TEKNOLOJİ MİMARI
www.teknolojimimari.com

# Sağlık Kurumlarında Alınması Gereken Siber Güvenlik Tedbirleri

**Şevki Hüseyin AKGÜN**

**Satış Müdürü**

sevki.akgun@teknolojimimari.com

**Aralık 2023**

# Siber Güvenlik ?

Siber güvenlik; bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir.

# Bilgi Güvenliği Kavramı

**Bilgi Güvenliği,** bilginin siber tehditlere karşı doğru standartlarda ve uygun bir şekilde korunmasıdır.

**BİLGİNİN KORUNMASI**


- **Gizlilik:** Bilginin yetkisiz kişi veya diğer varlıklar tarafından erişilememesi gerekmektedir.
- **Bütünlük:** Varlıkların doğruluğunun ve bütünlüğünün korunması gereklidir.
- **Erişebilirlik:** Bilgiler yetkili tarafından talep edildiğinde erişilebilir olmalıdır.

**Bilginin gizliliği, bütünlüğü ve erişebilirliğinin korunması gereklidir.**

**Kişisel Veri**

Kimliği belirli yada belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi

Örnek: Ad/Soyad, TCKN, adres, e-mail, …

**Özel Nitelikli Kişisel Veri**

Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği ve biyometrik ve genetik verileri

Örnek: Kan grubu, sağlık verileri vb.

**Veri Sorumlusu**

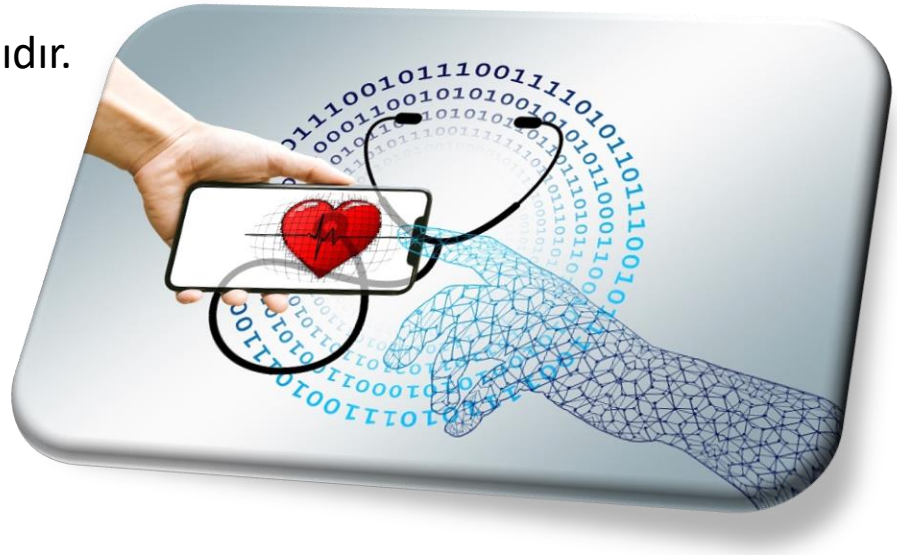
Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi

**Veri İşleyen**

Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi

# Sağlık Sektöründe Siber Güvenlik Riski Artıyor !!!

- Son 2 yılda sağlık sektörüne siber saldırı oranı **%71** oranında artmıştır.
- Güncelliğini yitirmiş teknolojik cihaz ve yazılımlar kullanmak olumsuz yönde etkilemektedir.
- Kullanıcılarda yetkilendirme ve kısıtlama yapılmaması olumsuz sonuçlar doğurabilir.
- Data sızıntıları ve kayıplarının büyük bir bölümünün temeli **“insan”** kaynaklıdır.
- Herkese açık ağ bağlantıları güvenli değildir.



