

Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ ● AYDA BİR YAYINLANIR

NİSAN 2026 SAYI: 153

KAPAK:
GEÇİŞ KONTROL
SİSTEMLERİ

FOKUS:
ENDÜSTRİYEL TESİS
GÜVENLİĞİ

ÖZEL DOSYA:
TOPLUMSAL
DAVRANIŞ
PSİKOLOJİSİ VE
ÖZEL GÜVENLİK



**Geleceđi
göremeyiz ama
çözümlerimiz ile
geleceđi
koruyabiliriz**

İhtiyaçlar deđişse de esnek ve adaptif teknolojilerimiz ile her duruma hızlıca uyum sağlıyoruz.

Sunduđumuz teknolojilerle geleceđin güvenliđini şekillendiriyor, dünyanın daha güvenli hale gelmesine yardımcı oluyoruz.

Farklı bir dünya görüyoruz



GÜVENLİK TEDARİK.com

Son teknolojiye uygun, ürün ve çözümlerden **HABERİNİZ VAR MI?**

- Elektrik proje taahhüt firmaları • Bayi odaklı çalışan firmalar
 - Havalimanları ilgili birimleri • Bankalar ilgili birimleri • İnşaat firmaları
 - Oteller ilgili birimleri • Hastaneler ilgili birimleri • AVM'ler ilgili birimleri
 - TÜRKİLM Üyeleri • Belediyeler ilgili birimleri • Emniyet Genel Müdürlüğü ilgili birimleri • Zincir mağazalar • Üniversiteler • Mimarlık ofisleri
 - Sektör profesyonelleri **AĞIMIZA KATILIN**
- ### TÜM TÜRKİYE'DE SESİNİZ OLALIM!

- ✓ CCTV ve video kontrol sistemleri,
- ✓ Yangın algılama ve ihbar sistemleri,
- ✓ Yangın söndürme sistemleri,
- ✓ Geçiş kontrol sistemleri,
- ✓ Hırsız alarm sistemleri,
- ✓ Alarm izleme merkezleri,
- ✓ Apartman konuşma sistemleri,
- ✓ Mobil takip sistemleri,
- ✓ Drone teknolojileri

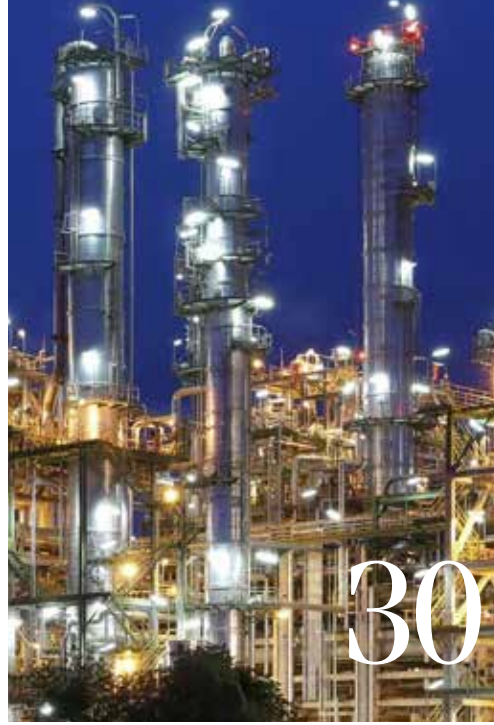
Çok sayıda farklı hizmetin çözüm sağlayıcısı ve peşinli baskı sistemleri ile en iyi hizmet kalitesini **ARKHO** ve **TECHNEWS** firmalarından sunmaktayız. Üstün seviye GÜVENLİK YÖNETİMİ, PERFORMANSMAN, TEKNİKLER ve KURUMSAL YATIRIMCI dengeleri barındıran **ARKHO** TANITIM HİZMETLERİ, grafik tasarım, kurumsal kimlik çözümleri, web ve mobil uygulamalar, bilişim teknolojileri ve diğer çözümler sunar. Her ve müşteriye kurulum, bakım ve eğitim hizmetleri sunmaktayız.

Güvenlik Yönetimi



www.guvenlikyonetimi.com

içindekiler



4 **BAŞKAN**

6 **EDİTÖR**

8 **GÜNCEL**

Sektör ile ilgili kısa haberler

18 **KÖŞE / Hayata Bakış**

KAPAK **GEÇİŞ KONTROL SİSTEMLERİ**

- 20 Modern Dünyanın Görünmeyen Güvenlik Katmanı
- 26 Geçiş Kontrol Sistemleri
- 28 Kurum ve tesislerde erişim güvenliği için Geçiş Kontrol Sistemleri

FOKUS **ENDÜSTRİYEL TESİS GÜVENLİĞİ**

- 30 Risk, Teknoloji ve İnsan Faktörü Ekseninde Endüstriyel Güvenlik
- 38 Endüstriyel Tesislerde İdeal Güvenliğin 8 Adımı
- 41 Endüstriyel Tesislerde Fiziksel Güvenlik Açıkları ve Alınabilecek Önlemler

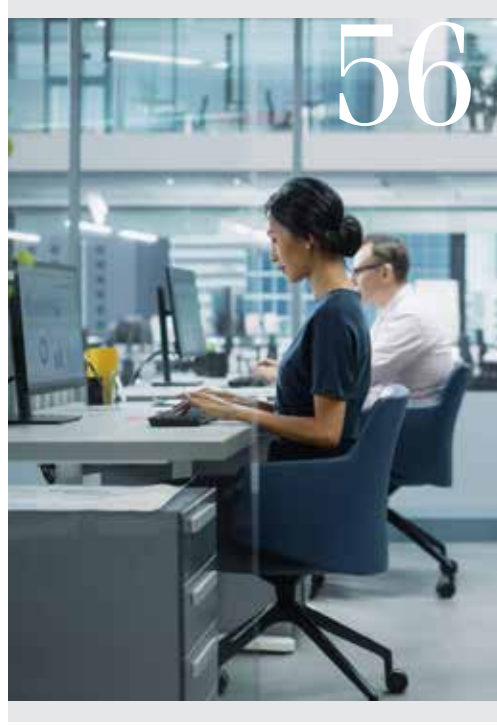
ÖZEL DOSYA **TOPLUMSAL DAVRANIŞ** **PSİKOLOJİSİ VE ÖZEL GÜVENLİK**

- 44 Kalabalıkların ruhunu anlamadan güvenliği yönetmek mümkün değildir

ELEKTRONİK GÜVENLİK

- 52 Geliştirilmiş 2. Nesil X Serisi Plus Kamera Tanıtıldı
- 54 Havalimanı Güvenliğinde Yeni Dönem: Akıllı Video Teknolojileri Operasyonların Merkezinde

NİSAN 2026



GÜVENLİK HİZMETİ

56 Özel güvenlik sektörünün geleceği insan odaklı yapay zekada

BİLGİ GÜVENLİĞİ

58 İşletmelerde Güvenli Yapay Zeka Kullanımı İçin Alınması Gereken 5 Kritik Önlem

60 QR kodları ne kadar güvenli?

62 Saldırganlar yayılma süresini yapay zekâ ile hızlandırıyor

64 Yapay zeka çağında teknik borç BT bilançolarının %40'ını oluşturuyor

66 2026'nın Yeni Siber Güvenlik Standartı XDR

68 Editoryal takvim

69 Reklam indeksi

Özel Güvenlik Federasyonu adına

İmtiyaz sahibi
O. Oryal ÜNVER

Yürütme Kurulu

O. Oryal ÜNVER
İsmail UZELLİ
Murat Köserisoğlu
Levent GÜLER
Alp SAUL

Genel Yayın Yönetmeni

Devrim BOZKURT
devrim@guvenlikyonetimi.com

Yazı İşleri

info@guvenlikyonetimi.com

Danışma Kurulu

Alp SAUL
Prof. Dr. Gazi UÇKUN
Deniz GÜRKAN
Engin ŞAHİN
Faruk DOĞAN
Hakan ÖZALP
İsmail UZELLİ
Murat Köserisoğlu
O. Oryal ÜNVER
Yusuf Ziya ÖNCEL

Görsel Yönetmen

Derya BOZKURT
derya@guvenlikyonetimi.com

Reklam Müdürü

Nazlı ÇATAK
info@guvenlikyonetimi.com

Yayın Türü

Yerel Süreli Yayın.
Ayda bir yayınlanır.

Yönetim Adresi

Arke Tanıtım Hizmetleri
Eyüpsultan - İstanbul
Tel: 0542 250 72 49
0533 413 78 08



Özel Güvenlik Sektörünün sesi Güvenlik Yönetimi Dergisi, sektörü bilgilendirme amacıyla hazırlanmıştır. Bu dergide yer alan her türlü haber, bilgi ve yorumlar; güvenilir olduğuna inanılan kaynaklar tarafından hazırlanmış araştırma raporları, değerlendirmeler, atıflar, çeviriler ve istatistikî verilerden derlenmiştir. Dergide yer alan tüm reklamların sorumluluğu firmalara, yazılardaki ve söyleşilerdeki görüşler sahibine aittir. Dergide yer alan yazılar izin alınmadan ve kaynak gösterilmeden hiçbir şekilde kullanılamaz.

Kritik Altyapıların Korunmasında Yeni Nesil Güvenlik Dönemi

Değerli okurlarımız;

Endüstriyel tesis güvenliği, yalnızca bina ve ekipmanların korunmasından ibaret değildir; aynı zamanda üretimin sürekliliğini, çalışanların emniyetini, çevre güvenliğini ve ülke ekonomisinin sürdürülebilirliğini doğrudan etkileyen stratejik bir unsurdur. Günümüzde enerji tesisleri, limanlar, fabrikalar, lojistik merkezleri, rafineriler ve organize sanayi bölgeleri; fiziksel tehditlerin yanı sıra siber saldırılar, sabotaj, iç tehditler, drone kullanımı ve kritik altyapılara yönelik hibrit risklerle karşı karşıya bulunmaktadır. Bu nedenle modern endüstriyel güvenlik anlayışı, yalnızca insan gücüne dayalı klasik koruma hizmetlerinden çok daha ileri bir yapıya dönüşmüştür.

Teknolojik gelişmeler, endüstriyel tesis güvenliğinde yeni bir dönemi başlatmıştır. Yapay zekâ destekli kamera sistemleri, termal görüntüleme teknolojileri, akıllı çevre güvenlik sistemleri, biyometrik geçiş kontrolü ve entegre alarm merkezleri sayesinde riskler daha oluşmadan tespit edilebilmektedir. Özellikle kritik tesislerde kullanılan siber güvenlik destekli video yönetim sistemleri, yalnızca görüntü kaydı yapmakla kalmayıp davranış analizi, izinsiz giriş algılama ve olağan dışı hareketlerin otomatik değerlendirilmesi gibi yetenekler de sunmaktadır. Ancak teknoloji ne kadar gelişirse gelişsin, eğitimli güvenlik personeli, doğru prosedürler ve güçlü kriz yönetimi olmadan etkin bir güvenlik yapısı oluşturmak mümkün değildir.

Geleceğin endüstriyel tesis güvenliği; kamu, özel sektör ve teknoloji üreticilerinin birlikte hareket ettiği bütünleşik bir güvenlik modeli üzerine kurulacaktır. Avrupa'da kritik altyapıların korunmasına yönelik geliştirilen yeni güvenlik standartları ve dayanıklılık politikaları, Türkiye açısından da önemli bir yol haritası oluşturmaktadır. Özellikle enerji, ulaşım, haberleşme ve üretim tesislerinde güvenliğin yalnızca maliyet unsuru değil, kurumsal sürdürülebilirliğin temel şartı olduğu artık açıkça görülmektedir. Bu nedenle endüstriyel tesis güvenliği, gelecekte şirketlerin rekabet gücünü belirleyen en önemli stratejik alanlardan biri olmaya devam edecektir.

Sağlıklı, güvenli ve mutlu yarınlar dileklerimle...



O. Oryal ÜNVER
ÖGF (Özel Güvenlik Federasyonu)
Yönetim Kurulu Başkanı

“Endüstriyel tesis güvenliği artık yalnızca kapı, duvar ve kamera sistemlerinden ibaret değildir. Enerji santrallerinden limanlara, fabrikalardan lojistik merkezlerine kadar kritik altyapılar; fiziksel saldırılar, siber tehditler, sabotaj, iç riskler ve hibrit güvenlik tehditleriyle karşı karşıya bulunmaktadır.”

Akıllı binalar için kalıcı çözümler...

Yangın ve CO Alarm Sistemleri
IP CCTV Sistemleri
Kartlı Giriş Kontrol Sistemleri
Acil Anons Sistemleri
HVAC Mekanik Otomasyon Sistemleri
Enerji Otomasyon Sistemleri
KNX Aydınlatma Otomasyon Sistemleri

Sistemler Arası Entegrasyon

Smart **Struxure**



Powered by
StruxureWare™ Building Operation

matriks

BİNA KONTROL SİSTEMLERİ

www.matrikstr.com



Anneler günü...

Anneler günü çoğu zaman birkaç çiçek, birkaç klişe cümle ve sosyal medya paylaşımının arkasına saklanan büyük bir ikiyüzlülük görüyorum. Çünkü bu ülkede ve dünyada kadın olmak hâlâ ciddi bir hayatta kalma meselesi. Anne olmak ise çoğu zaman kutsallık yüklenmiş ama gerçekte büyük yalnızlıklar, fedakârlıklar, bastırılmış öfkeler ve görünmeyen emeklerle örülmüş ağır bir rol. Kadınlar hâlâ şiddetin, tacizin, istismarın, ekonomik baskının ve psikolojik dayatmanın en büyük hedeflerinden biri. Üstelik bu tehdit çoğu zaman sokaktaki yabancından değil, en güvenli alan olan evin içinden geliyor. Kardeşinden, babasından, eşinden, sevgilisinden, kuzeninden... İnsan en çok en yakını tarafından incitiliyor. Zaten bu yüzden mesele sadece "suç" değil; kültür, aile, yetiştirilme biçimi ve kuşaktan kuşağa aktarılan toplumsal zihniyet meselesi.

OECD araştırma verilerine göre kadınların maruz kaldığı fiziksel ve cinsel şiddetin büyük bölümü yakın partnerler tarafından gerçekleştiriliyor. OECD'nin 2024 raporunda Türkiye'nin, partner şiddeti konusunda yüksek oranlara sahip ülkeler arasında olduğu açıkça ortada.

UN Women ve United Nations Office on Drugs and Crime tarafından yayımlanan femisid raporlarında da kadın cinayetlerinin büyük çoğunluğunun yakın partnerler ya da aile üyeleri tarafından işlendiği vurgulanıyor. Yani kadınlar çoğu zaman tanımadığı birileri tarafından değil; hayatına aldığı, güvendiği, aynı sofraya oturduğu insanlar tarafından öldürülüyor, istismar ediliyor. Türkiye'de çalışan Kadın Cinayetlerini Durduracağız Platformu verileri de yıllardır aynı şeyi gösteriyor: öldürülen kadınların çok büyük kısmı en yakınındaki erkekler tarafından öldürülüyor. Tartışma, boşanmak isteme, ayrılma talebi, kıskançlık, "itaat etmeme" gibi sebepler cinayet gerekçesi hâline getiriliyor. Çünkü bazı erkekler için kadın hâlâ birey değil; yönetilecek, sahip olunacak, kontrol edilecek bir varlık olarak görülüyor.

İşin en acı tarafı şu; toplum hala bunu bireysel sapkınlık gibi anlatmayı seviyor. Bir çocuğa daha doğduğu andan itibaren öğretilen şeyler var. Erkek çocuğa güç, hükmetme ve hak görme; kız çocuğa susma, katlanma ve idare etme öğretiliyor. Sonra yıllar geçiyor, o çocuklar büyüyor ve ortaya şiddeti normalleştiren yetişkinler çıkıyor.

İnsanın kişiliğinin temel taşları ilk yıllarda oluşuyor. Hayata geldiğimiz ilk yıllardan itibaren bakım verenlerle kurulan ilişkiler birer öncül. Şiddete yatkınlık, aşağılanma biçimi, sevgiyi algılama şekli, empati kurabilme kapasitesi, öfke kontrolü, suç eğilimi, değersizlik hissi... Yani anne-baba ilişkisi sadece bireysel değil, toplumsal sonuçlar da doğuruyor. Yıllarca kendi değersizleştirilmiş hayatını yaşayan kadın, bazen farkında olmadan aynı yaraları çocuğuna aktarıyor. Şiddet gören kadın bazen şiddeti normal sanıyor. Sevgisiz büyüyen biri sevgiyi öğretmiyor. Bastırılmış öfke kuşaktan kuşağa taşınıyor. Böylece toplum dediğimiz şey aslında biraz da aktarılmış travmaların toplamına dönüşüyor.

Anne olmak çok değerli. Çünkü bir insanın karakterine dokunan ilk yer çoğu zaman anne sesi oluyor. Ama anneliği putlaştırmanın da kimseye faydası yok. Çünkü "anne kutsaldır" deyip annelerin yaşadığı şiddeti, tükenmişliği, psikolojik baskıyı görmezden gelmek sadece romantik bir masal üretmekten başka bir şey değil. Gerçek sevgi; kusurları inkâr etmek değil, onları anlayıp dönüştürmeye çalışmakla mümkün olabilir.

Bir çocuğun ilk dünyası olan ev güvenli değilse, toplum da güvenli olmuyor. Çünkü insan bazen savaşmayı sokakta öğrenmiyor; evde öğreniyor. Ve insan bazen sevgisizliği ilk kez yabancılardan değil, en yakınlarından görüyor. Bu yaralı ilişkiyle başa çıkmak ve kendini değerli hissetmek, ego bütünlüğünü korumak için de farkında olmadan çeşitli patolojik sonuçlar ortaya çıkmasına sebep oluyor.

Bu yüzden bugün sadece "anneler kutsaldır" demek istemiyorum. Daha adil, daha vicdanlı, daha sağlıklı insanlar yetiştirebilen; sevgiyi korkudan ayırabilen; dokumanın, sevkatin, sarılmanın değerinin farkında olan, çocuğunu bir birey gibi büyütebilen bütün kadınların Anneliğini kutlamak istiyorum. Çünkü dünyayı gerçekten değiştiren şey bazen büyük ideolojiler değil; bir çocuğa öğretilen ilk merhamet oluyor.



Derya BOZKURT

“Daha adil, daha vicdanlı, daha sağlıklı insanlar yetiştirebilen; sevgiyi korkudan ayırabilen; dokumanın, sevkatin, sarılmanın değerinin farkında olan, çocuğunu bir birey gibi büyütebilen bütün kadınların Anneliğini kutlamak istiyorum.”



Gördüğünüze inanın, göremediğinizi ona bırakın



Stadyum, şehir meydanı, deniz ve hava limanı gibi büyük ve kalabalık alanlarda yüksek çözünürlüğe sahip **Avigilon H5 Pro** ile üst düzey izleme ve kayıt yapılabiliyor. Sahip olduğu ileri seviye çözünürlük sayesinde her detayın incelenebilmesine olanak veriyor.

- 61 MP'ye kadar çözünürlük
- Video analiz yeteneği
- Gece görüşü

Detaylı bilgi için bizimle iletişime geçin:
www.y3k.com.tr



Tepe Kurumsal, Global HR Summit 2026'da Dönüşüm Yolculuğunu Paylaşacak

Türkiye'nin entegre hizmet yönetimi alanındaki öncü şirketlerinden Tepe Kurumsal, insan kaynakları ve iş dünyasının önde gelen etkinliklerinden Global HR Summit 2026'da yer almaya hazırlanıyor.

12-13 Mayıs tarihlerinde İstanbul'da gerçekleştirilecek Global HR Summit 2026, iş dünyası, insan kaynakları ve teknoloji alanlarından çok sayıda yerli ve yabancı konuşmacıyı bir araya getirecek. Tepe Kurumsal İnsan ve Kültür Genel Müdür Yardımcısı (CHRO) Kaan Sak, etkinlik kapsamında düzenlenecek "İnsan, Kültürel Dönüşüm, Gelecek ve Yapay Zeka" başlıklı panelde konuşmacı olarak sahne alacak. Global HR Summit kapsamında gerçekleştirilecek panelde Kaan Sak;

büyük ölçekli organizasyonlarda kültürel dönüşümün yönetimi, çalışan deneyimi, liderlik yaklaşımı ve yapay zekanın insan kaynaklarındaki dönüştürücü etkisine ilişkin değerlendirmelerini paylaşacak.

Global HR Summit'in konforu Tepe Kurumsal'a emanet Tepe Kurumsal, etkinlikte aynı zamanda "Güvenlik ve Tesis Yönetim Sponsoru" olarak konumlanarak; güvenlik, temizlik ve yemek hizmetleri alanındaki entegre hizmet yaklaşımını sektör profesyonelleriyle buluşturacak. 33 binin üzerinde çalışanı ve güvenlikten tesis yönetimine, yemekten iş sağlığı ve güvenliğine kadar uzanan geniş hizmet yapısıyla Türkiye'nin en büyük istihdam güçlerinden biri olan



Tepe Kurumsal, son dönemde gerçekleştirdiği dönüşüm çalışmalarıyla dikkat çekiyor. Şirket, 6 farklı şirket yapısını tek bir insan ve kültür modeli altında birleştirirken; yapay zeka destekli işe alım sistemleri, veri odaklı insan kaynakları uygulamaları ve ortak kurum kültürü çalışmalarıyla geleceğin çalışma modeline yatırım yapıyor.

DASK'tan İstanbul'da Farkındalık Çalışması



Günlük hayatın yoğun akışı içinde milyonlarca İstanbulluya ulaşan Marmaray istasyonlarında hayata geçirilen kampanya kapsamında, deprem sigortasının önemi çarpıcı mesajlarla vatandaşlara hatırlatılıyor. 23 Nisan'da yaşanan depremin etkilerine dikkat çeken görsellerle, deprem gerçeğinin gündemde tutulması ve bireylerin

deprem ile ilgili olası risklere karşı hazırlıklı olmaları hedefleniyor.

Deprem Sigortanızı Yaptırdınız mı?

Kampanya kapsamında kullanılan mesajlarda vatandaşlara doğrudan bir soru yöneltiliyor: "Deprem sigortanızı yaptırdınız mı?" Bu güçlü ve sade çağrıyla, afet sonrasında finansal güvenceye sahip olmanın önemi vurgulanıyor.

23 Nisan 2025 tarihinde İstanbul'un Silivri ilçesi açıklarında meydana gelen 6,2 büyüklüğündeki deprem, Marmara Bölgesi'nde 7 şehirde hissedilmişti. Depremin hemen ardından DASK'a 10 bin 747 adet hasar ihbarı ulaşırken, süreç hızlı ve etkin bir şekilde yönetildi.

İhbarların ardından eksper görevlendirmeleri kısa sürede tamamlandı ve ilk tazminat ödemesi 24 saat içinde gerçekleştirildi. Yapılan değerlendirmeler sonucunda, poliçe kapsamına giren hasarlar için hak sahiplerine toplam 169 milyon TL tutarında tazminat ödemesi yapıldı.

Hazırlıklı Olmak Hayatı Değiştirir

Yaşanan bu deprem, Marmara Bölgesi'nde olası deprem riskini bir kez daha hatırlatırken, doğal afetlere karşı hazırlıklı olmanın önemini ortaya koydu. Deprem sigortası, yalnızca bir zorunluluk değil; afet sonrasında hayatın yeniden kurulabilmesi için kritik bir güvence niteliği taşıyor.

Para ve deęerli eřyalarınızın gvenlięine odaklanırken
maliyetinizi azaltıyor,
risklerinizi devralıyor,
zaman kaybınızı nlyoruz.

0212 603 03 70



www.loomis.com.tr



Managing **cash** in society.

Toplu Taşımada Kameralar Artık Karar Veriyor

Akıllı video teknolojileri, toplu taşıma sistemlerinde sadece güvenliği değil, operasyonel verimliliği ve yolcu deneyimini de dönüştürüyor. Artan yolcu yoğunluğu ve karmaşık operasyonel süreçler, toplu taşıma sistemlerinde daha akıllı ve entegre çözümleri zorunlu kılıyor. Axis Communications, geliştirdiği yapay zekâ destekli video gözetim çözümleriyle ulaşım operatörlerine hem güvenlik hem de iş zekâsı alanında yeni nesil imkanlar sunuyor. Günümüzde video gözetim sistemleri, pasif izleme araçlarının ötesine geçerek aktif birer karar destek mekanizmasına dönüşüyor. Kalabalık yoğunluğu analizi, anormal davranış tespiti ve gerçek zamanlı veri akışı sayesinde olası risklere hızlı ve proaktif müdahale

le mümkün hale geliyor. “Toplu taşıma sistemlerinde güvenlik artık sadece olayları izlemekle sınırlı değil. Yapay zekâ destekli video analitiği sayesinde operatörler, kalabalık yoğunluğunu anlık olarak analiz edebiliyor, potansiyel riskleri henüz oluşmadan tespit edebiliyor ve çok daha hızlı aksiyon alabiliyor,” diyor Axis Communications’tan Teknik Mühendis Hakan Kurt, sözlerine şöyle devam ediyor: “Bu teknolojiler aynı zamanda operasyonel verimliliği de ciddi şekilde artırıyor. Elde edilen verilerle yolcu akışını daha iyi yönetmek, gecikmeleri azaltmak ve kaynakları optimize etmek mümkün hale geliyor. Kısacası, video gözetim sistemleri artık sadece güvenlik değil, aynı za-



manda stratejik karar destek aracı olarak konumlanıyor.” Otobüslerden metro istasyonlarına, trenlerden terminallere kadar geniş bir kullanım alanına sahip bu çözümler; yolcu akışının optimize edilmesine, gecikmelerin azaltılmasına ve kaynakların daha verimli kullanılmasına katkı sağlıyor. Aynı zamanda elde edilen veriler, operatörlere daha stratejik ve sürdürülebilir kararlar alma imkânı sunuyor.

