**Türkiye Siber Güvenliğini Nasıl Sağlayacak**

Adli Bilimciler Derneği Başkanı Başkanı Prof.Dr.İ.Hamit HANCI -Adli Bilimciler Derneği Adli Yöneylem Komisyonu Başkanı Dr.Alp Aslan- Adli Bilimciler Derneği Adli İstihbarat Komisyonu Başkanı Mete Uzgur -

**2018 ve 2020 de yazmıştık ve demiştik ki (Tam metin eklidir)**

*“Adli Bilimciler Uyarıyor!!*

*Yeni Nesil Terör Saldırılarına Hazır Olmalıyız…*

 *BİLİŞİM SİSTEMLERİ İLE SİBER SALDIRILARLA GERÇEKLEŞEBİLECEK TERÖR SALDIRILARINA*

*HAZIR MIYIZ!!*

*Bilgisayar sistemleri günümüzde tamamıyla hayatımızın içinde ve doğru şekilde ve insanlığın hizmetinde kullanıldığı sürece fayda da sağlıyorlar.*

*Ancak bu sistemlerde bulunan açıklar kullanılarak kötü amaçlı kullanılabilir mi?*

*Daha da ötesi bu yolla cinayet ya da terör saldırıları gerçekleşebilir mi?*

*Özellikle, tıbbi, otomotiv, havacılık sistemlerinde risk değerlendirmelerini yeterince yapabiliyor muyuz?*

*Öncelikle şu soruyu sormak gerekiyor gerçekten bilişim sistemi kullanılarak cinayet işlenebilir mi ?*

*İnternet ortamında varlık gösterebilecek şekilde teknik donanıma sahip olan ve sanal olarak tanımlanabilir nesnelerin oluşturduğu ağ yapısı kolaylığın yanı sıra tehlikelere de açık.*

*…..Diğer bir deyişle hayatımızın her alanında akıllı cihazlarla yaşayacağız.*

*Bu cihazlar art niyetli olarak kullanılırsa ne olur ? ABD güvenlik firması IID nin 2013 yılındaki raporuna dayanarak Europol’ün tehdit değerlendirme raporu, çevirim içi (on-line) cinayetlerin olabileceğini iddia etmiştir.*

*GERÇEKLEŞTİRİLMESİ VE OLASI SUİKAST VE SALDIRILAR*

*TIBBİ CİHAZLAR*

*Sağlık merkezleri siber saldırıların kurbanı OLMA RİSKİ TAŞIMAKTADIR.*

*Ünlü bilgisayar korsanı(Hacker) Barnaby Jack Ekim 2011’ de düzenlenen McAfee FOCUS 11 konferansında insülin pompası aletlerine uzaktan saldırarak insülin miktarını değiştirmeyi başarmıştır. Şubat 2012 yılında ise San Francisco da RSA Güvenlik Konferansında transparan bir manken kullanarak doksan metre uzaklıktan yüksek kazançlı anten yardımıyla insülin pompasını kontrol etmiştir. Bu durumda şeker hastası olan bir kişi rahatlıkla suikast kurbanı olabilir.*

*Bir diğer saldırıya uğrayabilecek medikal cihaz ise uzaktan kontrollü kalp pilleridir (pacemaker).*

*ABD’de doktorun uyguladığı ilaçların takibi için kullanılan sistemdeki teknik hataları tespit eden Charles Cullen isimli hemşire sistemdeki açığı kullanarak 2006 yılında yakalanana kadar 16 yılda en az 40 hastayı ölümüne neden olduğunu kabul etmiştir.*

*2-Bir başka suikast yöntemi ise arabalar üzerinden olmaktadır.*

*Bu yöntemle ilgili en revaçtaki tartışma Rolling Stone and Buzzfeed gazetecisi Michael Hastings’in 18 Haziran 2013 te aracıyla hızla bir ağaca çarpması sonucu ölmesidir. Eski ABD Ulusal Güvenlik, Altyapı Koruma ve Terörle Mücadele Koordinatörü Richard Clarke, kazanın "bir otomobil siber saldırısıyla yapıldığını açıklamıştır.*

*Çinli Keen güvenlik laboratuarı araştırmacıları Samuel LV, Sen Nie, Ling Liu ve Wen Lu Bazı araçların modellerini fren sistemleri de dahil olmak üzere hackleyerek kontrol altına aldıklarını duyurmuşlardır.*

*3-AKILLI EV SİSTEMLERİ :Evlerinizde bulunan tüm aletler, havalandırma sistemleri ve kapı sistemlerinin bilgisayar sistemlerine bağlandığı ve bu sistemlerin ele geçirildiğini düşünürsek ölümcül sonuçlar doğurabilir.*

