DİJİTAL DÖNÜŞÜM VE SİBER GÜVENLİK DERNEĞİ

KAMUOYU BİLGİLENDİRME YAZISI

www.ddsgd.org

İnternetin Görünmeyen Motorunda Ciddi Açık: Bugün Ne Yapmalıyız?

Kurumlar hızlı davranmalı, işletmeler sağlayıcısına sormalı, vatandaş tedbirli olmalı

Bu hafta dünyanın birçok ülkesinde devlet internet siteleri birdenbire kapandı. Hollanda'da vatandaşların kamu hizmetlerine girdiği sistemler, Belçika ve Finlandiya'da resmî siteler, ABD'de bir insan kaynakları şirketinin maaş sistemi geçici olarak erişime kapatıldı. Türkiye'de ise Cumhurbaşkanlığı Siber Güvenlik Başkanlığı 21 Ekim akşamı acil bir uyarı yayımladı ve ülke genelinde güvenlik taraması başlattı. Bütün bunların nedeni, adını çoğumuzun hiç duymadığı bir yazılımdaki iki ciddi açık: PHP.

PHP Nedir, Neden Bu Kadar Önemli?

PHP, internet sitelerinin arka planında çalışan bir yazılım dilidir. Bir haber sitesine girdiğinizde, belediyenizin sitesinden başvuru yaptığınızda ya da bir alışveriş sitesinde sepetinizi onayladığınızda, bu işlemleri çoğu zaman PHP yürütür. Bir binanın duvarların içinden geçen elektrik tesisatı gibidir: Görmezsiniz ama her şey onun üzerinden çalışır. Dünyadaki internet sitelerinin çok büyük bir bölümü bu altyapıyı kullanıyor.

Açık Ne Anlama Geliyor?

Tespit edilen iki hata, kötü niyetli bir kişinin **hiçbir kullanıcı adı ve şifreye ihtiyaç duymadan**, yalnızca internet üzerinden özel hazırlanmış bir istek göndererek siteyi barındıran bilgisayarın kontrolünü ele geçirebilmesine imkân tanıyor. Saldırgan, o sırada siteyi kullanan başka kişilerin şifre gibi bilgilerini de okuyabiliyor.

Bu açığı ayrıca tehlikeli kılan, sorunun sitenin kendisinde değil, altındaki temelde olmasıdır. Yani en özenle hazırlanmış bir site bile, üzerinde çalıştığı PHP güncellenmemişse risk altındadır. Uzmanlar açıkların tehlike derecesini 10 üzerinden 9,2 olarak değerlendirdi.

Neden Bu Kadar Acil?

Normalde bu tür açıklar, düzeltmesi hazır olduğunda kamuoyuna duyurulur. Bu kez ayrıntılar planlanan tarihten önce sızdı ve kötü niyetli kişiler, düzeltme yayımlanmadan önce açığı inceleme fırsatı buldu. Uluslararası güvenlik şirketleri, saldırganların açığı denemeye başladığını bildirdi. Bugüne kadar doğrulanmış büyük bir veri hırsızlığı açıklanmadı. Ancak riskin büyüklüğü nedeniyle birçok ülke "önce kapat, sonra onar" yolunu seçti.

İyi haber şu ki çözüm hazır. PHP'yi geliştiren ekip 21 Ekim'de güncellemeleri yayımladı. Siber Güvenlik Başkanlığı da e-Devlet Kapısı'ndaki kontrollerin tamamlandığını ve herhangi bir sorun bulunmadığını açıkladı. Bundan sonrası, her kurumun ve işletmenin kendi sistemini güncellemesine bağlı.

Kim Ne Yapmalı?

Kamu kurumları, şirketler ve kritik hizmet sağlayıcılar

- İnternete açık bütün sistemlerini gözden geçirmeli ve PHP'yi 21 Ekim'de yayımlanan güncel sürüme yükseltmelidir. Elektrik, su, iletişim gibi kritik hizmetler ile vatandaşa açık kamu sistemleri ilk 24 saatte ele alınmalıdır.
- Hemen güncellenemeyen sistemleri geçici olarak kapatmaktan çekinmemelidir. Kısa süreli bir kesinti, olası bir veri sızıntısından çok daha az maliyetlidir.
- Yalnızca güncelleme yapmakla yetinmemeli, sistemlerin güncellemeden önce ele geçirilip geçirilmediğini de kontrol etmeli ve önemli şifreleri değiştirmelidir.
- Online alışveriş siteleri ödeme sayfalarına, hosting firmaları ise binlerce müşteriyi barındıran sunucularına öncelik vermelidir.

Küçük işletmeler ve internet sitesi sahipleri

Kendi teknik ekibiniz yoksa endişelenmeyin; yapmanız gereken ilk iş bir telefon görüşmesi. Sitenizi barındıran firmayı ya da sitenizi yapan ajansı arayıp şu soruyu sorun: **"Sunucumdaki PHP, 21 Ekim'de yayımlanan güvenlik güncellemesiyle güncellendi mi?"** Yanıt net bir "evet" değilse, güncelleme yapılana kadar siteyi kapatmayı değerlendirin. Ardından site yönetim panelinizin şifresini değiştirin ve güncel bir yedeğiniz olduğundan emin olun.

Vatandaşlar

Açık, internet sitelerini barındıran bilgisayarlarda bulunuyor. Bu nedenle kendi telefonunuza ya da bilgisayarınıza bir şey yüklemeniz gerekmiyor. Yine de birkaç basit tedbir sizi korur:

- **Aynı şifreyi birden fazla yerde kullanmayın.** Bir sitedeki şifreniz çalınırsa diğer hesaplarınız da tehlikeye girer.
- **Önemli hesaplarınızda iki aşamalı doğrulamayı açın.** E-posta, banka ve sosyal medya hesaplarınıza girişte telefonunuza gelen ek kod, en etkili korumalardan biridir.
- **Sahte uyarılara dikkat edin.** Dolandırıcılar bu tür gündemleri fırsat bilir. "Güvenlik açığı nedeniyle şifrenizi güncelleyin" diyen e-posta ve SMS'lerdeki bağlantılara tıklamayın; gerekiyorsa siteye kendiniz girin.
- **Hesap hareketlerinizi takip edin.** Banka ve alışveriş hesaplarınızda tanımadığınız bir işlem görürseniz hemen kurumunuzla iletişime geçin.
- **Bildirimleri ciddiye alın.** Bir kurum size bilgilerinizin etkilenmiş olabileceğini bildirirse o hesabın şifresini vakit kaybetmeden değiştirin.

Bu Olaydan Çıkarmamız Gereken Ders

Binalarımızın tesisatına nasıl düzenli bakım yapıyorsak, dijital hizmetlerimizin altyapısına da düzenli bakım yapmak zorundayız. Güncellemeyi "sonra yaparız" diye ertelemenin bedeli, bir gün tek bir açıkla birlikte çok ağır ödenebilir. Kurumların hangi yazılımı nerede kullandığını bilmesi, artık desteklenmeyen eski sürümlerden kurtulması ve kritik bir güncellemeyi günler değil saatler içinde uygulayabilmesi gerekiyor.

Taner Çıtak
Dijital Dönüşüm ve Siber Güvenlik Derneği Başkanı
www.ddsgd.org

Bu yazı, 23 Ekim 2026 itibarıyla Cumhurbaşkanlığı Siber Güvenlik Başkanlığı açıklamaları (TR-26-1372), PHP projesinin resmî güvenlik duyurusu ve kamuya açık uluslararası kaynaklar temel alınarak kamuoyunu bilgilendirmek amacıyla hazırlanmıştır.