KARABÜK ÜNİVERSİTESİ ÇALIŞANLARINA YÖNELİK KİŞİSEL SİBER GÜVENLİK ÜZERİNE ARAŞTIRMA

Abdullah KARAKAYA
Prof. Dr., Karabük Üniversitesi, İktisadi ve İdari Bilimler Fakültesi,
e-posta: akarakaya@karabuk.edu.tr
ORCID:0000-0002-3214-6771

Muhammed Ali YETGİN
Dr. Öğr. Üyesi, Karabük Üniversitesi, Sosyal Bilimler MYO,
e-posta: m.ali.yetgin@karabuk.edu.tr
ORCID: 0000-0002-8120-4704

Öz

Günümüzde, bilişim teknolojileri hayatın her alanında olduğu gibi yüksek öğretim faaliyetlerinde de yaygın olarak kullanılmaktadır. Bu durum son kullanıcılar açısından birçok güvenlik sorunlarını da beraberinde getirmektedir. Özellikle, üniversite çalışanları tarafından teknolojinin güvenli ve bilinçli bir şekilde kullanılması oldukça önemlidir. Bu araştırma, Karabük Üniversitesinde görev yapan akademik ve idari personelin kişisel siber güvenlik algılarını ölçmeyi amaçlamaktadır. Bu amaçla üniversite çalışanlarını istatistiki açıdan temsil eden örnek kitleden online anket yöntemiyle toplanan veriler paket programı kullanılarak; Cronbach Alpha, tek örneklem t testi, bağımsız örneklem t testi ve ANOVA testi ile analiz edilmiştir. Sonuçlar, çalışanların kişisel siber güvenliğe dair algılarında, bireylerin yaş, konum ve cinsiyetlerine göre farklılıklar olduğunu göstermektedir. Buna göre, tüm çalışanlara, dışarıdan gelebilecek siber tehlike ve sosyal mühendislik konularında, temel düzeyde bilgisayar, parola ve internet güvenliğini bireysel olarak uygulayabilmede, yeterli bilgi donanımına sahip olmaları gerekliliği ortaya çıkmıştır. Kişilerin siber güvenlik algılarını daha iyi anlayabilmek için özellikle hizmet sektörü ve bilgi teknolojileri alanında siber güvenliğin daha ön planda görüldüğü kurum ve kuruluşlarda yapılacak olan çalışmalar literatüre katkı sağlayabilecektir.
Anahtar Kelimeler: Siber, Siber Güvenlik, Siber Güvenlik Algıları.

A SURVEY ON PERSONAL CYBER SECURITY: THE CASE OF KARABUK UNİVERSITY*

Abstract

Information technologies are frequently used in today's world. Using the information technology brings many security problems for the users. Especially, it is important that university staff must use consciously the IT equipments. The purpose of this research is to measure the personal cyber security perceptions of academic and administrative staff who work in the University of Karabuk. The

* This study had been presented at the 2nd International Econder Congress and had been only included in the abstract book, not in the full text book.

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

research was made by random survey method and data collected from 185 people who work in the different departments both in administrative and academic positions. The data of the research was tested by package program. Cronbach Alpha (α) value was found to be reliable in the study. One sample t test, independent samples t test and one way ANOVA test were applied in the research. As a result of the research, it is found that there are some differencies in the responses according to the gender, position and age among the employees. As a suggestion, employees should be trained face-to-face on social engineering and information technologies including computer and web security. This study is recommended to be done for institutions using information technologies in a high level such as banks, insuarance companies and IT sectors.
Key words: Cyber, cyber security, cyber security perceptions.

GİRİŞ

Son çeyrek asırdır, internete erişimin çok hızlı bir şekilde yaygınlaşması, bilgisayarların küçültülerek taşınabilir bir teknolojiye dönüştürülmesi, cep telefonlarının benzer bir yazılım desteği ile kullanılması gibi gelişmeler ile bireylerin iletişim alışkanlıkları büyük bir dönüşüm geçirmiş, bireyler arasındaki coğrafi mesafeler bu hızlı iletişim ile kısalmış ancak tüm bu değişim ve yenilikler beraberinde yeni problemleri de ortaya çıkarmıştır. (Bıçakcı, 2014:102). İnternet kullanımının yaygınlaşması ile, sosyal medya gibi birçok platformlarda her türden bilginin paylaşılıyor olması içeriği suç teşkil edecek şekilde bireylerin ve örgütlerin bilgilerinin gizlilik ve bütünlüğü açısından bazı tehlikeleri de beraberinde getirmiştir, bu nedenle bilgi güvenliğinin önemi artmış, bireylerin ve örgütlerin daha fazla gerekli önlemleri almaları gerektiği ortaya çıkmıştır ve bu önlemlerin en başında son kullanıcı olan bireylerin, çalışanların siber güvenliğe dair olarak bilgilendirilmesi, bilinçlendirilmesi ve siber güvenlik alanında nitelikli personelin örgütte istihdamı gibi konular başı çekmiştir (Önaçan ve Atan, 2016:13). Bilgi güvenliğine dair risk ve tehditler, bilişim sistemine girme ve bilgiye yetkisiz erişim, sistemi engelleme, bozma ve verileri yok etme veya değiştirme, kimlik hırsızlığı ve verileri kötüye kullanma olarak tanımlanmıştır (Henkoğlu ve Yılmaz, 2013:457). Son kullanıcılar bilgi güvenliğinin bu belirtilen risk ve tehditlerine karşı bilinçli olmalıdırlar. Siber güvenlik konusunda bilgi sahibi olan katılımcıların yanıtları, farklı siber saldırı türlerini ayırt edebildiklerini, acemi katılımcıların ise saldırı türlerine duyarlı olmadığını göstermiştir (Asher ve Gonzalez, 2015:51). Türkiye'de 5237 sayılı Türk Ceza Kanunu'nda 243, 244, 245 ve 246. maddelere göre bilişim suçlarına yönelik düzenlemeler ile hukuki tedbirler alınmıştır (Hatipoğlu, 2017: 166). Bu çalışma ile Karabük Üniversitesinde çalışan akademik ve idari personelin çalıştıkları örgütleri nezdinde kişisel siber güvenlik algıları ölçülmüştür. Çalışanların algılarının analizi ile yapılan değerlendirmelerde, bireylerin siber güvenliğe dair gereksinim ve ihtiyaçları ortaya çıkarılmıştır. Çalışmanın ilk bölümü bilginin önemi ve güvenliği ile siber güvenliğin tanımlarına dair bir literatür araştırması iken, ikinci bölümde Karabük Üniversitesinde çalışan akademik ve idari personelin örgütsel açıdan kişisel siber güvenlik algılarına yönelik görgül bir araştırmadan oluşmuştur. Son bölümde, elde edilen bulgular değerlendirilmiştir.

