Deloitte.

Siber Güvenlik

Hazırlan. Farkında ol. Müdahale et.

Kurumsal Risk Hizmetleri

Siber Güvenlik
Hazırlan. Farkında ol. Müdahale et.

Bu savaş...

Organizasyonunuz siber saldırıları yönetmekte ne kadar başarılı? Saldırılara en açık dijital varlıklarınız neler ve bunlar organizasyonunuz için ne kadar değerli? Kurumunuzun karşı karşıya olduğu siber tehditler konusunda bir plana ve bu planı harekete geçirecek yetkinliğe sahip misiniz?

Siber suçlar artık devlet destekli casusluk veya yalnızlığı seven bir bilgisayar korsanının yaptıkları ile sınırlı değil. Bugün iyi organize olmuş siber suçlular karmaşık saldırılar yoluyla suç işlemekte ve çoğunlukla önemli finansal kazançlar elde etmektedirler. Son dönemde yaşanan olaylar finansal etkinin yanı sıra siber ortamın kurumlara/yapılan işe ciddi etkileri olabileceğini göstermiştir. Bu etkiler hisse senedi fiyatlarının düşmesi ve hissedar değerinin gerilemesinden, rekabet avantajının yitirilmesi, tüketici ve kamuoyu güveninin azalmasına kadar uzanmaktadır. İşiniz ne olursa olsun siber saldırılara karşı korunmak artık ekonomik ve stratejik bir zorunluluk haline gelmiştir.

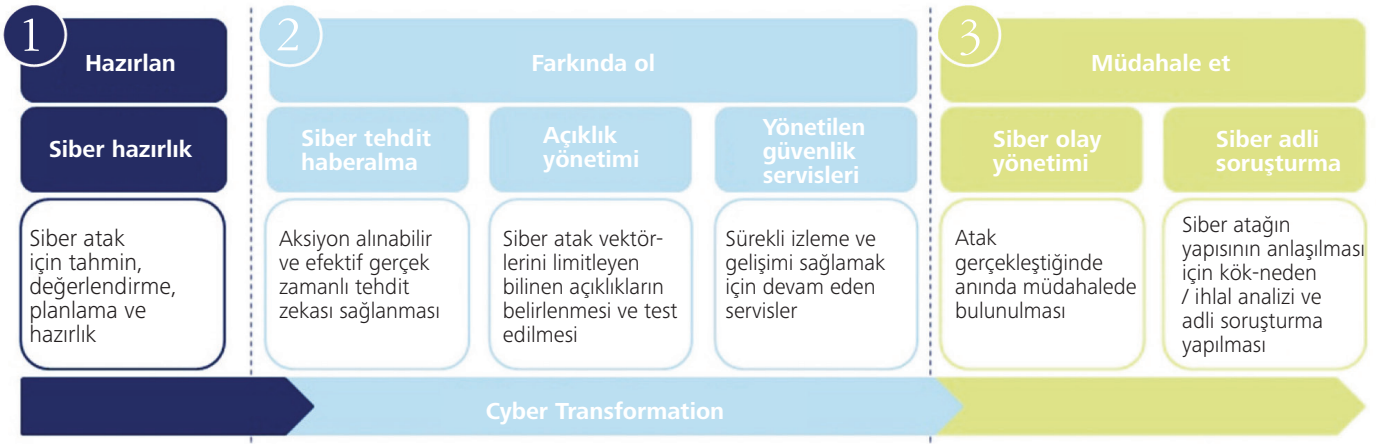
Çözüm nedir?

Farklı tehditler farklı müdahaleler gerektirmektedir. Sadece güvenlik kontrollerine odaklanan geleneksel savunma mekanizmaları, tehditleri tam olarak tespit edemeyip, karşılaşılan problemi de yönetemeyecektir. Hangi sektörde olursa olsun kurumların yaygın ve karmaşık sorunlarını çözümlemesinde odaklanılacak üç temel alan bulunmaktadır:

Hazırlan: Hedefli siber saldırılara karşı kurumun korunması ve atağın gerçekleşmesi durumunda meydana gelecek etkinin anlaşılması için hazırlık yapılmasını sağlayacak kaynakların tahsis edilmesi.

Farkında ol: Siber saldırıların hedeflerini ve mekanizmalarını tanımlamak ve tahminlemek için sektörünüze ve kurumunuza özel, gelişen tehdit alanlarını kapsayan bir haberalma mekanizmasının oluşturulması.

