AVRUPA BİRLİĞİ

NIS2 DİREKTİFİ

(Directive EU 2022/2555)

Birlik Genelinde Yüksek Düzeyde Ortak Siber Güvenlik İçin Önlemler

CISO'lar ve Uyum Yöneticileri için Türkçe Özet

Belge Bilgileri

Alan	Değer
Resmi Adı	Directive (EU) 2022/2555
Kabul Tarihi	14 Aralık 2022
Yayım Tarihi	27 Aralık 2022 (OJ L 333/80)
Yürürlük Tarihi	16 Ocak 2023
Ulusal Aktarım Son Tarihi	17 Ekim 2024
Yürürlükten Kaldırılan Araç	Directive (EU) 2016/1148 (NIS1)

> Bu belge, 14 Aralık 2022 tarihli AB NIS2 Direktifi'nin gayri resmi bir özetidir; yetkili bir çeviri niteliği taşımaz. Bağlayıcı yorum için OJ L 333/80, 27.12.2022 adresindeki resmi metne başvurunuz.

İçindekiler

1. Yönetici Özeti

NIS2 Direktifi (Directive EU 2022/2555), Avrupa Parlamentosu ve Konseyi tarafından 14 Aralık 2022'de kabul edilen ve AB'nin genel siber güvenlik taban direktifidir. 18 Ekim 2024 itibarıyla önceki NIS1 Direktifi 2016/1148'i yürürlükten kaldırarak yerini almıştır.

Yapılan incelemeler, NIS1'in Birlik genelinde siber dayanıklılık düzeyinin yükseltilmesine katkı sağlamış olmakla birlikte, bugünün ve geleceğin siber güvenlik tehditlerini karşılamak için yetersiz kaldığını ortaya koymuştur. NIS2; kapsamı önemli ölçüde genişletmekte, tekdüze kriterler getirmekte, risk yönetimi ve olay raporlama yükümlülüklerini güçlendirmekte ve daha caydırıcı yaptırım hükümleri öngörmektedir.

Direktifin Beş Temel Sütunu

1. **Genişletilmiş kapsam**: daha fazla sektör ve şirket düzenleme kapsamına alınmıştır.
2. **Sıkılaştırılmış risk yönetimi**: Article 21 kapsamında 10 asgari teknik ve organizasyonel tedbir zorunlu hale getirilmiştir.
3. **Hızlı ve aşamalı olay raporlama**: 24 saatlik erken uyarı, 72 saatlik olay bildirimi, 1 aylık nihai rapor.
4. **Yönetim organı sorumluluğu**: üst yönetim kişisel olarak sorumlu tutulabilir.
5. **Caydırıcı cezalar**: yıllık küresel ciro üzerinden yüzde 2 veya 10 milyon Euro'ya kadar idari para cezası.

2. Amaç ve Hukuki Dayanak

Direktifin hukuki dayanağı, iç pazarın kurulması ve işleyişinin sağlanması amacıyla ulusal kuralların yakınlaştırılmasına ilişkin tedbirlere olanak tanıyan **Avrupa Birliği'nin İşleyişi Hakkındaki Antlaşma'nın (TFEU) 114. maddesidir**.

Direktifin temel hedefleri şunlardır:

- Üye Devletler arasındaki büyük farklılıkları gidermek ve ortak asgari siber güvenlik kuralları oluşturmak;
- Sınır ötesi iş birliği ve bilgi paylaşımı için etkin mekanizmalar kurmak;
- Siber güvenlik yükümlülüklerine tabi sektörler ve faaliyetler listesini güncel tehdit ortamını yansıtacak şekilde güncellemek;
- Yükümlülüklerin etkin biçimde uygulanmasını sağlayan yaptırım ve başvuru mekanizmaları sunmak;
- Kritik altyapı operatörleri ve dijital hizmet sağlayıcılarının siber dayanıklılık kapasitelerini güçlendirmek.

Direktif, kişisel verilerin korunmasına ilişkin AB mevzuatına (GDPR, Regulation EU 2016/679) ve elektronik iletişim gizliliğine (Directive 2002/58/EC) halel getirmeksizin ve bu mevzuata uygun biçimde uygulanır.

3. NIS1'den NIS2'ye: Neden Yeni Bir Düzenleme?

2016 yılında yürürlüğe giren NIS1, AB'nin ilk yatay siber güvenlik düzenlemesiydi. İnceleme süreci, uygulamada Üye Devletler arasında ciddi farklılıklar bulunduğunu ve kapsam belirlemenin büyük ölçüde Üye Devletlerin takdirine bırakılması nedeniyle iç pazarın parçalandığını ortaya koydu.

NIS1'de Tespit Edilen Eksiklikler

Sorun Alanı	NIS1 Durumu	NIS2 Çözümü
Kapsam belirleme	Üye Devletlerin takdirine bırakıldı; uygulamada önemli farklılıklar oluştu.	AB genelinde tekdüze "büyüklük eşiği" kuralı (orta ve büyük ölçekli işletmeler).
Sektör listesi	Sınırlı sayıda sektör; dijital ekonominin önemli bir bölümü kapsam dışında kaldı.	Çok daha geniş sektörel kapsam; dijital altyapı, kamu yönetimi, uzay vb. dahil edildi.
Olay raporlama	Tek aşamalı; son tarihler ve içerik Üye Devletler arasında farklılık gösterdi.	Çok aşamalı raporlama: 24 saatlik erken uyarı + 72 saatlik bildirim + 1 aylık nihai rapor.
Risk yönetimi	Genel ifadeler; belirli asgari tedbirler net değildi.	Article 21, 10 zorunlu asgari tedbir kategorisini listelemektedir.
Cezalar	Üye Devletler arasında çok farklı düzeylerde uygulandı.	AB genelinde uyumlaştırılmış azami cezalar (10 milyon Euro / cirosunun yüzde 2'si).
Üst yönetim sorumluluğu	Net değildi.	Yönetim organı uyumdan kişisel olarak sorumlu; zorunlu eğitim.

