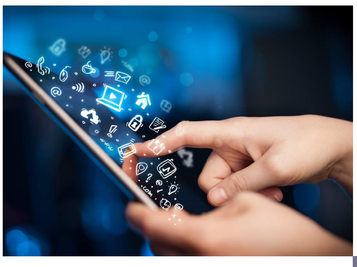
2019 Veri Sızıntılarının Yılı Oldu, 2020 farklı mı?

Geride bıraktığımız 2019 yılında birçok kurum ve kuruluş veri sızıntısına uğrayarak müşterilerinin çok değerli verilerini kaybetme sorunu ile karşı karşıya kaldı. 2020'de hepimizin evde ve daha çok veri kullanıp ürettiğini düşünürsek, bu yıl da pek farklı olmayacak.

Siber güvenlik dünyasında 2019 çok hatırlanacak yıllardan bir tanesi olarak tarihteki yerini aldı. Siber saldırganlar; saldırı düzenledikleri, bankadan otele, sağlık kurumundan kamu kuruluşuna kadar birçok kurumu ve bu kurumun kullanıcılarını milyarlarca liralık zarara uğrattı. Biz de 2019 yılının kara bir yıl olarak hatırlanmasına neden olan bu saldırıların bir kısmını sizler için derledik ve 2020'ye bir pencere açtık.

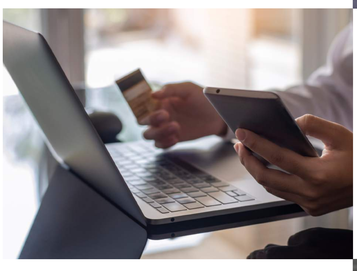


Sosyal medyaya dikkat

2019 yılındaki sızıntılar, ihlaller ve riskler listesinde birkaç teknik çalışan olayı da ön plana çıktı. Yaklaşık 100 uygulama geliştiricisine ve profil verilerine uygunsuz erişim sağlandığı belirlenen Facebook ise yeniden manşetleri süsledi. Özellikle Kasım ayındaki çılgın alışveriş döneminde kullanılan birçok kredi kartı bilgisinin ifşa edilerek satışa çıkarıldığı söylendi ancak online alışveriş siteleri tarafından konuya ilişkin resmi bir açıklama yapılmadı.

Veri sızıntısına dokunulmazlık yok

2019 için son olarak Hollanda'da yaşanan bir iCloud sızıntısını da sizlerle paylaşalım. Yıl sonunda Apple'ın bulut sistemi iCloud hesaplarıyla ilgili bir sorun fark edildi. Hollandalı savcılar, 100'den fazla kadının kişisel iCloud hesaplarını ihlal eden, özel fotoğraflar ve videoları sızdırdığı iddia edilen yerel bir politikacı için üç yıl hapis cezası istedi.

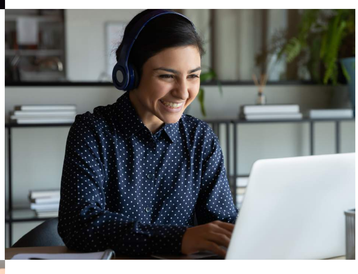


2020 iyi başlamadı

Ocak 2020'de bir dijital cüzdan uygulaması üzerinden 14 milyon kullanıcının tüm kredi kartı bilgileri (CVV numaraları dahil), e-posta adresleri, doğum tarihleri, adresleri, üyelik kimlik numaraları, perakende kulüp ve sadakat kartı üyelikleri, devlet kimlikleri, hediye kartları, sağlık sigortası kartları, tıbbi bilgileri ve IP adresleri sızdırıldı.
Bu olayla birlikte 44 milyon fazla fotoğraf da kötü niyetli kişilerin eline geçti.

Popüler görüntülü konferans uygulamasına darbe

500.000'den fazla kullanıcı hesabının kimlik bilgileri dark web ve hacker forumlarında 0,02 $ civarında fiyatlarla satıldığı ortaya çıktı.

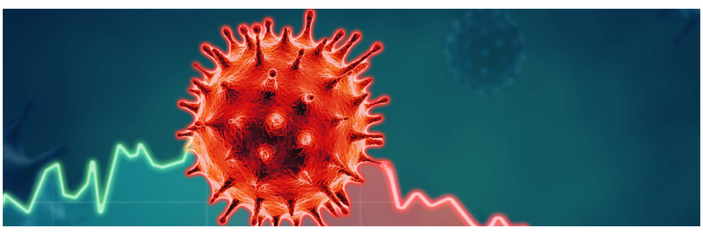


Güvenli bir otel yok mu?

