TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

BİLGİ GÜVENLİĞİ ve KİŞİSEL VERİ GÜVENLİĞİ

FARKINDALIK EĞİTİMİ

HOŞ GELDİNİZ

07 Nisan 2026

ÇERÇEVE

6698 Sayılı Kişisel Verilerin Korunması Kanunu

TÜRK STANDARDLARI ENSTİTÜSÜ

Türk Standardı

TS ISO/IEC 27001

Aralık 2022

BİLGİ NEDİR?

Karar verme aşamasında kullanılan, anlam taşıyan, işlenmiş ve analiz edilmiş veriye bilgi denir.

Bilgi, farklı ortamlarda farklı formatlarda bulunabilir. Bilgi :Kopyalanabilir, taşınabilirdir.

Bilgi hangi ortamda olursa olsun özenle korunmalıdır.

Süreçlerin devamlılığı için gerekli olan ve bu nedenle değeri olan, dolayısı ile uygun şekilde korunması gereken bir varlıktır.

TEMEL KAVRAMLAR GİRİŞ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Bilgi Güvenliği (tanım) :

Bilgi varlıklarının;

İzinsiz, yetkisiz veya istenmeyen bir şekilde

* **Erişim ve kullanımının aksamasına,**
* **ifşa olmaya,**
* **değiştirilmeye, hasar verilmeye ve ortadan kaldırmaya**

karşı korunması

TEMEL KAVRAMLAR GİRİŞ

Bilgi Güvenliği (kısa tanım) :

Bilgi varlıklarının;

* **Kullanabilirliğinin**
* **Gizliliğinin,**
* **Bütünlüğünün,**

korunması

BİLGİ GÜVENLİĞİ TEMEL KAVRAMLAR

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

GİZLİLİK

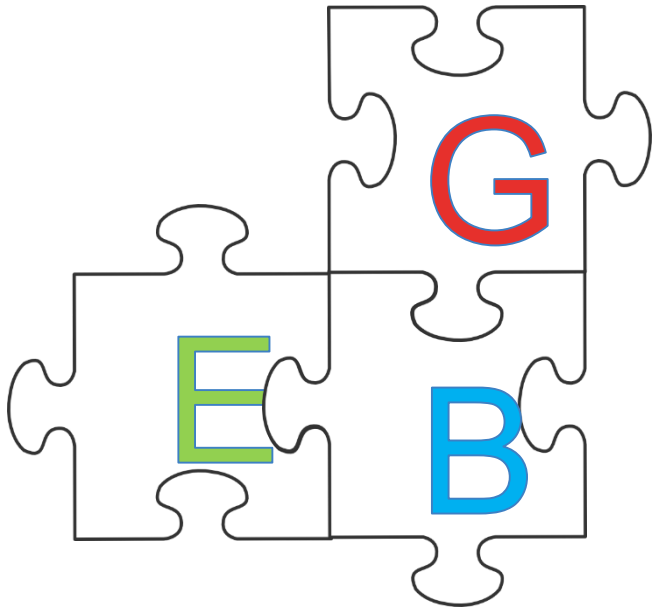
Bilginin;

- Yalnızca yetkisi olan kişiler, varlıklar ya da süreçler tarafından erişilebilir olması ve
- Yetkisiz erişimlerin engellenmesidir.

BÜTÜNLÜK

Bilginin;

- İçeriğinin doğru,
- Güncel, geçerli ve
- Yetkisiz kişiler tarafından değiştirilmediğinin garanti altına alınmasıdır.



ERİŞİLEBİLİRLİK

Bilginin;

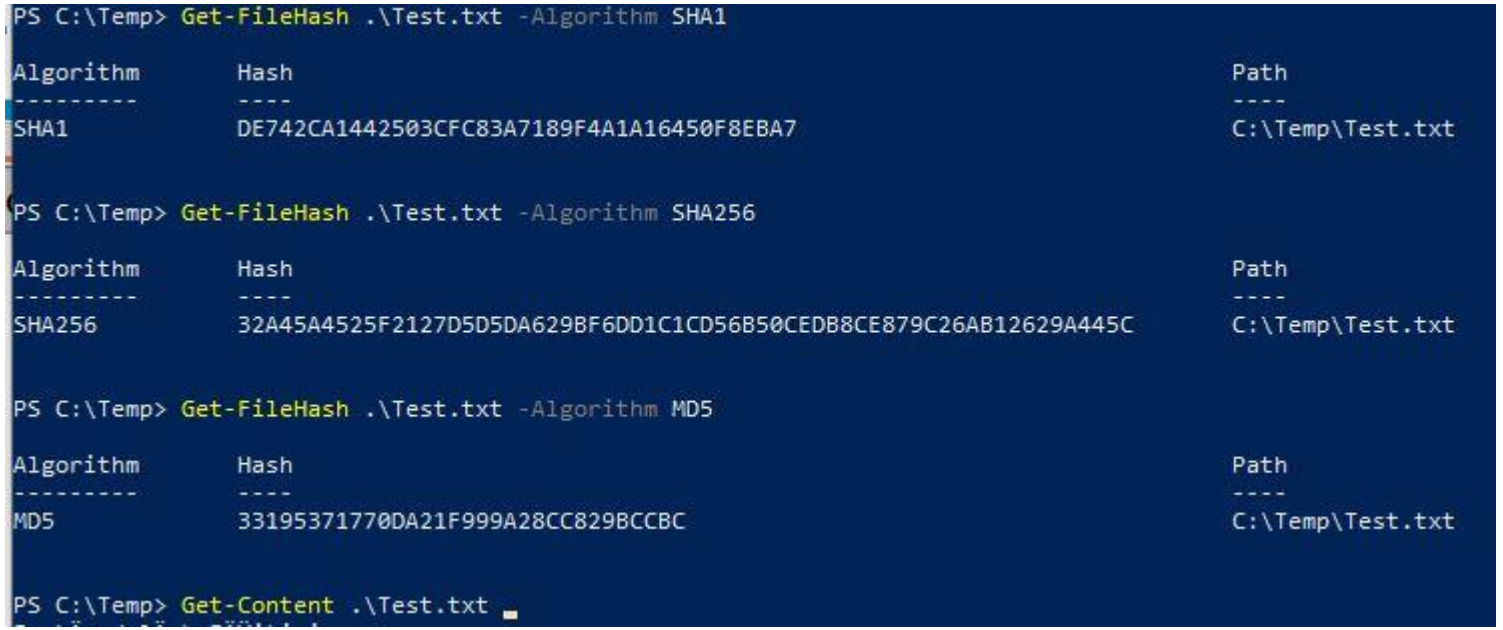
- Olması gerektiği yerde,
- Erişmeye yetkisi olan kişiler, varlıklar ve süreçler için,
- Tam ve eksiksiz olarak kullanıma hazır olmasıdır.

Uygulama: Windows PowerShell ile Dosya Bütünlük Kontrolü

Özetleme (hashing), temel olarak verinin bütünlüğünü sağlamak için kullanılan bir yöntemdir.

- Verinin bütünlüğü kontrol edilir.
- Büyük boyutlardaki verinin boyutu sabit uzunlukta olan daha küçük boyuta indirgenir.

En Yaygın Kullanılan Özetleme Algoritmaları: SHA1, SHA2, SHA256, MD5



Get-FileHash Test.txt -*Algorithm* SHA256

DOSYA BÜTÜNLÜĞÜ KONTROLÜ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

VMware-ESXi-7.0U3m-21686933-depot View Details

Build Number: 21686933
Version: 7.0
Download Size: 379.4 MB

MD5SUM: 9cd52571752b939637f80b351daace94
SHA1SUM: 4ca9b58c2306bb0cc1d143f116e9a6b2557902e5

Get-FileHash Filename -*Algorithm* SHA256

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.1.1	1	Kurulum Güvenliği	Kurulum esnasında kullanılan işletim sistemi dosyalarının özet bilgisi orijinal dağıtıcı özet değerleriyle teyit edilmelidir.

VMware-ESXi-7.0U3l-21424296-depot View Details

Build Number: 21424296
Version: 7.0
Download Size: 570.6 MB

MD5SUM: bc8be7994ff95cf45e218f19eb38a4f1
SHA1SUM: b8cefd6de1cf3f285d697a99ff7021d9dcb4758a

TEMEL KAVRAMLAR

BİLGİ GÜVENLİĞİ İLKELERİ

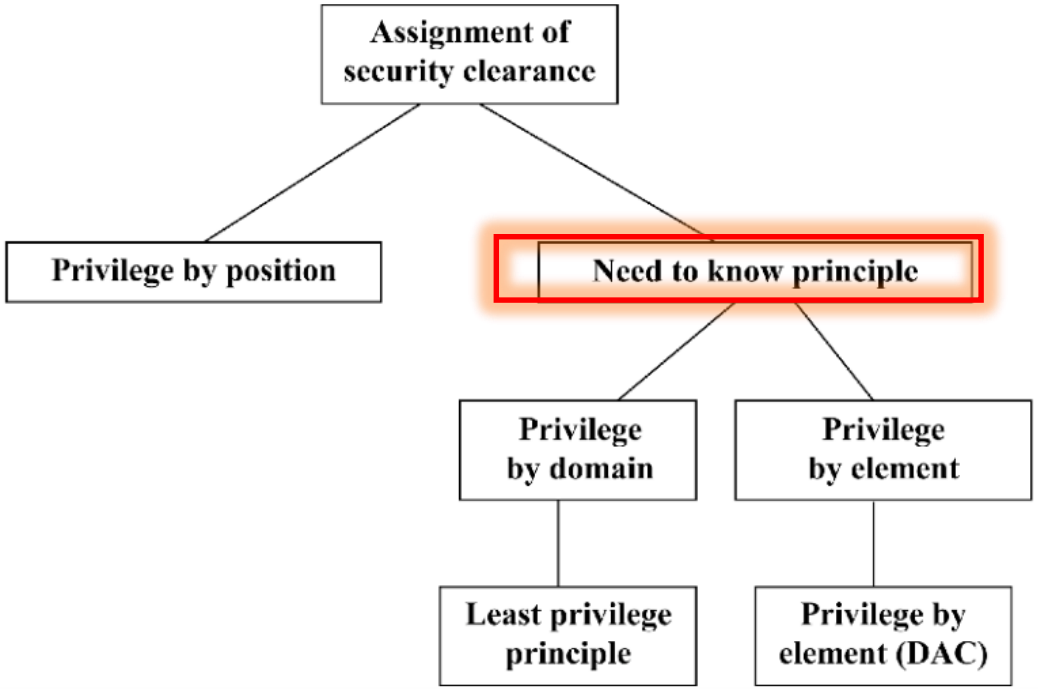
Güvenliğin sadece küçük bir kısmı teknik güvenlik önlemleri ile sağlanır.

Büyük kısım ise kullanıcıya bağlıdır.

'Ve zincir en zayıf halkası kadar güçlüdür.'

Bilmesi Gereken İlkesi

Bazen tarafın en az resmi bir güvenlik belgesi olması (klerans) gerekir.



Bilmesi gereken temelinde bilgilendirmek gerekir.

