KAOS GL ÇALIŞANLARI İÇİN DİJİTAL GÜVENLİK YÖNERGESİ

Bu metin Kaos GL Derneği çalışanlarının ofis bilgisayarlarının ve internet bağlantılarının güvenli hale getirilmesi için oluşturulmuştur. Yönerge oluşturulurken Alternatif Bilişim Derneği'nin Kem Gözlere Şiş projesinden ve Electronic Frontier Foundation'ın Surveillance Self Defence projesinden faydalanılmıştır.

"Güvenlik bir ürün değil, süreç meselesidir.

Güvenlik tıpkı doğruluk gibi sisteme sonradan eklenebilen bir şey değildir."

Bruce Schneier

1. İNTERNET TARAYICISI GÜVENLİĞİ

1.A. HTTPS Everywhere

https://www.eff.org/https-everywhere

HTTPS Everywhere (her yerde güvenli http) birçok büyük web sitesine bağlantınızı güvenli hale getiren bir Firefox ve Chrome eklentisidir. Electronic Frontier Foundation ve TOR ekibi ortaklığı ile geliştirilmiştir.

Bildiğiniz gibi birçok site sayfa ve içerikleri şifreli https üzerinden sunabilecek alt yapıya sahipken, genellikle şifreli olmayan http üzerinden kullanıcılarını karşılarlar. Kimi zaman da şifreli sayfalarda şifreli olmayan öğelere bağlantı içerirler. Bu da gizliliğimizi ihlal edebilecek durumlar yaratır.

HTTPS Everywhere şifresiz bağlantıları henüz bize ulaşmadan tespit edip olanaklı olduğu her durumda şifreli bağlantılar halinde yeniden yazar ve şifreli bağlantı üzerinden içeriklere erişmemizi otomatize eder, kolaylaştırır.

Her tarayıcımızda olması gereken bir eklentidir.

Kurulum:

- https://www.eff.org/https-everywhere adresinden kullandığınız tarayıcıyı gösteren simgeye tıklayın.
- Karşınıza çıkan uyarı mesajını dikkatlice okuyun ve eff.org sitesinden gelen eklentiye güvendiğinizi onaylayın.
- Kurulumu başlatın.
- Tarayıcınızı yeniden başlatın.

1.B. Adblock Edge

Adblock, web siteleri üzerindeki reklamları engelleyen bir tarayıcı eklentisidir. Eklenti, içerisinde reklam yollarının/adreslerinin bulunduğu bir liste birlikte yüklenir ve bu yollar üzerinden gelen reklamları engeller. Bu listeyi özelleştirebilir ya da kendi listenizi oluşturabilirsiniz. Fakat bir değişiklik yapmasanız da öntanımlı olarak gelen "EasyList" yeterli koruma sağlayacaktır.

Reklamların engellenmesi yalnızca görüntü rahatsızlığı ya da sayfanın hızlı açılması için değil güvenliğiniz için de avantaj sağlayacaktır. Çünkü zaman zaman bu reklamları oluşturan kodlar aynı zamanda takip mekanizmaları ya da kişisel verilerinizin güvenliğini tehdit eden zararlı kod parçacıkları barındırır.

1.D. NoScript

NoScript web sitelerinde bulunan aktif içeriği yönetmek için oluşturulmuş bir tarayıcı eklentisidir. Bu eklenti yüklendiğinde öntanımlı güvenlik listesinde bulunan ayrıcalıklı sayfalar haricindeki(bu liste isteğe göre değiştirilebilir) tüm sayfalarda çalışan JavaScript, Java, Flash, Silverlight vs. otomatik olarak engellenmiş olur. Sebebi ise sayfada çalışan bu tür kodların zaman zaman kullanıcıyı gözetleme ve hakkında veri toplama ya da direk saldırı (XSS vs.) amacında çalışıyor olmasıdır. NoScript bulunduğunuz web sayfasındaki bu tür içeriği yönetmenizi sağlar. Bu eklenti aynı zamanda sayfaların hızlı yüklenmesine de yardımcı olacaktır.

Eklentiyi kurmak için Firefox üzerinden Araçlar>Eklentiler yolunu izleyip (Kısayol: Ctrl+Shit+A) arama aralığına eklentinin adını yazıyor ve "Kur"(install) butonuna tıklıyoruz. Eklentiyi yükledikten sonra ziyaret ettiğiniz her hangi bir web sitesinde, sayfa üzerinde sağ tık ile açılan menüyü kullanarak; yalnızca mevcut sayfa ya da bağlı tüm sayfalara geçici ya da kalıcı izinler verebilirsiniz.

