T.C. SANAYİ VE TEKNOLOJİ BAKANLIĞI

#YEREL KALKINMA HAMLESİ

İSTANBUL KALKINMA AJANSI

İSTANBUL'DA SİBER GÜVENLİK EKOSİSTEMİ

2025

MEVCUT DURUM VE BEKLENTİLER

T.C. SANAYİ VE TEKNOLOJİ BAKANLIĞI

#YEREL KALKINMA HAMLESİ

İSTANBUL KALKINMA AJANSI

İSTANBUL KALKINMA AJANSI

Asmalı Mescit Mah. İstiklal Cad. No: 142 Odakule Kat 6-7-8 34430 Beyoğlu / İstanbul
Tel: 0 (212) 468 34 00 Faks: 0 (212) 468 34 44
E-Posta: iletisim@istka.org.tr

2025, İstanbul

Proje Koordinatörleri

Abdurrahim AHAT
Ayşen YAZICIOĞLU
Hakan SİPAHİOĞLU
Mevlana C. KAPLAN

Hazırlayanlar

Prof. Dr. Kemal BIÇAKCI
Ece EFE
Anıl Nevzat SOLMAZ
Saliha İŞCEN
Umut Ulvi YAVUZLAR

İSTANBUL'DA SİBER GÜVENLİK EKOSİSTEMİ

Yayın Sahibi

İstanbul Kalkınma Ajansı

RAPORUN KAPSAMI

On İkinci Kalkınma Planı, 2030 Sanayi ve Teknoloji Stratejisi ve 2024-2028 İstanbul Bölge Planında imalat sanayinin dijital dönüşümünün; üretkenliğin ve rekabet gücünün artırılması için kritik öneme sahip olduğu vurgulanmıştır. Aynı şekilde ulusal ve bölgesel raporlarda dijital dönüşüm için en acil ihtiyaç olarak teknolojik atılıma işaret edilmiş, Türkiye'nin küresel rekabet gücünü artıracak ekonomik ve teknolojik bağımsızlığını temin edecek kritik teknolojilere atılım sağlayacak politikalar, "Milli Teknoloji Hamlesi" yaklaşımı ile belirlenmiştir. On İkinci Kalkınma Planında ve 2030 Sanayi ve Teknoloji Stratejisinde; yapay zekâ, nesnelerin interneti, artırılmış gerçeklik, büyük veri, siber güvenlik, blokzincir, bulut teknolojileri, enerji depolama, ileri malzeme, robotik, mikro/ nano/ optro-elektronik, nanoteknoloji, biyoteknoloji, kuantum, sensör teknolojileri ve eklemeli imalat, vd. başlıklardaki teknolojiler Milli Teknoloji Hamlesi için belirlenen hedeflere ulaşılması için odaklanılması gereken kritik teknolojiler olarak tespit edilmiştir. Kritik teknolojilerde ekosistem ve sosyal alanlarda bir dönüşümü hedef alan süreç dijitalleşme ve dijital dönüşüm alanında önemli bir araç olup, bu alanlarda nitelikli işgücü yetiştirilmesi, işletmelerin farkındalıklarının artırılması, teknoloji kullanımının yaygınlaştırılması, teknoloji geliştiricilerin ve ilgili girişimlerin desteklenmesi ve ilgili paydaşlar arasında etkin bir yönetişim ile söz konusu alanlarda ihtiyaç duyulan müdahalelerin yapılması gerekmektedir. Bunun için öncelikle, ilgili teknolojilerin dünyada ve İstanbul'daki mevcut durumunun tespiti ve potansiyellerin belirlenmesine ihtiyaç duyulmuştur. Bu kapsamda kritik teknolojiler alanında bölgesel mevcut durum raporları hazırlanmaya başlanmış; tanım, kullanım alanları, dünyada genelinde mevcut durum, İstanbul bölgesindeki yaygınlığı, bölgedeki talep, ilgili paydaşlar, gerçekleştirilen projeler, eğitim ve araştırma altyapıları tespit edilmiştir. Belirli periyotlar ile güncellenecek mevcut durum raporları ile rapor konusu teknoloji alanında İstanbul'un potansiyelini tespit etmek, politika yapıcılara veri sağlamak, ilgili tarafların farkındalıklarının artırılmasını sağlamak ve bu alanda çalışma yapacak kurum ve kuruluşlara yol göstermek hedeflenmiştir. Kritik teknolojilere ilişkin rapor serisi Siber Güvenlik Teknolojileri odaklı rapor ile devam etmekte olup diğer kritik teknoloji başlıklarındaki analiz ve raporlama çalışmaları devam etmektedir.

İÇİNDEKİLER

KISALTMALAR

KISALTMA	İNGİLİZCE AÇIKLAMA	TÜRKÇE AÇIKLAMA
AES	Advanced Encryption Standard	İleri Düzey Şifreleme Standardı
AI	Artificial Intelligence	Yapay Zekâ
API	Application Programming Interface	Uygulama Programlama Arayüzü
BT	Information Technology	Bilgi Teknolojileri
BIT-ITC	Information and Communication Technologies	Bilişim ve İletişim Teknolojileri
BTK	Information Technologies and Communication Authority	Bilgi Teknolojileri ve İletişim Kurumu
CISA	Certified Information Systems Auditor	Sertifikalı Bilgi Sistemleri Denetçisi
CISM	Certified Information Security Manager	Sertifikalı Bilgi Güvenliği Yöneticisi
CISO	Chief Information Security Officer	Bilgi Güvenliği Üst Yöneticisi
CIPP	Certified Information Privacy Professional	Sertifikalı Bilgi Gizliliği Uzmanı
CISSP	Certified Information Systems Security Professional	Sertifikalı Bilgi Sistemleri Güvenlik Uzmanı
CTF	Capture The Flag	Bayrağı Yakala (Siber Güvenlik Yarışması)
DDos	Distributed Denial of Service	Dağıtılmış Hizmet Engelleme Saldırısı
DoS	Denial of Service	Hizmet Engelleme Saldırısı
ECC	Elliptic Curve Cryptography	Eliptik Eğri Kriptografisi
E2EE	End-to-End Encryption	Uçtan Uca Şifreleme
FIDO2	Fast Identity Online 2	Hızlı Çevrimiçi Kimlik Doğrulama 2
GDPR	General Data Protection Regulation	Genel Veri Koruma Tüzüğü
GenAI	Generative Artificial Intelligence	Üretken Yapay Zekâ
GIAC	Global Information Assurance Certification	Küresel Bilgi Güvenliği Sertifikası
GRC	Governance, Risk, and Compliance	Yönetişim, Risk ve Uyum
GSYİH	Gross National Product (GNP)	Gayri Safi Milli Hasıla
HSM	Hardware Security Module	Donanım Güvenlik Modülü
IAM	Identity and Access Management	Kimlik ve Erişim Yönetimi
ICS	Industrial Control Systems	Endüstriyel Kontrol Sistemleri
IDS	Intrusion Detection System	Saldırı Tespit Sistemi
Iot	Internet of Things	Nesnelerin İnterneti
IPS	Intrusion Prevention System	Saldırı Önleme Sistemi
ISO 27001	International Organization for Standardization 27001	Uluslararası Standardizasyon Örgütü 27001 (Bilgi Güvenliği Yönetim Sistemi Standardı)
KVKK	Law on Protection of Personal Data	Kişisel Verilerin Korunması Kanunu
LLM	Large Language Model	Büyük Dil Modeli
MitM	Man-in-the-Middle	Ortadaki Adam (Saldırısı)
MYO	Vocational School	Meslek Yüksekokulu
OT	Operational Technology	Operasyonel Teknoloji
PAM	Privileged Access Management	Ayrıcalıklı Erişim Yönetimi
RBAC	Role-Based Access Control	Rol Tabanlı Erişim Kontrolü
RSA	Rivest, Shamir, Adleman	Rivest, Shamir, Adleman (Asimetrik Şifreleme Algoritması)
SBCP	Security Behavior and Culture Programs	Güvenlik Davranışı ve Kültürü Programları
SCADA	Supervisory Control and Data Acquisition	Denetleyici Kontrol ve Veri Toplama Sistemi
SIEM	Security Information and Event Management	Güvenlik Bilgi ve Olay Yönetimi
SOAR	Security Orchestration, Automation and Response	Güvenlik Orkestrasyonu, Otomasyon ve Yanıt
SSB	Savunma Sanayii Başkanlığı	Presidency of Defence Industries
SSL	Secure Sockets Layer	Güvenli Soket Katmanı
TOBB	The Union of Chambers and Commodity Exchanges of Turkey	Türkiye Odalar ve Borsalar Birliği
TÜBİTAK	The Scientific and Technological Research Council of Turkey	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
VPN	Virtual Private Network	Sanal Özel Ağ

SİBER GÜVENLİK TEKNOLOJİLERİ

Siber Güvenlik Nedir?

Dijital sistemleri, ağları, verileri ve altyapıları tehditlerden, yetkisiz erişimlerden ve güvenlik açıklarından korumak için kullanılan stratejilerin, teknolojilerin ve uygulamaların bütünüdür.

Siber Güvenlik Neden Önemlidir?

Siber güvenlik, veri ihlallerini ve siber saldırıları önleyerek ekonomik ve hukuki riskleri azaltan, kurumlar için stratejik öneme sahip bir koruma alanıdır.

Koruma Yöntemleri

- Saldırı Tespiti & Önleme
- Olay Müdahalesi
- Risk Yönetimi
- Güvenlik Farkındalığı

Siber Güvenlikten Kimler Sorumludur?

- Bireyler: İlk savunma hattını oluşturur.
- Kurumlar: Sistemlerini ve verilerini güvence altına almalıdır.
- Devletler: Ulusal düzeyde düzenleme ve koruma sağlamalıdır.

Siber Güvenlik ve Bilgi Güvenliği Arasındaki Fark

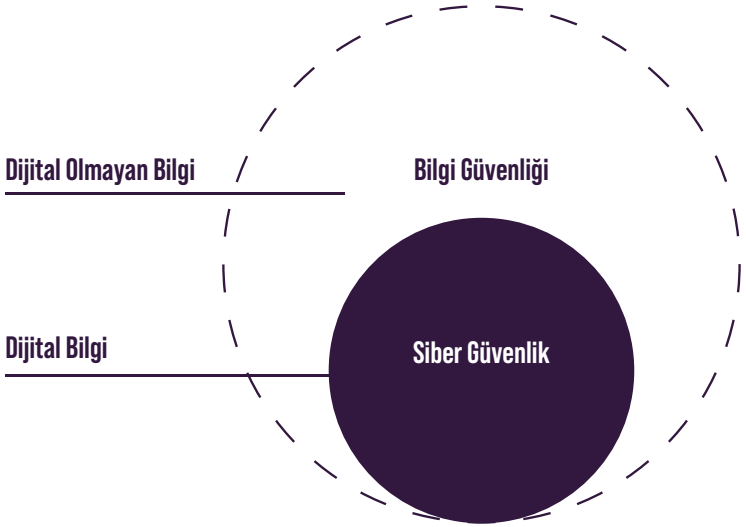
Siber güvenlik ve bilgi güvenliği birbirine yakın ancak farklı kavramlardır.

Bilgi Güvenliği

- Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korur.
- Fiziksel belgeler, elektronik veriler ve sözlü bilgiler gibi her türlü bilgi varlığını kapsar.

Siber Güvenlik

- Dijital sistemler, ağlar ve siber tehditlere karşı korumaya odaklanır.
- Bilgi güvenliğinin bir alt alanıdır.



Ana Hedefler

Gizlilik (Confidentiality)
Bilgiye yetkisiz erişimi önler.

Bütünlük (Integrity)
Bilgilerin değiştirilmesini engeller.

Erişilebilirlik (Availability)
Yetkili kullanıcılar için her zaman bilginin ulaşılabilir olmasını sağlar.

Siber Olayların Yıllık Maliyeti

Cybersecurity Ventures verilerine göre, küresel ölçekte siber saldırı kaynaklı ortaya çıkan zarar 2024 yılı için **9,5 trilyon dolar** olarak öngörülmüştür.

Bu tahmin, siber olayların maliyetinin küresel GSYİH'nin yaklaşık **%8,6**'sına denk geldiğini göstermektedir.

Siber Güvenlikte En Çok Karşılaşılan Tehditler ve Saldırı Teknikleri

1 Kötü Amaçlı Yazılımlar (Malware)

Kötü amaçlı yazılımlar; bilgisayar sistemlerine, ağlara veya kullanıcı cihazlarına zarar vermek, veri çalmak veya kontrol altına almak amacıyla geliştirilen yazılımlardır. Farklı türleri olup yayılma yöntemleri ve etkileri değişiklik gösterebilir.

Fidye Yazılımı
Sana şantaj yapar

Solucanlar
Ağ üzerinden yayılır

Casus Yazılım
Bilgilerini izler ve çalar

Truva Atları
Başka bir yazılım gibi görünür

Reklam Yazılımı
İstenmeyen reklam gösterir

BOT AĞI
Bilgisayarını uzaktan kontrol eder

2 Kimlik Avı (Phishing), Sosyal Mühendislik Saldırıları ve Deepfake Tehditleri

Kimlik avı saldırıları, kullanıcılardan hassas bilgileri (parolalar, kredi kartı bilgileri, vb.) çalmak için sahte e-postalar, SMS'ler veya web siteleri kullanarak güvenilir kurum veya kişi kılığına girer. Sosyal mühendislik saldırıları ise insan psikolojisini manipüle ederek kullanıcıları gizli bilgileri paylaşmaya zorlayan saldırılardır.

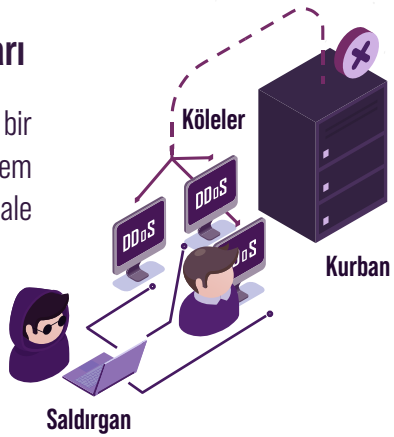
Deepfake teknolojisi, yapay zekâ ile sahte görüntüler ve sesler üreterek dolandırıcılık saldırılarına yeni bir boyut katmıştır. Saldırganlar, yöneticiler veya tanınmış kişiler gibi davranarak finansal dolandırıcılık ve sahte kimlik doğrulama saldırıları gerçekleştirmektedir. Özellikle finansal dolandırıcılık ve sahte kimlik doğrulama saldırılarında deepfake kullanımı artmaktadır.