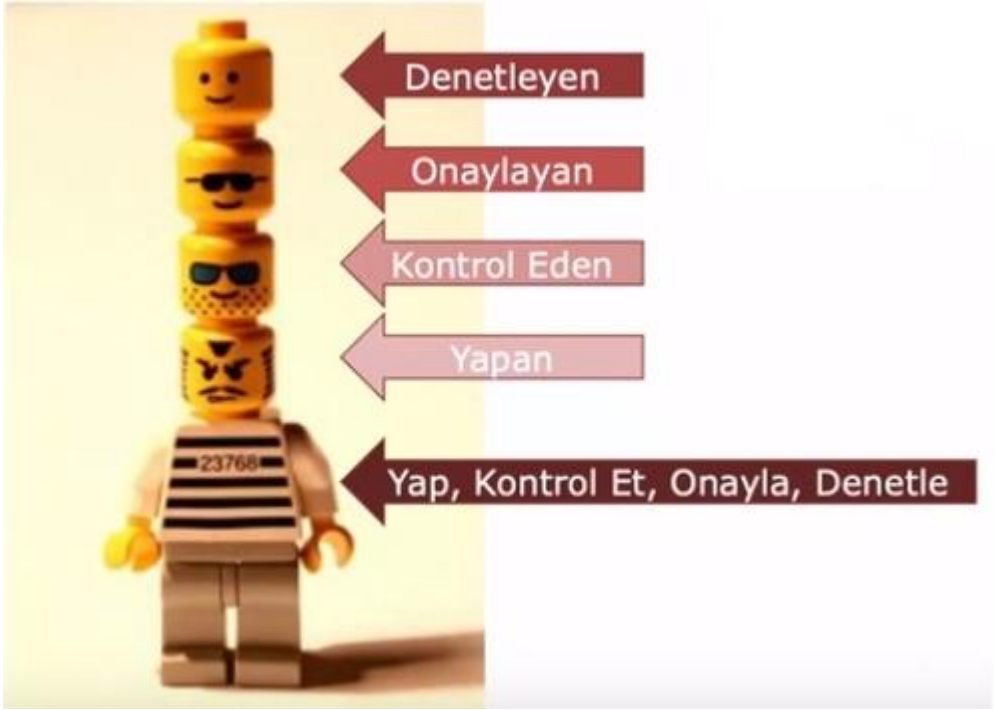
En Az Haklar İlkesi

5.1.3. Windows İşletim Sistemi Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.3.1	1	Kullanıcı Haklarının Kısıtlanması	Kullanıcı hakları en az yetki prensibi göz önünde bulundurularak sadece ihtiyaç duyulan kullanıcı ve gruplara verilmelidir.
3.2.3.3	1	En Az Yetki Prensibinin Uygulanması	Kullanıcılara verilecek yetkiler, yürütülen görevler ve ihtiyaçlar doğrultusunda belirlenmelidir. En az yetki prensibine göre kullanıcının gerçekleştirebileceği ilgili işlemler için gereken asgari yetkilerin haricinde bir ayrıcalık tanımlanmamalıdır.

Görevler Ayrılığı İlkesi



Hassas bir işi tamamlamak için birden fazla kişinin gerekli olmasıdır.

Bütün şapkaları aynı kişi giymemelidir.

BİLGİ GÜVENLİĞİ NEDEN ÖNEMLİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Bilgi uygun şekilde korunmazsa;

- Kuruma ait hassas bilgiler çalınabilir veya açığa çıkabilir,
- Kurumsal imaj sarsılabilir,
- İş sürekliliği aksayabilir,
- Yasal yaptırımlarla karşılaşılabilir,
- Elektronik ortamda kurum adınıza işlem yapılabilir,
- Siber Savaşlar kaybedilebilir

BİLGİ GÜVENLİĞİ NEDEN ÖNEMLİ

Personel Farkındalığının Önemi;

- Bilgi güvenliğinin en önemli parçası kullanıcı güvenlik bilincidir.
- Saldırganlar çoğunlukla kullanıcı hatalarını kullanmaktadır.
- Bir kullanıcının güvenlik ihlali tüm sistemi etkileyebilir. KVKK kapsamında tüm kurumu sorumlu kılabilir.
- Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır.
- Siber güvenliğin sağlanması için kritik öneme sahiptir.

BİLGİ GÜVENLİĞİ NEDEN ÖNEMLİ?

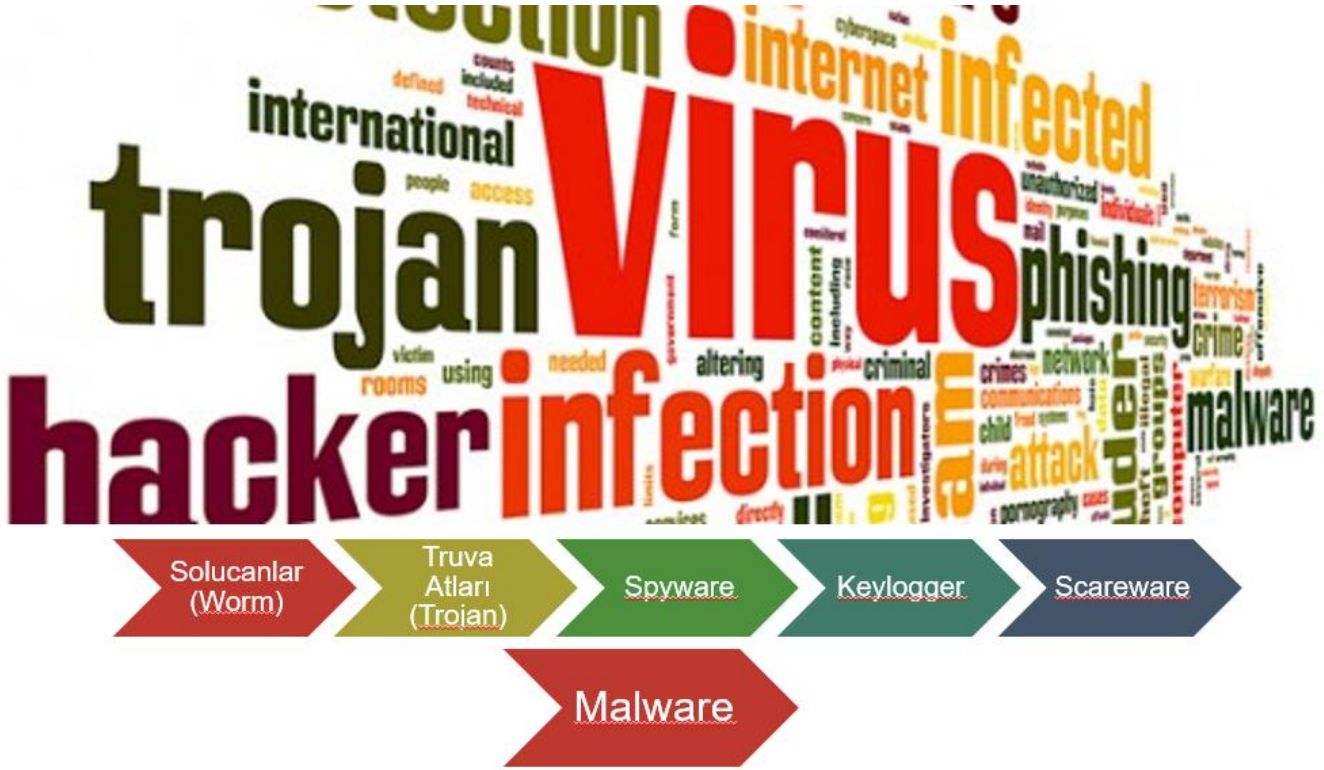
Siber Uzayda saldırılar **7/24** devam etmektedir. Ülkemiz hedef ülkeler arasında genellikle **ilk 3** sırada yer almaktadır.

TEHDİTLER ve ZARARLI YAZILIMLAR

Bilgiye ve bilgi varlıklarına yönelik bazı tehditler şunlardır;

- Kimlik bilgilerinizin ele geçirilerek kötü amaçla kullanılması,
- Servis dışı bırakma saldırıları (DDoS).
- Virus, trojan, Ransomware vb.zararlı yazılımlar.
- Bilgisayarınızın başkası tarafından ele geçirilerek suç işlenmesi,
- Bilgisayarınızın kurum ağına giriş kapısı olarak kullanılması,
- Web sayfası içeriğinin değiştirilmesi.
- İzinsiz kaynak kullanılması,
- Bilginin bozulması ya da çalınması.

Virüs, Ransomware, Malware Saldırıları

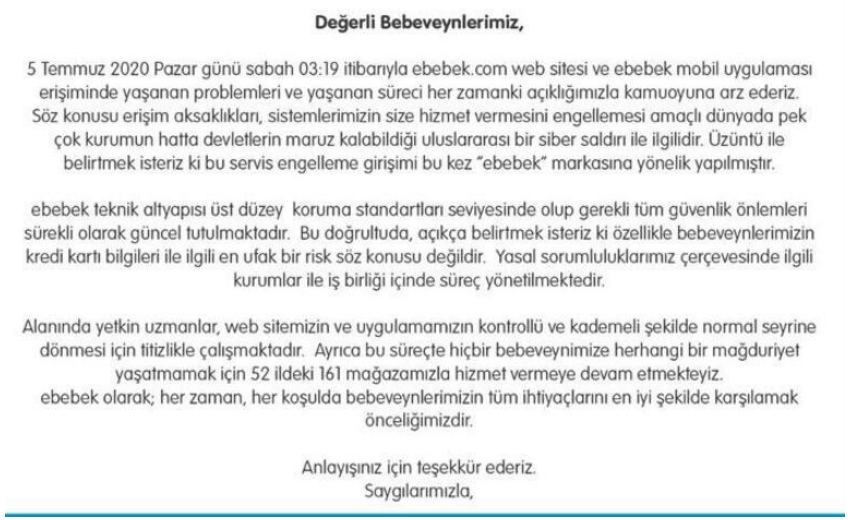


Zararlı yazılım, kötü amaçlı yazılım veya malware, bilgisayar ve mobil cihazların işlevlerini bozmak, kritik bilgileri toplamak, özel bilgisayar sistemlerine erişim sağlamak ve ya istenmeyen reklamları göstermek amacı ile kullanılan yazılımdır.

Fidye Yazılımı (Ransomware)

Fidye yazılımı, kurbanın **verilerini yayınlamakla tehdit eden** veya bir fidye ödenmedikçe bu **verilere erişimi sürekli olarak engelleyen**, zararlı yazılım türüdür.

Saldırgan verilerinize yeniden erişebilmeniz için ihtiyaç duyduğunuz şifreyi size vereceğini ancak belirtilen süre içerisinde talep edilen fidyenin ödenmesi gerektiğini belirten bir mesaj gönderir.



Değerli Bebeveynlerimiz,

5 Temmuz 2020 Pazar günü sabah 03:19 itibarıyla ebebek.com web sitesi ve ebebek mobil uygulaması erişiminde yaşanan problemleri ve yaşanan süreci her zamanki açıklığımızla kamuoyuna arz ederiz. Söz konusu erişim aksaklıkları, sistemlerimizin size hizmet vermesini engellemesi amaçlı dünyada pek çok kurumun hatta devletlerin maruz kalabildiği uluslararası bir siber saldırı ile ilgilidir. Üzüntü ile belirtmek isteriz ki bu servis engelleme girişimi bu kez "ebebek" markasına yönelik yapılmıştır.

ebebek teknik altyapısı üst düzey koruma standartları seviyesinde olup gerekli tüm güvenlik önlemleri sürekli olarak güncel tutulmaktadır. Bu doğrultuda, açıkça belirtmek isteriz ki özellikle bebeveynlerimizin kredi kartı bilgileri ile ilgili en ufak bir risk söz konusu değildir. Yasal sorumluluklarımız çerçevesinde ilgili kurumlar ile iş birliği içinde süreç yönetilmektedir.

