# BORSA İSTANBUL GRUBU
# BİLGİ GÜVENLİĞİ BÜLTENİ


## ARTAN SİBER SALDIRILAR VE OLTALAMA (PHISHING) TEHDİTLERİ

Son dönemde yaşanan bölgesel gelişmelerin etkisiyle Türkiye'deki kamu kurumları ve özel sektöre yönelik siber saldırılarda ciddi bir artış gözlemlenmektedir. Bu saldırılar, hizmet kesintileri ve veri sızıntıları gibi ciddi güvenlik sorunlarına yol açabilmektedir.

### Cloudflare, Küresel Sektörleri Hedefleyen 3,8 Tbps ile Şimdiye Kadarki En Büyük DDoS Saldırısını Püskürttü

Cloudflare, tarihindeki en büyük ve en karmaşık DDoS (Distributed Denial of Service Attack) saldırısını başarıyla bertaraf etmiştir. 3,8 Tbps seviye...

### Bilgi Güvenliği Yönüyle Eylül Ayında Lübnan'da Gerçekleşen Çağrı ve Telsiz Cihazlarına Yönelik Saldırılardan Çıkarılacak Dersler

Eylül ayında Lübnan'da gerçekleşen çağrı ve telsiz cihazlarına yönelik saldırılar, kritik iletişim altyapılarının güvenliğine yönelik tehditleri bir kez daha gündeme getirmişti. Bu ol...

### Internet Archive'a Siber Saldırı: 31 Milyon Kullanıcının Verileri Çalındı

Dijital bilgi ve kaynakların korunmasını amaçlayan önde gelen platformlardan biri olan Internet Archive, geniş çaplı bir veri ihlaliyle karşı karşıya kalmıştır. Saldırı sonu...

# ARTAN SİBER SALDIRILAR VE OLTALAMA (phishing) TEHDİTLERİ

Son dönemde yaşanan bölgesel gelişmelerin etkisiyle Türkiye'deki kamu kurumları ve özel sektöre yönelik siber saldırılarda ciddi bir artış gözlemlenmektedir. Bu saldırılar, hizmet kesintileri ve veri sızıntıları gibi ciddi güvenlik sorunlarına yol açabilmektedir. Özellikle oltalama (phishing) ve sosyal mühendislik saldırılarına karşı farkındalığın artırılması, bilgi güvenliği açısından büyük önem taşımaktadır.

## Oltalama ve Sosyal Mühendislik Saldırılarına Karşı Alınması Gereken Önlemler

- **Gelen E-postalara Karşı Dikkatli Olunması:** Tanınmayan kişilerden gelen veya güvenilir gibi görünse de şüpheli içerik taşıyan e-postalar alındığında, durumun kurumların ilgili bilgi güvenliği birimlerine bildirilmesi önemlidir. Bu tür durumlarda, bilgi güvenliği ekipleri gerekli incelemeleri yaparak olası tehditleri değerlendirmektedir.
- **Kişisel ve Kurumsal Bilgilerin Paylaşılmaması:** Oltalama saldırıları kullanıcı adı, parola veya diğer kişisel bilgileri talep edebilir. Güvenlik politikaları gereği, bu tür bilgilerin e-posta yoluyla paylaşılmaması gerektiği unutulmamalıdır.
- **Kuruma Ait E-posta Adreslerinin Üyeliklerde Kullanılmaması:** İş kapsamı dışında kalan üyelikler için kuruma tahsis edilen e-posta adreslerinin kullanılmaması önerilmektedir. Üye olunan platformlarda yaşanan veri sızıntıları, kurumsal e-posta adresleri ve parola bilgilerinin ifşa edilme riskini artırabilmektedir.


- **Parolaların Güçlü ve Güncel Tutulması:** Güçlü, karmaşık ve düzenli olarak güncellenen parolalar, bilgi güvenliği açısından büyük önem taşır. Ayrıca, iş ortamında kullanılan parolaların kurum dışındaki platformlarda tekrar kullanılmamasına özen gösterilmelidir.
- **Şüpheli Durumların Bildirilmesi:** Bilgi güvenliği açısından şüpheli durumlarla karşılaşılması halinde, kurumların bilgi güvenliği birimleri ile iletişime geçilerek gerekli önlemlerin alınması sağlanmalıdır.

