Siber Güvenlik

ÇÖZÜM KATALOĞU

ÖLÇSAN
"kalitenin ölçüsü"

GENEL

Uluslararası projelerde görev almış, konusunda otorite ekibiyle ÖLÇSAN, bölgemizdeki öncü finans, e-ticaret, savunma, eğitim, sanayi ve devlet kurumlarına; yerli / milli ve açık kaynak teknolojilerinin güç ve esnekliğini, dünya standartlarında kurumsal destek ekipleriyle sağlıyor.

NIST Cyber Security Framework

Ağlarınızda 360 Derece Alan Hakimiyeti

LAN içinde de WAN kadar güvensiz kabul eden “ZeroTrust” paradigmasıyla dikkatinizi gerçekten korumanız gerekenlere yoğunlaştırmanızı sağlayan, bunu gerçekleştirirken açık kaynak bileşenlerin kullanımıyla yönetilebilir maliyetlerde kalabilen yerli ve milli çözümleri, Türkiye’de birçok kurum ağında gerçek defansif çözümleriyle farklılaşıyor. Günümüzde NIST Siber Güvenlik Çerçevesi Amerika’daki federal kurumlar için zorunlu olmuştur. Bu çerçeveyi globalde tüm kurumlar rehber olarak kullanmakta ve faydalanmaktadır. ÖLÇSAN olarak bu çerçeveyi kendi tecrübemizle özgünleştirerek “BİLSAVUN” felsefemiz ile hareket etmekteyiz.

YAKLAŞIM: “ZERO TRUST” ve DEFANSİF SİSTEM GÜVENLİĞİ

“SecOPS” yaklaşımıyla, işletim sistemi ve uygulama bağımsız, ihtiyaçlarınız doğrultusunda sürdürülebilir süreçlerle merkezi ve kolay yönetilebilir güvenlik servisleri sağlıyoruz. Kurum ağındaki güvenli çekirdeğin etrafına boşluk kalmayacak Zero Trust Network Architecture (ZTNA) kurgulamanızda bu konudaki otorite uzmanlığımızla yardımcı oluyoruz. Ağlarınızda yatay hareketleri (Lateral Movement) takip edebilmenize olanak sağlayan Monitor -> Analyze -> Detect -> Response süreçlerinizin hayata geçirilmesinde destek oluyoruz.

Çözümler

ÖLÇSAN, “SAVUNMAMIZI, SALDIRGANLARIN ZATEN AĞIMIZDA OLDUĞU KURAMINA GÖRE YÖNETMELİYİZ” prensibinden hareketle siber güvenliğin tüm katmanlarında (L1-L7) çözümler sunmaktadır.

AĞ ve ALTYAPI GÜVENLİĞİ

Ağ güvenliği genel olarak organizasyonun veri kaynaklarını basit kullanıcı hatalarından ve kötücül ataklardan korumak olarak özetlenebilir.

Ağ güvenliği alanında; Güvenlik analizi, Güvenlik kontrolleri, İyileştirme ve güncelleme, Servislerinin yanı sıra; Firewall, Ağ tabanlı IPS, VPN, Secure Web Gateway, Veri Sızıntı Koruması (DLP), İkili kimlik doğrulama (2F Authentication), Anti-Virus ve Anti-Spam ürünlerinin seçimi, kurulum, konfigürasyon ve yönetim çözümleri sunmaktayız.

UYGULAMA GÜVENLİĞİ

Uygulamalar kendilerine ayrılmış kaynaklarla çalışırlar. Uygulamalar, sırasıyla, uygulama güvenliğinin belirlediği yoldan, uygulama kullanıcıları aracılığıyla bu kaynakların kullanımını belirlerler. İlerleyen teknolojiyle birlikte, kurumların kritik ticari uygulamaları artık web teknolojileriyle birleşmiş ve yaygın olarak kullanılmaya başlamıştır. Bu teknolojinin avantajlarıyla birlikte karşı karşıya kalınacak risklerin boyutları da değişmiştir. Web tabanlı uygulamaların güvenliğinin kontrol edilmesi ve tespit edilen güvenlik zafiyetlerinin giderilmesi büyük önem kazanmıştır. Uygulama Güvenliği konusunda; Test ve Raporlama, Application Firewall, Application Scanner, Uygulama Konfigürasyonu çözümlerini sunmaktayız.

VERİ GÜVENLİĞİ

Veri kaybını önleme (DLP) yazılımı ve araçları, uç nokta etkinliklerini izler ve kontrol eder. Şirket ağlarındaki veri akışlarını filtreler ve duran, hareket eden ve kullanımdaki verileri korumak için buluttaki verileri izler. DLP ayrıca (KVKK, PCI vb.) uyumluluk ve denetim gerekliliklerini yerine getirmek ve anormallik alanlarını belirlemek için raporlama sağlar.

WEB GÜVENLİĞİ

Web Güvenliği Çözümlerimiz, kullanıcılarınızı WannaCry da dahil olmak üzere günümüzün sürekli değişen kötü amaçlı yazılımları, hedefli saldırıları ve fidye yazılım varyantları gibi tehditlere karşı korur, çok katmanlı entegre koruma ile kullanıcılarınızın uç nokta e-posta, web, SaaS uygulamalarının ağ veya yerleşke fark etmeksizin korunmasını sağlar.

Web, sosyal medya ve bulut uygulamaları için uyarlanabilir DLP teknolojisi ile gerçek zamanlı izleme ve inceleme, yalnızca gizli bilgilerin sızmasını engelleyebilir veya kaldırabilirken, web trafiğinin geri kalanının rahatsız edici karantinalar veya yanlış alarmlar olmadan devam etmesine olanak tanır. Veri gizliliği ve yasal uyumluluk için optimize edilmiştir. (PCI, HIPAA, GDPR, vb.).

Çalışan gizliliğini ve güvenliğini korurken markanızı uygunsuz sosyal paylaşımlardan korunması gerekir. Sosyal medya iletişimleri, marka bütünlüğünü sağlamak, gizli bilgi sızıntılarını önlemek ve hedefli kimlik avı ve kötü amaçlı yazılım saldırılarına karşı koruma sağlamak için temizlenir.

UÇ NOKTA GÜVENLİĞİ

Kaynaklarınızı zorlamadan kuruluşunuzu hedef alan gelişmiş tehditlere karşı etkili bir savunma sunar. Güçlü koruma, algılama ve yanıt teknolojilerini tek bir güçlendirilmiş entegre çözümde bir araya getiren çok katmanlı yaklaşımımız sizi saldırılara karşı korur. Antivirüs, uçtan uca şifreleme, loglama vb çözümlerini sunmaktayız.

GÜVENLİ MESAJLAŞMA ve HABERLEŞME

Kendi sunucularınıza kurabileceğiniz, şirket içi profesyonel mesajlaşma yazılımı olan OLC-MSJ, askeri seviyede şifreleme özelliği ile güvenliği ön planda tutanlar için vazgeçilmez bir çözümdür.

Tüm metin ve dosya iletim mesajları hem istemci hem de sunucu tarafında günlüğe kaydedilir, bu da işleri izlenebilir hale getirir. Ayrıca, geliştirmiş olduğumuz ODAK Meet aracılığıyla mesaj teslimi kesin olarak sağlanır. Kurumunuzdaki tüm ODAK Meet kullanıcılarının bilgisayarlarına uzaktan bağlanabilir, destek olabilirsiniz. Ofis dışındayken bile bilgisayarlara tam olarak erişme fırsatı verir. ODAK Meet, Active Directory'nizden, LDAP sunucunuzdan veya önceden kaydedilmiş bir adres defterinden kullanıcıları içe aktarmanızı sağlar. Gelen ve giden tüm ODAK Meet mesajları, askeri standartlara uygun AES256 kullanılarak şifrelenir. Havaalanı, otel, kafe gibi ortak alanlarda bile WiFi'ye bağlandığınızda ODAK Meet'e erişmek güvenlidir. Yöneticiniz atölye çalışması için bir ekip atayabilir ve üye olarak kendinizi görev kuvvetleri için gruplayabilir veya sadece onlarla tartışabilirsiniz.