2 tane otel çalışanının hesap bilgilerinin 3. parti otel misafir hizmetleri uygulaması kanalı ile kullanılması ile ortaya çıkan büyük sızıntıda dünya çapında 5,2 milyon konuğun ; kişisel bilgileri, isimleri, posta adreslerini, e-posta adreslerini, telefon numaralarını, sadakat hesap numaralarını ve puan bakiyelerini, şirketi, cinsiyetleri, doğum tarihlerini, bağlantılı havayolu sadakat programları ve numaraları, oda tercihleri ve dil tercihleri ifşa oldu.

Avrupa GDPR konusunda çok hassas

Avrupa Birliği yasaları, ülkemizde Kişisel Verileri Koruma Kanunu-KVKK olarak bilinen GDPR konusunda çok hassas davranıyor ve ilgili kurumlara ceza yağdırmaktan bir adım bile geri adım atmıyor. Bunun son örneklerinden bir tanesi de 2019 yılının Temmuz ayında Yunanistan'da yaşandı. İşin en ilginç yanı ise 150 bin avro cezaya çarptırılan kurumun Yunan Veri Koruma Kurumu (Helenic DPA) olmasıydı. PricewaterhouseCoopers tarafından yapılan denetimde ortaya çıkan sorun Helenic DPA'nın başını oldukça ağrıttı diyebiliriz.



Pandemi dönemi nasıl olacak?

Maalesef global bir pandemi dönemindeyiz. Bu yüzden pek çoğumuz evlerimizden çalışıyoruz. Hiç olmadığı kadar çok veri üretiyor ve kullanıyoruz. Ayrıca evlerimizde iş yerlerimizdeki gibi güvenlik önlemlerini uygulamamız pratik olarak zorlaşıyor. Bu yüzden de 2020 yılında şu ana kadar ki en büyük veri sızıntıların yaşanacağı ve global ölçekte yüz milyarca dolar zarar oluşturacağı ön görülüyor. Üzücü olan bir başka konu ise bu dönemde özellikle hastanelerin hedef alınmış olması. Amerika'daki hastanelere yapılan saldırılar geçen seneye göre iki katından fazla artmış durumda. Şimdiden 2.5 Milyon kişinin verisi 105 saldırıda ele geçirildi. Bu saldırılar büyük oranda Ryuk Ransomware ile yapıldı. Ülkemizde de evden çalışanların ve özellikle sağlık personelinin veri sızıntılarına karşı her zamankinden daha dikkatli olması gerekiyor.

2020’de Mobil ve Akıllı Cihazlara Dikkat

Dünya 2020’de 6 trilyon dolarlık siber saldırı riskine hazırlanıyor. En büyük risk grubunda ise akıllı mobil ve IoT’li cihazlar yer alıyor.

Yapılan araştırmalara göre geçtiğimiz yıl dünya genelinde yaklaşık 700 milyon kişi siber saldırıların kurbanı oldu. Bu saldırılardan siber korsanlar 1,5 trilyon dolar gelir elde ederken önümüzdeki yıl siber saldırılar sonucu açığa çıkacak zararın dünya genelinde 6 trilyon dolara ulaşması bekleniyor.

En büyük tehdit akıllı ve IoT tabanlı cihazlara

Çeşitli araştırma sonuçlarına göre dünyada halihazırda 17 milyar civarında akıllı cihaz bulunuyor. Akıllı cep telefonlarının da dahil olduğu bu grupta telefonlarla beraber en çok tehdit ise IoT destekli cihazlarda yaşanıyor. Kapı zili, buzdolabı, aydınlatma, ısıtma, araba ve güvenlik sistemleri gibi birçok yerde hayatımıza temas eden IoT (Nesnelerin İnterneti) tabanlı akıllı cihazlar siber saldırılar sonucu kamu kurum ve kuruluşlarının yanı sıra bireysel olarak da en çok zarar görülebilecek cihazlar olarak karşımıza çıkıyor. Geçtiğimiz yıl şirketlerin yüzde 61’i IoT sistemlerinin hacklenmesi nedeniyle mağdur oldu.

