NarDC

Nardatabank Bilişim ve Teknoloji A.Ş.

Verilerinizi **Güvenle Depoluyoruz**

www.nardc.com

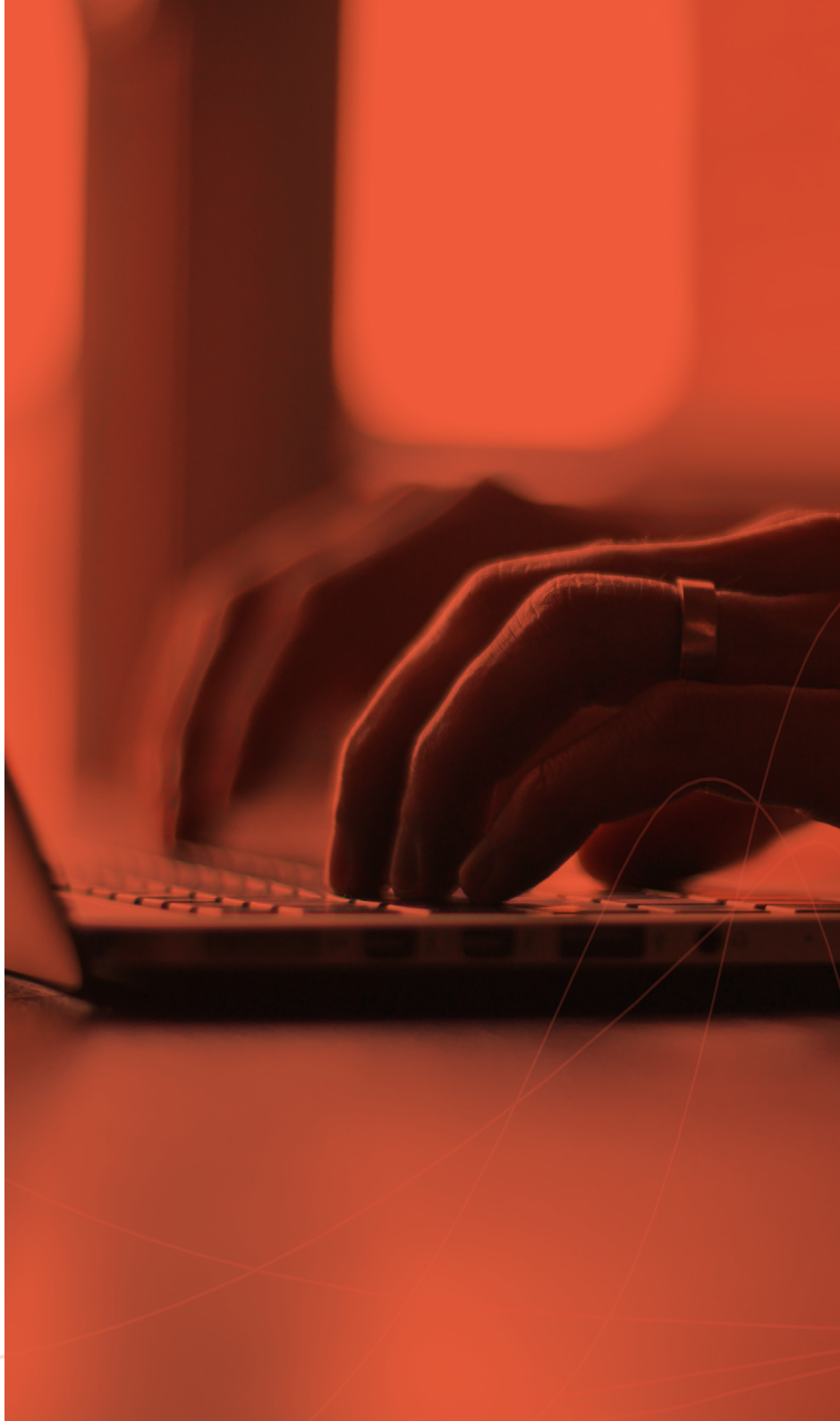
Bizi Yakından Tanıyın.

NarDC 2020 yılında kurulmuş olan **NARDATABANK BİLİŞİM VE TEKNOLOJİ AŞ.** firmasının ilk markasıdır.

Dijitalleşen dünyada ticaretin küreselleşmesi nedeniyle müşterilerimize vereceğimiz kaliteli hizmetler ile dünya markalarıyla rekabet ederek, NarDC'yi bir dünya markası yapmayı hedeflemekteyiz. NarDC markasıyla, **NARDATABANK A.Ş.** gücünü ve sermayesini %100 milli ve yerli olan **NAR İŞLETME KOOPERATİFİ**'inden almaktadır.

Verilerinizi Güvenle Depoluyoruz

Kamu kurumları ve şirketlere; yüksek deneyim ve tecrübeye sahip, uzun yıllardır sektörün içerisinde uzmanlaşmış takım arkadaşlarımızla tarafımıza ulaşan talepleri en kısa zaman içerisinde değerlendirerek veya çözüm üreterek, müşterilerimize en uygun maliyetlerle hizmet vermekteyiz. Takım arkadaşlarımızla beraber 7/24 esaslı hızlı hizmet vermekteyiz.



