ANT TEKNİK
BİLGİ GÜVENLİĞİ/KVKK/ETİK EĞİTİMİ

Oğuz Türkkorkmaz, 2025

Eğitim Kuralları

- Katılımcıların konuşmadıkları süre içinde mikrofonlarını kapalı ve kameralarını açık tutmaları başarılı bir eğitim için gereklidir. Lütfen buna uymaya çalışın.
- Eğitimciye sorularınızı sormanız için eğitim süresince sorunuz var mı ya da ekleyeceğiniz bir şey var mı diye sorulacaktır. Mümkünse sorularınızı ve paylaşımlarınızı bu zamanlarda iletin.
- Eğitim konularıyla ilgili eğitim ortasında ve sonunda iki kısa anketimiz olacaktır. Lütfen bu anketleri cevaplayın.
- Eğitim boyunca sesli ve görsel hiçbir kayıt alınmayacaktır. Katılımcıların da bu kurala riayet etmesi gereklidir.

Etik Davranış ve Bilgi Güvenliği: Yeni İş Dünyasının Temel Beklentisi

Yasal düzenlemeler,**müşteri ve iş ortağı beklentileri**,**Global şirketlerin etik standartları** tüm çalışanlardan;

- **Etik ilkelere tam uyum**,
- **Ticari sırların ve kişisel verilerin korunması**,
- **Bilgi güvenliği farkındalığı**
  konularında yüksek sorumluluk beklemektedir.

Bu ilkeler; yalnızca birer uyum yükümlülüğü değil, aynı zamanda **şirketimizin itibarı**, **müşteri güveni** ve **uluslararası iş birliklerinde sürdürülebilir başarı** için vazgeçilmezdir.

Etik Kuralları- https://antteknik.info

İletişim

Ant Teknik, bu politika hakkında çalışanlarına ve iş ortaklarına sürekli eğitimler vermiş ve beklentileri anladıklarını teyit etmiştir. Ant Teknik, katılımcıların etik kurallar ve rüşvetle mücadele farkındalığını değerlendirmekte ve çalışanın politikayı ve genel ilkeleri okuduğunu ve anladığını gösteren kayıtları tutmaktadır.

İş Ortakları ve Alt Bayiler

Ant Teknik, alt bayilerini rüşvetle mücadele ve yolsuzluk konusunda bilgilendirmektedir. Ant Teknik, sözleşme gereklilikleri doğrultusunda iş ortaklarını ve alt bayilerini sistematik olarak desteklemekte, böylece bu taraflar mevzuata ve sözleşme yükümlülüklerine uyum sağlama yetkinliklerini gösterebilmektedir.

Politikalar ve Süreçler

Ant Teknik, tüm çalışanların ve iş ortaklarının rüşvetle mücadele ve yolsuzlukla ilgili yasalara uyacağını belirten bir uyum politikası oluşturmuştur. Ant Teknik, bu politikaları çalışanları ve iş ortaklarıyla internet ve e-öğrenme platformları aracılığıyla paylaşmaktadır.

Kısıtlı, Reddedilen Taraflar ve İhracat Kontrolleri

Ant Teknik ve tedarikçileri, ürünler ABD menşeli ise veya sözleşmeye tabi ise, bu ürünleri Reddedilen Listede yer alan şirket veya kişilere ya da Özel Olarak Belirlenmiş Vatandaşlar ve Engellenmiş Kişilere satmamayı veya devretmemeyi açıkça kabul eder. Ant Teknik, yukarıda belirtilen kapsamda yer alan ürünler için ABD hükümeti tarafından ambargo uygulanan ülkelere satış yapmamaktadır.

Kayıt Tutma ve İndirimler

Ant Teknik muhasebe kayıtları, ürün satışlarıyla ilgili harcamaların açık bir şekilde kaydını sağlar. Müşteri hediyeleri, yemekleri ve konaklamaları dahil olmak üzere tüm harcamalar fişlerle belgelenir ve muhasebe sistemlerinde harcama amacı gösterilecek şekilde ayrıştırılabilir.

ABD'nin Türk ve Çinli Tedarikçilere Yaptırımı – 2025

Sanctions List Search

Yaptırımı Uygulayan: ABD Hazine Bakanlığı (OFAC)

- **Hedef Alınan Şirketler**:
  - **XXXX Txxxxx Xxxxyard** (Türkiye)
  - **Sinno Electronics Co. Ltd.** (Çin)
  - **AeroTech LLC** (BAE merkezli, Rusya bağlantılı)
- **Gerekçe**: Bu şirketlerin Rusya'ya yönelik ambargoları ihlal ederek savunma sanayiine parça ve teknoloji sağladığı tespit edildi.
- **Yaptırım Türleri**:
  - ABD ile tüm ticari ilişkilerin kesilmesi
  - ABD finans sistemine erişim yasağı
  - Varlıkların dondurulması
  - Global iş ortaklarının sözleşme iptalleri (örneğin Boeing ve Honeywell gibi firmalar bu şirketlerle olan iş ilişkilerini sonlandırdı)
- **Etki**: Bu şirketler, global tedarik zincirinden çıkarıldı ve birçok **uluslararası iş ortağı tarafından kara listeye** alındı.