Siber Güvenlikte En Çok Karşılaşılan Tehditler ve Saldırı Teknikleri

3 Hizmet Engelleme (DoS) Saldırıları

Hizmet engelleme saldırıları (DoS), bir sistemi aşırı trafikle doldurarak veya sistem kaynaklarını tüketerek erişilemez hale getirmeyi amaçlar.

Dağıtılmış Hizmet Engelleme (DDoS) saldırıları ise birden fazla kaynaktan gelen eş zamanlı trafik sebebiyle önlenmesi daha zor olan DoS saldırı türüdür.



4 Ortadaki Adam (MitM) Saldırıları

Ortadaki adam saldırıları, iki taraf arasındaki iletişime gizlice sızarak veri hırsızlığı veya manipülasyon gerçekleştirmeyi amaçlar. Örneğin; bir saldırgan, bir Wi-Fi ağına sızarak bankacılık bilgileri veya oturum açma kimlik bilgilerini ele geçirebilir.

5 İç Tehditler

İç tehditler; bir organizasyon içindeki çalışanlar, yükleniciler veya iş ortakları tarafından gerçekleştirilen güvenlik ihlalleridir.

2024 yılında organizasyonların %83'ü iç tehditlerden kaynaklanan en az bir saldırı yaşadıklarını raporlamıştır. [1]

6 Kimlik Hırsızlığı

Kimlik hırsızlığı, bir kişinin kimlik bilgilerini çalarak sahte hesaplar açması veya finansal dolandırıcılık yapmasıdır. Çalıntı kimlik bilgileri genellikle dark web'de satılabilir.

1. Kaynak: https://securityintelligence.com/articles/83-percent-organizations-reported-insider-threats-2024/

1 Güçlü ve Güvenli Parolalar Oluşturma

Güçlü parolalar, saldırganların tahmin etmesini zorlaştırarak, hesapların ele geçirilmesini engeller ve kişisel bilgilerinizi koruyarak siber saldırılara karşı ilk savunma hattını oluşturur.

UYARI

Güçlü parolalar önemli bir güvenlik önlemi olsa da, tek başına yeterli değildir. Kullanıcıların birçok farklı siteye giriş yapma gerekliliği göz önüne alındığında, her bir site için benzersiz ve güçlü parolaların belirlenmesi ve hatırlanması, pratikte zorlu bir yük haline gelmektedir.

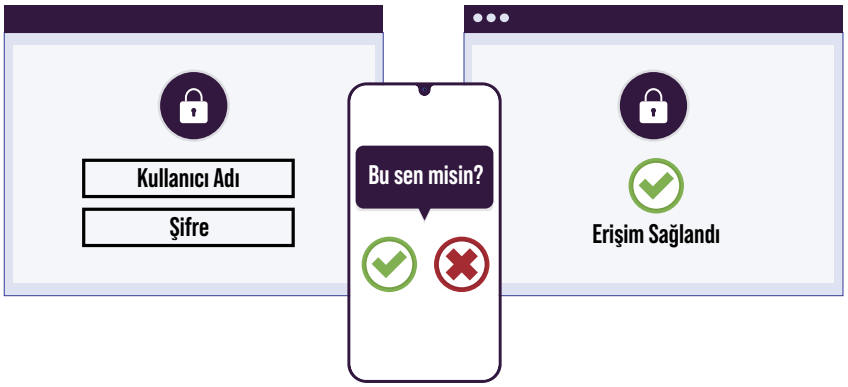
Bir Hacker'ın Parolalarınızı Kaba Kuvvetle Kırması Ne Kadar Sürer?

Karakter Sayısı	Yalnızca Sayılar	Küçük Harfler	Büyük ve Küçük Harfler	Sayılar, Büyük ve Küçük Harfler	Sayılar, Büyük ve Küçük Harfler, Semboller
4	Anında	Anında	Anında	Anında	Anında
5	Anında	Anında	Anında	Anında	Anında
6	Anında	Anında	Anında	Anında	Anında
7	Anında	Anında	1 saniye	2 saniye	4 saniye
8	Anında	Anında	28 saniye	2 dakika	5 dakika
9	Anında	3 saniye	24 dakika	2 saat	6 saat
10	Anında	1 dakika	21 saat	5 gün	2 hafta
11	Anında	32 dakika	1 ay	10 ay	3 yıl
12	1 saniye	14 saat	6 yıl	53 yıl	226 yıl
13	5 saniye	2 hafta	332 yıl	3 bin yıl	15 bin yıl
14	52 saniye	1 yıl	17 bin yıl	202 bin yıl	1 milyon yıl
15	9 dakika	27 yıl	898 bin yıl	12 milyon yıl	77 milyon yıl
16	1 saat	713 yıl	46 milyon yıl	779 milyon yıl	5 milyar yıl
17	14 saat	18 bin yıl	2 milyar yıl	48 milyar yıl	380 milyar yıl
18	6 gün	481 bin yıl	126 milyar yıl	2 trilyon yıl	26 trilyon yıl

2. Kaynak: Hive Systems Password Table - 2023

2 Çok Faktörlü Kimlik Doğrulama Kullanımı

Çok faktörlü kimlik doğrulama, güvenliği artırmak için çok önemlidir, ancak SMS veya e-posta gibi geleneksel yöntemler yerine daha güçlü FIDO2 tabanlı biyometrik doğrulama veya donanım anahtarları tercih edilmelidir. FIDO2, parolasız kimlik doğrulama sunarak güvenliği artırır ve kullanıcı deneyimini iyileştirir.



Çok Faktörlü Kimlik Doğrulama Türleri

- Tek Kullanımlık Parola
- Kimlik Doğrulama Uygulaması
- E-posta ve SMS
- Biyometri
- Donanım Anahtarları

3 Zararlı Yazılımlardan Korunma Önlemleri

Antivirüs yazılımları kullanmanın yanı sıra güvenilmeyen bağlantılardan ve e-posta eklerinden kaçınılmalı, cihaz ve yazılımların güvenlik güncellemeleri zamanında yapılmalı ve önemli veriler düzenli olarak yedeklenmelidir. Bu önlemler, güvenlik açıklarını kapatarak ve veri kaybı durumunda hızlı kurtarma sağlayarak riskleri azaltır.

Kötü Amaçlı Yazılımları Nasıl Önleyebilirsiniz?

- Antivirüs yazılımı kullanın
- Şüpheli bağlantılardan kaçının
- E-posta ayarlarını yapılandırın
- Yazılımlarınızı güncel tutun
- Yazılımları güvenilir mağazalardan indirin

Fidye Yazılımları

Fidye yazılım bulaşır.

Fidye yazılım, dosyaları şifreler (kilitler).

Kilidi açmak için fidye talep edilir.

Fidye yazılım için bir parantez...

10 Eylül 2020'de Almanya'daki Düsseldorf Üniversite Hastanesi fidye yazılım saldırısına uğradı, sistemleri çöktü ve acil tedavi gerektiren bir hasta 60 km uzaklıktaki başka bir hastaneye sevk edildi. Tedavi gecikmesi sonucu hasta hayatını kaybetti.

Bu olay siber saldırıya bağlı İLK ÖLÜM olarak kaydedildi.

4 Sosyal Medya ve Kişisel Veri Gizliliği

Kişisel veriler, ticari ve stratejik açıdan büyük bir değere sahiptir ve çeşitli amaçlarla toplanıp işlenir. Sosyal medya, çevrim içi hizmetler ve akıllı cihazlar, yalnızca doğrudan paylaşılan bilgileri değil aynı zamanda alışkanlıkları ve düşünce yapılarını da çözümleyebilir. Bu nedenle, veri güvenliği ve mahremiyet konusunda daha bilinçli olmak önemlidir. Kişisel verilerin nasıl toplandığını ve işlendiğini anlamak, dijital dünyada güvenli bir şekilde var olabilmenin temel şartıdır.

Kişisel VERİLERİN nasıl toplandığını hiç merak ettiniz mi?

DAVRANIŞSAL VERİLER
- Fitness ve aktivite verileri
- Bankacılık işlemleri
- Akıllı telefon uygulama kullanımı

ZİHİNSEL EĞİLİMLER /NİYET VERİLERİ
- Kişilik özellikleri
- İlgi alanları ve tercihler

AÇIKÇA PAYLAŞILAN VERİLER
- Anket yanıtları
- Sosyal medya paylaşımları

DUYGUSAL DURUM VERİLERİ
- Duygular ve istekler
- Değerler ve inançlar

5 Açık Wi-Fi Ağları ve VPN Kullanımı

Açık Wi-Fi ağları, şifrelenmemiş veri iletimi nedeniyle siber saldırılara karşı savunmasız olabilir.
Bu ağları kullanırken hassas bilgileri girmemek ve mümkünse veri trafiğini şifreleyen güvenli bir VPN kullanmak önemlidir.

VPN, internet bağlantısını güvence altına alarak üçüncü şahısların verilerinizi izlemesini engeller, özellikle halka açık ağlarda güvenliği artırır.

1 Siber Güvenlik Politikaları ve Farkındalık Eğitimleri

Güvenlik politikaları; veri güvenliği, erişim kontrolü, şifreleme, cihaz kullanımı ve veri paylaşımı gibi alanlardaki kuralları belirler. Bu politikaların yalnızca kâğıt üzerinde kalmaması, uygulanabilir ve denetlenebilir olması önemlidir. Çalışanların bu kuralları benimseyebilmesi için politikaların açık, anlaşılır ve günlük işleyişle uyumlu şekilde hazırlanması gerekir.

Siber güvenlik politikaları nasıl oluşturulur?

- **ADIM 1** — Hedefleri ve kapsamı tanımlayın
- **ADIM 2** — Risk değerlendirmesi yapın
- **ADIM 3** — Güvenlik yönergeleri oluşturun
- **ADIM 4** — Çalışan eğitimleri düzenleyin
- **ADIM 5** — Politikaları gözden geçirin ve güncelleyin

Farkındalık Eğitimleri: Çalışanların bilhassa sosyal mühendislik saldırılarına karşı eğitilmesi gerekir.
Siber saldırıların %98'i sosyal mühendisliğe dayanmaktadır.[2]

Güvenlik bir zincirdir ve bu zinciren zayıf halkası kadar güvenlidir. En zayıf halka da genelde insanın KENDİSİDİR.

Yetkilendirme ve Erişim Yönetimi: Her çalışanın sadece iş gereksinimleri doğrultusunda yetkilendirilmesi, gereksiz erişimlerin sınırlandırılması gerekir. En az ayrıcalık ilkesi uygulanmalıdır.

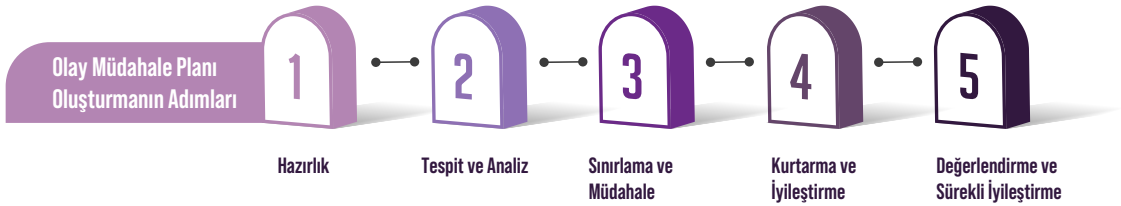
2 Risk Yönetimi ve Sürekli Güvenlik Değerlendirmeleri

Risk Analizi:
Organizasyon, varlıklarını, bu varlıklara yönelik tehditleri ve zayıf noktalarını belirleyerek bir risk haritası oluşturmalıdır.

Sürekli Güvenlik Denetimleri:
Periyodik penetrasyon testleri (sızma testleri) ve güvenlik değerlendirmeleri yapılmalıdır.

Siber Dayanıklılık Planları:
Riskleri minimize etmek için yedekleme, iş sürekliliği ve felaket kurtarma stratejileri geliştirilmelidir.

Siber Olay Müdahale Planı:
Bir saldırı gerçekleştiğinde hangi adımların izleneceğini belirleyen detaylı bir plan hazırlanmalıdır.



3 Ağ Güvenliği ve Veri Koruma Önlemleri

Güvenlik Duvarları ve IDS/IPS Kullanımı:
Şirket ağına gelen ve giden trafiğin kontrol edilmesi ve anormal hareketlerin tespit edilmesi gerekir.

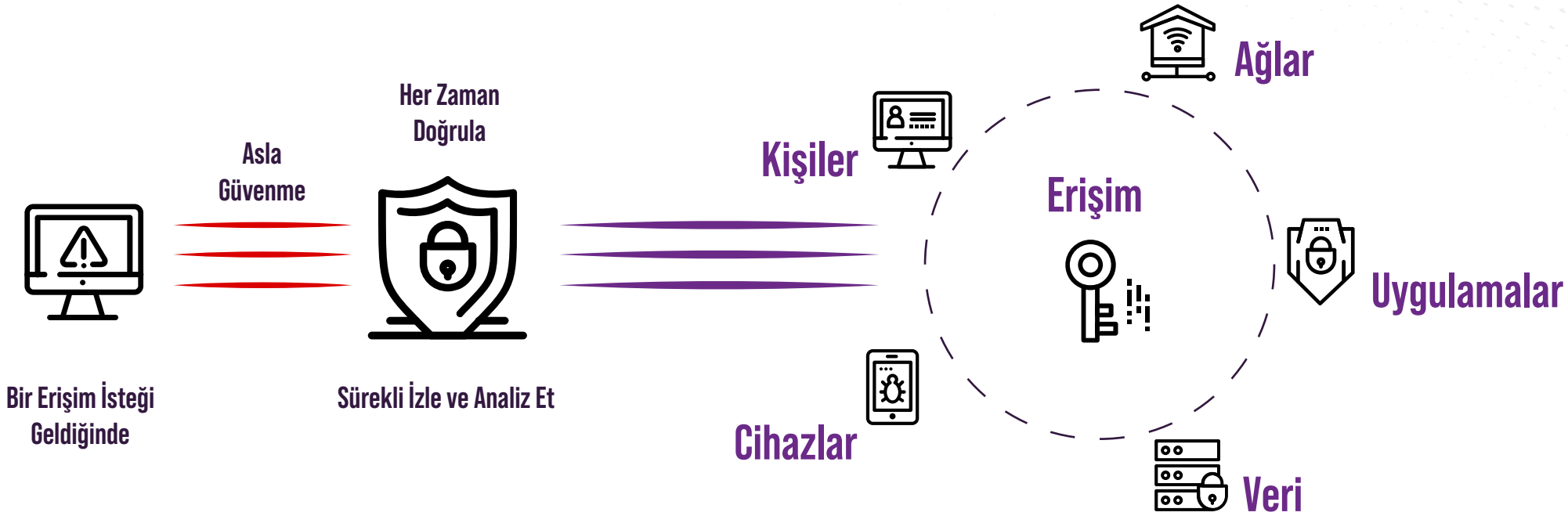
Veri Şifreleme:
Hassas veriler hem taşınırken hem de saklanırken güçlü şifreleme algoritmaları ile korunmalıdır.

