AEC Partners

AEC PARTNERS
TEKNİK ve İDARİ TEDBİRLER REHBERİ

İstanbul, 2020

AEC Partners

A. TEKNİK TEDBİRLER

Uyum süreci boyunca her bir veri sorumlusu nezdinde gerçekleştirilen yoğun çalışmalar kapsamında işin hukuki ve idari boyutu bir tarafa, sistem yöneticilerini ilgilendiren, teknik tedbirlerin alınması, kişisel verilerin güvenliğinin sağlanması da ciddi anlamda ele alınması gereken bir konu olarak karşımıza çıkmaktadır. Kişisel Verilerin Korunması Kanunu kapsam olarak, adından da anlaşılacağı üzere sadece "Kişisel Veri" ile sınırlıdır. Kişisel Verinin tanımı ise, Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Daha önce de belirtmiş olduğum üzere esasen yasal çerçevesi kanun ile belirlenmiş, başlı başına hukuki bir konudur. Kanun metninde "Veri" kelimesi geçiyor diye bu işin, sadece sistem yöneticilerine –bileşim uzmanlarına- yüklenmesi doğru bir yaklaşım değildir. İdari, hukuki ve teknik bakımdan uyumluluk gerektiren ve yönetilmesi gereken kritik bir süreçtir. Kurumlardaki işlenen verilerin büyük bir yüzdesinin elektronik ortamda bulunan dijital veri olduğunu varsayarsak, bileşim uzmanlarını da yakından ilgilendiren bir konudur. Sistem yöneticisi şirket nezdinde kurulacak komisyonun da doğal üyesi olmalıdır.

KVKK kapsamında yapılması gerekenler ise, hazırlanacak detaylı kişisel veri işleme envanteri teknik tedbirlerin tespiti açısından da önem arz etmektedir. Verinin niteliği, saklama alanı, işleme yöntemi tespit edilerek en uygun teknik tedbirlerin alınması gerekmektedir. Verilerin sınıflandırılması, Kişisel Verilerin İşlenmesi ve Korunması Prosedürünün hazırlanması ile birlikte bu dokümantasyonlar veri sorumlusuna yol haritası oluşturacaktır.

Sistem yöneticilerinin amacı, sadece kanunda bahsedilen kişisel verilerin güvenliğini sağlamak değil, dijital ortamda bulunan tüm kişisel, kurumsal ve ticari verilerin güvenliğini sağlamak olmalıdır. Buradan hareketle, tüm dijital verileri, bütünlük, gizlilik ve erişilebilirlik üçgeninde değerlendirerek, sistem yöneticilerine rehberlik edecek, bilgi güvenliği, yöntem, teknoloji ve uygulama pratiklerini ele alacağız. Veri sorumlusunun mevcut kaynakları yeterli ise ayrıca yatırıma ihtiyaç duymadan, KVKK için gerekli olan asgari teknik gereklilikleri sağlamış, aynı zamanda tüm verileri için de sürdürülebilir bir Bilgi Güvenliği Sistemi yapılandırmış olacaktır.

AEC Partners

1. SİSTEM YÖNETİMİ VE BİLGİ GÜVENLİĞİ:

1. SİSTEM YÖNETİMİ VE BİLGİ GÜVENLİĞİ:

Sistem yönetimi karmaşık bir iştir, genel prensip; merkezileştir, sadeleştir ve standartlaştır. Sanallaştırma sistemlerinin de bulut bilişimin de temel yaklaşımı budur. Dağıtık mimariler, genellikle sistem yönetimini zorlaştırır, hakimiyet alanını daraltır ve zafiyetler ortaya çıkabilir, fark edilmesi güçtür, veri kaybı ve sızıntısı kaçınılmazdır.Teknolojik gelişmelere paralel olarak her gün yeni ve farklı siber tehditler ve atak metotları ile karşılaşıyoruz. Siber tehditleri ve riskleri tamamen yok etmem mümkün olmamakla birlikte, önleyici tedbirler ile mevcut risklerin minimize edilmesi mümkündür. Siber ataklar, "genellikle dışarıdan içeriye yönlüdür" tezi artık geçerli değildir. İç networkteki bir aygıt, kullanıcı veya uygulama ile ataklar gerçekleştirilebilir. Örneğin; kullanıcının masum görünen bir linke yönlendirilmesi bilgi kaybına yol açabilir, tüm sisteme zarar verebilir. Özellikle, güvenlik duvarı, network ve uygulama açıkları yetkisiz kişilere davetiye çıkarabilir. Eskiden siber saldırıların amacı, zarar vermek veya sistemi çalışmaz hale getirmek iken, bugün, bilgi çalmak, yok etmek ve ticari menfaat elde etmektir. Saldırıları, bireysel tatmin, hobi ya da eğlence için gerçekleştirenler, günümüzde örgütlenerek profesyonelleştiler, daha bilinçli, daha sistematik ve global ölçekte ataklar yapabilmektedirler. Çevrimiçi herhangi bir cihazla, mail yolu ile veya Sosyal Medya hesapları ile böyle bir saldırıya maruz kalabilmek, KVKK kapsamında karşılaşılabilecek veri güvenliği risklerindendir.