Son yıllarda, bir çok kamu üniversitesi farklı şehirlerde eğitim ve öğretim faaliyetlerine başlamıştır. Böylelikle ülkenin dört bir yanında kamu üniversitelerinde akademik ve idari personel istihdamı da genişlemiştir. Üniversiteler, idari işler ile eğitim ve öğretim faaliyetlerinde teknolojinin

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

gelişimine ayak uydurabilen kuruluşlardır. Bu nedenle, personelin siber güvenlik farkındalığının önemi kaçınılmazdır. Bu çalışma da kamu üniversitesinde akademik ve idari personelin siber güvenlik algılarının ölçülmesi ile elde edilen bulgulardaki çıkarımların literatüre katkı sağlaması amaçlanmıştır.

1.KURAMSAL ÇERÇEVE

1.1. Bilgi, Önemi ve Güvenliği

Örgütlerin varoluş kaynağı, sürekliliği, verimliliği sahip olduğu bilginin üretilmesi, elde edilmesi ile yürütülmektedir. Bilgi, devletler, toplumlar, örgütler için bir güçtür ve teknolojinin sağladığı imkanlar ile bilginin üretimi, elde tutulması, işlenmesi ile küresel platformda bir güç kazanımı sağlanabilmektedir (Özdemirci ve Torunlar, 2018:78). Günümüzde, örgütlerin sahasında hakim olması; bilginin üretimi, kullanımı, yönetilmesi, hayatın merkezine yerleştirilmesi ile orantılı bir işlev olduğu belirtilmiştir (Özdemirci ve Torunlar, 2018:78). Bazı bilgiler örgütler için hususidir ve örgütler nezdinde kritik teknolojiyi ifade etmektedir. Bazı bilgiler umumi olarak paylaşımdadır ve bu paylaşımın önemli araçlarından birisi olarakta interneti gösterebilmekteyiz. İletişim ve haberleşmede çağımızın en güncel platformlarından biri olan internet ile dünya üzerindeki mesafeler, sınırlar ortadan kalkmış, aynı düşünce, merak, ilgi ve idrake sahip bireylerin birbirleri ile bilgiyi paylaştığı bir ortama dönüşmüştür (Bıçakcı, 2014:102). İnternetin gelişmesi ile Çin'de yaşayan birisinin, Güney Afrika'da yaşayan insanların durumundan, ekonomik problemlerinden, devletlerinin ikili ilişkilerinden haberdar olduğu görülmektedir (Bıçakcı, 2014:102).

İnternet kullanımının yaygınlaşması ile bilgi teknolojilerinde kişisel bilgi gizliliğini tehdit eden unsurlarda ortaya çıkmış, siber suç oranlarında artış görülmüştür, tehditlerin çoğalarak karmaşık bir durum haline gelmesi ile yasal sorumlulukların belirlenmesi ve bireylerin bilişim dünyasında bilinçli hareket etmeleri bir zorunluluk halini almıştır (Henkoğlu ve Yılmaz, 2013:452). Bilgi, bir örgütün önemli bir varlığıdır ve bilginin zarar görmesi, kaybı örgütsel bir itibar kaybına ve maddi kayba neden olabilmektedir (Henkoğlu ve Yılmaz, 2013:452), bu kayıpların önüne geçilebilmesi için örgüt tarafından bilgi güvenliği politikalarının oluşturulması, bilgi teknolojilerini kullanan kullanıcıların bilgi güvenliği konusunda bilinçlendirilmesi zorunlu hale gelmiştir (Henkoğlu ve Yılmaz, 2013:453). Bilgi teknolojilerinin zarar görmesi, saldırıya maruz kalması ya da çalışmasında meydana gelebilecek aksaklıklardan dolayı bilişim tabanlı hizmet akışının duraklaması ya da kesilmesi çok ciddi sonuçlar doğurabilecek riskleri ortaya çıkarabilecektir, bu doğrultuda örgüt çalışanlarının bilim ve teknolojideki gelişmelerden haberdar olabilmesi, ortaya çıkan siber saldırılara ve tehditlere karşın farkında olabilmesi için bilgi güvenliği konusuna eğilmelerinin önemli olduğu anlaşılmıştır (Yılmaz ve vd., 2015:142).

Bilgi güvenliğinde temel amaç doğru bireyin doğru bilgiye erişmesini sağlamaktır, farklı bir tanımı ile, bilen olan birey ile bilinen olan nesne arasında kurulan bağın güvenliğin sağlanması bilgi güvenliği olarak tanımlanmıştır (Henkoğlu ve Yılmaz, 2013:453). Bilgi teknolojilerinde, bilişim sistemlerinde, ilk olarak gizlilik, bilgilerin gizliliği, ikinci olarak bilginin bütünlüğü ve gerçekliği, üçüncü olarak bilginin kullanımı için kullanılabilirliği güvence altına alınmalıdır (Elmaghraby ve Losavio, 2014:493). Örgütlerde, bilgiye erişimde kullanıcılar arasındaki yetkilendirmeler doğru bir şekilde uygulanmalı, kolay olmayan dizinde

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

parolalar kullanılması ve kimse ile paylaşılmaması gerektiği belirtilmeli, açık anahtar altyapısı kurarak evrakların, belgelerin yetkisiz kişilerce erişimi, değiştirilmesi, kopyalanması engellenmelidir (Yılmaz ve vd., 2015:143).

