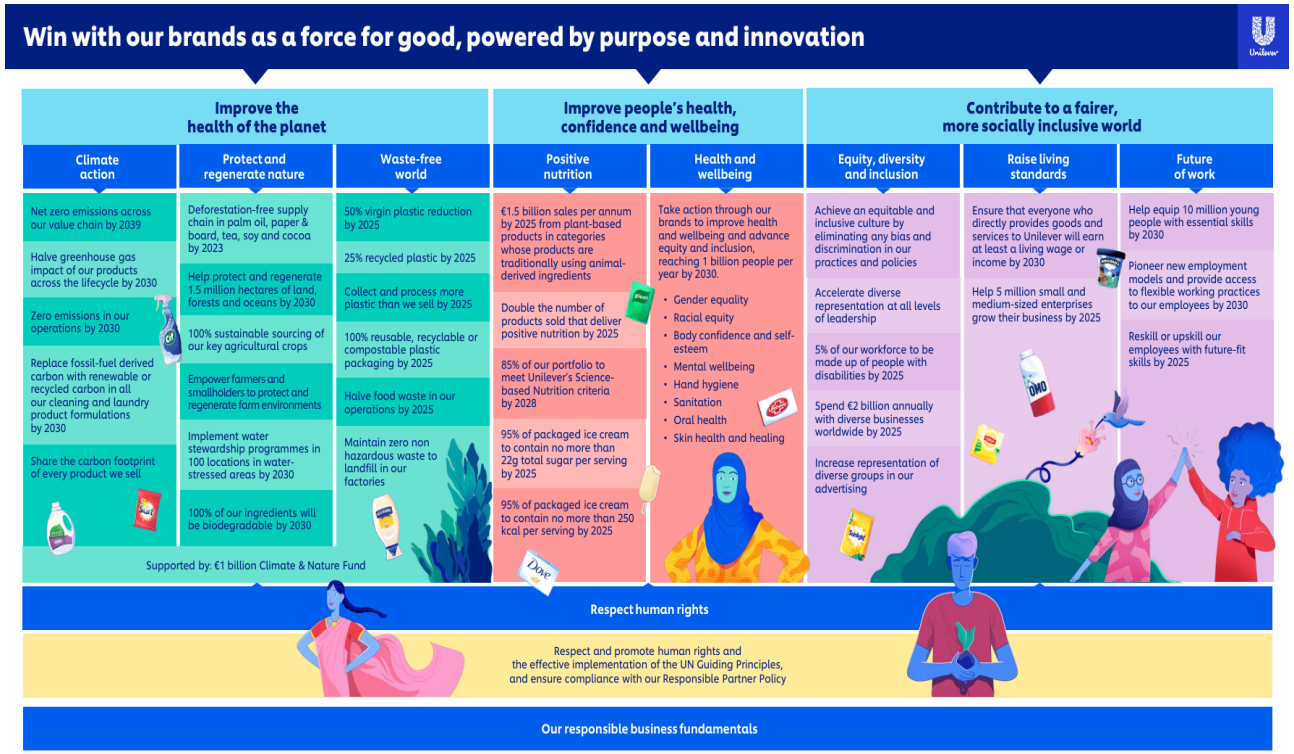
Ant Teknik

Bilgi Güvenliği Eğitimi

Ant Teknik İş Kuralları



Ant Teknik çalışanları olarak; Müşteri/**Tedarikçi** Beklentilerine, Sözleşme Gereksinimlerine, İnsan Kaynakları Prosedürlerine, Bilgi Güvenliği, KVKK ve Etik kurallarına uymamız gerekmektedir.
Bu konularda detaylı bilgiler www.antteknik.info adresinde bulunabilir.

Neden Bilgi Güvenliği ?

Bilgi güvenliği şirketlerin kanunlara, müşterileri ve tedarikçilerle yapılan anlaşmalara uyumu ve şirketin sürdürülebilirliğinin sağlanması için önemlidir.

Yasalara ve Standartlara Uyum

KVKK, GDPR ve **TCK'**nın 135-140.maddeleri, ISO 27001.

Finansal Varlıkların Korunması

Şirketin ve çalışanların ve **finansal** varlıklarının, gizliliği ve korunması.

Bilgi Varlıklarının Korunması

Sahip olan şirket sözleşmelerinin, müşteri ve ürün bilgilerinin, **ücret bilgilerinin**, stratejik kararlarının, kritik üretim ve satın alma bilgilerinin korunması.

Hissedarların ve Çalışanların Güvenliği

Kişilerin özel hayatının, kritik bilgilerinin (davalar, mali bilgiler, konum bilgileri, resimleri, e-posta iletişimi, internet ve sosyal medya kullanımının) korunması.

KVKK : İlgili Yasalar ve Yaptırımlar

KİŞİSEL VERİLERİN KORUNMASI KANUNU

MADDE 17- (1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.

(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun **138 inci maddesine** göre cezalandırılır.

Kabahatler
MADDE 18- (1) Bu Kanunun;
a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler

hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,
b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine

getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar....

TÜRK CEZA KANUNU

Madde 135- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye **bir yıldan üç yıla kadar hapis** cezası verilir.

Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, **iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.**
Madde 138- (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın **verileri sistem içinde yok etmekle yükümlü olanlara** görevlerini yerine getirmediklerinde **bir yıldan iki yıla kadar hapis cezası verilir.**

Madde 139- (1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması **şikayete bağlıdır.**

TÜRKİYE CUMHURİYETİ ANAYASASI

MADDE 20-

(Ek fıkra: 12/9/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Bilgi Güvenliği : İlgili Yasalar ve Yaptırımlar

KVKK & TCK — Kişisel Verilerin Korunması (TCK 135-139)

- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. (TCK 135)

İş Kanunu — Çalışanın Sadakat Yükümlülüğü (Madde 25-26)

- İş ilişkisi devam eden işçi tarafından sır saklama borcunun ihlal edilmesi durumunda işçinin iş akdini İş Kanunu 25. maddenin 1. fıkrasının (II) numaralı bendinde yer alan "ahlak ve iyi niyet kurallarına" aykırılıktan haklı nedenle feshedebilecek ve işçinin bu eylemleri sebebi ile uğramış olduğu zararları ispat edebildiği ölçüde maddi ve manevi tazminat talep edebilecektir.

Borçlar Kanunu — TBK Madde 396. Fıkra 4.

- TBK 396. maddenin 4. fıkrasında “İşçi, iş gördüğü sırada öğrendiği, özellikle üretim ve iş sırları gibi bilgileri, hizmet ilişkisinin devamı süresince kendi yararına kullanamaz veya başkalarına açıklayamaz.

Bilgi Güvenliği : İlgili Yasalar ve Yaptırımlar

Çalışanlar Hangi Bilgileri Dikkatle Korumalıdır?

