T.C. SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĞÜ

Siber Olaylara Müdahale (SOME) Birimi

ICANN'den DNSSEC Dağıtımı ile Ağınızı Korumanız için Çağrı.

SOME GD. 19-04

10.04.2019

T.C. SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĞÜ

ICANN'den DNSSEC Dağıtımı ile Ağınızı Korumanız için Çağrı

ICANN, 1998 yılında kurulan ve dünyanın her yerinden bir katılımcı topluluğu ile birlikte kar amacı gütmeden çalışan kamu yararı şirketi olarak kurulmuştur.İnternetin ademi merkeziyetçi yönetimine dahil olan birçok kuruluştan biri olan ICANN, istikrarlı ve güvenli çalışmasını ve evrensel çözülebilirliğini sağlamak için DNS'nin en üst seviyesini koordine etmekten özellikle sorumludur.

ICANN alan adı sisteminin güvenliğinin sağlanması amacıyla kullanılan **DNSSEC** (Etki Alanı Adı Sistemi Güvenlik Uzantıları) eklentisine ilişkin olarak DNS altyapısının doğası gereği doğan zafiyetleri kullanarak, artan zararlı hareketlilikten dolayı tam DNSSEC kontrole geçilmesi ve korumasız olan alan adlarının DNSSEC eklentisi ile koruma altına alınması için 22 Şubat günü çağrı yayınlamıştır.

DNSSEC, alan adı sistemi **(DNS) bilgisinin sayısal olarak imzalanarak, alan adının ele geçirilmesini, alan adı hırsızlığını veya bu yolla yapılabilecek siber saldırıların engellenmesini sağlayan bir DNS eklentisidir.**

Saldırılardan bazıları, etki alanı adlarının delegasyon yapısında yetkisiz değişikliklerin yapıldığı ve hedef sunucuların adreslerinin saldırganlar tarafından kontrol edilen makinelerin adresleriyle değiştirildiği DNS'yi hedefliyor. DNS'yi hedef alan bu belirli saldırı türü, yalnızca DNSSEC kullanımda değilken çalışır.

DNSSEC, geçerliliğini sağlamak için verileri dijital olarak imzalayarak bu değişikliklere karşı koruma sağlamak için geliştirilmiş bir teknolojidir.

DNSSEC kullanıldığında, DNS bilgisinde yetkisiz değişiklikler tespit edilebilir ve kullanıcıların yanlış yönlendirilmeleri engellenir. DNSSEC, İnternet'in güvenlik sorunlarını çözmese de, İnternet kullanıcılarının, bilmeden potansiyel olarak kötü amaçlı bir siteye yeniden yönlendirildiği "**man in the middle**" saldırılarını önlemeye yardımcı olmayı amaçlamaktadır.

DNSSEC, son kullanıcı etki alanı iletişimini koruyan Aktarım Katmanı Güvenliği gibi diğer teknolojileride tamamlar.

T.C. SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĞÜ

Etki

DNSSEC kullanılmayan sistemler verdiği hizmetlerde kullanıcılarını olası **man in the middle** saldırılarına açık hale getirmektedir.

İzlenebilecek yollar:

- DNSSEC kullanılmayan sistemlerde DNSSEC eklentisin ayarlanarak gerekli önlemlerin alınması önem arz etmektedir.
- Tüm DNSSEC sistem güvenlik yamalarının gözden geçirildiğinden ve uygulandığından emin olun;
- Sistemlere, özellikle yönetici erişimine yetkisiz erişim için günlük kayıt dosyalarını inceleyin;
- Yönetici (“kök”) erişimi üzerindeki iç kontrolleri inceleyin;
- Her DNS kaydının bütünlüğünü ve bu kayıtların değişiklik geçmişini doğrulayın;
- Yeterli şifre karmaşıklığını ve şifre uzunluğunu güçlendirin. Düzenli ve periyodik şifre değişikliklerini uygulayın.
- Parolaların diğer kullanıcılarla paylaşılmadığından emin olun;
- Parolaların asla açık metin olarak saklanmadığından veya iletilmediğinden emin olun;
- Bir şifre kilitleme politikası uygulayın;
- DNS bölge kayıtlarının DNSSEC imzalı olduğundan ve DNS çözümleyicilerinizin DNSSEC doğrulama gerçekleştirdiğinden emin olun;
- İdeal olarak, çok faktörlü kimlik doğrulamanın tüm sistemlerde, özellikle yönetici erişimi için etkinleştirildiğinden emin olun;

Ek Bilgi(Referanslar):

1-https://www.usom.gov.tr/tehdit/520.html

2-https://www.icann.org/news/announcement-2019-02-22-en

3-https://www.icann.org/news/announcement-2019-02-15-en

4-https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

5-https://www.icann.org/octo-ssr