BİLGİ GÜVENLİĞİ PAROLA GÜVENLİĞİ, HBYS EĞİTİMİ

- Güvenliğin sadece küçük bir kısmı % 20 teknik güvenlik önlemleri ile sağlanıyor.
- Büyük kısım ise % 80 kullanıcıya bağlı.

Bilgi Güvenliği Kavramı

- Bilişim ürünleri/cihazları ile bu cihazlarda işlenmekte olan verilerin gizliliğini, bütünlüğünü ve sürekliliğini korumayı amaçlayan çalışma alanıdır.

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım
  - Temizlik görevlisinin sunucunun fişini çekmesi
  - Eğitilmemiş çalışanın veri tabanını silmesi
- Kötü Niyetli Hareketler
  - İşten çıkarılan çalışanın, kuruma ait Web sitesini değiştirmesi
  - Bir çalışanının, ağda sniffer çalıştırarak e-postaları okuması
  - Bir yöneticinin, geliştirilen yeni bir ürünün bilgilerini rakip firmalara satması

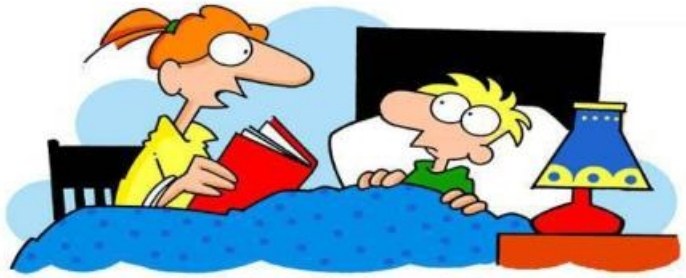
Harici Tehdit Unsurları

Hedefe Yönelmiş Saldırılar

- Bir saldırganın kurumun web sitesini değiştirmesi
- Bir saldırganın kurumun korunan bilgisini çalması
- Birçok saldırganın kurum web sunucusunu servis dışı bırakma saldırısı yapması

Bilgisayar Teknolojilerinin Kötüye Kullanımı Sonucu Oluşan Zararlar

- Bilginiz başkalarının eline geçebilir
- Kurumun toplumdaki imajı zarar görebilir (en kötü durum)
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir
- Önemli veriye zamanında erişememek
- Parasal kayıplar
- Vakit kayıpları



Romeo ve Juliet bir chat odasında buluşmuşlar ama beraberlikleri trajik bir sonla noktalanmış.

Kullanıcı Bilincinin Önemi

- Bilgi güvenliğinin en önemli parçası kullanıcı güvenlik bilincidir.
- Oluşan güvenlik açıklıklarının büyük kısmı kullanıcı hatasından kaynaklanmaktadır.
- Saldırganlar (Hacker) çoğunlukla kullanıcı hatalarını kullanmaktadır.
- Bir kullanıcının güvenlik ihlali tüm sistemi etkileyebilir
- Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır
- Kullanıcılar tarafından dikkat edilmesi gereken kurallar sistemlerin güvenliğinin sağlanmasında kritik bir öneme sahiptir.

Şifreler Güvenli Muhafaza Edilmeli

Şifre Güvenliği - I

- En önemli kişisel bilgi şifrenizdir
- Hiç kimseyle herhangi bir şekilde paylaşılmamalıdır
- Mümkünse bir yere yazılmamalıdır. Yazılması gerekiyorsa güvenli bir yerde muhafaza edilmelidir

Şifre Güvenliği - 2

- En az sekiz karakterli olmalıdır.
- Rakam ve özel karakterler (?, !, @ vs) içermelidir.
- Büyük ve küçük harf karakteri kullanılmalıdır.
- Kişisel bilgilerle ilişkili olmamalıdır (doğum tarihi, öğrenci numaranız, vb.)
- Örnek: Güçlü bir şifre: Ag6486kt!
- Güvenli olmadığını düşündüğünüz mekanlarda kurumsal şifrelerinizi kullanmanızı gerektirecek uygulamaları kullanmayınız.

