Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri

Literatür Makalesi/Review Article

İhsan TUĞAL[1]*, Cengiz ALMAZ[1], Mehmet SEVİ[2]

[1]Bilgisayar Mühendisliği Bölümü, Muş Alparslan Üniversitesi, Muş, Türkiye
[2]Bilgi İşlem Daire Başkanlığı, Muş Alparslan Üniversitesi, Muş, Türkiye
i.tugal@alparslan.edu.tr, c.almaz@alparslan.edu.tr, m.sevi@alparslan.edu.tr
(Geliş/Received:18.06.2020; Kabul/Accepted:17.05.2021)
DOI: 10.17671/gazibtd.754458

***Özet*—** Üniversite kampüsleri farklı ağ yapıları ve kullanıcı sınıfları barındıran yerlerdir. Kampüs ağları günümüzde çok karmaşık hale geldi. Öğretimin kalitesini yükseltmek için bilgi teknolojileri kampüslerde en iyi şekilde kullanılmaktadır. Üniversiteler birçok kesimin ilgisini çeken verileri kendi sistemlerinde barındırırlar. İnternete çıkışı olan bu yapılar sürekli siber tehditlere maruz kalmaktadır. Bu çalışmada siber tehlikelere karşı birçok zayıf halkası bulunan üniversitelerin neden saldırıların hedefinde olduğu anlaşılmaya çalışıldı. En çok kullanılan saldırı yöntemlerinin neler olduğuna bakıldı. Siber zayıflıkların giderilmesi için çözümler önerildi. Bilgi güvenliği politikalarının oluşturulması ve uyulması, kullanıcılara siber farkındalık eğitimleri aldırılması, bilgi sistemleri altyapılarının güçlendirilmesi gerektiği görüldü. Siber farkındalık eğitimleri konusunda izlenecek yol önerildi. Üniversiteleri kötü algılardan koruyacak, siber zararlara karşı güçlü kılacak çok boyutlu çalışmalardan ve politikalardan taviz verilmemelidir.

***Anahtar Kelimeler*—** siber tehditler, ağ güvenliği, bilgi güvenliği, üniversite, siber farkındalık.

Cyber Security Issues and Awareness Training at Universities

***Abstract*—** University campuses accommodate different network structures and user classes. Campus networks have become very complex today. In order to improve the quality of teaching, information technologies have been used in the best way on campuses. Universities host the data in their own systems that attract the attention of many groups. These structures, which have access to the internet, are constantly exposed to cyber threats. In this study, we tried to understand why these structures are the target of attacks, which have many weak links against cyber hazards. What are the most used attack methods were examined. Solutions were proposed to overcome these weaknesses. It was observed that information security policies should be established and followed, users should be provided with cyber awareness training and information systems infrastructures should be strengthened. A following path for cyber awareness training was proposed for universities. Studies and policies that will protect universities from bad perceptions and make them strong against cyber harms should not be compromised.

***Keywords*—** cyber threats, campus network, information security, university, cyber awareness.

1. GİRİŞ (INTRODUCTION)

Günümüzde üniversiteler siber suçluların en çok hedefine aldığı yerlerden biridir. Hedef haline gelmesinin nedenleri arasında binlerce kişinin kişisel bilgilerini barındırması, öğrenci, personel ve hizmet verdiği kişilerin verilerini bilgi sistemlerinde saklaması ve çevrimiçi olarak birçok hizmeti vermesidir. Bünyesinde araştırma merkezleri, enstitüler, teknoparklar, hastaneler barındırmaktadır. Araştırma, geliştirme faaliyetleri ve bilimsel bilgi paylaşımı üniversitelerin asli görevleridir [1].

Üniversiteler bilgi teknolojileri deneyimini kesintisiz sürdürmek için imkânlarını her geçen gün arttırmaktadır.

Teknolojinin gelişmesi ile üniversiteler dijital yeteneklerini geliştirmiş, eğitim-öğretim, araştırma, iletişim ve başka hizmetlerinde bilgi teknolojilerini sonuna kadar kullanmaya başlamıştır. 2019 yılında başlayan Kovid-19 pandemi süreci de uzaktan eğitim gibi ihtiyaçları ortaya çıkarmış, üniversitelerin teknoloji altyapılarının önemini bir kez daha göstermiştir. Günümüz üniversiteleri teknolojiye bağımlı hale gelmiştir. Teknoloji ve internet, öğrenme süreçlerinin zorunlu bir parçası olmuştur.

Öğrencilerin ve üniversite çalışanlarının mesleki ve kişisel gelişimine bilgi teknolojilerinin ve internetin etkisi artık göz ardı edilemez. Öğrenciler ve üniversite çalışanları aynı anda birden fazla cihazı kampüs ağlarında kullanmaya başlamıştır. İnternet ile bütün üniversiteler çeşitli servislerle birbirine bağlanmış, ağın bir parçası haline gelmişlerdir. İnternet eğitim hayatına büyük katkılar sağlamaktadır. Faydalarına rağmen internet ve bilgisayar ağları çok güvensiz ortamlardır. Bunu güvenli hale getirmek için bir bütün olarak çok çaba göstermek gerekmektedir.

Siber uzay, dünyada ve uzayda bulunan bilişim sistemleri ve ağlarının oluşturduğu yapının tümüne denir [2]. Sadece donanım, yazılım, veri ve bilgi sistemlerini ifade etmez. Aynı zamanda bu ağları ve altyapıları kullanan insanları ve sosyal etkileşimleri içinde barındırır. İnternetten daha fazlasıdır. Siber güvenlik ise bu sistemleri istenmeyen durumlara karşı korumaktır. Teknolojik hizmetlerin artışı ile paralel olarak siber tehditlere maruz kalma ihtimali artmaktadır. Bu tehditler siber güvenliği kritik öneme sahip hale getirmiştir. Her geçen gün farklı kurumlarda ve daha özel olarak yükseköğrenim kurumlarında birçok rahatsız edici siber suç vakalarının olduğu bilinmektedir [3,4]. Bu yüzden kurumlar sistemlerini oluştururken ve planlamalarını yaparken siber tehditlere karşı bir savunma geliştirmesi, çözümler oluşturması gerekmektedir. Bu çok ciddi üzerinde durulması gereken, son derece teknik ve hızla gelişme gösteren bir konudur.

Aslında üniversitelerin siber güvenlik konusundaki endişeleri 1970'lerden itibaren var [5]. Savunma yöntemleri geliştikçe, bilgisayar korsanları da değişikliklere uyum sağlayarak karmaşıklıklarını arttırmakta ve yeni saldırı yöntemleri geliştirmektedirler. Eğitim kurumlarının karşılaştığı siber tehditlerden örnek vermek gerekirse; web sayfalarının çökertilmesi, istenmeyen video ve duyuruların sayfalara atılması, araştırma verilerinin çalınması, e-posta yoluyla tehdit ve kullanıcıların aldatılması, servislerin hizmet vermesinin engellenmesi, sistem kaynaklarının başka amaçlar için kullanılması, kişisel verilerin çalınması ve değiştirilmesi gibi olaylar sayılabilir [6].

