Bilgisayar nasıl güvenli hale gelir? Bilgisayarı nasıl daha güvenli kullanabiliriz? (Introduction)

Anti virüs programları: Bilgisayar zararlılarına karşı yazılmış, tespit etme, temizleme, kurtarma işlemlerini yerine getiren koruyucu programlara verilen genel isimdir.

Güvenlik duvarları (Firewall): Ağ ve bilgisayar sistemleri arasındaki güvenliği sağlayan yazılım ve donanımsal sistemlerdir. Ağınıza gelen ve ağınızdan çıkan trafiği belirli kurallar çerçevesinde denetleyen ve bu trafiğin akışını sağlayan güvenlik sistemine "firewall" denir.

Sızma tespit sistemleri/testleri (penetration test): insan odaklı bir güvenlik açığı tespit sürecidir ve işletmelerin siber zayıflıkları tespit etmek için kullandığı birincil yöntemdir. Bir pentest, ağlarınızdaki ve sistemlerinizdeki savunmasız noktaları bulmak ve ortaya çıkarmak için sisteminize karşı simüle edilmiş bir siber saldırının başlatılmasını içerir.

Yukarıda sayılan programların en iyileri ve güncelleri de yüklenmiş olsa eğer bilgisayar kullanıcısı bilinçsiz ise siber saldırılar kaçınılmazdır ve başarılı olmuş siber saldırıların birçoğu sistem açığından değil, kullanıcı hatasından dolayı gerçekleşmiştir. Güvenlik kendisini oluşturan halkalardan en zayıfı kadar güçlüdür ve güvenlik alanında kabul görmüş ilkelerden biri de insanın en zayıf halka olduğudur.

Çözüm(!):

- Network bağlantısını kapatın
- Bilgisayarın fişini çekin
- Pilini çıkarın
- Sabit diske 5 adet çivi çakın

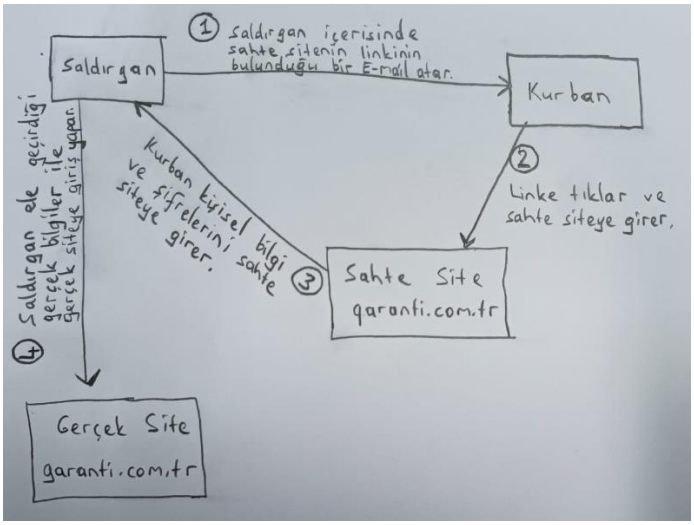
GÖREV İÇIN GÜVENLIK GÜVENLIK İÇIN GÖREV İHMAL EDILEMEZ.

İkisi bir birinin alternatifi değildir.

➢ **Dikkatli Olun**

Bilgisayar sistemlerini kullanırken, elektronik cihazları kullanırken dikkatli olun.

- Kimin gönderdiğini bilmediğiniz e-postları açmayın.
- Sizinle ilgisi olmayacak e-postaları açmayın.
- Açtıysanız içerisindeki linke tıklamayın ve ekteki dosyayı açmayın (oltalama saldırısı - phishing attack).



Şekil 1. Oltalama saldırısı anlatım.

- İnternette rasgele yerlerden rastgele yazılımlar yüklemeyin. İhtiyacınız olan ilgi çekici yazılımlar casus yazılımlar ile paketlenmiş olabilir (trojen horse, spyware, backdoor, botnet, …).

➢ **Güncellemeleri Yükleyin ve En Son Yazılımları Kullanın (Updates)**

İşletim sisteminizi ve kullandığınız yazılımları güncel tuttuğunuzdan emin olun.

- Windows güncellemelerini açın ve güncelleme yapmasına izin verin.
- Kullandığınız yazılımın en son sürümünü kullandığınızdan emin olun. Çünkü yazılım güncellemeleri genellikle hatalar ve güvenlik açıkları ile ilgili düzeltmeler içerir.
- Antivirüs yazılımlarının veri tabanlarını güncel tutun.
- İşletim sistemindeki ve kullanıcı programlarındaki bütün açıklıkları kapatmak zorundasınız. Siber güvenliğe defansif yönden bakarsanız duvardaki bütün delikleri kapatmanız gerekir eğer saldırgan gözü ile bakarsanız duvardaki tek açıklık başarı için yeterlidir.

➢ **Şifreler (Passwords)**

Kullandığınız hizmete uygun düzeyde şifreler belirleyin.

- Basit şifre kurmayın (rakam, küçük harf, büyük harf, noktalama işareti, özel karakter kullanın). Şifre kırma algoritmaları genellikle ya brute force çalışır veya şifre listesi kullanarak çalışır.
- Aynı şifreyi birden fazla platformda kullanmayın.
- Şifreleri veya hesapları başkaları ile paylaşmayın.
- Şifreleri yönetmek için şifre yönetim araçlarını kullanın (1Password, Keepass, Lastpass vb.).