2. SANSÜRÜ AŞMA YÖNTEMLERİ

LGBTİ içerikli web sitelerine dönük TİB sansürünün yoğun olduğu ülkemizde erişime engellenen sitelere erişmek için kullanılabilecek pratik yollar ve erişim engelleme biçimleri

Türkiye'de erişim engellemeleri genellikle üç biçimde yapılmaktadır.

1- Alan adı temelli engelleme

Bu tür engelleme yönteminde alan adları (twitter.com, kaosGL.org) yanlış IP adreslerine yönlendirilmektedir. Girmek istediğimiz site yerine genellikle “mahkeme kararı sayfasına” yönlendiriliriz.

Çözüm önerileri: DNS ayarları değiştirme, VPN veya TOR kullanmak

2- URL temelli engelleme

Bu engelleme türünde ise alan adı bizi doğru siteye yönlendirmeye devam etse de ilgili sitedeki engelli içerikleri ayrı ayrı engelleyebilir.

Çözüm önerileri: VPN ve/veya TOR kullanmak

3- IP temelli engelleme

IP temelli engelleme ise Internet Servis Sağlayıcılarının erişmek istenilen sitenin IP adresine giden isteklere izin vermemesi şeklinde yapılır.

Çözüm önerileri: VPN ve/veya TOR kullanmak

TOR

TOR dünyada binlerce kullanıcısı olan özel bir ağdır. TOR'u indirip bilgisayarınıza veya cep telefonunuza kurduğunuzda siz de bu ağın bir parçası haline gelirsiniz. Ağ üzerinde her kullanıcı bir düğüm (nokta) olarak tasarlamıştır. Düğümler birbirlerine tünellerle bağlıdırlar. Siz herhangi bir siteye bağlanmak istediğinizde bu tünelleri kullanarak erişim sağlarsınız. Yapısı gereği biraz yavaş olsa da sansürü aşmak ve trafiğimizi kriptolamak için oldukça etkili bir yöntemdir. Önemli bir özelliği de anonimlik sağlamanıza yardımcı olur.

TOR kurulumu için **şu linkten** faydalanabilirsiniz:

TOR'u Android telefonlarda kullanmak için **Orweb** uygulamasını, iPhone veya iPad lerde kullanmak için **Onion Browser** uygulamasını kurabilirsiniz.

Google Zenmate

Özellikle Google Chrome için kullanılan bu eklenti açık kaynak kodlu olmadığından güvenlik açısından yüzde yüz sonuç vermez. Ancak, LGBTİ içerikli websitelerine dönük TİB sansürünün yoğun olduğu ülkemizde bu sitelere erişebilmenin en kolay yollarından biri Google Zenmate kullanmak olarak görülüyor. TOR indirip kullanamadığınız, VPN'niz olmadığı durumda Zenmate tercih edilebilir. Ama unutmayın: Zenmate kullanmak sadece ve sadece engellenen siteye girmenizi sağlar, takip edilmeyeceğiniz anlamına gelmez.

3. KÖTÜ AMAÇLI YAZILIMLAR

Malware, diğer adıyla kötü amaçlı yazılım, bilgisayar kullanıcılarına zarar veren yazılımdır. Bu tarz yazılımlar bilgisayar işlemlerine zarar vermek, hassas bilgiler toplamak, kullanıcıyı taklit ederek onun adına spam veya sahte mesajlar yollamak ya da gizli bilgisayar sistemlerine erişim sağlamak gibi birçok farklı yola başvururlar, ancak çalışmaları sadece bunlarla sınırlı değildir. Kötü amaçlı yazılımların büyük çoğunluğu suç teşkil eder ve genellikle banka bilgilerini ya da eposta veya sosyal medya hesaplarının giriş bilgilerini toplamak için kullanılırlar. Kötü amaçlı yazılımlar ayrıca devletler, emniyet teşkilatları ve hatta sivil vatandaşlar tarafından şifrelemeyi aşmak ve kullanıcıları gözetlemek için kullanılırlar. Kötü amaçlı yazılımların çok çeşitli kabiliyetleri vardır; bir saldırganın bir webcam ya da mikrofondan veri kaydetmesi, belli anti-virüs programlarının bildirgelerinin engellenmesi, tuş darbelerinin kaydedilmesi, epostaların ve diğer dökümanların kopyalanması, şifrelerin çalınması ve daha birçoğu bunlardan bazılarıdır.

