

Bilgi Güvenliđi Çerçevesi

Bulutta yazılım hizmetlerimizi müşterilerimize, güvenli ve sürdürülebilir hizmet seviyelerinde sunuyoruz. Yazılım hizmetlerinin güvenliđini, bulut veri merkezleri ile birlikte bütünleşik mimaride, uçtan uca sağlıyoruz.

Risk analizleri neticesinde hazırlanan güvenlik mimarimiz, sertifikalandırılmış bir disiplin ve yaşam döngüsüne sahiptir. Kişisel Verilerin Korunması (KVKK & GDPR) ve diğer mevzuatlara uyum için tanımlı süreçlerimiz kapsamında doğrulama, veri koruma, izleme ve iş sürekliliđi metodolojilerini işletiyoruz. Kalite güvencesi için tüm süreçlerimizi periyodik olarak gözden geçiriyor ve yeniliyoruz.

Bulut Hizmetlerinde Güvenlik Yaklaşımı

Birlikte çalıştığımız bulut veri merkezlerinin, servis ve hizmet altyapılarına erişim süreçleri, Next4biz tarafından periyodik olarak gözden geçirilmektedir. Hizmet sağlayıcılar, kendi bilgi güvenliđi yaşam döngüsü içinde uyguladıkları metodolojiler ile süreçlerini işletmekte ve kurumumuz tarafından izlenerek, düzenli olarak raporlama yapmaktadırlar.

Hizmet sağladığımız alanda, en çok önemsemiğimiz konu, bulut modelinde tüm hizmetlerin küresel güvenlik ve uyumluluk sertifikasyonlarına tabi tutulmasıdır. Bu yaklaşım, bulut bilişim hizmetini alan müşterilerimizin global süreçlere uyumluluğunun desteklenmesini hedefler.

Bulut veri merkezleri, kendi sistemleri üzerinde bağımsız güvenlik testlerini gerçekleştirmektedir. Veri merkezlerindeki katmanlı mimarileri ile gerek ISO, gerek Uptime'ın standartları geređi planlı saldırılar ve doğal afetlere karşı en yüksek seviyede korunmaktadırlar. İleri teknolojiye sahip sanallaştırma mekanizmaları ile yönetilmekte, geri döndürme süreçlerini bağımsız uygulamalarla sağlamaktadırlar.

Hizmet sağlayıcılarımız, doğal afet (yangın, sel, deprem, vb.) ve planlı saldırılara (terör eylemleri, hırsızlık girişimleri, vb.) karşı gerekli fiziksel önlemleri almış durumdadır.

Cluster (failover) mimarisi ve TIER III standardına sahip bulut hizmetleri üzerinden verdiğimiz SaaS hizmetlerimiz, CSP desteği ile paylaşımlı güvenlik duvarı altyapısına sahiptirler.

Hizmet sağlayıcılarımızda, yük dağıtıcı/dengeleyici özelliklere sahip ve esnek sunucuları ile veri merkezleri ve olağanüstü durum merkezleri konuşlandırılmış ve yapılandırılmıştır. Aynı doğal afetten etkilenmeyen lokasyonda aktif-pasif çalışabilecek şekilde kurgulanmış süreklilik sağlayan topolojiye sahiptirler.

Bulut Bilişim hizmeti için coğrafi sınırları sözleşmede belirlenmiş yedekli "hosting" seçenekleri sunmaktadırlar. NTP (Ağ Zaman Protokolü) kullanılır ve Next4biz tarafından izlenir durumdadır.

Next4biz Bilgi Güvenliği Temel Prensipleri

Yönetişim

Bilgi sistemleri ve bilgi güvenliği çerçevesinin yönetim ve yaşam döngüsünden "Bilgi Güvenliği, Teknoloji ve Yönlendirme" komitesi sorumludur. Komite gerekli kontrolleri planlamakta, her çeyrek dönemde veya ara dönemlerde ihtiyaç duyulması halinde daha kısa periyotlarla bir araya gelmektedir. Şirket topolojisi, güvenlik altyapısı ve üretim gelişimi planlamakta ve izlemektedir.

Next4biz'de, öne çıkan güvenlik yaşam döngüleri; **SDL** (Secure Development Lifecycle) olarak tanımlanan güvenli yazılım geliştirme, güvenli erişim metodolojisi ve denetim mekanizması olarak tanımlanan; **OSA** (Operational Security Assurance)'dır.