Etik Olaylar - **Giorgio Armani – Etik İhlal Cezası (2025)**

- **Şirket**: Giorgio Armani (İtalya merkezli lüks moda markası)
- **İhlal Nedeni**: Tedarik zincirindeki taşeron firmaların, kamuya açıklanan etik değerlerle örtüşmeyen çalışma koşulları sunması.
- **Tespit Edilen Sorunlar**:
  - Kayıt dışı çalışma
  - Hijyenik olmayan ve güvenli olmayan iş ortamları
  - İşçi güvenliği standartlarına uyulmaması
- **Denetim Bulguları**: Armani'nin iç yazışmalarında bazı tedarikçi ortamlarının "ciddi hijyen sorunları içerdiği" ve "en iyi ihtimalle kabul edilebilir sınırda" olduğu belirtilmiş.
- **Ceza**: **3,5 milyon euro** para cezası
- **Kararı Veren Kurum**: İtalya Rekabet Kurumu (AGCM)
- **Şirketin Tepkisi**: Armani, karara itiraz edeceğini ve faaliyetlerini şeffaflıkla yürüttüğünü savundu. Giorgio Armani'ye yanıltıcı etik beyanlar nedeniyle milyonluk ceza | AVMDergi-Türkiye'nin AVM ve Perakende Haber Portalı

Ant Teknik BGYS/KVKK ve ETİK Kuralları

1. Bilgi Güvenliği (ISO 27001 Temel Prensipleri, CIA)

- Kritik bilgiler (müşteri, ürün, finansal, stratejik) yetkisiz kişilerle paylaşılmamalıdır.
- Şifreler güçlü olmalı, cihazlar kilitli tutulmalı, belgeler açıkta bırakılmamalıdır.
- Bilgi güvenliği ihlalleri BT birimine derhal bildirilmelidir.

2. KVKK Uyum

- Kişisel veriler yalnızca görev tanımı kapsamında işlenmelidir.
- Açık rıza olmadan veri paylaşımı yapılmamalıdır.
- Sorumlu olunan alanlardaki müşteri sözleşmeleri, iş kuralları öğrenilmeli ve uyum sağlanmalıdır.
- Kişisel veri içeren belgeler şifrelenmeli, dijital ortamda güvenli paylaşılmalıdır.

3. Etik Kurallar

- Tüm çalışanlar ve iş ortakları etik kuralları bilmeli ve uygulamalıdır.
- Yolsuzluk, rüşvet ve çıkar çatışmalarına karşı sıfır tolerans politikası geçerlidir.
- Etik ihlaller **etik@antteknik.info** adresine bildirilmelidir.

4. Eğitim ve Farkındalık

- Etik, KVKK ve bilgi güvenliği eğitimleri düzenli olarak alınmalıdır.
- antteknik.info/egitimler adresinden eğitim içeriklerine erişilebilir.
- Tüm çalışanlar işlenen kritik bilgileri tanımlayıp riskleri yönetmelidir.

Mobil Cihazlar

1. Instagram, TikTok gibi uygulamalarda konum ve mikrofon erişimini sınırla. Ayarlardan uygulama izinlerini gözden geçir, gereksiz erişimleri kapat.

2. Mobil e-posta uygulamalarında şüpheli e-postaları açmadan önce göndereni kontrol et. Alan adını dikkatle incele, tanımadığın adreslerden gelen linklere tıklama.

3. Bankacılık uygulamalarında sadece resmi uygulamaları kullan Uygulama mağazasından indir, SMS ile gelen sahte linklere tıklama.

4. Tüm uygulamalarda güçlü ve farklı şifreler kullan. Aynı şifreyi birden fazla uygulamada kullanma, mümkünse 2FA (iki faktörlü doğrulama) etkinleştir.

5. Kullanmadığın uygulamaları sil, arka planda veri toplayabilirler. Özellikle kamera, mikrofon ve rehber erişimi olanları kontrol et.

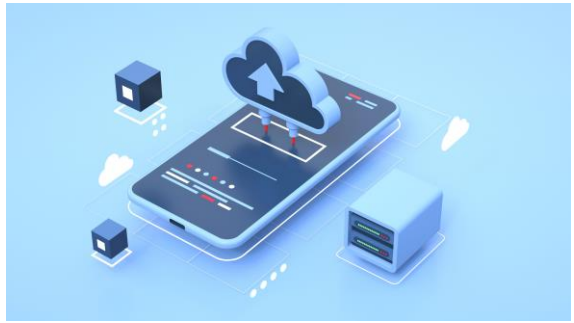
6. WhatsApp, Instagram gibi uygulamalarda hassas bilgileri yazılı paylaşma. Kritik bilgiler için telefon veya kurumsal kanalları tercih et.

7. Mobil cihazına güvenlik yazılımı yükle. Android cihazlarda antivirüs ve zararlı yazılım koruması kullan. https://www.youtube.com/watch?v=1PAl5ZYBzyo

8. Açık Wi-Fi ağlarında VPN kullan. Kafe, havaalanı gibi yerlerde bankacılık ve e-devlet işlemi yapma.

9. Mobil cihazını kaybedersen uzaktan silme özelliğini aktif tut.iPhone için “iPhone’umu Bul”, Android için “Cihazımı Bul” özelliğini kullan.

10. Uygulama güncellemelerini zamanında yap. Güvenlik açıkları genellikle eski sürümlerde kalır, otomatik güncellemeyi aç.