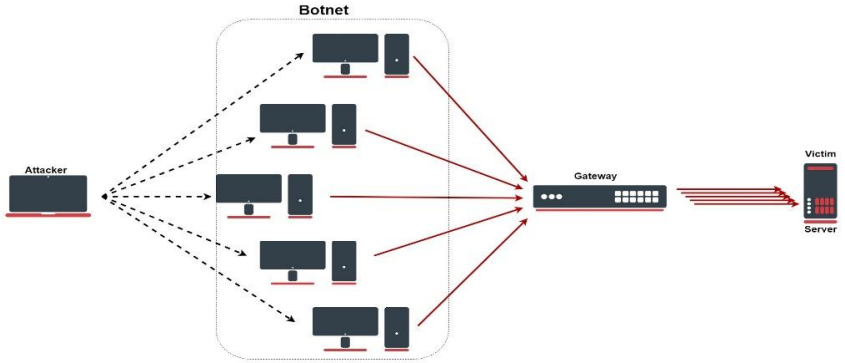
Alanında yetkin uzmanlar, web sitemizin ve uygulamamızın kontrollü ve kademeli şekilde normal seyrine dönmesi için titizlikle çalışmaktadır. Ayrıca bu süreçte hiçbir bebeveynimize herhangi bir mağduriyet yaşatmamak için 52 ildeki 161 mağazamızla hizmet vermeye devam etmekteyiz.
ebebek olarak; her zaman, her koşulda bebeveynlerimizin tüm ihtiyaçlarını en iyi şekilde karşılamak önceliğimizdir.

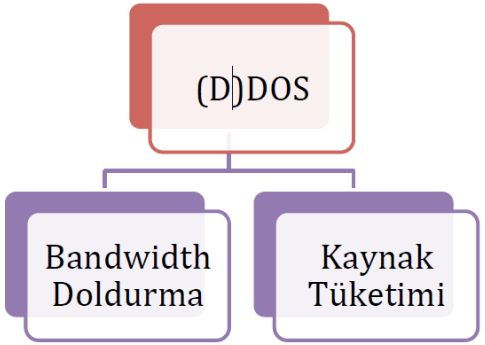
Anlayışınız için teşekkür ederiz.
Saygılarımızla,

SERVİS DIŞI BIRAKMA SALDIRILARI

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

- **DOS (Denial Of Service):** Herhangi bir sistemi, servisi, ağı işlevini yerine getiremez hale getirmek için yapılan saldırılar
- **DDOS (Distributed Of Service)** DOS saldırılarının organize şekilde birden fazla kaynakla yapılmasına DDOS denir.
- **Zombi:** Ele geçirilmiş ve sahibinden habersiz şekilde çeşitli amaçlar için kullanılan bilgisayar sistemleri. Zombiler en önemli DDOS kaynaklarındandır.
- **Botnet (Robot Networks**) Zombiler tarafından oluşturulan ve çeşitli amaçlarla kullanılan sanal bilgisayar ordularıdır. Zombiler botnetleri oluşturur, botnetler organize siber suçlarda sık kullanılan ara elemanlardır.
- **IP Spoofing:** Saldırganın yakalanma riskini yok etmek için IP adresini olduğundan farklı göstermesi





Zero Day (Sıfırıncı Gün) Saldırıları

Zeroday (Sıfırıncı gün açıklıkları) daha önceden bilinmeyen veya tespit edilmemiş ancak ciddi saldırılara yol açacak zafiyetler barındıran yazılım veya donanım Kusurlarıdır. Zeroday açıklıkları çoğunlukla saldırı gerçekleşene kadar tespit edilmesi zor olan zafiyetlerdir

FİREEYE: Merkezi Kaliforniya da bulunan halka açık bir siber güvenlik şirketidir. Siber güvenlik saldırılarını araştırmak, kötü amaçlı yazılımlara karşı korumak ve BT güvenlik risklerini analiz etmek için donanım, yazılım ve hizmetler sağlıyor. **8 Aralık 2020** de yapılan açıklama da Red Team testlerinde kullandıkları araçların çalındığını bildirdi.

https://www.bleepingcomputer.com/news/security/fireeye-reveals-that-it-was-hacked-by-a-nation-state-apt-group/

Leading cybersecurity company FireEye disclosed today that it was hacked by a threat actor showing all the signs of a state-sponsored hacking group.

TEHDİTLER ve ZARARLI YAZILIMLAR

Siber suçlular, e-posta şablonunda iyi bilinen bir hizmet olarak görünmeye çalışır (genellikle bilinen bir kurumun bilinen bir markası gibi görünmeye çalışırlar, ISP, Üniversite, Belediye, Banka vb.. kurumsal hizmetler). Daha sonra kullanıcıyı bir bağlantıya tıklamaya ikna etmeye çalışırlar.

KİMLİK HIRSIZLIĞI

ZARARLI YAZILIM TRENDLERİ

CloudMensis;

- MacOs, iOS, iPadOS Cihazlarını hedef alan casus yazılım,
- Kod yürütme ve yetki yükseltme yapabiliyor. İzinleri kendisi aktif edebilmektedir.
- Gerekli yetkileri elde ettiği anda, veri kaçırma faaliyetlerine başlar.
- **İyileştirme:** MacOS cihazlarında

“System Integrity Protection (SIP)”

Güvenlik mekanizması aktif olmalıdır.

ZARARLI YAZILIM TRENDLERİ

ChromeLoader;

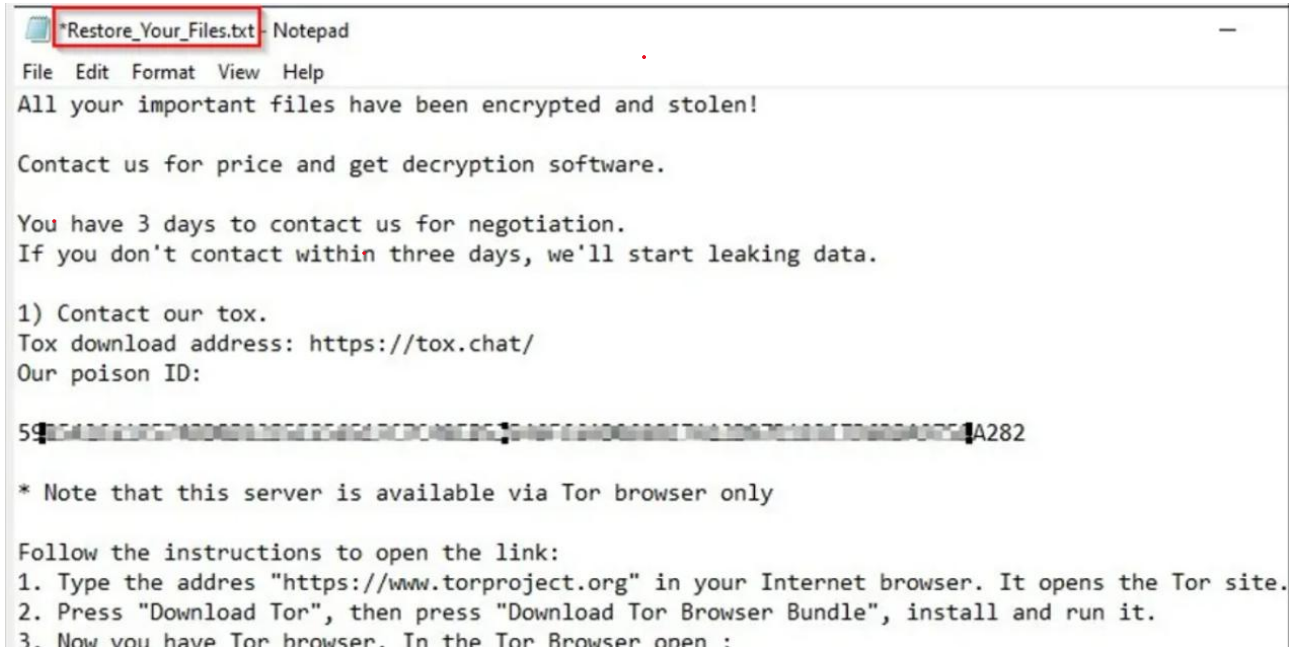
- Ocak 2022 tarihinde ortaya çıkan zararlı yazılım, Chrome eklenti kurup ele geçirmektedir.
- Bulaşma yöntemi QR kodları aracılığı ile ISO, DMG veya AHK dosyası indirmektedir.
- Güvenlik cihazlarını atlatmaktadır. Tarayıcı verilerini okumakta ve manipüle etmektedir.
- Kullanıcıları reklam sitelerine yönlendirmektedir.

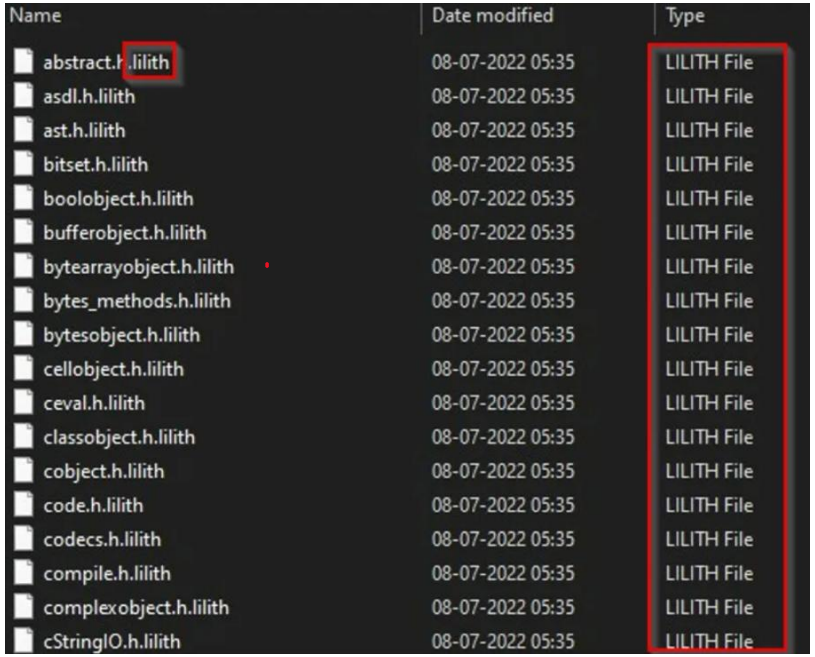
ZARARLI YAZILIM TRENDLERİ

Ciphbit Ransomware;

- 2024 yılının ilk çeyreğinde tespit edildi.
- Şifrelediği dosyalara “**.CiphBit**” uzantısını eklediği gözlemlendi.

Orijinal Dosya	Şifreli Dosya
`rapor.docx`	`rapor.docx.ciphbit`
`veri.xlsx`	`veri.xlsx.cipherbit`
`db.sql`	`db.sql.locked`
`image.jpg`	`image.jpg.enc`





2026 HEDEFLİ FİDYE OPERASYONLARI

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Live Ransomware Statistics

26269
Total Incidents
Ransomware attacks documented across all time periods

212
Active Groups
Ransomware groups currently tracked in our database

0APT
Most Active Group
144 incidents (30 days)

920
This Month
New incidents reported in the last 30 days

309
This Week
New incidents reported in the last 7 days

69
This Day
New incidents reported today

https://www.ransom-db.com/ransomware-statistics

Overview - Last 30 Days

238
Total Incidents
34.0 per day avg

37
Active Groups
of 218 total

42
Countries Affected
Geographic spread

-19.6%
Growth Rate
vs previous period

CISCO NASIL HACK'LENDİ?