NIS2, NIS1'in bir güncellemesi değil; Birlik genelinde **tek uyumlu ve uygulanabilir bir siber güvenlik çerçevesi** oluşturmak amacıyla hazırlanmış bir yeniliktir.

4. Kapsam ve Hariç Tutulan Alanlar

Direktif, AB içinde **Annex I (yüksek kritiklik)** veya **Annex II (diğer kritik)** sektörlerinde faaliyet gösteren ve en az orta ölçekli işletme tanımını karşılayan kuruluşları kapsar. Komisyon Tavsiyesi 2003/361/EC'nin Eki'nin 2. maddesine göre orta ölçekli işletme, 250'den az çalışana ve 50 milyon Euro'yu aşmayan yıllık ciroya (veya 43 milyon Euro'yu aşmayan bilanço toplamına) sahip işletme olarak tanımlanmaktadır. NIS2, orta ölçekli eşiği karşılayan veya bu eşiğin üzerindeki kuruluşları kapsamaktadır: kapsam dahilindeki kuruluşlar için pratik alt sınır, aynı Tavsiye kapsamındaki "küçük işletme" üst sınırı olan 50 çalışan veya 10 milyon Euro cirodan oluşmaktadır.

Büyüklükten Bağımsız Olarak Kapsama Giren Kuruluşlar

- Kamuya açık elektronik iletişim ağı sağlayıcıları ve kamuya açık elektronik iletişim hizmet sağlayıcıları;
- Güven hizmet sağlayıcıları (eIDAS Regulation EU 910/2014 kapsamında);
- Üst düzey alan adı (TLD) kayıt kuruluşları ve DNS hizmet sağlayıcıları;
- Bir Üye Devlette hizmetin tek sağlayıcısı olan ya da hizmetin kesintiye uğraması durumunda kamu güvenliğini, sağlığını veya emniyetini önemli ölçüde etkileyebilecek kuruluşlar;
- Tüm merkezi kamu idaresi kuruluşları (Üye Devletler tarafından ulusal düzeyde tanımlanır).

Kapsam Dışında Tutulan Alanlar

Faaliyetleri ağırlıklı olarak **ulusal güvenlik, kamu güvenliği, savunma veya kolluk** alanında (suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması) yürütülen kamu kuruluşları direktif kapsamı dışındadır. Üye Devletlerin üçüncü ülkelerdeki diplomatik ve konsolosluk temsilcilikleri ile kapalı sistemlerde kullanılan güven hizmetleri de kapsam dışında tutulmaktadır.

5. Temel Tanımlar

Direktifin doğru yorumlanabilmesi için bazı temel kavramların açıkça anlaşılması gerekmektedir.

Terim	Tanım
Ağ ve bilgi sistemi	Elektronik iletişim ağları; dijital veri işleyen herhangi bir cihaz veya cihaz grubu; bunların işletimi, kullanımı, korunması ve bakımı amacıyla işlenen tüm dijital veriler.
Siber güvenlik	Ağ ve bilgi sistemlerini, kullanıcıları ve diğer kişileri siber tehditlere karşı korumak için gerekli tüm faaliyetler.
Olay	Depolanan, iletilen veya işlenen verilerin ya da ağ ve bilgi sistemleri aracılığıyla sunulan veya erişilen hizmetlerin kullanılabilirliğini, özgünlüğünü, bütünlüğünü veya gizliliğini tehlikeye atan bir olay.
Önemli olay	İlgili kuruluş için hizmetlerin ciddi şekilde aksamasına veya mali kayba neden olan ya da neden olabilecek; ya da diğer gerçek veya tüzel kişilere önemli maddi veya manevi zarar veren ya da verebilecek bir olay.
Siber tehdit	Ağ ve bilgi sistemlerine zarar verebilecek, bunları bozabilecek veya başka şekillerde olumsuz etki edebilecek potansiyel koşul, olay veya eylem.
Önemli siber tehdit	Teknik özellikleri itibarıyla bir kuruluşun ağ ve bilgi sistemleri, kullanıcıları veya diğer kişiler üzerinde önemli maddi ya da manevi zarara yol açacak şekilde ciddi etki yaratma potansiyeline sahip olduğu varsayılan siber tehdit.
Güvenlik açığı	Siber tehdit tarafından istismar edilebilecek BİT ürün veya hizmetlerindeki zayıflık, duyarlılık veya kusur.
Ramak kala	Depolanan, iletilen veya işlenen verilerin ya da ağ ve bilgi sistemleri aracılığıyla sunulan veya erişilen hizmetlerin kullanılabilirliğini, özgünlüğünü, bütünlüğünü veya gizliliğini tehlikeye atabilecekken başarıyla önlenen olay.
CSIRT	Computer Security Incident Response Team; olay müdahalesinden sorumlu teknik ekip.
ENISA	European Union Agency for Cybersecurity; direktifin uygulanmasında merkezi bir danışma ve destek rolü üstlenmektedir.

