Siber Güvenlik ve Veri Koruma Hizmetleri

Siber dünyanızı güvenle yönetin!

Hizmetlerimiz

Deneyimli, farklı konularda uzmanlaşmış uzman, çözüm odaklı ve global ağın bir parçası olarak en iyi uygulamalara hızlıca ulaşabilen profesyonel bir ekibiz. Geniş bir yelpazede sunduğumuz **Siber Güvenlik ve Veri Koruma Hizmetlerimiz** ile bilgi güvenliğini en güncel stratejileri kullanarak kurumunuzun iş önceliklerinizle uyumlu şekilde sağlamanıza yardımcı oluyoruz.

Nasıl yardım edebiliriz?

Kurumlar, dijital iş modellerine yöneldikçe organizasyonlar, ortaklar ve müşteriler arasında gittikçe daha fazla veri paylaşımı gerçekleşiyor. Günümüzün birbirleriyle bağlantılı ekosistemlerinin yaşam kaynağı olan dijital bilgi, kurumlar ve bilgi güvenliğini tehdit eden aktörler için gittikçe daha değerli hale geliyor. Dijitalleşme, siber güvenlik ve gizliliği her zamankinden daha önemli hale getirdi.

İletişim

Ulvi Cemal Bucak
Siber Güvenlik ve Veri Koruma Hizmetleri Lideri,
0212 326 6838
cemal.bucak@pwc.com

Özkan Kıvanç
Siber Güvenlik ve Veri Koruma Hizmetleri Şirket Ortağı,
0212 326 6886
ozkan.kivanc@pwc.com

Strateji ve Dönüşüm

Bilgi Güvenliği Stratejisi

Bilgi güvenliği kurumun iş yapma kültürünün bir parçası olup, büyüme stratejilerine uygun iş hedefleri doğrultusunda bir bütün olarak yönetilmelidir. Bu strateji sadece kurumun kendisini değil tedarikçi ve hizmet sağlayıcılarını da kapsamalıdır.

Hizmetlerimiz

- Kurumsal Bilgi Güvenliği ve Siber Güvenlik Stratejisi
- Bilgi Güvenliği Organizasyonu
- Bilgi Güvenliği Yönetim Sistemi
- Üçüncü Taraf Güvenlik Riskleri Yönetimi

Yönetmelik ve Standartlara Uyum

Bilgi güvenliği kalitenizin belirli standartlarda olması, kritik bilgilerinizin gizliliği ve korunmasına ilişkin güven ortamının sağlanmasında önemli faktörlerden biridir.

ISO 27001 ve PCI-DSS standartlarına uyum bazı sektörlerde yasal zorunluluk haline gelmiştir. Bu standartlara uyum danışmanlığı ve uyumun denetimi konusunda hizmetlerimizle yanınızdayız.

Information Security Forum'un üyesi olduğumuz için, kurumunuzun bilgi güvenliği olgunluk seviyesini belirleyip, dünyadaki benzerleriyle karşılaştırma (benchmark) yapma imkânımız bulunuyor.

Hizmetlerimiz

- Bilgi Güvenliği Olgunluk Değerlendirmesi
- ISO 27001 Denetimi ve Danışmanlığı
- PCI-DSS Denetim ve Danışmanlığı

CISO Destek ve Gelişim Hizmetleri

Bilgi güvenliği dış kaynak (outsource) hizmeti veya eşkaynak (co-sourcing) hizmeti ile organizasyonel ihtiyacınıza yanıt verebiliriz.

Hizmetlerimiz

- Bilgi Güvenliği çerçevesinin belirlenmesi ve gözden geçirilmesi, farkındalık oturumlarıyla grup içinde bilgi güvenliğinin tanıtılması
- Bilgi Güvenliği risk değerlendirme faaliyetlerinin ve ilgili kontrollerin tanımlanması, ikinci seviye inceleme faaliyetleri (mantıksal ve fiziksel erişimin incelenmesi, projelerde güvenlik vb.)
- Kilit performans ve güvenlik göstergelerinin (KPI/KRI) belirlenmesi, düzenli olarak kontrol testleri ile ölçülmesi
- BT faaliyetlerine ilişkin günlük BT güvenlik kontrolleri (değişimin güvenlikteki etkileri, güvenlik duvarı kurallarının doğrulanması vb.).