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

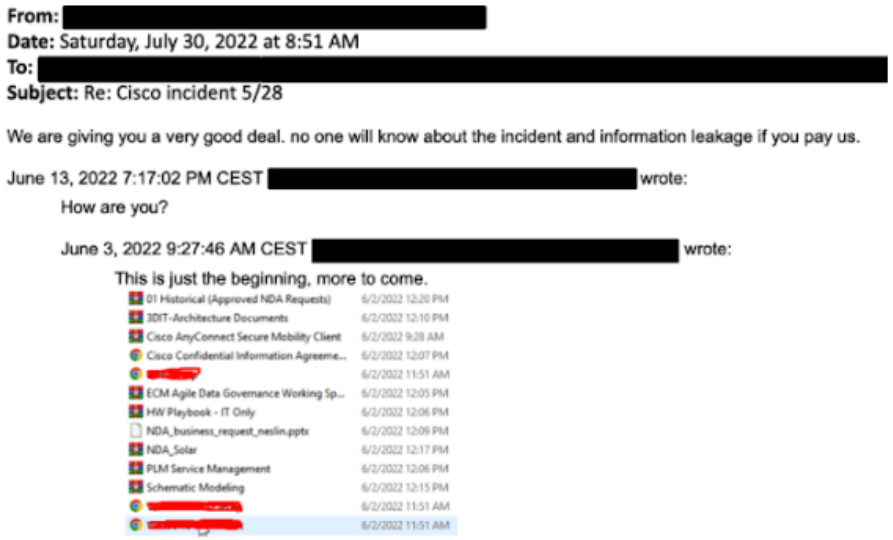
10.08.2022 tarihinde tehdit aktörlerinin dosyaları yayınlayacağı iddiası ile ortaya çıkıyor.

1. Çalışanın Google hesabı ele geçirilmiş.

2. Chrome tarayıcıda saklanan kurumsal kimlik bilgileri ele geçiriliyor.

3. Voice phishing MFA atlatma teknikleri kullanarak VPN erişimi ele geçiriliyor.

4. Active Directory hesapları ele geçirilip, sızdırılmış.


From: [redacted]
Date: Saturday, July 30, 2022 at 8:51 AM
To: [redacted]
Subject: Re: Cisco incident 5/28

We are giving you a very good deal. no one will know about the incident and information leakage if you pay us.

June 13, 2022 7:17:02 PM CEST [redacted] wrote:

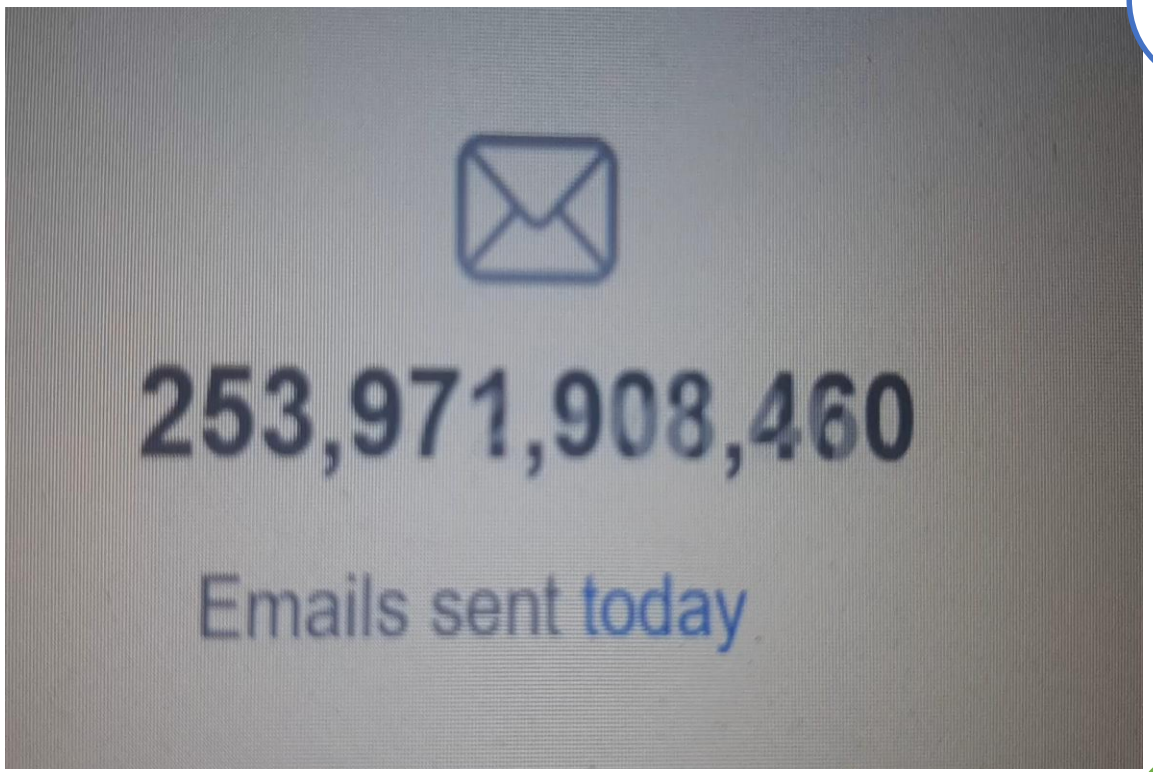
How are you?

June 3, 2022 9:27:46 AM CEST [redacted] wrote:

This is just the beginning, more to come.

01 Historical (Approved NDA Requests) 6/2/2022 12:20 PM
3DIT-Architecture Documents 6/2/2022 12:10 PM
Cisco AnyConnect Secure Mobility Client 6/2/2022 9:28 AM
Cisco Confidential Information Agreeme... 6/2/2022 12:07 PM
[redacted] 6/2/2022 11:51 AM
ECM Agile Data Governance Working Sp... 6/2/2022 12:05 PM
HW Playbook - IT Only 6/2/2022 12:06 PM
NDA_business_request_neslin.pptx 6/2/2022 12:09 PM
NDA_Solar 6/2/2022 12:17 PM
PLM Service Management 6/2/2022 12:06 PM
Schematic Modeling 6/2/2022 12:15 PM
[redacted] 6/2/2022 11:51 AM
[redacted] 6/2/2022 11:51 AM

E-POSTA GÜVENLİĞİ – PROBLEM NEDİR?



- Günde 260 Milyar E-posta gönderiliyor
- Bunların %70 i zararlı kod içeriyor
- Zararlı engelleme yetersiz
- Güvenlik Sorunları Yaşanıyor
- Kurumlar Karaliste ye düşüyor.

E-Postamı neler tehdit edebilir?

Mesajlarını zararsız gibi gösterirler.

İçine istedikleri her şeyi gizleyebilirler

Dolandırıcılar sizi yanıltmak için çeşitli hilelerden faydalanır.

En belirgin örnek **manipülatif ifadelerdir**. Örneğin, para veya önemli bir hizmete erişiminizi kaybedeceğinizi söyleyen ve zaman daraldığı için bir an önce harekete geçmenizi (örneğin, şifrenizi veya bilgilerinizi göndermenizi) isteyen mesajlar.

E-POSTA GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Eğer teklif edilen şey size gerçek dışı geliyor ise büyük ihtimalle öyledir.

E-POSTA GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Dolandırıcılar, her şeyden önce bir e-postanın tehlike oluşturup oluşturmayacağını düşünmeyen dikkatsiz kullanıcılara güvenir..

- Şifrenizi veya kredi kartı bilgilerinizi hiçbir zaman e-postayla göndermeyin.
- **E-Posta ile Gönderilmesi Riskli Veri Türleri**;
- Kimlik Bilgileri.
- Araç Ruhsatı
- Tıbbı Kayıtlar
- Tapu
- Doğum Belgesi

Belgelerinizi hiçbir zaman yabancılara göndermeyin.

Alıcının gerçek olup olmadığını her zaman dikkatlice kontrol edin

Herhangi bir şey göndermeden önce isteğin meşru olup olmadığını kontrol edin.

PAROLA GÜVENLİĞİ

- **Parola** okunduğunda anlam ifade **açık metin** şeklindeki ifadelerdir.
- **Şifre** ise kriptografik algoritma ile işlenmiş, okunduğunda anlam ifade etmeyen farklı algoritmalar ile oluşturulabilen ifadelerdir.
- Açık metni şifreleyen birçok algoritma bulunmaktadır. Bunların en eskisi **Sezar Şifresi** olarak bilinen harf kaydırma yöntemi ile şifreleme yapan algoritmadır. **Günümüzde çok gelişmiş şifreleme yöntemleri mevcuttur.**
- **Secure Hashing Algorithm** olarak adlandırılan, şifreleme algoritmaları içerisinde en yaygın olarak kullanılan algoritma **SHA1**,dir.
- **Siber Saldırgan parolanızın şifreli hali ile de erişim sağlayabilir.** (Pass the hash)

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Parolamız neden tehdit altında?

Kullanıcıların %28'i şifrelerini bir deftere, %9'u ise bilgisayarın en yakınında duran kağıda not alıyor.

Bir hackleme girişimi olduğunu fark etsek bile dolandırıcıların hedeflerine ulaşmadığını anladığımızda şifremizi değiştirmeden sakinleşebiliyoruz.

Bilgi güvenliğinin temel ilkelerinden haberdar olup olmadıklarını bile bilmeden şifreleri akrabalarımıza, iş arkadaşlarımıza veya arkadaşlarımıza verebiliyoruz.

Halihazırda ezberlediğimiz güvenli bir şifrenin (örneğin, kişisel e-postamızın şifresi) neden kurumsal kaynaklar için de kullanamayacağımızı çoğunlukla anlayamıyoruz. Bir kaynakta kullandığımız şifre, hacklenmesi zor bir şifreyse bunun diğer kaynaklar için de işe yarayacağını düşünüyoruz.

PAROLA GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Parolalarınızı güvenli bir şekilde saklamanın birçok farklı yolu vardır. Örneğin, bir **parola yöneticisi** kullanabilir veya parolanızı sizden başka hiç kimsenin anlayamayacağı şekilde değiştirerek bir yere yazabilirsiniz (yani bir **hatırlatma notu** kullanabilirsiniz).

GÜVENLİ PAROLA SAKLAMANIN İKİ ÖNEMLİ KURALI

Parolanızı asla tam olarak hesabınızda oturum açmak için kullandığınız şekliyle saklamayın. Diğer bir deyişle, parolanın hatırlatıcısı, gerçek parolanızın kendisi olmamalıdır.

Parola hatırlatıcınızı başkalarından gizli tutun. Değiştirilmiş olsa bile, dolandırıcıların gerçek parolanızı bulmalarına yardımcı olabilir.

PAROLA GÜVENLİĞİ

PAROLA HATIRLATICI NASIL OLUŞTURULUR

Ortasına, başına veya sonuna rastgele birkaç karakter ekleyerek,

Birkaç karakteri değiştirerek,

Parolanın yalnızca bir kısmını yazıp gerisini akılda tutarak.

Parolanızı hatırlamanıza yardımcı olan her şey parola hatırlatıcısıdır.

Parola hatırlatıcısı, şunlardan biri olabilir:

- parolanın değiştirilmiş hali (örneğin, ilave karakterler eklenerek)
- bir soru (cevabı parolanızdır ve yalnızca sizin bildiğiniz bir şeydir)
- parolanızı aklınıza getiren bir çizim

...ve benzerleri.

PAROLA GÜVENLİĞİ

- Diş fırçanızı başkasıyla paylaşır mısınız?
- Aynı diş fırçasını yıllarca kullanır mısınız?
- Ortak kullanılan bir diş fırçası olabilir mi?

- Parolanızı da **paylaşmayın!**
- Parolanızı da belirli aralıklarla **yenileyin!**
- Parolanız da size özeldir, kimseyle **paylaşmayın!**

PARODA GÜVENLİĞİ

Here is the list of the TOP 20 worst passwords of this year:

1. 123456
2. 123456789
3. 12345
4. qwerty
5. password
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567
11. qwerty123
12. 000000
13. 1q2w3e
14. aa12345678
15. abc123
16. password1
17. 1234
18. qwertyuiop
19. 123321
20. password123

Yalnızca dolandırıcılar, şifrelerinizi nerede ve nasıl sakladığınızı sorar.

