

Editörden

21. Yüzyılda Siber Güvenlik

21. yüzyılda hızla gerçekleşen değişimi yakalamak ve değişime adapte olmak biz bireyler için daha önce alışmadığımız yeni bir süreçtir. Bu değişimlerin en başında da bilişim dünyası gelmektedir. Bilişim teknolojilerinin hızla gelişmesi ile hayatımızda gerçekleşen köklü değişimler interneti ve teknolojik cihazları hayatlarımızın vazgeçilmez parçası haline getirmiştir. Dijital platforma yüklenmiş her bilgiye her yerden erişim sağlanması ve insanlar arasındaki tüm coğrafi sınırları kaldırarak dünya iletişimini kurması gibi etkileriyle dijital platformların insan hayatını kolaylaştıran ve özgürlük tanıyan olumlu etkileri olmuştur.

Tüm bu pozitif yanlarının yanı sıra ise oluşabilecek güvenlik açıkları ve sorunları da kimi zaman insanlara zorlu anlar yaşatabilmektedir. Bir durumun ya da bir buluşun sonuçları insanın elinde var olanı nasıl kullandığına bağlıdır. İnternet, bilgisayar, teknoloji gibi insanlığa çok fazla faydası olan buluşlar bile art

niyetli insanların elinde çok ciddi sorunlara yol açabilmektedir. Bu sorunlar kimi zaman bireyleri etkilerken kimi zaman da bir bireyin ihmalkârlığı nedeniyle büyük sistemleri de etkileyebilmektedir. Her geçen gün bilişim dünyasına yeni bir cihazın, yeni bir kullanıcının girmesi ve sayılarının artması ortada olan güvenlik sorununu daha ciddi boyutlara taşımaktadır. Yeni çağa adapte olmak için bilişim dünyasına hâkim olmak, bu konu hakkında makaleler okumak ve eğitimlere katılım sağlamak, birey olarak kendimizi bilinçlendirmek için başlıca yapabileceklerimiz arasındadır. Daha küçük yaşlardan itibaren yeni çağın çocukları olarak da görebileceğimiz gençlerimizi ve çocuklarımızı doğru bir şekilde bu alana yönlendirebilirsek siber güvenlik alanında önemli ilerlemeler kaydetmemiz mümkün olacaktır. Şu an günümüzde bile birçok siber saldırı yöntemi ve bu yöntem yüzünden mağdur olan birçok insan olduğu düşünülürse, gelecekte bilinçli nesillerimize daha güvenilir ve iyi bir dünya için ihtiyacımızın olacağı kaçınılmazdır.

P-Wise Bülteninin bu sayısında "21.Yüzyılda Siber Güvenlik" konusunu ele alarak siber güvenliğin ne demek olduğunu, tam olarak neyi kapsadığını öğrenmeyi, bu alanda nasıl bilinçlenebileceğimize ve nasıl önlemler alabileceğimize değinmeyi hedefledik.

Okyanus Kolejleri olarak sizlerin de destekleriyle sürekli değişen ve gelişen dünyada öğrencilerimizi daha iyiye taşıyabilmek için çalışmaktayız. Yarınlarımız için bilişim yetenekleri yüksek, donanımlı, duyarlı, araştıran, bilinçli, geleceğe ışıkla bakan bireylerin olması dileğiyle...

YASEMİN ŞENOCAC

Okyanus Kolejleri

Din Kültürü ve Ahlak Bilgisi Bölüm Başkanı



Siber Güvenlik Nedir?

Siber güvenlik nedir sorusunu; bilişim sistemlerinde insanlarla veya kurumlar arası kurduğumuz iletişimin, yaşamın, entegrasyonun, maddi veya manevi varlıklarımızın hatta elektronik ortamdaki verilerimizin güvenliğinin, bütünlüğünün ve gizliliğinin korunması şeklinde tanımlayabiliriz.



Günümüz teknoloji çağında, hayatımızın büyük bir kısmını elektronik ortamlarda yansıtmaya ve yaşamaya başlamış durumdayız. Yalnızca biz bireyler değil! Devletler, kamu kurumları, sosyal platformlar, kobiler, irili ufaklı tüm özel şirketler de biz tüketicilere veya diğer şirket ve kurumlara sunmuş oldukları hizmet ve ürünler ile iletişimlerini sanal ortamlar üzerinden gerçekleştirmeye başladılar.

