ULUSLARARASI KIBRIS ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM-ÖĞRETİM VE ARAŞTIRMA ENSTİTÜSÜ

Yönetim Bilişim Sistemleri

ÜNİVERSİTE AĞLARINDA SİBER GÜVENLİĞE ETKİ EDEN FAKTÖRLER

(Yüksek Lisans Tezi)

Ferat ÖNAL

Lefkoşa – 2019

ULUSLARARASI KIBRIS ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM-ÖĞRETİM VE ARAŞTIRMA ENSTİTÜSÜ

Yönetim Bilişim Sistemleri

ÜNİVERSİTE AĞLARINDA SİBER GÜVENLİĞE ETKİ EDEN FAKTÖRLER

(Yüksek Lisans Tezi)

Ferat ÖNAL

Tez Danışmanı

Doç. Dr. Ahmet ADALIER

Lefkoşa – 2019

ULUSLARARASI KIBRIS ÜNİVERSİTESİ LİSANSÜSTÜ EĞİTİM-ÖĞRETİM VE ARAŞTIRMA ENSTİTÜSÜ

TEZ ONAY SAYFASI

Yönetim Bilişim Sistemleri Dalı'nda, 21706492 numaralı, Ferat ÖNAL'ın hazırladığı "Üniversite Ağlarında Siber Güvenliğe Etki Eden Faktörler" konulu Yüksek Lisans tezi ile ilgili savunması yapılmış ve adayın çalışması jüri tarafından oybirliği ile başarılı bulunmuş ve Yönetim Bilişim Sistemleri tezi olarak kabul edilmiştir.

Tez Savunma Tarihi: 26/08/2019

Jüri üyeleri **İmza**

1) Tez danışmanı
   Doç. Dr. Ahmet ADALIER .....

2) Üye
   Doç. Dr. Tolgay KARANFİLLER .....

3) Üye
   Yrd. Doç. Dr. Kamil YURTKAN .....

Prof. Dr. Tahir ÇELİK

Enstitü Müdürü

BEYANNAME

Ad ve Soyad: Ferat ÖNAL

Tezin Başlığı: Üniversite Ağlarında Siber Güvenliğe Etki Eden Faktörler.

Danışman: Doç. Dr. Ahmet ADALIER

Yıl: 2019

Yukarıda başlığı verilen ve tarafımca kaleme alınan bu tez çalışması içerisinde verilen tüm bilgileri, akademik kurallara ve etik davranışlara uygun olarak elde ettiğimi ve sunduğumu; bu çalışmaya özgün olmayan ve başka kaynaklardan aldığım bilgileri, akademik kuralların ve etik davranışların gerektirdiği şekilde, metinde ve kaynakçada eksiksiz olarak gösterdiğimi beyan ederim.

Bu tez çalışmasının; Uluslararası Kıbrıs Üniversitesi, Lisansüstü Eğitim, Öğretim ve Araştırma Enstitüsü tarafından saklanmasına ya da elektronik olarak sunulmasına izin veriyorum.

Tarih: 26/08/2019

İmza:

TEŞEKKÜR

Bu konuda tez yazma fikrimi kabul edip bana çalışma imkânı sağlayan, tez çalışmam sırasında kıymetli fikirleri ve tecrübeleri ile bana yol gösteren ve desteğini hiçbir zaman esirgemeyen değerli danışman hocam Sayın Doç. Dr. Ahmet ADALIER'e verdiği emekler ve gösterdiği özveri için teşekkür ederim. Balküpü uygulamasının hayata geçirilmesi hususunda desteklerini esirgemeyen Uluslararası Kıbrıs Üniversitesi Bilgi İşlem Müdürü Sayın Mustafa ÇAĞATAYLI'ya ve balküpü uygulaması tasarımında desteğini esirgemeyen Sayın Uygar KÖROĞLU'na verdiği emekler ve gösterdiği özveri için teşekkür ederim.

Eğitim ve iş hayatım boyunca maddi manevi destekleriyle beni hiçbir zaman yalnız bırakmayan aileme de teşekkürü bir borç bilirim.

ÖZ

Bilgi ve iletişim teknolojilerindeki baş döndüren hızlı değişme ve gelişmeler her alanda olduğu gibi eğitim alanının ortamını, kapsamını ve çehresini her geçen gün etkilemektedir. Bu değişme ve gelişmeler siber güvenlik konularını ön plana çıkarmaktadır. Bu çalışmanın amacı, üniversitede kullanılan bilgi sistem ağlarında siber güvenliğe etki eden iç faktörlerin incelenmesi, bu kapsamda bir balküpü uygulaması tasarlanarak ağ üzerindeki hareketlerin izlenmesi ve öğrencilerin siber güvenlik konusundaki farkındalıklarının anketle ölçülmesidir. Çalışmada nicel ve nitel araştırma yöntemleri kullanılmıştır. Araştırmada Uluslararası Kıbrıs Üniversitesinin Türkçe programlarında öğrenim gören 242 öğrencisine Akgün ve Topal'ın (2015) "Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları" anketi ve yazarlar tarafından hazırlanan demografik forum uygulanmıştır. Kötü amaçlı yazılım veya kullanıcının yetkisiz erişimi, ağın ve uygulama sunucularının işleyişinde hatalara neden olabilmekte ve üniversitenin sağladığı bilgi sistem hizmetlerinde kesintiler oluşturabilmektedir. Bu sorunları ortaya çıkmadan önce tespit etmek ve gerekli güvenlik önlemlerini almak için üniversite iç ağında aynı üniversitenin bilgisayar salonunu kullanan ve üniversite bilgisayarlarının yanı sıra kişisel bilgisayarları ile de üniversite ağına bağlanan öğrencilere balküpü uygulaması ile bir çalışma yapılmıştır. Uygulamada toplanan veriler incelenmiş ve ağ güvenliğini etkileyen risk faktörleri belirlenmiştir. Araştırma sonucunda üniversitede kullanılan bilgi sistem ağlarında siber güvenliğe etki eden iç faktörler saptamış, üniversite öğrencilerinin bilişim güvenliği farkındalıklarının düşük seviyede olduğu, almaları gereken önlemler hakkında yeterince bilgi sahibi olmadıkları ve güvenliklerini sağlamak için yeterli seviyede önlem almadıkları görülmüştür. Balküpü uygulamasınca toplanan veriler, üniversite ağında, ağ içinden gelebilecek siber saldırıların olabileceğini göstermiştir. Bu araştırmada elde edilen bulgular üniversite ağlarında güvenliğe etki eden iç faktörlerin belirlenmesine, güvenliği artırmak için yapılacak teknik çalışmalara ve üniversite öğrencileri için hazırlanacak bilişim güvenliği farkındalığı çalışmalarına yardımcı olacaktır.

Anahtar Kelimeler: Bilgi Güvenliği, Ağ Güvenliği, Siber Saldırı, Balküpü.

ABSTRACT

The rapid changes and developments in information and communication technologies affect the setup and scope of the education field, as in every field. These changes and developments highlight the cyber security issues. The aim of this study is to investigate the internal factors affecting cyber security in the information system networks used in the university, to monitor the movements on the network by designing a honeypot application, and to measure the awareness of the students on cyber security through a questionnaire. Quantitative and qualitative research methods were conducted in the study. In this study, the "Information Technology Security Awareness of Senior Students of the Faculty of Education" questionnaire developed by Akgün and Topal (2015) and a demographic form prepared by the authors were applied to 242 students studying in Turkish programs of Cyprus International University. Malware or unauthorized access by the user may cause problems in the functioning of the network and application servers and may interrupt the information system services provided by the university. In order to detect these problems and facilitate the necessary security measures before the emergence of related problems, a study was conducted with the use of a honeypot application for students using the university computer hall and/or those connected to the university network with their personal computers. The data collected in the application were examined and the risk factors affecting the network security were determined. As a result of this research, the following were determined: the internal factors affecting cyber security in the information system networks used in the university, the level of information security awareness of the university students was low, they did not have enough information about the precautions to be taken, and they did not take enough measures to ensure their security. Also, the data gathered by the honeypot application indicated that there may be cyber attacks within the university network. The findings of this study will help: to identify the internal factors affecting security in university networks, to develop technical studies to increase security, and to prepare information technology security awareness studies for university students.

Key Words: Information Security, Network Security, Cyber Attack, Honeypot Application.

İÇİNDEKİLER

TABLO LİSTESİ

Tablolar **Sayfa**

ŞEKİL LİSTESİ

Şekiller **Sayfa**

KISALTMALAR

ABD	Amerika Birleşik Devletleri
BT	Bilgi Teknolojileri
CSI	Bilgisayar Güvenliği Enstitüsü (Computer Security Institute)
IDS	Saldırı Tespit Sistemi (Intrusion Detection System)
NIST	ABD Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
SIEM	Güvenlik Bilgisi ve Etkinlik Yönetimi (Security Information and Event Management)
DOM	Belge Nesnesi Modeli (Document Object Model)
DMZ	Arındırılmış Bölge (DeMilitarized Zone)
MHN	Modern Bal Ağı (Modern Honey Network)

BÖLÜM 1

GİRİŞ

Bilgi Teknolojilerinin (BT) günümüzde daha fazla kişi tarafından erişilebilir olması, erişim için kullanılan aracı yazılım ve donanımların sürekli artan bir şekilde, daha fazla kullanıcı tarafından kullanılıyor olması sayesinde bilgiye erişim hızlanmaktadır. Bu güzel faydanın yanında önceden tahmin edilemeyen bilgi ve BT güvenliğine dair riskler de ortaya çıkmaktadır. Siber tehditler teknoloji kullanılarak gerçekleştirilebilmesinin yanı sıra herhangi bir teknoloji kullanmaksızın doğrudan insanın zayıf noktalarını kullanarak da gerçekleştirilebilmektedir (Yiğit & Seferoğlu, 2019). Bu durum BT kullanıcılarının farkındalıklarının yüksek olmasının ne kadar önemli olduğunun bir göstergesidir. Kurumsal ağların dışından yapılabilecek siber saldırılar BT çalışanları tarafından öngörülmekte ve buna özel çözümler ağda uygun noktalara konumlandırılmaktadır. Elbette ki kurum dışından gelebilecek siber saldırılar, kurumsal ağı etkileyebilecek tek nokta değildir. Kurumsal ağın yanlış tasarlanmış olmasından ötürü ortaya çıkabilecek riskler, iç ağ kullanıcılarının farkında olarak veya olmayarak ortaya çıkaracakları tehditlerde göz ardı edilmeyecek kadar önemlidir. Hem kurumsal ağda, hem de internet ağında herhangi bir güvenlik önlemi uygulanmamış şahsi BT cihazları ile (bilgisayar, akıllı telefon veya tablet vb.) gezinen kullanıcılara ait cihazların, bir malware (kötücül yazılım) tarafından enfekte olarak botnet ağına (köle bilgisayar ağı) düşmesi olasılığı son derece yüksektir. Botnet ağının parçası olsun veya olmasın herhangi bir zararlı yazılım tarafından enfekte olmuş cihaz ile kurumsal ağda gezinmek, içerden gelecek riskleri artıracaktır. Daha önce de bahsedildiği gibi tüm risk farkında olmadan yapılan davranışlar değildir. Bilgi ve BT güvenliği tehditleri arasında, kurum içerisinde çalışan kişilerin yaratabileceği iç tehditler önemli bir yer tutmaktadır. İç tehditleri bilinçli veya bilinçsiz tehditler olarak tanımlayabiliriz. Bilinçli tehditleri ikiye ayırabiliriz. Birincisi, kurumda çalışan art niyetli bir kişinin kendisine verilen yetkileri kötüye kullanmasıdır. İkincisi ise, kişinin başkasına ait erişim bilgilerini ele geçirerek, yetkisiz olduğu bilgilere erişmesi ve kötücül bir eylem gerçekleştirmesini kapsar (Kandemirli, 2012).

Ağ Güvenlik Yöneticisinin, kurum tarafından onaylanmamış kişilere maddi çıkar gözeterek erişim hakkı vermesi ve bilginin dışarı sızmasına sebep olması ilk kategoriye örnek olarak gösterilebilir. Ağ yöneticisi olmayan bir kişinin herhangi bir şekilde yönetici yetkilerini elde ederek Bilgi Sistem Ağında açıklıklar yaratması ve bunu çıkarı için kullanması ikinci kategoriye örnektir. CSI (Computer Security Institute) tarafından yapılan ankete göre katılımcıların %44'ü 2008 yılı içerisinde iç suistimal yaşamışlardır. Söz konusu oran, iç suistimallerin %50'lik virüs tehdidinden sonra ikinci büyük tehdit olduğunu göstermektedir (Kandemirli, 2012).

Eğitim-öğretim kurumları olan üniversite ağı kullanıcıları gelişime açık, araştırıcı, yeni teknolojileri denemek açısından sabırsız kullanıcılardır. Bu kullanıcılar karşılaştıkları teknolojik gelişmelere çok çabuk adapte olarak, ortaya çıkan zorukları aşmak konusunda son derece isteklidirler. Eğitim kurumlarında edindikleri bilgileri uygulamak isteyerek, bilgiye erişim için her türlü yolu deneyebilecek kimselerdir. Bu özellikleri bakımından zararlı yazılımların da hedefi olmaktadırlar. Üniversite öğrencilerinin, sanal zorba / sanal kurban olmaları hakkında yapılan bir araştırmada yüksek oranda sanal kurban oldukları, buna karşın düşük bir oran da olsa sanal zorba oldukları görülmüştür. Sanal zorbaların virüslü e-posta yollama, başkasının yerine geçerek mesaj gönderme, kişisel bilgisayar, mail adresi, web sayfasını ele geçirme gibi davranışlar sergiledikleri görülmektedir (Köse, Özdilek, Doğan, & Göktaş, 2018).

1.1 Problem Cümlesi

Üniversite ağlarında siber güvenliğe etki eden faktörlerden, iç ağ kaynaklı olanlar nelerdir, ağ kullanıcıları bu sorunlar hakkında ne kadar bilgiye sahiptirler, ağ güvenliğini sağlamak için neler yapılabilir?

1.2 Çalışmanın Amacı

Bu çalışmanın amacı, üniversitelerin kullandığı bilgi sistem ağlarında siber güvenliğe etki eden iç kaynaklı faktörlerin incelenmesi, bu kapsamda bir balküpü uygulaması tasarlanarak ağ üzerindeki hareketlerin izlenmesi, anket yoluyla üniversite öğrenclerinin siber güvenlik konusundaki farkındalıklarının ölçülmesi ve

ortaya çıkacak sonuç özelinde siber güvenliğin tesis edilmesi için çözüm önerilerinin belirlenmesidir.

1.3 Araştırma Soruları

H1:Üniversite ağı kullanıcıları bilgi teknolojilerini kullanırken kişisel güvenliklerine yeterince önem vermezler.

H2:Ağ kullanıcıları bilinçli veya bilinçsiz bir şekilde ağ ve sistemin kararlı çalışmasına engel teşkil edecek davranışlarda bulunabilirler.

H3:Ağ aktif cihazlarında alınacak güvenlik tedbirleri riskleri azaltabilir.

1.4 Çalışmanın Önemi

Araştırmanın alanı, üniversite içerisinde kullanılan bilgi sistem ağlarıdır. Ağın kullanıcıları tarafından farkında olarak (kötü niyetli) veya farkında olmadan yapılabilecek davranışların ağ güvenliğine hangi oranda etki ettiğinin ölçülmesidir. Bu araştırmada elde edilen bulgular ile üniversite bilgi sisem ağının güvenliğini artırmak için çözüm önerileri geliştirmektir.

1.5 Çalışmanın Kapsamı

Bu araştırmada nicel ve nitel araştırma yöntemleri kullanılmıştır. Araştırma evrenini Kuzey Kıbrıs Türk Cumhuriyeti'ndeki üniversite öğrencileri oluşturmaktadır. Kuzey Kıbrıs Türk Cumhuriyeti'ndeki özel bir üniversitenin uygun yargısal örnekleme yöntemiyle belirlenen 242 öğrenciyi kapsamaktadır. Ayrıca üniversite ağında çalıştırılan uygulama yazılımları ile ağda bir balküpü yaratılarak bal küpü üzerinde oluşacak hareketler izlenerek yorumlanmıştır.

BÖLÜM 2

LİTERATÜR TARAMASI

2.1 Bilgi

Bilgi; insanların ve organizasyonların düşüncesini, arayışını, hareket ve tutumlarını, gelişimini ve stratejilerini belirleyen faktörlerin başında gelmekte, önemini hayatımızın birçok alanında, sanatta, politikada, iş hayatında, eğitimde vb. artırarak sürdürmektedir (Demirtaş, 2013).

Bilgiye zaman içerisinde verilen önemde meydana gelen artış sonucunda onu yeniden tanımlama gereği ortaya çıkmış ve anlamı günün ihtiyaçlarına göre yeniden belirlenmiştir. Bilgi, 1950'lerde organizasyonlarda sadece bürokrasinin gerekliliği olarak kabul edilirken, 1990'larda rekabet avantajı sağlayabilecek stratejik bir kaynak olarak kabul edilmiştir. Geçen zaman içerisinde, organizasyonların en değerli varlığı çalışanların sahip olduğu bilgi haline gelmiş, bu nedenle de yapısal sermaye ile birlikte insan sermayesine de önem verilmiş, organizasyon bilgisinin dışında, çalışanların bilgisi de geliştirmeye çalışılmıştır (Atılgan, 2009).

Organizasyonların, kurumların veya bireylerin iş süreçlerinde vazgeçilmez olarak varlığını koruyan bilgi kimi zaman belgeler üzerinde yazılı olarak, kimi zamansa bilişim sistemleri aracılığıyla elektronik ortamda saklanabilmektedir. Bilginin üretilme ve aktarılma hızı Bilgi Teknolojilerinin de gelişimi ile birlikte her geçen gün daha da artmaktadır. Dünya çapında küresel bir ağın varlığı, mobil cihazlar ve sosyal medya uygulamaları bilgiye istenildiği zaman ulaşmayı mümkün kılmaktadır. Bu durum bilginin korunması ihtiyacını da artan bir şekilde beraberinde getirmiştir.

Önceleri kendimizin, yaşam alanlarımızın (ev, iş yeri vb.), arabamızın güvenliği yani fiziksel güvenlikler konusu ön plandayken, günümüzde, kişisel haklar, fikri mülkiyet hakları, ticari sırlar vb. kişisel veya kurumsal verilerimizin başka kişilerin eline geçmesini engellemeye yönelik önlemler daha fazla önem kazanmıştır. Hayatımıza giren bu değişiklik ile birlikte, "kredi kartlarımızın güvenliği, bilgisayarlarımıza virüs bulaşma olasılıkları, Banka hesaplarının güvenliği, kurumsal

bilgisayarların yetkisiz erişim ile istenmeyen kişilerin bilgiye nüfuz etmesi, Sosyal medya hesaplarımızın başkalarının eline geçme korkusu" gibi soruların daha fazla sorulduğu ve bu sorunlara çözüm arandığı bir zamanda bulunuyoruz (Mart, 2012).

2.2 Bilgi Teknolojileri (BT)

Bilgi Teknolojisi (BT) genel olarak bilgi edinme olarak tanımlanır. Bilgiyi mümkün olan en hızlı şekilde depolamak, işlemek ve istenen kişiye veya birimlere teslim etmek için telekomünikasyon altyapıları ile iletişim ve iletişim tesislerinin entegrasyonunu içeren sistemleri, bilgisayar ve bilişim sistemlerini içeren araç ve gereçlerin tutarlı kullanımı bilgi teknolojilerinin geniş tanımı olarak kullanılmaktadır (Zorlu, 2018).

Bilgi Teknolojileri servislerinin küresel internet altyapısının da getirileri ile birlikte bilgiye her yerden ve herhangi bir zamanda erişimi mümkün hale getirmesinden dolayı Bilgi Teknolojileri yaşamın her alanına nüfus etmiştir. Öyle ki; evlerimize masaüstü bilgisayarlar formu ile giren bilgisayarlar, tablet-dizüstü bilgisayar formlarına dönüşerek seyyar hale gelmiş, mobil ve akıllı telefonlar ile cebimizde taşıyabileceğimiz forma erişmiştir. Son dönemde ise giyilebilir teknolojilerin gelişmesi ile akıllı kol saatleri üzerinden internet bağlantısı sağlanmış ve küresel ölçekte birçok veriye erişilebilir hale gelmiştir. Bilgiyi artık bilgi teknolojilerinden bağımsız olarak düşünmek neredeyse imkânsız haldedir.

Üniversiteler bilginin üretiminde, öğretiminde, sunumunda ve dağıtımında sorumluluğu bulunan ve bu konuda önemli görevler üstlenen kurumlardandır. Bu sebeple bilgi teknolojisinde yaşanan tüm gelişmeler üniversiteler için son derece önemlidir (Tonta, 1999).

Bilginin, bilgi teknolojileri ile birlikte erişebilirliğinin ve üretiminin artması onun korunması ihtiyacını da beraberinde getirmektedir. Kamusal alanda artan bilgi teknolojileri kullanımı vatandaşlara hitap eden hizmetlere erişimi hızlandırmış fakat kritik sistemlere olan güvenlik riskini de beraberinde getirmiştir.

2.3 Bilgi Güvenliği ve Bilgi Güvenliği Prensipleri

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zaafiyeti oluşur (Pesen, 2015). Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün korunarak güvenli bir şekilde iletilmesi süreci de bilgi güvenliğinin bir diğer tanımıdır (Sharp, 2004). Oluşan güvenlik zaafiyeti Bilgi Teknolojilerinin hatalı sonuçlar üretmesine, kullanılamaz-cevap veremez hale gelmesine, kullanıcılarının maddi manevi zarar görmesine vb. farklı sorunların yaşanmasına sebep olacak sonuçlar doğurabilir.

Bilgi güvenliğini tam anlamıyla sağlamak çok zor bir görevdir. Çünkü tehditler zaman içerisinde boyut ve nitelik değiştirmekte, etki alanlarını genişletmektedirler. Buna bağlı olarak bilgi güvenliğini en üst seviyede sağlamak için, tedbirlerin birçok prensip dâhilinde ele alınması gerekmektedir (Ercan, 2015).

Bilgi güvenliğinde uyulması gereken temel prensipler, Gizlilik, Veri Bütünlüğü, Erişebilirlik olarak sıralanmaktadır. Bunların dışında, Loglama, Kimlik Doğrulama, İnkâr Edilmezlik ve Güvenilirlik'de önemli prensiplerin içinde yer almaktadır (Çek, 2017).

