SİBER GÜVENLİK NEDİR?

Siber güvenlik; bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir. Bu terim, işletmelerden mobil bilgi işleme kadar çeşitli bağlamlarda geçerlidir ve birkaç ortak kategoriye ayrılabilir.

- **Ağ güvenliği**, hedefli saldırganlar veya fırsatçı kötü amaçlı yazılımlar olması fark etmeksizin bir bilgisayar ağını davetsiz misafirlerden koruma uygulamasıdır.

- **Uygulama güvenliği**, yazılım ve cihazların tehditlerden etkilenmemesine odaklanır. Ele geçirilmiş bir uygulama, korumak için tasarlanan verilere erişim sağlayabilir. Başarılı güvenlik, daha tasarım aşamasındayken bir program veya cihaz dağıtılmadan önce başlar.

- **Bilgi güvenliği**, hem depolama hem de aktarma sırasında verilerin bütünlüğünü ve gizliliğini korur.

- **Operasyonel güvenlik**, veri varlıklarının işlenmesi ve korunmasına ilişkin süreçleri ve kararları içerir. Kullanıcıların bir ağa erişirken sahip oldukları izinler ve verilerin nasıl ve nerede depolanabileceğini veya paylaşılabileceğini belirleyen prosedürler bu kapsama girer.

- **Olağanüstü durum kurtarma ve iş sürekliliği**, bir kuruluşun siber güvenlik olayına veya işlem ya da veri kaybına neden olan başka bir olaya nasıl yanıt verdiğini tanımlar. Olağanüstü durum kurtarma ilkeleri, kuruluşun etkinlikten öncekiyle aynı çalışma kapasitesine dönmesi için işlemlerini ve bilgilerini nasıl geri yüklediğini belirler. İş sürekliliği, belirli kaynaklar olmadan faaliyet göstermeye çalışırken kuruluşun geri çekildiği plandır.

- **Son kullanıcı eğitimi**, en öngörülemeyen siber güvenlik faktörünü ele alır: insanlar. İyi güvenlik uygulamalarına uymayan herkes yanlışlıkla güvenli başka bir sisteme virüs bulaştırabilir. Kullanıcılara şüpheli e-posta eklerini silmeyi, tanımlanmamış USB sürücüleri takmamalarını ve diğer çeşitli önemli dersleri öğretmek, herhangi bir kuruluşun güvenliği için hayati önem taşır.

Siber tehdit türleri

Siber güvenliğin karşı karşıya olduğu tehditlerin üç katmanı vardır:

1. Siber suç finansal kazanç veya işlerin kesintiye uğraması için sistemleri hedefleyen tek aktörleri veya grupları içerir.
2. Siber saldırı genellikle politik nedenli bilgi toplamayı içerir.
3. Siber terör, elektronik sistemleri panik veya korkuya neden olacak şekilde baltalamak için tasarlanır.

Peki, kötü amaçlı aktörler bilgisayar sistemlerinin kontrolünü nasıl kazanır? Siber güvenliği tehdit etmek için kullanılan bazı yaygın yöntemler şunlardır:

Kötü Amaçlı Yazılım

Kötü amaçlı yazılım, "Malware" olarak da anılır. En yaygın siber tehditlerden biri olan kötü amaçlı yazılım, bir siber suçlu veya korsanın meşru bir kullanıcının bilgisayarını bozmak veya ona zarar vermek için oluşturduğu yazılımdır. Genellikle istenmeyen bir e-posta eki veya meşru görünümlü indirme yoluyla yayılan kötü amaçlı yazılım, siber suçlular tarafından para kazanmak için veya politik nedenli siber saldırılarda kullanılabilir.

Çeşitli kötü amaçlı yazılım türleri bulunur:

Virüs: Kendi kendine çoğalan, kendini temiz dosyaya bağlayan ve bilgisayar sistemine yayılan bir programdır, kötü amaçlı kod kullanarak dosyalara bulaşır.

Truva atları: Meşru yazılım kılığındaki bir tür kötü amaçlı yazılım türüdür. Siber suçlular, kullanıcıları bilgisayarlarına Truva atları yüklemeleri için kandırırlar ve böylece bilgisayarlarına zarar verir ya da veri toplarlar.

Casus yazılım: Bir kullanıcının ne yaptığını gizlice kaydeden programdır, böylece siber suçlular bu bilgileri kullanabilir. Örneğin casus yazılım, kredi kartı bilgilerini yakalayabilir.

Fidye yazılımı: Bir fidye ödenmediği sürece kullanıcının dosya ve verilerini silmekle tehdit edip bunları kilitleyen kötü amaçlı yazılımdır.

Reklam yazılımı: Kötü amaçlı yazılım yaymak için kullanılabilen reklamcılık yazılımıdır.

Botnet'ler: Siber suçluların, kullanıcının izni olmadan çevrimiçi görevleri gerçekleştirmek için kullandıkları, kötü amaçlı yazılımın yayıldığı bilgisayar ağlarıdır.

