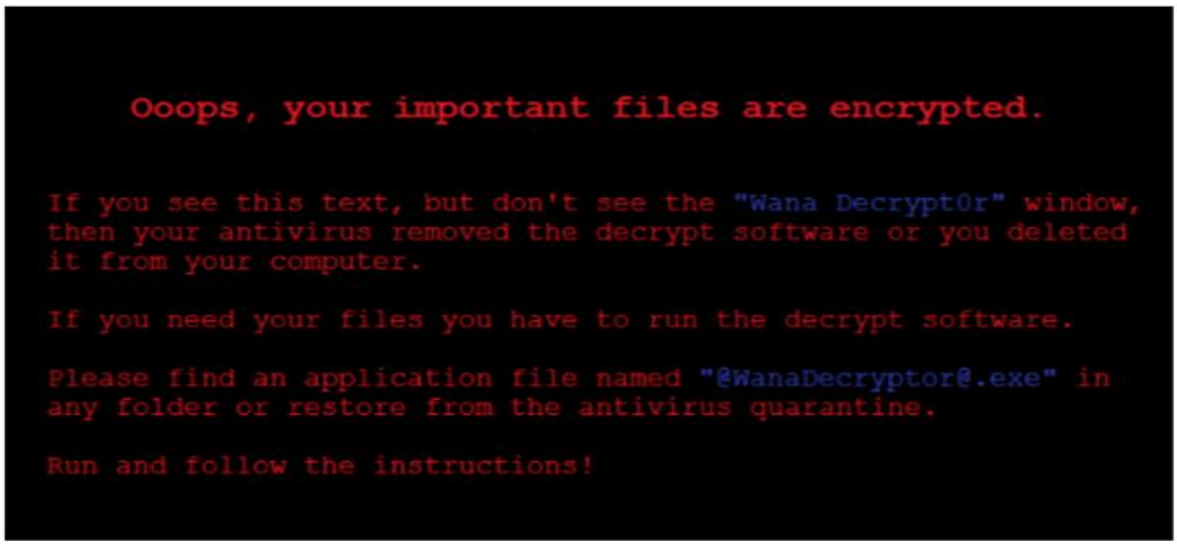
Araştırma neticesinde İran'da bulunan Natanz adlı nükleer yakıt zenginleştirme tesislerini hedef alan virüs saldırısı ilki 22 Haziran 2009'da yerel saatle 16.30'da, ikincisi ise 7 Temmuz 2009 tarihinde yerel saatle 17.00' de olmak üzere iki farklı tarihte meydana gerçekleştirilmiştir (wired.com).

Bu konuda İran Sivil Savunma Kurumu'nın yaptığı açıklamaya göre Stuxnet virüsünün nükleer santraller hakkındaki topladığı bilgileri nereye ve kimlere rapor edildiğinin takibinin yapılarak ABD'nin Texas eyaletinde olduğunun tespit edildiği belirtilmiştir. Bu saldırının arka planında ABD ve İsrail'in bulunduğu öne sürülse de kanıtlanabilirlik ölçütlerini sağlayacak bir bulguya rastlanılmamıştır.

### 6.2. WannaCry

İlk 11 Mayıs 2017'de Rusya'nın Cheboksary kentinde ortaya çıkan WannaCry fidye yazılımı buradan tüm dünyaya yayılmıştır. İzlenimleri Rusya Federasyonu, ABD, İran, İspanya, Brezilya, Çin, Romanya, İtalya, Kazakistan, Tacikistan, Lüksemburg Vietnam, Hindistan, Ukrayna ve Tayvan'ında olduğu 120 farklı ülkede görülen yazılımın bu ülkelerde 230.000'den daha fazla bilgisayara 54 erişerek 28 farklı dilde fidye talep eden büyük çaplı bir siber saldırı olduğu kabul edilmiştir.

*WannaCry'ın etki altına aldığı bilgisayar uyarısı*




Fidye yazılımlar (ransomware) eriştikleri sistemlerde kurbanın ekranına bir bildiri göndererek kullanıcı dosyalarını şifreledikleri ve sınırlandırdıkları sistemin kullanılmasının yeniden mümkün olabilmesi için kurbanın belli bir miktar fidye ödenmesi gerektiğini bildirmektedir. Günümüze kadar fidye yazılımları için geleneksel para birimleri ile ödemeler kolluk kuvvetleri tarafından tespit edilebilir olması sebebiyle saldırganlar açısından ciddi bir tehdit olmuştur.

Ancak günümüzde Bitcoin vb. sanal ödeme sistemlerinin kullanılması ve yaygınlaşması ile bu ödemeler bu sistemler aracılığıyla yapıldığı için siber savunma ekipleri tarafından para akış kanallarının izlenmesi ve saldırganların tespiti zorlaşmıştır (Çelik ve Çeliktaş, 2018). WannaCry saldırısı sonucunda bilgisayar ekranında beliren ve mağdur kişiden fidye talebi görselde gösterilmiştir.

*WannaCry saldırısı sonucunda fidye talebi*

### 6.3. Mirai Botnet Saldırısı

Bilgi üretebilen ve bunu internet aracılığıyla aktarabilen bütün bilgi işlem cihazlarını, dijital ve mekanik makineleri, nesneleri, hayvanları ve hatta insanları birbirine bağlayan nesnelerin interneti teknolojisi IoT kısaltmasıyla bilinmektedir. IoT'nin en belirgin özelliği nesnelere eşsiz bir kimlik tanımlayarak onları kendi aralarında ve merkezi kontrol sistemleri ile insan müdahalesine ihtiyaç duyulmadan veri paylaşımı sağlayabilmesidir (Wortmann ve Flüchter, 2015). Japonca kökenli olup gelecek anlamına gelen "Mirai" adlı zararlı yazılımın ana hedefi; DVR, IP tabanlı kameralar, uydu alıcıları, ev tipi küçük yönlendirici cihazlar (ADSL router modem) gibi internete bağlı aygıtların güvenlik önlemleri alınmadan üretilmesi, varsayılan kullanıcı adları ve parolalar aracılığıyla ağlara bağlanması ve bu aygıtları kullanan bireylerin büyük bir kısmının yeterli güvenliği sağlamak konusunda eksik bilgiye sahip olmasından dolayı bu cihazlardır.

Bu yazılım, içerisinde sahip olduğu 60 farklı kullanıcı adı ve parola ikilisini Telnet protokolünü desteklemekte olan IoT cihazları üzerinde deneyerek deneyerek bu cihazlara giriş yapmayı amaçlamaktadır. Botnet'in sistemleri kontrol altına almak için kullandığı güvenlik açığı '' Zayıf veya varsayılan kullanıcı adı ve parola''dır. Botnet saldırganların kullandığı yazılımların birbiriyle bağlantılı olan birden fazla cihaza yayarak onlara görev vermeye yarar.