Mayıs 2019'da Avustralya Bilgi Komiserliği (OAIC), Avustralya'daki tüm veri ihlallerinin % 35'ine insan hatasının neden olduğunu ortaya çıkardı [7]. İstatistiklere göre 2019 yılında siber yollarla 8,5 milyar kayıt ihlal edildi ve saldırganlar daha fazla çalıntı kimlik bilgilerine erişim sağladı. Fidye yazılımı saldırıları 2019'un dördüncü çeyreğinde yıllık %67 oranında arttı. Operasyonel Teknoloji (OT) saldırıları yıldan yıla %2.000 artıyor. Nesnelerin İnterneti (Internet of Things IoT), OT ve bağlantılı endüstriyel ve tıbbi sistemler saldırılara daha çok hedef olmaya başlamıştır. Tablo 1'de görüldüğü gibi eğitim sektörü gün geçtikçe daha çok siber hedef haline gelmektedir. Her biri farklı bir motivasyona sahip olan saldırganlar, akademik kurumların ağlarını ihlal etmek için çeşitli yöntemler kullanmaktadırlar. En yaygın olarak gözlemlenen yöntem ise, belirli akademik kurum veya araştırma alanına uyarlanmış kimlik avı e-postaları olmaya devam etmektedir. 2019'da yayınlanan raporlar, 2019'da yalnızca ABD'de en az 500 okulun çoğunlukla fidye yazılımı mağduru olduğunu göstermektedir [8]. Araştırma verilerini çalmak için siber saldırılar her geçen gün artarak devam etmektedir. Spam saldırılarından korunmak için Türkiye'deki üniversitelerin %49'u e-posta sistemlerini kendi sunucuları dışında (Google, Outlook, Yandex gibi) ücretsiz imkan sağlayan servislerde barındırmaktadır [9]. Erişim denetimlerini güvence altına almak her geçen gün daha da önemli ve zor hale gelmektedir.

Kampüs ağları günümüzde çok karmaşık hale gelmiştir. Bu karmaşık yapının yönetilmesi, işlevini tam olarak yerine getirmesi için çok çaba gösterilmesi gerekir. Bu çalışmada mevcut kampüs ağlarının siber tehditlere karşı mevcut durumu, alınması gereken kritik önlemlerin neler olduğu anlaşılmaya çalışıldı. Bir üniversitenin hedef seçilmesinin sebepleri, tehdit çeşitleri, en çok hangi tür saldırılara maruz kaldığı, bunların nasıl önleneceği analiz edildi. Üniversitelerde savunma hattının en zayıf halkası personel ve öğrencilerdir. Güvenlik bilincinin geliştirilmesi uzun zaman alır ve zordur [6]. Siber farkındalık oluşturmak eğitim yolu ile olur. Bu amaçla farkındalık eğitiminde izlenecek bir yol önerildi. Bu çalışmada amaçlanan, yükseköğretim kurumlarının siber güvenlik alanındaki sorunlarına odaklanmak ve çözüm önerileri sunmaktır.

Tablo 1. Siber saldırılarda hedeflenen ilk 10 sektör [8]
(Top 10 sectors targeted in cyber attacks)

Sektör	2019 sıralama	2018 sıralama	Değişim
Finans	1	1	-
Perakende	2	4	2
Taşımacılık	3	2	-1
Medya	4	6	2
Danışmanlık	5	3	-2
Kamu	6	7	1
Eğitim	7	9	2
İmalat	8	5	-3
Enerji	9	10	1
Sağlık	10	8	-2

2. HEDEFTE OLMA SEBEPLERİ (REASONS FOR BEING ON TARGET)

Bir sisteme veya yazılıma siber saldırı gerçekleştirmenin birçok amacı olabilir. Bu amaç bazen bilgilerin ele geçirilmesi, bazen sistemlere zarar verilmesi, çalışamaz hale getirilmesi veya algı oluşturulmasıdır. Üniversiteler bu kapsamda en çok saldırı hedeflenen noktalar arasındadır

[8]. Bunun sebeplerine baktığımızda en önemli nedenlerinden biri, kişisel olarak tanımlanabilir öğrenci, personel ve hizmet alan kişilerin saklanan her türlü verileridir. Bu veriler dolandırıcılık amacıyla kişileri, kurumları zor durumlara sokmak için kullanılabilir. Araştırmacıların verilerinin ele geçirilmek istenmesi de önemli etkenlerden biridir.

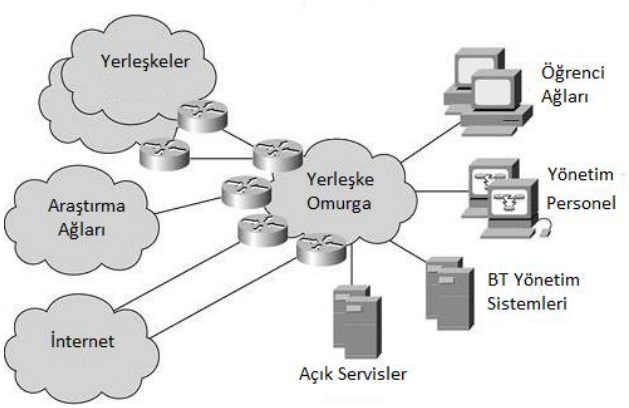
Üniversiteler genç ve tecrübesiz kişilerin bulunduğu ortamlardır. Öğrenciler yüksek zekâ ve tutkuya sahiptirler, ancak davranışlarının sonuçları için sorumluluklarının çok farkında değillerdir [10]. Zafiyete sebep olabilecek birçok davranışı kolayca yapabilirler. Dış tehditlere aracı olabilir veya kendileri saldırılar düzenleyebilirler. Bu saldırılar sınav notlarını düzeltmek, arkadaşlarına kendilerini ispatlamak, kötü ders notlarından dolayı ders hocalarını hedef almak şeklinde olabilir.

Çok sayıda bilgisayar barındıran üniversiteler oltama e-postaları ve spam yöntemleri kullanılarak da hedef alınmaktadır. Personelin e-posta adreslerinin web sayfalarında gösterilmesi bu tür saldırıları artırmaktadır. Ayrıca ele geçirilen bilgisayar kaynakları başka sistemlerin hedef alınması için de kullanılmaktadır.

Ülkeler arasında da siber savaşlar olmaktadır. Siber güçlerini sürekli test etmektedirler. Ülkelerin sahip olduğu akademik bilgileri çalmak, ülkelerin yapmış olduğu bilimsel çalışmalardan haberdar olmak içinde bu tür saldırılar yapılmaktadır. Bilimsel kabiliyetlerini arttırmak isteyen devletler, siber saldırılarla ülkelerin gizli çalışmalarından haberdar olmak istemektedirler. Bu yüzden hedeflerinde üniversitelerde bulunmaktadır [11].

Üniversitelere yönelik siber saldırıların başarılı olma şansı yüksektir. Büyük ve karmaşık bir ağ yapısı vardır. Şekil 1'de en basit şekliyle temel elemanları barındıran bir üniversite ağ topolojisi gösterilmiştir [12]. Üniversite teknolojik altyapıları sadece fakülte, personel ve öğrencilerin ihtiyaçlarını karşılamak için kurulmamıştır. Bu yapılar aynı zamanda ziyaretçilerin ve büyük miktarlarda veri paylaşan farklı konumlardaki araştırmacıların ihtiyaçlarını karşılamak için de tasarlanmıştır [13]. Bu tür sistemleri korumak zordur. Aşırı güvenlik tedbirleri hizmetlerin istenilen seviyede verilmesini engeller. Tam tersi yetersiz güvenlik tedbirlerinin alınması, kötü niyetli kullanım ve saldırıların artmasına neden olur. Karmaşık yapısından dolayı eksik tanımlanmış kurallar ve yapıların olma ihtimali yüksektir. İnternet ağına bağlı birçok farklı cihaz vardır. Büyük bir üniversitenin herhangi bir zamanda yüz binlerce kullanıcısı olabilir.

Bu kullanıcılar sisteme daha az güvenli donanımlardan erişebilirler. Cep telefonu, tablet, dizüstü bilgisayar, IOT cihazları bunlardan bazılarıdır. Eski donanım, en son yazılım güncellemelerini yüklemek için gereken özelliklere sahip olamayabilir ve bunları bilgisayar korsanlarına karşı savunmasız bırakır. Bu cihazları sürekli güncel tutmak çok zordur. Mutlaka açıklıkları olacaktır. Cihazları tek tip ayarlarda tutma şansı yoktur. Üniversitenin ağına erişmek isteyen cihazları kontrollü ağa dahil etmek iş yükünü arttırır ve zordur. Üniversitelerde bu cihazlar birbirinden çok farklı amaçlarla kullanılabilir. Bilgi işlem biriminden çok farklı izinler talep edilebilir. Araştırma ve eğitim faaliyetlerinin yürütülmesi için bu istekler büyük çoğunlukla kabul edilir.



