BİLGİ İŞLEM DAİRE BAŞKANLIĞI
BİLİŞİM FARKINDALIĞI EĞİTİMİ 2020

SÜLEYMAN DEMİREL ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

EĞİTİMİN AMACI | HEDEFLER

01 Bilgi/Bilişim Sistemlerindeki tehdit, açıklar hakkında bilgi edinmek ve güvenlik yöntemlerini anlamak

02 Bilgi/Bilişim Sistemlerinin bileşenlerini tanımak

03 Siber güvenlik ile ilgili kavram ve teknolojileri öğrenme

04 Siber saldırılarda kullanılan yöntemler hakkında bilgi edinmek

BİLGİNİN ÜÇ **TEMEL ÖZELLİĞİ**

01

Erişilebilirlik (Availability)

Bilgi yetkili kullanıcılar için her zaman erişilebilir olmalıdır.

02

Gizlilik (Confidentiality)

Bilgiyi yalnızca yetkili kullanıcılar tarafından görüntülenebilmelidir.

03

Bütünlük (Integrity)

Bilgi yalnızca yetkili kullanıcı tarafından değiştirilebilmelidir.

BİLİŞİM FARKINDALIĞI **EĞİTİMİ**

Gizlilik: Bilgi ya da kaynakların gizlenmesi.

Orijinallik: Bilginin kaynağından emin olmak.

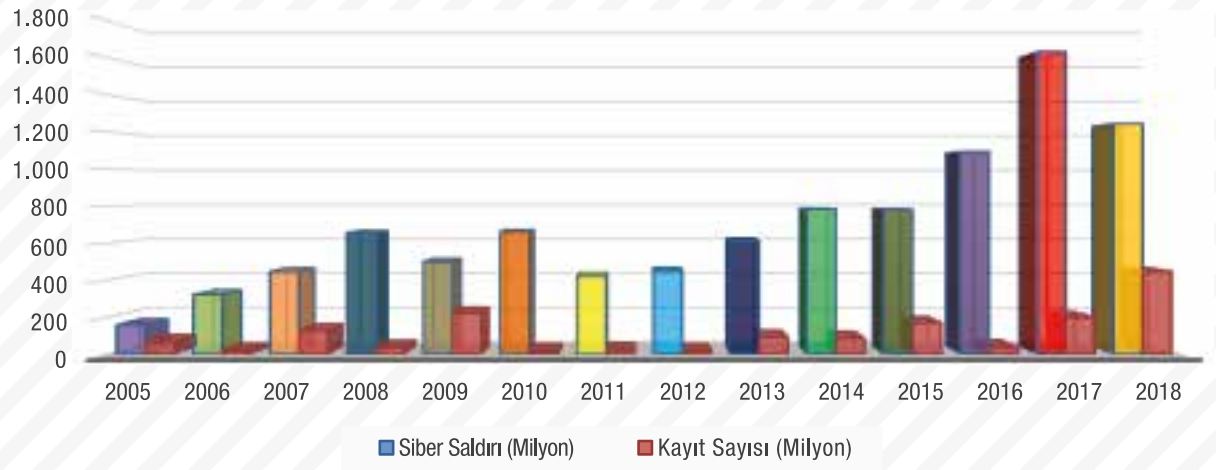
Güvenilirlik: Veri ya da kaynağın uygunsuz ya da yetkisizce değiştirilmediğinden emin olmak.

Kullanılabilirlik: İstenildiği zaman veri ve kaynakların ulaşılabilir durumda olması.

Yüzlerce saldırı türü var en yaygın olanları ;

- Virüsler
- Worms(Solucanlar)
- Trojan(Truva Atı)
- Ddos (Servis Dışı Bırakma)
- Phishing (Oltalama)

SİBER SALDIRI **İSTATİSTİĞİ**



KULLANICI BİLİNCİNİN **ÖNEMİ**

Kişisel verilerin herhangi bir bozulma, değiştirilme ya da çalınmasına karşı, verilerinizi korumaya yönelik **siber güvenlik bilincidir**.

Oluşan güvenlik açıklarının büyük kısmı, **kullanıcı hataları** kaynaklıdır ve saldırganlar **(hacker)** çoğunlukla bu hatalardan faydalanmaktadır.

Kullandığınız bilgisayara otomatik **ekran kilidi** ve **güçlü bir şifre** ayarlanmalıdır.

Bilgisayar başından ayrılmanız halinde **MUTLAK SURETLE kilitlenmelidir**.