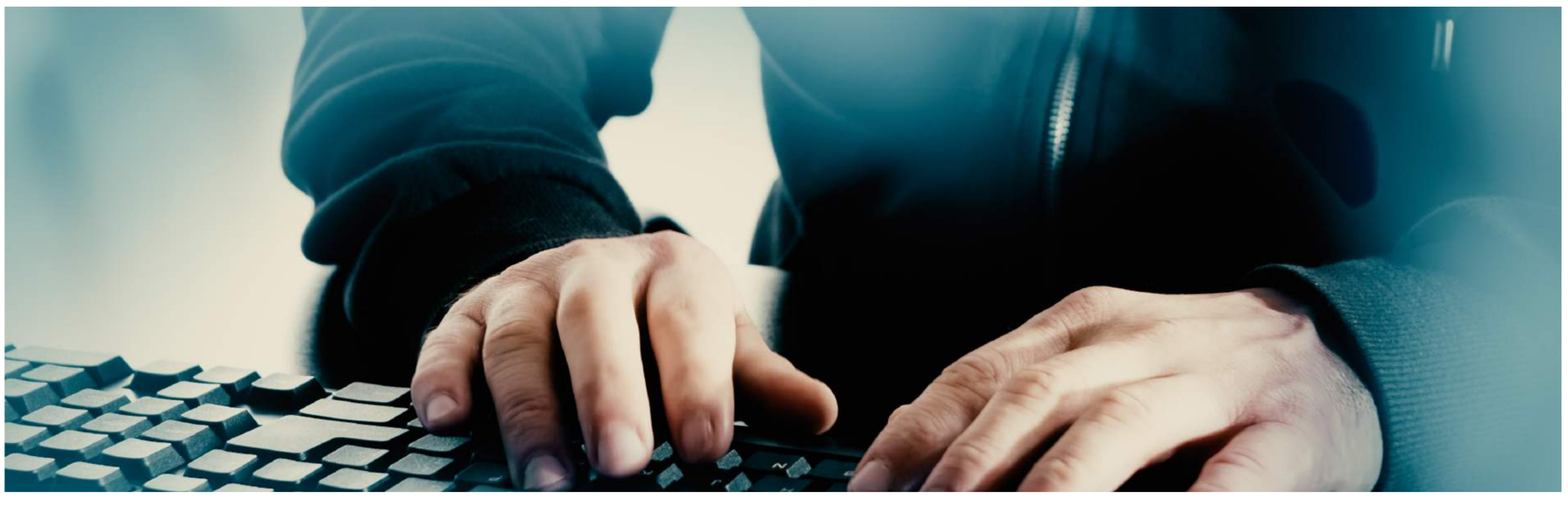
Peki neler yapmalı?

Öncelikle ülkemiz, bireysel bilgisayarlardaki kötü amaçlı yazılım kullanımında Çin ve Tayvan’ın ardından üçüncü sırada yer alıyor. Türkiye’de bilgisayarların yüzde 42’sinde kötü amaçlı yazılım ve uygulamalar bulunurken dünya genelinde tam 23,2 milyon kişi şifre olarak “123456” kombinasyonunu kullandığı için çeşitli şekillerde mağdur oldu. Yine dünya genelinde dolandırıcılık için ayda 400 bin sahte web sitesi açıldığını da düşünecek olursak bir dizi önlem almanın zamanının çoktan geldiğini göreceğiz.

Öncelikle siber saldırıların sadece yüzde 3’ü teknik bir açık kullanılarak gerçekleştiriliyor. Geri kalan bilgiler sosyal medya veya benzer kanallar üzerinden yapılan sosyal mühendislikle ele geçirilen bilgiler aracılığıyla gerçekleştiriliyor. Bu da demek oluyor ki öncelikle güçlü şifreler belirleyeceğiz ve sonrasında sosyal medyada paylaştıklarımıza dikkat edeceğiz.