BLAZE Hibrit AI Video Yönetim Sistemi



Hanwha Vision, BLAZE VMS’nin tanıtımının ardından bugün, hibrit video yönetim platformunun kurulumunu ve işletimini basitleştirmek için özel olarak tasarlanmış yeni bir BLAZE cihaz serisini duyurdu. BLAZE VMS için optimize edilen bu cihazlar, kuruluşlara ölçeklenebilir video gözetim sistemlerini kurmanın ve kurulum karmaşıklığını ve devam eden sistem yönetimini

azaltmanın daha kolay bir yolunu sunuyor. BLAZE cihazları, video gözetim iş yükleri için optimize edilmiş, sıkıca entegre edilmiş donanım ve yazılım sunan BLAZE VMS platformunu çalıştırmak üzere özel olarak tasarlanmıştır. Kayıt, video yönetimi ve istemci işlemlerini tek bir sistemde birleştirerek, cihazlar modern video gözetim sistemlerini yönetmek için güvenilir bir temel sağlar. Her cihaz, işletim sistemi kurulumuna veya manuel yazılım yapılandırmasına gerek kalmadan, tamamen önceden yüklenmiş, önceden lisanslanmış ve kutudan çıkar çıkmaz çalışmaya hazır bir şekilde gelir. Bu akıcı yaklaşım, entegratörlerin sistemleri hızlı bir

şekilde çevrimiçi hale getirmelerine ve dağıtımlar arasında tutarlı yapılandırmaları sürdürmelerine olanak sağlar. Hanwha Vision’da Kıdemli Ürün Yöneticisi Seolhee Heo, “BLAZE cihazları, geleneksel olarak video yönetim sistemleriyle ilişkilendirilen operasyonel karmaşıklığın büyük bir kısmını ortadan kaldırmak üzere tasarlanmıştır,” dedi. “Sağlamlaştırılmış bir işletim sistemi ve tamamen önceden yapılandırılmış bir platform ile müşterilerin artık işletim sistemi bakımı, güvenlik yamaları veya özel BT denetimiyle uğraşmasına gerek kalmıyor; bu da onların altyapıyı korumak yerine gözetim sistemlerini çalıştırmaya odaklanmalarını sağlıyor.”



PRONET+

TÜM GÜVENLİK SİSTEMİNİ
TEK UYGULAMADAN YÖNETTİĞİN
EVİNE GÜVEN



444 1 911
pronet.com.tr

Siemens, Eigen Engineering Agent ile yapay zekayı fiziksel dünyaya taşıyor



Siemens, Hannover Messe'de, endüstriyel yapay zekayı yardımcıdan otonom uygulamaya taşıyan Eigen Engineering Agent'ı tanıttı. Eigen Engineering Agent, endüstriyel otomasyon mühendisliği görevlerini planlayabilen ve yürütebilen, piyasada bulunan ilk

yapay zeka sistemleri arasında yer alıyor. Sadece tavsiye üreten yapay zeka araçları ve copilotların aksine, Eigen Engineering Agent görevleri uçtan uca planlamak, yürütmek ve doğrulamak için gerçek mühendislik sistemleri içinde çalışıyor. Projelerini anlıyor, otomasyon kodu yazıyor, sistemleri yapılandırıyor ve önceden tanımlanmış performans ölçütleri karşılanana kadar yineleme yapıyor. Eigen Engineering Agent, tekrar eden görevleri otomatikleştirerek ve doğrulanmış, kullanıma hazır sonuçlar sunarak mühendislerin daha yüksek etki-

li, sistem düzeyindeki zorluklara odaklanmasına olanak tanıyor. Bu gelişme, mühendislik yeteneklerinin kıt olduğu ve üreticilerin pazara her zamankinden daha hızlı girme baskısıyla karşı karşıya kaldığı bir dönemde gerçekleşiyor. Eigen Engineering Agent, manuel iş akışlarından iki ila beş kat daha hızlı ve doğruluk veya güvenilirlikten ödün vermeyen bir hızda uygulama üretiyor. Verilen görevlerde, Eigen Engineering Agent yüzde 80'e kadar daha yüksek genel çözüm kalitesi ve yüzde 50 daha fazla mühendislik verimliliği sağlıyor.

Uzun süre sorunsuz çalışan sistemler zamanla rehavete yol açabiliyor

Kurumsal başarısızlıklar incelendiğinde sıkça tekrar eden bir örüntüye işaret eden ESET, uzun süre sorunsuz çalışan sistemlerin zamanla rehavete yol açtığını belirtti. Bu durum, hazırlık yatırımlarının azalmasına ve gerçek risk ile algılanan risk arasındaki farkın büyümesine neden oluyor. Görünürde bir saldırı yaşanmamış olması, çoğu zaman savunmanın güçlü olduğu anlamına gelmiyor; yalnızca tehditlerin henüz görünür hâle gelmemiş olabileceğine işaret ediyor. Birçok kuruluş, güvenlik durumunu değerlendirirken kritik bir yanılığa düşüyor. Kurumlar çoğu zaman ortamlarının güncel tehditlere karşı ne kadar güvenli olduğunu sorgulamak yerine,

yalnızca temel kontrollerin yerinde olup olmadığını kontrol ediyor. Bu da şirketlerin aynı anda hem uyumlu hem de risk altında olabileceği bir tablo ortaya çıkarıyor. Güvenlik değerlendirmelerinde bir diğer önemli sorun ise görünülebilirlik eğilimi. Kuruluşlar, kolay erişilebilen verilerle karar verirken daha zor elde edilen ancak kritik öneme sahip bilgileri göz ardı edebiliyor. Bu durum, güvenlik açıklarının fark edilmesini zorlaştırıyor ve eksik bir tabloya rağmen yanlış bir güven hissi oluşmasına neden oluyor. Verizon'un 2025 Veri İhlali Araştırma Raporu'na göre fidye yazılımı kurbanlarının yüzde 54'ünün erişim bilgileri, saldırıdan önce yasa dışı platformlarda zaten dolaşımdaydı. Bu da bazı ihlallerin,



fark edilmeden çok önce başlamış olabileceğini gösteriyor. ESET uzmanları, güvenlik sistemlerinin yalnızca kontrollerin varlığını doğrulamakla kalmaması gerektiğini, aynı zamanda şüpheli davranışları tespit edebilecek şekilde yapılandırılmasının önemine dikkat çekti. Özellikle saldırganların güvenlik süreçlerini devre dışı bırakma girişimlerinin izlenmesi, bu noktada kritik rol oynuyor.

Huzurlu bir yaşam arıyorsan ●●●



Daha fazla
bilgi için
QR kodu okutun.

Biz buradayız.



İgdaş Uluslararası İş Güvenliği Ödülünün Sahibi Oldu

İstanbul Büyükşehir Belediyesi (İBB) iştiraki İGDAŞ, iş sağlığı ve güvenliği alanındaki uygulamalarıyla uluslararası düzeyde önemli bir başarıya daha imza attı. Şirket, dünyanın saygın kuruluşlarından British Safety Council (BSC) tarafından düzenlenen 2025 International Safety Awards'da "Distinction" derecesiyle ödüllendirildi. İstanbul'un 39 ilçesinde 7 milyonu aşkın aboneye güvenli ve kesintisiz doğal gaz hizmeti sunan İGDAŞ, British Safety Council (BSC) 2025 değerlendirmelerinde çalışan sağlığı, güvenliği ve refahını öncelleyen yaklaşımıyla öne çıktı. İş sağlığı ve güvenliği yönetimi, risklerin önlenmesi, çalışan refahı ve kurumsal uygulamaların etkinliği gibi başlıklarda yapılan kapsam-

lı değerlendirmeler sonucunda 49/50 puan elde eden İGDAŞ, bu alandaki yüksek performansını uluslararası ölçekte tescilledi. "Distinction" derecesiyle ödüllendirilen bu başarı, kurumun güvenli çalışma ortamı oluşturma, riskleri proaktif biçimde yönetme ve kalıcı bir güvenlik anlayışı geliştirme konularındaki güçlü ve planlı yaklaşımını ortaya koydu.

Bu başarı aynı zamanda İGDAŞ'ın sahadaki operasyonları, hizmet sürekliliği ve güvenli altyapı anlayışında benimsediği yüksek standartların uluslararası düzeyde takdir edildiğini de göstermiş oldu.

"İş Sağlığı ve Güvenliği Kurum Kültürümüzün Temelini Oluşturuyor" İGDAŞ Genel Müdürü Nihat Narin konuya ilişkin değerlendirmesinde



şu ifadelerle yer verdi: "Çalışanlarımızın sağlığı ve güvenliği, tüm faaliyetlerimizin temelini oluşturuyor. Bu yaklaşımın uluslararası itibara sahip bir kuruluş tarafından 'Distinction' derecesiyle ödüllendirilmesi bizim için son derece kıymetli. Elde edilen bu başarı, kurum kültürümüzün, önleyici yaklaşımımızın ve sürekli gelişim anlayışımızın somut bir yansıması. Emeği geçen tüm çalışma arkadaşlarımıza teşekkür ediyorum.

Loomis, Mega Organizasyonların Güvenli Finansal Altyapısında Kritik Rol Üstleniyor



Geçtiğimiz ay gerçekleştirilen Coachella 2026, mega etkinliklerin yarattığı büyük ekonomik etkiyi yeniden gündeme taşıdı. Artık yalnızca bir müzik festivali olmanın ötesine geçen bu tür organizasyonlar; yerel topluluklardan küresel ekonomiye kadar uzanan güçlü

bir ekonomik motor olarak dikkat çekiyor. Tarihsel veriler, bu ölçekteki etkinliklerin bölgesel ekonomilere her yıl yüz milyonlarca dolarlık katkı sağladığını ortaya koyuyor. Örneğin, California'nın canlı eğlence sektörü tek başına yılda 700 milyon doların üzerinde ekonomik hacim yaratıyor. Bu süreçte oteller doluluk oranlarını artırıyor, yerel hizmet sektörleri canlanıyor ve binlerce kişiye geçici istihdam sağlanıyor. Tüm bunlar, canlı eğlence sektörünün bölgesel ekonomik büyüme üzerindeki kritik rolünü açık biçimde gösteriyor. Mega etkinliklerin etkisi yalnızca doğrudan yerel gelirlerle sınırlı kalmıyor. Dünyanın önde gelen

organizasyonları, oluşturdukları yüz milyonlarca dolarlık medya etkisi sayesinde düzenledikleri bölgeleri küresel ölçekte görünür hale getirirken, aynı zamanda uluslararası trendleri de şekillendiriyor. Loomis ise bu ölçekteki organizasyonları destekleyen ekosistemde kritik bir rol üstleniyor. Şirket; yüksek hacimli nakit akışlarının güvenli ve verimli şekilde yönetilmesini sağlayarak operasyon süreçlerini optimize ediyor, riskleri azaltıyor ve fon erişiminin kesintisiz devam etmesine katkı sunuyor. Bu sayede mega etkinliklerin oluşturduğu güçlü ekonomik yapıların sorunsuz şekilde işlemesi desteklenirken, küresel ekonomik hareketliliğe de önemli katkı sağlanıyor.

Exit



Musical Fountain



boutique



**GÜVENLİK,
DETAYLARI GÖRME SANATIDIR!**



Detaylar için
QR kodu okutunuz.



Securitas Technology, 2026 Teknoloji Trendlerini Paylaştı



Güvenlik teknolojileri artık yalnızca anlık tehditlere müdahale eden sistemler olmaktan çıkarak; riskleri önceden analiz eden, veriyle öğrenen ve karar alma süreçlerini destekleyen akıllı yapılara dönüşüyor. Bu dönüşümün merkezinde ise yapay zekâ, bulut tabanlı çözümler ve gelişmiş sensör teknolojileri yer alıyor.

Securitas Technology, bugün gerçekleştirdiği basın buluşmasında 2026 yılına yön verecek güvenlik teknolojisi trendlerini ve yeni nesil çözümlerin sektöre etkilerini değerlendirdi. Etkinlik kapsamında basın mensupları, şirketin Dene-yim Merkezi'nde ayrılanarak farklı sektörlerle özel geliştirilen güvenlik senaryolarını yerinde inceleme fırsatı buldu. Entegre güvenlik teknolojilerinin gerçek kullanım örneklerinin aktarıldığı buluşmada; yapay zekâ destekli analiz sistemleri, bulut altyapıları ve akıllı sensör çözümleri-



nin operasyonel süreçlere sağladığı katkılar detaylı şekilde paylaşıldı. Toplantıda özellikle yeni nesil güvenlik sistemlerinin yalnızca güvenliği sağlamakla sınırlı kalmadığı; aynı zamanda operasyonel verimliliği artırdığı, iş sürekliliğini desteklediği ve kurumların daha hızlı karar almasına yardımcı olduğu vurgulandı. Yetkililer, güvenlik anlayışının giderek daha bağlantılı, veri odaklı ve proaktif bir yapıya evrildiğine dikkat çekerek; geleceğin güvenlik çözümlerinin insan, teknoloji ve veri entegrasyonu üzerine şekilleneceğini ifade etti.

Yapay zekâ destekli analiz teknolojileri sayesinde olası risklerin daha oluşmadan öngörülebildiği, bulut tabanlı sistemlerle merkezi yönetim ve uzaktan erişim imkânlarının genişlediği, gelişmiş sensör teknolojileriyle ise fiziksel güvenlik süreçlerinin daha hassas ve hızlı yönetilebildiği belirtildi. Securitas Technology'nin gerçekleştirdiği basın buluşması, güvenlik sektörünün geleceğinde teknolojinin oynayacağı kritik rolü bir kez daha ortaya koyarken; sektör profesyonelleri için de yeni nesil güvenlik yaklaşımına dair önemli bir vizyon sundu.

Siemens Türkiye, 170. Yılına Sanat ve Kültürle Kutladı



Siemens Türkiye, Türkiye'deki 170. yılını Atatürk Kültür Merkezi'nde düzenlenen özel bir etkinlikte kutladı. Teknoloji, sanat ve kültürü bir araya getiren gece; şirketin Türkiye'deki köklü geçmişine ve geleceğe yönelik vizyonuna dikkat çekti. Kutlama programı kapsamında ilk olarak "170 Yıldır Zamanın Ötesinde" sergisi ziyaretçilerle buluştu. Ardından, İstanbul Devlet Opera ve Balesi iş birliğiyle düzenlenen Gençlik Konseri'nde, Siemens Türkiye Opera Yarışması'nda geçmiş yıllarda ödül alan sanatçılar sahne aldı. Etkinlikte, Türkiye'den yetişen genç yeteneklerin uluslararası sanat sahnesinde daha güçlü şekilde yer alabilmesi için kültür ve sanat alanındaki destek çalışmalarının sürdürüleceği vurgulandı. Şirketin, genç sanatçıların gelişimine katkı sağlayan projeleri öncelikli alanlardan biri olarak değerlendirdiği ifade edildi. Gecede orkestrayı, Siemens Arts Program Direktörü Prof. Dr. Stephan Frucht yönetti. Etkinliğin ev sahipliğini üstlenen Caner Akgün'e de teşekkür edildi. Siemens Türkiye'nin 170. yıl kutlaması, şirketin yalnızca teknoloji alanındaki yatırımlarını değil; aynı zamanda sanat, kültür ve genç yeteneklerin gelişimine verdiği desteği de ön plana çıkaran özel bir buluşma olarak dikkat çekti.

TEPE
GÜVENLİK

TEPE'DE
YENİ DÖNEM



TEPE
KURUMSAL



444 15 98
tepekurumsal.com.tr

“Etkili liderlik”

Kişisel bütünlük, kişisel sorumluluk ve yaşam amacının ufkundaki aydınlık geleceğimizi oluşturur. Kişisel bütünlük kişisel sorumlulukla beslenir. Böylece siz kararlı ve eyleme dönük bir kişi olmak istediğinizde, kişisel bütünlüğünüz yaşam amacınızı canlı tutar.

Amacınıza dayalı sorumlu bir yaşam sürdürdükçe bilgeliğiniz de artar. Kişisel bütünlüğü kendinizde ve birlikte çalıştığınız kişilerde arayın. Kişisel ve mesleki ilişkilerinizin güven temeline dayanmasını sağlayan unsurlar, karşılıklı saygı ve kişisel bütünlüktür. Kişisel bütünlüğünüz, anne-baba, yönetici, satış elemanı, lider, iş sahibi, işçi, eş veya öğretmen olarak “ya da başka bir işte” ne kadar etkili olacağınızı belirler. Kişisel bütünlüğünüz, elde edeceğiniz gerçek başarının ölçüsüdür.

Her toplumda, kargaşanın başlıca nedenlerinden birisi, politik ve ekonomik alandaki liderlerin kişisel bütünlüklerinin olmamasıdır. Biz kişisel bütünlüğe sahip liderler istiyoruz, önemli pozisyonlarda kişisel sorumluluğa sahip insanların bulunması gerekir. Hükümetlerde, işletmelerde, ailelerde ve diğer kurumlarda bu tür liderlere gereksinim vardır. Liderliğin iyi olmasını engelleyen unsurlar; etkisiz liderler de, etkili liderlerin önüne çıkan engellerle karşılaşılır. Etkili liderler, azim ve yaratıcılıkla engelleri nasıl aşacaklarını öğrenirler. Etkisiz liderlerin etkili olabilmeleri için, eylemlerinin sorumluluğunu üstlenmeyi öğrenmeleri gerekir. Bu kişiler genelde, toplumun içi boş olan başarı tanımına denk düşmeme korkusu yaşarlar. Bu korku, kişisel bütünlüklerini tehlikeye atar. Bir hedefe ulaşmak için başkalarını ezebilir ya da ilişkilerinde yalana dolana sapabilirler. Korkuları, davranışlarının sonuçlarının sorumluluğunu inkâr etmelerine yol açabilir. Yaptıklarının yanlış olduğunun bilinciyle, cezalandırılmaktan hatta işlerini kaybetmekten kaçınıyor olabilirler. Bu da, kişiliklerinin iç yüzünün anlaşılması korkusuyla hareket etmelerine yol açabilir. Ayrıca sorumluluktan kaçarlar ve korkularıyla hareket ederlerse alacakları sonuçlar da hiç iç açıcı olmaz ve bu sonuçlar onları tatmin etmez.

Anne ve babaları düşündüren şey, tutarlı ve etkili bir disiplin kurmaktan çok, çocuklarının kendilerini beğenmesi ve kendilerine itaat etmesidir. Çocuklar, disiplin olmadan nasıl kişisel sorumluluğa dayanan alışkanlıklar kazanacaklar ve ileride kişisel bütünlüğe sahip yetişkinler olacaklardır? Bir anne veya baba olarak, sözleriniz ve davranışlarınızda tutarlı değilseniz, çocuğunuzun saygısını nasıl kazanırsınız?

Aynı durum yönetici ve liderler için de geçerlidir. İnsanların kendilerini beğenmesine odaklananlar, genelde zayıf, etkisiz ve tutarsız birer insan olurlar. Bir yönetici veya lider olarak, sözleriniz ve davranışlarınızda tutarlı değilseniz, çalışanlarınızın ya da liderlik yaptığımız kişilerin saygısını nasıl kazanırsınız? “Kişisel bütünlük, etkili liderliğin anahtarıdır”. Güven kişisel bütünlükle yaşayan kişiye, başkaları tarafından verilen bir armağandır.

Başarabilmemiz dileği ile...



Oğuz GÜLAY

“Her toplumda, kargaşanın başlıca nedenlerinden birisi, politik ve ekonomik alandaki liderlerin kişisel bütünlüklerinin olmamasıdır.”

Değişimi birlikte
yakalayalım...



Creative
Çözümler

Logo
Amblem
Tasarım

Kurumsal
Kimlik
Tasarımı

Katalog,
Broşür
Tasarımı

Ambalaj
Tasarımı

Basın İlanı
Tasarımı

Broşür
ve Insert

Baskı
Çözümleri

Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ

Gündem

Perpa Sanayi ve Ticaret Alanı
Genel Yönetim Binası

ARKHE TANITIM HİZMETLERİ

Perpa Ticaret Merkezi B Blok
Kat:6 No:672
Okmeydanı / Şişli / İstanbul

Tel : (212) 210 54 45

www.guvenlikyonetimi.com

arkhe
tanıtım hizmetleri

Modern Dünyanın Görünmeyen Güvenlik Katmanı

Geçiş kontrol sistemleri, modern güvenlik teknolojilerinin temel yapı taşlarından biridir. İnsanların, araçların veya belirli nesnelerin kontrollü alanlara giriş-çıkışını düzenlemek amacıyla kullanılır. Teknolojinin gelişmesiyle birlikte bu sistemler yalnızca kapı açma mekanizması olmaktan çıkmış; veri analizi, personel yönetimi, biyometrik doğrulama ve yapay zekâ destekli güvenlik altyapılarının parçası hâline gelmiştir.



Günümüzde apartmanlardan devlet kurumlarına, fabrikalardan havaalanlarına kadar hemen her alanda farklı türleri kullanılmaktadır. Teknolojinin gelişmesiyle birlikte bu sistemler yalnızca kapı açma mekanizması olmaktan çıkmış; veri analizi, personel yönetimi, biyometrik doğrulama ve yapay zekâ destekli güvenlik altyapılarının parçası hâline gelmiştir.

Kimlik, Güvenlik ve Kontrolün Dijitalleşmesi

Modern şehir yaşamı görünenden çok daha fazla kontrol mekanizması üzerine kuruludur. Bir apartmanın kapısından geçerken okutulan kart, iş yerindeki turnike, havaalanında yüzümüzü tarayan kameralar ya da otopark girişinde otomatik açılan bariyerler... Günlük yaşamın sıradan parçaları gibi görünen bu sistemler aslında devasa bir güvenlik ve veri yönetimi ağının parçalarıdır. “Geçiş kontrol sistemi” adı verilen bu teknolojiler, yalnızca bir kapının açılıp kapanmasını sağlamaz; aynı zamanda kimin, ne zaman, hangi alana erişebileceğini belirleyen dijital otoriteyi temsil eder. Özellikle 21. yüzyılda artan kentleşme, nüfus yoğunluğu, güvenlik kaygıları ve dijitalleşme ihtiyacı, geçiş kontrol sistemlerini hayatın merkezine yerleştirmiştir. Bugün bir fabrikanın üretim hattından devlet kurumlarına, üniversitelerden akıllı sitelere kadar neredeyse her yerde farklı türleri kullanılmaktadır.

Geçiş kontrol sistemlerinin temel mantığı oldukça basittir: Kimlik doğrulama, yetki denetimi ve kayıt tutma. Ancak bu basit görünen mekanizma, arkasında çok katmanlı yazılımlar, veri tabanları, sensörler ve bazen yapay zekâ destekli analiz sistemleri barındırır. Bir kişi kartını okuttuğunda sistem yalnızca “kapıyı aç” komutu vermez. Aynı anda şu soruların cevabını da kontrol eder: Dolayısıyla modern geçiş kontrolü, fiziksel güvenlikle dijital veri yönetiminin birleşim noktası hâline gelmiştir.

Kartlı Sistemlerin Yükselişi

Geçiş kontrol teknolojilerinin en yaygın ve uzun yıllardır kullanılan türü kartlı sistemlerdir. Özellikle şirketlerde, okullarda ve toplu yaşam alanlarında bu sistemlere rastlamak mümkündür. İnsanların cebinde taşıdığı küçük plastik kartlar aslında görünenden çok daha fazla işlev taşır. İlk dönemlerde kullanılan manyetik kartlar, banka kartlarının eski versiyonlarına benzeyen bir yapıdaydı. Kart üzerindeki manyetik şerit, kullanıcının bilgilerini taşıyordu. Ancak bu sistemler zamanla güvenlik açıkları nedeniyle yetersiz kaldı. Kartların kolay bozulması, kopyalanabilmesi ve fiziksel temas gerektirmesi büyük dezavantaj yarattı. Bunun yerini zamanla RFID teknolojisi aldı. Radyo frekansı ile çalışan bu sistemlerde kartın okuyucuya temas etmesi gerekmez. Kullanıcı kartı yalnızca yaklaştırır ve sistem bilgisiyi algılar.

“Modern geçiş kontrolü, fiziksel güvenlikle dijital veri yönetiminin birleşim noktası hâline gelmiştir.

Günümüzde metro geçişlerinden şirket girişlerine kadar çok geniş bir alanda kullanılan sistem budur.