KİMLİK ve ERİŞİM YÖNETİMİ

Gelişmiş yüksek güvenlikli Açık Anahtarlama Altyapısı (AAA), biyometri, akıllı kart sistemleri desteği ile bilgi güvenliği algoritmalarıyla geliştirilmiş kullanıcı ve kimlik doğrulama çözümlerimizle gerek sistem yöneticilerinin gerekse de son kullanıcıların kullandığı sistemlerin izinsiz kullanıma ve erişimine engellenmesini/kapatılmasını sağlıyoruz.

MOBİL GÜVENLİK

Çevrim içi seanslarda yanlış kimlik kullanımı, finansal veri ve değerli bilgi veri sızıntısı engellenmesi ile beraber bilinen virüs ve trojanlara karşı koruma Antivirüs, Web Control, Kimlik Koruma, Anti-Exploit, Web tabanlı merkezi yönetim konsolu, kolay kullanım ve raporlama özellikleri, Active Directory Entegrasyonu, GPO ile kurulum ve Push Deployment, kurum içi güncelleme sunucuları, Syslog ve SIEM entegrasyonu. Biyometrik yüz tanıma tabanlı kimlik doğrulaması ile firmamız, mobil güvenlik teknolojilerinin kurumun ihtiyacına göre belirlenip uygulanması noktasında en avantajlı çözüm ve hizmetleri sunmaktadır.

GÜVENLİK OPERASYONLARI VE OLAY YÖNETİMİ

Güvenlik bilgileri ve olay yönetimi (SIEM); olay müdahalesi ve düzeltmesi için saptamayı hızlandırmanın yanı sıra güvenlik yönetimi, otomasyonu ve müdahalesi (SOAR) platformlarıyla sorunsuz bir şekilde entegre edilmek için kullanıcı davranışı analizi (UBA), ağ akışı içgüdüleri ve yapay zeka gibi gelişmiş analizleri içerecek şekilde geliştirilmiştir. Ayrıca mevzuat ve kurumsal standartlara uyumluluk gereksinimlerinde SIEM kullanımı için güzel bir örnek oluşturmaktadır. Yerli, global ve firmamızca geliştirilen ürünlerle bu alanda da çözüm sunmaktayız.

BULUT GÜVENLİĞİ

Bulut bilişim kapsamında çevrimiçi olarak depolanan verilerin ele geçirilmesi, silinmesi ihtimallerine karşı, güvenli veri iletimi, güvenli yazılım ara yüzleri, güvenli veri depolama, kullanıcı erişim kontrolü ve veri bölümlendirme ile en üst düzey önlem ve saldırı öncesi tespit ve önleme sistem çözümleri sağlıyoruz.

BİLGİ GÜVENLİĞİ ve RİSK YÖNETİMİ

Bilgi Güvenliği Yönetim Sistemini, şirketlerin finansal verilerini, fikri mülkiyetlerini ve hassas müşteri bilgilerini korumalarına yardımcı olan uluslararası bir sistemdir. Bilgi Güvenliği Yönetim Sistemi çözümünün temelini oluşturan Bilgi Güvenliği Politikasında şirket risklerinizi tanımlayabilir, gizli bilgilerinizin risklerini yönetebilir veya azaltabilirsiniz. Risk yönetimi ve değerlendirmesi ile, risklerinizi araştırıp tespit edebilir, bu risklerin çeşitli faaliyet aşamaları üzerindeki etkilerini gözlemleyip, risklerin yaratacağı olası zararlardan korunmak amacı ile bu riskleri önceliklerine göre sıralayan ve buna bağlı olarak yöntem ve strateji geliştirme çözümü sunuyoruz. ISO 27001 Bilgi Güvenliği Yönetimi sertifikası için ön hazırlık, danışmanlık, şirket içi uyum ve denetim konu başlıklarında çözüm sağlıyoruz.

SAHTEKARLIK ve İŞLEM GÜVENLİĞİ

İnternet üzerinden dolandırıcılık birçok farklı iş sektörü için sorun haline gelmiş durumda. Bundan en çok etkilenen Finans sektörü yanı sıra program sağlayıcıları ve e-ticaret şirketleri de bu durumdan etkileniyor. Dolandırıcılığın en aza indirilmesi ve internet güvenliğinin sağlanması, kullanıcı deneyimini iyileştirme ve çok yönlü kimlik doğrulama gibi ek güvenlik önlemlerinin alınmasını gerektiriyor.

Davranışsal ve biyometrik veriler, cihaz güvenilirliği ve kişisel olmayan meta verileri analiz edilerek, kimlik doğrulama sırasında kullanıcının belirli bir işlem yapmasına gerek kalmayacak şekilde giriş yapmasına ortam sağlar. Site/program güvenliği ve kriminal veri kontrolü öncelikli olarak yer alır.

DİJİTAL RİSK YÖNETİMİ

Son zamanlarda ortaya çıkan finansal sıkıntılar ve çıkarılan yasal düzenlemeler ile artık günümüzde geleneksel denetim yöntemlerinden ziyade, dijital ortamda yapılan denetimler giderek önemli bir hale gelmektedir. Sürekli denetim, gerçek zamanlı dijital ortamda işlemlerin kaydedilmesi, raporlanması ve denetim yapılması ile gerçekleşir. Sürekli denetim sayesinde şirketlerin güvenlik düzeylerinin arttığı görülmektedir. Yapılan iç ve dış denetimler, dijital risk yönetim güvenliğinde önemli bir noktada yer almaktadır.

IoT

Uçtan uca güvenlik kapsamında olağan dışı etkinlikleri ve olası tehditleri belirlemek için OT (Operasyonel Teknoloji) ve Secure IoT (Nesnelerin interneti) çözümleri üretiyoruz. Uçtan uca şifreleme çözümleri sunan IoT cihazlardan güvenli veri iletişimi, hali hazırda mevcut IoT sistemlerin güvenliği, mevcut güvenlik açıklarının tespiti ve önlemi, IoT cihazların güvenli veri loglaması gibi operasyonlara alanında uzman ekibimiz ile gömülü sistem ve işletim sistemi bazında müşteri ve ihtiyaca göre özel çözümler sunmaktayız.

BLOCKCHAIN

Açıklardan yararlanma, hedefli saldırılar ya da yetkisiz erişime ilişkin riskler, anında olay müdahalesi ve sistem kurtarma ile azaltılabilir. İzinsiz girişleri engellemek için kaynak kodu incelemesi, dolandırıcılık ve kimlik avına karşı koruma sağlama çözümleri sunmaktayız.

SİBER SALDIRI İSTİHBARAT SİSTEMİ

Siber istihbarat, tehdidin tespit edilmesi, önceliklendirilmesi veya acil durum müdahalesinin doğru yönlendirilmesi gibi belirli konulardaki yeteneklerin iyileştirilmesi açısından kurum ve kuruluşlar için hayati öneme sahiptir. Siber istihbarat, kurum ve kuruluşların bilgi teknolojileri departmanlarının, yönetilen ağlardaki mevcut ve olası tehditlerin tespiti ve olaya doğru biçimde müdahale edilmesi için ihtiyaç duyulan bilgi olarak tanımlanmaktadır. Siber istihbarat, siber tehdit araştırmaları ve bunların analiz edilmelerinin neticesinde elde edilir.

Siber istihbarat neden bu kadar önemli?

Bugüne kadar gerçekleşen veri ihlalleri değerlendirildiğinde, ön almak için gerçekleştirilen faaliyetlerin yüzde yüz olarak koruma sağlamadığı ortaya çıkmaktadır Siber güvenlik konusunda sınırsız bütçe ayıran kurum ve kuruluşlar bile veri sızıntılarından mağdur olabilmektedirler. Siber saldırganların üzerine çalıştıkları yeni teknik ve taktikler bunun en önemli nedenidir. Her gün yeni bir stratejiye tanık olunması nedeniyle kritik sistemleri hedef alan saldırganları takip edebilmek kolay değildir. Kullanılan bilgi sistemlerinin her daim hedef alınma ihtimali olduğunun farkında olunmalıdır. Bu noktada saldırıların hedeflerini, kullanılan taktiklerini ve tekniklerini içeren siber istihbarat olgusu kurum ve kuruluşlar için çok önemlidir. Siber istihbarat, siber saldırıların önüne geçebilmek için en önemli silahtır.

