# Netaş SOC Hizmetleriyle Sektörde Fark Yaratıyor.

## Netaş, siber güvenlik hizmetleri kapsamında sunduğu ürün ve çözümleriyle sektöre yön vermeye devam ediyor.

Netaş Siber Güvenlik Hizmetleri Direktörü **Fatma Hacıoğlu Doğar** ile siber güvenlik alanındaki hikayemiz, sunduğumuz ürünler ve uçtan uca bütünleşik hizmetlerimiz hakkında konuştuk.

Sohbetimiz sırasında Netaş'ın güvenlik alanındaki farkını bir kez daha detaylarıyla dile getiren **Fatma Hacıoğlu Doğar** siber güvenlik alanındaki hizmetlerimizi şöyle özetliyor:

"Netaş, tüm teknolojilerde Türkiye pazarında lider bir şirket. Son 2 yıllık çalışmalarımız ile Netaş'ı uçtan uca bütünleşik siber güvenlik hizmetleri de sunan bir yapıya dönüştürdük. Netaş Siber Güvenlik bünyesinde müşterilerimizin ve sektörün ihtiyaçlarına yönelik hizmetleri, teknolojileri hatta ürün Ar-ge çalışmalarını modelledik. SOC/SIEM Hizmetleri, Bütünsel Güvenlik ve MSS Hizmetleri'nin yanında Teknoloji Danışmanlığı ve Test Hizmetleri ile Yeni Nesil Güvenlik alanlarında müşterilerimize çözümler sunuyoruz. Örneklemek gerekirse; yeni bilgi güvenliği analiz dönüşümü ile beraber firewall servisinin yanı sıra son kullanıcı analitiği servislerini kurguladık. Tüm bu hizmetlerimiz ve geniş teknoloji-ürün portföyümüz ile enerji, kamu, finans, perakende, uluslararası pazarlar gibi pek çok sektöre hizmet veriyoruz.

Doğar, 'Netaş, Siber Güvenlik Hizmetleri alanında hangi çözümleri sunuyor?' sorusuna ise şu yanıtı verdi:
"4-5 ana temel üzerine güvenliği oturtacak olursak; SOC/SIEM Hizmetleri, Bütünsel Güvenlik ve MSS Hizmetleri ile Teknoloji Danışmanlığı ve Test Hizmetleri ve Yeni Nesil Güvenlik Ar-ge alanlarında çözümler sağlıyoruz.
Hizmetlerin katma değerinin ise özellikle güvenlik olaylarının müşterilerden güvenlik bilgi ve olay yönetimi sistemi ve platformunda toplanması, korelasyonu, tehdit olup olmadığına yönelik çalışmaların yapılması, izlenmesi, güvenlik bilgi olayları sonuçlarından elde ettiğimiz riskleri bertaraf edecek çalışmaların proaktif ve prediktif olarak yapılması şeklinde özetleyebiliriz."

### Önemi giderek artan Siber Güvenlik İstihbaratı

"Netaş'ı farklılaştıran hizmetlerimizden bir diğeri olan Siber Tehdit İstihbaratı da tehdit riski taşıyan, dünya üzerinde yayılmak üzere olan bulgular yani IOC (Indicator of Compromise) ortaya çıktığında dünyadaki otoritelerden verileri toplayan bir teknolojidir." Toplanan verilerin, müşterilerine ve kendi altyapılarına tehdit olabilir mi diye değerlendirildiğini ve verilerin yeri, zamanı, kimleri hedeflediği, zamanı, kimleri hedeflediği, hangi sistemlerle ilişkili olduğu gibi donelerle filtrelendiğini belirten Doğar, "Gelecekte siber güvenlik istihbaratının öneminin arttığını göreceğiz. Bu konuda çok ciddi bir gelecek görüyoruz. Bu nedenle bu alana yatırım yapıyoruz. Uzmanlarımız bu konu üzerinde yoğun bir şekilde çalışıyorlar. Yeni tehdit ve risk taşıyan verileri toplayarak hem kendi altyapımız hem de müşterilerimiz için kullanıyorlar." şeklinde görüş belirtiyor.