Erişim Kontrolleri ve Yetkilendirme:
Kullanıcılar, sistemler ve uygulamaların gereksiz erişim yetkilerini sınırlandırmak için rol tabanlı erişim kontrolü (RBAC) gibi yöntemler uygulamalıdır.

3. Kaynak: https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html

Sıfır Güven Modeli Nedir?

Geleneksel güvenlik modellerinde, ağ içindeki sistemlere genellikle güvenilir gözüyle bakılırken, Sıfır Güven Modeli her erişimi şüpheli kabul eder ve sürekli doğrulama gerektirir. Artan siber tehditler ve uzaktan çalışmanın yaygınlaşması ile bu yaklaşım giderek daha fazla benimsenmektedir.



4 Üçüncü Taraf Risk Yönetimi ve Uyumluluk

Tedarikçi Güvenliği: Şirketin çalıştığı üçüncü taraf hizmet sağlayıcılarının siber güvenlik standartlarını karşılayıp karşılamadığı kontrol edilmelidir.

Mevzuata Uygunluk: Şirketler, KVKK, GDPR, ISO 27001 gibi standartlara uygun hareket etmelidir. Bu uyumluluk, hem yasal yükümlülüklerin yerine getirilmesi hem de veri güvenliğinin sağlanması açısından büyük önem taşır.

Risk Yönetimi: Maliyet ve Fayda Dengesi

Siber güvenlik yatırımları sınırsız bir bütçe gerektirmez, stratejik bir yaklaşım gerektirir.

Siber Güvenlik Yatırımları = Stratejik Seçimler

Her riskin azaltılması bir maliyet gerektirir.

Maliyet ve Fayda Dengesini Kurmak

Bazı riskler için alınan önlemler ekonomik olarak mantıklı olmayabilir.

Risk Yönetimi = Verimli Yatırım

Risklerin doğru yönetilmesi, ekonomik açıdan verimli çözümler üretir.

Siber Güvenlik Zorlukları

Yeni Tehditler

Siber saldırganlar sürekli yeni teknikler geliştiriyor.

İnsan Faktörü

Çalışan hataları ve kimlik avı gibi insan kaynaklı açıklar her zaman mevcut.

Sınırlı Kaynaklar

Güvenliği güçlendirmek ciddi maliyetler doğurabilir, ancak kaynaklar sınırlıdır.

%100 Güvenlik Yoktur

Güvenlik her zaman bir risk yönetimi sürecidir.

Tehditleri Tamamen Kaldıramazsınız

Siber güvenlik, her zaman yeni tehditlerle karşı karşıyadır.

Risk Azaltma Stratejisi

Maliyet-fayda analizine dayalı çözümler geliştirilir.

Siber Güvenlik = Yönetim Süreci

Siber güvenlik, proaktif ve sürekli bir çaba gerektirir.

Risk Yönetiminde Temel Sorular

**Bir riskin gerçekleşme olasılığı nedir?
(Çok Düşük, Düşük, Orta, Yüksek, Çok Yüksek)**

**Gerçekleştiğinde şirkete maliyeti ne seviyede olacak?
(Finansal zarar, müşteri kaybı, yasal ceza vb.)**

C (maliyet veya etki)	P (olasılık)				
	ÇOK DÜŞÜK	DÜŞÜK	ORTA	YÜKSEK	ÇOK YÜKSEK
ÇOK DÜŞÜK (ihmal edilebilir)	1	1	1	1	1
DÜŞÜK (sınırlı)	1	2	2	2	2
ORTA (ciddi)	1	2	3	3	3
YÜKSEK (şiddetli veya felaket)	2	2	3	4	4
ÇOK YÜKSEK (çoklu felaket)	2	3	4	5	5

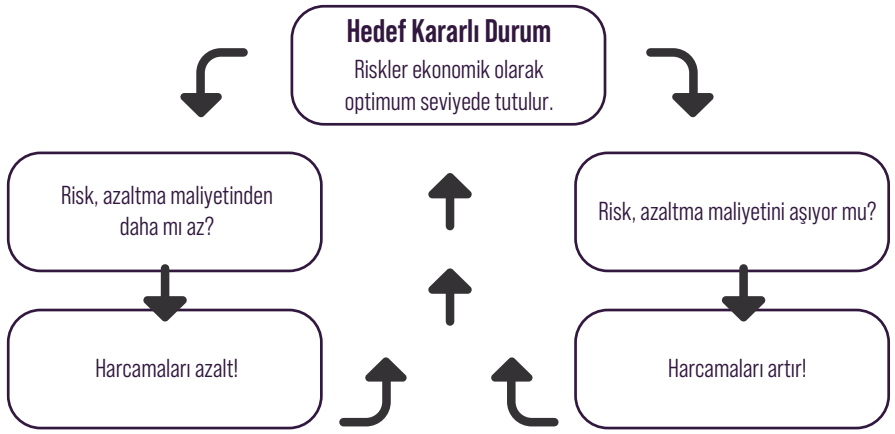
Bu risk derecelendirme matrisi, bir saldırının gerçekleşme olasılığı ile bu saldırının yaratacağı olası etkinin birleşimini değerlendirerek risk seviyesini belirler. Risk, 1'den 5'e kadar kodlanmış olup düşük olasılık ve düşük etkiye sahip olaylar en düşük risk seviyesine atanırken, yüksek olasılık ve yüksek etkiye sahip olaylar en yüksek risk seviyesine atanmıştır.

Bu riski yönetmek için ne kadar yatırım yapmalıyım?

Bu soruların yanıtlarını bulmak için Maliyet-Fayda Analizi uygulanır.

RİSK FAKTÖRÜ	Gerçekleşme Olasılığı (1-5)	Olası Etki (1-5)	Risk Seviyesi (Çarpım)	Maliyet Türleri	Önleme Yatırımı (CBA Sonucu)
Örnek Risk 1	Orta (3)	Yüksek (4)	12	Finansal zarar, itibar kaybı	Orta düzey yatırım
Örnek Risk 2	Yüksek (4)	Çok Yüksek (5)	20	Yasal ceza, müşteri kaybı	Yüksek düzey yatırım
Örnek Risk 3	Düşük (2)	Orta (3)	6	Operasyonel gecikme, ek güvenlik maliyeti	Düşük düzey yatırım

Örnek: Bir şirkete yönelik potansiyel bir fidye yazılımı saldırısının yıllık maliyetinin 10 milyon lira olduğu tahmin ediliyorsa, bu saldırıyı önleyecek güvenlik önlemleri için 500.000 liralık bir yatırım makul ve gerekli olabilir. Ancak 50 milyon liralık bir yatırım yapmak, maliyet-fayda açısından mantıklı değildir.

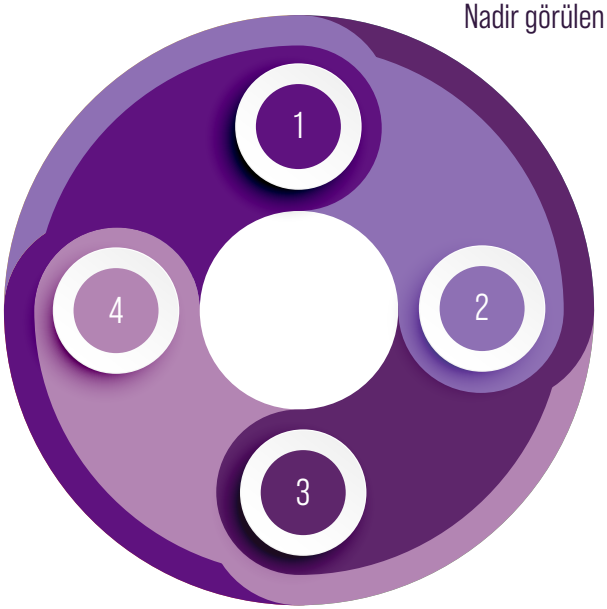


Siber Güvenlikte Risk Yönetiminin 4 Adımı

1

Risklerin Tanımlanması:
Hangi sistemler, uygulamalar ve veriler korunmalı?
Bu varlıkları tehdit eden siber riskler nelerdir?

Örneğin:
Bir bankanın müşteri bilgileri, en kritik varlıklarından biridir ve veri sızıntısı büyük bir risk oluşturur.



2

Risk Değerlendirmesi ve Önceliklendirme:
Her risk, olasılığı ve etkisine göre değerlendirilir.

Örneğin:
Kimlik avı saldırıları ➔Yüksek olasılık + Yüksek etki (Öncelikli önlem alınmalı).
Nadir görülen DDoS saldırıları➔ Düşük olasılık + Orta etki (İkinci öncelik)

3

Risklerin Azaltılması:
Maliyet ve fayda dengesini kurarak gerekli önlemler alınır.

Örneğin:
Bir e-ticaret sitesi, müşterilerinin kredi kartı bilgilerinin çalınması durumunda büyük finansal kayıplara uğrayabilir. Bu yüzden, çok faktörlü kimlik doğrulama gibi önlemler öncelikli olarak uygulanmalıdır.
Her risk için en uygun ve en ekonomik güvenlik önlemleri belirlenir.
Örneğin: Siber Sigorta ile riskin bir kısmı finansal olarak yönetilebilir.

4

Risklerin Sürekli İzlenmesi ve Güncellenmesi:
Siber tehditler sürekli değişebildiği için risk yönetimi statik bir süreç olmamalıdır.

Örneğin:
Düzenli sızma testleri ile güvenlik açıkları belirlenmeli, log ve olay izleme sistemleri ile saldırı girişimleri sürekli izlenmelidir. Risk değerlendirmeleri yılda en az bir kez güncellenmelidir.

Kriptografi Nedir?

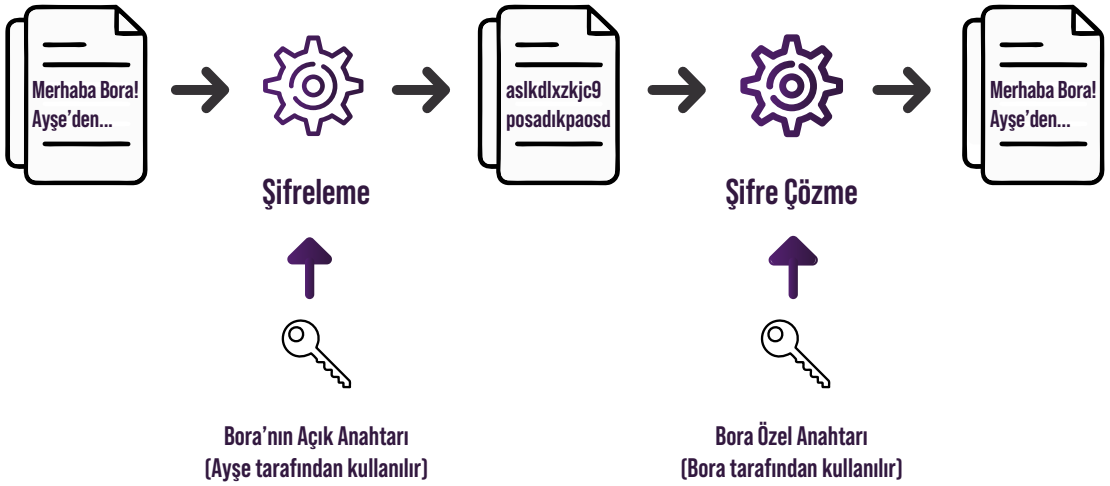
Kriptografi, başlangıçta bilgileri yetkisiz kişilerden gizleme sanatı olarak ortaya çıkmıştır. Ancak günümüzde sadece bilgi gizleme ile sınırlı kalmayıp kimlik doğrulama, veri bütünlüğü, dijital imzalar ve güvenli iletişim gibi birçok alanda kullanılmaktadır. Örneğin; internet bankacılığı, güvenli web siteleri ve dijital sözleşmeler kriptografi sayesinde güvenli hale gelir.

Kriptografik Anahtar Nedir?

Kriptografik anahtar, bilgileri şifrelemek (gizlemek) ve tekrar açmak (çözmek) için kullanılan özel bir kod gibidir. Verileri yalnızca doğru anahtara sahip olan kişi okuyabilir.

Şifreleme Türleri

- **Simetrik Şifreleme** : Aynı anahtar hem şifreleme hem de şifre çözme için kullanılır. Hızlıdır, ancak anahtar paylaşımı risklidir. (Örnek: AES)
- **Asimetrik Şifreleme** : Bir açık anahtar şifreleme, bir özel anahtar şifre çözme için kullanılır. Daha güvenlidir, ancak daha yavaştır. (Örnek: RSA, ECC)



Kuantum Bilgisayarlar ve Kriptografi Tehditleri

Kuantum bilgisayarlar, RSA ve ECC gibi asimetrik şifreleme sistemlerini Shor Algoritması ile hızla kırabilir.

Bu nedenle, kuantum dirençli (post-kuantum) kriptografi yöntemleri geliştirilmektedir.

NOT

TOBB Ekonomi ve Teknoloji Üniversitesi, Türkiye'nin ilk kuantum bilgisayarı olan QuanT'ı 21 Kasım 2024 tarihinde tanıtmıştır.

SİBER SALDIRILARIN KRONOLOJİSİ: TARİHTEKİ EN ÖNEMLİ SİBER GÜVENLİK İHLALLERİ

1983
İlk kez "bilgisayar virüsü" terimi, Fred Cohen tarafından tanımlandı.

