Siber Saldırı E-postaları Dil Bilgisi Hatalarından Tespit Edilebilir

- İnfrasis Siber Mühendislik Genel Müdürü Can Sobutay: - “Dolandırıcılar, kimlik avı iletileri oluştururken genellikle bir yazım denetleyici veya çeviri makinesi kullanırlar. Bu da onlara doğru kelimeleri verir ancak cümleler uygun bağlamda, dizilimde olmayabilir” *- 11.11.2020*

İnfrasis Siber Mühendislik Genel Müdürü Can Sobutay, siber saldırı e-postalarını fark etmek için yazım hataları yerine dil bilgisi hatalarına dikkat edilmesi gerektiğini belirterek, “Bu e-postalarda cümleler uygun bağlamda, dizilimde olmayabilir.” ifadesini kullandı.

İnfrasis açıklamasına göre, Kovid-19'un ardından gelen hızlı dijital dönüşüm, siber saldırıların artmasına da neden oldu. Bu kapsamda siber saldırıların içeriği de salgın kapsamında yaşanan gelişmeler ya da yine salgın döneminde meydana gelen ekonomik zorlukları kullanmak amacıyla çeşitli indirim ve ödülleri içeren iletilere dönüştü.

Açıklamada görüşlerine yer verilen İnfrasis Siber Mühendislik Genel Müdürü Can Sobutay, bu tür siber saldırıların en yaygın olanlarının kimlik avı, oltalama saldırıları olduğunu belirterek, “Yayınlanan raporlara baktığımızda, bu tip saldırıların 2020'nin ilk 6 ayında Türkiye'de 1,2 milyona ulaştığını görüyoruz. Yine raporlara göre dünya genelinde ise bir günde yaklaşık 6,4 milyar sahte e-posta gönderildiği belirlendi. Siber saldırıyı yapan kişi veya kişilerin, planlarına bağlı olarak kullanıcının bilgisayarına, kişisel verilerine veya çeşitli hizmetler için kimlik bilgilerine erişebilmesine yol açan kimlik avı saldırıları, bu yıl bir önceki yıla göre dünya genelinde yüzde 58 artış gösterdi.” değerlendirmesinde bulundu.

Pandeminin ardından yaşanan ekonomik sıkıntılar nedeniyle bankacılık sektöründe genellikle borçlulara çeşitli indirimler ve ödüller sunan e-postaların kullanıldığını aktaran Sobutay, şunları kaydetti:

“Avantajlara erişim, bir kılavuz içeren bir dosyanın indirilmesini veya bir bağlantıyı izlemeyi içeren e-postalar çok sık önümüze çıktı. İkinci olarak, sahte banka e-postalarından müşterilere hesaplarının engellendiğini ve erişimlerini geri alabilmeleri için özel bir sayfaya giriş ve şifrelerini girmeleri gerektiği bildirildi. Bir başkası, Kovid-19 bağlantılı düşük oranlı bir kredinin ayrıntılarını almak için eki açmayı teklif eden e-postalar, bankacılık sektöründe kullanılan en yaygın oltalama saldırılarıdır. Bu tür saldırı iletilerinde devlet desteği ve tazminatları sunan sahte e-postalara da yer verildi.”

- “e-postalara şüpheci yaklaşmak gerekiyor”

Can Sobutay, salgın kapsamında vakaların en fazla artış gösterdiği dönemde ülkeler arasında yaşanan posta hizmetinin kısıtlamalar sebebiyle karmaşık hale geldiğini ve teslimat sürelerinin de gözle görülür şekilde arttığını vurgulayarak, “Mektupların ve paketlerin tesliminden sorumlu kuruluşlar, alıcıları her türlü olası gecikme hakkında bilgilendirmek için büyük bir efor harcadı. Bu tam olarak dolandırıcıların taklit etmeye başladığı e-posta mesajlarının bir türü aslında. Bu kapsamda e-posta sahiplerine hedefe, kendisine ulaşamayan paketin bulunduğu deponun adresini bulmak için eki açması teklif edildi. Eğer bu kişi bağlantıyı izlerse bilgisayarı yavaşlamaya başlar, perde arkasında kötü amaçlı yazılımlar, kayıtlı kredi kartı bilgileri ve kişi listeleri gibi kişisel veriler dahil olmak üzere bilgisayarınızın bilgilerinin büyük bir kısmını tüketir ve saldırı hedefine ulaşmış oluyor.” ifadelerini kullandı.

e-postalara şüpheci yaklaşmak gerektiğini belirten Sobutay, şu değerlendirmede bulundu:

“Kişisel veya finansal bilgileri asla e-posta ile göndermeyin. Her zaman, doğru olduğunu bildiğiniz web sitesi adresini (URL) kullanarak bankanızın web sitesine girin. URL yönlendirmelerine dikkat edin ve web sitesi içeriğindeki küçük farklılıklara dikkat edin. e-posta yoluyla gelen bilgi talebi yasal mı diye muhakkak sorgulayın. Bankanız, şifreniz, kredi ya da banka kartı numaranız veya annenizin kızlık soyadı gibi kişisel bilgilerinizi ifşa etmenizi talep ederek size asla bir e-posta göndermez.

Ayrıca, bu tür saldırı e-postalarını fark etmek için yazım hataları yerine dil bilgisi

hatalarına dikkat edilmeli. Çünkü dolandırıcılar, kimlik avı iletileri oluştururken genellikle bir yazım denetleyici veya çeviri makinesi kullanırlar. Bu da onlara doğru kelimeleri verir ancak cümleler uygun bağlamda, dizilimde olmayabilir. Tüm bunlarla birlikte bu tür iletilerde genellikle bir aciliyet duygusu hakimdir. Şüpheli yaklaşmanın faydalı olacağı bir başka e-posta tipi de gerçek olamayacak kadar iyi haberler veren e-postalardır.”

Telefon: +90 (312) 473 84 23
E-Posta: mts@mevzuattakip.com.tr
Adres: Çetin Emeç Bulvari Hürriyet Cad. No: 2/12 Çankaya ANKARA