



HAVACILIK GÜVENLİĞİ

**Havacılık Güvenliğini Etkileyen Yeni Gelişmeler:
Siber Saldırıları ve Hava Trafik Yönetimi Güvenliği**

Dr. Öğr. Üyesi Ebru BAĞCI



7 Mart'ta radardan kaybolan Malezya Havayolları'na ait Boeing 777-200ER uçağı ile ilgili ortaya atılan iddialar arasında uçağın siber saldırılarla kaçırılmış olduğu dikkat çeken varsayımlardandır. İngiltere İçişleri Bakanlığı'nın eski bilim danışmanı terörle mücadele uzmanı Dr. Sally Leivesley'nin iddiasına göre hackerların uçağın yönetim sistemine radyo sinyalleri göndererek uçağın hızını, irtifasını ve yönünü değiştirmiştir.

İddiasına göre hackerların uçağın uçak içi elektronik sistemlerine girerek uçağın ana bilgisayar ağına ulaşmaları ve uçağı kontrol etmeleri mümkündür. Bu elim olayla beraber havacılığın siber saldırılar konusundaki düzenlemeleri önem arz eder hale gelmiştir.

Peki havacılık sektörü açısından siber saldırılar ne denli büyük bir risk teşkil etmektedir?

Siber saldırılar nasıl yapılabilir?

Hava Trafiđi Açısından Siber Saldırılar

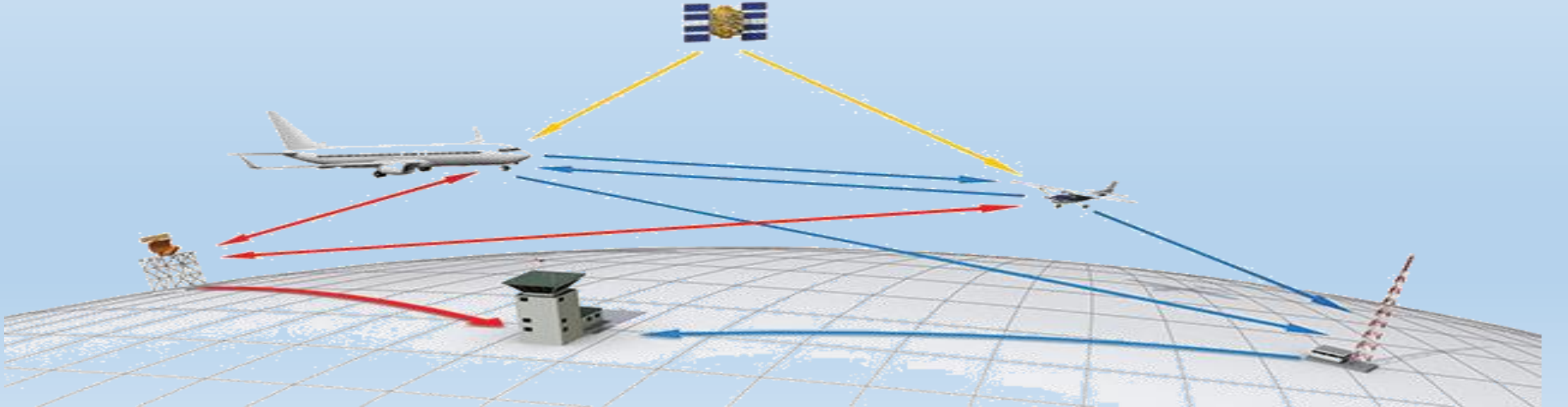
Bugün hava trafiđi halen daha insanlar tarafından gerçekleştirilmektedir. Trafiđin artışı dolayısıyla teknolojik ilerlemeler sayesinde **trafiđin insan eliyle deđil ancak insanın yönetimi ile** gerçekleştirilmesi planlanmaktadır.

İnsansız hava araçlarının yakın gelecekte yaygın kullanımı ile de beraber hava trafiđinin artışı karşısında **internet bazlı çözümlerle hava trafik kontrolünün** gerçekleştirilmesi halinde **siber saldırılar ihtimalini arttıracaktır.**



Otomatik Bağımlı İzleme (**ADS - Automatic Dependant Surveillance**) sistemi olacaktır.

