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"*

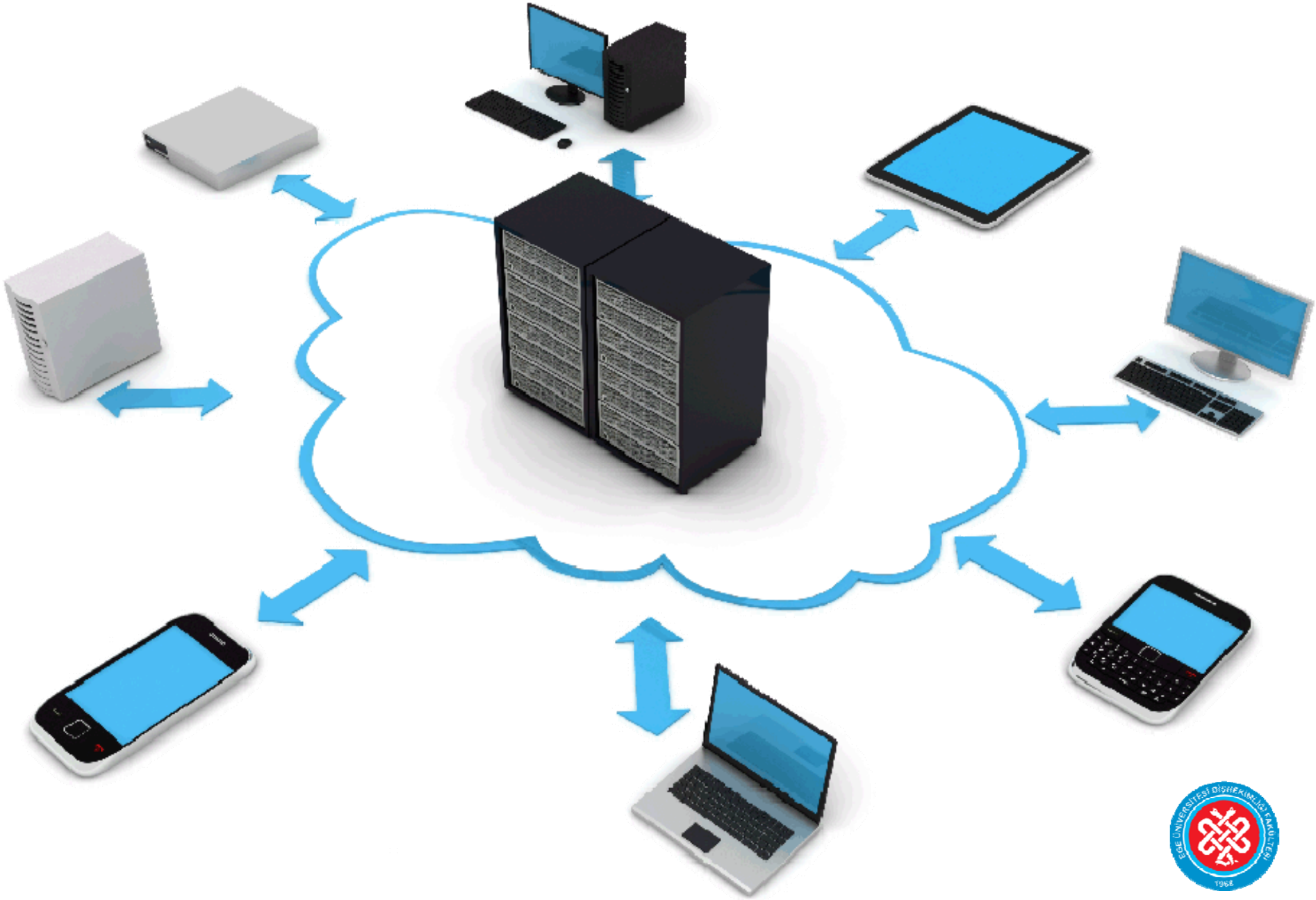
diye genelleme yapmakta bir sakınca yoktur.

Herkes sorumlu ise bilgi güvenliğinin seviyesi nasıl belirlenir?

Bilgi sistemlerini bir zincir gibi düşündüğümüzde bu zincirin en zayıf halkası çoğunlukla sistemin kullanıcılarıdır. Unutulmamalıdır ki

«bir zincir en zayıf halkası kadar sağlamdır.»