Temiz Masa Temiz Ekran

FİZİKSEL GÜVENLİK

- Yetkili kişi/kişilerin odada bulunmadığı zamanlarda oda kilitli tutulmalıdır,
- Yetkisiz kişilerin ortama erişimleri kontrollü olmalıdır,
- Kritik bilgi içeren belgeler yazıcılarda, fotokopi veya faks cihazlarında bırakılmamalıdır,
- Hatalı çıktısı alınan doküman kağıt öğütücü ile veya elle okunamayacak şekilde ufaltılana kadar yırtarak imha edilmelidir.
- Güvenli alanlarda çalışma kuralları belli olmalıdır,
- Güvenli alanlara kayıt cihazlarının sokulmasını engelleyici kontroller olmalıdır vb.

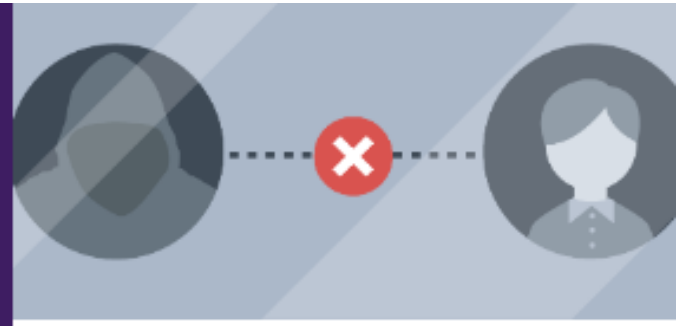
PC ve MOBİL CİHAZ GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

BİLGİSAYARLARIMIZI KORUMA KONUSUNDA NEDEN YETERİ KADAR ÖZENLİ DEĞİLİZ?

Bilgisayarımıza yalnızca fiziksel olarak bilgisayarımızın başına oturan bir kişinin erişebileceğini düşünüyoruz. Ancak durum böyle değil.

Virüsten koruma yazılımının kötü amaçlı programlara karşı her derde deva olduğuna inanıyoruz. Ama bu doğru değil.

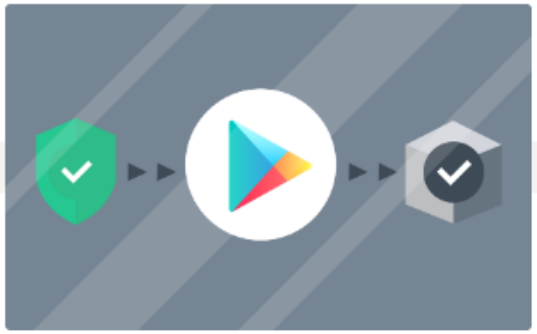


Bir dolandırıcının isteyebileceği neredeyse hiçbir şeye sahip olmayan sıradan insanlarla kimsenin ilgilenmediğini düşünüyoruz. Fakat bu bir yanılsama.

PC ve MOBİL CİHAZ GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Mobil uygulamalar nasıl güvenli ve emniyetli bir şekilde yüklenir



Google Play

2008'de kurulan bu en büyük Android uygulama mağazasıdır (3.000.000'den fazla uygulama). Tüm gerçek Android uygulamaları burada bulunabilir. Platform, entegre bir antivirüse sahiptir.

App Store

2008'de kurulan bu en büyük iOS uygulama mağazasıdır (2.500.000'den fazla uygulama içerir). Var olan tüm iOS uygulamaları burada bulunabilir.

1. Resmi mağazalar her zaman en geniş uygulama yelpazesine sahiptir.
2. Resmi mağazalardaki uygulamalar her zaman dikkatlice doğrulanır.
3. Resmi mağazalar, istediğiniz zaman uygulama geliştiricisiyle iletişim kurmanıza izin verir.
4. Resmi mağazalar şikayetleri ve iddiaları kabul eder ve hatta paranızı iade eder.
5. Resmi mağazalarda, uygulama derecelendirmelerini görebilir ve gerçek kişilerin yorumlarını okuyabilirsiniz.
6. Resmi bir mağazadan uygulama satın aldığınızda kesinlikle yasaları veya geliştiricilerin telif haklarını ihlal etmemiş olursunuz.

PC ve MOBİL CİHAZ GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Bir mobil cihazda işletim sistemini ve tarayıcıyı güncellemek neden önemlidir?

Telefonunuzun çalındığını düşünün. Cihaza erişim elde eden hırsız;

- sosyal medya gönderilerinizi ve mesajlarınızı okuyabilir,
- kişisel fotoğraflarınızı kendi amaçları doğrultusunda kullanabilir,
- telefon numaranıza bağlı bir banka hesabından para çalabilir,
- bulutta depolanan kurumsal belgeleri şirketinizin rakiplerine satabilir
- ve telefonun geri vermek için fidye talep edebilir.

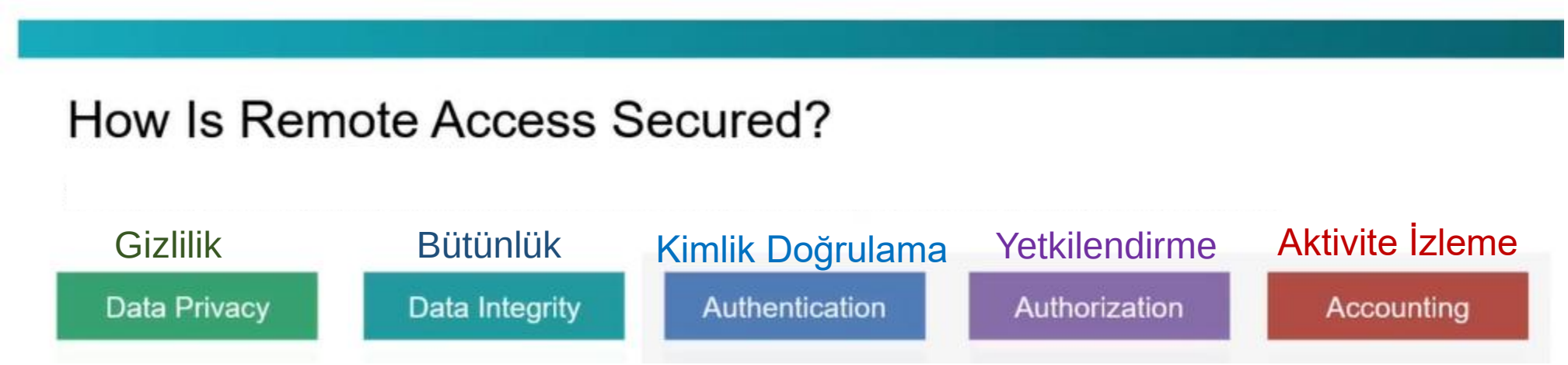
1 2

Uygulamalar genellikle arka planda güncellenir; uygulamalar güncellenirken akıllı telefonunuzu ve diğer uygulamalarınızı güvenle kullanabilirsiniz. Büyük olasılıkla, bir uygulama güncellenirken bunun farkına bile varmazsınız.

Ancak, **işletim sisteminin güncellenmesi gerekirse telefon yeniden başlatılır**, dolayısıyla belli bir süre için kullanılamaz. Bu nedenle, işletim sistemini güncellemek için en iyi zaman, başka aramalar yapmanız gerekmediği veya acil olarak akıllı telefonunuza ihtiyaç duymadığınız zamanlardır.

GÜVENLİ UZAKTAN ERİŞİM

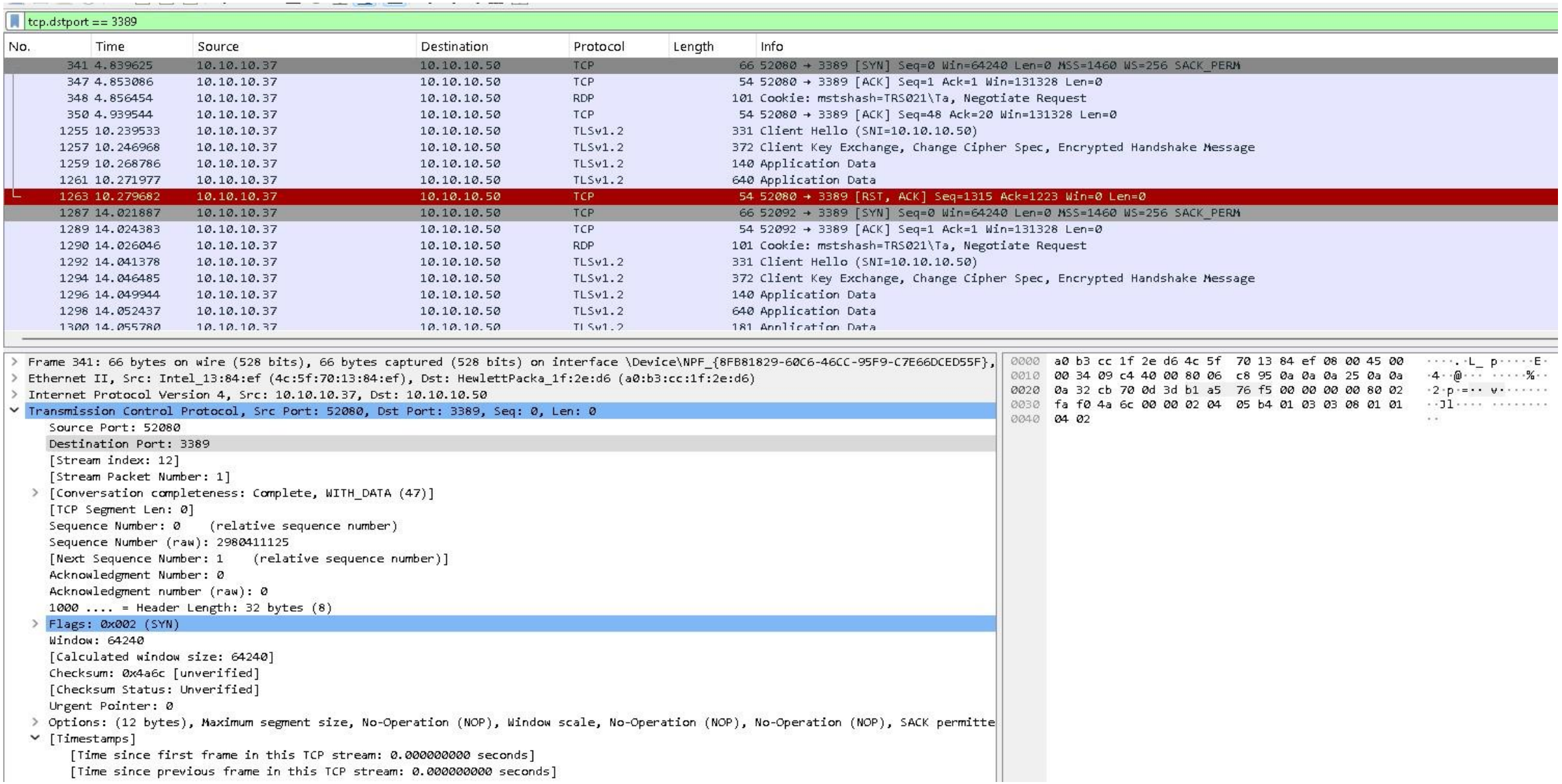
Uzaktan çalışmanın yaygınlaşması ile birlikte **güvenli uzaktan erişim**, şirketler için vazgeçilmez bir hale geldi.



Güvenli Uzaktan Erişim yapılandırmanıza bağlı olarak bu özelliklerini tümüne sahip olmalıdır.