Eposta yoluyla gelen formlara asla şifre ve kişisel bilgiler girilmemelidir!

Şüphe uyandıran isim, resim ve sayfalara erişimden kaçınılmalıdır.

Akraba, arkadaş ve tanımadığınız kişilerle kullanıcı bilgileriniz kesinlikle paylaşılmamalıdır.

Bilgi işlem ve resmi kurumlar **KESİNLİKLE sizden şifre talep etmez**.

BİLGİ GÜVENLİĞİNE **YÖNELİK TEHDİTLER**

TEHDİTLER

İç Tehdit Kavramı

Masum

- Şifre ve değerli bilgileri bilgisayarın yanında bulundurmak.
- Doğum yılı, özel gün gibi tahmin edilebilir şifreler kullanmak.
- Güvenli olmayan sitelerden içerik edinmek.
- Lisanslı ürünler kullanmamak.
- İşletim sistemi ve güvenlik güncellemelerini aksatmak.

Kötü Niyetli

- Şifre ve değerli bilgileri bilgisayarın yanında bulundurmak.
- Şifre ve değerli bilgileri gayri resmi kayıt altına almak.
- Değerli bilgi ve erişim bilgilerini kurum dışına çıkarmak/göndermek.
- Bağlantı ve uzaktan erişim güvenlik prosedürlerine uymamak.
- Taşınmaz ve iletişim cihazlarına zarar vermek.

Dış Tehdit Kavramı

Eski Çalışan

- Şifre ve değerli bilgileri bilgisayarın yanında bulundurmak.
- Kurumdan bilgi sızdırmak.
- Kuruma karşı art niyet beslemek ve zarar verici tutumlarda bulunmak.
- Kuruma ait değerli bilgileri kullanım amaçlı şahsen depolamak.
- İş akdini sekteye uğratabilecek önemli yerlere, giriş ve erişim yetkisinin bulunması.

Saldırgan

- Zararlı yazılımları kurum içerisine yerleştirmek.
- Kişisel hesap ve bilgileri hedef alarak kimlik hırsızlığına yönelik saldırılarda bulunmak.
- Kurum makine ve cihazlarını hedef alarak hizmet dışı bırakmaya yönelik saldırılarda bulunmak.
- Veri manipülasyonu, hırsızlığı ve tahrip etmeye yönelik saldırılarda bulunmak.

KABLOSUZ **AĞ SALDIRILARI**

Amacı kötü olduğu için "sahte" olarak isimlendirilir, gerçeğinden ayırt edilemez.

- Saldırganlar genellikle kablosuz internet kullanıcılarını hedefler
- İstemcinin, saldırgan tarafından yayın yapan bir ağa katılması halinde, tüm internet trafiği saldırganlar tarafından kaydedilebilir.
- Saldırganlar, DNS önbelleğini "zehirleyerek" sahte erişim sayfaları ve kimlik avı yapabilir.

ZARARLI YAZILIMLAR **NE YAPAR?**

Bilgisayarınızdaki **bilgilerinizi çalabilir** ve başkalarına iletebilirler.

İşletim sitemi ve programlarınızın çalışmasına **engel olabilirler**.

Bilgisayarınızdaki dosya ve klasörleri **silebilir**, kopyalayabilir, değiştirebilir veya yenilerini ekleyebilirler.

Ekranınıza can sıkıcı görseller yerleştirebilir ve **kötü amaçlı yönlendirmeler**, açılır pencereler oluşturabilirler.

Başka saldırganların da kullanması için **güvenlik açıkları** oluşturabilirler.

Zararlı programların bulaşmasına ön-ayak olabilirler.

Kişisel bilgisayarınız üzerinden başkalarına **saldırıda** bulunabillirer.

Bilgisayarınızın ya da internetin kaynaklarını kullanıp **yavaşlama**lara neden olabilirler.

Tüm verileriyle **diskinizi silebilir** biçimlendirebilirler.

ZARARLI YAZILIMLARDAN **KORUNMANIN YOLLARI**

Zararlı içerik barındırdığından şüphelenilen internet siteleri ziyaret edilmemelidir.

Güvenilirliği hakkında şüphe bulunmayan **internet siteleri** dışındaki sayfalardan hiçbir dosya indirilmemeli.

Posta kutunuza gelen hiçbir çalıştırılabilir **dosya uzantısı (.exe)** doğrudan başlatılmamalıdır.