Nitelikli siber istihbarat toplamak için uzmanlık gerektiren ayrıntılı tehdit analizleri yapılmalıdır. Tehdit analizi ile birlikte elde edilen veriler ile, siber saldırganların kullandığı araç, taktik ve teknikler ile bilgiler birleştirildiğinde olası tehditler en doğru şekilde tespit edilir ve müdahale sağlanabilir.

Önemli Çözüm Başlıkları:

SİBER SALDIRI TESPİT SİSTEMİ

IDS/IPS sistemleri ağı sık sık monitör etmek, olası tehditleri tanımlamak ve bunlarla ilgili olay kayıtlarını (logları) tutmak, saldırıları durdurmak ve güvenlik yöneticilerine raporlamak gibi işlevlere sahiptir. Bu sistemler bazı durumlarda kurumların güvenlik politikalarındaki zayıflıkları ortaya çıkarmak için de kullanılabilmektedir. IDS/IPS aynı zamanda saldırganların ağla ilgili bilgi toplama faaliyetlerini algılayarak saldırganları bu erken aşamada da durdurabilme işlemini gerçekleştirebilirler.

AĞ PAKET YAKALAMA ve ANALİZ ÇÖZÜMLERİ

Paket Yakalama, bir veri ağındaki belirli bir noktayı geçen bir veri paketini yakalamak için kullanılan bir ağ terimidir. Bir paket gerçek zamanlı olarak yakalandığında, analiz edilebilmesi ve ardından indirilebilmesi, arşivlenebilmesi veya atılabilmesi için belirli bir süre saklanır. Paketler, aşağıdaki ağ sorunlarını tanılamaya ve çözmeye yardımcı olmak için yakalanır ve incelenir:

- Güvenlik tehditlerini belirleme
- İstenmeyen ağ davranışlarında sorun giderme
- Ağ tıkanıklığını tanımlama
- Veri / paket kaybını tanımlama
- Adli ağ analizi

Paket yakalama, sıralı olarak veya ağ anahtarlama cihazları tarafından bir paket yakalama cihazına gönderilen trafiğin bir kopyası kullanılarak gerçekleştirilebilir.

Tam Paket Yakalama, bir paketin tüm paketleri veya belirli bölümleri yakalanabilir. Tam paket iki şey içerir: payload ve header. Payload, paketin gerçek içeriğidir, header ise paketin kaynak ve hedef adresi dahil olmak üzere meta verileri içerir.

Paket yakalama verilerinin analizi tipik olarak önemli teknik beceriler gerektirir ve genellikle Wireshark gibi araçlarla gerçekleştirilir.

"HONEYPOT" VE TUZAK/KAPAN SİSTEMLERİ ile ERKEN UYARI

Ağ içerisine, zafiyetli sistemler yerleştirilerek herhangi bir sızma faaliyetini erkenden tespit etme yöntemidir.

Kötü amaçlı yazılımlara yönelik honeypot , kötü amaçlı yazılım saldırılarını davet etmek için yazılım uygulamalarını ve API'leri taklit eder. Kötü amaçlı yazılımın özellikleri, daha sonra kötü amaçlı yazılımdan koru yazılımı gerçekleştirmek veya API'deki güvenlik açıklarını kapatmak için analiz edilebilir.

Spider Honeypot, yalnızca gezginler tarafından erişilebilen web sayfaları ve bağlantılar oluşturularak web gezginlerini (spider) yakalamaya yöneliktir. Gezginleri tespit etmek, kötü amaçlı botların yanı sıra reklam ağı gezginlerini de engellemeyi öğrenmemize yardımcı olmaktadır.

Honeypot sistemine gelen trafiği izleyerek; siber suçların nereden geldiğini, tehdit düzeyini, hangi yöntemi kullandıklarını, hangi veri ve uygulamalarla ilgilendiklerini, güvenlik önlemlerimizin siber saldırıları durdurmak için ne kadar iyi çalıştığını denetleyebiliriz.

5651 ve LOG ÇÖZÜMLERİ

5651 nolu "İnternet Yoluyla İşlenen Suçların Engellenmesi" hakkında kanuna uygun içerik filtrelenmesi, Logların Gateway cihazlarından toplanıp imzalanması ve saklanması, Firewall, Hotspot ve Mirror uygulamalarının üzerinde oluşturulan zaman damgalı kayıtların analiz edilmesi ve raporlanması çözümlerini sağlıyoruz.

UYUMLULUK YÖNETİMİ

BT uyumluluk yönetimi, NIST, ISO veya CSA gibi gerekli standartlarla düzenleyici gereksinimlerin karşılanmasını içerir. Özel içerik miktarı nedeniyle bunları tamamlamak zor olabilir ve genellikle kuruluşların değerlendirmeleri tamamlamaları için uzmanlar getirmesini gerektirir.

BT uyumluluk yönetimi çözümümüz, öncelikle siber riski ve uyumsuzluğu ele almanıza ve iyileştirmenize yardımcı olacak, profesyoneller için risk ve uyum yönetimi çözümü olarak kullanılır. Platformumuz, uyumlu olmanız gereken herhangi bir standardı seçmenize olanak tanır ve ekibinizin tamamlaması için danışman gerektirmeden bir değerlendirme oluşturur.

KRİMİNAL VERİ TOPLAMA

Büyük veri (Big Data), insan ve makine tarafından üretilen, devasa bilgi haznelerinin neden olduğu, analiz ve işleme için standart bir veritabanına sığmayacak kadar büyük olan veri miktarıdır. İstihbaratın yapı taşlarını oluşturan makine öğrenmesi, büyük verilerden yararlanır.

Veri toplama, araştırma problemine cevap bulmak, hipotezi test etmek ve sonuçları değerlendirmek için ilgili kaynaklardan bilgi toplama sürecidir. Veri toplama yöntemleri;

İkincil veri toplama; kitaplarda, gazetelerde, dergilerde, çevrimiçi portallarda yayınlanmış veri türüdür. Bu kaynaklarda bolca veri bulunmaktadır. Bu nedenle araştırma yapılırken kısıtlamalar, kriterler belirleyerek çalışılması önerilir. Örneğin tarih, yazar, kaynağın güvenilirlik seviyesi, tartışmaların kalitesi, analizlerin ayrıntı ve derinliği gibi kriterler belirlenebilir.

Birincil veri toplama, kendi içinde nicel ve nitel veri toplama türleri olarak ayrılır; Nicel veri toplama yöntemi: Nicel veri toplama ve analiz yöntemleri arasında kapalı uçlu sorular içeren anketler, korelasyon ve regrasyon yöntemleri, ortalama, mod, medyan gibi yöntemler sayılabilir. Nitel veri toplama yöntemi: Nitel araştırmalar, derinlemesine anlayış ve nitel veri toplama yöntemlerinin daha yüksek düzeyde olmasını sağlamayı amaçlar; röportajlar, açık uçlu sorular içeren anketler, gözlem çalışmaları gibi çalışmalar örnek gösterilebilir.

Nicel ve nitel veri toplama yöntemleri arasındaki seçimimiz, araştırma alanımıza ve araştırma amaç ve hedeflerine bağlıdır. ÖLÇSAN hızlı çevrimiçi ve çevrimdışı araştırma çözümleri sunarak, kaliteli veri toplama, kodlama ve tablolaştırma hizmeti sunmaktadır.