Teknolojinin birçok alanda hayatımızı kolaylaştırması söz konusuyken, insanlığın doğasında var olan nefret, intikam, zorbalık gibi olumsuz davranışların yansıması ile bilgi teknolojilerine karşın risk ve tehditler süregelmiştir (Dikmen ve Tuncer, 2017:675). Dünya'da ve Türkiye'de bilgi güvenliği üzerine yapılmış çalışmaların genel itibariyle bilgi güvenliği yönetim sistemleri, risk değerlendirmesi, bilgi güvenliği farkındalık eğitimleri ve bilgi güvenliği sorunlarıyla ilgili durum tespiti şeklinde olduğu görülmüştür (Keser ve Güldüren, 2015:1169). Bu çalışmaların daha çok durum tespitine yönelik olduğu ancak bilgi güvenliğinde en zayıf halka olan insan unsurunun bilgi güvenlik düzeyinin farkındalık düzeylerine yönelik yeterli çalışma yapılmadığı görülmüştür (Keser ve Güldüren, 2015:1169). Siber güvenliğe dair insan boyutunu anlamak için genel olarak insan davranışını etkileyen faktörlerin ve siber güvenlik davranışının anlaşılması gerektiği önemle belirtilmiştir (Ünal ve Ergen, 2018:199). Özellikle son on yıldır siber alanda süregelen bilişim risk ve tehditleri göz önünde bulundurulduğunda bireylerin siber güvenliğe dair bireysel algılarının ölçüldüğü çalışmaların kapsamının bilhassa ulusal nezdinde yetersiz olduğu görülmektedir.

1.2. Siber Güvenlik

Siber güvenlik kavramı Soğuk Savaş sonrası gündeme gelen bir kavram olarak karşımıza çıkmıştır (Hansen ve Nissenbaum, 2009:1155). Siber güvenlik terimi genellikle bilgi güvenliği terimi ile dönüşümlü olarak kullanıldığı görülmüştür, ancak bu iki kavram esasında benzer değildir (Solms ve Niekerk, 2013:97). Siber güvenlik, geleneksel bilgi güvenliğinin sınırlarının ötesine geçerek yalnızca bilgi kaynaklarının korunmasını değil, kendisi de dahil olmak üzere diğer varlıkların korunmasını da içermektedir ve bilgi güvenliğinde, insan faktörüne atıf genellikle güvenlik sürecinde insanların rolü ile ilgili iken siber güvenlikte bu faktörün ek bir boyutu vardır, yani insanlar siber saldırıların potansiyel hedefleri olarak veya hatta farkında olmadan siber saldırılara katılmaktadırlar (Solms ve Niekerk, 201397).

Örgütlerdeki bilgisayarlar, tabletler, mobil telefonlar, dizüstü bilgisayarlar ve internet hatta gibi binlerce türden makineler siber güvenliğinin etki alanını oluşturmaktadır (Özdemirci ve Torunlar, 2018:82). Siber güvenlik, bilgi ve iletişim teknolojilerinin kötü amaçlı kullanımı ile ortaya çıkmış olan güvenlik sorunlarına karşın geliştirilmiş bir güvenlik yaklaşımıdır ve güvenlik alanının genişlemesine bir örnek oluşturmuştur (Barbak, 2016:281). Bir başka ifade ile, "küresel olarak birbirine bağlı elektronik verilerin veya ekipmanların, kriminal amaçlarla, yetkisiz veya kazayla kullanımına karşı korunması ve bu korumayı sağlamak için gereken teknoloji ve süreçler" olarak tanımlanmıştır (Ünal ve Ergen, 2018:194). Siber güvenliğin amacı; kurumların ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulması şeklinde açıklanmıştır (Ünver ve v.d., 2011:3).

Bilgi teknolojilerinin enerji, sağlık, ulaşım, finans gibi hemen her sektörde kullanımının yaygınlaşması, örgütlerin ve bireylerin bilgi ve iletişim teknolojilerine bağımlılığının gün geçtikçe artması ile bilgi teknolojileri devlet ve toplum

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

düzeninin sağlanmasında kritik bir rol üstlenmiş, bilgi ve iletişim teknolojilerinin sağladığı birçok yararların yanı sıra siber tehditlerde karşımıza çıkmıştır ve bu tehditlerinden korunmanın önemli bir adımı bireylerin bilinçliliği olarak gösterilmiştir (Karabacak, 2011:1). Siber tehditlerin başlıca üç nedenden oluştuğu belirtilmiş, bunlar "Internet tasarımındaki zafiyetler (adresleme sistemi, yönetim eksikliği, internetin çalışmasını sağlayan sistemlerin çoğunun açık ve şifresiz olması, zararlı yazılımları dağıtma kabiliyeti ve internetin merkezî olmayan büyük bir ağ olması), donanım ile yazılımlardaki hatalar, kritik sistemlere çevrim içi erişim imkânı" olarak sıralanmıştır (Aslay, 2017:25).