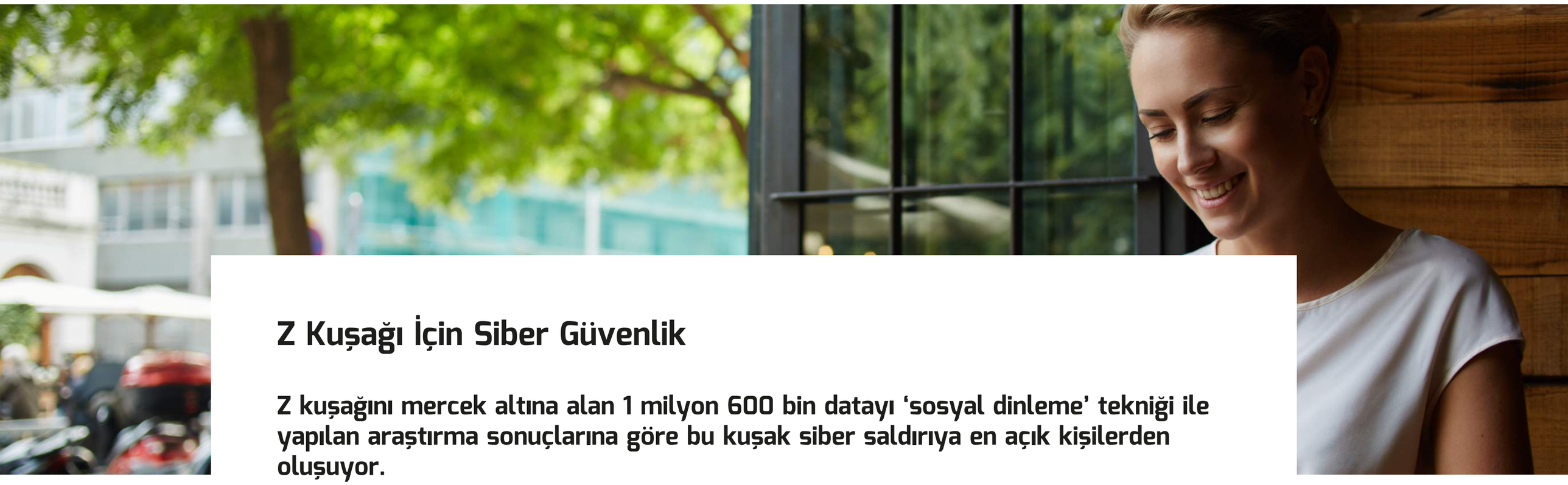
Yedeksiz şirket olmaz

Şirketler ne kadar küçük veya büyük olursa olsun, depoladığı veriler çok önemli. Bir siber saldırı, yıkıcı sonuçlara yol açarak verilerin kaybedilmesine neden olabiliyor. Geçmiş verileri yedeklemek ve gelecekteki otomatik yedeklemeleri planlamak gerekiyor.



Güvenli bir iş ortağı seçin

Siber güvenlikte en önemli nokta güvenli bir iş ortağı seçiminden geçer. Kaldı ki araştırmalar, KOBİ’lerin yarısının siber saldırılara maruz kaldığını gösteriyor. Sizi ve verilerinizi koruması için Netaş gibi sistem entegratörlüğünde lider, ArGe’sinden güç alan, bütünleşik bakış açısıyla uçtan uca anahtar teslim entegre siber güvenlik hizmeti sağlayan bir iş ortağı ile çalışmak geceleri yastığa başınızı rahat koymanızı sağlayacaktır.



Z Kuşağı İçin Siber Güvenlik

Z kuşağını mercek altına alan 1 milyon 600 bin datayı ‘sosyal dinleme’ tekniği ile yapılan araştırma sonuçlarına göre bu kuşak siber saldırıya en açık kişilerden oluşuyor.

Z kuşağı. Kimimize göre çocuk, kimimize göre iş yerimizde bizimle yeni çalışmaya başlamış “gençler”. Zillenials, Gamers, Kuşak I, İnternet Kuşağı, Next Generation, iGen, Instant Online gibi pek çok farklı isimle anılan Z kuşağının hangi yıl başladığıyla ilgili tüm dünyada farklı görüşler mevcut.

2000 yılını başlangıç kabul eden uzmanların yanı sıra, teknolojinin hayatımıza yoğun bir şekilde nüfuz etmeye başladığı 90’lı yılların ikinci yarısıyla Z kuşağının doğduğunu savunanların sayısı da oldukça fazla. Bu kuşağın iş yaşamından en önde gelen beklentileri; şeffaflık, fırsat eşitliği, kendini özgürce ifade edebilme, katılımcı olma ve hiyerarşiden uzak bir ortam şeklinde tanımlanıyor.

Ancak Teknosa tarafından yapılan araştırmaya göre çoğunun ortak bir özelliği siber saldırılara en açık kişiler olmaları. Aynı araştırmaya göre yetişkinler, dijital dünyada aktif olan Z kuşağına dair endişe ve kaygılarını da sıklıkla paylaşıyor. Dijital ortamda “çocukların kullanılması” olarak tabir edilen yabancılar ile kontrol dışı iletişim, yüzde 77 oranıyla en fazla paylaşım alan konu olarak göze çarpıyor. Siber zorbalık olarak adlandırılan, dijital ortamda psikolojik etkileme durumu ise ebeveynler arasında yüzde 13 ile yine en çok konuşulan konular arasında. Bağımlılık tehlikesi ise genel kanının aksine yüzde 10 oranla son sıralarda yer alıyor.

E-ticareti Z Kuşağı “uçuracak”

Öte yandan e-ticaret başta olmak üzere birçok sektörün büyümek için hedefinde Z kuşağı yer alıyor. Bu beklenti öylesine büyük ki e-ticaret şirketleri Z kuşağının gelecek 10 yılda kendilerine 15 milyon yeni müşteri kazandırmasını bekliyor. Ancak 15 milyon yeni kullanıcı demek daha güçlü ve güvenli bir altyapı anlamına da geliyor. Bu yüzden e-ticaret şirketleri tüm süreçlerini daha güvenli hale getirmek için yoğun bir çaba harcamak durumunda kalacak zira Z kuşağının marka bağımlılığı da çok düşük seviyede.

