**IT FUNDAMENTALS – SECURITY BASICS**

**Malwares**

1. MALWARES

Zararlı yazılım, kötü amaçlı yazılım veya malware (malicious software), bilgisayar ve mobil cihazların işlevlerini bozmak, kritik bilgileri toplamak, özel bilgisayar sistemlerine erişim sağlamak ve istenmeyen reklamları göstermek amacı ile kullanılan yazılımdır.

Kötü amaçlı yazılımların ilk türü, parazit (asalak) yazılım parçalarını yürütülebilir, çalışan içeriklere eklemekle ilgileniyordu. Bu yazılım parçaları, mevcut çalışan uygulamayı, sistem üstünde çalışan programları ve hatta bilgisayar sistemlerinin ayağa kaldırılmasında önemli rol oynayan önyükleme (boot) kodlarını etkileyen makine kodları olabilir.

Kötü amaçlı yazılımlar, kullanıcıların gereksinimlerine karşı bir davranış sergiler ve sistemin yetersizliğinden kaynaklanan bir sorun yüzünden istemsiz, rastgele bir şekilde verecek yazılım parçaları içermez.

Kötü amaçlı yazılımlar, uzun bir süre boyunca, bulaştığı bilgisayar sisteminin haberi olmadan bilgi toplama ve casusluk işlemlerini yapabilir. Bunun yanında, girdiği sisteme zarar verme, sabotaj etme amacı da taşıyabilir (Stuxnet gibi) veya ödemeler üstünde para sızdırma işinde kullanılabilir (CryptoLocker). 'Kötü amaçlı yazılım', bilgisayar virüsü, solucan(virüs), truva atı, fidye virüsü, casus yazılım, reklam destekli yazılım ve diğer zararlı yazılımları oluşturan gruba verilen genel isimdir. Bu yazılımlar çalıştırılabilir kod, betik, aktif içerik ve diğer farklı yazılım türleri şeklinde ortaya çıkabilir.

Kötü amaçlı yazılımlar genellikle zararsız görünen dosyaların içine gizlenir.2011 yılından itibaren solucanlar ve truva atları, aktif tehlikelerin çoğunluğunu oluşturmaktadır.

Casus yazılım ya da kötü amaçlı yazılımlar bazen şirketler tarafından sağlanan, internet sayfalarından indirilebilen yazılımlar içinde gömülü olarak bulunabilir. Bu programlar dışarıdan kullanışlı ve cezbedici gözükse bile, piyasa için istatistik araştırması yapan, kullanıcının hareketlerini gizlice izleyen parçalar içerebilir.

Anti virüs ve güvenlik duvarları, kötü amaçlı yazılımlara karşı koruma sağlamak amacı ile kullanılmaktadır.

Bazen scumware (kirli yazılım) olarak da ifade edilen kötücül yazılımlar, hemen hemen her programlama veya betik (script) dili ile yazılabilmekte ve birçok farklı dosya türü içinde taşınabilmektedirler.

Bilgisayar teknolojilerinin gelişmesi ile bilgi ve bilgisayar güvenliği konusunda en ciddi tehditlerin başında kötü amaçlı yazılımlar gelmektedir. Bu yazılımlar bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır

İnternetin yaygınlaşması ve internet reklamcılığı sektörünün gelişimine paralel olarak kötü amaçlı yazılımlar rotasını internete erişim vasıtası olan web tarayıcılarına çevirmişlerdir. Bu tip yazılımlar internet gezinimi sırasında kullanıcıyı çeşitli reklamlara yönlendirerek gelir elde etmeye çalışmaktadır.

**1. Fidye yazılımı (Ransomware)**

Fidye yazılımı dosyalarınızı kilitler ve kilidi açıp yeniden dosyalara erişebilmeniz için fidye ödemenizi ister. Size virüs bulaştığı anda hemen dosyaları silmeye başlayabilir ve size ödeme yapmanız için baskı yapabilir. Fidye yazılımlarının bilgisayarınıza erişmesinin en yaygın yollarından biri kimlik avıdır. Kimlik avı, e-posta’yı bir silah olarak kullanır, kendini meşru bir e-posta olarak gizler ve kullanıcıyı e-posta’yı veya eki açması için kandırır. Bu tür kötü amaçlı yazılımlar hızla gelişmektedir.

**2. Truva atı (Trojan)**

Bir truva atı sisteminize girip daha sonra saldırmak için kendisini güvenilir bir yazılım programı veya uygulaması olarak gizler.