Bu temel güvenlik önlemleri ile oltalama ve sosyal mühendislik saldırılarına karşı daha dirençli olunması ve bilgi güvenliği seviyesinin korunması hedeflenmektedir.

# DDOS ATTACK

## CLOUDFLARE, KÜRESEL SEKTÖRLERİ HEDEFLEYEN 3,8 TBPS İLE ŞİMDİYE KADARKİ EN BÜYÜK DDOS SALDIRISINI PÜSKÜRTTÜ

Cloudflare, tarihindeki en büyük ve en karmaşık DDoS (Distributed Denial of Service Attack) saldırısını başarıyla bertaraf etmiştir. 3,8 Tbps seviyesine ulaşan bu saldırı, şirketin altyapısına yönelik gerçekleştirilen en güçlü DDoS saldırılarından biri olarak kayıtlara geçmiş olup çeşitli sektörlerde faaliyet gösteren dijital varlıklar için kritik bir tehdit teşkil etmektedir. Şirketin bu büyüklükteki bir saldırıyı engelleyebilme kapasitesi, bilgi güvenliği alanında sağlam altyapıların önemini bir kez daha gözler önüne sermektedir.

### Saldırı Nasıl Gerçekleşti?

DDoS saldırıları, hedef sistemlerin aşırı yüklenmesi amacıyla yoğun veri trafiği yaratarak sunucuları devre dışı bırakmaya odaklanmaktadır. Bu saldırıda, siber saldırganlar yüksek hacimli bir botnet ağı kullanarak trafiği olağan dışı seviyelere çıkararak hedef sistem üzerinde baskı kurmayı başarmıştır. DDoS saldırıları, hizmet kesintisi yaratmakla kalmamakta; aynı zamanda veri ihlali ve müşteri kaybı risklerini de artırarak ciddi maliyetlere neden olmaktadır.

### Cloudflare'in DDoS Saldırısına Müdahale Stratejisi

Cloudflare, bu saldırıyı tespit ve bertaraf etmek için dinamik DDoS savunma mekanizmalarını devreye almış; küresel düzeyde yaygın altyapısı aracılığıyla anormal trafik artışlarını otomatik olarak analiz ederek saldırının kaynağını ve yoğunluğunu hızlı bir şekilde belirlemiştir. DDoS önleme sistemleri, saldırı boyunca ölçeklenebilirlik sağlayarak hizmetlerin kesintisiz devam etmesine imkân tanımıştır. Bu sayede müşteriler etkilenmeden saldırının önüne geçilmiş, güvenlik sağlanmıştır.

### Bu Tür Saldırılara Karşı Alınabilecek Önlemler

DDoS saldırıları, dijitalleşme çağında tüm kurumlar için önemli bir tehdit unsuru olmaya devam etmektedir. Bu tür saldırılara karşı savunmayı güçlendirmek için aşağıdaki önlemler önerilmektedir:

