VERİ GÜVENLİĞİ

Tehditler ve Korunma Yöntemleri

Hazırlayan : İbrahim Yalçınlar

SystemSoft®

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

HAKKIMIZDA

SystemSoft otomotiv sektörüne özel çözümler üreten 2012 yılında kurulmuş olan konusunda uzman bir yazılım firmasıdır.

Türkiye'de otomotiv yedek parça piyasasında hizmet vermekte olan yedek parça firmalarının büyük çoğunluğunda SystemSoft ürünleri kullanılmaktadır.

Otomotiv yedek parça yazılımı konusunda 20 yıllık bilgi birikimini elinde bulunduran SystemSoft, 300 üzerinde otomotiv yedek parça firmasına destek ve hizmet vermektedir.

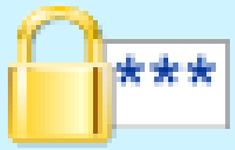
SystemSoft'un özel üretmiş olduğu B2B, Sanal Pos, BI-Rapor, E-ticaret, CRM, İhracat, PIM ürünlerinin yanında server kurulum ve bakım hizmetleri, yedekleme hizmetleri, iş zekası çözümleri, yazılım geliştirme, proje yönetimi ve danışmanlık gibi hizmetleri de uzman ekibi ile müşterilerine sunmaktadır.

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

TEHDİTLER



SİBER SALDIRI

CİHAZ ARIZALARI

YANGIN

SEL,SU BASMASI

DEPREM

SAVAŞ

SEHVEN VERİ KAYIPLARI

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1985

SIZMA YÖNTEMLERİ

Oltalama mailleri ile PC'ye trojan bulaştırarak

Ağdaki herhangi bir bilgisayara bulaşması yeterlidir, sonrasında sunucular ve yedeklerin olduğu yerleri tespit sızma işlemlerine başlarlar

Lisanssız Yazılımlar ile trojan bulaştırarak

Kullanıcı ilk bulduğu siteden yazılım indirir ve bilgisayarına kurar. Siteden indirilen lisansa gerek duyulmayan(crackli) yazılım aslında bir trojan içermektedir. Yazılımın orjinal kendi sitesinden indirilmesi gerekir

Açık portlar üzerinden şifre denemeleri ile

Tüm internete açık "Uzak Masaüstü" bağlantıları aslında gün içinde 10binlerce defa, haftalar ve aylar boyunca farklı şifre kombinasyonları ile denenir

USB'ye bulaşan trojanların çalıştırılması ile

USB'ye bulaşan trojanlar, farklı bilgisayarlara takıldığında otomatik olarak sisteme yayılır ve anında bulaşma gerçekleşir.

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1995

FİDYE YAZILIMI SALDIRILARI

- Genellikle gece saatlerinde gerçekleştirilir.
- Çoğunlukla sabah mesai saatlerinde fark edilir.
- Sunucu kontrol edildiğinde dosyaların şifrelendiği ve uzantılarının değiştirildiği görülür.
- Şifrelenen dosyalar genellikle veritabanı veri dosyaları ve bunların yedekleridir.
- Her şifrelenen klasörün içine bir metin dosyası bırakılır. Bu dosya, hacklenme durumunu ve kurtarma için iletişim bilgilerini içerir.
- Şirket önce yedeklerden veri kurtarmayı dener. Başarısız olursa fidyecilerle pazarlığa başlar. Ödeme genellikle bitcoin ile yapılır. Ödeme sonrası şifre çözme yazılımı sağlanarak veriler kurtarılır.
- Hackerlara fiziki olarak ulaşmak mümkün değildir, ancak e-posta üzerinden iletişim kurulabilir. Ayrıca, bitcoin yasal bir para birimi olmadığından takibi zordur. Çoğunlukla saldırılar yurt dışından yapılır, ancak Türkçe mesaj bırakmayı da tercih edebilirler.

FİDYE YAZILIMI SALDIRILARI

- Fidyeciler, şifreleme öncesinde ağınıza sızarak verileri hedef alır ve haftalarca bekleyebilirler. Amaçları, sadece verileri değil yedekleri de şifrelemektir. Aksi halde, şirketler fidye ödemek yerine yedeklerden geri dönüş yapabilir.
- Fidye ödemekten başka çare bırakmamak asıl amaçlarıdır.
- Büyük dosyaların şifrelenmesi zaman aldığı için genellikle gece saatleri ve hafta sonları tercih edilir.
- Yedekleri doğrudan silmeyi de tercih edebilirler.
- Buluta yedekleme yapılıyorsa buluttaki verileri de silmektedirler.
- Sorun çözüldükten sonra DDoS saldırılarının gözlemlendiği durumlar da olabilmektedir.

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

YAŞANMIŞ KÖTÜ ÖRNEKLER

Farklı şirketlerin yaşadığı ve benzer çözümlerle aşmaya çalıştıkları vakalar,

Fidye yazılımı saldırısına uğrayan firmalar genellikle hızlıca dış danışmanlık hizmeti alır. Bu danışmanlar, veri kurtarma sürecini üstlenmiş gibi görünerek mevcut IT ekibini yönetime karşı suçlar ve süreci devralır.
Genellikle eski bir yedek mevcut IT ekibi tarafından bulunsa da, danışman firma bu başarıyı kendine mal eder. Danışman firmalar, yüksek kurtarma ücreti, uzun süreli güvenlik danışmanlığı ve yeni donanım satışları gibi ek gelirler elde eder.
Çoğu zaman, firmanın hızlıca faaliyete geçmesi yerine sürecin uzaması tercih edilir; bu, faturaların kabul edilmesini kolaylaştırır. Benzer vakalarda sistem kesintileri 3 gün ila bir hafta sürebilir ve bu, firmalarda iş ve prestij kaybına neden olur.
IT çalışanları ve yöneticiler, uykusuz geceler geçirirken, diğer çalışanlar günlerce sistemlerin tekrar çalışmasını bekler.

Öneri

Olayla ilgili tedbir almak IT çalışanlarının sorumluluğundadır; ancak kriz döneminde en büyük çaba yine onlardan gelecektir. Veri kurtarma sürecinde sağduyulu bir yaklaşım benimsenmeli, ardından IT personelinin bilinç seviyesi artırılarak eksiklikler giderilmelidir.