Bilgi Güvenliği Yönetişimi (Information Security Governance)

Müşterilerimize ait bilgilerin gizliliğini korumak azami öneme sahiptir. Bilgi güvenliği risklerini azaltmak için gerekli donanım, yazılım, eğitim, farkındalığın sağlanması temel hedefimizdir. Bu hedefe ulaşmak amacıyla gerekli kontrollerin tesisi ve kaynakların tedariki, yönetişimde öncelikli prensibimizdir.

Edindiğimiz sertifikalar ile belgelendiği üzere;

(ISO 27001, ISO 27701, ISO22301, ISO 9001, ISO 10002, BS 10012) tüm çalışanlarımızın ve iş ortaklarımızın; bilgi güvenliğinin bütünsel yaklaşımı olan BGYS (Bilgi Güvenliği Yönetim Sistemi)'ne katılımını sağlamayı hedefler. Bu amaçla eğitim ve farkındalıkla beraber, BGYS'nin verimliliğini, iç ve dış denetimlerle kontrol etmek, izlemek, gözden geçirmek ve iyileştirmek yaşam döngümüzün temel aşamalarıdır.

Next4biz, gerek kendi mimarisi, gerekse iş ortaklarımızın bağlı oldukları yasal ve sözleşmelerden kaynaklı; işledikleri, sakladıkları, yönettikleri bilgi ve bilgi varlıklarının, sorumlulukları kapsam ve sınırlarında, gizliliğini, bütünlüğünü ve erişilebilirliğini korumaktadır.

ISO/IEC 27001 Bilgi güvenliği standardı ile risk odaklı yaklaşım hedeflenir. Kuruluşların, bu süreçlerinde bilgi ve bilgi varlıklarının korunması için doğru planlanmış insan kaynağı yaklaşımı şarttır. Kurumumuzda, prosedürler ve bilgi teknolojileri altyapıları ile hedeflenen güvenlik düzeyi bu disiplinle sağlanmaktadır.

Güvenlik izleme mimarisi, bileşenlerin konuşlandırıldığı, alarmların izlendiği (SOC, WAF, iç izlemeler vb.) yapı ile desteklenmektedir.

Ürün Geliştirme Süreçleri

Ürün geliştirme süreçlerimiz sürdürülebilir mimaride tanımlıdır. Analiz, kodlama ve testler için süreçler tanımlı ve UAT (Kullanıcı Kabul Testleri) ve geliştirici birim testleri için gerekli adımlar tesis edilmiştir.

Penetrasyon testi ve kaynak kod analizi, üçüncü taraf bilgi güvenliği uzmanları tarafından uygulanır.

Uygulama ve arayüzler ilgili endüstriyel standartlara (web uygulamaları için OWASP) göre tasarlanmakta, geliştirilmekte, konumlandırılmaktadır.

Müşteri memnuniyeti seviyesini arttırmak için kalite güvence süreçleri hassas bir şekilde ele alınmaktadır. Tüm prosedürler ve işlemler tanımlanmıştır.

Sisteme Erişim ve Görevler Ayrılığı

Görevler ayrılığı prensibi gereğince, kimlik doğrulama matrisleri oluşturulmuştur. Erişim, 2. bölümde tanımlanan Komite tarafından kontrol edilir ve gözden geçirilir. Tanımlanan tüm prosedürler ve işlemler aynı zamanda ilgili ve değişen şartlar nedeniyle gözden geçirilir ve güncellenir.

Kimlik, Log Yönetimi ve Yedekleme İşlemleri

Uygulama düzeyinde doğrulama, sistem erişim doğrulama işlemleri tanımlanmış ve çalıştırılabilir durumdadır. Tüm log kayıtları izlenebilir ve korumalıdır.

Yedekleme prosedürleri ve kurtarma işlemleri, RTO'lar (*) tanımlıdır.

Yönetişim ve Kimlik Doğrulama

Değişiklik yönetimlerimiz, problem ve sorun giderme metodolojilerimiz olgunluk seviyesi yüksek şekilde konuşlandırılmış, tanımlı, uygulanan ve izlenen mimaridedir.