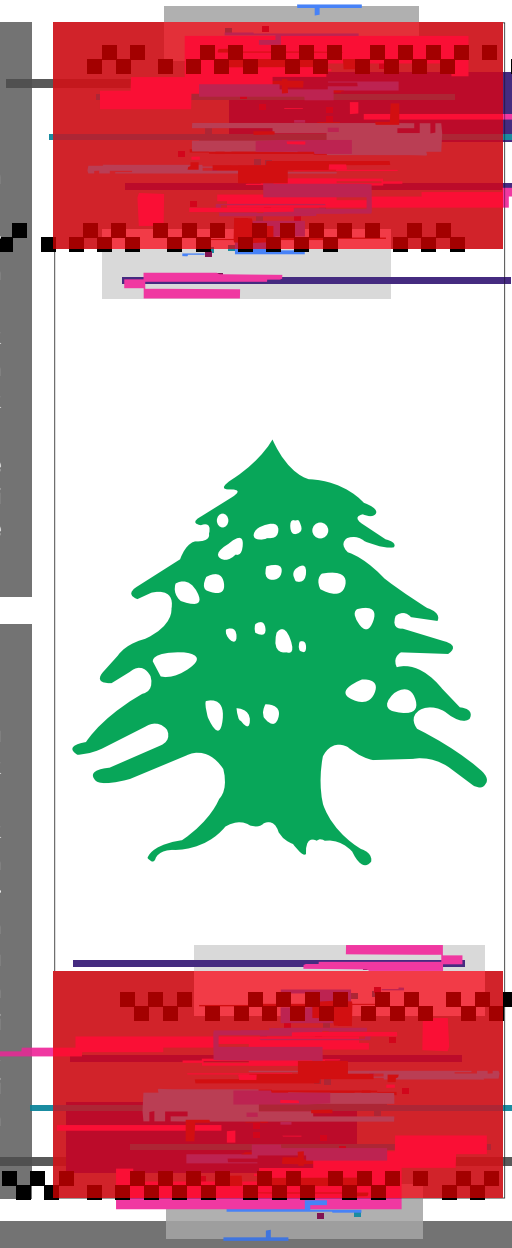
- **Güçlü Altyapı ve Yedekleme Planları:** Geniş ölçekte yedekli sunucu yapıları, DDoS saldırılarının etkilerini azaltmada kritik rol oynamaktadır.
- **Anormallik Tespiti ve Trafik İzleme:** Olağan dışı trafik akışını gerçek zamanlı olarak izleyen sistemler, DDoS saldırılarına karşı erken uyarı sağlamaktadır.
- **İç ve Dış Trafik Filtreleme:** Veri merkezlerinin güvenliğinin sağlanması amacıyla yalnızca yetkili IP adreslerine erişim sağlanarak saldırı ihtimali en aza indirilmektedir.

### Gelecekteki Siber Tehditlere Karşı Hazırlıklı Olmak

Bu olay, özellikle kritik sektörler ve büyük ölçekli altyapılar için siber güvenlik önlemlerinin önemini bir kez daha göstermektedir. Çeşitli endüstrilerde artan dijitalleşme, hizmetlerin kesintisiz devamlılığı için DDoS önleyici sistemlerin sürekli güncellenmesini gerekli kılmaktadır. Cloudflare'in bu saldırıyı başarıyla engellemesi, siber güvenlik dünyasında proaktif önlemlerin ve dayanıklı altyapının önemini bir kez daha kanıtlamaktadır.

# Bilgi Güvenliği Yönüyle Eylül Ayında Lübnan'da Gerçekleşen Çağrı ve Telsiz Cihazlarına Yönelik Saldırılardan Çıkarılacak Dersler

Eylül ayında Lübnan'da gerçekleşen çağrı ve telsiz cihazlarına yönelik saldırılar, kritik iletişim altyapılarının güvenliğine yönelik tehditleri bir kez daha gündeme getirmişti. Bu olaydan çıkarılabilecek önemli dersler, değişiklik yönetimi, tedarik zinciri güvenliği ve standartların önemini gözler önüne sermektedir. Bu başlıklar, sadece kamu kurumları değil, tüm sektörler için siber güvenlik stratejilerini geliştirmede büyük bir rol oynamaktadır.



## Değişiklik Yönetimi ve Risk Analizinin Önemi

Kritik iletişim altyapılarına yapılan saldırılar, değişiklik yönetiminin ve bu değişikliklerin önceden kapsamlı bir risk analiziyle değerlendirilmesinin gerekliliğini ortaya koymaktadır. Değişiklikler yapılmadan önce güvenlik analizlerinin yapılması, sistemlerin güvenliğini tehlikeye atabilecek açıkların belirlenmesini sağlar. Bu nedenle, düzenli risk analizleri ve değişiklik öncesi güvenlik testleri ile sistemler daha güvenilir hale getirilebilir.