Bahsi geçen prensipleri ele alırken, güvenliğin ancak güvenlik bileşenlerinin en zayıf noktası kadar güçlü olduğunu unutmamak gerekir. Bu sebeple güvenliğin her nokta ve uygulanacak her prensip için aynı ölçüde önemsenmesi elzemdir. BT güvenliği yalnızca BT yöneticileri ve personeli tarafından ele alınamaz. BT kullanıcılarının tamamı gerek şahsi donanımları ile gerek kuruma ait donanımlar ile olsun, kurumun BT Yönetimi tarafından yayımlanan prensiplerine uymak zorundadırlar. Kuralların bir kişi tarafından dahi ihlal edilmesi sistemin tümünü olumsuz yönde etkileyecek sonuçlar doğurabilecektir. Bahsi geçen prensipleri açıklayacak olursak;

2.3.1 Gizlilik

Bilginin yetkisiz kişiler tarafından ulaşılamaması anlamına gelmektedir. Gizliliği, veri gizliliği ve mahremiyeti olarak ayırabiliriz. Veri gizliliği, özel ve gizli gizlilik dereceli bilginin yetkisiz kişiler tarafından ifşa edilmediğini garanti ederken, mahremiyet bireylerin şahsına ait hangi bilgilerin toplanıp saklanabileceğini ve kimlerin kime ve kim tarafından ifşa edilebileceğini kontrol edilmesini sağlamaktadır (Kurtkaya, 2017). Bunun için kurum bilgi varlıklarında doğru bir yetki hiyerarşisi kurulması zorunludur. Bilginin üretildiği nokta ile paylaşıldığı birimler arasında doğru bir eşleşme yapılmalıdır. Burada BT yöneticilerinin rolü son derece önemlidir. Tüm yetkilendirmelerin yapıldığı BT birimlerinde çalışan kadroda da bir ayrıştırma yapılması uygun olacaktır. Yetki faktörlerinin BT çalışanları tarafından ayrıştırılması sayesinde her hangi bir siber saldırıda ele geçirilmesi gereken parola miktarı artacak, kötü niyetli olabilecek kurum içi işgörenlerin tek başlarına art niyetli işlem yapma olasılıkları ortadan kaldırılacaktır. Yetkilendirmelerin bir kurumsal onay sürecinden geçirilmesi BT yönetimine olan güveni artıracağı gibi hatalı işlem olasılığını da azaltacaktır.

Yetki hiyerarşisi kurulmasında başlanacak ilk nokta kuruma özel bir bilgi sistem işletme yönetim ve güvenlik dokümanı hazırlanarak üst yönetim tarafından onaylanması olmalıdır. Dokümanın yayımlanmasından sonraki her yetki talebinde onaylanan dokümana uygun işlem gerçekleştirilmelidir. Özellikle bilgi ve bilgi sistem ağını tehlikeye düşürebilecek kritik yetkilerin verilmesinde daha önceden hazırlanan ve üst yönetim tarafından onaylanan aşamalar ile talep, onay, işlem süreçleri işletilmelidir. İşletilecek bu süreç bürokrasinin hızlandırılması amacıyla geliştirilen bir uygulama üzerinden de gerçekleştirilebilir. Örneğin, İnsan Kaynakları Yönetimi (İKY) bölümüne yeni bir personel dâhil edildiğinde, bölüm çalışanı olduğundan çalıştığı bölümün dokümanlarına erişim yetkisi verilmesinde atama/görevlendirme belgesi yeterli görülebilir. Fakat farklı bir bölümdeki çalışanın İKY dokümanlarına erişim talep etmesi durumunda işletilmesi gereken onay süreci değişebilir. Yetkilendirmede bölümler arası geçişler, ikiz görevlendirmeler dikkate alınabileceği gibi aynı bölüm içerisinde de bir bilmesi gereken prensibine göre ayrıştırma yapılabilir. Onay süreci bir uygulama veya kuruma özel hazırlanan bir

formun doldurulması ile personelin talebi, ilk amir onayı, üst yönetici onayı ve bilgi işlem sorumlusu tarafından onay sürecinin uygunluğunu kontrol etmesinden sonra ret veya onayı ile işlemin gerçekleştirilmesi şeklinde gerçekleştirilebilir. Onay süreçlerinde basılı form yerine uygulama kullanılması hem bürokrasiyi azaltarak süreci hızlandırabilir. Uygulama kullanımının bir diğer faydası da istatistiki verilerin hızla oluşturularak yönetime karar almada kolaylık sağlaması olacaktır.

Verilen erişim yetkilerinin geçerlilik süresi de farklı bir olgu olarak karşımıza çıkmaktadır. Personel rotasyonu esnasında yetkiler de personel ile birlikte taşınmamalıdır (olumsuz). Bu sebeple İKY bölümü ile Bilgi İşlem birimi arasında bir koordinasyon kurulması gerekmektedir. Personel farklı bir görev yerine atandığında yetki süreci yeniden işletilmeli ve uygun yetkiler tanımlanmalıdır.

Verilen yetkilerin tanımlanan prosedürler çerçevesinde kullanıldığı veya yetkilerin art niyetli kişilerce ele geçirilebilirliğini kontrol etmek maksadıyla bir SIEM (Security Incident and Event Management) uygulaması ile 7/24 takip edilmesi uygun olacaktır. Bu takip bilgi işlem biriminin gözetiminde fakat uygulamaya girilen kriterlerin uygulama tarafından otomatik olarak kontrol edilmesi ve anlık rapor çıkartarak bilgi işlem sorumlularını uyarması şeklinde olması gerekmektedir.

Bilgi gizliliğin sağlanabilmesi için McCumber modeli, bilginin dolaşım ve depolanması süreçlerinde kripto kullanılması tavsiye edilmektedir (McCumber, 2004).

2.3.2 Veri Bütünlüğü

Bilginin, saklandığı veri tabanında veya iletim halindeyken yetkisiz kişilerce değiştirilmesi, tahrip edilmesi veya silinmesi istenmez. Veri bütünlüğünün korunması için kullanılan yöntemler arasında elektronik imza, açık anahtar altyapısı gibi kavramlar gösterilebilir (Çek, 2017).

2.3.3 Erişebilirlik

Erişebilirlik, bilginin yetkili kurumlar ve kişiler tarafından, istenilen herhangi bir zamanda ulaşılabilir veya kullanılabilir olması demektir. Sayısal olarak ifade etmek gerekirse, kullanılabilirlik herhangi bir sistemin yapılış amacına göre işlev

gördüğü zamanın, işlev gördüğü ve görmediği toplam zamana oranıdır. Sistemin bir kısmı veya bütününde herhangi bir sorun çıkması durumunda bile bilgiye erişilebilir olmalıdır. Ancak bu erişim kullanıcıya tanınan haklar çerçevesinde olmalıdır. Erişilebilirlik ilkesi gereğince her kullanıcı erişim hakkının olduğu veri kaynağına, yetkili olduğu zaman diliminde ve yetkili olduğu lokasyonda mutlaka erişebilmelidir. Bu verilen hizmetin güvenilirliğinin de bir ölçütüdür (Önel & Dinçkan, 2007).

2.3.4 Loglama

Bilişim sistemlerinde tehditlerin belirlenmesi, kötücül aktivitelerin, yapılan atakların tespitinde kullanılabilecek kaynaklardan biri de log dosyalarıdır. Bilişim sistemlerinde kullanılan ağ cihazları, sunucular ve genel olarak sistem üzerinde meydana gelen olaylar kayıt altına alınır. Log kayıtları, hangi kullanıcının, hangi aktiviteyi yaptığını zamana bağlı kalarak göstermektedir (Baykara, Daş, & Tuna, 2016).

Log kayıtlarının tutulması gerçekleşebilecek tehditlerin izini sürmek, çalışan sistemde oluşabilecek sorunların kaynağını tespit etmek için son derece önemlidir. Fakat gerçekleşen veri trafiği göz önüne alındığında tüm detayların kaydını tutmak büyük bir maliyet ortaya çıkaracaktır. Büyüyen kayıt boyutu için terabaytlarca veri deposuna itiyaç duyulacağı gibi depolanan verinin büyüklüğü, yapılacak incelemelerde çalışanları içinden çıkılamaz bir duruma sürükleyecektir. Her ne kadar Güvenlik Olay Yönetim Yazılımları ile olay kayıtlarını incelemek mümkün hale getirilmiş olsa da başlangıçta doğru kaynakların izlenmesini temin etmek sistemi ve yöneticilerini rahatlatacaktır. Temelde izlenmesi gereken olay kayıtları, oturum açma bilgileri, sistem yöneticisi hareketleri, veri erişim ve iletim detayları, ağ cihazları hareketleri ve kötücül yazılım tespit bilgileri şeklinde olmalıdır.

2.3.5 Kimlik Doğrulama

Erişimin sadece onaylanmış kullanıcılar tarafından yapıldığına dair gerekli kontroller yapılmalıdır. Öğretim üyeleri, öğrenciler ve personel için farklı hesaplar oluşturulmalı, bu hesaplar ile yapılan erişimler kullanıcı adı – parola eşleşmesi ile doğrulanmalıdır (Donaldson S., 2015).

Yalnızca kullanıcı adı ve parola kullanımı dışında daha güçlü erişim denetim yöntemleri de bulunmaktadır. Bunların arasında, yüz, parmak izi veya el izi uygulamalarını da barındıran biyometrik algılayıcılar, USB (Universal Serial Bus) girişli içinde yetki anahtarı bulunan tokenlar, akıllı kartlar gösterilebilir. Güvenliğin çok yüksek olduğu noktalarda bunların birkaç tanesi aynı anda kullanılabilmektedir. Örneğin, kullanıcı adı ve parola eşleşmesi ile oturum açan bir kullanıcı dosyalarına erişebilmek için el izi algılayıcısını içeren bir biyometrik algılayıcı kullanabilir.

Bilgi sistemlerine erişimde yalnızca rakam kullanıldığında kişilerin şifreleri 3'ncü şahıslar tarafından elde edilebilir. Fakat Biyometrik karakteristik kullanan sistemlerde; kişinin bir parçası olan biyometrik karakteristik elde edilme ihtimali yoktur. Bu sistemler de %100 güvenli değildir. Biyometrik karakteristiğe sahip kişi zor kullanılarak sistemlere erişim için kullanılabilir (Bayram, 2018). Biyometrik kimlik doğrulama yöntemleri arasında performans kriterlerinin dışında belirlenen diğer kriterler ile birlikte değerlendirilen yöntemler Tablo 2.1'de gösterilmiştir.

Tablo 2.1 Biyometrik Karakteristik Parametreleri

Biyometri / Parametre	Evrensellik	Eşsizlik	Süreklilik	Elde Edilebilirlik	Performans	Kabul Edilebilirlik	Maliyet
Yüz	5	3	3	5	4	4	2
Kulak	4	3	4	4	3	4	2
Termal Yüz	5	3	3	5	3	4	3
İris	4	5	4	2	4	2	5
İmza	3	2	2	5	3	5	1
Konuşma	3	3	2	3	3	4	2
El Geometrisi	4	2	3	4	2	3	4
Retina	4	5	5	2	5	2	5
DNA	4	5	5	1	5	1	5
Parmak İzi	4	5	3	3	4	3	4

Kimlik doğrulama yöntemleri, SIEM uygulamaları ile birlikte kullanılarak güvenlik artırılabilmektedir. Örneğin, Bina giriş bilgileri veritabanı ile kimlik

doğrulama sistemi (Microsoft Active Directory vb.) veri tabanı bilgileri ile eşleştirilerek binaya giriş yapmamış kişinin bina içerisindeki bilgisayarına erişimi kısıtlanabilir. SIEM böyle bir durumda bir alarm üretecek ve belirlenen yönetici ve/veya güvenlik personeline bilgi gönderebilecektir.

2.3.6 İnkâr Edilmezlik

Elektronik ortamda gönderici ile alıcı arasındaki haberleşmenin inkâr edilmemesi için gerekli olan önlemlerin alınmasını sağlayan güvenlik unsurudur (Gülmüş, 2010). Bu önlemler ile gönderici ile alıcı arasındaki anlamazlıkların ortadan kaldırılması hedeflenir. Bu sayede ortaya çıkacak zararlar azaltılabilecektir. İnkâr Edilemezlik daha çok gerçek zamanlı işlemlerde, bankacılık ve finansal işlemlerde önem kazanmaktadır.

2.3.7 Güvenilirlik

Çalışan sistemin üretmesi gereken sonuçlar ile sistemin ortaya çıkardığı sonuç arasındaki tutarlılık durumudur. Sistem her çalıştığında aynı girdilerle aynı sonucu üretmesi olarak da tanımlanabilir (Yıldız, 2014).

Sistem tarafından bilginin fizyolojisi ve anlamında herhangi bir değişiklik oluşmaması güvenilirlik prensibini etkin kılmaktadır (Grance & Jansen, 2011).

2.3.8 Siber Güvenlik

Siber kelimesi, bilgisayar ve bilgisayar ağlarını içeren kavram ya da varlıkları tanımlamak için kullanılmaktadır. Siber alan (cyber space) kelimesi de birbiriyle bağlantılı sistem, yazılım, donanım ve insanların iletişim veya etkileşim içerisinde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır (NATO , 2012).

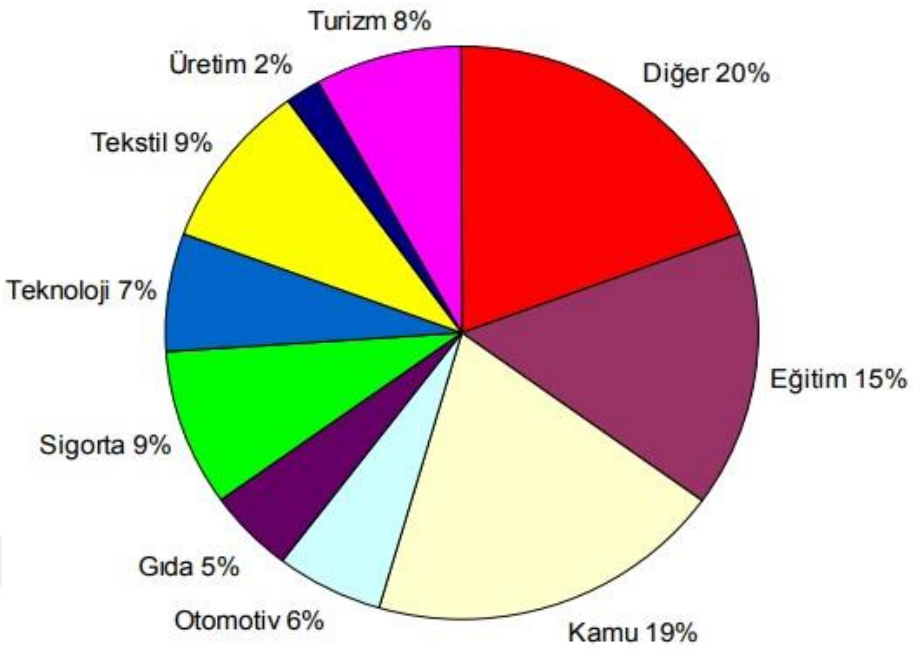
Siber güvenlik ise teknolojinin ilerlemesine bağlı olarak siber hayatın güvenliğinin (gizlilik, erişilebilirlik, aslına uygunluk ve inkâr edilemez bir bütünlüğün) sağlanması amacıyla gerçekleştirilen faaliyetler bütünüdür (Nemati & Yang, 2011). Siber ortam tarafından erişilebilen bilgi varlıklarının korunması maksadıyla uygulanması gereken politikaları, kılavuzları, risk yönetim faaliyetlerini,

eğitimleri, yazılım ve donanım tabanlı güvenlik çözümlerini kapsayan sanal dünyayı kapsamaktadır.

2.4 Bilgi Teknolojileri ve Bilgi Güvenliğine Dair Siber Saldırılar

Siber suç, bir bilişim sistemine izinsiz ve hukuka aykırı bir şekilde girilerek yapılan eylemlerdir (Yıldız, 2014). Siber saldırıda hedef bir kişi ve o kişiye ait varlıklar olabileceği gibi, bir kurum ve kuruma ait varlıklar da olabilir. Yapılan saldırılarda amaç bilgiye ulaşmak olabileceği gibi var olan bilgiyi bozmak veya erişilemez duruma getirmek de olabilir. Bir örnek vermek gerekirse, son dönemde sıkça karşılaşılan fidye yazılımlarından WannaCry, içerisinde Türkiye'nin de bulunduğu 100'e yakın ülkeyi etkisi altına almıştır. WannaCry saldırıları sebebiyle 2017 yılı içerisinde Rusya'da bankalar, İçişleri ve Sağlık bakanlıkları ile demiryolu şirketi etkilenmiştir. İngiltere ve İskoçya'da Ulusal Sağlık Sistemi (NHS) çökmüştür. En az 33 sağlık kuruluşu ile bazı aile hekimliği klinikleri etkilenmiş, bazı hastanelerde ameliyatlar yapılamamış, acil durumlar dışında hasta kabul edilememiştir. Fransa'da Renault, Portekiz'de Telecom, ABD'de FedEx ve İsveç'te bir yerel yönetim de yazılımın bulaştığı kuruluşlardandır (bbc.com, 2017).

Koç.net şirketinin yapmış olduğu, 1025 internet kullanıcısı ve 850 şirketi kapsayan "Rizikometre 2005 Türkiye Internet Güvenliği Araştırması" sonuçlarına göre, Kamu, Eğitim, Turizm, Tekstil ve Sigorta sektörlerinin risk altında olduğu tespit edilmiştir. Yapılan araştırma sonucunda şirketlerdeki yüksek düzeydeki güvenlik açıklarının sektörel bazda dağılımları Şekil 1'de gösterilmiştir. Buna göre eğitim kurumları da yüksek risk grubunda bulunmaktadır (Koç.net., 2005).



Şekil 2.1 Şirketlerin Kritik Seviyedeki Güvenlik Açıklıklarının Sektörel Dağılımları. (Koç.net., 2005)

Nesnelerin internete bağlanması ile birlikte tehditler boyut değiştirmektedir. 2020 yılında yaklaşık 50 Milyar cihaz internete bağlanmış olacaktır. Dünyada haftalık ortalama yüz binin üzerinde siber saldırı gerçekleşmektedir. Markets ans Markets'in raporuna göre siber güvenlik harcamaları 2020 yılında 170 milyar doları bulacağı tahmin edilmektedir (Özbilgin, 2019)

Kurumsal ağlarda karşılaşılabilecek birçok güvenlik riski bulunmaktadır. Risk faktörleri bilişim altyapısından ve kullanılan yazılımlardan kaynaklanabileceği gibi insan faktörü ile sosyal mühendislik kullanılarak elde edilecek bilgilerle yapılabilen saldırılar da mevcuttur.

Ağ üzerinde gerçekleştirilmesi mümkün olan saldırılar aşağıda anlatılmıştır.

2.4.1 Ağ Dinleme Saldırısı

Ağ Dinelem Saldırısı kaynak ile hedef sistemler arasındaki iletişimin dinlenmesi yolu ile verinin elde edilmesidir. Pasif bir saldırı türüdür (Allen, 2001).

Ağdaki veri trafiği birçok yöntemle dinlenebilir. Aynı fiziksel bölgedeki bir Yönetilemeyen Ağ Cihazı veya güvenlik protokolleri uygulanmamış herhangi bir

aktif ağ cihazına ağ kablosu ile bağlanılabilir. Bu bağlantı ile etki alanı sunucusu, elektronik posta sunucusu, internet ağı suncuusu ve diğer uygulama sunucuları ile özellikle aktif ağ cihazları tarafından üretilen syslog trafiği, sohbet oturumları, telnet, ftp parolaları ve yönlendirici yapılandırmaları ele geçirilebilir. Ele geçirilen erişim bilgileri saldırgana ağ içerisindeki diğer cihazlar üzerinde işlem yapabilme yeteneği kazandıracaktır.

2.4.2 Dağıtılmış Hizmet Dışı Bırakma Saldırısı

Dağıtılmış Hizmet Dışı Bırakma Saldırısı, yüzlerce ile yüz binlerce arasında değişen ve herhangi bir yerde konuşlandırılan, çok sayıda internet ağına bağlı köle bilgisayarın konuşlandırılmasını ifade eden Dağıtılmış Hizmet Reddi anlamına gelir. Köle bilgisayarlar, çok sayıda istek, paket veya mesajı tek bir sunucuya, ağa veya uygulamaya göndererek çalışanlar veya müşteriler gibi meşru kullanıcıların erişimini engellemeye çalışırlar (Nassiri, 2018).

Hizmeti sağlayan uygulama sunucuları veya ağ topolojisine göre varsa kurumsal ağ ya da sunucuların bulunduğu DMZ'den dışa açılan ağdaki bant genişliğinin doldurulması şeklinde uygulanır. Örneğin, 200 Mb/s bant genişliği üzerinden hizmet veren bir web sayfasına servis sağlayıcı tarafından veya sunucular tarafından bant genişliğinin karşılayamayacağı bir talep gönderildiğinde kullanıcılar sayfaya ulaşamayacaklardır. En klasik karşılaşılaşılan örneklerinden birisi sınav sonuçları açıklandığında ösym ve benzeri kurumların sayfalarına erişimde sıkıntılar yaşanmasıdır.