Öneri

Çoğu firmanın birden fazla fiziki güvenliği sağlayan görevlisi bulunabilir. Buna benzer şekilde, IT(BT) ekibi de siber güvenliğinizi sağlayan kişilerdir. Fiziksel güvenliğin yanı sıra, siber güvenliğe de yeterli çalışan sayısı, zaman ve bütçe ayırılması gerektiği unutulmamalıdır.

Öneri

Olay öncesinde yapılması gereken yatırımların aksatılmadan gerçekleştirilmesi büyük önem taşır. Firewall, Active Directory, antivirüs, yeni sunucular, yedekleme üniteleri, ek diskler ve güvenlik hizmetleri gibi bileşenlerin eksiksiz bir şekilde kurulması gerekir. Bu süreçlerin yaşanmaması adına, bütünleşik bir güvenlik yaklaşımı benimsenmeli ve sistemler, profesyonel gözlerle belirli aralıklarla gözden geçirilmelidir. Ayrıca, SOC (Security Operation Center) hizmetlerinin alınması da sistem güvenliğini sağlamak için kritik bir adımdır.

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1995

YAŞANMIŞ İYİ ÖRNEKLER

Bir şirkette çalışan IT Yöneticisinin anlattığı gerçek bir şifreleme saldırısı vakası,

Olay öncelikle bir ihtiyaç neticesinde oluşturulan önemsiz bir makinadaki RDP eşimiyle yaşanmıştır.
Bu sunucu tüm şirket kaynaklarında izole olmasına rağmen bir çalışan tarafından ikinci bir ağ kartı takılarak şirket ağına da dahil edilmiştir.
Saldırganla bu makina eriştiklerinde şirket içi ağa'da erişebilir duruma gelmişler. Bu ağ üzerinden öncelikle ip taramaları yaparak sunucu sistemlerine ulaşmış, sonrasında da işletim sistemlerindeki güvenlik açıklarından ERP veritabanı sunucularına dahi erişebilmişlerdir.

Aksiyon Planı

Kuruluş olarak uygulama ve veri tabanlarının bulunduğu sunucular için çok katmanlı veri yedekleme modeliyle gerekli tedbir ve önlemleri almış durumdaydı.

Bu yöntemler sırasıyla, D2D yedekleme disklerine günlük olarak verilerin yedeklenmesi, veritabanlarının haftanın her günü değişen datalar ve haftada 1 tüm verilerin off-line yedeklenmesi, sanal sunucuların günlük yedeklenmesi, SAN veri depolama cihazlarının gölge kopya veya fotoğraf olarak (Snapshot) yedeklenmesi şeklindedir. Son olarak aylık olarak TAPE ünitelerinde de yedekler alınmaktadır.

Olay günü saat 00:05 sıralarında sisteme yetkisiz ve olmaması gereken bir şekilde erişim yapılmıştır. Bu durum izleme sistemleri tarafından BT personeline SMS yoluyla mesaj olarak ulaştırılmış ve personel oluşan bu alarmın detaylarını incelemek üzere sistemlere erişmiştir. Bu erişim süresi takriben 20 dakika sürmüş ve 00:25 civarı sistemlerin saldırganlar tarafından ele geçirildiğini ve şifrelemeye başlandığını görmüşlerdir.

BT personeli henüz şifreleme tamamlanamadan firewall sistemlerinden erişimleri kapatmış ve makinaları da resetlemiştir.
Şifrelemeye maruz kalan bir kaç sistem gece saat 00:00'da alınan storage snapshot verilerine geri dönerek sanal makinaları saldırı öncesindeki ana geri döndürmüşlerdir.

1 tanesi dışındaki tüm sistemleri saldırı öncesindeki zaman çok kısa bir sürede (Yaklaşık 5 dakika) dönülmüştür.

Kalan 1 adet sistem doşya paylaşım sunucu olarak çalışan ve NAS ünitesindeki paylaşımlı alandır. Bu ünite de güvenlik yapıları eksik bir durumda olduğu için ele geçirilmiş olup bir türlü şifreleme süreci durdurulamamıştır. Yaklaşık 8 saat sonrasında tüm dosyalar şifrelenmiş olarak saldırgan işini tamamlamıştır.

Bu verilerin geri kazanımı ancak TAPE ünitelerindeki bir önceki ay'a ait yedekleme kartuşundan geri yüklenerek kurtarılabilmiş olup tahribi bir aylık dosya içeriği kayıp yaşanmıştır. Bu dosyalar şirketin süreç, talimat vb içerikleri olduğundan son 1 aylık süredeki değişikliklerin yeniden tespit edilmesi ve güncellenmesi gibi bir zaman kaybına da yol açmıştır.

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

ARAŞTIRMALARA GÖRE

Ransomware Gece 01:00 – 05:00 arasında yapılıyor.

%94 Oranında yedekleri hedef almaktadırlar.

Sorun yaşayanların %67'si yedekleri kriptolandığında hacker'a para ödeyerek geri döndürüyor.

Sorun yaşayanların %36'sı yedekleri kriptolanmadığı halde para ödeyerek geri döndürüyor.

Yedekleri şifrelemeyi başaramadılarsa ortalama olarak yarı fiyatı istenmektedir.

2021 yılında ortalama fidye yazılımı taleplerinin 2020 yılına göre %43 artışla 220.298 $ olduğu tahmin ediliyor.

Sophos, Nisan 2022'deki Fidye Yazılımı Durumu raporunda, 1 milyon dolar veya daha fazla fidye ödeyen kurbanların oranında neredeyse üç kat artış tespit etti: 2020'de %4'ten 2021'de %11'e yükseldi. Aynı dönemde, 10.000 dolardan az ödeyenlerin oranı %34'ten %21'e düştü.

Bitcoin, fidye yazılımı ödemelerinin yaklaşık %98'ini oluşturuyor. Ancak, Bitcoin'in akışını ve kaynaklarını tespit etmek giderek daha kolay hale geliyor. Daha fazla gizlilik odaklı dijital para birimlerinin (ör. Monero) siber suçlular için tercih edilen ödeme yöntemi olarak popülerlik kazanacağına dair erken belirtiler var.

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

ARAŞTIRMALARA GÖRE

2022'de fidye yazılımı mağdurlarının tahmini %41'i fidye ödedi. Bu, 2021'de %50, 2020'de %70 ve 2019'da %76 ile karşılaştırılabilir.

2022'de fidye ödeyen kuruluşlar ortalama olarak verilerinin yalnızca %61'i geri aldı. Yalnızca %4'ü tüm verilerini geri aldı.