Şekil 1. Kampüs ağı
(Campus network)

Öğrencinin ihtiyacı olan bilgilere erişmek için kullandığı yöntem okulun ağıdır. Zayıf şifreler ve çok fazla alana erişimi olan çok fazla kullanıcı ciddi bir güvenlik tehdidi oluşturur. Ayrıca üniversitelerin internet bant genişliğinin yüksek olması, saldırganları çeşitli amaçlar için bu ağı kullanmaya iter.

Teknoloji cihazlarının çoğalması ve maliyetteki düşüşle birlikte, çalışanlar ve öğrenciler kişisel kullanım için kendi gelişmiş bilgi işlem ve ağ cihazlarına sahip olabilirler. Bunlar dizüstü bilgisayarlar, tabletler, akıllı telefonlar ve e-okuyucular olabilir. Öğrencilerin ve akademik personelin kendi cihazlarını kullanması güvenlik kontrollerinin tam olarak uygulanmasını engeller.

Bireyler sadece veri uygulamalarına erişim için değil, aynı zamanda birbirleriyle iş birliği yapmak için de ağa bağlanmak ister. Bu kampüs dışından kişilerinde kampüs ağına bağlanması demektir. Bu serbestiyet siber saldırganların giriş noktasının binlerce olması anlamına gelir.

Güvenlik politikalarının, prosedürlerinin eksik olması, sorumlulukların dengeli paylaştırılmaması sıkıntıdır. Kullanıcılar hukuki yaptırımların kendilerini bağladığını çoğu zaman bilmezler. Siber güvenlik konularında bilinçsiz kullanıcı sayısı çok fazladır. Bilgi güvenliği bilinci, bir kuruluştaki kullanıcıların güvenlik görevlerinin farkında olduğu bir durum olarak tanımlanır [14]. Sonuçlar, kişilerin bilgi güvenliği ilkelerinin önemi ve günlük çalışmalarında pratik uygulamaları konusunda gerekli bilgi ve anlayışa sahip olmadıklarını ortaya koymaktadır [15]. Örneğin Malezya'da üniversite öğrencilerinin üçte birinin sosyal ağ sitelerindeki dolandırıcılıklardan etkilendiği tespit edilmiştir [16]. Yapılan araştırmalar yükseköğretimde okuyanların siber

farkındalık seviyelerinin düşük olduğunu göstermektedir. Siber farkındalığı olanların bile bu bilinci kullanmadığını gösteriyor. Bilgi güvenliğinin gereklerine uyum, anlaşılmasından veya farkındalığından daha düşüktür [17].

Bir kurumdaki minimum güvenlik düzeyini sağlayabilmek için, derinlemesine analizler yapmak, çözümler üretmek gerekir. Bir sistemi tam koruyabilmek için sistemin bütününe hâkim olmak gerekir. Birçok farklı sistemin olduğu üniversitelerde bunu gerçekleştirmek, bu sistemlerden sorumlu kişilerin siber konularda bilgi sahibi olmasını gerektirir. Sadece bilgi işlem personeli ile gerçekleştirilecek bir durum değildir.

3. TEHDİTLER (THREATS)

Bilgi sistemlerine karşı birçok farklı tehdit çeşidi sayılabilir. İç ve dış tehditler olarak sınıflandırılabilir. Saldırı yapacak dış tehditleri azaltma şansı çok olmayabilir. Bu yüzden iç tehditleri azaltmak için kurumsal politikalar ve önlemler güçlü olmalıdır.

3.1. Kötü Niyetli Yazılımlar (Malicious Software)

Bilgisayar virüsü bilgisayarınıza veya verilerinize zarar vermek amacıyla yazılmış program veya kod parçalarıdır. Sistem dosyalarını bozmak, kaynakları boşa harcamak, verileri silmek, veri çalmak, yetkisiz erişimlere izin vermek gibi zararları vardır. Bilgisayarlarda izinsiz ve yetkisiz birçok işlem yapabilirler. Dosyalara ve diğer bilgisayarlara kendilerini kopyalama yetenekleri vardır. Birçok çeşit virüs vardır. Truva atı (trojans), casus yazılım (spyware), solucan (worms), fidye yazılımı (ransomware) ve reklam (adware) amaçlı virüsler vb. şeklinde sınıflandırılırlar [18].

3.2. Siber korsanlar (Hackers)

Siber uzayda saldırı gerçekleştirmek isteyen kişilere siber korsanlar denir. Siber korsanlar niteliklerine ve amaçlarına göre Beyaz Şapkalılar, Siyah Şapkalılar ve Gri Şapkalılar olmak üzere üçe ayrılırlar. Beyaz şapkalı korsanların amacı zarar vermek değildir. Buldukları açıklıkları bildirerek, sistem ve yazılım sorumlularına destek olurlar. Bunlar iyi niyetli kişilerdir. Siyah şapkalı korsanlar ise güvenlik sistemlerini izinsiz olarak aşarak bilgi hırsızlığı, menfaat sağlama, dolandırıcılık, terörizm, bilinçli yıkım gibi zarar verici faaliyetlerde bulunurlar. Gri şapkalı korsanlar ise siyah şapkalı ve beyaz şapkalı arasında melezdir. Sistemin güvenliğini test etme iznine sahip olmasalar bile, herhangi bir sisteme sızabilir ancak sisteme zarar vermezler [19].

3.3. Bilinçsiz Kullanıcılar ve Ağ Kullanım Politikalarına Uyulmaması (Unconscious Users and Non-Compliance to Network Usage Policies)

Bilgisayar okuryazarlığı günümüzde gelişmiş olsa bile tam ve bilinçli bir seviyeye gelmemiştir. Kişiler ihtiyaçları kadar bilgiye sahip olmakla beraber, farklı durumlara çözümleri (tepkileri) çok iyi olmayabiliyor. Kullanıcıların bu eksiklilerini bilen bilgisayar korsanları oltalama, sosyal mühendislik vb. yöntemlerle bilgisayarlara ve kişinin hesaplarına sızmaktadırlar. Bilinçsiz (Dikkatsiz) kullanıcılar genellikle bir saldırganın verilere yanlışlıkla erişmesine izin veren veya kurumun siber güvenlik politikalarına dikkat etmeyen iyi niyetli kişilerdir. Birçok saldırının ortaya çıkmasının sebebi olarak görülmektedirler [20]. Çalışanlar ve öğrenciler bazen hesabını ve şifresini paylaşma veya cihazlarını gözetimsiz bırakma riskinin farkında değildir.

3.4. Ağ ve Sistem Zayıflıkları (Network and System Weaknesses)

Bir ağda yazılımların güncel olmaması, saldırı tespit sistemlerinin olmaması, ağ kurallarının doğru tanımlanmamış olması, yetki tanımlamalarının sağlıklı yapılmamış olması, ağ cihazlarının ayarlamalarının eksik yapılmış olması veya maddi imkansızlıklardan alınamayan eksik yazılım ve cihazlar sistem için zayıflıktır.

4. SALDIRI YÖNTEMLERİ (ATTACK TYPES)

Yaygın olarak kullanılan birkaç tehdit türü aşağıda açıklanmıştır. Saldırılar aktif ve pasif olarak sınıflandırılabilir. Pasif saldırılarda daha çok sistem hakkında bilgi edinilmeye çalışılır. Bilgi toplama sürecidir. Aktif saldırılarla sisteme sızmaya, zarar vermeye çalışılır. Yoğun aktif saldırılar aşağıda kısaca açıklanmıştır.

