12. HAFTA

TBT182

TEMEL BİLGİSAYAR BİLİMLERİ

Yrd. Doç. Dr. Şafak BAYIR

safakbayir@karabuk.edu.tr

KBÜ-UZEM
Karabük Üniversitesi
Uzaktan Eğitim Uygulama ve Araştırma Merkezi

12. Haftanın Konuları (İçerik)

Bilgisayar ve Veri Güvenliği

Temel Kavramlar

Veri güvenliği, disk, iletişim ağı, yedekleme ünitesi ya da başka bir yerde tutulan verilerin, programların ve her türlü bilginin korunmasını ifade eder.

Bu koruma sadece tek bir yönde düşünülmemelidir.

Veri güvenliğinin 3 ana boyutu vardır.

Fiziksel güvenlik; çalınma, düşme gibi dış etkenlerden dolayı hasar görme risklerini kapsar.

Bilgisayar güvenliği ile, bilgisayara fiziksel olarak erişen yerel kullanıcıların yetki denetimlerinden, sistem arızalarına kadar uzanana geniş bir koruma perspektifini ifade eder.

İletişim güvenliği ise, ister yerel ağ düzeyinde, ister internet düzeyinde olsun bilgisayarlar arası iletişimden doğan tehditler ile ilgilenir.

Tehdit Sınıflandırmaları

Bilgisayarlara yönelik tehditler, kaynaklarına ve türlerine göre sınıflandırılabilir.

Tehditlerin kaynağı, teknik saldırılar, kötü niyetli kişi saldırıları, sistem hataları veya yangın, su baskını, terör gibi dış etkenler olabilir.

Tehdit türleri ise para hırsızlığı, yazılıma zarar verilmesi, bilgi çalınması, bilgiye zarar verilmesi, servislerin izinsiz kullanılması, zarar vermeden güvenlik ihlali ve sistemlerin kısmen veya tamamen devre dışı kalması olarak sayılabilir.

Bazı tehditlerin bu açıdan önemsiz olarak değerlendirilmesi ise büyük bir hata olacaktır.

Zarar vermeden güvenlik ihlali yapılan bir sistem, aynı zamanda her türlü hasara da açık demektir.

Ayrıca sistemlerin kısmen veya tamamen devre dışı kalması, çok ciddi zaman maliyetlerine sebep olabilir.

Saldırı Yöntemleri

Günümüzde bilgisayara yönelik saldırıların çok sayıda türü vardır.

En yaygın saldırı türü, virüsler, solucanlar ve truva atları gibi kötü amaçlı yazılımlardır.

Bir sonraki önemli tehdit yazılım açıkları ve arka kapılardır.

DoS saldırıları ile sistemi aşırı yükle bloke etme…

Somut hasar hedefleri olan mantıksal bombalar…

Phishing saldırıları…

IP spoofing saldırıları…

Host dosyasının çalınması…

Sosyal mühendislik ile aldatılma…

Mesajlaşma yazılımları ve internet trafiğinin izlenmesi…

Ve şifre kırma sistemleri, diğer saldırı yöntemleri olarak sayılabilir.

Korunma Yöntemleri

Bilgisayara yönelik saldırılar ve tehditler karşısında, elbette çok sayıda da korunma yöntemi söz konusudur.

Kimlik doğrulaması, güvenlik yazılımları, yazılım güncellemeleri, verilerin yedeklemesi, veri erişim izinleri, verilerin şifrelenmesi ve güvenli silme bu kapsamda ele alınacak başlıklardır.

Ancak kullanıcının eğitimi, saldırılara karşı korunmada en iyi yöntemdir.

Kimlik Doğrulaması ve Şifreler

Kimlik doğrulamasında en yaygın yöntem şifrelerdir.

Şifreler belirli bir kullanıcı adına bağlı olarak girilebileceği gibi, kullanıcı adı olmaksızın sadece şifre ile koruma sağlayan sistemler de vardır.

Kimlik doğrulamasının işe yaraması, yani güvenlik sağlaması için, güçlü bir şifrenin oluşturulması ve bu şifrenin iyi korunması zorunludur.

Dünyada aşılması “imkansız” bir şifre yoktur.

Ancak aşılması imkansıza yakın derecede zor olan şifreler vardır.

Şifre Oluştururken Dikkat Edilecekler

Şifre oluştururken dikkat etmeniz gereken çok önemli detaylar vardır.

Öncelikle şifrelerinizde kesinlikle kişisel bilgilerinizi kullanmayın.

Sizi az da olsa tanıyan bir kişinin bile tahmin edemeyeceği şifrelerler üretin.

Hatta mümkünse şifrelerinizin anlamlı bir dizilimi olmasın.

Mümkün olduğu kadar harf, rakam ve diğer sembolleri bir arada kullanın.

Klavyeden basılabilecek özel karakterleri araya alın.

Ardışık veya klavye dizlimi kolay şifreleri asla kullanmayın.

Şifresi 123456 ve qwerty olan binlerce kullanıcı bulabilirsiniz.

Şifreleriniz çok kısa tutmayın; en az 6 veya 8 basamaklı şifreler kullanın.

Şifreleri Korumak

Güvenli bir şifre oluşturmak kadar, onu korumak da önemlidir.

Şifrenizi kesinlikle anlık mesajlaşma yazılımlarından göndermeyin.

Düzenli aralıklarla şifrenizi değiştirmeyi unutmayın.

Her yere aynı şifreyi kullanmayın; daha az güvenli bir siteye üye olduğunuz zaman, sakın mail adresinizin şifresini girmeyin.

Eğer site e-posta adresleriniz ile şifrelerinizi açık bir şekilde saklıyor ise, mail hesabınızın bilgilerini ellerinizle teslim etmiş olabilirsiniz.

Bilgisayarınızda bir metin dosyasında veya şifresiz bir Word belgesinde şifrelerinizi sakın kaydetmeyin.

Şifrelerinizi saklamak için şifreli Word veya Excel dosyalarını kullanın ve bu dosyalara alakasız isimler verin.

En güzel, mümkünse şifrelerinizi bilgisayar ortamında depolamayın.

BIOS Şifreleri

Bilgisayara koyabileceğiniz ilk şifreler BIOS şifreleridir.

Çoğu BIOS yazılımında, BIOS ayarlarını değiştirebilmek ve bilgisayarı açmak için 2 ayrı şifre belirlenebilmektedir.

Bu şifreler fiziksel erişim imkanı bulunan kişiler için anlamlıdır.

Yani bu şifreler herhangi bir ağ veya internet güvenliği sunmaz.

Ayrıca yetkisiz kişi sistem kasasını açabilecek durumda olursa, BIOS şifrelerini geçersiz kılması son derece kolaydır.

Buradaki koruma, çok güçlü bir güvenlik sağlamasa da, basit şekilde erişimlerin önünün kesmekte idealdir.