1986
Tarihin ilk bilgisayar virüslerinden biri olan Brain virüsü, Pakistan'da yazıldı.

1988
Morris Solucanı, interneti etkileyen ilk büyük zararlı yazılım olarak kaydedildi ve 6.000'den fazla bilgisayara zarar verdi.

1994
İlk büyük şifrelemeye yönelik saldırılardan biri olan Netscape SSL saldırısı gerçekleşti.

1995
Kevin Mitnick, FBI tarafından yakalandı ve siber suçlardan hüküm giyen en ünlü hackerlardan biri oldu.

1999
Melissa Virüsü, e-posta yoluyla yayılan ilk büyük zararlı yazılımlarda biri olarak binlerce kurumu etkiledi.

2000
Mafiaboy lakaplı genç hacker, Amazon, eBay ve CNN gibi büyük sitelere DDoS saldırıları düzenledi.

2001
Code Red Solucanı, Microsoft'un IIS web sunucularını hedef aldı.

2003
Slammer Solucanı, interneti yavaşlatarak dünya çapında büyük zarara yol açtı.

2004
MyDoom virüsü, en hızlı yayılan e-posta solucanlarından biri oldu.

2007
Estonya Siber Saldırıları, bir ülkeye yönelik en büyük koordineli saldırılardan biri olarak tarihe geçti.

2008
Conficker Solucanı, milyonlarca bilgisayara bulaştı.

2010
Stuxnet Solucanı, İran'ın nükleer tesislerine saldırarak endüstriyel sistemlere yönelik ilk büyük siber saldırı olarak kayıtlara geçti.

2013
Target Veri İhlali, 40 milyon müşterinin kredi kartı bilgilerinin çalınmasına yol açtı.

2014
Sony Pictures Hack, Kuzey Kore bağlantılı olduğu iddia edilen bir saldırıyla büyük ölçüde veri sızıntısına neden oldu.

2016
Yahoo Veri İhlali, 3 milyar hesabın etkilenmesiyle tarihin en büyük veri ihlallerinden biri oldu.

2017
NotPetya, Ukrayna merkezli olarak başlayan ve küresel ekonomik zarara neden olan bir saldırıydı.

WannaCry Fidye Yazılımı, dünya çapında yüz binlerce bilgisayarı etkiledi.

2018
Facebook-Cambridge Analytica Skandalı, kullanıcı verilerinin kötüye kullanılması konusunda büyük bir kriz çıkardı.

2019
Capital One Veri İhlali, 100 milyondan fazla ABD müşterisini etkiledi.

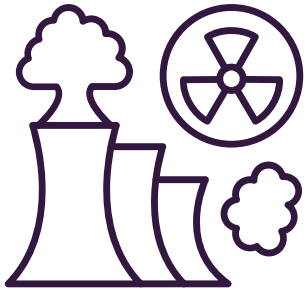
2020
SolarWinds Saldırısı, ABD hükümetine ve büyük şirketlere yönelik sofistike bir tedarik zinciri saldırısı olarak dikkat çekti.

2021
Colonial Pipeline Fidye Yazılımı Saldırısı, ABD'nin doğu kıyısında büyük yakıt kıtlığına neden oldu.

2022
Lapsus$ Hacker Grubu, Microsoft, Nvidia ve Okta gibi büyük şirketleri hackledi.

2023
MOVEit Saldırısı, büyük çaplı bir veri sızıntısına yol açarak dünya genelinde binlerce kurumu etkiledi.

2024
Yapay zekâ kullanan daha sofistike saldırılar arttı.



Santralleri Hedef Alan Zararlı Yazılım

2005-2010 arasında geliştirildi, 2010'da keşfedildi.
Hedef: İran Nükleer Tesisleri

Stuxnet Nedir?

Bir bilgisayar virüsü gibi değil, siber silah olarak tasarlanmış özel bir zararlı yazılımdır.

- Hedefi, endüstriyel kontrol sistemlerine (SCADA/ICS) zarar vermektir.
- İran'ın nükleer santrallerindeki santrifüjleri bozarak uranyum üretimini yavaşlatmayı amaçladı.

Neden Önemli?

İlk siber saldırı ile fiziksel hasar verilen olaydır.
Devlet destekli siber savaşın başlangıcı olarak kabul edilir.

- SCADA ve endüstriyel sistemlerin ne kadar savunmasız olduğunu gösterdi.
- Sıfırıncı gün açıklarının ve siber güvenliğin kritik rolünü ortaya koydu.

6 Adımda Stuxnet Nasıl Çalışır?

Bulaşma
USB bellek aracılığıyla Windows sistemlerine bulaşır.

Hedef Analizi
Sistemin hangi markaya ait bir endüstriyel kontrol sistemi olduğunu kontrol eder.

Güncellenme
Eğer hedef uygun ise, internetten daha güncel bir sürüm indirir.

Sistemi Ele Geçirme
Yazılım, cihazın güvenlik açıklarını (Zero-day) kullanarak kontrolü ele alır.

Kontrol ve Sabotaj
Santrifüjleri bozarak yanlış hızlarda döndürür ve fiziksel olarak hasar verir.

Yanıltma ve Yok Etme (Deceive & Destroy)
Dışarıya yanlış veriler göndererek sistemin normal çalıştığını gösterir.

SİBER GÜVENLİK TAKSONOMİSİ: TÜRLER, DAĞITIM MODLARI, KULLANICILAR VE ÇÖZÜMLER

Siber güvenlik, yatay bir teknoloji alanı olarak değerlendirilmektedir; çünkü sektör veya uygulama alanından bağımsız olarak tüm teknolojilerde güvenliğin sağlanması için temel bir gerekliliktir. Havacılıktan sağlığa, e-ticaretten otonom araçlara kadar her alanda siber güvenlik, altyapının güvenliğini sağlamak için çapraz bir katman olarak işler.

SİBER GÜVENLİK UYGULAMA ÖRNEKLERİ

Google - Yapay Zekâ Destekli Tehdit Algılama
Google, Chronicle Security Operations platformuna yapay zekâ destekli tehdit tespit ve analiz yetenekleri eklemiştir. ***cloud.google.com***

Microsoft - Kuantum Güvenli Şifreleme
Microsoft, kuantum bilgisayarlara karşı dayanıklı şifreleme algoritmaları üzerinde çalışmaktadır. ***microsoft.com***

IBM - Zero Trust Güvenlik Modeli
IBM, Zero Trust güvenlik modelini benimseyerek sistemlerine erişimi sıkı kontrol altına almıştır. Bu yaklaşım, şirketlerin iç ve dış tehditlere karşı daha güvenli bir yapı oluşturmasına katkı sağlamaktadır.

CrowdStrike - Davranış Analizi ile Fidye Yazılımı Önleme
CrowdStrike, Falcon Insight XDR platformu ile anomali tabanlı davranış analizi kullanarak fidye yazılımlarını erken tespit etmektedir. Bu sayede firmalar, saldırılara maruz kalmadan savunma yapabilmektedir.

Apple - Donanım Tabanlı Güvenlik Çipi (Secure Enclave)
Apple, Secure Enclave teknolojisi ile biyometrik verileri daha güvenli hale getirmiştir. Bu yenilik, kullanıcı gizliliğini korurken siber saldırılara karşı ek bir koruma sağlamaktadır.

Amazon (AWS) - Güvenli Bulut Hizmetleri
AWS, Nitro Enclaves özelliği ile hassas verileri yalıtılmış bir ortamda işleme imkânı sunmaktadır. Bu özellik, finans ve sağlık sektöründeki firmalar için güvenlik riskini azaltmaktadır.

Cisco - Güvenli E-Posta ve Kimlik Doğrulama
Cisco, Advanced Phishing Protection ile e-posta sahtekarlığını önleyen yapay zekâ destekli bir sistem geliştirmiştir. Bu sayede şirketler, oltalama saldırılarından kaynaklanan veri sızıntılarının önüne geçebilmektedir.

Securify Identity - Behavioral
Securify Behavioral, adaptif erişim kontrolü ile kullanıcı davranışlarını sürekli analiz eder, risk skorları hesaplar ve bu skor doğrultusunda kimlik doğrulama yöntemlerini dinamik olarak ayarlar. Bu sayede güvenliği artırırken, yalnızca gerekli durumlarda güvenlik seviyesini yükselterek kullanıcı deneyimindeki gereksiz zorlukları ortadan kaldırır.

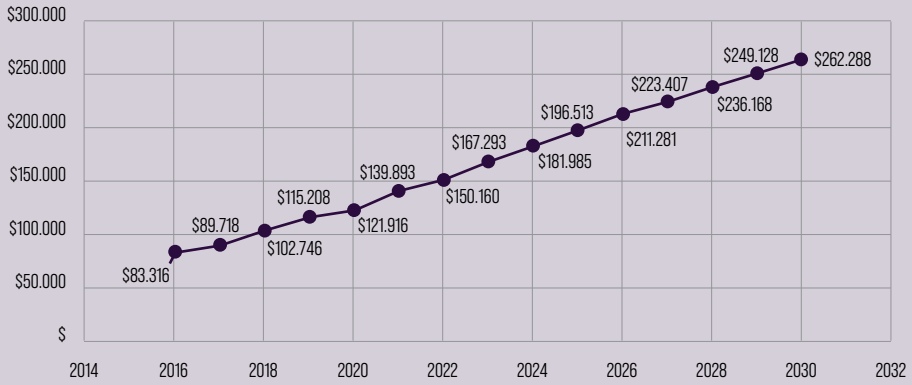
Picus - Saldırı Yolu Doğrulama
Picus'un Saldırı Yolu Doğrulaması çözümü, potansiyel siber saldırı yollarını tespit ederek kuruluşların bu yolları proaktif bir şekilde engellemelerine olanak tanır. Bu çözümler, kuruluşların siber dayanıklılıklarını artırmalarına ve olası ihlalleri önceden tespit etmelerine destek olur.

DÜNYADA SİBER GÜVENLİK TEKNOLOJİLERİ

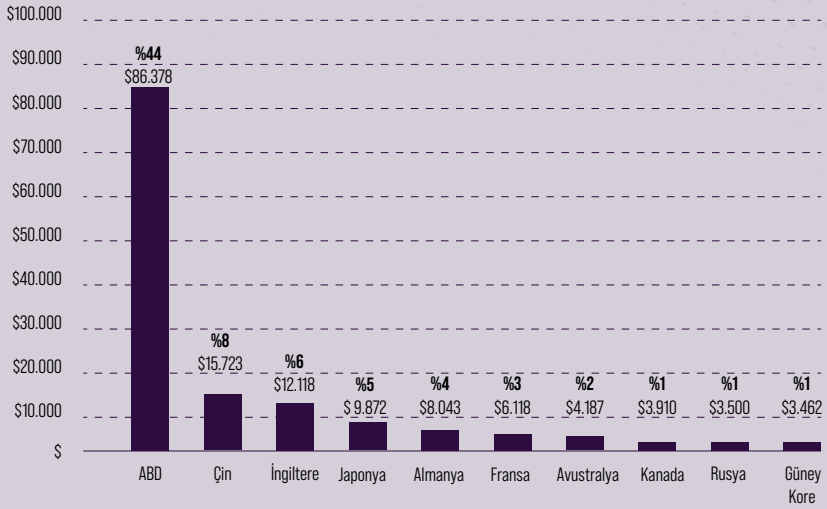
DÜNYADA SİBER GÜVENLİK PAZARININ DURUMU

Son 20 yılda, dünyada siber güvenlik farkındalığının hızla arttığı gözlemlenmektedir.
Başlanıçta yalnızca birkaç profesyonelin ilgilendiği ve bazı kurumların yatırım yaptığı bu alan günümüzde dev bir sektör haline gelmiştir. 2016 yılında toplam büyüklüğü yaklaşık 80 milyar dolar iken 2023 yılı sonuna kadar geçen sürede ikiye katlanarak 166 milyar dolar seviyesine ulaşmıştır. 2029 yılında pazarın yıllık ortalama %8'lik bir büyüme ile 270 milyar dolara ulaşması tahmin ediliiyor.

Siber Güvenlik - Küresel Gelir Karşılaştırması (Milyon ABD Doları)



Kaynak: https://www.statista.com/outlook/tmo/cybersecurity/worldwide?currency=USD



Türkiye bu sıralamada 514 milyar USD ve %0,2 ile 33. sırada yer almaktadır.
Kaynak: https://www.statista.com/outlook/tmo/cybersecurity/worldwide?currency=USD

Bilişim ve İletişim Teknolojileri(BİT-ITC) Sektörü İçindeki Siber Güvenlik Pazar Payı

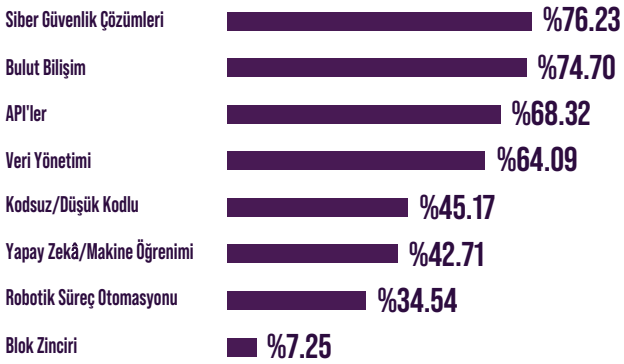
BÖLGE/ÜLKE	YIL	YAKLAŞIK PAY(%)
Dünya Genelinde	2024	4%
ABD	2023	5.3%
Avrupa Birliği	2023	4.5%
Türkiye	2025 (projeksiyon)	2.5-3%

NOT: Sektörel bazda (ör. finans, sağlık, kamu) bu oran %10'u aşabilir.

Kaynak: https://www.tubisad.org.tr/tr/images/pdf/tubisad-bit-2023-tr.pdf

BT Harcamaları Artıyor, Siber Güvenlik Zirvede Kalıyor

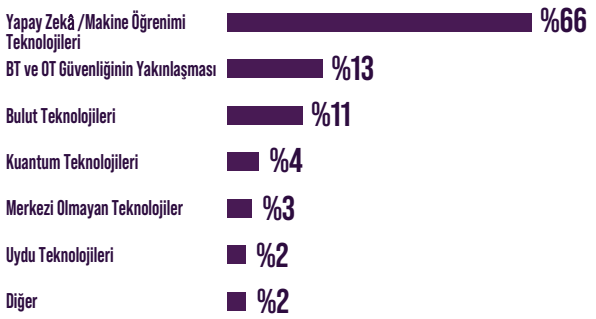
2025 için yatırım öncelikleri



Kaynak: BT'nin Geleceği 2025 Anketi, 2024; n=674

Siber Güvenlik Açıklarının 2025'te Beklenen Durumu

Sizce önümüzdeki 12 ay içinde siber güvenliği en çok etkileyecek olan aşağıdakilerden hangisidir?



