Gazeteciler İçin Siber Güvenlik

Günümüzde gazeteci olmak, hiç olmadığı kadar tehlikeli.Artan sayıda **siber tehdit**, siber saldırı, cinayet ve savaş zayiatının yanı sıra, şu anda istihbarat servisleri, kanun uygulayıcılar ve diğerleri tarafından çevrimiçi olarak aktif bir şekilde hedef haline gelebiliyor.

Gazeteciler iletişimlerini güvenceye alabilir ve kaynaklarını koruyabilir mi?

Gazetecilerin , **çevrimiçi güvenliklerini** geliştirmelerine yardımcı olmak için , birçok mevcut kaynaklara internet üzerinden erişmek mümkün.

Bu makalede , **gazetecilerin dijital güvenliği** adına , temel olan **parola güvenliğinden** , dikkat edilmesi gereken diğer hususlardan ve siber tehdit unsurundan bahsedeceğim.

Öncelikle neyi neyden , niye ve nasıl koruyacağımızı , niçin **siber güvenliğe** gereksinim duymamız gerektiğini açıklayalım.

Siber Güvenlik :

“Siber güvenlik nedir ?” sorusunu; bilişim sistemlerinde insanlarla veya kurumlar arası kurduğumuz iletişimin, yaşamın, entegrasyonun, maddi veya manevi varlıklarımızın hatta elektronik ortamdaki **verilerimizin güvenliğinin**, bütünlüğünün ve gizliliğinin korunması şeklinde tanımlayabiliriz.

Her gazetecinin , kendi çapında haber aldığı ve bilgi akışı sağladığı kaynaklar vardır. Gazetecinin , hem kendi güvenliğini sağladığı hem de ona haber gönderen **“kaynak”** ile ilgili , iletişim güvenliğinden bahsedebiliriz. Bu **“iletişim güvenliği”** sağlanmazsa, birçok kötü sonucun da beraberinde gelme riski artacaktır.

Kimse bilgi kaynaklarını , haber akışı sağladığı kaynakları ifşa etmek istemez. Bu sebeple dikkat edilmesi gereken birçok husus var. Örneğin ; Hedefteki gazeteci de **siber güvenlik farkındalığı** yeteri kadar yoksa , elindeki her şeyi kaybedebilir. Ufak bir senaryo örneği verelim...

Hedefimizde bir **gazeteci** olduğunu varsayalım.Gazetecinin bilgi akışı sağladığı muhbirlere , elindeki kaynak ya da bilgilere ulaşmamız gerekiyor. Hedef gazetecimiz hakkında ufak bir araştırma sonucu mail adresini ediniyoruz. Mail adresini "**Google Hacking**" yöntemi ile bulmak mümkün.

Sonrasında mail adresine göndereceğimiz **zararlı yazılım** ile beraber bilgisayar kontrolünü elimize alıyoruz. Genel olarak, gazetecilerin büyük çoğunluğu kendilerine gelen mailleri aktif olarak kontrol etmektedirler. Dikkat çeken içerik bağlantısı sayesinde kurban göndermiş olduğumuz bağlantıya tıklayacaktır ve sonrasında zararlı yazılım içeren sitemize yönlendirilecektir. Bununla beraber ilk adımı atmış oluyoruz.

Hedef kişinin mail adresine gönderdiğimiz **zararlı yazılım** sonucu hedef kişiyi dinlemeye alıyoruz ve hedefimiz hakkında raporumuzu oluşturuyoruz. Rapor içeriği ne kadar detaylı olursa , o kadar işimize yarayacaktır.

İletişim halinde olduğu muhbirlerin isimlerine ulaştıktan sonra da benzer senaryolar aracılığı ile hedef yolunda ilerliyoruz . Hedef kişinin mail adresine , dikkat çekici bağlantılar ile **zararlı yazılım** göndermek sadece ufak bir örnekti.

Bunun gibi onlarca saldırı senaryosu üretilebilir. Çalıştığı kuruma gidip **yerel ağ saldırıları** sonucu, istenen bilgiler elde edilebilir. Bu tarz örnekler çok ...

Varsayalım **“siber güvenlik farkındalığı”** hakkında az çok bilgi sahibiyiz. Gelecek olan saldırı ve senaryolara karşı hazırlıklıyız . Bu yeterli mi ? Tabii ki hayır. Her zaman bilmemiz ve unutmamamız gereken bir şey var ki , o da hiçbir zaman **yüzde yüz güvenlik** olmayacağıdır.