Müdahale et: Haberalma sadece üzerinde aksiyon alabiliyorsan faydalıdır. Kurumlar tehdit zekasına ve saldırılara cevap verebilmek için hem organizasyonel hem de teknik seviyede hazırlıklı olmalıdırlar. Bu şekilde başarılı saldırılara karşı daha iyi savunma sağlanabildiği gibi atağın başarılı olması durumunda etkinin azaltılması da mümkün olabilir.



1. Hazırlan
Plan ve test

Siber tehdide karşı hazırlıklı olmak, kurumunuzun saldırılara etkin bir şekilde yanıt vermesini sağlayan en önemli araçlardan birisidir. Hazırlıklı olmak, işinizde karşılaştığınız zorlukların aşılmasında ve yaptığınız işin değerinin korunmasında destekleyici bir yöntemdir. Etkili hazırlık ve planlama üç ana konuyu kapsamalıdır:

- Tanımlı roller, sorumluluklar ve karar verme prosedürleri
- Müdahale etmek için yetki devirlerinin gerçekleştirilmesi ve iş liderlerine eskalasyon süreçlerinin açık bir şekilde tanımlanması
- Masa başı testler ve simülasyonlar yoluyla deneyim kazanmış kadrolar ve etkinliği kanıtlanmış planlar

Siber konuların iş birimleri tarafından ele alınması ve müdahale için eskalasyon süreçlerinin oluşturulması ile kurumun yanıt verebilme becerilerinin geliştirilmesi sağlanır. Bu durum kurumun tehditleri önceden görerek bu tehditlerle en az iş kesintisine neden olacak şekilde baş etmesine yardımcı olur.

Siber Hazırlık yetkinliklerimiz ile müşterilerimize siber kriz yönetimi prosedürlerinin oluşturulması, kontrollü şekilde test edilmesi, kuramsal planlara dayalı testler yerine daha gerçekçi senaryolar oluşturulmasına yönelik hizmetler sunmaktayız.

- **Siber hazırlık çalışma grupları;** uyarlanmış masa başı testleri yönetimi ile siber tehditlerin doğası hakkında bilgilendirme, etkisi hakkında düşündürme ve mevcut yanıt/müdahale prosedürleri konusunda anlayış kazandırmayı amaçlar.
- **Siber hazırlık simülasyonları;** müşterilerimizin teknik ve stratejik anlamda müdahale/yanıt becerilerini test eder, iş birimlerinden ve yöneticilerden oluşan katılımcılar, rollerini ve süreçlerini uygulamalı olarak test ederek planların ve prosedürlerin güvenilirliğini gözden geçirirler.

Neden Deloitte?
Yetkin profesyonel kadromuz, askeri savaş tatbikatlarından uyarlanmış metodolojileri baz alan stratejik siber simülasyonlar ve kriz yönetimi çalışmaları konusunda deneyim sahibidir. Takım baskı testleri, siber olay yönetim stratejileri ve planlama yöntemleri ile yapılabilecek hataları, yanlış varsayımları ve gerçekçi olmayan beklentileri ortaya çıkarmakta, gerçek hayatta etkin uygulama sağlayacak yönlendirmeyi yapmaktadırlar.

2. Farkında ol
Siber farkındalığın ölçülmesi

Etkin siber güvenlik farkındalığı üç temel unsura dayanmaktadır:

- Aksiyon alınabilir ve gerçek zamanlı tehdit zekası oluşturulması
- Siber atak vektörlerini sınırlandırmak için bilinen açıklıkların tanımlanması ve testlerinin gerçekleştirilmesi
- Yüksek riskli alanlara ilişkin sürekli izleme mekanizmalarının kurulması

Siber farkındalık konusundaki bilgi birikimimiz müşterilerimize onlar için özelleştirilen hizmetler sunmamızı ve bu sayede, dış siber tehdit zekası ve açıklık değerlendirmelerinden dışarıdan yönetilen güvenlik servislerine kadar geniş yelpazade yetkinliklerimizi bir araya getirebilmemizi sağlamaktadır.

- **Siber tehdit haber alma servisi;** değişik kaynaklardan toplanan verilerin merkezi bir portalde konsolide edilerek müşterilerimizin kendi kurumları, endüstrileri ve bölgelerine ilişkin tehdit bilgilerine ulaşmalarına olanak sağlar.

- **Açıklık yönetimi;** altyapı, uygulama ve mobil ortamlara ilişkin değerlendirmeler ve testler ile müşterilerimize bu ortamlarda bulunan teknik açıklıklar konusunda derinlemesine bir görüş verilmesini sağlar. Böylece açıklıkları iyileştirme çalışmalarına odaklanılması ve siber atak vektörlerinin dışında kalanların kapatılması sağlanır.

