EDİRNE ROTARY KULÜBÜ 1977

İnsanlığı İçimizdeki Güç İle Kucaklayın

2011 - 2012

Kalyan BANERJEE (UR Bşk.) **Fatih R SARAÇOĞLU** (2420.Böl.Guv.) **Erdal ATAÖZDEN** (13.Grup.Guv.Yrd.)

Tarih: 21.02.2011 **Toplantı No**: 1727 **Bülten No**: 1352 **Kuruluş:** Mart !977 **Charter** : Mart 1980

DUYURULAR

MERHABA SEVGİLİ DOSTLARIM,

Mimar Sinan Rotary Kulübü üyesi Rotaryen Prof.Dr. Nazan ERDA'nın babası vefat etti. Meftaya Allahtan rahmet yakınlarına başsağlığı diliyorum.

Kulüp üyemiz sevgili Mehmet EREN 21.02.2012 tarihinde başarılı bir operasyon geçirdi sağlığının gayet iyi olduğunu öğrendiğim dostuma geçmiş olsun dileklerimi sunuyorum.

Dostlarım son kulüp toplantımızı 21.02.2012 günü Rotary evimizde yaptık. Bu toplantıda mayıs ayında gerçekleştireceğimiz Mimar Sinan yolunda bisikletçiler temalı projemiz hakkında durum değerlendirmesi yaptık. Oldukça etkin olacağını düşündüğüm bu proje için EBİS ile beraber çalışmalarımız sürmektedir.

03.03.2012 tarihinde Başkanlar eğitim semineri ve 10-11.03.2012 tarihinde Bölge Konferansı İstanbul Hilton Convention Center de yapılacak. Bölge Konferansında elbette gelecek dönem başkanımızın yanında olacağız.

SAĞLIK MUTLULUK DİLEKLERİMLE,

Muzaffer MEMİŞ

MİSAFİRİMİZ :	Koray KARABEYOĞLU	Deniz Men.Yat.Uz	Kenan KARAKUŞ Misafiri
	Efekan EGELİ	Öğrenci	Halil ALTUĞ Misafiri
MAZERETLİ ÜYELERİMİZ :	Cengiz TUĞLU – Demirkan ÇAĞLAYAN – Hasan ALTUNTAŞ – İsmet AÇIKGÖZ Mehmet EREN – Serhad CEYLAN		
ARAMIZDA GÖREMEDİKLERİMİZ:	Kaya ZEYBEKOĞLU – Kemal KARAKUŞ – Recayi ARAN – Oktay ALEMDAR Tarık ETKER		
DEVAM DURUMU :	**56.00**		
MUTLU GÜNLERİMİZ :	27 ŞUBAT Doruk BENAKMAN	Doğum Günü	KUTLARIZ……

Önümüzdeki hafta toplantımız: 28.Şubat.2011 Salı Saat 19.30 ROTARY EVİNDE

Başkan : Muzaffer MEMİŞ **Sekreter : Halil ALTUĞ** **Sayman : Reşat AYAN**
Üye : Cengiz TUĞLU **Geç.D.B. : Serhad CEYLAN**
Bülten irtibat : Faruk ETKER **Tel: (284) 225 25 10 - 213 25 13** **edirnerotary@gmail.com** **- www.edirnerotary.com**

BİLGİSAYAR VE İNTERNETTE CİDDİ SORUNLAR YAŞAMAMAK İÇİN AŞAĞIDAKİLERİ OKUMANIZ TAVSİYE EDİLİR !

İNTERNETİ ÇOK DİKKATLİ KULLANINIZ !.

Bu haftaki konuğumuz olan İnan Taptık, 1961 İstanbul doğumlu. Ankara İktisadi Ticari İlimler Akademisi mezunu. İlk bilgisayarını 1982'de aldı. Hayatını uzunca bir süre yazdığı programlardan kazandı. Ancak, 40 yaşında kendini emekliye ayırıp teknede yaşamaya başladığı günlerde bir sorunla karşılaştı: Hobi olsun diye hazırladığı internet siteleri sürekli hack'leniyordu. "Kendimi hacker'lardan nasıl korurum?" diye bir araştırma yapınca, ABD'nin bilgisayar güvenlik firması Hacker Safe'le tanıştı.

Taptık, şirket merkezinin pek çok güvenlik araştırmasından geçtikten sonra Türkiye temsilcisi oldu. Halihazırda büyük firma ve kuruluşların data güvenlik sistemlerini koruyan Taptık'la günlük hayatımızı internetin son tehlikelerinden nasıl koruyacağımızı konuştuk:

Bilgisayarda ciddi bela var

Sizinle buluşmadan önce telefonda konuştuğumuzda internet kullanıcıları için ciddi bir beladan söz etmiştiniz. İsterseniz o konudan başlayalım?..