Fidye ödeyen şirketlerin %80'i ikinci kez saldırıya uğradı, %40'ı tekrar ödeme yaptı. Tekrarlanan mağdurların %70'i ikinci seferde daha yüksek bir miktar ödemek zorunda kaldı.

2022 yılında işletmelere yönelik fidye yazılımı saldırılarının %69'u e-posta yoluyla başlatıldı.

250'den fazla çalışanı olan kuruluşlarda fidye yazılımı saldırılarının %75'i e-posta yoluyla başlatıldı.

Tüm e-postaların yaklaşık %1'i fidye yazılımıyla ilgili bir bağlantı veya dosya içeriyor.

Tüketici hizmetlerinde fidye yazılımı saldırılarının %70'i web trafiği ve web uygulamalarından kaynaklanıyor.

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

ARAŞTIRMALARA GÖRE

Fidye yazılımlarının küresel toplam maliyetinin 2023 yılında 30 milyar doları aşması bekleniyor.

Yıllık geliri 10 milyon doların altında olan şirketler için 2023 yılında ortalama kurtarma maliyeti 205.400 dolardır.

Bir işletme ödeme yapmaya karar verdiğinde, fidye ödemesi saldırının toplam maliyetinin yaklaşık %15'idir. Geri kalanı olay raporlama çabası, sistem geri yüklemesi, yasal ücretler, izleme maliyetleri ve iş kesintisinin genel etkisini içerir.

Fidye yazılımı saldırısına uğrayan şirketlerin %40'ı bu nedenle çalışanlarını işten çıkarıyor.

Şirketlerin %39'u fidye yazılımı saldırısından kurtulmak için bir haftaya kadar zaman harcıyor.

2021 yılında fidye yazılımı saldırıları yoluyla kazanılan tüm paranın yaklaşık %74'ünün Rusya bağlantılı bilgisayar korsanlarına gittiği tahmin ediliyor.

Barracuda Networks, siber sigortası olan kuruluşların %77'sinin en az bir kez saldırıya uğradığını, sigortası olmayan kuruluşların ise %65'inin saldırıya uğradığını buldu. Saldırganların, bu şirketlerden ödeme alma olasılığının daha yüksek olduğu varsayımıyla, sigortalı olduğu bilinen hedeflere kasıtlı olarak odaklanmak için sosyal mühendislik kullanabilecekleri tahmin ediliyor.

SystemSoft®

www.systemsoft.com.tr

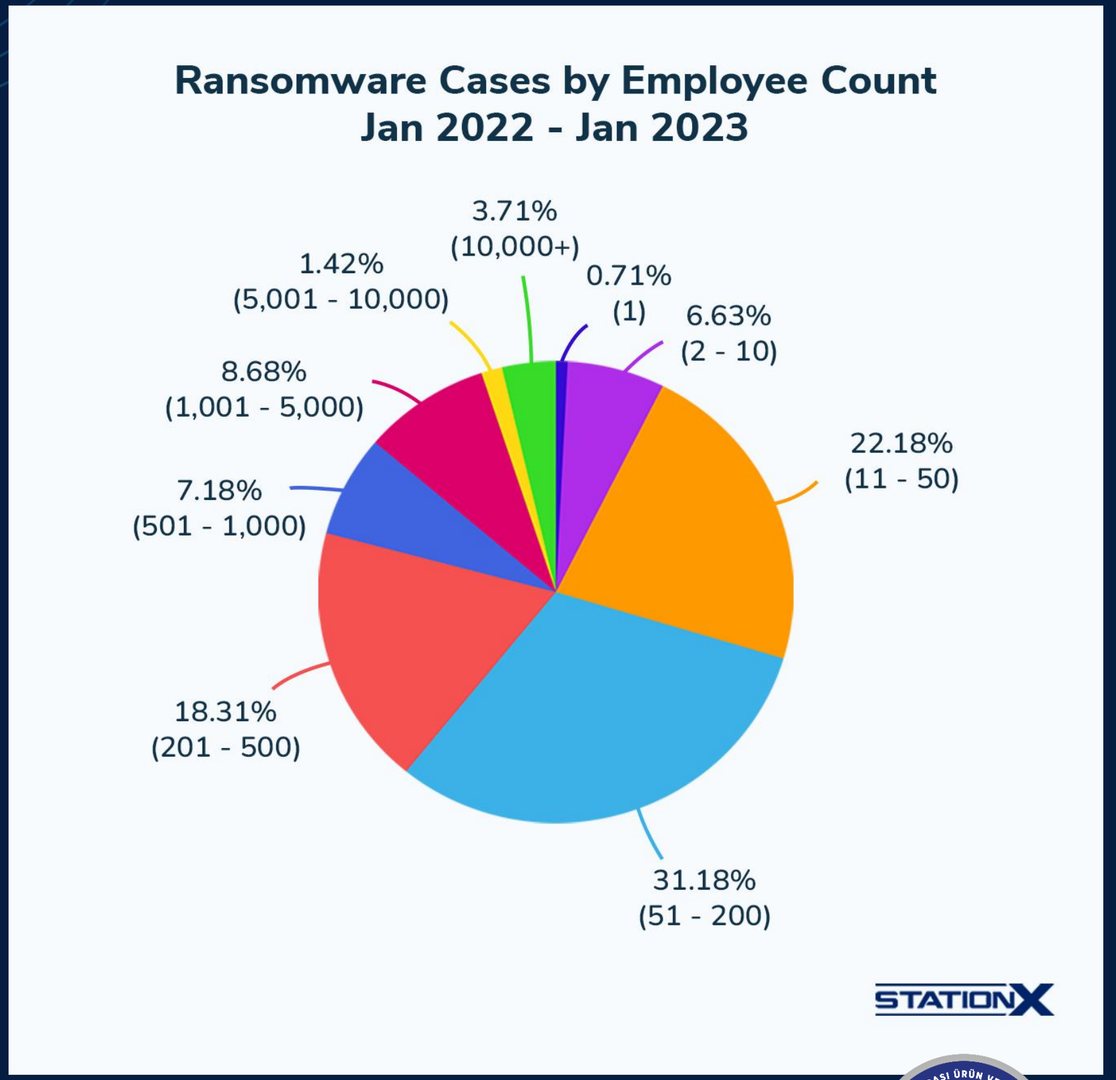
OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

ARAŞTIRMALARA GÖRE

Yandaki grafikten, çalışan sayısı arttıkça daha az vaka olduğu görünüyor.

Bunun sebebi kalabalık şirketlerin İnternet Güvenliği üzerine daha çok eğilim göstermesi olabilir.

