SİBER GÜVENLİK VE AKILLI SÖZLEŞMELER

DOÇ. DR. MEHMET BEDİİ KAYA

DOÇ. DR. MEHMET BEDİİ KAYA

İstanbul Bilgi Üniversitesi Hukuk Fakültesi Bilişim ve Teknoloji Hukuku Ana Bilim Dalı Öğretim Üyesi

E-posta: mehmet@mbkaya.com

Web : www.mbkaya.com

Twitter : MBediiKaya

SUNUM PLANI

- Siber güvenlik hukuku
- Siber güvenliğin temel çerçevesi
- Siber güvenliğin hukuki boyutları
- Geleneksel siber güvenlik tehditleri
- Akıllı sözleşmelere yönelik özgün tehditler
- Akıllı sözleşmelere yönelik bir düzenleme arayışı
- Avrupa Birliği Siber Güvenlik Hukuku
- Türk Siber Güvenlik Hukuku

SORULAR

- Akıllı sözleşmeler siber tehditlere karşı risk altında mıdır?
- Akıllı sözleşmelere yönelik özgün tehditler var mıdır?
- Siber güvenlik düzenlemeleri akıllı sözleşmeleri kategorik olarak yasaklamakta mıdır?
- Sözleşme özgürlüğüne siber güvenlik gerekçesiyle müdahale meşru kılınabilir mi?

Akıllı Sözleşme

Koşulları, klasik hukuki ifadeler yerine bilgisayar dilinde yazılan sözleşmeler.

Akıllı Sözleşme

Bir güven otoritesine ihtiyaç duymadan, kişiler veya kurumlar arasında yapılan ve şartları dağıtık defter teknolojileri protokolleri ile garanti altına alınmış sözleşmeler.

Akıllı Sözleşme: Koşulları, klasik hukuki ifadeler yerine bilgisayar dilinde yazılan sözleşmeler. Akıllı Sözleşmeler, uygun bir dağıtık kayıt sistemi gibi bir bilişim sistemi tarafından otomatik olarak icra edilebilir.

UK Government Office for Science, Distributed Ledger Technology: Beyond Blockchain.

Akıllı Sözleşme: Bir güven otoritesine ihtiyaç duymadan, kişiler veya kurumlar arasında yapılan ve şartları dağıtık defter teknolojileri protokolleri ile garanti altına alınmış anlaşmalardır. Anlaşma şartları blokzincir doğrulama mekanizmaları vasıtası ile sağlandığında; yükümlülükler otomatik olarak yürürlüğe girer ve blokzincir ağında kayıt altına alınır.

TC Cumhurbaşkanlığı Dijital Dönüşüm Ofisi


Merkezi otoriteye ihtiyaç duymaz
Uçtan uca şeffaflık sağlar
Objektif koşullar içerir (önceden belirlenmiş fonksiyonlarla sınırlı)
Otomatik icra edilir
Kaderi blokzincirine/koda bağlıdır
Gizlilik açısından riskler içerir
Yoruma açık değildir
Telafi imkanı yoktur

Bireylerin güven içinde yaşamalarının sağlanmasında devlete yüklenen ödevler arasında şüphesiz siber güvenliğin sağlanması da yer almaktadır.

AYM, E. 2017/16

Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi

Türkiye Ulusal Siber Güvenlik Stratejisi

Siber güvenlik: ağ ve bilgi sistemlerini, bu sistemlerin kullanıcılarını ve siber tehditlerden etkilenen diğer kişileri korumak için gerekli faaliyetler

AB Siber Güvenlik Yasası

Siber tehdit: ağ ve bilgi sistemlerine, bu sistemlerin kullanıcılarına ve diğer kişilere zarar verebilecek, bunları kesintiye uğratabilecek veya başka bir şekilde olumsuz etkileyebilecek her türlü potansiyel durum, olay veya eylem

AB Siber Güvenlik Yasası

BLOKZİNCİR EKOSİSTEMİ

- Madenciler
- Borsalar
- Kripto varlık hizmet sağlayıcılar
- Cüzdan hizmet sağlayıcıları
- Altyapı yazılım geliştiricileri
- Altyapı hizmet sağlayıcılar
- Validatörler
- Merkeziyetsiz organizasyonlar
- Aracı kurumlar
- Son kullanıcılar