OLAY MÜDAHALESİ

Olay müdahalesi (Incident Response), bir kuruluşun saldırı veya ihlalin sonuçlarını yönetmeye çalışma biçimi de dahil olmak üzere, veri ihlali veya siber saldırıyı ele alma sürecini tanımlamak için kullanılan bir terimdir. Nihayetinde amaç, olayın etkili bir şekilde yönetilmesi, böylece hasarın sınırlı olması ve hem toparlanma süreci hem de maliyetlerin yanı sıra marka itibarı gibi hasarların asgari düzeyde tutulmasını sağlamaktır. Olay Müdahalesi, planına ihtiyaç vardır. Başarılı bir Olay müdahalesi planı aşağıda bulunan 6 aşamayı kapsar:

- Hazırlık: Merkezi Kayıt Sistemi Oluşturma, Zaman Senkronizasyonu, Kullanıcı Hesabı Yönetimi, Sistem ve Servis Hesaplarının Yönetimi, Varlık Yönetimi, Güvenli İletişim, Hukuki İşlemleri
- Tanımlama: Ön Bakış, Atama, Kontrol Listesini Kullanma
- Kapsam Belirleme: Aksiyon Alma - Veri Toplama - İzolasyon
- Yok Etme: Ana Sebebini Belirleme - Rootkit Potansiyelini Belirleme - Savunmayı Güçlendirme - Zafiyet Taraması
- Kurtarma: Doğrulama - Geri Yükleme - İzleme
- Alınan Dersler: Takip Raporu Oluşturma

Kuruluşlar en azından bir olay müdahale planına sahip olmalıdır. Bu plan, şirket için bir olayı neyin oluşturduğunu tanımlamalı ve bir olay meydana geldiğinde izlenecek açık ve yönlendirilmiş bir süreç sağlanmalıdır. Hem olay müdahalesini yöneten hem de olay müdahale planında belirtilen her eylemi gerçekleştirmekten sorumlu ekipleri, çalışanları veya liderleri belirlemek gereklidir.

SİBER OPERASYON MERKEZLERİ İÇİN KURUMSAL ZAFİYET TARAMA

Kurum içinde kurulan Siber Operasyon Merkezlerinin (SOC) temel amacı; kurum ağına gelebilecek siber saldırıları mümkünse daha gerçekleşmeden etkisiz hale getirmektir ve önlemler almaktır. Kurumlar bu nedenle periyodik zamanlarda kurum içi sızma testi hizmeti satın almaktadırlar. Oysa bu testler genelde yılda yalnızca bir defa icra edilmekte, bu ise özellikle yeni çıkan zafiyetlere karşı yetersiz kalmakta, zamanla çok temel ama çok önemli güvenlik açıklarının gözden kaçmasına neden olmaktadır.

Kurumsal Zafiyet Tarama Aracı, kurumların bu en temel siber güvenlik ihtiyacını karşılamak için geliştirilmiş bir çözümdür:

- Belirlenen zaman dilimlerinde hedef ağ ve sistemleri periyodik ve otomatik olarak sürekli taramakta, kritik tüm bulguları ana panel ekranında servis tabanlı olarak ayrı ayrı sunmaktadır.
- Alternatif zafiyet tarama araçlarından çok daha hızlı taramayı tamamlamaktadır.
- Tarama sonunda seçilen IP için o makinede tespit edilen zafiyetleri ayrıca göstermektedir.
- Türkçe ve İngilizce desteğine bulunmakta, tarama sonuçlarında tespit edilen hususları Yönetici Özeti ile birlikte anlaşılır bir Sonuç Raporu olarak sunmaktadır.
- Tespit edilen zafiyetlerin birim yöneticisi tarafından Görev Ataması ekranı üzerinden sorumlusuna atanmasını, ilgilinin e-posta ile bilgilendirilmesini ve sürecin takibini sağlamaktadır.
- Tespit edilen zafiyetlerden en yaygınları için anlaşılır çözüm önerileri sunmaktadır.
- Temel cihazlar ve servisler için envanter taraması yaparak sistem farkındalığını güncel tutmaktadır.
- İnternet olmayan Kurumsal Kapalı Ağ ortamında da çevrimdışı olarak çalışabilmektedir.
- Dilenirse bütünleşik cihaz (appliance) olarak konumlandırılabilmektedir.
- Siber Operasyon Merkezinde faaliyet gösteren SIEM ve diğer güvenlik ürünlerine log beslemesi sağlayabilmektedir.

Hizmetler

AÇIK KAYNAK YAZILIMIN ESNEKLİĞİ ve TİCARİ YAZILIMLARIN GÜCÜ BİR ARADA

Türkiye'de satışını gerçekleştirdiğimiz BigData - büyük veri -, yenilikçi güvenlik ürünleri ve açık kaynak uzmanlığımızla en uygun ve en doğru çözümleri kurguluyoruz. Yurt dışında katıldığımız etkinliklerle en uygulanabilir Siber Savunma altyapılarını Türkiye'de yurtdışı gelişmeleri ile eş zamanlı olarak ve uygulanabilir hale getiriyoruz.

Ürün, hizmet ve danışmanlıkların projelendirmesini, kurulumunu, yapılandırmasını ve bakım hizmetini uluslararası ve yerli sertifikalara sahip teknik uzmanlarımızla sağlamaktayız.

SİBER GÜVENLİK HİZMETLERİ

Artan siber tehditler karşısında, tüm kurum ve kuruluşlar evrensel güvenlik ve veri güvenliği yatırımlarını arttırıyor. Günümüzde birçok kuruluş onlarca değişik güvenlik teknolojisini entegre şekilde çalıştırmakta ve güvenlik kayıtlarını izleyip olayları tespit etmekte zorlanıyor. Teknolojilerdeki hızlı değişime, yetkin personeli bulmanın, eğitiminin ve görevde tutmanın zorluğu ile bütçe kısıtları da eklenince, etkili bir güvenlik izleme ve olay müdahale altyapısı işletmenin zorluğunu, tüm kuruluşlar hissediyor.

Tüm bu ihtiyaçları karşılamak, kuruluşların yaptıkları güvenlik yatırımlarından mevcut personelleriyle azami verimi almalarını sağlamak üzere yapılandırılan Siber Güvenlik Operasyon Merkezi (SOME), çeşitli alanlarda uzmanlaşmış personelin görev yaptığı küresel standartlara göre işletilmektedir.

Kritik iş uygulamalarının kesintisiz çalışması için sistem ve ağ yapısını servis izleme araçları ile izliyor ve canlı olarak uygulamalarda oluşabilecek sorunların önceden tespit edilmesi ve bu sorunlara karşı önlem alınmasını sağlamaktayız.

SİBER GÜVENLİK OPERASYON MERKEZİ (SOME)

Siber Güvenlik Operasyon Merkezi (SOME); bilgi varlıklarını, bilgisayar ve iletişim altyapısını gerçekleşecek ihlallere karşı 7/24 esasına göre izleyen ve gözlemleyen, oluşmuş veya oluşabilecek ihlalleri değerlendiren, bu ihlallere karşı kurum ve kuruluşu savunan, kurum ve kuruluşta yer alan özel bir alandır. Bu merkezler, saldırı tespit ve kayıt yönetimi, izleme ve olay yönetimi, zafiyet analizi, zararlı yazılım analizi gibi siber güvenlik konularında uzman kişilerden oluşan ekip tarafından işletilmekte ve yönetilmektedir. Bu merkeze yetkisiz kişiler tarafından giriş yapılması/denemesi engellenmektedir. Bu operasyon merkezinde siber olayların izlenmesi, analiz edilmesi, raporlanması ve alarm üretilmesi işlemleri gerçekleştirilmektedir.

Siber Güvenlik Operasyon Merkezinden verilecek hizmetler, kuruluşların siber güvenlik alanında ihtiyaç duyduğu dört temel yetkinliği sağlayacak şekilde geliştirilmiştir:

- Önleme – Tespit – İstihbarat – Müdahale

Siber Güvenlik Operasyon Merkezinin (SOME), müşterilerine verdiği hizmet seviyesini garantilemesinin amacı, kurum ve kuruluşların, binlerce bilgi arasında gerçek tehditlere en hızlı şekilde odaklanmasını; bu tehditlere riski ve potansiyel zararı azaltacak şekilde müdahale edilmesini sağlamaktır.

Siber Güvenlik Operasyon Merkezinde (SOME) verilen servisler:

- Güvenlik olaylarına müdahale - Bilgi güvenliği zayıflık analizi - Zafiyet Yönetimi - Sürekli penetrasyon testi - Uygulama güvenlik testleri - Siber Tehdit istihbaratı - VOIP güvenliği - Güvenlik altyapısının güvenliği - Yasal uyum raporlama

SİBER İSTİHBARAT HİZMETİ

ÖLÇSAN, kurum ve kuruluşlarla ilgili mevcutlu ve olası siber tehditler hakkında nitelikli ve metodolojik olarak veri toplamak üzere siber istihbarat hizmetine büyük önem vermektedir. Siber istihbarat hizmetinin temel motivasyonunu, kurum ve kuruluşların olası siber güvenlik risklerini anlamalarını sağlamaktır. Siber istihbarat çalışmalarıyla, bilgi varlıklarınıza ve markanıza ciddi zararı olabilecek saldırı hazırlıkları ve saldırı türleri hakkında detaylı bilgi sahibi olunabilecektir.