Z Kuşağı kripto paraya güveniyor

Z Kuşağı kripto para kavramıyla da erken tanışan bir nesil. Bizler henüz kripto para nedir diye anlamaya çalışırken bu nesil birçok işlemini daha güvenli ve kolay bulduğu kripto paralara kaydırmaya başladı bile. Ancak kripto para dünyası ne kadar güvenli işte o sorunun cevabı kocama bir soru işareti.

KPMG’nin gerçekleştirdiği son araştırma, ABD’de yaşayan 18-24 yaş arası gençlerin yüzde 83’ünün kripto paraların geleceğiyle yakından ilgilendiğini ortaya koydu. Araştırmaya göre ABD’lilerin yüzde 82’si kripto paraları, banka, restoran gibi yerlerin ‘müşteri sadakat programlarında’ kullanmaya istekli olduklarını belirtiyor. Buradan çıkan sonuç o ki 2020 yılında daha güvenli kripto para kullanımı sunan işletmeler rekabette de bir adım öne geçmeyi başaracak.

Genlerinde teknoloji var

Ancak bilinen bir gerçek var ki teknoloji bu kuşağın genlerine kazınmış durumda. Teknoloji ile bu denli iç içe geçmiş bir kuşağın iyi niyetlileri harika birer siber güvenlik uzmanı olacak. Peki kötü niyetliler? Onların da birer hacker olacağını düşünmek yanlış olmayacaktır. İsmi Z kuşağı da olsa Zillenials da olsa teknoloji hayatımızın içinde olduğu sürece iyi ve kötünün savaşı daha uzun süre devam edeceğe benziyor.

Zafiyet Yönetimi Çözüm ve Hizmetlerimiz

Şirketinizde bulunan bütün bilişim ile ilgili sistemler (sunucular, bilgisayarlar, modemler, yazıcılar, vs.) potansiyel bir zafiyet ve açık oluşturur. Hatta çalışanlarınız bile şirketiniz için bir zafiyet sayılabilir. Bunun önüne geçmek için Netaş sizler için ipuçları hazırladı.

Bir saldırgan şirketinizde bulunan zafiyetleri kullanabilir ve sitemlerinize ulaşarak sizin için çok değerli sayılacak bilgilerinizi çalabilir, şifreleyebilir, sisteminizi kilitleyebilir ve kullanılamaz hale getirebilir. Sisteminize erişebilmiş bir kişi için bu işlemleri gerçekleştirmek hiç zor olmayacaktır.

- Aktif işletim sistemi kullanan bütün cihazlar aslında potansiyel olarak bir açık yani zafiyet içerirler. Bu cihazlara örnek verecek olursak;
- Taşınabilir ve Masaüstü Bilgisayarlar
- Serverlar (Sunucular)
- Veri Depolama Cihazları
  (Harici Diskler, USB depolama aygıtları ve Hafıza Kartları)
- Tablet ve Akıllı Cihazlar(Telefonlar)
- Linux işletim sistemi bulunduran cihazlar
- Kablosuz erişim cihazları
- ADSL Modemler
- Network ağ cihazları
- Ağ güvenlik kameraları
- Ağ yazıcıları
  olarak sıralanabilir.

Bu sebeple Netaş Siber Güvenlik Çözümleri bünyesinde hayata geçirilen zafiyet yönetimi sistemiyle, zafiyete sahip tüm sistemlerin taraması, analizi ve iyileştirmesi süreçleri hizmet haline getirilmiş durumda. Ayrıca Netaş müşterilerinin sahip olduğu zafiyet tarama sistemlerinin Netaş tarafından geliştirilen Sweep uygulaması üzerinden kontrolü de mümkün. Bu sayede Sweep üzerinden tüm tarama sonuçları kontrol edilebilir, ilgili zafiyetler envanter ya da servis sahibine atanabilir. İlgili zafiyetlerin, zafiyet sahipleri tarafından kapatılmasının ardından, Sweep doğrulama taraması yaparak bu zafiyetin tamamen giderildiğinden emin olur ve tüm bu süreçleri kurum için otomatikleştirir.

Netaş Kırmızı Takım'ı tarafından genel zafiyet taramaları anlık olarak kontrol edilerek gelişmiş servis raporları periyodik sürelerde Netaş müşterileriyle paylaşılır.

Siber Güvenliğe Bütünsel Yaklaşım

2022'ye gelindiğinde,
"anonimlik" sadece "dark web'e " özgü olacak; ticari veya sosyal faaliyetler yürütenlerin **tamamı** ya takma adlı (yani isimlerin koruma altında olup ancak mahkeme kararıyla açıklanabilmesi) ya da tanımlı olacak.