Dünya genelinde en çok ses getiren beş Dağıtılmış Hizmet Dışı Bırakma Saldırısı aşağıda listelenmiştir (Nassiri, 2018).

a. **GITHUB (1.35 TBPS):** Rekor büyüklükteki saldırı 28 Şubat 2018 tarihinde 1.35 TBPS ağ trafiği ile Github uygulaması tarafından gerçekleştirilmiştir. Uygulama ile bankalardan haber sitelerine kadar birçok uygulama hedeflenmiş, insanların önemli bilgileri yayınlayabilmeleri için önemli bir zorluk çıkartmaktadırlar (github, 2019).

b. **OCCUPY CENTRAL (500 GBPS):** Hong Kong'daki Occupy Central protestoları içindeki yoğun çatışmalar yalnızca sokaklarda değil, internette de gerçekleşti. Saldırılar, Hong Kong'daki bağımsız medya sitelerine karşı gerçekleştirildi. Dağıtılmış hizmet reddi (DDoS) saldırıları, haber siteleri olan Apple Daily ve PopVote'a karşı gerçekleştirildi (Olson, 2014). Saldırıların ağ trafiği içerisindeki büyüklüğü 500 GBPS'e ulaşmıştır (Nassiri, 2018).
c. **CLOUDFLARE (400 GBPS):** Sanfrancisco merkezli bir şirket olan Cloudflare'in müşterilerinden yalnızca birine yönelik olarak gerçekleştirilen saldırı ile Ağ Zaman Protokolü sunucuları hedef alınmıştır. 400 GBPS büyüklüğe ulaşan saldırı bir müşteriyi hedef alsada yoğunluğu şirketin bütününü etkilemiştir (Prince, 2014).
d. **SPAMHAUS (300 GBPS):** 1998 yılında kurulan Spamhaus, İngiltere, Cenevre, İsviçre ve Londra merkezlidir ve 10 ülkede bulunan 38 araştırmacı, adli tıp uzmanı ve ağ mühendisinden oluşan bir kadro tarafından yönetilmektedir (spamhaus.org, 2019). Saldırı ağ trafiği 300 GBPS büyüklüğe ulaşmıştır (Vijayan, 2013).
e. **U.S. BANKS (60 GBPS):** Kendisine "Izz ad-Din el Qassam Cyber Fighters" adını veren bir grup tarafından gerçekleştirilen saldırılar neticesinde birkaç ABD bankasının çevrimiçi ve mobil bankacılık hizmetlerinde erişim kesintileri oluşmuştur. Saldırı ağ trafiği 60 GBPS'e ulaşmıştır (Constantin, 2012).

2.4.3 IP Aldatması

Bilgisayarlar arasındaki bağlantı çeşitli protokoller aracılığıyla sağlanmaktadır. Bu protokoller aracılığıyla başka bir bilgisayara bağlanıldığında bağlanan bilgisayar kendi kimliğini karşı tarafa tanıtır. Bağlanılan bir bilgisayara gerçek IP adresinin gösterilmemesi yani asıl kimliğin gizlenmesine IP spoofing (Aldatma) denir (Arslan, 2016).

Sahte ip paketini alan taraf paketin gerçekten gönderilen ip adresinden gelip gelmediğini bilemez. Genellikle internet dünyasında ip spoofing denildiğinde başkasının ip adresinden mail göndermek, bir foruma mesaj yazmak işlemleri

gelmektedir. IP spoofing günümüz siber dünyasında yoğunlukla Dağıtık Servis Dışı Bırakma Saldırılarında kullanılmaktadır (BGA Security, 2019).

2.4.4 Sosyal Mühendislik

İnsanlar arasındaki iletişimdeki ve insan davranışlarındaki modelleri açıklıklar olarak tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahaleler sosyal mühendislik olarak tanımlanmaktadır (Güldüren & Keser, 2017). Güvenlikle ilgili süreçler belirlenmiş olsada bilgi sistemlerini kullanan personelin bu süreçlerin önemine dair farkındalıkları sürecin sağlıklı olarak yürütülebilmesi için önem taşımaktadır. Tıpkı bir bulmacanın parçaları gibi her bilgi kendi başına ilgisiz durabilir. Ancak parçalar bir araya getirildiğinde, açık bir resim oluşur (Mitnick & Simon, 2001). En basit anlamda bilgi sistemini kullanması için kendisine verilen kullanıcı adı ve parolasının başkasının eline geçmesine göz yuman, yeterince güvenli bir şekilde saklamayan personelin parolaları art niyetli kişilerce ele geçirilebilir. Ele geçirilen parolanın yetkisi düşük olsa dahi yetki yükseltme adımları bilgisayar korsanlarının uyguladığı bir yöntemdir. Bu durum normal bir kullanıcı hesabı ile sistem yönetimine dair işlemler yapılabilmesine kadar uzayacak bir sürecin başlamasına sebep olabilir.

2.4.5 SQL Enjeksiyonu

SQL (Yapılandırılmış sorgu dili), veri tabanlarından veri seçme, silme ve güncelleme gibi işlemleri yapabilmek için kullanılan sorgulama dilidir. Hem ANSI, hem de ISO standardı olan SQL, modern veri tabanı yönetim sistemlerinin temelini oluşturmaktadır (Vural, 2007). Günümüzde, özellikle içerik sağlayan web uygulamalarının birçoğu veri tabanlarını kullanmaktadır. Web uygulamaları, veri tabanı ile bir sorgulama dili olan SQL aracılığıyla haberleşirler. SQL Enjeksiyon ise, web uygulamalarından alınan kullanıcı girdileri ile oluşturulan SQL sorgularının manipülasyonu olarak tanımlanabilir (Anley, 2002).

Saldırgan, internet tarayıcı adres çubuğuna veya uygulamada bulunan giriş kutucuklarına kötücül kodlar ekleyerek, SQL enjeksiyon saldırısını gerçekleştirir (Daş, Baykara, & Demirol, 2013).

2.4.6 Komut Enjeksiyonu

Komut enjeksiyon saldırıları SQL enjeksiyon ve XSS saldırılarının aksine doğrudan sunucuları hedefleyen bir saldırı tipidir. Web uygulamasının komut satırını kullanarak uzaktan erişimle işletim sistemi, veri tabanı yönetim sistemi ve sunucudaki bilgilere erişimi hedefler.

2.4.7 HTML Enjeksiyonu

Web programcılarının kodlamada yaptıkları hataları kullanarak sayfalara yetkili bir kullanıcı ile erişmek ve sayfaya erişen kullanıcılar hakkında bilgi sahibi olmak için kullanılabilen bir saldırıdır. HTML enjeksiyonu tehlikesiyle, çoğunlukla, uygulamanın kullanıcıdan aldığı verileri kaydedip daha sonra işlediği durumlarda karşılaşırız. Örnek ile açıklama gerekirse; bir ziyaretçi defteri uygulamasında, yeterli güvenlik bilincine sahip olmayan geliştiricinin kullanıcıdan aldığı verileri herhangi bir koruma işlemine tabi tutmadan saklayıp, ekrana çıktı olarak aktarması bu saldırıya kapı aralamaktadır (Yılmaz O. , 2009).

2.4.8 Siteler Arası Komut Çalıştırma Enjeksiyonu

Siteler arası komut çalıştırma enjeksiyonu web sayfalarının bir güvenlik açığıdır. Saldırgan, kullanıcıyı kötü amaçlı bir siteye yönlendirmek için kötü amaçlı JavaScript kodunu web sitesine enjekte eder. Bir web sayfasındaki yorum bölümü bu açıklığın çalıştırılabileceği en savunmasız bölümdür (Sivanesan, Mathur, & Javaid, 2018). Saldırgan, web sayfasında kullanıcının giriş yapabileceği alanlarda; herhangi bir güvenlik önlemi bulunmaması durumunda, javascript veya html gibi kodların bu alanlara girilerek ilgili sayfanın kodları yorumlamasını sağlamasına çalışır. Kullanımına göre 3 farklı tipi mevcuttur. Bunlar Reflected XSS, Stored XSS ve DOM XSS olarak listelenebilir (Shalini & Usha, 2011). DOM (Belge Nesnesi Modeli) en çok kullanılan türdür.

2.4.9 Arka Kapılar

Bilgisayarlara erişimde kimlik kanıtlama süreçlerini atlatmak maksadıyla bırakılan açık kapılar olarak tanımlanmaktadır. Sistemlere sızan bilgisayar korsanları, daha sonra kolaylıkla tekrar erişebilmek için bir dinleme ajanı yerleştirilmiş açık port bırakırlar. Birçok virüs böyle bir arka kapı bırakarak

sistemlere erişebilmektedir (Yıldız, 2014). Açık kapılar her zaman kötücül yazılımlar ile oluşturulmaz. İşletim sistemlerinin veya bilgisayarlara daha sonradan kurulan birçok uygulama yazılımlarının da başlangıçta bilinmeyen ya da firma tarafından yayımlanmayan açıklıkları vardır. Uygulamalar fonksiyonlarını yerine getirebilmek maksadıyla bazı portları kullanabilmektedirler. Bu durum bilgisayar korsanları tarafından istismar edilebilmektedir. İşletim Sistemlerinin (Windows, MacOS, Linux vb.) kararlı sürümlerinden sonra dahi yayımladıkları güncellemelerin bazıları bu açık kapıların kapatılmasını sağlamaktadır. Yayımlanan güvenlik güncellemelerinin sistem bileşenlerine ve kullanıcı bilgisayarlarına uygulanması bahsi geçen açık kapıların kapanmasını da sağlamaktadır.

2.4.10 Oltalama Saldırısı

Kullanıcıların kandırılarak kullanıcı adı ve parolalarının elde edilmesi mantığı ile yapılan saldırılardır. Kimlik hırsızlığı adı da verilen, banka hesap numaraları, kredi kartı numaraları vb. kişisel bilgilerin, resmi bir kurumdan gönderiliyormuş gönderilen e-postalarla kişilerden elde edilmesidir. Sahte epostaları alan kişinin, istenilen kişisel bilgileri göndermesi, bu bilgilerin art niyetli üçüncü kişilerin eline geçmesine ve bunun sonucunda oluşabilecek zararlara maruz kalınmasına neden olacaktır (Bennett, 2004).

Oltalama saldırıları günümüzde daha çok internet üzerinden (kurumsal ağ dışından) e-mail ile yayılmaktadır fakat kurum içerisinde bulunan e-mail sunucuları üzerinden de yayılabilir. Kurum içerisinden yayılıma özellikle virüs kontrolünden geçirilmeyen USB Bellek, CD/DVD gibi taşınabilir sayısal veri ortamları ile kurumsal ağa taşınan veriler neden olmaktadır. Bu sebeple kritik öneme sahip sistemlerin bulunduğu kurumlarda bilgi aktarım merkezleri kurulmakta ve kurum dışından gelen veriler bu merkezlerde kontrollü olarak aktarılmaktadır.

2.4.11 Klavye Dinleme

Klavye hareketlerini kaydeden programlar ile yapılan saldırı türüdür. Saldırgan, bu programlar ile farkına varılmadan klavyede dokunulan her tuşun kaydedilip, kendisi tarafından belirlenen web adreslerine gönderilmesini sağlamaktadr. Klavye dinleme ile daha çok bankacılık işlemlerinde kullanılan kişisel

bilgiler hedef alınsada e-posta ve sosyal ağ sayfalarına erişim için kullanılan hesaplar için de kullanım yaygındır (Arslan, 2016). Yazılımsal klavye dinleme yöntemlerinin dışında donanım tabanlı klavye dinleme yöntemleri de mevcuttur. Bunun için Şekil.2'de örneklenen klavye bağlantı kablosu üzerine takılan aygıtlar örnek gösterilebilir.

Şekil 2.2 Klavye Dinleme Aygıtları

2.4.12 İstemdışı Elektronik Posta Gönderimi

İstemdışı elektronik postalar, toplu halde gönderilen, ticari, istenmeyen elektronik mesajlardır. Kaspersky.lab tarafından yapılan araştırmaya göre 2014 yılında yalnızca elektronik posta spamı, dünya çapında gönderilen tüm elektronik postaların ortalama % 63,5'ini oluşturmuştur (Shcherbakova & Vergelis, 2014). Gönderilen istemdışı elektronik posta içeriğindeki zararlı yazılımlar ile kullanıcılar için büyük tehdit oluşturmaktadır.

2.5 Üniversite Öğrencilerinin Bilgi Güvenliğine Yaklaşımı

Üniversite öğrencileri aynı kurumsal ağı kullanan birbirlerinden farklı demografik özelliklerde (yaş, cinsiyet, kültür, eğitim düzeyi) insanlardan oluşan bir topluluktur. Bu topluluğun Bilişim Teknolojilerine ve güvenliğine olan yatkınlığının ölçülmesi yapılacak çalışma için önemlidir. Bartın Üniversitesi tarafından yapılan bir nitel araştırma sonucuna göre üniversite öğrencilerinin yaklaşık yarısı bilgisayarlarında parola dahi kullanmazken, güvenlik duvarı kullanma oranı %9.8

düzeyinde kalmıştır (Yılmaz, Yılmaz, & Sezer, 2014). Aynı şekilde Antivirüs kullanma oranı da son derece düşüktür. Bu durumda kurum iç ağda gezinmekte olan üniversite öğrencilerinin siber saldırılara son derece açık oldukları görünmektedir. Bu durum, üniversite ağındaki iç kullanıcılarının büyük çoğunluğunu oluşturan üniversite öğrencilerinin zararlı yazılımlar ile enfekte olarak ağda zararlı yazılım dağıtıcısı olmasını, botnet ağlarına dâhil olarak üniversite ağı dışındaki kötü amaçlı kullanıcıların üniversite ağı içinden hedeflerine ulaşacak stratejiler geliştirmesine olanak sağlayacaktır.

2.6 Balküpü Tuzak Sistemleri

Kurumsal Ağ içerisinden gelebilecek saldırılan tespiti için İz Takip Yazılımları, Ağ İzleme Yazılımları, Web Uygulama Güvenlik Duvarları ve Sistem sunucularının kaynaklarını takip etmek üzere tasarlanmış yazılımlar kullanılabilmektedir. Fakat bunların yanında saldırganlara bilinçli bir şekilde açık kapı bırakmak suretiyle onların davranışlarını izlemek mantığıyla çalışan Balküpü (Honeypot) yazılımları da kullanılabilecek bir diğer yöntemdir.

Balküpleri bilgi ve ağ güvenliğine yönelik yapılan saldırıların farkına varmak, saldırganların yöntemlerini izlemek, metodlarını belirlemek, yeni geliştirilen saldırı sistemlerinden önceden haberdar olmak için özel olarak tasarlanmış yazılım veya sistemlerdir (Bektaş & Spysal, 2018).

"Bal küpü" ya da "bal çanağı" şeklinde ifade edilen Honeypot'lar bilişim sistemlerine karşı gerçekleştirilen saldırıların tespit edilmesi için kurulmuş tuzaklardır. Saldırılara açık şekilde tasarlanan Balküpü uygulamaları, tasarlandıkları sisteme göre farklı kanallar için açıklıklar barındırırlar. Yapılan erişimler kayıt altına alınarak bir erişim günlüğü (log) vasıtası ile saldırgan profili çıkartılarak kötücül yazılımlar ile kötü amaçlı kullanıcılar tespit edilmeye çalışılır.

Tuzak sistemlerden oluşan ağ "Honeynet" olarak adlandırılmaktadır. Bunun yanı sıra, "Honeyd" yazılımı ile bir makine üzerinde farklı işletim sistemlerini simüle eden sanal bilgisayarlar, yönlendiriciler ve sanal ağların oluşturulması mümkündür. Ayrıca "Honeywall" yazılımı ile sistem, üzerinden geçen trafik analiz edilmekte, alt

ağdaki tuzak sistem makinelerinin ele geçirilmesi ve buradan dışarı saldırı yapılmasının da önüne geçilebilmektedir (Karaaslan, Akın, & Demir, 2008).

2.7 Bilgi Teknolojileri Güvenliğinde Farkındalık

Bilgi güvenliği uzmanlarıyla gerçekleştirilen bir çalışmada yükseköğretim kurumlarının bilişim sistemleri güvenliği açısından dünyadaki en güvensiz yerlerden biri olduğu ifade edilmektedir. Yapılan testler ve denetimler yükseköğretim kurumları bilgi sistemlerinde birçok açıklıklar ve zayıflıkların bulunduğunu göstermektedir. Üniversite çalışanlarının birçoğu parolalarını işe girdiği tarihten beri değiştirmediklerini ifade etmişlerdir (Puhakainen, 2006).

Bilgi ve bilgi teknolojileri güvenliği eğitimleri diğer kurumlarda olduğu gibi yükseköğretim kurumları için de bir zorunluluktur. ABD'de Winsconsin Üniversitesi tarafından 435 yükseköğretim kurumunda uygulanan ankete katılan enstitülerden sadece üçte birinde öğrenci ve personel için bilgi güvenliği farkındalık eğitimi verildiği tespit edilmiştir (Caruso, 2003).

Bir kurum, maliyetine bakmaksızın paranın satın alabileceği en ileri güvenlik teknolojilerini kullanabilir, sistemler tasarlayabilir ve adeta kendisini bir güvenlik çemberinden geçirebilir. Bu şekilde en son teknolojiyi kullanarak, üst seviyede güvenlik önlemleri alabilen bir kurumda bilgi güvenliğinin %100 sağlanmış olduğundan bahsedilemez (Şahinaslan, 2009). Çünkü kurum personeli ve kurum Bilgi Teknolojileri tarafından sağlanan hizmetleri kullanan diğer insanlar, belirlenen güvenlik önlemlerini takip etmez ve/veya uygulamak istemez ise alınan önlemlerin hiçbir anlamı kalmaz.

Bilgi güvenliği risklerinden korunmak için en iyi yol, bilgi teknolojilerine çok para harcamak ve korunma amaçlı teknolojilere (güvenlik duvarı, sanal özel ağ sınırlamaları, saldırı tespit ve önleme sistemleri, anti virüs yazılımları, uç nokta kontrol sistemleri, içerik kontrol yazılımları, veri şifreleme, kimlik doğrulama yöntemleri, yetkilendirme hiyerarşisi vb.) daha çok yatırım yapmak olmamalıdır. Bundan önce, insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojilerini doğru yer ve zamanda, doğru Bilgi Teknolojileri için kullanmak akla gelmelidir (Thomas & Gardner, 2017).

İnsan kaynaklı bilgi güvenliği risklerini tam olarak ortadan kaldırmak mümkün olmasa da doğru planlanmış bir farkındalık eğitimi ile bu riskleri azaltmak mümkündür. Ancak bu sayede güvenlik için yapılan teknoloji yatırımlarından istenilen verim alınabilecektir. Bu amaçla kurumlarda bilgi güvenliği farkındalık eğitimlerinin düzenlemesi önem arz etmektedir.

Temel bilgi güvenliği farkındalık eğitimlerinde bireylere bilgi güvenliği ile ilgili bakış açılarını genişletecek bilgiler verilmelidir. Eğitimlerde ele alınabilecek başlıklar aşağıda sıralanmıştır (Güldüren & Keser, 2017);

- Genel kavramlar,
- Bilginin bulunduğu ortamlar,
- Bilginin korunması gereken nitelikleri,
- Bilgi güvenliğinin önemi ve tehditler,
- Sosyal mühendislik saldırıları,
- Sosyal medya riskleri ve güvenlik,
- Ağ riskleri,
- Dikkat edilmesi gereken kurallar ve temiz masa kuralları,
- E-posta ve mesajlaşma güvenliği,
- Şifre güvenliği,
- Taşınabilir bilgisayar ve mobil cihaz güvenliği,
- Fiziksel güvenlik ve veri sızıntıları,
- Yasal düzenlemeler,
- Kurum politika ve yöntemleri,
- Bireyin sorumlulukları ve kendisinden beklenenler yaşanmış örnek olaylarla zenginleştirilerek sunulmalıdır.
- Hazırlanan içerik, güncel teknolojiler ve kuruma dâhil olan yeni BT varlıklarını da içerecek şekilde, bireylerin beklentileri de dikkate alınarak güncellenmelidir.

Kurumlarda bilgi ve bilgi teknoloileri güvenliğinin sağlanması, düzenlenecek bilgi ve bilgi güvenliği farkındalık eğitimlerinin periyodik olarak verilmesi ile

sağlanabilir. Bu eğitimlere katılımcıların ilgisini çekmek için içeriklerde sürekli bir güncellemeye gitmekte ve etkileşimli, görsel ve işitsel içerikler ile zenginleştirilmiş olmasında yarar vardır. Bu konuda yeni bir uygulama da e-öğrenme tekniklerini kullanan, çoktan seçmeli sorularla oluşturulan interaktif oyunların katılımcılara zaman ve mekân bağımsız olarak ve eğlenerek öğrenmelerine imkân sağlamalarıdır (Constantin, Lucian, 2018).

Kurumlarda bilgi güvenliğinin sağlanması için uygulanan kısıtlamaların BT kullanıcılarının alışkanlıklarına ters düştüğü için güvenlikle ilgili uygulamalarda zaman kaybı yaşanmaktadır. Farkındalık eğitimlerinin başarılı olabilmeleri için katılımcıların eğitimin gereğine ikna edilmeleri gerekmektedir. Katılımcılar BT kullanımındaki pozisyonlarının BT bütününü etkileyecek bir soruna neden olmayacağını düşünebilirler. Oysaki güvenlik BT yöneticisi veya son kullanıcı arasında bir fark olmaksızın önem taşımaktadır.

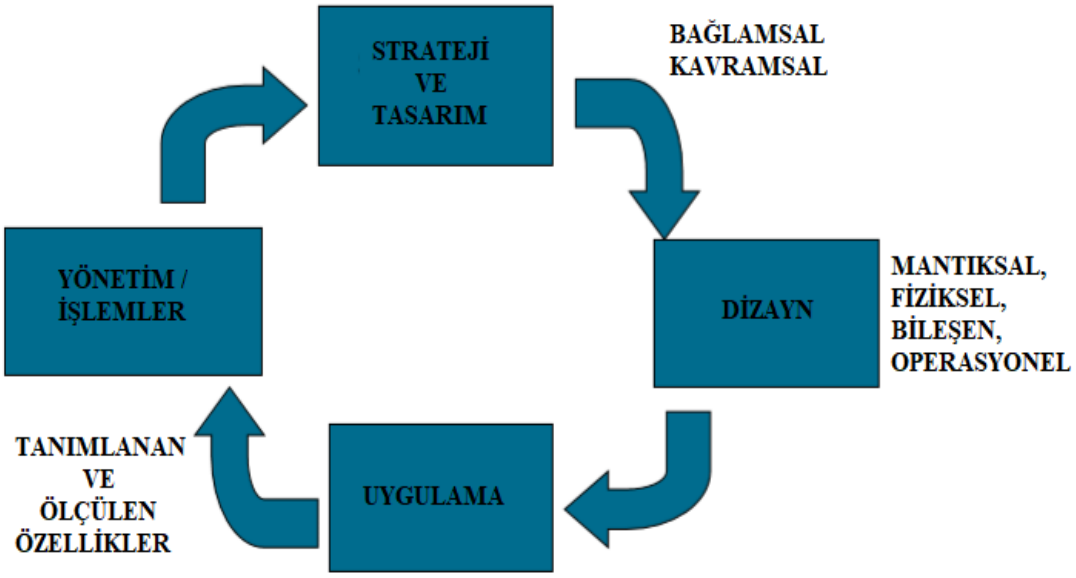
Etkili bir bilgi güvenliği farkındalığının sağlanması için tercih edilecek eğitim programının geliştirilmesinde önem arz eden konular aşağıda sunulmuştur.