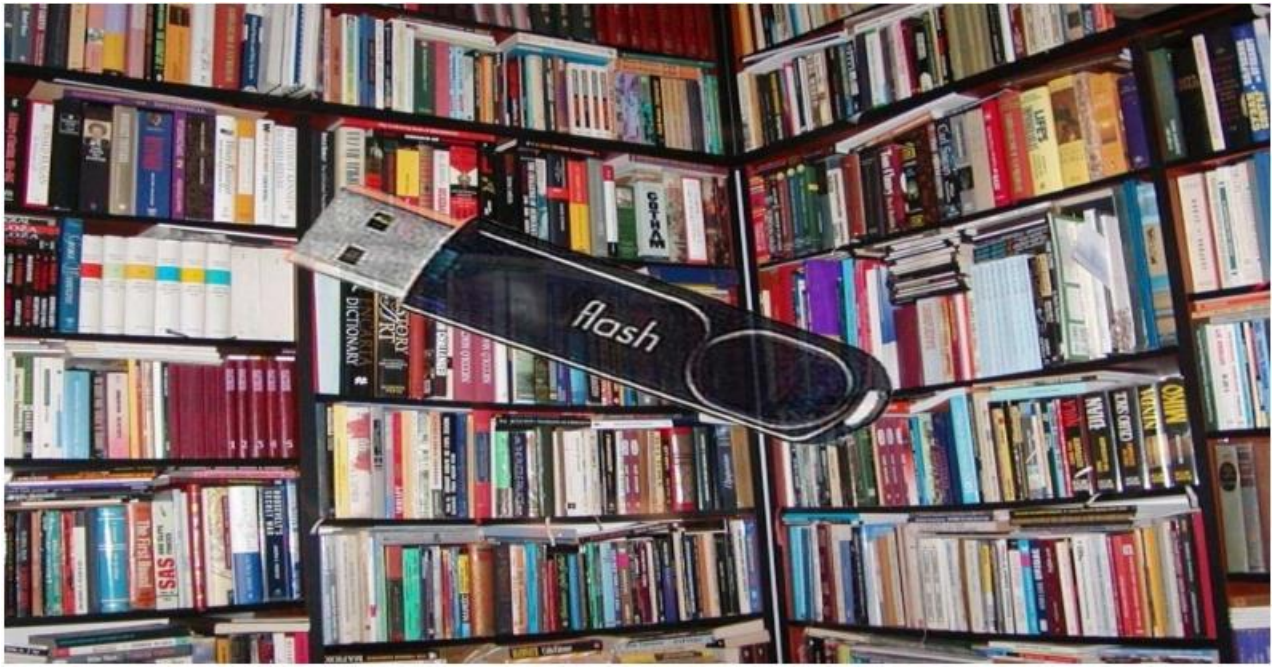
Kötü Şifre Örnekleri

- 12345
- abcdef
- 1905
- 111111
- 13579
- aaaaa
- q1w2e3
- 123123 …
- 000000
- zeynep
- zeynep2012
- Zeynep123

Yazılım Yükleme- Güncelleme

- Kurum tarafından belirlenmiş yazılımların dışında bilgisayarlarda program bulunmamalıdır. Her bir programın açıklık oluşturma ihtimali vardır.
- Güvenilir olmayan sitelerden yazılımlar indirilmemeli ve kullanılmamalıdır

- ☐ Bir USB bellek, 1 milyon adet kağıtta yer alan bilgi kadar veri içerebilir.



Dizüstü Bilgisayar Kullanımı

- Çalınmalara karşı fiziksel güvenlik sağlanmalıdır.
- Şifre güvenliği sağlanmış olmalıdır.
- İçinde kurumsal veri olmamalıdır.
- Eğer veri şifreleme sistemi kurumda kullanılıyor ise gizli bilgiler şifrelenmelidir.

Zararlı Programlar- Virüsler

- Tüm bilgisayarlarda virüs koruma programı çalıştırılmalı ve güncellemesi yapılmalıdır.
- Anti virüs programı kapatılmamalıdır.
- Dosyalar virüs taramasından geçirilmelidir.

E-posta Güvenliği

- Virüslerin en fazla yayıldığı ortam e-postalardır.
- Kaynağı tanınmayan e-postalar kesinlikle açılmamalıdır.
- Güvenilmeyen eklentiler açılmamalıdır.
- Gizli bilgi şifrelenmedikçe e-postalarla gönderilmemelidir.
- Spam e-postalara cevap verilmemelidir.
- E-posta adres bilgisi güvenilir kaynaklara verilmelidir.