HİZMETLERİMİZ

- Veri Merkezi Çözümleri
- IT Danışmanlığı
- Dijital Güvenlik

Hizmetlerimiz

Veri Merkezi Çözümleri

- Fiziksel Sunucu Kiralama
- Sunucu Barındırma
- Bulut Çözümleri
- Sanallaştırma Çözümleri
- Bulut Yedekleme Çözümleri
- Sistem ve Ağ İzleme
- Felaket Kurtarma Çözümleri
- VPN Çözümleri

Fiziksel Sunucu Kiralama

Intel® Xeon® E5-2650v2	32GB DDR3	2 x 500GB SSD	Limitsiz Trafik 100Mbit
2X Intel® Xeon® E5-2650V2	64GB DDR3	4 x 500GB SSD	Limitsiz Trafik 100Mbit
2X Intel® Xeon® E5-2690V2	128GB DDR3	2 x 1TB SSD	Limitsiz Trafik 100Mbit
2X Intel® Xeon® E5-2690V2	256GB DDR3	2 x 1TB SSD	Limitsiz Trafik 100Mbit
2X Intel® Xeon® E5-2697V2	256GB DDR3	2 x 1TB SSD	Limitsiz Trafik 100Mbit
2x Intel® Xeon® E5-2670V3	128GB DDR4	2 x 1TB SSD	Limitsiz Trafik 100Mbit

Sunucu Barındırma

Bizi benzersiz kılan özelliklerimiz şeffaf hizmet ilkemiz ile benzer kullanıcılar arasında ayrım göstermeyen fiyatlarımız/tarifelerimiz, kabinet ve network otomasyon sistemimiz, işinizi bize entegre edebilmeniz için gerekli API desteğini sağlamamız, ücretsiz olarak remote hands (fiziksel destek) desteği sunuyor olmamızdır.

Maliyet avantajı sağlayan özelliklerimiz, tek sunucu barındıracaklar için sunulan paylaşımlı kabinetler içerisinde trafik kotasız hizmet alabilmeniz, yüksek hacimli ve özel kabinet sahibi işletmeler için sadece bir internet erişimi satın alarak kendi ağınıza sahip olmanız, akıllı kabinet sistemlerinde enerji ölçümlerinin hassas sayaçlar ile her bir kWh için yapılarak faturalandırılması, rakipsiz internet erişimi seçenekleri ile kabinet kiralama tarifelerimizi sıralayabiliriz.

Bulut Çözümleri

Birebir Yedekli Donanım

NarDC Bulut Sunucu hizmetinde kullanılan hypervisor sunucular, storage ekipmanları, kullanılan ara switchler tamamen birebir yedekli olarak konumlandırılmıştır. DELLEMC özel tasarım sunucular da yapılacak tüm fiziksel işlemlerde sanal sunucunuz kapanmaz, herhangi bir arıza durumunda ise sanal sunucunuz hemen müsait bir hypervisor sunucuda yeniden başlar. NarDC Bulut sunucu hizmeti ile donanım arızalarını düşünmeniz gerekmez.

Bulut Sunucu Güvenliği

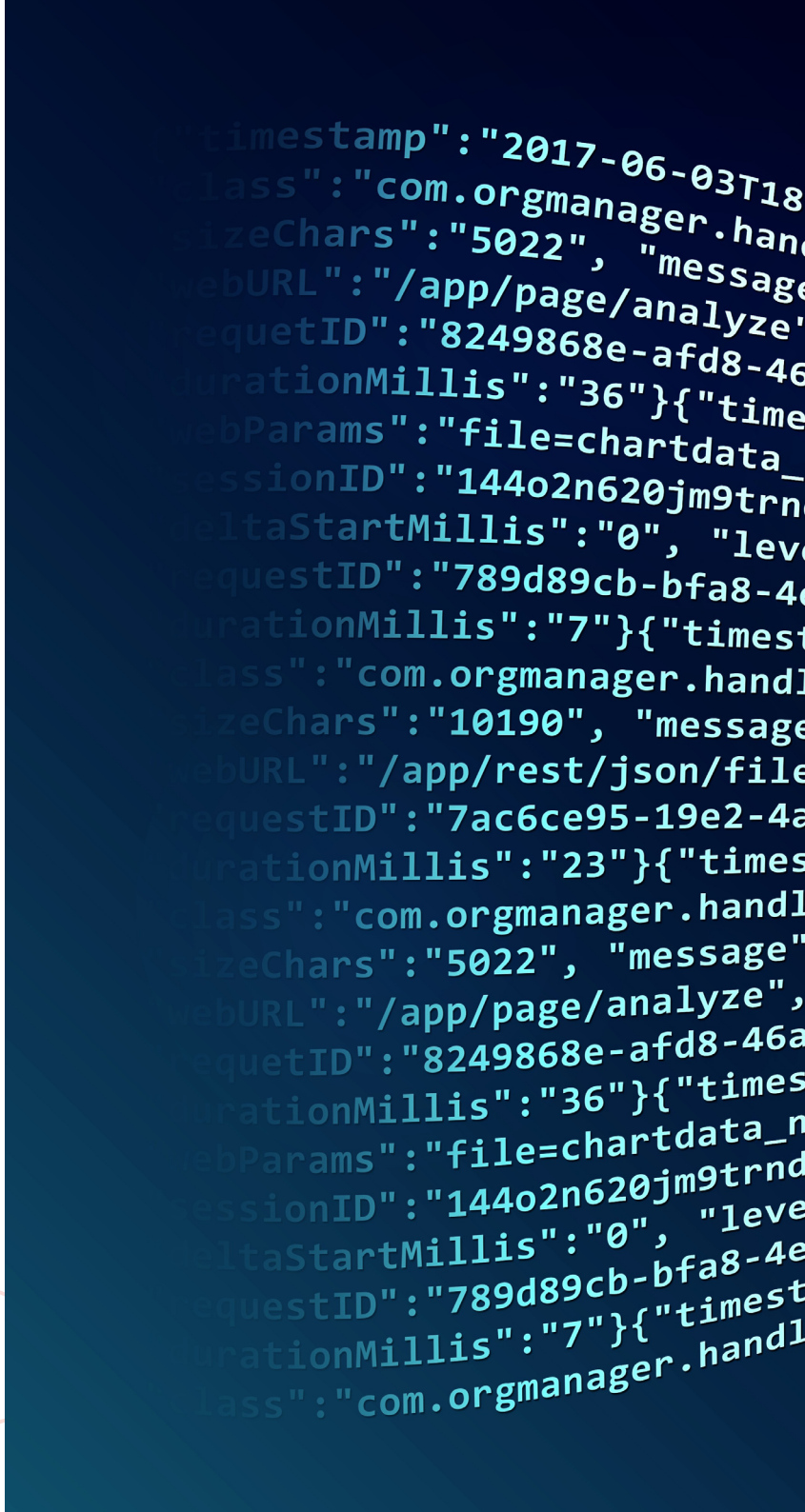
Her bir müşterimiz için ayrılmış vlan ile sanal sunucunuz diğer kullanıcılardan izole çalışmaktadır. Kendinize ait sanal sunucuları aynı vlan ağı içerisinde tutabilir, 40Gbps/sn port ile local ağ üzerinden yüksek hızda sunucularınız arasında erişim sağlayabilirsiniz. Kullanılan ağ ekipmanlarının tamamı 2x40Gbps/sn uplink ile omurga dan yedekli beslenmekte, bu sayede internet erişiminizin kalitesi olabilecek her durumda sekteye uğramamaktadır.