2.7.1 Kurumsal Bilgi Güvenliği Politikalarının Oluşturulması

Kurum özelinde hazırlanan bir güvenlik politikası bilgi teknolojileri güvenliğinin temelini oluşturmaktadır. Güvenlik politika dokümanı güncel gelişmeler ve kurum BT varlıklarındaki değişimler dikkate alınarak sürekli güncel olarak bulundurulmalıdır. Güvenlik politikaları farkındalık eğitimlerinin de temelini oluşturacaktır. Kullanıcılar belirlenen güvenlik politikalarına uymamanın getireceği yaptırımlardan da haberdar olmalıdır (Güldüren & Keser, 2017).

ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı, kurumsal bilgi güvenliğinin sağlanması maksadıyla “Uluslararası Standartlar Organizasyonu” tarafından geliştirilen bir standarttır. ISO 27001 Bilgi Güvenliği Yönetim Sistemleri – Gereklilikler (Gereksinimler) Standardı kurumsal bilgi güvenliğinin bir kurumda nasıl uygulanabileceğini açıklayan standarttır. Bu standart ile kurumda Bilgi Güvenliği Yönetim Sisteminin kurulması, gerçekleştirilmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve iyileştirilmesi sağlanmaktadır (Doğantimur, 2009).

Risk odaklı kurumsal bilgi güvenliğini geliştirmek için tasarlanan SABSA (Sherwood Uygulamalı iş Güvenliği Mimarisi) işletmelerde tutarlı BT güvenlik politikalarının belirlenmesi için önerilen bir diğer yöntemdir. BT yaşam döngüsünün dört bölümünü de (Strateji, Tasarım, Uygulama ve Yönetim/İşlemler) kapsayan altı katmanlı (Bağlamsal, Kavramsal, Mantıksal, Fiziksel, Bileşen, Operasyonel) bir modeldir. Bu modeli tanımlayan SABSA Yaşam Döngüsü Şekil ‘de sunulmuştur (Battersby, 2013). SABSA 1995’ten bu yana yaklaşık 50 ülkede Bankacılık, Evsiz Yönetimi, Nükleer Enerji, Bilgi Hizmetleri, İletişim Teknolojisi, Üretim ve Hükümetler gibi farklı sektörlerdeki kuruluşlar için uygulanmaktadır (sabsa.org, 2018).

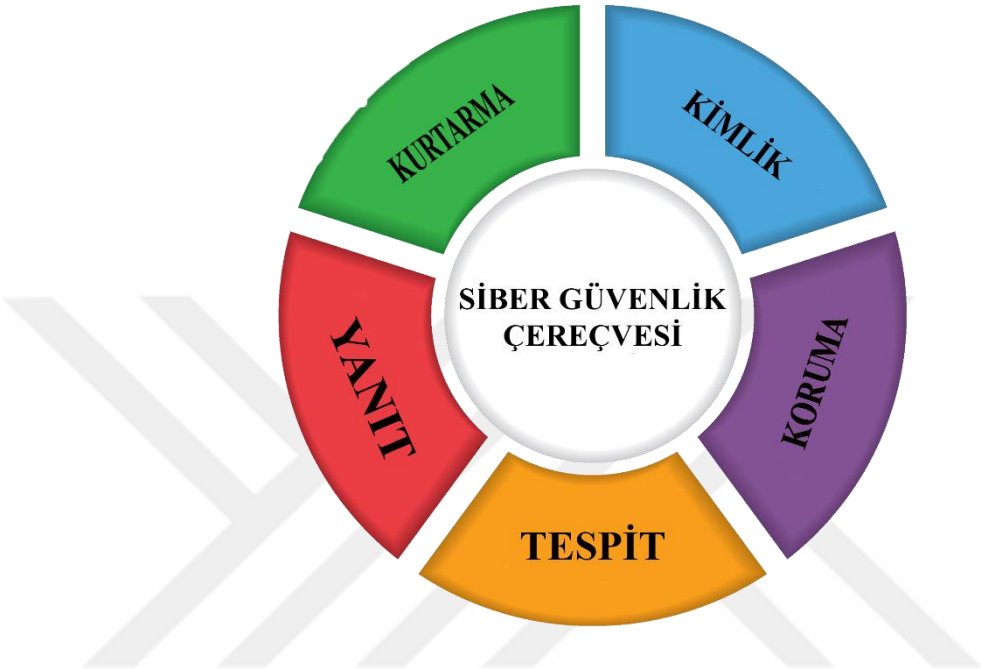


Şekil 2.3 SABSA Yaşam Döngü

2018 yılında yapılan son değişikliklerle SABSA’da ağır ITIL odağından uzak ve daha genel bir kurumsal risk görüşüne doğru bir hareket görünmektedir.

SABSA, ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından Kuruluşların siber güvenlik risklerini daha iyi anlamalarına ve yönetmelerine yardımcı olmak için tasarlanan (https://www.nist.gov/cyberframework, 2019) Siber Güvenlik Çerçevesinin (Şekil.2.4) geliştirilmesi için bir proje yürütmektedir. SENC

(The SABSA Enhanced NIST Cybersecurity Framework), SABSA Gelişmiş NIST Siber Güvenlik Çerçevesi adındaki proje ile SABSA İşletme Nitelikleri Profiline dayanan, iş odaklı bir süreçle geliştirilmesini amaçlamaktadır (sabsa.org, 2019).



Şekil 2.4 NIST Siber Güvenlik Çerçevesi

2.7.2 Eğitim İhtiyaçlarının Tespit Edilmesi

Başarılı bir eğitim programının hazırlanmasındaki bir diğer husus kurum içerisindeki personelin bilgi seviyelerinin gözetildiği bir eğitim planının hazırlanmasıdır. Personelin bilgi seviyelerinin ölçülmesi için onlarla kısa sohbetler yapılmalıdır. Personelin öğrenme yeteneği, ilgi alanları, verilecek eğitime karşı olan direnç veya sempatileri, önceki eğitimlerde kullanılan materyaller, eğitim programı hazırlanmasında faydalanılabilecek kurum veya kişileri belirlemek, eğitimin ihtiyaç ve önceliklerinin belirlenmesine destek olacaktır (Güldüren & Keser, 2017).

Eğitim ihtiyaçlarının tespit edilmesinde yakın tarihlerdeki örnek güvenlik olayları ve bunların doğurdukları sonuçlar hem kurum genelinde hem de personel özelinde ele alınmalıdır. Personel özelinde alınan sonuçların doğurduğu hukuki yaptırımlar örneklenirken, kurum genelinde verilecek örneklerde güvenlik ihlalinin kurum için doğurduğu zararlardan bahsedilmelidir.

2.7.3 Gerekli Desteğin Sağlanması

Yönetim kademesi ve kullanıcıların desteğinin alınması bir diğer önemli aşamadır. Gerekli destek alınmadan hazırlanan eğitimde aksaklıklar meydana gelebilir. Ancak güvenlik bilincine sahip bir yönetim eğitim faaliyetine zaman ve maddi kaynak ayırabilecektir.

Eğitim planı hazırlanmadan önce kurum iş takviminde kendine yer bulmalıdır. Plan eğitimin verileceği yerler, katılımcı ve eğitimci sayısı da dikkate alınarak hazırlanmalıdır. Eğitimler kurumun iş planını aksatmayacak şekilde azami katılımın sağlanması hedeflenmelidir.

2.7.4 Eğitim Gruplarının Belirlenmesi

Kullanıcılar kurum içinde kendi faaliyet alanlarında çalışırken aynı seviyede güvenlik bilincine ihtiyaç duymazlar. Kullanıcılar arasında doğru ayırımı yaparak her gruba ihtiyacı olan güvenlik bilincine uygun bilgiyi sunan eğitim programı daha iyi bir sonuç almayı olanaklı kılacaktır. Bilgi güvenliği bilinçlendirilmesi maksadıyla düzenlenen eğitimlerde verilen bilgilerin önemsenmesi için yalnızca ihtiyacı olan bilgilerin doğru gruplara iletilmesi gerekmektedir.

Yapılan bir çalışma (Güldüren, 2015) kapmasındaki araştırmalarda tek tip eğitim programların tüm gruplara uygulandığı ve bilinçlendirme programının istenilen başarıya ulaşamadığı tespit edilmiştir. Eğitim grupları kurumların ihtiyaçlarına uygun olarak güvenlik bilinci seviyesi, teknik bilgi seviyesi, ünvan/yetki durumu, görev alanı, kullanıcının eriştiği teknolojiler gibi yöntemler ile izlenerek belirlenebilir.

2.7.5 İletişim Araçlarının Belirlenmesi

Eğitim programındaki bir sonraki adım iletişim araçlarının belirlenmesidir. Her kurumun kendine özgü farklı iletişim araçları mevcuttur. Kurumda bulunan iletişim araçları tespit edildirkten sonra bunlardan eğitimde kullanılabilecek olanlar hakkında kullanım dokümanları hazırlanmalıdır. Eğitimlerde kullanılabilecek

kurumsal iletişim araçları için elektronik posta, sesli veya görüntülü çoklu ortam dosyaları, genelgeler, kurum ağı, yazılı yayınlar (posterler, dergiler, kitaplar, broşürler, kurum yayınları), yüz yüze yapılan görüşmeler (toplantılar, sunumlar, eğitim ve güvenlik seminerleri) örnek olarak verilebilir (Güldüren, 2015).

BÖLÜM 3

YÖNTEM

Bu bölümde tezin araştırma modeli, hipotezleri, evren ve örneklemi, veri toplama araçları ve veri toplama süreci yer almaktadır.

3.1 Araştırmanın Modeli

Bu çalışma da üniversitelerin kullandığı bilgi sistem ağlarında siber güvenliğe etki eden iç kaynaklı faktörlerin incelenmiş, bu kapsamda bir balküpü uygulaması tasarlanarak ağ üzerindeki hareketlerin izlenmiş, anket yoluyla üniversite öğrenclerinin siber güvenlik konusundaki farkındalıkları ölçülmüş ve ortaya çıkacak sonuç özelinde siber güvenliğin tesis edilmesi için çözüm önerileri belirlenmiştir. Çalışmanın hipotezlerine yanıt aramak amacıyla Nicel ve Nitel araştırma yöntemleri kullanılmıştır.

Üniversite öğrencileri üzerinde uygulanan farkındalık anketi ile üniversite öğrencilerinin bilgi güvenliği konusundaki bilgi seviyeleri ölçülmüştür. Üniversite ağında içeriden gelebilecek zararlı yazılım, bilinçsiz ve/veya art niyetli kullanıcılar tarafından yaratılması muhtemel siber güvenlik zaafiyetlerinin/saldırılarının neler olduğunu ortaya çıkartmak maksadıyla çalışmalar yapılmıştır. Görünürde sistemin bir parçası olan ama aslında tecrit edilmiş ve gözlem altında tutulan verilerin saldırganları açığa çıkartmak ve engellemek için yem olarak sunulduğu bir bal küpü sistemi tasarlanmıştır. (Bıçakçı, Doruk, & Çelikpala, 2015).

Araştırma sonucunda elde edilen veriler ile üniversite öğrencilerinin bilgi güvenliği farkındalığını artırmak için izlenecek yol belirlenecek ve bal küpü uygulamasınca toplanan veriler incelenmiş üniversite ağı bilgi sisteminin daha güvenli hale getirilmesi için gerekli güvenlik önlemi önerileri belirlenmiştir.

Verilerin analizi için SPSS-24 programı kullanılmıştır.

3.2 Hipotezler

H1:Üniversite ağı kullanıcıları bilgi teknolojilerini kullanırken kişisel güvenliklerine yeterince önem vermezler.

H2:Ağ kullanıcıları bilinçli veya bilinçsiz bir şekilde ağ ve sistemin kararlı çalışmasına engel teşkil edecek davranışlarda bulunabilirler.

H3:Ağ aktif cihazlarında alınacak güvenlik tedbirleri riskleri azaltabilir.

3.3 Evren ve Örneklem

Bu çalışmanın evrenini Kuzey Kıbrıs Türk Cumhuriyeti'ndeki özel bir üniversitenin uygun yargısal örnekleme yöntemiyle belirlenen 242 öğrencisi ile aynı üniversitenin genele açık bilgisayar salonuna yerleştirilen ve bilgisayar salonunda hazır bulunanlar ile öğrencilere ait bilgisayarların da aynı ağa bağlandığı en az 100 bilgisayardan oluşan bir ağdaki bilgisayar kullanıcılarını kapsamaktadır. Bilgisayar kullanıcıları ve ağa bağlı öğrenci grubu sürekli değişmekte olduğundan üniversitenin her bölümünde okuyan öğrencilere ulaşıldığı düşünülmektedir.

Anket araştırmasının evrenini Uluslararası Kıbrıs Üniversitesi Özel Eğitim Öğretmenliği, Okul Öncesi Öğretmenliği, Türkçe Öğretmenliği, Sınıf öğretmenliği, Bilgisayar Öğretmenliği, Beden Eğitimi ve Spor Yüksek Okulu (BESYO) ile Pisikolojik Danışmanlık ve Rehberlik (PDR) bölümlerinde okuyan toplam 242 lisans öğrencisi oluşturmaktadır. Araştırma evreninde konu hakkında daha fazla bilgi sahibi olması beklenen

3.4 Veri Toplama Araçları

Araştırmada veri toplama aracı olarak anket uygulaması ve balküpü uygulaması kullanılmıştır.

3.4.1 Anket Uygulaması

Araştırmada Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü tarafından geliştirilerek aynı üniversitede farklı bölümlerde okuyan toplam 217 öğrenci üzerinde uygulanan "Bilişim Güvenliği Anketi" kullanılmıştır (Akgün & Topal,

2015). Anketin amacı üniversite öğrencilerinin bilişim güvenliği konusundaki farkındalık seviyelerini tespit etmektir. Bu amaçla öğrencilere aşağıda dağılımları verilen soru grupları yöneltilmiştir.

1. Bilişim güvenliği ile ilgili olarak;

   a. Parola hakkında (8 Soru)
   b. İnternet üzerinden alışveriş hakkında (3 Soru)
   c. Kullanıcı hesap güvenliği hakkında (5 Soru)
   d. Zararlı yazılımlar ve antivirüsler hakkında (6 Soru)
   e. Yazılım güncellemesi hakkında (3 Soru)
   f. Sosyal ağlar hakkında (5 Soru)
   g. Anlık mesajlaşma uygulamaları ve elektronik posta hakkında (7 Soru)
   h. Kablosuz ağlar hakkında (3 Soru)
   i. Yürürlükteki yasalar ile etik konular hakkında (3 Soru)
   j. Bilgilerini güncelleme ve bilişim güvenliği hakkında (5 Soru)

2. Öğrencilerin bilişim güvenliği seviyeleri hakkındaki cevaplarının dağılımları;

   k. Cinsiyetleri
   l. Katılımcıların Doğdukları Ülkelere Göre Dağılımları
   m. Katılımcıların Yaşlarına Göre Dağılımları

3. Bilişim güvenliği ile ilgili olarak katılımcılara yöneltilen sorular;

   n. Alış-veriş sitelerinden ürün satın alırken sitesinin ne tür özelliklerine dikkat etmektedirler?
   o. Parola belirlerken dikkat ettikleri kriterler nelerdir?
   p. Yazılım ihtiyaçları olduğunda ne şekilde temin etmektedirler?
   q. Bilişim güvenliği konusunda bilgi aldıkları internet sitesi, resmi ve özel kurum / kuruluşlar vb. kaynaklar nelerdir?

Araştırmada uygulanan ankette amaç toplam puan elde etmek değil, sorulan sorularda istenen özelliğin gerçek durumunu ortaya koymaya yöneliktir. Ankette bulunan 48 soru 3'lü likert ("Benim İçin Doğru", "Kararsızım", "Benim İçin Doğru Değil") ve 18 soru da demografik bilgiler ile kullanım alışkanlıklarını ölçmeye yönelik sorulardan oluşmaktadır. Ayrıca 4 soru da açık olarak düzenlenerek katılımcıların bilgi ve fikirleri toplanmıştır. Açık uçlu sorulara verilen yantlar için içerik analizi yapılarak sunulmuştur. Çalışmada kullanılan anket formu tezin ekler bölümünde yer almaktadır.

3.4.2 Balküpü Sisteminin Uygulaması

İç ağda konuşlandırılacak olan olan bal küpü uygulaması ile site erişim denemeleri, sunucu erişim denemeleri ve port taramaları için açık portlar barındıran ve saldırganların erişimine açık bırakılan bu noktalara giriş denemelerini kayıt altına alan tuzaklar kurulmuştur. Tuzak makinalar üzerinde bu amaçla 3 adet sensör devreye alınmıştır. Bunlar, p0f, Glastopf ve Kippo Cowrie'dir.

Kippo Cowrie ile ssh uzak bağlantı portundan yapılan talepler dinlenmektedir. Kippo python programlama dili ile yazılmış bir balküpüdür (Arıkan & Benzer, 2018). Varsayılan porttan dinleme yapar ve saldırganlara saldırılarının başarılı olduğuna dair yanıt dönerken, saldırganın kullandığı komutları da kayıt altına almaktadır. Bu bize başarılı bir saldırının ardından yapılacak işlemler hakkında sonuç çıkartmamızda yardımcı olacaktır.

Glastopf ile web uygulamalarına yönelik talepler dinlenmektedir. Glastopf ile uzaktan dosya ekleme, POST istekleri ve HTML enjeksiyonu için açıklıklar yaratılmakta ve yapılan korsan denemeler kayıt altına alınabilmektedir (glastopf, 2019). Glastopf python diliyle yazılmış minimalist bir web sunucu emülatörüdür ve web uygulaması tabanlı saldırılar hakkında bilgi toplayabilmektedir (Rist, 2019).

p0f sensör ile TCP/IP atakları dinlenmektedir. Bu sensör TCP/IP iletişimdeki SYN paketleri kadar küçük paketleri tanımlayabilmek için bir trafik izi mekanizması kullanmaktadır (Zalewski, 2012). Bu sensör ile TCP/IP paketleri için tuzak oluşturulacak ve yapılan saldırılar kayıt altına alınacaktır.

Tuzak sistemdeki sensörler için okul web sitesi veya başka bir alanda erişim linki düzenlenmemiştir. Dolayısıyla bu sensörleri bir web sayfası, dosya sunucusu, uygulama sunucusu gibi algılayarak erişmeye çalışan insanların ağ üzerinde tarama veya ağ cihazlarında yetki yükseltme işlemleri gibi eylemler ile sensörlerin varlığını tespit etmesi ve sonrasında bunlara saldırıda bulunması gerekmektedir. Sonuç olarak sensörlere erişim yapan tüm kullanıcılar birer saldırgan olarak tanımlanabilir.

Balküpü sistemi için MHN (Modern Honey Network-Modern Balküpü Ağı) sunucu ve bununla beraber çalışacak iki adet istemci bilgisayar kurulmuştur. Kullanılan sensörler Oracle VM masaüstü sanallaştırma yazılımı ile oluşturulmuş sanal sunucular üzerinde kurulmuştur. Kurulan bu balküpü sistemi için açık kaynak tabanlı Debian altyapısını kullanan Pardus Ahtapot sürümü ile birlikte yine açık kaynak tabanlı SUSE Linux işletim sistemleri kullanılmıştır. Pardus Ahtapot, derinlemesine savunma için ihtiyaç duyulan siber güvenlik bileşenlerinin bir araya getirildiği bir sistemdir (ahtapot.org.tr, 2019). İstemciler, sistemin tuzak makinalarını oluşturacak, MHN ise verilerin depolanmasından ve tuzak makinaların yönetiminden sorumlu olacaktır. Bu sayede doğası gereği açıklık barındıran tuzak sistemlerde bir problen yaşanması durumunda MHN çalışmaya devam edebilecektir. Sorun yaşanan tuzak bilgisayarı yeniden kurularak veya üzerindeki sensör başka bir sunucuya aktarılarak sistemin kullanımına devam edilebilecektir.

3.5 Veri Toplama Süreçleri

Araştırmanın hedef kitlesini Uluslararası Kıbrıs Üniversitesinin farklı bölümlerde okuyan öğrencileri oluşturmaktadır. Sınıf ortamında doldurulan anketler yine aynı sınıfta toplanarak akademik personele teslim edilmiştir. Toplam 272 öğrenciye ulaşılmıştır. Tüm anketler incelenmiş ve katılımcılar tarafında yeterince doldurulmayan 30 adet anket araştırmanın güvenirliliğini düşürmemesi için çalışmadan çıkarılmıştır. Kullanılmaya uygun 242 anket çalışmaya dahil edilmiştir.

Balküpü sistemi üniversitenin bilgisayar salonunda korunaklı bir odada konuşlandırılmıştır. Bilgisayar salonu gece çok geç saatlere kadar açık olduğundan ağa erişimde kesinti olmadığı varsayılmıştır. Sistem okulun birinci yarıyılında iki ay süresince aktif olarak çalışmıştır.

BÖLÜM 4

BULGULAR

Bu araştırmada uygulanan anketten toplanan ve balküpü tuzak sisteminden toplanan veriler sonucunda elde edilen bilgiler ve bu bilgiler ışığında derlenen analizler aşağıda sunulmuştur.

4.1 Bilişim Güvenliği Farkındalığı Anketinin Demografik Bilgileri

Uluslararası Kıbrıs Üniversitende uygulanan bilişim güvenliği farkındalık anketi demografik bilgileri aşağıda yer almaktadır.

Tablo 4.1 Katılımcıların Bölümlere Göre Dağılımları

Bölümler	Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
Özel Eğitim Öğretmenliği	51	21,1	21,1	21,1
Okul Öncesi Öğretmenliği	107	44,2	44,2	65,3
Türkçe Öğretmenliği	22	9,1	9,1	74,4
BESYO	9	3,7	3,7	78,1
PDR	16	6,6	6,6	84,7
Sınıf öğretmenliği	25	10,3	10,3	95,0
Bilgisayar öğretmenliği	12	5,0	5,0	100,0
Toplam	242	100,0	100,0	

Katılımcıların bölümlere göre dağılımlarına ait demografik dağılımları Tablo 4.1'de görülmektedir. Ankete katılan öğrencilerin 7 farklı bölümde eğitim görmektedirler.

Tablo 4.2 Katılımcıların Öğrenim Gördükleri Sınıfa İlişkin Dağılımları

Öğrenim Gördükleri Sınıf	Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
1	50	20,7	20,7	20,7
2	71	29,3	29,3	50,0
3	64	26,4	26,4	76,4
4	57	23,6	23,6	100
Toplam	242	100,0	100,0	

Katılımcıların kaçıncı sınıfta okuduklarına ilişkin demografik dağılımları Tablo 4.2'de görülmektedir. Ankete her sınıftan %20 ve üzerinde öğrenci katılım sağlamıştır.