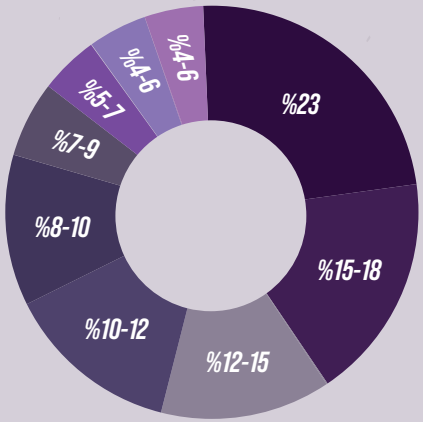
Kaynak: WEF Global Cybersecurity Outlook 2025

DÜNYADA SİBER GÜVENLİK PAZARININ DURUMU

Sibergüvenlik pazar büyüklüğü endüstri dağılımı

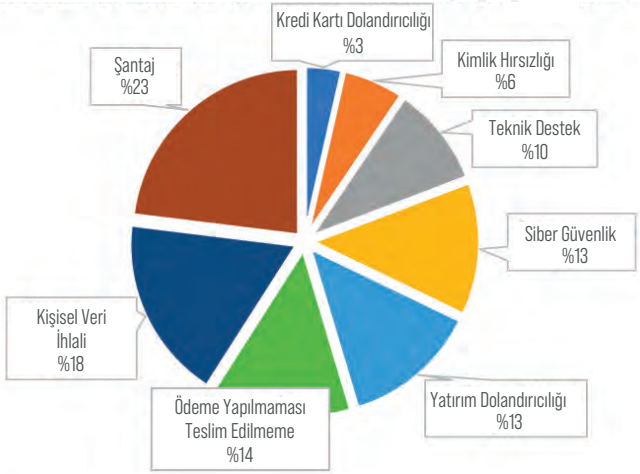
- *BFSI – %23,0*
- *IT ve Telekomünikasyon – %15-18*
- *Üretim – %12-15*
- *Sağlık – %10-12*
- *Perakende – %8-10*
- *Kamu – %7-9*
- *Enerji ve Kamu Hizmetleri – %5-7*
- *Ulaşım ve Taşımacılık – %4-6*
- *Diğer – %4-6*

Siber Güvenlik Teknolojilerinin Kullanıldığı Sektörler



Kaynak: www.fortunebusinessinsights.com

KÜRESEL SİBER SALDIRI TÜRLERİNDEKİ PAY (%) 2024



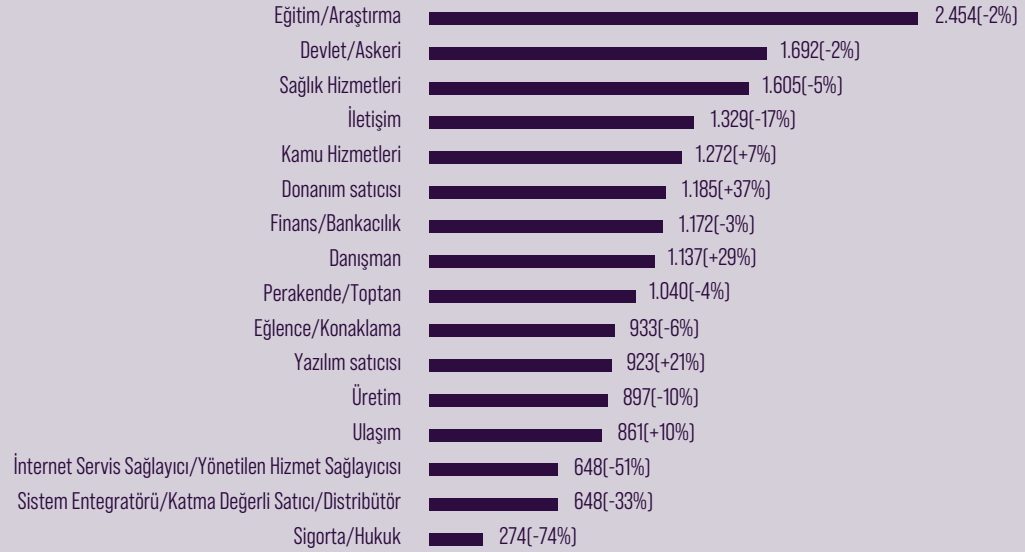
Kaynak: https://www.statista.com/outlook/tmo/cybersecurity/worldwide?currency=USD

Siber Saldırılarda Hedef Sektörler ve Yeni Eğilimler

Siber saldırılarda eğitim/araştırma sektörü, en fazla hedef alınan sektör olurken; onu kamu, askeri ve sağlık sektörleri izlemiştir. Bu durum, toplumsal işleyiş açısından kritik sektörlerin ciddi güvenlik açıklarına sahip olduğunu göstermektedir. Öte yandan, donanım üreticileri sektöründeki saldırılar %37 artış göstererek siber suçluların hedef tercihinde stratejik bir değişim yaşandığını ortaya koymuştur. Özellikle IoT ve akıllı cihazlara olan bağımlılığın artması, donanım üreticilerini siber saldırılar için cazip hedefler haline getirmiştir.

Kaynak: Checkpoint 2024

Sektöre Göre Küresel Ortalama Haftalık Siber Saldırılar



Siber Güvenlik'teki bu hızlı büyüme ile birlikte yeni kurulan startup firması sayısı da ciddi ölçüde artmaktadır.

2024 yılında dünya çapında **5.700**'ün üzerinde siber güvenlik startupı olduğu tespit edilmiştir.

Kurulan startupların çoğunluğu **Kuzey Amerika merkezli** olmakla birlikte **Güney Doğu Asya'da** da ciddi bir artış gözlemlenmektedir.

Silikon Vadisi, özellikle ABD'de, siber güvenlik firmaları ve bu firmalara yapılan yatırımların merkezi konumundadır.

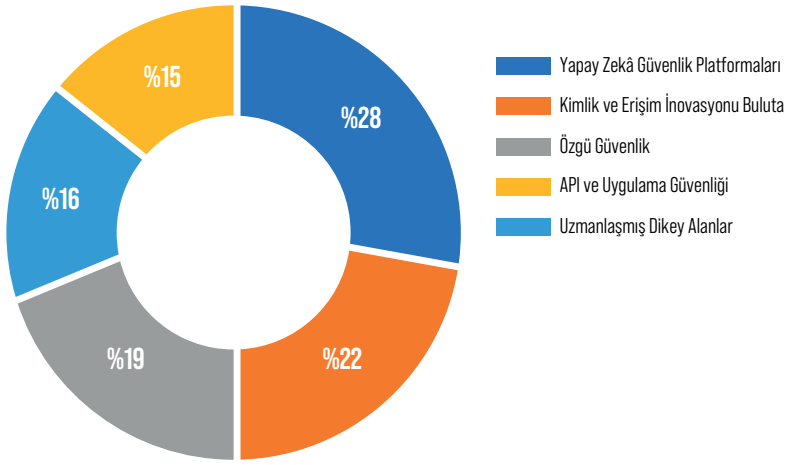
Yalnızca 2023 yılında bu bölgede farklı siber güvenlik firmalarına toplamda **10 milyar** dolar civarında yatırım yapılmıştır. 2024 ise bu rakam 432 firmanın yatırım alması ile **16 milyar** doları aşmıştır.

ÖNEMLİ

Teknoloji devi Google, 2025 Mart ayında, kolay kullanılabilir bir bulut güvenlik ürününe sahip WIZ firmasına 32 milyar dolarlık yatırım yaptıklarını duyurdu.

Kaynak: https://www.reuters.com/technology/cybersecurity/googles-32-billion-deal-wiz-accelerated-under-trump-sources-say-2025-03-19/

Siber Güvenlik Startup Ekosistemi Odak Alanları



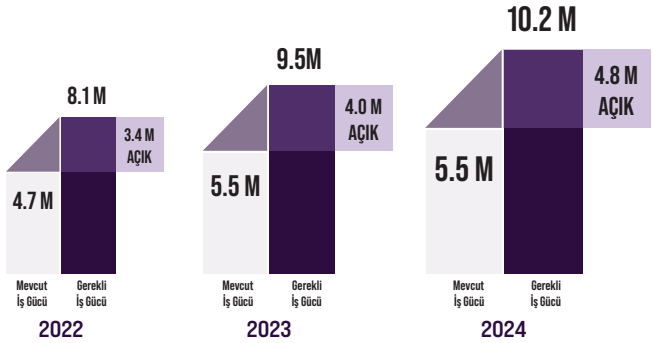
Kaynak: https://quickmarketpitch.com/blogs/news/cybersecurity-how-big

"Küresel Siber Güvenlik İş gücü"

- 2024 yılında küresel siber güvenlik iş gücü 16 milyondan fazla.
- ABD'de 2023 yılı itibarıyla 1.3 milyon siber güvenlik çalışanı bulunuyor ve Brezilya, 750 bin çalışan ile ikinci sırada.

"Siber Güvenlik Uzmanı Açığı"

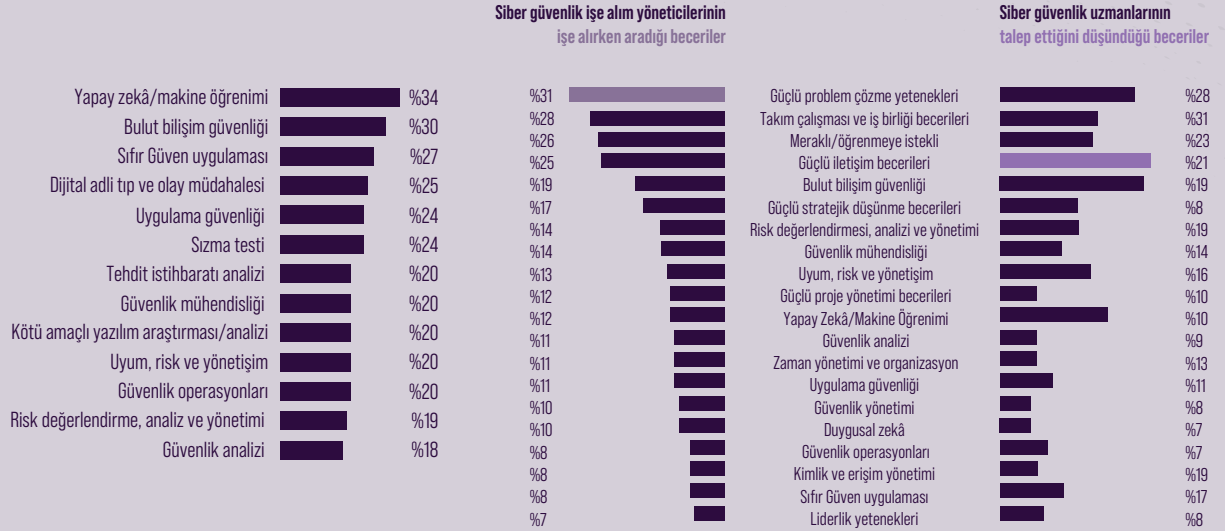
- 2022-2023 yılları arasında siber güvenlik çalışan sayısı %12.6 oranında arttı.
- Ancak, 2030 yılına kadar 80 milyon yeni siber güvenlik uzmanına, ideal siber güvenlik ekosistemine ulaşmak için ise 4.8 milyon yeni uzman istihdamına ihtiyaç duyulacağı tahmin ediliyor.



Kaynak: 2024 ISC2 Siber Güvenlik İş Gücü Araştırması.

Siber güvenlikte hangi teknik alanlar / yetenekler öne çıkıyor?

Güvenlik ekiplerinde teknik beceri eksiklikleri nerelerde?



Kaynak: 2024 ISC2 Siber Güvenlik İş Gücü Araştırması.

Siber Güvenlik Uzmanlığı Alanında Öne Çıkan Sertifikalar

- CompTIA Security+: En yaygın siber güvenlik sertifikalarından biridir.
- Sertifikalı Bilgi Sistemleri Güvenlik Uzmanı (CISSP): Yapılan bir arastırmaya göre, CISSP, iş ilanlarında en çok talep edilen sertifika olarak öne çıkmaktadır.
- Bu iki sertifikayı takiben aşağıdaki sertifikalar iş ilanlarında en sık karşılaşılan sertifikalardır; Küresel Bilgi Güvencesi Sertifikası (GIAC), Sertifikalı Bilgi Sistemleri Denetçisi (CISA), Sertifikalı Bilgi Güvenligi Yöneticisi, Sertifikalı Bilgi Gizliligi Uzmanı (CIPP)

Kaynak: 2025 Cyberseek

·Son beş yılda ABD'de en fazla siber güvenlik patenti başvurusu yapan ilk 5 şirket:

1. Microsoft - ***133 başvuru***
2. IBM - ***122 başvuru***
3. Intel - ***121 başvuru***
4. KnowBe4 - ***108 başvuru***
5. Darktrace Holdings - ***74 başvuru***

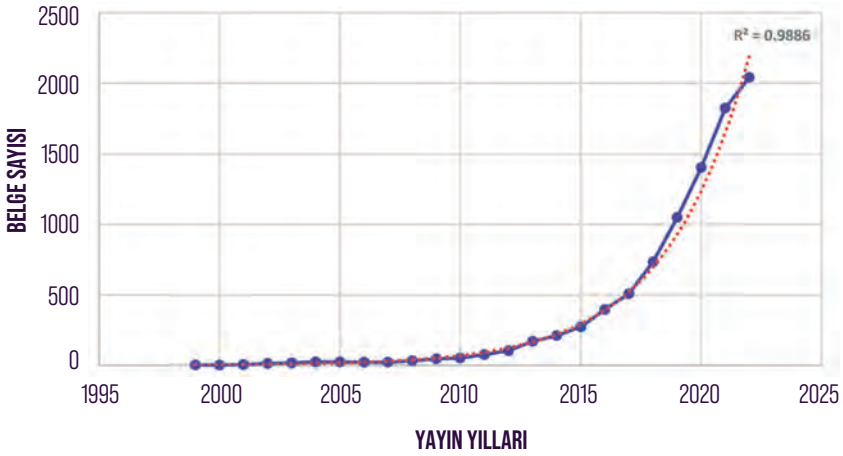
·Siber güvenlik alanında verilen patentler son 10 yılda her yıl yaklaşık %11 oranında artış gösterdi.