İnsanların güvenliğe yönelik siber davranışlar göstermesi gerektiğine yönelik bazı araştırmalar yapılmıştır. Coventry, Briggs, Blythe ve Tran'ın 2004 yılında yaptığı bir araştırmaya göre bireylerin siber davranışlar göstermemesinin temel bazı nedenleri ortaya konulmuştur (Ünal ve Ergen (aktaranlar), 2018:199-200). Sürekli internet bağlantısına açık olmak, internette mesaj olarak karşıya çıkabilen bir metinde "katılıyorum" seçeneğini okumadan, incelemeden seçmek, güvenilirliğini araştırmadan rast gele sitelerden video, ses, belge indirmek, anti virüs gibi güvenlik yazılımları kullanmamak, anlık kazanç ve eğlence amaçlı çeşitli internet platformlarında bazı bilgilerini paylaşmak, kolay parolalar belirlemek gibi bazı nedenler gösterilmiştir (Ünal ve Ergen, 2018:199-200). Siber tehditler; internetten gelen casusluk ya da hırsızlık amaçlı yetkisiz ve izinsiz erişim istekleri, izinsiz indirmeler ile zararlı kodların bilgi teknolojilerine bulaşabilmesi, yetkisiz kişilerce kod çalıştırma ile zararlı kodların enjeksiyonu, sisteme bulaşması, siteler arası istek sahteciliğine (Cross-site request forgery-CSRF) maruz kalmak, SQL enjeksiyonu, Xpath Enjeksiyonu, SSI enjeksiyonu, işletim sistemi enjeksiyona maruz kalmak, kimlik hırsızlığı (Phishing) ve oturum ihlaline (Session Violation) maruz kalmak, spamlara maruz kalmak, sosyal mühendislik ve hizmet aksattırmaya (DoS- Denial of Service) maruz kalmak şeklinde açıklanmıştır (Yaşar ve Çakır: 2015:491-495). Bireysel saldırıların yanında çeşitli bazı gruplarında siber saldırıları olabilmektedir, örneğin gönüllü grupların katılımı ile büyük katılımcıları organize eden Anonymous saldırıları bu kapsamda bilinmektedir (Bıçakcı, 2014: 125). Sızma testi yapacak kişide, kötü niyetli saldırganda, sistemde bulunan açıklıkların bulunması, kullanılması ve sisteme sızılmasında da aynı adımları gerçekleştirmektedir, buradaki fark kötü niyetli saldırganların sistemlere zarar vermesi ya da bilgi çalması, uzmanların ise bu açıklıkları kapatmasıdır ve sızma testleri yapılırken uygulanacak olan adımlarda bilgi toplanmalı, keşif yapılmalı, zafiyetler bulunmalı ve zafiyetleri istismar eden tehditler izole edilmelidir (Yiğit ve Akyıldız, 2014:15). Bilgisayar Mühendisliği ile Bilgisayar ve Öğretim Teknolojileri Öğretmenliği bölümlerinden 170 öğrenci üzerine yapılan bir araştırmada siber güvenliğe yönelik davranışlarının siber güvenliği sağlayacak düzeyde olduğu görülmüştür, bulgulara göre öğrenciler kişisel gizliliklerini koruyabildiği, güvenilmeyen uygulamalardan kaçındığı ve güvenlik için önlem alabildiği, kredi kartı veya banka kartı gibi ödeme bilgilerini koruyabildiği görülmüştür ve erkek ve kızların siber güvenlik davranışları arasında anlamlı bir farklılık olmadığı anlaşılmıştır (Ünal ve Ergen, 2018:202).

Dünyada da ülkeler ve uluslararası örgütler siber güvenlik konusunda çeşitli çalışmalar yapmaktadırlar. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) örgütü 2002 yılında üyelerinin bilgi teknolojileri ile ilgili altyapılarını korumalarına yönelik "Bilgi Sistemleri ve Ağlarının Güvenliği: Bir Güvenlik Kültürüne Doğru"

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

rehberi yayınlamıştır, Şanghay İşbirliği Teşkilatı (SCO)'nın 2007 yılındaki toplantılarında "SCO ülkelerinin uluslararası bilgi güvenliğini koruma eylem planı" imzalamışlardır (Ünver ve vd.., 2011:65). İngiliz Milletler Topluluğu (Commonwealth) üyeleri arasında 2002 yılında "Bilgisayar ve Bilişim Suçları Yasası" tasarlanmıştır, 2006 yılında Güney Doğu Devletleri Topluluğu (ASEAN) tarafından yapılan ASEAN Bölgesel Forumunda "siber saldırılar ve siber ortamın terörist amaçlı kötüye kullanımı ile mücadelenin, yasal ve diğer konularda hızlı ve iyi işleyen bir işbirliği ile mümkün olacağının bilincinde olarak, üye devletler bir an önce siber suçlar ve siber güvenlikle ilgili ulusal yasalarını çıkaracak ve bu yasaları ilgili uluslararası tavsiyelerden veya rehberlerden yararlanarak kendi ulusal koşullarına uygun şekilde uygulayacaklardır" kararı açıklanmıştır, Arap Devletleri Topluluğu siber suçlar ile yasaları yürürlüğe koymuştur, Afrika Birliğinde siber suç yasaları çalışmalarına başlanılmıştır (Ünver ve v.d., 2011:64). Amerikan Devletleri Topluluğu (OAS) 2004, 2005 ve 2006 yıllarında düzenlenen toplantılarda Avrupa Konseyi tarafından yürürlüğe konulan "Siber Suç Sözleşmesi" ne ait prensiplerin benimseneceğini açıklamıştır, Birleşmiş Milletler, APEC, OECD, G8, Commonwealth, Interpol örgütleri de siber güvenlik ve siber suçlar ile ilgili konularda bilgi alışverişi yapılabilecek mekanizmaların yürütüleceğine önem verdiklerini belirtmişlerdir (Ünver ve vd., 2011:63). Türkiye'de Siber Güvenlik Enstitüsü'nün (CSI) faaliyetleri, ulusal siber güvenlik kapasitesini geliştirmeyi amaçlayan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü bünyesinde 1997 yılında kurulmuştur (TÜBİTAK, 2020). TÜBİTAK Bilgem, 2012 yılından bu yana Türkiye'nin siber güvenliğini geliştirmek için faaliyet göstermektedir (TÜBİTAK, 2020).

Siber güvenliğin karşı önemli oyuncuları arasında bulunan hacker ya da diğer tabiri ile bilişim korsanları, devletlerin ilgi ve alakasını çekmiştir, birçok devlet bu korsanları casusluktan, istihbarata, güvenlikten siber suçlara kadar farklı alanlarda yönetimlerine destek vereceklerini düşünmelerinden dolayı bu kişiler ile çalışmayı istemişlerdir (Bıçakcı, 2014:115).

2. Karabük Üniversitesi Çalışanlarına Yönelik Araştırma

2.1.Araştırmanın Tanıtılması

Çalışma, Karabük Üniversitesi çalışanlarına yönelik kişisel siber güvenlik araştırmasıdır. Araştırmada, üniversite de görev yapan idari ve akademik personelin siber güvenliğe dair algıları ölçülmüştür.