Tablo 4.3 Katılımcıların Cinsiyete Göre Dağılımları

Cinsiyetleri	Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
Kadın	152	62,8	62,8	62,8
Erkek	90	37,2	37,2	100,0
Toplam	242	100,0	100,0	

Katılımcıların cinsiyetlerine göre dağılımları Tablo 4.3'de görülmektedir.

Tablo 4.4 Katılımcıların Doğdukları Ülkelere Göre Dağılımları

Ülkeler	Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
Türkiye Cumhuriyeti	221	91,3	91,3	91,3
K.K.T.C.	19	7,9	7,9	99,2
Suudi Arabistan	1	,4	,4	99,6
Türkmenistan	1	,4	,4	100,0
Toplam	242	100,0	100,0	

Katılımcıların doğdukları ülkelere göre dağılımları Tablo 4.4'de görülmektedir.

Tablo 4.5 Katılımcıların Yaşlarına Göre Dağılımları

Yaş Grupları	Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
18	3	1,2	1,2	1,2
19	22	9,1	9,1	10,3
20	36	14,9	14,9	25,2
21	48	19,8	19,8	45,0
22+	133	55,0	55,0	100,0
Toplam	242	100,0	100,0	

Katılımcıların yaşlarına göre dağılımları Tablo 4.5'de görülmektedir. Katılımcılarda 22 yaş üstü yoğunluk bulunmakla birlikte 18-21 yaş arası katılımcılar da bulunmaktadır.

Tablo 4.6 Katılımcıların Mezun Oldukları Liselere Göre Dağılımları

Mezun Olunan Lise	Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
Düz Lise	155	64,0	64,0	64,0
Meslek Lisesi	83	34,3	34,3	98,3
Fen Lisesi	4	1,7	1,7	100,0
Toplam	242	100,0	100,0	

Katılımcıların mezun oldukları liseye göre dağılımları Tablo 4.6'da görülmektedir.

4.2 Bilişim Güvenliği Farkındalık Anketi Bulguları

Uluslararası Kıbrıs Üniversitesinde uygulanan bilişim güvenliği farkındalık anketi ile toplanan bulgular aşağıda sunulmuştur.

Parola Soruları ile İlgili Bulgular

Katılımcılar tarafından parola güvenliği ile ilgili sorulara verilen yanıtlar ve istatistiki bilgiler Tablo 4.7'de sunulmuştur.

Tablo 4.7 Parola Sorularına Verilen Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S1- "Farklı e-posta adreslerim için aynı parolayı (şifreyi) kullanırım."	Benim İçin Doğru (BD)	137	56,6	56,6	56,6
	Kararsızım	40	16,5	16,5	100,0
	Benim İçin Doğru Değil (BDD)	65	26,9	26,9	83,5
	Toplam	242	100,0	100,0	

S2-“Farklı sitelere üye olurken aynı kullanıcı adı ve parolayı kullanırım.”	BD	127	52,5	52,5	52,5
	Kararsızım	59	24,4	24,4	76,9
	BDD	56	23,1	23,1	100,0
	Toplam	242	100,0	100,0	
S7-“İnternette parolamı yazarken yakın arkadaşlarımın parolamı görmesi benim için sorun değildir.”	BD	65	26,9	26,9	74,0
	Kararsızım	63	26,0	26,0	100,0
	BDD	114	47,1	47,1	47,1
	Toplam	242	100,0	100,0	
S8-“Güvendiğim insanlara kullanıcıadı ve şifremi veririm.”	BD	63	26,0	26,0	74,8
	Kararsızım	61	25,2	25,2	100,0
	BDD	118	48,8	48,8	48,8
	Toplam	242	100,0	100,0	
S13-“Parolamı yönetmek (saklamak) için bir bilgisayar yazılımı kullanırım.”	BD	55	22,7	22,7	100,0
	Kararsızım	73	30,2	30,2	77,3
	BDD	114	47,1	47,1	47,1
	Toplam	242	100,0	100,0	
S28-“Parolamı belirli zaman aralıklarında değiştiririm.”	BD	104	43,0	43,0	43,0
	Kararsızım	74	30,6	30,6	73,6
	BDD	64	26,4	26,4	100,0
	Toplam	242	100,0	100,0	
S43-“Nasıl güvenli bir parola belirleyeceğim hakkında bilgi sahibiyim.”	BD	171	70,7	70,7	70,7
	Kararsızım	50	20,7	20,7	91,3
	BDD	21	8,7	8,7	100,0
	Toplam	242	100,0	100,0	
S44-“Parola güvenliğinin zayıf, orta, yüksek olmasının parolamın güvenliğini nasıl etkilediğini biliyorum.”	BD	172	71,1	71,1	71,1
	Kararsızım	55	22,7	22,7	93,8
	BDD	15	6,2	6,2	100,0
	Toplam	242	100,0	100,0	

Tablo 4.7’deki sonuçları incelediğimizde ankete katılan öğrencilerin yarısından fazlasının farklı site üyelikleri ile e-posta adresleri için aynı kullanıcı adı

ve parolayı kullandıkları görülmektedir. Yakın arkadaşlar tarafından parolanın görülmesi %47,1 ve güvenilen insanlara kullanıcı adı ile şifrelerin verilmesi hususu ise yalnızca %48,8 oranındaki katılımcı tarafından doğru bir davranış olarak görülmemiştir. Katılımcıların yarıdan fazlası ya doğru bulmuş ya da konu hakkında kararsız kalmıştır.

Buna rağmen katılımcıların ortalama %70'i güvenli parola oluşturmak konusunda bilgi sahibi olduklarını düşünmekte ve parola güvenliğinin zayıf, orta, yüksek olmasının güvenliğe etkilerinin farkında olduklarını düşünmelerine karşın yalnızca %43 oranında katılımcının parolasını belirli zaman aralıklarında değiştirdikleri görülmüştür.

Katılımcıların yalnızca %22,7'si parola yönetimi için bir bilgisayar yazılımı kullandıklarını belirtmişlerdir.

Katılımcıların 43 ve 44 numaralı sorulara verdiği yanıtlarla yüksek oranda parola güvenliği konusunda bilgi sahibi olduklarını düşünmelerine karşın özellikle kararsızların oranıda dikkate alındığında diğer sorulara verilen yanıtların bu düşünceleri ile çeliştiği görülmektedir. Bu durum öğrencilerin parola kullanımı konusunda güvenlik açığına sebep olabileceklerini ve bu konuda farkındalıklarının yeterli olmadığını göstermektedir.

İnternet Üzerinden Alış-Veriş Hakkında Verilen Yanıtlara Ait Bulgular

Katılımcıların internet üzerinden alış-veriş yaparken dikkat ettikleri konular hakkındaki sorulara verdikleri cevaplar ve istatistiki bilgiler Tablo 4.8'de gösterilmiştir.

Tablo 4.8 İnternet Üzerinden Alış-Veriş Hakkındaki Sorulara Verdikleri Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S4-"Kişisel bilgisayarımın dışındaki bilgisayarlar üzerinden internet aracılığı ile alış veriş yaparım."	BD	55	22,7	22,7	100,0
	Kararsızım	67	27,7	27,7	77,3
	BDD	120	49,6	49,6	49,6
	Toplam	242	100,0	100,0	
S5-"İnternette alış-veriş yaparken internetten ödeme güvenliği hakkında nelere dikkat etmem gerektiğini bilirim."	BD	176	72,7	72,7	72,7
	Kararsızım	45	18,6	18,6	91,3
	BDD	21	8,7	8,7	100,0
	Toplam	242	100,0	100,0	
S6-"Kredi kartım ile ilgili önemli bilgileri girerken eğer varsa sanal klavye kullanırım."	BD	94	38,8	38,8	38,8
	Kararsızım	59	24,4	24,4	100,0
	BDD	89	36,8	36,8	75,6
	Toplam	242	100,0	100,0	

Katılımcıların, Tablo 4.8'de verdikleri yanıtlar incelendiğinde yaklaşık %73 ile ödeme güvenliği hususunda bilgi sahibi olduklarını düşünmektedirler. Fakat buna rağmen katılımcıların yalnızca yaklaşık % 39'u sanal klavye kullanmakta ve sadece yaklaşık yarısı kişisel bilgisayarları dışındaki bilgisayarları kullanarak internet üzerinden alış veriş yapmayı kesin bir şekilde hatalı bulmaktadırlar.

Ortaya çıkan tablo ile katılımcıların genel olarak internet üzerinden alış veriş ile ilgili nelere dikkat etmeleri gerektiğini bildikleri fakat bunu yeterince uygulamadıkları tespit edilmiştir.

Kullanıcıların Bilgisayar Hesap Güvenliği Hakkındaki Sorulara Verdikleri Cevaplara Ait Bulgular

Katılımcılar tarafından bilgisayar kullanıcı hesapları ve güvenliği ile ilgili sorulara ilişkin yanıtları ve istatistiki bilgiler Tablo 4.9'da sunulmuştur.

Tablo 4.9 Kullanıcıların Bilgisayar Kullanıcı Hesap Güvenliği Hakkındaki Sorular Verdikleri Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S3-"Bana ait olmayan bir bilgisayardan internete girerken, tarayıcının kişisel bilgilerimi kaydedip kaydetmediğini kontrol ederim."	BD	203	83,9	83,9	83,9
	Kararsızım	23	9,5	9,5	93,4
	BDD	16	6,6	6,6	100,0
	Toplam	242	100,0	100,0	
S9-"Bilgisayarımda bir açılış parolası kullanırım."	BD	128	52,9	52,9	52,9
	Kararsızım	54	22,3	22,3	100,0
	BDD	60	24,8	24,8	77,7
	Toplam	242	100,0	100,0	
S10-"Bilgisayarımı kullanmak isteyen kişiler için açtığım, ayrı, sınırlı bir oturum vardır."	BD	56	23,1	23,1	100,0
	Kararsızım	61	25,2	25,2	76,9
	BDD	125	51,7	51,7	51,7
	Toplam	242	100,0	100,0	
S11-"Bilgisayarımda kendi oturumumdaki önemli belgeler şifreli haldedir."	BD	89	36,8	36,8	75,6
	Kararsızım	59	24,4	24,4	100,0
	BDD	94	38,8	38,8	38,8
	Toplam	242	100,0	100,0	
S12-"Bilgisayarımı kullanmak isteyen olursa sadece konuk oturumunu kullanmasına izin veririm."	BD	59	24,4	24,4	100,0
	Kararsızım	68	28,1	28,1	75,6
	BDD	115	47,5	47,5	47,5
	Toplam	242	100,0	100,0	

Katılımcıların Tablo 4.9'da verdikleri yanıtlar incelendiğinde yalnızca %24,4'ünün bilgisayarlarını kullanmak isteyenler için konuk hesap ile kullanıma izin verdikleri bunun yanında kararsızlarla birlikte yaklaşık %75 oranındaki katılımcının buna dikkat etmediği görülmektedir. Katılımcıların yalnızca %36,8'i önemli belgelerini şifreli olarak saklamaktadırlar.

Katılımcılar %83,9 oranında başka bir bilgisayardan internete girerken tarayıcının kişisel bilgileri kaydedip kaydetmediğini kontrol ettiklerini belirtemekte ve %52,9 oranında katılımcının bilgisayarlarında açılış parolası kullandıklarını belirtmişlerdir.

Ortaya çıkan tablo, öğrencilerin internet kullanımı esnasında hesap bilgilerinin risk altında olduğu hususununda farkındalıklarının yüksek olduğu ve internette gezinirken buna dikkat ettiklerini fakat bunun için yeterince önlem almadıklarını göstermektedir.

Antivirüs ve Zararlı Yazılımları Engelleme Hakkındaki Sorulara Verilen Yanıtlara Ait Bulgular

Katılımcıların antivirüs ve zararlı yazılımları engelleme hakkındaki sorulara verdikleri yanıtlar ve istatistiki bilgiler Tablo 4.10'da sunulmuştur.

Tablo 4.10 Antivirüs ve Zararlı Yazılımların Engellemesi Hakkındaki Sorulara Verilen Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S21-"İnternetten bilgisayarıma indirdiğim dosyaları açmadan önce virüs taramasından geçiririm."	BD	91	37,6	37,6	37,6
	Kararsızım	85	35,1	35,1	72,7
	BDD	66	27,3	27,3	100,0
	Toplam	242	100,0	100,0	
S22-"USB Bellek, harici disk veya cd-dvd medyası bilgisayarıma bağlandığında öncelikle anti-virüs taramasından geçiririm."	BD	96	39,7	39,7	39,7
	Kararsızım	88	36,4	36,4	76,0
	BDD	58	24,0	24,0	100,0
	Toplam	242	100,0	100,0	
S29-"Bilgisayarımı belli zaman aralıklarında güvenlik taramasından geçiririm."	BD	118	48,8	48,8	48,8
	Kararsızım	81	33,5	33,5	82,2
	BDD	43	17,8	17,8	100,0
	Toplam	242	100,0	100,0	

S35-“İnternet kaynaklı tehditler ile ilgili yeterli bilgiye sahibim.”	BD	84	34,7	34,7	85,5
	Kararsızım	123	50,8	50,8	50,8
	BDD	35	14,5	14,5	100,0
	Toplam	242	100,0	100,0	
S42-“İnternet tarayıcım vasıtasıyla internette gezindiğim web sitelerinin güvenirliği ile ilgili bilgi edinmeye çalışırım.”	BD	131	54,1	54,1	54,1
	Kararsızım	78	32,2	32,2	86,4
	BDD	33	13,6	13,6	100,0
	Toplam	242	100,0	100,0	
S48-“Bilgisayarın güvenliğini sağlayacak yazılımları bulma ve kullanmada yeterli bilgiye sahibim.”	BD	71	29,3	29,3	76,4
	Kararsızım	114	47,1	47,1	47,1
	BDD	57	23,6	23,6	100,0
	Toplam	242	100,0	100,0	

Verilen yanıtlar incelendiğinde çok az bir orandaki (%29,3) katılımcının bilgisayar güvenliğini sağlayacak yazılımlar hakkında yeterli bilgiye sahip oldukları görülmektedir. Yine katılımcıların yalnızca %34,7’sinin internet kaynaklı tehditler konusunda yeterli bilgiye sahip olduğunu düşündüklerini ve yalnızca katılımcıların yaklaşık yarısının web sitelerinin güvenliği konusunda bilgi edinmeye çalıştıkları görülmektedir.

Katılımcıların yaklaşık %40’ının bilgisayarına bir dosya indirdiğinde veya harici bellekler üzerinden kopyaladığında antivirüs taramasından geçirdikleri ve ancak katılımcılarının yarıya yakınının belli zaman aralıklarında bilgisayarını güvenlik taramasından geçirdikleri görülmektedir.

İncelenen Tablo 10’a göre katılımcıların antivirüs ve zararlı yazılımları engelleme hakkındaki farkındalıklarının son derece yetersiz olduklarını söyleyebiliriz.

Korumasının düşük olduğu görülen ve kampüs ağına da bağlanan öğrenci bilgisayarları ağda ve ağa bağlı diğer istemciler üzerinde birçok problemin yaşanmasına sebep olabilir.

Güncelleme Soruları Hakkında Verilen Cevaplara Ait Bulgular

Katılımcıların, işletim sistemleri, güvenlik yazılımları ve ofis paket yazılımları güncellemesi hakkındaki sorulara verdikleri cevaplar ve istatistiki bilgiler Tablo 4.11'de sunulmuştur.

Tablo 4.11 Güncelleme Sorularına Verdikleri Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S14-"Kullandığım anti-virüs yazılımının güncelliğini denetlerim."	BD	127	52,5	52,5	52,5
	Kararsızım	67	27,7	27,7	80,2
	BDD	48	19,8	19,8	100,0
	Toplam	242	100,0	100,0	
S15-"İşletim sistemi güncellemelerini kontrol eder ve zamanında yüklerim."	BD	105	43,4	43,4	43,4
	Kararsızım	78	32,2	32,2	75,6
	BDD	59	24,4	24,4	100,0
	Toplam	242	100,0	100,0	
S16-"Kullandığım ofis yazılımlarının güncellemelerini denetlerim"	BD	105	43,4	43,4	43,4
	Kararsızım	80	33,1	33,1	76,4
	BDD	57	23,6	23,6	100,0
	Toplam	242	100,0	100,0	

Güncelleme konusu ile ilgili verilen yanıtlar incelendiğinde genel olarak katılımcıların yaklaşık yarısının antivirüs yazılımlarının güncelliğini kontrol etikleri, bu oranın işletim sistemi ve ofis uygulamalarında yaklaşık %40'a geriledği görülmektedir.

Görülen bu durum sonuçlar katılımcıların güncelleme konusundaki farkındalıklarının yeterli olmadığını göstermektedir.

Sosyal Ağ Hakkındaki Sorulara Verilen Cevaplara Ait Bulgular

Öğrencilerin, sosyal ağ hakkındaki sorulara ait verdikleri yanıtlar ve istatistiki bilgiler Tablo 4.12'de sunulmuştur.

Tablo 4.12 Sosyal Ağ Hakkındaki Sorulara Verilen Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S18-"Sosyal ağ sitelerinde tanımadığım insanları arkadaş listeme eklerim."	BD	34	14,0	14,0	100,0
	Kararsızım	66	27,3	27,3	86,0
	BDD	142	58,7	58,7	58,7
	Toplam	242	100,0	100,0	
S19-"Sosyal ağlarda kişisel bilgilerimi paylaşırım."	BD	27	11,2	11,2	100,0
	Kararsızım	65	26,9	26,9	88,8
	BDD	150	62,0	62,0	62,0
	Toplam	242	100,0	100,0	
S26-"Sosyal ağlarda tanıştığım insanlarla yüz yüze buluşurum."	BD	41	16,9	16,9	100,0
	Kararsızım	77	31,8	31,8	83,1
	BDD	124	51,2	51,2	51,2
	Toplam	242	100,0	100,0	
S27-"Kişisel fotoğraf ve videolarımı herkesin erişebileceği ortamlarda paylaşırım"	BD	34	14,0	14,0	100,0
	Kararsızım	66	27,3	27,3	86,0
	BDD	142	58,7	58,7	58,7
	Toplam	242	100,0	100,0	
S40-"Sosyal medya platformlarında bulunan kullanıcı hesaplarımın gizlilik ayarlarını yönetebilecek bilgiye sahibim."	BD	144	59,5	59,5	59,5
	Kararsızım	73	30,2	30,2	89,7
	BDD	25	10,3	10,3	100,0
	Toplam	242	100,0	100,0	

Sosyal Ağ hakkında düzenlenen sorulara yönelik düzenlenen ve Tablo 4.12'de görülen sonuçlar incelendiğinde katılımcıların yaklaşık %60'ı sosyal ağlarda

güvenlik ve gizlilik konularında bilgi sahibi oldukları görülmektedir. Katılımcıların Sosyal Ağ hakkındaki sorulara verdikleri yanıtlar, onların sosyal ağların kullanımında güvenlik ve gizliliklerine dair farkındalıklarının diğer konulara göre daha yüksek olduğunu göstermektedir. Buna rağmen halen %40 oranında bir kullanıcı grubunun farkındalıklarının yeterli olmadığı görülmekte ve bu konuda da bir farkındalık çalışması yapılmasına ihtiyaç olduğu anlaşılmaktadır.

Anlık Mesajlaşma Uygulamaları ile E-posta Güvenliği Hakkındaki Sorulara Verilen Cevaplara Ait Bulgular

Ankete katılan öürencilerin anlık mesajlaşma ve e-posta güvenliği hakkındaki sorulara verdikleri cevaplar ve istatistiki bilgiler Tablo 4.13'de sunulmuştur.

Tablo 4.13 Anlık Mesajlaşma ve E-posta Uygulamaları Güvenliği Hakkındaki Sorulara Verilen Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S17-"Anında ileti yazılımı kullanarak benimle dosya paylaşıldığında gelen dosya ile ilgili bilgim yoksa gönderen kişiye sormadan dosyayı açmam."	BD	109	45,0	45,0	45,0
	Kararsızım	85	35,1	35,1	80,2
	BDD	48	19,8	19,8	100,0
	Toplam	242	100,0	100,0	
S20-"Gönderenini tanımadığım bir epostaya eklenmiş dosyayı anti-virüs taramasından geçirmeden açarım."	BD	52	21,5	21,5	100,0
	Kararsızım	87	36,0	36,0	78,5
	BDD	103	42,6	42,6	42,6
	Toplam	242	100,0	100,0	
S30-"Göndereni tanımasam da tepkimi çeken postaları yanıtlarım."	BD	45	18,6	18,6	100,0
	Kararsızım	66	27,3	27,3	81,4
	BDD	131	54,1	54,1	54,1
	Toplam	242	100,0	100,0	

S31-“Anında ileti yazılımları kullanırken yazışmaları arşivlerim.”	BD	71	29,3	29,3	100,0
	Kararsızım	97	40,1	40,1	40,1
	BDD	74	30,6	30,6	70,7
	Toplam	242	100,0	100,0	
S34-“E-posta adresime gelen sahte içerikli postaları ‘‘Spam’’ olarak işaretlerim.”	BD	121	50,0	50,0	50,0
	Kararsızım	70	28,9	28,9	78,9
	BDD	51	21,1	21,1	100,0
	Toplam	242	100,0	100,0	
S37-“E-posta adresim kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğim konusunda bilgi sahibiyim.”	BD	90	37,2	37,2	74,8
	Kararsızım	91	37,6	37,6	37,6
	BDD	61	25,2	25,2	100,0
	Toplam	242	100,0	100,0	
S38-“Göndereni tanımadığım halde ilgimi çeken epostaları yanıtlarım.”	BD	31	12,8	12,8	100,0
	Kararsızım	80	33,1	33,1	87,2
	BDD	131	54,1	54,1	54,1
	Toplam	242	100,0	100,0	

Katılımcıların Tablo 4.13’de verdikleri yanıtlar incelendiğinde öğrencilerin %42,6’sının göndereni belli olmayan e-posta ve dosyaları anti-virüs yazılımları ile taramadan açmadıklarını, yarıdan fazlasının göndereni tanımadıkları e-postaları yanıtlamadıkları görülmektedir. Bunun yanında e-posta adresleri başkalarının eline geçerse nasıl geri alabilecekleri konusunda yalnızca %37,2 oranında bilgi sahibi oldukları görülmektedir.

