GÜVENLİ GÜNLER BÜLTENİ

NİSAN 2017

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Bültenlerin her ay size ulaşması için üye olunuz: http://eepurl.com/bP-tWn

Düzenli Yedekle, Veri Kaybetme

GÜNÜMÜZDE İHTİYAÇ DUYDUĞUMUZ, KULLANDIĞIMIZ BİRÇOK BİLGİ DİJİTAL ORTAMDA SAKLANMAKTA VE KAYBEDİLMELERİ TELAFİSİ MÜMKÜN OLMAYAN SORUNLARA NEDEN OLABİLMEKTEDİR. ***Yıllardır sakladığınız aile fotoğraflarınızı veya şirketinize ait bazı finansal bilgileri bir sabah kalktığınızda bulamadığınızı, bu durumun üzerinizde yaratacağı hayal kırıklığını, sinir bozukluğunu düşünün.***

Bireyler olarak genellikle verilerimizi kaybetme riskimizin bulunmadığını veya böyle bir tehlikeyle karşılaşma ihtimalimizin çok düşük olduğunu varsayarız ama ne yazık ki gerçek öyle değildir.

Özellikle son dönemde giderek yaygınlaşan cryptolocker (dosya şifreleme zararlısı) zararlı yazılımı bu tehlikelerin en önemli örneklerinden sadece biridir. Gün içinde gelen onlarca e-posta arasında cryptolocker zararlı yazılımı bulunanlar olabilir ve durumu fark etmeden e-postayı açmanızla bilgisayarınızdaki, bilgisayarınıza bağlı flash diskteki, harici diskteki ve ağdaki paylaşılan verileri şifrelemiş olursunuz. Üstelik, sağlıklı çalışan güncel bir yedeğiniz yoksa verilerinize erişimiz kesilmiş demektir.

VERİ KAYIPLARININ BAŞLICA NEDENLERİ

» İşletim sistemlerinde oluşan teknik sorunlar
» Donanım kaynaklı teknik sorunlar
» Kullanıcı hatası (hatalı dosya silme vb.)
» Zararlı yazılımlar
» Siber saldırılar

Kuşkusuz kimse bu tip tatsız durumlarla karşılaşmak istemez. Ne var ki günümüz dünyasında bu risklere neredeyse herkes açık olduğundan en iyisi durumu kabullenmek ve gerekli hazırlıkları yapmaktır. En büyük hazırlıksa, her zaman, çalışan güncel bir yedek bulundurmaktır.

YEDEKLEME İŞLEMİNE BAŞLAMADAN ÖNCE PLANLAMA

Her işte olduğu gibi yedekleme işlemine başlanmadan önce de bir plan hazırlanması gerekir. Bu planın oluşturulmasında şu bilgilerin göz önüne alınması önemlidir:

» Hangi bilgiler yedeklenmeli (kişisel resimler, muhasebe kayıtları vb.)
» Bu bilgiler ne sıklıkla yedeklenmeli (günlük, haftalık, aylık vb.)
» Yedekler nasıl bir sistemde tutulmalı (flash disk, harici disk, Storage, Cloud vb.)
» Yedekler nasıl korunmalı (kasa, kilitli dolap vb.)
» Yedekler ne süreyle saklanmalı (6 ay, 1 yıl, 5 yıl vb.)
» Yedeklerin çalışır durumda olup olmadığı kontrol edilmelidir (her yedekleme sonrası)

Yukarıda belirlenen maddeler özelinde yedekleme planınızı hazırlayabilir ve bu maddeleri uygulayarak verilerinizi güvenli bir şekilde saklayabilir, ihtiyaç duyduğunuz da erişebilirsiniz.

YEDEKLERİNİZİ ALIRKEN NELERE DİKKAT ETMELİSİNİZ?

1. Yedeklenen dosyaların adları

Özellikle düzenli ve sık yedeklenen dosya adlarında tarih bilgisinin de bulunması gerekli veriye erişimde kolaylık sağlayacaktır. Bu nedenle dosya adlarının tarih bilgisi (IK_20_03_2017 gibi) içermesine özen gösterilmelidir.