Fatma
Hacıoğlu Doğar

### Hacker perspektifiyle sürekli izleyen Kırmızı Takım

Diğer fark yaratan Kırmızı Takım hizmeti hakkında Fatma Hacıoğlu Doğar, şu bilgileri paylaşıyor:
"Gördük ki güvenlik alarmının alınmasından sonra değerlendirme, risklerin yönetilmesi, aksiyonların belirlenmesi ve müşteri tarafında aksiyonların alınması alanında zamanla otomasyona bağlı bir körlük oluşabiliyor. Biz bu körlüğü nasıl engelleriz diye düşünerek bunu sahada yaşayan, sürekli hacker perspektifiyle zafiyetleri gören ve bu zafiyetlerden istifade edilip edilmeyeceğini araştıran, gerçek bir risk varsa SOC ekibine bilgi veren ve onları değişime zorlayan bir hizmeti daha hayata geçirdik. Kırmızı Takım Hizmetleri'nde, testler sosyal mühendislikten ağ güvenliğine, fiziksel seviyedeki güvenlik testlerine, uygulama güvenliğine kadar geniş bir yelpaze içerisinde ele alınıyor. Kırmızı Takım olgusunu herkes kullanabilir ama kimse içinde bu modüllerle ve sürekli şekilde yapmıyor. Bu da Netaş'ı öne çıkaran farklardan biri."

### Gelişmiş Siber Operasyon (SOAR) ve Proaktif Yönetilen Hizmetler (MDR):

Netaş olarak yıllardır başarıyla sürdürdüğümüz SOC altyapısı artık klasik SIEM Sistemleri - Siber Güvenlik Olay Yönetim Merkezi'nden çok daha fazlası. Makine öğrenme; analitik, yapay zeka, siber istihbarat ile destekli; gerek uç nokta, gerek son kullanıcı gibi tüm güvenlik sinir uçlarına erişebilen bütünsel bir operasyon merkezinden bahsediyoruz.
Siber Güvenlik Operasyon Merkezimizde Geleneksel SOC'lerin sınılarını aştık. İçerisinde farklı kaynaklardan beslenen siber istihbaratın bulunduğu, son kullanıcıdan oluşabilecek tehditleri ihmal etmeden EDR, UBA gibi yeni teknolojilerin entegre edildiği ve NOVA gibi yerli ve milli ürünlerle güçlendirilmiş bir yapı ortaya koyduk.
Merkezimiz bünyesinde SIEM Yönetimi, Checkup, Eğitim ve Danışmanlık hizmetlerinin yanı sıra Mavi&Kırmızı Takım Hizmetleri, Zafiyet Yönetimi, Siber Tehdit İstihbaratı, MDR&EDR&UBA, Olay Otomasyonu ve Oltama Saldırı Farkındalığı gibi gelişmiş hizmetler sayesinde kurumları korumaya devam ediyoruz.


# 2018'de dünyayı kasıp kavuran siber güvenlik olayları

**İçinde bulunduğumuz 2019 yılı siber olaylar açısından yoğun geçerken; geride bıraktığımız 2018 yılı diğer son yıllarda güvenlik tehdit ve ataklarının en yoğun yaşandığı sene oldu. 2018'de akıllara yer eden olayları sizler için hazırladık.**

Acısıyla tatlısıyla geride kalan 2018, siber güvenlik anlamında birçok olumsuz olaya tanıklık etti. Birçok araştırma kurumu tarafından açıklanan en önemli olaylardan seçtiklerimizi ay sırasına göre derledik.


## OCAK
**Kripto Paraya Hücum**

2018 yılının Ocak ayı kripto para birimlerindeki ani yükselişlere sahne oldu. En popüler kripto para birimi Bitcoin 20 bin dolara kadar yükselirken kullanıcılar arasında kripto para birimlerine olan ilgi de arttı.