DriveLock Denetimi Şifresi

DriveLock denetimi ise, özellikle taşınabilir bilgisayarlarda kullanılan bir sistemdir.

Etkinleştirilmesi durumunda, bilgisayarın önyüklemesi sırasında kullanıcının hard disk için şifre girmesi istenir.

Yanlış şifre girilirse sürücü kilitlenir ve önyükleme yapılamaz.

Bu koruma, özellikle bilgisayarın çalınması durumunda kritik verilerinizin güvenliği açısından önemlidir.

Eğer bilgisayarın bu özelliği varsa, bu da BIOS üzerinden yapılandırılır.

Windows Kullanıcı Hesabı Şifreleri

Windows erişimi için bir kullanıcı hesabı adı ve şifresi gereklidir.

Kullanıcı hesabı şifresi sadece oturum denetimi sunar; verileri şifrelemez.

Eğer kullanıcı isterse, kullanıcı hesabını şifresiz olarak da kullanılabilir; ancak bu ciddi bir güvenlik açığı kabul edilir.

Aynı zamanda bazı ağ servisleri de, şifresiz hesaplarla çalışmayacaktır.

Denetim masası, yönetimsel araçlar dizininde bulunan yerel güvenlik ilkelerinden, kullanıcı hesabı parolalarının tabi olacağı kurallar değiştirilebilir.

Buradan en kısa parola limiti koyabilir, parolanın maksimum ve minimum geçerlilik süresini belirleyebilirsiniz.

Tekrar kullanım limiti ise, geçişte kullandığınız parolayı tekrar kullanmanız için arada değiştirmeniz gereken parola sayısını ifade eder.

Karmaşıklık derecesini zorunlu tutarsanız, parolalarda harf ve rakamın bir arada kullanılması gibi zorunluluklar aranır.

Windows normalde parolaları geri dönüştürülemez şekilde kaydeder.

Ancak kullanıcı isterse, özel durumlar için parolaların ters çevrilebilir şifrelemeler ile depolamasına da izin verebilir.

Windows Şifrelerinin Sınırları

Windows kullanıcı hesaplarının şifrelenmesi sadece oturum denetimi sunduğunu, sabit disk üzerinde bulunan verileri ise şifrelemediğini söylemiştik.

Bu sebeple, Windows hesabına şifre koysanız dahi, sabit diskiniz başka bir PC'ye takıldığında bu şifre bir anlam ifade etmeyecektir.

Ayrıca bilgisayarı CD sürücüsünden başlatma imkanı olan bir kişi, özel bir yazılım ile Windows kullanıcı hesabı şifresinin üzerine yazabilir, şifreyi silebilir veya yedekleyebilir.

Yapamayacağı tek şey, şifrenin ne olduğunu öğrenmektir.

Size fark ettirmeden güvenliğinizi aşmaya çalışan bir kişi, öncelikle oturum şifrenizi bir flash bellek veya diskete yedekleyebilir.

Daha sonra şifreyi silip oturumunuzu açar; işini bitirdikten sonra da yedeklediğin şifreyi geri yükler.

Bu sayede siz birisinin sisteminize girdiğini hiçbir şekilde anlamayabilirsiniz.

Bu yazılım aracının tek iyi tarafı, şifresi kaybolmuş sistemlerde kurtarma amaçlı olarak kullanabilmesidir.

Kullanıcılar, Windows şifrelerinin sınırlanırını iyi bilmelidir; kendisini sonsuz güvende hissetmek olabilecek en yanlış şeydir.

Windows Kullanıcı Hesaplarını Yönetme

Her Windows sürümü denetim masasında farklı bir kullanıcı hesabı yönetimi sunar.

Bilgisayar yönetimi ekranındaki kullanıcı hesabı yönetimi ise her sürüm için aynıdır; daha tutarlıdır ve eksiksizdir.

Kullanıcı hesaplarının şifrelerini sıfırlamak ve hesapları aktif veya pasif duruma getirmek için bu ekranları kullanın.

Bu ekranda kullanıcı yönetiminin yanında grup yönetimi olduğunu göreceksiniz.

Kullanıcı yetkilerinin üye oldukları kullanıcı gruplarına bağlı olduğunu unutmayın.

Güvenliği Etkileyen Oturum Açma Davranışları

Bilgisayarın kullanım yeri ve özelliklerine göre Windows'ta oturum açma davranışları biçimlendirmek oturum güvenliğinin sağlanmasına yardımcı olacaktır.

Karşılama ekranı veya klasik oturum ekranı kullanma tercihini, denetim masasındaki kullanıcı hesaplarından yapabilirsiniz.

Karşılama ekranı kullanılırsa, sistemdeki olası tüm kullanıcı isimleri görünecektir. Doğal olarak bu şartlara göre güvenlik açığı olarak kabul edilebilir.

Hızlı kullanıcı geçişini kapatmak da bir güvenlik önlemli olabilir.

Eğer bu geçişi kapatırsanız sizin hesabınız kapatılmadan diğer bir hesap ile oturum açılamayacaktır.

Öğlen arasında kilitli bıraktığınız bilgisayarı geldiğinizde aynı konumda bulamazsanız, birilerinin sisteminizde oturum açtığından şüphelenebilirsiniz.

Ctrl+Alt+Del zorunluluğu getirmek, klavye tuşlarının kontrolsüz biçimde oturum açma denemesi yapmasını engelleyecektir.

Guest ve diğer gereksiz hesapların devre dışı bırakılması ve geçersiz oturum açma denemelerinin sayısının ayarlanması da önemlidir.

Eğer geçersiz oturum açma denemelerine sınır koyamazsanız, şifre kırma yazılımlarına bir açık kapı bırakmış olabilirsiniz.

Windows Administrator Hesabı

Tüm Windows'ların kurulumunda, tanımladığınız kullanıcı hesabının dışında bir Administrator hesabı vardır.

Bu hesap Windows XP'de arka planda olmasına rağmen aktifken, Windows Vista ve 7'de pasif durumdadır.

XP kurulumu sırasında girdiğiniz bilgisayar şifresi, bu hesabına aittir ve boş bırakılmamalıdır.

Aksi halde kendi hesabınızı şifreleseniz dahi, Administrator kullanıcı adı ile isteyen herkes oturum açabilir.

Windows Vista ve 7'de bu hesabın pasif olarak geliyor olmasından dolayı, böyle bir risk olmadığı söylenebilir.

UAC: Kullanıcı Hesabı Denetimi

Kullanıcı hesabı denetimi, sadece Windows Vista ve Windows 7'de bulunan bir özelliktir.

Yönetimsel yetki gerektiren bir işlem söz konusu olduğunda, bu işlem güvenli bir masaüstü ile kullanıcıya iletilir ve kullanıcının onayı istenir.

Bu her ne kadar güzel bir koruma sistemi gibi görünse de, Windows Vista'da kullanıcıyı bunaltacak düzeyde uyarılar vermesiyle çoğu kullanıcı tarafından pasif duruma getirilmiştir.