E-Devlet

1. Güçlü Şifre Kullan. En az 12 karakter, büyük/küçük harf, rakam ve sembol içermeli.

2. Mobil Uygulamayı Sadece Resmi Mağazadan İndir. Geliştirici olarak “T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi” yazmalı.

3. Şifreyi Düzenli Olarak Değiştir.3-6 ayda bir şifre yenile.

4. Şifreyi Kimseyle Paylaşma. Aile bireyleri dahil kimseye verme.

5. İki Faktörlü Kimlik Doğrulama (2FA) Kullan. SMS doğrulama veya mobil bildirim ile giriş güvenliğini artır.

6. Kişisel Veri İçeren Belgeleri Şifreleyerek Paylaş. E-posta ile gönderimlerde parola korumalı dosya kullan.

7. e-Devlet Giriş Geçmişini Kontrol Et turkiye.gov.tr > “Hesabım” > “Giriş Geçmişi” bölümünden kontrol et.

8. Şüpheli Girişleri Bildir. Bilinmeyen cihazlardan giriş varsa hemen bildir.

9. e-Devlet Üzerinden Tapu Güvence Altına Alma Adımları

- turkiye.gov.tr adresine gidin.
- T.C. kimlik numaranız ve e-Devlet şifrenizle giriş yapın.
- **2. Web Tapu Hizmetine Ulaşın**
- Arama çubuğuna **“Web Tapu”** yazın.
- **Tapu ve Kadastro Genel Müdürlüğü** hizmetine tıklayın.
- **3. Beyan İşlemleri Menüsüne Girin**
- Sol menüden **“Beyan İşlemleri”** sekmesini seçin.
- **4. “İşlem Yapılamaz Beyan Tesisi”ni Oluşturun**
- Açılan ekranda **“İşlem Yapılamaz Beyan Tesisi”** seçeneğini işaretleyin.
- Adınıza kayıtlı taşınmazlar için bu güvenlik kaydını ekleyin.

Masaüstü

1. Ekran Kilidi Kullanın. Bilgisayardan uzaklaştığınızda otomatik kilit devreye girmeli.

2. Güçlü Parola Kullanın. En az 12 karakter, karmaşık ve sadece size özel olmalı.

3. Temiz Masa Politikası Uygulayın. Hassas belgeleri açıkta bırakmayın, kilitli dolapta saklayın.

4. USB ve Harici Diskleri Dikkatli Kullanın. Sadece şirket onaylı cihazları kullanın, virüs taraması yapın.

5. Güvenli Ağ Kullanımı. Ofis dışı bağlantılarda VPN kullanın, halka açık Wi-Fi'den kaçının.

6. Gereksiz Yazılımları Kaldırın. Kullanılmayan programlar güvenlik riski oluşturabilir.

7. Güncellemeleri Aksatmayın. İşletim sistemi ve yazılımlar güncel olmalı.

8. Antivirüs ve Güvenlik Duvarı Aktif Olsun. Gerçek zamanlı koruma açık olmalı, lisanslı yazılım kullanılmalı.

9. Dosya Paylaşımında Yetki Kontrolü Yapın. Kim hangi dosyaya erişebiliyor, düzenli kontrol edin.

10. Şüpheli Durumları BT'ye Bildirin. Bilgisayarda olağan dışı hareket varsa hemen haber verin.

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.

Çalışanlar Neler 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 Neler Yapmalı ?

Risk

Yönetimi

Güvenlik risklerinin ve seviyesinin belirlenmesi.

Aksiyon

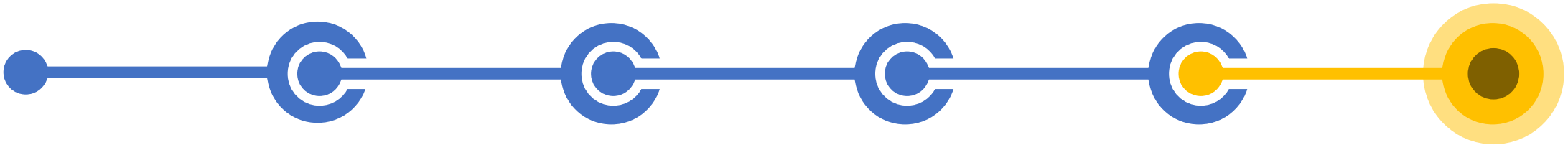
Listesi

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

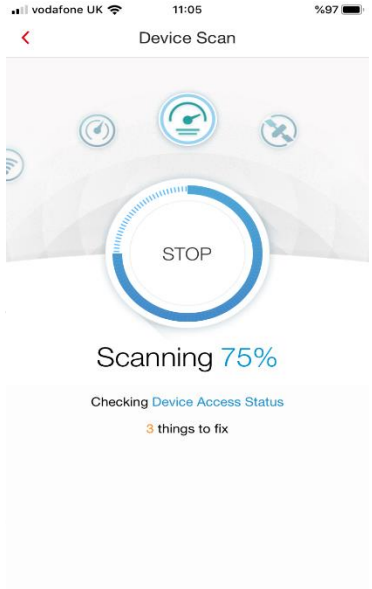
Farkındalık

KPI ve Risk bazlı prosedürler ve özelleştirilmiş eğitimler.