2. Yedekleme zamanı

Yedeklenecek dosyaların ne sıklıkla yedeklenmesi gerektiğine karar verilirken kapsadıkları verinin ne sıklıkla değiştiği ve verinin önem seviyesi göz önüne alınmalıdır. Örneğin finansal verilerin tutulduğu ve günden güne çok fazla değişiklik gösteren verilerin bulunduğu dosyalar günlük olarak, sertifika ve belgelerin yer aldığı personel dosyaları ise aylık olarak yedeklenebilir.

3. Yedeklenen dosyanın yeri

Gerçek veri ile yedeklenen verinin aynı diskte, lokasyonda vb. olması tavsiye edilmez. Evinize girebilecek bir hırsız hem notebook'unuzu hem de harici diskinizi çalabilir. Bu durumda hem notebook'unuzdaki gerçek verilerinizi hem de harici diskinizdeki yedek verilerinizi kaybedersiniz. Dolayısıyla, harici diskinizi banka kasası gibi güvenli bir yerde saklamanız çok daha iyi bir çözümdür.

4. Yedeğin çalıştığından emin olun

Bazı durumlarda yedeklenen dosyalar bozulabilir, doğru yedeklenmemiş olabilir ve bu nedenle verilerinize erişiminiz olanaksız hale gelebilir. Bu gibi olumsuzlukları yaşamamak için, için her yedekleme işlemi sonrasında yedeklerin sağlıklı bir şekilde çalışıp çalışmadığını kontrol etmeniz gerekir.

5. Yedeklerinizi şifreli olarak saklamayı deneyebilirsiniz

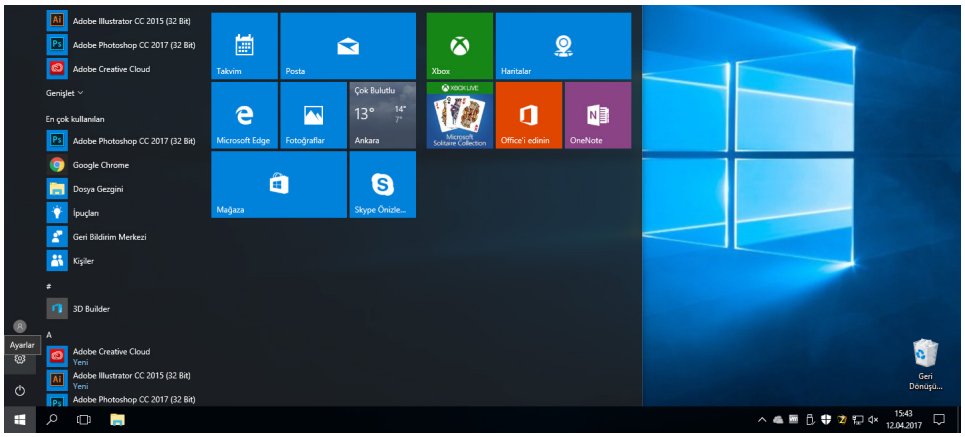
Özellikle gizlilik seviyesi yüksek verilerinizi yedeklediğinizde veya sakladığınız ortamın yeterince güvenli olmadığını düşündüğünüzde verilerinizi şifreleyerek saklayabilirsiniz. Şifreli yedekler başkalarının eline geçse bile, içeriğine erişemeyecekleri için sizin başınız ağrımayacaktır.

Eğer Windows 10 işletim sistemi kullanıyorsanız aşağıdaki yapılandırma ayarlarıyla düzenli olarak yedek alabilirsiniz.