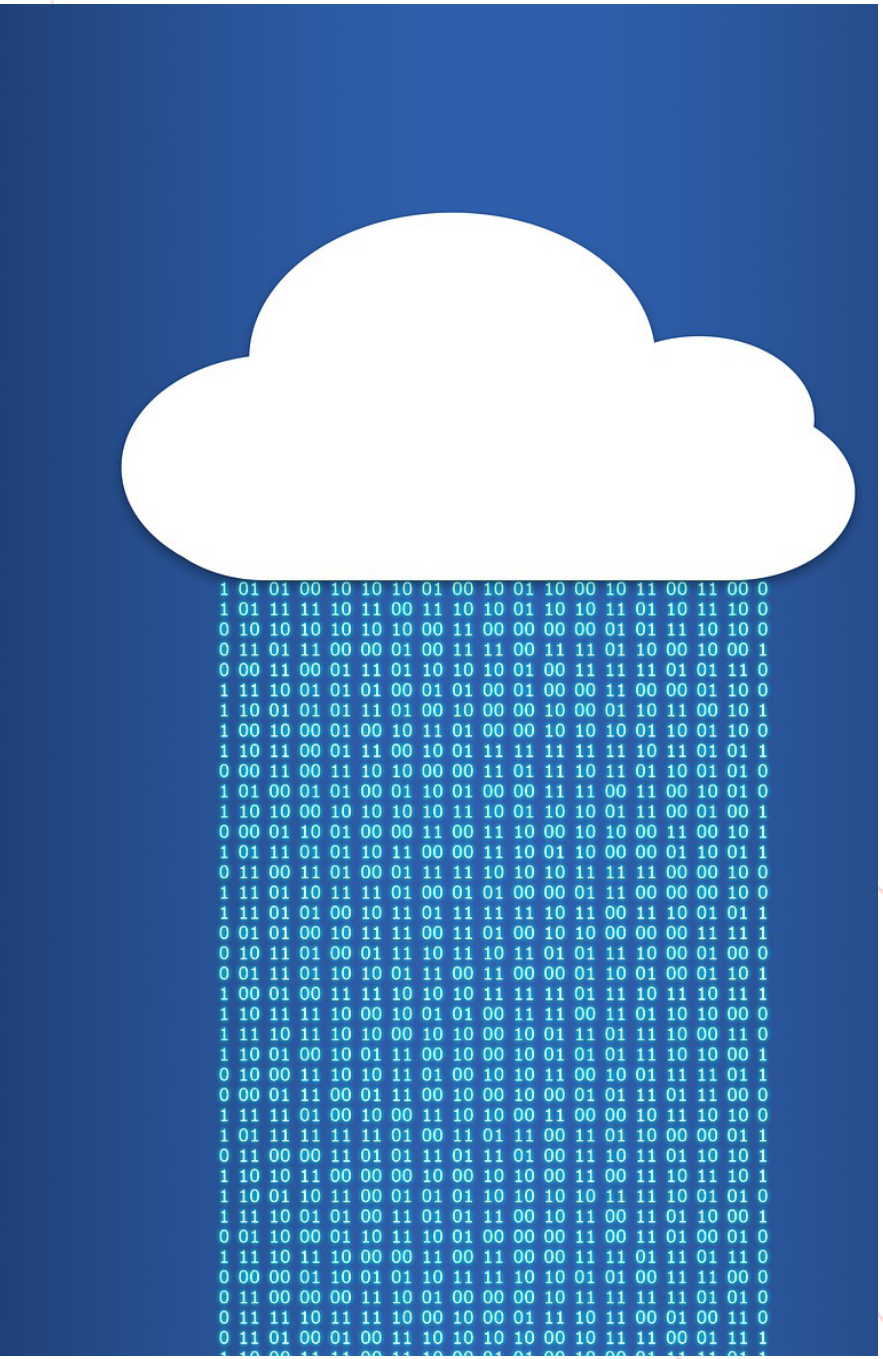
Sanallaştırma Çözümleri

Sanallaştırma teknolojisi kuruluşunuzun maliyetlerini azaltırken, uygulamalara erişimi artırır ve BT yönetimini kolaylaştırır. NarDC Sanallaştırma hizmeti ile ağır yüklerinizden rahatlıkla kurtulabilirsiniz...