- İş veya iş yeri ile ilgili bulunan veya müşteri / tedarikçi sözleşmelerinde tanımlanan,
- Üçüncü kişiler tarafından bilinmeyen,
- Kamuya mal olmamış ve aleniyet kazanmamış,
- Ancak iş yerinde çalışan kişi ve/veya kişilerce bilinebilen,
- İşverenin de başkaları tarafından öğrenilmesini istemediği,
- Saklı kalmasında haklı bir menfaatinin bulunduğu,
- Basitçe ve kolayca öğrenilemeyecek her türlü ticari ya da **kişisel bilgidir.**

Türkiye’de ve Dünya’da Örnek Vakalar

SMS ve Telefon

Dolandırıcılık

Şirket Sırları

esla Çalışanı, Binlerce Dosyalık Ticari Sırları Çaldı

alışanını Şirketteki İlk Haft
irket Sırrını' Çaldığı İçin Dav

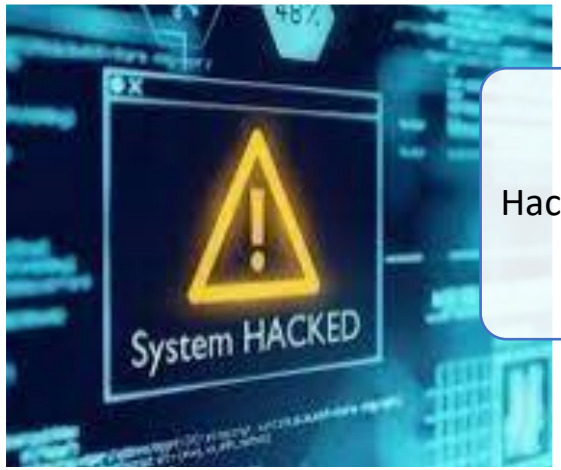
önce 2 dk okuma süresi

ette çalışmaya başladığı ilk üç gün için
almaya başladığı için bir yazılım mühe ndisin
en çalışan ise iddiaları reddediyor.

erin sık sık karşılaştığı durumlardan biri de şirkete ait hassa
ması girişimleri. Elektrikli otomobil sektöründe bayrağı ta
urumlarla karşılaşıyor. Yaşanan son vaka ise bir bakıma oldu

Ticari Sırların Çalınması

Sistemlerin Hacklenmesi

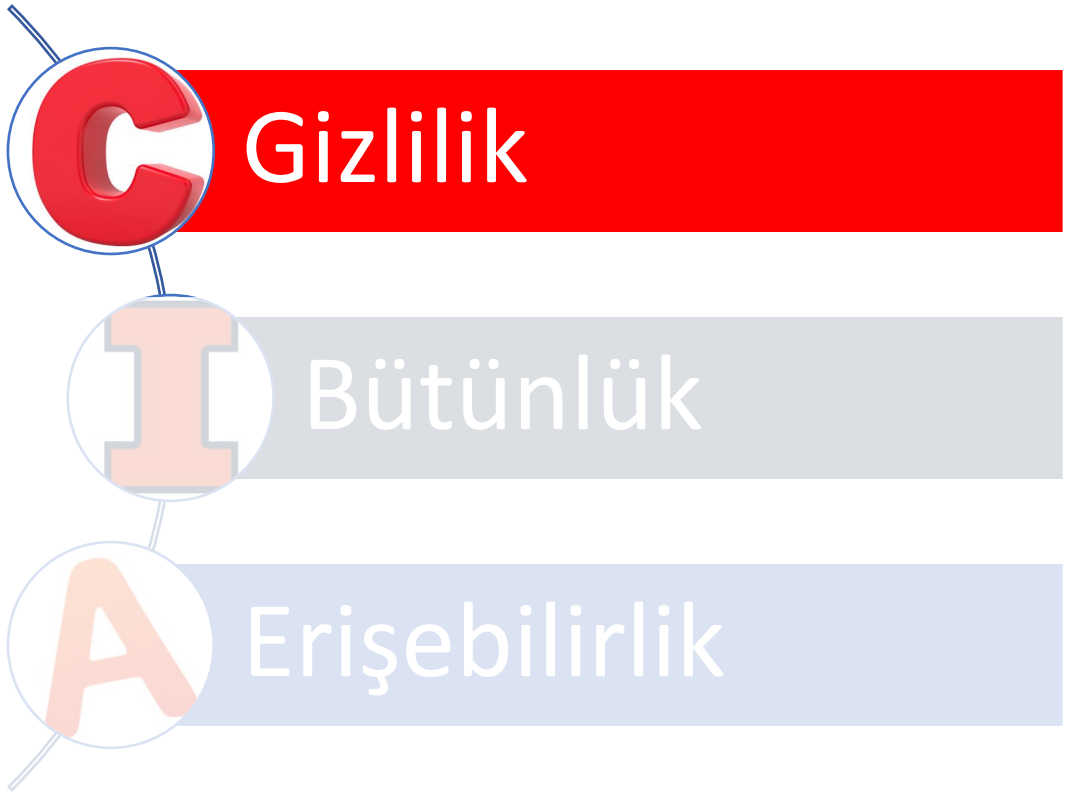


Hacklenme

Bilgi Güvenliği: Temel Kavramlar

Bilgi Güvenliği: Temel Kavramlar

Gizlilik (Confidentiality): Bilginin **yetkisiz kişilerin** eline geçmesini engellemeyi amaçlamaktadır. Bilgi hem bilgisayar sistemlerinde **işlenirken** (process), hem saklama ortamlarında **depolanırken** (storage), hem de ağ üzerinde gönderici ve alıcı arasında **taşınırken** (transport) yetkisiz erişimlerden korunmalıdır. Saldırgan bir yapılandırma veya yazılım hatasını istismar ederek yahut Sosyal Mühendislik teknikleri ile yetkili insanların hatalarını istismar ederek bilgilere izinsiz olarak erişebilir. Bu prensipte dikkat edilmesi gereken nokta, bilginin tamamen gizlenmesini sağlamak değil, **yetkisiz bir şekilde** elde edilmesini engellemek ve erişilebildiği durumunda da bundan haberdar olunabilmektir.