6. Kuruluş Kategorileri: Temel ve Önemli Kuruluşlar

Direktif, kapsam dahilindeki tüm kuruluşları iki ana kategoriye ayırmaktadır. Bu ayrım, yükümlülüklerin ve denetim/yaptırım rejiminin nasıl uygulanacağını belirler.

Kriter	Temel Kuruluşlar	Önemli Kuruluşlar
Sektör	Annex I, Yüksek kritiklik sektörleri	Annex II, Diğer kritik sektörler (ve Annex I'deki orta ölçekli kuruluşlar)
Büyüklük	Büyük işletmeler (250 ve üzeri çalışan veya 50 milyon Euro ve üzeri ciro)	Orta ölçekli işletmeler (50 ila 249 çalışan)
Denetim rejimi	Hem ön denetim hem de sonraki denetim	Yalnızca kanıt veya şikayete dayalı sonraki denetim
Azami idari para cezası	10 milyon Euro veya küresel yıllık cirosunun yüzde 2'si (hangisi daha yüksekse)	7 milyon Euro veya küresel yıllık cirosunun yüzde 1,4'ü (hangisi daha yüksekse)
Üst yönetim yaptırımları	Geçici yönetim yasağı uygulanabilir	Geçici yönetim yasağı uygulanamaz

Önemli not: Bir kuruluş NIS1 kapsamında "temel hizmet operatörü" olarak tanımlanmışsa, Üye Devlet bu kuruluşun doğrudan NIS2 kapsamında temel kuruluş sayılmasına karar verebilir. Ayrıca Directive 2022/2557 (CER) kapsamında "kritik kuruluş" olarak tanımlanan tüm kuruluşlar, NIS2 kapsamında otomatik olarak temel kuruluş kabul edilir.

7. Kapsam Dahilindeki Sektörler (Annex I ve Annex II)

Annex I, Yüksek Kritiklik Sektörleri

Bu sektörlerdeki büyük işletmeler temel kuruluş; orta ölçekli işletmeler ise önemli kuruluş sayılır.

Sektör	Alt Sektör / Kuruluş Türü
Enerji	Elektrik (üretim, iletim, dağıtım, arz); Bölgesel ısıtma/soğutma; Petrol (boru hattı, üretim, depolama, iletim); Doğalgaz; Hidrojen üretimi, depolanması ve iletimi
Ulaştırma	Hava (havayolları, havalimanları, hava trafik kontrolü); Demiryolu (altyapı işleticileri, demiryolu operatörleri); Deniz/İç su yolu (denizcilik/iç su yolu operatörleri); Karayolu (akıllı ulaşım sistemleri, karayolu operatörleri)
Bankacılık	Regulation (EU) 575/2013 kapsamındaki kredi kuruluşları
Finansal piyasa altyapıları	İşlem yerleri (borsalar) ve merkezi karşı taraflar (CCP)
Sağlık	Sağlık hizmet sağlayıcıları; AB referans laboratuvarları; Tıbbi ürünlerin Ar-Ge faaliyetlerini yürüten kuruluşlar; İlaç üreticileri; Halk sağlığı acil durumlarında kritik sayılan tıbbi cihaz üreticileri (Regulation (EU) 2022/123 uyarınca)
İçme suyu	İnsanın tüketimine yönelik su tedarikçileri ve dağıtıcıları
Atık su	Kentsel atık su, evsel atık su veya endüstriyel atık su toplayan, bertaraf eden veya arıtan kuruluşlar
Dijital altyapı	İnternet değişim noktaları (IXP); DNS hizmet sağlayıcıları (kök DNS hariç); TLD kayıt kuruluşları; Bulut bilişim hizmet sağlayıcıları; Veri merkezi hizmet sağlayıcıları; İçerik dağıtım ağı (CDN) sağlayıcıları; Güven hizmet sağlayıcıları; Kamuya açık elektronik iletişim ağı/hizmet sağlayıcıları
BİT hizmet yönetimi (B2B)	Yönetilen hizmet sağlayıcıları (MSP); Yönetilen güvenlik hizmet sağlayıcıları (MSSP)
Kamu yönetimi	Üye Devletler tarafından tanımlanan merkezi ve bölgesel yönetim kuruluşları
Uzay	Üye Devletler veya özel sektör tarafından işletilen yer tabanlı altyapı operatörleri

Annex II, Diğer Kritik Sektörler

Sektör	Alt Sektör / Kuruluş Türü
Posta ve kurye	Posta hizmet sağlayıcıları (kurye hizmetleri dahil)
Atık yönetimi	Atık toplama, geri dönüşüm ve bertaraf hizmetleri sunan kuruluşlar
Kimyasallar	Kimyasal maddelerin üretimi, işlenmesi ve dağıtımıyla iştigal eden kuruluşlar
Gıda	Gıdanın üretimi, işlenmesi ve toptan dağıtımıyla iştigal eden büyük işletmeler
İmalat	Tıbbi cihazlar/in vitro tıbbi cihazlar; Bilgisayar, elektronik ve optik ürünler; Elektrikli ekipman; Başka yerde sınıflandırılmamış makine ve ekipman; Motorlu taşıtlar, römorklar ve yarı römorklar; Diğer taşıt araçları imalatı
Dijital sağlayıcılar	Çevrimiçi pazar yerleri; Çevrimiçi arama motorları; Sosyal ağ hizmet platformları
Araştırma	Ticari amaçlı araştırma yürüten araştırma kuruluşları

8. Üye Devlet Yükümlülükleri

Direktif, özel sektör kuruluşlarının yanı sıra Üye Devletlere de yükümlülükler getirmektedir. Her Üye Devletin aşağıdaki adımları atması gerekmektedir:

Ulusal siber güvenlik stratejisi. Net stratejik hedefler, öncelikler ve bir yönetim çerçevesi içeren ulusal bir siber güvenlik stratejisi kabul edilmesi. Strateji; tedarik zinciri güvenliği, fidye yazılımları, KOBİ desteği, açık kaynak ve aktif siber savunma gibi konuları kapsamaktadır.