**3. Solucanlar (Worms)**

Solucanlar, kendini çoğaltmak ve yaymak için bilgisayar ağı kullanan bir tür kötü amaçlı yazılımdır. Kendi kendine çoğalırlar ve virüslerin aksine bilgisayarınıza ve tüm ağa hızla yayılmak için insan eylemine ihtiyaç duymazlar. Solucanlar genellikle bir güvenlik açığı veya zayıflığı yoluyla bir bilgisayara girer.

**4. Bot**

Bot, otomatik bir bilgisayar programı olarak çalışan ve bir veya daha fazla dış kaynak tarafından kontrol edilebilen kötü amaçlı bir yazılım türüdür. Botlar, sohbet veya benzer web tabanlı programlar aracılığıyla bilgi toplamak için kullanılır. Bir bot veya botnet saldırısı düzenlemek için saldırgan genellikle bir virüs veya diğer kötü amaçlı yazılımları kullanarak bir bilgisayara erişim kazanır.

**5. Rootkit**

Rootkit nedir, diye sorarsanız; kullanıcılar veya güvenlik yazılımı programları tarafından tespit edilmeden bir bilgisayara uzaktan erişmek veya kontrol etmek için tasarlanmış kötü amaçlı bir yazılım türüdür. Siber suçlular, rootkit’leri kullanarak dosyaları yürütebilir, bilgileri çalabilir, yapılandırmaları değiştirebilir, yazılımı değiştirebilir ve hatta daha fazla kötü amaçlı yazılım yükleyebilir. Rootkit’ler yazılım uygulamalarına dahil edilebilir ve  kimlik avı saldırıları veya bir güvenlik açığı yoluyla bilgisayarınıza girebilir. Rootkit’lerin kaldırılması çok zordur, bu nedenle bu saldırıları önlemek çok önemlidir.

**6. Casus yazılım (Spyware)**

Casus yazılım, tarayıcı geçmişine ve veri toplamaya kadar kullanıcı faaliyetlerini gözetleyen kötü amaçlı bir yazılım türüdür. Genellikle güvenlik ayarlarınızı değiştirmekten ağ bağlantılarına müdahale etmeye kadar çeşitli ek yeteneklere de sahiptir. Casus yazılım, bilgisayarlara virüs veya truva atı olarak girer veya kendisini güvenilir programlarla bir araya getirir.

**7. Virüs**

Virüslerin insanlara yayılmasına benzer şekilde, bir bilgisayar virüsü de, etkinleştirilmek üzere kendisini bir programa veya uygulamaya ekleyen ve bilgisayardan bilgisayara veya tüm ağ üzerinden geçirilebilen bir yazılımdır. Bir kez bağlandıktan sonra, program her açıldığında veya çalıştırıldığında, virüs de çalışır ve diğer programlara veya belgelere bulaşabilir.

**8. Reklam destekli yazılım (Adware)**

Adware nedir, diye sorarsanız; şanslıysanız, temas kurduğunuz tek kötü amaçlı yazılım programı olmasını dileriz.

Adware son kullanıcıyı istenmediği, potansiyel olarak kötü niyetli reklamlara maruz bırakmaya çalışan reklam yazılımıdır. Yaygın bir reklam yazılımı programı, bir kullanıcının tarayıcı aramalarını, diğer ürün promosyonlarını içeren benzer web sayfalarına yönlendirebilir.

**9. Scareware**

**Scareware nedir, diye sorarsanız; kullanıcıları işe yaramaz veya zararlı yazılım satın almaları için kandıran kötü amaçlı bir yazılımdır. Sahte virüs uyarıları, yanlış yazılım güncellemeleri veya sahte kötü amaçlı yazılım temizleme araçları şeklinde olabilir.**