Parola Güvenliğine gelecek olursak belli başlı kurallar var bunlardan bazıları ;

- Anlamlı bir bütün oluşturmayan parolalar tercih edilmeli.
- Parolanın içinde hem büyük hem de küçük harf, rakamlar ve işaretler bulunmalı.
- Kullanılan tüm çevrimiçi hizmetler için ayrı parola oluşturulmalı.
- Belirli zaman aralıklarıyla parolalarınızı yenilemelisiniz.
- Güvenlik sorularına verilen yanıtlar “gerçek” olmamalıdır.

“Anlamlı bütün oluşturmayan” parola ne demek?

Sizinle ilişkili plaka, doğum tarihi, isim, soy isim, şirket ismi vs. bilgileri içermeyen, birleştirildiğinde bir anlam ifade etmeyen parolalara **“anlamlı bütün oluşturmayan”** parolalar diyebiliriz. Buna örnek olarak **“a'^sD/)2+W-a”** tarzında bir parolayı gösterebiliriz.

Olay sadece parola güvenliği ile bitmiyor.

Korsanlar her zaman sisteminizi hedef almayabiliyor. Hedef siz de olabilirsiniz. Dikkat edilmesi gereken unsurlardan bir tanesi de insan faktörü .

Sosyal mühendislik kurbanı olmayın. Girdiğimiz , gireceğimiz sitelere dikkat etmeliyiz. Sahte haber sitelerine ya da sayfalarına yönlendiren **kötü amaçlı bağlantılar** sayesinde ufak bir **sosyal mühendislik** senaryosu ile tuzağa rahatça düşebilirsiniz.

Tıklandığında daha da inanılmaz ve skandal açıklamalar vaadinde bulunan, önemli haberler gibi ilgi çekici başlıklara sahip haber bağlantılarını da örnek gösterebiliriz.

Bu bağlantılar genellikle söz konusu ünlü ile ilgili basındaki yalan haberlerden faydalanacak şekilde, özel olarak tasarlanmış **zararlı yazılım** içeren sitelere yönlendirir. Bunun tarihte yüzlerce örneği var...

Bu tür **gerçeklik payı bulunmayan** bağlantılarla her yerde karşılaşabiliriz. Milyonlarca insan her gün kullandığı sosyal medya platformlarında saatlerini geçirmekte.

Durum böyle olunca da **sosyal mühendislik saldırılarının** sosyal medya hesaplarımız üzerinden olma ihtimali oldukça yüksektir. Bu nedenle, sosyal medya platformlarının bilinçli kullanılması gerekiyor.

Bu vermiş olduğum bilinen yöntemler , sıradan günlük hayatta başımıza gelebilecek rutin örnekler. Tüm bu vermiş olduğumuz unsurlara dikkat bile etsek , hiçbir zaman güvenliği sağlayamayız , sağlayamazsınız. Bu sebeple kesin güvendeyiz tabiri yanlış olur.

Haberleşme ortamı güvenli olmalı.

İletişimi şifrelemek için kullanılan birçok yöntem yalnızca içeriği şifrelemektedir. Bu da sizi gözetlemek isteyen kişinin içeriğe ulaşamasa bile birçok değerli kaynağa ulaşmasına imkân sağlayabilmekte. Bu da siz ve kaynaklarınız ile ilgili detaylı haritalar oluşturulmasını sağlamaktadır.

Bu sebeple , günümüzde birçok istihbarat servisinin de **Metadata** toplamada büyük payı vardır.

Metadata Nedir?

Metadata, kısaca, bir kaynağın ya da verinin öğelerini tanımlayan bilgilerdir. Detaylı olarak açıklanırsa, belirli bir veri seti ya da kaynak hakkında nasıl, ne zaman ve kim tarafından oluşturulduğu hakkında tanımlayıcı bilgiler içerir. Bir **metadata** saat kaçta, nereden, hangi baz istasyonunu kullanarak kimi aradığınızı, arama yaptığınız telefonun **IMEI** numarasını, ne kadar süre konuştuğunuzu vb. bilgileri içerir.

Bunun önüne geçme yöntemlerine gelecek olursak internet trafiğimizi tamamen şifrelememiz gerektiğini söyleyebilirim. Trafiğimizin güvensiz olması sadece **metadatamızın** toplanması değil **DPI (derin inceleme)** gibi yöntemlerle iletişim kurduğumuz her şeyin de ifşa olmasına sebep olacaktır. Bu sebeple dikkatli olmak gerek.