4.1. Oltalama (Phishing)

Kurbanların e-postalarına cezbedici sahte iletiler gönderilerek parola, kimlik bilgisi, kredi kartı ve banka hesap bilgileri gibi bilgilerin elde edilmesine çalışılır. Zararlı içerik barındıran bağlantılara tıklandığında virüslü dosyalarla hedefteki kişinin bilgisayarına sızılır, bilgileri çalınabilir. Sahte hazırlanmış web sitelerine yönlendirmelerle parolaları ele geçirilebilir [21]. Yükseköğretim kurumlarında ek olarak akademik personelin parolaları ile öğrenci otomasyonlarına giriş yapılarak öğrenci notları değiştirilebilir. Resmi yazışmalara ulaşılabilir. Yayınlanmamış akademik çalışmalar çalınabilir. Hedef bilinçsiz kullanıcılardır. Bu yüzden kullanıcıların bu tür konularda uyarılması, eğitilmesi gerekmektedir. Oltama ile en çok hedef alınan sistemler web, e-posta ve hizmet olarak yazılım (SaaS) yapılarıdır[22]. E-posta sistemlerinin bu tür iletileri engellemesi için önlemler alınmalıdır. Eğitim sektöründeki en büyük saldırı tipi oltalama saldırılarıdır [8].

4.2 Kimlik Sahteciliği (Spoofing)

Saldırgan, güvenilir bir kişiyi veya varlığı taklit eder. IP, ARP ve DNS sahteciliği olarak isimlendirilen türleri vardır. IP sahteciliğinde, saldırgan başkasının IP adresini kullanarak kendini gizler. Günümüzde daha çok DDOS saldırılarında kullanılır[23]. ARP (Adres Çözümleme Protokolü), veri iletimi için IP adreslerine karşılık gelen MAC adreslerini çözümlemek için kullanılır. Kötü niyetli taraflar genellikle bilgi çalmak, aktarılan verileri

değiştirmek veya LAN (Yerel Alan Ağı) üzerindeki trafiği durdurmak için ARP kimlik sahtekârlığını kullanır. Hizmet reddi, oturum ele geçirme ve ortadaki adam saldırıları da dahil olmak üzere diğer saldırı türlerini kolaylaştırmak için de kullanılabilir. Genelde yerel ağda bu tür saldırılar gerçekleştirilir. DNS (Etki Alanı Adı Sunucusu), etki alanı adlarını IP adresleriyle ilişkilendiren bir sistemdir. İnternete veya diğer özel ağlara bağlanan cihazlar, web adreslerini, e-posta adreslerini ve diğer okunabilir alan adlarını ilgili IP adreslerine yönlendirmek için DNS'e güvenir. Bir DNS sunucusu kimlik sahtekarlığı saldırısında, kötü niyetli bir taraf belirli bir etki alanı adını farklı bir IP adresine yeniden yönlendirmek için DNS sunucusu bilgilerini değiştirir. Çoğu durumda, yeni IP adresi aslında saldırgan tarafından kontrol edilen ve kötü amaçlı yazılım bulaşmış dosyalar içeren bir sunucu için olacaktır. DNS sunucusu kimlik sahtekarlığı saldırıları genellikle bilgisayar solucanlarını ve virüslerini yaymak veya sahte kopya sitelere yönlendirme yaparak kimlik, sistem giriş bilgilerini çalmak için kullanılır [24]. Ağda statik IP kullanılması, ARP kayıtlarının statik olarak eklenmesi tehditleri azaltır. DNS sunucularının güvenliğinin sağlanması gerekir.

4.3 Paket Çözümleme (Sniffing)

Bir ağ trafiğindeki paketler yakalanır ve içeriği okunmaya çalışılır. Şifreler ve gönderilen metin içerikleri elde edilmeye çalışılır. Ağdaki trafiğin şifreli olması bu tür saldırıların amacına ulaşmasını engeller[25]. Kurum ağındaki herhangi biri gerekli önlemler alınmazsa ağdaki şifresiz paketleri toplar. Gönderilen e-postalar, kullanılan şifreler gibi özel bilgileri ele geçirebilir. Şifreleme yapmayan ara yüzlerde bilgi girişi yapılırsa, ağ dinleniyorsa bilgiler ele geçirilir. Ağ anahtarlarında port güvenliğini sağlayacak ayarların aktif hale getirilmesi gerekir. Kampüs ağında farklı VLAN'lar (sanal ağlar) tanımlanmış olmalıdır. Misafir, öğrenci, akademik ve idari personelin VLAN'ları farklı olmalıdır. Sunucular DMZ (Arındırılmış Bölge) alanında olmalıdır. Sunuculara veya ağ cihazlarına bağlanırken SSH (Güvenlik Kabuğu) gibi şifreli bağlantılar kullanılmalıdır. İzinsiz ağa dâhil olmaların önüne geçilmesi gerekir. Kablosuz ağların şifresiz yayın yapması veya kırılabilir şifrelemelerin kullanılması engellenmelidir. İzinsiz dinlemelerin tespiti için geliştirilmiş yazılımlar kullanılmalıdır [26].

4.4 Ortadaki Adam (Man In The Middle)

İki bağlantı arasına sızılır. Bağlantı dinlenir ve şifrelenmemiş çeşitli türdeki veriler ele geçirilmeye çalışılır. Birbirleriyle doğrudan iletişim kurduğuna inanan iki taraf arasındaki iletişimi gizlice dinler ve muhtemelen değiştirir[27]. Saldırgan sahte bir yanıt gönderebilir, değiştirilmiş bir iletiyi iletebilir ve bilgileri başka amaçlarla değiştirebilir. Bu tür saldırılara karşı ağ güvenliğinin sağlanmış olması gerekir. Saldırı tespit sistemleri (IDS) kullanılmalıdır. Yapay zeka geliştikçe bu tür yazılımlar saldırıları önlemede çok daha yararlı olacaktır. Uçtan uca şifreleme kullanılmalıdır. Kötü amaçlı yazılımların bilgisayarlara yüklenmesini engellemek ve bilinçli kullanıcılar bu tür saldırıların amacına ulaşmasını engelleyecektir [28].

4.5 Kimlik Doğrulama (Authentication Hacking)

Kimlik doğrulama, web uygulamalarının güvenliğinde kritik bir rol oynar. Saldırgan, bilinen ve geçerli bir kullanıcı olduğunu kanıtlayarak sisteme girdiğinde, yönetici ayrıcalığına erişebilir. Oltalama, basit şifreler, sistem açıkları, sosyal ilişkiler vb. yöntemlerle şifrelerin ele geçirilmesidir. Sistemde istenmeyen durumların oluşmasına sebep olabilir [21]. Basit şifreler kaba kuvvet (brute force) atakları ile çözülebilir. Yetkili kullanıcı şifrelerinin çeşitli yöntemlerle ele geçirilmesi için ortam oluşturulmamalıdır.

4.6 DDOS Saldırısı (Distributed Denial of Service)

Servisleri çalışamaz duruma getiren bir yöntemdir. Bilgisayarlara bulaştırılmış kötü amaçlı yazılımlar kullanılarak hedefe kaldırabileceğinden fazla istekler göndererek, hizmet durma noktasına getirilir [29]. DDOS saldırılarına çeşitli çözümler üretilse de tam anlamıyla korunma yöntemleri yoktur. Uluslararası bilgisayar korsanlarının hedefi haline gelecek durumlardan uzak durmak gerekir. Sınav döneminde veya başvuru dönemlerinde sistemler hizmet veremez duruma getirildiğinde itibar kaybı, iş ve işlemlerde gecikmelere neden olunur.

4.7 Enjeksiyon (Injection)

Web gibi dış dünyaya açık uygulamalar, dış kullanıcılara güvenlik önlemlerini kırmak, sistemlerin açıklarını tespit ve istismar için ortam sunmaktadır. Ayrıca bu sistemler optimize çalışmak için çeşitli servisler ve uygulamalarla ile veri alışverişinde bulunurlar. Bunu yaparken de yetkilendirme kullanırlar. Bu sunuculardan biri ele geçirildiğinde diğer sistemlerde risk altına girer [24]. Enjeksiyon saldırıları, kullanıcı adı ve parola bilmeden bir uygulamada oturum açmak, aynı zamanda özel, gizli veya hassas bilgileri ortaya çıkarmak veya hatta tüm sunucuyu ele geçirmek için kullanılabilir. Bu saldırılar yalnızca web uygulamaları için değil, verileri bu uygulamalarda ve diğer bağlı uygulama ve hizmetlerde bulunan kullanıcılar için de bir tehdittir. Birçok türü vardır. En çok kullanılanlar aşağıda açıklanmıştır.