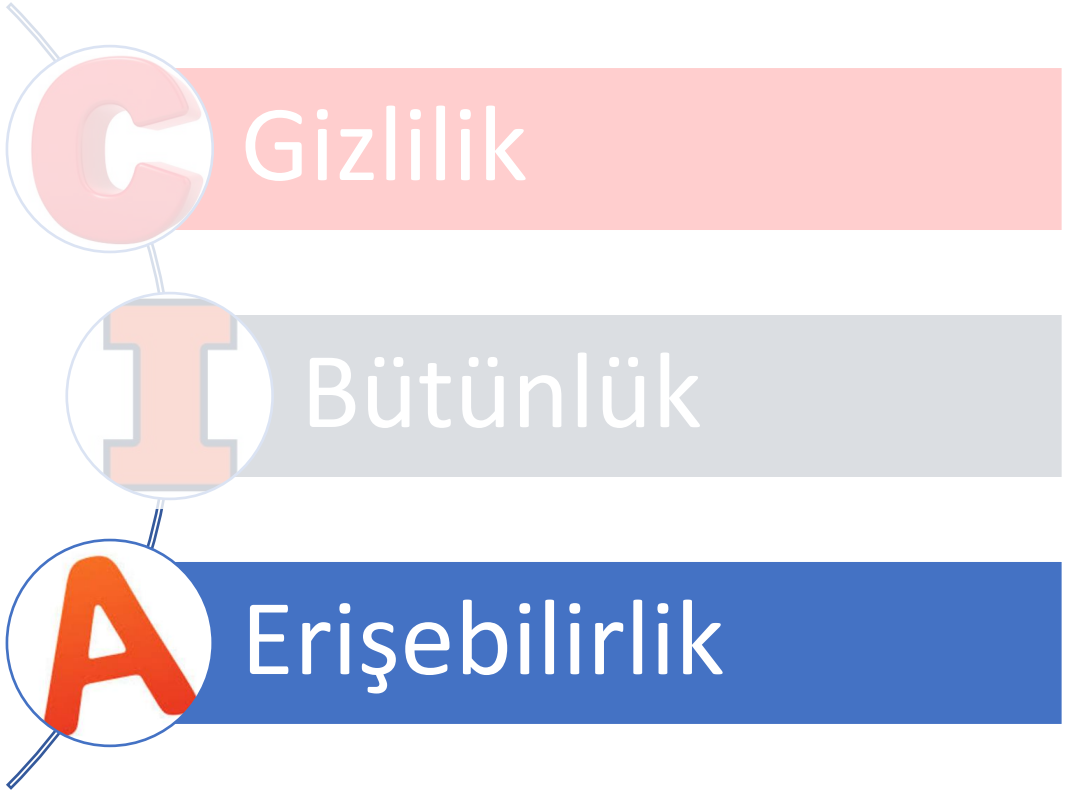


Bilgi Güvenliği: Temel Kavramlar

Bütünlük (Integrity): Amaç, bilgiyi olması gerektiği şekilde tutmak ve korumaktır.
Bilginin **bozulma**sını, **değiştirilme**sini, yeni veriler **eklenme**sini, bir kısmının veya tamamının **silinme**sini engellemeyi hedefler. Bu durumda veri, saklama veya haberleşme sırasında değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş şekilde işlenir. Bütünlük prensibi temel olarak Sistem Bütünlüğü ve Veri Bütünlüğü olarak iki kısımda incelenebilir. Bu prensipte dikkat edilmesi gereken nokta, bilginin değiştirilmemesini sağlamak değil, **yetkisiz bir şekilde** değiştirilmesini engellemek ve değişiklik durumunda da bundan haberdar olabilmektir.

Bilgi Güvenliği: Temel Kavramlar

Erişilebilirlik (Availability): Bilginin (verinin, kaynağın, sistemin) **hedeflenen ve ihtiyaç duyulan süre** boyunca ulaşılabilir ve kullanılabilir olmasını, **tam** ve **eksiksiz** olarak yapılmasını amaçlayan prensiptir. Erişilebilirlik; bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarım düşürücü tehditlere karşı korumayı hedefler. Erişilebilirlik hizmeti sayesinde, kullanıcılar, **erişim yetkileri dahilinde** olan verilere, **veri tazeliğini yitirmeden**, zamanında ve **güvenilir** bir şekilde ulaşabilirler. Bu prensipte dikkat edilmesi gereken nokta, erişilebilirlilik ile gerekli verilere ilgili kullanıcıların güvenli ve sürdürülebilir erişim imkanının sağlanmasıdır.



Tehdit Türleri ve Riskler

Hackerlar

Siber Tehditler

- Phishing (oltalama), sosyal mühendislik saldırıları, malware (zararlı yazılımlar), ransomware (fidye yazılımları) gibi yaygın siber tehditler.

Çalışanlar

İç Tehditler

- Çalışanların kasıtsız hataları veya kasıtlı kötü niyetli hareketleri.

Suçlular

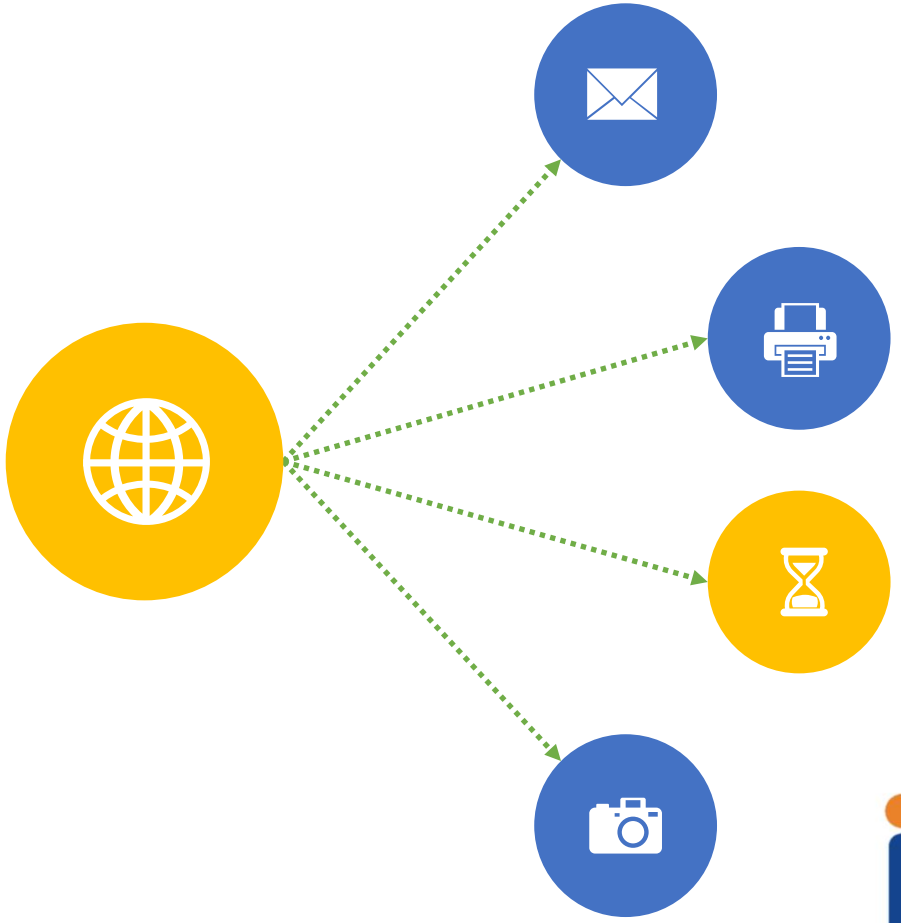
Fiziksel Güvenlik Tehditleri

- Fiziksel güvenlik, cihazların çalınması, kaybolması veya sabotaj gibi durumlar.

Hackerlar Kimi Hedef Alıyor ?

Siz olsanız kimleri hedeflerdiniz?

Yapılan araştırmalar göstermiştir ki, yöneticiler ve çocuklar saldırıların ana hedefleridir. Dark Web pazarlarında, CEO e-posta adres listeleri genellikle ek kimlik avı saldırıları gerçekleştirmek, hassas bilgilere erişim sağlamak veya iş e-postası uzlaşması (BEC) ve kimliğe bürünme gibi diğer sosyal mühendislik saldırılarını gerçekleştirmek amacıyla satılır ve satın alınır. (Trendmicro). Hırsızlıktan tacize bir çok suç için kötü niyetli kişiler tarafından sosyal mühendislik çalışmaları yapılmaktadır.