Araştırmanın Amacı ve Katkısı

Günümüzün bir teknoloji çağı olduğu bir gerçekliktir. İnsanların iş hayatında teknoloji ile sürekli iç içe olması bir zorunluluk olarak karşımıza çıkmaktadır. Bireyler, çalıştıkları örgütlerdeki bilgisayar ve diğer bilişim teknolojilerine dair yazılım ve donanımların güvenliğinin sağlamasında dikkatli, tedbirli ve bilgi sahibi olmalıdır. Örgütler için bilgi, bilgi sürecinin güvenli transferi önemlidir. Günümüzde bilişim teknolojilerini kullanarak, siber saldırılar gerçekleştirerek bazı kötü niyetli kişiler örgüt ya da bireylere dair bilgileri çalabilmekte, bilginin bütünlüğünü bozabilmekte ve maddi kayıpların yanısıra paha biçilemez manevi kayıplara da sebebiyet verebilmektedirler. Bu kapsamda, siber saldırılara karşı siber güvenliğin farkındalığının örgüt çalışanları nezdinde anlaşılması, uygulanması örgütsel verimlilik ve etkinlik açısından önem arz etmektedir. Siber Güvenlik, siber ortamda kurum ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, stratejiler, güvenlik kavramları, risk yönetimi vb., uygulamalar ve teknolojiler bütünü olarak tanımlanmaktadır. Bu araştırmanın

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

temel amacı, 2019 yılında Dünya sıralamasında ilk bine girmiş olan Karabük Üniversitesinin akademik ve idari personelinin kişisel siber güvenlik yönündeki algılarının ölçülmesidir. Personelin siber saldırılara karşı farkındalığının yanısıra, bilgi teknolojilerini siber güvenlik açısından nasıl kullandıklarının da sonuçlarını görebilmek ve bu sonuçlara göre uygun nitelikte çözümler geliştirebilmektir.

Kapsamı ve Sınırlılıkları

Araştırmanın evreni, Karabük Üniversitesi olarak belirlenmiştir. Araştırmanın örneklemi akademik ve idari çalışanlar olmak üzere 1307 kişiden oluşmaktadır. Araştırmanın sınırlılıkları, Karabük Üniversitesine bağlı merkez ve ilçelerinde faaliyet gösteren akademik ve idari tüm birimler ile sınırlıdır. Anketteki sorular araştırmanın bir diğer sınırlığını oluşturmuştur.

Araştırmanın Sorunsalı, Hipotezleri ve Modeli

Araştırmada Erol ve arkadaşlarının (2015) uyarladıkları Kişisel Siber Güvenliği Sağlama Ölçeği kullanılmıştır. Araştırma ölçeği, likert olarak 25 maddeden oluşmaktadır. 1 hiçbir zaman, 2 nadiren, 3 arasıra, 4 sık sık ve 5 her zaman olarak uyarlanmıştır. Araştırmanın güven düzeyi %95, güven aralığı 7, ana kitle 1307 olarak hesaplandığında gerekli örneklem büyüklüğünün 171 olduğu görülmüştür. 1307 anketten, eksik ve yanlış olanlarında çıkartılması ile neticede 185 anket olarak örneklem büyüklüğünü karşıladığı görülmüştür.

Bu araştırma, çalışanların kişisel siber güvenlik algılarını ölçmek için amaçlanmıştır. Araştırmada kişisel siber güvenlik ölçeği tek boyutta 25 maddeden oluşmaktadır. Araştırmanın hipotezleri bağlamında, t testine göre 3 adet, bağımsız örneklem t testine göre 4, ANOVA testine göre 2 olmak üzere toplam 9 hipotez test edilmiştir. Hipotezler aşağıdaki gibi oluşturulmuştur.

H_1: Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem.

H_2: Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim.

H_3: Bilgisayarımda anti virüs yazılımı bulundururum.

H_4: Cinsiyetin, şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım üzerinde anlamlı bir etkisi vardır.

H_5: Cinsiyetin, online alışveriş işlemlerini şahsi bilgisayarımdan yaparım üzerinde anlamlı bir etkisi vardır.

H_6: Konumun, güvenmediğim sitelerden dosya indirmem üzerinde anlamlı bir etkisi vardır.

H_7: Konumun, tanımadığım kişilerden gelen e-posta eklerini açarım üzerinde anlamlı bir etkisi vardır.

H_8: Yaşın, sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm üzerinde anlamlı bir etkisi vardır.

H_9: Yaşın, internet şifrelerimin tümünün aynı olmasına dikkat ederim üzerinde anlamlı bir etkisi vardır.

Bulgular

Tüm istatistiksel analizlerin, verilerin geçerli ve güvenilir şartına bağlı olması gerektiğinden, istatistiksel olarak testlere başlamadan önce ilk olarak

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

verilerin güvenilirliğine ilişkin kontrol yapılması gerekmektedir (Bursal, 2019:226).

Tablo 1. Güvenilirlik

Cronbach's Alpha Değeri	Soru Madde Sayısı
,757	25

Güvenirlilik analizi sonucunda, Cronbach Alfa güvenirlilik katsayısı α = ,757 bulunduğundan ve 70'ten büyük olduğu için ölçeğimizin güvenirlilik katsayısının yeterli düzeyde olduğu böylelikle ölçek maddelerinden elde edilen puanların güvenilir olduğu sonucuna ulaşılmıştır. Demografik bilgilerin frekansları aşağıdaki gibi çıkmıştır.