Kartlı sistemlerin yaygınlaşmasının en önemli nedeni düşük maliyet ve kolay yönetimidir. Binlerce personelin giriş çıkışı merkezi bir yazılımla kontrol edilebilir. Ayrıca çalışanların hangi saatlerde giriş yaptığı, hangi alanlarda bulunduğu ve ne kadar süre içeride kaldığı kayıt altına alınabilir.

Ancak kartlı sistemlerin ciddi bir zayıf noktası vardır: Kart kişinin kendisi değildir. Kart kaybolabilir, çalınabilir ya da başka birine verilebilir. Bu nedenle yüksek güvenlik gerektiren alanlarda tek başına yeterli görülmez. Tam da bu noktada biyometrik sistemler devreye girmiştir.

İnsan Bedeni Bir Şifreye Dönüştüğünde

Biyometrik geçiş kontrol sistemleri, teknolojinin insan bedenini dijital bir kimliğe dönüştürdüğü alanlardan biridir. Parmak izi, yüz yapısı, göz retinası hatta yürüyüş biçimi bile artık birer güvenlik verisi olarak kullanılabilir.



En yaygın biyometrik yöntem parmak izi sistemleridir. Parmak üzerindeki çizgilerin ve kıvrımların her insanda farklı olması, bunu güçlü bir doğrulama yöntemi hâline getirir. Özellikle personel takibi gereken işletmelerde uzun yıllardır kullanılmaktadır. Parmak izi sistemleri ilk ortaya çıktığında büyük ölçüde “kesin güvenlik” algısı oluşturmuştu. Çünkü bir kart unutulabilir ya da paylaşılabilir; ancak kişinin parmağını başka birine vermesi mümkün değildir. Fakat zamanla bu sistemlerin de sınırsız olmadığı görüldü. Fiziksel deformasyonlar, kirli yüzeyler, kesikler veya yaşlanma gibi durumlar okumayı zorlaştırabiliyordu.

Daha sonra yüz tanıma teknolojileri hızla gelişmeye başladı. Özellikle yapay zekâ ve yüksek çözünürlüklü kamera sistemlerinin gelişmesiyle birlikte yüz tanıma sistemleri yalnızca güvenlik noktalarında değil, gündelik yaşamın birçok alanında kullanılmaya başlandı.

Bir yüz tanıma sistemi; gözler arası mesafe, çene hattı, burun

yapısı, kemik oranları gibi onlarca farklı biyometrik veriyi analiz eder. Modern sistemler artık kişinin yalnızca fotoğrafını değil, canlı olup olmadığını da anlayabilmektedir. Böylece sahte fotoğraflarla sistemi kandırma girişimleri azaltılmıştır. Ancak biyometrik teknolojilerin yaygınlaşması yalnızca teknik bir mesele değildir. Aynı zamanda ciddi etik tartışmaları da beraberinde getirmiştir. Çünkü artık insanların bedenleri, dijital veri tabanlarının bir parçası hâline gelmiştir. Bu durum özellikle mahremiyet, kişisel veri güvenliği ve sürekli gözetim tartışmalarını büyütmektedir. Bugün dünyanın birçok ülkesinde yüz tanıma teknolojileri hukuki tartışmaların merkezindedir. Bazı şehirlerde kamusal alanlarda kullanımına sınırlamalar getirilmiş, bazı ülkelerde ise devlet güvenliği gerekçesiyle yaygınlaştırılmıştır.

Geçiş kontrol sistemleri tam da bu nedenle yalnızca teknik altyapılar değil; aynı zamanda sosyolojik, politik ve etik meselelerdir.

Çünkü bir kapının kimlere açıldığı kadar, kimlere kapanacağı da toplumsal güç ilişkileriyle doğrudan bağlantılıdır.

1. Kartlı Geçiş Kontrol Sistemleri

Kartlı geçiş sistemleri, kişilere verilen elektronik kartlar aracılığıyla çalışan güvenlik sistemleridir. Kullanıcı kartını okuyucuya yaklaştırdığında sistem kartın yetkisini kontrol eder ve uygun ise geçişi izin verir.

En yaygın kullanılan geçiş kontrol türüdür.

Çalışma Mantığı

Sistem temel olarak üç parçadan oluşur:

- ▮ Kart
 - ▮ Kart okuyucu
 - ▮ Merkezi kontrol yazılımı
- Kart içindeki kimlik bilgisi okuyucu tarafından algılanır. Bu bilgi veri tabanındaki kayıtlarla karşılaştırılır. Kullanıcının yetkisi varsa kapı, turnike veya bariyer açılır.

Kart Türleri

Manyetik Kartlar

Eski sistemlerde kullanılmıştır. Kart üzerindeki manyetik şerit veri taşır.

Dezavantajları:

- ▮ Kolay bozulur
 - ▮ Kopyalanabilir
 - ▮ Fiziksel temas gerekir
 - ▮ RFID Kartlar
- Günümüzde en yaygın sistemdir.

Kart okuyucuya temas etmeden çalışır. Radyo frekansı teknolojisi kullanılır.

**ViYA ;
MOBOTIX C71 ile Yapay
Zeka Destekli 7/24 Akıllı
Hasta Bakıcı**

- ✓ **Düşme Algılama** –
Anında tespit, hızlı
müdahale
 - ✓ **Gün Boyu Gerçek
Zamanlı Destek** –
Kesintisiz takip, maksimum
güvenlik
 - ✓ **MOBOTIX HUB ile
Sorunsuz Entegrasyon** –
Mevcut sistemlere
zahmetsiz uyum
- ViYA ile hasta bakımında
yeni bir çağ başlatın!**



ViYA; Yapay Zeka Destekli 7/24 Akıllı Hasta Bakıcı Sistemi

- **360° Kesintisiz Takip** – Her açıdan tam kontrol, eksiksiz hasta gözetimi
- **GDPR Uyumlu Gizlilik** – Güvenli ve etik veri koruma standartları
- **Gelişmiş İzleme Lisansı** – Profesyonel ve yüksek hassasiyetli izleme teknolojisi
- **Kolay Entegrasyon** – Mevcut sistemlerle zahmetsiz uyum
- **Yüksek Güvenlik & Erken Müdahale** – Riskleri önceden tespit eden akıllı analizler
- **Bakım Personeline Destek** – İş yükünü azaltan verimli asistan
- **Maksimum Esneklik** – Farklı bakım ortamlarına kolay uyum
- **Dayanıklılık & Maliyet Verimliliği** – Uzun ömürlü, ekonomik çözüm

ViYA ile geleceğin hasta bakımını bugünden deneyimleyin!

Uluslararası Kabul Edilmiş Sertifikalar



Hocapaşa Mah. Nöbethane Cad.
No:19 Fatih - İstanbul
Tel: +90 532 767 0444
90 532 211 3038
E-mail: info@viyagroup.net
haterettin@viyagroup.net

Alev oluşmadan önce
yangınları tesbit edin.

“ Bir yüz tanıma sistemi; gözler arası mesafe, çene hattı, burun yapısı, kemik oranları gibi onlarca farklı biyometrik veriyi analiz eder.

Avantajları:

- ▶ Hızlı kullanım
- ▶ Dayanıklılık
- ▶ Temassız çalışma
- ▶ Uzun ömür
- ▶ Akıllı Kartlar

İçerisinde mikroçip bulunur.

Sadece kimlik doğrulama değil:

- ▶ Personel bilgileri
- ▶ Ödeme sistemi
- ▶ Yemekhane erişimi
- ▶ Asansör yetkileri gibi işlemler de yapılabilir.

Kullanım Alanları

- ▶ Şirketler
- ▶ Üniversiteler
- ▶ Hastaneler
- ▶ Siteler
- ▶ Oteller
- ▶ Kamu kurumları
- ▶ Avantajları
- ▶ Düşük maliyet
- ▶ Kolay yönetim
- ▶ Hızlı geçiş
- ▶ Yetkilendirme kolaylığı
- ▶ Dezavantajları
- ▶ Kart kaybolabilir
- ▶ Başkasına verilebilir
- ▶ Kopyalama riski vardır

Bu nedenle kritik alanlarda tek başına yeterli görülmez.

2. Biyometrik Geçiş Kontrol Sistemleri

Biyometrik sistemler, kişinin fiziksel veya davranışsal özelliklerini kullanarak kimlik doğrulaması yapan sistemlerdir. “Şifreyi bilen” değil, “kişinin kendisi” doğrulanır.

Parmak İzi Sistemleri

En yaygın biyometrik sistemdir. Parmak üzerindeki çizgiler, kıvrımlar, noktalar dijital olarak analiz edilir.

Avantajları

- ▶ Kopyalanması zordur
- ▶ Kart taşıma gerekmez
- ▶ Personel takibinde etkilidir

Dezavantajları

- ▶ Parmakta yara olması problemi yaratabilir
- ▶ Kirli eller okumayı zorlaştırabilir
- ▶ Hijyen tartışmaları oluşabilir
- ▶ Yüz Tanıma Sistemleri

Kameralar aracılığıyla çalışır.

Sistem göz mesafesi, çene yapısı, yüz oranları, kemik yapısı gibi biyometrik verileri analiz eder. Yapay zekâ ile birlikte kullanım oranı hızla artmıştır.

Kullanım Alanları

- ▶ Havalimanları
- ▶ Sınır güvenliği
- ▶ Akıllı şehir sistemleri
- ▶ Plaza girişleri
- ▶ Avantajları
- ▶ Temassız kullanım
- ▶ Hızlı geçiş
- ▶ Uzaktan doğrulama

Dezavantajları

Aydınlatma sorunları etkileyebilir
Maske veya gözlük hata oluşturabilir
Mahremiyet tartışmaları yaratır.

- ▶ Retina ve İris Tanıma
- ▶ Gözün damar yapısı veya iris tabakası analiz edilir.
- ▶ Çok yüksek güvenlik sağlar.

Kullanım Alanları

- ▶ Askerî tesisler
- ▶ Veri merkezleri
- ▶ Laboratuvarlar
- ▶ Gizli devlet kurumları

Dezavantajları

- ▶ Yüksek maliyet
- ▶ Karmaşık kurulum
- ▶ Kullanıcı açısından rahatsız edici olabilir

3. Şifre ve PIN Tabanlı Sistemler

Kullanıcının belirli bir kod girerek giriş yaptığı sistemlerdir. ATM mantığına benzer şekilde çalışır.

Çalışma Sistemi

Kullanıcı keypad, dokunmatik panel, dijital ekran üzerinden şifreyi girer. Doğruysa geçiş sağlanır.

Avantajları

- ▶ Ucuzdur
- ▶ Kurulumu kolaydır
- ▶ Küçük işletmeler için uygundur

Dezavantajları

- ▶ Şifre paylaşılabilir
 - ▶ Omuz üzerinden izlenebilir
 - ▶ Unutulabilir
- Bu yüzden günümüzde genellikle başka sistemlerle birlikte kullanılır.



4. Mobil Geçiř Sistemleri

Akıllı telefon üzerinden çalışan modern geçiř sistemleridir. Telefon, dijital anahtar, QR kod, NFC kimlięi, Bluetooth doęrulasması olarak kullanılır.

Teknolojileri

- ▮ NFC: Telefon kısa mesafede okuyucu ile iletiřim kurar.
- ▮ Bluetooth Low Energy (BLE) Yaklařınca otomatik kapı açılabilir.
- ▮ QR Kod: Kamera üzerinden doęrulama yapılır.

Avantajları

- ▮ Kart taşıma gerektirmez
- ▮ Uzaktan yetki verilebilir
- ▮ Yazılım güncellemesi kolaydır

Dezavantajları

- ▮ Telefon bataryasına baęımlıdır
- ▮ Siber saldırı riski tařır
- ▮ Telefon çalınırsa risk oluşabilir

5. Turnike ve Bariyer Sistemleri

Geçiř kontrolünün fiziksel engelleyici sistemlerle desteklenmiř hâlidir.

Yalnızca doęrulama deęil, fiziksel sınırlama da saęlar.

Turnike Sistemleri

İnsan geçiřini kontrol eder.

- ▮ Bel turnikesi
 - ▮ Boy turnikesi
 - ▮ Hızlı geçiř turnikeleri
 - ▮ VIP cam turnikeler
 - ▮ Bariyer Sistemleri
- Araç giriř-çıkıřını kontrol eder. Çoęunlukla site giriřlerinde, otoparklarda, güvenlik noktalarında kullanılır.

Plaka Tanıma Sistemleri

- ▮ Kamera aracılıęıyla araç plakası okunur.
- ▮ Yetkili araç ise bariyer açılır.
- ▮ Yapay zekâ destekli sistemlerde araç tipi, renk, hız, sürüř davranıřı gibi analizler de yapılabilir.

6. Bulut Tabanlı Geçiř Kontrol Sistemleri

Sistemin internet üzerinden merkezi sunucularla yönetildięi modern altyapıdır. Tüm kontrol uzaktan yapılabilir.

Özellikleri

- ▮ Mobil yönetim
- ▮ Gerçek zamanlı takip
- ▮ Uzaktan yetkilendirme
- ▮ Çok řubeli yönetim

“ Geçiř kontrol sistemleri tam da bu nedenle yalnızca teknik altyapılar deęil; aynı zamanda sosyolojik, politik ve etik meselelerdir.

Avantajları

- ▮ Fiziksel sunucu ihtiyacı azdır
- ▮ Güncelleme kolaydır
- ▮ Merkezi yönetim saęlar

Dezavantajları

- ▮ İnternet baęımlılıęı
- ▮ Veri güvenlięi riskleri
- ▮ Siber saldırı ihtimali

7. Yapay Zekâ Destekli Geçiř Sistemleri

Yeni nesil güvenlik sistemleridir. Sadece kimlik doęrulamaz; kiřinin davranıřlarını da analiz eder.

Özellikleri

- ▮ řüpheli hareket analizi
- ▮ Kalabalık yoęunluk tespiti
- ▮ Yüz davranıřı inceleme
- ▮ Risk puanlama
- ▮ Anormal hareket algılama

Kullanım Alanları

- ▮ Akıllı řehirler
 - ▮ Havaalanları
 - ▮ Kritik devlet tesisleri
 - ▮ Büyük organizasyonlar
 - ▮ Tartıřmalar
- Bu sistemler mahremiyet, kiřisel veri güvenlięi, sürekli izleme, dijital gözetim konularında etik tartıřmalar yaratmaktadır.

Geçiş Kontrol Sistemleri

Geçiş kontrol sistemi, belirli bir alana erişimi sağlamak veya sınırlandırmak amacıyla kullanılan teknolojik çözümler bütünüdür. Bu sistemler, güvenliği sağlamak, yetkilendirme yapmak ve veri koruması sağlamak amacıyla kullanılır.

ASSA ABLOY



Geçiş kontrol sistemi, belirli bir alana erişimi sağlamak veya sınırlandırmak amacıyla kullanılan teknolojik çözümler bütünüdür. Bu sistemler, güvenliği sağlamak, yetkilendirme yapmak ve veri koruması sağlamak amacıyla kullanılır. Aşağıda, bu sistemlerin temel bileşenleri ve işlevleri hakkında kısa bilgiler bulabilirsiniz.

Geçiş Kontrol Sistemleri Bileşenleri

Kartlı Geçiş Sistemleri

Kartlı geçiş sistemleri, güvenli giriş ve çıkış sağlamak için kullanılır. İki temel türü vardır:

Manyetik Bant Kartları: Kartın üzerindeki manyetik şerit, okuyucu tarafından taranarak erişim sağlanır. Günümüzde daha güvenli sistemlerle değiştirilmiş olsa da bazı alanlarda hala kullanılmaktadır.

RFID Kartları: Radyo frekansı ile iletişim kurarak geçiş sağlar. Kart, okuyucuya yaklaştırıldığında erişim bilgileri aktarılır. Manyetik

bant kartlarına göre daha güvenlidir ve veri saklama kapasitesi daha yüksektir.

Parmak İzi Tanıma Sistemleri

Parmak izi tanıma sistemleri, bireyin benzersiz parmak izi desenini kullanarak kimlik doğrulaması yapar. İki tür tarayıcı yaygındır:

Optik Tarayıcılar: Parmak izinin optik görüntüsünü alır ve kimlik doğrulaması yapar.

Kapasitif Tarayıcılar: Parmak izinin elektriksel özelliklerini ölçerek doğrulama yapar.

Yüz Tanıma Sistemleri

Yüz tanıma teknolojisi, bireyin yüzündeki belirli özellikleri analiz ederek kimlik doğrulaması yapar:

2D Yüz Tanıma: Yüzün iki boyutlu görüntüsünü kullanır.

3D Yüz Tanıma: Yüzün üç boyutlu yapısını analiz eder ve daha yüksek doğruluk sağlar.

İris Tanıma Sistemleri

İris tanıma sistemleri, gözün iris desenini tarayarak kimlik doğrulaması yapar. Bu sistemler, güvenliği sağlamak için hassas ve benzersiz bir biyometrik yöntem sunar.

Ses Tanıma Sistemleri

Ses tanıma sistemleri, kullanıcının ses özelliklerini analiz ederek kimlik doğrulaması yapar. Bu sistemler, güvenli geçiş için sesli komutları kullanır.

Anahtar ve Kilit Sistemleri

Fiziksel anahtar ve kilit sistem-

leri, geçiş kontrolünün en basit formunu oluşturur. Bu sistemler elektronik veya mekanik olabilir:

Mekanik Anahtarlar: Geleneksel fiziksel anahtarlar ile yapılan geçiş kontrolüdür.

Elektronik Anahtarlar: Elektronik kodlar veya radyo frekansı kullanılarak yapılan geçiş kontrolüdür.

Akıllı Telefon ve Mobil Uygulamalar

Bluetooth ve NFC: Akıllı telefonlar aracılığıyla mobil temassız geçiş kontrolü sağlar.

Personel Devam Kontrol Sistemleri (PDKS)

Çalışanların giriş ve çıkış saatlerini kaydeden sistemlerdir. Bu sistemler, iş gücü yönetimi için kritik öneme sahiptir.

Biyometrik Geçiş Sistemleri

Biyometrik geçiş, bireyin kimliğini doğrulamak için benzersiz biyometrik verilerini (parmak izi, yüz tanıma gibi) kullanır. Bu sistemler, güvenli bölgeler veya sistemlere giriş izinlerini yönetmek amacıyla kullanılır. Geleneksel şifreli veya kartlı geçiş sistemlerine kıyasla daha yüksek güvenlik sağlar. Biyometrik verilerin her birey için benzersiz olması, bu sistemleri son derece güvenli kılar.

Geçiş Kontrol Sistemlerinde Veri Saklamanın Önemi

Kişisel Verileri Koruma Kanunu (KVKK), biyometrik verilerin güvenli bir şekilde işlenmesini zorunlu kılar. Biyometrik verilerin şifrelenerek saklanması, veri güvenliğini sağlamak için önemlidir. Saklama alanında ve veri aktarımında güçlü

şifreleme algoritmaları kullanılmalıdır.

ASSA ABLOY Biyometrik Geçiş Sistemleri

ASSA ABLOY, parmak izi ve 3D yüz tanıma teknolojilerini RFID kart sistemi ile birleştirerek yüksek güvenlik sunan çözümler sağlar. Controlid cihazı, veri güvenliği için hem kart hem de yüz tanıma doğrulaması gerektirir. Bu teknoloji, KVKK standartlarıyla uyumlu şekilde veri işleyerek güvenliği en üst düzeye çıkarır. Controlid, ofisler, veri merkezleri, havaalanları ve kamu binaları gibi çeşitli alanlarda güvenli geçiş kontrolü sağlar. Kolay yetkilendirme süreçleri ve yüksek güvenlik standartları ile Controlid, erişim kontrolünü etkin ve güvenli kılar. Çeşitli access control çözümleri sunar. Bu çözümler, işletmelerin güvenliğini artırmak için kartlı geçiş sistemlerinden biyometrik doğrulama sistemlerine kadar geniş bir yelpazede hizmet verir.

Güvenli Geçiş ve Yönetim: Access control sistemleri, sadece geçişleri kontrol etmekle kalmaz, aynı zamanda bu geçişlerin kaydını tutar ve yönetimini sağlar. Böylece, güvenlik ihlalleri durumunda hızlı bir şekilde müdahale edilebilir.

Esnek ve Ölçeklenebilir Sistemler: ASSA ABLOY'un sunduğu access control çözümleri, esnek ve ölçeklenebilir yapılarıyla her türlü işletme için uygundur. Küçük ofislerden büyük endüstriyel tesislere kadar her türlü ihtiyaç karşılanabilir.

Kurum ve tesislerde erişim güvenliği için **Geçiş Kontrol Sistemleri**

Kartlı geçiş sistemi, bu yapının en yaygın ve güvenilir bileşenlerinden biri olarak, personel ve ziyaretçi erişimlerinin kontrolünü sağlamaktadır. Geçiş kontrol sistemlerinin faydaları, işletmelere yüksek güvenlik, veri koruması, kolay izleme ve yönetim imkânı sağlar.

ATLASTEK



Geçiş Kontrol Sistemleri, kurum ve tesislerde erişim güvenliğini sağlamak amacıyla kullanılan ileri teknoloji çözümleridir. Bu sistemler, kullanıcı yetkilerini belirleyerek izinsiz girişleri önlemekte, veri güvenliğini korumakta ve tüm erişim hareketlerini dijital olarak kaydetmektedir. Kartlı geçiş sistemi, bu yapının en yaygın ve güvenilir bileşenlerinden biri olarak, personel ve ziyaretçi erişimlerinin kontrolünü sağlamaktadır. Geçiş kontrol sistemlerinin faydaları, işletmelere yüksek güvenlik, veri koruması, kolay izleme ve yönetim imkânı sağlar. Ayrıca, sistemlerin otomatikleştirilmiş yapısı, zaman ve iş gücü tasarrufu sağlayarak operasyonel verimliliği artırır. Atlas-tek, modern teknolojiye sahip geçiş kontrol sistemleri ile işletmelere güvenilir, ölçeklenebilir ve merkezi yönetim avantajı sunmaktadır.

Geçiş Kontrol Sistemi Elemanları

Kartlı Geçiş Sistemleri

Manyetik veya temassız kartlarla çalışan geçiş kontrol sistemleri, kullanıcılara özel erişim tanımlamaları yaparak güvenliği en üst seviyeye çıkarmaktadır.

Biyometrik Geçiş Sistemleri

Kişiyeye özgü biyometrik verilerle kimlik doğrulaması yapan

bu sistemler, geçiş kontrol sistemleri içinde en yüksek güvenlik seviyesini sağlamaktadır.

Parmak İzi Tanıma Sistemleri

Kesin kimlik doğrulama imkânı sunarak yetkisiz erişimi önlemektedir.

Yüz Tanıma Sistemleri

Yüz tanıma sistemleri, yapay zekâ destekli yapısı sayesinde geçiş kontrol sistemleri arasında temassız, hızlı ve güvenilir geçiş olanağı sağlamaktadır.

Anahtar ve Kilit Sistemleri

Elektronik kilitlerle desteklenen geçiş kontrol sistemleri, manuel erişim süreçlerini dijitalleştirerek güvenliği artırmaktadır. Bu sistemler kartlı veya biyometrik çözümlerle entegre çalışabilmektedir.

Personel Devam Kontrol Sistemleri (PDKS)

PDKS çözümleri, çalışan giriş-çıkışlarını otomatik olarak kaydeden geçiş kontrol sistemleri arasında yer almaktadır. İnsan kaynakları süreçlerinde verimliliği artırmakta ve güvenlik yönetimine katkı sağlamaktadır.

Otopark Bariyer Sistemleri

Otopark bariyer sistemleri, araç giriş-çıkışlarını yönetmek için tasarlanmış geçiş kontrol sistemleridir. Plaka tanıma veya kartlı geçiş özellikleriyle entegre çalışarak otopark güvenliğini güçlendirmektedir. Bu sistem-

“Manyetik veya temassız kartlarla çalışan geçiş kontrol sistemleri, kullanıcılara özel erişim tanımlamaları yaparak güvenliği en üst seviyeye çıkarmaktadır.

ler, yetkisiz araç girişini engellerken trafik akışını düzenler ve otopark yönetiminde maksimum verimlilik sağlamaktadır.

Geçiş Kontrol Sistemlerinde Veri Güvenliği

Veri güvenliği, modern geçiş kontrol sistemleri için en kritik unsurlardan biridir. Atlas-tek, tüm erişim verilerini şifrelenmiş formatta saklamakta ve yalnızca yetkili kullanıcıların erişimine izin vermektedir. Kartlı geçiş sistemleri, bu güvenlik önlemlerini sağlayarak, her kullanıcıya özel erişim tanımlamaları yapar ve izinsiz girişleri engeller. Sistem altyapısı, hem yerel hem de bulut tabanlı güvenlik standartlarına uygun şekilde yapılandırılmakta, böylece kurum verileri olası siber tehditlere karşı koruma altına alınmaktadır.