GÜVENLİ UZAKTAN UYGULAMA ÖRNEĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT



GÜVENLİ UZAKTAN UYGULAMA ÖRNEĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT


```
Connection received from 10.10.10.37:32072
Warning: RC4 not available on client, attack might not work
Listening for new connection
Server enforces NLA; switching to 'fake server' mode
Enable SSL
Connection lost on enableSSL: [Errno 104] Connection reset by peer
Hiding forged protocol request from client
Exception in thread Thread-3:
Traceback (most recent call last):
  File "/usr/lib/python3.10/threading.py", line 1016, in _bootstrap_inner
    self.run()
  File "/home/center/Seth/seth/main.py", line 49, in run
    self.run_fake_server()
  File "/home/center/Seth/seth/main.py", line 79, in run_fake_server
    self.lsock.send(resp)
  File "/usr/lib/python3.10/ssl.py", line 1235, in send
    return self._sslobj.write(data)
ssl.SSLEOFError: EOF occurred in violation of protocol (_ssl.c:2426)
Connection received from 10.10.10.37:32073
Warning: RC4 not available on client, attack might not work
Listening for new connection
Enable SSL
'NoneType' object has no attribute 'getsockopt'
Hiding forged protocol request from client
W10E01\administrator:Password01!
[*] Cleaning up...
[*] Done
root@center-egitim:/home/center/Seth#
```

SOSYAL MEDYA GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

GENELGE

Cumhurbaşkanlığından:
Konu: Bilgi ve İletişim Güvenliği Tedbirleri

GENELGE
2019/12

5. Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

6. Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir.

19. Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.

SOSYAL MEDYA GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Özel hayatın gizliliğini ihlal

Madde 134- (1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.[59]

(2) **(Değişik: 2/7/2012-6352/81 md.)** Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

KVKK GDPR AİHS Anayasa

Unutmayın: Gizliliğiniz bir lüks değil, temel bir haktır!

🔴 En kritik madde: TCK m.134 – Özel hayatın gizliliğini ihlal

Madde 134/1:

> Kişilerin özel hayatının gizliliğini ihlal eden kimse,
> **1 yıldan 3 yıla kadar hapis cezası** ile cezalandırılır.

Madde 134/2:

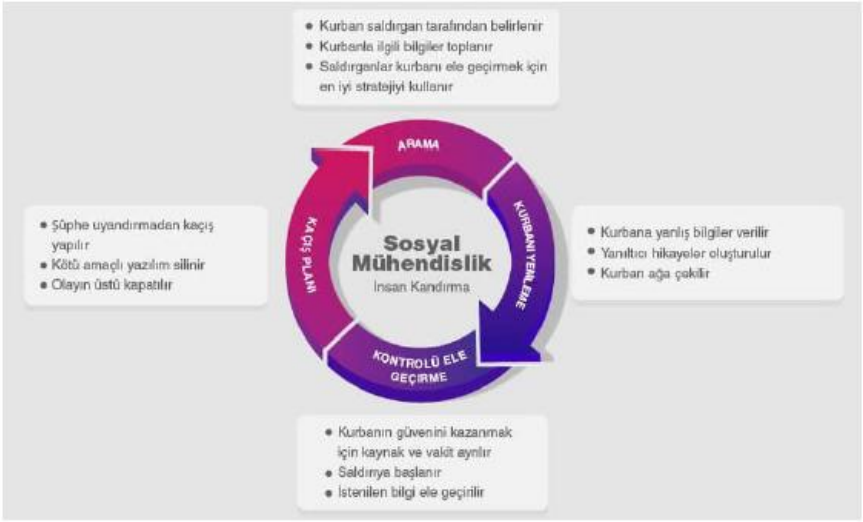
> Bu gizliliğin **görüntü veya seslerin ifşası suretiyle** ihlal edilmesi halinde, **ceza artırılır.**

📌 Önemli nokta:

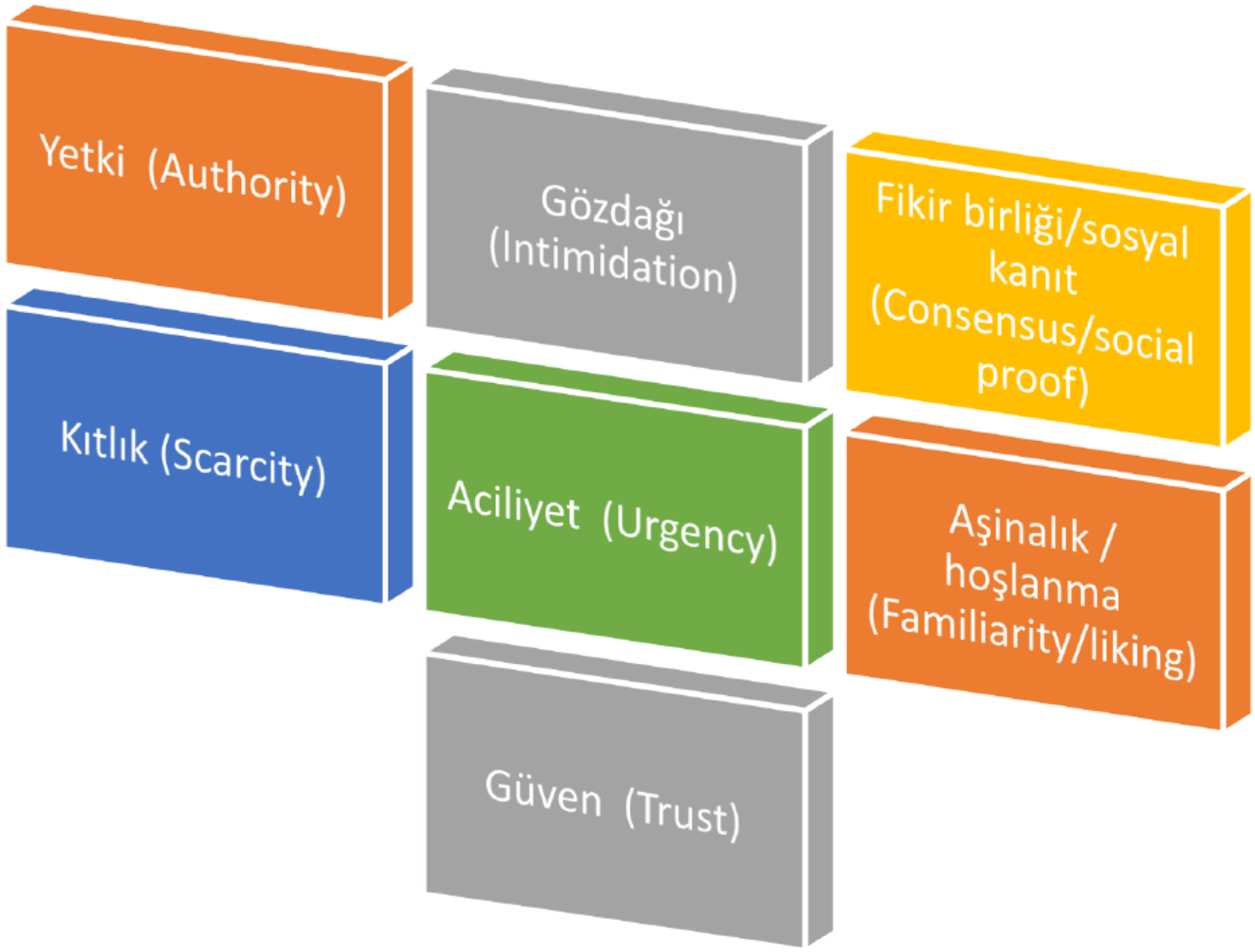
- Görüntü **daha önce internette yayınlanmış olsa bile**
- Kişinin **özel hayatına ilişkinse**
- Yeniden paylaşım **ayrı bir ihlal** sayılabilir

Sosyal Mühendislik Kavramı

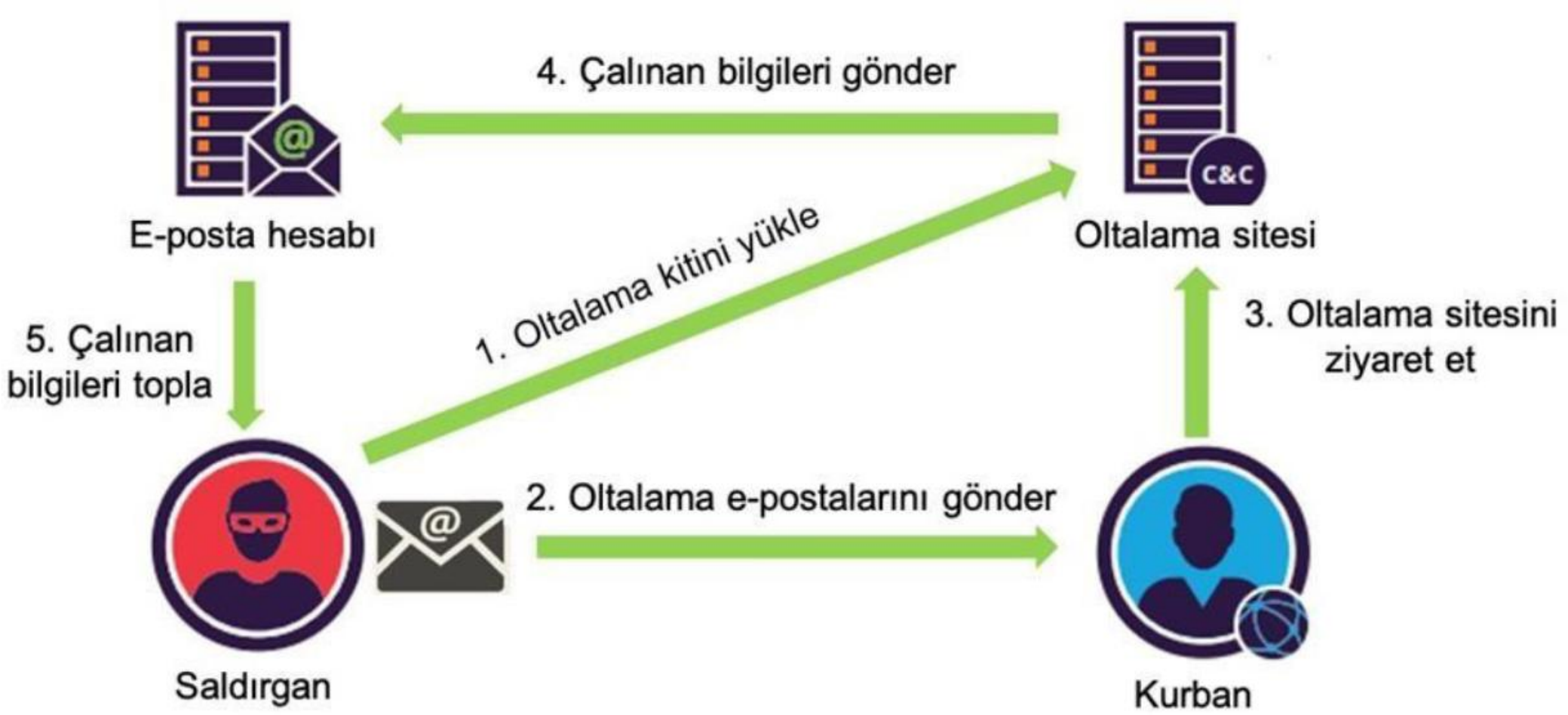
- Sosyal mühendislik, insan etkileşimleri yoluyla gerçekleştirilen çok çeşitli kötü niyetli faaliyetler için kullanılan terimdir.
- Kullanıcıları güvenlik hataları yapmaya veya hassas bilgilerini verme konusunda kandırmak için psikolojik manipülasyon kullanır.
- Sosyal mühendislik saldırıları bir veya daha fazla adımda gerçekleşir.