Ne yazık ki, bu aynı zamanda siber saldırıların da fitilini ateşlemiş oldu. Takip eden günlerde kripto para birimi borsaları saldırıya uğradı, kullanıcılar dolandırıldı, kimlik avı vb. dolandırıcılıklar tavan yaptı.

## ŞUBAT
**Petya or NotPetya**

2017 yılında sağlık, ulaştırma, devlet kurumları ve büyük ve küçük işletmelere yönelik yıkıcı saldırılarla Petya fidye yazılımı her zaman göz önünde oldu. Dünyada 2018'in Şubat ayı ise ABD hükümetinden gelen açıklama ile başladı: Trump yönetimi, 2017 yılına yapılan yıkıcı NotPetya ransomware saldırılarını Rusya'nın başlattığını iddia etti. Bu duyuru, siber savaşın sadece şirketleri değil ülkeleri de kapsayabileceğini göstermesi açısından da önem taşıyordu.

## MART
**Tüm Zamanların En Yoğun DDoS Saldırısı**

Mart ayı çoğu internet kullanıcısı için sorunlarla başladı. İlk olarak, GitHub şimdiye kadar kaydedilen en büyük DDoS saldırısına uğradığını açıkladı. Saldırı, GitHub sunucularına karşı, saniyede 1,3 terabit trafik yaratan tüm zamanların en güçlü DDoS atağı olarak kayıtlara geçti. Bu saldırı web sitesi yükleme hızından sorumlu veritabanlarının sorgulanmasına dayanan başka bir DDoS saldırısı türü olarak da farklı bir boyuta sahipti.

## NİSAN
**Alexa Casus Cihaza Dönüştü**

Nisan ayı özellikle Android kullanıcıları için hiç de iyi haberlerle başlamadı. Android tabanlı telefonlara yapılan çeşitli saldırıların ardından asıl bomba Alexa kullanıcılarının kucağına düştü. Güvenlik araştırmacıları akıllı evlerin en önemli araçlarından olan ve sahiplerinin söylediği her şeyin yapmakla yükümlü Alexa'ya bir saldırı yapıldığını keşfetti. Bu saldırıyla akıllı evlerin vazgeçilmezi olması beklenen Alexa bir anda veri toplayıp dağıtan uluslararası bir casusa dönüşmüş oldu.


## MAYIS
**Sosyal Medya Yangını**

Facebook, 2018 yılında en fazla tehdit alan sosyal medya platformu iken, Twitter da büyük bir güvenlik sorunuyla sarsıldı. Mayıs ayında, Twitter'ın baş teknoloji sorumlusu, platformun kullanıcı parolaları tüm bilgilerin düz metin olarak saklandığını açıkladı. Twitter, suçluların bu şifreleri ele geçirmesinin muhtemel olmadığını söylerken, güvenlik uzmanları kullanıcıları şifrelerini değiştirmeleri yönünde uyarılarda bulundu.

## HAZİRAN
**Veri İhlalleri Dikkat Çekti**

2018 yılında yaşanan veri ihlalleri Haziran ayında en üst seviyeye çıktı. Basında sürekli milyonlarca kullanıcının risk altında kaldığını gösteren haberler yer aldı. İlk olarak, 340 milyon kaydı olan ABD'li bir şirketin kullanıcı verileri çalındı. Gerekli düzenlemeler hızla yapılsa da şirket kullanıcılarının bir kısmı bu olumsuzluktan etkilendi.

## TEMMUZ
**Sağlık Sektörüne Büyük Vurgun**

Genelde dünya çapında sakin geçen yaz ayları, ABD'nin Atlanta kentinde yaşayanlar için çok daha yoğun ve sıcak geçti. Atlanta şehrini vuran ve 10 milyon dolar civarında maddi hasara yol açan SamSam zararlı yazılımı LabCorp isimli şirketin tüm makinelerini şifreledi.