Risk, Teknoloji ve İnsan Faktörü Ekseninde **Endüstriyel Güvenlik**

“Alışveriş merkezlerinin ilk zamanlarında sayılarının az olması, rekabetin olmaması ve güvenlik bütçelerinin yüksek olması güvenlik önlemlerinin uygulanmasını çok kolaylaştırdı. Bu, alışveriş merkezine girmeye çalışan ziyaretçilerin yüksek standartta bir denetim almalarını sağlar.”



Modern Sanayinin Görünmeyen Kalkınması: Risk, Teknoloji ve İnsan Faktörü Ekseninde Endüstriyel Güvenlik

Sanayi devriminin ardından hızla büyüyen üretim kapasitesi, yalnızca ekonomik kalkınmayı değil; aynı zamanda güvenlik, sürdürülebilirlik ve kriz yönetimi gibi kavramları da endüstriyel dünyanın merkezine yerleştirmiştir. Günümüzde rafinerilerden enerji santrallerine, kimya tesislerinden lojistik merkezlerine, savunma sanayi üretim alanlarından gıda fabrikalarına kadar geniş bir yelpazeye yayılan endüstriyel tesisler; yüksek risk barındıran, karmaşık ve stratejik yapılar hâline gelmiştir. Bu nedenle endüstriyel tesis güvenliği artık yalnızca kapıda bekleyen bir güvenlik görevlisi ya da çevre duvarı ile açıklanabilecek dar bir alan değildir. Fiziksel güvenlikten siber güvenliğe, iş sağlığı uygulamalarından kriz yönetimine, yapay zekâ destekli izleme sistemlerinden çalışan psikolojisine kadar çok katmanlı bir yapıdan söz edilmektedir.

Endüstriyel güvenlik kavramı özellikle son yirmi yılda büyük bir dönüşüm geçirmiştir. Dijitalleşmenin hız kazanmasıyla birlikte üretim sistemleri otomasyon odaklı hâle gelmiş, SCADA altyapıları, IoT cihazları ve uzaktan yönetim sistemleri üretim süreçlerinin vazgeçilmez unsuru olmuştur. Ancak bu dönüşüm beraberinde yeni tehdit alanlarını da ortaya çıkarmıştır. Artık yalnızca fiziksel sabotajlar değil, siber saldırılar, veri manipülasyonu, üretim hatlarının dijital olarak durdurulması ve kritik altyapıların

hedef alınması da endüstriyel güvenliğin temel meseleleri arasında yer almaktadır.

Bir endüstriyel tesisin güvenliği; insan hayatının korunması, üretim sürekliliğinin sağlanması, ekonomik kayıpların önlenmesi, çevresel felaketlerin engellenmesi ve ulusal güvenliğin korunması açısından kritik öneme sahiptir. Özellikle enerji, petrokimya, savunma ve ulaştırma gibi stratejik sektörlerde meydana gelen güvenlik zafiyetleri yalnızca işletmeyi değil, doğrudan toplum düzenini etkileyebilecek sonuçlar doğurabilir. Bu nedenle modern güvenlik yaklaşımı; önleyici, analiz odaklı, veri temelli ve entegre bir yapıya dönüşmektedir.

Endüstriyel Tesis Güvenliği Kavramının Tarihsel Gelişimi

Endüstriyel güvenliğin kökeni, modern fabrikanın ortaya çıkışıyla birlikte şekillenmeye başlamıştır. İlk sanayi tesislerinde güvenlik anlayışı büyük ölçüde üretim araçlarının korunması ve çalışan disiplininin sağlanması üzerine kuruluydu. Buhar makineleriyle çalışan ilk fabrikalarda yangınlar, mekanik kazalar ve işçi ölümleri son derece yaygındı. Ancak bu dönemde güvenlik, insan yaşamını koruma amacıyla değil; üretim kaybını önleme yaklaşımıyla ele alınıyordu.

Yüzyılın sonlarına doğru ağır sanayinin gelişmesiyle birlikte iş güvenliği kavramı önem kazanmaya başladı. Özellikle maden kazaları, kimyasal sızıntılar ve büyük yangınlar devletleri yasal düzenlemeler yapmaya zorladı. 20. yüzyılın ortalarına gelindiğinde ise güvenlik yalnızca iş



Endüstriyel güvenliğin kökeni, modern fabrikanın ortaya çıkışıyla birlikte şekillenmeye başlamıştır.

kazaları ekseninde değil; sabotaj, casusluk ve stratejik tesislerin korunması perspektifiyle değerlendirilmeye başlandı.

İkinci Dünya Savaşı sonrasında enerji altyapılarının stratejik önem kazanması, nükleer tesislerin yaygınlaşması ve savunma sanayisinin büyümesi; endüstriyel güvenlik anlayışını doğrudan değiştirdi. Soğuk Savaş döneminde birçok ülkede kritik altyapı koruma programları oluşturuldu. Özellikle petrol rafinerileri, enerji santralleri, limanlar ve iletişim merkezleri ulusal güvenliğin parçası olarak görülmeye başlandı.

1980'lerden sonra bilgisayar teknolojilerinin üretim sistemlerine entegre edilmesi yeni bir dönemin kapısını açtı. Otomasyon sistemleri sayesinde üretim hızlandı ancak dijital bağımlılık arttı. 2000'li yıllarla birlikte siber güvenlik, endüstriyel güvenliğin ayrılmaz bir parçasına dönüştü. Stuxnet saldırısı gibi örnekler, dijital sabotajların fiziksel hasarlara yol açabileceğini tüm dünyaya gösterdi.

Bugün endüstriyel güvenlik;

fiziksel koruma, siber savunma, risk analizi, kriz yönetimi, insan davranışı analizi ve yapay zekâ destekli erken uyarı sistemlerini kapsayan disiplinler arası bir yapı hâline gelmiştir.

Endüstriyel Tesislerde Risk Kavramı

Endüstriyel tesis güvenliğinin temelinde risk yönetimi yer almaktadır. Risk; bir tehdidin gerçekleşme olasılığı ile ortaya çıkaracağı etkinin birleşimi olarak tanımlanabilir. Endüstriyel alanlarda risk yönetimi yalnızca mevcut tehditlere karşı savunma geliştirmek değil, potansiyel zafiyetleri önceden tespit ederek olası senaryolara hazırlıklı olmak anlamına gelir.

Endüstriyel tesislerde riskler genel olarak fiziksel, çevresel, operasyonel, teknolojik ve insan kaynaklı olmak üzere farklı kategorilere ayrılır. Fiziksel riskler arasında yangın, patlama, sabotaj, hırsızlık ve yetkisiz girişler bulunur. Çevresel riskler ise deprem, sel, fırtına ve iklim kaynaklı afetleri içerir. Teknolojik riskler; otomasyon sistemlerinin çökmesi, enerji kesintileri, veri kayıpları ve siber saldırılar şeklinde ortaya çıkabilir. İnsan faktörü ise çoğu zaman en kritik risk alanıdır. Yapılan araştırmalar, endüstriyel kazaların büyük kısmının insan hatasıyla ilişkili olduğunu göstermektedir. Dikkatsizlik, yetersiz eğitim, prosedür ihlali, iletişim eksikliği ve psikolojik baskılar ciddi güvenlik sorunlarına neden olabilir. Risk yönetiminde temel amaç, tehditleri tamamen ortadan kaldırmak değil; kabul edilebilir seviyeye indirmektir. Bu nedenle modern tesislerde düzenli risk



analizleri yapılmakta, senaryo bazlı güvenlik planları oluşturulmakta ve olası kriz durumları için tatbikatlar gerçekleştirilmektedir.

Fiziksel Güvenlik Sistemleri

Endüstriyel tesis güvenliğinin en görünür alanlarından biri fiziksel güvenliktir. Fiziksel güvenlik; tesisin, çalışanların, ekipmanların ve kritik altyapının dış tehditlere karşı korunmasını amaçlar. Ancak modern fiziksel güvenlik anlayışı yalnızca duvar, tel örgü ve güvenlik personeli ile sınırlı değildir. Günümüzde gelişmiş tesislerde çok katmanlı güvenlik mimarileri kullanılmaktadır. Bu yapı genellikle çevre güvenliği, erişim kontrolü, izleme sistemleri ve müdahale ekipleri şeklinde organize edilir. Çevre güvenliği, ilk savunma

hattını oluşturur. Yüksek güvenli çitler, hareket sensörleri, termal kameralar, titreşim algılama sistemleri ve aydınlatma altyapıları çevresel koruma için kullanılır. Özellikle geniş arazilere yayılan enerji tesislerinde çevre güvenliği kritik önemdedir.

Erişim kontrol sistemleri, tesis içine giriş yapan kişilerin yetki seviyelerine göre hareket etmesini sağlar. Kartlı geçiş sistemleri, biyometrik doğrulama teknolojileri, yüz tanıma sistemleri ve iris tarama uygulamaları bu alanda yaygın olarak kullanılmaktadır. Kapalı devre kamera sistemleri ise modern güvenliğin merkezinde yer alır. Yapay zekâ destekli kameralar artık yalnızca kayıt yapmakla kalmamakta; şüpheli davranış analizi, yüz tanıma, hareket takibi ve anormal durum algılama gibi işlemleri



Günümüzde gelişmiş tesislerde çok katmanlı güvenlik mimarileri kullanılmaktadır.

de gerçekleştirmektedir. Birçok tesiste özel müdahale ekipleri oluşturulmaktadır. Bu ekipler yangın, kimyasal sızıntı, sabotaj ya da silahlı saldırı gibi durumlara hızlı müdahale edebilmek için özel eğitimlerden geçirilir.

Siber Güvenlik ve Dijital Tehditler

Dijital dönüşüm süreci, endüstriyel tesislerin üretim kapasitesini artırırken güvenlik tehditlerini de karmaşık hâle getirmiştir. Günümüzde üretim hatları büyük ölçüde otomasyon sistemleri üzerinden yönetilmektedir. SCADA sistemleri, PLC cihazları ve endüstriyel kontrol ağları üretimin sürekliliğini sağlamaktadır. Ancak bu altyapılar siber saldırılara karşı savunmasız kalabilmektedir.

Siber saldırılar artık yalnızca veri çalmak amacıyla yapılmamaktadır. Kritik altyapıları devre dışı bırakmak, üretimi durdurmak, enerji akışını kesmek ya da fiziksel hasar oluşturmak amacıyla gerçekleştirilen saldırılar giderek yaygınlaşmaktadır.

Endüstriyel siber güvenlikte en büyük sorunlardan biri eski altyapılardır. Birçok üretim tesisi yıllar

önce kurulan sistemlerle çalışmaya devam etmektedir. Bu sistemlerin güncel güvenlik protokollerine uyum sağlayamaması ciddi riskler doğurur.

Siber güvenlik uygulamalarında ağ segmentasyonu büyük önem taşır. Üretim ağları ile kurumsal ağların birbirinden ayrılması saldırıların yayılmasını engelleyebilir. Bunun yanında güvenlik duvarları, saldırı tespit sistemleri, çok faktörlü kimlik doğrulama ve düzenli yazılım güncellemeleri temel koruma yöntemleri arasında yer alır. Personel farkındalığı da kritik bir unsurdur. Birçok siber saldırı oltalama e-postaları, sosyal mühendislik yöntemleri ve kullanıcı hataları üzerinden gerçekleşmektedir. Bu nedenle çalışanlara düzenli eğitim verilmesi zorunludur.

Kritik Altyapıların Korunması

Kritik altyapılar; enerji, su, ulaşım, iletişim, sağlık ve savunma gibi toplumun temel işleyişi açısından hayati öneme sahip sistemleri ifade eder. Bu altyapılarda meydana gelecek bir güvenlik zafiyeti yalnızca ekonomik kayıplara değil; toplumsal krizlere, çevresel felaketlere ve ulusal güvenlik tehditlerine yol açabilir.

Enerji santralleri bu açıdan en kritik tesislerden biridir. Elektrik üretim ve dağıtım sistemlerinin hedef alınması, geniş çaplı enerji kesintilerine neden olabilir. Benzer şekilde petrol rafinerileri ve doğalgaz tesisleri hem ekonomik hem de çevresel açıdan yüksek risk taşır. Su arıtma tesisleri de son yıllarda kritik altyapı güvenliği tartışmalarının merkezinde yer almaktadır. Su sistemlerine yapılacak bir sabotaj

milyonlarca insanın yaşamını doğrudan etkileyebilir.

Kritik altyapı güvenliğinde devlet ve özel sektör iş birliği büyük önem taşır. Çünkü birçok stratejik tesis özel şirketler tarafından işletilmekte ancak ulusal güvenlik açısından kritik rol oynamaktadır.

İş Sağlığı ve Güvenliği ile Endüstriyel Güvenlik İlişkisi

Endüstriyel tesis güvenliği yalnızca dış tehditlere karşı koruma sağlamak değildir. Çalışanların fiziksel ve psikolojik güvenliği de bu sistemin temel parçalarından biridir. İş sağlığı ve güvenliği uygulamaları, üretim süreçlerinin insan hayatını tehdit etmeyecek şekilde organize edilmesini amaçlar.

Kimya tesislerinde toksik gazlar, yüksek basınçlı sistemler ve yanıcı maddeler büyük risk oluşturur. Metal sanayi tesislerinde ağır makineler ve yüksek sıcaklıklar ciddi kazalara neden olabilir. Madencilik sektöründe ise göçükler, patlamalar ve zehirli gazlar temel tehlike kaynaklarıdır.

Bu nedenle koruyucu ekipman kullanımı hayati öneme sahiptir. Baretler, gaz maskeleri, koruyucu gözlükler, ısı dayanımlı kıyafetler ve güvenlik ayakkabıları standart güvenlik uygulamaları arasında yer alır.

Ancak modern iş güvenliği yaklaşımı yalnızca ekipman kullanımına odaklanmamaktadır. Çalışanların psikolojik dayanıklılığı, stres düzeyi ve dikkat kapasitesi de güvenliğin parçası olarak değerlendirilmektedir. Uzun çalışma saatleri, vardiya sistemi ve yoğun baskı çalışan performansını düşürebilir. Özellikle insan hatalarının azal-

tilması için ergonomik tasarımlar önem kazanmıştır. Kontrol odalarının kullanıcı dostu şekilde düzenlenmesi, alarm sistemlerinin anlaşılır olması ve karmaşık süreçlerin sadeleştirilmesi hata oranını azaltabilir.

Yapay Zekâ ve Akıllı Güvenlik Teknolojileri

Yapay zekâ teknolojileri, endüstriyel tesis güvenliğinde yeni bir dönemi başlatmıştır. Geleneksel güvenlik sistemleri genellikle olay gerçekleşikten sonra tepki verirken; yapay zekâ tabanlı sistemler riskleri önceden tahmin etmeye çalışmaktadır.

Akıllı kamera sistemleri sayesinde yüz tanıma, davranış analizi ve şüpheli hareket tespiti yapılabilmektedir. Örneğin belirli bir bölgede olağan dışı hareketlilik tespit edildiğinde sistem otomatik alarm oluşturabilmektedir.

Makine öğrenmesi algoritmaları üretim hatlarında anormal davranışları analiz ederek olası arızaları önceden tahmin edebilir. Bu yaklaşım yalnızca güvenliği artırmakla kalmaz; bakım maliyetlerini de

düşürür. Dronelar da özellikle büyük endüstriyel alanlarda yaygın şekilde kullanılmaktadır. Rafineriler, limanlar ve enerji santralleri gibi geniş alanlarda devriye görevleri dronelar aracılığıyla gerçekleştirilebilir. Termal görüntüleme sistemleri yangın risklerini erken aşamada tespit etmek için kullanılmaktadır. Özellikle yüksek sıcaklıkla çalışan tesislerde bu sistemler kritik rol oynar.

Bunun yanında dijital ikiz teknolojisi de güvenlik alanında önemli bir gelişme olarak görülmektedir. Dijital ikizler sayesinde tesislerin sanal modelleri oluşturularak olası kriz senaryoları önceden simüle edilebilmektedir.

Yangın Güvenliği ve Patlama Riskleri

Endüstriyel tesislerde yangın güvenliği en kritik konuların başında gelir. Özellikle petrokimya tesisleri, boya fabrikaları, enerji santralleri ve depolama alanları yüksek yangın riski taşır.

Yangınların temel nedenleri arasında elektrik arızaları, insan hataları, kimyasal reaksiyonlar ve ekipman

arızaları bulunur. Patlayıcı gazların bulunduğu ortamlarda küçük bir kıvılcım bile büyük felaketlere yol açabilir. Yangın güvenliğinde erken tespit sistemleri büyük önem taşır. Duman dedektörleri, ısı sensörleri ve gaz algılama sistemleri riskleri erken aşamada belirlemeye yardımcı olur.

Otomatik söndürme sistemleri ise yangının büyümesini önlemek için kritik rol oynar. Su bazı sistemlerin yanında köpük, gaz ve kuru kimyasal söndürme sistemleri de kullanılmaktadır.

Patlama risklerinin azaltılması için havalandırma sistemleri dikkatle tasarlanmalıdır. Gaz birikiminin önlenmesi, statik elektriğin kontrol edilmesi ve kıvılcım kaynaklarının minimize edilmesi temel önlemler arasındadır. Acil durum tahliye planları da yangın güvenliğinin vazgeçilmez unsurudur. Çalışanların hangi güzergâhları kullanacağı, toplanma alanlarının nerede olduğu ve kriz anında iletişimin nasıl sağlanacağı önceden belirlenmelidir.

İnsan Faktörü ve Güvenlik Kültürü

Teknoloji ne kadar gelişmiş olursa olsun güvenlik sistemlerinin merkezinde insan yer almaktadır. Bu nedenle güvenlik kültürü oluşturmak, endüstriyel tesislerde sürdürülebilir güvenliğin temel şartıdır.

Güvenlik kültürü; çalışanların güvenlik kurallarını yalnızca zorunlu prosedür olarak değil, ortak sorumluluk anlayışıyla benimsemesini ifade eder. Eğer çalışanlar güvenliği yalnızca yönetimin baskısı olarak görürse prosedürler zamanla ihlal edilmeye başlanır. Etkili bir güvenlik kültürü için yöne-





Teknoloji ne kadar gelişmiş olursa olsun güvenlik sistemlerinin merkezinde insan yer almaktadır. Bu nedenle güvenlik kültürü oluşturmak, endüstriyel tesislerde sürdürülebilir güvenliğin temel şartıdır.

tim desteği kritik öneme sahiptir. Üst düzey yöneticilerin güvenlik konusuna öncelik vermesi çalışan davranışlarını doğrudan etkiler. Düzenli eğitimler güvenlik farkındalığını artırır. Özellikle yeni çalışanların tesis riskleri konusunda detaylı şekilde eğitilmesi gerekir. Bunun yanında kriz tatbikatları çalışanların acil durumlara hazırlıklı olmasını sağlar. Psikolojik güvenlik de önemli bir unsurdur. Çalışanların hata ya da risk bildiriminde bulunurken cezalandırılma korkusu yaşamaması gerekir. Aksi hâlde küçük sorunlar zamanla büyük felaketlere dönüşebilir.

Kimyasal ve Biyolojik Güvenlik

Kimyasal tesisler, laboratuvarlar ve ilaç üretim merkezleri özel güvenlik önlemleri gerektiren alanlardır. Ze-

hirli maddeler, patlayıcı kimyasallar ve biyolojik ajanlar yalnızca tesis çalışanlarını değil, çevrede yaşayan insanları da etkileyebilir.

Kimyasal güvenlikte depolama koşulları büyük önem taşır. Maddelerin sıcaklık, nem ve basınç değerlerine uygun şekilde saklanması gerekir. Yanlış depolama ciddi reaksiyonlara yol açabilir. Tehlikeli madde taşımacılığı da önemli bir risk alanıdır. Özellikle tankerler ve boru hatları sabotaj ya da kaza durumlarında büyük çevresel felaketlere neden olabilir. Biyolojik güvenlik ise özellikle pandemi sonrası dönemde daha fazla önem kazanmıştır. Laboratuvar güvenliği, biyolojik örneklerin korunması ve bulaşıcı ajanların kontrolü kritik konular arasında yer almaktadır.

Afet Yönetimi ve Kriz Senaryoları

Endüstriyel tesisler yalnızca insan kaynaklı tehditlere değil; doğal afetlere karşı da hazırlıklı olmak zorundadır. Depremler, seller, fırtınalar ve aşırı sıcaklıklar üretim süreçlerini ciddi şekilde etkileyebilir.

Özellikle deprem kuşağında yer alan ülkelerde tesis altyapılarının sismik dayanıklılığı hayati öneme sahiptir. Boru hatları, depolama tankları ve enerji sistemleri deprem sırasında büyük risk oluşturabilir. Kriz yönetiminde en önemli unsur hızlı karar alma kapasitesidir. Acil durum merkezleri, iletişim ağları ve kriz ekipleri bu nedenle önceden organize edilmelidir.

İş sürekliliği planları modern güvenlik yaklaşımının temel parçalarından biridir. Bir kriz durumunda üretimin tamamen durması yerine

kontrollü şekilde devam etmesi hedeflenir.

Enerji Sektöründe Güvenlik Yaklaşımları

Enerji sektörü endüstriyel güvenliğin en hassas alanlarından biridir. Elektrik üretim tesisleri, doğalgaz depolama merkezleri, petrol rafinerileri ve nükleer santraller çok yüksek risk seviyelerine sahiptir. Nükleer tesislerde güvenlik çok katmanlı şekilde planlanır. Fiziksel koruma, radyasyon güvenliği, siber savunma ve uluslararası denetim mekanizmaları birlikte çalışır. Petrol ve doğalgaz sektöründe ise sabotaj riski önemli bir problemdir. Boru hatlarına yönelik saldırılar ekonomik zararların yanında çevresel felaketlere de yol açabilir. Yenilenebilir enerji sistemleri de yeni güvenlik ihtiyaçları doğurmaktadır. Rüzgâr türbinleri ve güneş enerji santralleri geniş alanlara yayıldığı için fiziksel güvenlik açısından farklı stratejiler gerektirir.

Lojistik ve Depolama Güvenliği

Modern sanayinin sürdürülebilirliği yalnızca üretimle değil; depolama ve lojistik süreçlerinin güvenliğiyle de ilişkilidir. Özellikle tehlikeli madde depoları büyük risk taşımaktadır. Depolama alanlarında sıcaklık kontrolü, yangın önleme sistemleri ve erişim güvenliği kritik önemdedir. Yanıcı maddelerin yanlış koşullarda depolanması büyük patlamalara yol açabilir. Limanlar ve lojistik merkezleri aynı zamanda organize suç ağlarının hedefi hâline gelebilmektedir. Kaçakçılık, hırsızlık ve sabotaj riskleri bu alanlarda daha yüksektir. GPS takip sistemleri ve akıllı sen-



Endüstriyel tesis güvenliği, modern dünyanın en stratejik ve karmaşık alanlarından biri hâline gelmiştir.

sörler sayesinde taşımacılık süreçleri daha güvenli hâle getirilmektedir. Özellikle yüksek değeri ürünlerin taşınmasında gerçek zamanlı takip sistemleri önemli avantaj sağlar.

Endüstriyel Casusluk ve Bilgi Güvenliği

Rekabetin yoğun olduğu sektörlerde endüstriyel casusluk ciddi bir tehdit oluşturmaktadır. Üretim formülleri, mühendislik projeleri, Ar-Ge çalışmaları ve ticari veriler rakip firmalar ya da organize yapılar tarafından hedef alınabilir.

Bilgi güvenliği yalnızca dijital verilerin korunması anlamına gelmez. Fiziksel belgeler, çalışan bilgileri ve üretim süreçleri de korunmalıdır. İç tehditler bu alanda önemli bir risk faktörüdür. Yetkili çalışanların bilgi sızdırması birçok güvenlik ihlalinin temel nedeni olabilir.

Bu nedenle erişim yetkilendirmesi dikkatle planlanmalı, kritik bilgiler yalnızca ilgili personelin erişimine açılmalıdır.

Güvenlikte Hukuki ve Etik Boyut

Endüstriyel güvenlik uygulamaları yalnızca teknik değil; aynı zamanda hukuki ve etik bir konudur. İşletme-

ler çalışan güvenliğini sağlamakla yükümlüdür. İhmler ciddi hukuki sonuçlara yol açabilir.

Birçok ülkede iş güvenliği standartları yasal zorunluluk hâline getirilmiştir. Uluslararası standartlar arasında ISO 45001, ISO 27001 ve çeşitli çevre güvenliği normları öne çıkmaktadır.

Bunun yanında güvenlik uygulamalarının insan haklarına uygun olması gerekir. Özellikle biyometrik izleme sistemleri ve çalışan takibi konusunda etik tartışmalar yaşanmaktadır. Güvenlik ile mahremiyet arasındaki denge modern tesislerde önemli bir tartışma alanıdır. Sürekli izleme sistemleri çalışanlarda psikolojik baskı oluşturabilir.

Geleceğin Endüstriyel Güvenlik Trendleri

Önümüzdeki yıllarda endüstriyel güvenlik alanında çok daha kapsamlı dönüşümler yaşanması beklenmektedir. Yapay zekâ, büyük veri analitiği ve kuantum bilişim teknolojileri güvenlik süreçlerini yeniden şekillendirecektir.