**Firewall**

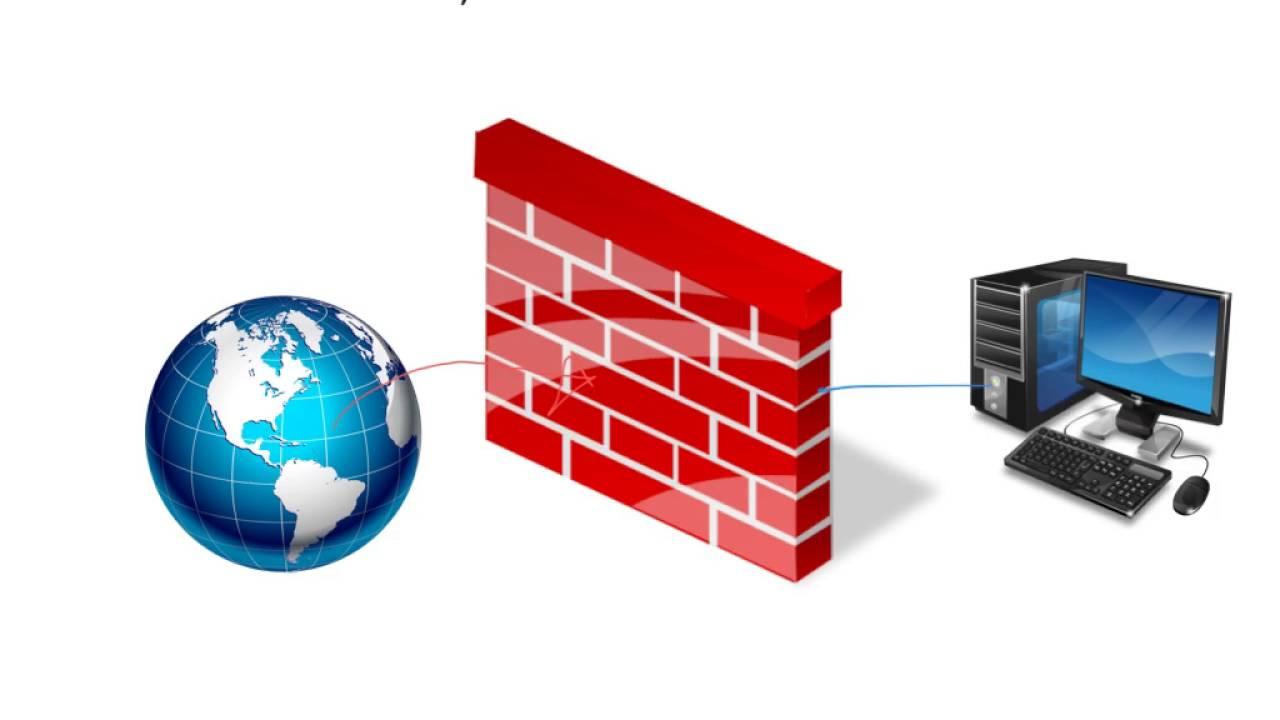
2- Firewall

Firewall nedir?

Dijital güvenlik duvarı olarak da tanımlayabileceğimiz firewall; yazılım ve donanım tabanlı olarak belirli kurallar çerçevesinde ağa gelen ve ağdan giden veri paketlerini kontrol eden bir ağ güvenlik sistemidir. Ağı kontrol ederken kullandığı filtreye bağlı olarak her daim internet trafiğini IP filtreleme, port filtreleme, web filtreleme, içerik filtreleme gibi kontrollerden geçirir.

Günümüzde işletim sistemlerinin pek çoğu kendi yazılım tabanlı firewall sistemini kullanır. Aynı zamanda ağlar arası veri aktaran yönlendiriciler de kendi firewall sistemlerine sahiptirler. İnternet ve bilgisayar kullanımının yaygınlaşması oldukça yeni bir durum olmasına rağmen firewall güvenlik sistemleri 1980’li yıllarda ortaya çıkmış bir teknolojidir.

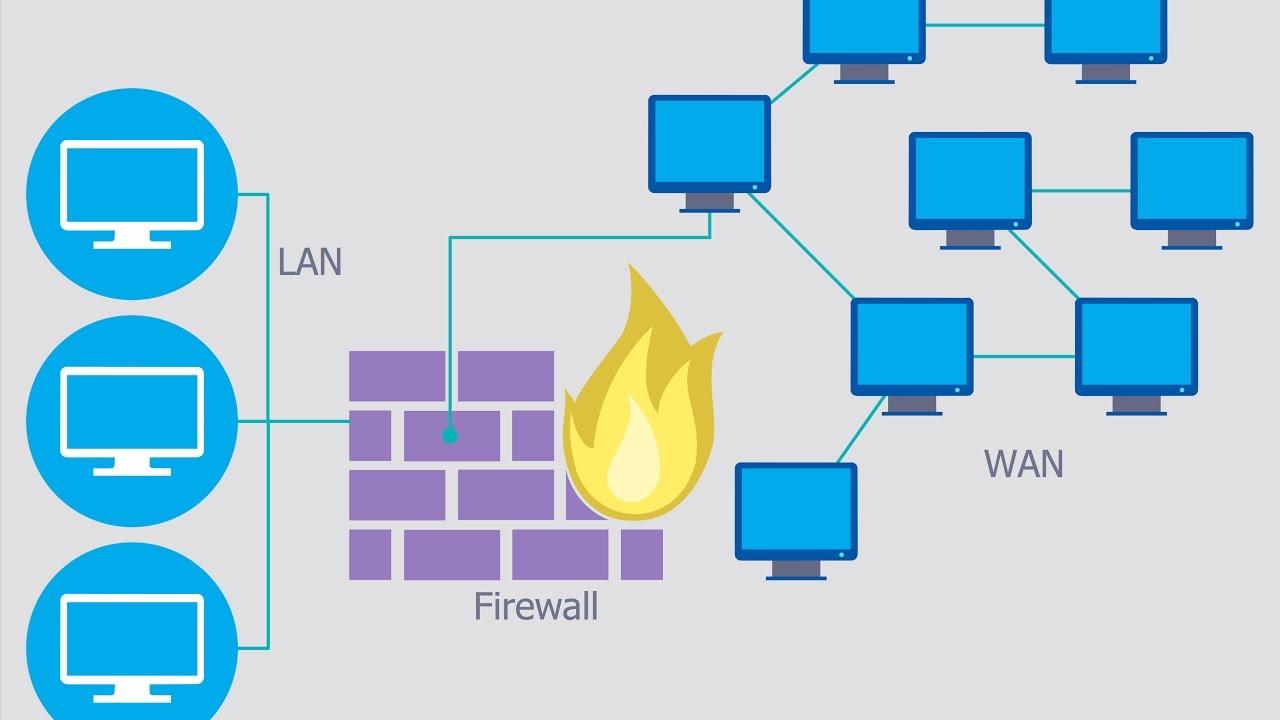
Firewall ne işe yarar?