Sosyal Medya

Her uygulamayı kendiniz denetleyemezsiniz. Pratik çözümler kullanın.

Mobil Cihazlar

Mobil cihazlarınızı ve uygulamalarınızı kendiniz yönetin.

Ev Networkleri

İş yerinizde ağ güvenliği için yatırımlar yapılıyor. Peki ev networkünüzü kimler kullanıyor biliyor musunuz?

Şifre Yönetimi

Basit önlemler ile ve multi factor authentication ile riskinizi azaltın.

MANASSET Staffing Solutions

MANASSET Staffing Solutions

Bilgi Güvenliği Riskleri

ÖZEL HAYAT

Özel Hayatın Gizliliği

- Kişisel varlıklar
- Davalar
- Cinsel hayat
- Resimler

İFŞA RİSKLERİ

KURUMSAL

Şirket Bilgileri

- Ar-Ge
- Üretim Proses Bilgileri
- Fiyatlar-Müşteriler
- Kritik Çalışanlar

BİLGİ HIRSIZLIĞI

FİNANSAL

Finansal Bilgiler

- Banka hesapları
- Ödeme emirleri
- E-Devlet uygulamaları
- Talimatlar

FİNANSAL RİSKLER

MARKA

Algı

- Şirketin dijital algı yönetimi
- Şirket çalışanlarının sosyal medya algı yönetimi
- Müşteri ve tedarikçilerin sosyal medya algı yönetimi
- Kullanım esasları

ALGI YÖNETİMİ

Neden Bilgi Güvenliği?

Şirketlerin bilgi güvenliği konusunda gerekli önlemlere sahip olmamasının olumsuz sonuçlarını aşağıdaki başlıklarda gözlemledik:

- Çevrimiçi hesaplara erişimin sağlanamaması
- Adınıza yapılan çevrimiçi suiistimaller
- Bağlantılarınızın sosyal olarak tasarlanması riski
- Yanlış çevrimiçi iddialarla itibarınızın zedelenmesi
- Şantaj veya dolandırılma
- Hassas fotoğrafların veya videoların açığa çıkarılması

Hacker'lardan şantaj ve para talebi, kritik sistemlerin fidye almak için ele geçirilmesi, mali işlerle iletişime geçme sonrasında ödeme çıkartılması, davalarının ve özel bilgilerinin yetkisiz kişilerce işlenmesi sıkça yaşanan bilgi güvenliği olaylarıdır.

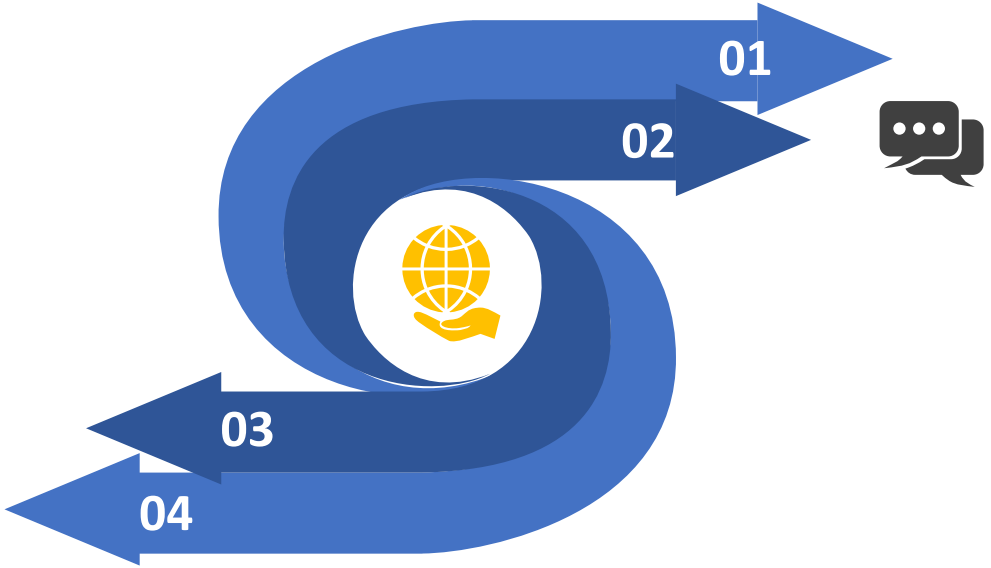
Neden Bilgi Güvenliği ? Algoritmalar Nasıl Çalışır?

Hackerlar Kimleri Hedef Alıyor?

Hackerlar dünyanın her yerinde kritik sektörlere, stratejik kurumlara ve ekonomik, politik, sosyal olarak nüfuslu kişilere yönelik saldırılar düzenlemektedirler.

Terör Örgütleri Kimleri Hedef Alıyor?

Sadece siber saldırılar değil fiziksel saldırılar, adi suçlar ve terör saldırıları da ekonomik, politik, sosyal olarak nüfuslu kişileri ve üst düzey yöneticileri hedef almaktadırlar.



Bilgi Hırsızları Kimin Verilerini Alır?

Bilgi hırsızları, şirket verilerini, ticari bilgileri, kişisel bilgileri kullanarak şirketleri ve çalışanları maddi veya manevi zararlara uğratmaktadırlar.

İstihbarat Birimleri Kimleri Takip Eder?

Dünya'da ve ülkemizde her türlü soruşturmada Teknik takipler, sosyal medya analizinden şikayetlerin takibine kadar birçok alanda kamuya mal olan ya da önemli mevkilerde bulunan kişiler için daha hassasiyetle yapılmakta bir çok önemli kişi, soruşturmalarla ve tahkikatlarla karşı karşıya kalmaktadırlar.

Sosyal Medyanın Hukuki Davalara Etkisi

Günümüzün dijital çağında sosyal medya günlük hayatımızın ayrılmaz bir parçası haline geldi. Facebook, Twitter, Instagram ve TikTok gibi platformlar düşüncelerimizi, deneyimlerimizi ve anlarımızı küresel bir izleyici kitlesiyle paylaşmamıza olanak tanıyor.

Sosyal medya sayısız faydalar sunarken, özellikle hukuki konular söz konusu olduğunda önemli riskleri de beraberinde getiriyor.

Sosyal Medya Faaliyetleri Ceza Davalarını Nasıl Etkileyebilir?
I. Ceza Davalarında Delil Olarak Sosyal Medya

II. Hukuki Davalarda Sosyal Medya Etkinliği ve Karakter Değerlendirmesi

III. Hukuki Davalarda Sosyal Medyanın Tanık Güvenilirliğine Etkisi

IV. Sosyal Medyada Gizlilik Yanılsaması ve Hukuki Sonuçları

Amerikan Aile Hukuku Akademisi'nin (American Academy of Matrimonial Lawyers - AAML) 2010 yılında yaptığı bir araştırmada, aile hukuku avukatlarının %81'i, davalarda sosyal medyanın önemli bir delil kaynağı haline geldiğini bildirmiştir.