## Tüm Yumurtaları Aynı Sepete Koymama Stratejisi

Kritik iletişim sistemlerinin güvenliği, tek bir altyapı ya da tek bir teknolojik kaynağa dayandırılmamalıdır. Lübnan'daki olayda olduğu gibi, tüm iletişim ağlarının tek bir sistem üzerinde toplanması, saldırılara karşı savunmasız hale getirebilir. Kurumların altyapı ve sistemlerini dağıtık bir yapıda planlamaları, güvenliği artırmak adına önemlidir. Böylece, bir sistemdeki zafiyet diğer sistemleri etkilemez ve hizmetin devamlılığı korunur.

## Tedarik Zinciri Güvenliği

Güvenlik zincirinin en zayıf halkası olan tedarik zinciri güvenliği, kritik sistemler için büyük önem taşır. Telsiz cihazları ve benzeri teknolojik altyapılar, farklı tedarikçilerden gelen bileşenler içerebilir ve bu bileşenler güvenlik riski yaratabilir. Tedarikçilerin güvenlik standartlarına uygun çalışması ve ürünlerinin güvenlik testlerinin yapılması, siber saldırılara karşı önemli bir koruma sağlar. Bu bağlamda, tedarikçi güvenliği hakkında düzenli değerlendirmeler ve sertifikasyonların sağlanması kritik bir adımdır.

## Yeni Nesil Kabul Kriterleri

Gelişen teknolojiyle birlikte, eski sistemler yeni tehditlere karşı savunmasız hale gelmektedir. Bu nedenle, sistemlerin kabul kriterlerinin güncellenmesi ve yeni nesil güvenlik standartlarına göre yeniden düzenlenmesi önemlidir. Kabul kriterlerinin güncel tehditleri ve güvenlik ihtiyaçlarını karşılaması, siber saldırılara karşı daha sağlam bir savunma sağlar. Bu durum, sadece yeni sistemlerin kurulumu sırasında değil, mevcut sistemlerin güncellenmesinde de dikkate alınmalıdır.

## Standartlar ve Regülasyonların Önemi

Kamu ve özel sektör kuruluşları için uluslararası güvenlik standartları ve regülasyonlara uyum, siber güvenlik stratejisinin temel taşlarından biridir. İlgili standartlar, sistemlerin güvenliğini sağlamak için minimum gereksinimleri belirler ve bu standartlara uygun hareket etmek, güvenlik risklerini azaltır. Ayrıca, ulusal ve uluslararası regülasyonlara uyum, bilgi güvenliği açısından zorunluluk haline gelmektedir. Bu nedenle, bilgi güvenliği süreçlerinde regülasyonların düzenli olarak takip edilmesi ve uygulanması büyük önem taşır.

# Internet Archive'a Siber Saldırı: 31 Milyon Kullanıcının Verileri Çalındı

Dijital bilgi ve kaynakların korunmasını amaçlayan önde gelen platformlardan biri olan Internet Archive, geniş çaplı bir veri ihlaliyle karşı karşıya kalmıştır. Saldırı sonucunda 31 milyon kullanıcının kişisel bilgilerinin siber saldırganlar tarafından ele geçirildiği açıklanmıştır. Bu olay, dijital içerik sağlayıcı platformların veri güvenliğine yönelik sorumluluklarının önemini bir kez daha gözler önüne sermektedir.

## Saldırının Boyutu ve Çalınan Veriler

Saldırganlar, sistemlere sızarak kullanıcı bilgilerine erişim sağlamış olup çalınan veriler arasında kullanıcı adları, e-posta adresleri, IP adresleri ve şifrelenmiş parolalar yer almaktadır. Saldırının ardından güvenlik protokolleri devreye alınarak kullanıcı bilgileri koruma altına alınmaya çalışılmıştır; ancak çalınan verilerin kapsamı, dijital platform kullanıcılarının verilerini daha dikkatli koruma ihtiyacını bir kez daha vurgulamaktadır.