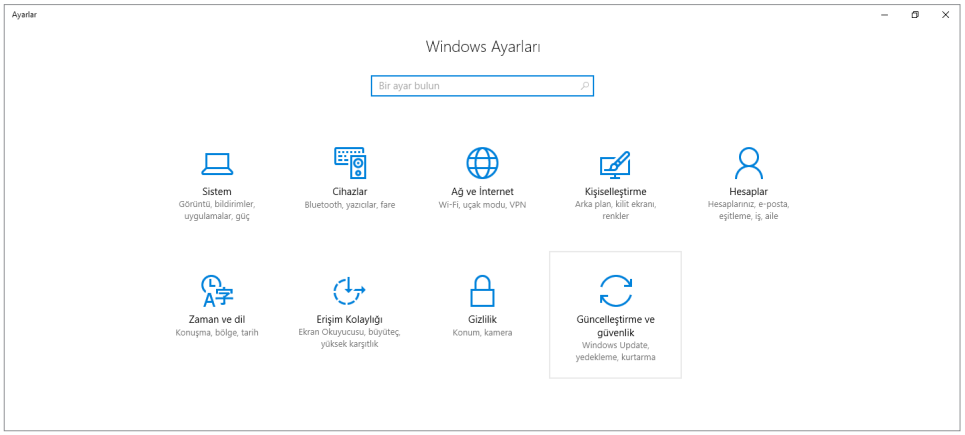
Windows 10 Yedekleme Ayarı

Windows 10 ile birlikte gelen Yedekleme çözümünden yararlanmak için:

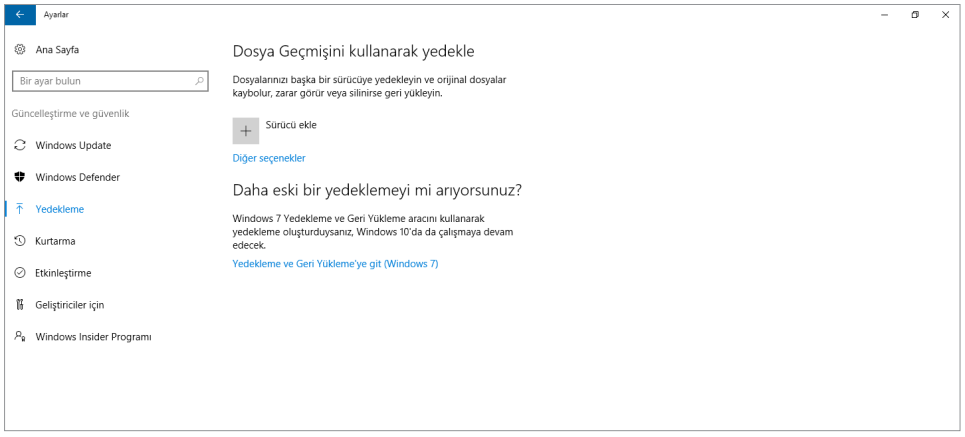
- **Başlat > Ayarlar** yolu izlenir.



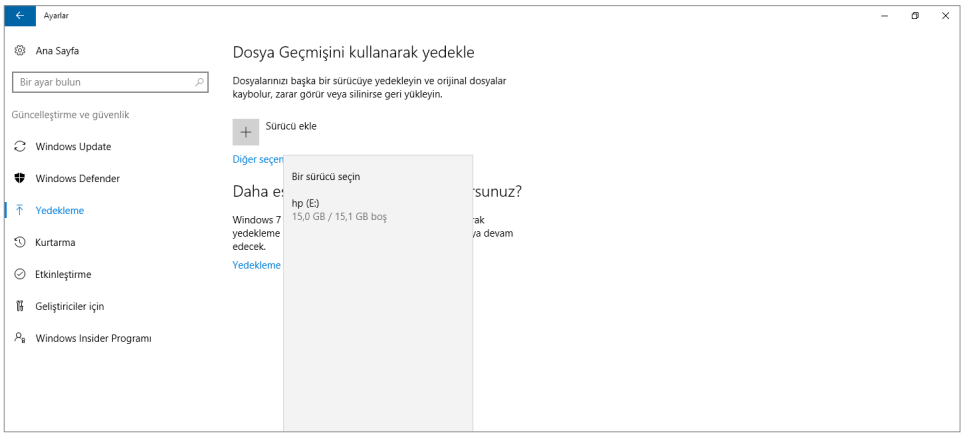
- **Güncelleştirme ve güvenlik** menüsüne gidilir.