Verinin bütünlüğü, gizliliği kadar erişilebilir olması da önemlidir. Ancak, erişilebilir bir verinin gizliliğinden söz edilebilmesi için, erişim yönetimi ve politikaları gereklidir. Yetkilendirme, veri gizliliğinin ana omurgasıdır, herkesin her veriye ulaşabilir olması durumunda veri güvenliği ve bütünlüğünden söz edilemez. Kaynaklara erişim, sınırlı, ölçülü ve kontrollü yapılmalıdır. Bunun için Erişim Yetkilendirme Matrisi oluşturulmalıdır.

Peki, kritik verileri hem erişilebilir hem de görünmez yapmak mümkün müdür? Evet mümkün, bu konuda birçok teknolojiden bahsedilebilir tabi, her sistem yöneticisi de farklı yöntem ve uygulama pratikleri geliştirmiştir. Tek bir cihaz, yazılım veya yöntem ile siber güvenliğin sağlanması mümkün değildir. Uçtan uca tüm sistemin güvenliği için, birçok yöntem ve tedbirler uygulanmalı, sürekli geliştirilmelidir. Kullanıcıların eğitimi ve farkındalığın artırılması gereklidir.
Uyumluluk sürecinde kurumların göz önünde bulundurması gereken konular:

Kurum bağlamının oluşturulması: Kurumsal bağlamı, ilgili tarafların ihtiyaç ve beklentilerini saptamak ve Bilgi Güvenliği Yönetimi Sisteminin("BGYS") kapsamını belirlemektir. Standart; uyumlu bir BGYS'nin oluşturulmasını, uygulanmasını, idame ettirilmesini ve sürekli olarak iyileştirilmesini şart koşmaktadır.

Yönetim: Üst düzey yönetici kadrosu belirlenen politikaların uygulanmasını zorunlu kılmak, bilgi güvenliği sorumluluk ve yetkilerini tahsis etmek gibi işlemleri sıkı tutarak BGYS'nin etkili yönetimini gerçekleştirmelidir.

Planlama: Bilgi güvenliği risklerinin etkili yönetimi için gerekli işlemlerin belirlenmesi, analizlerin yapılması ve süreçlerin planlanması; aynı zamanda BGYS'nin hedeflerinin açıklığa kavuşturulması gerekmektedir.

Destek: Yeterli kaynaklar ayrılmalı, farkındalık arttırılmalı, belgelendirme işlemi ve kontrolleri yapılmalıdır.

Operasyon: Risklerin belirlenip ele alınması, değişikliklerin yönetimi ve dokümantasyon gibi önemli işlemlerin daha ayrıntılı uygulanması gerekmektedir.

Performans değerlendirmesi: Bilgi güvenliği kontrollerinin, süreçlerinin ve yönetiminin izlenmesi, ölçülmesi, analiz edilmesi ve değerlendirme-denetleme-analiz adımlarının uygulanması, böylece gerektiği durumlarda sistematik iyileştirmenin yapılmasıdır.

İyileştirme: Denetleme ve gözden geçirme işlemlerinin bulgu ve sonuçlarını analiz ederek BGYS için sürekli bir düzeltme ve geliştirme süreci sağlamaktır.

AEC Partners

2. EN SIK ORTAYA ÇIKAN VERİ İHLALİ SEBEPLERİ

2019'da en sık ortaya çıkan veri ihlali sebepleri yanlış yapılandırılmış bulut depolama ortamları, korunmasız kod depoları, zafiyetli açık kaynak yazılımlarıdır.

A. Yanlış Yapılandırılmış Bulut Depolama

Birçok şirket verilerini depolamak için bulut sunucularını kullanmaktadır. Büyük avantajlarına rağmen, yanlış yapılandırılmış sunucular, bilgisayar korsanlarının kötü niyetli etkinlikleri için bir şirketin verilerini ele geçirmesi ve kullanması için ihlale yol açabilir. Herhangi bir yanlış yapılandırmada verileri halka açıklayan ve ilk olarak bu hatayı fark eden hackerler olacaktır. Yanlış Güvenlik Yapılandırmasının Açık Web Uygulama Güvenliği Projesi ("OWASP") İlk 10'da # 6 olması da önemli bir husus olduğunu göstermektedir. Neredeyse tüm büyük bulut ve IaaS sağlayıcıları yanlış konfigürasyondan oluşabilecek veri ihlallerinde suçu üzerine almamaktadır.

Yaygın Yapılan Yanlış Yapılandırmalar:

- Varsayılan sistem kimlik bilgilerinin kullanımı (kullanıcı adı / parolalar)
- Devre dışı bırakılmayan ve arama motorları aracılığıyla kolayca erişilebilen dizin ve dosya listeleri
- Bazı kullanıcı izleri, (hata mesajı olarak kullanıcılara döndürülen sayfalar çok fazla bilgiye sahip olabilmektedir.)
- Model uygulamaları, kullanılmayan yetkileri ve kullanıcı hesaplarını açık bırakmak, silmemek
- Güncel olmayan yazılımlar, eski sistemlerin kullanımı, güncel olmayan yamalar.