Dijital Ayak İzi - WhatsApp

Devletler, yasal düzenlemelere uygun olarak belirli durumlarda mesajları inceleyebilir. Bu tür incelenebilirlik, genellikle suç soruşturması veya ter örle mücadele gibi durumlarda gerçekleştirilir.

- **Mesajları Kalıcı Olarak Sil: Mesajları tek tek silmek yerine, bir konuşmayı tamamen silmek daha güvenlidir. WhatsApp'ta bir konuşmayı silmek için, ilgili sohbeti basılı tutup "Sil" seçeneğini seçebilirsiniz.**
- **Yedeklemeleri Kapat: WhatsApp yedekleme özelliğini kapatarak, gelecekteki yedeklemelerde silinen mesajların bulunmamasını sağlayabilirsiniz. Bunun için Ayarlar > Sohbetler > Sohbet yedeği > Yedekleme ayarları kısmından otomatik yedeklemeleri kapatabilirsiniz.**
- **Veri Temizleme Uygulamaları Kullan: Cihazında kalan artık dosyaları ve önbellek dosyalarını temizlemek için güvenilir bir veri temizleme uygulaması kullanabilirsiniz. Bu tür uygulamalar, silinen mesajların kalıntılarını cihazından tamamen kaldırır.**
- **Cihazı Fabrika Ayarlarına Döndür: En kesin çözüm cihazını fabrika ayarlarına döndürmektir. Bu yöntem, cihazındaki tüm verileri kalıcı olarak siler, ancak bu işlemin geri alınamayacağını unutmayın.**

Çalışanlar Ne Yapmalı ?

Süreç Sahipleri/Birim Yöneticileri, sorumluluk alanlarında işledikleri kritik bilgileri tanımlamalı ve riskleri yönetmelidirler.

Risk yönetiminde riskin oluşma olasılığı, şirkete etkisi ve CIA açısından değerlendirme yapılmalıdır.

Çalışanlar Ne Yapmalı?

1. Şifre Güvenliği

•Güçlü Şifre Oluşturma:

Şifreler en az 8-12 karakter uzunluğunda olmalı ve büyük/küçük harfler, sayılar ve özel karakterler içermelidir. Örneğin, "B1lG!GvNlk21".

•Şifreleri Düzenli Olarak Değiştirme:

Şifreler her 3 ayda bir yenilenmelidir. Aynı şifrenin farklı hesaplarda kullanılmaması gerekiyor.

•Şifreleri Paylaşmama:

Hiçbir koşulda şifreler başka biriyle paylaşılmamalıdır. Şirket yönetimi bile şifre istememelidir.

2. İki Faktörlü Kimlik Doğrulama (2FA) Kullanımı

•2FA'yı Aktif Hale Getirme:

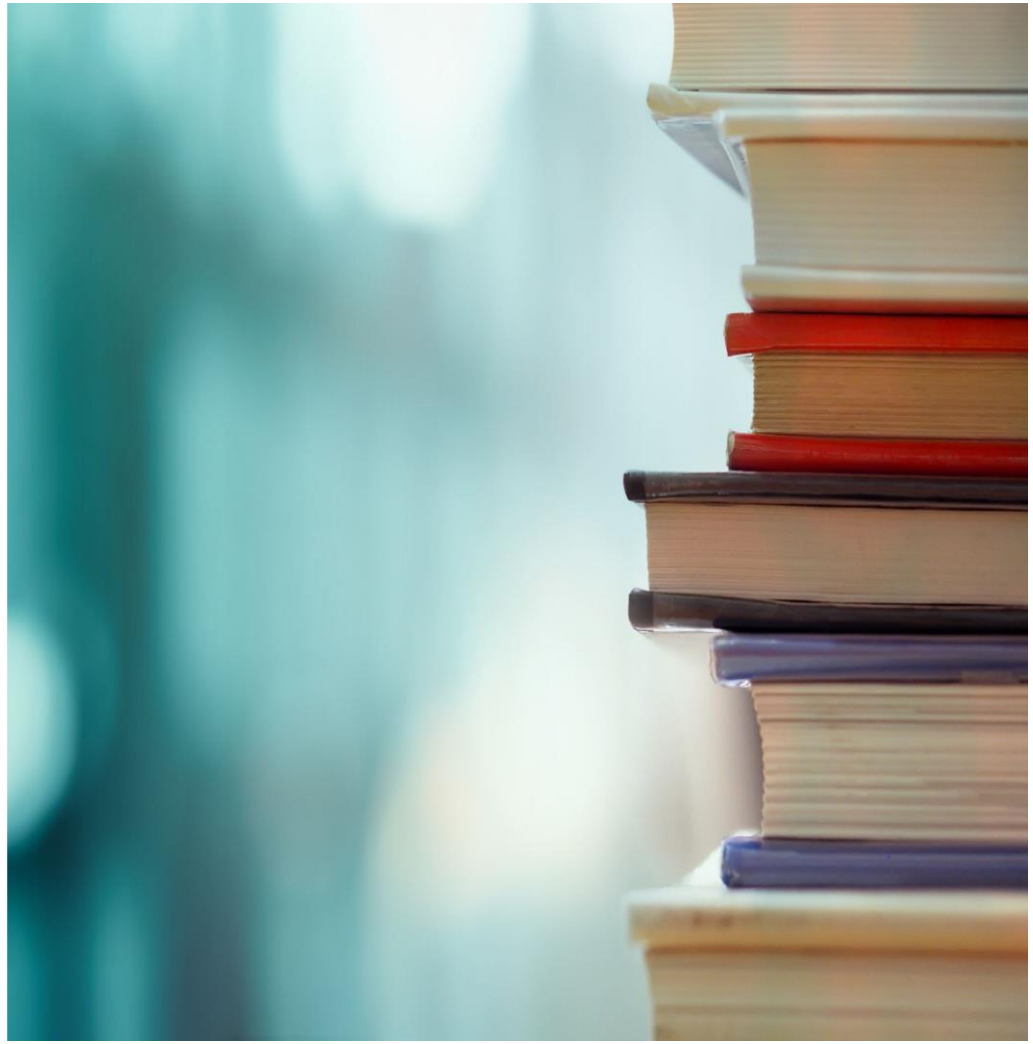
Özellikle e-posta, bulut sistemleri ve kritik sistemlere girişlerde 2FA kullanılmalıdır. Çalışanlar, SMS veya uygulamalar aracılığıyla ek güvenlik doğrulaması yapmalıdırlar.

•Kimlik Doğrulama Bilgilerini Güvende Tutma:

Kimlik doğrulama kodları, telefon veya başka cihazlarda kaydedilmemelidir.

Vakıfbank Olayı (2018)

2018 yılında, Vakıfbank'a ait bazı şifrelerin sızdırıldığı ve internette dolaşıma sokulduğu haberi basında geniş yer buldu. Bu olay, çalışanların şifre güvenliği kurallarına yeterince dikkat etmemesi ve basit şifreler kullanması nedeniyle yaşandı. Çalışanların şifrelerini güvenli hale getirmemesi, banka hesap bilgilerinin tehlikeye girmesine yol açtı.