Yetkili otorite(ler). Direktifin uygulanmasını ve denetimini sağlamak üzere bir veya birden fazla yetkili otorite belirlenmesi veya kurulması.

Tek İrtibat Noktası (SPOC). AB düzeyinde sınır ötesi koordinasyondan sorumlu tek bir irtibat noktasının belirlenmesi.

CSIRT. Olay müdahalesi, proaktif izleme, koordineli güvenlik açığı ifşası ile ulusal ve uluslararası iş birliğinden sorumlu bir veya birden fazla CSIRT'in kurulması veya belirlenmesi.

Kuruluş listesi. Temel ve önemli kuruluşların ve alan adı tescil hizmetleri sunan kuruluşların listesinin tutulması, düzenli olarak güncellenmesi ve Komisyon'a iletilmesi.

Koordineli güvenlik açığı ifşası. Koordinatör olarak bir CSIRT'in belirlenmesi; güvenlik açığı araştırmacıları için yasal netliğin sağlanması.

Karşılıklı yardım. Sınır ötesi denetim ve yaptırım konularında diğer Üye Devletlere karşılıklı yardım sağlanması.

KOBİ desteği. Küçük ve mikro işletmeler için rehberlik, ücretsiz araçlar ve ulusal/bölgesel irtibat noktası sağlanması.

9. Siber Güvenlik Risk Yönetimi Tedbirleri (Article 21)

Direktifin en önemli teknik hükmü Article 21'dir. Temel ve önemli kuruluşların uygulamak zorunda olduğu asgari teknik, operasyonel ve organizasyonel tedbirleri listelemektedir. Yaklaşım, **"tüm tehlikeler" perspektifine** dayanmaktadır; yalnızca siber saldırılar değil, fiziksel hasar, doğal afetler, ekipman arızası ve insan hatası gibi tehditler de kapsama alınmaktadır.

Article 21, On Asgari Tedbir

#	Tedbir	Açıklama
1	Risk analizi ve bilgi sistemi güvenlik politikaları	Tüm risklerin analizi ve genel bilgi güvenliği politikalarının yazılı olarak hazırlanması.
2	Olay müdahalesi	Olayların önlenmesi, tespiti, müdahale edilmesi ve kurtarılmasına yönelik süreçler.
3	İş sürekliliği	Yedekleme yönetimi, felaket kurtarma ve kriz yönetimi.
4	Tedarik zinciri güvenliği	Tedarikçilerin güvenlik uygulamalarını da kapsayan; doğrudan tedarikçilerle yapılan sözleşmelere siber güvenlik hükümleri eklenmesi.
5	Ağ ve bilgi sistemlerinin edinimi, geliştirilmesi ve bakımında güvenlik	Güvenlik açığı yönetimi ve ifşasını da kapsayan yaşam döngüsü boyunca güvenlik.
6	Tedbirlerin etkinliğinin değerlendirilmesi	Risk yönetimi tedbirlerinin etkinliğinin düzenli olarak değerlendirilmesi.
7	Temel siber hijyen uygulamaları ve güvenlik eğitimi	Siber hijyen uygulamaları ve personele yönelik farkındalık eğitimleri.
8	Kriptografi ve şifreleme	Şifreleme kullanımına ilişkin politikalar; uygun durumlarda uçtan uca şifreleme.
9	İnsan kaynakları güvenliği, erişim kontrolü ve varlık yönetimi	Personel güvenlik kontrolleri, yetkilendirme ve varlık envanteri.
10	Çok faktörlü kimlik doğrulama ve güvenli iletişim	Uygun durumlarda MFA, sürekli kimlik doğrulama, güvenli sesli/görüntülü/metin iletişimi ve acil durumlarda güvenli iletişim sistemleri.

Bu tedbirler, kuruluşun risk maruziyeti, büyüklüğü, sektörel önemi ve olayların potansiyel etkisi dikkate alınarak **orantılılık ilkesi** çerçevesinde uygulanır.

10. Olay Raporlama Yükümlülükleri (Article 23)

Direktifin en kritik operasyonel yeniliği, çok aşamalı olay raporlama rejimidir. Temel veya önemli kuruluşlar, ciddi operasyonel aksama, mali kayıp veya diğer kişiler üzerinde önemli etki yaratan olaylar olarak tanımlanan **önemli olayları** aşağıdaki süreler içinde CSIRT'e veya yetkili otoriteye bildirmek zorundadır.