IDC'nin Netaş'ın desteğiyle hazırladığı **Siber Güvenliğe Bütünsel Yaklaşım Raporu** bilgi ve iletişim sektörüne ışık tutuyor. Rapora göre Dijital dönüşüm (DX) dalgası kurumların, siber güvenlikle baş etme biçimleri de dahil olmak üzere çalışma yöntemlerini değiştirmeye zorluyor.
Dijital dönüşüm (DX) dalgası kurumların, siber güvenlikle baş etme biçimleri de dahil olmak üzere çalışma yöntemlerini değiştirmeye zorluyor. BT altyapısının giderek artan karmaşıklığı, cihazların yaygınlaşması, Kişisel Verileri Koruma Kanunu (KVKK) gibi yeni yönetmeliklerin yürürlüğe girmesi ve hızla değişen tüketici talepleri de kurumların işleyiş biçimlerini değiştiren diğer unsurlar arasında. Ayrıca, Nesnelerin İnterneti (IoT) ve Yapay Zeka (AI) gibi yeniliği hızlandıran etkenlerin yanı sıra Büyük Veri Analitiği, bulut bilişim, sosyal iş ve mobilite gibi 3. Platform teknolojileri de tehditlerin kapsamını genişleterek kurumları yeni zorluklarla baş başa bırakıyor.

BT güvenliği Türkiye'deki üst düzey yöneticilerin en önemli sorunu olarak öne çıkıyor. Ancak, son zamanlardaki yüksek maliyetli ve yüksek profilli saldırılara rağmen, ülkedeki üst seviye yöneticiler ve şirket direktörleri genellikle BT güvenliğine pek dikkat etmiyor ve birçoğu siber güvenlik konusunda sorumluluğu tamamen BT departmanlarına yüklerken bunu yapınca da güvenliğin artık bir endişe konusu olmaktan çıktığına inanıyor. CIO ve CISO'ların önündeki en önemli sorun da işte bu aşırı güven tuzağıdır.

2021'e gelindiğinde,

yasal güvenlik alarmlarının **%50'si** analistlerin müdahalesi olmadan otomatik olarak cevaplanabilecek.

2024'e kadar,

DevSecOps o derece otomatikleşmiş olacak ki yeni uygulamaların **%60**'ında sürekli teslimat veri hattında yer alan kapsamlı güvenlik ve uyumluluk değerlendirmeleri yapılıyor olacak.

Güçlü bir "Olaylara Müdahale Planı" Yapın

Kurumlar olaylara müdahale planlarında bir yaşam döngüsü yönetimi yaklaşımına yer vermeli ve gerektiğinde modası geçmiş prosedürleri iptal etmelidir. Tehdidin izlenmesi, sınırlandırılması, düzeltilmesi ve adli bilişim kuruluşların kendi olay ve müdahale stratejilerine dahil ederek düzenli olarak güncellemesi gereken alanlardır.

Siber Güvenlik Stratejilerinizi DX Platformu Genelinde Uygulayın

İşletmeler alışılmış güvenlik stratejilerini kuruluşun DX ihtiyaçlarını karşılayacak şekilde genişletmelidir. Kurumlar riski yönetmek ve operasyonlarını korumak için ayrıca DX girişimleri paralelinde yeni siber güvenlik stratejileri de belirlemelidir.

Proaktif bir Güvenlik Yaklaşımı Benimseyin

Tehditlerin değişken niteliğinin üzerine gidebilmek için güvenlik kontrolleri yapılmalıdır. Hızlı değişim gösteren tehditlerin üstesinden gelebilmek için, kuruluşlar alışılmış, reaktif güvenlik modellerinden daha proaktif yaklaşımlara geçiş yapmalıdır.

Güvenlik Uzmanlarınızı Sürekli Olarak Eğitin

Siber güvenlik alanı geliştikçe bilgi güvenliği uzmanları da kendi bilgi ve becerilerini sürekli güncelleyebilmelidir. Bu nedenle siber güvenlik uzmanlarının yeni mimarilerden, güvenlik yaklaşımlarından ve AI, makine öğrenimi ve otomasyon gibi teknolojilerden haberdar olmasını sağlayan esaslı geliştirme programları hayata geçirilmelidir.

Tehdit Avcılığı Becerilerinizi Geliştirin

Kuruluşlar, sistemlerinin tehlike altında olup olmadığını anlamak için organize ve sistematik bir tehdit avcılığı metodu uygulamalıdır. Örneğin, analitik teknolojileri kullanılarak şüpheli faaliyet işaretleri takip edilebilir ve tehdit avcılığı süreçleri kapsamında araştırmalar yapılabilir.