Aynı anda Kanada'da ise CarePartners, 80.000 hastanın tıbbi geçmişini ve iletişim bilgilerini benzer bir saldırıya kurban vererek bu alada bir rekora imza attı. İşin ilginç yanı ise CBC'nin haberine göre saldırganların CarePartners'ın ağında iki yıldır güncellenmemiş bir güvenlik açığı bulduklarını ve bu sayede tüm bilgilere kolayca ulaştıklarını paylaşmaları oldu.

## AĞUSTOS
**Apple'a WannCry Şoku**

Ağustos ayında Apple'ın en büyük bileşen tedarikçilerinden biri olan TSMC (Tayvan Yarı İletken Üretim Şirketi) WannaCry şoku ile sarsıldı. Enfekte bir cihazın TSMC şebekesine bağlanmasıyla birlikte şirket, fidye yazılımının üç büyük tesisine yayılmasının önüne geçemedi.

## EYLÜL
**Havada Hack Kokusu Var**

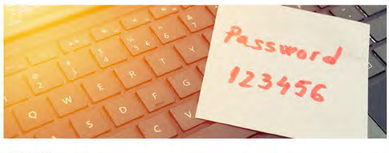
Yaz aylarının sonunda dünyaca ünlü havayolu şirketi British Airways'in 380 bin müşterisinin başı ciddi şekilde ağrıdı. Şirketin 21 Ağustos-5 Eylül tarihleri arasında yaşadığı saldırı sırasında rezervasyon işlemlerinin dahi tehlikeye girdiği görüldü. Bu saldırıyla isimler ve adresler gibi temel bilgiler çalınsa da British Airways müşterisi gezginlerin sorunları orada bitmedi. Çünkü bilgisayar korsanları müşterilerin kredi kartı detaylarına da ulaşmayı başarmıştı.


## EKİM
**Eski Çamlar Bardak Oldu**

Ekim ayı ile birlikte tüm dünya eski moda saldırı tekniklerinin hala işe yaradığını gördü. Cyrptomining olarak bilinen malware yeni bir malware olsa da güncelleme yapmayan ya da savunma sistemi kurmamış kişi ve kurumlar için yepyeni saldırı yöntemi olarak boy gösterdi. Adobe yazılımları üzerindeki açıkları kullanan son malware birçok bilgisayar sahibinin cihazını köleleştirdi.

## KASIM
**Dünya Bilgisayar Güvenlik Günü Kutlu Olsun**

Japonya Siber Güvenlik Bakanı'nın hiç bilgisayar kullanmadığını ve yanında çalışanların da bilgisayar kullanmasını yasakladığını açıklamasıyla birlikte doğan tartışmaların sonunda 30 Kasım, Dünya Bilgisayar Güvenlik Günü olarak ilan edildi.


## ARALIK
**Bu Şifrelerle Hackerlara Hayat Çok Kolay**

2018 yılının son ayında kitlesel bir Google+ veri gündemi meşgul etmeye başladı. Bu ihlali takip eden büyük çaplı bitcoin dolandırıcılığı 2019 yılının da siber güvenlik olaylarıyla geçeceğinin müjdesini verdi adeta.

Öte yandan SplashData'nın yayınladığı ve dünya genelinde en yaygın kullanılan parolaların hala "12345" ve "123456" türevleri olması hackerların işinin ne denli kolay olduğunu bir kez daha gözler önüne serdi.

# Siber güvenlik alanında 2019 beklentileri.

## 2018 yılının siber güvenlik konusunda birçok olumsuz olaya sahne olmasının ardından 2019 yılı da benzer olaylara sahne oluyor.

Siber güvenlik konusunda kişi, şirket ya da kurumlar ne kadar çok güvenlik önlemi alırsa o kadar korunaklı bir sisteme sahip oluyor. 2019 yılında uzmanların dikkat çektiği en önemli güvenlik sorunlarını sizler için hazırladık.