Çalışanlar Ne Yapmalı?

3. E-posta ve İletişim Güvenliği

•Şüpheli E-postaları Açmama:

Tanınmayan gönderenlerden gelen e-postalar dikkatlice incelenmelidir. Özellikle beklenmeyen eklentiler veya tıklanması istenen linkler barındıran e-postalar açılmamalıdır.

- Örneğin: **Phishing (oltalama) saldırılarına dikkat**: “Hesabınızı doğrulamak için buraya tıklayın” gibi e-postalardan kaçınılmalı.

•Kurumsal E-posta Hesabını Kullanma:

İş ile ilgili tüm iletişimlerde kurumsal e-posta kullanılmalı, kişisel e-posta hesapları kullanılmamalıdır.

4. Veri Koruma ve Paylaşım İlkeleri

•Veri Sınıflandırması:

Çalışanlar, ellerindeki verilerin gizlilik düzeyini bilmeli ve buna uygun şekilde işlem yapmalıdırlar. Örneğin, "Hassas", "Gizli" veya "Genel" veri türlerine göre farklı güvenlik önlemleri alınmalıdır.

•Veri Şifreleme:

Önemli veya hassas veriler (müşteri bilgileri, ticari sırlar gibi) paylaşıldığında mutlaka şifrelenmelidir. Örneğin, şifre korumalı dosya gönderimi.

•Dosya Paylaşımı:

Veriler, güvenli bulut sistemleri veya şifrelenmiş USB’ler ile paylaşılmalı. Sosyal medya veya herkese açık paylaşım platformlarından veri paylaşılmamalıdır.

BDDK Phishing Saldırısı (2020)

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), 2020 yılında kurumu hedef alan bir phishing saldırısına maruz kaldı. Sahte e-postalar yoluyla bankalardan ve çalışanlardan kritik bilgiler çalınmaya çalışıldı. Çalışanların şüpheli e-postaları açması ve linklere tıklaması sonucunda, hassas bilgilere erişim sağlandı.

Çalışanlar Ne Yapmalı?

5. Fiziksel Cihaz Güvenliği

- **Cihazları Korumak:**

Laptop, tablet ve cep telefonları gibi cihazlar her zaman fiziksel olarak korunmalıdır. Özellikle kamuya açık alanlarda cihazlar gözetimsiz bırakılmamalıdır.

- **USB ve Harici Cihaz Kullanımı:**

Çalışanlar, şirkette onaylanmamış USB cihazlarını veya harici diskleri kullanmamalıdır. Kendi cihazlarını kullanmaları gerektiğinde, cihazın virüs taramasından geçtiğinden emin olmalıdırlar.

- **Çalışma Alanını Güvence Altına Alma:**

Masalarda belgelerin veya cihazların görünür bırakılmaması ("Temiz Masa Politikası"). Çalışma alanından ayrılırken belgeler kilitlenmeli, cihazlar ekran kilidi ile korunmalıdır.

6. Güvenli İnternet Kullanımı

- **Şirket Ağı Dışında Çalışma:**

Şirketin internet ağı dışında (örneğin, bir kafe veya halka açık bir Wi-Fi bağlantısı üzerinden) çalışıyorsanız, VPN kullanarak güvenli bir bağlantı oluşturmalısınız.

- **Şüpheli Web Sitelerine Girmeme:**

İş amaçlı olmayan, güvensiz veya şüpheli web sitelere girmemek; özellikle korsan içerik, bilinmeyen yazılım indirme gibi tehlikeli faaliyetlerden kaçınmak.

Türk Telekom Veri Merkezi Sabotajı (2017)

2017 yılında, Türk Telekom'a ait bir veri merkezine fiziksel bir saldırı düzenlendi. Veri merkezine giren sabotajcılar, kritik donanımları ve sunucuları hedef aldı. Fiziksel güvenlik tedbirlerinin yeterince alınmaması nedeniyle şirket büyük zarara uğradı.

Çalışanlar Ne Yapmalı ?

7. Mobil Cihaz Güvenliği

- **Mobil Cihazlarda Şifreleme ve Kilitleme:**

Mobil cihazlar şifre ile korunmalı, ekran kilidi aktif olmalı ve belirli bir süre hareketsizlikten sonra otomatik olarak kilitlenmelidir.

- **Kaybolan Cihazları Bildirme:**

Eğer bir cihaz kaybolur veya çalınırsa, hemen IT birimine bildirilmelidir. Cihazda bulunan bilgiler uzaktan silinmelidir.

8. Sosyal Mühendislik ve Dolandırıcılığa Karşı Dikkat

- **Şüpheli İletişimler:**

Tanınmayan kişilerden gelen telefon aramaları, e-postalar veya yüz yüze talepler konusunda dikkatli olunmalı. Bilgi talep eden kişilerin kimliklerinden emin olunmadıkça, şirketle ilgili kritik bilgiler paylaşılmamalıdır.

- **Kimlik Doğrulaması:**

Şirket içinden gelen tuhaf isteklerde (örneğin, acil veri paylaşımı talepleri gibi) mutlaka ikinci bir doğrulama alınmalıdır.

Mobil Cihaz Güvenliği İhlali

Sağlık Bakanlığı Veri Sızıntısı (2020)

2020'de Sağlık Bakanlığı’nın e-Nabız sistemindeki kullanıcı bilgileri, bir çalışanın mobil cihazından sızdırıldı. Çalışanın mobil cihazını şifrelememesi ve kritik uygulamaları güvende tutmaması nedeniyle, kişisel sağlık verilerine erişim sağlandı. Bu veri ihlali halk sağlığı bilgilerini tehlikeye attı.

Çalışanlar Ne Yapmalı ?

9. Fiziksel Güvenlik Tedbirleri

- **Ofis Giriş Kontrolü:**

Çalışanlar giriş kartlarını sadece kendileri kullanmalı ve başkalarına ödünç vermemelidir. Ziyaretçiler her zaman kayıt altına alınmalı ve ofis içinde refakat edilmelidir.

- **Kilitli Dolap ve Çekmeceler:**

Gizli belgeler ve önemli cihazlar kilitli dolaplarda saklanmalıdır.

10. Yedekleme ve Veri Kurtarma

- **Verilerin Düzenli Yedeklenmesi:**

Çalışanlar, önemli dosyalarını güvenli sunuculara veya bulut ortamına düzenli olarak yedeklemelidir. Yedekleme yapılmadığında veri kayıpları kalıcı olabilir.

- **Yedekleme Politikalarını Bilme:**

Yedekleme süreçlerini takip etmeli ve gerektiğinde veri kurtarma süreçlerini nasıl başlatacaklarını bilmelidirler.

2017 yılında, TRT arşivlerinden büyük miktarda veri kaybı yaşandı. Yedekleme politikalarının doğru uygulanmaması nedeniyle arşivlerdeki önemli belgeler ve videolar kurtarılamadı. Verilerin düzgün yedeklenmemesi, arşivin büyük bir kısmının kalıcı olarak kaybolmasına yol açtı.