Tablo 2. Demografik Özelliklere İlişkin Bilgiler

		Sayı	**Yüzde**
Eğitimi	Ön lisans veya altı	9	4,9
	Lisans	45	24,3
	Yüksek Lisans	42	22,7
	Doktora	89	48,1
Cinsiyet	Kadın	63	34,1
	Erkek	122	65,9
Deneyim Yıl	10 yıl ve az	98	53,0
	11-20 yıl arası	87	47,0
Yaş	20-30 yaş	50	27,0
	31-40 yaş	50	27,0
	41-50 yaş	57	30,8
	51 yaş ve üzeri	28	15,1
Konum	Akademik	129	69,7
	İdari	56	30,3
	Toplam	185	100,0

Demografik bilgilere bakıldığında, %30 oranında bir katılım sağlayan idari personelin araştırmaya ilgisinin daha az olduğu görülmüştür. Araştırmaya katılanların ilk 10 yıl iş deneyimine sahip olan bireyler ile 10 yıl üzerinde bir iş deneyimine sahip olan bireyler arasında birbirine yakın bir frekans oranına sahip oldukları görülmüştür. Araştırmaya katılım sağlayanların %66 'u erkek, %34 kadın cinsiyetinden olmuştur. Araştırmaya katılan bireylerin %5'i ön lisans veya altı, %24'ü lisans, %23'ü yüksek lisans, %48'i doktora eğitimi aldıklarını belirtmişlerdir. Araştırmanın tek yön t testi sonuçları Tablo 3'te gösterilmiştir. İfadeler "S" olarak kodlanmıştır.

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

Tablo 3. İfadelere Yönelik Hipotez Testleri

	Maddeler	t	p	Ort. Fark
S1	"Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim."	-12,658	,000	-1,14054
S2	"Kullandığım yazılımları güncellerim."	-6,073	,000	-,49730
S3	"Bilgisayarımda anti virüs yazılımı bulundururum."	-1,302	,194	-,12432
S4	"Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım."	-,439	,661	-,03243
S5	"İnternet şifrelerimin tümünün aynı olmasına dikkat ederim."	-12,136	,000	-1,10270
S6	"Web tarayıcımın güvenlik ayarlarını düzenlerim."	-12,883	,000	-1,15676
S7	"E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım."	-16,808	,000	-1,72973
S8	"Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim."	4,470	,000	,34595
S9	"İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam."	-,748	,455	-,09189
S10	"Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem."	-2,106	,037	-,24865
S11	"Güvenmediğim sitelere üye olmam**."**	-1,166	,245	-,14054
S12	"Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım."	-26,276	,000	-2,42162
S13	"İnternet ortamında gerektiğinde kişisel bilgilerimi (T.C. No, Doğum tarihi, GSM No vb.) paylaşırım."	-19,941	,000	-1,83784
S14	"Web geçmişimi temizlerim."	-10,432	,000	-,87027
S15	"İnternet bankacığı işlemlerini şahsi bilgisayarımdan yaparım."	1,536	,126	,12973
S16	"Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım."	-,423	,673	-,03784
S17	"Tanımadığım kişilerden gelen e-posta eklerini açarım."	-29,690	,000	-2,11892

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

S18	"Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm."	-26,451	,000	-2,05946
S19	"İnternet üzerinden yer bildirimi yaparım."	-25,804	,000	-2,04865
S20	"Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım."	-31,237	,000	-2,21622
S21	"Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım."	-2,256	,025	-,20541
S22	"Güvenmediğim sitelerden dosya indirmem."	-3,220	,002	-,32973
S23	"İnternette kullandığım (eposta, sosyal ağ vb.) şifreleri değiştiririm."	-9,957	,000	-,74595
S24	"Unutmamak için akılda kalan kolay bir şifre belirlerim."	-13,944	,000	-1,27027
S25	"Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım."	-33,277	,000	-2,45946

*P değeri ,000 ise ileri düzeyde anlamlıdır.

Tablo 3'e göre, S3, S4, S9, S11, S15, S16 maddeleri $p \leq 0,05$ olmadığından istatistiksel olarak anlamlı bulunmamıştır. S1, S2, S5, S6, S7, S8, S10, S12, S13, S14, S17, S18, S19, S20, S21, S22, S23, S24, S25 maddeleri için $p \leq 0,05$ olduğundan istatistiksel olarak anlamlı bulunmuştur.

Bağımsız örneklem t testinde, bağımsız değişkenler cinsiyet, konum ve bağımlı değişken maddeler arasındaki bulgular Tablo 4'te ki gibi oluşmuştur. Konum için S15, S16, S20, S23, S25 ve cinsiyet için S1, S2, S6, S7 değerleri $p \leq 0,05$ olduğundan istatistiksel olarak anlamlı diğer tüm maddeler konum ve cinsiyet için $p \leq 0,05$ olmadığından istatistiksel olarak anlamlı bulunmamıştır.

Tablo 4. Cevaplayıcıların Cinsiyet ve Konum ile İfadeler Arasındaki İlişkiler

	Maddeler	**p değ.**	
		Konum	Cinsiyet
1	"Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim".	,808	,003
2	"Kullandığım yazılımları güncellerim".	,326	,020
3	"Bilgisayarımda anti virüs yazılımı bulundururum."	,542	,393
4	"Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım."	,773	,125

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

5	"İnternet şifrelerimin tümünün aynı olmasına dikkat ederim."	,584	,289
6	"Web tarayıcımın güvenlik ayarlarını düzenlerim."	,251	,015
7	"E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım."	,176	,014
8	"Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim."	,691	,792
9	"İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam."	,057	,869
10	"Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem."	,837	,222
11	"Güvenmediğim sitelere üye olmam."	,913	,306
12	"Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım."	,558	,764
13	"İnternet ortamında gerektiğinde kişisel bilgilerimi (T.C. No, Doğum tarihi, GSM No vb.) paylaşırım."	,451	,403
14	"Web geçmişimi temizlerim."	,072	,072
15	"İnternet bankacığı işlemlerini şahsi bilgisayarımdan yaparım."	,003	,806
16	"Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım."	,009	,287
17	"Tanımadığım kişilerden gelen e-posta eklerini açarım."	,112	,382
18	"Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm."	,514	,742
19	"İnternet üzerinden yer bildirimi yaparım."	,197	,674
20	"Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım."	,004	,288
21	"Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım."	,106	,907
22	"Güvenmediğim sitelerden dosya indirmem."	,278	,190
23	"İnternette kullandığım (eposta, sosyal ağ vb.) şifreleri değiştiririm."	,020	,448
24	"Unutmamak için akılda kalan kolay bir şifre belirlerim."	,619	,615
25	"Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım."	,000	,651