ADS yayını sayesinde uçak dünyanın neresinde olursa olsun **pozisyon hız, irtifa, baş açısı ve yapmak istediği manevrası ile ilgili bilgiler** otomatik olarak uydu veya diğer haberleşme veri hatları vasıtasıyla hava trafik yönetim birimine; tüm **ADS – B ekipmanlı uçaklara ve yerdeki araçlara** iletilecektir.



T.C. Sayıştay Başkanlığı Devlet Hava Meydanları İşletmesi Genel Müdürlüğü (DHMI)'nin 2012 yılı raporuna göre **Trabzon Havalimanı'nda ADS-B sistemlerinin 2 yıl süre ile test edilmesine** ilişkin olarak 2007 yılında **Eurocontrol** ve **S.H.G.M.** arasında anlaşma imzalanmış ve Mart 2008 tarihinde Eurocontrol tarafından sağlanan **ADS-B donanımına ait yer istasyonu, anten ve ilgili diğer cihazların tedariki** ve sistemin kurulumu ile beraber proje kapsamında çalışmalara başlanılmıştır.



2002 yılından itibaren kullanımı için ICAO tarafından sertifikalandırılmış olan sistemin 2020 yılından itibaren hava trafik yönetiminde yaygın bir şekilde kullanımı amaçlanmaktadır. Sistem ile ilgili olarak güvenlik kaygıları mevcuttur:

- Kimlik doğrulama eksikliğinden ötürü **kaynağı bilinmeyen kişilerce yapılabilecek yerleştirme mesajlardan korunma** sorunsalı.
- Mesaj doğrulama kodu veya imzası eksikliğinden kaynaklanan **mesajlar üzerinde değişiklik yapabilme veya belirli bir uçaktan gönderiliyormuşçasına** veri akışı sağlanmasına karşı korunma sorunsalı.
- Mesaj şifreleme eksikliğinden ötürü oluşan **gizli dinlemeye karşı koruma** sorunsalı.
- Özel bilgi girişi yoluyla sağlanmaya çalışılan **korumanın sürekli ataklara karşı yetersiz kalması sorunsalı.**
- Tanımlama sistemlerinin kısa ömürlü hafızalarının **özel bilgi takip etme ataklarına karşı etkisiz kalması** sorunsalı

Eylül 2012'de Las Vegas'ta gerçekleştirilmiş olan Black Hat ve Defcon güvenlik konferansında da yine ADS-B'nin iletişimin gizliliğini sağlayan şifreleme ve sahte/yanıltıcı iletişimi engelleyen kimlik doğrulama özelliğinin eksik olması sebebiyle **hackerların radyo cihazları ile mesajları ve hava araçlarını yanıtlamasının mümkün olduğu araştırmacılar tarafından ifade edilmiştir.**



Uçak Üreticileri Açısından Siber Saldırıları

Hava aracı tasarımları hava trafik kontrolünden daha da radikal bazı değışimlere uğramıştır.

Günümüz hava araçları havayolu şirketleri, hava alanları ve havacılık hizmetleri sağlayıcıları tarafından işletilen yer bazlı sistemler ile bağlantılı sistemlerle çalışmaktadır. Üreticiler hazır **ticari yazılım ve donanımları** hava araçlarında **maliyeti düşürme amaçlı** olarak kullanmaktadırlar.

Bu aynı zamanda bazı kaynaklara göre emniyet açısından risk teşkil etmektedir. Hava aracı üreticileri aynı zamanda **hava trafik kontrolü ile hava aracı arasındaki rutin havacılık komutlarının yeni teknoloji kullanımına** olanak sağlayacak şekilde sistemler geliştirmişlerdir.



Bu sistemler ticari servislerde kullanılmakla beraber pilot tarafından güvenlik amaçlı olarak teyit edilmektedir bu da radyo trafiğinin yoğunlaşması suretiyle yine bir emniyet zaafiyeti olmaktadır.

İnsansız hava araçları açısından da siber saldırılara açık olması dolayısıyla üretim aşamasında gereken tedbirlerin alınması gerekmektedir.

2011 yılında **İran A.B.D.'ye ait bir İHA'yı** GPS verilerini aldatarak (spoofing) İHA'yı kendi ana üssüne iniyormuş gibi yanlış yönlendirerek ele geçirmişti.



Havaalanları Açısından Siber Saldırıları

Amerikan Ulusal Güvenlik Bakanlığı'nın Ulusal Siber Güvenlik Departmanı tarafından hazırlanmış olan 2013-2023 Ulaştırma Endüstri Kontrol Sistemleri Siber Güvenlik Standartları Stratejisi'ne göre şu anda mevcut sistemlerde havaalanları için **siber güvenlik standartları** bulunmamaktadır.