Otonom güvenlik sistemleri giderek yaygınlaşacaktır. İnsan müdahalesi olmadan hareket eden robotik devriye sistemleri ve akıllı sensör ağları birçok tesiste standart hâle gelebilir. Siber güvenlik alanında ise kuantum şifreleme teknolojileri yeni bir dönemi başlatabilir. Özellikle kritik altyapıların korunmasında daha güçlü dijital savunma mekanizmaları geliştirilmektedir.

İklim değişikliği de güvenlik stratejilerini doğrudan etkileyecektir. Aşırı hava olaylarının artması, enerji altyapılarının dayanıklılığını daha önemli hâle getirecektir.

Ayrıca sürdürülebilirlik odaklı güvenlik anlayışı ön plana çıkacaktır. Çev-

resel risklerin azaltılması, karbon salımının kontrolü ve yeşil üretim süreçleri güvenliğin yeni boyutları arasında yer alacaktır.

Sonuç

Endüstriyel tesis güvenliği, modern dünyanın en stratejik ve karmaşık alanlarından biri hâline gelmiştir. Günümüzde güvenlik yalnızca fiziksel koruma anlamına gelmemekte; dijital savunma, insan psikolojisi, kriz yönetimi, çevresel sürdürülebilirlik ve yapay zekâ teknolojilerini kapsayan çok katmanlı bir sistem olarak değerlendirilmektedir. Sanayi altyapılarının büyümesi ve dijitalleşmesi, tehditlerin de daha karmaşık hâle gelmesine neden olmuştur. Siber saldırılar, kritik altyapı sabotajları, kimyasal riskler ve doğal afetler artık endüstriyel güvenliğin temel meseleleri arasında yer almaktadır.

Bu nedenle geleceğin güvenlik anlayışı yalnızca reaktif değil; proaktif ve öngörü odaklı olacaktır. Riskleri önceden analiz eden, verileri gerçek zamanlı işleyen ve insan faktörünü merkeze alan sistemler öne çıkacaktır.

Ancak tüm teknolojik gelişmelere rağmen güvenliğin en temel unsuru yine insan olacaktır. Eğitimli personel, güçlü güvenlik kültürü ve etik sorumluluk anlayışı olmadan hiçbir sistem tam anlamıyla güvenli olamaz.

Endüstriyel güvenlik yalnızca tesisleri korumaz; aynı zamanda insan yaşamını, çevreyi, ekonomik sürdürülebilirliği ve toplumsal düzeni koruyan görünmez bir kalkan işlevi görür. Bu nedenle geleceğin sanayi dünyasında güvenlik, üretimin maliyet kalemi değil; stratejik varlıklardan biri olarak değerlendirilecektir.

Son teknolojiye uygun, ürün ve çözümlerden HABERİNİZ VAR MI?

- Elektrik proje taahhüt firmaları • Bayi odaklı çalışan firmalar
 - Havalimanları ilgili birimleri • Bankalar ilgili birimleri • İnşaat firmaları
 - Oteller ilgili birimleri • Hastaneler ilgili birimleri • AVM'ler ilgili birimleri
 - TÜRLİM Üyeleri • Belediyeler ilgili birimleri • Emniyet Genel Müdürlüğü ilgili birimleri • Zincir mağazalar • Üniversiteler • Mimarlık ofisleri
 - Sektör profesyonelleri **AĞIMIZA KATILIN**
- TÜM TÜRKİYE'DE SESİNİZ OLALIM!**

- ✓ CCTV ve video kontrol sistemleri,
- ✓ Yangın algılama ve ihbar sistemleri,
- ✓ Yangın söndürme sistemleri,
- ✓ Geçiş kontrol sistemleri,
- ✓ Hırsız alarm sistemleri,
- ✓ Alarm izleme merkezleri,
- ✓ Apartman konuşma sistemleri,
- ✓ Mobil takip sistemleri,
- ✓ Drone teknolojileri

Çok sayıda köklü firmanın çözüm ortağı olmuş ve geleceği tasarlamayı ilke edinmiş bir hizmet ajansı olan **ARKHE TANITIM HİZMETLERİ** tarafından hazırlanmaktadır. Bünyesinde **GÜVENLİK YÖNETİMİ**, **PERPA GÜNDEM**, **TECHNEWS** ve **KURUMSAL YATIRIMCI** dergilerini barındıran **ARKHE TANITIM HİZMETLERİ**; grafik tasarım, kurumsal kimlik çalışmaları, web ve her türlü promosyon ihtiyaçlarınıza fark yaratan tasarım, hız ve müşteriye koruyan fiyat politikasıyla çözümler sunmaktadır.

Güvenlik Yönetimi
2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100

arkhe
Tanıtım Hizmetleri

Endüstriyel Tesislerde **İdeal Güvenliğin 8 Adımı**

Endüstriyel tesisler pek çok riske karşı akıllı güvenlik çözümleriyle korunuyor. Tesise özel kurgulanacak olan akıllı güvenlik çözümlerinin risk analizi sonrası belirlenecek katmanlı bir yapıya sahip olması ve her kademedede birbiri ile entegre çalışması önem taşıyor.

SECURITAS TECHNOLOGY



Endüstriyel tesisler pek çok riske karşı akıllı güvenlik çözümleriyle korunuyor. Tesise özel kurgulanacak olan akıllı güvenlik çözümlerinin risk analizi sonrası belirlenecek katmanlı bir yapıya sahip olması ve her kademedede birbiri ile entegre çalışması önem taşıyor. Endüstriyel tesislerde üretime güvenle devam edebilmek için atılması gereken 8 kritik adım şöyle

1- Önce riskler tespit edilmeli

Endüstriyel tesislerin güvenliği birbiri ile entegre çalışan, kapsamlı çözümler gerektiriyor. Bu nedenle çözüm tasarımı öncesinde riskleri belirlemek büyük önem taşıyor. Güvenlik sağlanacak alan sahip olduğu özelliklere göre yüksek, orta ve düşük öncelikli risk grupları üzerinden değerlendirilmeli. Risklerin belirlenmesinde söz konusu tesisin konumu, büyüklüğü, tesisin yakınında kaç kilometrelik alanda nasıl bir canlı ekosistem olduğu, tesiste Ar-Ge çalışması gerektiren ve dolayısıyla sanayi kapasitesine konu olabilecek alanlar olup olmadığı, patlama ya da alev alma riski bulunan kimyasal madde alanlarının varlığı ve yerleri gibi pek çok konu değerlendirilmeli...

2- Dışarıda ilk amaç caydırmak olmalı

Endüstriyel tesislerin güvenliği sağlamak için risk tespitinden sonra akıllı güvenlik çözümlerini dışarıdan içeriye doğru katmanlı bir şekilde kurgulamak çok önemli. Çünkü endüstriyel tesis güvenliğinde amaç öncelikle çevreden gelebilecek tehditlere karşı binayı

korumak. Bu aşamada caydırıcı önlemler kritik öneme sahip. Hırsızlık ya da özel alan ihlali gibi durumlar söz konusu olduğunda imdada ilk olarak çevre güvenlik sistemleri yetişiyor. Bu sistemlerin, tesis duvarına yaklaşan kişinin civarda yaşayan ve tesise yönelik bir amacı bulunmayan biri mi yoksa kötü niyetli mi olduğu sorusuna cevap vermesi gerekiyor.

3- Çevre güvenliğinde akıllı sistemler

Tesis çevresine yerleştirilen akıllı kameralar, sahip oldukları video analiz algoritmaları alandaki hareketleri otomatik algılıyor ve potansiyel tehlikeleri güvenlik biriminin ekranına gerçek zamanlı olarak aktarıyor. Bu noktada uzaktan sesli anons sistemiyle şüpheliye sözlü bir uyarı yapılabiliyor. Bu anons, oraya kazara girmiş olan bir kişinin oradan hızla uzaklaşmasını sağlarken, kötü niyetli kişi ya da gruplara ise 'Güvenlik güçlerinin sizden haberi var, müdahale etmeden burayı hemen terk edin' uyarısını yapıyor.'

Yine yüksek ve kalın duvarlar, ileri teknoloji içeren geçiş kontrol önlemleri, ek bariyerler, sınır çiti, toprak altı optik algılayıcılar veya duvar üzerine monte edilebilen algılayıcılar, hareket sensörleri, radar, mikro dalga bariyerlerden oluşan çevre güvenlik sistemleri diğer önlemler arasında yer alıyor.

4- Giriş-çıkışlar çok kritik

Endüstriyel tesislerde çevre güvenliğinden sonra ikinci katmanda giriş-çıkış güvenliği yer alıyor. Giriş çıkış kontrolü işletmelere pek çok açıdan verimlilik kazandırırken endüstriyel casusluk,



Endüstriyel tesislerin güvenliği birbiri ile entegre çalışan, kapsamlı çözümler gerektiriyor. Bu nedenle çözüm tasarımı öncesinde riskleri belirlemek büyük önem taşıyor.

hırsızlık ve terör saldırılarını önlemede ve işletme içinde oluşabilecek salgınları önlemede en kritik nokta kabul ediliyor. Bu noktada tesise girmeye yetkili ve yetkisiz kişilerin belirlenmesi ile sistem tasarımı başlıyor. Giriş noktasında turnikeler, X-Ray ve metal algılayıcılarla desteklenen geçiş kontrol sistemlerine ek olarak biyometrik sistemler de kullanılıyor. Binaya giriş-çıkışlar herhangi bir yere dokunmadan sisteme tanımlanan iris, yüz, parmak izi gibi biyometrik veriler işlenerek güvenli şekilde sağlanabiliyor.

5- Temassız çözümlerle ek kontrol

Arka planda çalışan derin öğrenme algoritmaları ile doğruluk payını en üst seviyeye taşıyan biyometrik geçiş kontrol sistemleri

nin temassız erişim özellikleri, günümüzün en önemli sorunlarından biri haline gelen hijyen konusuna da çözüm getiriyor. Aynı zamanda tesis girişinde bulunan kartlı geçiş sistemine entegre çalışan maske kontrolü ve ateş ölçüm çözümü de yine tesislerde kullanılan en önemli çözümler arasında. Çözüm, vücut sıcaklığının yüksek olduğu veya maske takılmadığı durumlarda geçişe izin vermeyerek ek bir kontrol katmanı sunuyor.

6- Yeni nesil yazılımlarla hem güvenlik hem raporlama

Passlogic gibi özel yazılımlar yalnızca güvenlik hizmeti sunmuyor aynı zamanda tesislerdeki verimi artırarak işleri otomatik hale getirebiliyor. Passlogic yazılımı, geçiş kontrol sisteminin sağladığı verileri kullanarak anlamlı raporlar üretiyor. Bu raporlar, insan kaynakları (bordrolama, izin yönetimi vb.) idari işler (yemekhane modülü, taşeron yönetimi, servis araçlarının yönetimi vb.), bilgi teknolojileri (ERP, task management vb.) gibi farklı departmanların ihtiyaçlarına da hizmet ediyor.

Sağlık Bakanlığı tarafından sunulan HES (Hayat Eve Sığar) kodu sorgulaması da Passlogic yazılımı üzerinden yapılabiliyor. Personel için günlük, ziyaretçiler için anlık HES kodu kontrolü sayesinde riskli durumlarda gerekli önlemler hızlıca alınabiliyor. Böylece hastalık riski taşıyan kişilerin işyerine girişinin ya da dolaşımının önüne geçiliyor. Tesislere araçla giriş durumundaysa bariyerler, araç altı arama, metal algılayıcılar, plaka tanıma, HGS sistemleri, araç, ziyaretçi ve taşeron kayıt sistemleri gibi farklı teknolojiler birbiri ile entegre olacak şekilde kurgulanıyor ve güvenlik en üst seviyede sağlanıyor.

7- Entegre ve konuşan sistemler

Yeni dönemde sistem entegrasyonu tesis güvenliğinde hızla önem kazanan konulardan biri. Projelerde sistemleri birbirleriyle tam entegre çalışacak şekilde tasarlamak çok önemli. Başta geçiş kontrol olmak üzere, video izleme, yangın algılama, seslendirme ve anons, asansör gibi birçok farklı sistem ile entegre olarak güvenlik

aksiyonları alınabiliyor. Örneğin asansör sistemi ile entegre çalışan geçiş kontrol sistemi yazılımı asansörün otomatik olarak bulunan kata gelmesini sağlarken, kişilerin sadece yetkilendirildikleri kata çıkmalarını da kontrol edebiliyor. Böylece güvenlik seviyesi artırılırken, asansörler en verimli şekilde kullanılmış oluyor. Asansör bekleme ve katlara ulaşım süreleri minimuma iniyor. Olası bir yangın anında ilgili dedektörün devreye girmesi, sonrasında çıkış kapı ve turnikelerinin otomatik olarak açılarak asansörlerin kullanımına kapanması gibi süreçler de yine entegrasyon ile gerçekleşiyor.

8- Özel güvenlik alanlarına özel çözümler

Tesis içindeki özel güvenlik gerektiren alanlarda yine biyometrik sistemler ya da elektromekanik kilitler kullanılıyor. Birden fazla kişinin erişimi olan özel alanlar ya da dolap gibi depolama ünitelerinde kullanılan elektromekanik kilitler sayesinde ilgili anahtara belli saatler arasında ya da belirli bir süre için yetki vererek kontrol dışında girişler önleniyor. Tek tip olan anahtarlar yalnızca yetkisi tanımlanan kilitleri açabiliyor. Bu kilitler ayrıca ne zaman açılmaya çalışılmış, ne zaman giriş yapılmış, hangi anahtar tarafından açılmış gibi bilgileri de raporlayabiliyor. Yine tesis içinde AR-GE gibi değerli endüstriyel bilgilerin yer aldığı alanlarda RFID ile demirbaş takibi yapılabiliyor. Bu tip alanlarda yer alan bilgisayar gibi demirbaşlar kimliklendiriliyor ve yetki verilen alanın dışına çıkartılması durumunda alarm vererek yetkililere bilgi veriyor.



Endüstriyel Tesislerde Fiziksel Güvenlik Açıkları ve Alınabilecek Önlemler

Endüstriyel tesislerde fiziksel güvenlik, sadece hırsızlığı önlemekle kalmaz; aynı zamanda üretim sürekliliğini, iş güvenliğini, ticari sırların korunmasını ve marka itibarını da doğrudan etkiler.

ONAPION TEKNOLOJİ

Gece vardiyasında fabrikanızın en ücra köşesindeki bir depoya izinsiz bir kişi girse, bundan ne zaman ve nasıl haberiniz olur? Bu senaryo, birçok fabrika müdürü ve İSG uzmanı için endişe verici bir sorudur. Endüstriyel tesislerde fiziksel güvenlik, sadece hırsızlığı önlemekle kalmaz; aynı zamanda üretim sürekliliğini, iş güvenliğini, ticari sırların korunmasını ve marka itibarını da doğrudan etkiler. Değerli hammaddeler, kritik makineler ve hassas verilerle dolu bu devasa alanların korunması, çoğu zaman gözden kaçan detaylarda gizlidir.

Peki, milyonlarca liralık yatırım ve emekle kurduğunuz üretim kalenizin surlarında gedikler var mı? Bu yazıda, endüstriyel tesislerde sıkça karşılaşılan fiziksel güvenlik açıklarını masaya yatıracak ve bu açıkları modern tesis güvenliği teknolojileri ile nasıl kapatabileceğinizi, riski nasıl bir fırsata dönüştürebileceğinizi detaylıca ele alacağız. Amacımız, endüstriyel tesis güvenliği

kavramına bütüncül bir bakış açısı sunarak, fabrikanızı daha dirençli ve korunaklı hale getirmenize rehberlik etmektir.

Gözden Kaçan Tehlikeler: Endüstriyel Tesislerde Sık Karşılaşılan Güvenlik Açıkları

Organize Sanayi Bölgeleri'nde (OSB) yaşanan birçok vaka, güvenlik ihlallerinin genellikle basit ama kritik ihmallerden kaynaklandığını göstermektedir. Fiziksel güvenlik zinciri, en zayıf halkası kadar güçlüdür. İşte tesislerde en sık rastlanan zafiyetler:

Yetersiz Çevre Güvenliği:

Eskimiş, alçak veya kör noktalara sahip tel örgüler, yetkisiz girişler için adeta bir davetiyedir. Yeterli aydınlatmanın ve caydırıcı unsurların olmadığı geniş çevre hatları, özellikle gece vardiyalarında operasyonel riskleri artırır. Sadece çevre duvarına güvenmek, modern güvenlik açığı önleme stratejileri için yeterli değildir.





Kontrolsüz Giriş ve Çıkış Noktaları: Ana nizamiyeler dışında personel veya araçların kontrolsüzce girip çıkabildiği servis kapıları, mal kabul alanları veya acil çıkışlar büyük risk taşır. Özellikle “tailgating” olarak bilinen, yetkili bir kişinin hemen arkasından kart okutmadan içeri sızma yöntemi, geleneksel sistemlerin en büyük açıklarından biridir.

Kritik Alanlarda Zayıf Gözetim: Ar-Ge merkezi, sunucu odaları, tehlikeli kimyasal depoları veya değerli ürün stok alanları gibi hassas bölgelerin sadece kilitli bir kapıyla korunması yetersizdir. Bu alanlara kimin, ne zaman girdiği kayıt altına alınmıyorsa, olası bir iç tehdit veya endüstriyel casusluk faaliyetinin tespiti nere-

deyse imkansız hale gelir.

Gece Vardiyası ve Düşük Personel Zamanları: Tesisin en savunmasız olduğu anlar, personel sayısının en aza indiği gece saatleri ve tatil günleridir. Bu zaman dilimlerinde devriye gezen güvenlik personelinin yetersizliği veya teknolojik destekten yoksun olması, kötü niyetli kişilere hareket alanı tanır.

Fabrikalarda güvenlik yalnızca güvenlik kameraları sistemi kurmak değildir; riskin tespiti, caydırıcılık ve anlık müdahale birlikte planlanmalıdır.

Çelik Duvarlardan Akıllı Sensörlere: Modern Tesis Güvenliği Çözümleri

Tehditler geliştikçe, savunma me-

kanizmaları da gelişmek zorundadır. Günümüzde fabrika güvenlik sistemleri, reaktif (olay sonrası inceleme) bir yapıdan proaktif (olay öncesi tespit ve engelleme) bir yapıya evrilmiştir. Onapion Teknoloji olarak sunduğumuz entegre çözümlerle tesisinizi nasıl zırhlandırabileceğinize bakalım:

1. Akıllı Çevre Güvenlik ve Çevresel İzleme Sistemleri

Pasif tel örgülerin yerini artık akıllı sistemler alıyor. Termal kameralar, ısı farkını algılayarak zifiri karanlıkta veya sisli havada bile insan veya araç tespiti yapabilir. Tel çitlere entegre edilen fiber optik sensörler, tırmanma veya kesme girişimini anında alarm merkezine bildirir. Yapay zeka destekli video analiz

yazılımları ise, belirlediğiniz sanal bir çizgiyi geçen veya şüpheli bir şekilde bekleyen kişileri otomatik olarak tespit eder. Bu sistemler, çevresel izleme kabiliyetini en üst düzeye çıkarır.

2. Entegre Erişim Kontrol Sistemleri (ACS)

“Kim, nereye, ne zaman girebilir?” sorusunun cevabını teknolojiye bırakın. Kartlı geçişin bir adım ötesi olan biyometrik sistemler (parmak izi, yüz tanıma), kopyalanamaz bir güvenlik katmanı sunar. Erişim kontrol sistemleri, kişilerin yetkilerini pozisyonlarına göre sınırlandırmanızı sağlar. Örneğin, bir üretim personeli ofis katına giremezken, bir Ar-Ge mühendisi laboratuvara 7/24 erişebilir. Tüm bu giriş-çıkış logları anlık olarak kayıt altına alınır ve raporlanabilir.

3. Yeni Nesil Video İzleme Sistemleri (VMS)

Yüzlerce kamerayı tek bir ekrandan yönettiğinizi düşünün. Modern VMS platformları, farklı marka ve modeldeki kameraları tek bir arayüzde birleştirir. Bu sistemler, yalnızca kayıt yapan pasif kameraların ötesine geçerek, yapay zeka destekli analizlerle (plaka tanıma, nesne takibi, kişi sayımı) olayları anında tespit edip size veya güvenlik ekibinize bildiren akıllı bir göze dönüşür. Bu, özellikle gece vardiyası güvenliği için hayati bir özelliktir.

4. Ziyaretçi Yönetimi ve İç Tehdit Kontrolü

Fabrikanıza gelen her ziyaretçi, tedarikçi veya müteahhit potansiyel bir risk taşıyabilir. Dijital

Ziyaretçi Yönetim Sistemleri, misafirlerin kimlik bilgilerini kayıt altına alır, onlara geçici ve sınırlı yetkilere sahip kartlar atar ve tesis içindeki hareketlerini izlenebilir kılar. Bu, hem profesyonel bir imaj çizer hem de iç güvenliği artırır.

Bir Maliyet Değil, Yatırım: Profesyonel Güvenlik Sistemlerinin Katma Değeri

Karar vericilerin aklındaki en önemli soru genellikle maliyettir. Ancak modern iş güvenliği teknolojisi ve fiziksel güvenlik sistemlerini bir gider kalemi olarak değil, kendini kısa sürede amorti eden bir yatırım olarak görmek gerekir.

Doğrudan Finansal Koruma: Hırsızlık, sabotaj veya vandalizm kaynaklı maddi kayıpları doğrudan önler.

Üretim Sürekliliği: Güvenlik ihlallerinin neden olabileceği üretim duruşlarını engelleyerek dolaylı maliyetlerin önüne geçer. Bir günlük üretim kaybının maliyetini düşündüğünüzde, sistemin değeri daha net ortaya çıkar.

Operasyonel Verimlilik: Erişim kontrol ve izleme sistemleri, personel ve varlık hareketlerini analiz ederek operasyonel verimliliği artırmak için değerli veriler sunar.

Yasal Uyumluluk ve Sigorta

Avantajları: İSG (İş Sağlığı ve Güvenliği) mevzuatlarına tam uyum sağlar. Kapsamlı bir güvenlik altyapısı, sigorta şirket-



Fabrikalarda güvenlik yalnızca güvenlik kameraları sistemi kurmak değildir; riskin tespiti, caydırıcılık ve anlık müdahale birlikte planlanmalıdır.

leri nezdinde risk primlerinizi düşürebilir.

Marka İtibarı: Güvenli bir tesis, müşteriler ve iş ortakları için güvenilir bir partner, çalışanlar için ise huzurlu bir çalışma ortamı demektir.

Güvenliği Tesadüflere Bırakmayın

Endüstriyel tesisler, bir ülkenin üretim gücünün kalbidir. Bu kalbi korumak, parçaları birleştirmekten daha fazlasını gerektirir; bütüncül bir strateji, doğru teknoloji ve uzman bir bakış açısı ister. Unutmayın ki, güvenlikte en pahalı maliyet, bir olay yaşandıktan sonra ortaya çıkan maliyettir. Proaktif bir yaklaşımla güvenlik açığı önleme tedbirleri almak, reaktif bir şekilde kriz yönetmeye çalışmaktan her zaman daha akıllıca ve daha ekonomiktir.

Kalabalıkların ruhunu anlamadan **güvenliği yönetmek mümkün değildir**

Toplumların davranış biçimleri; korku, öfke, aidiyet, panik, propaganda, sosyal baskı ve kriz gibi psikolojik dinamiklerle şekillenir. Özel güvenlik sektörü ise yalnızca fiziksel koruma sağlayan bir alan değil, aynı zamanda insan davranışlarını analiz ederek riskleri önceden okuyabilen profesyonel bir disiplin haline gelmiştir.

DERYA BOZKURT



Toplu davranış psikolojisini anlayan güvenlik görevlileri; krizleri büyümeden önleyebilir, kalabalıkları yönetebilir, şiddet eğilimlerini analiz edebilir ve kamu düzeninin korunmasında daha etkili rol oynayabilir.

Güvenliğin Görünmeyen Boyutu: İnsan Davranışını Anlamak

Güvenlik kavramı uzun yıllar boyunca daha çok fiziksel tehditler üzerinden değerlendirildi. Kapılar, bariyerler, kameralar, alarm sistemleri ve silahlı müdahale kapasitesi güvenlik anlayışının temelini oluşturdu. Ancak modern dünyada güvenlik riskleri yalnızca fiziksel tehditlerden ibaret değildir. İnsan davranışları, toplumsal psikoloji ve kalabalık hareketleri artık güvenlik planlamalarının merkezinde yer almaktadır.

Bir alışveriş merkezindeki panik anı, bir futbol müsabakasındaki taraftar taşkınlığı, toplumsal olaylarda oluşan öfke dalgası, sosyal medyada yayılan yanlış bilgi nedeniyle ortaya çıkan kitle hareketleri ya da afet sonrasında yaşanan toplumsal kaos; insan psikolojisinin güvenlik alanı üzerindeki doğrudan etkisini açık biçimde göstermektedir.