Tablo 9’daki yanıtlar incelendiğinde e-posta ve anlık mesajlaşma güvenliği hakkında öğrencilerin yarıya yakınının farkındalıklarının olduğu fakat bir o kadar öğrencinin ise bu konuda yeterli seviyede bilgi sahibi olmadıkları görülmektedir.

Kablosuz Ağlardaki Güvenlik Hakkındaki Sorulara Verilen Cevaplar Ait Bulgular

Katılımcıların kablosuz ağ güvenliği hakkındaki sorulara verdikleri yanıtlar ve istatistiki bilgiler Tablo 4.14’de sunulmuştur.

Tablo 4.14 Kablosuz Ağlardaki Güvenlik Faktörleri Hakkındaki Sorulara Verilen Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S23-"Cep telefonum ya da bilgisayarım ile kaynağını / sahibini bilmediğim kablosuz ağlara bağlanırım."	BD	86	35,5	35,5	35,5
	Kararsızım	73	30,2	30,2	100,0
	BDD	83	34,3	34,3	69,8
	Toplam	242	100,0	100,0	
S32-"Şifrelenmemiş ve kimin sağladığını bilmediğim kablosuzağlara bağlanırım."	BD	98	40,5	40,5	40,5
	Kararsızım	62	25,6	25,6	100,0
	BDD	82	33,9	33,9	74,4
	Toplam	242	100,0	100,0	
S33-"Kablosuz internet ağımda şifre kullanmam."	BD	26	10,7	10,7	100,0
	Kararsızım	38	15,7	15,7	89,3
	BDD	178	73,6	73,6	73,6
	Toplam	242	100,0	100,0	

Katılımcıların cevapları incelendiğinde yüksek bir oranda (%73,6) kendi kablosuz ağlarında şifre kullandıkları görülmüştür. Kendilerine ait kablosuz ağlarda güvenliğe dikkat eden öğrencilerin kaynağı belli olmayan kablosuz ağlara bağlanma oranlarındaki yükseklik (yaklaşık %40) dikkati çekmektedir. Bu oran kararsızlarla birlikte %65'in üzerine çıkmaktadır. Katılımcıların yalnızca %34,3'ü bu tür ağlara bağlanmadıkları görüşünü bildirmişlerdir.

Bu durum öğrencilerin kablosuz ağlarında güvenlik önlemi almaları altında yatan sebeplerin sorgulanmasını gerektirmektedir. Bunun sebepleri arasında servis sağlayıcıların önerileri ve ilk kurulumları ile birlikte gelen şifre uygulaması, satın aldıkları hizmetin kullanıcı sayısının artmasıyla kalitesinin düşme endişesi veya kota aşımı sorunu olabilir? Aksi takdirde içinde bulundukları ağa tanımadıkları insanların girmesi ve herhangi bir güvenlik politikası olmadan aynı ağda farklı bilgisayarlar ile

birlikte çalışacaklarını bilen katılımcıların bu tür güvensiz bir bağlantıyı reddetmeleri beklenirdi.

Bilişim Güvenliği Hakkındaki Yasalar ve Etik Konulara İlişkin Sorulara Verilen Cevaplara Ait Bulgular

Katılımcıların bilişim güvenliği hakkındaki yasalar ve etik konularla ilgili cevapları ile cevapların dağılımına ait istatistiki bilgiler Tablo 4.15'de sunulmuştur.

Tablo 4.15 Bilişim Güvenliği Hakkındaki Yasalar ve Etik Konulara İlişkin Sorulara Verilen Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S24-"Bilgisayarımdaki yazılımları lisans bedellerini ödeyerek satın aldıktan sonra kullanırım."	BD	65	26,9	26,9	100,0
	Kararsızım	95	39,3	39,3	39,3
	BDD	82	33,9	33,9	73,1
	Toplam	242	100,0	100,0	
S25-"Bilgisayarımda yasa dışı yolla edinilmiş (kırılmış) yazılımlar bulunmaktadır."	BD	37	15,3	15,3	100,0
	Kararsızım	53	21,9	21,9	84,7
	BDD	152	62,8	62,8	62,8
	Toplam	242	100,0	100,0	
S39-"Yazılım kullanmada telif hakları konusundayeterli bilgi sahibiyim."	BD	46	19,0	19,0	100,0
	Kararsızım	130	53,7	53,7	53,7
	BDD	66	27,3	27,3	81,0
	Toplam	242	100,0	100,0	

Katılımcıların yasal ve etik konular hakkındaki görüşleri incelendiğinde yalnızca %19'unun yazılım telif hakkı konusunda bilgi sahibi olduğu, yarıdan fazlasının bilgilerinden emin olmadıklarını ve %27,3 oranında da bilgi sahibi olmadıklarını görmekteyiz. Yalnızca yaklaşık %27 oranında katılımcının lisans

bedellerini ödedikleri yazılımları kullandıklarını belirttikleri çalışmada yaklaşık %63 oranında ise yasadışı yollarla edinilmiş yazılım kullanmadıklarını (olumsuz) belirtmişlerdir. Bu analiz ışığında öğrencilerin bilişim güvenliği hakkındaki yasal ve etik konularda yeteri kadar farkındalık sahibi olmadıklarını görülmektedir. Bu durum, öğrencilere bilişim güvenliğinin kanuni ve etik çerçeveleri hakkında bilgi seviyelerinin artırılması için farkındalık çalışmaları yapılmasının bir gereklilik olduğunu göstermektedir.

Katılımcıların Bilişim Güvenliği Konusundaki Bilgilerini Güncelleme ile İlgili Sorulara Verdikleri Cevaplara İlişkin Bulgular

Katılımcıların bilişim güvenliği hakkındaki bilgilerini güncellemeye yönelik sorulara verdikleri yanıtlar ve istatistiki bilgiler Tablo 4.16'da sunulmuştur.

Tablo 4.16 Bilişim Güvenliği Konusundaki Bilgilerini Güncelleme ile İlgili Sorulara Verilen Cevapların Dağılımları

Soru		Frekans	Yüzde	Geçerli Yüzde	Yığılan Yüzde
S36-"Kullandığım internet tarayıcısının güvenlik ayarları hakkında yeterli bilgi sahibiyim."	BD	81	33,5	33,5	82,2
	Kararsızım	118	48,8	48,8	48,8
	BDD	43	17,8	17,8	100,0
	Toplam	242	100,0	100,0	
S41-"İnternet tarayıcım vasıtasıyla internette gezindiğim web sitelerinin güvenirliği ile ilgili bilgi edinmeye çalışırım."	BD	116	47,9	47,9	47,9
	Kararsızım	91	37,6	37,6	85,5
	BDD	35	14,5	14,5	100,0
	Toplam	242	100,0	100,0	
S45-"Bilişim güvenliği konusunda bilgi alabileceğim adresleri bilirim."	BD	66	27,3	27,3	77,7
	Kararsızım	122	50,4	50,4	50,4
	BDD	54	22,3	22,3	100,0
	Toplam	242	100,0	100,0	

S46-“Bir bilişim suçuna maruz kalırsam kime başvuracağımı biliyorum.”	BD	83	34,3	34,3	78,1
	Kararsızım	106	43,8	43,8	43,8
	BDD	53	21,9	21,9	100,0
	Toplam	242	100,0	100,0	
S47-“Bir bilişim güvenliği sitesini düzenli olarak takip ederim.”	BD	41	16,9	16,9	100,0
	Kararsızım	119	49,2	49,2	49,2
	BDD	82	33,9	33,9	83,1
	Toplam	242	100,0	100,0	

Katılımcıların cevapları incelendiğinde %33,5’inin kullandıkları web tarayıcısının güvenlik ayarları hakkında bilgi sahibi oldukları görülmekte fakat yarıya yakınının web tarayıcıları aracılığıyla girdikleri sitelerin güvenilirliği hakkında bilgi sahibi olmaya çalıştıkları görülmektedir. Buna rağmen öğrenciler bu bilgileri genel olarak nereden elde edecekleri konusunda bilgi sahibi değillerdir.

Bir bilişim suçuna maruz kaldıklarında nereye başvuracağı hakkında bilgi sahibi olan öğrencilerin oranı yalnızca %34,3 olarak görülmüştür. Öğrencilerin çok az bir bölümü bir bilişim güvenliği sitesini düzenli olarak takip ettiklerini dile getirmişlerdir.

Tablo 4.7 – 4.16 sonuçlarına göre H1 ve H2 hipotezleri kabul edilmiştir.

Katılımcıların Cinsiyetlerine Göre Verdikleri Cevapların Dağılımlarındaki Değişimlere İlişkin Bulgular

Katılımcıların cevaplarının cinsiyet değişkenine göre incelendiğinde dağılımlarda anlamlı bir fark görülen sorular Tablo 4.17’de gösterilmiştir.

Tablo 4.17 Cinsiyet Değişkenine Göre Ki-Kare Test Sonuçları

Soru		Kadın %	Erkek %
S10– "Bilgisayarımı kullanmak isteyen kişiler için açtığım, ayrı, sınırlı bir oturum vardır."	BD	20,4	27,8
	Kararsızım	17,1	38,9
	BDD	62,5	33,3
S18– "Sosyal ağ sitelerinde tanımadığım insanları arkadaş listeme eklerim."	BD	9,9	21,1
	Kararsızım	21,7	36,7
	BDD	68,4	42,2
S25– "Bilgisayarımda yasa dışı yolla edinilmiş (kırılmış) yazılımlar bulunmaktadır."	BD	9,2	25,6
	Kararsızım	17,1	30,0
	BDD	73,7	44,4
S26– "İnternette, sosyal ağlarda, anında ileti yazılımlarıyla tanıştığım bir insan ile yüz yüze görüşürüm."	BD	10,5	27,8
	Kararsızım	28,3	37,8
	BDD	61,2	34,4
S36– "Kullandığım internet tarayıcısının güvenlik ayarları hakkında yeterli bilgi sahibiyim."	BD	24,3	48,9
	Kararsızım	57,9	33,3
	BDD	17,8	17,8
S37–"E-posta adresim kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğim konusunda bilgi sahibiyim."	BD	26,3	55,6
	Kararsızım	44,1	26,7
	BDD	29,6	17,8
S38– "Göndereni tanımadığım halde ilgimi çeken epostaları yanıtlarım."	BD	8,6	20,0
	Kararsızım	27,6	42,2
	BDD	63,8	37,8
S48–"Bilgisayarımın güvenliğini sağlayacak yazılımları bulma ve kullanmada yeterli bilgiye sahibim."	BD	18,4	47,8
	Kararsızım	53,9	35,6
	BDD	27,6	16,7

Tablo 4.17'deki sonuçlar ışığında, erkekler %33,3 oranında bilgisayarlarını kullanmak isteyenler için ayrı bir oturum açmayı gerekli görmezken bu oran kadınlarda %62,5 olarak görülmüştür. Kadınlar, sosyal ağ sitelerinde tanımadıkları kişileri %9,9 oranında eklediklerini belirtirken bu oran erkeklerde %21,1 olarak görülmüştür. Kadınlar yüksek bir oranda (%73,7) yasa dışı yollarla edinilmiş programların kullanımını doğru bulmazken, erkeklerin %25,6'sı kullandıklarını dile getirmiş ve %30'u ise kararsız kalmıştır. Kararsızlarla birlikte erkeklerin yarısından fazlası yasa dışı yollarla edinilmiş programların kullanımına yatkın görülmektedir. Kadınların %61,2'si sosyal ağlarda tanıştıkları insanlarla yüzyüze görüşmenin doğru olmadığını dile getirirken erkeklerde bu oran %34,4 olarak görülmüştür. Kullandıkları internet tarayıcısının güvenlik ayarları hakkında erkekler %48,9 bilgi sahibi olduklarını düşünürken bu oran kadınlarda %24,3 olarak ölçülmüştür. E-posta adreslerinin tanımadıkları kişilerin eline geçmesi durumunda ne yapılabileceği konusunda erkekler %55,6 bilgi sahibi olduklarını dile getirirken bu oran kadınlarda %26,3 olarak ölçülmüştür. Göndereni tanınmayan e-postaları yanıtlayabileceğini söyleyenler ise kadınlarda %8,6 iken erkeklerde %20 olarak görülmüştür. Kadınlar %63,8 ile yüksek oranda yanıtlamayacaklarını dile getirmişlerdir. Bilgisayar güvenliğini sağlayacak yazılımları bulma ve kullanma konusunda erkekler (%47,80), kadınlara (%18,4) göre daha bilgili olduklarını dile getirmişlerdir.

Alış-Veriş Sitelerinden Ürün Satın Alırken Sitenin Ne Tür Özelliklerine Dikkat Ettikleri Hakkındaki Sorulara Verilen Cevaplara Dağılımı

Katılımcıların internet üzerinden alış-veriş yaparken sitedeki dikkat ettikleri özelliklere ilişkin bulgular Tablo 4.18'de gösterilmiştir.

Tablo 4.18 Alış-veriş Sitelerinden Ürün Satın Alırken Sitenin Ne Tür Özelliklerine Dikkat Ettikleri Hakkındaki Sorulara Verilen Cevapların Dağılımları

Cevaplar	%	f
Güvenirliğine dikkat ederim	57,0%	138
Marka değeri ve tanınmış olması	21,1%	51
Kalite	8,3%	20
Reklamların yönlendirmesi	2,1%	5
Site ve arkadaş yorumları	17,4%	42
Kurumsallık	6,2%	15
Kargo seçenekleri ve teslimat süresi	5,4%	13
Ödeme yöntemi	3,3%	8
Teknolojik yenilik ve güvenlik ölçütleri	4,5%	11
Uygun fiyatlı ürünler	5,0%	12
Site görünümü ve kullanım kolaylığı	3,3%	8
Gizlilik	1,7%	4
Müşteri hizmetleri kalitesi	1,7%	4
İnternet üzerinden alış-veriş yapmıyorum	5,8%	14

Katılımcıların Tablo 4.18'de verdiği cevaplar incelendiğinde güvenirliğe dikkat edenlerdeki %57'lik yüksek oran dikkati çekmektedir. Öte yandan katılımcılar güvenirliği destekleyecek çok fazla özelliğe değinmemişlerdir. Önemli özelliklerden olan gizliliğe %1,7 ile sadece 4 katılımcı, ödeme yöntemine %3,3 ile 8 kullanıcı değinmiştir. Katılımcıların güvenirlik ile ilgili farkındalıklarının yüksek olmasının yanında bu konuda yeteri kadar bilgiye sahip olmadıkları anlaşılmaktadır.

Parola Belirlerken Parolanın Hangi Özellikleri Taşımasının Önemli Olduğuna Dair Sorulara Verlen Yanıtlara Ait Bulgular

Katılımcıların parola belirlerken parolanın hangi özellikleri taşımasına dikkat ettiklerine dair bulgular Tablo 4.19'da gösterilmiştir.

Tablo 4.19 Parola Belirlerken Dikkat Ettikleri Kriterler Hakkındaki Sorulara Verilen Cevapların Dağılımları

Cevaplar	%	f
Zor olmasına, bilinen kelimeleri içermemesine	13,2%	32
Güçlü ve karmaşık olmasına, en az 8 karakter içermesine	7,9%	19
Rakam, sembol ve harf içermesine	35,1%	85
Kolay hatırlanabilir olmasına	24,4%	59
Ardışık gelen sayı ve harflerden oluşmamasına	2,1%	5
Farklı, gizli ve güvenilirliği yüksek olmasına	8,3%	20
Kişisel bilgiler içermesine (olumlu)	1,2%	3
Kişisel bilgiler içermemesine (olumsuz)	3,7%	9
Özel kavramlar (gün, tarih, yer vb..) içermesine	4,1%	10
Kısa olmasına	0,4%	1

Katılımcıların Tablo 4.19'da verdikleri yanıtlar incelendiğinde karmaşıklık, güçlü parola seçimi ve parolanın kolay tespit edilmemesine ilişkin yüksek oranda bir farkındalık olduğu görülmektedir. Kolay hatırlanabilir parola tercih edenlerin oranı (%24,4) ise azımsanamayacak kadar çoktur.

Bir Yazılıma İhtiyaç Duyduklarında Nasıl Temin Ettikleri Konusundaki Sorulara Verilen Cevaplara Ait Bulgular

Katılımcıların bir yazılıma ihtiyaç duyduklarında nasıl temin ettiklerine dair bulgular Tablo 4.20'de gösterilmiştir.

Tablo 4.20 Yazılım İhtiyacı Olduğunda Ne Şekilde Temin Ettikleri Hakkındaki Soruya Verilen Cevapların Dağılımları

Cevaplar	%	f
İnternet üzerinden araştırarak	15,7%	38
Hiç ihtiyaç duymadım	7,0%	17
Bilen kişilerden yardım isterim	41,3%	100
Yasa dışı yollardan temin ederim	3,7%	9
Online alışveriş ile satın alırım	1,2%	3

Katılımcıların Tablo 4.20'de verdikleri yanıtlar incelendiğinde katılımcıların yüksek oranda internetten ve bilen kişilerden yardım alarak temin ettikleri görülmektedir. Sadece 3 katılımcı online alışveriş seçeneğini değerlendirmiştir ve bir mağazadan satın almayı düşünen katılmcı ise hiç yoktur. Yasa dışı yolları tercih edebileceğini yani kaçak yazılım kullanacağını söyleyen katılımcılarda bulunmaktadır. Bu durum diğer katılımcıların kaçak yazılıma yönelebileceklerini düşündürmektedir.

Kaçak yazılımlar bilişim güvenliğini tehlikeye atabilecek önemli etmenlerdendir. Kaçak yazılım kullanılan bilgisayarlar üniversite ağını ve ağdaki diğer kullanıcıların güvenirliğini tehlikeye sokabileceğinden bu konuda bir farkındalık çalışmasının yanı sıra kontrolden geçirilmiş bir yazılım deposu hizmeti sunulması da düşünülebilir.

Bilişim Güvenliği Hakkında Bilgi Aldıkları Kaynaklar Konusundaki Sorulara Verilen Cevaplara Ait Bulgular

Katılımcıların bilişim güvenliği hakkında bilgi aldıkları internet sitesi, resmi ve özel kurum / kuruluşlar gibi kaynaklara dair bulgular Tablo 4.21'de gösterilmiştir.

Tablo 4.21 Bilişim Güvenliği Hakkında Bilgi Aldığınız İnternet Sitesi, Resmi ve Özel Kurum / Kuruluşlar vb. Kaynaklara Dair Verilen Cevapların Dağılımları

Cevaplar	%	f
Bilgi aldığım bir yer yoktur	33,1%	80
İnternet ve arama motorları (Google, Wikipedia)	6,2%	15
Çevremdeki deneyimli kişilerden ve firmalardan	0,8%	2
Eğitim / kursa giderek	1,2%	3

Katılımcıların Tablo 4.21'de verdikleri yanıtlar incelendiğinde yüksek oranda bilgi güvenliği konusunda bilgi alınan bir yer gösterilmemiştir. Çok az katılımcının ise internetten ve çevrelerindeki deneyimli kişilerden bilgi aldıkları, yalnızca 3 katılımcının ise eğitim aldığı görülmüştür. Bunun yanında 242 katılımcıdan yalnızca 100 katılımcının bu konuda fikir beyan etmiş olması dikkat çekicidir. Üniversite öğrencilerinden oluşan katılımcı grubunun eğitim hayatları boyunca bilgi güvenliği konusunda eğitim almamış olmaları ise ayrıca üzerinde düşünülmesi gereken bir konudur.

4.3 Balküpü Tuzak Sistemi Bulguları

Uluslararası Kıbrıs Üniversitesinde bulunan bilgisayar salonunda erişime açık halde bırakılan balküpü tuzak sistemince toplanan verilere ait analizler aşağıda sunulmuştur.

Balküpü Sisteminde Tespit Edilen Saldırılara Ait Bulgular

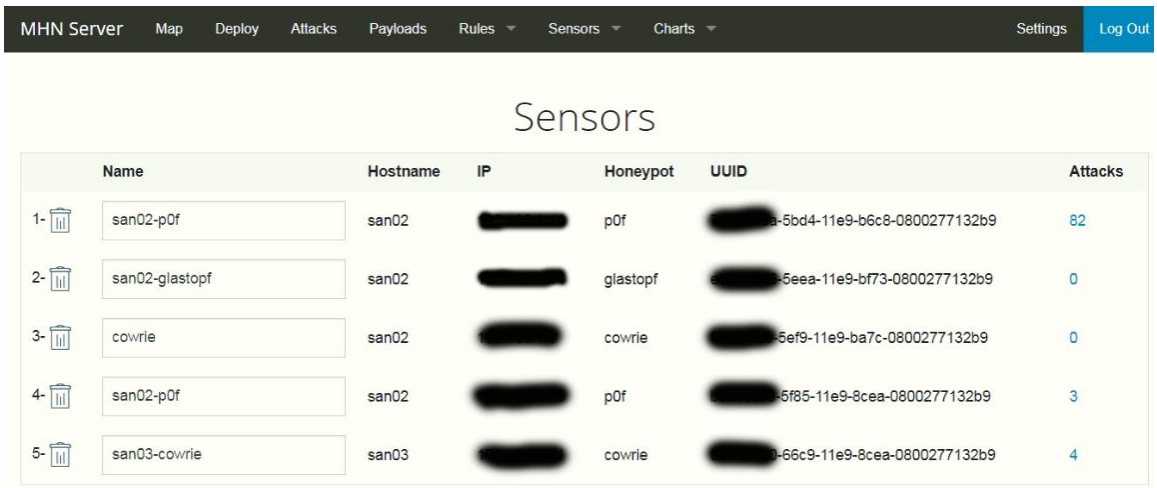
Balküpü sisteminde sensörler vasıtası ile yapılan tespitlerde yaklaşık p0f sensörü ile 82 TCP/IP erişimi listelenmiştir. Yapılan bu erişimlerin 40'ı sistem

devreye alındığı sırada yapılan test erişimleridir. Dolayısıyla geriye örneklem olarak kabul edilen 42 TCP/IP erişimi kalmıştır. MHN üzerinden atak raporu incelendiğinde iki tuzak makinasına da farklı portlardan birer defa erişim denemesi olduğu görülmektedir. Glastopf sensörüne ait bulgularda açıklık barındıran web uygulamasının dosyalarına (index, style.css, favicon.ico) erişildiği görülmüştür. Bu erişimlerde denenen kullanıcı adları genelde "root123" ve "admin" olmuştur. Denenen şifreler ise "asd" , "passw" , "test" , "123456" gibi gelişi güzel seçilen kelimelerden oluşmuştur. Şifre denemelerinde bir yazılım vasıtası ile zorlama yapılmadığı bunun yerine elle girilen denemeler yapıldığı görülmektedir. Bu durum saldırının profesyonel olmayan kişiler tarafından yapıldığını göstermektedir.