Sunucu Sanallaştırma
Ağ Sanallaştırması
Masaüstü Sanallaştırması
Uygulama Sanallaştırması
Depolama Sanallaştırması

Sanallaştırma, kapalı kalma sürelerini azaltıp gelir kaybını en aza indirir.
Sunucu birleştirme yatırım ve işletme giderlerini azaltmanıza yardımcı olur.
Sunucu birleştirme yoluyla enerji verimliliğini artırıp daha az donanım gerektirerek yatırım ve işletme maliyetlerinizi düşürür.
Basitleştirilmiş olağanüstü durum kurtarma çözümleri sunarak, altyapınız için iş sürekliliği sağlar.
Veritabanları (Oracle Veri Tabanı, Microsoft SQL Server, SAP HANA, SAP Sybase) dahil kritik kurumsal uygulamaları, iş uygulamalarını (SAP Business Suite, Microsoft Exchange, SQL Server, SharePoint, SAP) sanallaştırarak hizmet seviyeleri ve performansı en üst seviyeye çıkarır.
Sanallaştırma teknolojisine geçerken, uygun yazılımı bulmak; doğru sunucu, veri depolama ve network altyapısını seçmek gibi zorluklarla karşılaşabilirsiniz.
NarDC ‘nin benzersiz saha tecrübesinden yararlanarak VMware ve Hyper-V çözümlerimizle standartlara dayalı bir sanallaştırma stratejisi oluşturup, kısa sürede hayata geçirebilirsiniz.





Bulut Yedekleme

NarDC’ nin bulut ortamında sunduğu Sunucu Yedekleme sistemi Bulut Yedekleme, disk tabanlı bir yedekleme (backup) ve yedekten geri dönme (recovery) sistemidir. Bulut Yedekleme, bulut sunucunuzun içerisindeki dosyaların yedeklenmesini sağlar.

Bulut Yedekleme ile yedeklenen veriler günlük olarak şifrelenerek NarDC sunucularında depolanır. Yedeği alınan bulut sunucunuzun geri yüklenmesi tümüyle sağlanır. Bulut yedekleme servisinde sunucularınızın yedekleri sizin tercih edeceğiniz periyotlarla alınır (Günlük, Haftalık, Aylık). Geri yükleme sırasında veri, uygulama vs. aktarımı %100 güvenli olarak sağlanırken, hiçbir şekilde data kaybı yaşanmaz.

Sistem ve Ağ İzleme

Günümüz dünyasında, ağ izleme terimi BT endüstrisinde yaygın olarak kullanılmaktadır. Ağ izleme sürecinde, router, switch, güvenlik duvarı, sunucu ve VM'ler gibi tüm ağ cihazlarının hata ve performans açısından izlenir. Bu bileşenlerin kullanılabilirliklerini korumak ve optimize etmek için sürekli olarak değerlendirildiği kritik bir BT sürecidir.

Ağ izleme yazılımlarıyla Router, Server, switch ve diğer önemli network cihazları veya uygulamalar gibi belirlenmiş hostlardan istatikler toplanır, Network trafiği detayı, CPU değerleri, disk kullanımı, Up-Down durumu gibi önemli verileri kontrol edilebilir.

Ağ izlemenin önemli bir yönü proaktif olması gerektiğidir. Performans sorunlarını ve darboğazları proaktif olarak bulmak, ilk aşamada sorunların tanımlanmasına yardımcı olur. Etkili proaktif izleme ağ kesintilerini veya arızalarını önleyebilir.

Felaket Kurtarma

Disaster Recovery (DR) Türkçe'deki deyişiyle Felaket Kurtarma verilerinizin başka bir konumda yaptığımız veri yedekleme ve bu sistem aracılığıyla güvene aldığımız veri merkezi (data center) olarak doğal felaket ve oluşabilecek data kayıplarında bir yedek olarak oluşturulmasıdır. Bu oluşturulan merkezlere Felaket Kurtarma merkezleri denir. Asıl amaç veri yedeklemek değil, coğrafik konum olarak başka bir konumda verileri saklayarak felaket durumlarına karşı önlem almaktadır.

İşte bu noktada en dikkat edilmesi gereken özelliklerden biri de Felaket Kurtarma Merkezi birebir ana veri merkezleri ile aynı sistemlere, özellikle veri depolama üniteleri konusunda aynı olmalıdırlar ki olası bir felaket durumda aynı hizmeti vermeye devam edebilsin.