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

ANOVA tablosu, hem gruplar arasında, hem de gruplar içinde kareler toplamını, serbestlik derecesini verir, esas temel nokta p değeridir ve Sig. değeri .05'ten küçük ya da ona eşit ise, bağımsız değişkenler için bağımlı değişken üzerinden elde edilmiş olan ortalama puanlarda anlamlı bir fark var olduğu anlaşılmaktadır (Pallant, 2017, s. 281). Tablo 5'te yer alan ANOVA testine göre, yaş için S7, S9, S10, S11, S16, S17, S20, S22; $p \leq 0,05$ olduğundan istatistiksel olarak anlamlı diğer tüm maddeler $p \leq 0,05$ olmadığından istatistiksel olarak anlamlı bulunmamıştır. ANOVA testinde elde edilen bu bulgulara göre hipotezlerin kabul ya da ret durumları sonuç kısmında açıklanmıştır.

Tablo 5. Cevaplayıcıların Yaşı ve İfadeler Arasındaki İlişki

	Maddeler	**P değ.**
		Yaş
1	"Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim."	,481
2	"Kullandığım yazılımları güncellerim."	,121
3	"Bilgisayarımda anti virüs yazılımı bulundururum."	,929
4	"Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım."	,382
5	"İnternet şifrelerimin tümünün aynı olmasına dikkat ederim."	,948
6	"Web tarayıcımın güvenlik ayarlarını düzenlerim."	,186
7	"E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım."	,003
8	"Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim."	,738
9	"İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam."	,000
10	"Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem."	,000
11	"Güvenmediğim sitelere üye olmam."	,000
12	"Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım."	,437
13	"İnternet ortamında gerektiğinde kişisel bilgilerimi (T.C. No, Doğum tarihi, GSM No vb.) paylaşırım."	,072
14	"Web geçmişimi temizlerim."	,717
15	"İnternet bankacığı işlemlerini şahsi bilgisayarımdan yaparım."	,143
16	"Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım."	,024

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

17	"Tanımadığım kişilerden gelen e-posta eklerini açarım."	,029
18	"Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm."	,072
19	"İnternet üzerinden yer bildirimi yaparım."	,415
20	"Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım."	,018
21	"Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım."	,389
22	"Güvenmediğim sitelerden dosya indirmem."	,017
23	"İnternette kullandığım (eposta, sosyal ağ vb.) şifreleri değiştiririm."	,363
24	"Unutmamak için akılda kalan kolay bir şifre belirlerim."	,133
25	"Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım."	,762

SONUÇ VE ÖNERİLER

Araştırmada ifadelere yönelik oluşturulan hipotezlere göre; H_1: "Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem" hipotezinde p değeri için 0,05 altında olduğundan, katılımcılar açısından istatistiksel olarak anlamlı bulunmuş ve katılımcıların sosyal ağlardan gelen arkadaşlık isteğini kabul etmediği görülmüştür. H_2: "Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim" hipotezinde p değeri için 0,05 altında bulunduğundan katılımcıların kendi bilgisayarı dışında başka bilgisayarda bilgi tutmadığı görülmüştür. Buna göre H_1 ve H_2 hipotezleri kabul edilmiştir. H_3: "Bilgisayarımda anti virüs yazılımı bulundururum" hipotezinde p değeri için 0,05 üzerinde bulunduğundan katılımcıların antivirüs kullanımına pek dikkat etmedikleri görülmüştür. Buna göre H_3 hipotezi reddedilmiştir.

Araştırmada, H_4: "Cinsiyetin, şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım üzerinde anlamlı bir etkisi vardır" hipotezine göre p değeri 0,05'in üzerinde olduğundan istatistiksel olarak anlamlı değildir ve şifre belirlemede basit dizilimler kullanmak kişinin cinsiyeti ile farklılaşmamaktadır. H_5: "Cinsiyetin, online alışveriş işlemlerini şahsi bilgisayarımdan yaparım üzerinde anlamlı bir etkisi vardır" hipotezinde p değeri 0,05'in üzerinde olduğundan istatistiksel olarak anlamlı değildir ve online alışverişi şahsi bilgisayardan yapmanın kişinin cinsiyeti ile farklılaşmamaktadır. Bu sonuçlara göre H_4 ve H_5 hipotezleri reddedilmiştir. Araştırmanın bulgularından elde edilen sonuçlara göre konuma göre H_6: "Konumun, güvenmediğim sitelerden dosya indirmem üzerinde anlamlı bir etkisi vardır" hipotezine göre p değeri 0,05'in üzerinde olduğundan istatistiksel olarak anlamlı değildir. Buna göre güvenilmeyen sitelerden dosya indirmek konuma göre farklılık göstermemektedir. Diğer sonuca göre H_7: "Konumun, tanımadığım kişilerden gelen e-posta eklerini açarım üzerinde anlamlı bir etkisi vardır" hipotezinde p değeri 0,05'in üzerindedir. Bu sonuçta, konuma göre

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

tanınmayan kişilerden gelen e-postaları açmak istatistiksel olarak farklılık göstermemektedir. Bu sonuçlara göre H_6 ve H_7 hipotezleri reddedilmiştir. Araştırmada, H_8: "Yaşın, sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm üzerinde anlamlı bir etkisi vardır" hipotezinde p değeri 0,05'in üzerindedir. Buna göre, yaş ile sosyal paylaşım sitelerinde kişisel bilgilere yer vermek arasında istatistiksel olarak bir anlamlılık bulunmamaktadır. Bir diğer çıkan sonuçta H_9: "Yaşın, internet şifrelerimin tümünün aynı olmasına dikkat ederim üzerinde anlamlı bir etkisi vardır" hipotezinde p değeri 0,05 üzerinde bulunduğundan yaş ile internet şifrelerinin hepsini aynı yapmak arasında istatistiksel olarak bir anlamlılık görülmemiştir. Bu sonuçlara göre H_8 ve H_9 hipotezleri reddedilmiştir.

