Güvenlik Uyumluluğu Kontrol Listesi

AB Genel Veri Koruma Düzenlemesi (GDPR) işletmelerin kişisel bilgileri güvenceye almak ve kişisel verileri de içeren bir güvenlik ihlali durumunda etkilenen bireyleri ve yetkili mercileri bilgilendirmek için teknik ve kurumsal önlemler almasını gerektirmektedir.

Bu da, işletmeleri uyum sağlamak için gereken zaman ve kaynakları bulma zorluğuyla karşı karşıya bırakmaktadır.

Öte yandan, işletmeler saldırılara karşı basit bir güvenlik duvarından daha fazlasını sunmada başarısız olurlarsa güvenlikleri ihlal edilebilir ve milyonlara ulaşan para cezalarıyla karşı karşıya kalabilirler. Her işletme büyük ihtimalle bir noktada güvenlik ihlali yaşayacaktır. Bir ihlali ortaya çıktığı anda tespit etmek ve mümkün olan en kısa süre içerisinde doğru ürün, araç ve işlemlerle düzeltmek büyük önem taşımaktadır.

Bu kontrol listesi; BT güvenliğini artırmak ve ihlalin pahalı sonuçlarından kaçınmak isteyen işletmeler için pratik bir kaynak görevi görmektedir. Temel maddelerle başlayarak maksimum güvenlik katmanlarına doğru ilerlediğinizde yazıcı uç noktalarınızın güvende kalacağından ve GDPR gereklilikleri ile uyumlu olacağından emin olabilirsiniz.

Ağınızdaki uç nokta cihazlarını korumaya almanız için pratik bir liste.

Temel güvenlik katmanı

- Sadece dâhili kötü amaçlı yazılım koruması ve şifreli sabit diski olan cihazları satın alın
- Cep telefonunuzda uygulamaları güncellediğiniz gibi ürün yazılımlarını da, özellikle kritik güvenlik yaması olan sürümleri, güncelleyin.
- Cihaz arayüzlerini yapılandırın ve uygulamalarınızın gerektirmediği FTP ve telnet gibi protokolleri kilitleyin.
- Yeni cihazları gözden geçirin ve davetsiz misafirlere erişim imkanı sağlayabilecek kullanılmayan bağlantı noktalarını veya protokolleri kapatın
- Her cihaz için özel yönetici parolaları kullanın
- Yönetimsel özelliklere erişimi devre dışı bırakmak için ön paneli kilitleyin
- Cihaza gelen ve cihazdan giden verileri şifreleyin
- Eski veriler için sabit disk silme prosedürlerini belirleyin – özellikle de takas ettiğiniz yazıcılarda

Bu işlemler tamamlandıktan sonra bir sonraki güvenlik katmanına geçin.

Orta seviye güvenlik katmanı

- Tehditlere karşı ağınızı daha kapsamlı izleyebilmek için yazıcı sistemlerindeki günlük verilerinizi SIEM aracınızla tümleştirin. Yeni uyumluluk düzenlemelerinde raporlama gerekliliklerini karşılamak için görünürlük temel anahtardır.
- Cihazdan kimin kopyalama, tarama, faks gönderme işlemleri yaptığını izlemek için yazıcıda kimlik doğrulama özelliği dağıtın. Bu veriler, herhangi bir güvenlik ihlali sonrası yapılacak adli soruşturmada yardımcı olacaktır.
- Hassas bilgilerin unutulmasını önlemek için kimlik doğrulamalı baskı özelliği dağıtın. Boşuna alınan baskıları azaltmak çevre standartlarınızı da korumanıza yardımcı olacaktır

Bu işlemler tamamlandıktan sonra son güvenlik katmanına geçin.

İleri seviye güvenlik katmanı

- İş takibi ve muhasebe raporlamasını düzenleyin
- Rol tabanlı yetkilendirme ile kimin hangi yazıcılara ve neden erişebileceği konusunda kurallar koyun ve bu kuralların otomatik olarak uygulanmasını sağlayın
- Ağınızdaki diğer internet bağlantılı cihazlara olduğu gibi, her bir yazıcıya da benzersiz dijital sertifikalar dağıtın
- Veri şifreleme, ağ içi cihaz erişimi, kullanıcı kimlik doğrulaması ve izleme için bir yönetilen mobil baskı çözümü dağıtın

4AA7-1093TRE