Windows 7'de ise bir çok açıdan düzenlenmiş ve sadece gerçekten önemli işlemlerde uyarı vermesi sağlanmıştır.

Windows 7'de kullanıcı hesapları kısmından uyarı düzeyleri yönetilebilirken, Windows Vista'da sadece bu denetim açık veya kapalı duruma getirilebiliyordu.

Akıllı Kartlar

Akıllı kartlar, kimlik doğrulamasında kullanılan ikinci yöntemdir.

"Kişinin sahip olduğu bir şey" kategorisine giren bu kartlar bir kredi kartı yapısındadır ve veri depolanabilen bir çipe sahiptir.

Bu çip üzerinde kullanıcı kimliğini tanımlayan veriler bulunur.

Gelişmiş akıllı kartlar ileri düzey şifreleme algoritmaları kullanan özelleştirilmiş donanıma sahiptirler.

Bugün Maliye Bakanlığı gibi bazı kamu kuruluşları, Tübitak tarafından geliştirilen akıllı kartlar ile dijital imza kullanımını kabul etmektedirler.

Biyometrik Aygıtlar

Biometrik aygıtlar, parmak izleri, retina ve iris örüntüleri ile kemik yapısı gibi bedensel özellikleri algılayan aygıtlardır.

Günümüzde parmak izi tarayıcıları taşınabilir bilgisayarlar veya USB aygıtlarında yaygın biçimde kullanılmaya başlamıştır.

Windows oturum açma şifresi yerine parmak izinizi kullanmanız bile mümkündür.

Havaalanı veya devlet kurumları gibi ortamlarda ise, daha gelişmiş biometrik okuyucu sistemleri kullanılmaktadır.

Kötü Amaçlı Yazılımlar

Kötü amaçlı yazılımlar, bu eğitim en önemli ana başlıklarından birisidir.

Kullanıcını bilgi veya izni olmadan bir bilgisayara sızmak ve muhtemelen zarar vermek için tasarlanmış kod parçaları, kötü amaçlı yazılımlar olarak tanımlanabilir.

Bilgisayar virüsü, solucan, truva atı, spyware, rootkit, adware ve diğer bir çok tipte olabilen istenmeyen yazılımlar bu kapsamdadır.

Güvenlik açısından öncelikli önlem bu yazılımların sisteme bulaşmasını önlemektir. Ancak bu günümüzde çoğu sistem için kaçınılmaz bir durumdur.

İkinci aşama ise sisteme bulaşan bir zararlı yazılımın tespit edilmesi, kaldırılması veya karantinaya alınmasıdır.

Kötü amaçlı yazılımlar ile mücadele etmek için mutlaka uygun ve güncel güvenlik yazılımları gereklidir.

Bilgisayar Virüsleri

Zararlı yazılımların başında bilgisayar virüsleri gelmektedir.

Virüsler, Kullanıcının bilgisi haricinde bilgisayarda çalışan bir koddur.

Önemli olan nokta, sadece koda erişildiğinde ve kod çalıştırıldığında bilgisayara bulaşıyor olmasıdır.

Virüsler çoğalabilme yeteneğine sahiptir ve kendilerini bilgisayarın her yerine bulaştırabilirler.

Virüs bulaşan dosyalara diğer bilgisayarlar tarafından ulaşıldığında virüs diğer sistemlere de bulaşabilir.

Günümüzde yanlış olarak her türlü zararlı yazılımın, virüs olarak tanımlandığını duyabilirsiniz.

Şimdi virüsler dışındaki diğer önemli zararlı yazılımları incelemeye devam edelim.

Solucanlar / Worms

Solucanlar, virüslere göre sanki daha önemsizmiş gibi algılanırlar ki; bu algı tamamen yanlıştır.

Virüsler ile arasındaki asıl fark, kendilerini çoğaltamamalarıdır.

Solucanlar, uygulamalardaki ve işletim sistemindeki güvenlik açıklıklarından ve arka kapılardan yararlanırlar.

Çalışmak için kullanıcıya gereksinim duymazlar.

Daha çok ağ paylaşımları ve toplu e-posta mesajları ile yayılırlar.

Truva Atları / Trojanlar

Truva atları, efsanevi truva savaşının tahta kalelerinden esinlenerek çalışırlar.

Görüntüde istenilen fonksiyonları çalıştıran, ancak arka planda kötü amaçlı fonksiyonları da gerçekleştiren yazılımlardır.

Bunlar teknik olarak virüs değillerdir ve farkında olmadan kolayca download edilebilirler.

Bir truva atı, saldırgana sistemin sahibinden daha yüksek ayrıcalıklar tanıyabilir ve çok tehlikeli sayılacak becerilere sahip olabilir.

Truva atları, ücretsiz olarak yüklediğiniz yazılımlarla bir arada da gelebilir.

Spyware

Spyware farkında olmadan bir web sitesinden download edilebilen veya herhangi bir üçüncü parti yazılım ile birlikte yüklenebilen kötü amaçlı bir yazılım tipidir.

Genelde, kullanıcının izni olmaksızın kişisel bilgilerini toplar.

Bilgisayarda spyware fonksiyonları içeren bazı normal yazılımlar da bulunabilir.

Herhangi bir kullanıcı etkileşimi olmaksızın bilgisayar konfigürasyonunu değiştirebilmektedirler.

Çoğunlukla web reklamları ile bütünleştirilmiş olan bir saldırı türünün en belirgin bulgusu, tarayıcı açılış sayfasının değiştirilmesidir.

Bu casuslardan korunmak için, özellikle ücretsiz yazılım araçlarının kurulumlarına dikkat edin.

Botnet: Zombi Bilgisayarlar

Botnet, kötü amaçlı yazılımlar tarafından ele geçirilmiş "zombi" bilgisayar sistemlerini ifade eder.

Bu sistemler bir kısır döngü içerisinde sürekli olarak zararlı yazılım yayarlar ve kullanıcıları bunun farkında değildir.

Aynı zamanda bilişim suçları için potansiyel eylem bilgisayarları durumundadırlar.

Botnet, spam yollamak ve şantaj yapmaya çalışmaktan, devlet ağlarına saldırmaya kadar farklı alanlarda, siber suçlular tarafından saldırıları yürütmek amacıyla kullanılabilir.

Hatta bu yüzden işlemediğiniz suçlar ile ilgili adli makamlarla muhatap bile olabilirsiniz.

Yazılım Açıkları ve Arka Kapılar

Yazılım açıkları ve arka kapıların oluşturduğu tehditler, herhangi bir istenmeyen zararlı yazılımının sisteminize bulaşmasına bağlı değildir.

Yazılımda bulunan bir kod düzeni, yetkisi olmadığı halde bir kullanıcının üstün yetkilerle sisteme müdahale etmesini sağlayabilmektedir.