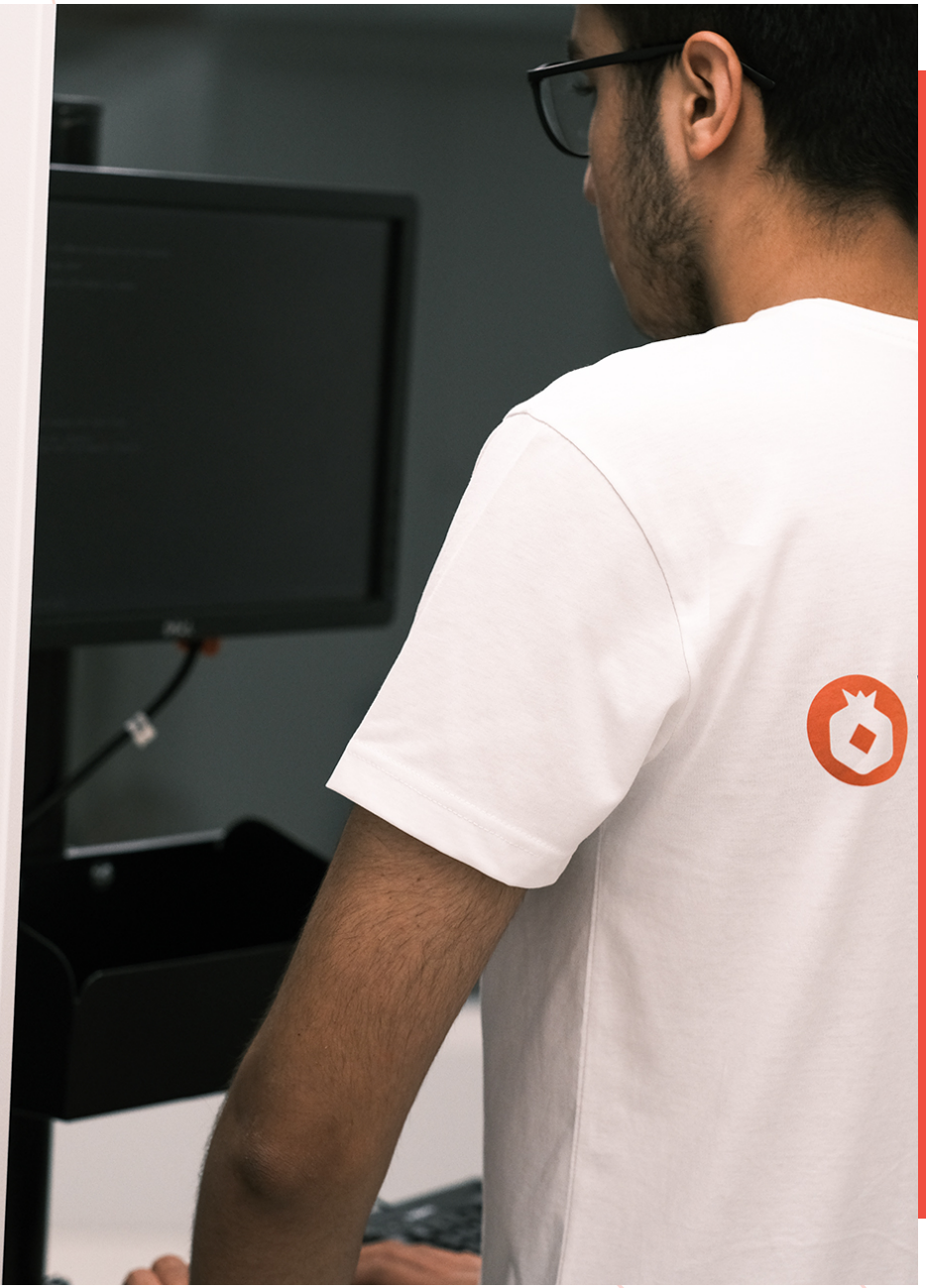
VPN Çözümleri

Mobil çalışanların şirket ağına ve bilgilerine her zaman her yerden ve hızlı bir şekilde ulaşabilmesi çok büyük bir önem taşımaktadır. Ancak bu bağlantının güvenli olması da gerek kurum, gerekse çalışanlar için son derece önemlidir. Bu noktada devreye giren NarDC işletmelere güvenli ve kurulumu kolay VPN hizmeti sunmaktadır. VPN hizmetlerinde uç noktalar arası veri iletişimi yanı sıra internet erişim hizmetleri de sunulmaktadır.

Başlıca Hizmetler:
Sadece merkeze internet erişim izni verilmesi,
Sadece ihtiyaç duyulan uç noktalara internet erişim izni verilmesi,
Tüm uç noktaların internete erişimi,
İnternet erişiminin loglanması,

IT Danışmanlığı

- Altyapı Kurulumu
- Güvenlik Duvarı
- Yedekleme & Backup
- Bakım & Destek
- SMS Hizmeti
- Kurumsal Mail (KVKK)



Altyapı Kurulumu

Bilgi teknolojileri ve sistemleri neredeyse her kurumun iş süreçlerinin zorunlu bir parçası haline gelmiştir. Teknolojinin çok hızlı bir şekilde değişmesi ve gelişmesi nedeniyle de BT/BS sistemlerinde her konuda uzmanlaşmak neredeyse imkânsız bir hale gelmiştir.

Günümüzde hızla gelişmekte olan bilgi iletişim teknolojileri, düşük maliyetli, hızlı, yüksek kaliteli bir ağ alt yapısı ihtiyacını beraberinde getiriyor. NarDC yetişmiş, deneyimli uzman kadrosu ile müşteri odaklı, ihtiyaçlarınıza uygun çözümler sunarak, ağ altyapı sisteminin kurulması, yönetilmesi, aktif ve pasif ağ ekipmanlarının birbirileri ile sorunsuz entegre edilmesi, mevcut ağ alt yapınızın son teknolojik çözümlerle yeniden yapılandırılması anlamında anahtar teslim projeler ve danışmanlık hizmetleri verebilmektedir.

Firewall (Güvenlik Duvarı)

“Verilerinizi Güvenle Depoluyoruz”
Layer 7 Filtreleme ve Ters Proxy Servisi
Layer 4 Stateless Firewall
DDoS Atak Filtreleme
UDP Atak Filtreleme
SYN Spoofing Atak Filtreleme
IPS Firewall Hizmeti
Saldırı Tespiti ve Loglama
SSL VPN Çözümü

Kurumsal Firewall Hizmetleri
NarDC kurumsal hizmetleri kapsamında sizlere IT güvenliği sunuyor. Firewall Servisi, müşteri yerel ağına doğru ya da yerel ağından Internet’e doğru oluşan izinsiz erişimlerin engellenmesi için, firewall cihazları üzerinde müşteri tarafından talep edilen kuralların tanımlanmasını ve firewall cihazlarının yönetimini kapsamaktadır.