Yanlış Yapılandırılmış Verileri Önlemek İçin Basit Adımlar:

- Veri sorumlusunun kullandığı tüm 3. ve 4. taraf servis sağlayıcılarını ve bulut depolama sunucularını keşfetmesi,
- Bulut depolama sunucularının yanlış yapılandırılıp yapılandırılmadığını kontrol edilmesi,
- 3. ve 4. parti sağlayıcılarınızın siber riskinin izlenmesi,
- Saldırı Tespit Sistemi (IDS) günlüklerini düzenli olarak kontrol edilmesi ve ana bilgisayar düzeyindeki olayları incelemek için ağ tabanlı IDS yerine ana bilgisayar tabanlı IDS'nin göz önünde bulundurulması,
- Çalışanların siber güvenlik bilincinin arttırılması ve düzenli olarak sızan kimlik bilgilerinin kontrol edilmesi.

B. Korunmasız Kod Depoları

Açık kod depoları Ar-Ge'de verimliliği artırırken, aynı zamanda güvenlik açıklarını da gündeme getirmektedir. Saldırganlar, açık kaynak kodunun ne kadar yaygın kullanıldığının farkındadır. Kod için kimin katkıda bulunduğunu ve hangilerinin sorunlu olduğunu tespit etmek için bu kod depolarını izlemektedirler. Üçüncü taraflar, özellikle dış yazılım geliştiricileri, genellikle en zayıf halkadır. Bu geliştiriciler kodlarını gereğince korumak için gerekli eğitim ve güvenlik bilincinden yoksundur. Aynı anda birkaç projeye, zorlu teslim tarihlerine ve sabırsız müşterilere sahip olmaları nedeniyle, kodlarını kamuya açık alanlara bırakarak güvenliğin temellerini göz ardı ediyor veya unutuyorlar.

Korunma Yöntemleri:
-Şirket genelinde gizli ve kişisel verilerin yayınlanmadan önce kaldırılmasını veya yeniden düzenlenmesini sağlamak. Ek olarak, katılımcılar, genellikle yararlı istihbarat içerebileceği için ekran görüntülerini paylaşırken ya da herkese açık olan görüşlerini yayınlarken dikkatli olmalıdırlar.
- Yalnızca dâhili kullanım için depoların, kamu tüketimine uygun olanlara karşı uygun izinlerle yapılandırıldığından emin olmak için mevcut kod depo izinlerinin denetlenmesi veya gözden geçirilmesi düşünülmelidir.
- Daha sonra bir siber saldırıda yararlanılacak olan keşif aşaması sırasında tipik olarak maruz kalan verileri toplayacak olan istihbarat önderliğinde bir penetrasyon testi talep edin. Buna ve oluşturulan raporlara dayanarak, bunlara karşı daha iyi hazırlık yapmak ve bunları azaltmak için potansiyel saldırı ve tehditlerin daha iyi anlaşılması sağlanabilir.

C. Zafiyetli Açık Kaynak Yazılımlar
Açık Kaynak Kodlu Yazılımların ("OSS") kurumsal sistemlerde hızlı bir şekilde çoğalması, daha fazla bilinmeyen unsur ekleyerek siber tehdit ortamını genişletmektedir. OSS, kuruluşlar için para, geliştiriciler için zaman kazandırır, ancak aynı şekilde geniş bir eşzamanlı ve geniş ölçüde küçümsenmeyen risk yelpazesi sunar. OSS'ye yönelik kod güncellemeleri ve düzeltmeleri konusunda güncel kalınması önemlidir.

Açık Kaynaklı Yazılımların Güvenlik Riskleri ve Dikkat Edilmesi Gereken Güvenlik Açıkları:
- Açık kaynaklı projelerde kod herkes tarafından kullanılabilir. Bilgisayar korsanları bu bilgilere erişebilir ve zafiyeti bulanan açık kaynaklı uygulamaları kullanan ve yamalama konusuna önem göstermeyen kuruluşları takip edebilir.
- Açık kaynaklı bileşenler, bu projelerin standart ticari kontrolleri olmadığından fikri mülkiyet ihlali riskleri oluşturabilir.
- Açık kaynak bileşenleri kullanan bir işletmenin karşı karşıya olduğu önemli bir risk alanı örgütün operasyonel verimsizliğidir. Operasyonel açıdan ciddi bir endişe kaynağı, bir kuruluşun açık kaynaklı bileşenleri takip etmemesi ve bu bileşenleri yeni sürümlerle uyumlu olarak güncellememesidir.
- Açık kaynak kitaplıklardan kod kopyalayıp yapıştırma dâhil geliştiricinin yanlış uygulamasıdır. Kopyalama ve yapıştırma, geliştiricilerin proje kodunda yapabilecekleri tüm açıkları kopyaladıkları için sorunludur.

AEC Partners

3. VERİ GÜVENLİĞİ İÇİN YÖNTEM VE UYGULAMALAR

1 - Güvenlik duvarı yönetimi: Global ölçekte kendini kanıtlamış, Firewall tercih edilmesi ve güncel tutulması gerekmektedir. Wan to Lan erişimleri kapalı tutulmalıdır. Tüm kurallara,IDS(IntrusionDetectionSystems),IPS(Intrusion Prevention Systems), ATP(Advanced Threat Protection) diğer adıyla SANDBOX, SSL(Secure Sockets Layer), VPN(Virtual Private Network), Bootnet Filter, Antivirüs, AntiSpyware, Application Control, Content Filter vb. servisleri aktif edilebilir ve yapılandırılabilir. Kurum tarafından da belirtilen bu teknik tedbir bilgi güvenliğinin en önemli aşamalarından biridir.