# Fidye Saldırıları RANSOMWARE

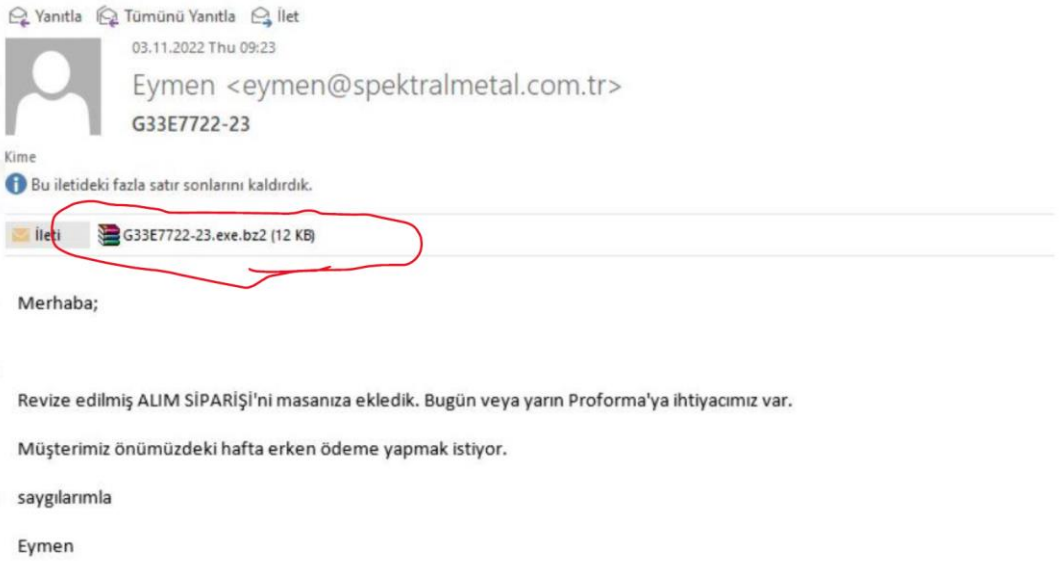
Fidye yazılımı, saldırganların bir cihazı kilitlemek veya içeriğini şifrelemek için kullanabilecekleri bir zararlı yazılımdır. Saldırganlar cihazın sahibinden veya kullanıcısından verileri geri vermek üzere para talep eder fakat fidye ödense de verilerin geri alınacağının garantisi yoktur.


Fidye yazılımı üreten siber suçluların kullandıkları birkaç teknik vardır. Bunlar;

- Ekran kilitleyen fidye yazılımı
- PIN kilitleyen fidye yazılımı
- Disk şifreleyen fidye yazılımı
- Şifreli fidye yazılımı

# Fidye Saldırıları Oltalama (Pishing)

**Oltalama (Pishing)**
Bilgilere ulaşmak için en sık kullanılan yöntemlerden biridir.




| |
|---|
| **Bilişim Güvenliği Sorunu:** Mail Sunucusuna Saldırı ve Güvenlik Açığı |
| **Sorun Yaşanan Müşteri:** YYY Hastaneler Grubu |
| **Sorun Tarihi:** Şubat 2016 |
| **Sistemin Çalışamadığı Zaman:** 5 Gün kesintisiz (Sorun farkındalığına kadar 15 gün) |
| **Sorunun Olmaması için Yapılması Gereken Yatırım:** 150.000,00 TL |
| **Sorun Çözülmemesi Durumunda Müşterinin Tahmini Zararı:** 4.000.000,00 TL |
| **Sorun Çözümlenmesi İçin Harcanan Bedel:** 250.000,00 TL |
| **Kurtarılan Data Oranı:** %95 (ancak prestij ve hasta kayıpları) |

**Olayın Detayı:**

Hali hazırda hizmet veren YYY Hastaneler grubunda güvenlik açıklarından dolayı Exchange mail sunucularının hacklenmesi ile birlikte kurum için/dışı iletişim kesilmiş anlaşmalar, provizyonlar ve birçok noktada tedarikçi/müşteriler ile olan süreçler yürütülemez duruma gelmiştir.