·En çok başvuru ve tescil alan 5 Siber Savunma Teknolojisi sınıfı:

·Ağ mimarileri
·Bilgisayarları korumaya yönelik güvenlik düzenlemeleri
·Sinyal işleme için desen tanıma
·Kriptografik mekanizmalar
·Makine öğrenimi

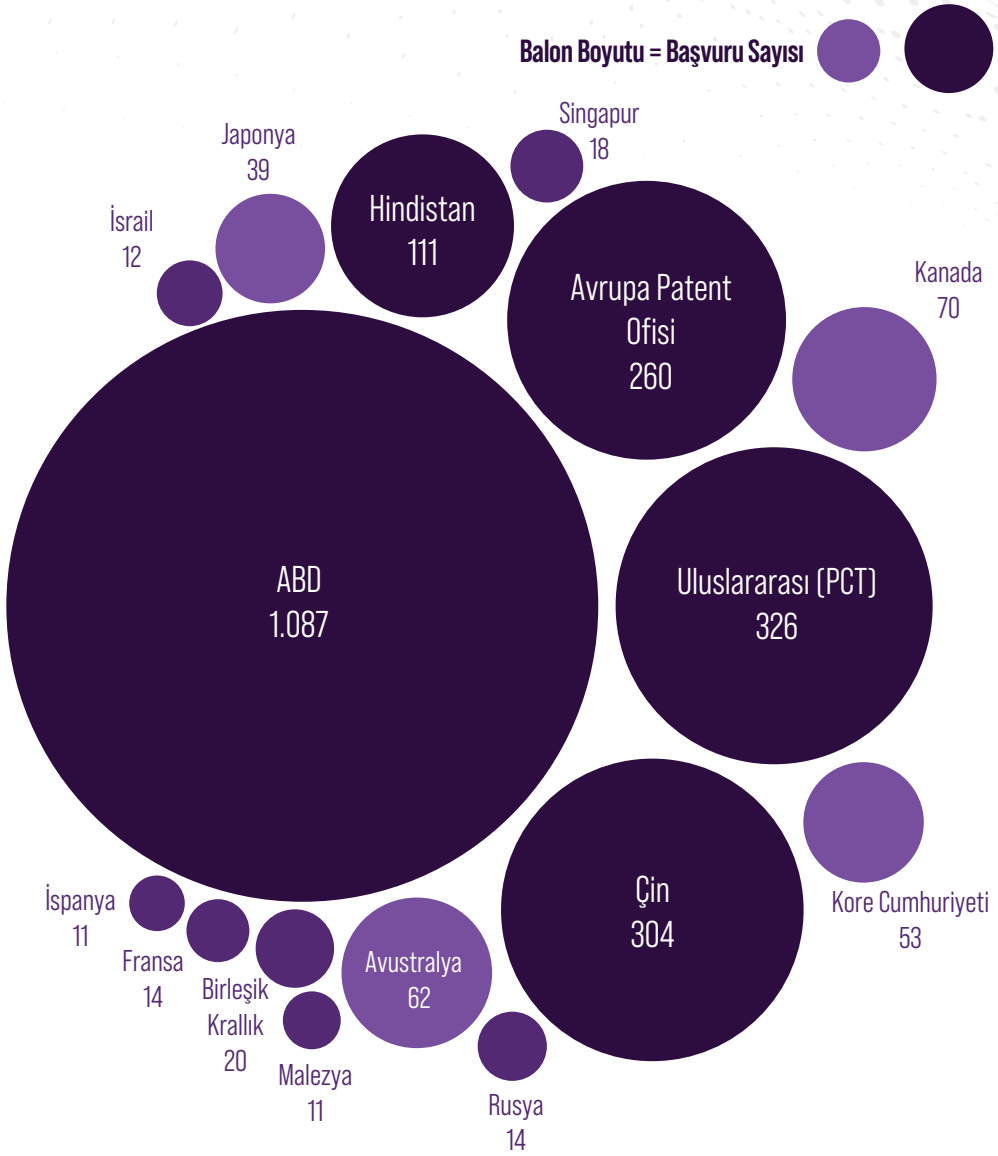
Kaynak: IFI CLAIMS Patent Services, Kasım 2024

Siber güvenlik ile ilgili basılan bilimsel makale sayılarının yıllara göre değişimi



Kaynak: https://www.tandfonline.com/doi/full/10.1080/23742917.2024.2400729#d1e412

SİBER GÜVENLİK PATENT BAŞVURULARINDA ÖNCÜ ÜLKELER



WIPO Patentscope'ta listelenen "siber güvenlik" terimini içeren 2.438 patent başvurusu 2000-2022 yılları arasında analiz edilmiştir.

2025 SİBER GÜVENLİK TRENDLERİ

1. GenAI'nin Veri Güvenliği Stratejilerini Yeniden Tanımlaması

1. Generative AI kullanımının artması, veri güvenliği stratejilerini yapılandırılmış veriden (veritabanları) yapılandırılmamış veriye (metin, görsel, video) yönlendirmektedir.
2. Bu dönüşüm, büyük dil modellerinin (LLM) eğitimi, veri dağıtımı ve çıkarım süreçleri üzerinde önemli etkiler yaratmakta ve yatırım önceliklerini değiştirmektedir.

2. Makine Kimliklerinin Stratejik Yönetimi

1. GenAI, bulut hizmetleri, otomasyon ve DevOps'un yaygınlaşması ile makine hesaplarının ve kimlik bilgilerinin hızla artması, kurumların saldırı yüzeyini genişletmektedir.
2. Etkin bir kurum çaplı makine kimlik ve erişim yönetimi (IAM) yaklaşımı, siber saldırılara karşı kritik bir savunma unsuru haline gelmektedir.

3. Taktiksel Yapay Zekâ Yaklaşımları

1. AI projelerinde karmaşık ve belirsiz sonuçlar alan kurumlar, dar kapsamlı, ölçülebilir ve doğrudan fayda sağlayan kullanım alanlarına yönelmektedir.
2. Üçüncü taraf AI çözümlerinin güvenliği, kurumsal AI uygulamalarının korunması ve AI ile siber güvenliğin güçlendirilmesi öncelikli konular arasında yer almaktadır.

4. Siber Güvenlik Teknoloji Yığınlarının Optimizasyonu

1. Büyük ölçekli kuruluşlar **ortalama 45 farklı siber güvenlik aracı** kullanmaktadır.
2. Güvenlik liderlerinin, araç setlerini sadeleştirerek çekirdek güvenlik kontrollerini konsolide etmesi, veri taşınabilirliğini artıran mimarilere odaklanması ve tehdit modelleme gibi yöntemlerle ileri ihtiyaçlarını belirlemesi önerilmektedir.

5. Güvenlik Davranışı ve Kültürü Programlarının Stratejik Katkısı

1. Güvenlik davranışı ve kültürü programları (SBCP), çalışan kaynaklı güvenlik risklerini azaltmada kritik bir araçtır.
2. GenAI ile entegre edilmiş platform tabanlı SBCP'lerin, 2026 yılına kadar **çalışan kaynaklı siber güvenlik olaylarını %40 oranında azaltması** beklenmektedir.

6. Siber Güvenlikte Tükenmişliğin Önlenmesi

1. Süregelen yetenek açığı, karmaşık tehdit ortamı ve sınırlı kaynaklar; güvenlik liderleri ve ekiplerinde tükenmişlik riskini artırmaktadır.
2. Etkili liderler, hem kendi hem de ekiplerinin dayanıklılığını artırmak için iyi oluş programlarına yatırım yapmakta ve stres yönetimini stratejik bir öncelik olarak ele almaktadır.

Kaynak: Gartner Security & Risk Management Summit Sydney, 3-4 Mart 2025

DÜNYADA SİBER GÜVENLİK İLE İLGİLİ YAPILAN ETKİNLİKLER

RSA Conference

ABD (San Francisco) & APAC bölgesi **www.rsaconference.com**

Siber güvenlik dünyasının en büyük etkinliklerinden biri olup yenilikler, tehditler ve en iyi uygulamalar üzerine paneller ve sunumlar içerir.

Black Hat

ABD (Las Vegas), Avrupa, Asya, Orta Doğu **www.blackhat.com**

Gelişmiş güvenlik araştırmaları, atölyeler ve hacking gösterileriyle tanınan prestijli bir etkinliktir.

DEF CON

ABD (Las Vegas) **www.defcon.org**

Dünyanın en ünlü hacker konferanslarından biri olup güvenlik açıkları, kriptografi ve siber tehditler üzerine atölyeler içerir.

Gartner Security & Risk Management Summit

ABD, Avrupa, Asya (farklı şehirlerde) **https://www.gartner.com/en/conferences**

Kurumsal siber güvenlik ve risk yönetimi stratejlerine odaklanan, iş dünyası liderleri ve CIO'ları hedefleyen bir zirvedir.

Infosecurity Europe

İngiltere (Londra) **www.infosecurityeurope.com**

Avrupa'nın en büyük siber güvenlik etkinliklerinden biri olup sektördeki en son yenilikler ve çözümler üzerine odaklanır.

CyberTech Global

İsrail (Tel Aviv), ABD (New York), BAE (Dubai), Kolombiya (Bogotá) **www.cybertechconference.com**

Küresel çapta düzenlenen bu etkinlik, siber güvenlik inovasyonlarına ve yeni tehditlere odaklanır.

European Cyber Week

Fransa (Rennes) **www.european-cyber-week.eu**

Avrupa'nın siber savunma ve güvenlik stratejilerine odaklanan, kamu ve özel sektör temsilcilerini bir araya getiren bir etkinliktir.

IT-SA Expo & Congress

Almanya (Nürnberg) **www.it-sa.de/en**

Avrupa'nın en büyük IT güvenliği ticaret fuarı olup siber güvenlik teknolojileri ve çözümleri sergilenir.

GovWare Conference & Exhibition

Singapur **www.govware.sg**

Asya-Pasifik bölgesinin en büyük siber güvenlik etkinliklerinden biri olup hükûmet ve özel sektör temsilcilerini bir araya getirir.

SANS Cyber Defense Initiative

ABD & Çeşitli ülkelerde farklı lokasyonlar **www.sans.org/**

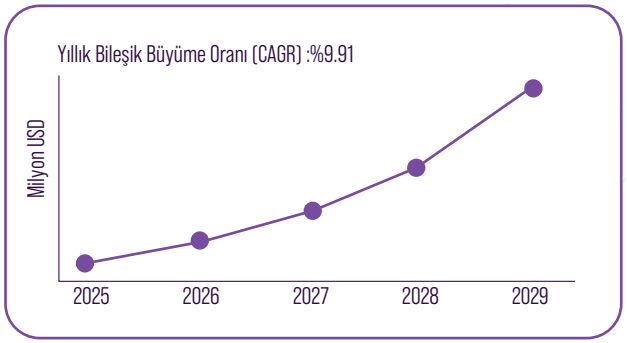
Uygulamalı siber güvenlik eğitimleri, tehdit istihbaratı ve olay müdahale konularına odaklanan teknik bir etkinliktir.

İSTANBUL'DA SİBER GÜVENLİK

İSTANBUL SİBER GÜVENLİK EKOSİSTEMİ

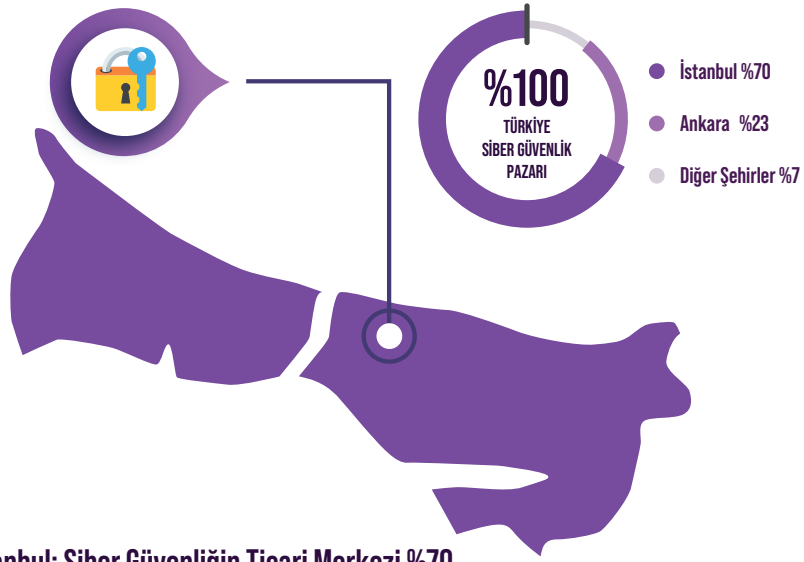
Pazar Büyüklüğü & Büyüme Oranı

	Türkiye	İstanbul
2025 :	$ 308,04 M	$ 127,390 M
2029 :	$ 449,52 M	$ 165,318 M



- Siber Güvenlik Patent Sayısı Türkiye (2020-2024) **307**
- Startup sayısı (2019-2025) **34**
- Araştırma Merkezi Sayısı **13**
- Yüksek Lisans Programı Sayısı **9**
- Doktora Programı Sayısı **4**

Kaynak: turkpatent.gov.tr , Startupwatch Raporu Nisan 2025, robot.universitetercihrobotu.com



İstanbul: Siber Güvenliğin Ticari Merkezi %70

- Türkiye siber güvenlik yatırımlarının büyük kısmı İstanbul'dadır.
- BIST 100, bankalar, telekom operatörleri ve büyük üreticiler İstanbul merkezlidir.
- Türkiye Bankalar Birliği üyelerinin %80'i İstanbul'da bulunmaktadır.
- Palo Alto, Cisco, Fortinet, Trend Micro gibi global siber güvenlik üreticilerin Türkiye ofisleri İstanbul'dadır.
- Finans ve telekom sektörlerindeki en büyük siber güvenlik yatırımları da İstanbul merkezli olarak yürütülmektedir.