2 - Ağ yönetimi: Network topoloji haritası oluşturulmalıdır. Network ağı optimize edilerek veri sorumlusunun kendi internet ağları oluşturulmalıdır. Tüm network erişimlerinde MAC Authentication uygulanması sağlıklı olacaktır. Serverlara ve uygulamalara erişim sınırlandırılarak sadece gerekli port ve servisleri açılmalı dışarıdan ve içeriden tüm uzaktan erişimler kapatılmalı, zorunlu ise IP bazında sınırlandırılmalıdır. Web Serverları için WAF(Web Application Firewall) ve SSL kullanılmalıdır. Sadece güvenli VPN ile, erişime kontrollü izin verilebilir. WiFi network için mümkünse Controller kullanılmalı ve misafir ağı ayrı yapılandırılması sağlıklı olacaktır.

3 - Kimlik doğrulama ve erişim yönetimi: AD(Active Directory) yapısı kurularak ve diğer uygulamalarla entegre edilerek kimlik doğrulama ve erişim kontrolü tek merkezde yönetilebilecektir. Admin hesapları değiştirilerek komplike şifreler oluşturulmalıdır. DC(Domain Controller) Server'a erişimi engellemelidir. Mutlaka ADC(Additional Domain Controller) yapılandırılmalıdır. Misafir Wifi ağlarınız için mutlaka kimlik doğrulama sistemi kullanılmalıdır. Radius, hotspot vb. Network ve internet erişimleri için Erişim Politikaları uygulanabilecektir. Kimliği doğrulanmayan bilgisayar, cihaz, aygıt, kullanıcı vb. networke sokulmamalıdır. İnternet erişimleri sınırlanmalı ve filtrelenmelidir, kurallarda asla any/any kullanmamalıdır.

Patch yönetimi için ayrı bir Server yapılandırılmalı ve tüm sistemlere dağıtılmalıdır. Microsoft sistemleri için ücretsiz sunulan WUS(Windows Update Service) kullanılabilecektir.

4 - File Server dosya yönetimi: Eğer doküman yönetim sistemi yoksa, veri sorumlusu, Microsoft File Server ile dosyaları sınıflandırıp, ortak klasörlere koyarak, tüm dosyaları bir merkezde yönetebilir ve yedekleyebilir. Bunun için, ayrı bir File Server yapılandırabilir, Şirket, Departman ve Pozisyon bazında klasörler oluşturup ve yetkilendirmeler yapılabilir. Tüm kullanıcıların kişisel, kurumsal ve ticari verilerini bu klasörlerde barındırması konusunda politikalar oluşturulmalıdır. KVKK ile ilgili kişisel verilerin hangi klasörlerde saklanacağı ve kimlerin erişebileceği konusunda Klasör Matrisi ve Yetkilendirme Matrisi oluşturulmalıdır. Ortak klasörler haricinde ayrıca, File Server Folder Redirection servisi yapılandırılmalı ve tüm kullanıcılar için uygulanmalıdır. Uzaktan erişimler için mutlaka VPN kullanılmalı böylece olası ihlallerin önüne geçilmelidir. Kullanıcılar çevrimdışı çalışabilecek ve Networke bağlandığı an senkronize olacaktır. Bilgisayarların arızalanması, kaybolması veya dosyaların silinmesi durumunda her zaman bir kopyası veri sorumlusunun yedeklerinde olacaktır. Bu sayede tüm dosyalarınızı sınıflandırmış, yetkilendirmiş ve tek merkezde toplanmış olacaktır. Kişisel veriler için, DLP kuralları oluşturulabilir. Örneğin; İçerisinde T.C. Kimlik Numarası geçen dosyalar kaydedilemesin veya başka klasöre yönlendirilebilsin vb. erişim, yedekleme, imha etme vb. işlemlerinizi kolayca yapılabilecektir. Kritik veriler için, Disk Encryption şifrelemeyöntemi kullanılabilir. Disk Encryption, uygulama zorlukları ve sistem kaynakları kullanımı bakımından dezavantajları olsa da verilerinizi yetkisiz kişilere karşı koruyan bir teknolojidir.

5 - Kurumsal Mail yönetimi: Mail sistemleri hem kurumlar hem de KVKK için çok önemlidir. Kişisel, kurumsal ve ticari verilerin büyük bölümü mail sisteminde işlenir. Global ölçekte kendini kanıtlamış, lisanslı, destek sağlanan ve stabil çalışan Kurumsal Mail sistemleri tercih edilmesi sağlıklı olacaktır.Mail Sistemi, mutlaka spam mail ve kötü amaçlı yazılım güvenlik sistemlerine sahip olmalıdır. Arşivleme veya yedekleme özelliği olmalıdır. Kurallar oluşturulmasına olanak sağlamalı ve yönetilebilmelidir.
KVKK için, veri sorumlusu tarafından kurallar oluşturulabilir. Örneğin, tüm kullanıcıların posta kutularındaki, içerisinde CV geçen mailleri cv@sirketadi.com mail hesabına yönlendirilmesini sağlayabilir, böylece kişisel veriler bir merkezde toplanabilir. DLP sisteminde de kişisel veri içeren mailler için kurallar oluşturulabilir.