Bilgi güvenliğinin seviyesi de bu durumda kullanıcılara bağlı olduğundan, **kullanıcı bilinci** bilgi güvenliğinin sağlanması için son derece hayati bir öneme sahiptir ve bilgi güvenliği 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 açtığında 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,

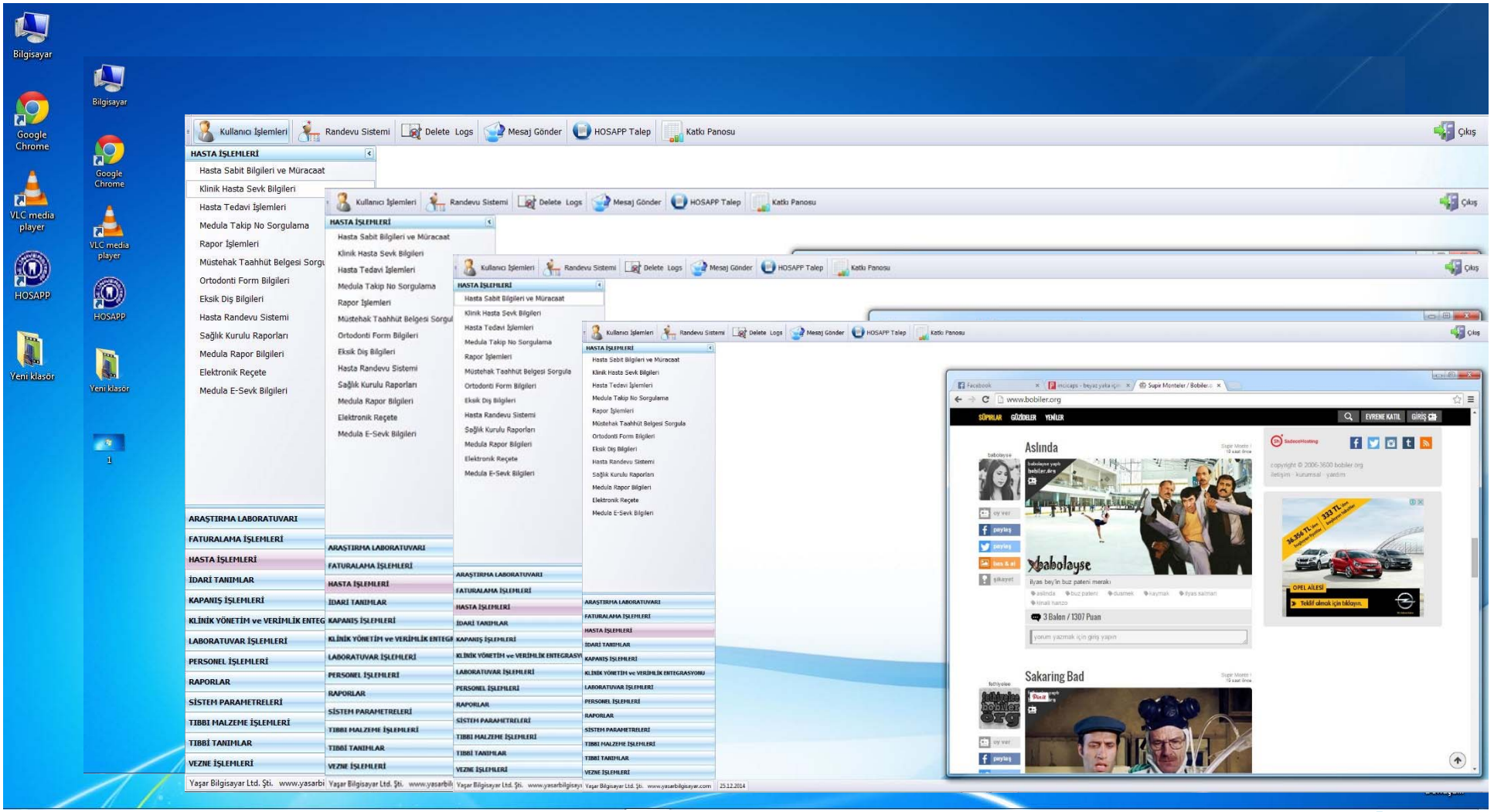
Sizin müdahaleniz olmadan bir bilgi kaybı veya değişikliği ile karşılaştığınızda,

Kontrol dışı programların çalışması durumunda,

Kontrol dışı web sayfalarının açılması durumunda,

Virüs tespit ajanlarının çalışmadığını fark ettiğinizde.

GÜVENSİZ VERİ EKRAN GÖRÜNTÜLERİ



Bilgi güvenliğinin en önemli parçası kullanıcı güvenlik bilincidir.

Oluşan güvenlik açıklıklarının önemli bir kısmı kullanıcı hatasından kaynaklanmaktadır.

Saldırganlar (Hacker) çoğunlukla kullanıcı hatalarını kullanmaktadır.

Bilgi güvenliğinin en zayıf halkası kullanıcılardır.

Bir kullanıcının güvenlik ihlali tüm sistemi etkileyebilir.

Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır.

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

TEŞEKKÜRLER