Günümüzde yüzlerce **haberleşme ve mesajlaşma** sistemi var. Fakat güvenli bir şekilde haberleşebilmemiz için her ne olursa olsun şifreleme yöntemlerini kullanmamız gerekiyor.Hemen her cihazın farklı şifreleme alternatifleri mevcut.

Tüm bunlara rağmen **metadatanın** ele geçirilebileceği, kimi durumlarda riskin hala var olduğu unutulmamalıdır.

- Mail olarak : **PGP/GPG** , **Protonmail** gibi şifrelenmiş mail servislerini önerebilirim.
- Chat sistemleri olarak : **IRC** , **JABBER** , **İCQ** , **TELEGRAM** kullanmamız artı sağlayacaktır.

Herkese açık ağlara bağlanmamak , **modem güvenliğini** sağlamak , sırf para vermemek için crackli uygulamaları edinmenin ve **warez** programları kullanmanın sizi riske atacağını unutmayın.

Trafiği şifrelerken basit yoldan DNS adresinizi değiştirebilirsiniz.
VPN ya da PROXY kullanıp bağlantınızı şifreleyerek daha anonim bir halde gezmenizi sağlayabilirsiniz.

Ek olarak **Privacy Badger , No script , Don't track me** gibi eklentileri kurarak , bilgi toplayan servisleri engelleyebilirsiniz. Trafiğimizi şifrelediğimiz gibi , mutlaka kullanmakta olduğumuz sistemi de şifrelemeliyiz.

Unutmayın size gelebilecek olası tehditler sadece siber dünya üzerinden değil fiziksel olarak da gelebilmektedir. Örneğin , **Bad USB** gibi zararlı donanım cihazları ile ,açık bıraktığınız ve başından ayrıldığınız bilgisayarınıza sadece bir flash disk takıp çıkarmak kişisel verilerinizin çalınmasına neden olacaktır.

Günümüzde genel olarak birçok kurum ve şirketlerde nedense işletim sistemi olarak windows tercih ediliyor , sebebi ise kullanımı kolay ve işletim sistemine alışkın olmamızdan kaynaklı. Windows gibi işletim sistemlerinin çok güvenli olduğunu söylememiz doğru olmaz.

Bu sebeple ; işletim sistemi olarak mümkünse , **Parrot OS** kullanın. Sebebi ise özgür yazılım kullanılarak açık kaynak kodlu halde olmasıdır. **Parrot OS,** GNU/Linux tabanlı işletim sistemi olup, diğer GNU/Linux işletim sistemlerine göre daha stabil çalışmaktadır.

Verileri doğru yerde sakladığınızdan emin olun.

İşini profesyonel olarak yapan , bir araştırmacı gazetecinin tartışmasız en önemli sorumluluklarından olan **veri güvenliği** dikkat edilmesi gereken diğer hususlardan bir tanesidir.

Bulut yedeklemelere dikkat etmekte fayda var . Her şeyi oraya atmanız demek bilgilerinizin ortaya çıkabilmesi demektir. Bu yüzden fiziksel yedekleme, sunucu yedeklemelerine göre daha güvenlidir ancak fiziksel yedeklemenin ise şöyle bir riski vardır: **"Fiziksel yedekleme"** yaptığınız diskin yabancı kişilerin ellerine geçebilmesi riskli var. Bu yüzden fiziksel yedeklemelerde mutlaka ya diski şifreleyin ya da dosya klasörlerine parola koyun. Kullanmış olduğunuz program ve işletim sisteminizi daima güncel tutunuz. Güncellemeleri zamanında yapmayı unutmayınız.

Yabancı Kaynaklardan Gelen Dosya ve Bağlantılar

Özellikle bilinmeyen kaynaklardan gelen mesajları direk açmayın.
Sadece bir resim görüntülemek ile hacklenmeniz mümkün. Güvenmediğiniz dosyaları offline bir ortamda sanal makinede açabiliriz.

Mobil Casusluk kurbanı olmayın.

2011 ‘de yapılan açıklamaya göre **“Kaspersky”**, mobil cihazlar için yaklaşık 5.300 yeni kötü amaçlı yazılım tespit ettiğini belirtti. 2012’de bu sayı 6 milyona çıkarken , Günümüzde ise bu sayı kat ve kat artmış durumda.

Bir sonraki yazım olan **“ Siber Espiyonaj Faaliyetlerinde Gazetecilerin Yeri** adlı yazımızda görüşmek üzere...

yazar : Eren Talha Altun
https://twitter.com/erenaltun_tr