Kuruluşunuz, gelişmiş ve etkili siber istihbarat hizmetiyle bilgi varlıklarının korunmasına dair daha önleyici ve kapsamlı bir yaklaşıma sahip olacaktır. Uzman ve tecrübeli ekibimiz, siber saldırganlar henüz sistemlerinize ve verilerinize telafisi olmayan zararlar vermeden önce sizi uyarır ve bu sayede tehditlere karşı hazırlıklı olabilirsiniz.

ÖLÇSAN, tehdit aktörleri hakkında detaylı incelemeler yaparak, olası saldırılara karşı ön almak adına en etkili ürün ve hizmetleri geliştirir. Bununla beraber, risklerin azaltılması, siber olaylara müdahale yeteneği ve kapasitesinin geliştirilmesi ile kurum ve kuruluşların güvenlik tedbirlerinin iyileştirilmesi için siber istihbarat uzmanlarımızın çalışmalarından faydalanılarak tehditlerin başlamadan bertaraf etmek adına etkili adımlar atılır.

ÖLÇSAN Siber istihbarat hizmeti sayesinde elde edeceğiniz kazanımlar:

- Kuruluşunuza yönelik risklerin değerlendirilmesi, gelen uyarıların analizi ve güvenliğinizin sağlanması,
- Siber güvenlik operasyonlarının niteliği ve verimliliğinin arttırılması,
- Güncel siber tehditler konusunda eksiksiz bilgi edinimi,
- Sisteminizin olası zafiyetlere karşı analiz edilmesi,
- Siber saldırganların kullandığı taktik ve tekniklerin anlaşılması,
- Siber istihbaratın güvenlik prosedürleri ile bütüncül olarak entegrasyonu.

Siber istihbarat hizmeti beş ana başlıkta fayda sağlar:

- Gerçek zamanlı siber tehdit tespiti,
- Siber saldırıları tanımlamak için taksonomik kabiliyet kazandırma,
- Siber saldırganların kullandığı teknik ve taktikleri doğru analiz edebilme,
- Siber tehditler hakkında gerçekçi ve detaylı analizler gerçekleştirme,
- Kuruluşunuzun genel siber güvenliğine dair önemli öngörüler elde etme.

TEST HİZMETLERİ

ISO 27001 Uyumu

ISO 27001 çalışmalarınızda, başvuru öncesinde veya periyodik denetimlerinizde, kalite standartlarınız çerçevesinde ihtiyaç duyduğunuz güvenlik denetim ve iyileştirme çalışmalarını uyumlulukla yürütmenizi destekliyoruz. Denetim öncesi güvenlik çalışmalarını tamamlamak üzere sızma testi raporu sağlamak, ihtiyaç halinde güvenlik yol haritanızı oluşturmak, periyodik denetimlerde ise hem mevcut kalitenizi korumak hem de güvenlik iyileştirmeleri yapabilmeniz için raporlarımızı sunuyor, açık kapamalarını takip ediyoruz.

Zafiyet taraması hizmetleri

Zafiyet taraması güncel veri tabanına sahip lisanslı yazılımlar ile yapılmaktadır. Güvenlik kapsamındaki güncel açıklıkların, ağınızda bulunup bulunmadığına dair yapılan tarama çalışmasıdır. Ağınız içerisindeki cihazlar bilinen zafiyetlere karşı taranarak, tespit edilen zafiyetler var ise uzman ekibimiz tarafından değerlendirilerek raporlanır.

Sızma testi hizmetleri

Sızma (Penetrasyon) testi birçok testi içeren tarama ve zafiyet tespit aracıdır. Sosyal Mühendislik, ağ güvenliği, DDoS testleri, internet üzerinde uygulama testleri vb. birçok alanda bilgi teknolojilerine uzman ekip tarafından testlerin yapılması, güvenlik açıklıklarının tespit edilmesinde en genel geçer koruma ve açıklık analizi yapma araçlarından birisidir.

Dış ağ sızma testi

Bu çalışma kurum dışından, internet üzerinden gerçekleştirilir, kontrollüdür ve zararsızdır, işi aksatıcı bir girişimde bulunulmaz. Güvenlik kapsamında yer alan sunucu ve sanal istemcilerde çalıştırılan işletim sistemi, yazılım, sürücü gibi temel noktalardan kaynaklı açıklıkların ağınıza izinsiz girişim imkânı barındırıp barındırmadığı tespit edilir ve var ise bulunan açıklar genel tavsiyeler ile birlikte raporlanır.

İç ağ sızma testi

İç ağ üzerinde gerçekleştirilebilecek saldırılara karşı önlem almak amacıyla yapılan, ağ içerisinde yer alan sunucu, ağ cihazları ve istemcilerinde sızma testleri yapılarak gerçekleştirilen tarama çalışmasıdır. Test yapılacak ağın yapısı, konumu ve ağ içerisindeki yer alan sunucu, ağ cihazı ve istemci sayısı dikkate alınarak çalışma VPN ile kuruma internet üzerinden bağlanarak veya kurum ziyaret edilerek lokal ağ üzerinden gerçekleştirilir, tespit edilen açıklıklara yönelik kapama önerileri ve uzman ekip görüşü raporlanır.

Kablosuz ağ testi

Kablosuz ağlarınızın sinyallerini takip eden saldırganların, ağ içerisine sızma çalışmalarının simülasyonunu içerir. Kablosuz ağ, değişik düzeylerdeki saldırı risklerine göre kademeli olarak testten geçirilir, varsa açıklar ve iyileştirme önerileri raporlanır.

Web sitesi güvenlik denetimi

OWASP gibi sızma testinde kullanılan programların listelerinde belirtilen web uygulama güvenlik riskleri incelenerek analizler yapılır. Web sayfasının çalışma akışına göre karışık saldırılar düzenlenerek zafiyet tespitleri yapılır ve açıkların kapatılması için raporlama yapılır.

DDOS Testi

DDoS simülasyonu, olası bir saldırı durumunun sonuçlarını tam olarak tespit etmek için mevcut değişkenlere göre bant genişliği kapasitesi, hizmet türü, altyapı, yazılım yapısı ve/veya mimari vb. farklı konuları içerir. Bu simülasyon, trafik kapasitenizi farklı saldırı, gereksiz bant genişliği yatırımları, gereksiz bant yükseltme ve/veya saldırı yönlendirme gibi yatırımlardan koruyarak, gerçek zayıf noktayı bularak doğru noktaya yatırım yapılmasını ve maliyetten tasarruf edilmesini sağlar.

Uygulama Yük ve Stres Testi

DDos testleri ile elde edilemeyen bulguların ortaya çıkarılması için uygulamanın yazılımsal özellikleri, yazılım uzmanlığı olan güvenlik uzmanları tarafından tespit edilerek yük ve stres testi yapılır, uygulama hatalarını ve zayıflıkları kod seviyesinde belirleyerek güvenli hale getirilir.

Özel Yazılmış Uygulamaların Denetimi

Güvenlik denetimlerinin yapılması gereken kritik alanlardan birisidir. Özel olarak yazılmış uygulamaların manuel denetimin gerçekleştirilmesi önemlidir. Yazılım geliştirme ekibimizin güvenli yazılım geliştirme bilgisi ile güvenli yazılımlarda bulunması gereken özellikler gözden geçirilerek yazılım denetimi gerçekleştirilir ve raporlanır.

Sosyal Mühendislik

Güvenlik zincirinde en zayıf halkanın insan olduğu ve zafiyet taşıdığı göz önüne alındığında, oluşabilecek güvenlik risklerini sosyal mühendislik denetimleri ile tespit eder, farkındalık eğitimleri ile risklere karşı prosedür ve kurallar oluşturulmasına yardımcı oluruz.

KVKK Uyumu

Kurumunuzun KVKK kanunu kapsamında geliştirmekte olduğu disiplini, sızma testi çalışmalarımız ve KVKK denetimlerimiz ile destekliyoruz. Bununla birlikte çalışmalarımızın tamamını kişisel verilere yönelik hassasiyet ile yürütürken hem verinin doğru alanlarda saklanması hem erişimin kontrollü olması hem de çalışma sırasında ifşa olmaması için gereken özeni gösteriyoruz.