Kod enjeksiyonu, en yaygın enjeksiyon saldırı türlerinden biridir. Saldırgan bir web uygulaması tarafından kullanılan programlama dilini, çerçeveyi, veri tabanını veya işletim sistemini biliyorsa, web sunucusunu istediklerini yapmaya zorlamak için metin giriş alanları aracılığıyla kod enjekte edebilir. Bir metin giriş alanı, kullanıcıların istediklerini girmesine izin veriyorsa, uygulama potansiyel olarak kullanılabilir. Bu saldırıları önlemek için, uygulamanın kullanıcıların veri girişlerini kısıtlaması gerekir. Girilecek veri miktarını sınırlamalı, kabul etmeden önce veri biçimini kontrol etmeli ve izin verilen karakter kümesini kısıtlamalıdır. SQL enjeksiyonu, saldırı için SQL komut

dosyasını bir metin giriş alanına ekler. Komut dosyası, doğrudan veri tabanını yürüten uygulamaya gönderilir. Sonuç olarak, saldırgan giriş ekranından geçip hassas verileri doğrudan veri tabanından okumak, veri tabanı verilerini değiştirmek, yok etmek veya veri tabanında yönetici işlemleri yürütmek gibi daha tehlikeli şeyler yapabilir. Komut enjeksiyonu türü ise saldırganın programlama kodu veya komut dosyası yerine sistem komutları eklemesi yoluyla sisteme sızmasıdır. Siteler Arası Betik Çalıştırma (Cross-site scripting, XSS), güvenlik açığı bulunan bir web sitesini kullanıcılara kötü amaçlı betik döndürmesi için işleyerek çalışır [30][31]. XSS, web sayfalarına istemci taraflı kodun enjekte edilmesine imkân sağlar. Web sayfası kullanıcıdan aldığı girdileri gerekli html ve script filtrelerinden geçirmediği zaman oluşan bir zafiyettir.

5. ÖNLEMLER (PREVENTIONS)

Siber güvenlik; yönetimsel, teknik ve sosyolojik olarak bütün paydaşların içinde olduğu bir yapıyı gerektirir. Başarı için bütünlüğün sağlanması gerekir. Bilgi varlıklarının farkında olunmalıdır. Yöneticiler ve bilgi işlem birimleri bu konuya özel hassasiyet göstermelidir. Sürekliliği olan ve risklere karşı önlem alınmış yapılar oluşturulmalıdır. Teknolojik sistemlerini modernize etmelidir. Şekil 2'deki temel unsurların sağlanması için gerekli düzenlemeleri yerine getirmelidir. Güvenliğin temel prensipleri gizlilik, bütünlük ve erişilebilirliktir [32].

Bilgilerin korunması, siber tehditlere karşı savunma sisteminin oluşturulması bilgi işlem birimleri için temel bir görev haline gelmelidir. Teknoloji ve standartlardaki dinamik değişim sebebi ile siber tehditlerle ilgili en son gelişmelerden haberdar olmak ağı korumak, çeşitli önlemler almak için gereklidir. Siber güvenlik uzmanları ve bir plan olmadan veri ihlali riskleri azaltılamaz. Bu yüzden bir işi en iyi, sadece işi bu olanlar yapabilir. Teknik personellere bu konularda sürekli eğitim aldırılmalıdır. Bu konularda tecrübeli ve eğitimli insan kaynağının oluşturulması kaçınılmazdır. Saldırıyı önlemek için saldırı yapanları da tanımak ve kullanabilecekleri yöntemleri bilmek gerekir.

Siber savunma için teknik altyapılar güçlü olmalıdır. Altyapıların güçlendirilmesi için risk analizlerinin yapılması ve önceliklerin belirlenmesi gerekir. Bazı altyapılarda tasarrufa gidilmesi büyük sorunlar çıkarabilir. Belli bütçelerin altyapılara ayrılması kaçınılmazdır. Güncel güvenlik yazılımları kullanılmalıdır. Güvenlik duvarları, uçtan uca şifreleme, iki adımlı kimlik doğrulama ve akıllı denetim, benimsenmesi gereken adımlar olmalıdır. Donanım ve yazılımların güncel ve günümüze uygun olması gerekir. Güncel anti virüs yazılımları son kullanıcı bilgisayarlarında kurulu olmalıdır. İş sürekliliğinin sağlanması için yedekli yapılar oluşturulmalıdır. Verilerin farklı lokasyonlarda yedekleri mutlaka tutulmalıdır.

Kampüs ağındaki fiziksel cihazlara, ağ altyapılarına erişim konusunda tedbirler alınmalı, kişilerin bilgiye erişimi konusunda sınırlandırmalara gidilmelidir Güvenlik riskleri belirlenmeli, buna göre düzenlemeler yapılmalıdır. İş tanımına göre erişimler, yetkilendirmeler yapılmalı, sorumluluklar verilmelidir. Kişilerin yetkisi olmayan bilgilere erişimi engellenmelidir. Kimin hangi bilgiye veya servise ulaşabileceği tanımlanmalı ve bilinmelidir. Yetkisiz erişimler engellenebilmeli, ağ ve sistem üzerinde oluşan her türlü olayın kaydı tutulabilmelidir. Siber olaylara neden olanlar tespit edilebilmeli, inkâr edemeyecekleri kanıtlar sunulabilmelidir

Sorumlular koruyacağı verilerden haberdar olmalıdır. Siber ekipler haberdar olmadığı verileri güvence altına almak için önlemler alamaz. Araştırmacılar ve siber güvenlik ekipleri arasındaki iletişim, kurumdaki son derece hassas araştırmalar için planlama sürecinin bir parçası olmalıdır.

Şekil 2. Bilgi güvenliği unsurları
(Information security facts)

Üniversitelerde bilgi sistemlerinden yararlanan kişiler risk seviyesine göre sınıflandırılmalıdır. Birim bazında kullanıcılar daha detaylı sınıflandırılmalıdır. Üst yöneticiler bu bireylerin farkında olmalı, iş ve işlemleri buna göre düzenlemelidirler. Bilgi güvenliği farkındalığı konusunda hiyerarşik bir sistem oluşturulmalı üst yönetimden başlayarak kilit kişiler belirlenmeli, bütün bireylere ulaşacak, bu farkındalığı iletecek mekanizma oluşturulmalıdır. Şekil 3'te belirtilen hiyerarşi buna uygun olabilir. Üst yönetimdekiler görevlendirme vasıtasıyla bilgi güvenliği ile ilgili görevlerini daha yetkin kişilere devredebilirler. Bilgi güvenliği bilinci bütün dış paydaşlara bilgi işlem birimi vasıtasıyla verilebilir.

Üniversite öğrencilerinin çoğu interneti kullanırken takip edildiklerine ve verilerinin üniversite sistemlerinde bile güvende olmadığına inanırlar, buna rağmen verilerini nasıl koruyacaklarının pek farkında değillerdir. Bilgi güvenliği bilgisine uyum, onu anlamaktan veya farkında olmaktan çok daha düşüktür. Üniversitelerin, potansiyel siber saldırılardan öğrencilerini nasıl koruyacaklarına ve eğiteceklerine dair aktif bir yaklaşımlarının olmadığı görülmektedir [33]. Öğrencilerin güvenlik kavramlarını çeşitli kaynaklardan parça parça öğrendikleri görülmektedir [34]. Bütün personel ve öğrencilerin siber

konularda eğitilmesi günümüzde zorunluluktur. Tablo 2'de bilgi sistemleri kullanıcıları bilinç, uygulama, katkı zarar durumuna göre sınıflandırılmıştır. Sorumluluk bilinci zayıf kişiler genelde kendilerine zararı dokunmayan konularda çok dikkatli davranmazlar.