SWIFT Müşteri Güvenlik Programı

Sanal dünyadaki saldırganların para transferi yapan sistemleri neden hedef aldıklarını sormaya gerek yok. Çünkü para orada! SWIFT Customer Security Programme (CSP) tamamen bu sebepten dolayı SWIFT tarafından oluşturulmuş güvenlik programına verilen isimdir. 2020 yılı içerisinde bütün SWIFT kullanıcılarının Customer Security Controls Framework'e (CSCF) göre bağımsız denetim gerçekleştirmeleri gerekiyor.

Hizmetlerimiz

- SWIFT CSCF'ye Göre Mevcut Durum Analizi
- SWIFT Sistemlerine Yönelik Sızma Testi
- SWIFT CSCF'ye Uyum Danışmanlığı
- SWIFT CSP Uyum Denetimi

Gizlilik ve Veri Koruma

Veri Koruma Hizmetleri

En hassas kurum veya kişisel bilgilerinizin istemediğiniz kişi veya kurumların eline geçmesini nasıl önleyebilirsiniz?

Bilgi günümüzde kurumlar için en değerli varlık haline geldi, ve bu varlığı korumak için önlemler almak artık bir tercih değil gereklilik.

Hizmetlerimiz

- Kişisel Verileri Koruma Kanununa (KVKK) Uyum
- Gizlilik Uyum Değerlendirmesi
- Veri Koruma Stratejisinin Oluşturulması
- Veri Sınıflandırması
- Veri Sızıntısı Önleme (DLP)

Güvenlik ve Farkındalık Eğitimleri

Bir kurumda bilgi güvenliği kimin sorumluluğundadır?

Hemen hemen bütün bilgi güvenliği farkındalık eğitimlerinde sorulan bu sorunun yanıtı “bilgi güvenliği kurumdaki herkesin sorumluluğudur” olmalıdır. Tutarlı bir bilgi güvenliği süreci oluşturmak ve bu sürecin sürdürülebilirliğini sağlamak, ancak çalışanların tamamının katılımı ile sağlanabilir.

Sürdürülebilir bilgi güvenliğinin omurgasını, çalışanların farkındalık düzeyini en üst seviyede tutacak kurum kültürü oluşturur.

Hizmetlerimiz

- Game of Threats™
- Kurum Geneli ve Üst Yönetime Özel Güvenlik Farkındalık Programları
- Bilgi Güvenliği Farkındalık Eğitimi
- Kişisel Verileri Koruma Eğitimi
- Oltalama (Phishing) Testleri
- CISO ve CSO Koçluk Hizmetleri

Game of Threats™

Siber tehditleri ve bu tehditlerle mücadele yöntemlerini eğlenerek öğrenin

PwC tarafından geliştirilen Game of Threats™ oyun atölyesinde, kurumların üst yönetimleri gerçek zamanlı bir siber tehditle başa çıkmaya çalışırken, konu hakkındaki farkındalıklarını en eğlenceli şekilde arttırma fırsatı buluyor.

Nedir?

Game of Threats™ gerçek siber saldırıların hızı ve yarattığı karmaşayı taklit etmek üzere tasarlanan bir oyun atölyesi. Oyun sırasında katılımcılar, “saldıran” ve “saldırıya uğrayan” olarak iki gruba ayrılıyor. Saldıran ekibe nasıl saldırıda bulunacakları, saldırıya maruz kalan ekibe ise nasıl kendilerini koruyacakları öğretiliyor. Moderatörler oyun süresince katılımcılara gerçek zamanlı geri bildirimler yaparak tercihleriyle ilgili yönlendirmede bulunuyor; strateji geliştirme ve karar alma sürecinde birebir destek oluyor. Oyunlaştırma teorisini interaktif katılımcı deneyimi ile birleştirerek yaratılan oyun ortamında, her iki ekip de minimum bilgi ile hızlı ve etkili kararlar alarak bu gerçekçi deneyimde zor durumdan kurtulmanın yolunu arıyor.

Kapsam:

Maksimum verimlilik açısından, bir Game of Threats™ oturumunun; - En az altı, en çok on altı katılımcı ile düzenlenmesi, - Toplam oturum süresinin 150 dakika ile 180 dakika arasında olması, ve - Oturumdan önceki hafta kurum BT ve Siber Güvenlik yöneticileri ile hazırlık amaçlı bir toplantı yapılması,
- Oturumu takip eden hafta tüm katılımcıların dahil olduğu bir değerlendirme toplantısı düzenlenmesi, tavsiye edilmektedir.

Kimler Katılmalı?

Şirket ortakları, CEO, Yönetim Kurulu Üyeleri, Genel Müdür, Genel Müdür Yardımcıları, Finans Direktörü, İnsan Kaynakları Liderleri, Baş Hukuk Müşavirleri, Bilgi Teknolojileri Direktörleri, Risk Yönetimi Liderleri, İç Denetim Liderleri, Bilgi Güvenliği Yöneticileri.