6 - Yedekleme ve Felaket Yönetimi: Sistem yöneticileri için, yedekleme her zaman hayat kurtarır. Tüm sistemler için mutlaka yedekleme planlarınız olmalıdır. Bu planları yaparken 3-2-1 kuralına uyumlu yapılmalıdır:

Kural-1: *Verilerin en az 3 kopyası olmalıdır,*
Kural-2: *Bu kopyalar en az 2 farklı ortamda depolanmalıdır,*
Kural-3: *Bir yedek kopyası mutlaka farklı lokasyonda tutulmalıdır.*

Yedekleme cihazları (Storage, NAS, Teyp vb.) mutlaka ayrı VLAN'da olmalı ve erişim sınırlı olmalıdır. Fiziki ve Sanal Serverların image, clone yöntemi ile yedeklenmesi en yaygın yöntemdir.
Global olarak kendisini kanıtlamış, lisanslı, destek sağlanan bir Kurumsal Yedekleme sistemi kullanılması faydalı olacaktır. Tüm yedekler için, belirli periyotlarda restore/recovery testi yapılmalıdır. Uzak lokasyonlardaki dağıtık verilerin yedeklenmesi her zaman daha güçtür. Verilerin sınıflandırılması ve merkezileştirilmesi bu bakımdan çok önemlidir.
Felaket Yönetimi ve İş Sürekliliği için mutlaka, felakey yönetimi planı yapılmalıdır. Veri sorumlusunun ihtiyaçlarına göre kritik server ve veriler baz alınarak Felaket ve Kurtarma planı yapılabilir. Son yıllarda, bulut sistemlerin yaygınlaşması ve maliyetlerinin düşmesi ile daha kolay ve daha az bütçe ile felaket planları oluşturulabilir. Kritik server ve veriler veri merkezlerinde konumlandırılacak bir server ve/veya kiralanacak bir server'a replike edilebilir. Replikasyon server ve verilerinizin kritiklik durumuna göre farklı şekillerde konumlandırılabilir.

7 - Uç nokta yönetimi: Lisanslı yazılım kullanılmalı ve güncel tutulmalıdır. Tüm müşteriler "kullanıcı" yapılmalıdır. Sistem yönetici dışında uygulama kurulması/kaldırılması engellenmelidir. Veri güvenliği ve sızıntısına karşı, USB, DVD, SD, Bluetooth vb. aygıtları ve boot aygıtları da engellenmelidir.
Taşınabilir cihazlar için kurallar oluşturulmalı network dışında da aktif olmalıdır. « Veri Kayıp Önleme » (Data Loss Prevention) sistemi kurularak ve gerekli kuralları yapılandırılmalıdır. Veri sızıntılarını önlemenin en önemli adımıdır. Sınıflandırılmış veriler için erişim, paylaşım ve silme politikaları oluşturulmalı ve bu veriler loglanmalıdır.

8 - SIEM ve LOG yönetimi: Log toplama, log yönetimi ve analizi, bilgi güvenliği için olmazsa olmazdır. KVKK, 5651 yasa ve ISO27001 standartları çerçevesinde tüm sistemlerdeki erişim kayıtlarının tutulması bir zorunluluktur. Log kayıtlarının HASH yöntemi ile imzalanarak, değiştirilemez olduğu garanti altına alınmalıdır. Log kayıtları güvenli alanlarda, yasalarda belirlenen süreler kadar saklanmalıdır ve erişim sınırlı olmalıdır.
SIEM(Security Information and Event Management) SIEM gerçek zamanlı olarak, tüm sistemlerin ürettiği logları merkezi olarak toplayan, saklayan ve analiz eden bir sistemdir. SIEM Sistemleri, Log analizlerine göre daha detaylı yapılandırma ve raporlama özelliğine sahiptir.

SIEM belirlenen politika ve kurallar ile olaylar arasında anlamlı ilişki kurar ve korelasyon tekniği ile muhtemel saldırılara yönelik alarmlar üretir, tehditleri önlemeye yardımcı olur. Global ölçekte kendini kanıtlamış, destek sağlanan ve stabil olan bir SIEM ürününe sahip olunması veri sorumlusu açısından sağlıklı olacaktır. Veri sorumlusunun yapısına göre gerekli kuralları, korelasyonları ve alarmları yapılandırılmalıdır. Bazı SIEM ürünleri açık tarama servisleri de içermektedir. Ancak belirli periyotlarda, uzman firmalar ile Penetrasyon(Sızma) testi yapılması ve açık tarama raporları alınması önemlidir.

9 - IT varlıkları yönetimi: Bilgi teknolojileri fiziki varlıkların takip edilmesi ve yönetilmesi için, mutlaka IT Envanteri çıkartılmalı ve yönetilmelidir. Tüm cihaz ve aygıtları, kullanıcılara zimmetleyerek gerekli idari tedbirler alınmalıdır.
Sistem Odası(Veri Merkezi), korunaklı bir alanda konumlandırılmalı ve mutlaka ISO27001 standartlarına göre yapılandırılmalıdır. Özellikle soğutma, yangın, su baskını, sarsıntı, nem vb. alarm sistemleri kurulmalıdır. Güvenlik kamerası ile 7/24 izlenmeli. Sistem odası giriş/çıkışlarının kontrollü yapılması sağlanmalıdır. İzinsiz girişler engellenmelidir. Kritik Server ve cihazlar işaretlenmelidir.

