CONSULTA

Siber Saldırılara Karşı 10 İpucu

1 Akıllı Cihazlarınızı ve Bilgisayarlarınızı Güncel Tutun

Bilgisayar korsanları tarafından kullanılan kötücül yazılımların kullanıcıları mağdur etmesinin en önemli sebeplerinden biri, kullandığımız cihazların ve uygulamaların güncel olmamasıdır.. Güvenlik açıkları çıktıkça üretici firmalar, bu açıklarının kapatılması için yazılım güncelleme paketleri yayınlamaktadır. Bilgisayar korsanlarının cihazlara erişmek için kullandığı bu açıkları engellemenin en önemli tedbirlerinden biri kullandığımız donanım ve yazılımların güncel olmasıdır.

2 Ücretsiz Uygulamalardan Kaçının

Bedava peynirin sadece fare kapanında olacağını unutmayın. Çok zorunda kalmadıkça Kaynağından emin olmadığınız uygulamaları, akıllı telefonlarınıza ve bilgisayarlarınıza kurmayın. Kullanımı zaruri olan uygulamalar için kurulum sonrası uygulamanın, akıllı cihazlarınız ve bilgisayarınız üzerinde erişiyor olduğu cihaz ve uygulamaları (Mikrofon, Kamera, Rehber vb) kontrol edin ve gereksiz erişimleri engelleyin. Aksi durumda yetkisiz yetkisiz erişimlere maruz kalma ihtimaliniz artacaktır.

3 Güçlü Parolalar ve Parola Yönetim Aracı Kullanın

Güçlü parolalar çevrimiçi güvenlik için kritik olduğunu unutmayın. Gerçek şu ki, parolalar bilgisayar korsanlarını verilerinizden uzak tutmak için en önemli kontroldür. Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) şifre politikası çerçevesine göre şifreleriniz, en az sekiz karakter uzunluğunda olmalı, büyük harf, küçük harf ve semboller içermelidir.

Eğer çok fazla şifreniz varsa ve bunları yönetmekte zorlanıyorsanız, işinizi kolaylaştırmak için keepass gibi şifre yönetim araçlarını şifre hesabı kasanız olarak kullanmak işinizi çok daha kolaylaştıracaktır.

4 İki Faktörlü veya Çok Faktörlü Kimlik Doğrulama Kullanın

İki faktörlü veya çok faktörlü kimlik doğrulama, standart çevrimiçi kimlik doğrulama yöntemine ek güvenlik katmanları ekleyen bir hizmettir. İki faktörlü kimlik doğrulama olmayan bir erişimde, kullanıcı adı ve şifre girerek erişim sağlayabilirsiniz. Ancak, iki faktörlü erişim yönteminde, ikinci aşamada kişisel kimlik kodu, cep telefonuna gelen bir şifre veya parmak izi gibi bir ek kimlik doğrulama yöntemi kullanmanız yabancı erişimlere karşı ekstra bir güvenlik önlemi sağlayacaktır.

5 Herkese Açık WI-FI Kullanmayın

Sanal Özel Ağ (VPN) kullanmadan herkese açık bir Wi-Fi kullanmayın. VPN kullanımı, trafiği şifreli duruma getirerek, siber saldırganın cihazınızdaki verilerinize erişme olasılığını çok daha düşük kılacaktır. Güvenliğinden şüphe duyduğunuz Açık Wİ-Fİ ağlarında mobil telefonunuz üzerinden internete erişim sağlayın.

6 Modeminizin Varsayılan Şifresini Değiştirin

Telekom ve Superonline vb İnternet hizmeti aldığımız firmalar, kablosuz modemleri size varsayılan (admin,1234 vb) şifreler ile teslim etmektedir. Bu cihazların varsayılanını tarayarak kolay bir şekilde internet trafiğinizi takip eden uygulamalar olduğunu bilin ve varsayılan olarak gelen şifreleri modeminizi kullanmaya başlamadan önce değiştirin.

Bilgi Teknolojileri Müdürü
Hakan Keçeci

7 Kimlik Avı Dolandırıcılığından Şüphe Edin

Kimlik avı dolandırıcılığı hiç olmadığı kadar revaçta . Bir kimlik avı girişiminde, saldırgan, gönderenin alıcıyı kimlik bilgilerini açıklamak, kötü amaçlı bir bağlantıyı tıklatmak veya kullanıcının sistemine kötü amaçlı yazılım, truva atı veya sıfır gün güvenlik açığından yararlanma amaçlı bir eklenti açmak için oltalama saldırıları gerçekleştirir. Bu genellikle bir fidye yazılımı saldırısına yol açar.

Kimlik avı düzenleri hakkında hatırlanması gereken birkaç önemli siber güvenlik ipucu şunları içerir:

- Tanımadığınız kişilerden gelen e-posta açmayın
- Hangi bağlantıların güvenli ve hangilerinin güvenli olmadığını bilin - nereye yönlendirildiğini keşfetmek için ilgili link üzerine gelerek bağlantının nereye yönlendiğini kontrol edin.
- Genel olarak size gönderilen e-postalardan şüphelenerek bakın. Nereden geldiğini ve gramer hataları olup olmadığını görün
- Kötü amaçlı bağlantılar enfekte olmuş bildiğiniz bir kişiden gelebilir. Her durumda dikkatli olun.

8 Hassas ve Kişisel Bilgilerinizi Koruyun

Kişisel bilgileriniz (TC, Doğum tarihi, adres vb) bir siber suçlu tarafından sizi tanımlamak veya bulmak için kullanılabilir.. Özellikle sosyal medya dünyasında çevrimiçi olarak eklediğiniz bilgiler konusunda çok dikkatli olun. Görüntülenen kişisel verilerinizi, gizlilik ayarları üzerinden tekrar gözden geçirin.. Aksi durumda bilgisayar korsanları bu bilgileri kendi yararlarına kullanıcaklardır.

9 Kurumsal ve Kişisel Şifrelerinizi Ayırın

Kişisel kullandığınız şifreleriniz ile şirketiniz için kullandığınız şifreler aynı olmamalıdır. Kişisel şifreniz ile birçok yere üye olursunuz ve bu üye olduğunuz siteler bilgisayar korsanları tarafından ele geçirildiğinde o site için kullandığınız şifre ve kullanıcı adınız kurumsal hesaplarınızda denenmektedir.

10 Verilerinizi Düzenli Olarak Yedekleyin

Fidye yazılımı veya kötü amaçlı yazılım kurbanı olursanız ya da çeşitli sebeplerden ötürü veri kaybı yaşadığınız durumda, verilerinizi geri yüklemenin tek yolu yakın zamanda gerçekleştirilen bir yedeklemeyi geri yüklemek olacağını unutmayın.