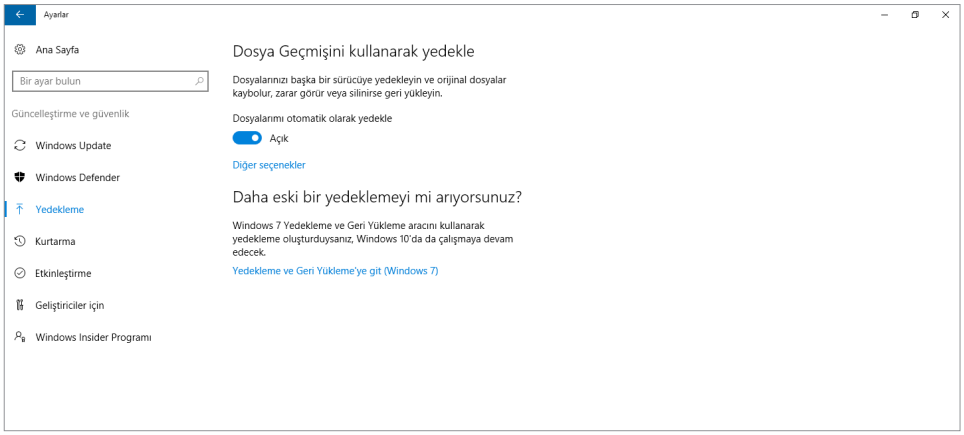
- **Yedekleme** sekmesine gidilir.



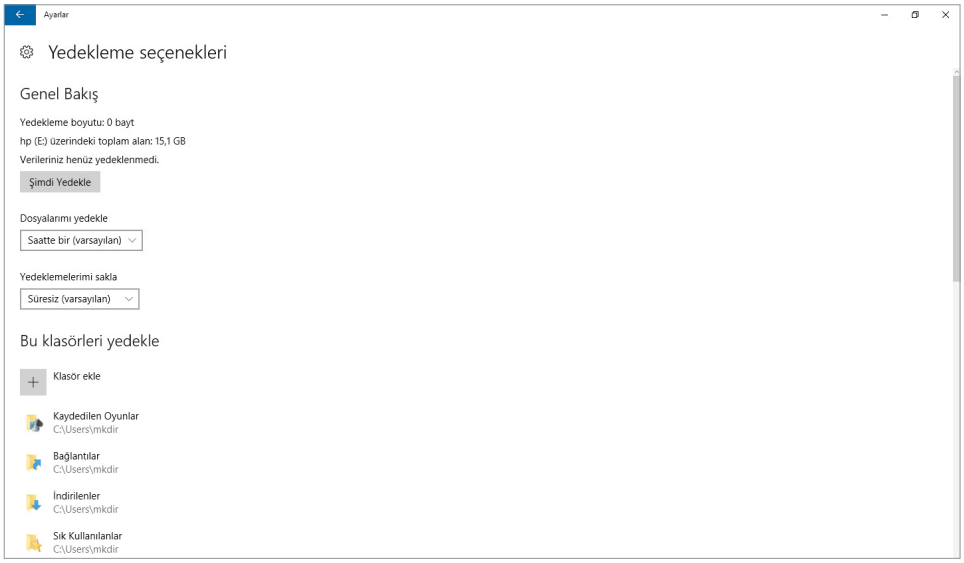
- **Sürücü ekle** butonuna tıklanır ve sisteme bağlı harici disklerden yedekleme için kullanılmak istenilen seçilir.