İnternet üzerinden indirilen "**antivirüs ve spyware**" gibi programların da birer virüs olma ihtimali unutmamalı ve lisanslı ürünler kullanılmalıdır.

YAZILIM YÜKLEME **VE GÜNCELLEME**

Güvenilir olmayan yazılımlar indirilmemeli ve kullanılmamalıdır.

Kullanılan her bir programın **güvenlik açığı oluşturma** ihtimali vardır.

Kurumlarca belirlenmiş yazılımların dışında bilgisayarınızda program bulunmamalıdır.

İşletim sistemi ve **güvenlik güncellemeleri atlanmamalı** ve geciktirilmemelidir.

LOGLAMA **NEDİR?**

Tüm kurum çalışanları, öğrencileri ve misafirlerinin; erişim sağladıkları web siteleri, internet uygulamaları ve yapılan işlemlerin kayıt altına alındığı tarihte orijinal haliyle var olduğunu, **sonradan değiştirilmediğini ispatlamak** amacıyla **ZAMAN DAMGALI** olarak tutulmasına Loglama denmektedir.

LOGLAMA **YASAL MI?**

İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkındaki **5651 Sayılı Kanun** gereği kurum ve kuruluşlarda loglama zorunlu tutulmuştur.

KULLANICI ALANI **(USER DOMAIN)**

Tüm kullanıcıların merkezi bir sistemde toplandığı ve çeşitli araçlar Katmanlı bir güvenlik stratejisi için savunmanın başladığı ilk katmandır.

Kullanıcılar, yetkilerine ve erişim haklarına bağlı olarak sistemlere, uygulamalara ve verilere erişebilir.

Çalışanlar, kullanıcı kılavuzları ve yönergelere uymalıdır.

Kurumlar; çalışanlarının ve hizmet aldığı kuruluşlardan bilgiyi gizli tutmaları için bir sözleşme imzalamalarını gerekli görebilir.

Merkezi Veri Depolama: Sistemde yer alan tüm veriler tek bir veri tabanında saklanır.
Ölçeklenebilirlik: Farklı ağ gereksinimlerini karşılamak üzere (akademisyen, memur, öğrenci) ölçeklenebilme yeteneğine sahiptir.

Genişletilebilirlik: Active Directory yapısı genişletilebilme özelliğine sahiptir.

Hiyerarşik: Domain yapısı hiyerarşik bir adlandırma sistemini destekler.

Yönetilebilirlik: Birçok araç destekler ve sistem yöneticileri tarafından bu araçla yönetilebilir.

Domain Name System (DNS) ile Entegrasyon: Standart bir Internet (TCP/IP) servisi olan DNS ile entegre çalışır.

Politika-Tabanlı Yönetim: Kullanıcı ve bilgisayarların yapabileceği işlemleri yapılandırabilen merkezi politikalar düzenlenebilir. Böylece kullanıcıların yalnızca izin verilen işlemleri ve bilgisayar ayarların yapması sağlanır.

Verinin Çoğaltılması (Replication): Verinin sürekliliğini, hataya dayanıklılığını ve yük dengelemesini sağlamak için gelişmiş bir replikasyon teknolojisine sahiptir. Bu sayede bilgisayarlar arası veriler kopyalanabilir.

Entegrasyon: Sistemde oluşturulan her bir nesne için erişim kontrol edilebilir.

Tek noktadan erişim (Single Sing On): Kullanıcı adı ve şifreniz ile yapacağınız her giriş bütün özelleştirilmiş ayarlarınız ile birlikte açılır.

Active Directory

GEÇMESEK **OLUR MU?**

Başkalarının, sizin bilgisayarınızla yaptıklarından sorumlu olmamak

Bilgisayarınızı virüs ve zararlı yazılımlara karşı korumak ve

Daha güvenli bir ortamda çalışmak için bu sisteme geçilmelidir.

ISO **27001?**

Bilgi Güvenliği Yönetim Sistemi'ni tanımlayan tek uluslararası denetlenebilir standarttır.

Bilgi güvenliği yönetim sürecini sistematik bir şekilde kurmak ve işletmek için gerekli olan işlemleri içerir.

Doğru, güvenilir ve geçerli bilgiler sağlar.

Bilgi gizliliğinin korunmasını sağlar.

Riskleri minimize eder.

İş sürekliliğini sağlar.

Riski düşürerek güvenliği arttırmayı hedefler.

Yasal zorunluluk kriterlerini sağlamış olur.

75% Riskleri azaltır

80% Kuruma güven artar.