Yedekleme – Backup

İhtiyaca Özel Yedekleme Politikası ve Planlama
FTP Üzerinden Yedekleme
SAN/NAS mimarileri üzerinde yedekleme
Yerel ve geniş ağ üzerinden merkezi yedekleme
Periyodik İşletim Sistemi İmajı
Sunucu bağımsız yedekleme (Server-Free Backup)

Güvenli ve Yüksek Kapasiteli Yedekleme Çözümleri

Yedekleme günümüz işletmelerin genellikle göz ardı ettikleri ancak sorun anında paha biçilemeyen IT gereksinimlerinden birisidir. Günümüzde bir çok işletme ihtiyacı IT sistemleri üzerinde karşılanıyorken bu sistemlerin olası problemlere karşı hazırlıklı olması kaçınılmaz bir ihtiyaçtır. NarDC bu noktada sizlere güvenli ve yüksek kapasiteli yedekleme çözümleri sunar. İster NarDC Veri Merkezi'nde barınsın, isterse kendi lokasyonunuzdaki sistem odasında barınıyor olsun, her türlü IT altyapınızın yedekleme işlemlerini bizim ile gerçekleştirebilirsiniz

Bakım & Destek

Günümüzün kurumsal BT altyapıları coğrafi olarak dağınıktır ve çok sayıda telekomünikasyon, donanım ve yazılım çözümünü içermektedir. Son kullanıcı üretkenliğinin sürekli sağlanabilmesi için BT altyapıları, SLA standartları uyarınca profesyonel bakım ve teknik desteğe ihtiyaç duymaktadır.

NarDC Hizmet Merkezi geniş bir yelpazeye yayılan yazılım, donanım ve telekomünikasyon çözümleri için çok amaçlı BT altyapısı planlama, uygulama, yönetim, bakım ve teknik destek hizmetleri sunmaktadır. NarDC, yetkili teknik uzmanlardan oluşan deneyimli bir ekibe sahiptir ve müşterilerin yüksek SLA şartlarının sağlanabilmesi adına esnek hizmet planları sunmaktadır.

SMS Hizmeti

SMS, bugün hala en akılda kalır ve kişiye özgü iletişim yolu olmayı sürdürüyor. Şunu bir düşünün: ortalama her mesajın iletilmesi 6 saniye sürüyor ve alıcıların %90'ı bu mesajı 5 dakika içinde okumuş oluyor.

Bugün dünyada 5 milyar cep telefonu kullanılıyor, ki bu sayı en büyük sosyal paylaşım sitesinin kullanıcı sayısının 5 katı kadar ve cep telefonları yoluyla mevcut ve yeni müşterilere ulaşma fikri cazibesini her geçen gün artırıyor.

Sıra beklemeden, yüksek miktarlarda mesaj iletimi
Mobil operatörlere direkt bağlantılar
Gerçek zamanlı iletim raporları
Güçlü SMS mesajlaşma ve hesap yönetimi web portalı
Kurumsal düzeyde API desteği NarDC Sms Hizmeti Ayrıcalıkları.

Kurumsal Mail (KVKK)

Kurumsal e-mail hizmeti, işiniz için en uygun araçları sunan profesyonel bir cloud servistir. E-mail, takvim ve kişiler bir arada sunulur, tüm cihazlarınızda eşitlenir. Ayrıca Türkiye lokasyonlu sunucularda olması sayesinde KVKK ile uyumludur.

E-maillerinizi sadece imkan bulduğunuzda değil, ne zaman isterseniz o zaman kontrol edin. Windows, Mac ve Linux için özel programlar ve iOS ya da Android mobil cihazlarınız için geliştirilmiş özel uygulamalar ile e-maillerinize her an, her yerden erişebilirsiniz.

SpamExperts Profesyonel SPAM filtresi ile, kurumsal e-mail hizmetimizde SPAM maillerle uğraşmazsınız. Size gelen tüm e-mailler SPAM filtresinden geçer ve virüslere karşı taranır.

Dijital Güvenlik Danışmanlığı

- Sızma (Penetrasyon) Testleri
- Siber Olay Müdahale (SOME)
- Sosyal Mühendislik
- Siber Hijyen ve APT Tespiti
- Red Teaming ve Metodolojisi
- Endpoint Güvenlik İzleme
- Seviye Tespit ve İyileştirme
- SIEM/LOG Korelasyon
- Siber Suç İnceleme
- Düzenli Zafiyet Tarama
- DoS, DDoS Test ve Koruma

Sızma Penetrasyon Testi

Penetrasyon testi - Pentest şirketin güvenlik becerilerini üst düzeyde tutmak, dışarıdan gelebilecek saldırıları görüp önlem almak, sistemlerinize yapılan yatırımı güvende tutmak ve en önemlisi de güvenlik açıkları nedeniyle oluşabilecek bilgi kayıplarına engel olabilmek için yapılmalıdır.

Penetrasyon Testi / Pentest - Sızma Testi Türleri

1-) BlackBox Pentest (Siyah Kutu Penetrasyon Testi); Siyah kutu penetrasyon testi saldırı yapılacak network hakkında hiçbir bilgi sahibi olmadan yapılan saldırı türüdür.

2-) WhiteBox Pentest (Beyaz Kutu Penetrasyon Testi); Beyaz kutu penetrasyon testi network üzerindeki tüm sistemlerden bilgi sahibi olarak yapılan sızma testi türüdür.

3-) GreyBox Pentest (Gri Kutu Penetrasyon Testi); Gri kutu penetrasyon testi iç network de bulunan yetkisiz bir kullanıcının sistemlere verebileceği zararın analiz edilmesini sağlar. Veri çalınması, yetki yükseltme ve network paket kaydedicilerine karşı network zayıflıkları denetlenir.