Eğer bu bilinçli yerleştirilmiş bir işlem noktası ise, arka kapı; eğer yanlışlıkla unutulmuş bir işlev ise yazılım açığı olarak tanımlanır.

Örneğin mIRC scriptleri bolca güvenlik açığı bulunan yazılımlardır. Hatta bazıları, bilinçli yerleştirilmiş arka kapılardır.

DoS: Denial of Service

Denial of Service kelimelerinin kısaltmasından oluşan DoS ifadesi ile bilinen saldırılarda sistem veya programlara virüs bulaşmaz.

Saldırının amacı, hedef sistemi aşırı yükleme ile bloke etmeye dayanır.

Örneğin 10 dakika içinde 100.000 e-posta gelmesi durumunda e-posta hizmeti veren sunucular işlevlerini göremez hale gelebilir.

Saldırı türünden de anlaşılacağı üzere bu saldırı verilere ciddi bir zarar vermez; ancak bir web sitesinin yayının kesilmesi, çok daha önemli bir kayıp olabilir.

Mantıksal Bombalar

Mantıksal bombalar, genel amaçlı zararlı yazılımlardan farklıdırlar.

Daha önce bahsettiğimiz tüm zararlı yazılımlar geneldir; birden çok bilgisayarda etkili olurlar ve bir süre sonra güvenlik yazılımları tarafından tespit edilirler.

Mantıksal bombalar ise özel bir sistemi bir çok açıdan çalışmaz duruma getirmeyi amaçlar.

Somut bir sistemi ortadan kaldırmayı amaçladığından etkileri ve zarar verme başarısı daha yüksek; tespiti ve engellenmesi daha zordur.

Örneğin işten ayrılan bir yazılım elemanının eski sistemini gizlice yıkacak şekilde bıraktığı bir yazılım, bu kapsamda değerlendirilebilir.

Phishing

Phishing yani olta yöntemi, kullanıcının benzerlik ile kandırılmasına dayanır.

Bir internet sitesinin, veya e-posta mesajlarındaki gönderen adının, benzer bir isim kullanılarak taklit edilmesidir.

Kişilerin gizli şifre ve mali bilgilerini elde etmeyi hedefler.

Özellikle bankalardan geliyormuş gibi görünen e-posta mesajları ve banka web tasarımlarının kopyalandığı sahte banka web siteleri son zamanlarda çok yaygın görülmektedir.

IP Spoofing

Bir hedef IP adresine başka bir IP adresinden geliniyormuş gibi bağlantı sağlanması işlemine IP Spoofing denilir.

Günlük kullanımda IP adresinin çalınması olarak da bilinir.

Proxy sunucular üzerinden bağlanmak gibi çeşitleri olsa da gerçek IP spoofing giden paketlerdeki kaynak adresi değiştirerek yapılır.

Spoofing terimi, yanıltma anlamı ile diğer bir çok internet tabanlı tehdit için de kullanılır; ancak daha çok IP Spoofing terimi ile kullanımı yaygındır.

Örneğin DNS spoofing veya e-mail spoofing tabirlerini de duyabilirsiniz.

Host Dosyasının Çalınması

Bilgisayarınız web sunucu isimlerini host dosyasından ve devamında DNS sunucuları üzerinden öğrenir.

Eğer host dosyanızın içeriği değiştirilmiş veya bilgisayarınızı güvenli olmayan bir DNS veya Proxy sunucusuna yönlendirilmiş ise, gerçek olmayan web sitelerine gitme ihtimaliniz vardır

Yani eğer bir şekilde yanlış bir isim çözümlemesi yaparsanız, gerçek bankanın değil, taklit bankanın web sitesine gidebilirsiniz.

Phishing saldırısından dikkatli davranarak kurtulabilirsiniz; ancak host dosyasında, bunu anlamanız çok daha zordur.

Güvenlik yazılımları host dosyasını bu durumlar için takip ederler.

DNS sunucular için ise, internette her bulduğunuz her sunucu IP adresine güvenmeyin.

Eğer şüphe duyuyorsanız, DNS işini internet servis sağlayıcı firmanıza bırakın.

Sosyal Mühendislik İle Aldatılma

Sosyal mühendislik, kişiler ile insani ilişkileri ve iletişimi kullanarak bilgi sahibi olunmasıdır.

Bilgisayar dünyasında bu kavram, insanların bu yöntemlerle aldatılmasına dayanır.

Ağdaki insanları kullanarak yada kandırarak ağa giriş izni kazanmak, telefon dolandırıcılıkları, taklit vb yanıltmalar ile yapılan her türlü işlem bu kapsamda değerlendirilebilir.

Şirketten birini üst mevkiden bir çalışan gibi arayarak oturum şifrelerini istemek ya da kişileri bir banka yetkilisi gibi arayarak özel bilgilerini almak da bu saldırılara örnek olarak verilebilir.

Bu açıdan kurumsal güvenlik politikalarına uyulması önemlidir.

Kim olursa olsun, tüm işlerinizi formel standartların dışında yapmayın.

Sniffer: Ağ Trafiğinin İzlenmesi

Sniffer'lar ağ trafiğinin izleyen yazılımlardır.

Internet ortamında şifrelenmeden hareket eden tüm veriler, bu yardımcı yazılımlar ile takip edilebilmektedir.

Özellikle anlık mesajlaşma yazılımları ile gönderilen şifrelenmemiş veriler çok basit şekilde elde edilebilmektedir.

Bu sebeple bu anlık mesajlaşma yazılımlarından ve şifrelenmemiş web bağlantılardan, güvenlik riski taşıyan hiçbir bilgi gönderilmemelidir.

Ayrıca bir çok iş yeri çalışanlarını benzer sistemlerle takip etmektedir.

İş yerlerinizde bu yazılımları kullanırken bunun bilincinde olun.

Güvenlik Yazılımları

Güvenlik yazılımları çeşitli şekillerde sisteminizi korurlar.

Antivirüs ve antispyware yazılımları zararlı yazılımların sisteminize bulaşmasını engelleme ve sisteminize bulaşanlarını temizleme hizmeti sunarlar.

Firewall yazılımlar ağ paketlerinin erişim izinlerini denetlerken, denetim merkezleri güvenlik yazılımlarının etkinliğinin kontrolünü yapar.

Her bilgisayar, mutlaka bir antivirüs yazılımına sahip olmalıdır ve virüs veritabanı sürekli güncellenmelidir.

Windows XP, Vista ve 7 sürümleri, yerleşik güvenlik duvarı, antispyware yazılımı ve denetim merkezleri sunmaktadır.

Zararlı Yazılımların Tespit Edilmesi

Eğer bir sistem zararlı bir yazılım tarafından etkilenirse, en basit bulgu sistemin cevap verme süresinin gecikmesi olacaktır.

Sisteminiz istenmeyen veya yanlış davranışlar sergileyebilir.