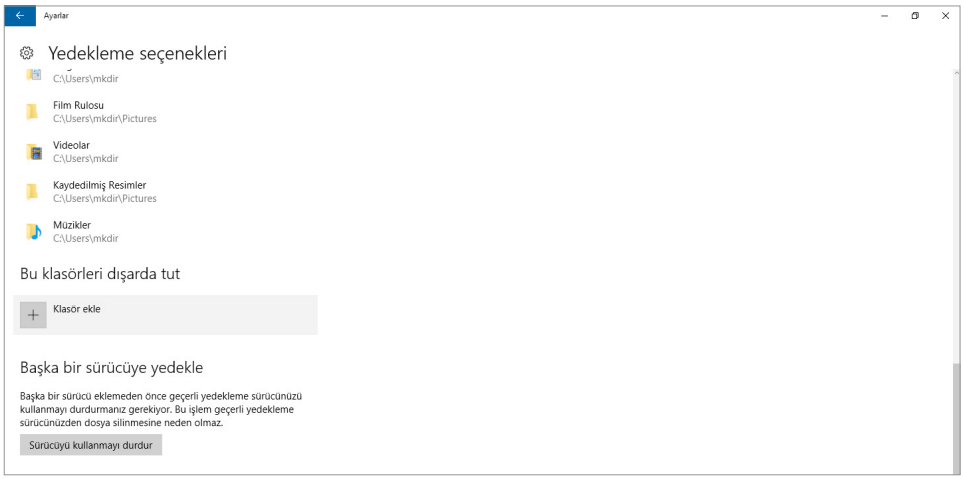
- Otomatik yedekleme aktif hale gelir.



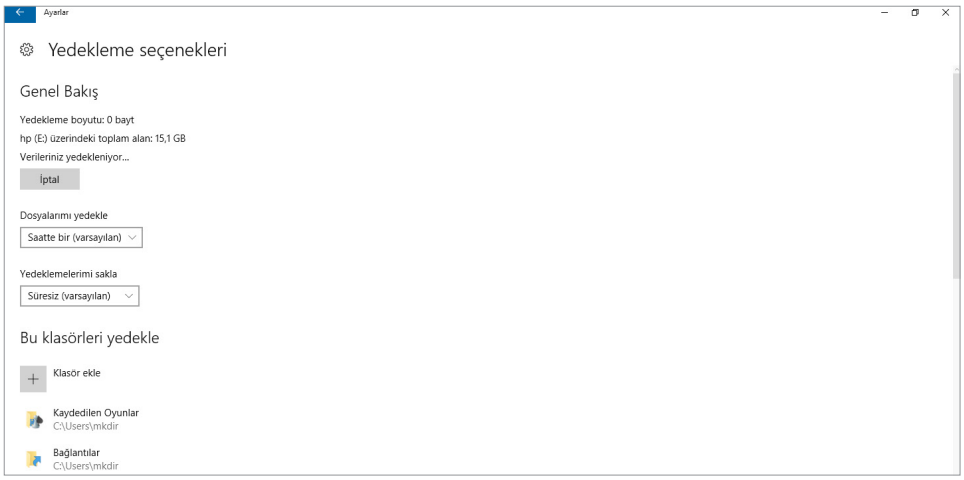
- **Diğer seçenekler** seçildikten sonra açılan menüde yedekleme yapılması istenilen klasörler seçilir.



- Yedekleme dışı bırakılacak klasörlerin seçimi yapılır.



- Klasör seçimleri yapıldıktan sonra yedekleme sıklığı ve yedeklerin saklanma süresi de seçilir ve **Şimdi Yedekle** seçilerek yedekleme işlemi başlatılır.



YAZAR HAKKINDA

KAYHAN KAYIHAN, 1989 İzmir doğumlu, Gazi Üniversitesi Yönetim Bilişim Sistemleri bölümünden 2014'te mezun oldu. 8 yıldır bilişim sektörü içerisinde yer alan Kayhan Kayıhan 2015'ten beri Lostar Bilgi Güvenliği A.Ş'de kıdemli danışman olarak görev yapmaktadır.