Bu, sadece internet kullanıcıları değil, bilgileri bilgisayar ortamında kayıtlı olan, yani herkesin sorunu: Kimlik hırsızlığı. Kimlik bilgileriniz, adresleriniz, numaralarınız, şifreleriniz, banka işlemleriniz, alışveriş tercihleriniz, hepsi çalınıp, başkaları tarafından kullanılabilir.

Bu eskiden de mümkün değil miydi zaten?

Elbette, hacker'lar şifre kırarak yapardı. Ama, artık çok daha kolay. Hacker olmayan, daha az yetenekli biri bile artık kimliğinizi çalabilir.

Değişen ne?

Çünkü, artık wireless (kablosuz internet) var ve kullanımı hızla artıyor. Aldığınız ve yolladığınız e-mail'lerden bankacılık bilgilerinize kadar ekranınızdaki her şey okunabiliyor.

Kim okuyabiliyor?

İsteyen herkes. Mesela, wireless'ı olan kahve zinciri dükkânlardan birine girdiniz. Ya da havaalanındasınız. Veya otelde... Oradaki wireless'a bağlandınız ve işlem yapıyorsunuz. Yaptığınız her şey arka masadaki ya da yan odadaki biri tarafından rahatlıkla görülebilir.. Buna "blackberry" gibi cihazlar dahil...

Başkasının bilgisayarındaki bilgileri nasıl izliyorlar peki?

Çünkü, bu wireless dediğiniz şey aslında zaten bir yayın. Ve herkes tarafından çok kolay izlenebilir bir yayın. Sizin bilgisayarınızla wireless router'ı arasında havadaki sinyalleri herkes izleyebilir. Üstelik bunu yapmak öyle fazla bir yetenek de gerektirmez.

- Peki, acaba o bahsettiğiniz kafeler ya da havaalanlarında şöyle tipler var mıdır; birilerinin gelip bankacılık işlemlerini wireless'tan yapmasını bekleyenler... Yani avını bekler gibi?..

Tabii ki çok... Bazen kredi kartı kullanarak bir şey alanları beklerler... Bazen de gizli aşığıyla yazışanları... Bu da bir tür kapkaç sonuçta. "Wireless kapkaççılığı"... Ve bu tüm dünyanın da en yaygın siber suçudur.

Wireless'e dikkat edin

Öneriniz?..

Kesinlikle, wireless bağlantılı yerlerde bilgisayarınızdan sadece gazete veya haber portallarına bağlanın, hiç değilse insanlarla sizin için risk taşımayan bilgilerinizi paylaşmış olun.

Açık alanlarda durum böyle, ya peki evlerimizdeki wireless'ı kullanırken?..

Sizi evinizde monitor edecek kimse yoktur, ancak, burada da çok başka bir sorunla karşı karşıyasınız. O da yetkisiz kişiler tarafından sizin wireless internet hattınızın kullanılarak suç işlenebilmesi...

Banka dolandırıcılığı, çocuk pornosu vs. gibi... Belki üst komşunuz, belki de aşağıdaki lokantada oturan, hatta belki de arabasını sizin evinizin önüne park eden biri sizin wireless'nızı kullanarak birtakım suçlar işleyebilir.

Wireless şifremizin olması yetmez mi?

Yetmez. Onu da çok kolay bir şekilde kırıyorlar. Hatta nasıl kırılacağını bilgisayar dergileri ek olarak verdi. Google'a "wireless şifre kırma" yazınca bile yüzlerce program bulunuyor.

Ee o zaman evde de wireless kullanmayalım?..

Yok, kullanabilirsiniz, ama internet dünyasındaki mantık hep aynıdır: Tolere edebileceğiniz riskleri taşıyın. Çalınmasını tolere edemeyeceğiniz bilgilerinizi kablolu internet üzerinden yazışın. Ayrıca, sadece yazışmamak da yetmez, işiniz yoksa wireless'inizi kapatın. Programın içine girip disable edin. Hatta şifrelemek için de birkaç önerim olabilir: Kablosuz

internet modeminizin ayarlarından bağlanacak bilgisayarınızın MAC (Media Access Control) numarasını tanımlayabilirseniz, başka bir bilgisayar sizin sisteminize bağlanamaz.
Bir de üreticilerin verdikleri standart cihazlardaki IP numaralarını değiştirirseniz hacker'ların işlerini çok zorlaştırmış olacaksınız. Daha başka yöntemler de var, ancak, bu yöntemler herkes tarafından kolay uygulanabilir ve her şartta standart şifrelemeden çok çok daha güvenlidir.
Kablolu internetin olmadığı yerlerde GPRS ile bağlanmak?.. Biraz fazla tuzlu oluyor, ama güvenli mi?
Tabii daha güvenli. Çünkü şifrelenerek giden bir sistemi kullanıyorsunuz. Onun için bunu scan etmek zor. İlla ki edilir de çok daha zor ve daha büyük bir teknik yapı gerektiriyor.