71% Korumaya yardımcı olur

55% Mevzuata yardımcı olur

53% Rekabet avantajı sağlar.

50% Hata oranını azaltır.

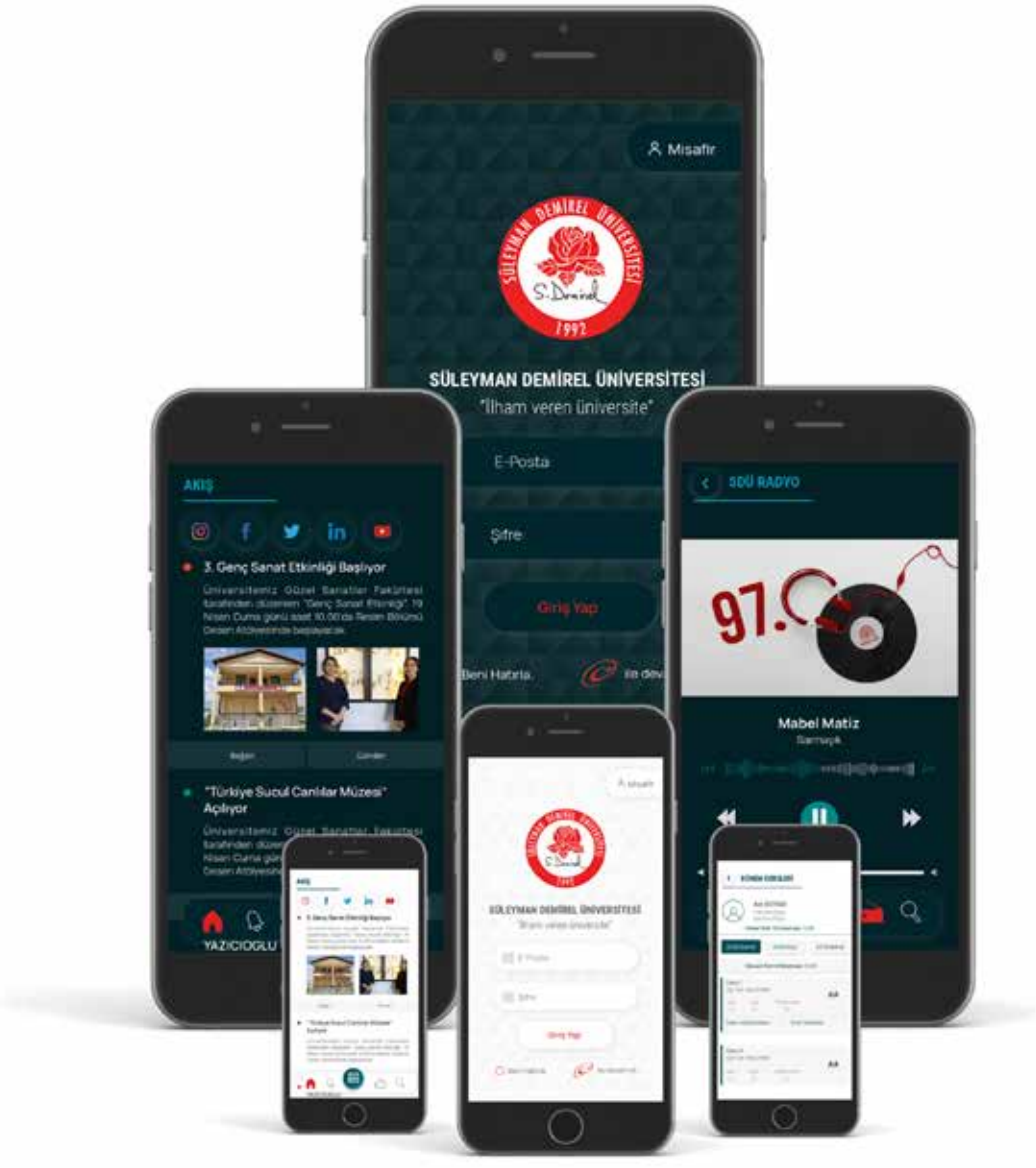
KULLANICILARA YÖNELİK **BİLİŞİM HİZMETLERİ**

Online Dilek ve
Şikayet Sistemi

Destek ve Yardım
Masası (Call Center)

Online Teknik
Destek Sistemi

MOBİL **UYGULAMA**



BİLGİ İŞLEM DAİRE BAŞKANLIĞI

BİLİŞİM FARKINDALIĞI EĞİTİMİ 2020