Aslında şirketinizde ne kadar çok PC ve kullanıcı varsa tehdit daha da artmaktadır. Ancak alınan tedbirlerin, siber tehditlere karşı işe yaradığını yandaki grafikle görebilmekteyiz.



SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1995

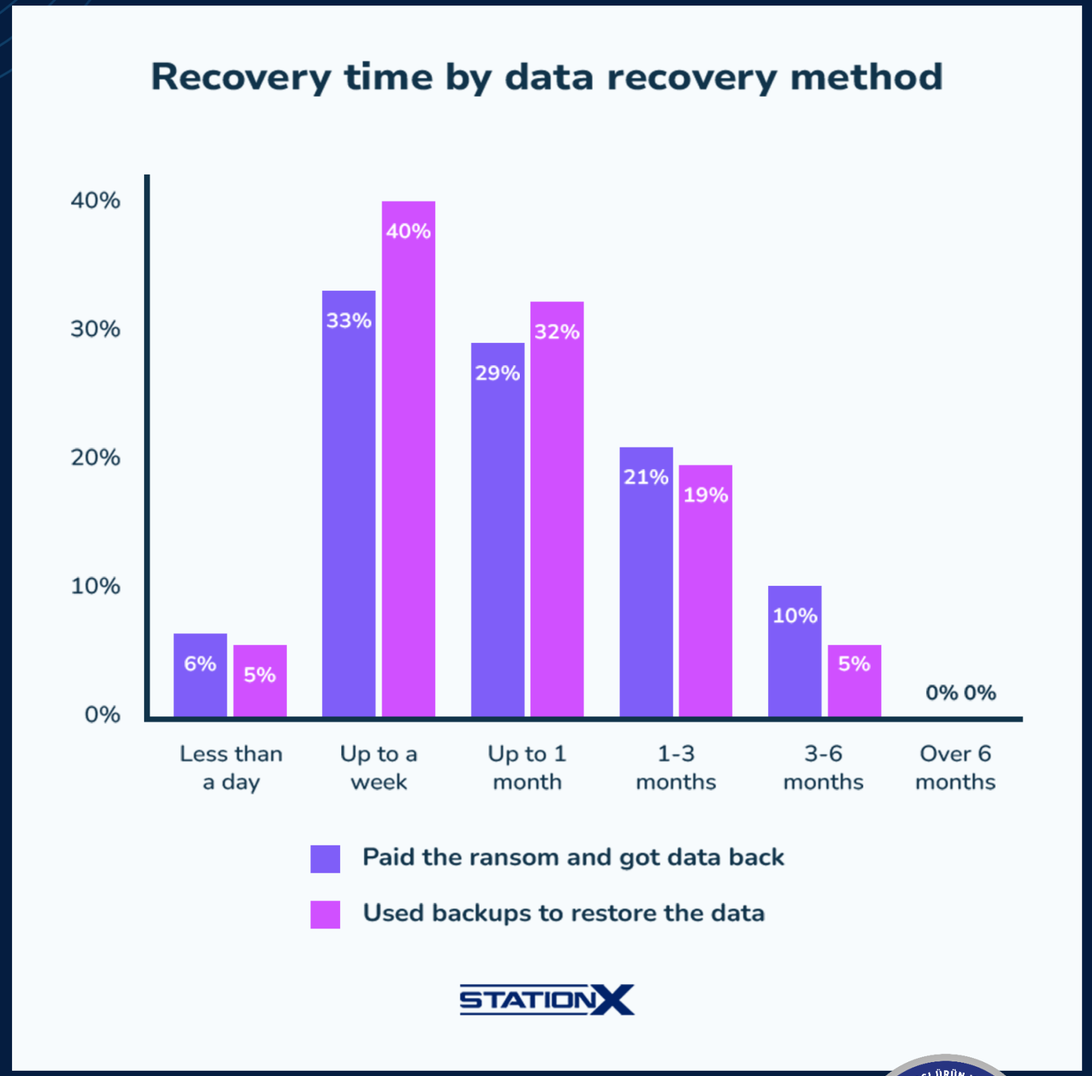
ARAŞTIRMALARA GÖRE

Soldaki Mavi sütunlar hackerlara para ödeyerek sorunun çözüldüğünü gösterir.

Sağdaki Mor sütunlar yedekten geri dönülerek sorunun çözüldüğünü gösterir

1 Günde
1 Haftada
1 Ayda
3-6 Ayda
6 Aydan Uzun

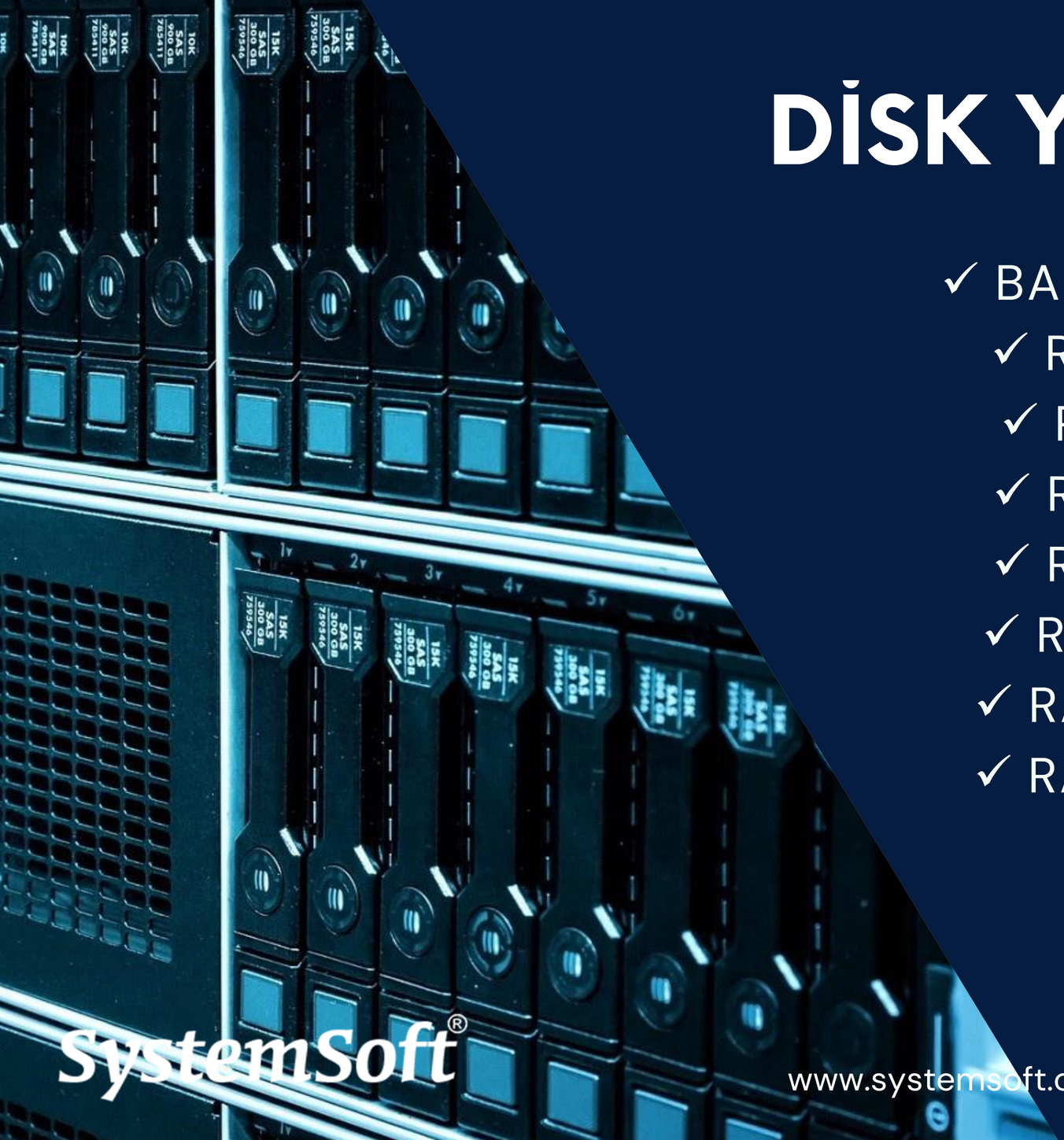
Süreler için vaka analizi yapılmıştır.



SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1995



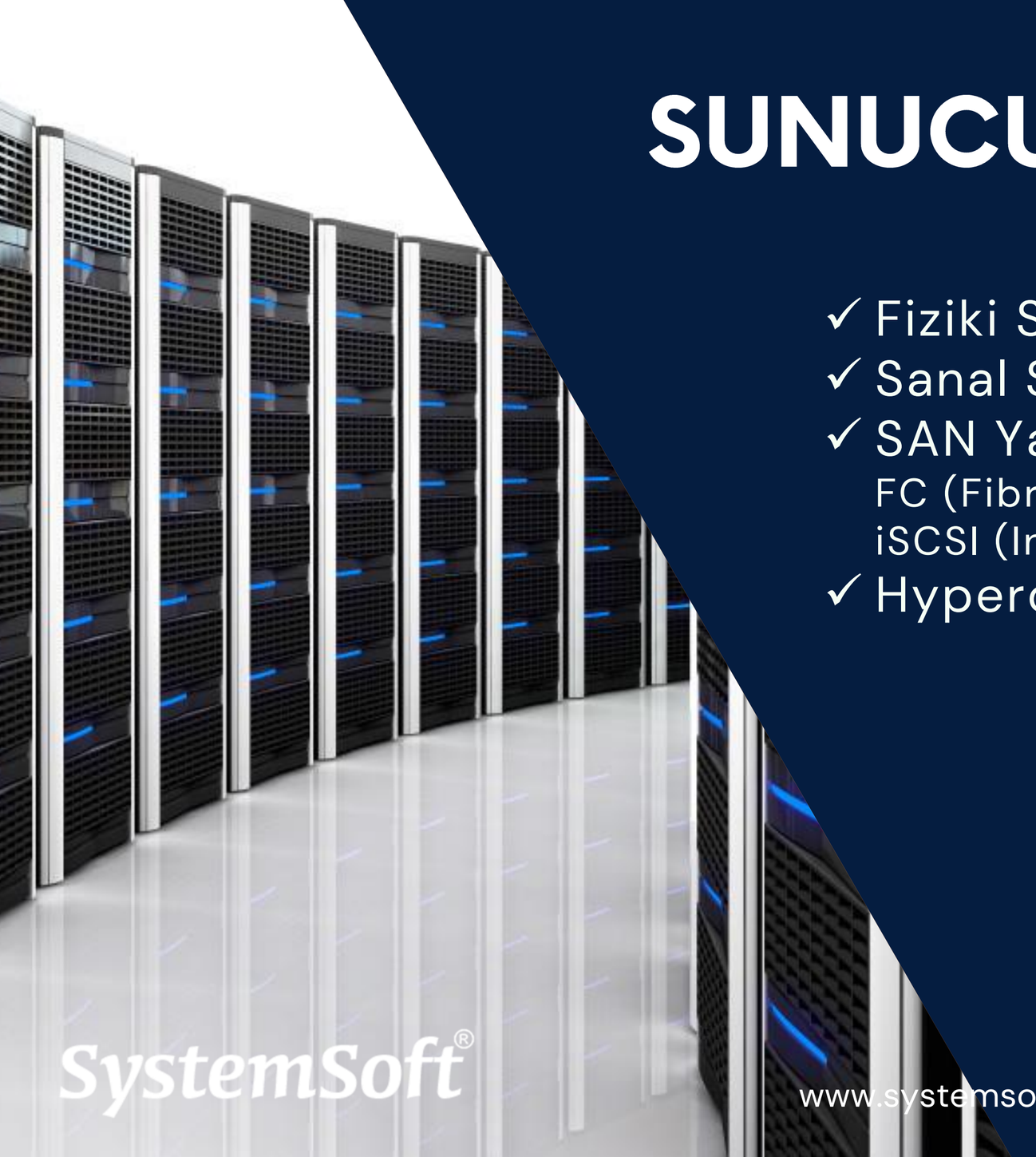
DİSK YAPILARI

- ✓ BASİT YAPI
- ✓ RAID 0
- ✓ RAID 1
- ✓ RAID 5
- ✓ RAID 6
- ✓ RAID 10
- ✓ RAID 50
- ✓ RAID 60

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995



SUNUCU YAPILARI

- ✓ Fiziki Sunucular
- ✓ Sanal Sunucular
- ✓ SAN Yapılı Sanal Sunucular
  FC (Fibre Channel)
  iSCSI (Internet Small Computer Systems Interface)
- ✓ Hyperconverge Sanal Sunucular