CPU ve bellek kaynakları doğrudan veya arka planda kullanılır.

Tutarsız davranışlar karşısında sistem mutlaka güvenlik yazılımları ile taranmalıdır.

Tipik Virüs Bulguları

Bilgisayar sistemine virüs bulaşmasının bazı tipik bulguları vardır.

Bunlar; bilgisayarın normalden daha yavaş çalışması…

Normal olmayan hata mesajları…

Antivirüs programlarının çalışmaması…

Bilgisayarın sık sık kilitlenmesi…

Bozuk görüntü veya bozuk baskılar…

Tuhaf sesler oluşması…

Sabit diskin sürekli kullanımda olması…

Bilgisayarın istem dışı davranışlarda bulunması…

Disk sürücüleri veya uygulamaların doğru çalışamaması…

Simgelerin kaybolması veya yanlış görünmesi…

Veri dosyalarının artan sayıda bozuk çıkması…

Otomatik olarak oluşturulmuş klasörler ve dosyalar olarak sıralanabilir.

Tipik Spyware Bulguları

Bilgisayar sistemine spyware bulaşmasının tipik bulguları olarak ise;

Web tarayıcının açılış sayfasının sürekli değişmesi..

Her arama yapılmasında özel bir web sitesinin açılması…

Aşırı derecede popup penceresi görüntülenmesi…

Ağ bağdaştırıcısının aktivite LED'inin veri aktarımı olmadığı anlarda bile yoğun aktivite göstermesi…

Kendiliğinden çalışan yazılımlar…

Firewall ve/veya antivirüs programlarının kapanması…

Yeni programlar, simgeler ve sık kullanılanların kaybolması…

ADSL kotanızın beklenenden çok fazla kullanılmış olması sayılabilir.

Zararlı Yazılımların Temizlenmesi

Bilgisayar sisteminde zararlı bir yazılım tespit edildiğinde, temizleme için internet bağlantısını kesin ve mümkünse güvenli moda geçin.

Kurulu güvenlik yazılımları devre dışı kalmış ise veya veritabanları güncel değil ise, harici ortamlardan çalışan tarama yazılımları kullanın.

Knoppix, BartPE veya MiniPE gibi Linux tabanlı önyükleme ortamları, bu durumlar için ideal uygulamalardır.

Öncelikli işlem zararlı yazılımın temizlenmesi veya karantinaya alınmasıdır.

Üçüncü alternatif ise maalesef veri veya programların silinmesidir.

Firewall: Güvenlik Duvarları

Güvenlik duvarları, bilgisayarın veya ağların, ağ ve internet ortamı ile iletişimini takip eden ve tanımlı kurallara göre bu trafiği yöneten yazılımlardır.

Kurumsal alanlarda genellikle ağın internet çıkışında bulunurken, bilgisayarlar da özel yazılım olarak da bulunabilir.

Bir güvenli duvarı yazılımı, izin verilenler dışındaki tüm portlar kapatır.

Açık olan portlar üzerindeki paket trafiği ise sıkı kurallar tarafından denetlenir.

Windows XP, Vista ve 7, yerleşik güvenlik duvarı bulundurur.

Yazılım Güncellemelerinin Edinilmesi

Başta işletim sistemleri olmak üzere, sistemdeki tüm yazılımların güncelleştirmelerinin takip edilmesi güvenlik açısından son derece önemlidir.

Bu güncelleme gerekliliği, yazılım işlevleri açısından değerlendirmeyiniz.

Stabil şekilde çalışan ve işinizi gördüğü için dokunmadığınız bir yazılım, sizin için bir güvenlik riski taşıyor olabilir.

Web tarayıcılar ve e-posta istemcileri, yapıları gereği bir çok güvenlik açığı barındırabilmektedir.

Bu tip yazılımlar için sürekli olarak güncellemeler yayınlanmaktadır.

Windows'lar için otomatik güncelleme hizmetleri açık olması son derece önemlidir.

Verilerin Erişim İzinlerinin Ayarlanması

Güvenlik konusunun diğer bir ayağı, verilerin erişim izinlerinin ayarlanmasıdır.

Erişim güvenliği, işletim sisteminin, hangi verilerin, hangi kullanıcı erişimine açık olduğunu kontrol etmesine dayanır.

Dolayısı ile bu denetimin başarılı olması yani güvenlik sağlaması için kullanıcı kimliğinin başarılı şekilde doğrulanması gereklidir.

Dosya ve klasör erişim izinleri, fiilen bilgisayarı kullanan veya ağ üzerinden sisteminize bağlanan kullanıcılar için aynı mantıkla düzenlenir ve işler.

Ağ üzerinden gelen kullanıcılar için sadece fazladan paylaşım izinleri de verilmiş olması gerekir.

Dosya ve Klasör Özellikleri Grubu

Dosya ve klasörlerin RASH olarak bilinen özellikler grubu, salt okunur, arşiv, sistem veya gizli etiketlerine izin verir.

Örneğin salt okunur olarak işaretlenen bir klasörün içeriği değiştirilemez.

Ancak bu bir güvenlik ayarı olarak düşünülmemelidir.

Çünkü kötü amaçlı yazılımlar, klasörlerin bu izinlerini çok rahat şekilde değiştirebilirler.

Bu ayarlar daha çok bilgisayar legal olarak kullanan kişiler için geçerlidir.

Bu etiketlere göre işaretlenen bazı sistem dosyaları, korunan işletim sistemi dosyaları olarak ayrıca gizlenirler.

Sadece gizli dosya ve klasörleri görünür yapmak, bunların görünmesini sağlamaz.

Bu özel dosya ve dizinleri görmek için, klasör seçeneklerinden ayrıca izin vermelisiniz.

Paylaşım İzinlerini Anlamak

Paylaşım izinlerinin güvenli ve etkin biçimde ayarlanabilmesi için, nasıl çalıştığını anlamanız gereklidir.

Dosya ve klasör erişim izinleri ile paylaşım izinleri, birbirinden farklı iki izin grubudur.

Bir klasöre ağ üzerinden paylaşım izni vermeniz, sadece o klasöre erişim izni olan kullanıcılar için anlamlıdır.

Yani bir kullanıcının paylaşılan bir kaynağa erişmesi, hem gerekli dosya ve klasör yetkilerine, hem de paylaşım izinlerine sahip olmasına bağlıdır; ikisinden birisi eksik olmamalıdır.

Aynı şekilde ağ üzerinden paylaşıma açılmadığı sürece, uzaktan bağlanan bir kullanıcı, yetkisi olsa da dosya ve klasöre erişemez.

Windows'ta Yönetimsel Paylaşımlar

Bilgisayar yönetim ekranından, paylaşıma açık olan dizinler görülebilir ve paylaşım özellikleri yönetilebilir

Bu ekrana geldiğinizde, bilgisayarınızda paylaşım dizini olarak görünmeyen bazı paylaşım tanımları görürsünüz.