Sosyal Mühendisliğin Arkasındaki Prensipler



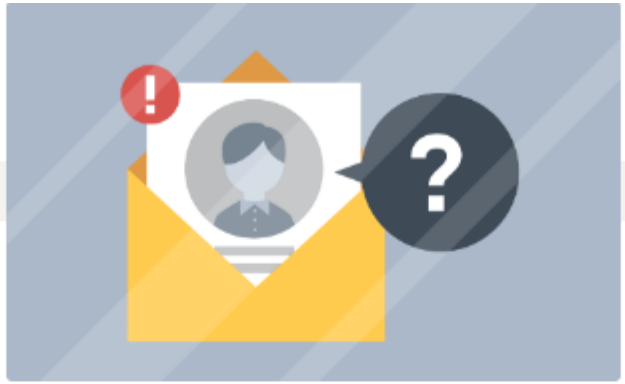
SOSYAL MÜHENDİSLİK SALDIRI TEKNİKLERİ



SOSYAL MEDYA GÜVENLİĞİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Sosyal medya hesabımın saldırıya uğrayıp uğramadığını nasıl anlarım ve ne yapmalıyım?



KURALLAR

- Birisinin sosyal medya hesabınıza eriştiğinden şüpheleniyorsanız, şifrenizi hemen değiştirin.
- Sosyal medya hesabınız hacklendiyse, hesabınıza tekrar erişim sağlayın ve en kısa sürede şifrenizi değiştirin.

İlk işaret, **hesabınızda yapmadığınız bir işlemle ilgili bir e-posta almanızdır**. Örneğin:

- Yetkisiz giriş denemesiyle ilgili bir uyarı,
- Bir şifre değişikliği isteği,
- Şüpheli hesap etkinliği hakkında bir mesaj.

Bu uyarıların veya isteklerin birçok farklı türü vardır. Ancak, hangisini alırsanız alın olun, birinin hesabınızı ele geçirmeye çalıştığını anlamanız gerekir.

~~YASAKLANMADIKÇA HERŞEY SERBESTTİR~~

İZİN VERİLMEDİKÇE HERŞEY YASAKTIR

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİ GÜVENLİĞİ

FARKINDALIK EĞİTİMİ

Anayasa Madde:20

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.

ANAYASA İLE GÜVENCE ALTINA ALINMIŞTIR

KVKK ÇIKIŞ SÜRECİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

7 Nisan 2016
Resmi Gazetede Yayınlandı

7 Ekim 2016
1. Son Tarih

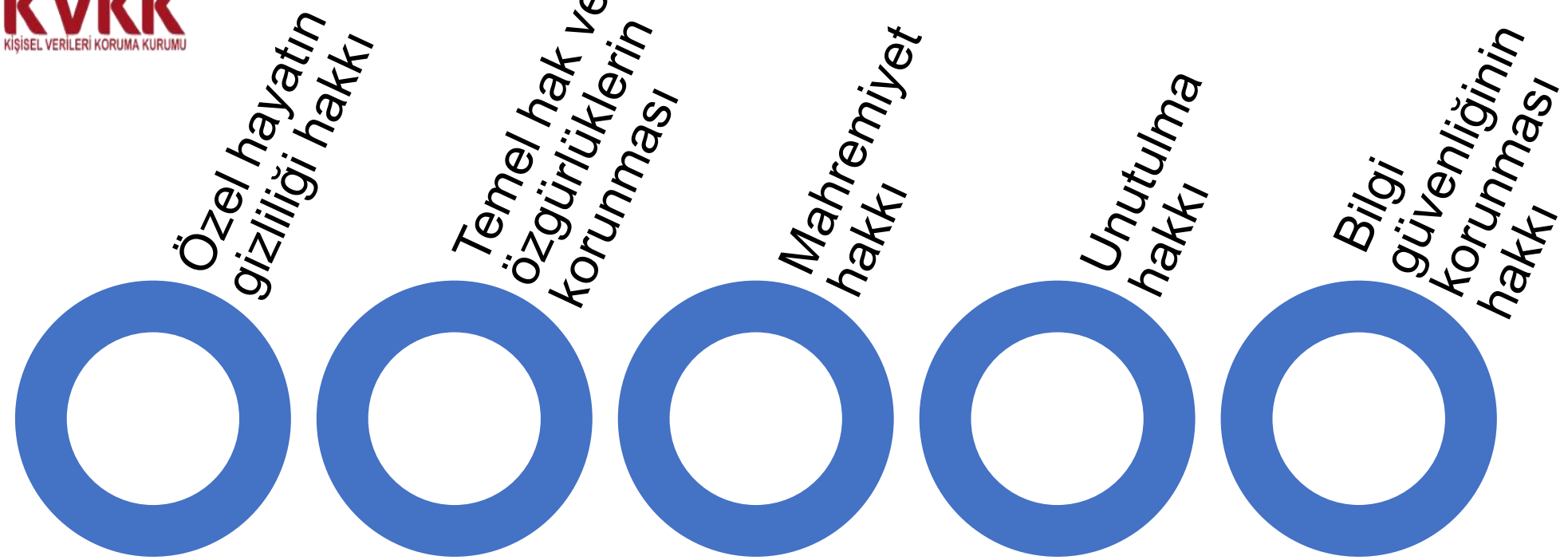
Kurul ve Sicil Kuruluşu
- VERBİS KAYIT
- Kişisel Verilerin Aktarılması
- İlgili Kişi haklarının belirlenmesi
- Hapis ve İdari para cezası yaptırımları

31 Aralık 2021
5. Son Tarih

Kurumlarda, 7 Nisan 2016 öncesindeki mevcut verilerin Kanun'a uyumlu hale getirilmesi aksi takdirde silinmesi, yok edilmesi ya da anonimleştirilmesi için son tarih.

KVKK DEĞİŞİKLİK

AMACI

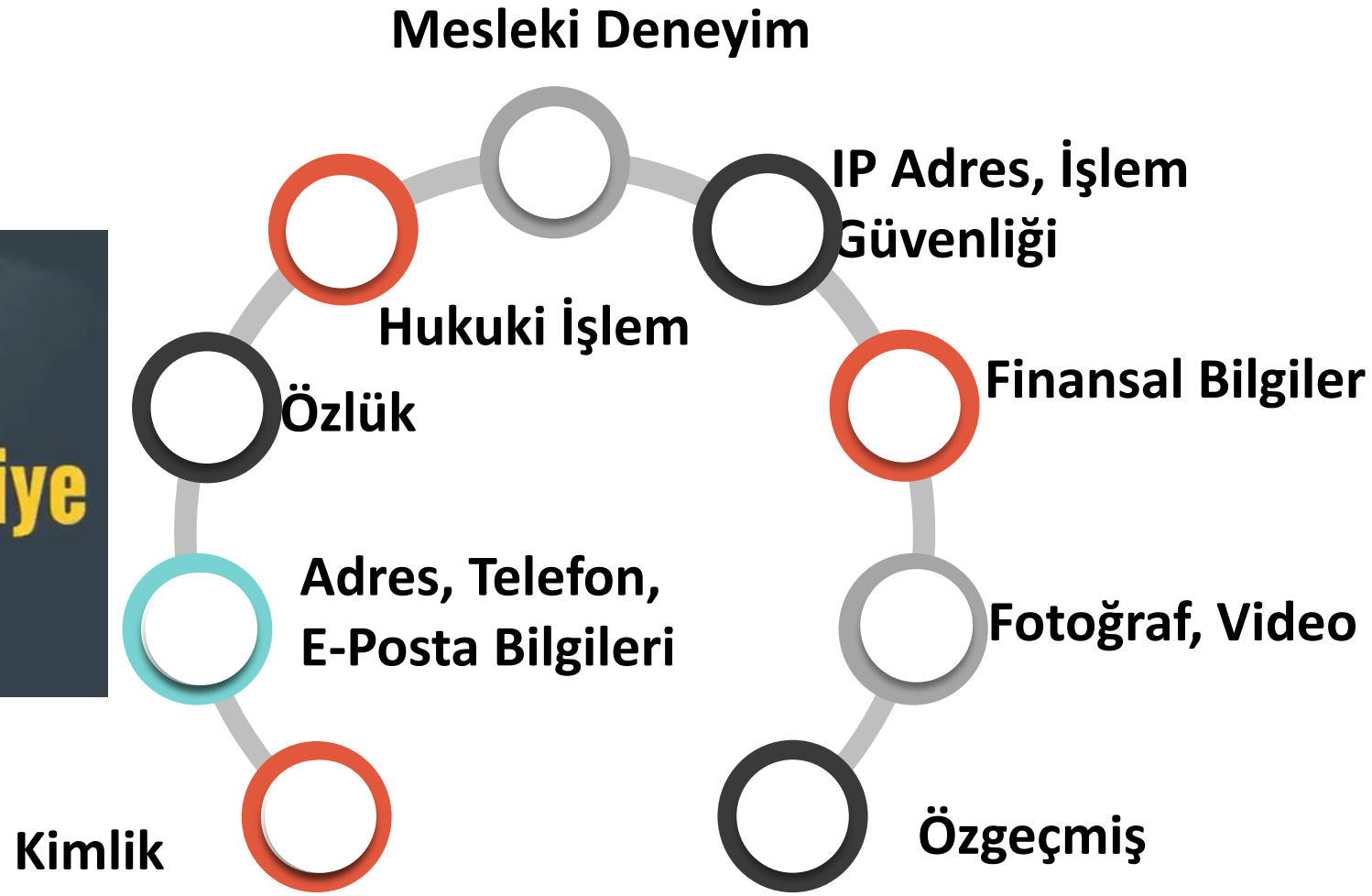


Kanunla koruma altına alınan veriler gerçek kişilere ait olan verilerdir. Tüzel kişilere ait olan veriler kanunun korumasından yararlanamaz.

KİŞİSEL VERİ NEDİR?

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin veri.



ÖZEL NİTELİKLİ KİŞİSEL VERİ NEDİR?

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Özel nitelikli kişisel verilerin işlenme şartları

MADDE 6- (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

Özel nitelikli kişisel veriler öğrenilmesi halinde **ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir.**

VERİ SORUMLUSU

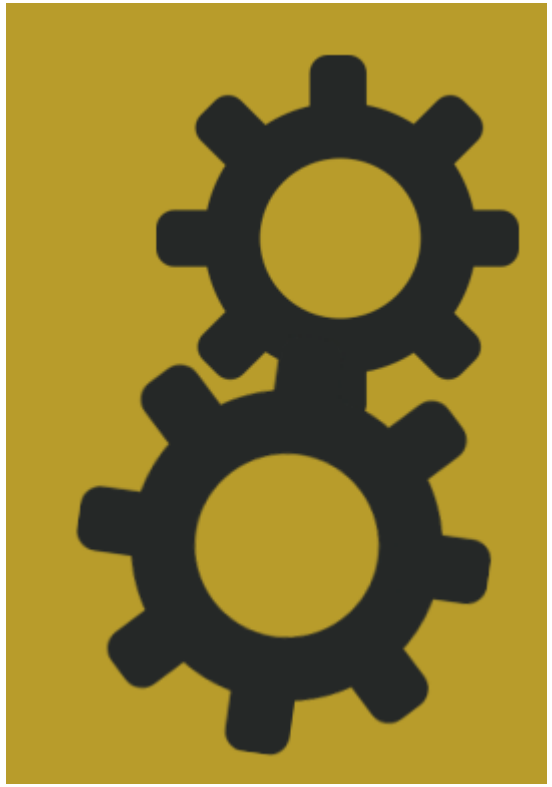
TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

VERİ İŞLEMEDE UYULMASI ZORUNLU İLKELER

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

- Hukuka ve dürüstlük kurallarına uygun olma.
- Doğru ve gerektiğinde güncel olma.
- Belirli, açık ve meşru amaçlar için işlenme.
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme



KVKK TEKNİK TEDBİRLER

- Kişisel Veri Güvenliği Rehberinde; Kişisel veri güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin, **çalışanların ilk müdahaleyi yapmaları**, kişisel veri güvenliğinin sağlanması konusunda büyük önem taşımaktadır.

- Çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.

KVKK TEKNİK TEDBİRLER

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

- YETKİ MATRİSİ
- YETKİ KONTROL
- ERİŞİM LOGLARI
- KULLANICI HESAP YÖNETİMİ
- AĞ GÜVENLİĞİ
- UYGULAMA GÜVENLİĞİ
- ŞİFRELEME
- SIZMA TESTİ
- SALDIRI TESPİT VE ÖNLEME SİSTEM
- LOG KAYITLARI
- VERİ MASKELEME
- VERİ KAYBI ÖNLEME YAZILIMLARI
- YEDEKLEME
- GÜVENLİK DUVARLARI
- GÜNCEL ANTİ-VİRÜS SİSTEMLERİ
- SİLME, YOK ETME VE ANONİM HALE GETİRME
- ANAHTAR YÖNETİMİ

KVKK 2026 YILI CEZALAR

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Madde	Aykırılık Oluşturan Madde	Açıklama	2026 YILI CEZA TUTARLARI (TL) %25,49 Artış ile	
			En Az	En Çok
18/a	10	Aydınlatma yükümlülüğünü yerine getirmeme	**85.437 TL**	**1.709.200 TL**
18/b	12	Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi	**256.357 TL**	**17.092.242 TL**
18/c	15	Kurul kararlarının yerine getirilmemesi	**341.809 TL**	**17.092.242 TL**
18/ç	16	Veri Sorumluları Siciline Kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi	**341.809 TL**	**17.092.242 TL**

TCK m.135

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.

Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, **iki yıldan dört yıla kadar hapis** cezası ile cezalandırılır.

Kanunların belirlediği sürelerin geçmiş olmasına karşın **verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis** cezası verilir.

Suçların işlenmesi dolayısıyla **tüzel kişiler** hakkında bunlara özgü **güvenlik tedbirlerine** hükmolunur."

ÖRNEK KURUL KARARLARI

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

"Bir üniversite tarafından ilgili kişilerin kişisel ve özel nitelikli kişisel verilerinin yer aldığı belgenin e-posta ekinde üçüncü kişilerle paylaşılması" hakkında Kişisel Verileri Koruma Kurulunun 01/06/2023 Tarihli ve 2023/928 Sayılı Karar Özeti

Karar Tarihi : 01/06/2023
Karar No : 2023/928
Konu Özeti : : Bir üniversite tarafından ilgili kişilerin kişisel ve özel nitelikli kişisel verilerinin yer aldığı belgenin e-posta ekinde üçüncü kişilerle paylaşılması

Veri sorumlusu üniversitenin kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirleri yeterli düzeyde almadığı,

Kanunun 18'inci maddesinin üçüncü fıkrası kapsamında kamu tüzel kişiliği niteliğindeki veri sorumlusu bünyesinde **görev yapan sorumlular hakkında disiplin hükümlerine göre işlem yapılarak sonucundan Kurul'a bilgi verilmesine,**

ÖRNEK KURUL KARARLARI

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Bir e-ticaret platformu tarafından Kurula intikal ettirilen veri ihlal bildirimi" hakkında Kişisel Verileri Koruma Kurulunun 08/08/2024 tarih ve 2024/1385 sayılı Karar Özeti

Karar Tarihi : 08/08/2024
Karar No : 2024/1385
Konu Özeti : Bir e-ticaret platformu tarafından Kurula intikal ettirilen veri ihlal bildirimi

•İhlalden etkilenen 7.202 müşterinin 1.213 tanesinin hesabında şüpheli sipariş oluşmasına neden olunduğunun tespit edildiği,

•Satıcıların ihlale konu portala ilk defa giriş yapmaları ya da son IP'lerinden farklı bir IP adresinden giriş denemeleri yapmaları durumunda tetiklenen tek seferlik parola sisteminin ancak ihlalden sonra uygulamaya konulduğu; veri sorumlusunun, ihlal öncesinde alması gereken tedbiri ihlalden sonra aldığı,

•Satıcıların (kullanıcı hesaplarına giriş yapmasının ardından) bilgi değişikliği ve giriş yapma süreçlerine çift faktörlü kimlik doğrulama (2FA) aşaması eklenmesi önleminin ancak ihlalden sonra alınan tedbirler kapsamında hayata geçirildiği; ihlalin olumsuz etkilerini azaltabilecek bir tedbirin ihlalin gerçekleşmesinden önce alınmadığı

Veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 3.250.000 TL idari para cezası uygulanmasına karar verilmiştir.

VERİ İHLALİ - VERİ SORUMLUSU BİLDİRİMİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Kişisel Veri İhlali Bildirimi

*Formu doldururken ihlale konu olan herhangi bir kişisel veriyi bu forma dahil etmeyiniz.

A) HAKKINIZDA

1. **Veri sorumlusunun unvanı/ismi :**
2. **Veri sorumlusunun adresi :**
3. **Veri sorumlusu adına bu bildirimi hazırlayan kişinin:**
   (Bu bildirim veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından doldurulması/gönderilmesi durumunda tevsik edici belgeleri (sözleşme, vekâletname vb.) ekleyiniz.)

   Adı ve Soyadı :

   Görevi/Unvanı :

   E-postası :

   Telefonu :

   Adresi :

B) İHLAL HAKKINDA

4. **Bildirim türü** : ☐ İlk bildirim ☐ Takip bildirimi ☐ Takip No
5. **İhlalin başlama tarihi ve saati** : GG/AA/YYYY - SS:DD

VERİ İHLAL BİLDİRİM ÖRNEKLERİ

Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Vodafone Net İletişim Hizmetleri A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri sorumlusu sıfatını haiz Vodafone Net İletişim Hizmetleri A.Ş tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin 10.01.2026 tarihinde başladığı ve 26.01.2026 tarihinde tespit edildiği,
- Veri sorumlusunun elektronik haberleşme hizmetlerine bağlı kurulum, nakil, arıza, evrak toplama ve aktivasyon süreçlerinin bölgesel hizmet tedarikçisi olarak söz konusu yetki bölgesinde yerleşik Vodafone ev interneti abonelerine sunulması kapsamında hizmet tedarik ettiği,
- VodafoneNet aboneleri, veri işleyen çalışanları ve veri işleyenin saha operasyonları adına hizmet aldığı tedarikçi çalışanı verilerinin DarkWeb üzerinden satışa sunulduğunun istihbar olunduğu,
- İstihbar olunan ilgili kayıtların yer alabileceği sistemler üzerinde detaylı bir soruşturma süreci başlatıldığı; yapılan incelemeler sonucunda, olaya konu kişisel verilerin, veri işleyenin sisteminden elde edilmiş olabileceği kanısına varıldığı,
- İhlalden etkilenen ilgili kişi sayısının tam olarak bilinemediği ve tespit etme çalışmalarının devam ettiği; ihlalden etkilenen ilgili kişi sayısının çok daha az olduğu düşünülmekle birlikte en fazla 321.504 olabileceği,

VERİ İHLAL BİLDİRİM ÖRNEKLERİ

Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Baydöner Restoranları A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri sorumlusu sıfatını haiz Baydöner Restoranları A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin 15.02.2026 tarihinde başladığı, 08.03.2026 tarihinde tespit edildiği,
- İhlalin; veri sorumlusu tedarikçi firması tarafından geliştirilen, yönetilen ve aynı zamanda host edilen Müşteri Hizmetleri ve Çağrı Merkezi yönetimi platformunda yer alan bilgilerin yetkisiz kişiler tarafından ele geçirilmesi sonucu gerçekleştiği,
- İhlal edilen kişisel verilerin; ad-soyad, telefon numarası, e-posta adresi, T.C. kimlik numarası uygulama parolaları ve sipariş/teslimat bilgileri olduğu,
- İhlalden etkilenen kişi grubunun kullanıcılar olduğu,
- Sistemde bulunan kişi sayısının 1.490.789 olduğu, kaç kişinin etkilendiğinin bilinmediği,
- İlgili kişilerin, veri ihlali ile ilgili bilgi almak için kvk@apazgroup.com adresinin iletişim adresi olarak kararlaştırıldığı, ilgili kişilere yapılan e-posta bildirimde ve internet sitesi duyurusunda bu adresin bildirildiği, bunun yanında Çağrı Merkezi numarasının da iletişim için kullanıldığı

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 12.03.2026 tarih ve 2026/523 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

VERİ İHLAL BİLDİRİM ÖRNEKLERİ

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Köfteci Yusuf Hazır Yemek Temizlik Canlı Hayvan Et Mamulleri Entegre Gıda İthalat İhracat San. Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri sorumlusu sıfatını haiz Köfteci Yusuf Hazır Yemek Temizlik Canlı Hayvan Et Mamulleri Entegre Gıda İthalat İhracat San. Tic. AŞ tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin 22.01.2026 tarihinde başladığı ve 23.01.2026 tarihinde tespit edildiği,
- İhlalin; veri sorumlusunun bordro yazılımı ve online yemek siparişlerinin yönetildiği bilgi sistemlerini barındıran yerel SQL veritabanının dışardan bir müdahale ile şifrelenerek erişimin engellenmesi neticesinde gerçekleştiği,
- İhlalden etkilenen ilgili kişi grubunun; çalışanlar ve müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin; müşteriler için kimlik (ad soyad), iletişim (adres, cep telefonu), müşteri işlem (yemek sipariş detayı) etkilenirken çalışanların kimlik, iletişim ve özlük verilerinin etkilendiği,
- İhlalden, veri sorumlusunun 13.000 çalışanı ve 150.000 müşterisi olmak üzere toplam 163.000 kişinin etkilendiği

Kişisel Veri İhlali Öncesi

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

1) **KVKK** Açısından **Veri İhlali Öncesinde** Yapılması Gerekenler

- **YEDEKLEME** — Sahiplik → **Bilgi Sistemleri Ekibi**
- Veri İhlali Yönetim Planı — Sahiplik → **BGYS Ekibi**
- Mahremiyet Etki Analizi — Sahiplik → **BGYS Ekibi**
- Sistem Açıklarının Belirlenip Uygun Çözümlerle Kapatılması — Sahiplik → **BT Ekibi**
- **Bilinmeyen** kaynaklardan gelen maillerdeki linke **tıklamamak** — Sahiplik → **Tüm Çalışanlar**

Kişisel Veri İhlali Olurken

TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

2) KVKK Açısından **Veri İhlali Esnasında** Yapılması Gerekenler

- **72 Saat** İçerisinde Kurula Bildirim Yapılması,
- Mevcut **Adli Bilişim** Raporlarının Kurula Yapılacak Olan Bildirime Eklenmesi,
- Hızlı Aksiyon Alınması,

Süreç yönetiminin tam anlamıyla kontrol altında ilerletildiğinin **kurul** tarafından da anlaşılabilmesi için **kritiktir**.

BİLGİ GÜVENLİĞİ ve KİŞİSEL VERİ GÜVENLİĞİ

SORULAR

2026 YILI BİLGİ GÜVENLİĞİ ve KVKK

FARKINDALIK EĞİTİMİ

TEŞEKKÜRLER.