Standartlar **genelde hava araçları ile ilgilidir**. Havaalanları bilgi yönetim sistemler, özel ve kamu iletişim sistemleri, internet ağları, yeni teknoloji sistem tasarımları üzerinde çalışılması beklenilmektedir.



Havaalanlarının ne denli siber tehditlere açık olabileceğine ilişkin olarak bir örnek vermek gerekirse; **Heathrow**'da 5 numaralı terminalin bilişim altyapısı **1500 kapalı devre kamera sistemi (CCTV)**, **1100 güvenli erişim kontrol noktası**, **750 bağlantı noktalı kablosuz LAN ağı** ve **2800 tane hibrid teknoloji** kullanılarak yapılmış telefon altyapısından oluşmaktadır ve bütün bu sayılanlar da siber saldırılara açık haldedir.



Havaalanı ağlarına siber saldırı gerçekleştirilebilmesi aşağıdaki vasıtalarla mümkündür :

- USB Bellek
- Elektronik Sistemler
- Kablosuz ağ bağlantı noktaları
- Dijital kamera, MP3 çalar gibi muhtelif USB aygıtı
- Başkalarının makinalarını ödünç almış personel
- Optik medya (CD, DVD, vs.)
- E mail
- Smartphone
- Sosyal ağlar
- Çapraz site betik saldırısı

Ülkemizde de hatırlanacağı üzere 26.07.2013'te pasaport sisteminin kilitlenmiş olması sisteme yapılmış virüs saldırısı sebep olduğu iddia edilmişti. İstanbul İl Emniyet Müdürlüğü Polnet Bilgi Sistemi'nde meydana gelen arıza nedeniyle Atatürk Havalimanı ve Sabiha Gökçen Havalimanı'nda yolcu giriş ve çıkışları yapılamadı ve de pasaport noktalarında uzun kuyruklar oluşmuş ve uçaklar da bu gecikme dolayısıyla rötarlı olarak kalkabilmişlerdi.

Google Haberler | İbrahim YILDIZ/İSTANBUL | Haber Giriş: 19.05.2016 - 09:19, Son Güncelleme: 19.05.2016 - 10:03

POLNET bozuldu, havalimanı kilitlendi

f t e | Yazdır | A+ | Yüzü



Abone Ol | Google News

Atatürk Havalimanı'nda sabah saatlerinde meydana gelen POLNET Bilgi Sistemi'nde meydana gelen arıza nedeniyle uzun bir süre yurda giriş çıkış yapılamazken, yolcular pasaport kontrol noktaları önünde saatlerce beklemek zorunda kaldı.

University of Zurich executive MBA

Register for a virtual meeting with us now.

More information:
www.emba.uzh.ch

EFMD EQUIS ACCREDITED AACSB ACCREDITED AMBA ACCREDITED LE RU

En Çok Okunan Haberler

Havayolu Şirketleri Açısından Siber Saldırıları

Uluslararası taşıyıcılar birliği IATA Deloitte'un Uluslararası Havayolu İç Denetçiler Birliği ile birlikte hazırlamış olduğu Havayolu Dolandırıcılık Araştırması raporuna atıfta bulunarak konunun önemine dikkat çekmiştir.

2010 yılındaki Deloitte Havayoluyla Dolandırıcılık araştırmasına göre havayolu şirketleri dolandırıcılık dolayısıyla ortalama yıllık 2.4 milyon \$ kaybetmektedirler.

2011 Siber kaynaklı Havayolu Dolandırıcılık Araştırması'na göre havayolu şirketleri kendi web siteleri üzerinden yaptıkları satışlarda online kredi kartı dolandırıcılığı dolayısıyla **1.4 milyar \$** kaybetmişlerdir.

The Deloitte logo is displayed in white text on a black background. The word "Deloitte" is in a bold, sans-serif font, followed by a small green dot.

Pilotlar Açısından Siber Saldırıları



Elektronik uçuş çantası (electronic flight bag) sistemi sayesinde uçuş sırasında ihtiyaç duyulan ve kağıt üzerinde saklanan bilgilerin elektronik ortamda tutulabilmektedir ve de söz konusu sistem uçaktaki aviyonik sistemler ile entegre olabilen ve de uçuş sırasında oluşturulan dokümanların elektronik ortamda yaratılmasına ve yönetilmesine imkan veren bir sistemdir.