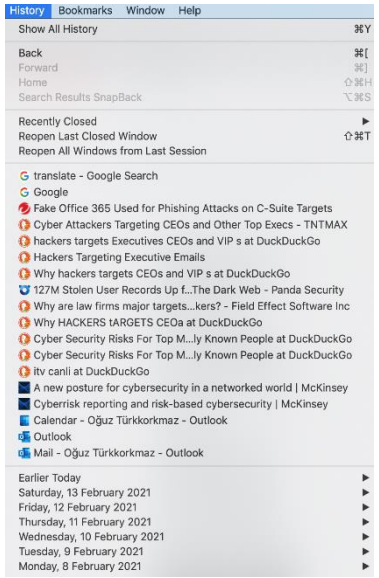
MANASSET
Staffing Solutions

Çalışanlar Neler Yapmalı ?

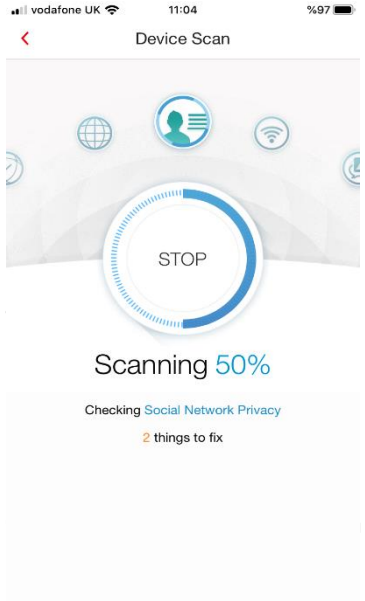
Mobil cihazlar ve ev ağ altyapıları başta olmak üzere çalışanların cihazlarının güvenliğini kendi sorumluluklarındaki basit kontroller ve uygulamalarla geliştirmek mümkündür. Bu uygulamalar sayesinde özel hayatın gizliliğinden, mobil bankacılık hizmetlerinin kötü niyetli risklere karşı korunmasına kadar birçok alanda farkındalık ve iyileşme sağlayacaktır.



Erişim Önlemleri

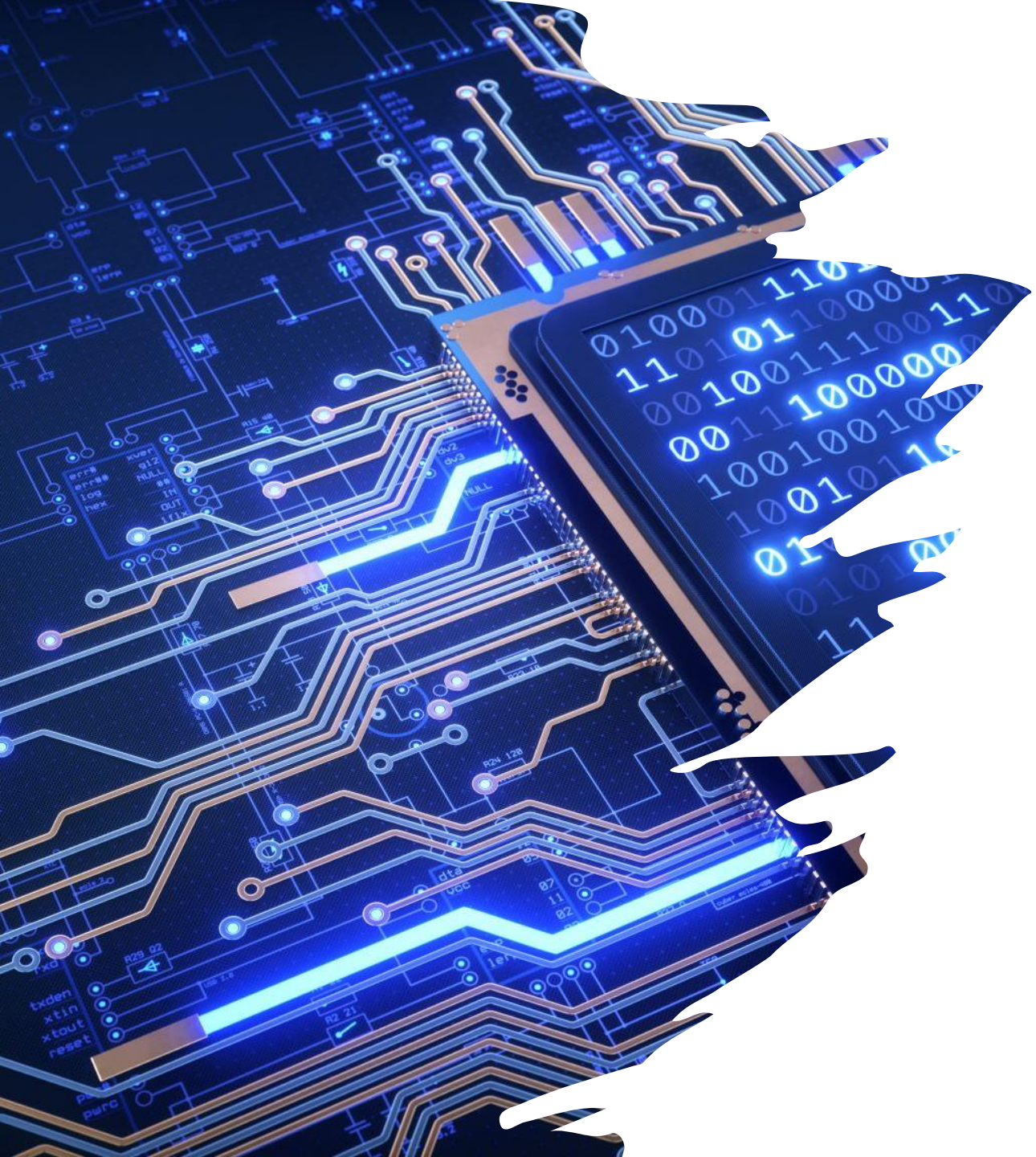


Kullanım Tarihçesi



Özel Hayatın Gizliliği

Konum Servisleri



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 iletmelidirler.