### 1. İnsan Faktörü

Tüm siber güvenlik tehditlerinin altında yatan en önemli etken, insan. Kişisel kullanıcı da olsa büyük bir şirketin ya da kamu kurumunun çalışanı da olsa kişiler öncelikle bilinçli ve bu konuda eğitimli olmak zorunda. Nasıl ki motorlu taşıtlar kanununa göre araç kullanacak kişilerden ehliyet isteniyor, bilgisayar kullanıcılarının da fiziksel olmasa da bilişsel olarak bir ehliyete sahip olması gerek şart.

### 2. KOBİ'ler En Cazip Hedef

Dünyada da ülkemizde de KOBİ'ler kendi işlerine yoğunlaştıkları ya da yeterli siber güvenlik yatırımı yapmadıkları için siber saldırganların hedefindeki en kolay av durumundalar. KOBİ'lerin bu hedef olma durumundan kurtulabilmeleri için yapmaları gereken ise mutlaka ama mutlaka siber güvenlik yatırımı.

### 3. Buluta Dikkat

Bir araştırmaya göre bulut tabanlı hizmetler, 2019'da da popülerliğini artırmaya devam ediyor. Güncel bir araştırma, bulut tabanlı hizmetlerdeki şirket verilerinin yüzde 7'sinin halka açık, yüzde 35'inin ise şifrelenmemiş olduğunu gösteriyor. Bu rakamlar olumlu yönde değişmediği sürece bulut, şirketlerin korkulu rüyası olabilir.

### 4. IoT İştah Kabartıyor

Nesnelerin interneti olarak bilinen IoT hizmetleri yaygınlaştıkça hackerların iştahı kabarıyor. Zira yeterli güvenliği sağlanmayan IoT'li cihazlar bulundukları her ortam için adeta pimi çekilmiş el bombası niteliğinde.

### 5. Modem Saldırıları Sürecek

Modem üreticilerinin yeterli olmayan güvenlik önlemleri ve kullanıcıların zayıf şifre tercihleri 2018'de başlarına önemli sorunlar açmıştı. 2019 yılında da kötü niyetli saldırganlar modemleri ev ve işyerlerinin giriş kapısı olarak kullanmaya devam edecek.

### 6. Saldırı Yazılımları Güçlenmeye Devam Ediyor

Her ne kadar kendimizi korumak önem kazansa da saldırganların kullandığı yazılım ve yöntemler de her geçen gün güçleniyor ve çeşitleniyor. Bu çeşitlilik karşısında gündemi takip etmek her zaman faydalı olacaktır.

### 7. "123456" Şifre Değil

Çoğu kullanıcı rahat hatırlamak ya da şifresini unutmamak için hackerlar tarafından kolayca kırılabilecek şifreler kullanıyor. Güçlü bir şifre oluşturmak çok önemli ama unutma sorununuz varsa şifre üreten cihaz ya da yazılımlar tercih edebilirsiniz.

### 8. Ülkeler Arası Siber Savaşlar

İlk kez geçtiğimiz yıllarda Rusya'nın, Estonya internet sistemini bir günlüğüne kilitlemesi ile yaşanan ülkeler arası siber savaşlar 2019'da da yine karşımıza çıkacakmış gibi görünüyor.

### 9. Bilgi Güvenliği Yöneticilerine Yine Çok İş Düşecek

Bilgi güvenliğindeki en zayıf halkanın insan olduğunu ilk maddede yazdık. İnsani faktörleri engelleyecek ve dışarıdan gelecek müdahalelere karşı bir savunma oluşturacak bilgi güvenliği yöneticileri ve onlara bağlı ekiplere yine çok iş düşecek. Bu ekiplerin şirketlerdeki önemi de artacak.