Normalde elle yürütülen ve uçuş için oldukça önemli olan uçuş öncesi performans analizi gibi hesaplamaların da otomatik olarak yapılmasını sağlayan amaca yönelik alt uygulamaları bünyesinde bulunduran bu sistemin de hacklenmesi halinde ciddi zararların olabileceği iddia edilmektedir.

ICAO Açısından Siber Saldırıları



ICAO'nun 2010 yılında gerçekleştirilmiş olan 21. Havacılık Güvenlik Panel Toplantısı'nda (AVSECP / 21, 22 – 26 Mart 2010) siber tehditlerle ilgili olarak Şikago Konvansiyonu'nun Güvenlikle ilgili 17 no.lu ekinin 12. maddesinin değiştirilmesi için öneride bulunulmuştur.

17 Kasım 2010'da kabul edilmiş, 26 Mart 2011'de yürürlüğe girmiş ve 1 Temmuz 2011'de uygulanmaya başlanmış olan tavsiye niteliğindeki usul uyarınca her Akit Devlet sivil havacılıkta kullanılan bilgi ve iletişim teknoloji sistemlerini etkileşime açık olması sebebiyle sivil havacılık emniyetini tehdit eder halde olmayacak şekilde önlemler alması tavsiye edilmektedir. Siber güvenlik ile ilgili hassasiyetin değerlendirilmesi de yine toplantıda önerilmiştir.

Montreal'de 12-14 Eylül 2012 tarihleri arasında gerçekleştirilmiş olan Havacılık Güvenliği'ne İlişkin Üst Düzey Konferans'ta da ICAO'nun siber saldırılar ile ilgili düzenleme yapmasının gerektiği hususu ifade edilmiştir.

Yeni teknoloji siber saldırılar açısından henüz yeterli güvenliğe sahip değildir:

a) Linux, Windows, Ipv6 protokolleri ve Ethernet (AFDX) gibi az sayıda teknolojiye güvenilmektedir ve bunlar IT sektöründe yaygın olarak kullanılmaktadır;

b) Netice itibarıyla bu teknolojilerin ve **bunların zayıf noktalarının ve eksikliklerinin yaygın bir şekilde bilinirliği** olmuştur;

c) Sistemler çok fazla birbiri ile bağlantılıdır ve bu nedenle de sistemlerden herhangi birindeki **güvenlik sorunu diğerini de etkilemektedir.**

d) Sistem hatalarının tesiri sistemler daha yoğun kullanıldığı için daha fazladır.

ICAO hava seyrüsefer sistemlerinin dönüşümü için önümüzdeki 10 ila 15 yıl içinde **120 milyar Amerikan Doları'nın** harcanacağını öngörmüştür.

Ülkemiz Açısından Siber Saldırıları

Bakanlar Kurulu'nca alınan 11.06.2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonu'na İlişkin Karar 20.10.2012 tarihli ve 28447 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

İşbu karar uyarınca Siber Güvenlik Kurulu kurulmuştur. Kurul'un görevleri şu şekildedir :

- a. Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak.
- b. Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak.
- c. Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.
- ç. Kanunlarla verilen diğer görevleri yapmak.

Hali hazırda mevcut düzenlemeler uyarınca ulusal siber güvenliğin sađlanmasına ilişkin politika, strateji ve eylem planını hazırlama görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na verilmiştir.

Eylem planında siber güvenlik riskleri, ilkeler, stratejik siber güvenlik eylemlerinin yanısıra mevzuatın oluşturulması çalışmalarına başlatılmasına da karar verilmiştir ve söz konusu çalışmaların ceza hukuku, medeni hukuk, idari yargı ve bunlarla ilişkin tüm usul hükümlerinin düzenlenmesine destek olacak şekilde olmasının gerektiđi de ifade edilmiştir.

Havacılık sektörü çok boyutlu olarak siber saldırı tehditlerine açıktır.

Gerek hava trafik kontrol sistemi, gerekse havaalanı terminali ve uçak sistemleri muhtemel siber saldırı tehditlerine karşı azami ölçüde korunmalıdır. Hukuk platformunda da yine bu yönde daha fazla çalışma yapılmalı ve ülkemizde de mevcut siber saldırılar ve bilişim suçları ile ilgili düzenlemelerin havacılık ile ilgili olarak da değerlendirmesi yapılmalıdır.