Anti-virüs yazılımı

Anti-virüs yazılımları, suçlular tarafından yüzlerce hedefe karşı kullanılabilen ucuz ve "hedefsiz" kötü amaçlı yazılımlara karşı savaşmada oldukça etkili olabilirler. Ancak anti-virüs yazılımları, hedefli saldırılara karşı genellikle etkisizlerdir

Güvenlik ihlalinin belirtileri

Anti-virüs yazılımlarını kullanarak kötü amaçlı yazılımları saptamak mümkün olmadığında bile, bazı durumlarda güvenlik ihlalinin belirtilerini bulmak mümkündür. Örneğin Google kimi zaman Gmail kullanıcılarını uyararak, hesaplarının devlet destekli saldırganlar tarafından hedef alındığını belirtir. Ek olarak, siz aktifleştirmediğiniz halde webcam'inizin ışığının yandığını fark edebilirsiniz (kötü amaçlı yazılımların gelişmiş olanları bu ışığın yanmasını engelleyebilir) — bu da bir başka güvenlik ihlalinin belirtilerinden biri olabilir. Diğer belirtiler çok bariz olmayabilir; epostalarınıza bilinmedik bir IP adresinden erişildiğini ya da ayarlarınızın her epostanızın kopyasının başka bir eposta adresine gönderilecek şekilde ayarlanmış olduğunu fark edebilirsiniz. Ağ trafiğinizi izlemek gibi bir kabiliyetiniz varsa, bu trafiğin zamanlaması ve yoğunluğu bir güvenlik ihlalinin yaşandığını belirtebilir. Bir başka tehlike işareti ise bilgisayarınızın bilinen bir Komut ve Kontrol sunucusuna (Command and Control server) bağlanmasıdır — bu tarz sunucular kötü amaçlı yazılımın bulaşmış olduğu bilgisayarlara komutlar yollarlar ya da bu bilgisayarlardan veri toplarlar.

Bilgisayarınızda kötü amaçlı yazılım bulursanız, bilgisayarınızın internet bağlantısını kapatın ve bilgisayarınızı kullanmayı hemen bırakın. Bilgisayarınızı, sahip olduğunuz kötü amaçlı yazılımla ilgili daha fazla bilgi edinebilecek bir güvenlik uzmanına götürmeyi isteyebilirsiniz. Eğer kötü amaçlı yazılımı bulduysanız, bu yazılımı silmek bilgisayarınızın güvenliğini sağlamış olduğunuz anlamına gelmez. Kötü amaçlı yazılımların bazıları, yazılımın bulaştığı bilgisayar üzerinde saldırganın keyfi kod çalıştırmasına izin verir ve saldırganın bilgisayarınızın kontrolüne sahip olduğu süre içinde, bilgisayarınıza başka bir kötü amaçlı yazılım yüklemediğinin garantisi yoktur. Güvenli olduğunu düşündüğünüz bir bilgisayara giriş yapın ve tüm şifrelerinizi değiştirin; kötü amaçlı yazılımların

bilgisayarınıza bulaştığı süre boyunca yazdığınız her şifrenin güvenliğinin ihlal edilmiş olduğunu varsaymalısınız.

4. SOSYAL MEDYADA PAYLAŞIM GİZLİLİĞİ

Paylaşımlarınızın gizliliğini korumak için uygulayabileceğiniz bazı yöntemler şunlar:

1. Özellikle size sıkıntı yaratabileceğini düşündüğünüz içerikleri en çok paylaştığınız platformlar olan Facebook ve Twitter hesaplarınızı kamuya kapatın. Paylaşımlarınızı sadece arkadaş ve takipçilerinizin görmesine izin verin.

- Facebook > Ayarlar > Gizlilik > Diğer arama motorlarının zaman tüneline bağlantı vermesini istiyor musun? > Hayır şıkkını seçerek Facebook profilinizi Google aramalarına kapatın.

- Twitter > Ayarlar > Güvenlik ve Gizlilik > Gizlilik > Tweetlerimi korumaya al şıkkını işaretleyerek Twitter profilinizdeki tweet'leri (takipçileriniz haricinde) tüm kullanıcılara kapatın.

2. Facebook hesabınız kamuya açık olsa bile yaptığınız bazı paylaşımları sadece arkadaşlarınızın görmesini sağlayabilirsiniz. Facebook gizlilik ayarlarından mutlaka faydalanın.