Kurulum ve Operasyon

Kimlik ve Erişim Yönetimi

Dijital dünyadaki kimliklerinizi doğru yönetiyor musunuz? Peki ya erişim haklarını?

Muhasebe sistemlerinden üretim uygulamalarına, kapı giriş sistemlerinden insan kaynakları uygulamalarına kadar teknoloji bağımlılığının giderek artmasıyla dijital dünyadaki kimliklerimizin ve bu kimlikler üzerindeki erişim haklarının da önem kazandığını söyleyebiliriz. Kimlik ve erişim yönetim süreçleri iyi yönetilmeyen kurumların dijital dünyadaki saldırganlar için bulunmaz nimet olduğunu söyleyebiliriz.

Kritik bilgilerinizin yetkisiz kişiler tarafından kullanılması ve paylaşılması riskini kontrol edebilmek için kurum içerisinde doğru kişinin, doğru bilgiye, doğru zamanda erişimi olduğundan emin olmak gerekir. Bunun için öncelikle olması gereken süreçlerin tasarlanması, daha sonra da süreçlerin uygulamalar yardımıyla otomasyonunun yapılması gerekmektedir.

Hizmetlerimiz

- Kimlik ve Erişim Yönetimi Olgunluğu Değerlendirme
- Kimlik ve Erişim Teknolojilerinin Entegrasyonu
- Ayrıcalıklı Kullanıcı Yönetimi

Altyapı ve Operasyon Güvenliği

Bilgi Teknolojileri altyapısı ve operasyonu, kurumunuzun iş önceliklerine uygun bir tasarıma sahip olmalıdır. Bu tasarıma uygun bir şekilde seçilen teknoloji ve ürünler ise kurumun iş hedeflerini destekleyecek nitelikte olgunlaştırılıp en uygun şekilde yönetilmelidir.

Hizmetlerimiz

- Bilgi teknolojileri güvenlik mimarisi
- Güvenlik teknolojileri ve ürünleri seçimi
- Güvenlik ürünleri ile kurumsal süreçlerin entegrasyonu
- Yönetilen güvenlik hizmetleri

Güvenlik Mimarisi

Teknoloji bağımlığının artması ve bilginin kurum içi ve kurum dışı paylaşma ihtiyacının da vazgeçilmez olmasıyla birlikte, kurumların tehdit yüzeyi de genişlemektedir. En güvenilir güvenlik yaklaşımlarından biri olan katmanlı güvenlik anlayışını uygulamak için iletişimin her seviyesinde güvenlik kontrollerini tesis etmeyi gerektirir.

İç ağ ve dış ağ güvenlik kontrollerinin uygulanması, kurumların dijital varlıklarını korumasındaki ilk adımı oluşturur. Bu kontrollerin uygulanmasından sonra düzenli olarak bu kontrollerin yeterliliği ve verimliliği de sınanmalıdır.

Hizmetlerimiz

- Kurumsal Güvenlik Mimarisinin Değerlendirmesi
- Hedef Kurumsal Güvenlik Mimarisinin Oluşturulması

Bulut Güvenliği

Bulut teknolojisinin devreye alınması diğer BT fonksiyonlarının devreye alınmasından farksızdır. İyi bir yönetişim modeli ve mimari tasarlanarak devreye alınmalıdır. Ancak yönetişim modelinin uygulanabilir olması gerekmektedir ve bulut teknolojisinin nimetlerini baltalamayacak şekilde tasarlanmalıdır. Dünyada kabul görmüş ISO 27017 Bulut Ortamında Bilgi Güvenliği Kontrolleri standardı kullanmak hem çalışanlarımıza hem de iş ortaklarımıza güvence vermeye yardımcı olur.

Hizmetlerimiz

- Bulut Güvenliği Denetimi
- ISO 27017 – Bulut Güvenliği Danışmanlığı

Olay ve Zafiyet Yönetimi

Tehdit ve Zafiyet Yönetimi

Kurum altyapınızda var olan açıklar saldırganlardan önce tespit edilerek kapatılmaz ise, itibar ve finansal kayıplara yol açabilecek güvenlik ihlalleri meydana gelebilir. Bilgi teknolojileri operasyonunuzun güvenliğini, saldırganların bakış açısıyla inceleyerek olası güvenlik ihlallerinin önüne geçebilirsiniz.