Farkındalık Eğitimleri

Raporlanan açıklıklara yönelik alınabilecek sistemsel tedbirlerin dışında, insanı tedbirler daha büyük önem taşır. İnsanı tedbirlere ve kurumlarda yer alan, sistemde zafiyete yol açabilecek tüm kullanıcılara yönelik bilgi güvenliği eğitimleri, en temel seviyeden; gündelik yaşantımızda karşılaşabileceğimiz sorunlara kadar bilgilendirme eğitimleri yapılmaktadır.

BAKIM ve DESTEK SİSTEMİ

BT Güvenlik Ürünleri ve Sistemleri Bakım ve Destek; hizmet alanların BT sistemlerinin sürekliliğini, veri bütünlüğünü, doğruluğunu ve gizliliğini sağlayacak bilgi güvenliği destek ürün ve sistemlerinin kuruluşlarını, donanım ve sistem sorunlarının giderilmesini ve sorunsuz çalışmayı sağlamak üzere, belirli servis seviyelerine uygun olarak verilen teknik destek hizmetleridir. Çağrı bazlı ve servis seviyesi esaslı olarak yürütülür. “Uzaktan” veya “Hizmet Alan Yerinde” verilebilir.

Bilgi güvenliği ürünlerine ve sistemlerine verilecek olan bakım ve destek hizmetleri, servis sağlayıcı ile müşteri arasındaki hizmet sözleşmesinin içeriğine bağlı olarak aynı zamanda bilgi güvenliği süreçlerinin belirlenmesi ve organizasyonlar içerisindeki bilgi akışının güvenilir hale getirilmesi konularını da kapsayabilir.

BT Güvenlik Ürünleri Bakım ve Destek hizmetleri; bilgi teknolojilerini iş akışlarının önemli parçası olarak barındıran bilgi teknolojilerinden kaynaklanabilecek problemlerin iş akışlarının devamlılığını, bütünlüğünü ve gizliliğini zaafa düşürmesi ile zarar görme olasılığı bulunan, iş ortaklarının ve müşterilerinin bilgilerini gizli tutmakla sorumlu olan tüm firmalar tarafından kullanılabilir.

Danışmanlıklar

SİBER GÜVENLİK ÇERÇEVESİ DANIŞMANLIĞI

Siber güvenlik ve bilgi güvenliği danışmanlığı kurumların iç ve dış tehditlerden korunmasını amaçlamaktadır. Siber güvenlik; kurum bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini doğrulayarak iletimi ile saklanması sırasında bilgi güvenliği politikalarının doğru bir şekilde uygulanması için gerekli olan işlemlerin yapılması amaçlamaktadır. Bu işlemlerin devamlılığını sağlamak için gelişen teknoloji ve yenilenen siber saldırılar sırasında siber güvenlik danışmanlığı zorunlu bir hale gelmiştir. Siber güvenlik danışmanlığı kapsamında "siber saldırgan" olarak da tanımlanan kötü niyetli kişilerin kullandıkları teknikler, hedef sistem üzerindeki zafiyetleri tespit etmek için kullandıkları araçlar, sistemleri ele geçirmek için kullanılan istismar kodları ve web uygulamalarına yönelik saldırılar ile saldırganların psikolojileri ele alınmaktadır.

Bu hizmet kapsamında olası bir siber olaya müdahale edip (bilgi hırsızlığı, şantaj, hacking, vb gibi olaylarda) müşteri bünyesinde yer alan ve ilgili olayların çözülmesinde kullanılacak gerekli sayısal delilleri elde etme ve bu delilleri analiz edip, gerekli raporları hazırlama hizmeti de yer almaktadır. Siber güvenlik danışmanlığı kapsamında yapılan görüşmeler sonucu verilecek olan danışmanlık hizmetinin genel çerçevesi müşteriden gelen talepler doğrultusunda belirlenerek Ölçsan Siber Güvenlik danışman kadrosu tarafından kurumun envanteri, internet ortamındaki varlığının haritası çıkartılır. Ardından sızma testleri, web güvenliği veya yerel pentest gibi yöntemler uygulanmaktadır. Bu yöntemlerin ve testlerin sonuçları analiz edilerek kurumun siber risk haritası çıkartılır ve yapılması gereken güvenlik yatırımları için en doğru şekilde yönlendirmeler ve öneriler uzmanlarımız tarafından sağlanır. Bu sayede kurum kendisine karşı yapılabilecek siber saldırılara karşı doğrudan önlem alabilmesine olanak sağlanarak geri dönüşü olmayacak harcamaların önüne geçilir.

GÜVENLİK DENETİMLERİ VE SIZMA TESTLERİ

Sızma Testi (penetrasyon testi) olası güvenlik zaaflarını risk gerçekleşmeden önce tespit etmek için zorunludur. Bu nedenle PCI, ISO27001, SoX/Cobit gibi tüm regülasyonlarda güvenlik denetimi ve/veya penetrasyon testleri zorunlu tutulmuştur.

ÖLÇSAN penetrasyon testi ve güvenik denetimi başlıkları altına iki farklı hizmeti Certified Ethical Hacker (CEH) sertifikasına sahip bilgi güvenliği uzmanlarıyla sunmaktadır. Güvenlik denetimi testleri genellikle regülasyon uyumluluğu için kullanılır ve DoS/DDoS, sisteme sızma, kanıt alma veya kanıt bırakma gibi işlemler yapılmaz.

Denetimlerimiz aşağıdaki gibidir;

- Internet güvenlik denetimi
- Web uygulama denetimi (Kullanıcı adı ve şifre ile girilebilen web uygulamaları dahil)
- Güvenlik ürünleri atlama denetimleri
- Üçüncü parti testleri (alan adı, google hacking)
- DoS/DDoS denetimi
- Yerel güvenlik denetimi
- Kablosuz ağ güvenlik denetimi

GÜVENLİ KOD GELİŞTİRME DANIŞMANLIĞI

Günümüz dünyasında uygulamaların %75'ini web uygulamaları oluşturuyor ve bunların çoğu da bankacılık, e-devlet siteleri gibi kritik uygulamalar. Kurumlara para ve zaman kazandıran bu uygulamaların kullanıcı dostu, her zaman erişilebilir, performanslı ve "güvenilir" olması büyük önem taşımaktadır.

Güvenli yazılım geliştirme kavramının önemi günümüzde çok iyi anlaşılmış, bu kavram yazılım geliştirme maliyetini, süresini azaltan ve yazılımın kalitesin arttıran bir unsur olarak kabul görmüştür. Ayrıca yazılım kullanımı sırasında ortaya çıkabilecek pek çok güvenlik olayını da kaynağında engellemenin en etkili yoludur.

ÖLÇSAN, "Güvenli Yazılım Geliştirme Yaşam Döngüsü"nün oluşturulması için kurumlara danışmanlık hizmeti sağlar. Uygulama yazılmaya başladığı anda güvenlik katmanı oluşturmanın gerekli olduğu bilinciyle, kaynak kod analizleri yaparak uygulamanın hem erişilebilir hem güvenilir olmasını garanti altına alır, yük testleri ile performansı analiz eder. Aynı zamanda hali hazırda geliştirilmiş uygulamalardaki açıkları tespit etmek üzere güvenlik testleri gerçekleştirir.

Bunun yanı sıra, kod geliştiren ekiplerin bu konuda bilgili olması ve güvenlik faktörünün hep göz önünde bulundurmasını sağlamak üzere "Güvenli Kod Geliştirme Eğitimleri" verir.

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ DANIŞMANLIĞI

ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), risk yönetimi ile belirlenen güvenlik kontrollerine ve bu kontrollerin sürekli iyileşmesine dayanan yönetim sistemidir. Kurumların bilgilerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması adına, risk yönetimi ve risk işleme planlarının, görev ve sorumlulukların iş devamlılığı planlarının, acil durum olay yönetiminin, bilgi güvenliğinin operasyonel prosedürlerinin hazırlanmasının ve uygulanmasının ve bunların kayıtlarının tutulması gerekmektedir. Tüm bu faaliyetler içinde bir dizi Bilgi Güvenliği (BG) politikası ve prosedürü yayınlanmalı ve personeli bilgi güvenliği anlamında bilinçlendirmelidir.