Sonunda $ işareti olan bu paylaşımlar gizli paylaşımlardır. Aramalarda ve klasör göz atmalarında listelenmezler.

Ancak böyle bir paylaşım olduğunu bilen bir kişi tam paylaşım adını yazarak erişim sağlayabilir.

Burada gördüğünüz paylaşımlar yönetimsel amaçla açıldığı için, aynı zamanda gizlemiştir.

Yani bir kişi bilgisayarınızın adının yanına C$ yazarak erişim denemesi yapsa bile, kimlik doğrulamasından geçemeyeceğinden erişim sağlayamayacaktır.

Windows XP'de Paylaşımlar

Windows XP, klasik erişim ve paylaşım izinlerini gizleyen, "basit paylaşım" modunu kullanır.

Bu mod ile kullanıcı, sadece "klasörü paylaşma" ve "içeriğinin değiştirilmesine izin verme" olmak üzere 2 ayar seçebilmektedir.

Ancak basit modu kapatırsanız, ayrıntılı erişim ve paylaşım izinlerini düzenleyebileceğiniz sekmeler görünür hale gelir.

Windows Vista ve Windows 7 Paylaşımları

Vista ve Windows 7'de basit paylaşım modu bulunmaz.

Bunun yerine kullanıcının karmaşık izin verme ekranları ile uğraşmaması paylaşıma açma sihirbazları kullanılır.

Windows XP'deki basit paylaşımın veya buradaki sihirbazların aslında yaptığı şey sizin yerinize ilgili izinleri düzenlemektir.

Ayrıca paylaşımlarda uygulanacak genel kurallar, ağ ve paylaşım merkezi uygulaması içinden belirlenebilir.

İleri İzin Yapılandırması ve Yayılım

Eğer sabit diskinizi NTFS olarak formatlamış iseniz, daha ileri düzey erişim izinleri ayarlayabilirsiniz.

FAT32 kullanmak ise, daha sınırlı bir güvenlik sağlar.

Bir dizin için yapılan yetki düzenlemeleri, aksi belirtilmedikçe alt dizin ve dosyalar için geçerli olacaktır.

Üst klasörden alınan izinler, sadece üst dizinden düzenlenebilir.

İzin devralma işlevi, klasörler ve dosyaların kopyalama ve taşınma işlemlerinden de etkilenir.

Eğer bir klasör aynı veya farklı bir disk bölümünde kopyalanırsa, klasör üst öğesindeki izinler hedef dizine aktarılır.

Eğer bir klasörü aynı diskte farklı bir yere taşıyorsanız, bu sefer klasör kendi orijinal izinleri ile kalacaktır.

Verilerin Yedeklemesi

Bilgisayarda herhangi bir değişiklik yapmadan önce önemli verilerin yedeklendiğinden emin olmanız, her zaman söylenen bir konudur.

Bunun dışında herhangi bir problem yokken de, belirli aralıklarla kritik verilerinizin yedeğini alın.

Bunu bir alışkanlık haline getirin ve insanlara tavsiye edin.

Çünkü bir güvenlik tehdidinin ne zaman geleceğini ve sisteminizi hangi derecede etkileyeceğini asla önden kestiremezsiniz.

Yedeklerin şu an çalıştığınız alanın dışında bir yere alınması da önemlidir.

Bu hem bilgisayar sistemi, hem de fiziksel mekan anlamında gereklidir.

Örneğin, iş yerinizdeki verilerin DVD yedeğinin bir kopyasını evinizde de saklayın.

Yangın, su baskını, hırsızlık gibi risklerin sizi "taş devrine" göndermesine izin vermeyin.

Verilerin Şifrelenmesi

Şifreleme, verilerin bir algoritma ile, doğru anahtara sahip olunmadığı sürece okunamaz hale getirilmiş olmasıdır.

Bu anahtar okuma veya değiştirme şifresi gibi tanımlarla da ifade edilir.

Eğer şifreleme ve şifrelenmiş veriyi okuma işlemleri aynı anahtar ile gerçekleşiyor ise simetrik şifreleme yapılmıştır.

Birazdan bazılarına değineceğimiz EFS, BitLocker, WEP, WPA, Kerberos, AES gibi şifreleme sistemleri simetrik şifreleme yaparlar.

Eğer verinin şifrelenmesi için ortak, verinin okunması için ise özel olarak 2 anahtar var ise, asimetrik şifreleme yapılmıştır.

RSA ve ECC en yaygın kullanılan asimetrik şifreleme tekniklerdir.

Asimetrik anahtar kullanımı kesinlikle daha güvenli, ancak çok daha karmaşıktır.

Asimetrik şifreleme için hafızada tutulamayacak, hatta elle yazılamayacak yapıda anahtarlar kullanılır.

Asimetrik şifreleme genelde kurumsal veri aktarım sistemlerinde, iletişim kanallarının güvenliğinde kullanılır.

Bütünlük Doğrulama Şifrelemeleri

Bütünlük doğrulama şifrelemeleri ise, matematiksel olarak oluşturulmuş sayılardır ve geri dönüşü olacak şekilde çözülemezler.

Daha çok download edilen dosyaların bütünlüğünün kontrolü veya veritabanlarında şifrelerin saklanması işlevlerinde kullanılırlar.

SHA ve MD5 en bilinen bütünlük doğrulama şifreleme yöntemleridir.

Siz bir sitede oturum açmak istediğiniz şifreniz MD5 e dönüştürülür, ve daha önce oluşturulan MD5 ile karşılaştırılır.

Bu sayede site yöneticileri bile girdiğiniz şifreleri öğrenemezler. Tabi web sitesi altyapısının kötü niyetli bir kullanıcı tarafından düzenlenmediğini varsayarsak.

Ağ Kimlik Doğrulaması

Veri şifreleme yöntemlerine bir örnek kullanım da Windows'un ağ kimlik doğrulama işlevidir.

Windows'ta network için oturum açtığınız zaman kimlik doğrulaması Kerberos protokolü ile korunmaktadır.

Bu koruma, ağ boyunca kimlik doğrulaması yapılacak şekilde kullanıcı adı ve şifresi için koruma katmanı sağlamış olur.

Windows EFS: Şifreli Dosya Sistemi

Windows EFS, klasör ve dosya şifrelemesinde kullanılan NTFS bileşenidir.

Herhangi bir klasör veya dosyayı şifreli duruma getirmek için özellikler görünümünden gelmiş ekranına gitmeniz gerekir.

Buradan "veriyi korumak için içeriği şifrele" seçeneğini işaretlemeniz durumda içerik şifrelenir ve simge metni yeşil renk alır.

Bu sistem simetrik ve asimetrik anahtarları ortak kullanılır ve o klasör sadece ilgili Windows hesabı ile kullanılabilir.