Tablo 2. Bilgi sistemleri kullanıcıları analizi (Information systems users analysis)

Farkındalık seviyesine göre kullanıcılar				
Seviye	Bilinç	Uygulama	Katkı	Zarar
Yüksek	+	+	+	-
Orta	+	-	-	+
Zayıf	-	-	-	+
İç tehdit oluşturacak üniversite içi saldırgan kullanıcılar				
Seviye	Bilinç	Uygulama	Katkı	Zarar
Siyah Şapkalı	+	-	-	+
Beyaz Şapkalı	+	+	+	-
Gri Şapkalı	+	-/+	-/+	-/+

Kullanıcıların güçlü şifreler oluşturmaları sağlanmalıdır. Sistem kullanıcıları e-posta şifrelerini düzenli değiştirmeli, ataklardan nasıl kaçınacaklarını bilmelidir. Ağa dahil olurken kimlik denetimi sağlanmalıdır. Sistemlere kimlik kontrollü erişimler sağlanmalıdır.

Üniversite web sayfalarında çalışanların kişisel bilgilerinin ve e-posta adreslerinin paylaşımı mümkün oldukça yapılmamalıdır. Risk oluşturacak bilgiler web sayfalarında paylaşılmamalıdır. Kullanıcılar şüphe duydukları gelen e-postaları Bilgi İşlem birimine bildirerek, destek almalıdır.

Kampüs içinde rasgele veri paylaşımı yapılmamalı, belli bir plan ve yetki gerektirmelidir. Bazı hizmet alıcılarını rahatsız etse de kısıtlamalardan taviz verilmemelidir. Zayıf bir halkanın oluşması bütün önlemleri boşa çıkarabilir. Tüm risk altındaki sistemlerini merkezi kontrol altında tutmalıdır.

Kablosuz ağların kampüslerde kullanımı günümüzde kaçınılmazdır. Bu yüzden kullanılan bu yapıların standartlara uygun olması gerekir. Yayın şekli nedeniyle, kablosuz ağlar yetkili veya yetkisiz bütün kullanıcılar tarafından erişilebilirdir. Açık iletişim ortamı yüzünden kötü niyetli saldırılara karşı daha savunmasızdır [35]. Kablosuz ağların kullanımı merkezileştirilmeli, kişisel kablosuz ağ cihazlarının kullanımları engellenmeli veya izne tabi tutulmalıdır. Şifreleme algoritmalarının güçlü olmasına dikkat edilmelidir. Kablosuz ağ mevcut kimlik doğrulama sistemine entegre edilmelidir.

Hangi verinin hangi cihazlarca ulaşılır olabileceği tanımlanmalı ve gizli bilginin istenmeyen yerlerde (cihazlarda) seyahat etmesi engellenmelidir [10]. Sanal özel ağlara (VLAN) bölünen yapıların erişim sınırlandırılmaları şartlara göre güncellenmelidir. VPN servisleri kullanımları kontrol altında tutulmalıdır. DMZ dışında sunucu tutulmamalıdır. Sunucular üzerindeki açık portlar takip edilmeli, kullanılmayan portlar kapatılmalıdır. İç kullanıcıların ağ ve port taraması yapması engellenmelidir. Güvenlik duvarının izni dışında kaçak akışların olmamasına dikkat edilmelidir.

Ağ görüntüleme ve güvenlik yazılımları sürekli izlenmeli, etkin kullanılmalı, anormal durumlara hemen müdahale edilmelidir. Bu sistemleri yönetenler güncel eğitimler almalıdır. Virüs bulaşmış bilgisayarlar otomatik karantinaya alınmalı, ağa bağlantısı engellenmelidir. Hangi kullanıcının hangi cihaz ve portu kullandığının bilinmesi güvenlik tedbirlerine destek olacaktır[36].

Öğrencilerin teknoloji kullanım alanları kontrol altında tutulmalıdır [26]. Ağ ve bilgi sistemleri kullanım kuralları öğrenciler için daha da sıkılaştırılmalıdır.

Birimler çalıştığı firmaların güvenli ve profesyonel olmalarına dikkat etmelidir. Belli standartları yakalamamış firmalarla çalışılmamalıdır. Firmaların güvenlik politikalarının olmasına dikkat edilmelidir. Güvence istenmeli ve güvencelerin doğruluğunun tespiti için güvenlik ihlalleri veya veri sızıntısı kanıtları için ağ sürekli izlenmelidir.

Bilgi güvenliği yönetim sisteminin gerçekleştirilmesi güvenli bir yapı için gereklidir. Bu şekilde riskler minimize edilir, iş sürekliliği sağlanır, yasal kriterler sağlanmış olur. Kurumsal güven ve saygınlık sağlanmış olur.

Siber suçlarla mücadele edilmesi için hukuki ve mevzuat düzenlemelerinin sürekli güncellenmesi gerekir. Dinamik bir eylem planının oluşturulması kaçınılmazdır. Kampüs ağ kullanım politikalarının oluşturulmaması büyük sıkıntıdır. Üniversitelerin gerçek anlamda siber tehditlerden korunması ancak doğru politikaların uygulanması ile olur. Bu politikalarda kullanıcıların ağ, internet ve bilgisayar kullanımdaki hakları, uyması gereken kurallar ve sorumlulukları belirtilir. Kullanıcıların bu kurallara uyması beklenir. Siber tehditlere karşı en büyük sorunlardan biri kullanıcıların tanımlanan kuralları bilmemesi veya bildiği halde uymamasıdır. Siber tehditlere karşı bütünlüğün ve gizliliğin sağlanması ancak bu politikalara uyulması ile mümkün olabilir. Kurum içinden oluşacak tehditlerden korunmak için güvenlik gereksinimleri göz önüne alınarak mutlaka Bilgi Güvenliği Politikalarının oluşturulması ve buna uyulması kaçınılmazdır [32]. Çeşitli rehber ve çerçeve dokümanlarının hazırlanması gerekmektedir. Tüm tarafların görev, sorumluluk ve yasal dayanaklarının belirlenip, kişilere iletilmesi gerekmektedir. Kullanıcılar sebep oldukları sıkıntılı durumlarda ceza alacaklarını, yaptırım ile karşılaşacaklarını bilseler daha dikkatli hareket edeceklerdir.

Düzenli sızma testleri yapılmalı ve yaptırılmalıdır. Kurum tarafından geliştirilen veya satın alınan yazılım ve uygulamalar siber uygunluk testlerinden geçirilmelidir.

Öğrenci otomasyonu, elektronik belge yönetim sistemi vb. yazılım hizmetleri firmalar üzerinden yapılıyorsa bu firmaların ürünlerini düzenli olarak sızma testlerinden geçirip geçirmedikleri kontrol edilmelidir. Ağın tümü içten ve dıştan sızma açıklıklarına karşı düzenli taranmalıdır. Bu tür görevler için üniversitenin siber ekibinin olması gerekir. Sızma testlerini bu ekip yapabilir. Bazı dönemlerde yapılan testlerin uygunluğunun karşılaştırılması için firmalara da testler yaptırılmalıdır. Raporlar tutularak mevcut durum analiz edilmelidir.

İletişim bir güvenlik ihlali sonrasında çok önemlidir. Etkilenen kişilerin kimlerle irtibata geçeceğini, hangi talimatları uygulayacağını bilmesi gerekir. Ayrıca zafiyetler tespit edildikten sonra gerekli önlemler alınmalı, ulaşılabilecek diğer birimlerde bu konu hakkında bilgilendirilmelidir.

