

# GÜVENLİ GÜNLER BÜLTENİ



Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için [guvenligunler.com](http://guvenligunler.com) adresini ziyaret ediniz.

EYLÜL 2017



## **HAYATIMIZI KOLAYLAŞTIRMAYA ÇALIŞIYORKEN güvenliğimizi tehlikeye atıyor olabilir miyiz? Hem de kendi evimizde!**

Son yıllarda gittikçe artan bir şekilde akıllı cihazlar hayatımıza girmeye başladı. Önce telefonlarımız, daha sonra saatlerimiz, şimdi ise evlerimiz akıllandı. Televizyonlarımızda sık sık bu tarz evlere ait olabilecek farklı sistemlerin tanıtımlarını görüyoruz.

### **PEKİ "AKILLI EV" NEDİR?**

Akıllı Ev kavramıyla anlatılmak istenen, en basitinden görüntülü diyafon gibi Akıllı Ev sistemlerinin kurulu olduğu yaşam alanlarıdır; ev sakinlerine bu sayede güven, hız ve konfor kazandırılması amaçlanır. Söz konusu sistemleri kullanabilmek için genellikle kullanıcının, akıllı telefonuna ya da tabletine uygulamalar indirmesi ve internet bağlantısı sahibi olması gerekmektedir. Bu uygulamalarla ev dışındayken ısıtma sisteminize

haber göndererek eve geldiğinizde evinizin istediğiniz sıcaklıkta olmasını sağlayabilir ya da ev sahiplerine özel olarak yazılan senaryolarla seyahatleyken güvenlik için oda ışıklarını ya da televizyonu açıp kapatarak evdeymiş izlenimi yaratabilirsiniz.

### **AKILLI EV'LER TAMAMEN GÜVENLİ Mİ?**

Evlerimizde Akıllı Ev sistemleriyle hayatımızı kolaylaştırmaya çalışırken, sistemlerin kullandığı uygulamalar, yazılımlar ya da internete bağlı olma gereksinimleri ile ne kadar güvendedeyiz?

Akıllı Ev'lerde sistemleri yönetebilmeniz için uygulamaları, telefonunuzun desteklediği uygulama mağazasından indirmeniz gerekmektedir. Akıllı Ev'ler için hazırlanan programlarda, siz telefonunuzun ekranında bir tuşa dokunduğunuzda uygulama arkada

bir kod bloğu çalıştırır. Böylece uzaktan evinizde bulunan sistemleri çalıştırıp yönetebilirsiniz. Bu uygulamaları indirirken kullanım koşullarının kabul edilmesi ve telefon üzerinden ulaşılabilecek yerlere izin verilmesi istenir. Ancak uygulamalardaki güvenlik açıkları ve verdiğiniz izinler nedeniyle evinizin güvenliği tehlikeli hale gelebilir.

Akıllı Ev sistemlerinin kullanılabilmesi için internete bağlı olmaları gerekmektedir; kendilerini güncelleyebilmeleri ya da uygulamalardan gelen istekler üzerine yazılımları çalıştırabilmeleri internet aracılığıyla mümkündür. Ne var ki bu sistemlerin internete bağlı olması, dış dünyaya açık oldukları anlamına da gelmektedir. Güvenliğinden tamamen emin olmadığınız yazılımları, internetteki tehlikelere açarak ne kadar güvende olabilirsiniz?

Evlerimiz bizim için özel alanlardır. Evimizin yönetiminin her şekilde bizde olmasını, dışarıdan gelebilecek tehlikelere karşı korunuyor olmayı isteriz. Kullandığımız Akıllı Ev sistemleri yazılımları alarm, ısınma, elektrik sistemlerine erişim sağlamaktadır. Gelişen teknolojiyle birlikte siber saldırıların arttığı ve siber saldırganlar için sistem kontrollerinin ele geçirilmesinin çocuk oyuncağı olduğu bir dönemde evinizin kontrolü ne kadar sizde olabilir?

Evinizden çıkarken bütün pencereleri ve kapıları kapattığınızdan, ısınma ayarını düşürdüğünüzden ve alarmı kurduğunuzdan eminsiniz ama eve geldiğinizde devre dışı kalmış bir alarm buluyorsunuz ve bütün kapı ve pencereleriniz açık durumda. Bu durumda gerçekten Akıllı Ev'ler için "güvenli" diyebilir miyiz?

## AKILLI EV'LERİ NASIL DAHA GÜVENLİ HALE GETİREBİLİRİZ?

Akıllı Ev sistemlerinizi birkaç yöntemle daha güvenli hale getirebilirsiniz:

### **Akıllı Ev sistemleri için güçlü parola kullanılmalıdır.**

Parolalarınız 8 karakter uzunluğunda olmalı ve anlamlı bir kelime içermeden büyük ile küçük harf, sayı ve özel karakterler içermelidir.

### **Varsayılan olarak gelen parolalar değiştirilmelidir.**

Varsayılan olarak gelen parolalar zayıf parolalardır ve kırılmaları daha kolaydır. Parolalar değiştirilirken doğum tarihi ve yakınların adları gibi kolay tahmin edilebilir bilgilerin kullanılmasından kaçınılmalıdır.

### **Her sistem için farklı bir parola kullanılmalı ve bu parolalar da belirli aralıklarla değiştirilmelidir.**

Farklı parola kullanılması ve parolaların değiştirilmesi, parolaların tahmin edilebilme olasılığını azaltarak sistemlere ulaşma süresini uzatacaktır.

### **Akıllı Ev sistemlerinin güncellemeleri kontrol yapıldıktan sonra yüklenmelidir.**

Güncellemeleri otomatik olarak yükleyin.

### **Güvenilir markaların ürünleri alınmalıdır.**

### **Ürünleri almadan önce güvenlikle ilgili yorumlar okunmalıdır.**

### **Uzun süre güvenlik güncelleştirmesi almayan ürünler değiştirilmelidir.**

## YAZAR HAKKINDA

**HİRAL CANBAĞI** Bilgisayar ve Öğretim Teknolojileri Öğretmenliği'nden mezun oldu. 2016 yılından beri ISACA-Istanbul Chapter Öğrenci üyesidir. 2017, Eylül ayından beri Lostar firmasından GRC Hizmetleri Departmanı'nda danışman olarak çalışmaktadır.



## YASAL UYARI

Bu dokümanın tüm hakları Lostar Bilgi Güvenliği A.Ş.'ye aittir ve Creative Commons BY-NC-ND 4.0 (Attribution-NonCommercial-NoDerivatives 4.0 International - (CC BY-NC-ND 4.0) lisansı altında dağıtılır. Herhangi bir değişiklik yapmadan kaynak gösterilerek dağıtılabılır. Ticari olarak kullanılamaz.