Yönetilen Güvenlik Hizmeti AR&GE Yol Haritanızı Değerlendirin

İleriye dönük yönetilen güvenlik hizmeti sağlayıcıları gelişmiş tespit teknikleri, tehdit istihbaratı, AI, ML, ve Büyük Veri Analitiği gibi şeyleri içeren hizmetler sunmalıdır; ayrıca bulut evrimini ve olaylara müdahaleyi de hizmete dahil etmelidir.

(IDC FutureScape: Dünyadaki Güvenlik Ürünleri ve Hizmetleri 2019 Tahminleri)

IDC
ANALYZE THE FUTURE

Bizden Haberler

Netaş, BTK tarafından üçüncü kez düzenlenen 3.Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi'ne katıldı.

3.Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi'nde "Kamuda Siber Güvenlik Stratejileri" paneline katılan Netaş Danışmanlık ve Yönetilen Hizmetler Direktörü Baran Korukluoğlu: "Siber güvenlikte insan, teknoloji ve süreç üçgenini göz önünde tutuyor, Ar-Ge'deki gücümüzle sunduğumuz uçtan uca entegre siber güvenlik hizmeti altında uzman insan kaynağımızla konuya odaklanıyoruz. Mevcut ihtiyaçlara en doğru çözümleri sunarak bütünsel güvenlik, bütçe fayda dengesi, proaktif koruma ve güvenlik sürekliliğini sağlıyoruz" dedi.

Netaş, yeni yapısıyla yüzde 20 büyüdü

Enerji, havayolu, perakende ve finans başta olmak üzere sektörlerinin öncü şirketlerine sunduğu SOC ve NOC hizmetleriyle Türkiye'nin en büyük oyuncularından olan Netaş, her geçen gün daha kritik hale gelen siber güvenlik alanına odaklandı. Siber güvenlik ile ilgili tüm ürün ve kanalları Yönetilen Hizmetler çatısı altında tek elde toplayarak güçlü kaslarının çevikliğini daha da artıran Netaş son 4 ayda hizmet verdiği şirket sayısını yüzde 20 artırdı.

Sistem entegratörlüğündeki liderliği ve ArGe gücüyle uçtan uca entegre siber güvenlik hizmeti sunarak farklılaşan Netaş, yetkin insan kaynağıyla sağladığı Kırmızı Takım ve hem global hem yerli farklı birçok kaynaktan beslenen Siber İstihbarat Hizmetleriyle ön plana çıkıyor.

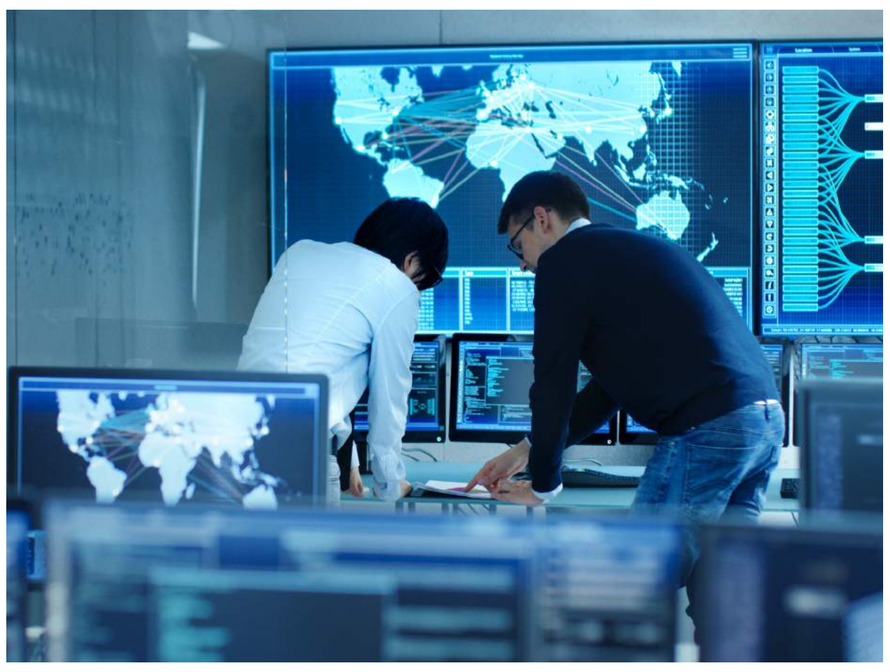
Siber istihbarat ve Kırmızı Takım

Netaş, yetkin insan kaynağıyla oluşturduğu Siber İstihbarat ve Kırmızı Takım ile şirketlere özel siber güvenlik hizmeti sunuyor. Hem global hem yerli birçok kaynaktan beslenen Netaş Siber İstihbarat Servisi, kurum ve kuruluşlara karşı bir atak kampanyası olup olmadığını analiz ediyor. SOC ise sözkonusu analizlerden şirkete özel risk haritası çıkarıp, aksiyon planı belirliyor. Kırmızı Takım bakış açısıyla ise Netaş, şirketlerin sistemleri olası atak senaryolara göre dışardan test ediyor.