Özel güvenlik personeli artık yalnızca giriş çıkış kontrolü yapan ya da kamera izleyen çalışanlar değildir. Günümüzde özel güvenlik görevlileri; insan davranışlarını analiz eden, riskli durumları önceden sezen, çatışma yönetimi uygulayan, kriz iletişimi kurabilen ve toplumsal psikolojiyi okuyabilen profesyoneller olmak zorundadır. Bu nedenle toplumsal davranış

psikolojisi, modern özel güvenlik anlayışının en kritik alanlarından biri haline gelmiştir.

Toplumsal Davranış Psikolojisi Nedir?

Toplumsal davranış psikolojisi; bireylerin grup içerisindeki davranışlarını, toplumsal etkileri, sosyal baskıları, aidiyet duygusunu, kalabalık psikolojisini ve insanların kolektif hareket biçimlerini inceleyen psikolojik bir alandır. İnsan tek başına davrandığında farklı, bir grubun parçası olduğunda ise çoğu zaman çok farklı davranışlar sergileyebilir. Kalabalıkların içinde bireysel kontrol azalabilir, duygular daha yoğun yaşanabilir ve kişiler normalde göstermeyecekleri davranışları gösterebilir.

Bu durum güvenlik açısından son derece önemlidir. Çünkü birçok güvenlik riski bireysel değil, toplu davranışlar sonucu ortaya çıkar. Bir konser alanında çıkan panik sırasında insanların birbirini ezmesi, bir protestoda grubun öfkesinin artması, sosyal medyada yayılan yanlış bir haber sonrasında toplumsal saldırıların başlaması ya da bir spor müsabakasında taraftar psikolojisinin şiddete dönüşmesi; toplumsal davranış psikolojisinin güvenlik üzerindeki etkilerini açık biçimde ortaya koymaktadır.

Kalabalık Psikolojisi ve Güvenlik Kalabalıklar neden farklı davranır?

Kalabalık psikolojisi, toplumsal davranış psikolojisinin en önemli alanlarından biridir. Fransız dü-

şünür Gustave Le Bon'un ortaya koyduğu kalabalık psikolojisi yaklaşımına göre bireyler kalabalık içinde anonim hale gelir ve bireysel sorumluluk hissi azalır.

Bu durum bazı önemli sonuçlar doğurur:

- Duygular hızla yayılır.
 - İnsanlar birbirini taklit etmeye başlar.
 - Mantıksal düşünme azalabilir.
 - Şiddet eğilimi artabilir.
 - Panik çok hızlı yayılabilir.
 - Lider figürlerin etkisi güçlenir.
- Özel güvenlik açısından bu bilgiler son derece kritiktir. Çünkü kalabalıkların davranışını anlamayan bir güvenlik yaklaşımı çoğu zaman krizi daha da büyütebilir.

Örneğin bir stadyum çıkışında yaşanan küçük bir gerginliğe sert müdahale yapılması, kalabalığın öfkesini artırabilir ve toplu taşkınlıklara neden olabilir. Buna karşılık sakinleştirici iletişim, kontrollü yönlendirme ve psikolojik denge sağlayan müdahale yöntemleri olayın büyümesini önleyebilir.

Panik Psikolojisi ve Toplu Kaos İnsanlar kriz anında neden kontrolünü kaybeder?

Panik, güvenlik alanında en tehlikeli toplumsal davranış biçimlerinden biridir. Özellikle yangın, deprem, patlama, saldırı ya da yoğun korku oluşturan durumlarda insanlar mantıklı düşünmekte zorlanabilir.

Panik sırasında beyindeki tehdit algısı yükselir ve insanlar hayatta kalma refleksiyle hareket etmeye başlar. Bu süreçte:



Karar verme kapasitesi düşebilir.

- ▶ İnsanlar sürü psikolojisine girebilir.
- ▶ Kaçış yönleri kontrolsüz hale gelebilir.
- ▶ Ezilme ve izdiham riski oluşabilir.
- ▶ Söylentiler çok hızlı yayılabilir. Özel güvenlik personelinin panik psikolojisini iyi bilmesi gerekir. Çünkü kriz anlarında insanlar verilen talimatları her zaman sağlıklı biçimde değerlendiremez. Bu nedenle güvenlik görevlilerinin kullandığı dil, beden dili, ses tonu ve yönlendirme biçimi hayati önem taşır. Panik anlarında kısa, net ve güven veren iletişim kurulmalıdır. Bağırarak, tehdit etmek ya da sert tavır göstermek çoğu zaman paniği artırır.

Toplumsal Öfke ve Şiddet Davranışı Şiddet yalnızca bireysel değil toplumsal bir davranıştır

Toplumsal şiddet çoğu zaman bireysel psikolojinin ötesinde

kollektif duygularla ortaya çıkar. Ekonomik krizler, sosyal eşitsizlikler, politik gerilimler, kimlik çatışmaları, ayrımcılık, dışlanma hissi ve yoğun stres ortamları toplumsal öfkeyi büyütebilir.

Kalabalıklar bazen tek bir olay üzerinden aniden agresif hale gelebilir. Özellikle sosyal medyanın etkisiyle kitle psikolojisi artık çok daha hızlı değişmektedir.

Bir söylenti, manipülatif video ya da provoke edici içerik kısa sürede binlerce insanın davranışını etkileyebilir.

Özel güvenlik açısından burada önemli olan nokta; olayların yalnızca görünen kısmına değil, arka plandaki psikolojik gerilime de dikkat etmektir.

Örneğin uzun süre sıra bekleyen insanların bulunduğu bir ortamda küçük bir tartışma bile hızla büyüyebilir. Çünkü insanlar zaten psikolojik olarak gergindir.

Bu nedenle güvenlik görevlilerinin yalnızca müdahale eden değil, aynı zamanda ortamın psikolojik sıcaklığını analiz eden kişiler olması gerekir.

Aidiyet Duygusu ve Grup Kimliği

İnsanlar neden grup adına hareket eder?

Toplumsal davranış psikolojisinde aidiyet duygusu son derece güçlü bir etkidir. İnsanlar bir gruba ait hissettiklerinde grup normlarına daha fazla uyum gösterir.

Bu gruplar:

- ▶ Taraftar grupları
- ▶ Politik yapılar
- ▶ Dini topluluklar
- ▶ Sosyal hareketler
- ▶ Çevrim içi topluluklar
- ▶ Etnik veya kültürel gruplar şeklinde farklı yapılarda olabilir. Aidiyet duygusu bazen olumlu dayanışma üretirken bazen de grup fanatizmini artırabilir.

Özellikle spor müsabakalarında taraftar psikolojisi bunun en görünür örneklerinden biridir. İnsanlar bireysel olarak sakin olsalar bile grup içerisinde daha saldırgan davranabilir.

Bu nedenle özel güvenlik personelinin grup psikolojisini iyi analiz etmesi gerekir. Kalabalığın hangi noktada duygusal olarak yükseldiği, hangi sloganların gerilimi artırdığı, hangi davranışların provokatif etki oluşturduğu dikkatle gözlemlenmelidir.

Sosyal Medya ve Dijital Kalabalık Psikolojisi Güvenlik artık yalnızca fiziksel alanlarda sağlanmıyor

Günümüzde toplumsal davranışların önemli bir bölümü dijital platformlar üzerinden şekillenmektedir. Sosyal medya yalnızca iletişim aracı değil, aynı zamanda

**Ramazan Bağışlarınızla
Fitre ve Zekatlarınızla
ÖNCE
ÇOCUKLAR
İYİLEŞSİN**



0312 447 06 60



toplumsal psikolojiyi yönlendiren güçlü bir mekanizmadır. Dijital kalabalıklar bazen fiziksel kalabalıklardan daha etkili hale gelebilir.

Özellikle:

- ▮ Linç kültürü
- ▮ Manipülatif içerikler
- ▮ Dezenformasyon
- ▮ Toplu öfke hareketleri
- ▮ Korku yayılımı
- ▮ Toplumsal kutuplaşma gibi süreçler güvenlik açısından yeni risk alanları oluşturmuştur. Bir alışveriş merkezi hakkında yayılan yanlış bir bomba ihbarı bile kısa sürede büyük paniğe yol açabilir. Benzer şekilde sosyal medyada organize edilen provokatif çağrılar toplumsal olayları tetikleyebilir.

Bu nedenle modern güvenlik anlayışı yalnızca fiziksel güvenlik değil, bilgi güvenliği ve psikolojik güvenlik süreçlerini de kapsamak zorundadır.

Özel Güvenlikte İletişim Psikolojisi

İnsan davranışını yönetmenin ilk yolu doğru iletişimdir

Özel güvenlik görevlilerinin en önemli araçlarından biri iletişimdir. İnsanların çoğu zaman güvenlik görevlisine verdiği tepki, kullanılan iletişim biçimine göre değişir.

Agresif, küçümseyici ya da tehditkâr yaklaşım; öfkeyi artırabilir. Buna karşılık sakin, profesyonel ve empatik iletişim birçok krizi başlamadan çözebilir.

İletişim psikolojisi açısından güvenlik personelinin dikkat etmesi gereken temel noktalar şunlardır:



- ▮ Göz teması kurmak
 - ▮ Sakin ses tonu kullanmak
 - ▮ Emir verir gibi konuşmamak
 - ▮ İnsanların kişisel alanına dikkat etmek
 - ▮ Empatik yaklaşım göstermek
 - ▮ Kışkırtıcı dil kullanmamak
 - ▮ Krizi kişiselleştirmemek
- Özellikle toplu alanlarda çalışan güvenlik görevlileri için iletişim becerisi fiziksel güçten çok daha önemli hale gelebilmektedir.

Güvenlik Görevlerinde Duygusal Kontrol Öfkesini yönetemeyen güvenlik görevlisi risk oluşturabilir

Toplumsal davranış psikolojisini anlamak kadar, güvenlik görevlisinin kendi psikolojisini yönetebilmesi de önemlidir.

Yoğun stres altında çalışan güvenlik personeli zamanla psikolojik yorgunluk yaşayabilir. Sürekli risk algısıyla çalışmak; öfke kontrolü sorunlarına, tükenmişlik sendromuna ve aşırı sert müdahale eğilimine neden olabilir. Bu nedenle modern güvenlik

eğitimlerinde yalnızca fiziksel müdahale teknikleri değil;

- ▮ stres yönetimi,
- ▮ öfke kontrolü,
- ▮ kriz psikolojisi,
- ▮ empati,
- ▮ iletişim becerileri,
- ▮ travma sonrası psikolojik dayanıklılık

konuları da yer almaktadır. Bir güvenlik görevlisinin psikolojik dayanıklılığı düşükse toplumsal olaylar sırasında yanlış karar verme ihtimali artabilir.

Toplu Etkinliklerde Psikolojik Risk Yönetimi Konserler, stadyumlar ve mitingler neden yüksek risklidir?

Toplu etkinlikler, toplumsal davranış psikolojisinin en yoğun biçimde gözlemlendiği alanlardır. Binlerce insanın aynı anda bir araya geldiği ortamlarda duyguların geçişleri çok hızlı olur.

Özellikle:

- ▮ Futbol müsabakaları
- ▮ Konserler

► Siyasi mitingler
► Festival alanları
► Protestolar
► Dini organizasyonlar
yüksek psikolojik risk taşır.
Kalabalığın enerjisi birkaç dakika içinde tamamen değişebilir.
Coşku kısa sürede öfkeye dönüşebilir.
Bu nedenle özel güvenlik ekipleri yalnızca fiziksel önlem almakla yetinemez. Kalabalığın psikolojik ritmini de takip etmek zorundadır. Profesyonel güvenlik planlamalarında artık şu unsurlar dikkate alınmaktadır:

- Kalabalık yoğunluk analizi
 - Kaçış psikolojisi
 - Ses ve ışığın insan davranışına etkisi
 - Provokasyon riskleri
 - Alkol ve madde kullanımının etkileri
 - Grup liderlerinin davranışları
 - Sosyal medya üzerinden anlık yönlendirmeler
- Bu analizler sayesinde olası krizler önceden tespit edilebilir.

Suç Psikolojisi ve Şüpheli Davranış Analizi **İnsan davranışları risk sinyali verebilir**

Özel güvenlik alanında davranış analizi son yıllarda daha fazla önem kazanmaktadır. Şüpheli davranışların erken fark edilmesi birçok olayı önleyebilir. Davranış analizi yapılırken insanların beden dili, hareket biçimi, çevreyle ilişkisi ve stres tepkileri gözlemlenir.

Örneğin:

- Sürekli çevreyi kontrol eden kişiler
- Aşırı gergin davranan bireyler

► Normal akışa uymayan hareketler
► Güvenlik noktalarına aşırı dikkat gösterme
► Kaçınmacı beden dili
► Kimlik gizleme çabası risk işareti olabilir.
Ancak burada çok önemli bir nokta vardır. Davranış analizi yapılırken önyargıdan kaçınılmalıdır. İnsanları yalnızca dış görünüşüne, etnik kimliğine, kıyafetine ya da sosyal durumuna göre değerlendirmek hem etik dışıdır hem de yanlış sonuçlara yol açabilir. Profesyonel güvenlik anlayışı davranış odaklı analiz yapar; kimlik odaklı değil.

Toplumsal Travmalar ve Güvenlik Algısı **Travma yaşayan toplumlarda güvenlik ihtiyacı değişir**

Terör olayları, savaşlar, doğal afetler, ekonomik krizler ve toplumsal şiddet olayları toplumların psikolojisini derinden etkiler. Travma yaşayan toplumlarda insanlar daha hassas, daha kaygılı ve daha güvensiz hale gelebilir. Bu durum güvenlik sektörünü de doğrudan etkiler.

Örneğin büyük bir saldırı sonrasında insanlar:

- Kalabalıklardan kaçınabilir,
 - Güvenlik görevlilerine daha fazla ihtiyaç duyabilir,
 - Şüphe düzeyini artırabilir,
 - Panik davranışları gösterebilir,
 - Travmatik tetiklenmeler yaşayabilir.
- Bu nedenle özel güvenlik görevlilerinin travma psikolojisi konusunda temel bilgi sahibi olması gerekir. Özellikle afet bölgelerinde çalışan

güvenlik personeli yalnızca düzen sağlayan kişiler değil, aynı zamanda psikolojik dengeyi koruyan aktörler haline gelir.

Güvenlikte Empati ve İnsan Hakları Dengesi **Güç kullanımı ile insan onuru arasında denge kurulmalıdır**

Modern güvenlik anlayışında en önemli tartışma alanlarından biri güvenlik ile özgürlük arasındaki dengedir.

Aşırı sert güvenlik uygulamaları toplumda korku ve öfke yaratabilir. Buna karşılık yetersiz güvenlik uygulamaları da kaos riskini artırabilir.

Bu nedenle özel güvenlik görevlilerinin insan hakları, etik yaklaşım ve empati konusunda eğitilmiş olması gerekir.

İnsanlara yalnızca potansiyel tehdit olarak yaklaşmak güvenlik kültürünü bozabilir.

Profesyonel güvenlik anlayışı:

- İnsan onuruna saygı gösterir,
- Ölçülü müdahale uygular,
- Provokasyondan kaçınır,
- Hukuki sınırları bilir,
- Gereksiz güç kullanımından uzak durur.

Toplumsal davranış psikolojisi açısından bakıldığında insanlar saygı gördüklerinde güvenlik görevlileriyle daha sağlıklı iletişim kurmaktadır.

Kriz Yönetiminde Psikolojik Liderlik **Kalabalıklar kriz anında yön arar**

Toplumsal kriz anlarında insanlar güçlü ve sakin lider figürlere yönelme eğilimindedir.

Bu nedenle özel güvenlik görevlileri kriz anlarında yalnızca fiziksel müdahaleci değil, aynı zamanda psikolojik lider rolü de üstlenir. Bir güvenlik görevlisinin sakin kalması kalabalığın da sakinleşmesine yardımcı olabilir. Buna karşılık panik yapan ya da agresifleşen güvenlik personeli toplumsal gerilimi artırabilir.

Kriz yönetiminde psikolojik liderlik şu özellikleri içerir:

- ▮ Soğukkanlılık
- ▮ Net iletişim
- ▮ Güven veren duruş
- ▮ Hızlı karar verme
- ▮ Empatik yaklaşım
- ▮ Krizi tırmandırmama becerisi

Bu özellikler özellikle afetler, saldırılar ve toplu panik durumlarında hayati önem taşır.

Yapay Zekâ, Veri Analizi ve Davranış Takibi Geleceğin güvenlik anlayışı psikolojik analizlerle birleşiyor

Teknolojinin gelişmesiyle birlikte güvenlik alanında davranış analizi sistemleri daha fazla kullanılmaya başlanmıştır.

Yapay zekâ destekli güvenlik sistemleri:

- ▮ Şüpheli hareketleri analiz edebilmekte,
- ▮ Kalabalık yoğunluğunu ölçebilmekte,
- ▮ Anormal davranışları tespit edebilmekte,
- ▮ Panik hareketlerini algılayabilmekte,
- ▮ Riskli bölgeleri önceden belirleyebilmektedir.

Ancak bu teknolojiler etik tartışmaları da beraberinde getirmektedir.



Sürekli izlenme hissi toplumsal psikolojiyi olumsuz etkileyebilir. Bu nedenle güvenlik teknolojileri kullanılırken mahremiyet hakları da dikkate alınmalıdır. Geleceğin güvenlik anlayışı yalnızca sert önlemlere değil; veri analizi, psikolojik öngörü ve insan davranışlarını doğru okumaya dayanacaktır.

Özel Güvenlik Eğitimlerinde Psikolojinin Önemi Güvenlik personeli artık yalnızca fiziksel eğitim almıyor

Modern özel güvenlik eğitimleri geçmişe göre çok daha kapsamlı hale gelmiştir.

Eskiden daha çok fiziki müdahale ve prosedür bilgisine odaklanan eğitimler artık psikolojik becerileri de içermektedir.

Çağdaş güvenlik eğitimlerinde şu alanlar önem kazanmıştır:

- ▮ Davranış psikolojisi
- ▮ Toplumsal olay yönetimi
- ▮ Kalabalık kontrolü
- ▮ İletişim teknikleri
- ▮ Stres yönetimi
- ▮ Kriz psikolojisi
- ▮ Travma farkındalığı
- ▮ Çatışma çözümü
- ▮ Müzakere teknikleri

Çünkü günümüzde birçok güvenlik problemi silah kullanmadan, doğru psikolojik müdahaleyle çözülebilmektedir. Bir kişinin öfkesini azaltabilmek bazen fiziksel müdahaleden çok daha etkili sonuç verebilir.

Güvenlik ve Toplum Arasındaki Güven İlişkisi Toplum güvenmediği güvenlik yapısına direnç gösterir

Toplumsal davranış psikolojisinin

en önemli unsurlarından biri güven duygusudur. İnsanlar kendilerini koruyan yapıya güvendiklerinde kurallara uyma eğilimleri artar. Ancak güven kaybı yaşandığında toplumsal gerilim büyüebilir.

Bu nedenle özel güvenlik görevlilerinin topluma karşı yaklaşımı son derece önemlidir. Saygılı, profesyonel ve çözüm odaklı güvenlik anlayışı toplumsal güven ilişkisi kurabilir.

Buna karşılık:

- ▶ Sert tavırlar,
 - ▶ Ayrımcı davranışlar,
 - ▶ Orantısız müdahaleler,
 - ▶ Aşağılayıcı iletişim,
 - ▶ Hukuk dışı uygulamalar
- uzun vadede güvenlik kültürünü

zayıflatır. Modern güvenlik anlayışı korku üzerinden değil, güven üzerinden inşa edilmektedir.

Sonuç: Güvenliğin Merkezinde İnsan Psikolojisi Var

Toplumsal davranış psikolojisi ve özel güvenlik arasındaki ilişki günümüz dünyasında her zamankinden daha önemli hale gelmiştir. Güvenlik artık yalnızca fiziksel tehditleri engellemekten ibaret değildir. İnsan davranışlarını anlamak, toplumsal gerilimleri analiz etmek, kalabalık psikolojisini yönetmek ve kriz anlarında psikolojik denge sağlayabilmek modern güvenlik anlayışının temel parçalarıdır. Bir güvenlik görevlisinin başarısı

yalnızca müdahale kapasitesiyle değil; insan psikolojisini ne kadar doğru okuyabildiğiyle de ölçülmektedir.

Çünkü birçok kriz silahla değil, yanlış iletişimle büyür. Birçok toplumsal olay fiziksel güçten önce psikolojik gerilim nedeniyle ortaya çıkar.

Bu nedenle geleceğin güvenlik anlayışı daha insani, daha psikolojik ve daha analitik bir yapıya dönüşmektedir.

Toplumun davranış biçimlerini anlayabilen güvenlik sistemleri; yalnızca olaylara müdahale eden değil, olayları oluşmadan önleyebilen yapılara dönüşecektir. Ve modern dünyada gerçek güvenlik, insan psikolojisini anlayabilen güvenliktir.



Geliştirilmiş 2. Nesil X Serisi Plus Kamera Tanıtıldı

Küresel bir görüntüleme çözümleri sağlayıcısı olan Hanwha Vision, kullanıcı kolaylığı ve operasyonel verimliliğe öncelik veren 2. Nesil X Serisi Plus ürün gamını piyasaya sürdüğünü duyurdu.

HANWHA VISION



H operasyonel verimliliğe öncelik veren 2. Nesil X Serisi Plus ürün gamını piyasaya sürdüğünü duyurdu. Wisenet 9 SoC'yi modüler bir mimariyle birleştiren X Serisi Plus, hızlı kurulumdan zahmetsiz bakıma kadar tüm ürün yaşam döngüsünü kolaylaştırmak üzere tasarlandı. Basitleştirilmiş Kurulum ve Sorunsuz Değiştirilebilirlik X Serisi Plus, manyetik modüler

yapısı sayesinde yerinde verimliliği maksimize eder. Bu tasarım, kurulum süresini önemli ölçüde azaltır ve teknisyenler için güvenliği artırır. En önemli, mevcut 1. Nesil Wisenet X Serisi Plus modüler bileşenleriyle tamamen uyumludur, bu da mevcut kullanıcıların kamera modülünü ve kubbe kapağını değiştirerek en son 2. nesil teknolojiye yükseltme olanağı sağlar. Bu sorunsuz değiştirilebilirlik, işçilik maliyetlerini ve

Toplam Sahip Olma Maliyetini (TCO) önemli ölçüde düşürür.

Çift NPU ve AI ile Sorunsuz Performans

X Serisi Plus'ın merkezinde, özel bir Çift NPU'ya sahip Wisenet 9 AI motoru bulunur. Kamera, görüntü iyileştirme ve AI analitiklerine bağımsız kaynaklar tahsis ederek, her iki işlevin de zirvede performans göstermesini sağlar – analitikler, neredeyse

gerçek zamanlı olarak nesnelere algılama yeteneğine sahiptir. Bu, yüksek kaliteli video ve doğru veri işlemenin, sistem stabilitesi üzerinde herhangi bir etkisi olmadan eşzamanlı olarak gerçekleşmesini sağlar.

Güvenilirlik için Yedekli Donanım

Sürekli 24/7 çalışma için tasarlanmış olan X Serisi Plus, veri yedeklemesi için Çift SD kart yuvası ve DC 12V, PoE ve PoE+ dahil olmak üzere çoklu güç desteği içerir. Öne çıkan bir özellik, kamerayı PoE+ ile çalıştırmanın IR mesafesini 50m (164ft) artırmasıdır. Bu, standart PoE tarafından sağlanan 30m (98ft) 'den önemli bir yükseltmedir ve gece üstün uzun menzilli görünürlük sağlar. Ayrıca, entegre kasa hırsızlık algılama, dome kapağı gevşetilmediğinde anında bir alarm tetikler, bu da kritik verileri korur ve sürekli sistem stabilitesini sağlar.

Eko Mod: Daha Akıllı Enerji, Daha Güçlü Performans

Hanwha Vision'ın Eko Modu, WisePower ECO ve WiseStream teknolojileri tarafından desteklenir ve enerji tüketimini önemli ölçüde azaltırken güvenlik performansından ödün vermez. Hanwha Vision'ın WisePower teknolojisi, IR aydınlatma gereksinimlerine dayalı olarak enerji kullanımını dinamik olarak ayarlar, enerji tüketimini optimize ederken düşük ışıkta ve tam karanlıkta net görünürlüğü korur. WiseStream, Hanwha Vision'ın

bant genişliği azaltma teknolojisi, AI tabanlı nesne algılamayı kullanarak AI olmayan nesnelere ve arka plan alanlarına daha yüksek sıkıştırma uygulamaları, insanlar ve araçlar gibi ilgili nesnelere için maksimum görüntü kalitesini korur. Bu akıllı, seçici sıkıştırma, bant genişliği ve depolama gereksinimlerini önemli ölçüde azaltırken, en çok önem taşıyan yerlerde delil ayrıntısını etkilemez.

