Türkiye'nin en yaygın 10 güvenlik sorunu

E-güvenlik firması InfoNet'in InfoSecure Güvenlik Denetim ve Danışmanlık Ekibi, incelediği kurumsal bilgisayar ağlarında karşılaştığı 10 temel güvenlik zaafını açıkladı. En sık rastlanan e-güvenlik sorunları şöyle sıralanıyor:

1. İşletim Sistemleri ve Uygulamaların Varsayılan Ayarlarla Kurulması: Birçok yazılım, standart bir kurulum tarif eden programlar ile birlikte geliyor. Bunun için, kurulum sırasında ürünün çoğu zaman kullanıcının da onayını almadan, birçok kimsenin ihtiyaç duyduğundan daha fazla özelliği çalışır hale getiriliyor. Bu yaklaşım, kullanım kolaylığı için faydalı görünse de, birçok tehlikeli güvenlik açığına da yol açıyor çünkü sistemde gereksiz yere açık kapı bırakılmış oluyor. Saldırganlar sistemlere bu gereksiz bağlantı noktalarını kullanarak sızıyor.

2. Şifresi Olmayan Kullanıcı Hesapları veya Zayıf Şifreler: Tahmin edilmesi kolay şifreler veya standart kurulumla gelen standart şifreler büyük bir problem. Ancak hiç şifresi olmayan kullanıcı hesapları daha büyük bir problem teşkil ediyor. Zayıf şifrelerin, standart kurulum şifrelerinin veya hiç şifresi olmayan kullanıcı hesaplarının hepsinin temizlenmesi gerekiyor.

3. Yedeklemenin Yeterli Olmaması veya Hiç Yedekleme Yapılmaması: Bazı kurum ve kuruluşlar günlük yedekler alıyor, ancak yedeklerin gerektiğinde işe yarayıp yaramayacağını kontrol etmiyorlar. Bazı kuruluşlar da yedekleme için politika ve prosedürler oluşturmakla beraber bu yedeklerden sistemin yeniden kurulması konusu ile hiç ilgilenmiyor. Oysa bir sistem çökmesi sonucunda en çok ihtiyaç duyulan şey bu yedekler oluyor.

4. Gereksiz Ağ Bağlantı Noktalarının Kullanımda Olması: Sistem kullanıcıları da, saldırganlar da sistemlere açık ağ bağlantı noktalarından (port) erişerek bağlanıyorlar. Ne kadar çok bağlantı noktası kullanıma açıksa sisteme de o kadar değişik kapıdan girilebiliyor. Sisteme erişim için minimum sayıda bağlantı noktasının açık bırakılması çok önemli bir husus.

5. Ağ Trafiğinde Doğru Adresler Dışındaki Veri Paketlerinin Filtrelenmemesi: Başka bir Internet adresinden geliyormuş gibi görünmek, birçok saldırganın kendilerini gizlemek için kullandığı bir yöntem. Örneğin, çok yaygın olan smurf saldırısı, yönlendiricilerin bir özelliğini kullanarak bir dizi veri paketini binlerce makineye göndermek suretiyle gerçekleştiriliyor. Sisteme gelen ve sistemden çıkan trafik üzerinde filtreleme yapılması ise böyle durumlara karşı önemli bir güvenlik ve koruma sağlayabiliyor.

6. Yetersiz Sistem Kaydı Tutulması veya Hiç Sistem Kaydı Tutulmaması: Saldırı ve sızmaların tespit edilmesi de üzerinde hassasiyetle durulması gerekli bir konu haline geldi. Bir bilgisayar sistemi internet'e bağlı olan veya olmayan bir bilgisayar ağı içerdiği sürece güvenlik problemleri yaşanabiliyor. Bir saldırıya uğranıldığında, eğer sistem yeterli kayıt tutmuyorsa, saldırganların neler yaptığını tespit etmek çok zorlaşıyor, hatta olanaksız hale geliyor. Sistem kayıtları ve saldırı tespit sistemleri, ağ üzerindeki hareketi sürekli izlemeyi sağlıyor. Ayrıca hangi sistemlere saldırıldığı ve hangi sistemlere sızıldığı da sistem kayıtlarından saptanabiliyor.

7. Güvenlik Açığı Bulunan CGI ve ASP Programlarının Kullanımı: Pek çok web sunucusu, CGI ve ASP programlarını destekliyor. Bu programlarla web sayfaları üzerinden veri toplanması ve doğrulanması gibi temel bazı işlemler yapılabiliyor. Ancak, bu programların birçoğu sadece örnek teşkil etmek amacıyla hazırlandıklarından internet üzerinden erişen kullanıcıların doğrudan işletim seviyesi sistemine erişim sağlamalarına izin verebiliyor.

8. Güvenliğin Denetlenmemesi: Birçok kuruluşta o güne kadar herhangi bir güvenlik kaybı yaşanmadığı düşünüldüğü için güvenliğe ilişkin bir problem olmadığına inanılıyor. Oysa o güne kadar bir güvenlik saldırısına maruz kalınmaması e-güvenliğin sağlam olduğuna değil, sadece o firmanın şanslı olduğuna işaret ediyor. Bu tür yanlış bir kanı, savunma kalkanlarının indirilmesine neden olabileceği için firmaları büyük risk altına sokabiliyor.

9. Güvenlik Politikası ve Prosedürlerinin Bulunmaması: Güvenliğin mutlaka bir bütün olarak ele alınması, teknik güvenlikten, fiziksel erişim güvenliğine, sözleşme güvenliğinden çalışanlarla yapılan iş akitlerine kadar ayrıntılı olarak düşünülmesi şart. Güvenlik politikası olmayan firmaların karşı karşıya bulunduğu risk, diğerlerine göre daha büyük.

10. Güvenlik ile İlgili Yeterli Kaynağın Ayrılmaması: Bilgisayar ağları giderek karmaşıklaşıyor. Günlük işleyiş sırasında sürekli ortaya çıkan yeni güvenlik açıkları ve tehlikeler karşısında gerekli teknoloji yatırımlarının yapılması ve güvenlik denetimleri ile güvenlik seviyesinin sürekli olarak yüksek seviyede tutulması gerekiyor. Ancak mevcut durumda, en sık rastlanan idari sorun, bilgi işlem bütçesinde bilişim güvenliğine yeterli pay ayrılmaması olarak ortaya çıkıyor. Kaynak sıkıntısı ise güvenlik tedbirlerinden fedakarlık yapılmasına yol açıyor.

InfoSecure güvenlik uzmanları e-güvenliğin dinamik bir süreç olduğunun unutulmamasını ve satın alınan bir antivirüs yazılımı ya da güvenlik duvarıyla e-güvenlik şemsiyesi altına girilemeyeceğinin altını önemle çiziyor.