Siber güvenlikte yerli ArGe çözümleri

Netaş, VoIP alanında NOVA markasıyla kendi ArGe'sinde geliştirdiği iletişim güvenliği alanındaki yeni nesil ürünleri ile de çözümler sunuyor. Geliştirdiği yerli çözümlerle sadece ülkemizde değil, bölgemizde de lider olmayı hedefleyen Netaş NOVA kapsamında sunduğu V-Spy çözümü ile VoIP'e özel sızma testleri otomatik olarak uygulanarak sistemin zafiyetleri tespit ediliyor. Tamamlayıcı bir sistemin parçası olan NOVA V-Gate ise VoIP sistemleri için bir güvenlik duvarı (firewall) niteliğinde. VoIP'e özel atak tespitlerini yaparak otomatik olarak bu saldırıları önleyebiliyor.

NOVA FMS ise büyük veri analitiği kullanarak, VoIP çağrı trafiğini makine öğrenmesi ile modelleyerek anlık verileri model ile karşılaştırıp, işletim sırasındaki anomali durumlarını NOVA V-Gate güvenlik duvarına alarm olarak iletiyor. NOVA S/COM ise güvenli çok kişili görüntülü veya sesli iletişim, dosya paylaşımı, ekran paylaşımını mümkün kılıyor.



Siber Güvenliğe Bütünsel Yaklaşım Raporu IDC Cyber Security Roadshow'da açıklandı

Siber Güvenlik ekosisteminin en önemli buluşmalarından biri olan IDC Cyber Security Roadshow Netaş'ın Platinum Sponsorluğunda 4 Mart'ta Wyndham gerçekleşti. Siber güvenliğe bütünsel yaklaşım ve yönetilen servislerin geleceğinin konuşulduğu zirvede IDC'nin hazırladığı Siber Güvenliğe Bütünsel Yaklaşım: Teknoloji, İnsan ve Süreç başlıklı rapor da Netaş'ın desteğiyle ilk kez açıklandı.
IDC Security Roadshow'da Yönetilen Hizmetlerde Yeni Dönem konusu altında konuşan Netaş Yönetilen Hizmetler Direktörü Baran Korukoğlu, "Şirketler, hızla gelişen yeni nesil teknolojilerin paralelinde güvenlik alanındaki teknoloji yatırımlarını sürekli güncellemeliler. Ancak bu maliyetler odak noktası farklı olan şirketler için sürdürülebilir değil. Öyle ki, siber güvenliğin yatırım gerektiren 17 öncelikli alanın yüzde 60'ında maliyet artışı yüzde 25'e ulaştı. Bu noktada siber güvenlikte iş ortaklığı önem kazanıyor. Netaş olarak; müşterilerimiz yerine yapay zeka, otomasyon ve insan kaynağına yatırımı biz yapıyoruz. Bunu da en uygun şekilde ve daha prokatif siber güvenlik operasyonu olarak şirketlere sunuyoruz" dedi.

IDC Security Roadshow 2020'de Siber Güvenliğe Bütünsel Yaklaşım: Teknoloji, insan ve süreç konusunda ise Netaş Yönetilen Hizmet ve Siber Güvenlik Hizmetleri Çözüm Direktörü İsmail Kar ve Sahibinden.com Bilgi Güvenliği Direktörü Erkan Sertoğlu birlikte konuştu. Netaş Yönetilen Hizmet ve Siber Güvenlik Hizmetleri Çözüm Direktörü İsmail Kar, "Netaş olarak bütünsel bir yaklaşımla siber güvenlik hizmeti sunuyoruz. Yetkin insan kaynağıyla Türkiye'nin en büyük Siber Güvenlik Operasyon Merkezlerinden birine sahibiz. Siber güvenlik alanında dünyanın önde gelen şirketlerinin ürün ve çözümlerini sunuyoruz. Tüm bu yetkinliklerimizi ArGe'miz ile pekiştiriyoruz. Enerji, finans, havacılık gibi stratejik sektörlerden 25 öncü markaya ihtiyaçlarına uygun modellerle uçtan uca hizmet sağlıyoruz. Yeni nesil teknoloji eğitim merkezi olarak açtığımız n-telligent institute'da da siber güvenlik alanında sektörün ihtiyacı olan insan kaynağını yetiştiriyoruz" dedi.