Siber Olay Müdahale (SOME)

Ülkemizde siber güvenlik yapılanmasını sağlamak amacıyla teknik ve hukuki yaptırımları içeren çalışmalar neticesinde siber güvenliğin önemi dikkate alınarak 20 Ekim 2012'de Resmi Gazete'de Bakanlar Kurulu Kararı olarak "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar" yayınlanmıştır. Bu karar ile siber güvenlik alanına yönelik usul, esas ve standartları onaylamak, bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla da "Siber Güvenlik Kurulu" oluşturulmuştur. Siber Güvenlik Kurulunun gerçekleştirmiş olduğu toplantı sonucunda da Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yayımlanan eylem planı kabul edilmiştir.

Bilişim sistemlerinde yaşanan ihlal olayları profesyonel bakış açısıyla değerlendirilerek ek aksiyonlar alınmadığı takdirde, benzeri olaylarla tekrar tekrar karşılaşma riski katlanarak artmaktadır. Her olay bir tecrübe olarak detaylı incelenmeli ve tekrar yaşanmaması için gerekli önlemleri alınmalıdır.

Sosyal Mühendislik

Sosyal mühendislik, insanların zaafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışma işlemlerinin bütünü olarak tanımlanmaktadır. Sosyal Mühendislik saldırılarında insanların karar verme süreçlerini değiştirmeye yönelik teknikler olduğu gibi, İnsan davranışları birer açıklık olarak kabul edilir ve bu açıklıklar kullanılarak saldırı yapılabilir.

Bu kadar yaygın ve başarı oranı yüksek bu saldırı tipi henüz bilişim güvenliği uzmanlarının büyük çoğunluğu tarafından ciddi saldırı olarak kabul edilmemektedir. Bunun temel nedeni de sosyal mühendislik saldırılarının herhangi bir teknik bilgiye sahip olmayi gerektirmeyecek kadar kolay gerçekleştirilebilmesidir. Oysa güvenlikte her zaman zor olan değil, basit olan ve son kullanıcıyı hedef alan saldırılar zarar verir.

Siber Hijyen ve APT Tespiti

Bu hizmet kurum bünyesinde yer alan sistemlerin Botnet'lere dahil olanları, zombi hale getirilmiş sistemleri, veri sızıntısı için kullanılan araçları, uzaktan yetkisiz erişim programlarının kurulu olduğu sistemleri, arka kapıları, trojan bulaşmış sistemleri, siber tehdit istihbaratı ağından gelen verilerden de faydalanılarak tespit edilmekte ve raporlanmaktadır.

Siber Hijyen Durumu ve APT tespiti için toplamda 30.000 anomali kuralından ve veritabanında 200.000.000 kategorize edilmiş alan adı (domain) bulunan özel sistemlerden faydalanılmaktadır. Talep edilen hizmet seviyesine bağlı olarak elde edilen trafik, altı farklı APT ve Antimalware sisteminde kontrol edilerek hata oranı (false positive – false negative) minimum seviyeye indirgenmektedir.

Red Teaming Hizmeti ve Metodolojisi

Red Teaming bir kurumun güvenlik cihazlarını, ağlarını, çalışanlarını, uygulamalarını ve fiziksel güvenlik kontrollerini gerçek hayattaki bir saldırıya ne düzeyde dayanabileceğinin ölçümlenmesi için tasarlanan tam kapsamlı ve çok katmanlı saldırı simülasyonudur. Şirketlerin güvenlik ekiplerinin, kurumun gerçek bir saldırı karşısında ne kadar iyi bir sonuç alacağını test etmeleri için özel bir yol sunmaktadır. İyi kurgulanmış bir Red Teaming aşağıdaki ilgili güvenlik açıklarını ve teknoloji altyapısındaki, insan gücündeki ve fiziksel güvenlik ile alakalı riskleri ortaya çıkaracaktır.

Red Teaming operasyonları sırasında, yüksek eğitimli güvenlik danışmanları potansiyel fiziksel, donanım, yazılım ve insan zafiyetlerini ortaya çıkarmak için saldırı senaryolarını yürürlüğe koymaktadır. Bu sayede Red Teaming, kötü niyetli kişilerin şirket sistemlerini ve ağlarını tehlikeye atma veya veri ihlallerine olanak verme fırsatlarını da ortaya çıkarmaktadır.

EndPoint (Uç Nokta) Güvenlik İzleme

Endpoint Detection and Response (EDR) güvenliği gelişmekte olan bir teknolojidir. Terim, şüpheli etkinlikleri ve sunucu ve uç noktalar üzerindeki sorunları tespit etmeye, araştırmaya ve azaltmaya odaklanan bir araç ve çözüm kategorisini tanımlar.

EDR yani uç nokta güvenlik izleme çözümleri, uç noktalarda daha zengin davranış temelli anormal durum tespiti ve görünürlük için geleneksel imza tabanlı teknolojileri desteklemektedir. Katmanlı network ve güvenlik yapılarının kurumları yeteri kadar korumadığı artık tüm firmalar tarafından anlaşılmış durumdadır. Gelişmiş kalıcı tehditler (APT) ve özelleştirilmiş hedefe yönelik kötü amaçlı yazılım saldırısı araçları, geleneksel imza tabanlı antivirüs çözümlerini bypass edebiliyor.

Seviye Tespit ve İyileştirme Hizmeti

NarDC “Siber Güvenlik Tespit Çalışması” ile kurumların güvenlik seviyeleri ve yaptıkları güvenlik yatırımlarının kurum güvenliğine sağladığı katkı ortaya çıkartılmaktadır. Kurumlar, verilerinin güvende olup olmadığını kullandıkları güvenlik teknolojilerini denetleyerek saptayabilirler.