3. Facebook'ta tanımadığınız kişileri arkadaş listenizden çıkarın, Twitter'daki şüpheli takipçilerinizi engelleyin.

4. Tanımadığınız kişilerden gelen arkadaşlık ya da takip isteklerini kabul etmeyin.

5. Facebook'un "Takip et" özelliğini kendi profilinizde kullanmayın.

6. Facebook zaman tünelinizi ve profillerinizi Facebook içi ve dışı aramalara kapatın.

7. Twitter profiliniz kamuya açıksa, tweetlerinizde taramalara takılabilecek anahtar kelime ya da isimleri kullanmayın.

8. Arkadaşlarınızdan gelen şüpheli mesajlara cevap vermeyin, mesajlarda bulunan linklere tıklamayın.

5. OLTALAMA SALDIRILARI

Oltalama siteleri, tercih ettiğiniz bankacılık veya telekomünikasyon kurumuna ait web sitesi ve hizmetleri taklit ederek sizi yanıltmak ve kişisel bilgilerinizi ele geçirmek üzere tasarlanmış sahte web adresleridir. Bankanıza veya Internet Servis Sağlayıcınıza aitmiş gibi görünen ve sizden bir takım bilgileri girmenizi isteyen bu siber dolandırıcılık teşebbüsleri, günümüzde saldırganların en sık başvurduğu yöntemlerden biridir.

Bir saldırgan size masum gözüken bir eposta ya da bir link yolladığında ancak bunlar masum olmadığında, buna oltalama (phishing) denir. Oltalama saldırıları kullanıcılara kötü amaçlı yazılım (malware) bulaştırmanın en yaygın yoludur. Kötü amaçlı yazılımlar bilgisayarınızda saklanan, bilgisayarınızın uzaktan kontrol edilmesine olanak sağlayan, bilgilerinizi çalan veya sizi takip eden yazılımlara verilen isimdir.

Bir oltalama epostasında, saldırgan sizi kötü amaçlı yazılım içeren bir eki açmaya ya da bir bağlantıya tıklamaya teşvik etmeye çalışabilir. Oltalama ayrıca internet sohbeti üzerinden de gerçekleşebilir. Size eposta ya da sohbet aracılığıyla gönderilen linklere tıklamadan önce iki defa düşünmek önemlidir.

Epostalardaki web adresleri yanıltıcı olabilir. Epostalardaki web adresleri güvenli gibi gözükebilir, ancak farenizle bu adreslerin üstüne geldiğinizde bu adreslerin sizi nereye

yönlendireceğine bakarsanız, linkin aslında sizi başka bir adrese götüreceğini görebilirsiniz.

Bazı oltacılar sizi kandırmak için popüler web adreslerine benzer adresler kullanabilir; http://wwwkaosgl.org/ adresi http://www.kaosgl.org/'dan farklıdır! Birçok insan uzun linkleri daha iyi okumak ya da yazmak için link kısaltıcıları kullanır, ancak bunlar kötü niyetli adresleri maskeleyebilir. Eğer link Twitter'ın t.co adresi gibi kısaltılmış bir linkse, linki http://www.checkshorturl.com/ adresine yapıştırarak linkin gerçekte nereye gittiğini kontrol edin.

Bir epostanın oltalama saldırısı olup olmadığını doğrulamanın yollarından biri, epostayı gönderen kişiyle başka bir kanal üzerinden iletişim kurmaktır. Eğer eposta bankanız tarafından gönderilmiş gibi gözüküyorsa, bunu doğrulamak için eposta içinde yer alabilecek linklere tıklamak yerine bankanızı arayabilir ya da tarayıcınızı açıp bankanızın sitesinin adresini adres çubuğuna yazabilirsiniz.

Bazı oltalama epostaları, bir bilgisayar destek departmanından ya da teknoloji şirketinden geldiğini iddia ederek, gönderilmiş olan epostaya şifrelerinizi yazarak cevap vermenizi ya da bir "bilgisayar tamircisinin" bilgisayarınıza uzaktan erişmesini sağlamanızı ya da cihazınızdaki bir güvenlik özelliğini devre dışı bırakmanızı ya da yeni bir uygulama yüklemenizi isteyebilir. Bunun neden gerekli olduğunu açıklamak için size sözde gerekçeler sunabilirler. Örneğin eposta kutunuzun dolu olduğunu, bilgisayarınızın bozuk olduğunu ya da hacklendiğinizi iddia edebilirler. Maalesef, bu tür düzmece talimatları takip etmenin sonuçları güvenliğiniz için çok zararlıdır. İsteğin kaynağının doğru olduğundan kesinlikle emin olmadıkça, birine teknik veri verirken veya teknik talimatları takip ederken özellikle dikkatli olmaya çalışın.