*Michigan Üniversitesinden profesör Atul PRAKASH ve çalışma ekibi Mayıs 2016 tarihinde yapılan bir araştırmayla akıllı ev sistemlerine bağlanarak evlere ait kapı sistemlerini açabildiklerini deney yaparak göstermişlerdir.Bu aynı zamanda bir saldırı da insanlar içerdeyken kapıların üstlerine kapatılmasını da sağlayabilir.*

*4-İNSANSIZ HAVA ARAÇLARI:Texas Üniversitesinden Todd Humphreys ve ekibi Radionavigation Laboratuvarında Gps bağlantılı insansız hava araçlarının nasıl hacklendiğini göstererek durmun ciddiyetini göstermiştir (Şubat 2012 )*

*Bu haberler göz önüne alındığında, insansız hava araçları da bilişim yoluyla ele geçirilerek özellikle silahlandırılmış İHA lar terör ya da suikast amacıyla kullanılabilir.*

***Ya uçaklara , boru hatlarına, doğalgaz ya da nükleer santrallere gerçekleştirilebilecek saldırlar. Düşünmek bile korkunç. yerli yazılımlar şart”***

Geçen süre maalesef bizi haklı çıkardı. Artık tüm dünya siber savaşların tehdidi altında.

Lübnan’da İlk gün Herhangi bir operasyona gerek kalmadan tek bir tuşla Çağrı cihazları patlatıldı, yüzlerce yaralı var.3000’e yakın kişi ölü, yaralı ya da sakat kaldı.

Hizbullah milislerinin iletişim için kullandığı Pager’lar aynı zamanda patladı

Lübnanlı Hizbullah grubu , savaşçılarının İsrail konum takibinden kaçınmak için Tayvan merkezli bir şirket tarafından üretilen düşük teknolojili cihazları kullanmaktaydı. Tayvanlı bu şirket ise patlamalarda kullanılan cihazların Budapeşte merkezli başka bir şirket tarafından üretildiğini söyledi.

Lübnan'ın dört bir yanında Hizbullah üyelerinin taşıdığı çağrı cihazlarında oluşan patlamalarla birlikte hem bu cihazları taşıyan Hizbullah üyeleri deşifre oldu, hem de saldırı sırasında kimisinin eli, kimisinin kolu, kimisinin parmakları koparak ağır yaralandı veya öldü.

Saldırıda, çağrı cihazına bir mesaj geldi ve kısa süre sonra patlama gerçekleşti. Görüntülerde, çağrı cihazlarının sahiplerinin ellerinde ya da ceplerinde infilak ettiği fark ediliyor.

Çağrı cihazları genellikle şifreli bir mesaj alındıktan sonra okunur, bu da yüz ve elin yakınında ciddi yaralanmalara neden oldu.

ABD ve İsrail medyası, Hizbullah üyelerinin savaş zamanında telefonların yerini şifreli mesajlarla hızlı ve güvenli bir iletişim aracı olarak çağrı cihazlarını kullandığını yakın zamanda ortaya çıkardı. Bu çağrı cihazları sadece 3 ay önce Hizbullah'a teslim edilmişti.

Yazılanlara göre, kullanılan eski ve güvenliği ihlal edilmiş cihazların, yenileriyle değiştirilmesi için bu cihazların varlığı ifşa edildi ve Hizbullah'ın yeni cihazlar alması teşvik edildi. Ardından da bu cihazlar uzaktan patlamaya hazır versiyonları ile Hizbullah'a satıldı.

Tabi bu eylemlerin yapılması için öncelikle içeride ajanlarının olması gerekiyordu.

Patlama ile ilgili iki olasılık söz konusu

1- İlk olasılık, Çağrı cihazlarına PETN türü bir patlayıcı yerleştirilmiş ve uzaktan sinyalle patlatılmış olması.

PETN'nin tek başına patlaması zor olduğu için tnt ve rdx ile birlikte kullanılması gerekiyormuş.

Bazı İddialara göre, Avrupa'da çakma bir firma Tayvan patenti ile parçaları alıp, montajlıyor.
İçine 3 gr patlayıcıyı da monte ediyor
Tayvan malı gibi Hizbullah'a, ya da onun mal temininden sorumlu firmasına satıyor.

Pacer ların içi çok dar olduğu için ancak düşük miktarda patlayıcı yerleştirilebiliyor.

2- Diğer olasılık , bu cihazların hacklenip patlatılması ki bu durumda hepimiz ceplerimizde cep telefonu şeklinde birer bomba taşıyoruz.

Bu olasılıklar üzerinde durulurken bir gün sonra, Birleşmiş Milletlerin Sivil Cihazların silaha dönüştürülmemesi uyarısının gelmesine yol açan diğer saldırılar geldi. Telsizler…..

**Devam edecek….**