Aşama	Son Tarih	İçerik
Erken uyarı	Olaydan haberdar olunmasından itibaren 24 saat içinde	Olayın hukuka aykırı/kötü niyetli bir eylemden kaynaklandığına dair şüphe; sınır ötesi etki ihtimali; CSIRT'in bilgilendirilmesine yönelik temel bilgiler.
Olay bildirimi	Olaydan haberdar olunmasından itibaren 72 saat içinde	Erken uyarının güncellenmesi; şiddet, etki ve mevcut olması halinde uzlaşma göstergeleri (IoC'lar).
Ara/nihai rapor	Olay bildiriminin ardından en geç 1 ay içinde	Olayın ayrıntılı açıklaması, şiddeti ve etkisi; istismar edilen tehdit türü; alınan ve planlanan azaltma tedbirleri; varsa sınır ötesi etki.
İlerleme raporu	Nihai rapor hazırlanması gereken tarihte olay hâlâ devam ediyorsa	Olayın mevcut durumuna ilişkin ilerleme raporu; olayın yönetiminin tamamlanmasından 1 ay sonra nihai rapor.

Hizmet alıcılarının bilgilendirilmesi: Önemli bir siber tehdidin gerçekleşme ihtimali bulunduğunda, kuruluşlar hizmet alıcılarını olası azaltma tedbirleri ve uygun olduğu durumlarda tehdidin kendisi hakkında açık ve anlaşılır bir dille, gecikmeksizin ve ücretsiz olarak bilgilendirmek zorundadır.

Ramak Kalalar ve Gönüllü Raporlama

Olaylara ek olarak, kuruluşlar **ramak kalaları ve önemli siber tehditleri gönüllü olarak** CSIRT'e veya yetkili otoriteye raporlayabilir. Direktif kapsamı dışındaki kuruluşlar da gönüllü raporlama yapabilir. Gönüllü raporlama, raporlayıcıya ek yükümlülük doğurmaz.

> **Pratik etki:** 24 saatlik erken uyarı zorunluluğu, kuruluşları olay tespit edildiğinde anında devreye alınabilecek bir siber olay müdahale planına ve iletişim akışına sahip olmaya zorlamaktadır. Bu süreye manuel ve dağık süreçlerle uymak son derece güçtür.

11. Tedarik Zinciri Güvenliği

Son yıllarda yaşanan büyük siber saldırıların büyük çoğunluğu, hedef kuruluşlara doğrudan saldırı yoluyla değil, tedarikçiler ve yazılım sağlayıcıları üzerinden ulaşmıştır. Bu nedenle direktif, tedarik zinciri riskini risk yönetimi yükümlülüklerinin merkezine yerleştirmektedir.

- Kuruluşlar, tedarikçilerinin ve hizmet sağlayıcılarının ürün/hizmetlerinin **kalitesini, güvenlik uygulamalarını ve güvenli geliştirme süreçlerini** değerlendirmek zorundadır.
- Doğrudan tedarikçilerle yapılan **sözleşmelere siber güvenlik gereksinimleri eklenmelidir**.
- **Yönetilen güvenlik hizmet sağlayıcıları (MSSP)** seçiminde özel özen gösterilmelidir; bu sağlayıcılar saldırganlar için yüksek değerli hedefler olmaktadır.
- Cooperation Group, Komisyon ve ENISA ile birlikte kritik tedarik zincirleri için **koordineli güvenlik riski değerlendirmeleri** yürütmektedir (5G ağları için yapıldığı gibi).
- Üçüncü ülkelerin tedarikçiler üzerindeki olası olumsuz etkisi, gizli güvenlik açıkları/arka kapılar ve sağlayıcıya bağımlılık gibi **teknik olmayan risk faktörleri** de değerlendirme kapsamındadır.

12. Yönetim Organı Sorumluluğu

Direktif, siber güvenliğin yalnızca teknik departmanların konusu olmaktan çıkarak **üst yönetimin doğrudan sorumluluk alanına** girmesini sağlamaktadır. Article 20 uyarınca temel ve önemli kuruluşların yönetim organları:

- Article 21 kapsamındaki risk yönetimi tedbirlerini **onaylamaktan ve uygulanmalarını denetlemekten** sorumludur;
- Bu yükümlülüklerin ihlali halinde **kişisel olarak sorumlu tutulabilir**;
- Yeterli bilgi ve becerileri kazanmak amacıyla düzenli olarak siber güvenlik eğitimi almak zorundadır;
- Personeline de benzer eğitimleri teşvik etmelidir.

> **Önemli:** Temel kuruluşlarda yetkili otorite, üst yönetimden (CEO veya yasal temsilci düzeyindekiler) **geçici yönetim yasağı** uygulanmasını talep edebilir. Bu, yalnızca diğer tüm yaptırım seçenekleri tüketildikten sonra başvurulabilecek son çare niteliğinde bir tedbirdir.

13. AB Düzeyindeki İş Birliği Yapıları

Direktif, Üye Devletler arasında etkin iş birliğini sağlayan çeşitli yapıları düzenlemekte veya güçlendirmektedir:

Yapı	İşlev
Cooperation Group	Stratejik düzeyde iş birliğini destekler; iki yıllık çalışma programları hazırlar; rehber belgeler yayımlar; kritik tedarik zincirleri için koordineli risk değerlendirmeleri yürütür.
CSIRTs Network	Operasyonel düzeyde iş birliği; olay bilgisi paylaşımı; karşılıklı yardım; ortak müdahale.
EU-CyCLONe	Avrupa siber kriz irtibat örgütü ağı; büyük ölçekli olaylarda ve krizlerde teknik ve siyasi düzeyler arasında köprü kurar; etki analizleri hazırlar.
ENISA	Avrupa güvenlik açığı veritabanını kurar ve yönetir; teknik destek sağlar; rehber geliştirir; Üye Devletlerin siber hijyen politikalarını izler.
IPCR Düzenlemeleri	AB Entegre Siyasi Kriz Müdahalesi düzenlemeleri (Council Implementing Decision 2018/1993); büyük ölçekli krizler için Birlik düzeyinde kriz yönetimi.
AB-CSIRT'leri CVD Koordinatörü	Her Üye Devlette bir CSIRT, sınır ötesi koordineli güvenlik açığı ifşasını yönetmek üzere koordinatör olarak belirlenir.