Donanım ya da yazılım tabanları olarak çalışan firewall ağ güvenlik sistemleri önceden belirlenmiş bir filtre ile ağa gelen ve giden veri paketlerini incelerler. Güvenli olmayan kaynaklardan gelen veri paketlerini bu filtreden geçirerek olası saldırıları engellemek temel amaçtır.

Firewall ağ güvenlik sistemleri, harici cihazlar ile ağ üzerinden veri paylaşımı yapılan bağlantı noktalarında bulunurlar. "Kaynak adresi 172.18.1.1'in 22 numaralı bağlantı noktası üzerinden 172.18.2.1 hedefine ulaşmasına izin verilir." tanımı, bu dijital güvenlik duvarlarının yaptığı işi en doğru şekilde anlatmaktadır.

Firewall nasıl çalışır?



Firewall ağ güvenlik sistemlerinin nasıl çalıştığını anlamak için bir örnek üzerinden gidelim; IP adreslerini evler, port numaralarını ise odalar olarak düşünelim. Eve yalnızca güvenli kişiler yani güvenli kaynak adresleri girebilir. Eve giren kişiler bir filtreden daha geçerek yalnızca belirli odalara yani bağlantı noktalarına ulaşabilirler. Yani firewall filtresi birden çok noktada kontrol ve denetleme sağlar.

**Eski tip paket filtrelemeli firewall güvenlik ağ sistemleri bu konuda biraz zayıftı. Temel bir filtre üzerinden veri paketlerini kontrol ediyor ve bazen güvenilir kaynaktan gelen isteği direkt olarak kabul ediyorlardı. Zaman içinde güvenilir bir kaynaktan gelen her isteğin iyi niyetli olmadığı anlaşılınca firewall ağ güvenlik sistemleri de geliştirilerek farklı türler ortaya çıktı.**

VPN

3-VPN

İnternette daha özgür dolaşmak, bazı sınırlı servislere daha rahat ulaşmak için VPN servislerini kullanmak gerekiyor. Peki en iyi VPN servisleri hangileri, VPN nasıl kullanılır, VPN nasıl kurulur? Gelin bu soruların cevaplarına birlikte bakalım.

VPN, erişim engeli bulunan sitelere ulaşmak için en yaygın çözüm. Ayrıca yasal olarak VPN kullanmak suç sayılmıyor. Böyle bir kolaylık için pek çok firma, farklı VPN uygulamalarıyla hizmet veriyor. Bugün hep birlikte en iyi VPN uygulamalarına yakından bakıyor, VPN’e dair aklınızdaki tüm soruları gideriyoruz.