### 6.4. Estonya Siber Saldırısı

Estonya siber saldırısını analiz edebilmek için ülkenin Rusya ile tarihsel birlikteliğini göz önünde bulundurmak gerekir. İkinci Dünya Savaşı sırasında Estonya, Sovyetler Birliği ile birlikte, Almanya'ya karşı savaşmış ve savaş sonunda da Estonya'nın Nazi istilasından korunmak için Sovyetler Birliği'ne karşı verdiği mücadeleyi sembolize eden "Bronz Asker Anıtı" dikilmiştir. 26 Nisan 2007'de Estonya'nın heykelin kaldırılması üzerine Rus hükümeti tarafından kınanması üzerine ülkede ayaklanmalar çıkmıştır.

Ülke nüfusunun yaklaşık %25 ini oluşturan Rus kökenli vatandaşlar, ülkenin çeşitli yerlerinde protesto yapmaya başladılar. Özellikle başkent Tallinn'de ayaklanmalar ve yağmalamalar ortaya çıkmıştır. Estonya'daki bu tepkiler Rus azınlıkla sınırlı kalmamış,

Moskova da, anıtın kaldırılmasını Estonya'yı Nazi işgalinden kurtarmaya çalışırken ölen Sovyet askerlerine hakaret olarak yorumlanmıştır. Kızıl Ordu anıtı, birçok Estonyalı için baskıcı Sovyet dönemini sembolize etmektedir. Estonya'daki Rus azınlık ve Rusya ise anıtın faşizme karşı mücadeleyi temsil ettiğini ileri sürmekteydi.

# 7. GEREÇ ve YÖNTEM

## 7.1. Veri Toplanması ve Soruların Hazırlanması

Adnan Menderes Üniversitesi Öğrencilerinin Katılacağı Anket yoluyla Öğrencilerin Siber Güvenlik Bilgi Düzeylerinin Ölçülmesi amaçlanmıştır.Öğrencilerin Hepsi Söke İşletme Fakültesinden Katılmıştır. Seçilen Soruların Konu Başlıkları ve Önem Puanları aşağıdaki tabloda verilmiştir.

Tablo 1. Konu Başlıkları Ve Önem Puanları

| KONULAR | |
|---|---|
| Temel Güvenlik | 10/10 |
| Şifre Oluşturma | 10/10 |
| Oltalama | 9/10 |
| SQL İnjection | 5/10 |
| Kötü Amaçlı Yazılım (Virüs) | 7/10 |
| Kriptografi | 2/10 |
| Sosyal Mühendislik | 10/10 |
| | |

### 7.1.1. Puanlama Sistemi

10 soru içinden Önem Sırasına Göre Doğru Bilinen Soru Başına 10 Puan. Farkındalık Eğitimi için yanlış bilinen Konular Üzerinde Daha Fazla Durulması Amaçlanmıştır.

## 7.2 Hazırlanan Sorular

| SORULAR VE CEVAPLAR | |
|---|---|
| Aşağıda verilen parola örneklerinden hangisi diğerlerine göre daha güçlü paroladır? | benBirsifreyim.! |
| Aşağıdakilerden hangisi zararlı yazılımlardan korunma yöntemlerinden biri değildir? | Her Linkten Dosya İndirmek |
| Virüsün Tam tanımı Aşağıdakilerden hangisinde tam olarak doğru verilmiştir? | Sisteme İzinsiz giren, Dosyalara Erişebilen, Dosyaları Değiştirebilen ve Kullanılmaz hale getirebilen Yazılımlar. |
| Güçlü Parola oluştururken aşağıda verilen kriterlerin hangisine dikkat edilmez? | Doğum tarihi gibi özel bilgilerin kullanılmasına. |
| Hangisi bir virüs türü değildir? | Eset Nod32 |
| Aşağıdakilerden hangisi Bir Kriptografi terimidir? | Şifreleme |
| Aşağıdakilerden hangisi Hacker Türlerinden değildir? | Sarı Şapkalı Hacker |
| Bir bilgisayar korsanı kullanıcıları kilitler ve kişisel bilgisayar dosyalarını ve verilerini şifreler ve saldırganı ödemeyi kabul edene kadar rehin tutar. Bu uygulamaya ne denir? | RANSOMWARE |
| Aşağıdakilerden hangisi zararlı yazılımlardan korunma yöntemlerinden biri değildir? | Çok kişinin kullandığı bilgisayarda, bankacılık işlemlerini yapmak |
| Aşağıdakilerden hangisi Sosyal Mühendislerde bulunan genel özelliklerden biridir? | İkna Kabiliyeti ve Aldatma Sanatında Ustadırlar. |