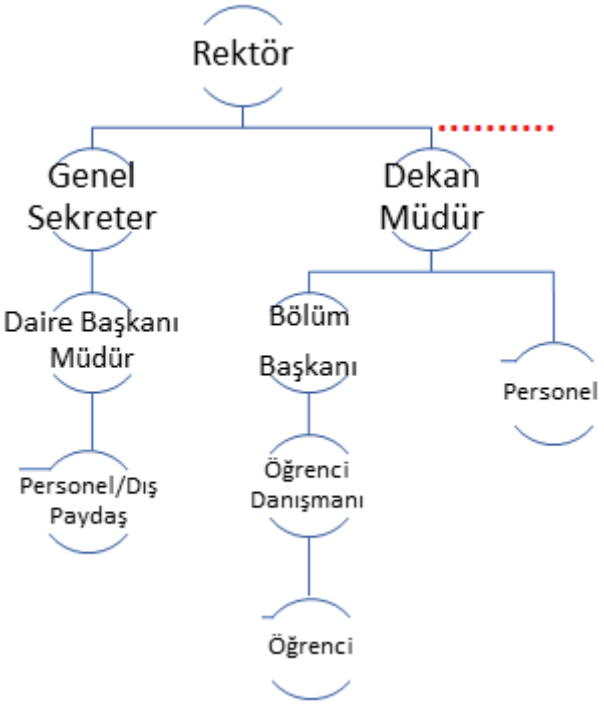
Üniversitelerin siber saldırı sonrası için de planlamalarının olması gerekir. Üniversiteyi kötü algılardan koruyacak, en az zararla durumu kurtaracak çalışmalar mutlaka yapılmalıdır.

6. SİBER FARKINDALIK EĞİTİMİ (CYBER SECURITY AWARENESS TRAINING)

Üniversiteler her türlü eğitim konusunda iyi olmalıdır. Personel ve öğrenciler bu eğitim olanaklarından, konularında uzman akademik personelden faydalanabilmelidir. Siber farkındalık eğitimleri bilgi teknoloji kullanıcıları tarafından mutlaka alınması gereken eğitimlerdendir. Kullanıcılar siber konularda eğitimli değil ise veya önlemlerini almıyorsa sosyal mühendislik vb. yöntemler ile bilgileri çalınabilir. Kullandığı cihazlar virüs barındırabilir, saldırganlara hizmet ediyor olabilir. Teknik olarak gerekli güvenlik standartları yerine getirilse bile bilinçsiz kullanıcılar varsa riskler devam ediyordur.

Üniversitelerden hizmet alan kişilerin sayısının çokluğu, siber farkındalık eğitimlerini herkese ulaştırmada sıkıntı yaratmaktadır. Bilgi güvenliği politikalarına uyum konusunda zorluklara sebep olmaktadır. Bu yüzden hiyerarşik bir yapı kullanılarak bütün insan kaynaklarına ulaşılmalıdır. Siber farkındalık eğitimi zorunlu hale getirilmelidir. Üniversite personeli ve öğrenciler bu sayede kurum adına kullandığı bilgi sistemlerinin ve verilerin güvenliğini sağlayacak, öğrenciler iş hayatına geçişte bu bilgileri kullanmaya devam edecektir.

Öğrenciler için ilk yıl bilgi güvenliği ile ilgili bir dersin müfredata alınması iş hayatına hazırlama ve siber güvenlik farkındalığı oluşturma açısından iyi olacaktır. Hiyerarşik yapı göz önünde tutularak eğitimler ve farkındalık programları ile zincire dahil bütün kullanıcılar bilinçlendirilmelidir. Eğitimlerin kişiye ve yaptığı göreve uygun verilmesi çok daha iyi olacaktır. Bildiğini uygulayan, durumun ciddiyetini anlayacak seviyede farkındalık oluşturulmalıdır. Düzenli toplantılarla eksik görülen kısımlarda eğitimler personele ve içeriğe göre detaylandırılmalıdır.



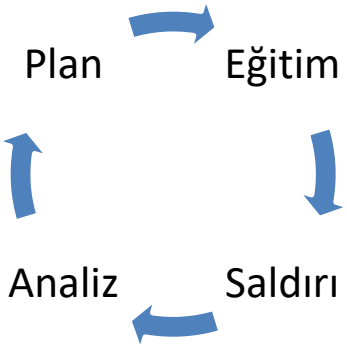
Şekil 3. Siber güvenlik farkındalık eğitimi takip hiyerarşisi
(Cyber security awareness training following hierarchy)

Eğitimin müfredata ders olarak eklenme imkanı yoksa, üniversitelerin uzaktan eğitim sistemlerine bu eğitimler yüklenebilir. Eğitim için ders kaynakları ve videolar hazırlanabilir. Öğrencilerin bu eğitimi zorunlu alması sağlanabilir. Öğrenci danışmanları tarafından eğitimlerin tamamlanıp tamamlanmadığı takip edilebilir. Akademik ve idari personellerde bu eğitimi almalıdır. Takibini de birim amirleri yapmalıdır. Eğitimler uzun vadeli olarak planlanmalıdır. Eğitim sürecinden sonra geri dönüşüm anketleri ile oluşan farkındalık ölçülmelidir. Ayrıca Şekil 4'te olduğu gibi eğitim almış kullanıcılara aldatıcı saldırılar düzenleyip, sonuçlar analiz edilmelidir. Eksiklikler tespit edilip, eğitim içeriklerinde sürekli iyileştirmeler yapılmalıdır [37].

Eğitim konuları riskleri anlamaya ve önlem almaya yardımcı olmalıdır. Saldırı türleri ve yoğunluğu konuları belirlemede önemlidir. Üniversitelerdeki bilgi güvenliği varlıkları dikkate alınmalıdır. Her bir konuda gerçek hayattan saldırı örneklerinden bahsedilmelidir. Savunma yapabilmek için saldırı detaylarını bilmek gerekir [38].

Bütün kullanıcılara verilmesi gereken eğitimler

1.Şifre Güvenliği Eğitimi
2.Güvenli İnternet Kullanma Eğitimi
3.E-Posta Güvenliği Eğitimi
4.Sosyal Mühendislik Eğitimi
5.Mobil Cihaz Güvenliği Eğitimi
6.Siber Tehdit Türleri Eğitimi
7.Kişisel Veri Gizliliği Eğitimi
8.Üniversite Uygulamaları Tanıtımı Eğitimi
9.Sorumluluklar ve Hukuki Süreçler Eğitimi



Şekil 4. Eğitim sonuçlarının analizi
(Analysing training results)

Bilgi işlem personeline verilmesi gereken eğitimler

1.Sızma Testi Eğitimi
2.Ağ Güvenliği Eğitimi
3.Sistem Güvenliği Eğitimi
4.Yazılım Güvenliği Eğitimi
5.IOT Cihazları Eğitimi
6.Fiziksel Sistemlerin Güvenliği Eğitimi
7.Bilgi Güvenliği Yönetim Sistemi Eğitimi
8.Risk Analizi Eğitimi

Ayrıca görev alanına ve risk seviyesine göre tanımlanmış özel eğitimlerde tanımlanabilir. Kilit konumdaki kişiler özel olarak eğitilebilir.

7. SONUÇLAR (CONCLUSIONS)

Üniversiteler diğer sektörlerde görülmeyen benzersiz güvenlik sorunları ile karşı karşıyadırlar. Güvenlik, dayanıklılık ve iş sürekliliği planları hazırlarken hepimizin göz önünde bulundurması gereken etkenlerden biri siber risklerdir. Siber tehditlerin üniversiteler ve eğitim kurumları için kritik bir risk taşıdığı açıktır, bu nedenle yöneticilerin bunun önemini kavraması, gerekli önlemleri alması hayati önem taşımaktadır. Bilgi işlem birimleri bu potansiyel risk alanlarıyla yüzleşmeli ve siber tehditleri azaltmanın yollarını bulmalıdır. Dürüst ve ayrıntılı değerlendirmeler yapılabilmelidir. Kampüs ağını ve sistemlerini kullanan kişiler sistemin en zayıf halkasıdır, bu yüzden eğitilmeli ve farkındalık oluşturulmalıdır. Riskler analiz edilmeli ve bir bütün olarak çözümler uygulanmalıdır. Ağ güvenliğinde ortam, ağ araçları ve gereksinimler dikkate alınmalıdır. Üniversitelerin mali kaynakları sınırlı olduğundan, risk analizlerine göre, tehditlerin oluşturabileceği etkiye göre planlamalar yapılmalı, altyapılar güçlendirilmelidir. Güvenlik politikalarından taviz verilmemelidir. Kullanıcıların ağdan beklediği hizmet kalitesine izin verirken, verileri güvence altına alabilmelidir. Siber tehdit öncesi ve sonrası için bütün planlama ve düzenlemelerin yapılması gerekmektedir.