Bu konuda kurumun yaşamış olduğu

-Resmi kurumlar ile olan iletişim kesiklikleri ve onay provizyon kesintileri

-Yurtdışı müşteriler ve sağlık turizmi için iletişim kopuklukları

-Kurum içi iletişim ve operasyonun nerdeyse tamamen durması

- Prestij kayıpları gibi sorunlardan dolayı, ölçülebilen zarar 4 milyon TL olmakla birlikte zedelenen kurum imajının maddi değerinin ölçülmesi çok mümkün olmamıştır. Kurumun sistem disaster ve yedekleme işlemleri için yatırım yapması gereken miktar zararının 1/30 katı kadar bir miktardır. Ancak zamanında uyarılara rağmen yatırımı dönüştürülmeyen yapılar, sorunlarla karşılaşıldığı durumlarda kat ve kat fazla bedel ile sistemin yeniden idamesi için bedel ödemektedir. Eş zamanlı olarak ise kaybedilen zaman, prestij, güven duygusu, iş gücü kurumların yanında kar olarak kalmaktadır.

# Yedek Almak Çok Önemli !

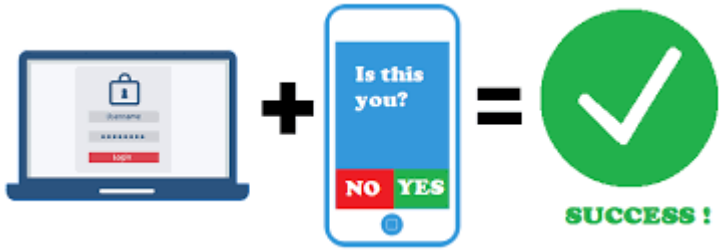
- ✓ Lisanslı programlar ile yedek alınması
- ✓ Alınan yedekten geri dönüş
- ✓ Belirli aralıklarla yedek alınması
- ✓ Güvenilir bulut(cloud) ortamlarına yedek alınabilir

TEKNOLOJİ MİMARI
www.teknolojimimari.com

# Sağlık Kurumlarında Alınması Gereken Siber Güvenlik Tedbirleri

Mutlaka bilgisayarlarınızda ve sunucularınızda lisanslı fideye koruması olan Endpoint çözümleri kullanın.


Uzaktan erişim durumlarında VPN bağlantılarını tercih edin.




VPN bağlantılarında mutlaka MFA yani çoklu faktörlü kimlik doğrulama çözümleri kullanın.

Çalışanlarınıza temel siber güvenlik eğitimi aldırın.

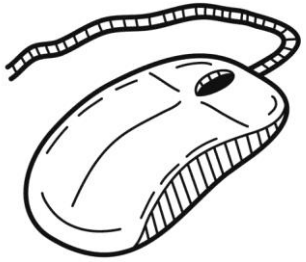
TEKNOLOJİ MİMARI
www.teknolojimimari.com

# Sağlık Kurumlarında Alınması Gereken Siber Güvenlik Tedbirleri

- ✓ Firewall ve Endpoint Koruma Sistemleri 5651
- ✓ DLP ve MDM Çözümleri
- ✓ DDOS ve SIEM Çözümleri
- ✓ İstenmeyen e-posta politikanızı geliştirin(SPAM)
- ✓ Network Yönetimi (Yönetilebilir cihazlar VLAN yapısı)
- ✓ Firmware Güncellemeleri
- ✓ Medikal Cihazlar Güvenliği
- ✓ Penetrasyon Testi
- ✓ Yeni Nesil Teknolojik Ürünler Kullanımı

# Siber Güvenlik Temel İpuçları

- ✓ Şifrenizi asla kimseyle paylaşmayın
- ✓ Basit şifreler kullanmayın ve aynı şifreleri farklı platformlarda kullanmayın
- ✓ Sahte mail hesaplarına dikkat edin
- ✓ İnternette güvenli gezinin
- ✓ Güvenli VPN bağlantısı kullanın
- ✓ İndirdiklerinize dikkat edin



# Bütüncül Yaklaşım


Bilişim Teknolojileri (BT) uygulamaları bir bütün olarak algılanmak zorundayız.

Hedef ne kadar piramidin üst katmanını sağlamak olsa da, alt katmanlarda oluşacak bir problem doğrudan üst katmanları etkileyecek ve kurumsal işlevselliği bozacaktır.


Bilgi işlem ekibi sizler için 7/24 sistemleri
ayakta tutmak için arka planda çalışan gizli kahramanlar.

Dinlediğiniz için teşekkürler.