Bu araştırmanın sonuçları, çalışanların dış tehditlere karşı farkındalıklarının olduğunu göstermektedir. Çalışanların bilgi güvenliğine yönelik eğilimlerinde konum, cinsiyet ya da yaş farklılıklarının çalışanların algılarında ayırıcı bir özellik teşkil etmediği anlaşılmıştır. Bu noktada çalışanların desteklenmesi yönü ile sağlanabilecek bilgi güvenliği eğitimlerinin, çalışanları aynı yönde geliştireceği düşünülmektedir. Bireylerin anti-virüs kullanımı konusundaki eksikliği, bilgi güvenliği eğitim desteğinin sağlanmasını kaçınılmaz kılmaktadır.

Bireylerin tanımadığı kişilere karşı yaş, konum ve cinsiyet olarak tedbir yönleri her ne kadar olumlu bir yönde gözüküyor olsa da oltalama (phishing), sosyal mühendislik olarak yapılan her türlü harici saldırılar gün geçtikçe daha profesyonelce çalışanların karşısına çıkabilmekte, bu nedenle güncel konu ve örneklemleri ile tüm çalışanlara konu ile ilgili eğitimin de verilmesinin yararlı olacağı öngörülmektedir.

Kişisel siber güvenlik algılarına yönelik farklı yöntemler ile yapılacak her türlü çalışmanın literatüre katkı sağlayacağı düşünülmektedir. Finans, sigorta, bilgi teknolojileri başta olmak üzere hizmet sektörünün birçok alanında faaliyet gösteren ve siber güvenliğin daha ön planda tutulduğu kurum ve kuruluşlarda çalışanların siber güvenlik algılarına yönelik çalışmaların yapılması yararlı olacaktır.

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

KAYNAKÇA

Aslay, F. (2017), **''Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi''** International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1), 24-28.

Barbak, A. (2017), **''Türkiye'de Kamu Politikası Sürecinde Güvenlik-Kalkınma Bağı: Ulusal Kalkınma Planları Üzerine Bir Araştırma''**, UİİİD-İJEAS, (18), 263-288.

Ben-Asher, N., Gonzalez, C. (2015), **''Effects Of Cyber Security Knowledge On Attack Detection'',** Computers in Human Behaivor, Volume 48, 51-61.

Bıçakcı, S. (2014), **''NATO'nun Gelişen Tehdit Algısı: 21.Yüzyılda Siber Güvenlik'',** *Uluslararası İlişkiler*, 10 (40), Güz 2014, 101-130.

Bursal, M. (2019), SPSS ile Temel Veri Analizleri, Anı Yayıncılık, Ankara

Dikmen, M. Tuncer, M. (2017), **''Akademisyenlerin Siber Zorbalığa Yönelik Algıları ve Mücadele Etme Yöntemleri'',** *Dicle Üniversitesi Ziya Gökalp Eğitim Fakültesi Dergisi*, Issue/Sayı 31, 675-686.

Elmaghraby, A.S., Losavio, M.M. (2014), **''Cyber security challenges in Smart Cities: Safety, Security and Privacy'',** *Journal of Advanced Research*, 5, 491–497.

Hatipoğlu, *C.* (2017), **''Teknolojik Savaşlar: Siber Terörizm Tehditleri''**, *International Congress on Political, Economic and Social Studies (ICPESS), 09-11 Nov. 2017*, 157.168.

Hansen, L., Nissenbaum, H. (2009), **''Digital Disaster, Cyber Security, and the Copenhagen School'',** *International Studies Quarterly*, Volume 53, Issue 4, 1155–1175.

Henkoğlu, T., Yılmaz, B. (2013), **'' Avrupa Birliği (AB) Bilgi Güvenliği Politikaları'',** *Türk Kütüphaneciliğ*i, 27, 3, 451-471.

Karabacak, B. (2011), **''Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri''**, *Siber Güvenlik Çalıştayı, Bilgi Güvenliği Derneği, Ankara*, *29 Eylül 2011*, 1-11.

Keser, H., Güldüren, C. (2015), **''Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması'',** *K. Ü. Kastamonu Eğitim Dergisi,* 23 (3), 1167-1184.

Solms, R. , Niekerk, J. (2013), **''From Information Security To Cyber Security''**, *Computers & Security*, Volume 38, 97-102.

Özdemirci, F., Torunlar, M. (2018), **''Bilgi-Değişim-Siber Güvenlik-Bağımsızlık''**, *Bilgi Yönetimi,* 1, 78-83.

Önaçan, M., B., K., Atan, H. (2016), **''Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği'',** *Trakya University Journal of Engineering Sciences,* 17(1), 13-21.

Pallant, J. (2017), **''SPSS Kullanma Kılavuzu''**, (Çev. Balcı, S., Ahi, B.), Anı yayıncılık, Ankara.

TÜBİTAK(2020).https://sge.bilgem.tubitak.gov.tr/en/kurumsal/cyber-security-institute, Erişim Tarihi: 18.12.2020.

Ünver, M., Canbay, C., Mirzaoğlu, A. G. (2011), **''Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler''** (1. Basım, Nisan 2011). *Bilgi Teknolojileri ve İletişim Kurumu*. ISBN: 978-9944-0189-6-8

Ünal, A.N., Ergen, A. (2018), **''Siber Uzayda Yeterince Güvenli Davranıyor Muyuz? İstanbul İlinde Yürütülen Nicel Bir Araştırma'',** *MCBÜ Sosyal Bilimler Dergisi,* Cilt:16, Sayı:2, 191-216.

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020

Yaşar, H., Çakır, H. (2015), **''Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri'',** *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 3, 488-507.
Yılmaz, E. N., Ulus, H. İ., Gönen, S. (2015), ''**Bilgi Toplumuna Geçiş ve Siber Güvenlik''**, *Bilişim Teknolojileri Dergisi*, 8 (3) , 133-146.
Yiğit, T., Akyıldız, M.A. (2014), **''Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi'',** *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 18(1), 14-21.

Araştırma Makalesi
DOI: 10.47147/ksuiibf.816171
Makale Geliş – Kabul Tarihi: 25.10.2020– 30.12.2020