Hastane Bilgi Yönetim Sistemi Güvenliği Prosedürü

- Çukurca Devlet Hastanesine başvuruda bulunan kişilere ait bilgilerin güvenliğinin sağlanması amaçlı öncelikle
- Verilerin doğru olarak toplanması,
- Depolanması, kullanılmasına ilişkin uygulamalarımızı ve güvenlik önlemlerimizi dâhili olarak gözden geçirmek.
- Kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemlerini almak ve bunun devamlılığını sağlamaktır.

Hastane Bilgi Yönetim Sistemi Güvenliği Prosedürü

- Bu talimatın amacı, hastaya ait bilgilerin mahremiyeti konusunda uyulması gereken kuralları tanımlamaktır.

FAALİYET AKIŞI

- Tüm hasta bilgilerinin girişi HBYS'nde tanımlanan alanlara yapılmaktadır.
- Hasta bilgilerinin güvenliği için tüm kullanıcılar için her kademede yetkilendirme yapılmalı ve kontrol edilmelidir.
- Sunucu üzerindeki her türlü yazılım, işletim sistemi, veritabanı, Yazılım Firması elemanları tarafından, Bilgi İşlem Bölümü denetiminde yapılır.
- Tüm fax-modem üniteleri ile haberleşme ve İnternet erişim yazılımlarının kurulması ve ayarları Hastane Bilgi İşlem Bölümünün yetkisinde olacaktır.

İŞLEYİŞ

1. Hastanemizde bilgi güvenliği konusunda *gizlilik, bütünlük ve erişebilirlik* olmak üzere 3 temel prensip göz önünde bulundurulmaktadır.
2. Bilgisayar uygulamalarında ve veri tabanı sunucularında donanım ve yazılıma ait problemler ortaya çıktığında Bilgi İşlem Sorumlusu durumdan haberdar edilir.
3. Hastanemize destek hizmeti veren firmaların dış ortamdan iç ortama hangi durumlarda erişim yapacağı hastanemiz ile firmalar arasında imzalanan ve her iki tarafın da onayladığı teknik şartname ve hizmet alım sözleşmelerine göre kayıt altına alınmıştır.

HASTALARIN VE ÇALIŞANLARIN KAYITLARININ GÜVENLİĞİ

- Hastalara ve çalışanlara ait bilgilerin güvenliğinin sağlanması amacıyla öncelikle sisteme kayıt edilen veriler doğru olarak toplanır, depolanır ve bilgilerin kullanımına yönelik uygulamalar ve güvenlik önlemleri belirli periyotlarla gözden geçirilir
- Tüm hasta bilgilerinin girişi HBYS'de tanımlanan alanlara yapılmaktadır.
- Kişisel verilerin depolandığı sistemler yetkisiz erişime karşı korunmaktadır.
- Elektronik ortamdaki verilerin güvenliği sağlanmaktadır.

HASTALARIN VE ÇALIŞANLARIN KAYITLARININ GÜVENLİĞİ

- Hasta ve çalışanların kişisel bilgilerine erişim, Yetkilendirme İşleyişi doğrultusunda, sadece bilgilere ulaşma yetkisi bulunan hastane çalışanları ile sınırlı tutulur ve bu kişiler gizliliği koruma yükümlülüklerini bilerek çalışır
- Hastanemizde hasta ile ilgili bilgilerin bütünlüğü ve güvenliği kurulmuş olan bilgisayar yazılım programlarında yetkilendirilmiş girişler ile korumaya alınmıştır.
- İlgili mevzuat hükümleri saklı kalmak kaydıyla, hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemektedir.

DÜZELTİCİ ÖNLEYİCİ FAALİYETLERİN PLANLANMASI

- Bilgi güvenliği ihlalleri raporlanır ve Bilgi Güvenliği Ekibi' ne bildirilir ve bu ihlalleri engelleyecek önlemler alınır.
- Yaşanan acil durumlar sonrası işleyiş ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmektedir.

-PLANLA

-UYGULA

-KONTROL ET

-GERİ BİLDİRİM AL

Eğitimi tamamla butonuna tıklamayı unutmayın!

TEŞEKKÜRLER ☺