Burada hemen merak edebilirsiniz; bu klasörlere sizin erişiminizde hiçbir değişiklik olmaz.

Yani Windows şifrelenmiş veriler için sizden herhangi bir erişim şifresi girmenizi istemez.

Şifrelenmiş verileri, şifrelemesi yapan Windows kullanıcı hesabından kullanılabilecek hale getirir.

Dolayısı ile verilere şifreyi koyan kullanıcı hesabı dışında erişim mümkün değildir.

Eğer bilgisayarınızı formatlar ve eski verilerinize ulaşmaya çalışırsanız, yeşil metinli klasörlerin halen şifreli olduğunu, ancak içeriğine ulaşamadığınızı görürsünüz.

EFS kurtarma araçları bulunsa da, bazı durumlarda bu verilere hiçbir şekilde ulaşamama riskiniz vardır. Onun için dikkatli olun.

EFS, bir bilgisayardan diğerine veri transferi sırasında veriyi korumak için tasarlanmamıştır. Sadece kullanıcı hesabı için geçerli olacak şekilde erişimin engellenmesi sağlar.

BitLocker

Windows EFS, çok popüler değildir; çünkü sadece o Windows hesabı için şifreleme yapar.

Windows Vista ve 7'de, BitLocker adında yeni bir disk şifreleme yazılımı ile birlikte gelmiştir.

BitLocker, AES şifreleme standardında 128 Bit simetrik şifreleme yapar.

Normalde BitLocker ile şifrelenmiş bir sürücüye erişmek için, erişim anahtarlarını o sürücü haricinde bir konumda depolamanız gerekmektedir.

Bu konum, anakart üzerinde yer alan bir TPM, yani güvenilen platform modülü yongası…

Bir USB flash bellek…

Veya ikinci bir sabit sürücü bölmesi olmalıdır.

Windows Vista ise sadece TPM desteği sunmaktadır.

Windows 7 ise, kurulum sırasında 100 MB'lık bir bölmeyi, hem diğer bazı sistem gerekleri için kullanmak için, hem de BitLocker için ayırır.

Verilere başka bir sistemden ulaşmak için en ideal yöntem, USB flash belleğe yedeklenmiş bir anahtar yedeği kullanmaktır.

BitLocker To Go

Windows 7, Vista'da gelen BitLocker uygulamasını bir adım daha ileri götürmüştür.

Windows 7 ile BitLocker, harici anahtarla yapılan disk şifrelemesinin yanında, veri dosyalarının içine saklanabilen anahtarlarla taşınabilir bellekleri de şifreleyebilir.

Bu şekilde şifrelenmiş bir sürücüyü başka bir sisteme taktığınızda, erişim için sizden parola istenir.

Windows 7 dışındaki sistemler de bu verilere şifreli şekilde erişebilir; ancak sadece okuma yapabilirler.

Değişiklik yapabilmek için Windows 7 kullanımı zorunludur.

Verilerin Güvenli Şekilde Silinmesi

Verilerin yedeklenmesi ve şifrelenmesi kadar önemli olan diğer bir konu da, güvenli şekilde silinmeleridir.

Windows'tan vereceğiniz bir silme komutu veya disk biçimlendirme işlemleri verileri gerçekte silmez.

Bu konuda daha detaylı bir için sabit diskler ilgili bölümlerimize bakabilirsiniz.

Bir veri ancak üzerine başka veri yazıldığı durumda silinebilir.

Aksi durumda özel yazılımlarla veriler yeniden elde edilebilir. Hatta bazen üzerine yazılmış veriler bile çok ileri düzey işlemlerle yeniden inşa edilebilirler.

Güvenli silme işlemi, bir verinin belirli bir yeniden inşa edilemeyecek şekilde kaldırılması işlemidir.

Bu yazılımlar, ilgili verinin üzerine defalarca veri yazarak geri dönüşünü imkansız hale getirmeye çalışmaktadır.

Eğer tarihe gömmek istediğiniz bir veri varsa, mutlaka güvenli silme yazılımı kullanın.

Bilinçli Kullanıcı Davranışları

Hangi güvenlik önlemini alırsanız alın, bilinçsiz bir kullanıcıdan bilgisayar sistemini koruyamazsınız.

Kullanıcının bilinçlendirilmesi ve buna göre davranmasının sağlanması, güvenlik önlemlerini en önemlisidir.

Kullanıcı yaptığı işlemlerin ve kullandığı yazılımların olası risklerinin farkında olmadığı sürece, diğer önlemler anlamsızdır.

HTTP ve HTTPS Erişim Farklarını Anlamak

Bilinçli bir kullanıcının farkında olması gereken ilk şey HTTP ve HTTPS erişimin farklarıdır.

HTTPS, yani güvenlik katmanı üzerinden HTTP iletişimi sağlar.

İnternet üzerinde HTTP ile gönderdiğiniz tüm bilgiler, hedefine ulaşana kadar yol üzerinde herkes tarafından görülebilir.

Bu kesinlikle doğrudur ve bunu asla unutmayınız.

HTTPS ise, verileri sunucuya şifreleyerek gönderir.

Bu sayede sniffer yazılımları iletişiminizi izlese bile, içeriklerini okuyamayacaktır.

Burada akla HTTP niye var, tüm iletişim HTTPS üzerinden olsun gibi bir soru gelebilir.

HTTPS, şifreleme ve denetim süreçleri sebebiyle doğal olarak daha yavaş çalışır ve daha fazla bant genişliği tüketir.

Bu yüzden kritik kabul edilebilecek iletişim süreçlerinde kullanılması makuldür.

İnternette kişisel bilgilerinizi girdiğiniz bir web sitesinde, HTTPS erişimi olup olmadığın kontrol ediniz.

Güvenli Tarayıcı Kullanımı

Bilgisayarın güvenlik zaaflarının önemli bir kısmı, bilinçsiz yapılan internet gezintileridir.

Web tarayıcınızı bilinçsiz şekilde kullandığınız sürece, sisteminizi korumak için alınan önlemler bir şekilde yetersiz kalacaktır.

Öncelikle internette en çok yapılan şey olan arama işlemlerine değinelim. Arama sonuçlarında öngörülü davranın; bir sitenin size zarar verip vermeyeceğini büyük oranda tahmin edebilirsiniz.

Arama sonuçlarında kullanılan tanıtım metinler, sitenin ismi gibi bir çok kriter size çok şey anlatır.

Örneğin "binlerce mp3 melodi bedava sınırsız hepsi süper hızlı" diye bir sonuç görürseniz, bu sitenin bilgisayarınıza zarar verecek bir içerik sunması çok büyük bir ihtimaldir.

Eğer illa ki böyle bir siteye girmeniz gerekiyorsa antivirüs vb güvenlik yazılımınızın aktif ve güncel durumda olduğuna emin olun.

Bu siteden çıkan bir uyarıyı onaylarken, normalden 10 kat fazla düşünün.