Next4biz faaliyetleri kapsamında, hukuka uygun bir biçimde kişisel veri işleme faaliyetleri yürütülmektedir. Bu çerçevesinde, veri sorumlusu olarak müşterileri, çalışanları ve ilişki içinde olduğu diğer gerçek kişilere ait kişisel verilerin korunması, büyük önem arz etmektedir. Kişisel verilerin işlenmesi ve korunması süreçleri için yazılı politikalar ile yönetilen süreçlerle tanımlıdır. Müşterilerimizin, potansiyel müşterilerimizin, çalışanlarımızın, çalışan adaylarımızın, ziyaretçilerimizin, işbirliği içinde olduğumuz kurum çalışanlarımızın kişisel verilerinin hukuka uygun biçimde işlenmesi ve korunması hedeflenmektedir.

Bu kapsamda, 6698 sayılı Kanun ve ilgili mevzuat gereğince kişisel verilerin işlenmesi ve korunması için Next4biz tarafından gereken idari ve teknik tedbirler alınmaktadır.

Bilgi sistemlerine erişim izni verilmeden önce, tanımlanmış güvenlik, sözleşme şartı ve tabi olunan düzenlemelerin getirdiği şartlar gözetilmektedir.

Veri tabanları erişim ve yetkilendirme standartları tanımlı ve uygulanır durumdadır. Her türlü kontrol ve istisnai durumlar tanımlı komiteler tarafından gözden geçirilmekte ve izlenmektedir.

Erişim ve Yetkilendirme

Kullanıcı şifreleri belirli kurallara göre verilmektedir. Şifre uzunluğu, karakter tekrarı vb. kontrol edilmektedir. Ayrıca admin tarafından belirlenen periyotlarda şifrelerin yenilenmesi gerekmektedir.

Kullanıcı bilgileri veri tabanına named userlar ile erişim sağlanmakta ve loglanmaktadır. Kullanıcı bilgileri encrypted saklanmaktadır. Kullanıcının bilgisi

dışında gerçekleşen parola denemeleri ve otomatik hesap kilitleme gerçekleşmektedir. Admin tarafından yapılan şifre yenilenmesi veya kullanıcı tarafından yapılan şifremi unuttum işlemlerinde bilgilendirme yapılmaktadır. Uygulama erişimi SSL protokolü ile sağlanmaktadır.

Kişisel Veri Politikaları

Bu kapsamda, 6698 sayılı Kanun ve ilgili mevzuat gereğince kişisel verilerin işlenmesi ve korunması için Next4biz tarafından gereken idari ve teknik tedbirler alınmaktadır. Kurumumuz ISO 27701 Kişisel Veri Güvenliği sertifikasına sahiptir.

Next4biz, kişisel veri politikalarında; Kişisel verilerin rıza kapsamında işlenmesi, kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi hususlarına yer verilmiştir. Kişisel verileri doğru ve gerektiğinde güncel tutma, kişisel verileri belirli, açık ve meşru amaçlar için işleme gereksinimi dikkate alınmaktadır. Kişisel verileri işlendikleri amaçla bağlantılı, sınırlı ve ölçülü işleme, kişisel verileri ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme, kişisel veri sahiplerini aydınlatma ve bilgilendirme esastır. Kişisel veri sahiplerinin haklarını kullanması için gerekli alt yapıyı oluşturma, kişisel verilerin korunması için gerekli tedbirleri alma konularında süreçler tanımlıdır. Kişisel verilerin işleme amaçlarının tespit ve uygulamasında, üçüncü kişilere aktarılmasında, ilgili mevzuata ve KVK Kurulu düzenlemelerine uygun davranma, özel nitelikli kişisel verilerin işleme ve koruma hususlarının özel olarak düzenlenmesi hususlarına yer verilmiştir.

Altyapı, Operasyonel Süreklilik

İş sürekliliği planları tanımlı ve sürdürülebilir mimaridedir. Son 2 yıllık verilere üretim, 2 yıldan eski verilere arşiv sistemi üzerinden erişim verilmektedir. Servis ile oluşturulan kayıtların servisin iptali veya sözleşme feshi durumunda müşteriye teslimi ham veri olarak uygulama arayüzünden sağlanmaktadır. Servisin iptali halinde tüm ilgili firma, firmaya ait müşteri ve bildirim verileri veritabanından silinmektedir. Kurumumuz ISO 22301 sertifikasına sahiptir.

Felaketten geri dönüş (DR) durumunda RPO değeri 12 saat, RTO değeri 8 saattir.

(*) RTO Recovery Time Objective

(**) RPO Recovery Point Objective