Ölçsan Bilgi Güvenliği, ISO 27001 Bilgi Güvenliği Yönetim Sistemi danışmanlık hizmeti ile BGYS süreçlerinin tamamını sizinle birlikte hayata geçirerek firmanızı ISO 27001 belgelendirme denetimine hazırlamaktadır. Bu hizmet kapsam dokümanının belirlenmesi ile başlayıp firmanın belgeyi alması ile son bulur. ISO 27001 Standardı kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlamaktadır. BGYS, kurumunuzdaki tüm bilgi varlıklarının değerlendirilmesi ve bu varlıkların sahip oldukları zafiyetleri ve karşı karşıya oldukları tehditleri göz önüne alan bir risk analizi yapılmasını gerektirir.

GÜVENLİ SÜREÇ YÖNETİMİ DANIŞMANLIĞI

Bilgi Güvenliği, kurumların iş süreçlerinin bir parçası olarak işletilmeli ve kurumsal politikalar, kurallar çerçevesinde yürütülmelidir. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) ihtiyaçları tanımlayan uluslararası bir standarttır. Kurum iş süreçlerine bilgi güvenliğinin dahil edilmesini, bilgi güvenliğinin yaşayan bir süreç haline gelmesini, politikaların ve uyumluluğun izlenmesi, iyileştirilip geliştirilmesini ve kurumun bilgi varlığının korunmasını sağlar. ISO 27001 çerçevesi, kurumların bilgi sistemleri altyapısına göre özelleştirilebilir bir çerçeve sunar. Ölçsan Siber Güvenlik Danışmanlık ekibi BGYS kapsamında kurumunuzun ISO 27001 süreçlerini başarıyla entegre edebilmesi için mevcut durumunuzu gözlemler, ihtiyaçlarınızı belirler ve ISO 27001 uyumlu olabilmeniz için gereken ihtiyaçlarınızı temin eder. Bilgi Varlığının Gizlilik-Bütünlük-Erişebilirlik dengesinde tutunabilmesi için ISO 27001 BGSY standardı kurumun tüm iş süreçlerine entegre edilmiş olmalıdır.

KİŞİSEL VERİLERİN KORUNMASI KANUNUNA UYUM DANIŞMANLIĞI

7 Nisan 2016 tarihinde yürürlüğe giren '6698 Sayılı Kişisel Verilerin Korunması Kanunu', kişisel verilerin işlenmesi konusunda özel hayatın mahremiyeti başta olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları kuralları düzenleme amacını taşımaktadır. Bu kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır. Kişisel verilerin alınma şekilleri, işlenme amaçları, hukuki nedenleri ve hakları konularında ilgili kişiler en şeffaf şekilde bilgilendirilmelidir.

Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır. Kanuna göre kişisel verileri ihlal edenlere 1 yıldan 3 yıla kadar hapis cezası öngörülmektedir. Ayrıca bu veriyi ihlal yolu ile ele geçiren kişiye de 2 yıldan 4 yıla kadar hapis cezası verilebilir.

Veri güvenliği ile ilgili tecrübelerimize güvenerek, Kişisel Verilerin Korunması Kanunu ile ilgili ihtiyaç duyabileceğiniz tüm danışmanlık hizmetini ve gerekli ürünleri sağlamaktayız. Konu hakkında, hukuki boyutunu da göz önünde bulundurarak, teknik önlemlerin en uygun şekilde alınması için, çözümler sunmaktayız. Müşterilerimizin kanunda öngörülen cezai yaptırımlara uğramadan uyumlu hale gelmesine yardımcı olmak önceliğimizdir.

EKS / SCADA GÜVENLİK DANIŞMANLIĞI

Enerji ve doğalgaz altyapıları, su şebekeleri, sağlık sistemleri, savunma sanayi altyapıları, nükleer tesisler ve üretim tesisleri gibi kritik altyapıların hepsinde kullanılmakta ve güvenlik kavramı bu sistemlerin tasarım ve işletiminde göz önünde bulundurulması gereken önemli bir kavram olarak karşımıza çıkmaktadır. Söz konusu sistemlerin zarar gördüğü ve çalışamaz hale geldiği senaryolarda, büyük boyutlu maddi ve manevi zararların ortaya çıkması mümkündür. Ölçsan, siber güvenlik alanındaki tecrübesinden yola çıkarak EKS/SCADA sistemlerinin güvenliğini sağlamak üzere kapsamlı hizmetler sunmaktadır. Bu sistemler üzerinden yapılacak güvenlik analizleri çok yönlü ve titiz bir çalışmayı gerektirmektedir.

- Güvenlik Testleri, saldırgan bakış açısı ile en az bilgi ile altyapı üzerindeki bileşenlerin güvenlik testine tabi tutulmasıdır. Bu testler EKS/SCADA ağları ile ilişkili tüm olası sızma noktalarının denetlemesini kapsar. Ek olarak EKS/SCADA bileşenleri sızma testine tabi tutulur.
- Konfigürasyon denetimleri, altyapı bünyesindeki EKS/SCADA altyapılarının güvenliği ve sürekliliğini ilgilendiren bileşenlerin sistem yöneticisi gözü ile denetime tabi tutulmasıdır.
- Süreç denetimleri, işletim süreçlerinin güvenlik bakış açısıyla denetlenmesidir. Bu denetim kapsamında, değişiklik yönetimi, kayıt/log yönetimi, kapasite yönetimi, fiziksel güvenlik, insan kaynakları güvenliği gibi temel süreçler NIST SP800-82, ISO 27019, ISO 27001 gibi genel kabul görmüş standartlara göre denetlenir.
- Fiziksel denetimler, altyapı bünyesinde kritik işlevlere hizmet eden kontrol odaları, veri merkezleri ve işletmenin genel güvenlik durumu en iyi uygulama örneklerine göre denetlenir.
- EPDK Endüstriyel Kontrol Sistemleri Bilişim Güvenliği Yönetmeliği Uyumluluk Hizmetleri, yönetmeliğin ön gördüğü envanter çıkarma, risk analizi yapılması ve risk aksiyon planlarının hazırlanması konularında danışmanlık hizmeti sağlanarak, kurumların yönetmeliğe uyumlu hale gelmeleri temin edilir.

EĞİTİMLER

SİBER GÜVENLİKTE YAPAY ZEKA KULLANIM EĞİTİMİ

Yapay zekâ ve makine öğrenmesinin modern siber güvenlik uygulamaları için geleneksel uygulamalara göre bazı önemli avantajlar sağladığı bilinmektedir. Makine öğrenmesi uygulamalarının deneyime dayalı öğrenme ve gelecekteki benzer sorunlarla karşılaşıldığında nasıl bir strateji izleneceğine ilişkin bulguları sunma gücü, geleneksel pasif uygulamalara kıyasla bir avantaj olarak değerlendirilebilir. Makine öğrenmesi tahmin, önleme, tespit, yanıt ve izleme gibi beş güvenlik kategorisinin tamamında kuruluşların yeteneklerini geliştirmeye yardımcı olmada rol oynaması söz konusudur.

Makine öğrenmesi, ağ trafiği analizi, sahtekarlık tespiti ve kullanıcı davranışı gibi alanlarda yeni verilerle karşılaştığında karar vermeyi var olan verilerden öğrenebilir. Bu, ağdan uygulamaya, uç noktaya ve kullanıcı seviyesine kadar güvenlik katmanları arasında farklı tipte saldırıları tespit etmesini sağlar.

“Siber Güvenlikte Yapay Zeka” başlıklı eğitimimiz, kurumlara yapay zekâ ve makine öğrenmesi yöntemlerinin siber güvenlik alanında nasıl ve nerelerde kullanılabileceğini öğretmeye yöneliktir. Ön işleme ile verinin yeniden düzenlenmesi, makine öğrenmesi algoritmalarının uygulanarak tahmin ve sınıflama modellerinin elde edilmesi ardından bu modellerin test ve değerlendirme süreçlerini gerçek veri kümeleri üzerinde uygulanması ve farkındalığın yaratılması amaçlanmaktadır. Eğitimde özellikle derin öğrenme algoritmalarına odaklanarak, veri kümeleri üzerinde Tensorflow Keras kütüphanelerine dayalı Geri Dönüşlü Derin Öğrenme (Recurrent Neural Networks =RNN), LSTM ve Otomatik Kodlayıcılar (Autoencoders) gibi algoritmalar uygulanmaktadır.