Reklamlara tıklarken özenli davranın, mümkün olduğu kadar tamam veya kabul ediyorum butonlarına tıklamayın. Pencereleri kapatmak için Alt + F4 bileşimini kullanın.

Tarayıcı güvenlik ayarlarını çok düşük düzeylere indirmeyin.

Web sitelerinin önerdiği tüm eklentileri iyice incelemeden kurmayın. Web siteleri binlerce anlamsız eklenti paketi kurmayı önerebilir.

Son olarak güncel bir internet tarayıcısı sürümü kullandığınızdan emin olun. Güncel olmayan her sürüm, güvenlik açıkları bulunan sürüm demektir.

e-Posta: Zararlı Yazılım Taşıyıcıları

e-Posta mesajlarını, asli işlevi olan iletişim kadar, zararlı yazılım taşıyıcıları olarak tanımlamak çok da yanlış olmaz.

Çünkü zararlı yazılımlar, en çok e-postalar aracılığı ile yayılırlar.

Bugün şirketimize gelen e-posta mesajlarının %80'i, güvenlik sorunları içeren veya çöp nitelikte mesajlardır.

Kullanıcılar bu açıdan kaynağını bilmedikleri e-posta mesajlarını doğrudan açmamalı, mesaj eklerini açmadan önce virüs taramalarından geçtiğinden emin olmalıdırlar.

Özellikle POP3 üzerinden bilgisayarınıza e-postaları alıyorsanız, daha fazla risk aldığınızı unutmayın.

Çünkü Hotmail veya Gmail gibi web arabirimleri üzerinde açtığınız e-posta mesajları, bir web sayfasından farksızdır.

Webmail uygulamalarında olabilecek risk, ekleri bilgisayarınıza indirip çalıştırmanız durumunda söz konusudur.

Kullanıcıları bir webmail mesajını açmakla, bir POP3 istemcisindeki mesajı açmak arasındaki farkı anlayacak şekilde bilinçlendirin.

Potansiyel Güvenlik Açığı Bulunduran Yazılımlar

Bazı yazılımlar, güvenlik tehditleri içeren yapılandırmalar gerçekleştirirler ve kullanıcılar bunun farkında olmaz.

Veya daha önce bahsettiğimiz gibi bizzat kendilerinde güvenlik açıkları veya arka kapılar vardır.

P2P yazılımları, mIRC vb sohbet scriptleri, bir zararlı yazılım olmamakla beraber çalışma mantıkları gereği güvenlik zafiyetleri bulunan yazılımlardır.

Bu yazılımlar çalışmaları için gerekli olan sistemler sebebiyle kullanıldıkları bilgisayarı saldırıya açık hale getirebilmektedirler.

Zorunlu olmadıkça kullanıcıları bu yazılımlardan uzak tutun; hatta iş yerinde bu tip yazılımların kullanımına kesinlikle müsaade etmeyin.

Kablosuz Bağlantılarda Güvenlik Tehditleri

Kişisel kullanıcı güvenliğinde günümüzde en çok güvenlik problemi yaşanan diğer bir konu da, kablosuz bağlantı güvenliğidir.

Kablosuz modem ve diğer erişim noktaları mutlaka şifreli olmalı ve mümkün olduğu kadar WPA şifreleme yöntemi kullanılmalıdır.

WPA kırılması çok daha zor olan bir şifreleme sistemidir.

Ayrıca erişim noktasının SSID yayınması ve istemcilere DHCP servisi sunması da zorunlu olmadığı sürece kapatılmalıdır.

Fabrika ayarında gelen erişim şifresi mutlaka değiştirilmelidir. Kullanıcıların %90'ı bunun farkında değildir.

Bu sebeple IP adresi bilinen bir ADSL kullanıcısının modemine yetkili olarak erişmek, çocuk oyuncağı olmuştur.

Yapabileceğiniz son güvenlik önlemi de MAC adresleri için filtre uygulamanızdır.

Bu sayede sadece sizin izin verdiğiniz MAC adresleri kablosuz ağınıza bağlanabilir.

Kurumsal Veri Sınıflandırması

Kurumsal alanda çeşitli veri sınıflandırmaları vardır.

Kurumsal açıdan önemli verilere yetkisiz kişiler tarafından ulaşıldığında, güvenlik kaybına veya bir şirket için yararlı olmama ile sonuçlanabilir.

Bir ISO standardına göre verileri 5 ana sınıfa ayrılırlar; genel, dahili, ticari, gizli ve çok gizli.

Bir diğer sınıflandırma yaklaşımına göre ise kategoriler genel, kişiye özel, hizmete özel, kuruma özel, gizli ve çok gizli olarak sayılır.

Askeri ve kamu hizmetleri alanında genellikle bu sınıflandırma yaklaşımını görürsünüz.

Önemli Kurumsal Güvenlik Açıkları

Kurumsal alanda, bireysel bilgisayar kullanımından daha fazla ve daha ciddi güvenlik açıkları söz konusu olabilir.

Hatalı kablosuz ağ yapılandırması…

Hatalı yapılandırılmış VPN sunucuları…

Web uygulamalarında yazılım açıkları ile SQL sorgularının değiştirilebilmesi…

Web uygulamalarında başka siteden kod çalıştırma…

Kolay tahmin edilebilir veya kırılabilir şifreler oluşturmak…

Güncellemeleri yapılmamış sunucular ve işletim sistemleri…

İşletim sistemi ve hazır uygulamaların standart ayarlarla kurulması…

Güvenlik duvarı tarafından korunmayan sistemler…

Hatalı yapılandırılmış saldırı tespit sistemleri, önemli kurumsal güvenlik açıkları olarak sayılabilir.

Kurumsal Güvenlik İhmalleri

Kurumsal alanda teknik güvenlik açıklarının yanı sıra, tehdit doğurabilecek önemli görev ihmalleri de olabilir.

En büyük ihmal, sorun çıkana kadar çözümün ertelenmesidir.

Kurumsal bilginin ve prestijin maliyetinin kavranılamaması de ciddi bir problemdir.

Bir online satış sitesinin yazılımsal açıklar sebebiyle hacker saldırısına kalması, o sitenin ticari hayatını bitirebilecek bir güven sarsılmasına sebep olabilir.

Bilgisayar güvenliğini yetersiz kişilere bırakmak ve sorumlu personelin eğitim süreçlerinin ihmal edilmesi de önemli bir etkendir.

Sorumlu personelin kendilerini geliştirmesine imkan verecek şekilde iş yüklerinin dengelenmesi son derece önemlidir.

Referanslar

A+ Bilgisayar Teknik Servis Elemanı Eğitimi / Bilgisayar ve Veri Güvenliği. Pazartesi, 6 Şubat 2012 03:18:12 +0200 Tarihinde http://www.cizgi-tagem.org/e-kutuphane/topic.aspx?id=1224 Web Adresinden Alınmıştır.