Sanal alem, siber alem gibi kavramlarla anlattığımız bu dünya üzerinde artık sanal ve gerçek mal varlıklarımızla üretmiş olduğumuz verilerle ve yaşantımızla yer alıyor. Diğer insanlarla kurduğumuz iletişiminin büyük bir kısmını elektronik ortamlarda gerçekleştiriyoruz. Bahsetmiş olduğumuz tüm bu sanal yaşam içerisinde siber saldırganlara karşı kendimizi ve kurumlarımızı korumak zorundayız. Bu noktada karşımıza "Siber Güvenlik" tanımı çıkıyor.

Siber kelimesi ise altyapısı bilişim sistemleri olan ağlara verilen addır. Genelde sanal gerçeklik şeklinde de tanımlanabilir. Kısaca Siber Güvenlik, alt yapısı bilişim sistemleri olan siber ağlar üzerinde yaşanan hayatın güvenliğinin sağlanması, bütünlüğünün ve gizliliğinin korunmasıdır.

21.Yüzyılda Siber Güvenlik Nedir?

21. yüzyılda dijital çağın başlamasıyla birlikte teknoloji ve bilim alanındaki gelişmelerin hızlanması güvenliğin yeni bir boyutunu ortaya çıkarmıştır. İnternet kullanımının uluslararası sınırları kaldırması, her türlü erişimi sağlaması ve insanların hayatının bir parçası haline gelmesi "Siber Güvenlik" kavramının 21.yüzyılda sıkça kullanılmasına neden olmuştur.



"Siber Uzak" olarak adlandırılan dijital platformda bulunan bilgiye ulaşmak amacıyla gerçekleştirilen siber saldırılar gerek ulusal gerek uluslararası sistemi bozarak organize suçlar, siber terör, siber savaş gibi tehditlerle büyük bir güvenlik sorunu oluşturmuştur. Özellikle gelişmiş ve gelişmekte olan ülkelerin alt yapılarının kapasitesi siber dünya için yeterli olmadığı için bu ülkeler siber uzaya bağımlı hale gelerek ulusal güvenlik problemleri ile karşılaşabilmektedirler.

Hacker olarak adlandırılan, teknoloji konusunda bilgili ve bilgisayarlar konusunda üst düzey donanımlı beceriye sahip olan kişiler siber güvenliğin en büyük tehditlerinden biridir. Dünyada yaklaşık 4 milyar internet kullanıcısı bulunmaktadır. Hackerların en aktif oldukları hedeflerinden biri ise internet kullanıcıların %64'ünün kullandığı sosyal medyadır. Siber güvenlik hakkında yeterli bilgisi olmayan yaklaşık 1,6 milyar insanın sosyal medya kullandığı göz önünde bulundurulursa her gün ortalama 600 bin Facebook kullanıcısının hesabının gizliliğinin ihlal edilmesi anlaşılabilir. Siber saldırıların başrolü olan virüsler çoğu

güncel olmayan bilgisayarda yüklü olan eklentiler üzerinden bulaştığı için istatistiklere göre dünyadaki bilgisayarların %99'unda güvenlik zafiyeti bulmak mümkündür.

Dünya çapında gerçekleşen siber güvenlik suçlarının dünya ekonomisine zararı sadece 2015 yılında 3 trilyon ABD doları olmuştur. 2021'de ise siber suçların dünya ekonomisine olan maliyetinin 6 trilyon ABD dolarına çıkması beklenmektedir. Ülkemiz ise gelişmekte olan bir ülke olması ve jeopolitik konumu nedeniyle uluslararası siber saldırılarda hedef halindedir. Uluslararası bir yazılım şirketi olan Symantec tarafından 2015 yılında yapılan araştırma sonucuna göre Türkiye en çok siber saldırıya maruz kalan ülkeler arasında 9. sırada yer almıştır.