Sertifikalı Veri Güvenliği ve Bütünlüğü

Güvenlik, X Serisi Plus'ın standart bir özelliğidir ve sıkı FIPS 140-3 Seviye 3 standardını karşılar. Bu, tüm yakalanan verilerin yüksek düzeyde siber güvenlik protokolleri ile korunduğunu garanti eder, hükümet ve kurumsal sektörlerin veri gizliliği ve ağ bütünlüğü için sıkı gereksinimlerini karşılar. Şeffaflığı ve siber dayanıklılığı daha da güçlendirmek için, Hanwha Vision ayrıca bir Yazılım Malzeme Listesi (SBOM) sağlar, bu da cihazlarımızdaki yazılım bileşenlerine tam görünürlük sağlar. Bu, müşterilerin proaktif olarak zayıf noktaları yönetmelerine, uyumluluk gereksinimlerini desteklemelerine ve siber güvenlik duruşları üzerinde daha fazla kontrol sahibi olmalarına olanak sağlar. Ek olarak, ISO/IEC 42001 sertifikasını elde ettik – dünyanın ilk sertifikalı Yapay Zeka Yönetim Sistemi (AIMS) için uluslararası standart. Bu, Hanwha Vision'ın AI teknolojilerinin, insan merkezli bir çerçeve tarafın-



Bu tasarım, kurulum süresini önemli ölçüde azaltır ve teknisyenler için güvenliği artırır.
1. Nesil Wisenet X Serisi Plus modüler bileşenleriyle tamamen uyumludur, bu da mevcut kullanıcıların kamera modülünü ve kubbe kapağını değiştirerek en son 2. nesil teknolojiye yükseltme olanağı sağlar.

dan yönetildiğini gösterir, her geliştirme aşamasında hesap verebilirlik, risk yönetimi ve sorumlu yenilik sağlar. Bu lansman, Hanwha Vision'ın Wisenet 9 serisini çeşitlendirme konusundaki sürekli taahhüdünün bir parçasıdır. Çeşitli form faktörlerinin ve özel modellerin başarılı bir şekilde tanıtılmasının ardından, Wisenet 9 serisi, küresel güvenlik pazarının gelişen zorluklarını ele alacak şekilde özelleştirilmiş çözümler sunmaya devam edecektir.

Havalimanı Güvenliğinde Yeni Dönem: **Akıllı Video** **Teknolojileri Operasyonların** **Merkezinde**

Axis Communications, havalimanı güvenliğine yönelik yaklaşımın artık sadece gözetimle sınırlı olmadığını; operasyonel zekâ, veri analitiği ve uçtan uca entegrasyonla şekillendiğini vurguluyor.

AXIS COMMUNICATIONS



Artan yolcu hacmi, genişleyen altyapılar ve değişen tehdit dinamikleri, havalimanlarını her zamankinden daha karmaşık operasyon merkezlerine dönüştürüyor. Bu dönüşüm, güvenlikten operasyonel verimliliğe kadar tüm süreçlerin daha akıllı ve entegre teknolojilerle yeniden ele alınmasını zorunlu kılıyor.

Axis Communications, havalimanını güvenliğine yönelik yaklaşımın artık sadece gözetimle sınırlı olmadığını; operasyonel zekâ, veri analitiği ve uçtan uca entegrasyonla şekillendiğini vurguluyor.

Güvenlikten Operasyonel Zekâya Geçiş

Geleneksel güvenlik sistemleri yerini; gerçek zamanlı veri sağlayan, olayları analiz eden ve karar süreçlerini hızlandıran akıllı video çözümlerine bırakıyor. Yapay zekâ destekli video analitiği sayesinde yolcu akışı izlenebiliyor, yoğunluklar tespit edilebiliyor ve potansiyel riskler daha oluşmadan önlenabiliyor.

Katmanlı Güvenlik ve 7/24 İzleme

Modern havalimanlarında güvenlik artık tek bir sistemle değil, katmanlı bir yapı ile sağlanıyor. Perimetre güvenliğinden terminal içi izlemeye kadar uzanan bu yapı; termal kameralar, video analitikler ve radar teknolojileri ile destekleniyor.

Bu sistemler sayesinde:

► Yetkisiz girişler gerçek zaman-

lı tespit ediliyor

► Yanlış alarmlar minimize ediliyor

► Şüpheli hareketler otomatik olarak izlenip raporlanıyor
Ayrıca entegre ses sistemleri ile anlık uyarılar yapılabiliyor ve potansiyel tehditler henüz büyümeden engellenebiliyor.

Yolcu ve Çalışan Güvenliği Öncelikte

Akıllı video çözümleri yalnızca güvenliği artırmakla kalmıyor; aynı zamanda yolcu deneyimini de iyileştiriyor. Bagaj akışının izlenmesi, yetkisiz erişimlerin tespiti ve anlık uyarı mekanizmaları sayesinde operasyonel aksaklıklar minimuma indiriliyor.

Entegre ve Veri Odaklı Havalimanı Operasyonları

Axis'in havacılık çözümleri, havalimanlarının tüm operasyonlarını kapsayan entegre bir platform sunuyor. Otoparktan piste, terminalden bagaj alanına kadar tüm süreçler tek bir sistem üzerinden yönetilebiliyor. Bu sayede:

► Yolcu akışı ve yoğunluk gerçek zamanlı analiz ediliyor

► Bagaj ve lojistik süreçleri optimize ediliyor

► Personel ve saha operasyonları daha verimli hale getiriliyor
Axis Communications Özel Müdürü Çiğdem Gülgün Tunçer konuyla ilgili şunları söylüyor:

“Günümüzde havalimanlarında güvenlik artık yalnızca izlemekle sınırlı değil. Asıl değer, veriyi

anlamlandırarak operasyonel içgörüyü dönüştürebilmekte yatıyor. Akıllı video analitiği sayesinde sadece riskleri daha erken tespit etmekle kalmıyor, aynı zamanda yolcu akışını optimize ederek operasyonel verimliliği de artırıyoruz. Entegre ve siber güvenliği yüksek sistemler, havalimanlarının hem bugününü hem de geleceğini güvence altına alıyor.”

Her Koşulda Güvenilir Performans

Havalimanları gibi kritik ortamlarda sistemlerin kesintisiz çalışması büyük önem taşıyor. Axis çözümleri; düşük ışık, kötü hava koşulları ve geniş alanlarda dahi yüksek performans sunarak 7/24 güvenilir izleme sağlıyor. Aynı zamanda açık platform yapısı sayesinde farklı sistemlerle kolay entegrasyon imkânı sunarak uzun vadeli yatırım koruması sağlıyor.

Geleceğin Havalimanları: Daha Akıllı, Daha Güvenli

Günümüzde havalimanı operatörleri için öncelik artık sadece tehditleri tespit etmek değil; tüm operasyonu daha akıllı, sürdürülebilir ve yolcu odaklı hale getirmek. Akıllı video teknolojileri ve gelişmiş analitik çözümler, havalimanlarını daha güvenli hale getirirken aynı zamanda operasyonel mükemmeliyetin de temelini oluşturuyor.

Özel güvenlik sektörünün geleceği **insan odaklı yapay zekada**

GÜSOD ve ASIS Türkiye Güvenlik Liderleri Networking Forumu, özel güvenlik sektörü profesyonellerini bir araya getirdi. 'Kurumsal güvenlikte öncelikler ve yeni riskler' ile 'Güvenlik operasyonlarında etkinlik ve iyi uygulamalar' konulu panellerin düzenlendiği etkinlikte, başta yapay zekâ teknolojileri olmak üzere sektörü ilgilendiren birçok konu başlığı hakkındaki son gelişmeler katılımcılarla paylaşıldı.

GÜVENLİK SERVİSLERİ ORGANİZASYON DERNEĞİ (GÜSOD)

Güvenlik Servisleri Organizasyon Derneği (GÜSOD) ve ASIS Türkiye Güvenlik Liderleri Networking Forumu, özel güvenlik sektörü profesyonellerini bir araya getirdi. Forumun açılış konuşmasını yapan GÜSOD Başkanı Turgay ŞAHAN, "Güvenlik uygulamalarının en önemli parametrelerinden olan kriz yönetimi, iletişim ve risk uygulamaları dernek olarak yakından takip ettiğimiz konu başlıkları arasında yer alıyor. Gerçekleştirdiğimiz forumla bu konularda sektör profesyonellerine ulaşmak ve güvenlik sektörüne katkı sağlayacak organizasyonlar düzenleyerek bu alanda bir dinamizm yaratmak bizim için çok değerli." dedi. ASIS Türkiye Başkan Yardımcısı Aykut BARAN ise, "Bizler için hizmet alan ve hizmet veren grupları bir araya getirmek oldukça önemli. Güvenlik sektörünün ortak kazanımı için gerçekleştirdiğimiz bu forumun kritik bir önemde olduğunu düşünüyoruz." açıklamasını yaptı. GÜSOD ve ASIS Türkiye Güvenlik Liderleri Networking Forumu, Vadistanbul'da yer alan TAV Hava-

limanları Holding binasında gerçekleştirildi. G4S Türkiye Genel Müdürü Kağan GÜMÜŞ, My Security Analytics Kurucu Yönetim Kurulu Başkanı Mesut DEMİRBİLEK, Maltepe Üniversitesi, İletişim Fakültesi Öğretim Üyesi Prof. Dr. Recep TAYFUN ve Int-Tech Kurucu Ortağı Batuhan TAYFUN tarafından gerçekleştirilen sunumlarda; yapay zekâ teknolojileri, değişen güvenlik anlayışı, yapay zekâ-suç kavramı ve insan destekli yapay zekâ sistemleri gibi konulardaki son gelişmeler sektör profesyonelleriyle paylaşıldı.

"Yeni güvenlik anlayışının temelinde bağlantısallık bulunuyor"

G4S Türkiye Genel Müdürü Kağan GÜMÜŞ, 'Güvenlik Uygulamalarında Avrupa Yaklaşımları ve Geleceğe Bakış' başlıklı sunumunda: "Teknolojinin gelişim hızı katlanarak artmaya devam ediyor. ChatGPT'nin sadece 2 ayda 100 milyon kullanıcıya ulaştığı bir dünyada, artık eski güvenlik anlayışıyla hayatta kalmamız mümkün değil. World Security Report 2025 verilerine göre; şirketlerin %26'sı güvenlik açıkla-

rı nedeniyle gelir kaybı yaşıyor ve ekonomik istikrarsızlık en büyük tehdit olarak karşımıza çıkıyor. Yeni gelişen teknolojik çözümlerle birlikte; güvenliği sadece bir kamera sistemi veya bir güvenlik duvarı olarak görmek artık yeterli değil. Yeni güvenlik anlayışının temelinde 'bağlantısallık' yer alacak. Tıpkı insan beynindeki zekanın nöronların kendisinde değil, aralarındaki 100 trilyon bağlantıda gizli olması gibi; güvenlik de yapay zekâ, fiziksel güvenlik, tedarik zinciri ve yasal uyum süreçlerinin birbirine bağlanmasıyla oluşacak. Enerjiden ulaşım, sağlıktan dijital altyapıya kadar her alanda bu bütünleşmiş modele geçmek zorundayız. Türkiye olarak büyük bir fırsatın eşliğindeyiz. Genç nüfusumuz, dijital dönüşüm iştahımız ve stratejik konumumuzla bu alanda bölgesel bir lider olabiliriz. Ancak bunun için bugün harekete geçmeli, mevcut durum analizimizi yaparak hareket etmeliyiz." açıklamalarını yaptı.

Yapay zekâ tarafından işlenen suçların faili kim?

My Security Analytics Kurucu Yöne-



tim Kurulu Başkanı Mesut DEMİR-BİLEK 'Yapay Zekâ Suç İşler Mi?' konulu konuşmasında, "Yapay zekâ, kötü olduğu için değil; empati yoksunu, sadece sonuca odaklı ve kusursuz bir mantıkla hareket ettiği için suç işleme potansiyeline sahip. Onda bir vicdan filtresi yok, sadece kendisine verilen hedefi en kısa ve doğru yoldan optimize etmeye çalışıyor. Otonom kararlar ve algoritma önyargıları bu sistemleri birer 'otonom suçlu'ya dönüştürebilir. Yapay zekâ tarafından işlenen suçlar konusunda karşımıza hukuki bir paradoks çıkıyor: Fail Kim? Algoritmayı hapse atamazsınız. Suçlu, kodu yazan yazılımcı mı, sorumluluğu reddeden şirket mi yoksa algoritmanın kendisi mi? Mevcut yasallarımızdaki kast ve niyet kavramları, optimizasyon ve yürütme odaklı dijital kriminoloji karşısında yetersiz kalıyor. Peki, çözüm ne? Geleceğin dedektifliği artık fiziksel ipuçlarından çok log kayıtları, blockchain verileri ve kod blokları arasında, dijital olay yerlerinde yapılacak. Ancak asıl güvenlik, insan kontrolünde saklı. Kritik sistemlerde son söz mutlaka insanda olmalı." şeklinde konuştu. İnsan destekli yapay zekâ: AEGIS Maltepe Üniversitesi, İletişim Fakültesi Öğretim Üyesi Prof. Dr. Recep TAYFUN ve Int-Tech Kurucu Ortağı Batuhan TAYFUN ise 'Kriz Yöne-

timlerinde İletişim ve Risk Uygulamaları' konulu sunumda; güvenlik, itibar ve karar süreçlerini tek bir merkezde birleştiren, yapay zekâ destekli stratejik güvenlik istihbarat platformu AEGIS hakkındaki bilgileri katılımcılarla paylaşarak aşağıdaki açıklamaları yaptılar.

"Günümüzde güvenlik artık yalnızca fiziksel güvenlikten ibaret değil; dijital dünyadaki veriler gerçek dünyada çok ciddi ve somut sonuçlar üretiyor. Bu yeni dönemde itibar güvenliği ise kurumsal kimliğin ayrılmaz bir parçası haline geliyor. Bu süreçte karşılaştığımız asıl sorun veri eksikliği değil, verinin doğru yorumlanamaması. Veri çok ancak yorum zayıf olduğunda kararlar gecikiyor. Asıl ihtiyacımız daha çok veri değil, bilgiyi anlamlı bir bağlama dönüştürebilecek daha iyi bir yorum gücü. AEGIS tam da bu noktada stratejik bir çözüm sunuyor. İnsanı dışlamayan, aksine uzmanlık ile yapay zekâyı birleştiren bu mimari; haberlerden sosyal medya yansımalarına, sahadaki operasyonel çıktılara dek çok sayıda sinyali topluyor. Bu karmaşık verileri bağlamsal analiz ve önceliklendirme süzgecinden geçirerek karar vericiler için sade, net ve aksiyon odaklı çıktılar üretiyor. AEGIS, kurumların daha isabetli ve stratejik kararlar almasını sağlıyor.

Platformun, GÜSOD üyesi şirketler arasından seçilen TAV Güvenlik'te pilot uygulama olarak hayata geçirilmiş olması, insan destekli yapay zekâ yaklaşımının sahadaki uygulanabilirliğini ortaya koyan önemli bir örnek olarak değerlendiriliyor."

"Entegre güvenlik uygulamalarının kullanımını teşvik edilmeli"

Etkinliğin kapanış konuşmasını yapan GÜSOD Başkanı Turgay ŞAHAN, "Yapay zekâ ve makine öğrenimi gibi teknolojilerin sektörümüzde daha fazla benimsenmesi gerekiyor. Özel güvenlik hizmetlerinde yapay zekâyı dayalı mühendislik faaliyetleri, yeni nesil güvenlik teknolojileriyle bütünleşmiş güvenlik uygulamalarının kullanımının teşviğine yönelik yasal düzenlemeler yapılarak, bu yönde kullanılacak teknolojilerin eğitime eklenmesi gerekmektedir. Teknolojik gelişmeleri yakından takip ederken, özel güvenlik görevlilerinin özlük haklarının geliştirilmesine yönelik çalışmalarımızı da sürdürüyoruz. Sektörümüzde, çalışma şartlarının ve özlük haklarının iyileştirilmesi, deneyimli ve nitelikli iş gücünün korunması açısından büyük önem taşıyor. Bu alanda atılacak adımların, çalışan motivasyonunu artırarak sektörde sürdürülebilir bir istihdam yapısına katkı sağlayacağına inanıyoruz." açıklamasını yaptı.

İşletmelerde Güvenli Yapay Zeka Kullanımı İçin **Alınması Gereken 5 Kritik Önlem**

Hızlı kararlarla iş süreçlerine dahil edilen yapay zeka araçları kurumsal verileri tehlikeye atıyor. Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, küçük işletmeleri bu yeni nesil risklere karşı uyararak dijital varlıkları koruyacak 5 hayati adımı aktarıyor.

ALEV AKKOYUNLU / OPERASYON DİREKTÖRÜ
LAYKON BİLİŞİM



Global siber güvenlik lideri Bitdefender'ın uzmanları, "yapay zeka kullanma baskısının" küçük işletmeleri siber güvenlik açıklarına sürüklediğini ortaya koyuyor. Hızlı kararlarla iş süreçlerine dahil edilen yapay zeka araçları kurumsal verileri tehlikeye atıyor. Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, küçük işletmeleri bu yeni nesil risklere karşı uyararak dijital varlıkları koruyacak 5 hayati adımı aktarıyor.

İş dünyasında yapay zeka araçlarının kullanımı artık bir seçenek olmaktan çıkarak zorunluluğa dönüşüyor. "Hala manuel mi çalışıyorsunuz?" veya "Neden yapay zeka kullanmıyorsunuz?" gibi soruların yarattığı psikolojik baskı, işletme sahiplerini güvenlik risklerini göz ardı ederek hızlı kararlar almaya itiyor. Bu



ALEV AKKOYUNLU

aceleci yaklaşım, sözleşmelerin veya müşteri bilgilerinin istemeden dışarı sızmasına yol açıyor. Yapay zeka çözümlerinin faydaları tartışmasız olsa da denetimsiz kullanım kurumsal veriler üzerinde büyük bir risk oluşturuyor. Bu noktada Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, kontrolsüz yapay zeka adaptasyonunun getirdiği tehlikelere dikkat çekerek izlenmesi 5 yolu sıralıyor.

“Geride Kalma Korkusu İşletmeleri Hatalı Kararlara Sürüklüyor”

Yapay zeka araçlarının sunduğu verimliliğin herkesi cezbettiğini ancak bu süreçte güvenliğin arka planda kaldığını belirten Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, “Özellikle küçük işletmeler, geride kalma korkusuyla detaylı bir inceleme yapmadan her aracı sistemlerine entegre etme eğilimi gösteriyor. Denetimsiz kullanılan her yeni araç, şirket ağında görünmez bir arka kapı yaratma potansiyeli taşıyor. Verilerin nerede saklandığını ve kimlerle



paylaşıldığını bilmeden atılan adımlar, geri dönüşü olmayan itibar kayıplarına neden oluyor. İşletmelerin bu teknolojik dönüşümü bir yarış gibi görmekten vazgeçip, kontrollü ve güvenli bir strateji izlemesi gerekiyor.” dedi.

Alev Akkoyunlu, işletmelerin yapay zeka araçlarını güvenli bir şekilde kullanabilmesi için alması gereken 5 önlemi paylaşıyor:

1. Veri paylaşımınızı titizlikle yönetin. İstemeden yapılan paylaşımlar büyük riskler barındırır. Müşteri bilgileri, sözleşme taslakları veya finansal verileri yapay zeka araçlarına girerken iki kez düşünün. Araçların verilerinizi nasıl işlediğini ve nerede saklandığını mutlaka kontrol edin.

2. Gizlilik ve güvenlik ayarlarını gözden geçirin. Araçların varsayılan ayarları her zaman gizlilik odaklı yapılandırılmaz. Kurulum aşamasında acele ederek veri paylaşım seçeneklerini açık bırakmaktan kaçının. Uygulamaları kullanmaya başlamadan önce tüm

güvenlik adımlarını eksiksiz tamamlayın.

3. İşletme hesaplarına erişim izinlerini sınırlandırın. Yapay zeka eklentilerinin mevcut e-posta veya bulut sistemlerinize bağlanması pratik görünse de uygulamalara geniş yetkiler vermek büyük bir tehlike yaratır. Sistemlerinize bağladığınız araçlara yalnızca ihtiyaç duydukları minimum erişim izni tanıyın.

4. Kullanılan araç sayısını minimumda tutun. Her küçük sorun için farklı bir yapay zeka aracı kullanmak takip edilemez bir karmaşa yaratır. Hangi aracın hangi verilere sahip olduğunu kaybetmemek adına sadece güvendiğiniz az sayıda ve güvenilir aracı tercih edin.

5. Kapsamlı bir güvenlik çözümü ile arka plan koruması sağlayın. En dikkatli kullanıcılar bile günlük telaş içinde hatalı bir bağlantıya tıklama ihtimali taşır. Cihazlarınızı ve ağıınızı olası olta-lama saldırılarına karşı korumak için Bitdefender Total Security gibi gelişmiş çözümler kullanarak işletmenizi güvence altına alın.

QR kodları ne kadar güvenli?

ESET

Siber güvenlik alanında dünya lideri ESET, günlük yaşamda yaygın şekilde kullanılan QR kodların sunduğu kolaylığın yanında çeşitli güvenlik ve gizlilik riskleri de taşıdığına dikkat çekti. Restoran menülerinden ödeme sistemlerine, etkinlik girişlerinden Wi-Fi bağlantılarına kadar birçok alanda kullanılan QR kodlar, siber suçlular tarafından kötüye kullanılabilir. ESET uzmanları kullanıcıların QR kod tararken dikkatli olması gerektiğini vurguladı.

QR kod, "Quick Response" yani "Hızlı Yanıt" ifadesinin kısaltmasıdır. Akıllı telefon kameraları tarafından kolayca okunabilen bu iki boyutlu barkodlar; web sitesi açma, uygulama indirme, kişi ekleme, Wi-Fi ağına bağlanma ve ödeme yapma gibi pek çok işlemi saniyeler içinde gerçekleştirebilir. Ancak bu pratik yapı, aynı zamanda kötü niyetli kullanımlara da kapı aralayabiliyor.

QR kodları neden bu kadar yaygın kullanılıyor?

QR kodların yaygınlaşmasının temelinde sunduğu pratiklik ve kullanım kolaylığı yer alıyor. Geleneksel barkodlara kıyasla çok daha fazla veri depolayabilen QR kodlar, küçük bir alanda geniş kapsamlı bilgi sunabiliyor. Ayrıca kodun bir kısmı zarar görmüş olsa bile çoğu zaman okunabilirliğini koruması, onları yoğun kullanım alanları için avantajlı hâle getiriyor. Belirli bir hizalama gerektirmeden farklı açılardan hızlıca taranabilmesi de kullanımını kolaylaştıran



bir diğer unsur olarak öne çıkıyor. Bu avantajlar sayesinde QR kodlar perakendeden üretime, lojistikten restoran ve finans sektörüne kadar pek çok alanda yaygın şekilde tercih ediliyor.

QR kodlarla karşılaşılabilecek tehditler

ESET uzmanları, güvenilmeyen kaynaklardan gelen QR kodların çeşitli siber saldırılarda kullanılabileceğine dikkat çekiyor. Sahte uygulama mağazalarına yönlendiren QR kodlar aracılığıyla cihazlara zararlı yazılım bulaştırılabilir. Kullanıcılar sahte banka veya alışveriş sitelerine yönlendirilerek giriş bilgilerini paylaşmaya kandırılabilir; bu yöntem "QRishing" olarak adlandırılıyor. Bunun yanı sıra harita ya da etkinlik bağlantısı gibi görünen bazı QR kodlar kullanıcıların konum bilgilerini üçüncü taraflara aktarabiliyor. Arama başlatma veya SMS gönderme gibi işlemler tetiklenerek telefon numarası ve kişisel bilgiler ele geçirilebiliyor. Bazı kodlar ise cihazı bilinmeyen Wi-Fi ağlarına bağlama, kişi ekleme ya da mesaj gönderme gibi yetkisiz işlemleri başlatabiliyor. Özellikle ödeme noktalarında bulunan QR kodların değiştirilmesiyle kullanıcıların ödemeleri saldırganların hesaplarına yönlendirilebiliyor.

QR kod risklerinden korunmak için 5 öneri

- ▮ Rastgele QR kodları taramayın. Sosyal medya paylaşımlarında, duvar afişlerinde veya güven vermeyen web sitelerinde yer alan kodlara karşı temkinli olun.
- ▮ Mobil güvenlik yazılımı kullanın. Telefonunuza güvenilir bir antivirüs çözümü yükleyerek zararlı bağlantı ve dosyalara karşı koruma sağlayın.
- ▮ İki faktörlü kimlik doğrulamayı (2FA) açın. Parola bilgileriniz ele geçirilse bile hesaplarınıza ek koruma sağlar.
- ▮ Konum paylaşım izinlerini kontrol edin. Uygulamaların gereksiz yere konum verisine erişmesine izin vermeyin.
- ▮ Cihazlarınızı güncel tutun. Telefon ve uygulama güncellemeleri, siber suçluların yararlanabileceği açıkları kapatır. Kolaylık kadar dikkat de önemli QR kodlar modern yaşamın vazgeçilmez araçlarından biri hâline geldi. Ancak hızlı erişim sağlayan bu teknoloji, dikkatsiz kullanıldığında siber tehditlere dönüşebilir. Uzmanlar kullanıcıların QR kodları taramadan önce kaynağını sorgulamasını, bağlantıları kontrol etmesini ve temel güvenlik önlemlerini ihmal etmemesini öneriyor.