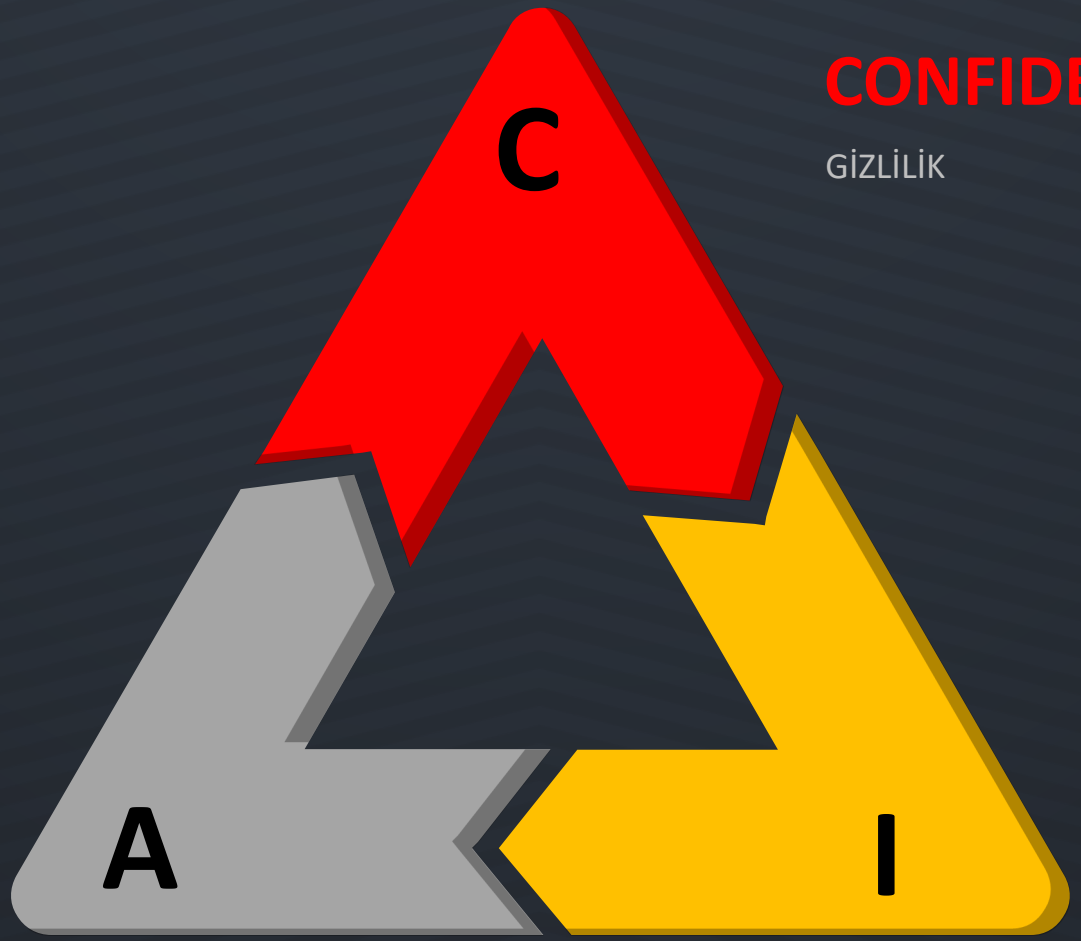
Kod, kanundur. Akıllı sözleşmeler, ilk kodlamanın fonksiyonelliği kadar güvenlidir.

CONFIDENTIALITY

GİZLİLİK

AVAILABILITY

ERİŞİLEBİLİRLİK



INTEGRITY

BÜTÜNLÜK

Disconnection is the only known mitigation measure currently available.

Cybersecurity and Infrastructure Security Agency's Emergency Directive 21-01, "Mitigate SolarWinds Orion Code Compromise"

AKILLI SÖZLEŞMELER İÇİN SİBER TEHDİT KAYNAKLARI

- Dış aktörler
  - Siber suçlular
  - Kiralık saldırganlar
  - Endüstriyel casuslar
  - İç tehditler
  - Teröristler
  - Devletler
- Sözleşmenin tarafları

GELENEKSEL TEHDİTLER

- Anahtar yönetimi
- Kriptografi
- Mahremiyet
- Kod gözden geçirme sorunları

DAĞITIK DEFTERLER ÖZGÜ TEHDİTLER

- Konsensüs saldırısı (consensus hijack)
- Yan zincir saldırıları (sidechain attack)
- İzinli blokzincirlerini istismar etmek (exploiting permissioned blockchains)
- Dağıtık hizmet dışı bırakma saldırıları (distributed denial of service)
- Cüzdan yönetimi (wallet management)
- Ölçeklenebilirlik (scalability)
- Beraber çalışabilirlik (interoperability)
- Yönetişim kontrolleri (governance controls)