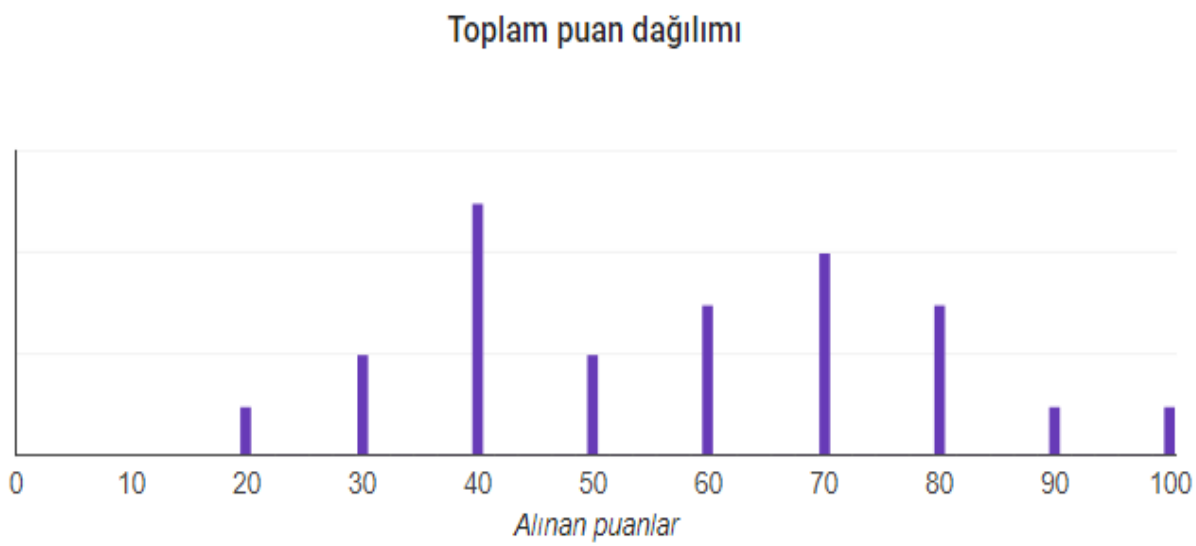
# 8. BULGULAR

## 8.1. Anket Sonuçları Analizi

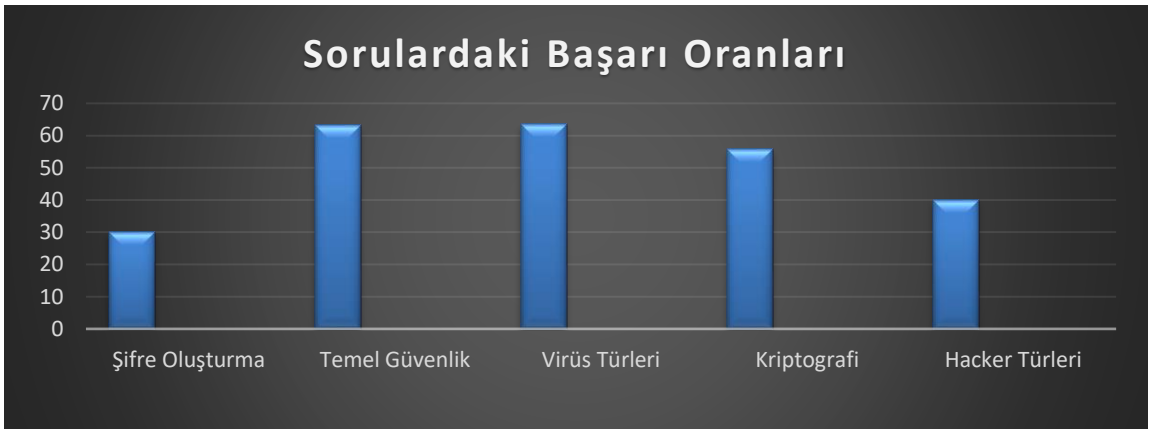
Anket çok şaşırtıcı şekilde sonuçlandı. Örnek vermek gerekirse Şifrelerimizi oluşturma Konusunda Gerçekten Büyük Problem Yaşıyoruz. En çok yanlış yapılan soru Şifre Oluşturma Sorusu oldu. Ardından ise, Hacker türleri geliyor. Özellikle Sosyal Mühendislerin Kimler olabileceğini ve onların özellikleri hakkında büyük bilgi eksikliği bulunmakta.

## 8.2. İstatistiksel Analizler

Aşağıdaki Grafikte “Toplam Puan Dağılımı” Verilmiştir.



Aşağıda “Sorulardaki Başarı Oranları” Verilmiştir.




Ankete Katılan ilk 100 Kişi Baz alındığında Bunlardan %70’i Şifre Oluşturmada %66’sı ise Hacker Türleri ve Sosyal Mühendisler Konusunda Yanlış Cevap verdi. Diğer Konularda ise Başarı oranı %50’nin biraz üzerindeydi.

Farkındalık Eğitimi Yanlış Bilinen veya Hiç bilinmeyen konular Üzerine odaklanmak olduğundan Eğitimde Bu iki konu üzerine yoğunlaşılacaktır.

# 9. FARKINDALIK EĞİTİMİ

Yaptığımız Ankette Üniversite Öğrencileri olarak en şaşırtıcı eksiklik Şifre Oluşturma konusu oldu. Bu yüzden Eğitime Şifre Oluşturma Konusuyla Başlanacaktır. Ardından Sosyal Mühendisler Hakkında Bilgiler Verilecektir.

## 9.1. Şifreleme – Tanımı ve Anlamı

Siber güvenlikte şifreleme, verilerin okunabilir bir biçimden şifreli bir biçime dönüştürülmesidir. Şifrelenmiş veriler yalnızca şifresi çözüldükten sonra okunabilir veya işlenebilir.

Şifreleme, veri güvenliğinin temel yapı taşıdır. Bu, bir bilgisayar sisteminin bilgilerinin çalınmamasını ve kötü amaçlarla kullanmak isteyen biri tarafından okunamamasını sağlamanın en basit ve en etkili yoludur.

Veri güvenliği şifrelemesi, bireysel kullanıcılar ve büyük şirketler tarafından, bir tarayıcı ile bir sunucu arasında gönderilen kullanıcı bilgilerini korumak için yaygın olarak kullanılmaktadır. Bu bilgiler, ödeme verilerinden kişisel bilgilere kadar her şeyi içerebilir. Şifreleme algoritması veya şifre olarak da bilinen veri şifreleme yazılımı, teorik olarak yalnızca büyük miktarda bilgi işlem gücüyle çözülebilecek bir şifreleme şeması geliştirmek için kullanılır.

## 9.2. Şifreleme nasıl çalışır?

Bilgiler veya veriler internet üzerinden paylaşıldığında, genel internetin bir parçasını oluşturan dünya çapında bir dizi ağ cihazı üzerinden geçer. Veriler genel internet üzerinde dolaşırken, korsanlar tarafından ele geçirilebilme veya çalınabilme ihtimali söz konusudur. Bunu önlemek için kullanıcılar, verilerin veya bilgilerin güvenli bir şekilde aktarılmasını sağlamak için belirli yazılımlar veya donanımlar kullanabilir. Ağ güvenliğinde bu işlemler şifreleme olarak bilinir.

Şifreleme, insan tarafından okunabilen düz metinleri şifreli metin olarak bilinen anlaşılmaz metinlere dönüştürmektir. Bu, okunaklı verileri alıp rastgele bir görünüme bürünecek şekilde değiştirmek anlamına gelir. Şifrelemede, gönderen ve alıcı tarafından kabul edilen bir dizi matematiksel değer, yani bir şifreleme anahtarı kullanılır. Alıcı, verilerin şifresini çözmek için bu anahtarı kullanır, böylece veriler tekrar okunabilir düz metne dönüştürülür.

Şifreleme anahtarı ne kadar karmaşık olursa şifreleme o kadar güvenli olur; çünkü üçüncü tarafların kaba kuvvet saldırıları (yani doğru kombinasyon tahmin edilene kadar rastgele numaraları deneme) yoluyla şifreleri çözme olasılığı daha düşüktür.
Şifreleme, parolaları korumak için de kullanılır. Parola şifreleme yöntemleri parolanızı şifreler ve korsanlar tarafından okuyamayacak bir hale getirir.

### 9.3. En Yaygın Şifreleme Teknikleri

En yaygın iki şifreleme yöntemi simetrik ve asimetrik şifrelemedir. Bu adlar, şifreleme ve şifre çözme için aynı anahtarın kullanılıp kullanılmadığını ifade etmek için kullanılır:

**Simetrik şifreleme anahtarları**: Bu, özel anahtar şifrelemesi olarak da bilinir. Şifreleme için kullanılan anahtar, şifre çözmek için kullanılan anahtar ile aynıdır. Bu, bireysel kullanıcılar ve kapalı sistemler için en iyi sonucu sağlar. Aksi takdirde, anahtarın alıcıya gönderilmesi gerekir. Bu durum, anahtarın bilgisayar korsanları gibi üçüncü taraflarca ele geçirilme riskini artırır. Bu yöntem asimetrik yönteme göre daha hızlıdır.