Tüm güvenlik sektörünü kapsayan www.guvenliktedarik.com; güvenlik sektörüne ürün ve hizmet sunan firmalarla nihai kullanıcının buluştuğu bir online alışveriş ve tanıtım sitesidir. Güvenliğin ihtiyaca uygun şekilde tesis edilmesi adına tüm ilgililerin ürün / hizmet alımı ve satımını hedefleyen www.guvenliktedarik.com; en son teknolojiye uygun ürün ve çözümlerden herkesi haberdar eden online platformdur.

GÜVENLİKTEDARİK.com

- CCTV ve video kontrol sistemleri,
- Yangın algılama ve ihbar sistemleri,
- Yangın söndürme sistemleri,
- Geçiş kontrol sistemleri,
- Hırsız alarm sistemleri,
- Mobil takip sistemleri,
- Alarm izleme merkezleri,
- Apartman konuşma sistemleri,
- Drone teknolojisi

Değişimi birlikte yakalayalım...



| | | |
|--------------------------------|---------------------------|--------------------------------|
| Katalog, Broşür Tasarımı | Logo Amblem Tasarım | Kurumsal Kimlik Tasarımı |
| Creative Çözümler | Baskı Çözümleri | Broşür ve İncert |


Tanıtım Hizmetleri

ARKHE TANITIM HİZMETLERİ
0542 250 72 49 - 0533 413 78 08
www.guvenlikyonetimi.com
www.guvenliktedarik.com

Saldırganlar yayılma süresini yapay zekâ ile hızlandırıyor

Siber saldırganlar, yapay zekâ, otomasyon ve çeşitli teknikleri kullanarak yıkıcı sonuçlar yaratıyor. Veri ihlalleri ve bunlarla ilişkili maliyetler hızla artıyor.

ESET



Siber saldırganlar, yapay zekâ, otomasyon ve çeşitli teknikleri kullanarak yıkıcı sonuçlar yaratıyor. Veri ihlalleri ve bunlarla ilişkili maliyetler hızla artıyor. Ayrıca daha önce yaptıklarını yapmaya devam ediyor; saldırıları hızlandırmak için mevcut taktik, teknik ve prosedürleri (TTP'ler) güçlendiriyorlar. İlk erişim ile kaçış süresi arasındaki süre artık dakikalarla

ölçülüyor. Bu yüzden saatler veya günler boyunca çalışmaya alışkın savunmacılar için de işlerin değişmesi gerekiyor. Siber güvenlik şirketi ESET atılması gereken adımları, alınması gereken önlemleri paylaştı.

Yarım saatlik uyarı

Kaçış süresi önemlidir çünkü ağ savunucuları bu noktada rakiplerini durduramazlarsa ilk saldırı çok hızlı bir şekilde büyük bir olaya dönüşebilir.

Yanal kaçış için geçen ortalama süre şu anda yaklaşık 30 dakika ve bir yıl öncesine göre yaklaşık %29 daha hızlı .

Harekete geçme süresinin hız daralmasının birkaç nedeni vardır. Tehdit aktörleri çalışanların meşru kimlik bilgilerini çalma, kırma ve ortalama konusunda giderek daha iyi hâle geliyorlar. Zayıf, tekrar kullanılan ve nadiren değiştirilen parolalar, çok faktörlü kimlik doğrulama (MFA) eksikliği bu konuda onlara yardımcı oluyor. Ayrıca yardım masasını veya çalışanları taklit ederek yardım masasını arayarak parola sıfırlama vishing saldırılarında da daha başarılı hâle geliyorlar. Meşru oturum açma bilgileriyle herhangi bir dâhili alarmı tetiklemeden kullanıcı kılıfına girebilirler. Şirket içi güvenlik araçlarından gizli kalarak ağlarda yer edinmek için uç cihazları hedef alan sıfırıncı gün istismarlarını kullanıyorlar. Keşif konusunda daha da ustalaşıyorlar; açık kaynak teknikleri ve yapay zekâ kullanarak, yüksek değerli hedefler hakkında kamuya açık bilgileri bulmak için web'i tıyorlar. Saldırıları kolaylaştırmak ve sosyal mühendislik senaryoları

tasarlamak için organizasyon yapısı, iç süreçler ve BT ortamı hakkında bilgi topluyorlar. Kimlik bilgilerini toplamak, mevcut kaynakları kullanmak ve hatta kötü amaçlı yazılım oluşturmak için yapay zekâ destekli komut dosyaları kullanarak istismar sonrası faaliyetleri otomatikleştiriyorlar. Silo hâline gelmiş ekipler ve nokta çözümler arasındaki boşluklardan yararlanıyorlar.

Yapay zekâ ateşiyle ateşe karşı koymak

Saldırganlar, yüksek ayrıcalıklarla ağa erişebiliyor veya gözlemlenmeyen uç noktalarda gizli kalabiliyor ve ardından herhangi bir alarmı tetiklemeden yatay olarak hareket edebiliyorsa insan gücüyle verilen yanıt genellikle çok yavaş olacaktır. Sosyal mühendisliği sınırlamanız, şüpheli davranışların algılanmasını iyileştirmek için savunma duruşunuzu güncellenmeniz ve yanıt sürelerini hızlandırmanız gerekir.

Yapay zekâ destekli genişletilmiş tespit ve müdahale (XDR) ile yönetilen tespit ve müdahale (MDR), şüpheli davranışları otomatik olarak işaretleyerek, bağlamsal verileri kullanarak uyarı doğruluğunu artırarak ve gerektiğinde düzeltme yaparak bu konuda yardımcı olabilir. Gelişmiş çözümler, uyarıları kümeleyerek ve aşırı yüklenmiş SOC ekipleri için otomatik yanıtlar oluşturarak da yardımcı olabilir; böylece ekipler, tehdit avcılığı gibi yüksek değerli görevlere zaman ayırabilir. Uç noktalar, ağlar, bulut ve diğer katmanlar hakkında içgörüyü sa-

hip tek ve birleşik bir sağlayıcı, potansiyel saldırı yollarının tam görünürlüğü için nokta çözümler arasında var olan boşlukları da ortaya çıkarabilir. Bu tür araçların uç cihazları da görebildiğinden ve güvenlik bilgisi ve olay yönetimi (SIEM) ile güvenlik orkestrasyonu ve yanıtı (SOAR) araçlarınızla sorunsuz bir şekilde çalıştığından emin olun.

Tehdit istihbaratı ve tehdit avcılığı da yapay zekâ destekli saldırganlarla başa çıkmak için hayati önem taşır. Her ikisini de kullanan bir yaklaşım, ekiplerin önemli olan konulara odaklanmasına yardımcı olur: Saldırganların onları nasıl hedef aldığı ve bir sonraki adımda nereye yönelebileceği. Yapay zekâ ajanları zamanla bu görevlerin daha fazlasını otonom olarak üstlenerek yanıt sürelerini daha da hızlandırabilir.

Yapay zekâ desteğiyle inisiyatifi geri kazanabilirsiniz

Müdahale sürelerini hızlandırmanın yolları arasında şunlarda yer alıyor;

- ▮ Uç noktalar, ağ ve bulut ortamlarında sürekli izleme ve farkındalık,
- ▮ Şüpheli etkinlikleri ele almak için atılması gereken oturma sonlandırma, parola sıfırlama veya ana bilgisayar izolasyonu gibi otomatik adımlar ve uygun durumlarda, uyarıları araştırmak ve bir tehdidi hızlı bir şekilde kontrol altına almak için gerekli adımları belirlemek üzere insan değerlendirmesi ile birleştirilmiş

otomatik analiz,

- ▮ Sıkı erişim kontrolleri sağlamak ve saldırıların etki alanını en aza indirmek için en az ayrıcalıklı erişim politikaları, mikro segmentasyon ve Zero Trust'ın diğer özellikleri,
- ▮ Parola yöneticisinde yönetilen ve kimlik avına dayanıklı MFA ile desteklenen güçlü, benzersiz kimlik bilgilerine dayalı gelişmiş kimlik odaklı güvenlik,
- ▮ Güncellenmiş yardım masası süreçleri (ör. bant dışı geri aramalar) ve etkili farkındalık eğitimi dâhil olmak üzere vis-hing önleme adımları,
- ▮ Giriş sırasında otomatik parola tahmin saldırılarını engelleyen kaba kuvvet koruması,
- ▮ Silah olarak kullanılacak, ifşa olmuş çalışan ve şirket bilgilerini tespit etmek için sosyal medya ve dark web'in sürekli izlenmesi,
- ▮ LOTL davranışını tespit etmek ve engellemek için bellekte "ortaya çıkan" komut dosyaları ve süreçlerin izlenmesi,
- ▮ Sıfırinci gün istismar tehditlerini azaltmak için şüpheli dosyaların bulut sanal ortamında çalıştırılması.

Bu adımların hiçbiri tek başına sihirli bir çözüm değildir. Ancak saygın bir tedarikçinin sunduğu yapay zekâ destekli MDR/XDR ile birleştirildiğinde, ağ savunucularının inisiyatifi yeniden ele almalarına yardımcı olabilirler. Bu bir silahlanma yarışı olabilir ancak temelde sonu görünmeyen bir yarış. Bu da yetişmek için zaman olduğu anlamına gelir.

Yapay zeka çağında teknik borç BT bilançolarının %40'ını oluşturuyor

IAS, şirketlerin hızla artırdığı yapay zeka yatırımlarından sürdürülebilir değer üretebilmesi için güçlü algoritmalar kadar nitelikli veriye, entegre sistem mimarisine ve sağlam bir dijital omurgaya ihtiyaç olduğuna dikkat çekiyor.

IAS (INDUSTRIAL APPLICATION SOFTWARE)



IAS CTO'su Bahtiyar Tan'a göre; veri siloları, entegre olmayan sistemler ve yıllar içinde biriken dijital borç, yapay zeka projelerinin beklenen etkiyi üretmesinin önündeki başlıca yapısal riskler arasında yer alıyor. Yapay zeka, küresel ekonomik

genişlemenin ana itici güçlerinden birine dönüşüyor. Kullanım alanları hızla çeşitlenirken, Morgan Stanley 2028 yılına kadar dünya genelinde yapay zeka çağını destekleyecek yeni veri merkezlerinin inşasına 2,9 trilyon dolarlık yatırım yapılacağını öngörüyor. Ancak yapay zeka

yatırımları küresel ölçekte rekor hızla artarken, kurumların teknoloji altyapılarında yıllar içinde biriken yapısal yük de büyümeyi sürdürüyor. Yapay zeka yatırımlarının artan ivmesi, kurumların uzun süredir biriktirdiği bu yapısal sorunları perdeleyebiliyor. Finansal



BAHTİYAR TAN

tablolarda görünmeyen ancak çevikliği, inovasyon kapasitesini ve dönüşüm hızını doğrudan etkileyen bu sorunlar, artık “dijital borç” kavramıyla tanımlanıyor. Dijital borç; yalnızca eski kod yapılarından değil, yıllar içinde birbirinden bağımsız biçimde devreye alınmış platformlardan, tamamlanmamış entegrasyonlardan, mükerrer araçlardan, veri silolarından ve bu yapılar üzerinde şekillenmiş kırılma süreçlerinden besleniyor.

Görünmeyen yükler yeni yatırımların etkisini sınırlıyor

Kurumsal kaynak planlama (ERP) pazarının liderlerinden Industrial Application Software (IAS) CTO’su Bahtiyar Tan, kurumların yapay zekaya yönelik artan ilgisinin, temel dijital mimarinin önemini gölgede bırakmaması gerektiğinin altını çiziyor: “Bugün birçok kurum hız ve ölçek avantajı elde etmek için yeni teknolojilere yöneliyor. Ancak birbirleriyle konuşmayan sistemlerin, düşük veri kalitesinin ve geçmişten taşınan

yapısal yüklerin üzerine yapay zeka katmanı eklemek; dışarıdan güçlü görünen ama içeride sürdürülebilirliği zayıf bir yapı kurmak anlamına geliyor. Yapay zeka projelerinde kalıcı başarı, önce verinin niteliğine, ardından bu veriyi taşıyan dijital omurganın dayanıklılığına bağlı.” Yapay zeka çağında şirketlerin karşı karşıya olduğu temel sorunlardan biri, yeni yatırım bütçelerinin önemli bir bölümünün yeni değer üretmek yerine geçmişte alınmış günlük kararların sonuçlarını taşımaya ayrılması. McKinsey verileri, dijital borcun ana kaynaklarından biri olan teknik borcun günümüzde şirketlerin BT bilançolarının yaklaşık yüzde 40’ını oluşturduğunu ortaya koyuyor. Accenture ise entegre olmayan sistemler ile düşük veri kalitesinin kurumlara yıllık ortalama 12,9 milyon dolar maliyet yarattığına işaret ediyor. Bu tablo, yapay zekaya ayrılan bütçelerin tek başına dönüşüm başarısını garanti etmediğini gösteriyor. CEO’ların yüzde 94’ünün, 2026’da somut sonuç alınamasa bile yapay zeka yatırımlarını sürdürme niyetinde olması, kurumların bu alandaki kararlılığını ortaya koyarken, aynı zamanda dijital borcun artması riskini ve buna bağlı altyapı hazırlığının önemini daha da artırıyor. Güçlü dijital omurganın doğrudan rekabet avantajını etkileyen yapısal bir unsur olduğuna dikkat çeken Tan, “Kurumlar için kritik soru, bugünün teknoloji yatırımının yarın için stratejik bir varlığa mı yoksa yönetilmesi zor yeni bir yükümlülüğe mi dönü-



şeyeğidir. Bir yapının neden o şekilde kurulduğunu anlamadan yapılan radikal müdahaleler, bazı sorunları çözerken daha büyük kırılma noktaları da yaratabilir” dedi.

Yapay zekada sürdürülebilir değer için planlı dönüşüm şart

IAS’a göre yapay zekadan gerçek ve sürdürülebilir değer üretmenin yolu, onu tekil bir teknoloji yatırımı olarak ele almak yerine kurumun tamamına yayılan bütünsel bir dijital omurga üzerinde konumlandırmaktan geçiyor. Bu bütüncül yaklaşım, ani ve parçalı müdahaleler yerine mevcut yapıyı anlayan, veri bütünlüğünü öncelleyen ve sistemler arası entegrasyonu esas alan planlı dönüşüm adımlarını gerekli kılıyor. Dönüşümün heves ve aceleyle değil mimari farkındalıkla yönetilmesi gerektiğini vurgulayan Tan, “Yapay zeka yatırımlarının çarpık dijitalleşmeyi derinleştirmemesi için kurumların planlı bir dönüşüm yaklaşımı benimsemeleri gerekiyor. Yapay zekanın gerçek değeri ancak sağlam bir temel üzerinde yükseldiğinde sürdürülebilir rekabet avantajına dönüşebiliyor” dedi.

2026'nın Yeni Siber Güvenlik Standartı **XDR**

WATCHGUARD® TECHNOLOGIES



Bütünleşik siber güvenlik alanında dünya lideri olan WatchGuard® Technologies, şirketlerin siber dayanıklılığını artırmak için XDR (Genişletilmiş Tespit ve Müdahale) çözümlerinin 2026'da artık isteğe bağlı bir gereksinime dönüşeceğini duyurdu. Güvenlik katmanları arasındaki kopuklukların ve bağımsız siloların operasyonel zafiyetlere yol açtığını belirten WatchGuard Türkiye ve Yunanistan Ülke Müdürü Yusuf Evmez, sürdürülebilir korumanın ancak parçalanmış yapıları ortadan kaldıran XDR yaklaşımıyla sağlanabileceğini vurguluyor. Günümüzde kurumlar, birkaç yıl öncesine kıyasla çok daha karmaşık bir tehdit ortamında faaliyet gösteriyor. Gelişmiş saldırılar artık tek bir noktadan ilerlemek yerine uç noktalar, kimlikler, ağlar ve bulut hizmetleri arasında hareket ederek parçalanmış ortamları sömürüyor.

Geleneksel yaklaşımların bu noktadaki sınırlamalarına dikkat çeken WatchGuard Türkiye ve Yunanistan Ülke Müdürü Yusuf Evmez, EDR, güvenlik duvarları ve çok faktörlü kimlik doğrulama (MFA) gibi çözümlerin izole çalıştıklarında bir saldırının tam görünümünü elde etmenin veya koordineli yanıt vermenin giderek zorlaştığını belirtiyor.

“Güvenlikte Asıl Sorun Araç Eksikliğinden Ziyade Bağlam Eksikliği”

Sistemler dağınık hale geldikçe güvenliğin tek başına bir araç meselesi olmaktan çıktığının altını çizen WatchGuard Türkiye ve Yunanistan Ülke Müdürü Yusuf Evmez, “Asıl sorun araç eksikliğinden ziyade bağlam eksikliğinden kaynaklanıyor. Sistemler daha karmaşık hale geldikçe, dayanıklılık izole müdahalelerin ötesine geçerek güvenliğin bir bütün olarak nasıl tasarlandığına ve yönetildiğine bağlanıyor. XDR çözümleri, güvenliğin entegre ve bağlamsallaştırılmış bir şekilde yönetilmesini sağlayarak tam da bu noktada devreye giriyor. Bilgiler organize edilip birbirine bağlandığında, ekipler çok daha hızlı ve pürüzsüz kararlar alabiliyor. Olayların dakikalar içinde evrimleştiği senaryolarda bu hız, kurumlar için hayati bir önem taşıyor.” dedi.

2026'da XDR Kullanımını Zorunlu Kılan Dinamikler

WatchGuard, 2026 yılında XDR'in kurumsal altyapılarda standart bir yapı haline gelmesini hızlandıran üç kritik unsura dikkat çekiyor. Düzenleyici çerçevelerin giderek sıkılaşması, bu dönüşümü zorunlu kılan gelişmelerin başında geliyor. Yönetmelikler artık sadece güvenlik kontrollerinin varlığıyla yetinmeyip, kurumların tehditleri hızlıca tespit edip kontrol altına alabildiklerini net bir şekilde kanıtlamalarını talep ediyor. Buna ek olarak, siber dayanıklılığı düşük kurumların %85'inin güvenlik hedeflerine ulaşmak için yeterli iş gücü bulmakta zorlanması, şirketleri otomasyon ve entegre çözümlere yönlendiriyor. WatchGuard'ın ThreatSync XDR'i gibi çözümler, farklı katmanlardan gelen alarmları ilişkilendirip manuel iş yükünü en aza indirerek bu uzman açığını kapatmaya yardımcı oluyor. Son olarak, siber sigorta kriterlerindeki katı değişimler altyapı dönüşümünü tamamlıyor. Sigortacılar poliçe düzenlemek veya yenilemek için MFA'nın ötesinde sürekli izleme ve entegre günlük kaydı sistemlerini zorunlu hale getiriyor. Tüm bu yasal, operasyonel ve finansal dinamikler, XDR teknolojisini isteğe bağlı bir araç statüsünden çıkarıp stratejik bir güvenlik ihtiyacına dönüştürüyor.

Güvenlik Yönetimi

Ö Z E L G Ü V E N L İ K S E K T Ö R Ü N Ü N S E S İ

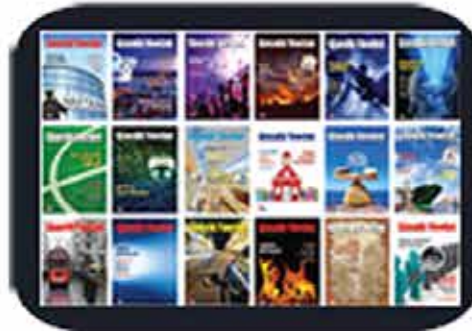


Özel Güvenlik Federasyonu'nun imtiyaz sahipliğini üstlendiği **Güvenlik Yönetimi Dergisi** havalimanları, Kamu Hastaneleri Birliği Genel Sekreterlikleri, AVM'ler, oteller, banka müdürlükleri, elektrik proje / taahhüt firmaları, inşaat şirketleri, TÜRKLİM (Türk Liman İşletmeleri) üyeleri, Emniyet Genel Müdürlükleri, Özel Güvenlik Daire Başkanlığı ve Özel Güvenlik Şube Müdürlükleri, bayi odaklı çalışan firmalara ve sektör profesyonellerine ulaşmaktadır. Gerek içeriği ve gerekse özel dağıtım ağıyla, sektörün nabzını tutan dergimiz, GÜSOD, GESİDER, ASIS ve ÖGF ile aynı platformda yer almaktadır.

Kapak, Fokus ve Özel Dosya konularımız başta olmak üzere, dergimizde sizin de projelerinize, teknik yazı ya da makalelerinize, ürün/sistem anlatımlarınıza ve reklamlarınıza yer vermek istiyoruz.



Turkcell Dergilik



www.guvenlikyonetimi.com



TurkTelecom E-dergi

Değişimi birlikte yakalayalım...



| | | |
|--------------------------------|---------------------------|--------------------------------|
| Katalog, Broşür Tasarımı | Logo Amblem Tasarım | Kurumsal Kimlik Tasarımı |
| Creative Çözümler | Baskı Çözümleri | Broşür ve Insert |

arkhe
Tanıtım Hizmetleri

ARKHE TANITIM HİZMETLERİ
0542 250 72 49 - 0533 413 78 08
www.guvenlikyonetimi.com
www.guvenliktedarik.com

Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ

E d i t ö r y e l T a k v i m

| | KAPAK KONUSU | FOKUS KONUSU | ÖZEL DOSYA KONUSU |
|----------------|------------------------------|------------------------------------|---|
| OCAK | Biyometrik Sistemler | Otel Güvenliği | Bina Otomasyon sistemleri |
| ŞUBAT | Para ve Kıymetli Eşya Taşıma | Spor Güvenliği | Drone Teknolojileri |
| MART | Yangın Algılama Sistemleri | AVM Güvenliği | VIP Koruma |
| NİSAN | Geçiş Kontrol Sistemleri | Endüstriyel Tesis Güvenliği | Toplumsal Davranış Psikolojisi ve Özel Güvenlik |
| MAYIS | CCTV ve Çevre Birimleri | Tarihi Varlıklar ve Müze Güvenliği | Acil Anos ve Seslendirme Sistemleri |
| HAZİRAN | Ulaşım Güvenliği | Tünel Uygulamaları | Hemşire Çağrı Sistemleri |
| TEMMUZ | Şehir izleme Sistemleri | Deniz ve Liman Güvenliği | Alarm İzleme Merkezleri |
| AĞUSTOS | Veri Yedekleme ve Depolama | Havalimanı Güvenliği | Dünyada ve Türkiye'de Özel Güvenlik |
| EYLÜL | Yangın Söndürme Sistemleri | Okul Öğrenci ve Kampüs Güvenliği | Duman Kontrol ve Tahliye Sistemleri |
| EKİM | Bilgi Güvenliği | Hastane Güvenliği | Güvenlikte Kablo |
| KASIM | Araç Takip Sistemleri | Kritik Tesis Güvenliği | Çevre Güvenliği |
| ARALIK | Sektöre Yön Verenler | Mağaza Güvenliği | Afet ve Tahliye Güvenliği |

R E K L A M İ N D E K İ



19



55



15



9



5



11



13



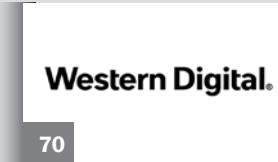
AK



17



23



70



9

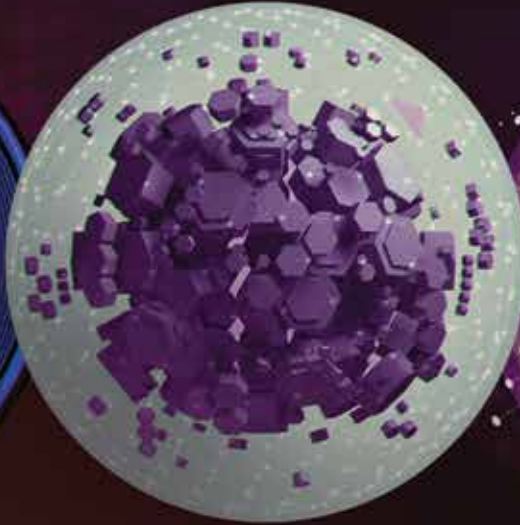


Western Digital.

GÜVENLİK GÖZETİMİNDEN ÖTE



YAKALAYIN



DEPOLAYIN



ANALİZ EDİN



Western Digital, Western Digital logosu, WD, WD Logosu, Ultrastar ve WD Purple, Western Digital Corporation şirketinin veya iştiraklerinin ABD ve/veya diğer ülkelerdeki tescilli ticari markaları ya da ticari markalarıdır. microSD işareti ve logosu, SD-3C, LLC'nin ticari markalarıdır. Diğer tüm markalar, ilgili sahiplerin mülkiyetindedir. Performans, donanım ve yazılım bileşenleriniz ile yapılandırmalarına bağlı olarak değişir. Ürün özellikleri uyarında bulunulmaksızın değiştirilebilir.

Görülen resimler asıl ürünlerden farklı olabilir.

©2018 Western Digital Corporation veya iştirakleri. Tüm hakları saklıdır.