Tablo 4.7 – 4.16 sonuçları ve balküpü tuzak sistemi verilerine göre H3 hipotezi kabul edilmiştir.

Balküpü MHN (Modern Honey Network) Sensörler ve Tespit Edilen Ataklar Ekranı

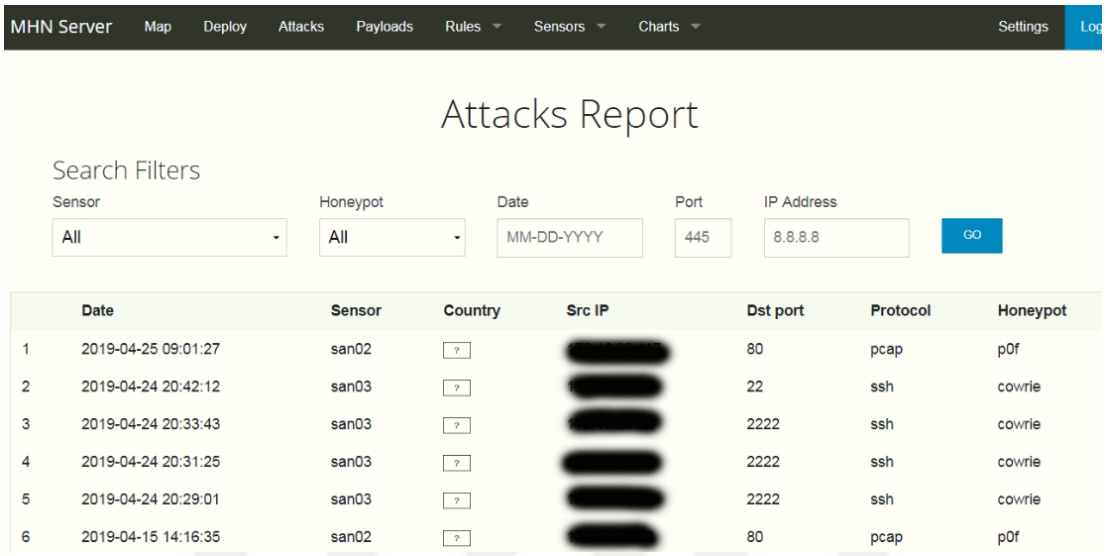
Şekil 4.1 incelendiğinde balküpü sisteminde kullanılan sensörler ve bu sensörlerin tespit ettikleri ataklar görülmektedir.



Şekil 4.1 MHN Sunucu Kullanılan Sensörler Ekranı

Balküpü MHN Atak Raporu Ekranı

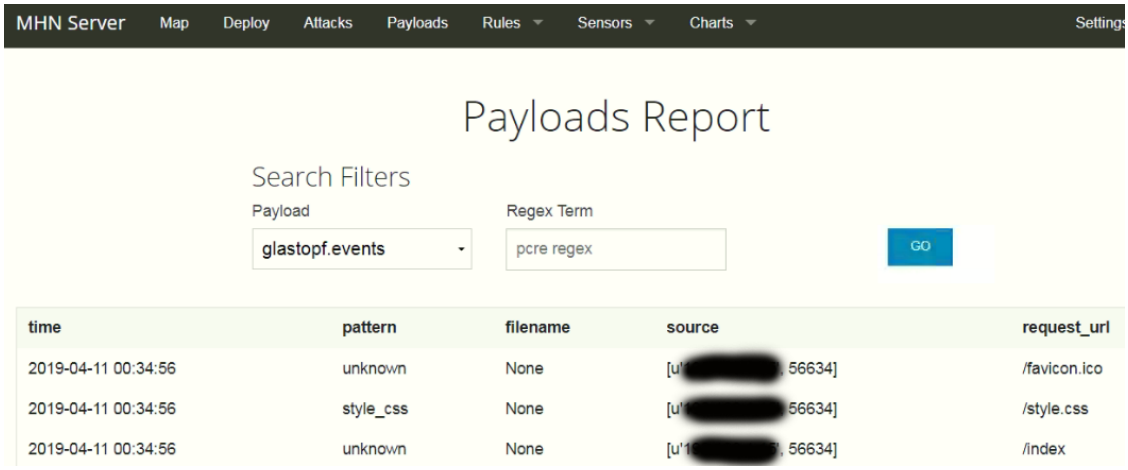
Şekil 4.2 incelendiğinde hangi port üzerinden hangi protokol ile saldırı yapıldığı ve bu saldırıları hangi sensörün tespit ettiği görülmektedir.



Şekil 4.2 MHN Sunucu Atak Rapor Ekranı

Balküpü MHN Glastopf Sensörü Raporu Ekranı

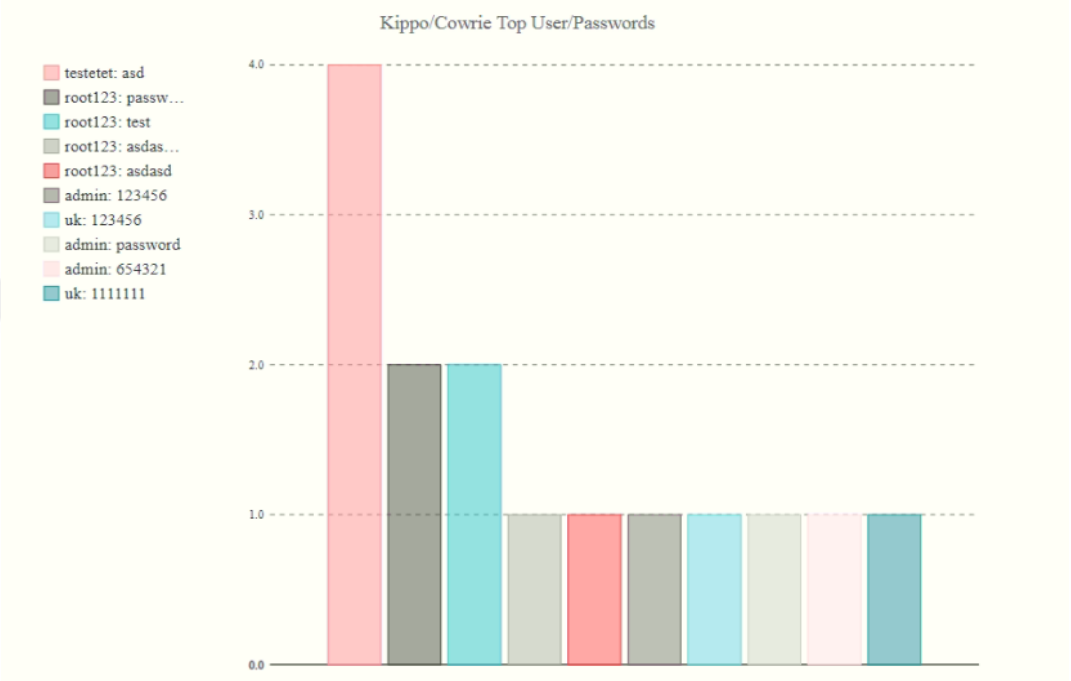
Şekil 4.3 incelendiğinde glastopf sensörü tarafından tespit edilen saldırı denemeleri görülmektedir.



Şekil 4.3 MHN Sunucu Glastopf Olay Rapor Ekranı

Balküpü MHN Kippo/Cowrie Sensörü Raporu Ekranı

Şekil 4.4 incelendiğinde Kippo / Cowrie sensörü tarafından tespit edilen kullanıcı adı şifre kombinasyonları görülmektedir.



Şekil 4.4 MHN Sunucu Kippo/Cowrie Rapor Ekranı

BÖLÜM 5

TARTIŞMA VE SONUÇ

5.1 Tartışma

Bu araştırmadaki ankete katılan öğrencilerin %62,8'i kadın (152 katılımcı) ve %37,2'i erkektir (90 katılımcı). Öğrencilerin yaş bilgileri: 18 yaşında 3 öğrenci, 19 yaşında 22 öğrenci, 20 yaşında 36 öğrenci, 21 yaşında 48 öğrenci, 22 ve üzeri yaşlarda ise 133 öğrencidir. Öğrencilerin bölümlere göre dağılımı, Okul Öncesi Öğretmenliği %44,2, Özel Eğitim Öğretmenliği %21,1, Sınıf Öğretmenliği %10,3, Türkçe Öğretmenliği %9,1, Pisikolojik Danışmanlık ve Rehberlik %6,6, Bilgisayar Öğretmenliği %5,0, Beden Eğitimi ve Spor Yüksek Okulu %3,7 şeklindedir. Toplam 7 farklı bölümden veriler toplanmıştır. Ankete katılan öğrencilerin %47,5'i şehir merkezinde, %40,9'u ilçelerde, %11,6 ise kırsalda yaşamaktadır. Bu anket çalışmasının öğrencilerin siber güvenlik faktörleri hakkındaki farkındalıkları kapsamında olumlu bir sonuç saptanmamıştır. Genel olarak öğrenciler önemli gördüklerini dile getirdikleri güvenlik önlemlerini dahi çoğunlukla uygulamadıklarını belirtmişlerdir. Birçok öğrenci sorulan güvenlik sorularına olumsuz yanıtlar vermiştir. Parola güvenliği konusunda bilgi sahibi olduğunu düşünen öğrencilerin oranı %71,1 iken sanal klavye kullandığını belirten öğrencilerin oranı ancak %38,8 olarak ölçülmüştür. Buna rağmen güvenliğin ve gizliliğin son derece önemli olduğu sosyal ağlarda %64,9 öğrenci her gün zaman geçirirken, yine çok önemli diğer bir konu olan çevrim içi alış-veriş yapanların oranının ise %75,6 ile yüksek bir düzeyde olduğu görülmüştür.

Akgün ve Topal (2015) tarafından Sakarya Üniversitesinde uygulanan Bilişim Güvenliği Anketinin örneklemini Bilgisayar ve Öğretim Teknolojileri Eğitimi (64 Kişi) , İlköğretim Matematik Eğitimi (39 Kişi), Türkçe Eğitimi (74 Kişi) ve Zihin Engelliler Eğitimi (35 Kişi) bölümlerinde okuyan toplam 212 kişi oluşturmuştur. Sonuçlar incelendiğinde öğrencilerin bilişim güvenliği farkındalıklarının olduğu fakat birçok konuda azımsanmayacak sayıda öğrencinin olumsuz yanıtlar verdiğini ya da kararsız kaldığı durumlar olduğu görülmektedir. Örneğin, öğrencilerin çoğunluğu parola güvenliği konusunda bilgi sahibi olduklarını

dile getirirken, aynı zamanda farklı sitelerde aynı parola ve kullanıcı adını kullanmakta, başka insanlarla parola ve şifrelerini paylaşmaktadırlar (Akgün & Topal, 2015).

Gizem Yılmaz, Ramazan Yılmaz ve Barış Sezer (2014) tarafından üniversite birinci sınıftaki 124 öğrenci üzerinde yapılan, yükseköğretim programlarında öğrenim gören öğrencilerin güvenli Bilgi ve İletişim Teknolojileri (BİT) kullanım davranışlarını inceleyen çalışmada, öğrencilerin belirli bir güvenli BİT kullanım davranışları olduğu fakat bunların gelişen ve hızla değişen teknolojik koşullarda yeni durumlara yanıt vermede yetersiz kaldığı görülmüştür. Öğrenciler, erişim güvenliği, zararlı programlardan korunma yolları, parola güvenliği vb. konularda temel seviyede ve en popüler güvenlik önlemlerinden yalnızca bir ya da birkaçını aldığını, diğer güvenlik önlemlerini ise almadıklarını göstermektedir (Yılmaz, S., & Yılmaz, 2014).

Balküpü sisteminde toplanan veriler incelendiğinde örneklem olarak kabul edilen 42 TCP/IP erişimi listelenmiştir. Tespit edilen erişimlerde “root123” ve “admin” kullanıcı adları ile denemeler yapılmıştır. Denenen şifreler ise “asd” , “passw” , “test” , “123456” gibi gelişi güzel seçilen kelimeleri içermektedir. Web uygulamasına index, style.css, favicon.ico dosyalarına erişim denemeleri görülmüştür. Yapılan 42 erişim denemesine karşın çok daha az miktarda kullanıcı adı parola denemesi mevcuttur. Bu durum yapılan erişimlerin bir kısmının virüs veya bot bilgisayarlar tarafından olabileceğini ya da iletişim sağlandıktan sonra öğrencinin erişim denemesinden vazgeçmiş olabileceğini göstermektedir.

Süleyman Muhammed Arıkan ve Recep Benzer tarafından 2018 yılında yayımlanan «Bir Güvenlik Trendi: Balküpü» adlı çalışmada, dört ay boyunca aktif tutulan Kippo SSH balküpü ile 298 farklı IP tarafından SSH servisi üzerinde 23.271 adet deneme kaydı tespit edilmiştir. Bal küpü, 12.269 benzersiz kullanıcı adı-parola çifti yakalamıştır. Bunların başında 142 deneme ile “root/123456” gelmektedir. Güvenlik Duvarları ve erişim denetleme listeleri gibi birçok pasif korunma yöntemleri, bilinen saldırı teknikleri üzerinde verimli bir şekilde çalışmasına karşın henüz keşfedilmemiş yöntemleri kullanan zararlı aktivitelerinin tespiti ve engellemesinde zayıf kaldığı görülmektedir. Balküpü sistemleri ile bu eksiklik

giderilerek bilinmeyen yöntemleri kullanan saldırıların yakalanması ve üzerinde analizler yapmanın olanaklı hale geldiği görülmüştür (Arıkan & Benzer, 2018).

5.2 Sonuç

Bilgi ve iletişim teknolojileri takibi mümkün olmayacak bir süratle gelişmektedir. Gelişen teknolojiye erişim ise her geçe gün daha da kolaylaşmakta ve bu teknolojiler daha çok kişi tarafından kullanılabilir olmaktadır. Eğitim-öğretim kurumları olan üniversite ağı kullanıcıları gelişime açık, araştırıcı, yeni teknolojileri denemek açısından sabırsız kullanıcılardır. Bu kullanıcılar karşılaştıkları teknolojik gelişmelere çok çabuk adapte olarak, ortaya çıkan zorukları aşmak konusunda son derece isteklidirler. Eğitim kurumlarında edindikleri bilgileri uygulamak isteyerek, bilgiye erişim için her türlü yolu deneyebilecek kimselerdir. Bu özellikleri bakımından zararlı yazılımların da hedefi olmaktadırlar (Köse, Özdilek, Doğan, & Göktaş, 2018).

Bilgi güvenliğini tam anlamıyla sağlamak çok zor bir görevdir. Çünkü tehditler zaman içerisinde boyut ve nitelik değiştirmekte, etki alanlarını genişletmektedirler. Buna bağlı olarak bilgi güvenliğini en üst seviyede sağlamak için, tedbirlerin birçok prensip dâhilinde ele alınması gerekmektedir (Ercan, 2015). Bilgi güvenliğinde uyulması gereken temel prensipler, Gizlilik, Veri Bütünlüğü, Erişebilirlik olarak sıralanmaktadır. Bunların dışında, Loglama, Kimlik Doğrulama, İnkâr Edilmezlik ve Güvenilirlik'de önemli prensiplerin içinde yer almaktadır (Çek, 2017).

Balküpleri bilgi ve ağ güvenliğine yönelik yapılan saldırıların farkına varmak, saldırganların yöntemlerini izlemek, metodlarını belirlemek, yeni geliştirilen saldırı sistemlerinden önceden haberdar olmak için özel olarak tasarlanmış yazılım veya sistemlerdir (Bektaş & Spysal, 2018). Yapılan erişimler kayıt altına alınarak bir erişim günlüğü (log) vasıtası ile saldırgan profili çıkartılarak kötücül yazılımlar ile kötü amaçlı kullanıcılar tespit edilmeye çalışılır.

Bu çalışmada Uluslararası Kıbrıs Üniversitesinde 2018 – 2019 öğretim yılında Türkçe programlarda öğrenim gören 242 öğrenciye Akgün ve Topal'ın

(2015) “Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları” anketi ile farkındalıkları ölçülmüş, üniversitede bulunan bilgisayar salonunda erişime açık halde bırakılan balküpü tuzak sistemi ile de ağ üzerindeki saldırılar tespit edilmeye çalışılmıştır. Anket analizi sonucunda öğrencilerin bilişim güvenliği konusundaki farkındalıklarının son derece düşük seviyede olduğu ve bu konuda almaları gereken önlemler hakkında yeterince bilgi sahibi olmadıkları, güvenliklerini sağlamak için yeterince önlem almadıkları görülmüştür. Tablo 4.7 – 4.16 sonuçlarına göre H1 (Üniversite ağı kullanıcıları bilgi teknolojilerini kullanırken kişisel güvenliklerine yeterince önem vermezler) ve H2 (Ağ kullanıcıları bilinçli veya bilinçsiz bir şekilde ağ ve sistemin kararlı çalışmasına engel teşkil edecek davranışlarda bulunabilirler) hipotezleri kabul edilmiştir. Tablo 4.7 – 4.16 sonuçları ve balküpü tuzak sistemi verilerine göre H3 (Ağ aktif cihazlarında alınacak güvenlik tedbirleri riskleri azaltabilir) hipotezi kabul edilmiştir.

Eğitim kurumları da ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından kuruluşların siber güvenlik risklerini daha iyi anlamalarına ve yönetmelerine yardımcı olmak için tasarlanan Siber Güvenlik Çerçevesinin geliştirilmesi için yürütülen projeyi yakından takip edilmelidir. Eğitim kurumları bu araştırmadan elde edilen verileri bu proje kapsamında kullanmalıdırlar.

5.3 Öneriler

Üniversite ağının kullanıcısı olarak onun bir parçası haline gelen üniversite öğrencilerinin bilişim güvenliği hakkındaki bilgi seviyeleri arttırılmalıdır. Bu öğrencilerin kişisel güvenliklerini sağlayabilmelerinin yanı sıra ağ içerisinde oluşabilecek sorunların azaltılabilmesi için de bir gerekliliktir. Bu amaçla bilgi ve iletişim güvenliği konusunda farkındalık çalışmaları yapılmalı, hatta modern hayatın bir parçası haline gelen bilgi sistemleri için güvenlik odağında hazırlanan bir ders eğitim müfredatına alınmalıdır. Farkındalık çalışmalarının sürekli hale getirilmesi için üniversite web sitelerinde bir sayfa açılmalı, öğrencilerin güncel tehditler ve önemler hakkında bilinçlendirilmesi sağlanmalıdır. Öğrencilerin korsan yazılımlara yönelmesini engellemek maksadıyla açık kaynak kodlu ücretsiz dağıtımı bulunan

yazılımlar hakkında bir tartışma platformu kurulmalı ve ağ kullanıcılarının, bilgi sistem kullanıcısı olarak ihtiyaç duyabilecekleri temel işlemleri yapabilmek için gerekli olan yazılımların servis edileceği bir sistem geliştirilmesi değerlendirilmelidir. Bu sistem bir komisyon tarafından dönemsel olarak değerlendirilerek güncellenen bir onaylı yazılımlar listesini içermelidir.

Balküpü tuzak sistemi gerçek sistemleri simule etmektedir. Bu sistemin daha çok öğrenciye hitap edebilmesi için tüm üniversite alanlarını kapsayacak şekilde tam gün çalışır bulundurulması üniversite ağında oluşacak zararlı aktiviteler hakkında bilgi sahibi olmak ve tedbirler alabilmek için kullanımına devam edilmesi önerilmektedir.

KAYNAKÇA

Ahtapot hakkında. (2019). 08 05, 2019 tarihinde www.ahtapot.org.tr. adresinden alındı

glastopf. (2019). 08 2019 tarihinde www.github.com. adresinden alındı

https://www.nist.gov/cyberframework. (2019). 07 12, 2019 tarihinde www.nist.gov: https://www.nist.gov/cyberframework adresinden alındı

Akgün, Ö. E., & Topal, M. (2015, Ağustos). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi örneği. *Sakarya Üniversitesi eğitim dergisi.*, s. 98-121.

Allen, J. H. (2001). *The CERT Guide to System and Network Security Practices.* Addison-WesleyProfessional.

Anley, C. (2002). *Advanced sql injection in sql server applications.* Surrey.

Arıkan, S. M., & Benzer, R. (2018). Bir güvenlik trendi bal küpü. *Acta Infologica*, 1-11.

Arslan, M. E. (2016). *Siber güvenlik ve siber saldırı türleri.* Ankara: Gazi Üniversitesi.

Atılgan, D. (2009). *Bilgi yönetimi kavramı ve gelişimi. Türk kütüphaneciliği,.*

Battersby, M. (2013, 05 15). *SABSA a brief introduction.* 08 03, 2019 tarihinde https://docplayer.net: https://docplayer.net/20367187-Sabsa-a-brief-introduction.html adresinden alındı

Baykara, M., Daş, R., & Tuna, G. (2016). Web sunucu erişim kütüklerinden web ataklarının tespitine yönelik web tabanlı log analiz platformu. *Fırat Üniv. Müh. Bil. Dergisi* , 291-302.

Bayram, K. S. (2018). *Çoklu biyometrik yöntemlerle kimlik doğrulama.* İstanbul: Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü.

Bbc.com. (2017, Mayıs 13). *5 soruda Türkiye'yi de etkileyen fidye yazılımı 'WannaCry'*. Mayıs 26, 2018 tarihinde bbc.com: https://www.bbc.com/turkce/haberler-39906717 adresinden alındı

Bektaş, O., & Spysal, M. (tarih yok). *Ulak-CSIRT balküpü çalışma grubu.* Mayıs 26, 2018 tarihinde http://www.ipv6.net.tr/kovan/docs/papers/balkupu_cal_grubu.pdf adresinden alındı

Bennett, J. (2004). *Digital Umbrella: Technology's attack on personal privacy in america.* Florida: Brown Walker Press.

BGA Security. (2019, Ocak 15). *Günümüz internet dünyasında ip spoofing*. 08 03, 2019 tarihinde www.bgasecurity.com: https://www.bgasecurity.com/2011/11/gunumuz-internet-dunyasnda-ip-spoofing/ adresinden alındı

Bıçakçı, S., Doruk, E., & Çelikpala, M. (2015). Türkiye'de siber güvenlik. *EDAM Siber Güvenlik Kağıtları Serisi*, 9.