# Finans Sektörü Siber Saldırıların Hedefinde.

**2018 yılında yapılan siber saldırılar konusunda çeşitli araştırmalar yapan analiz şirketleri, özellikle finans sektörünün tehlikede olduğunu belirtiyorlar. Yayınlanan raporlarda bir veri sızıntısı yaşanması durumunda finans sektörünün diğer sektörlere göre yüzde 40 daha fazla bedel ödediğini ortaya koyuyor.**

Riskin yapısı değişiyor, inovasyon beraberinde güvenlik ve risk yönetimi için yeniden düşünmeyi getiriyor. Siber tehditlere yönelik planlama yerine risk bazlı planlamaya geçmeliyiz. Finans sektörü dijital dönüşümü son hızda yaşarken siber saldırılar ve savunma yöntemleri de bu gelişen dünya ile birlikte kendilerini bir üst seviyeye taşıyorlar. Geniş saldırı alanlarına sahip daha hassas saldırı teknolojileri ile ataklar daha organize hale geldi. 2018 yılında en çok karşılaştığımız bilgi güvenliği açığı veri güvenliği sızıntısı oldu. Artık art niyetli kişiler kurum sistemlerinde buldukları zafiyetleri istismar ettikten sonra sistemlere zarar vermeyi amaçlamak yerine; sistemlerin sahip olduğu işlem gücünü çalarak kullanmayı amaçlıyor.

Siber suçların küresel ekonomiye maliyeti 600 milyar dolar ve bu rakamın 2021 yılında 6 trilyon dolara çıkması öngörülüyor. Türkiye'ye baktığımızda ise Trend Micro 2018 siber saldırı raporununa göre Türkiye, Orta Doğu bölgesinde en fazla e-posta saldırısına maruz kalan ülke oldu ve ayrıca fidye yazılım saldırılarının hedefinde olan ülkelerden. Yine yakın zamanda ülkemizde de bazı bankalarda ya da kurumlarda kullanıcı bilgilerinin sızdırılması ya da yüksek para transferleri ile karşı karşıya kaldık. Bunun 2019 yılında da devam edeceğini ön görüyoruz. Biometrik bilgilerin hacklenmesi, oltalama ataklarında artış ve yapay zekanın daha ileri seviyede kullanılması 2019'da en çok görülmesi beklenen siber saldırılarılar arasında yer alırken kimlik bilgilerinin çalınması haberlerini de duymaya devam edeceğiz.

Tüm bu riskleri bertaraf etmek ve bankacılık işlemlerin doğru yapılabilmesi için düzenlemeler ve kanunlar hem bankaları hem de son kullanıcıları korumak adına yayınlanmakta aynı zamanda Türkiye Bankalar Birliği tarafından da denetlenmektedir.

Özellikle teknoloji açısından BDDK, SPK, KVKK gibi regülasyonların hepsini yakından takip ederek risk konusuna eğilmek büyük önem kazanıyor.

Bu da hem banka sektörü IT birimleri hem bankalara hizmet sağlayan teknoloji firmalarının çok daha dikkatli ve konusunda uzmanlaşmış bakış açısına sahip olma gereksinimini beraberinde getiriyor. Durum böyleyken riski yönetimini, insan faktörü ve sürdürülebilir hizmet yaklaşımlarını benimsemek gerekiyor.

# Etkinlik Haberleri

## Netaş IDC Roadshow 2019'da

İstanbul Whydnam Otel'de gerçekleştirilen IDC Roadshow 2019'da 1 workshop ve 1 panelde yerimizi aldık. "Sürdürülebilir Siber Güvenlik Ekosisteminin Geliştirilmesi" sunumumuzdan öne çıkan başlıklar: "Her gün gelişen ve değişen teknoloji ile birlikte siber güvenlik servislerinin sürdürülebilir olması günümüzün yeni zorluklarından. Hem bu zorluğun üstesinden gelmek hem de paydaşlarımızın güvenilir iş ortakları olabilmek için içerisinde orkestrasyon, siber istihbarat, makine öğreniminin de olduğu gelişmiş SOC hizmetimiz, ihtiyaca göre şekillendirdiğimiz yönetilen hizmetlerimiz ve kurumların regülasyonlara uyumluluğunu amaçlayan danışmanlık hizmetlerimiz ile bir adım önde olmayı hedefliyoruz. Bu yolda teknolojiye güveniyoruz, müşterilerimize inanıyoruz."