10 - IT Strateji, Politika ve Prosedürler: Kurumsal stratejileri destekleyici, bilgi teknolojileri stratejisi oluşturulmalı ve uygulanmalıdır.. Kurumsal ihtiyaçlar ve gelecekteki dijital dönüşüm projelerinizi de kapsayacak, Bilgi Teknolojileri Yönetimi Politikaları oluşturulmalıdır. BT süreçleri ve iş akışları hazırlanmalı ve süreç bazında Risk Analizi yapılmalıdır.
Kişisel Veri İşleme Envanteri, Kişisel Verilerin İşlenmesi ve Korunması politikası, Bilgi Güvenliği Politikası, Sistem Erişim ve Yetkilendirme Matrisi, Bilgi Teknolojileri Yönetim Prosedürü, diğer yasal metinler vb. dokümantasyonları oluşturulmalı varsa ISO sistemleriniz ile entegre edilmelidir.
Kişisel veriler için, erişim, elde etme, işleme, imha etme ve aktarma operasyonları için tüm ilgili pozisyonları, Kişisel Veri İşleme Envanterine göre yetkilendirilmelidir.

11 - Sertifikasyon ve Standardizasyonlar: Veri sorumlusunun ISO/IEC 27001 standardizasyonu gibi uluslararası kabul gören sertifikalandırma süreçlerinden geçmesi alınabilecek teknik tedbirlere örnek olarak verilebilir. Örneğin ISO/IEC 27001 standardizasyonu kurumların bilgi varlıklarının risk düzeyini tanımlamak, analiz etmek ve ele almak gibi adımlardan oluşan bir bilgi güvenliği yönetim sistemi olarak tanımlanmaktadır. Bu kapsamda söz konusu standardizasyon risklerin sistematik bir şekilde tanımlanıp yönetilmesi, bilgi güvenliği uygulamalarının bağımsız bir şekilde gözden geçirilmesi, güvenli bilginin olanaklı kılınması için bütüncül ve risk tabanlı bir yaklaşım sunması, paydaşların güvenini kazanmayı sağlaması, uluslararası düzeyde kabul edilmiş kriterlere göre güvenlik seviyesinin tespiti, sertifikalandırmanın bir defa gerçekleştirilip küresel düzeyde kabul görmesi gibi avantajlar sağlayarak veri güvenliğinin temininde önemli bir rol oynayacak aynı zamanda kurumsal güvenilirliği ve itibarı da arttıracaktır.

4. KURUL TARAFINDAN YAYIMLANAN TEKNİK TEDBİRLER

Kurum tarafından yayımlanan Veri Güvenliği Rehberinde veri sorumlularınca alınabilecek idari ve teknik tedbirler belirtilmiştir. Aynı zamanda VERBİS'e bildirim yaparken de alınan idari ve teknik tedbirlerin belirtilmesi gerekmekte olup VERBİS ekranında yer alan idari ve teknik tedbirler listesinden de faydalanılabilmesi mümkündür. Kurum tarafından yayımlanan teknik tedbirler aşağıda belirtilmiştir:

- Ağ güvenliği ve uygulama güvenliği sağlanması
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılması
- Anahtar yönetimi uygulanması
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik - önlemleri alınması

Bulutta depolanan kişisel verilerin güvenliği sağlanması

- Çalışanlar için yetki matrisi oluşturulması
- Erişim loglarının düzenli olarak tutulması
- Gerektiğinde veri maskeleme önlemi uygulanması
- Güncel anti-virüs sistemlerinin kullanılması
- Güvenlik duvarlarının kullanılması
- Kişisel veri güvenliği sorunlarının hızlı bir şekilde raporlanması
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemlerinin alınması
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanması ve bunların takibinin yapılması
- Log kayıtlarının kullanıcı müdahalesi olmayacak şekilde tutulması
- Özel nitelikli kişisel verilerin elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmesi.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılması ve farklı birimlerce yönetilmesi
- Saldırı tespit ve önleme sistemlerinin kullanılması
- Sızma testi uygulanması
- Siber güvenlik önlemlerinin alınarak uygulanmasının sürekli takip edilmesi
- Şifreleme yapılması
- Veri kaybı önleme yazılımlarının kullanılması ve kişisel verilerin düzenli olarak yedeklenmesi

B. İDARİ TEDBİRLER

KİŞİSEL VERİLERİN KORUNMASI İÇİN İDARİ TEDBİRLER

Kanunun 12 nci maddesinin birinci fıkrasında;
"Veri sorumlusu;
a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c) Kişisel verilerin muhafazasını sağlamak
amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmü yer almaktadır.

Bu kapsamda, şirket sahipleri, bölüm yöneticileri ve çalışanlarının dijital, fiziksel ve benzer tüm ticari işlemlerinde 6689 sayılı KVK Kanunun yükümlülüklerine uyum gösterecek tedbirler alınması, alınan tedbirlerin uygulanmasını sağlamları gerekmektedir.
Bu tedbirlerin alınması her ne kadar yüksek maliyetler doğurduğu düşünülse de düşük maliyet ve sıkı denetimler sayesinde kolayca uygulanabilir hale dönüştürülebilir.
İdari tedbirler açısından kritik olanları sıralamak gerekirse;
- Kişisel verilerin hukuka aykırı olarak işlenmesinin önleyici tedbirlerin alınması,
- Kişisel verilere hukuka aykırı olarak erişilmesinin önüne geçilmesi,
- Kişisel verilerin muhafazasının sağlanması,
- Bireylerin temel hak ve özgürlüklerinin korunması için gereken özeni göstermek,

olarak sıralanabilir.