**Asimetrik şifreleme anahtarları**: Bu yöntemde, matematiksel olarak birbirine bağlanan iki farklı anahtar (genel ve özel) kullanılır. Anahtarlar, birbiriyle eşleştirilmiş ancak birbirinin aynı olmayan büyük sayılardır, bu nedenle asimetrik terimi kullanılır. Özel anahtar, sahip tarafından gizli tutulur ve genel anahtar ya yetkili alıcılar arasında paylaşılır ya da herkese açık olarak sunulur.
Alıcının genel anahtarıyla şifrelenen verilerin şifresi, sadece karşılık gelen özel anahtarla çözülebilir.

### 9.4. Şifreleme Algoritmaları Örnekleri

Şifreleme algoritmaları, verileri şifreli metne dönüştürmek için kullanılır. Bir algoritma, verileri tahmin edilebilir bir şekilde değiştirmek için şifreleme anahtarını kullanır. Sonrasında

şifrelenmiş veriler rastgele görünecek olsa da şifre çözme anahtarı ile daha tekrar düz metne dönüştürülmeleri mümkün olur.
Farklı amaçlara göre tasarlanmış birçok farklı şifreleme algoritması türü vardır. Eski algoritmalar güvensiz hale geldikçe yenileri geliştirilir. En iyi bilinen şifreleme algoritmalarından bazıları şunlardır:

**DES şifreleme**

DES, Veri Şifreleme Standardı anlamına gelir. Bu, günümüzdeki kullanımlara uygun olmayan, artık modası geçmiş bir simetrik şifreleme algoritmasıdır. Bu nedenle yerini diğer şifreleme algoritmalarına bırakmıştır.

**3DES algoritması**

3DES, Üçlü Veri Şifreleme Standardı anlamına gelir. Bu bir simetrik anahtar algoritmasıdır ve şifreleme işlemi sırasında veriler orijinal DES algoritmasından üç kez geçtiği için "üçlü" olarak ifade edilir. Üçlü DES de yavaş yavaş gündemden düşse de, hala finansal hizmetler ve diğer endüstriler için güvenilir bir donanım şifreleme çözümü sunmayı başarıyor.

**AES şifreleme**

AES, Gelişmiş Şifreleme Standardı anlamına gelir ve orijinal DES algoritmasını güncellemek üzere geliştirilmiştir. AES algoritmasının yaygın uygulamaları arasında Signal veya WhatsApp gibi mesajlaşma uygulamaları ve dosya arşivleme programı WinZip sayılabilir.

**RSA şifreleme**

RSA, ilk halka açık asimetrik şifreleme algoritmasıdır. RSA, anahtar uzunluğu nedeniyle popülerdir ve bu nedenle güvenli veri aktarımı için yaygın olarak kullanılmaktadır. RSA kısaltması, bu algoritmayı ilk tanımlayan matematikçilerin soyadları olan Rivest, Shamir ve Adleman'ın baş harflerinden oluşur. RSA, çift anahtar kullandığı için asimetrik bir algoritma olarak kabul edilir.

**Twofish şifreleme**

Hem donanım hem de yazılımda kullanılan Twofish, türünün en hızlılarından biri olarak kabul edilir. Twofish patentli olmadığından isteyen herkes tarafından kullanılabilir. Bu sayede

PhotoEncrypt, GPG gibi şifreleme programlarında ve popüler açık kaynaklı yazılım TrueCrypt'te bulunabilir.

### RC4 şifreleme

Kablosuz yönlendiricilerde yaygın olarak kullanılan şifreleme protokolleri olan WEP ve WPA'da kullanılır.

Asimetrik şifreleme örnekleri arasında RSA ve DSA verilebilir. RC4 ve DES ise simetrik şifreleme örnekleridir. Şifreleme algoritmalarının yanı sıra Ortak Kriterler (CC) vardır:

- Bu bir şifreleme standardı değil ancak ürün güvenlik iddialarını doğrulamaya yönelik bir dizi uluslararası kılavuzdur.
- CC kılavuzları, güvenlik ürünlerinin satıcıdan bağımsız olarak üçüncü taraflarca denetlenmesini sağlamak üzere oluşturulmuştur.
- İncelenen ürünler tedarikçiler tarafından gönüllü olarak gönderilir ve işlevlerin tümü veya bazıları incelenir.
- Bir ürün değerlendirildiğinde, ürün türüne göre belirlenmiş standartlara göre özellikleri test edilir.
- Başlangıçta şifreleme Ortak Kriterlerin kapsamı dışında olmasına rağmen, artık güvenlik standartlarına giderek daha sık dahil edilir hale gelmiştir.

### Aktarılan ve durağan verilerde şifreleme: Bu ikisi arasındaki fark nedir?

Veri şifreleme yazılımı ve bulut veri şifreleme gibi veri şifreleme çözümleri, genellikle aktarılan verilerde mi yoksa durağan verilerde mi kullanılmak üzere tasalandıklarına bağlı olarak kategorize edilir:

### Aktarılan verilerde şifreleme

Veriler, özel ağlarda veya internet üzerindeki cihazlar arasında yer değiştirdiğinde, aktarılan veriler olarak kabul edilir. Aktarım sırasında, aktarım öncesi şifre çözme ihtiyacı ve aktarım yönteminin kendisiyle ilgili güvenlik açıkları nedeniyle veriler daha fazla risk altındadır. Aktarım sırasında verilerin uçtan uca şifreleme adı verilen yöntemle şifrelenmesi, verilerin ele geçilmesi durumunda bile gizliliğinin korunmasını sağlar.

### Durağan verilerde şifreleme

Veriler, bir depolama aygıtına olduğunda ve etkin olarak kullanılmadığında veya aktarılmadığında, durağan veriler olarak kabul edilir. Cihaz güvenlik özellikleri erişimi

kısıtladığından dolayı, durağan veriler genellikle aktarımdaki verilere göre daha güvendedir ancak yine de dokunulmaz değildir. Ayrıca bu tür veriler genellikle daha değerli bilgiler içerir ve bu nedenle hırsızlar için daha cazip bir hedef teşkil eder.
Durağan verilerin şifrelenmesi, kaybolan veya çalınan cihazlar, yanlışlıkla paylaşılan şifreler veya yanlışlıkla verilen izinler nedeniyle ortaya çıkan veri hırsızlığı ile elde edilebilecek fırsatları azaltır. Bilgilere erişmek için gereken süreyi artırır ve veri sahibinin veri kaybını, fidye yazılımı saldırılarını, uzaktan silinen verileri veya değiştirilen kimlik bilgilerini tespit etmesi için değerli bir zaman sağlar.
Durağan verileri korumanın bir yolu da TDE'dir. Bu, Saydam Veri Şifrelemesi anlamına gelir ve Microsoft, Oracle ve IBM tarafından veritabanı dosyalarını şifrelemek için kullanılan bir teknolojidir. TDE, hem sabit sürücüdeki hem de yedekleme ortamındaki veritabanlarını şifreleyerek durağan verileri korur. TDE, aktarılan verileri korumaz.