Bilmeden suçlu olursunuz
Peki, bu yüzden başına iş açılan insanlar var mı Türkiye'de?
Az değil. Mesela bir adamın oğlu yurtdışına eğitime gittiği sırada çevreden bağlanan birisi onların wireless'ıyla suç teşkil edecek materyaller indirmiş. Tabii ki polisler IP'sini tespit edip adamın kapısına gelmişler. Adam şok. Bilgisayarı açmayı bile bilmiyorken hakkında dava açılmış.
Mahkemeye birkaç kez gidip geldikten sonra gerçek ortaya çıkmış. O yüzden de herkese wireless'larıyla ilgili güvenlik önlemlerini bir kez daha gözden geçirmelerini tavsiye ederim.

ANNEANNELER BİLE FACEBOOK'ÇU OLACAK
Cumartesi günü itibariyle Türkiye'den Facebook'a üye sayısı 1 milyon 415 bin 768. Taptık, bu ilginin daha da devam edeceğini, çünkü kullanıcıların henüz Facebook'un gerçek dinamiklerini keşfetmediklerini söylüyor. Mesela, henüz aile ağaçlarının kurulmadığını belirten Taptık, "Bu demektir ki Facebook'a daha anneanneler, babaanneler, dedeler de üye olacak" diyor.

Size de bir 'Cookie' bırakılmış olabilir
Bu "cookie bırakmak" nasıl bir şey?
Diyelim ki bir internet sitesine girdiniz. O site daha sonra yine geldiğinizde sizi tanıması için, size hiç söylemeden bir "cookie" veriyor. Sonra, bir daha ziyaret ettiğinizde o site size, "Merhaba bilmem kim" diyor. Ama, bazı cookie'lerin işi bu kadarla da bitmiyor. Akıllı cookie'ler sizin ne yaptığınızı, başka hangi sitelere girdiğinizi, hatta mouse'nızın tüm hareketlerini takip edebiliyor. Böylece, o cookie hakkınızda epey bilgi toplamış oluyor.

Ne işe yarıyor bu bilgiler?

Online mağazaların çok işine yarıyor. Kim olduğunuzu, ne aldığınızı, satın alma alışkanlıklarınızı öğreniyorlar ve ona göre satış stratejisi geliştiriyorlar.

Peki bunu istihbarat kuruluşları da yapabilir mi?
Eğer, istihbarat kuruluşlarının sitesine girerseniz ve onlar da sizin bilgisayarınıza bir cookie koyarlarsa sizi izleyebilirler.
6 banka var

Bankalar ne kadar güvenli?
Türkiye'de bankaların data güvenliği biraz sancılı. Altı banka dışında günlük güvenlik denetiminden geçen banka yok. Oysa, bankalar günde ortalama 30'a yakın güvenlik açığıyla karşı karşıyadır.

O altı banka hangileri diye sorsak?
Söyleyemem, çünkü Türkiye'de çok ağır bir Bankacılık Yasası var. Hatırlarsanız, rahmetli Sakıp Sabancı bile kendi bankası için en güvenli demişti ve ceza ödemişti.

Güvenliği iyi olmayan bankalardaki müşterileri bekleyen tehlike ne?
Hesap bilgilerinin ortaya çıkması ya da hesapların boşaltılması.
O zaman hiç değilse şunu söyleyin: Tüketici neye göre banka seçmeli?
Bu işte tüketicinin uzaktan anlayabileceği bir ayraç yoktur. Tek yapılabilecek şey, banka güvenliğiyle ilgili haberleri yakından takip etmektir.
Hani, hiç hack'lenemeyen bir site vardı, o hâlâ ayakta duruyor mu?
Evet, hâlâ hack'lenemedi. Amerikan deniz piyadelerinin "marines.com" sitesi... Yıllardır, en çok atak alan sitelerin başında geliyor, ama hâlâ indirilemedi. Çünkü güvenliği çok sağlam.

Türk hacker'ların ünü sürüyor mu?
Hacker'likten kazanç elde etme konusunda Ruslar bir numara, ama milliyetçi tarzda davranış biçimi olarak hâlâ bir numara Türk hacker'ları.

E-mail kaydediliyor

Aslında, biz yazışmalarımızı ne kadar korursak koruyalım, bunlar zaten görülüyor değil mi?

Hepimizinki görülmüyor, ama hepimizinki algoritmalı bir düzende izleniyor.

Kim tarafından?

ABD, TC ve her kim istiyorsa... Ancak, bu izleme ülkeler tarafından elektronik, yani data boyutundaki programcıklara yaptırılıyor.