“Siber Güvenlik Tespit Çalışması” kapsamında gerçekleştirilen teknik analizler ile kurumun bilgi sistemlerine ait siber güvenlik olgunluk seviyesi somut parametrelerle ortaya koyulmakta ve sistemi güvenlik açısından etkileyebilecek bilgi teknolojileri risklerine karşı önlemler sunulmaktadır.

SIEM / LOG Korelasyon Hizmeti

SIEM, Log izleme manasına gelmektedir. Sisteminizde bulunan tüm kritik ağlar ve cihazları kapsayan log yönetimi ve analizine SIEM projesi denilmektedir. Sistemin ürettiği olay kayıtlarının belirlenen kurallara göre analiz edilmesi olarak tanımlanmaktadır. SIEM Projeleri ile sistemin üretmiş olduğu logların kapsamlı bir şekilde toplanması, birleştirilmesi, saklanması ve doğru analizler gerçekleştirilmesi gibi adımlardan oluşan log yönetimi ise saldırının göstergelerini ve delillerini elde etmeyi ortaya çıkartabilir. Bu projelerin bir adı ise Log Yönetimi'dir.

SIEM sistemlerinin log üreten değil, logları toplayan, anlamlandıran ve alarm üreten bileşen olduğu unutulmamalıdır. Çoğu kurum sadece SIEM kurarak yerel ağdaki anormalliklerden haberdar olacağını düşünmektedir, oysa SIEM, bir hesap makinesi gibidir, ona doğru rakam ve işlemi söylemezseniz sonuç beklediğiniz gibi çıkmaz.

Siber Suç İnceleme Hizmeti

Bilişim sistemleri hayatın her alanında olduğu gibi suç ve suçlu olgularını da karşımıza çıkmaktadır. Teknoloji çağında gerçekleştirilen olayların aydınlatılmasında anahtar bileşen olarak konumlandırılan bilişim sistemleri doğru ve tarafsız analiz edildiğinde suçluya ait normal yollardan tespit edilemeyen deliller sunabilmektedir.

Adli bilişim analizi (Computer Forensics) suçlu psikolojisi ve teknolojinin gücü ile birleştirildiğinde inkar edilemez somut deliller ortaya çıkarmaktadır.

Siber suç inceleme hizmetinde işlenen suç veya yaşanan siber güvenlik ihlali sonrasında delillerin profesyonel bir ekip tarafından toplanması suçlu hakkında önemli bilgiler ve kanıtlar ortaya çıkarır. Ayrıca, bu tür olaylarda sıkça gözden kaçan “sisteme sızan kişi veya kişiler başka neler yapmış?” sorusuna da en kapsamlı cevabını bu çalışmalar sonucunda tespit edebiliriz.

Düzenli Zafiyet Tarama ve Yönetimi Hizmeti

Kurumların tercihine bağlı olarak proaktif güvenliğin temel bileşenlerinden olan sızma testi çalışmaları, (genellikle) maliyet faktöründen dolayı yılda bir kez yapılmaktadır. Oysa ki orta ve büyük ölçekli firmaların kullandığı IT sistemlerinde ortalama olarak her hafta kritik öneme sahip güvenlik açıklıkları ortaya çıkmaktadır.

Firmaların sızma testi yaptırmadığı zaman aralığında İnternet üzerinden otomatize bir şekilde düzenli olarak güvenlik taraması yapabilmesi için Düzenli Zafiyet Tarama ve Yönetim Aracı geliştirilmiştir.

Düzenli zafiyet tarama ve yönetim aracı kullanımında öncelikle kurumun varlıkları sisteme tanımlanır. Ardından da düzenli aralıklarla güvenlik tarama istekleri gönderilir. Güvenlik tarama istekleri Yönetim Aracı yöneticilerine gelir, talep ve varlığın tipine göre (Network, Sistem, Uygulama gibi) güvenlik taramaları gerçekleştirilir.

DoS, DDoS Testleri ve Koruma Hizmeti

DDoS, güvenlik üçgeninin erişilebilirlik ayağına yönelik yapılan, hedefin hizmet vermesini engellemeyi amaçlayan ve dağıtık kaynaklardan gerçekleştirilen servis reddi saldırısı çeşididir.

DDoS saldırılarını engellemenin en zor yanı, yoğun istek altında gerçek kullanıcı trafiği ile saldırı trafiğinin ayrıştırılmasıdır.

DDoS gibi zafiyet tabanlı olmayan saldırılar, imza tabanlı IPS sistemleriyle engellenememektedir. Mevcut bir çok IPS ve Firewall çözümü DDoS saldırıları karşısında iki seçenek sunmaktadır; yüklü trafik geldiğinde belirli limitin üzerindeki tüm paketleri engelle veya paket incelemeyi devre dışı bırak.
Limit üzeri paket engelleme, rastgele paket engelleyerek gerçek kullanıcıların servislere erişimine engel olduğu için saldırganların amacına ulaşmasını sağlar. Güvenlik sisteminin analizi devre dışı bırakması ise saldırganın ağ içerisindeki zafiyetleri suiistimal etmesine imkan tanır.

NarDC

Nardatabank Bilişim ve Teknoloji A.Ş.

Hüseyinağa Mahallesi İstiklal Caddesi No : 56-58 Grandpera **Beyoğlu / İSTANBUL**

Mücahitler Mah. 52043 Nolu Cad. Mehmet Karagülle İş Merkezi No:1 Kat:8 İç Kapı No:80

Şehitkamil / GAZİANTEP

0850 304 6 305 info@nardc.com www.nardc.com

nardatacenter