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

Çalışanlar Neler Yapmalı ?

Temel Güvenlik Önlemleri	Şifrenizi koruyun. Kolay şifrelerden kaçının ve mümkünse multi-factor authentication kullanın. Kritik bilgileri sadece bilmesi gereken kişilerle paylaşın. Gereksiz yetkilendirmelerden ve e-posta bilgilendirmelerinden kaçının. Kritik bilgileri şifreleyerek e-postalarda kullanın.
	Tüm kritik cihazlarınızda güncel anti-virüs yazılımları olmasına dikkat edin. Lisanssız uygulamalardan kaçının. Ağ güvenliğine dikkat edin. Güvenli olmayan ağlarda kritik işlemlerinizi yapmayın. Remote çalışma nedeniyle evinizdeki ağ şifresini herkes ile paylaşmayın. Ağlara hangi cihazların ve kimlerin bağlandığını zaman zaman kontrol edin. İşletim sistemlerinin güncel olmasını sağlayın.
	Kötü niyetli kişilere karşı dikkatli olun. Sürpriz hediyeler ve tehditler karşısında soğukkanlılığınızı koruyun ve gerekli araştırmaları yaptıktan sonra harekete geçin. Unutmayın bilgi güvenliği dijital bilgilerle sınırlı değildir, aldığınız çıktılara ve sözel olarak paylaştığınız bilgilere dikkat edin. Temiz masa, temiz ekran prensiplerine uyum sağlayın.

Çalışanlar Neler Yapmalı ?

www.antteknik.info

Ant Teknik'te bilgi güvenliğinin sağlanması tüm çalışanların ortak sorumluluğudur. Her türlü sorunuzda veya bilgi güvenliği problemi yaşadığınızda bilgi sistemleri ile iletişime geçebilir ve/veya www.antteknik.info adresinden bildirimde bulunabilirsiniz.