**Uçtan uca şifrelenmiş veriler nedir?**

Uçtan uca şifreleme, veri şifrelemeyle ilgili sık duyduğunuz bir terimdir. Bu, yalnızca iki kullanıcının iletişim kurduğu ve her ikisinin de görüşmenin şifresini çözebildiği anahtara sahip olduğu sistemleri ifade eder. Örneğin uçtan uca şifrelenmiş verilere erişim sağlayamayan servis sağlayıcısı bile bu kapsamın içine girer.
Uçtan uca şifrelenmiş verilerin sıfırlanması mümkündür. Örneğin, bir iPhone'da, şifrenizi unutursanız cihazınıza yeniden erişmek için sıfırlama gerekebilir. Bunu yapmanız durumunda, önceden şifrelenmiş yedekleme dosyalarından hiçbirini kullanamazsınız. Ancak iOS cihazınızı tekrar yedeklemek ve yedeklenen verileriniz için yeni bir şifre ayarlamak için iTunes'u kullanabilirsiniz.

Şifrelemenin altı temel avantajı;

**Şifreleme, veri bütünlüğünün korumasına yardımcı olur**
Bilgisayar korsanları yalnızca bilgileri çalmakla kalmaz, aynı zamanda dolandırıcılık yapmak için verileri değiştirebilir. Yetenekli korsanların şifrelenmiş verileri değiştirebilmesi mümkün olsa da, veri alıcıları bozulmayı tespit ederek duruma hızlı bir yanıt verebilir.

**Şifreleme, kuruluşların düzenlemelere uymasına yardımcı olur**

Finansal hizmetler veya sağlık hizmeti sağlayıcıları gibi birçok sektör, tüketici verilerinin nasıl kullanıldığı ve depolandığı konusunda katı düzenlemelere tabidir. Şifreleme, kuruluşların bu standartları karşılamasına ve uyumluluğu sağlamasına yardımcı olur.

**Şifreleme, tüm cihazlarda verileri korur**

Çoğumuz günlük yaşamlarımızda birden fazla cihaz kullanıyoruz ve cihazdan cihaza veri aktarımı riskleri de beraberinde getiriyor. Şifreleme teknolojisi, cihazlar arasında aktarım sırasında bile verilerin korunmasına yardımcı olur. Gelişmiş kimlik doğrulama gibi ek güvenlik önlemleri, yetkisiz kullanıcıların engellenmesine yardımcı olur.

**Şifreleme, veriler bulut depolama alanına taşınırken faydalıdır**

Giderek daha fazla kullanıcı ve kuruluş verilerini bulutta saklıyor, bu da bulut güvenliğinin önemini ortaya koyuyor. Şifrelenmiş depolama, bu verilerin gizliliğini korunmasına yardımcı olur. Kullanıcılar, verilerin aktarım sırasında, kullanım esnasında ve saklama süresince şifrelenmesini sağlamalıdır.

**Şifreleme, kuruluşların ofislerini korumalarına yardımcı olur**

Çoğu kuruluş, özellikle de pandemi sonrasında uzaktan çalışma yöntemini sıklıkla kullanıyor. Bu durumda verilere birden fazla farklı konumdan erişim sağlandığından, siber güvenlik riskleri söz konusu olabilir. Şifreleme, hırsızlığa veya verilerin kazara kaybolmasına karşı koruma sağlanmasına yardımcı olur.

**Veri şifreleme, fikri mülkiyetleri korur.**

Dijital hak yönetimi sistemleri, ters mühendisliği ve telif hakkıyla korunan materyallerin izinsiz kullanımını veya çoğalmasını önlemek için fikri mülkiyet haklarına tabi verileri (şarkılar veya yazılımlar gibi) durağan haldeyken de şifreler.

**Şifrelemenin kullanım alanları**

1. ATM'leri her kullandığınızda veya bir akıllı telefonla çevrimiçi bir şey satın aldığınızda, aktarılan bilgileri korumak için şifreleme kullanılır.
2. Cihazları güvenceye alma, örneğin dizüstü bilgisayar için şifreleme.
3. Çoğu yasal web sitesi, site üzerinden yapılan veri alışverişlerinde, bir şifreleme biçimi olan "güvenli yuva katmanını" (SSL) kullanır. Bu, aktarım sırasında bu verilere saldırganlar tarafından erişim sağlanmasını engeller. Çevrimiçi olarak güvenli ve şifrelenmiş işlemler gerçekleştirdiğinizden emin olmak için URL çubuğundaki kilit simgesine ve "https://" ibaresindeki "s" harfine özellikle dikkat edin.
4. WhatsApp mesajlarınız da şifrelenir, ayrıca telefonunuzda şifrelenmiş bir klasöre sahip olabilirsiniz.

5. E-postalarınız da OpenPGP gibi protokoller kullanılarak şifrelenebilir.
6. VPN'ler – Sanal Özel Ağlar şifreleme kullanır ve bulutta sakladığınız her şey şifrelenir. Tüm sabit sürücünüzü şifreleyebilir ve hatta şifreli sesli aramalar yapabilirsiniz.
7. Şifrelemede, bilgilerin bütünlüğünü ve doğruluğunu kanıtlamak için dijital imza kullanılır. Şifreleme, dijital hak yönetimi ve kopya korumasının ayrılmaz bir parçasıdır.
8. Şifreleme, verileri silmek için kullanılabilir. Silinen bilgiler bazen veri kurtarma araçları kullanılarak geri getirilebildiğinden, önce verileri şifreler ve anahtarı atarsanız kurtarılabilecek tek şey şifreli metinler olabilir, bu durumda orijinal verilere erişmek asla mümkün olmaz.

### 9.5. Güçlü şifre nasıl olmalı?

Genellikle isim, doğum tarihi, plaka numarası, telefon alan kodu, sadece harf veya sadece sayı kullanılması vb. gibi basit ve tahmin edilebilirliği yüksek olan şifre kombinasyonları insanlar tarafından sıklıkla kullanılmaktadır. Güçlü bir şifre oluşturmak için öncelikle dikkat edilmesi gerekenler;

- En az 8 karakterin kullanılmasıdır.
- Şifreniz harf, rakam ve mutlaka özel karakter içermelidir.
- Küçük ve büyük harf kullanılmalıdır.
- Şifre kişisel bilgi, sıklıkla kullanılan kelime, kolay tahmin edilebilir söz öbeği kullanılmamalıdır.
- Tüm hesaplar için ayrı ayrı şifreler belirlenmelidir.