Dünya çapında her geçen gün artan siber saldırılara karşı siber güvenlik uzmanlarının mücadele etmesi tek başına yeterli olmamaya başladığı için bireyler olarak yeni dijital çağda kendimizi bu saldırılara karşı korumada üzerimize düşen sorumluluğu alarak basit önlemler almalıyız. Hacklenmelere karşı alınabilecek önlemleri şu şekilde sıralamak mümkündür:





1) Tahmin Edilmesi Zor Şifreler

Zayıf, doğum günü tarihleri gibi kolay tahmin edilebilir ve bir yere kaydedilmiş şifreler siber suçlar için en büyük zaaftır. Noktalama işaretleri, büyük ve küçük harfler kullanarak oluşturulacak güçlü şifrelerle birlikte güvenliği arttırmak için kullanılan iki aşamalı kimlik doğrulama yöntemi saldırılara karşı alınabilecek en önemli güvenlik önlemidir.



2) Bilinçli Kullanım

Güvenlik sorununa neden olan bir başka etken ise insan psikolojisidir. Birçok internet kullanıcısı yetersiz bilgi nedeniyle saldırganların sistemlerine giriş yetkisi vermektedirler. Google'un yaptığı araştırmalara göre kullanıcıların bilinçsiz internet kullanımı sayesinde yapılan saldırılara göre %45'i başarıya ulaşmaktadır. Bu konuda alınabilecek en iyi önlem siber güvenlik hakkında makaleler okuyup eğitimlere katılarak bilinçli olmaktır.

3) Güvenlik Açıklarını Kapatmak

Bilişim uzmanları her ne kadar oluşan güvenlik açıklarını kapatırsa bile bilgisayar kullanıcılarının bilgisayarlarının işletim sistemini ve yazılımlarını güncel tutmanın güvenlik açıklarının oluşmasını engellemede önemi büyüktür.

4) Reklam Virüslerinden Kaçınmak

En sıkça karşılaşılan virüs bulaştırma yöntemi internet sayfalarında yer alan virüs içeren reklamlardır. Virüslü bir reklama tıklamak cihaza virüsün bulaşmasına neden olur. Bundan kaçınmanın en iyi yolu ise reklam engelleyiciler kullanmak ve güvenli web sitelerini kullanmaktır.



5) “HTTPS” Kullanmak

HTTPS kullanımı sunucular arasında güvenli bir bağlantı kurmayı sağlar. Siber saldırılara karşı oluşturulan bir protokol olan HTTPS kullanımı kullanıcılarına güvenli internet kullanımı sağlar.

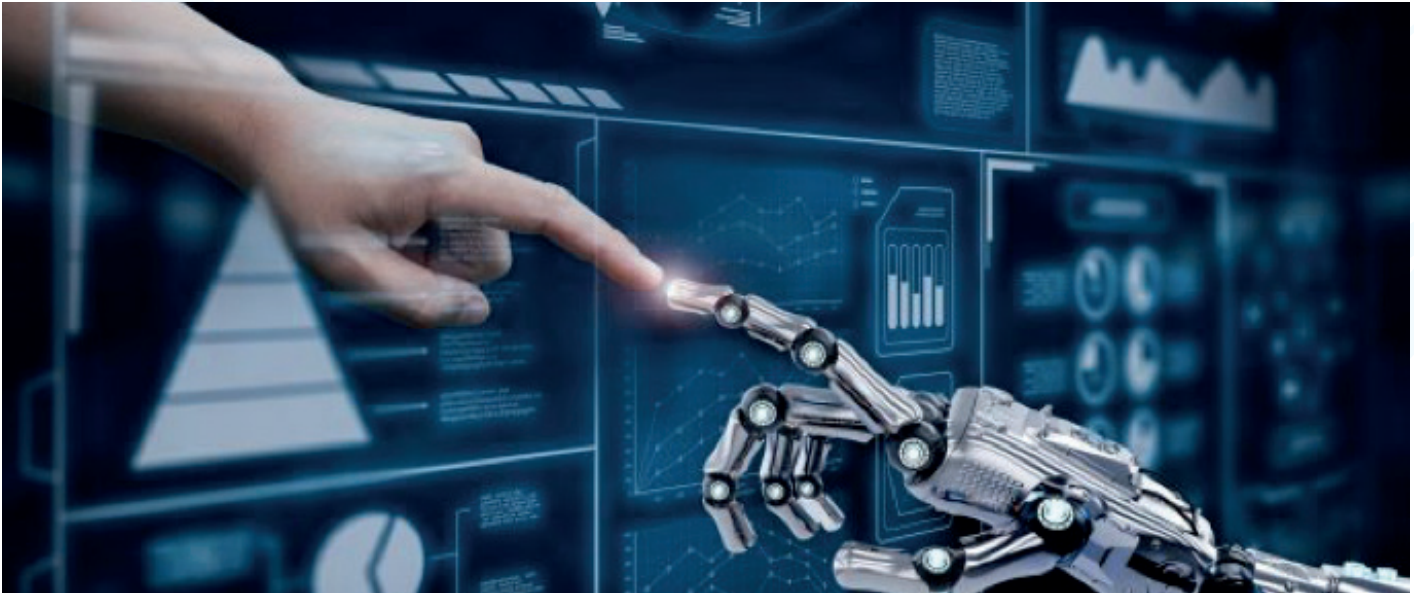
Siber saldırılara karşı yukarıdaki maddelerde belirtildiği gibi önlemler olarak dijital dünyada kişisel verilerimizi korumak mümkündür. Dijital dünyanın gelişimi göz önünde bulundurulduğunda önümüzdeki senelerde siber güvenlik alanında daha sağlam altyapılara ve bu alanda çalışan uzmanlara daha çok ihtiyaç duyulacaktır. Dünya'yı daha güvenli bir hale getirmek için daha çok çabalamanın gerektiği senelerde yeni bir meslek kavramı olan “Siber Güvenlik Uzmanı” ile karşılaşmak mümkündür. Siber uzayda artan saldırılar ve tehditler nedeniyle sadece kurumların değil, kişisel verilerin güvenliği de ekstra önem kazanmıştır. Bu güvenliği sağlamakla yükümlü Ağ ve Siber Güvenlik Uzmanı personel ihtiyacı da hem özel sektörde hem de devlette artış göstermektedir.