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

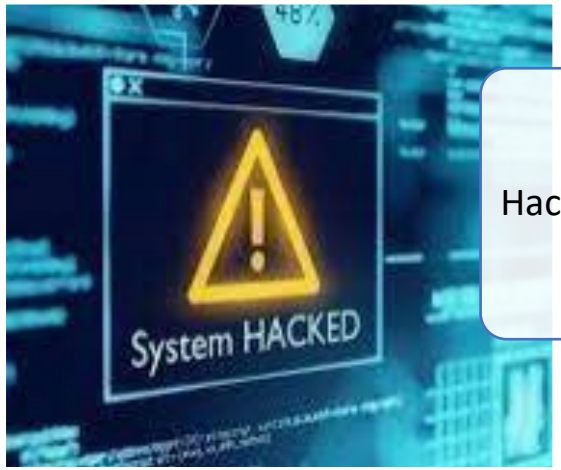
önce 2 dk okuma süresi

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

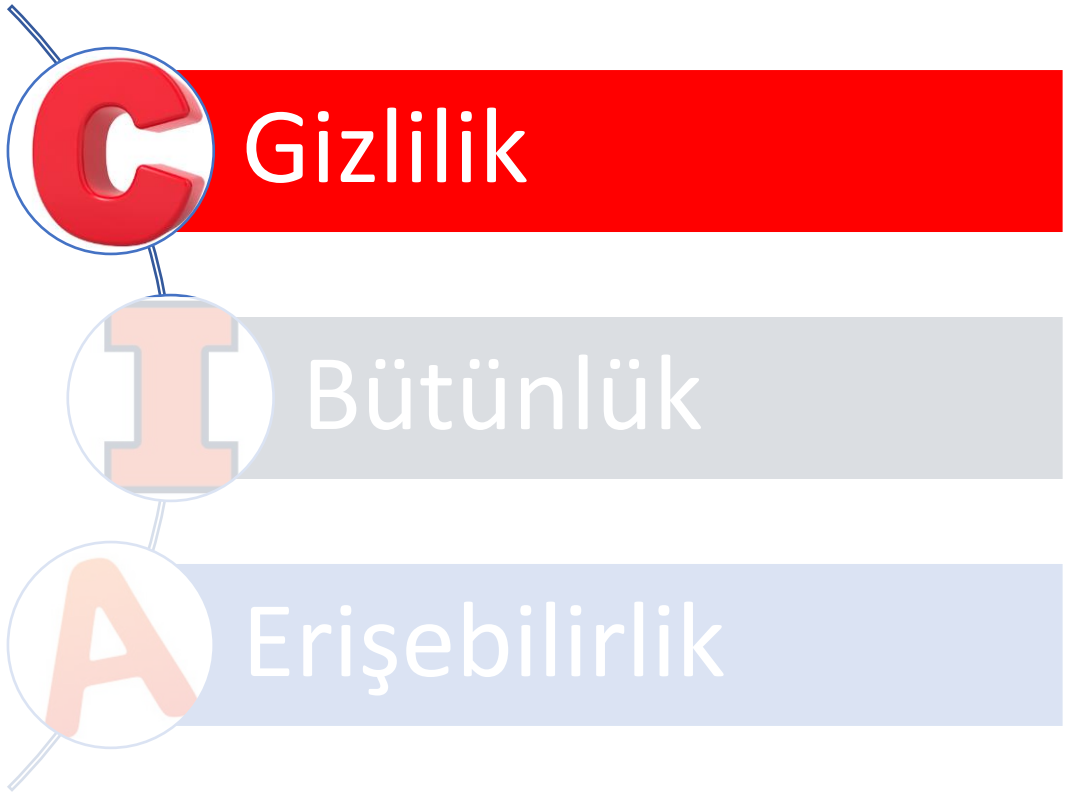


Hacklenme

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.

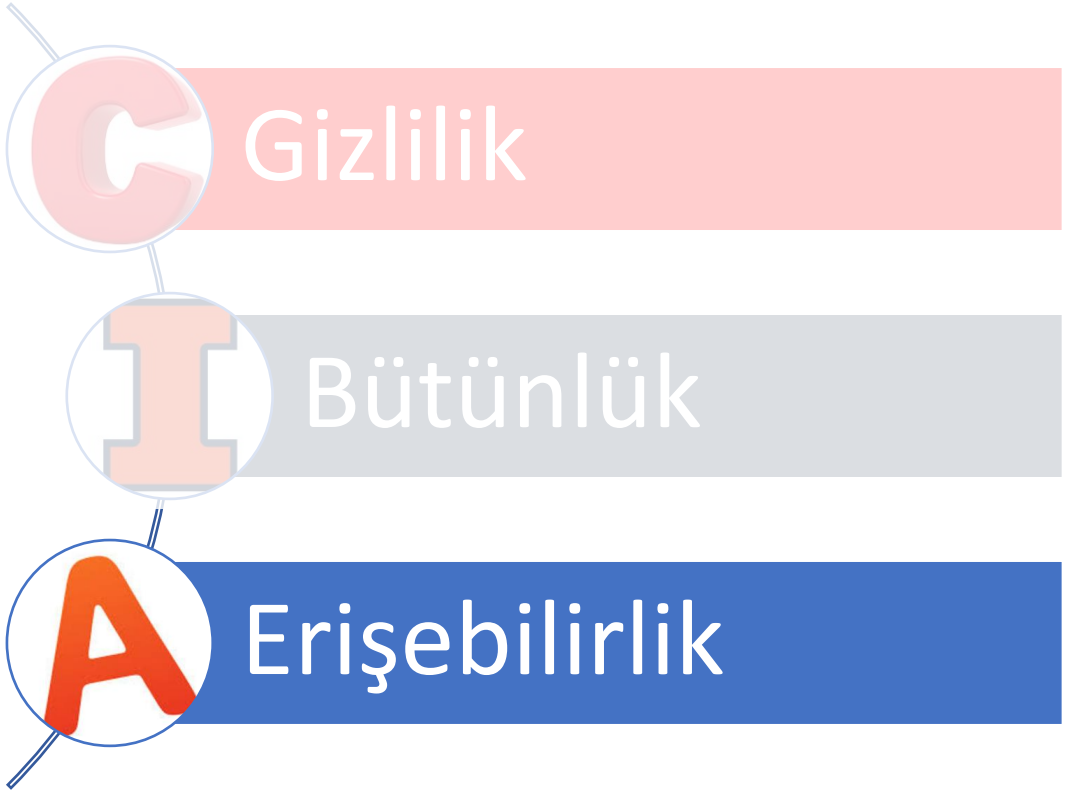


Bilgi Güvenliği: Temel Kavramlar

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.



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

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

Çalışanlar Hangi Bilgileri Dikkatle Korumalıdır?

- **İş veya iş yeri ile ilgili bulunan,**
- **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 bilgidir.**

Neden Bilgi Güvenliği?