Ancak bazı durumlarda şifrelerin güçlü olması ve/veya her bir hesap için farklı şifre kullanılması siber güvenlik için yeterli olmamaktadır. Bu nedenle parola güvenliğinde özellikle “çok faktörlü doğrulama” ve “iki faktörlü kimlik doğrulaması” teknolojilerinden yararlanılması gerekmektedir.

İki faktörlü kimlik doğrulama işlemi iki aşamalı bir süreç olarak tasarlanmaktadır. Birinci aşamadan kullanıcının zaten bildiği şifre kullanılır. İkinci aşamada ise, şifrematik tarafından üretilen tek kullanımlık şifreyle kimlik doğrulaması yapılması istenmektedir. Çok yönlü kimlik doğrulama sisteminde ise, parola ve şifrematik ile tek kullanımlık kimlik doğrulama kodlarının yanı sıra parmak izi gibi biyometrik verilerde kullanılmaktadır.

**Türkiye'de en fazla kullanılan şifreler**

- 123987456
- q1w2e3r4
- 963qaz
- istanbul24
- 06ankara
- 3we45r
- qazxsw
- waesrd
- 951753
- password
- parola
- sanene
- bjk1903
- 19921992
- 987oıu
- 123456789
- cimbom
- fenerbahce
- 112233
- 968574.

## 9.6. Sosyal Mühendislik

Siber güvenliği ciddi anlamda tehdit eden ve güvenlik önlemlerinin aşılmasını kolaylaştıran en önemli unsurların başında insan faktörü gelmektedir. Sosyal mühendislikte de teknik altyapılar ve sistemler yerine insanların zafiyetleri kötüye kullanılmaktadır.

*"Zincir en zayıf halkası kadar güçlüdür. Burada ise en zayıf halka insandır."*

Sosyal mühendislik, saldırganın istediği şekilde davranmanızı sağlayan psikolojik bir saldırı türüdür. İnsanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır. Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir. İnsanlar kandırılma ihtimalinin çok düşük olduğunu düşünür. Bu ortak inancın farkında olan saldırganlar, isteklerini çok akıllıca sunarak hiç kuşku uyandırmadan kurbanların güvenini sömürürler.

Aldatmak, kandırmak, dolandırmak gibi kavramlar binlerce yıldır var olmuş kavramlardır. Ancak saldırganlar bu tekniği dijital ortamda kullanmanın da son derece etkili olduğunu

keşfetmiştir. Bu tekniğin nasıl kullanıldığını anlamak için günümüzde yaygın olan örneklerine bakmakta yarar vardır.


Kendilerini “polis”, “asker”, “savcı” olarak tanıtanlar “ Ödül Kazandınız” gibi mesajlar göndererek insanlardan bilgi ya da para talep edenler
Sosyal Mühendislik; basit tarifiyle dolandırıcılığa benzese de, genelde bilgi sızdırmak veya bir bilişim sistemine sızmak için kullanılabilen bir yöntemdir. Bu yöntemde genel olarak saldırgan mağdur ile yüz yüze gelmez. Kötüye kullanılan unsur ise sistem zafiyetleri değil insan zafiyetleridir.

Zafiyetlerden yola çıkarak örneklendirmek gerekirse, kurumların ya da kişilerin çöplerinde bulunabilecek imha edilmemiş dokümanlar üzerinde bulunan ve geçerliliğini yitirmemiş bilgiler sayesinde kurumlar ve kişiler hakkında önemli bilgilere ulaşılabileceğinden bahsedilebilir.

- Bilginiz başkalarının eline geçebilir.
- Bağlı olduğunuz kurum veya kuruluşun onuru, toplumdaki imajı zarar görebilir.
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir.
- Önemli verilere erişim engellenebilir, parasal kayıplar ve vakit kaybı yaşanabilir.

**Sosyal Mühendislik Teknikleri**

- Omuz Sörfü
- Çöp Karıştırma
- Truva Atları
- Rol Yapma
- Oltalama
- Tersine Sosyal Mühendislik

**Sosyal Mühendislik Sızma Hedefleri**

- Sistemi Ele Geçirme
- Kritik Bilgilere Erişim
- Hedef Sistemlere Erişim Sağlama
- Yönetici Hakkı Elde Etme
- Sistemde Kalıcı Olma
- Gizlilik

**Sosyal Mühendislik Sızma Çeşitleri**

- Fiziksel Sosyal Mühendislik
- Telefon İle Sosyal Mühendislik
- Mail Yoluyla Sosyal Mühendislik

**Kendimizi Nasıl Koruruz?**

Kendinizi korumak için ilk olarak yapmanız gereken, sosyal mühendislik saldırılarının nasıl tespit edileceğini, engelleneceğini, durdurulacağını öğrenmektir.

Biri veya birilerinin sizi hedef almaya çalıştığından şüpheleniyorsanız, o kişi ile bir daha asla iletişim kurmayın. Sizinle telefon hattı üzerinden irtibat kuruyor ise telefonu kapatın. Eğer çevrimiçi sohbette iseniz bağlantınızı sonlandırın. Eğer güvenmediğiniz bir yerden gelen bir e-posta ise, eklentilerini indirmeyin ve bahse konu e-postayı silin. Eğer çalıştığınız kurum veya iş yeri ile ilgili bir saldırı olduğunu düşünüyorsanız, işyerindeki yardım masasına ya da ilgili güvenlik uzmanlarına haber verin. Bütün bu aşamalarda kaydedeceğiniz ekran görüntüleri sonraki süreçte oldukça önem arz edecektir.

**Olası Saldırıları Engellemek İçin Ne Gibi Önlemler Alınmalı?**

**Kişisel/Özel Bilgilerinizi Paylaşmayın:** Saldırganlar hakkınızda ne kadar çok bilgiye sahip olursa size o kadar kolay ulaşıp istediklerini yaptırmak için sizi yanlış yönlendirebilir. Her bilgi internet ortamında paylaşılmamalıdır. Kendinizle ilgili basit gördüğünüz paylaşımlarınız,

hayatınızın bütünü hakkında bilgi sahibi olmak amacıyla kötü niyetli kişilerce zamanla bir araya getirilebilir. Ne kadar az bilgi paylaşırsanız (forum siteleri, e-posta adresleri ya da sosyal medya siteleri) saldırıya uğrama riskiniz de o kadar az olur.

**Şifrelerinizi Paylaşmayın:** Hiçbir kurum ya da kuruluş şifrenizi sormak için sizinle iletişime geçmez. Eğer birileri size şifrenizi soruyorsa bu bir sosyal mühendislik saldırısıdır.