İdari Tedbirlerin Uygulamalarını Özetlemek Gerekirse ;
- Kurum İçi Departman Toplantıları Yapılarak Risk Analizlerinin Hazırlanması
- Kişisel Veri İşleme Envanteri Hazırlanması
- Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
- Sözleşmeler (Veri Sorumlusu – Veri Sorumlusu, Veri Sorumlusu – Veri İşleyen Arasında)
- Gizlilik Taahhütnameleri
- Kurum İçi Periyodik ve/veya Rastgele Denetimler Yapılması
- İş Sözleşmelerinin ve Disiplin Yönetmeliği Değişikliklerinin Yapılması (Kanuna Uygun Hükümler İlave Edilmesi)
- Kurumsal İletişim Yönetimi (Acil Durum Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme, İtibar Yönetimi vb.)
- Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanuna Uyum)
- Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

sağlanması olarak sıralanabilir.

1. RİSK ANALİZİ

(Mevcut Risk ve Tehditlerin Belirlenmesi)

Kişisel Verilerin Korunması Kanunu Uyum Süreci Yönünden İdari Tedbirler Kapsamında Şirketler Neler Yapmalıdır?

1. RİSK ANALİZİ – (Mevcut Risk ve Tehditlerin Belirlenmesi)

Veri Sorumlusu, bünyesinde kullanılan tüm verilerin departman bazında analiz edilerek, ne kadar kişisel veri kullanıldığının tespit edilmesini sağlamalıdır. Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir.

Bu riskler belirlenirken;

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,
- İçeriği gereği hangi derecede gizlilik seviyesi gerektirdiği,
- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.

Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri;

- Maliyet,
- Uygulanabilirlik,
- Yararlılık,

ilkeleri doğrultusunda değerlendirilmeli, gerekli idari tedbirler planlanarak uygulamaya konulmalıdır.

2. ÇALIŞANLARIN EĞİTİLMESİ VE FARKINDALIK ÇALIŞMALARI

2. ÇALIŞANLARIN EĞİTİLMESİ VE FARKINDALIK ÇALIŞMALARI

Dijitalleşme şirketlerin veri güvenliğine yapılacak saldırıları da beraberinde getirmektedir. Pazarlama faaliyetlerinde kişisel verilerin kaynak olarak kullanıldığı günümüzde, teknolojiye karşı geliştirilen siber saldırılarla tehdit altında kalan dijital kişisel verilerin güvenliğinin sağlanması konusunda, çalışanlara eğitimler verilerek, sınırlı olsa dahi ilk müdahaleyi yapmaları, kişisel veri güvenliğinin sağlanması konusunda büyük önem taşımaktadır.

Kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular başlıca kişisel veri güvenliği ihlallerindendir. Bu ihlaller, kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerinin kullanılması suretiyle kötü amaçlı yazılım içeren elektronik posta ekinin açılması veya elektronik postanın yanlış alıcıya gönderilerek kişisel verilerin üçüncü kişilerin erişimine açılması şeklinde de ortaya çıkabilmektedir. Verilecek **farkındalık eğitimlerinde** elektronik haberleşme kaynaklarının risklerinin neler olduğu, bu riskleri en aza indirgenmesi için basit anlaşılır paylaşımlar ve düzenli periyodik paylaşımlar yapılması önemlidir. Veri Sorumluları bu paylaşım ve eğitimleri kayıt altına alarak somutlaştırıp fiziki olarak da saklamalıdır.

Sosyal medya ve diğer tüm dijital platformlarda çalışanlara kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim verilmesi, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.

Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumluluklarının, sözlü ve yazılı olarak görev tanımlarında belirlenmesi ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanması bu kapsamdaki idari faaliyetlerini yürütürken etkinliğin artmasını sağlayacaktır.

Ayrıca kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken, kişisel veri paylaşımı yapmanın kanuna uyumlu şekilde olması gerektiği ilkesi ve her türlü risk içeren işlemlerde mutlaka **"risk almadan sor- öğren- uygula"** prensibine uygun hareket edilmesine dikkat edilmelidir.

Öte yandan, kişisel veri içeren alanlarda çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik anlaşmalarını imzalamaları istenmesi önemlidir. Çalışanların güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir yazılı disiplin süreci de mutlaka olmalıdır. Disiplin süreçlerinin aralıklı dönemlerde yapılan eksik-hatalı işlemlerin tespitleri ve sonuçlarının ilan edilerek duyurulması da etkili bir idari uygulama örneği olacaktır.

Kişisel veri güvenliğine ilişkin politika ve prosedürlerde önemli değişikliklerin meydana gelmesi halinde; yapılacak yeni eğitimlerle bu değişikliklerin, çalışanlarla düzenli şekilde paylaşılması ve kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerinin güncel tutulmasının sağlanması gerekmektedir.

3. KİŞİSEL VERİ GÜVENLİĞİ POLİTİKALARININ VE PROSEDÜRLERİNİN BELİRLENMESİ

3. KİŞİSEL VERİ GÜVENLİĞİ POLİTİKALARININ VE PROSEDÜRLERİNİN BELİRLENMESİ

Veri Sorumluları tarafından Kişisel veri güvenliğine ilişkin politikaların hazırlanması, bu kapsamdaki risklerin belirlenmesini ve önlem alınmasını sağlayacaktır.