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

YEDEKLEME YÖNTEMLERİ

- Database Yedekleme
  Full Backup
  Differencial Backup
  (Hızlı çalıştığı için ve az yer kapladığı için gün içerisinde birkaç defa uygulanabilir. Ancak Full Backup olmadan bir işe yaramaz.)
- Offline Yedekleme
  (Basit bir harici disk, DVD yada Tape Backup)
- NAS'a Sanal Makine Yedekleme
- Snapshot
- Immutable yedekleme
- Off-site yedekleme
- Replication
- Buluta yedekleme

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

YEDEKLEME MEDYALARI

Offline Yedekleme

NAS

SAN

HDD (D2D)

DVD

TAPE

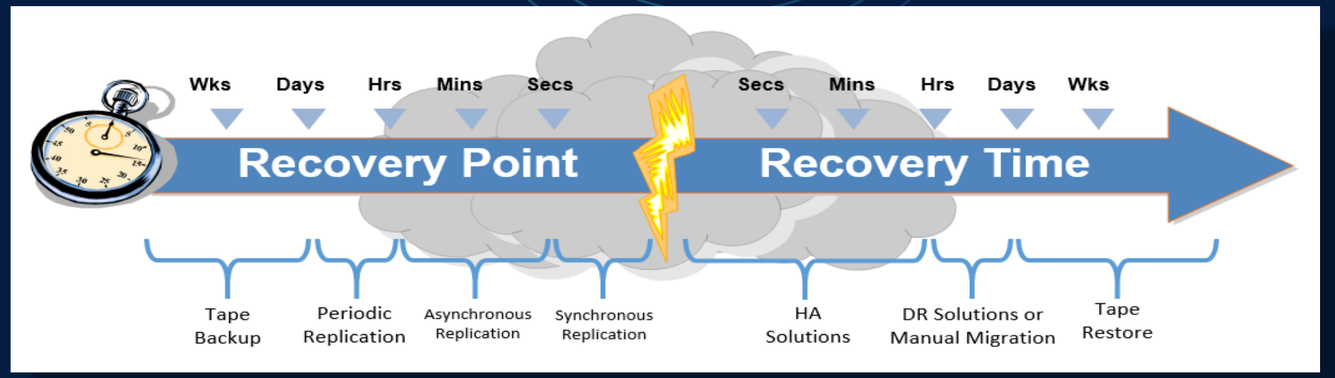
SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1995

	Maliyet	Faydası	1-20 Adet PC	21-50 Adet PC	51-100 Adet PC	100'den fazla PC
Güçlü Şifreler Kullanın	Bedava	Hacker	**Zorunlu**	**Zorunlu**	**Zorunlu**	**Zorunlu**
Şifrelerinizi koruyun	Bedava	Hacker	**Gerekli**	**Gerekli**	**Gerekli**	**Gerekli**
Ağ paylaşımı dikkatli yapılmalı	Bedava	Hacker	**Gerekli**	**Gerekli**	**Gerekli**	**Gerekli**
Offline Yedekleme	1000 ₺ - 10000 ₺	Yangın-Sel-Deprem-Hacker	**Zorunlu**	**Zorunlu**	**Zorunlu**	**Zorunlu**
Eski Yılların verileri	1000 ₺ - 10000 ₺	Yangın-Sel-Deprem-Hacker	**Zorunlu**	**Zorunlu**	**Zorunlu**	**Zorunlu**
NAS Cihazı	30k₺ - 300k₺	Yangın-Sel-Deprem-Hacker	İsteğe Bağlı	**Zorunlu**	**Zorunlu**	**Zorunlu**
Otomatik Yedekleme	Bedava	Hacker	İsteğe Bağlı	**Günde 1**	**En Az Günde 1**	**En Az Günde 1**
Firewall	20k₺ - 300k₺	Hacker	İsteğe Bağlı	**Gerekli**	**Zorunlu**	**Zorunlu**
Windows Firewall açık olmalı	Bedava	Hacker	**Zorunlu**	**Zorunlu**	**Zorunlu**	**Zorunlu**
VPN İle Erişim	Firewall + Switch	Hacker	Gerekirse	**Gerekli**	**Zorunlu - Çift Faktörlü**	**Zorunlu - Çift Faktörlü**
VLAN Yapısı	Firewall ile birlikte	Hacker	İsteğe Bağlı	**Gerekli**	**Gerekli**	**Zorunlu**
Active Directory	Windows Server	Hacker	İsteğe Bağlı	**Gerekli**	**Zorunlu**	**Zorunlu**
Antivirüs	2000₺ x PC	Hacker	**Zorunlu**	**Zorunlu**	**Zorunlu**	**Zorunlu**
Merkezi Antivirüs Yönetimi	Antivirüs ile Ücretsiz	Hacker	İsteğe Bağlı	**Gerekli**	**Zorunlu**	**Zorunlu**
RAID 1 - 5 - 6	Disk x 2	Donanım Arızası	İsteğe Bağlı	**Gerekli**	**Zorunlu**	**Zorunlu**
Hot Spare Disk	1 Adet Disk	Donanım Arızası	Gereksiz	Gereksiz	**Gerekli**	**Zorunlu**
Bilinçlendirme Eğitimleri	Bedava	Hacker	**Zorunlu**	**Zorunlu**	**Zorunlu**	**Zorunlu**
Güvenli E-Mail Hizmeti	6-10$ * PC	Hacker	İsteğe Bağlı	**Gerekli**	**Zorunlu**	**Zorunlu**
Misafir Ağı	Bedava	Hacker	İsteğe Bağlı	**Gerekli**	**Gerekli**	**Gerekli**
Sunucu Güncellemeleri	Bedava	Hacker	**Takip Edilmeli**	**Takip Edilmeli**	**Takip Edilmeli**	**Takip Edilmeli**
Log ve SIEM	Bedava	Hacker	İsteğe Bağlı	İsteğe Bağlı	İsteğe Bağlı	**Gerekli**
Sanallaştırma	Bedava - 1000$	Donanım Arızası	İsteğe Bağlı	**Gerekli**	**Zorunlu**	**Zorunlu**
SAN	10k$	Donanım Arızası	Gereksiz	**İsteğe Bağlı**	**Gerekli**	**Zorunlu**
Cluster Sunucu	20k$-60k$	Felaket	Gerekli Değil	Gerekli Değil	Gerekli Değil	İsteğe Bağlı
Hyperconverge	120k$	Hacker	Gerekli Değil	Gerekli Değil	Gerekli Değil	İsteğe Bağlı
Yangın Bastırma	20k₺	Yangın	İsteğe Bağlı	**Gerekli**	**Zorunlu**	**Zorunlu**
Yangın Korumalı Kasa	30k₺	Yangın	İsteğe Bağlı	**Gerekli**	**Zorunlu**	**Zorunlu**
10Gbit Ethernet	30k₺	Hacker	İsteğe Bağlı	İsteğe Bağlı	**Gerekli**	**Zorunlu**
Penetrasyon Testi	100k₺-200k₺	Hacker	Gereksiz	Gereksiz	İsteğe Bağlı	**Zorunlu**
SOC Hizmeti	10k$-150k$	Hacker	Gereksiz	Gereksiz	İsteğe Bağlı	**Zorunlu**