**Sizinle İrtibat Kuran Kişileri Sorgulayın:** Bankanızdan ya da servis sağlayıcınız gibi kuruluşlardan aranabilirsiniz. Arayan kişi hakkında herhangi bir şüpheniz varsa arayan kişinin adını ve ona ulaşabileceğiniz bir numarayı isteyerek güvenilir bir kaynaktan kuruluşa ait telefon numarasını bulabilirsiniz. (Örneğin banka hesap özetinizde yazan numaradan ya da telefon faturanızda bulunan numaralardan) Böylece bahse konu kurumu ya da şirketi aradığınızda gerçekten yetkili personel ile konuştuğunuzdan emin olabilirsiniz

**URL/Adres Kontrolü Yapın**: Oltalama saldırılarında oltaya takılmamanın en önemli unsurlarından biriside tarayıcıda bulunan adresi kontrol etmektir. Adres çubuğunda göz kaçırılan bir karakter değişikliği istenmeyen sonuçlara yol açabilir.

**Güvenilir Olmayan Kaynaklara Dikkat Edin:** Bir dosya indirmek istediğinizde güvenilir kaynaklardan ve mümkünse doğrulanmış yapımcılardan indirmelisiniz ve bilgisayarınızda düzenli olarak virüs taraması yapmalısınız.

**Kurum İçinde Periyodik Olarak Bilgi Güvenliği Testleri Yapın:** Kurum çalışanları periyodik olarak bilgi güvenliği eğitimleri almalı ve sızma testlerine tabi tutulmalıdır. Tüm bilgisayarlara antivirüs yazılımları kurulmalı, çöpe atılması gereken dokümanlar, mutlaka kırpma makinelerinden geçirilmelidir. Kuruma ziyaretçi olarak gelen kişilerden kimlik alınarak kurum çalışanları tarafından refakat edilmelidir.

*"En güvenli bilgisayar internet bağlantısı olmayan ve kapalı olandır. Ancak bir ihtimal var ki; saldırganlar ofise gidip bilgisayarı açması için birini ikna edebilir."*

# 10. ALINMASI GEREKEN ÖNLEMLER VE YAPILAN EĞİTİMLER

- Üniversiteler diğer sektörlerde görülmeyen benzersiz güvenlik sorunları ile karşı karşıyadırlar. Güvenlik, dayanıklılık ve iş sürekliliği planları hazırlarken hepimizin göz önünde bulundurması gereken etkenlerden biri siber risklerdir.

- Siber tehditlerin üniversiteler ve eğitim kurumları için kritik bir risk taşıdığı açıktır, bu nedenle yöneticilerin bunun önemini kavraması, gerekli önlemleri alması hayati önem taşımaktadır. Bilgi işlem birimleri bu potansiyel risk alanlarıyla yüzleşmeli ve siber tehditleri azaltmanın yollarını bulmalıdır.

- Dürüst ve ayrıntılı değerlendirmeler yapılabilmelidir. Kampüs ağını ve sistemlerini kullanan kişiler sistemin en zayıf halkasıdır, bu yüzden eğitilmeli ve farkındalık oluşturulmalıdır.

- Riskler analiz edilmeli ve bir bütün olarak çözümler uygulanmalıdır.

- Ağ güvenliğinde ortam, ağ araçları ve gereksinimler dikkate alınmalıdır.

- Üniversitelerin mali kaynakları sınırlı olduğundan, risk analizlerine göre, tehditlerin oluşturabileceği etkiye göre planlamalar yapılmalı, altyapılar güçlendirilmelidir.

- Güvenlik politikalarından taviz verilmemelidir. Kullanıcıların ağdan beklediği hizmet kalitesine izin verirken, verileri güvence altına alabilmelidir.

- Siber tehdit öncesi ve sonrası için bütün planlama ve düzenlemelerin yapılması gerekmektedir. Bu çalışmada konunun önemi, tehditlerin neler olduğu, zayıflıklar ele alındı.

- Bu zayıflıklara karşı ne tür önlemlerin alınabileceği konusu üzerinde duruldu.

- Siber güvenlik ancak bütün boyutlarıyla ele alındığında bir sistemde, ağda güvenlik sağlanabilir. En zayıf halka insan faktörüdür. Bundan dolayı bu çalışmada siber farkındalık eğitimi üzerinde duruldu, öneriler sunuldu.

- Siber bilincin dinamik bir süreç olduğu, bu dinamik sürece uygun eğitim modelinin seçilmesi gerektiği gösterildi. Üniversitelerin öncülüğünde siber farkındalığın bütün sektörlerde oluşması için destekleyici çalışmalar yapılmalıdır.

- Üniversiteler araştırma geliştirme merkezleri olduğu için güvenli yapıları oluştururken edindiği tecrübe ve birikimleri diğer sektörlerle de paylaşmalıdır.

- Siber farkındalığın oluşması için eğitimler düzenlemeli, sektörlerin güvenliğine katkı sunmalıdır.

# KAYNAKLAR


Manuel Castells, The Rise of the Network Society, West Sussex, Wiley-Blackwell , 2010, s. 355-406.

Roland B. Schmitt, The New Era in U.S. Export Controls. Report of a Workshop, Washington D.C., National Academy Press, 1992, s. 14. James Andrew Lewis (der.), Computer Exports and National Security: New Tools for a New Century, The CSIS Press, Washington D.C., 2001, s. 10-12.

Http://www.internetworldstats.com/stats.htm (Erişim tarihi: 11 Mart 2012).

Michel Foucault, Discipline and Punish: The Birth of the Prison, New York, Vintage Books, 1979 s. 27.

Nazlı Choucri, "Introduction: Cyber Politics in International Relations", International Political Science Review, Cilt 21(3), 2000, s. 243.

Joseph S. Nye Jr., Cyber Power, Cambridge, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010; Tim Jordan, Cyber Power: An Introduction to the Politics of Cyberspace, Londra, Routledge, 1999, s. 208.

Robert O. Keohane ve Joseph S. Nye Jr., "Power and Interdependence in the Information Age", Foreign Affairs, Cilt 7 (5), Eylül-Ekim 1998, s. 81-94.

Nye, Cyber Power; Jordan, Cyber Power, s. 208.

Cristina Carbone, "Staging the Kitchen Debate: How Splitnik Normalized in the United States", Ruth Oldenziel ve Karin Zachmann (der.), Cold War Kitchen Americanization, Technology and European Users, Cambridge, The MIT Press, 2009, s. 59-81; Ilina Kohonen, "The Space race and Soviet Utopian Thinking", The Sociological Thinking, Cilt 57 (1), Mayıs 2009, s. 114.

Columba Peoples, "Sputnik and 'skill thinking' revisited: technological determinism in American responses to the Soviet Missile Threat", Cold War History, Cilt 8(1), Şubat 2008, s.61.

National Research Council, Innovation in Information Technology, Washington D.C., The National Academies Press, 2003, s. 60.

Paul Baran, "On Distributed Communications Networks", Rand Corporation, Eylül 1962, http://www.prgs.edu/content/dam/rand/pubs/papers/2005/P2626.pdf (Erişim tarihi: 07 Haziran 2012).