Üçüncü ülkelerle iş birliği: AB, TFEU'nun 218. maddesi kapsamında üçüncü ülkeler veya uluslararası kuruluşlarla uluslararası anlaşmalar akdedebilir. Bu tür anlaşmalar; Birliğin çıkarlarını ve veri korumayı güvence altına alarak söz konusu tarafların Cooperation Group, CSIRTs Network veya EU-CyCLONe faaliyetlerine katılımına olanak tanıyabilir.

14. Denetim ve Yaptırım

Direktif, iki kuruluş kategorisi için farklı denetim rejimleri öngörmektedir. **Temel kuruluşlar** hem ön hem de sonraki denetime tabi tutulurken, **önemli kuruluşlar** yalnızca kanıt veya şikayete dayalı olarak sonraki denetimle denetlenmektedir.

Yetkili Otoritelerin Denetim Yetkileri

- Yerinde denetim ve uzaktan denetim gerçekleştirme;
- Hedefli güvenlik denetimleri talep etme (maliyetleri kuruluşa yüklenebilir);
- Güvenlik taramaları yaptırma;
- Risk yönetimi tedbirlerine uyuma ilişkin belge talep etme;
- Direktifi ihlal ettiğinden şüphelenilen eylemler hakkında bilgi talep etme;
- Gerektiğinde kişisel verilere ve trafik verilerine erişim gerektiren bilgileri talep etme.

Uygulanabilecek Yaptırım Tedbirleri

- Uyarı ve bağlayıcı talimat verme;
- Belirli tedbirlerin alınmasını veya güvenlik açıklarının belirli bir süre içinde giderilmesini emretme;
- Risk yönetimi tedbirlerini doğrulamak üzere bağımsız denetim yaptırılmasını emretme;
- Kuruluşlara hizmet alıcılarını ihlalin niteliği hakkında bilgilendirmelerini emretme;
- Kamuoyu açıklaması yapma (kuruluşun adını ve ihlalin niteliğini açıklayarak);
- Temel kuruluşlar için (son çare): Sertifika veya yetkilendirmelerin geçici olarak askıya alınması ve üst yönetime geçici yönetim yasağı uygulanması;
- İdari para cezası uygulama veya uygulanmasını talep etme.

15. İdari Para Cezaları

Direktif, Üye Devletler tarafından uygulanan idari para cezaları için **AB genelinde uyumlaştırılmış azami eşikler** belirlemektedir. Bu eşikler, GDPR'a benzer biçimde kuruluşun küresel cirosuyla ilişkilendirilmektedir.

Kuruluş Türü	Azami Tutar (hangisi daha yüksekse uygulanır)
Temel kuruluşlar	10.000.000 Euro veya küresel yıllık cirosunun yüzde 2'si
Önemli kuruluşlar	7.000.000 Euro veya küresel yıllık cirosunun yüzde 1,4'ü

Ceza Belirlemede Dikkate Alınan Faktörler

- İhlalin niteliği, ağırlığı ve süresi;
- Neden olunan maddi veya manevi zarar;
- İhlalin kasıtlı mı yoksa ihmalden mi kaynaklandığı;
- Zararın önlenmesi veya azaltılması için alınan tedbirler;
- Sorumluluk derecesi ve önceki ihlaller;
- Yetkili otorite ile iş birliği derecesi;
- Diğer ağırlaştırıcı veya hafifletici faktörler.

Cezalar **orantılı** olmalıdır; uygulamalarında savunma hakkı, masumiyet karinesi ve etkili başvuru hakkı gibi temel haklar gözetilmelidir. Üye Devletler, ulusal mevzuatın ihlali için cezai yaptırımlar da öngörebilir; ancak hiç kimse aynı eylem nedeniyle **ne bis in idem** ilkesini ihlal edecek biçimde iki kez cezalandırılamaz.

16. Uygulama Takvimi ve Geçiş Süreci

Tarih	Olay
14 Aralık 2022	Direktifin Avrupa Parlamentosu ve Konseyi tarafından kabul edilmesi
27 Aralık 2022	AB Resmi Gazetesi'nde yayımlanması (OJ L 333/80)
16 Ocak 2023	Direktifin yürürlüğe girmesi (yayımdan 20 gün sonra)
17 Ekim 2024	Üye Devletlerin direktifi ulusal hukuka aktarma son tarihi
18 Ekim 2024	Direktifin uygulanmaya başlanması
18 Ekim 2024	Directive (EU) 2016/1148 (NIS1)'in yürürlükten kaldırılması
17 Nisan 2025	Üye Devletlerin temel ve önemli kuruluşlar listesini Komisyon'a iletme son tarihi
17 Ekim 2027 ve sonrası	Direktifin uygulanmasının Komisyon tarafından periyodik olarak gözden geçirilmesi (her 36 ayda bir)

Önemli: NIS2 bir direktiftir; doğrudan uygulanmaz. Her Üye Devletin direktifi kendi ulusal hukukuna aktarması gerekmektedir. Bu nedenle bir kuruluşa uygulanacak kesin yükümlülükler ve cezalar, faaliyet gösterdiği Üye Devlet tarafından kabul edilen ulusal aktarım mevzuatına bağlıdır.