KİMLİK YÖNETİMİ EĞİTİMİ

Büyük ölçekli kurumlarda ve erişim kontrolü gereken kamusal alanlarda kimlik doğrulamalı denetiminin yapılmasında uygulanabilecek farklı sistemlerin ve stratejilerin tartışılması, uygun çözüm seçeneklerinin anlatılması ve farkındalığın yaratılması amaçlıdır.

Ana Başlıklar:

Mevcut Kimlik Yönetimi ve Geçiş Kontrol Sistemleri, Türkiye ve Dünyadan örnekler - Mevcut yöntemlerin açıkları ve uygulamalarda karşılaşılan sorunlar - Uçtan uca güvenliğin ilk adımı Kimlik doğrulama - İki ve üç faktörlü doğrulama yöntemleri – Güçlü kimlik doğrulama - Donanım sistemi öğeleri ve teknik özellikleri - Yazılım kapsamı ve çoklu yerleşke grup yönetimi - Görsel kontrollü geçiş sistemleri (kişi tanıma, hareket, ikinci kişi varlığının saptanması, görüntü optimizasyonu, kara liste/black list uygulamaları) - Fiziksel ve sanal erişimin entegrasyonun önemi.

UÇ NOKTA (EDGE) GÜVENLİĞİ EĞİTİMİ

Teknolojinin gelişmesiyle birlikte elektronik IOT (Internet Of Things) cihazların yaygınlığı hızla artmaktadır. Cihazların kullanımı kadar cihazdaki verilerinizin güvenliği kullanıcılar için oldukça önemlidir. Yeni bir IOT ürün oluşturmak isteyen firma ve girişimcilerin en çok yoğunlaştığı konulardan biri cihazın veri haberleşmesi esnasında verilerinin şifrelenip gönderilmesi ve 3. kişiler tarafından erişimin engellenmesidir.

“Arduino ve IOT cihaz tasarımı ve güvenliği” eğitimimizde yeni bir IOT cihaz üretmek ve ürününü ticari amaçlı kullanmak isteyen girişimcilerimize, arduino kart nedir, nasıl programlanır, arduino ile devre oluşturma ve IOT proje üretme, IOT haberleşmesinde şifreleme ve güvenlik konularında çeşitli uygulamalarla bu konularda hakimiyet kazanımı elde etme hedeflenmektedir.

BT FARKINDALIK EĞİTİMLERİ

Bilgi güvenliğini tehdit eden risklerin başında çalışanların güvenlik konusundaki farkındalık eksikliği gelmektedir. Dünyaca ünlü bilişim firmalarının son yıllarda yaşadığı bilgi güvenliği ihlal olayları detaylıca incelendiğinde sorunun ana kaynağının çalışanların bilgi güvenliği farkındalıklarının eksikliği olduğu ortaya çıkmaktadır.

Çalışanların farkındalık seviyelerinin artırılmasında en önemli maddelerden biri düzenli olarak eğitim verilmesi ve eğitimler sonrası farkındalık senaryolarını içeren saldırı uygulamalarının yapılmasıdır.

Bu amaçla aşağıdaki eğitimler uygulanmaktadır:

Bilgi Güvenliği Farkındalık Eğitimi

ISO 27001 Bilgi Güvenliği Yönetimi Eğitimi

LINUX İŞLETİM SİSTEMLERİ GÜVENLİK EĞİTİMLERİ

Linux ve Windows ortamlarında güvenlik ayarları ve sıkılaştırma yöntemlerini anlamak, örnek senaryolarla kullanıcı yetkilerinin ve hesapların güvenliklerinin artırılması, saldırı engellenmesi, hesap bloke edilmesi, kurulum ve konfigürasyon yapılması, dosya şifrelemesi, şifreli haberleşme, erişim listeleri oluşturma ve zafiyet taramasının yapılması sağlanmaktadır.

Kullanıcı Hesapları ve Güvenliği, Yetkilendirilmiş kullanıcılar, Linux Şifre Sıkılaştırması, Linux Güvenlik Duvarının Sıkılaştırması, Şifreleme Teknolojileri, SSH Güvenliği, Dosya ve Klasör Yetkilendirme Yönetimi, SELinux, ClamAV, RootkitHunter, Log Yönetimi ve Log Güvenliği eğitimin içeriğini oluşturmaktadır.

TEMEL SİBER SAVUNMA EĞİTİMİ

Siber Operasyon Merkezi, Ağ Güvenlik İzlemesi, Siber Güvenlik İzlemesi ve Son Nokta Güvenliğini bütünsel bir çerçevede örnek senaryolarla destekli anlatılmaktadır.
SOME Süreçleri;
Ulusal Siber Güvenlik Strateji ve Eylem Planı, SOC Amaç ve Etkinlikleri, SIEM Çözümleri, Savunma Araç ve Çözümleri, Modern Savunma Mekanizmaları, Saldırgan Tabanlı Tespit, Ağ Güvenlik İzlemesi, Balküpü Sistemleri, Sürekli Güvenlik İzlemesi, Durumsal Farkındalık, Uygulama İzleme ve Takibi, Yapılandırma Değişim Yönetimi, Log Yönetim ve İzlemesi, Uç nokta Güvenliği, Yönetici Hesapları İzleme ve Yönetimi, Tehdit Avcılığı, Siber İstihbarat, Yetkilendirme, Post-Yetkilendirme, Ün Tabanlı Tespit, Anomali Tespiti ve Analizi, Paket Analizi, İmza Tabanlı Tespit, Oturum Analizi, Sensör Platformları, Risk Yönetim ve Planlaması, Tehdit Avcılığı ve Tehdit Zekası Kavramları içeriği oluşturmaktadır.

WEB UYGULAMA GÜVENLİĞİ EĞİTİMİ

Bu eğitim sonunda katılımcılar, web uygulamaları üzerinde bulunan zafiyetlerin nasıl tespit edilip kullanılabileceğini öğreneceklerdir.

Web Uygulama Teknolojisi ve Güvenlik Bileşenleri, Veritabanı Sistemleri, Web Uygulama Zafiyetleri, Kimlik Doğrulama, Zerk (Injection) Saldırıları, XSS, NoSQL Uygulamalar, Javascript Tabanlı Web Uygulamaları, Zararlı Dosya Yükleme Saldırıları, CSRF, IDOR, Arka Kapı Oluşturma, Bilgi Toplama Yöntemleri, Web Zafiyet Tarama Araçları, Web Uygulama Güvenlik Duvarları, WAF/IPS/IDS Atlatma Teknikleri, Web Servisleri, LDAP Injection içeriği oluşturmaktadır.

GÜVENLİ YAZILIM GELİŞTİRME

Katılımcıların, güvenlik açıklarını bizzat yaşayarak öğrenmesi ve sonrasında bu zafiyetlere yol açmayan kod yazabilmesi amaçlanmaktadır.

Güvenli Yazılım Geliştirme Mimarisi ve Döngüsü, Tehdit Modelleme, Risk Nicelendirme, Doğrulama Eğilimi ve Şüpheci Yaklaşım, Temel Web Güvenlik Açıklarının Tanınması, Girdi Denetimleri, Kimlik Doğrulama / Yetkilendirme Farkı, İçerik İzolasyon Mantığı, Orijin Veraseti, Same-Origin Dışında Yaşam, İçerik Tanımlama Mekanizmaları, Belirsiz Kaynaklardan Gelen Kütüphaneler, OWASP-10, Beyaz Liste Yaklaşımının Uygulanması, ESAPI Mimarisi ve Yöntemleri, Prepared Statement / Paremeterized SQL Kullanımı, Object Relational Mapper, Güvenli Dosya Yükleme, Güvenli Kimlik Doğrulama, Güvenli CAPTCHA Kullanımı ve Bunu Atlatma ve Güvenli Oturum Yönetimi içeriği oluşturmaktadır.

www.olcsancad.com info@olcsancad.com T: +90 (212) 216 5080

ÖLÇSAN
"kalitenin ölçüsü"

SİBER_TR.03/2021