Laura K. Brendan, "Arpanet: An Efficient Machine as Social Discipline", Science as Culture, Cilt 10 (1), 2001, s. 76-77.

Ulrich Beck, Risk Society Towards A New Modernity, Londra, Sage Publications, 1992, s. 29-30; Bill Durodie, "The Limitations of Risk Management", Tidsskriftet Politik, Cilt 8 (1), 2005, s. 14-21.

Wendy Hui Kyong Chun, Control and Freedom: Power and Paranoia in the Age of Fiber Optics, Cambridge, The MIT Press, 2006, s. 247-297.

Charles L. Glaser, "Deterrence of Cyber Attack and US National Security", George Washington

University Cyber Security Policy and Research Institute, 1 Haziran 2011, http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-5%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf (Erişim tarihi: 21 Ocak 2013).

Ian Brown ve Peter Sommer, Reducing Systemic Cybersecurity Risk, OECD/IFP Proje Raporu, 14 Ocak 2011.

Mısır'da protestolar sırasında internet erişimin kapanması hakkındaki detaylı zaman şeridi için bkz., http://www.flickr.com/photos/ramyraoof/5814392791/sizes/l/in/photostream/ (Erişim tarihi 22 Nisan 2012).

Http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99 (Erişim tarihi: 22 Nisan 2012).

Ryan Paul, "Iran moving ahead with plans for national intranet", http://arstechnica.com/techpolicy/news/2012/04/iran-plans-to-unplug-the-internet-launch-its-own-clean-alternative.ars
(Erişim tarihi: 22 Nisan 2012).

Özgür yazılımlardaki "free" kelimesinden ne anlaşılması gerektiği hakkında bir yazı için bkz., http://www.gnu.org/philosophy/free-sw.html (Erişim tarihi: 18 Ağustos 2012).

Steven Levy, Hackers Heroes of the Computer Revolution, New York, Penguin, 2001, s. 41.

Eric S. Raymond, How to become hacker, http://catb.org/~esr/faqs/hacker-howto.html#skills1 (Erişim tarihi: 22 Haziran 2012).

Sam Williams, Free as in Freedom Richard Stallman's Crusade for Free Software, http://oreilly.com/openbook/freedom/ch11.html (Erişim tarihi: 23 Haziran 2012).

McKenzie Wark, A Hacker Manifesto, Cambridge, Harvard University Press, 2004.

Ibid., madde 71.

Eric S. Raymond, How to become hacker, http://catb.org/~esr/faqs/hacker-howto.html (Erişim tarihi: 22 Haziran 2012).

Http://www.belgeler.org/howto/hacker-howto/hacker-howto.html (Erişim tarihi: 22 Haziran 2012). Siber güvenlik söz konusu olduğunda hackerlar ve crackerlar dışında aktörler de vardır. Script kiddies ya da lamer tabiri bilgisayar sistemlerine izinsiz erişmek için başkaları tarafından yazılmış programları kullanan kişilere verilen isimdir. Bunların genellikle bilgisayar programlamasını ve çalışma mantığını derinlemesine bilmedikleri düşünülür.

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf (Erişim tarihi: 18 Ocak 2013).

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Resmi Gazete, Sayı 2013/4890, 20 Haziran 2013, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf (Erişim tarihi: 18 Ağustos 2018).

Kaspersky Lab Global Research and Analysis Team, Gauss: Abnormal Distribution, http://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf (Erişim tarihi: 12 Ağustos 2012).

"PKK'nın en önemli hacker'ı yakalandı", Hürriyet, 19 Kasım 2008, http://hurarsiv.hurriyet.com.tr/goster/printnews.aspx?DocID=10393202 (Erişim tarihi: 21 Ocak 2013).

Tübitak ve BTK, "I. Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu", 2011, http://www.uekae.tubitak.gov.tr/uekae_content_files/siber_tatbikat_raporlari/USGT_2011_tr.pdf (Erişim tarihi: 23 Ocak 2013).

"Türkiye'ye Siber Saldırı", Hürriyet, http://www.hurriyet.com.tr/teknoloji/20440458.asp (Erişim tarihi: 11 Ocak 2013).

Canbek, G., Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, 13, 31-32, 43, 50, 58, 154, Eylül 2005.

Heiser, J. G., Understanding Today's Malware,Information Security Technical Report. Vol. 9, No.2, 47-64, April-June 2004.

Calder, A., Watkins, S., It Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799, Kogan Page, 14, 163, September 1, 2003.

Thompson, R., The Four Ages of Malware,Infosecurity Today, 47-48, March/April, 2005.

Grimes, R. A., Malicious Mobile Code, O'Reilly, 3,201-203, 226-228, 238-244, 467-468, August 1, 2001.

İnternet: How Bad Is The Malware Problem?, http://searchsmb.techtarget.com/sDefinition/0.sid44_gci991471.00.html, Eylül 2005.

İnternet: 2005 CSI/FBI Computer Crime and Security Survey, http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml , Computer Security Institute, Kasım 2005.

İnternet: Spyware and Increasing Security Risks-Proactive Protection for fhe Enterprise Client,http://enterprisesecurity.symantec.com/content/we bcastinfo.cfm?webcastid=146, Kasım 2005.

İnternet: Symantec, Symantec Internet Security Threat Report, 2005, http://ses.symantec.com/WP000ITR8, Kasım 2005.

Peikari, C., Fogie, S., Maximum Wireless Security,Sams Publishing, 153, 164, December 18, 2002.

Skoudis, E., Malware: Fighting Malicious Code,Prentice Hall PTR, 13, 96, 123-125, 149-151, 179,November 7, 2003.

Mohay, G., Collie, B., Vel, O., McKemmish, R.,Anderson, A., Computer and Intrusion Forensics,Artech House, 236, April 1, 2003.

Koca, H. (2022). Türkiye'de siber güvenlik uygulamaları, (Yüksek Lisans Tezi). Hatay Mustafa Kemal Üniversitesi / Sosyal Bilimler Enstitüsü, Hatay.

Sayedi, O.S. (2020). Ulusal Siber Güvenlik Stratejisi Oluşturma Süreç Analizi ve Türkiye ile Afganistan'ın Ulusal Siber Güvenlik Stratejisinin Değerlendirilmesi, (Yüksek Lisans Tezi). Trakya Üniversitesi/ Fen Bilimler Enstitüsü, Edirne.

Tozlu, B. (2021). Siber Güvenlikte Sosyal Mühendisliğe Karşı Bir Model Geliştirilerek Test Edilmesi, (Yüksek Lisans Tezi). Gazi Üniversitesi / Bilişim Enstitüsü, Ankara.

Tuğal, İ., Almaz, C., Sevi, M., "Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri", Bilişim Teknolojileri Dergisi, Cilt: 14, Sayı: 3, 2021.

Canbek, G. "Kötücül ve casus yazılımlar: Kapsamlı Bir Araştırma", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt:22, Sayı: 1, 2007.