Çalışanlar Ne Yapmalı ?

11. İhlal ve Güvenlik Olaylarını Bildirme

- **Güvenlik İhlalinin Hemen Raporlanması:**

Şüpheli bir durum (şüpheli e-postalar, kötü niyetli yazılım belirtileri, veri sızıntısı vb.) fark edilirse, derhal IT ekibine veya bilgi güvenliği sorumlusuna bildirilmelidir.

- **İhlal Prosedürlerini Bilme:**

Her çalışan, bir ihlal yaşandığında izlemesi gereken adımları bilmeli ve prosedürlere uygun hareket etmelidir.

12. Eğitim ve Farkındalık

- **Düzenli Eğitimlere Katılma:**

Çalışanlar, düzenli olarak bilgi güvenliği farkındalık eğitimlerine katılmalı ve güncel tehditler hakkında bilgi sahibi olmalıdır.

- **Güncel Tehditleri Takip Etme:**

Çalışanlar, sektördeki yeni tehditler ve siber güvenlik gelişmeleri hakkında bilgi sahibi olmalı, şirket tarafından sağlanan kaynakları kullanarak kendilerini güncel tutmalıdırlar.

Türk Hava Yolları (THY) Veri Sızıntısı (2019)

2019’da THY'nin uçuş planlama sisteminde bir veri sızıntısı yaşandı ve çalışanlar bu durumu yeterince hızlı rapor etmedi. Veri ihlali geç fark edildiği için sızdırılan bilgiler üzerinden zararın boyutu büyüdü. Olayın zamanında bildirilmemesi, sistemin daha uzun süre savunmasız kalmasına neden oldu.

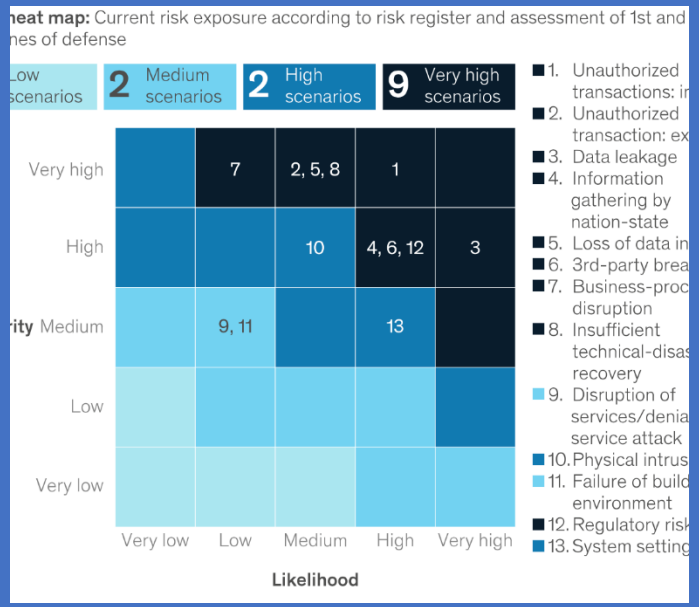
Şirketin bilgi Riskleri neler?

Şirketin en değerli bilgi varlıkları neler?

Şirketin bilgi varlıklarını kimler yönetiyor?

Şirketin bilgi risklerin gerçekleşme olasılığı nedir

Risklerin gerçekleşmesi halinde maliyeti ne olur?



McKinsey'e Göre Yalnız Değilsiniz (!)

Enhanced cyber risk reporting: Opening doors to risk-based cybersecurity

Risk managers are flying blind

Many companies rely on a patchwork of reports from different sources to manage cyber risk. Executives at these companies are unable to assess the return from their cybersecurity investments. They lack needed information about cyber risk levels, the effectiveness of countermeasures, and the status of protection for key assets. **Available data are incomplete, inconsistent, and not reliable as a basis for decision making**. Executives also question the complexity of their cyber risk-management tools, finding them overly complicated and their results **incomprehensible.**

Risk yöneticileri görüş açısı olmadan uçuyor. Birçok şirket, siber riski yönetmek için farklı kaynaklardan gelen bir dizi rapora güveniyor. Bu şirketlerdeki yöneticiler, siber güvenlik yatırımlarının getirisini değerlendiremiyor. Siber risk seviyeleri, karşı önlemlerin etkinliği ve temel varlıklar için önlemler hakkında gerekli bilgilere sahip değiller. **Mevcut veriler eksik, tutarsız ve karar vermek için güvenilir ya da yönetilebilir değildir.** Yöneticiler ayrıca siber risk yönetimi araçlarını karmaşık ve sonuçlarını da **anlaşılmaz** buluyorlar ve katkısını sorguluyorlar.

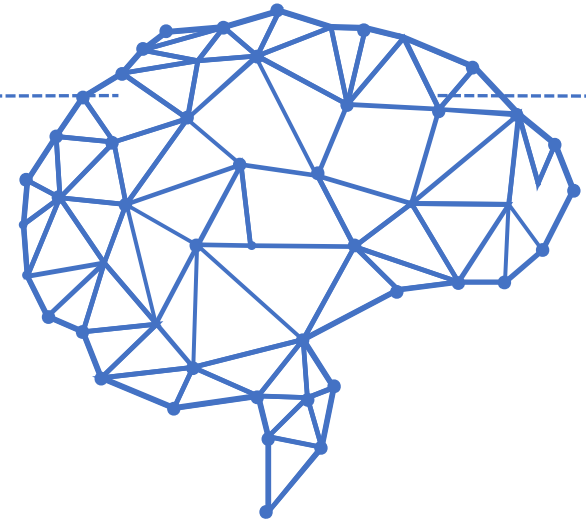
Çalışanlar Ne Yapmalı ?

Ant Teknik Süreç Risk Yönetimi

FORM NO:
YAYIN
REV.TARİHİ: -
REV. NO: -

	Tehdit	Olası (	Giz.(	Büt.(I	Eriş. (A)	MRD (
(Ortam - Altyapı)	Kaynakların yanlış kullanımı	2	4	2	2	40
kli bölgelerde bulunması	Mesajların yetkisiz kişilere yönlendirilmesi	2	3	2	2	12
(Ortam - Altyapı)	Endüstriyel bilgi sızması	2	4	2	2	32

Çalışanlar Ne Yapmalı ?



Risk Puanı
Tüm çalışanlar işledikleri bilgileri ve riskleri değerlendirerek ilgili güvenlik önlemlerini almalıdırlar.

Farkındalık

Tüm çalışanlar bilgi güvenliği eğitimlerini almalı bilgi sistemlerinin ve insan kaynaklarının ilgili iş kurallarına istisnasız uymalıdırlar.

ŞİFRELEME
Çalışanlar kompleks şifreler kullanmalı ve şifrelerini belirli aralıklarla değiştirmelidirler.

TEKNİK ve SÜREÇSEL ÇÖZÜMLER

Anti virüs programları yüklenmeli iş için kullanılan donanımlara lisansız programlar yüklenmemelidir.

CIA

Tüm kritik bilgiler CIA prensiplerine göre işlenmelidir.

Çalışanlar Ne Yapmalı ?

