

VERİ GÜVENLİĞİ



Bundan 20 yıl kadar önce, bilgi işlem servisleri günümüzdeki kadar yaygın kullanılmadığından, bilişim sistemleri günümüzdeki kadar önemli bir yere sahip değildi. Daha iyi açıklamak gerekirse, eskiden iş süreçleri ve faaliyetlerin çok küçük bir kısmı bilişim sistemleri kullanılarak yürütülmekte iken günümüzde bilişim sistemleri hemen hemen her iş sürecinin bir parçası olarak yerini almıştır. İşte bu sebeple bilişim sistemlerinin güvenliği iş süreçlerimizin ve faaliyetlerimizin yürütülebilirliği açısından çok önemlidir. Herhangi bir bilgi sisteminde aşağıdaki konumlardan **herhangi birisinde iseniz sorumluluğunuz var** demektir.

Bilginin sahibi

Bilgiyi kullanan

Bilgi sistemini yöneten

Bu durum çok geniş bir kitleyi içerdiğinden **"bilgi güvenliğinin sağlanmasından herkes sorumludur"**

diye genelleme yapmakta bir sakınca yoktur.



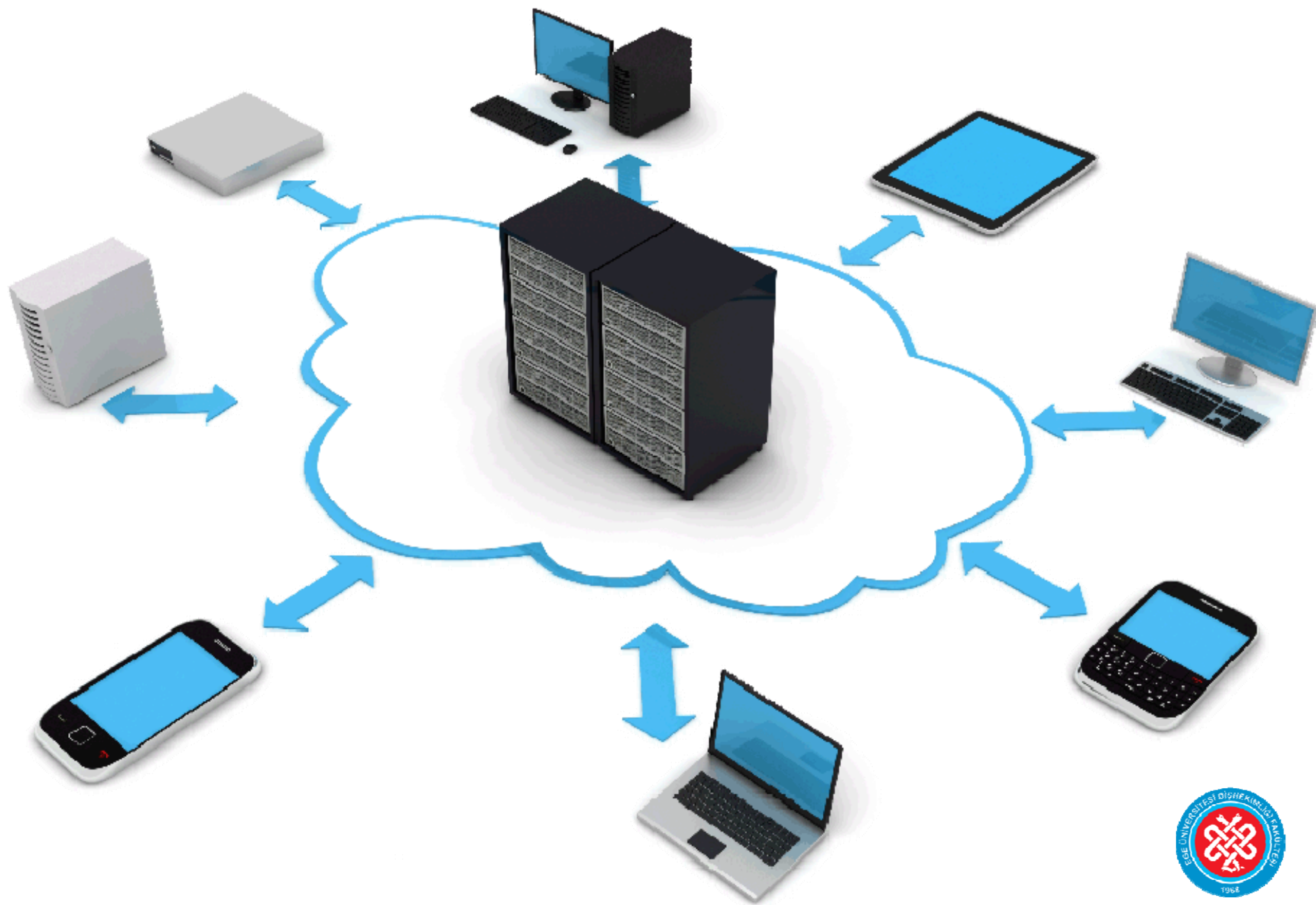
Herkes sorumlu ise bilgi güvenliđinin seviyesi nasıl belirlenir?