Bu çalışmada konunun önemi, tehditlerin neler olduğu, zayıflıklar ele alındı. Bu zayıflıklara karşı ne tür önlemlerin alınabileceği konusu üzerinde duruldu. Siber güvenlik ancak bütün boyutlarıyla ele alındığında bir sistemde, ağda güvenlik sağlanabilir. En zayıf halka insan faktörüdür. Bundan dolayı bu çalışmada siber farkındalık eğitimi üzerinde duruldu, öneriler sunuldu. Siber bilincin dinamik bir süreç olduğu, bu dinamik sürece uygun eğitim modelinin seçilmesi gerektiği gösterildi.

Üniversitelerin öncülüğünde siber farkındalığın bütün sektörlerde oluşması için destekleyici çalışmalar yapılmalıdır. Üniversiteler araştırma geliştirme merkezleri olduğu için güvenli yapıları oluştururken edindiği tecrübe ve birikimleri diğer sektörlerle de paylaşmalıdır. Siber farkındalığın oluşması için eğitimler düzenlemeli, sektörlerin güvenliğine katkı sunmalıdır.

KAYNAKLAR (REFERENCES)

[1] F. H. Katz, “The Effect of a University Information Security Survey on Instruction Methods in Information Security”, **Annual Conference on Information Security Curriculum Development - InfoSecCD ’05**, 43-48, 2005.

[2] **National Cybersecurity Strategy Guide**, ITU, 2011.

[3] L. Coleman, B. M. Purcell, "Data Breaches in Higher Education", *J. Bus. Cases Appl.*, 15(15), 1-7, 2015.

[4] **The State of Cyber Security Across UK Universities**, Redscan, 2020.

[5] B. Kerievsky, “Security and Confidentiality in a University Computer Network”, *ACM SIGUCCS Newsl*., 6(3), 9–11, 1976.

[6] NCSC, **The Cyber Threat to Universities**, UK National Cyber Security Centre, 2019.

[7] OAIC, **Notifiable Data Breaches Scheme 12-month Insights Repor**t, Australian Information Commissioner, 2019.

[8] IBM Security, **IBM X-Force Threat Intelligence Index 2020**, IBM, 2020.

[9] Ulakbim, **12.ULAKNET Çalıştayı Sunu**, Tübitak, 2018.

[10] L. Kumari, S. Debbarma, and R. Shyam, “Security Problems in Campus Network and Its Solutions”, *International Journal of Advanced Engineering & Application*, 1(1), 98–101, 2011.

[11] C. McGuffin, P. Mitchell, "On Domains: Cyber and The Practice of Warfare", *Int. J. Canada’s J. Glob. Policy Anal*., 69(3), 394–412, 2014.

[12] Internet:University of Insecurity, https://flylib.com/books/en/2.145.1/university_of_insecurity.html, 28.02.2021.

[13] Y. Rezgui, A. Marks, “Information Security Awareness in Higher Education: An Exploratory Study”, *Computers and Security*, 27(7), 241–253, 2008

[14] M. T. Siponen, “A Conceptual Foundation for Organizational Information Security Awareness”, *Information Management & Computer Security*, 8(1), 31–41, 2000.

[15] S. Al-Janabi, I. Al-Shourbaji, “A Study of Cyber Security Awareness in Educational Environment in the Middle East”, *Journal of Information & Knowledge Management*, 15(1), 2016.

[16] G. H. Kirwan, C. Fullwood, and B. Rooney, "Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students", *Cyberpsychology, Behavior and Social Networking*, 21(2), 123–128, 2018.

[17] L. Slusky and P. Partow-Navid, "Students Information Security Practices and Awareness", *Journal of Information Privacy and Security*, 8(4), 3–26, 2012.

[18] I. Khan, "An introduction to computer viruses: Problems and solutions", *Libr. Hi Tech News*, 7, 2012.

[19] Internet: R. Siciliano, Seven Types of Hacker Motivations, https://www.mcafee.com/blogs/consumer/family-safety/7-types-of-hacker-motivations/, 11.05.2020.

[20] M. Nkhoma, D. Dang Pham Thien, T. Le Hoai, C. Nkhoma, "Information Security Landscape in Vietnam: Insights from Two Research Surveys", **Cyber Criminology. Advanced Sciences and Technologies for Security Applications,** Editör: Jahankhani H.**,** Springer, Cham, 341–357, 2018.

[21] B. B. Gupta, A. Tewari, A. K. Jain, D. P. Agrawal, "Fighting Against Phishing Attacks: State of the Art and Future Challenges", *Neural Computing and Applications*, 28, 3629–3654, 2017.

[22] APWG, **Phishing Activity Trends Report,** Anti Phishing Work Group, 2020.

[23] P. Ramesh, D. L. Bhaskari, CH. Satyanarayana, "A Comprehensive Analysis of Spoofing", *International Journal of Advanced Computer Science and Applications*, 1(6), 157-162, 2010.

[24] D. Gollmann, "Securing Web applications", *Information Security Techical Report*, 13(1), 2008.

[25] P. Anu, S. Vimala, "A Survey on Sniffing Attacks on Computer Networks", **International Conference on Intelligent Computing and Control (I2C2 2017)**, Coimbatore, 1-5, 2017.

[26] C. Wu, "The problems in campus network information security and its solutions," **2nd International Conference on Industrial and Information Systems,** 2010.

[27] M. Conti, N. Dragoni, V. Lesyk, "A Survey of Man in the Middle Attacks", *IEEE Communications Surveys and Tutorials*, 18(3), 2027-2051, 2016.

[28] Internet: J. DeCleene, 3 Ways to Protect Against Man-In-The-Middle Attacks, https://medium.com/datadriveninvestor/3-ways-to-protect-against-man-in-the-middle-attacks-cbd35f3200a7, 30.05.2020.

[29] J. Mirkovic, P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", *Computer Communications Review*, 34(2), 39-54, 2004.

[30] Internet: geekflare.com Editorial, 9 Popular Web Application Injection Attack Types, https://geekflare.com/web-application-injection-attacks/, 06.05.2020.

[31] S. Lalia, A. Sarah, "XSS Attack Detection Approach Based on Scripts Features Analysis", *Advances in Intelligent Systems and Computing*, 197–207, 2018.

[32] Ö. Can, M. F. Akbaş, "Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması", *Türk Bilim Araştırma Vakfı Bilim Dergisi*, 7(2), 16-31, 2014.

[33] A. Moallem, "Cyber Security Awareness Among College Students", **International Conference on Applied Human Factors and Ergonomics (AHFE 2018)**, 79–87, 2018.

[34] E. B. Kim, "Recommendations for information security awareness training for college students", *Information Management and Computer Security*, 22(1), 115-126, 2014.

[35] Y. Zou, J. Zhu, X. Wang, L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends" , **Proceedings of the IEEE 104.9,** 1727–1765, 2016.

[36] A. El Bekkali, M. Boulmalf, M. Essaaidi, G. Mezzour, "Securing the Internet of Things (IoT)", *IGI Global*, 2019.

[37] Internet: Updating Your Awareness Training, https://www.sans.org/security-awareness-training/blog/updating-your-awareness-training, 28.02.2021.

[38] M. Yüksel, N. Öztürk, "SIP Saldırıları ve Güvenlik Yöntemleri", *Bilişim Teknolojileri Dergisi*, 10(3), 301-310, 2017.