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

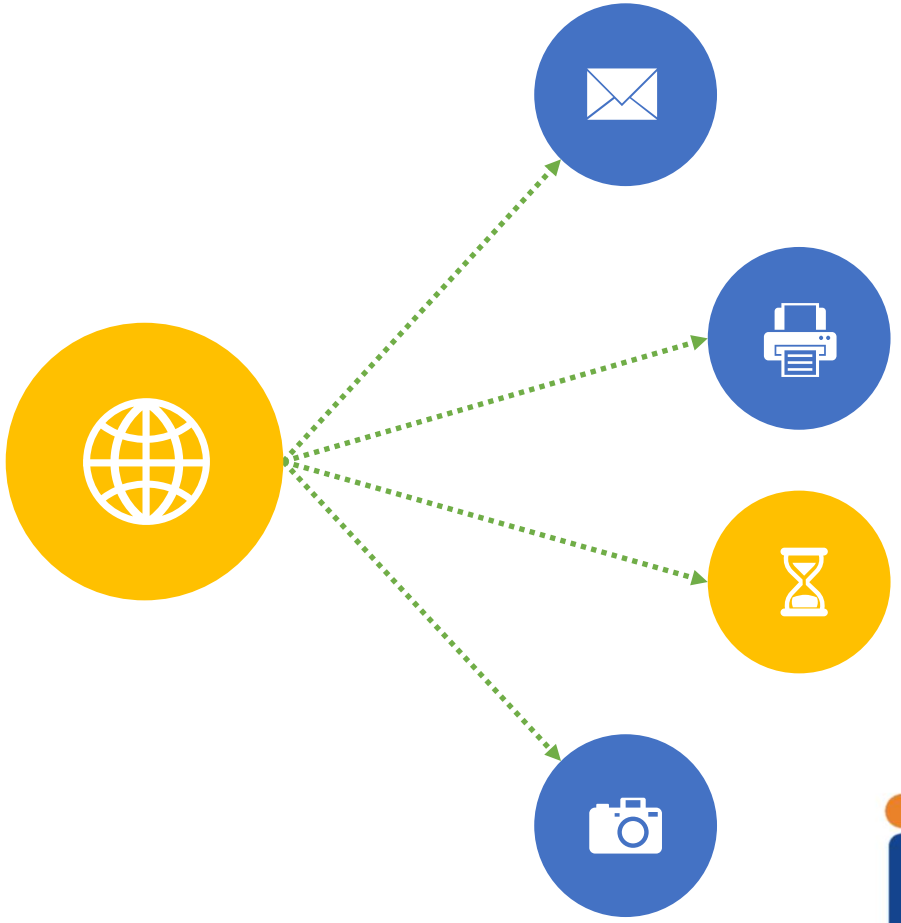
- Çevrimiçi hesaplara erişimin sağlanamaması
- Adınıza yapılan çevrimiçi suiistimaller
- Bağlantılarınızın sosyal olarak tasarlanması riski
- Yanlış çevrimiçi iddialarla itibarınızın zedelenmesi
- Şantaj veya dolandırılma
- Hassas fotoğrafların veya videoların açığa çıkarılması

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.

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

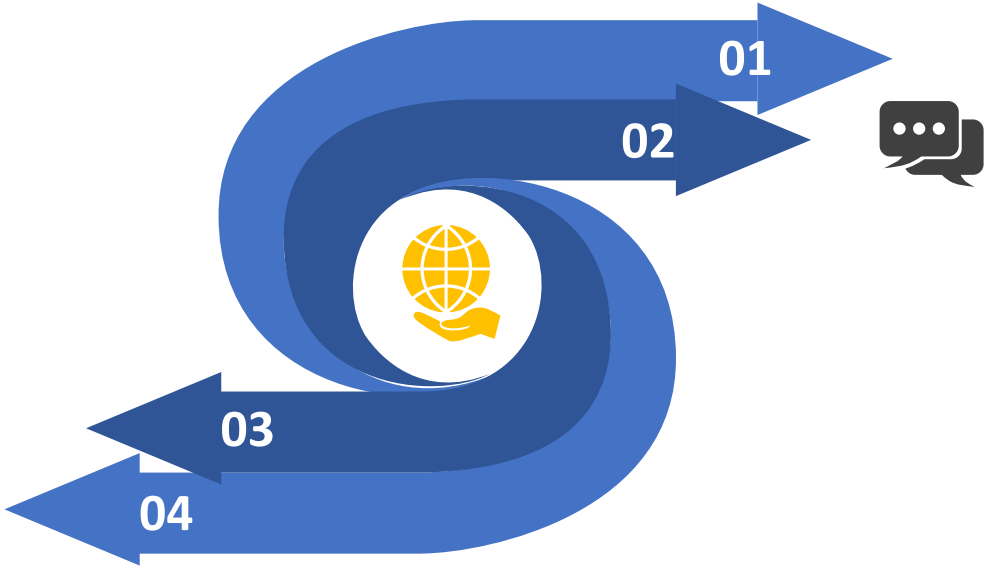
Neden Bilgi Güvenliği ? Algoritmalar Nasıl Çalışır?

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?

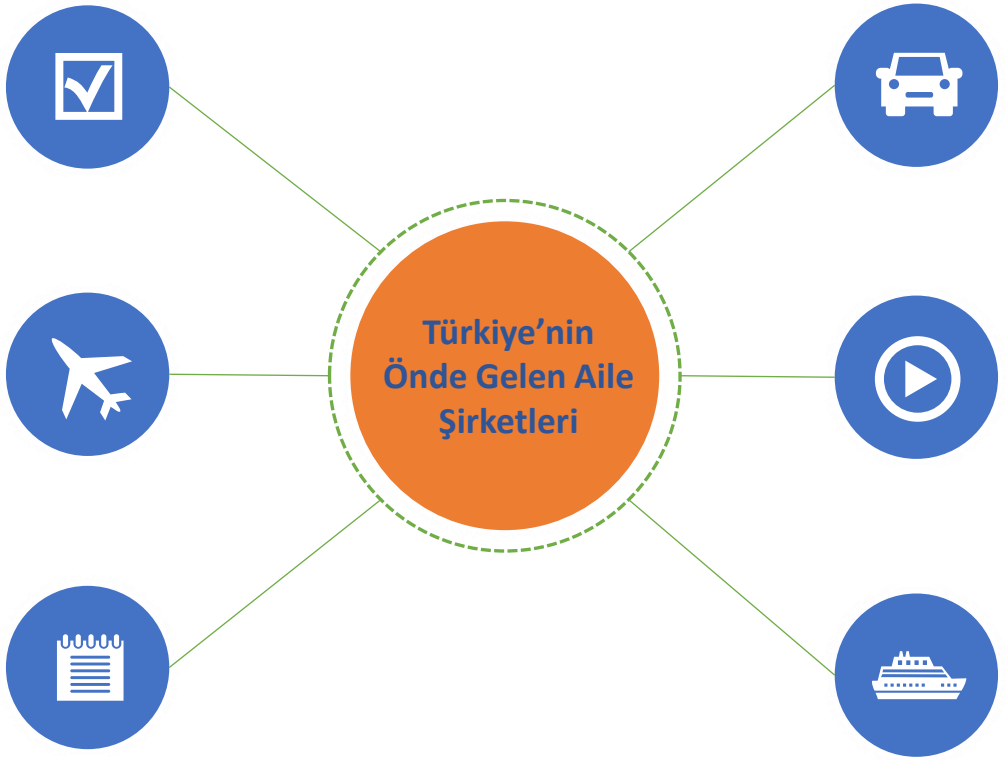
Dünya'da ve ülkemizde her türlü soruşturmada Teknik takipler, sosyal medya analizinden şikayetlerin takibine kadar birçok alanda kamuya mal olan ya da önemli mevkilerde bulunan kişiler için daha hassasiyetle yapılmakta bir çok önemli kişi, soruşturmalarla ve tahkikatlarla karşı karşıya kalmaktadırlar.