Hizmetlerimiz

- Uygulama güvenlik testleri
- Sızma (Penetrasyon) testleri ve sosyal mühendislik
- Yük testleri (DDos/DoS)
- Güvenlik açığı ve yama yönetimi
- Mobil uygulama testleri
- Konfigürasyon analizi

2020-0216

DDos ve Yük Testleri

Verdiğimiz DDoS testi hizmetlerimizle, kurumların muhtemel DDoS saldırılarına karşı direnç seviyelerini belirlemeyi amaçlıyoruz. DDoS/DoS (Servis Dışı Bırakma) saldırıları, gün geçtikçe daha fazla karşılaşılan saldırı vektörleri arasında yer alıyor. Bu saldırılar hem kurumların hem de kurumların hizmet verdiği müşterilerinin hayatını olumsuz yönde etkiliyor. Verdiğimiz DDoS testi hizmetimizle, kurumların muhtemel DDoS saldırılarına karşı direnç seviyelerini belirlemeyi amaçlıyoruz. Güvenli ve kontrollü ortamda yapılan DDoS testlerini senaryo bazlı veya ağ altyapısını test edecek şekilde kurgulayabiliriz.

Saldırı Vektörleri

- HTTP Get Flood
- Slowloris
- DNS Query Flood
- SYN Flood
- ACK Flood
- FIN Flood
- UDP Flood
- ICMP Flood
- Fonksiyonel Web Testleri

Siber Olaylara Müdahale

Siber saldırılara karşı hazırlıklı mısınız?

Modern iş dünyasında siber saldırılar kurumlar için en büyük risklerden birisini oluşturuyor. Olası bir saldırı durumunda bu saldırıya rağmen kritik iş süreçlerinin devamlılığı kurumlar için hayati önem taşıyor. Böyle bir olay olduğunda söz konusu sistemlerde kişisel veriler de bulunuyorsa olay bambaşka bir boyut kazanmaktadır.

Siber saldırılar gerçekleştiğinde teknik ve hukuki destek sağlayabilecek uzmanlarımızla hizmet veriyoruz. Proaktif olarak siber olaylara müdahale etkinliğini arttırmak isteyen kurumlara hazırlık ve simülasyon konusunda da yardımcı olabiliyoruz.

Hizmetlerimiz

- Kişisel Veri İhlallerinde Teknik ve Hukuki Danışmanlık
- Siber Olaylara Müdahale
- Olay Sonrası Tespit ve İnceleme
- Siber Olaylara Müdahale Süreçlerinin Değerlendirilmesi ve Tasarımı
- Siber Kriz Yönetimi Simülasyonu

Kaynak Kod Analizi

Kullandığınız yazılımlara ne kadar güveniyorsunuz?

Günümüzde internet ve mobil cihazların kullanımının yaygınlaşması ile yazılım güvenliğinin önemi giderek artmaktadır. Kurumunuzda yazılım güvenliğini sağlamak, doğru hedeflere odaklanarak uyum gereksinimlerini karşılamak, sürekli kontrol ortamını oluşturmak, yazılımın uygun güvenlik özelliklerine sahip olması ve yazılım geliştirme sürecinin sağladığı güvencenin beklenen seviyede olması için kaynak kod analizinin Yazılım Geliştirme Yaşam Döngüsü'ne (SDCL) entegre edilmesi gereklidir.

Hizmetlerimiz

- Yazılım Geliştirme Yaşam Döngüsünün (SDLC) değerlendirilmesi ve iyileştirilme adımlarının belirlenmesi
- Kaynak Kod Analizi ile mevcut yazılımlarınızın gözden geçirilmesi ve açıkların belirlenmesi
- Kaynak Kod Analizi araçlarının uyarlanması ve Yazılım Geliştirme Yaşam Döngüsü (SDLC) ile entegrasyonunun sağlanarak sürekli kontrol ortamının oluşturulması
- Farklı platformlardaki (Windows, Android, IOS, Linux vb.) yazılımlarınız için ayrı sistemlere ihtiyaç duymadan statik kaynak kodların analizi
- Derlenme seviyesine gelmemiş projelerin taranması (Continuous Integration)
- Sadece değişen kodların taranması özelliği ile değiştirilen dosyayı etkileyen dosyaları (üç önceki ve üç sonraki) tekrar tarayarak her seferinde tüm projeyi yeniden tarama ihtiyacı duymaksızın tarama sürelerinin optimize edilmesi (Incremantal Scan)
- Obje temelli script dili ile güvenlik sorgularının kolaylıkla ve hızlı bir şekilde özelleştirilebilmesi.
- Entegre edilecek araçların fazla sayıda güvenlik açıklarını desteklemesi