Kişisel veri güvenliğine ilişkin belirlenecek gerçekçi ve istikrarlı politika ve prosedürler, veri sorumlusunun iş yapış biçimine uygun şekilde adapte edilmelidir. Kişisel veri güvenlik seviyesi, politika ve prosedürlerin uygun şekilde hazırlanmamasından kaynaklanan sorunlar nedeniyle yeteri kadar sağlanamamaktadır.

Bu kapsamda alınacak tedbirlerin önceden belirlendiği örnek vaka çalışmalarının göz önünde bulundurularak hazırlanan uygulama politikaları, çalışanlar üzerinde ortaya çıkabilecek baskıyı azaltacaktır.

Veri sorumlularının, veri kayıt sistemlerinde hangi kişisel verilerin bulunduğundan ve mevcut güvenlik önlemlerini inceleyerek diğer yasal yükümlülüklerle uyumlu hareket edildiğinden emin olması gerekmektedir.

Politika ve prosedürler kapsamında; düzenli olarak kontroller yapılmalı, yapılan kontroller kayıt altına alınarak belgelendirilmelidir. Geliştirilmesi gereken hususlar periyodik kontrollerle tespit edilmeli ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilmelidir.
Ayrıca, her kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenerek kayıt altına alınmalıdır.

4. KİŞİSEL VERİLERİN MÜMKÜN OLDUĞUNCA AZALTILMASI

4. KİŞİSEL VERİLERİN MÜMKÜN OLDUĞUNCA AZALTILMASI

6698 KVK Kanunun 4 üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri uyarınca "kişisel veriler, gerektiğinde doğru ve güncel olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir."şeklindedir.
Her ne kadar kanun bu konuyu "gerekli olan süre kadar muhafaza edilmelidir" şeklinde belirtmiş olsa da , özellikle uzun süredir faaliyet gösteren veri sorumluları, çok fazla miktarda kişisel veri toplamakta olduğundan söz konusu kişisel verilerin bir kısmı zamanla doğru olmayan, güncelliğini yitirmiş ve herhangi bir amaca hizmet etmeyen veriler haline gelebilmektedir.

Bunun önüne geçebilmek için, Veri Sorumlularınca ;
- İşleme amaçları bakımından anılan kişisel verilere hala ihtiyaç duyuluyor mu?
- Kişisel verilerin doğru yerde muhafaza edilip, yeterli güvenliği sağlanıyor mu?

sorularını kendilerine sormalı ve risklerini de göz önünde bulundurarak, buna göre aksiyon almalıdırlar.

Ayrıca;

Fiziki, Dijital ortamlardaki, yetkisiz erişimin önüne geçilebilmesi için kişisel veri işleme amaçlarına uygun olmasına rağmen, veri sorumlularının sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel verilerin, daha güvenli ortamlarda muhafaza edilmesi tavsiye edilmekte ve ihtiyaç duyulmayan kişisel verilerin ise kişisel veri saklama ve imha politikası ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine uygun ve güvenli bir şekilde imha edilmesi gerekmektedir.

5. VERİ İŞLEYENLER İLE İLİŞKİLERİN YÖNETİMİ

5. VERİ İŞLEYENLER İLE İLİŞKİLERİN YÖNETİMİ

Kişisel Verilerin Korunması Kanunun 12 nci maddesinin ikinci fıkrası gereği "veri işleyenler de kişisel verilerin güvenliğinin sağlanması konusunda veri sorumlusuyla müştereken sorumludur" der.

Bazı veri sorumluları, bilgi teknolojileri ihtiyaçlarını karşılamak için veri işleyenlerden hizmet alarak ihtiyaçlarını karşılamaktadırlar. Veri sorumlularının, hizmet alırken söz konusu veri işleyenlerin kişisel veriler konusunda gerekli veri güvenliğinin sağlama standartlarını sorgulayarak, aralarında imzaladıkları sözleşmelerinde bu konuya yer vermelidirler.

Belirtiler sözleşmelerin;

- Veri işleyen ile imzalanan sözleşmenin yazılı olması,
- KVKK mevzuatına uyumlu olması
- Veri imha ve saklama politikası prosedürlerine uygun olması
- Veri işleyenin, işlediği kişisel verilere ilişkin olarak süresiz sır saklama yükümlülüğüne tabi olacağının yazılı olması,
- Herhangi bir veri ihlali olması durumunda, veri işleyenin bu durumu derhal veri sorumlusuna bildirmekle yükümlü olduğunun yazılı olması
- Veri sorumlusu, kişisel veri içeren sistem üzerinde gerekli denetimleri yapar veya yaptırır, denetim sonucunda ortaya çıkan raporları ve hizmet sağlayıcıyı yerinde inceleyebilir hükmünün sözleşmede yazılı olması,

Risklerin minimize edilmesi açısından önem taşımaktadır.

KAYNAKÇA ; KVKK Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)

AEC Partners

AEC PARTNERS
TEKNİK ve İDARİ TEDBİRLER REHBERİ

AEC Partners İletişim Bilgileri

Adres: Yeni Yol Caddesi No:3
Nurol Tower Kat:10 D:1009
Şişli/İstanbul
Telefon: 0 (212) 234 9728
E-Posta: kvkk@aecdanismanlik.com
İnternet Sayfası: www.aecdanismanlik.com