## Cisco ile birlikte teknoloji liderleri ile buluştuk

"Fonksiyonel Bir Araçtan Stratejik Bir Kaynağa Doğru" başlığı ile Les Ottomans Otel'de Cisco ile birlikte düzenlediğimiz etkinlikte Türkiye'nin önde gelen teknoloji liderleri ile SD-WAN ve SD-Access çözümlerinin sağladığı faydaları paylaştık. Bağlantı maliyetlerini düşürme, uygulama performansının hızını ve çevikliğini artırma, otomasyon ve yönetilen hizmetler ile hız kazanma gibi konuların derinlemesine incelendiği toplantıda IDC Türkiye'de dijital dönüşümün hızla değişen iş gereksinimlerini paylaştı.

## Güvenli Gelecek Çok Önemli

İnsanlık tarihi teknolojiyle birlikte en büyük dönüşümlerden birini yaşıyor. Bu noktada güvenlik konusu da en öne çıkan başlıklardan bir tanesi. Siber güvenlik konusunda ülkeler arasındaki siber savaşları ele aldığımızda konunun ciddiyeti bir kez daha ortaya çıkıyor. A Para'da yayınlanan Teknoloji Çağı programına konuk olan Netaş Siber Güvenlik Hizmetleri Direktörü Fatma Hacıoğlu Doğar, siber güvenlik hakkındaki görüşlerini paylaştı. Yayının tamamını **buradan** izleyebilirsiniz.

# Siber Güvenlik Sigortası Hakkında Bilinmesi Gerekenler

**KVKK, GDPR kapsamındaki kişisel veri sızıntıları ile veri kayıplarından doğabilecek itibar kaybına, iş kaybına ve maddi zarara uğramamak için Netaş güvencesiyle Siber Güvenlik Sigortası yaptırmak artık mümkün.**

Siber Güvenlik Sigortası ile herhangi bir siber saldırı ile karşılaştığınızda Netaş olarak; aksiyon planları oluşturuyor, saldırıdan en az şekilde etkilenmeniz için poliçemizdeki koşullar ve istisnalar çerçevesinde şirketinizi teminat altına alıyoruz.

Bir güvenlik ihlali yaşamadan önce hazırlıklı olmanız adına, güvenlik açısından hangi noktada olduğunuzu, bir siber saldırı durumunda olası risk durumunuzu görmeniz için Güvenlik Analizi ve Değerlendirme çalışmaları yapıyor, sizinle bir rapor halinde paylaşıyoruz.

Çıkan sonuçlara göre alınması gereken önlemleri ve eylem planı için çözüm önerilerini sunuyoruz.

**Siber Güvenlik Sigortanızı yapıyoruz.**

Siber Güvenlik Sigortası kapsamında siber saldırıya uğradığınızda, eksperlerimiz gelip olay yerinde inceleme ve adli bilişim, durum kayıp çalışması gerçekleştiriyor ve zararınızı karşılıyoruz.

Günümüzde gelişen riskler ve saldırı tekniklerine karşı, bütünsel güvenlik bakış açısı ile doğru çözüm ve hizmetler almak önemli.

**Bu kapsamda Netaş olarak;**

- Alınan önlemlerin seviyesini ölçmek, bir siber saldırı sırasında mevcut durumu görmek ve güvenlik önlemlerinin
- sürekliliğini sağlamak adına sızma testleri
- Kırmızı Takım aktiviteleri
- Kurum çalışanlarına yönelik sosyal mühendislik saldırı testleri
- Sistemlerde güvenlik sıkılaştırma

7x24 güvenlik olaylarını izleme ve müdahale hizmetleri ile 360 derece bir güvenlik hizmeti sunuyoruz.