

Gizlilik & Güvenlik

Veri Gizliliği ve Bağımsız Denetimler

Veri Gizliliği

Neden veri, neden bilgi değil de veri, önce bundan başlamak gerekiyor. Veri, bilginin yapı taşı olarak düşünülürse, bu seviyede kurgulanmayan koruma önlemlerinin, bilgi seviyesinde yetersiz kalacağı açıktır. Katmanları doğru ayırtmak, her katmanın güvenlik gereksinimleri doğru anlamak ve bunları doğru kontrol etmek son derece önemlidir. Bu katmanlar, uygulama, veri tabanı, sistem, ağ veya sizin kurumunuzun topolojisine özgü kurgulanabilir. Geliştirme ortamları, alt ağ kümeleri ve buna benzer birçok mantıksal ayrımı yapabilirsiniz.

Kontrol süreçlerindeki olgunluk seviyesi son derece önemlidir. Belki de hizmet kalitesini, güvenliğini ayırtan farkı belirleyen en önemli katman da budur.

Kontrol süreçlerini aşağıdaki şekilde sınıflandırabiliriz;

- İç kontrol ve testler,
- Dış kontroller ve testler,
- Standartlar,
- Yönetişim sistemleri, yaşam döngüleri, kontrol noktaları.

Gerçekçi bir bakış açısıyla tasarlayacağınız bilgi güvenliği yaşam döngüsü içinde kurumunuza özgü denetim noktalarını da kurgulamalısınız. Peki, bu kontroller çalışıyor mu? Bunu izleyen yapılar var mı? Kuvvetler ayrılığı ilkesine uygun şekilde bu kontroller değerlendiriliyor mu?

Bu sorulara gönül rahatlığıyla “evet” diyorsanız, birkaç sorumuz daha var...

Yaşam döngüleri, tanımlı bir disipliner yapıya (Örnek: ISO 27701) uygun mu? Bu standartların gereği olan tanımlar, talimatlar ve politikalar tanımlı mı?

Buraya kadar da cevap “evet” ise, iyi bir noktaya geldik demektir

Şimdi sıra, dışarıdan bir uzman gözün tanımlı politika ve uygulamalarınızı incelemesi ve doğrulamasında diyebiliriz.

Bağımsız Denetim ve Gözden Geçirmeler

Bağımsız gözden geçirme kavramı, kuvvetler ayrılığı ilkesinin kurumsal düzeyde yapılandırılmasıdır. Bir dış denetimin sağlıklı ve verimli olması için aşağıdaki adımları kapsamı gerekmektedir.

- Denetim kapsamı,
- Denetim yetkinliği,
- Bulgu yönetimi,
- Bulgu giderimi,
- Doğrulama.

Regülasyonlar, kurum hizmetleri kapsamında tabi olunan kanunlar ve sözleşmeler denetim kapsamının özü olacaktır. PCI, OWASP10 vb bilinen disiplinlerden, kod güvenliğine, sistem altyapı güvenliğinden, uygulama güvenliğine, IDOR testlerinden, penetrasyon testlerine kadar birçok şekilde bu denetimler gerçekleştirilebilir.

Next4biz ve Bağımsız Denetim Çalışmaları

Hizmet kalitesini ve güvenliğini ayarştıran en önemli farkın kontrol seviyelerindeki olgunluk olduğunu dile getirmiştik, bu olgunluk seviyesini yükselten en önemli etken ise bağımsız denetim ve gözden geçirme çalışmalarıdır.

Next4biz Bilgi Teknolojileri olarak, uyguladığımız bilgi güvenliği yönetim sistemi çerçevesinde iç denetimlerimizi periyodik olarak gerçekleştirmenin yanı sıra konusunda uzman bilgi güvenliği denetim firmaları ile çalışıyoruz.

Her katmanımızın test metodolojilerini,

- Her ortamın IDOR bakış açısını,
- Her ortamın mimarisini,
- Her platformumuzun güvenliğini,
- Sistem/Ağ altyapısını
- Denetim kapsamını

çok iyi belirledikten sonra her katmanımızın testini yapıyor, bulgularımızı yönetiyor ve yine bağımsız bir bakış açısıyla validasyonlarını başarı ile gerçekleştirip, güvenliği bütünleşik anlamda, kalitenin en önemli bileşeni olarak görüyoruz.

Geliştirdiğimiz yazılımlar üzerinde sızma testleri, statik kod analizleri, mantıksal testleri periyodik olarak yaptırıyoruz.

Gizli bilgi yönetim sistemi (PIMS) oluşturma, uygulama ve sürekli iyileştirme çalışmalarımızı bağımsız denetimler ile ISO 27701 sertifikamızı alarak sürdürüyoruz. Benzer şekilde sahip olduğumuz ISO 27001 kalite güvence belgemizle ve bağımsız olarak akredite edilmiş diğer sertifikalarımızla, müşterilerimize bilgi güvenliği alanında da yüksek kalite hizmetler sunuyoruz.