Ref: ENISA (2016) Distributed Ledger Technology & Cybersecurity, Improving information security in the financial sector

AKILLI SÖZLEŞMELER İÇİN TAVSİYELER

- Yazılım olgunlaştırma standartlarının kullanılması ve kodların sürekli gözden geçirilmesi
- Hataların ayıklanması
- Sıfırıncı gün saldırılarına karşı güncelleme imkanlarının tanınması
- Güvenlik denetimlerinin gerçekleştirilmesi

AKILLI SÖZLEŞMELERE YÖNELİK GÜVENLİK TAVSİYELERİ

- Kullanılan düzenli fonksiyonların standardizasyonu
- Onaylanmış akıllı sözleşme kütüphanelerinin yaygınlaştırılması
- Özel bir konsensüs protokolüyle zararlı yazılım olarak nitelendirilen durumların geçersizliğinin sağlanması
- Akıllı sözleşmelerin siber tehditlere göre uyarlanmasının temini (Bilhassa yönetişim kuralları (governance control) için de akıllı sözleşmelerin uyarlanmasının temini)
- Mahremiyet odaklı tasarımın teşviği (privacy preserving smart contracts)

SİBER GÜVENLİK VE AKILLI SÖZLEŞMELER

AVRUPA BİRLİĞİ SİBER GÜVENLİK HUKUKU

AVRUPA BİRLİĞİ TEMEL SİBER GÜVENLİK DÜZENLEMELERİ

- NIS 1 Directive (Repealed)
- Cybersecurity Act
- NIS 2 Directive
- Cyber-Attacks Directive
- Critical Entities Directive
- Digital Operational Resilience Act (DORA)
- Cyber Resilience Act (Proposal)
- Cyber Solidarity Act (Proposal)

Güncel detaylı liste için bkz. **LEX Digitalis:** mbkaya.com/it-law-lex-digitalis/

TEMEL HİZMET OPERATÖRÜ (OPERATORS OF ESSENTIAL SERVICES)

- Enerji
  - Elektrik
  - Petrol
  - Doğalgaz
- Ulaştırma
  - Karayolu taşımacılığı
  - Demiryolu taşımacılığı
  - Havayolu taşımacılığı
  - Denizyolu taşımacılığı
- Bankacılık
- Finansal hizmetler altyapıları
- Sağlık sektörü
- Su yönetimi (İçme suyu temini ve dağıtımı)
- Dijital altyapılar
  - İnternet Değişim Noktası (IXP)
  - Alan Adı Hizmet Sağlayıcıları (DNS)
  - Üst Seviye Alan Adı Kayıtları (TLD)

DİJİTAL HİZMET SAĞLAYICI (DIGITAL SERVICES PROVIDER)

- Dijital hizmet sağlayıcılar, Direktif EK-III'te listelenen tipte ve dijital bir hizmet sunan kişilerdir.
- Dijital hizmet sağlayıcılar:
  - Çevrimiçi pazarlar
  - Bulut bilişim hizmetleri
  - Çevrimiçi arama motorları

TEMEL YÜKÜMLÜLÜKLER

- **Siber güvenliği sağlama yükümlülüğü**
  - Riski önlemek veya etkilerini asgari düzeye indirmek için, riske uygun ve operasyonel tedbirler almak
  - Şebeke ve bilgi sistemlerinin güvenliğini sağlamak
- **Siber güvenlik olaylarını bildirim yükümlülüğü**
  - Olaydan etkilenen kullanıcı sayısı
  - Olayın süresi
  - Olaydan etkilenen coğrafi alan

NIS 1 DİREKTİFİ - YAPTIRIMLAR

- NIS Direktifinden doğan yükümlülüklere ilişkin yaptırımlar tamamen Devletlerin tasarrufundadır.
- Devlet, kuralların uygulanması için elinden geleni yapacaktır.
- Öngörülen yaptırımlar **etkili**, **orantılı** ve **caydırıcı** olmalıdır.

Yeni paradigma: Siber Dayanıklılık

Ağa bağlı olan her şey güvenli olmak zorunda!