17. AB Dışı İşletmelere Etkileri

NIS2 bir AB direktifi olmakla birlikte, özellikle AB pazarına hizmet veren veya AB merkezli kritik kuruluşlara tedarik yapan AB dışı işletmeler üzerinde önemli etkilere sahiptir:

Doğrudan Etkilenen AB Dışı İşletmeler

- AB'de hizmet sunan AB dışı **DNS sağlayıcıları, bulut hizmet sağlayıcıları, veri merkezi operatörleri, CDN sağlayıcıları, yönetilen hizmet ve yönetilen güvenlik hizmet sağlayıcıları, çevrimiçi pazar yerleri, arama motorları ve sosyal ağ platformları**, bir AB temsilcisi atamak ve direktif yükümlülüklerine uymak zorundadır;
- AB iştiraki veya şubesi bulunan AB dışı şirketler, bu birimler aracılığıyla direktife tabi olabilir;
- AB'deki temel veya önemli kuruluşlara ürün/hizmet temin eden AB dışı tedarikçiler, müşterileri tarafından dayatılan **tedarik zinciri güvenliği sözleşme gerekliliklerine** tabi olacaktır (Article 21(2)(d));
- AB dijital altyapısına veya finans kuruluşlarına hizmet veren AB dışı MSP/MSSP'ler doğrudan kapsam dahiline girebilir.

Dolaylı Etkiler

- AB müşterilerinin tedarik zinciri risk değerlendirmeleri, AB dışı tedarikçileri siber güvenlik standartlarını yükseltmeye zorlamaktadır;
- Direktifin getirdiği standartlar (ISO/IEC 27001, ENISA rehberleri vb.) küresel pazarda **fiili referans noktaları** haline gelmektedir;
- AB dışı yargı bölgeleri, kendi siber güvenlik mevzuatlarını geliştirirken NIS2'yi giderek artan ölçüde referans almaktadır.

18. Pratik Uyum Yol Haritası (10 Adım)

Aşağıdaki 10 adımlı yol haritası, hem AB içinde faaliyet gösteren işletmeler hem de NIS2 standartlarıyla gönüllü olarak uyum sağlamak isteyen işletmeler için pratik bir rehber niteliği taşımaktadır.

Adım	Faaliyet
1. Kapsam belirleme	Şirketin Annex I veya Annex II sektörlerine girip girmediğini, büyüklük kriterlerini karşılayıp karşılamadığını belirleyin ve kategorisini (temel/ önemli) tespit edin.
2. Boşluk analizi	Mevcut bilgi güvenliği yönetim sistemini Article 21'in 10 tedbir kategorisiyle karşılaştırın; boşlukları haritalandırın.
3. Yönetişim yapısı	Yönetim kurulu/üst yönetim düzeyinde sorumlulukları, raporlama hatlarını ve onay süreçlerini belirleyin; düzenli eğitim programı oluşturun.
4. Politika ve dokümantasyon	Bilgi güvenliği politikasını, risk yönetimi politikasını, olay müdahale politikasını, kabul edilebilir kullanım politikasını ve diğer belgeleri hazırlayın veya güncelleyin.
5. Risk değerlendirmesi	Tüm tehlikeler yaklaşımıyla varlık envanteri, tehdit analizi ve risk değerlendirmesi yapın; risk kabul kriterlerini belirleyin.
6. Teknik kontrollerin uygulanması	MFA, şifreleme, ağ segmentasyonu, sıfır güven mimarisi, log yönetimi, SIEM, EDR/XDR, yedekleme ve felaket kurtarma çözümlerini hayata geçirin.
7. Olay müdahale kapasitesi	Olay müdahale planını belgeleyin; rol ve sorumlulukları atayın; 24 saatlik erken uyarı iletişim akışını kurun; masaüstü tatbikatları gerçekleştirin.
8. Tedarik zinciri yönetimi	Tedarikçileri envanterleyin; risk düzeyine göre sınıflandırın; sözleşme şablonlarına siber güvenlik hükümleri ekleyin; periyodik denetimler yapın.
9. Eğitim ve farkındalık	Tüm personel için yıllık siber hijyen eğitimi düzenleyin; yönetim organına özel eğitim sağlayın; kimlik avı simülasyonları yürütün.
10. Sürekli iyileştirme	İç ve dış denetimler gerçekleştirin; KPI'ları takip edin; her olaydan ders çıkarın; risk değerlendirmesini yıllık olarak güncelleyin; sertifikasyon süreçlerini takip edin (ISO/IEC 27001, AB siber güvenlik sertifikası).

19. Sonuç ve Değerlendirme

NIS2 Direktifi, Avrupa Birliği'nin siber güvenlik tabanını önemli ölçüde yükseltmektedir. Yalnızca teknik gereksinimler getirmekle kalmayıp siber güvenliği şirketlerin **yönetim yapısının ve iş faaliyetlerinin ayrılmaz bir parçası** haline getirmektedir.