O nasıl oluyor?

Temel olarak kullandığımız sistemi, bir telefon sistemine benzetirsek biraz daha anlaşılır olur. Sizinle aramızda direkt bir hat olmadığı için görüşmeleri erişim noktalarına yani santrallere bağlanarak gerçekleştiriyoruz. Böylece, hem ulusal internet omurgamız üzerinden hem de uluslararası internet omurgası üzerinden iletişim sağlamış oluyoruz. Tabii, bu sırada da tüm yazışmalarımız geçici bir süre için sistem tarafından kayıt ediliyor. Bu kayıtlar insan gözüyle değil, programlar tarafından yapılıyor.

Ama, ne zaman ki izleyenler, "A kişisinin e-mailleri okunsun, hesaplarına bakılsın" der, ya da ne zamanki program o e-maillerin içinde bazı kelimelere rastlar, işte o zaman insan gözüyle takip seviyesine geçer.

Bu kayıtlar nerede yapılıyor?

İnternet omurgasından hat alınan herhangi bir yerde.

Böyle bir teknolojiye devletler mi sahip, yoksa canı isteyen herkes mi?

Güç odakları ve otorite sahipleri. Canı isteyen ve yetenekli bir hacker, ancak, iki kişi arasındaki yazışmayı kayıt edebilir, ama o omurgadan çıkan bütün yazışmaları tarayamaz.

Büyük güç otoritelerini kenara koysak, şirketlerde durum nasıl?

Birçok şirkette patronlar, çalışanlarının iş yerinde kullandıkları tüm ekranlarını izler. Üstelik, sadece şirketinizin e-mail adresinden yaptığınız yazışmaları değil, başka bir e-mail adresiniz varsa, onu da izlerler. Ve bu, emin olun, sanıldığından daha yaygın bir uygulamadır.

Arama motorunu kandırabilirsiniz

Arama motorlarında, kişi ya da kuruluşlar hakkında çıkan olumsuz bilgileri yok etmenin imkânı var mı?

Yok edemezsiniz, ama arama motorunu kandırabilirsiniz. Çünkü, yapılan bir araştırmaya göre, arama motorlarının ilk sayfasını açıp, ikinci sayfaya geçmeyenlerin oranı yüzde 88. Dördüncü sayfaya kadar gelenler ise sadece yüzde 1. Yani, hakkınızda istemediğiniz bilgileri yok edemezsiniz, ama 2'den sonraki sayfalara ötelerseniz, gözden kaçırmış olursunuz. Çünkü, kimse bakmıyor.

Peki, bu öteleme kolay bir şey mi?

Hiç değil. Üstelik pahalı. Çünkü istenmeyen bilgileri sonraki sayfalara kaydırıp, ilk sayfayı temizleyebilmek için en az 100 farklı kritere uygun ve en az 100 site, haberi yeniden kurgulamak gerekiyor.

'Zede' uyarısı

'Facebook'zedeler başladı mı?

Birkaç çeşit zede var. Birisi kendi adına başkaları tarafından adres alınanlar. Böyle bir duruma karşı yapabilecek tek bir şey var, o da kullanmasanız bile Facebook'a üye olmanız, kendi isim hakkınızı almanız. Artık, başkaları isminizi kullansa bile gerçeği de orada durmuş olur.

Başka zedeler?

Fotoğrafı kullanılanlar var. Facebook'a konulan resimlerin üzerinde oynamak mümkün. Ya da o resimleri başka ilişkilerin içine yerleştirmek... Bu

durumlarda yapacak hiçbir şey yok. Ne mahkemeye gidebilirsiniz ne de o resimleri yok edebilirsiniz. Resimlerinizi her türlü kişi tarafından kopyalanıp kullanılabileceğini düşünerek seçin.

Kendi sayfanızı kapatsanız?

Her zaman böyle bir hakkınız var, ama kendiniz Facebook'tan çıksanız bile başkasının albümündeki fotoğraflarınızı silemezsiniz. Bu tamamen o kişiye kalmış.

Aslında, kötülük yapmak isteyenler için internet inanılmaz güzel bir mecra. Kadınlar, çocuklar, erkekler... İsteyen herkes için kötülük üretilebilir.

Sanki, "Facebook'a girmeyin" der gibisiniz, ama galiba siz de Facebook'tasınız?

'Facebook'a girmeyin' demiyorum. Ama, riskleri bilin ve bu riskleri tolere edebiliyorsanız, taşıyabiliyorsanız girin. Orada karşılaşabileceklerinizi bilin. Fotoğraflarınızı ona göre koyun.

Facebook'taki konumunuzu belirleyin. Ama, yok, ben bu riskleri tolere edemem ve riske de açığım diyorsanız o zaman meraklarınızı

Okyar YAYALAR