Caruso, J. B. (2003). Information technology security: governance, strategy, and practice in higher education. *EDUCAUSE Center For Applied Research ECAR*.

Constantin, L. (2012, December 13). *DDoS Attacks Against US Banks Peaked At 60 Gbps*. 08 03, 2019 tarihinde www.cio.com: https://www.cio.com/article/2389721/security0/ddos-attacks-against-us-banks-peaked-at-60-gbps.html adresinden alındı

Constantin, L. (2018, 01 11). *DDoS attacks against US banks peaked at 60 Gbps*. 08 03, 2019 tarihinde www.infinityteknoloji.com: https://www.infinityteknoloji.com/projedetayi/quiz-show/ adresinden alındı

Çek, E. (2017). Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği İçin İnsan faktörünün önemi. *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*.

Daş, R., Baykara, M., & Demirol, D. (2013). *SQL enjeksiyon saldırı uygulaması ve güvenlik önerileri.* Elazığ: Fırat Üniversitesi.

Demirtaş, H. (2013). *Bilgi güvenliği yönetiminin gerekleri ve başarı dayanakları: bir uygulama örneği.* Sakarya Üniversitesi.

Doğantimur, F. (2009). *ISO 27001 standardı çerçevesinde kurumsal bilgi güvenliği, maliye bakanlığı strateji geliştirme başkanlığı, mesleki yeterlilik tezi.* Ankara: T.C. Maliye Bakanlığı.

Donaldson S., S. S. (2015). *Enterprise Cybersecurity: How to build a successful cyberdefense program against advanced threats.* New York: Apress Media.

Ercan, M. (2015). Kritik altyapıların korunmasına İlişkin belirlenen siber güvenlik stratejileri.

Github. (2019, Ocak 20). *DDos-Attack*. https://github.com: https://github.com/Ha3MrX/DDos-Attack adresinden alınmıştır

Grance, T., & Jansen, W. (2011). *Guidelines on Security and Privacy in Public Cloun.* NIST Special Publication 800-144.

Güldüren, C. (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi.* Ankara: Ankara Üniversitesi Doktora Tezi.

Güldüren, C., & Keser, H. (2017). Bilgi güvenliği farkındalık eğitimi. H. F. Odabaşi, B. Akkoyunlu, & A. İşman içinde, *Eğitim Teknolojileri Okumaları 2017* (s. 49). Ankara: Sakarya Üniversitesi.

Gülmüş, M. (2010). Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği. *Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü*.

SABSA (2019). 07. 12. 2019 tarihinde https://sabsa.org: https://sabsa.org/sabsa-nist-framework-project/ adresinden alındı

Kandemirli, B. M. (2012). Bilgi teknolojileri güvenliği ve sigorta şirketinde ISO/IEC 27001 standartları çerçevesinde bilgi güvenlik yönetim sistemi uygulaması.

Karaaslan, E., Akın, G., & Demir, H. (2008). Kurumsal ağlarda zararlı yazılımlarla mücadele yöntemleri. *Akademik Bilişim*.

Koç.net. (2005). *Rizikometre 2005 - Türkiye internet güvenliği araştırma sonuçları.* İstanbul: Koç.net.

Köse, S., Özdilek, R., Doğan, P., & Göktaş, S. (2018). Üniversite öğrencilerinin sanal zorba/sanal kurban olma durumları üzerine bir araştırma. *İstanbul Sosyal Bilimler Dergisi*, 54-70.

Kurtkaya, G. D. (2017). *Bilgi güvenliği ve siber güvenlik kapsamında bakanlık uygulamaları için güvenli yazılım geliştirme metadolojisi önerisi uzmanlık tezi.* Ankara: T.C. Çevre ve Şehircilik Bakanlığı.

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı. Yüksek Lisans Tezi,.* Kahramanmaraş: Kahramanmaraş Sütçü İmam Üniversitesi.

McCumber, J. (2004). *Assessing and managing security risk ın ıt systems a structured methodology.* New York: CRC Press.

Mitnick, K. D., & Simon, W. L. (2001). *Aldatma Sanatı.*

Nassiri, A. (2018, Ağustos 18). *5 most famous ddos attacks*. www.a10networks.com: https://www.a10networks.com/resources/articles/5-most-famous-ddos-attacks adresinden alınmıştır

NATO Cooperative Cyber Defence Centre of Excellence. (2012). *NATIONAL CYBER SECURITY FRAMEWORK MANUAL*. Estonia: NATO.

Nemati, H., & Yang, L. (2011). *Applied cryptography for cyber security and defense.* University of North Carolina and Tennessee.

Olson, P. (2014, November 20). *The largest cyber attack in history has been hitting hong kong sites.* www.forbes.com: https://www.forbes.com /sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/#7fcd4c9238f6 adresinden alınmıştır

Önel, D., & Dinçkan, A. (2007). Bilgi güvenliği yönetim sistemi kurulumu. *TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) Dergisi*, 1-16.

Özbilgin, İ. G. (2019). *Siber Güvenlik Pazarı Baş Döndürüyor*. 08 18, 2019 tarihinde kbd.org.tr. adresinden alındı

Pesen, M. M. (2015, 06 08). *Bilgi güvenliği nedir ve nasıl sınıflandırılır*. 08 03, 2019 tarihinde www.sibergah.com: https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/ adresinden alındı

Prince, M. (2014, February 13). *Technical details behind a 400gbps ntp amplification ddos attack*. www.cloudflare.com: https://blog.cloudflare.com/ technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/ adresinden alınmıştır

Puhakainen, P. (2006). *A design theory for information security awareness. PhD thesis.* University of Oulu.

Rist, L. (2019). *Introducing glastopf, a web application honeypot*. 08 2019 tarihinde honeynet.org. adresinden alındı

SABSA (2018). *SABSA executive summary*. 21. 01. 2019 tarihinde sabsa.org: https://sabsa.org/sabsa-executive-summary/#who-uses-sabsa adresinden alındı

Shalini, S., & Usha, S. (2011, Jully). Prevention of cross-site scripting attacks (xss) on web applications in the client side. *IJCSI International Journal of Computer Science Issues*, s. 651.

Sharp, E. D. (2004). Information security in the enterprise. *Information Security Management Handbook (Fift h Edition).* içinde New York: Auerbach Publications.

Shcherbakova, T., & Vergelis, M. (2014). *Spam report: March 2014*. 1 18, 2019 tarihinde http://www.securelist.com: https://securelist.com/spam-report-march-2014/59420/ adresinden alındı

Sivanesan, A. P., Mathur, A., & Javaid, A. Y. (2018). *A google chromium browser extension for detecting XSS attack in HTML5 based websites*. 1 18, 2019 tarihinde https://ieeexplore.ieee.org: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8500284 adresinden alındı

spamhaus.org. (2019, Ocak 20). *About Spamhaus*. https://www.spamhaus.org: https://www.spamhaus.org/organization/ adresinden alınmıştır

Şahinaslan, E. K. (2009). Bilgi güvenliği farkındalık eğitimi örneği. *XI.Akademik Bilişim Konferansı Bildirileri*, (s. 189-194). Şanlıurfa.

Thomas, V., & Gardner, B. (2017). Defending against social engineering and technical threats. *Building an Information Security Awareness Programs*.

Tonta, Y. (1999). *Bilgi toplumu ve bilgi teknolojisi. türk kütüphaneciliği.* İstanbul.

Vijayan, J. (2013, Mart 27). *Spamhaus hit by biggest-ever DDoS attacks*. www.computerworld.com: https://www.computerworld.com/article/2495967/cybercrime-hacking/update--spamhaus-hit-by-biggest-ever-ddos-attacks.html adresinden alınmıştır

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma testleri.* Ankara: Gazi Üniversitesi.

Yiğit, M. F., & Seferoğlu, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 186-215.

Yıldız, M. (2014, Kasım). Siber suçlar ve kurum güvenliği. *T.C. Ulaştrma, Denizcilik ve Haberleşme Bakanlığı*.

Yılmaz, F. G., Yılmaz, R., & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve İletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 1-6.

Yılmaz, O. (2009). *HTML injection attack & security*. 1 18, 2019 tarihinde https://www.webguvenligi.org: https://www.webguvenligi.org/dokuman/html-enjeksiyonu-yazi-dizisi-bolum-3.html adresinden alındı

Zalewski, M. (2012). 08 2019 tarihinde www.github.com. adresinden alındı

Zorlu, A. E. (2018). *Impact of information technology capability on finance firms performance.* İstanbul: Bahçeşehir Üniversitesi.

EKLER

ÜNİVERSİTESİ ÖĞRENCİLERİNİN BİLİŞİM GÜVENLİĞİ

FARKINDALIĞI ANKETİ

Sevgili Öğrenciler;

Bu çalışmanın amacı Üniversitesi öğrencilerinin bilişim güvenliği konusundaki farkındalıklarını araştırmaktır. Lütfen anket formuna adınızı, soyadınızı veya kimliğinizi belirten hiçbir şey yazmayınız. Lütfen her bir soruya mümkün olan en iyi yanıtı veriniz. Verdiğiniz cevaplar isteğe bağlıdır ve gizli tutulacaktır. Bireysel cevaplar dağıtılmayacak. Tüm cevaplar birlikte derlenecek ve bir grup olarak analiz edilecektir.

Çok teşekkür ederim.

Ferat ÖNAL
Yüksek Lisans Öğrencisi
Yönetim Bilişim Sistemleri Bölümü
Uluslararası Kıbrıs Üniversitesi

BÖLÜM 1: DEMOGRAFİK BİLGİLER

1. Okuduğunuz Bölüm:

   _____

2. Cinsiyetiniz:

   a) Kadın b) Erkek

3. Doğduğunuz

   Ülke:_____

4. Hangi tür liseyi tamamladınız?

   _____

5. Hangisi ülkenizde yaşadığınız bölgeyi en iyi şekilde tanımlar.

   a) Şehir Merkezi b) İlçe c) Kırsal

6. Yaşınız?

a) 18 b) 19 c) 20 d) 21 e) 22+

7. Sınıfınız?

a) 1 b) 2 c) 3 d) 4

8. Eğitiminiz düzeyiniz nedir?

a) Lisans b) Yüksek Lisans c) Doktora

9. Bilgisayarınız var mı?

a) Evet b) Hayır

10. Günde kaç saat bilgisayar kullanıyorsunuz?

a) Günlük kullanmam b) 1-3 saat c) 4-5 saat d) 6-8 saat e) 8 saatten fazla

11. Günde kaç saat internete girersiniz?

a) Günlük kullanmam b) 1-3 saat c) 4-5 saat d) 6-8 saat e) 8 saatten fazla

12. Bilgisayarlarla ilgili kaç yıllık tecrübeniz vardır?

a) 1 b) 2 c) 3 d) 4 e) 5+

13. En çok hangi işletim sistemini kullanıyorsunuz?

a) Windows b) Linuxc) MacOS d) Diğer……

14. Ne sıklıkla çevrimiçi alışveriş yapıyorsunuz?

a) Hiç b) Ayda 1'den az c) 1-3 defa/Ay d) 1-7 defa/Hafta e)Günde 1den fazla

15. Facebook gibi sosyal ağları ne sıklıkla kullanıyorsunuz?

a) Hiç b) Ayda 1'den az c) 1-3 defa/Ay d) 1-7 defa/Hafta e)Günde 1den fazla

16. Bilişim güvenliği konusundaki deneyiminizi nasıl değerlendiriyorsunuz?

1 (Deneyimsiz) 2 3 4 5 6 7 (Çok Deneyimli)

17. Bir Alış-Veriş sitesinden alış-veriş yaparken sitenin hangi özelliklerine dikkat edersiniz?

_____

_____

_____

18. Parola belirlerken parolanın hangi özellikleri taşımasına dikkat edersiniz?

_____

_____

19. Bir yazılıma ihtiyaç duyduğunuzda bunu nasıl temin edersiniz?

_____

_____

20. Bilişim güvenliği konusunda bilgi aldığınız bir web sitesi, kurum, kuruluş vb. varsa lütfen adını yazınız.

_____

_____

BÖLÜM 2:ÜNİVERSİTE ÖĞRECİLERİNİN BİLİŞİM GÜVENLİĞİ ANKETİ

Aşağıdaki ifadelerden, lütfen düşüncenizi en iyi yansıtan yanıtı seçiniz.

1 --- Benim İçin Doğru Değil **2 --- Kararsızım** **3 --- Benim İçin Doğru**

Sıra No.	ÜNİVERSİTE ÖĞRECİLERİNİN BİLİŞİM GÜVENLİĞİ ANKETİ*	Benim İçin Doğru Değil	Kararsızım	Benim İçin Doğru
1	Farklı e-posta adreslerim için aynı parolayı (şifreyi) kullanırım	1	2	3
2	Farklı sitelere üye olurken aynı kullanıcı adı ve parolayı kullanırım.	1	2	3
3	Bana ait olmayan bir bilgisayardan internete girerken, tarayıcının kişisel bilgilerimi kaydedip kaydetmediğini kontrol ederim.	1	2	3
4	Kişisel bilgisayarımın dışındaki bilgisayarlar üzerinden internet aracılığı ile alış veriş yaparım.	1	2	3
5	İnternette alış-veriş yaparken internetten ödeme güvenliği hakkında nelere dikkat etmem gerektiğini bilirim.	1	2	3
6	Kredi kartım ile ilgili önemli bilgileri girerken eğer varsa sanal klavye kullanırım.	1	2	3
7	İnternette parolamı yazarken yakın arkadaşlarımın parolamı görmesi benim için sorun değildir.	1	2	3
8	Güvendiğim insanlara kullanıcı adı ve şifremi veririm.	1	2	3
9	Bilgisayarımda bir açılış parolası kullanırım.	1	2	3
10	Bilgisayarımı kullanmak isteyen kişiler için açtığım, ayrı, sınırlı bir oturum vardır.	1	2	3
11	Bilgisayarımda kendi oturumumdaki önemli belgeler şifreli haldedir.	1	2	3
12	Bilgisayarımı kullanmak isteyen olursa sadece konuk oturumunu kullanmasına izin veririm.	1	2	3
13	Parolamı yönetmek (saklamak) için bir bilgisayar yazılımı kullanırım.	1	2	3
14	Kullandığım anti-virüs yazılımının güncelliğini denetlerim.	1	2	3

Sıra No.	ÜNİVERSİTE ÖĞRECİLERİNİN BİLİŞİM GÜVENLİĞİ ANKETİ*	Benim İçin Doğru Değil	Kararsızım	Benim İçin Doğru
15	İşletim sistemi güncellemelerini kontrol eder ve zamanında yüklerim.	1	2	3
16	Kullandığım ofis yazılımlarının güncellemelerini denetlerim.	1	2	3
17	Anında ileti yazılımı kullanarak benimle dosya paylaşıldığında gelen dosya ile ilgili bilgim yoksa gönderen kişiye sormadan dosyayı açmam.	1	2	3
18	Sosyal ağ sitelerinde tanımadığım insanları arkadaş listeme eklerim.	1	2	3
19	Sosyal ağlarda kişisel bilgilerimi paylaşırım.	1	2	3
20	Göndereninin tanımadığım bir epostaya eklenmiş dosyayı anti-virüs taramasından geçirmeden açarım.	1	2	3
21	İnternetten bilgisayarıma indirdiğim dosyaları açmadan önce virüs taramasından geçiririm.	1	2	3
22	USB Bellek, harici disk veya cd-dvd medyası bilgisayarıma bağlandığında öncelikle anti-virüs taramasından geçiririm.	1	2	3
23	Cep telefonum ya da bilgisayarım ile kaynağını/sahibini bilmediğim kablosuz ağlara bağlanırım.	1	2	3
24	Bilgisayarımdaki yazılımları lisans bedellerini ödeyerek satın aldıktan sonra kullanırım.	1	2	3
25	Bilgisayarımda yasa dışı yolla edinilmiş (kırılmış) yazılımlar bulunmaktadır.	1	2	3
26	Sosyal ağlarda tanıştığım insanlarla yüz yüze buluşurum.	1	2	3
27	Kişisel fotoğraf ve videolarımı herkesin erişebileceği ortamlarda paylaşırım.	1	2	3
28	Parolamı belirli zaman aralıklarında değiştiririm.	1	2	3
29	Bilgisayarımı belli zaman aralıklarında güvenlik taramasından geçiririm.	1	2	3
30	Göndereni tanımasam da tepkimi çeken postaları yanıtlarım.	1	2	3
31	Anında ileti yazılımları kullanırken yazışmaları arşivlerim.	1	2	3
32	Şifrelenmemiş ve kimin sağladığını bilmediğim kablosuz ağlara bağlanırım.	1	2	3
33	Kablosuz internet ağımda şifre kullanmam.	1	2	3
34	Eposta adresime gelen sahte içerikli postaları ‘‘Spam’’ olarak işaretlerim.	1	2	3
35	İnternet kaynaklı tehditler ile ilgili yeterli bilgiye sahibim.	1	2	3
36	Kullandığım internet tarayıcısının güvenlik ayarları hakkında yeterli bilgi sahibiyim.	1	2	3
37	Eposta adresim kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğim konusunda bilgi sahibiyim.	1	2	3
38	Göndereni tanımadığım halde ilgimi çeken epostaları yanıtlarım.	1	2	3

Sıra No.	ÜNİVERSİTE ÖĞRECİLERİNİN BİLİŞİM GÜVENLİĞİ ANKETİ*	Benim İçin Doğru Değil	Kararsızım	Benim İçin Doğru
39	Yazılım kullanmada telif hakları konusunda yeterli bilgi sahibiyim.	1	2	3
40	Sosyal medya platformlarında bulunan kullanıcı hesaplarımın gizlilik ayarlarını yönetebilecek bilgiye sahibim.	1	2	3
41	İnternet tarayıcım vasıtasıyla internette gezindiğim web sitelerinin güvenirliği ile ilgili bilgi edinmeye çalışırım.	1	2	3
42	İnternet tarayıcım vasıtasıyla internette gezindiğim web sitelerinin güvenirliği ile ilgili bilgi edinmeye çalışırım.	1	2	3
43	Nasıl güvenli bir parola belirleyeceğim hakkında bilgi sahibiyim.	1	2	3
44	Parola güvenliğinin zayıf, orta, yüksek olmasının parolamın güvenliğini nasıl etkilediğini biliyorum.	1	2	3
45	Bilişim güvenliği konusunda bilgi alabileceğim adresleri bilirim.	1	2	3
46	Bir bilişim suçuna maruz kalırsam kime başvuracağımı biliyorum.	1	2	3
47	Bir bilişim güvenliği sitesini düzenli olarak takip ederim.	1	2	3
48	Bilgisayarın güvenliğini sağlayacak yazılımları bulma ve kullanmada yeterli bilgiye sahibim.	1	2	3

*Geliştirenler: Akgün, Ö. ve Topal, M., (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. Sakarya University Journal of Education, 5(2), ss. 98-121.

ÖZGEÇMİŞ

Adı Soyadı : Ferat ÖNAL

Doğum Tarihi **:** 24/06/1979

Unvanı **:** Kıdemli Sistem Yönetim Uzmanı

Öğrenim Durumu **:** Yüksek lisans

Çalıştığı Kurum **:** STM Savunma Teknoloji ve Danışmanlık A.Ş.

İletişim **:** 0533 663 4610 / feratonal@gmail.com

Derece	Alan	Üniversite	Yıl
Sınıf Okulu	Bilgi İşlem Sınıfı Öğrenimi	T.S.K. K.K.K.lığı MEBS Okulu ve Eğitim Merkez K.lığı	1999
Lisans	Kamu Yönetimi Bölümü	Anadolu Üniversitesi	2006
Ön Lisans	Fotoğrafçılık ve Kameramanlık Bölümü	Anadolu Üniversitesi	2015
Y. Lisans	Yönetim Bilişim Sistemleri	Uluslararası Kıbrıs Üniversitesi	2019

Projeler

Mekândan Uzak Portreler Sergisi ve Söyleşi, Ankara Fotoğraf Akademisi 2012

Belgeler ve Sertifikalar

Gazi Üniversitesi, C++ Programlama Sertifikası (2001)

MEB, Photoshop Temel Eğitim Kusu Sertifikası (2009)

Gazi Üniversitesi, Indesign ile Sayfa Tasarımı Sertifikası (2011)

Microsoft Türkiye, Deploying Lync Server 2010 Sertifikası (2012)

Gazi Üniversitesi, Flash ile Web Tasarımı ve Animasyon Sertifikası (2012)

CCNA Exploration: Network Fundamentals ve CCNA Exploration: LAN Switching and Wireless Katılım Sertifikaları (2013)

TÜBİTAK, Microsoft Sistemleri Güvenliği, Windows Güvenliği, TCP/IP Güvenliği, Aktif Cihaz Güvenliği, Linux Güvenliği Kurs Katılım Sertifikası (2014)

Microsoft Türkiye, Uygulamalı Ağ Güvenliği, Cisco Router ve Switch Güvenliği Kurs Sertifikaları (2014)

Barikat Bilişim, Checkpoint Certified Security Administrator (2016)

Proya Bilişim, Lumension Device Control Yönetim Sertifikası (2016)

Türkiye Taekwondo Federasyonu Aday Hakem Belgesi (2016)

PADI İleri Seviye Dalgıç Sertifikası (2017)

Sosyal Aktiviteler

Fotoğrafçılık

Tüplü Dalış

Taekwondo

Doğa Sporları

Tecrübelerim

STM Savunma Teknoloji ve Mühendislik A.Ş. / Ankara'da Kıdemli Sistem Yönetim Uzmanı (2019-Devam Ediyor)

TSK Genelkurmay Başkanlığı ve Kara Kuvvetleri Komutanlığına bağlı karargâh ve birlik komutanlıklarında (Ankara, Kars, K.K.T.C., Çorlu/Tekirdağ) Microsoft Ağ ve Sistem Yöneticisi, Ağ Güvenlik Uygulamaları Yöneticisi, Kripto Sistemleri Yöneticisi, Bilgisayar Bakım Onarım Sorumlusu, Geniş Alan Ağı Kısım Amiri görevleri. (1999-2019)

Berçinler Elektronik / Samsun'da Orta Gerilim, Alçak Gerilim, Bobinaj, Bina tesisatı, Kompanzasyon Panosu Kurulumu, Fabrika Tesisatları Arızacılığı (Kömür Fabrikası, Tuğla Fabrikası, Torna Fabrikası vb.) Elektrik Teknisyeni (1995-1998)