Toplam Risk Puanı **210**

KPI Bazlı Takip

Toplam Risk Puanının yönetilmesi ve azaltılması için aksiyonlar alın.

Risk Yönetimi

Envanterdeki bilgilerin CIA kapsamında toplam riskini hesaplayın.

650 **Toplam Risk Puanı**

Toplam Risk Puanı **960**

Envanterinizi Oluşturun

Bölümünüzde işlediğiniz bilgilerin envanterini ve riskleri dokümante ediniz.

Çalışanlar Ne Yapmalı ?

Risk

Yönetimi

Güvenlik risklerinin ve seviyesinin belirlenmesi.

Aksiyon

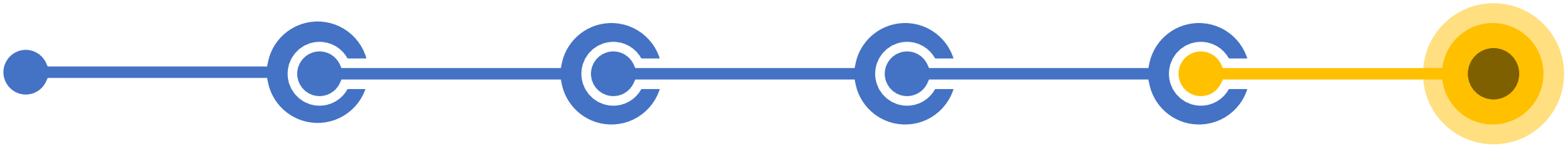
Listesi

Çevik ve yalın aksiyonların alınması ve uygulamaların kurulması.

Yol

Haritası

Bilgi güvenliği için yapılması gereken orta ve uzun vadeli projeler ve gelişim önerileri.



Çalışanlar

Bilgi Güvenliği Prosedürü

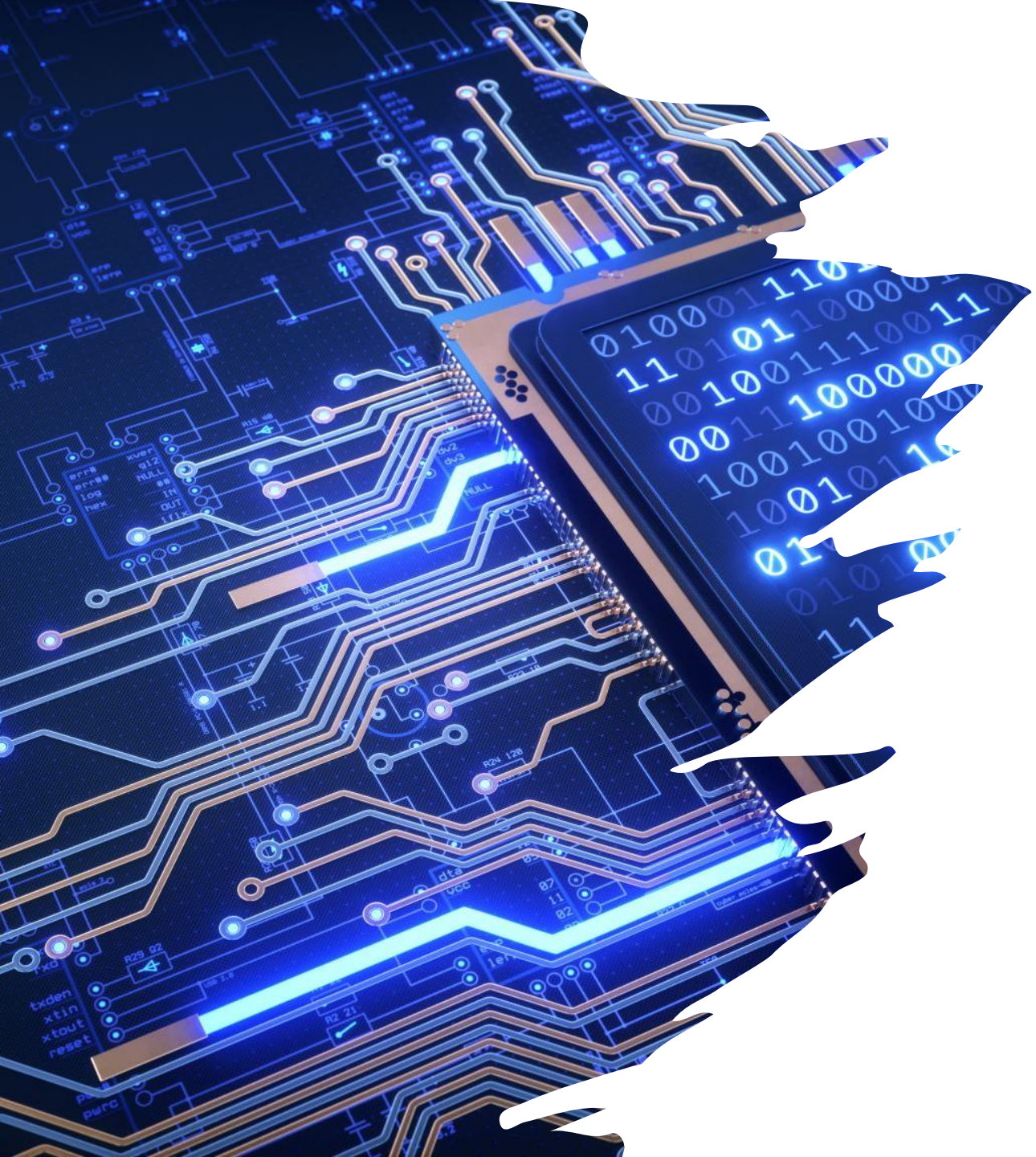
Çalışanların dikkat etmesi gereken temel konular ve aile güvenlik el kitabı.

Eğitim

Farkındalık

KPI ve Risk bazlı prosedürler ve özelleştirilmiş eğitimler.

MANASSET
Staffing Solutions



Çalışanlar Neler Yapmalı ?

- Ant Teknik Süreç Sahipleri ve Birim Yöneticileri **bilgi güvenliği eğitimi sonrasında** birimlerinde işlenen ve kaybolması, bozulması, yetkisiz kişilerin eline geçmesi ya da erişim sorunu yaşamaları durumunda süreçlerinin aksayacağını düşündükleri kritik bilgileri listeleyerek etik@antteknik.info adresine e-posta ile iletebilirler.

- Ant Teknik Bilgi Güvenliği sorumluları bu listeleri inceleyerek süreç sahipleri ile sonraki adımları planlayacaklardır.

Çalışanlar Ne Yapmalı ?

www.antteknik.info

Ant Teknik'te **Bilgi Güvenliğinin** sağlanması, **Kişisel Verileri Koruma Kanununa** Uyum ve **Etik** kurallarına uyum tüm çalışanların ortak sorumluluğudur.

Her türlü sorunuzda veya problem yaşadığınızda İK ile iletişime geçebilir ve/veya www.antteknik.info adresinden bildirimde bulunabilirsiniz.

TEŞEKKÜRLER

OGUZ TURKKORKMAZ
DPO