SON YEDEK SÜRESİ – GERİ GETİRME SÜRESİ & MALİYET TABLOSU



Recovery Time Objective (RTO) - Downtime

Recovery Point Objective (RPO) - Data Loss

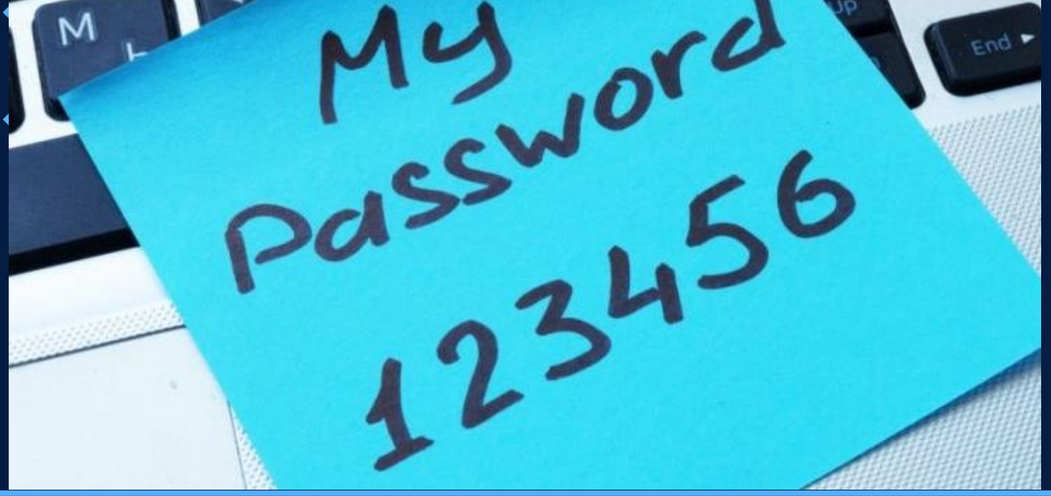
	Zero-1 Sec	1 Minute	1 Hour	1 Day
Zero-1 Sec	>$1,000,000 Multiple active servers with bidirectional replication (usually requires code change)	$100k-$500k Clustering w/SAN, synch AlwaysOn Availability Groups (EE), synch database mirroring	$100k-$250k Synch SAN replication, synch VM replication	
1 Minute			$50k-$250k Async AlwaysOn Avail Groups (EE), async DB mirroring (EE)	$5k-$100k Log shipping, async SAN replication, async VM replication
1 Hour			$5k-$100k Log shipping, async SAN replication, async VM	
1 Day				