TOP 10 MOST COMMON PASSWORDS IN 2022

Rank	Password	Time to crack it
1	password	< 1 Second
2	123456	< 1 Second
3	123456789	< 1 Second
4	guest	10 Seconds
5	qwerty	< 1 Second
6	12345678	< 1 Second
7	111111	< 1 Second
8	12345	< 1 Second
9	col123456	11 Seconds
10	123123	< 1 Second

Şekil 2. 2022 yılında en çok kullanılan şifreler.

➢ **Şifre Kurtarma Soruları**

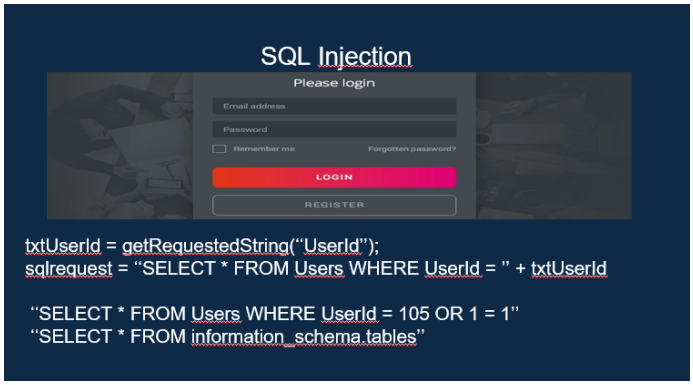
Şifre kurtarma sorularına düz mantık cevaplar vermeyin. Yani doğru veya yanlış sorunun cevabı olabilecek bir yanıt vermeyin.

- Tarihteki en önemli kişilik kimdir? Atatürk, Fatih Sultan Mehmet ✖
- En sevdiğiniz yemek hangisidir? Makarna ✖
- İlk okul öğretmeninizin adı nedir? İzmir ✓

➢ **İki Aşamalı Kimlik Doğrulama (Two Step Verification/Two Factor Authentication)**

Herhangi bir hesapta oturum açarken ikinci bir doğrulamayı kullanın. Böylece brute force, Sql injection, oltalama gibi bir çok saldırıya karşı korunmuş olursunuz.

- Kullanıcı adı – Şifre, Sms, desen çizimi, email vb.



Şekil 3. SQL injection için örnek sorgular.

Saldırgan, kullanıcıdan bir bilgi girilmesi gereken form nesnelerine sql sorguları girip sonuçlarını ister.

Bu sorgular için tablo isimleri gerekmektedir. Tablo isimlerini de şekilde görüldüğü gibi "SELECT * FROM information_schema.tables" komutu ile bulabilmektedir.

Yazılımcı önlem alır; sql sorgularının anahtar kelimelerinin kontrolü yapılabilir, bu tür kelimeler içeren kullanıcı isimlerine izin verilmez. Ayrıca önlem için stored procedure kullanılabilir yani sql sorgusu veri tabanının içerisinde çalıştırılır.

➢ **Şifreleme (Encryption)**

Bilgisayarınızı, diskiniz, dosyalarınızı ve gönderilen mesajlarınızı şifreleyin.

- İnternete açılırken güvenli protocol ve kanalları kullanın. (http → https).
- Önemli içeriğe sahip dosyalarınızı şifreleyin.

➢ **Yedekleme (Backup)**

Zararlı yazılımlar sistemlere, veri tabanlarına ve dosyalara geri dönülemez zararlar verebilirler. Dolayısı ile sürekli yedekli çalışmak gerekir.

- Periyodik aralıklar ile system geri yükleme noktası oluşturun. Sistem kurtarma diski oluşturun.
- Üzerinde çalıştığınız önemli bir dosyada çalışmalarınıza yedekleyerek devam edin (e-mail, USB disk, Bulut sistemler ile senkron çalışılabilir (google drive, one drive, dropbox)).

- **Mobil Cihazlar (Mobile Devices)**

Bir uygulamayı yüklemeden önce istediği izinlere dikkat edin ve uygulamanın bu izinleri istiyor olmasının makul olup olmadığını düşünün.

- Bir telefon rehberi uygulamasının network'e açılma izni istemiyor olması gerekir.
- Bir oyun programının telefon rehberine erişim izni istemiyor olması gerekir.
- Görüşme yapma izni, SMS okuma gönderme izni, lokasyon bilgisi, dosyalara erişim izni (foto, video)…

- **Yaygınlığı Az Olan Yazılımları Kullanın (Less Common Softwares)**

Çok talep gören ve kullanılan yazılımlar saldırganlar tarafından daha çok hedeflenen yazılımlardır. Saldırganlar daha çok büyük bir kitleye saldırmayı hedeflerler.

- Internet tarayıcı olarak Internet Explorer ve Chrome yerine daha az kullanılan bir yazılım tercih edilebilir.
- İşletim sistemi olarak Windows yerine Linux tercih edilebilir.

- **Antivirüs Programları (Antivirus Programs)**

Güncel bir antivirus programı kullanıp sağladığı bütün özellikleri açın.

- **Yönetici Hakları/İzinleri (Administrator Rights/Permissions)**

Güvenmediğiniz, üreticisi belli olmayan programları yönetici izni ile çalıştırmayın. Bir programı yönetici olarak çalıtırdığınızda program yönetici haklarına sahip olacağından kötü amaçlı yazılım etkinliklerini daha kolay gerçekleştrebilir.

- **Sanal Makine (Virtual Machine)**

Sanal makineler aslında üçüncü parti bir kullanıcı yazılımı. Tek farkları sanki sıfır bir makine gibi üzerine herhangi bir işletim sitemini kurabiliyoruz. Bilgisayarı ve içindekileri tehlikeye atabilecek bir işlem yapacaksanız sanal makine üzerinde yapabilirsiniz. İşiniz bittiğinde sanal makineyi silebilir veya sıfırlayabilirsiniz.

- Vmware, Fusion, Workstation etc.