SİBER GÜVENLİK UZMANLARININ GÖREV TANIMI	SİBER GÜVENLİK UZMANI OLMAK İÇİN YAPILMASI GEREKENLER
Algoritma çözümleme ve yenilerini geliştirme	Matematik, Bilgisayar ya da Yazılım Mühendisliği bölümlerinde öğrenim görmüş olmak
Çalıştığı kişi veya kuruluşun ağ sistemindeki saldırı zaaflarını belirleme ve bu zaaflara karşı önlem alma	Ağ ve Bilgisayar Sistemleri, Bilgisayar Programcılığı, Bilgisayar Destek Uzmanlığı, Yazılım Geliştirme ve Veritabanı Yönetimi gibi çeşitli alanlarda uzmanlıklara sahip olmak
Olası saldırılar karşısında yaşanacak olan kayıpları asgari seviyeye indirme	Oldukça dikkatli olarak, ileriye sezebilen, analitik düşünüp her anlamda eleştirel bakış açısına sahip olmak
Yeni yazılımlar oluşturarak siber saldırı ataklarına karşı en yüksek performansı gösterecek ürünleri planlama ve kullanma	

Siber saldırılar güncel bir sorun olarak her geçen gün artmaya devam ediyor. Bireysel ve kurumsal verilerin korunması konusu da beraberinde önem arz etmeye devam etmektedir. Bu yüzden Siber Güvenlik Uzmanlığı geleceğin mesleği olarak konumlanıyor.

Konu hakkında daha derin araştırmalarla çeşitlendirilebilir. “Siber Güvenlik” alanında kendimizi bilinçlendirmek yeni dünya düzeninde bir zorunluluk haline gelmiştir. Bilinçli internet kullanımıyla siber saldırılara karşı korunup gelişen teknolojilerin fırsatlarından yararlanmak mümkündür. Her ne kadar teknoloji ve bilim alanındaki gelişmeler bazı güvenlik sorunlarına yol açsa da Arthur Clarke’ın da dediği gibi unutmamalıyız ki “Yeterince gelişmiş bir teknoloji, sihirden farksızdır.”



KAYNAKÇA

<https://www.webtekno.com/internet/siber-saldiri-hacker-iginc-bilgiler-h15737.html>
<https://www.hurriyet.com.tr/teknoloji/dunya-6-trilyon-dolarlik-siber-saldiri-riskine-karsi-hazirlaniyor-41150325>
<https://www.karel.com.tr/blog/isletmelerin-siber-saldirilara-karsi-alabilecegi-8-basit-onlem>
<http://otomasyondergisi.com.tr/bolumler/gelecegin-meslekleri/siber-guvenlik-uzmani-kimdir/>
<https://berqnet.com/blog/siber-guvenlik-nedir>