- **Yönetilen güvenlik servisleri;** yüksek risk alanlarının belirlenmesi ve önceliklendirilmesi için tehdit modelleme, seçenekleri yönlendirmek için tehdit bazlı tasarım ve eş-kaynak kullanımı ile gerçekleştirilen güvenlik servislerinin birleştirilmesini sağlar.

Neden Deloitte?
Bir çok önemli güvenlik teknoloji sağlayıcısı ile sahip olduğumuz benzersiz iletişim, teknik yetkinliğimiz ve patentli "Siber Tehdit İstihbaratı" portalimizle birleştiğinde, kurumlara özel tehdit potansiyalinin sunulması ve aksiyon alınabilir, güncel ve entegre siber tehdit zekası oluşturulması için gelişmiş yaklaşımlar uygulanması mümkün olmaktadır.

3. Müdahale et
Hızlı, eksiksiz ve kesin

Siber ihlallerin gerçekleşmesi kaçınılmazdır, bu nedenle riski ve potansiyel etkiyi minimize etmek için kurumlar tanımlama, planlama, test ve siber müdahale stratejilerinin oluşturulmasında proaktif yaklaşım ortaya koymalıdırlar. Bu yaklaşım aşağıdakileri içermelidir:

- BT operasyonlarına ek olarak kapsamlı iş sürekliliği, ve halkla ilişkiler düşünülerek etkin bir şekilde olaya müdahalenin ve olayın etkisini azaltmak için gerekli olan süreçlerin ve ilgili planların tanımlanması
- İhlallerin kök nedeninin değerlendirilmesi için gerekli araçların ve teknik becerilerin tahsisi, adli soruşturmaların yönetilmesi ve teknik iyileştirmelerin hayata geçirilmesi
- Sürekli gözden geçirmenin, iyileştirme faaliyetlerinin gerçekleştirilmesi ve değişen organizasyonel risk profilleri ve müdahale becerilerinin siber tehditlerle uyumlu olarak uyarlanması

Siber Müdahale hizmetlerimiz ile, müşterilerimizin kriz zamanları boyunca ihtiyaç duyduğu beceri, deneyim ve uzmanlığa erişmelerini sağlıyoruz.

- **Siber olay yönetimi;** deneyimli kriz yönetim uygulayıcılarının, uzun dönemli ihlal değerlendirmesi, olay sonrası öğrenilen derslerin ortaya çıkarılması ve gelecek siber süreklilik planlamasının yapılması konularında olduğu gibi olaya anında müdahale ve olay yönetim aktivitelerinde de destek olması.
- **Siber adli soruşturma;** teknik kök neden değerlendirmesi, ihlal analizi ve adli soruşturmanın yönetilmesi için uzman ekiplerin tahsisi.

Neden Deloitte?
Etkin siber olay yönetimi, esneklik ve limitli bilgi ile proaktif kararlar alma kabiliyeti gerektirir. Geniş kapsamlı uzmanlığımız ile; soruşturma ve iyileştirme süreçlerinde olay yönetimi ve müdahale hizmetleri sunmakta ve bu sayede kurumların siber atakları ve sonuçlarını yönetmelerini sağlamaktayız.

Daha fazla bilgi için

Cüneyt Kırlar
Ortak
ckirlar@deloitte.com

Ali Yılmaz Kumcu
Direktör
akumcu@deloitte.com

Deloitte Türkiye

Sun Plaza
Maslak Mah. Bilim Sok. No:5
34398 Şişli, İstanbul
Tel: 90 (212) 366 60 00
Fax: 90 (212) 366 60 30

Punta Plaza
1456 Sok. No:10/1
Kat:12 Daire: 14 – 15
Alsancak, İzmir
Tel: 90 (232) 464 70 64
Fax: 90 (232) 464 71 94

Armada İş Merkezi
A Blok Kat:7 No:8
06510, Söğütözü, Ankara
Tel: 90 (312) 295 47 00
Fax: 90 (312) 295 47 47

Zeno Center İş Merkezi
Odunluk Mah. Kale Cad.
No: 10 d
Nilüfer, Bursa
Tel: 90 (224) 324 25 00

Adana
Günep Panaroma İş Merkezi
Reşatbey Mah. Türkkuşu Cad.
Bina No:1 B Blok Kat:7
Seyhan
+90 (322) 237 11 00

www.deloitte.com.tr
www.verginet.net
www.denetimnet.net