Ankara: Kamu ve Savunma Projeleri %23

- Kamu kurumları ve savunma sanayii odaklı çözümler Ankara'dadır.
- Kamu ihaleleri ve yerli üreticiler ağırlıklı olarak Ankara'da bulunmaktadır.
- TOBB, TÜBİTAK, BTK, SSB gibi kurumlar siber güvenlik alanında etkindir.

Diğer Şehirler %7

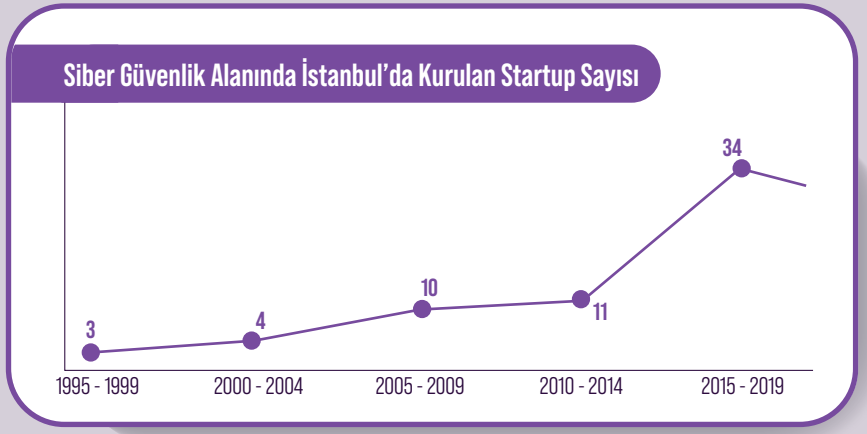
Teknoparklar,
sanayi kümelenmeleri

Kaynak: https://www.statista.com/outlook/tmo/cybersecurity/worldwide?currency=USD
Dipnot: Dağılım, IDC ve BTK gibi kaynaklarla desteklenen piyasa gözlemlerine dayanmaktadır.

İSTANBUL'DA BİLGİ GÜVENLİĞİ & AĞ GÜVENLIIĞİ ALANINDA İSTİHDAM GÖRÜNÜMÜ

İstanbul'da, **Bilgisayar Ağı Güvenliği alanında 354 firma mevcuttur.**

Siber güvenlik alanında toplam **30.517 çalışan** bulunmaktadır.

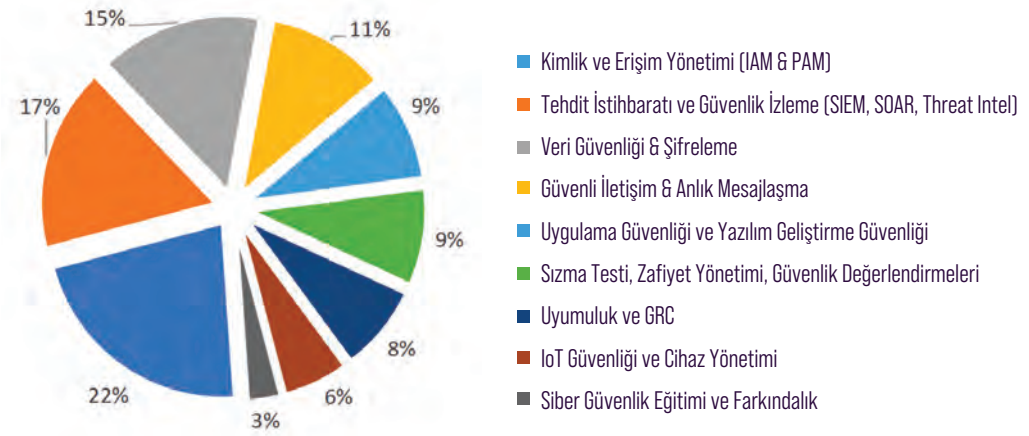


2020 - 2024 arasında kurulan siber güvenlik girişimleri, geleneksel yaklaşımların ötesine geçerek; davranışsal analiz, kimlik temelli güvenlik ve gerçek zamanlı tehdit yönetimi üzerine yoğunlaşmıştır.

Siber Güvenlik Kümelenmesine kayıtlı **43 İstanbul firması bulunmaktadır.**

- 20'si yalnızca **"Tedarikçi (Vendor)"**, 23 firma ise **"Hizmet", "Danışmanlık", "Eğitim"** ve **"Sistem Entegratörü"** gibi çeşitli iş kollarında faaliyet göstermektedir.

Bu firmaların odaklandığı siber güvenlik alanlarının yoğunluğu asağıdaki gibi gruplandırılmıştır:



Kaynak: https://www.siberkume.org.tr/

2025'te Siber Güvenlik Eğitiminde Neler Oldu?

- Ortaöğretimde, siber güvenliğin ayrı bir alan olarak tanınmasının ardından bu alandaki lise programlarının sayısı artmıştır.
- Ön lisans seviyesinde, "Bilişim Güvenliği Teknolojisi", "Siber Güvenlik Analistliği ve Operatörlüğü" gibi programlar yaygınlaştı.
- Lisans düzeyinde, 2024'te başlayan "Siber Güvenlik Mühendisliği" program 2025'te 2 üniversitede daha açıldı.
- "Bilgi Güvenliği Teknolojisi" programlarının da sayısı arttı.
- Mevcut programların kontenjanı sabit kalırken, yeni açılan programlarla genel kontenjan artışı sağlandı.

Ortaöğretim

- İstanbul'da siber güvenlik alanında **ortaöğretim** (lise) düzeyindeki ilk mesleki eğitim kurumu, **2020 yılında açılan Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi** oldu.

Ön Lisans

- İstanbul'da **önlisans düzeyinde siber güvenlik eğitimi,** İstanbul Teknk Üniversitedeki Siber Güvenlik Meslek Yüksek Okulu (MYO) ve 6 üniversitede çok alanlı MYO'larda sunulmaktadır.

Lisans

- **2025 itibarıyla İstanbul'da;** 2 üniversitede **Siber Güvenlik Mühendisliği** lisans programı 3 üniversitede **Bilgi Güvenliği Teknolojisi** lisans programları bulunmaktadır.

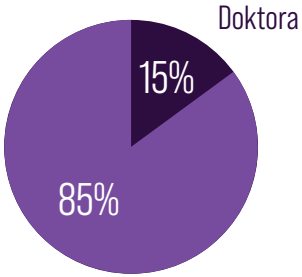
Eğitimin Geliştirilmesi Gereken Alanlar

- **Eğitici Kalitesi ve Uygulama:** Öğretmenlerin kalitesi, pratik eğitim imkânları ve sektörle iş birliği hususları geliştirilmesi gereken en önemli alanlardır.
- **Bütünleşik Yaklaşım:** Lise, ön lisans ve lisans programları arasındaki geçişlerin ve müfredatın uyumlu olması gerekir.
- **İstihdam Odaklılık:** Özellikle ön lisans mezunlarının kolayca iş bulabilmesi için teşvik edici politikalar oluşturulmalıdır.
- **Sektör Entegrasyonu:** Sektörün gerçek ihtiyaçlarına göre müfredatın düzenlenmesi ve işverenlerin eğitim sürecine aktif katılımı büyük önem taşımaktadır.

Siber Güvenlik Alanında Akademik Yayın Sayısı

Türkiye	2.628
İstanbul	898
Ankara	577
İzmir	143
Kocaeli	106

Siber Güvenlik Alanında Lisansüstü Tez Dağılımları



Siber Güvenlik Alanında Lisansüstü Tez Sayıları

Türkiye	1.509
İstanbul	559

İSTANBUL'DA DÜZENLENEN SİBER GÜVENLİK ETKİNLİK VE KONFERANSLARI

1- IDC Security Roadshow / İstanbul

- **Organizatör:** IDC Türkiye
- **Düzenlenme Sıklığı:** Her yıl Şubat ya da Mart aylarında düzenlenir.
- **Katılımcı Profili:** CISO'lar, BT yöneticileri, kamu ve özel sektör temsilcileri
- **Konular:** Siber tehditler, yapay zekâ, risk yönetimi, sıfır güven (Zero Trust), bulut güvenliği

2- ISAF Cyber Security / İstanbul

- **Organizatör:** Marmara Fuarcılık
- **Düzenlenme Sıklığı:** Her yıl Ekim ayında İstanbul Fuar Merkezi'nde düzenlenir.
- **Katılımcı Profili:** Güvenlik şirketleri, çözüm sağlayıcılar, kamu temsilcileri
- **Konular:** Fiziksel güvenlik + siber güvenlik entegrasyonu, sistem entegratörleri, savunma sanayi

3- SANS Istanbul / Training Event

- **Organizatör:** SANS Institute
- **Düzenlenme Sıklığı:** Her yıl genellikle Eylül ya da Kasım aylarında yapılır.
- **Katılımcı Profili:** Teknik uzmanlar, BT güvenlik ekipleri
- **Konular:** Uygulamalı siber güvenlik eğitimleri, tehdit avcılığı, ters mühendislik

4- ENBANTEC Cyber Security Conference

- **Organizatör:** ENBANTEC (Fintek & Bankacılık sektörü odaklı)
- **Düzenlenme Sıklığı:** Her yıl Nisan-Mayıs aylarında İstanbul'da yapılır.
- **Katılımcı Profili:** Bankalar, finans kurumları, regülasyon uzmanları
- **Konular:** Bankacılık siber güvenliği, veri koruma, dolandırıcılık önleme, IAM

DÖNEMSEL OLAN ETKİNLİKLER

- Siber Güvenlik Kümelenmesi'nin sektör özelinde düzenlediği firma buluşmaları
- Üniversitelerin siber güvenlik temalı konferans ve etkinlikleri
- Partner firmaların ürün tanıtımı ve networking etkinlikleri
- BT Haber, Webrazzi gibi platformların siber güvenlik odaklı oturumları
- TÜBİTAK destekli projelerin demo ve tanıtım günleri
- Teknopark ve kuluçka merkezlerindeki girişimci-yatırımcı demo günleri
- Üniversite topluluklarının düzenlediği CTF yarışmaları ve atölyeler
- Webrazzi Summit, TechDay gibi etkinliklerdeki siber güvenlik panelleri

İSTANBUL SİBER GÜVENLİK EKOSİSTEMİNDEN İYİ UYGULAMA ÖRNEKLERİ

1- Procenne

Türkiye'nin ilk HSM (Hardware Security Module) cihazını üreterek, şifreleme ve dijital imza işlemlerinin güvenliğini sağlama konusunda sektördeki eksikliği gideren bir teknoloji geliştirmiştir.

2-Verifone

Türkiye'de ilk kez ödeme sistemlerine "End-to-End Encryption" (E2EE) çözümünü entegre ederek, kredi kartı ve dijital ödeme verilerinin en yüksek güvenlikle şifrelenmesini sağlayan yenilikçi bir güvenlik teknolojisi sunmuştur.

3-Sistem Global

İlk kez "Zero Trust" güvenlik modelini geniş çapta entegre ederek, tüm ağ trafiğini doğrulama ve izleme gereksinimiyle ağ güvenliği anlayışını temelden değiştiren bir sistem geliştirmiştir.

4-Roketsan

Roketsan, endüstriyel güvenlik uygulamalarıyla kritik altyapıların savunmasına yönelik çözümler geliştirerek, güvenlik alanındaki en iyi uygulamaları hayata geçirmektedir.

5-Akinon

Akinon, güçlü bulut güvenliği çözümleri ve uygulama güvenliği testleri ile dijital platformlarda en yüksek güvenlik standartlarını sağlamaktadır.

6-ISTEC

Nesnelerin İnterneti Ekosistemi Güvenlik Test ve Değerlendirme Merkezi; IoT cihazları için donanım, yazılım, haberleşme ve kişisel veri güvenliği testleri yapmakta, üreticilere raporlama ve danışmanlık sağlamaktadır. Ayrıca siber güvenlik alanında eğitimler düzenlemekte, sektörle iş birlikleri yürütmekte ve uluslararası standartlara uygun test hizmetleri sunmaktadır.

7-BUSİBER

2017 yılında İSTKA desteği ile kurulan Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi tarafından 8 yılda üniversite öğrencilerine ücretsiz 15 siber güvenlik kampı düzenlenmiş, 2.000'den fazla öğrenciye eğitim verilmiştir. Ayrıca 13 adet Siber Güvenlik Zirvesi düzenlenerek kamu siber güvenlik farkındalığı oluşmasına katkı sağlanmıştır. Çalışmalar, Almanya - Pakistan - Türkiye ortaklı Avrupa Birliği Erasmus+ projesi (Rethinking Cybersecurity in Pakistan: Human Factors' Essential Role) ile yurt dışına taşınmış uluslararası bir boyut kazanmıştır.