Bilgi sistemlerini bir zincir gibi düřündüğümüzde bu zincirin en zayıf halkası çođunlukla sistemin kullanıcılarıdır. Unutulmamalıdır ki

«bir zincir en zayıf halkası kadar sağlamdır.»

Bilgi güvenliđinin seviyesi de bu durumda kullanıcılara bađlı olduğundan, **kullanıcı bilinci** bilgi güvenliđinin sağlanması için son derece hayati bir öneme sahiptir ve bilgi güvenliđi seviyesini belirler.





İçeriden gelebilecek hatalar/zararlar

Sistemi içeriden yani kullanıcıdan gelebilecek hatalara ve zararlara karşı koruyan bir mekanizma yoktur. Hatta dışarıdan gelen saldırganın herhangi bir kullanıcı adı ve şifresi mevcut değilken, içerideki kullanıcının kullanıcı adı ve şifresiyle bazı haklara sahip olması, içerideki tehdidin önemini arttırır.

Bu nedenle bilinçli kullanıcılar olmamız şart olduğu gibi, çevremizdeki kişilerin de bilinçli kullanıcılar olması için üstümüze düşeni yapmalıyız.



Kullanıcı güvenlik ihlalleri ne gibi sonuçlar doğurur?

Bir kullanıcının hatası tüm sistemi etkileyebilir.

Örneğin;

Bir kullanıcı kendi kullandığı bilgisayar ile tüm ağa bağlı olduğundan kullanıcıya bulaşan bir tehdit tüm sisteme yayılabilir.

E-posta ile gelen ".exe" uzantılı bir eklenti, resim dosyası ya da müzik dosyası beraberinde bir solucan ya da truva atı içerebilir. Kullanıcı ekteki dosyayı açtığı anda tüm sisteme zarar verebilecek bir yazılıma izin vermiş olabilir. Ekteki virüs ya da zararlı yazılım kullanıcının bilinçsizliği nedeniyle tüm sisteme bulaşmış olur.

Bunun en ünlü örneği conficker isimli virüsün Ocak 2009'da birçok sisteme zarar vermesidir. İnternete bağlı olan ya da olmayan birçok sistem bu virüsten etkilenmiştir.

Taşınabilir medyaların yaygınlaşması ile internet ortamından bulaşan bir virüs, taşıma yoluyla intranet adını verdiğimiz özel iç ağlara da bulaşabilir hale gelmiştir.



Hangi durumlarda bilgisayarınızda kontroller yapmanız ve/veya bilgi sistem personeline başvurmanız gerekir?

Bilgisayarınızda gereksiz bir yavaşlama durumunda,
Sizin müdahaleniz olmadan bir bilgi kaybı veya deęişikliği ile
karşılaştığınızda,

Kontrol dışı programların çalışması durumunda,
Kontrol dışı web sayfalarının açılması durumunda,
Virüs tespit ajanlarının çalışmadığını fark ettiğinizde.



GÜVENSİZ VERİ EKCRAN GÖRÜNTÜLERİ

The image displays a Windows desktop environment with a blue background. On the left side, there is a taskbar with several icons: 'Bilgisayar', 'Google Chrome', 'VLC media player', and 'HOSAPP'. The desktop is cluttered with multiple overlapping windows of a web browser. The browser windows show a medical software application with a menu on the left side. The menu items are organized into several categories: 'HASTA İŞLEMLERİ', 'ARAŞTIRMA LABORATUVARI', 'FATURALAMA İŞLEMLERİ', 'İDARI TANIMLAR', 'KAPANIŞ İŞLEMLERİ', 'KLİNİK YÖNETİM ve VERİMLİK ENTEGRASYONU', 'LABORATUVAR İŞLEMLERİ', 'PERSONEL İŞLEMLERİ', 'RAPORLAR', 'SİSTEM PARAMETRELERİ', 'TIBBİ HALZEME İŞLEMLERİ', 'TIBBİ TANIMLAR', and 'VEZNE İŞLEMLERİ'. A Facebook window is also open, showing a post from 'babolayse' with a video player and a comment section. The desktop is cluttered with multiple overlapping windows of a web browser, showing a medical software application interface. The interface includes a menu on the left side with various categories and sub-items. The browser windows are stacked on top of each other, creating a layered effect. The overall scene suggests a lack of security and privacy in the data displayed on the screen.



Bilgi güvenliđinin en önemli parçası kullanıcı güvenliđi bilincidir.

Oluşan güvenliđi açıklıklarının önemli bir kısmı kullanıcı hatasından kaynaklanmaktadır.

Saldırganlar (Hacker) çođunlukla kullanıcı hatalarını kullanmaktadır.

Bilgi güvenliđinin en zayıf halkası kullanıcılarıdır.

Bir kullanıcının güvenliđi ihlali tüm sistemi etkileyebilir.

Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır.

Kullanıcılar tarafından dikkat edilebilecek bazı kurallar sistemlerin güvenliđinin sağlanmasında kritik bir öneme sahiptir.





TEŞEKKÜRLER