BRENT OZAR UNLIMITED

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1995



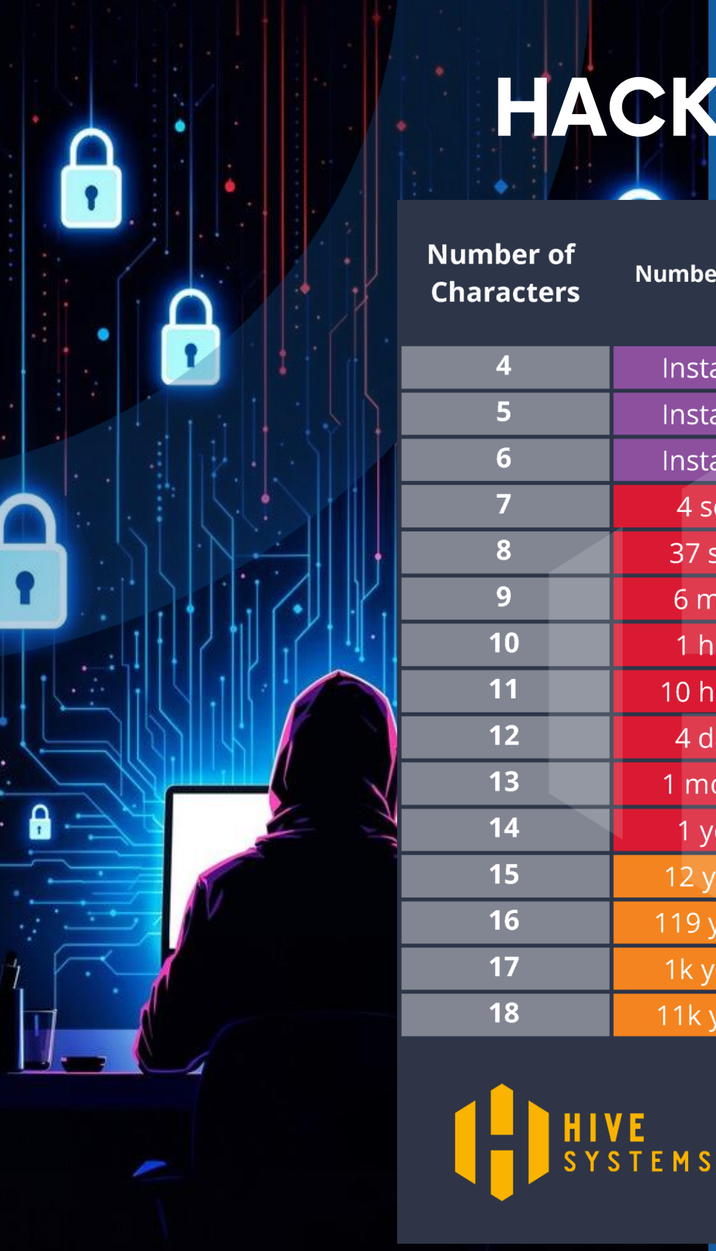
GÜVENLİK İPUÇLARI

- ✓ **Güçlü Parolalar Kullanın:** Parolalarınızı karmaşık ve tahmin edilmesi zor hale getirin.
- ✓ **Düzenli Yedekleme Yapın:** Verilerinizi düzenli olarak yedekleyin ve yedeklerinizi güvenli bir yerde saklayın.
- ✓ **Güncellemeleri İhmal Etmeyin:** Yazılım ve donanım güncellemelerini zamanında yapın.
- ✓ **Güvenlik Duvarları ve Antivirüs Yazılımları Kullanın:** Sistemlerinizi korumak için güvenlik duvarları ve antivirüs yazılımları kullanın.
- ✓ **Eğitim ve Farkındalık:** Çalışanlarınıza siber güvenlik konusunda eğitim verin ve farkındalık yaratın.
- ✓ **Çok Faktörlü Kimlik Doğrulama (MFA) Kullanın:** Hesaplarınızı ek bir güvenlik katmanı ile koruyun.
- ✓ **Şifreleme Kullanın:** Hassas verilerinizi şifreleyerek yetkisiz erişimlere karşı koruyun.
- ✓ **Sosyal Mühendislik Saldırılarına Karşı Dikkatli Olun:** Phishing ve diğer sosyal mühendislik saldırılarına karşı dikkatli olun ve çalışanlarınızı bu konuda bilgilendirin.
- ✓ **Ağ Segmentasyonu Yapın:** Ağınızı segmentlere ayırarak saldırıların yayılmasını önleyin.
- ✓ **Güvenlik Politikaları Oluşturun:** Şirketiniz için net ve uygulanabilir güvenlik politikaları oluşturun ve bunları düzenli olarak gözden geçirin.
- ✓ **İzleme ve Denetim:** Sistemlerinizi sürekli izleyin ve güvenlik denetimleri yaparak olası tehditleri erken tespit edin.
- ✓ **Yedekleme ve Kurtarma Planları:** Acil durumlar için yedekleme ve kurtarma planları oluşturun ve bu planları düzenli olarak test edin.

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1995



HACKERLARIN ŞİFRE ÇÖZME SÜRELERİ

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090
Password hash: bcrypt

HIVE SYSTEMS

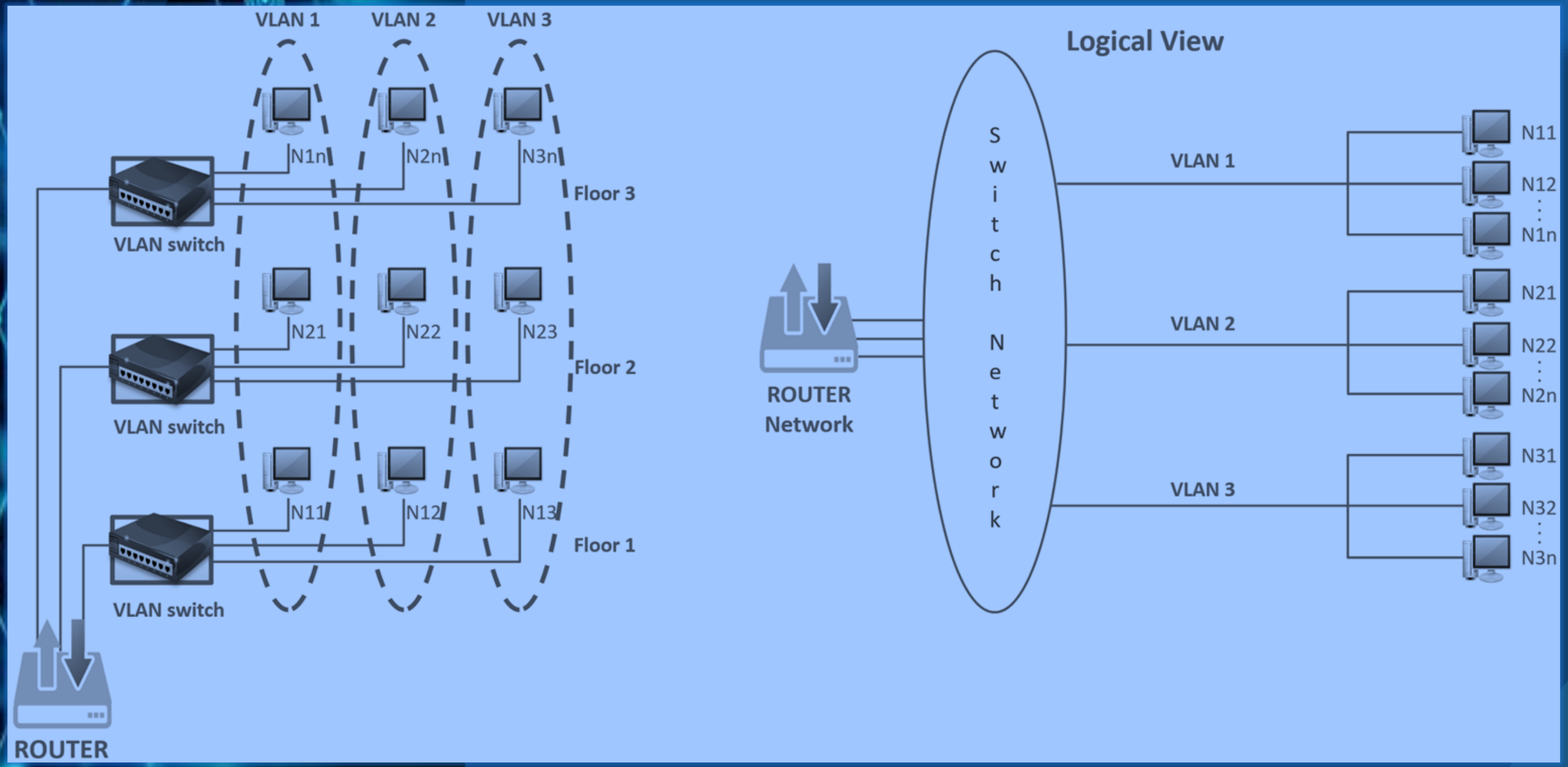
› Learn more about this at hivesystems.com/password

SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ OSS 1995

VLAN (Virtual LAN)



SystemSoft®

www.systemsoft.com.tr

OTOMOTİV SATIŞ SONRASI ÜRÜN VE HİZMETLERİ DERNEĞİ
OSS
1995

TEŞEKKÜR EDERİZ

WEB SİTESİ

www.systemsoft.com.tr
www.b2bkur.com

TELEFON

0850 242 0 444

E-POSTA

pazarlama@sistemyazilim.com

SystemSoft®