Son güncelleme tarihi: 07/11/2025

İSTANBUL'DA SİBER GÜVENLİK EKOSİSTEMİ

Özel Sektör

Beyaz Net, inventiv, DESTEL, ENDPOINT LABS, CYBER WISE, isteo, sekom, SECHARD, Nex Teknoloji, SOITRON, SECURE FUTURE, bilgisayar, ThreatMon, INVENTUM, Kron, AÇIK, DENİZ, HAVELSAN, isnet, KoçSistem, TUGAY, EGA, QUBITRIUM, CBERNET, idea, ADEO, BARİKAT, nebula, btrisk, BGA CYBER SECURITY, BİLİŞİM112, Secrise, STD BİLİŞİM, CenterOnDigital, gais, PHISHUP, CyberFortress, BAT, OrtakNet, Opinnate, CEREBRO, CRYPTTECH, CYBERPATH, Termtech, CertBy, SHIELDIA, VulnHero, ferrumgate, H2H, CASPIPOT, ekoruma, ERWALL, DIATTACK, AMANI, databin, Grizzle Technology, nss, NATIVE TEKNOLOJİ, CYNTE, intelegon, infinitum IT, identify, invento, Indata Technology, kondukto, Otak, PONA, TÜV AUSTRIA, MAGARSUS, ISTEC cyber security, nexracon, NCSOFT, PDA, procenne, BOA, VULNSIGN, PRODAFT, netsmart, SecroMix, Secrove, strixeye, Lostar, TerraMedusa, SODER, siberninja, TeSlakom, BBS BİLİŞİM, Logsign, treomind

Son güncelleme tarihi: 07/11/2025

Sivil Toplum Kuruluşları ve Meslek Örgütleri

TURKISH CYBER SECURITY CLUSTER, TASAM, BİLİŞİM VADİSİ, TÜBİSAD, TÜRKİYE BİLİŞİM DERNEĞİ

Üniversiteler, SEM ve Araştırma Merkezleri

MARMARA ÜNİVERSİTESİ, FATİH SULTAN MEHMET VAKIF ÜNİVERSİTESİ, MEDİPOL UNV-İSTANBUL, İSTANBUL ÜNİVERSİTESİ, Sabancı Üniversitesi, BAUPRO, İstanbul Bilgi Üniversitesi, KOÇ ÜNİVERSİTESİ, BOĞAZİÇİ ÜNİVERSİTESİ YÖNETİM BİLİŞİM SİSTEMLERİ SİBER GÜVENLİK MERKEZİ, İSTANBUL AYDIN ÜNİVERSİTESİ, İTÜ SÜREKLİ EĞİTİM MERKEZİ, İSTANBUL TOPKAPI ÜNİVERSİTESİ, SEM İSTANBUL AYDIN ÜNİVERSİTESİ SÜREKLİ EĞİTİM MERKEZİ, ARELSEM SÜREKLİ EĞİTİM MERKEZİ, FEYZİYE MEKTEPLERİ VAKFI IŞIK ÜNİVERSİTESİ SÜREKLİ EĞİTİM MERKEZİ, İstanbul Gedik Üniversitesi GEDİKsem Sürekli Eğitim Merkezi, BAU Bahçeşehir University

Kamu Kurumları

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI SAVUNMA SANAYİİ BAŞKANLIĞI, BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, teknopark istanbul

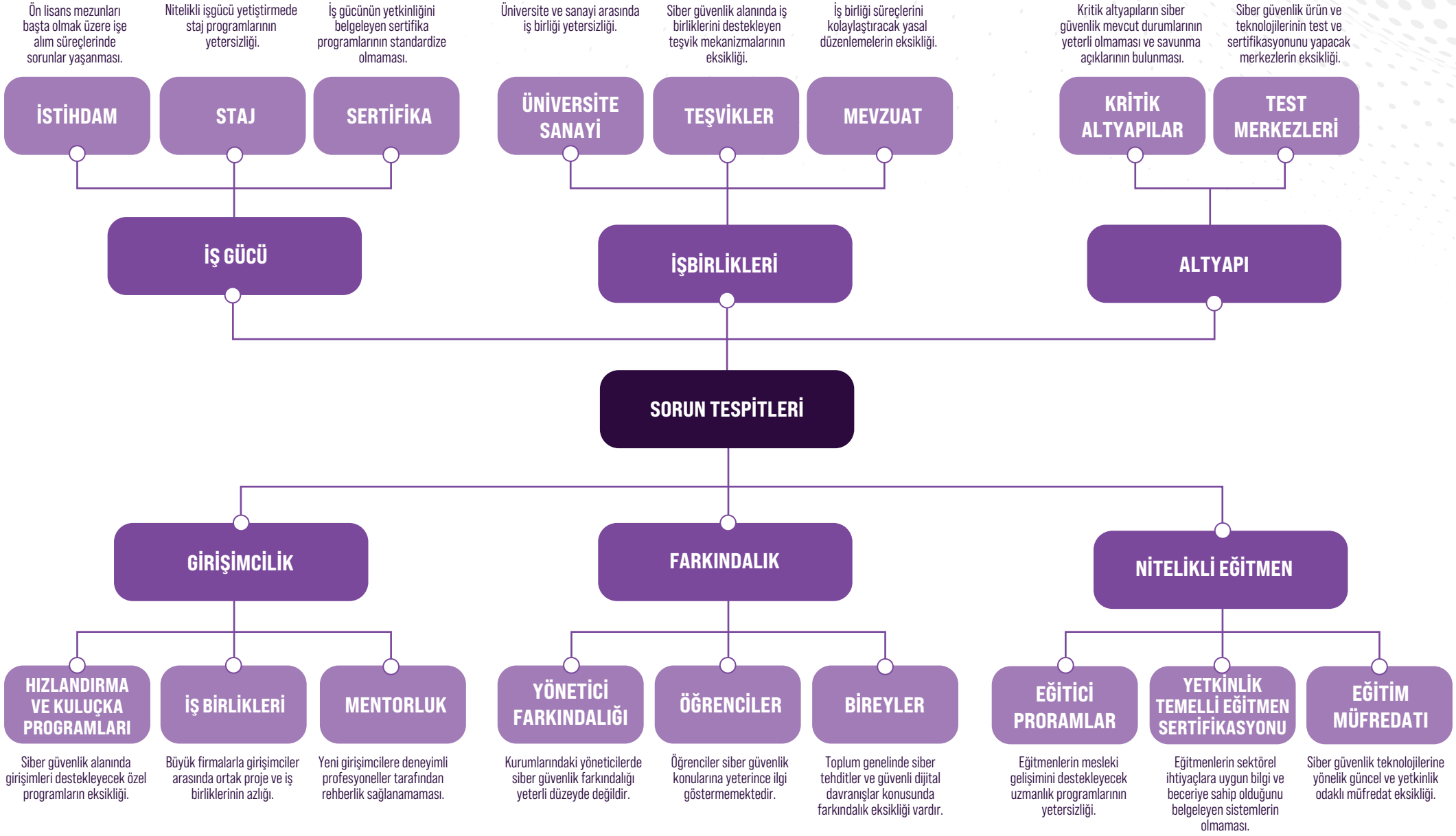
İSTANBUL SİBER GÜVENLİK ÇALIŞTAYI

İstanbul'da Siber Güvenlik Teknolojileri Çalıştayı, İstanbul özelindeki sorun ve ihtiyaçları tespit etmek, ekosistemin ihtiyaç duyduğu program, proje ve faaliyetleri bölgemizdeki tüm önemli aktörlerin katılımıyla tasarlamak üzere 03 Ekim 2025 tarihinde çevrimiçi olarak gerçekleştirilmiştir.

Siber güvenlik teknolojileri alanındaki ilerlemeleri tartışmak ve şekillendirmek üzere kapsayıcı bir bakış açısıyla kamu kurumları, girişimler, işletmeler, üniversitelerden uzmanların davet edildiği çalıştayda **13 farklı kuruluştan 22 katılımcı** yer almıştır.

İki oturumda gerçekleştirilen çalıştayın ilk oturumunda, **İstanbul Siber Güvenlik Teknolojileri Ekosisteminin** "İnsan Kaynağı ve Eğitim", ikinci oturumda "Ekosistem ve İşbirlikleri" ile "Ar-Ge, Ürünleşme ve Teknik Altyapı" başlıklarında daha önce gerçekleştirilen anket çalışması ile tespit edilen sorun ve ihtiyaçlara ilişkin çözüm önerileri ele alınmıştır. Çalıştay kapsamında gündeme gelen konular ve geliştirilen öneriler, bir sonraki sayfada gruplandırılmıştır.

İSTANBUL SİBER GÜVENLİK EKOSİSTEMİNDEKİ SORUN ALANLARI



Nitelikli Eğitici/ Eğitmen Eksikliği	· BTK Akademi ve YÖK iş birliğiyle sertifika tabanlı eğitici eğitim programları hazırlanmalı. · Diploma yerine yetkinlik temelli yaklaşım önceliklendirilmeli. · Pratik uygulamaları merkeze alacak eğitim müfredatı hazırlanmalı. · Ön lisans, lisans ve yüksekokul düzeylerinde sanal laboratuvarlar kurulmalı. · Ön lisans, lisans ve yüksekokul programlarında, özel sektörde çalışan deneyimli profesyonellerin ders verebilmesi kolaylaştırılmalı.
Staj ve İstihdam Sorunu	· Ulusal staj programlarının sayısı artırılmalı. · Türkiye Siber Güvenlik Kümelenmesi tarafından sürdürülen istihdam ve staj fırsatlarının yaygınlaştırılması sağlanmalı. · Özel sektörün işe alım süreçlerinde yetkinlik temelli değerlendirme yapılmalı. · Mesleki Yeterlilik Kurumu (MYK) nezdinde siber güvenlikle ilişkili mesleklerin tespiti yapılmalı. · Önlisans mezunlarının istihdam süreçleri kolaylaştırılmalı. · Kamu tarafından istihdam programları hazırlanmalı ve işletmelere teşvikler verilmeli. · Ulusal düzeyde akredite bir kurum tarafından yürütülecek sertifikasyon programları geliştirilmeli.
İş Birliklerinin Güçlendirilmesi	· Üniversite-sanayi işbirliklerini güçlendirecek arayüz mekanizmaları oluşturulmalı. · Akademide yer alan öğretim görevlilerin aynı zamanda girişimcilik faaliyetlerine katılımı kolaylaştırılmalı. · Sanayi-doktora programları daha nitelikli ve verimli hale getirilmeli. · Kamu kurumlarının yerli siber güvenlik ürünlerini kullanması için mevzuatsal düzenlemeler yapılmalı.

İSTANBUL SİBER GÜVENLİK EKOSİSTEMİNİ İLERİYE TAŞIYACAK ÇÖZÜMLER

Girişimcilik Ekosisteminin Güçlendirilmesi	· Siber güvenlik alanında yenilikçi çözümler üreten girişimlerin sayısının ve niteliğinin artırılması için kapsamlı destek mekanizmaları oluşturulmalı. · Siber güvenlik odaklı hızlandırma ve kuluçka programları hayata geçirilmeli. · Girişimcilerin kamu kurumları, özel sektör ve akademiyle etkileşim kurabileceği, prototip geliştirme, test ve ticarileşme süreçlerine yönelik desteklerin sunulacağı bir iş birliği ortamı tesis edilmeli. · Yerli siber güvenlik ürünlerinin uluslararası pazarlara açılması ve geliştirilen ürünlerin uluslararası standartlara uygun şekilde geliştirilmesi için gerekli mentorluk destekleri sağlanmalı. · Kurumsal firmalar ile startuplar arasındaki ilişkiler, karşılıklı faydaya dayalı, uzun vadeli ve yenilik odaklı iş birliği modelleri üzerinden geliştirilmeli.
Ar-Ge ve Ür-Ge Çalışmalarının Güçlendirilmesi	· İşletmelerin, geliştirdikleri ürünleri bağımsız olarak test edebilmelerini sağlayacak özdeğerlendirme araçları geliştirilmeli. · Yapay zekâ teknolojilerinin getirdiği siber güvenlik tehditlerine yönelik yeni Ar-Ge çözümlerinin geliştirilmeli. · Finansmana erişimi kolaylaştıracak yeni hibe, teşvik ve fon mekanizmalar hayata geçirilmeli. · Büyük ölçekli yerli siber güvenlik ürünlerinin geliştirilmesi amacıyla, ekosistemdeki paydaşların bir araya geldiği konsorsiyumlar oluşturulmalı. · Kamu kurumları ile yerli ürün üreticileri arasındaki iş birliklerinin artırılarak, siber güvenlik ürünlerinin gerçek kullanıcı ihtiyaçları ve geri bildirimleri doğrultusunda geliştirilmesi sağlanmalı.
Teknik Altyapı Eksiklikleri	· Kritik altyapıların ve siber güvenlik ürünlerinin test edilebilmesi için ulusal ve yerel test merkezleri kurulmalı. · Mevcut siber güvenlik altyapılarının kapasiteleri ürün sertifikasyon süreçlerinin regülasyonlara uygunluğunu denetleyecek şekilde artırılmalı.
Farkındalık Çalışmaları	· Kamu kurumlarındaki karar vericilerin siber güvenlik farkındalığının artırılmalı. · Toplumun tüm kesimlerini gözetecek farkındalık çalışmalarının yapılmalı. · Öğrencilere yönelik yarışmalar/kamplar düzenlenmeli.

ÇÖZÜM ÖNERİLERİNİN UYGULANMASIYLA ELDE EDİLECEK ÇIKTILAR

- Nitelikli Eğitici Kadrosunun Oluşması
- Uygulamalı Eğitim Kapasitesinin Artması
- Gençlerin İstihdam ve Staj Fırsatlarına Erişimi
- Yetkinlik Temelli İşe Alım Kültürünün Yerleşmesi
- Üniversite–Sanayi İş Birliklerinin Güçlenmesi
- Girişimcilik Ekosisteminin Gelişmesi
- Yerli Ar-Ge ve Ür-Ge Kapasitesinin Artması
- Ülkemizin Uluslararası Siber Güvenlik Pazarında Söz Sahibi Olması
- Güçlü ve Güvenilir Teknik Altyapının Oluşması
- Toplumsal Siber Güvenlik Farkındalığının Artması

KATILIMCILAR

Kadir Kağan İNALOĞLU - Batı Karadeniz Kalkınma Ajansı

Muhammet TEMLİ - Batı Karadeniz Kalkınma Ajansı

Duygu FİDANCIOĞLU - Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

Tolga MATARACIOĞLU - Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

Edip GÜMÜŞ - Erdemir

Selçuk YILDIRIM - Erdemir

Ebu Yusuf GÜVEN - İstanbul Üniversitesi Cerrahpaşa

Mehmet Yavuz YAĞCI - İstanbul Üniversitesi Cerrahpaşa

Muhammed Ali AYDIN - İstanbul Üniversitesi Cerrahpaşa

Furkan KARA - İTÜ Mesleki ve Teknik Anadolu Lisesi

Kemal BIÇAKCI - İTÜ Siber Güvenlik Meslek Yüksek Okulu

Oğuz POLAD - İTÜ Siber Güvenlik Meslek Yüksek Okulu

Alptekin KÜPÇÜ - Koç Üniversitesi

Albert LEVİ - Sabancı Üniversitesi

Ece EFE - Securify Identity

Saliha İŞÇEN - Securify Identity

Burak TAŞBAŞ - Siemens Türkiye

Ruşen ÇELİK - Siemens Türkiye

Şükrü Güçlü DUTLUCA - Siemens Türkiye

Muttalip TULGAR - Turkcell

Eren HASİPEK - Türkiye Siber Güvenlik Kümelenmesi

Serhat BAŞKONAKLIOĞLU - Türkiye Siber Güvenlik Kümelenmesi

İSTANBUL KALKINMA AJANSI

Asmalı Mescit Mah. İstiklal Caddesi
No:142, Odakule Kat: 6-7-8 Beyoğlu/İstanbul
PK: 34430 - Tel: 0 (212) 468 34 00
E-Posta: iletisim@istka.org.tr