Direktifin Güçlü Yönleri

- **Geniş erişim**: AB-27 genelinde yaklaşık 18 sektör ve 100.000'den fazla kuruluş kapsam dahilinde;
- **Uyumlaştırma**: AB genelinde tekdüze kriter ve yaptırım rejimiyle iç pazarda eşit rekabet koşulları;
- **Yönetişim odağı**: Üst yönetimi hesap verebilir kılarak siber güvenliğin şirketin tüm katmanlarına nüfuz etmesini sağlama;
- **Tedarik zinciri vurgusu**: Modern saldırıların büyük çoğunluğunun tedarik zinciri üzerinden geldiği gerçeğine karşılık verme;
- **İş birliği yapıları**: Cooperation Group, CSIRTs Network ve EU-CyCLONe aracılığıyla çok katmanlı AB düzeyinde koordinasyon.

Eleştiriler ve Zorluklar

- Üye Devlet aktarımındaki gecikmeler ve farklılıklar; pratikte AB-27 genelinde tekdüze uygulama eksiklikleri;
- Özellikle orta ölçekli işletmeler için uyum maliyeti ve teknik kapasite açığını kapatma ciddi bir zorluk oluşturmaktadır;
- Yeterli olgunluk sağlanmadan 24 saatlik erken uyarı son tarihinin uygulanmaya konması, yüzeysel veya hatalı raporlama akışlarına yol açabilir;
- Sektörel düzenlemelerle (DORA, finans; eIDAS, güven hizmetleri; sektörel havacılık düzenlemeleri vb.) örtüşen alanlar, kuruluşlar için karmaşıklık yaratabilir.

Genel Değerlendirme

NIS2, siber güvenliği teknik bir mesele olmaktan çıkararak **iş sürekliliği, kurumsal yönetim ve müşteri güveni** meselesi olarak yeniden çerçevelemektedir. AB'de faaliyet gösteren veya AB ile etkileşim içinde olan kuruluşlar için uyum, hem yasal bir yükümlülük hem de operasyonel dayanıklılığı güçlendirmenin bir aracıdır.

AB dışındaki işletmeler için NIS2, AB pazarına erişimde yeni bir **fiili standart** oluşturmakta ve küresel ölçekte siber güvenlik beklentilerini yükseltmektedir. Erken uyum, sözleşme yükümlülüklerinin karşılanmasını kolaylaştırmakta ve genel siber dayanıklılığı artırmaktadır.

> **Son not:** Bu belge, direktifin ana hükümlerini Türkçe konuşan okuyucular için özetlemektedir. Kuruluşunuza özgü uyum gereksinimleri için resmi metni (OJ L 333/80, 27.12.2022), faaliyet gösterdiğiniz Üye Devletin ulusal aktarım mevzuatını ve sektöre özgü düzenlemeleri inceleyin; gerektiğinde hukuki ve siber güvenlik danışmanlığı alın.

Kaynaklar

- Directive (EU) 2022/2555, EUR-Lex CELEX numarası 32022L2555
- AB Resmi Gazetesi L 333/80, 27 Aralık 2022
- ENISA, European Union Agency for Cybersecurity (www.enisa.europa.eu)
- Avrupa Komisyonu Dijital Strateji portalı (digital-strategy.ec.europa.eu)

Rediacc'tan NIS2 Hakkında Daha Fazla Bilgi

Bu özet, direktifin yapısını ve yükümlülüklerini ele almaktadır. rediacc.com'daki yardımcı rehberler, söz konusu yükümlülükleri somut operasyonel ve tedarik kararlarına dönüştürmektedir.

Üç yardımcı rehber

- **Article 21(2)(d) ve kendi barındırma.** Veri düzlemi hiçbir zaman kiracınızın sınırlarını aşmadığında üçüncü taraf BİT kaydı neden küçülür. 2026'da DPA'larını yeniden müzakere eden CISO'lar ve tedarik yöneticileri için.
- **Tiyatrosuz sürekli etkinlik.** Article 21(2)(e), (f) ve 23 bir arada ele alındığında. Haftalık tatbikatları gerçekçi kılan sabit süreli fork ve adli kalitede artefaktlar olmadan karşılanamayan Article 23 raporlama takvimi. SRE ve operasyon liderleri için.
- **NIS2 uyumunun yapısal maliyeti.** Orta ölçekli temel kuruluşların sessiz sedasız bir araya getirdiği beş araçlı yığın, kendi barındırmalı bir kontrol düzleminin ortadan kaldırdıkları ve her iki durumda da size ait kalan kalemler. CFO'lar ve yenileme döngüsüne giren alıcılar için.

Nerede bulabilirsiniz

Her üç rehber ve bu özet indirilebilir PDF olarak şu adreste yer almaktadır:

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ, Estonya'da kayıtlı bir kendi barındırmalı altyapı platformudur (Ticaret sicil numarası 17363830, KDV EE102920091). Ürün, bir güvenlik programının yerine geçmez; geleneksel yedekleme, felaket kurtarma ve test verisi araçlarının ortadan kaldıramadığı veri düzlemi satıcı riskini gideren bir araç katmanıdır. Ücretsiz Community katmanı ve aylık 349 dolardan başlayan ücretli katmanlar mevcuttur.

> Bu belge ve yardımcı rehberler eğitim materyali niteliği taşımaktadır. Kuruluşunuza özgü uyum kararları için faaliyet gösterdiğiniz yargı bölgesindeki ulusal aktarım mevzuatına ve hukuk danışmanlığına başvurulması gerekmektedir.