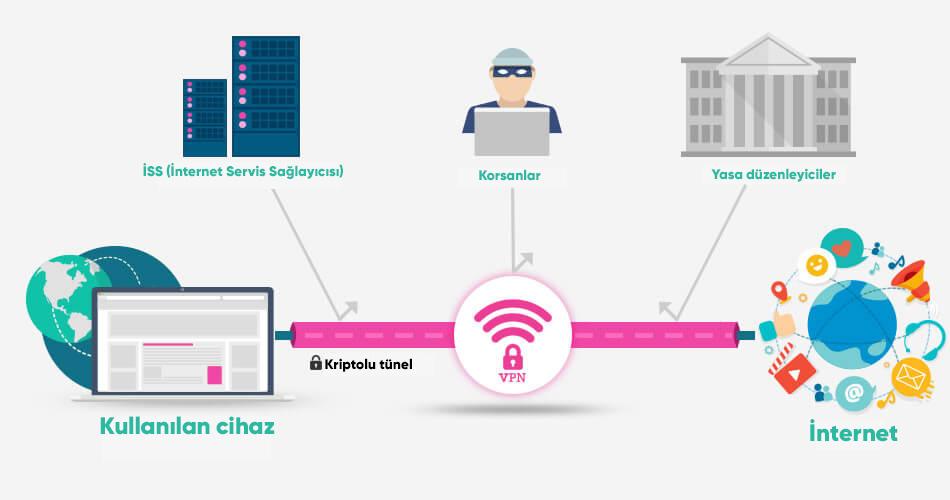
Peki VPN nedir, nasıl kullanılır, Android, iOS, Google Chrome dahil kullanabileceğiniz en iyi VPN servisleri hangileri, sizin için her şeyi baştan sona anlattık.

VPN nedir?



İngilizce olarak Virtual Private Network, Türkçesiyle Sanal Özel Ağ anlamına geliyor. VPN’in temel amacı, fiziksel olarak bulunmadığınız bir yerdeki ağa sizi uzaktan bağlamaktır. Aslında temel amaç daha güvenli bir iletişim yolu sağlayarak kurumsal çözümler sunmaktır. Ancak bu sırada mevcut fiziksel konum dışından bağlanmak mümkün olduğu için, engelli sitelere erişim için de VPN kullanmak mümkün oluyor. Yani tıpkı DNS servislerinde olduğu gibi...

VPN nasıl çalışır?



VPN, internete bağlandığınız cihazı sanal olarak farklı bir konumda gösterir. Bunun için karşıdaki ağa kriptolu bir tünel açar. Aktarılan bilgiler bu tünelden karşılıklı olarak paylaşılır. Yani örneğin Vikipedi’ye VPN üzerinden bağlanırsanız, cihazınız ve bağlandığını VPN ağı (Örneğin: Kanada) arasında veri akışı olur. Bu akış kriptolu olduğu için dışarıdan görüntülenemez. Böylece trafik Kanada üzerinden gerçekleşir, Kanada’nın ağ usüllerine göre internette dolaşırsınız.

VPN yazılımları ya da mobil uygulamaları bu özel tünele erişmeniz için bir ağ sürücüsü kurar. Sanal bir ağ bağdaştırıcısı gibi davranan bu yazılım size bağlanmak istediğiniz ağdan bir IP adresi verir. IP adresi bir bakıma bağlantınızın kimlik numarasıdır. Bu adres otomatik olarak hedeflediğiniz ağ üzerinden internet sitelerine erişmenizi sağlar.

Temel olarak 3 çeşit VPN bulunur:

* Evdeki bilgisayardan ofisteki kurumsal özel ağlara bağlantı kurulan VPN’ler. Bunlar özeldir, şirketlere ya da kurumlara özel olarak kurulabilir.  (Örn: SEÇSİS - YSK)
* Tüm trafiği toplu şekilde alıp farklı bir konumdan bağlantı kuran VPN’ler. Genelde başka ülke üzerinden internete erişim imkanı sunarlar. Kamuya açıktır. Güven riski yüksektir. En yaygın VPN türüdür; saldırılara, bilgi sızıntılarına açıktır.
* Oyunlarda “ping” adı verilen yanıt sürelerini hızlandırmak için kullanılan özel VPN’ler. Oyunlara özeldir.

VPN nasıl kullanılır?



VPN, amacınıza göre farklı kullanım seçeneklerine sahiptir. Eğer engelli sitelere erişim için VPN kullanmak istiyorsanız, kamuya açık olan VPN ağlarına, yani 2 tür VPN servislerine erişmeniz gerekmektedir. (Kurumsal sistemlere erişim amacıyla VPN kullanmak için şirketteki IT sorumlularına danışabilirsiniz.)

VPN kullanmak için iki seçeneğiniz bulunmaktadır. Birincisi ücretli hizmetlerden satın almak ki daha güvenlidir, ikincisi ücretsiz yazılım ya da uygulamaları kullanmak. Eğer teknik kabiliyete sahipseniz, cihazınızın ağ ayarlarından manuel olarak VPN kurulumu yapabilirsiniz. Ancak burada bağlandığınız ağı hızlıca değiştirmeniz mümkün değildir. Dolayısıyla güvensiz bir ağa manuel olarak bağlanmak, kişisel verilerinizi tehlikeye düşürecektir.