Bilgi Güvenliği Yaklaşımı

Tüm çalışanların, çocuklar da dahil olmak üzere ailelerinin sosyal medya kullanımı, internet kullanımı ve bilgi paylaşımı konularında bilgilendirilmesi.

Çalışanların evde kullandığı donanımların ve networklerinin bilgi güvenliğinin sağlanması.

Kritik personele eğitim verilmesi (şirket araçlarını kullananlar, çay servisi yapanlar ve yemek servisinde çalışanlar da kritik personeldir).



Yolculuklarda, havaalanlarında ve uzaktan çalışma alanlarda yapılması gerekenler.

Şirketin ve çalışanların ve dava, gayrimenkul, adres bilgilerinin ve özel hayatlarının korunması.

Kritik bilgi varlıklarının ve risklerin belirlenmesi ve yönetilmesi.

MULTI FACTOR AUTHENTICATION

Tüm yumurtaları tek sepete koymayın. Sadece şifreler için değil kritik bilgilerinizi koruyan, işleyen ve yöneten kişiler ve sistem yöneticileri için de çoklu denetim mekanizmaları kurmalısınız. Gelişmiş bir güvenlik sistemi çift kilit, farklı anahtarlar ve çoklu kontrol esasına dayanmaktadır.

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

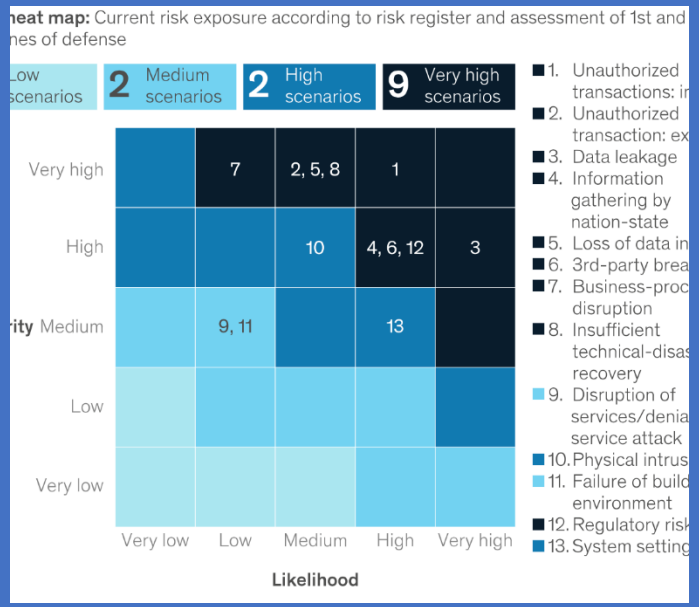
Şirketin bilgi Riskleri neler?

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 Neler 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.

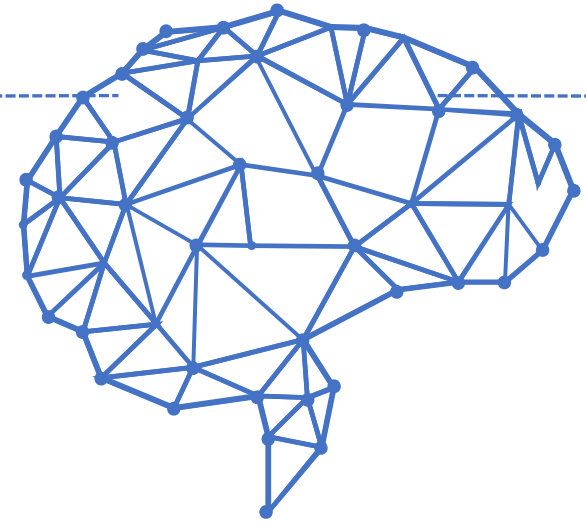
Çalışanlar Neler Yapmalı ?

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

Ant Teknik Süreç Risk Yönetimi

	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 Neler 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.

TEŞEKKÜRLER

OGUZ TURKKORKMAZ
DPO