SQL aşılama

SQL (yapılandırılmış dil sorgusu) aşılama, bir veritabanının verilerini kontrol etmek ve çalmak için kullanılan bir siber saldırı türüdür. Siber suçlular, kötü amaçlı bir SQL deyimi aracılığıyla bir veritabanına kötü amaçlı kod eklemek için veri odaklı uygulamalardaki güvenlik açıklarından yararlanırlar. Bu, veritabanında bulunan hassas bilgilere erişmelerini sağlar.

Kimlik avı

Kimlik avı, siber suçluların, hassas bilgiler isteyen ve meşru bir şirketten geliyormuş gibi görünen e-postalar kullanarak kurbanları hedef almasıdır. Kimlik avı saldırıları genellikle kredi kartı verilerini ve diğer kişisel bilgileri aktarmaları için insanları kandırma amacıyla kullanılır.

İşlemlere müdahale etmeye yönelik saldırı

İşlemlere müdahale etmeye yönelik saldırı, siber suçluların verileri çalmak için iki kişi arasındaki iletişimi alıkoyduğu bir siber tehdit türüdür. Örneğin, güvenli olmayan bir WiFi ağında bir saldırgan kurbanın cihazından ve ağdan geçirilen verileri alıkoyabilir.

Hizmeti engelleme saldırısı

Hizmeti engelleme saldırısı, siber suçluların ağları ve sunucuları trafikle boğarak bir bilgisayar sisteminin meşru istekleri yerine getirmesini engellemesidir. Bu,

sistemi kullanılamaz hale getirerek bir kuruluşun hayati işlevleri yerine getirmesini önler.

Son kullanıcı koruması

Son kullanıcı koruması veya uç nokta güvenliği, siber güvenliğin önemli bir unsurudur. Nihayetinde masaüstü bilgisayar, dizüstü bilgisayar veya mobil cihazlarına yanlışlıkla kötü amaçlı yazılım veya başka bir siber tehdit biçimini yükleyen bir bireydir (son kullanıcı).

Peki, siber güvenlik önlemleri son kullanıcıları ve sistemleri nasıl korur? Öncelikle siber güvenlik; e-postaları, dosyaları ve diğer önemli verileri şifrelemek için kriptografik protokollere dayanır. Bu yalnızca aktarılan bilgileri korumakla kalmaz aynı zamanda kayıplara veya hırsızlığa karşı koruma sağlar.

Ayrıca, son kullanıcı güvenlik yazılımları bilgisayarlardaki kötü amaçlı kod parçalarını tarar, bu kodu karantinaya alır ve ardından makineden kaldırır. Güvenlik programları, Ana Önyükleme Kaydında (MBR) gizlenen kötü amaçlı kodları bile algılayıp kaldırabilir ve bilgisayarın sabit sürücüsündeki verileri şifrelemek veya silmek için tasarlanmıştır.

Elektronik güvenlik protokolleri, gerçek zamanlı kötü amaçlı yazılım algılamasına da odaklanır. Bunların çoğu, bir programın davranışını ve kodunu izlemek için sezgisel ve davranışsal analiz kullanarak her çalıştırmada şeklini değiştiren virüslere veya Truva atlarına karşı savunmaya yardımcı olur (polimorfik ve metamorfik kötü amaçlı yazılım). Güvenlik programları, davranışlarını analiz etmek ve yeni bulaşmaları daha iyi nasıl tespit edebileceğini öğrenmek için olası kötü amaçlı programları kullanıcının ağından ayrı bir sanal balonla sınırlandırabilir.

Siber güvenlik uzmanları yeni tehditleri ve bunlarla mücadele etmenin yeni yollarını belirledikçe güvenlik programları yeni savunmalar geliştirmeye devam etmektedir. Son kullanıcı güvenlik yazılımından en iyi şekilde yararlanmak için çalışanların yazılımı nasıl kullanacakları konusunda eğitim almaları gerekir. En önemlisi bu güvenlik yazılımlarının çalışır durumda tutulması ve sık sık

güncellenmesi, kullanıcıları en güncel siber tehditlere karşı koruyabilmesini sağlar.

Siber güvenlik ipuçları: Siber saldırılara karşı kendinizi koruyun

İşletmeler ve bireyler siber tehditlere karşı nasıl korunabilir? İşte en iyi siber güvenlik ipuçlarımız:

Yazılımınızı ve işletim sisteminizi güncelleyin: Bu, en güncel güvenlik yamalarından yararlandığınız anlamına gelir.

Antivirüs yazılımı kullanın: Antivirüs yazılımları gibi güvenlik çözümleri tehditleri algılar ve kaldırır. En iyi seviyede koruma sağlamak için yazılımınızı güncel tutun.

Güçlü parolalar kullanın: Parolalarınızın kolayca tahmin edilebilir türden olmamasını sağlayın.

Bilinmeyen göndericilerden gelen e-posta eklerini açmayın: Bu eklere kötü amaçlı yazılım bulaşmış olabilir.

Bilinmeyen göndericilerden gelen e-postalardaki veya tanınmayan web sitelerindeki bağlantılara tıklamayın: Bu, kötü amaçlı yazılımların yayılmasını sağlayan yaygın bir yöntemdir.

Halka açık yerlerde güvenli olmayan WiFi ağlarını kullanmaktan kaçının: Güvenli olmayan ağlar, işlemlere müdahale etmeye yönelik saldırılara karşı sizi savunmasız bırakır.