## Internet Archive'ın Müdahale Süreci

Veri ihlalinin fark edilmesinin ardından platform, kullanıcılarını bilgilendirerek parolalarını güncellemeleri yönünde uyarıda bulunmuştur. Güvenliği artırmak amacıyla kapsamlı bir inceleme süreci başlatılmış olup saldırının kaynağı ve yöntemi detaylı olarak analiz edilmeye çalışılmaktadır. Internet Archive, ilerleyen süreçte daha güçlü güvenlik önlemleri almak üzere çalışmalarını sürdürmektedir.

## Kullanıcılar İçin Güvenlik Önerileri

Bu gibi olaylar, dijital hesap güvenliği konusunda bireylerin alabileceği önlemleri tekrar hatırlatmaktadır. Kullanıcıların hesaplarını güvence altına alabilmesi için şu öneriler öne çıkmaktadır:

**Parola Güvenliği:** Karmaşık ve benzersiz parolalar kullanmak, siber saldırılara karşı ilk savunma hattını oluşturmaktadır.

**Çok Faktörlü Kimlik Doğrulama (2FA):** Hesapların korunmasını güçlendirmek için e-posta ve diğer platformlarda 2FA kullanımı önemlidir.

**Şüpheli Faaliyetleri İzleme:** Hesap etkinliklerini düzenli olarak kontrol etmek, olağan dışı hareketlerin hızlı bir şekilde tespit edilmesini sağlar.

## Dijital Platformlar İçin Çıkarılacak Dersler

Bu saldırı, dijital arşivlerin kullanıcı verilerini koruma sorumluluğunu hatırlatmakta olup benzer hizmet sağlayıcıların da güvenlik altyapılarını düzenli olarak güncellemelerinin önemini ortaya koymaktadır. Özellikle geniş kullanıcı tabanına sahip dijital platformların veri ihlallerine karşı daha kapsamlı güvenlik önlemleri alması ve kullanıcılarını olası güvenlik riskleri konusunda bilgilendirmesi gerekmektedir.

Internet Archive'a yönelik bu saldırı, geniş çaplı veri tabanlarına sahip tüm dijital platformlar için önemli bir uyarı niteliği taşımakta ve dijital güvenliği sağlamak için proaktif adımların gerekliliğini bir kez daha ortaya koymaktadır.

# Siber Güvenlik Terimleri

## DDoS

### Dağıtık Hizmet Engelleme Saldırısı


DDoS saldırısı, hedef alınan sistemin, sunucunun veya ağın normal işleyişini engellemek amacıyla çok sayıda cihazdan aynı anda aşırı miktarda trafik gönderilmesiyle gerçekleştirilmektedir. Bu tür saldırılar, sunucuya aşırı yük bindirerek hizmetin kesintiye uğramasına yol açmaktadır. DDoS saldırılarında saldırganlar, genellikle "botnet" adı verilen bir ağda kontrol ettikleri cihazları kullanarak hedef sistemleri etkisiz hale getirmeyi amaçlamaktadır. Bu saldırılara karşı, sistemlerin güçlü altyapılarla donatılması ve olağan dışı trafiği tespit edebilen güvenlik önlemlerinin uygulanması büyük önem taşımaktadır.

## End-to-End Encryption

### Uçtan Uca Şifreleme


Uçtan uca şifreleme, iki iletişim cihazı arasında aktarılan verilerin yalnızca gönderen ve alıcı cihazlar tarafından okunabilir hale getirilmesini sağlamaktadır. Bu yöntemle, veri iletimi sırasında üçüncü şahısların veya saldırganların verilere erişmesi engellenmektedir. Veriler, gönderici tarafından şifrelenmekte ve yalnızca alıcı tarafından deşifre edilebilmektedir. Çevrim içi mesajlaşma uygulamaları ve veri transferlerinde yaygın olarak kullanılan bu teknoloji, veri gizliliği ve güvenliğin sağlanması açısından temel bir güvenlik önlemidir.