NIS 2

- Temel hizmet sağlayıcılar (Essential entities)
- Önemli hizmet sağlayıcılar (Important entities)

YÜKSEK KRİTİK SEKTÖRLER (SECTORS OF HIGH CRITICALITY)

1. Enerji: Elektrik, Isıtma ve Soğutma, Petrol, Doğalgaz, Hidrojen
2. Ulaştırma: Hava, Demiryolu, Su, Karayolu
3. Bankacılık
4. Finansal piyasa altyapıları
5. Sağlık
6. İçme suyu
7. Atık suyu
8. Dijital altyapı
9. Bilişim hizmetleri yönetimi (B2B)
10. Kamu hizmetleri
11. Uzay

DİĞER KRİTİK SEKTÖRLER (OTHER CRITICAL SECTORS)

1. Posta ve diğer taşıma hizmetleri
2. Atık yönetimi
3. Kimyasalların imalat, üretim ve dağıtımı
4. Gıdaların üretimi, işlemesi ve dağıtımı
5. İmalat
6. Dijital sağlayıcılar
7. Araştırma

YENİ KAPSAMA ALANLARI

- Elektronik haberleşme hizmet sağlayıcıları
- Sosyal ağ sağlayıcıları ve veri merkezi hizmetleri gibi dijital hizmetler
- Atık su ve atık yönetimi
- Uzay
- Bazı kritik ürünlerin imalatı (İlaç, medikal aletler ve kimyasallar)
- Posta ve taşıma hizmetleri
- Gıda
- Kamusal yönetim hizmetleri

NIS 2 DİREKTİFİ TEMEL YÜKÜMLÜLÜKLERİ

- Siber olay yönetimi ve kriz yönetimi
- Açık yönetimi ve ifşası
- Risk yönetim tedbirlerinin etkinliğinin değerlendirilmesi
- Basit bilişim hijyen uygulamaları ve sibergüvenlik eğitimi
- Kriptografinin etkin şekilde uygulanması
- İnsan kaynağı güvenliği
- Erişim kontrol politikaları
- Varlık yönetimi

NIS 2 DİREKTİFİ - YAPTIRIMLAR

- NIS 1'in aksine özel sınırlar belirlendi.
- €10 Milyon Euro'ya kadar idari para cezası or kürsel cironun %2'sine kadar idari para cezası (hangisi yüksekse).

SİBER GÜVENLİK VE AKILLI SÖZLEŞMELER

TÜRK SİBER GÜVENLİK HUKUKU

BTK

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

CUMHURBAŞKANLIĞI

T.C. CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ

ULAŞTIRMA VE ALTYAPI

SİBER GÜVENLİK KURUMSAL ÇERÇEVE

EMNİYET

KVKK

KİŞİSEL VERİLERİ KORUMA KURUMU

MİT

BDDK

SPK

TCMB

SİBER GÜVENLİK KURUMSAL ÇERÇEVE

SANAYİ VE TEKNOLOJİ BAKANLIĞI

EPDK

TSE

SİBER GÜVENLİK KURULU - KRİTİK ALTYAPI SEKTÖRLERİ

Kritik Altyapılar: İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar.

- Elektronik Haberleşme
- Enerji
- Finans
- Ulaştırma
- Su Yönetimi
- Kritik Kamu Hizmetleri

Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır.

Elektronik Haberleşme Kanunu - Madde 60(11)

Veri sorumlusu; (1) kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, (2) kişisel verilere hukuka aykırı olarak erişilmesini önlemek, (3) kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Kişisel Verilerin Korunması Kanunu, Madde 12

SİBER GÜVENLİK VE AKILLI SÖZLEŞMELER

DEĞERLENDİRMELER

DEĞERLENDİRMELER

- Kısıtlı uygulama alanları sebebiyle akıllı sözleşmeler siber güvenlik düzenlemelerinin öncelikli regülasyon radarında değildir.
- Geleneksel tehditlere yönelik kurallar ve bilişim ile veriye yönelik kısıtlayıcı kurallar - bir bilişim sistemi olmaları ve veri içermeleri sebebiyle- akıllı sözleşmeler için de geçerlidir.
- Türk hukukunda siber güvenliğe ilişkin kurumsal çerçeve dağınıktır. Siber güvenliğe ilişkin bağlayıcı kurallar kısıtlıdır. Akıllı sözleşmelere ilişkin özel bir kural yoktur.
- Genel ve sektörel siber güvenlik düzenlemelerine göre akıllı sözleşmelerin konu bakımından sınırlanması söz konusu olabilecektir. Risk temelli yaklaşım temel belirleyici faktördür.
- Akıllı sözleşmelerin yaygınlaşmasıyla ve akıllı sözleşmelere ilişkin özgün tehditlerin nitelik ve ölçek değiştirmesiyle birlikte özel siber güvenlik düzenlemelerin gündeme gelmesi kaçınılmazdır. Bu düzenlemelerde muhtemel sektörel veya konu bakımından kısıtlamalar gündeme gelebilecektir.

TEŞEKKÜRLER!