Home-Office Güvenlik Rehberi

Taha Mumcu

Covid-19 ile beraber köklü dijital dönüşümler geçiren işletmelerde güvenlik en önemli konulardan birisi. Veri ihlalleri şirketlerin itibarına zarar verirken maddi kayıplara da neden oluyor. Home-office çalışma modeli artık bazı şirketler tarafından kalıcı hale getirilmiş durumda. Birçok şirket pandemi sonrası ofislerine dönmeyi planlamıyor.

Home-office çalışanlar siber güvenlik bilincine sahip olmadığı ve belirli önlemleri almadığı sürece veri güvenilirği risklerine karşı savunmasız. Home-office çalışma modeli bireylerin işe gidip gelerek kaybettikleri vakti onlara geri kazandırıyor.

Home-office çalışmanın getirdiği özgürlüklerin yanısıra siber riskler ortaya çıkıyor.

Başlıklar [Gizle]

- Güvenilir Wi-Fi
- Phishing Saldırıları
- Kimlik Doğrulama
- Güçlü Şifreler
    - Şifreli İletişim

Güvenilir Wi-Fi

Şirket ağına VPN ile bağlanıyor musunuz? Home-office çalışırken kullandığınız ev ağınız ne kadar güvenilir? Ev Wi-Fi ağının şifresi basit bir biçimde siber saldırganlar tarafından bulunabilir mi?

Home-office modelinde VPN teknolojisi vasıtası ile çalışanlar ofistelermiş gibi güvenilir ofis ağına bağlanabiliyor. VPN (Sanal Özel Ağ) teknolojisi uzun uzun yıllardan beri şirketler tarafından home-office çalışanların ve sık seyahat eden çalışanların şirket ağına bağlanabilmesi için kullanılıyor.

Ev Wi-Fi ağının şifresi komplike rakam ve harflerden oluşmalıdır. Siber saldırganlar ardışık rakam ya da harflerden oluşan ya da basit tahmin edilebilir sözcüklerden oluşan şifreleri kaba kuvvet saldırısı ile kısa bir sürede bulabilir.

VPN kullanılan bilgisayar ve aynısı cihazların siber hijyeninin sağlanmış olması gerekiyor. Aksi takdirde, bir home-office bilgisayarına bulaşan virüs, fidye programı gibi kötücül programlar şirket ağına bağlı diğer cihazlara da berişebilir.

Phishing Saldırıları

Siber saldırganlar phishing e-postaları ya da mesajları göndererek şirket ya da çalışanların bilgilerini çalmaya çalışırlar.

2015 yılının Aralık ayında Ukrayna'da bulunan üç enerji dağıtım şirketinin bilgi sistemlerinin siber saldırganlar tarafından ele geçirildiği ortaya çıktı. Siber saldırganlar elektrik tedariğini sekteye uğrattı ve 200 binden çok insan bir ve altı saat aralığında elektriksiz kaldı.

Siber saldırganlar bu saldırıyı kolay bir spear-phishing (zıpkınla avlama) olarak bilinen ve belirli şirket çalışanlarını hedef alan phishing saldırısı ile başlattı. Microsoft'tan gelmiş gibi gözüken ve bir Office güncellemesine benzeyen dosya ekindeki makroyu bir çalışanın etkinleştirmesi sonrası siber saldırganlar enerji dağıtım şirketinin sistemine girmeyi başardı.

Phishing e-postaları bir mega saldırının başlangıcı da olabilir. Bir e-postanın phishing (yemleme) e-postası olduğunu Nasıl anlarsınız?

- Resmi şirketler e-posta üzerinden sizden bilgi istemez. Sizden e-posta ile bilgi isteyen ya da dosya eki göndererek cihazınıza indirmenizi isteyen e-postalar büyük ihtimalle phishing e-postasıdır. Hesap şifrenizi, kredi kartı bilgilerinizi, TC kimlik numaranızı ve aynısı bilgilerinizi e-posta üzerinden paylaşmayınız.
- Hesabınızı kurtarmanız için beklemediğiniz anda gelen e-postadaki urle tıklamayın ya da dosya ekini indirmeyin. Söz konusu hesaba tarayıcıdan normal bir biçimde girin ve hesabınızda şüpheli etkinlik olup olmadığını teyit edin.
- Resmi şirketler e-postada isminizde hitap eder. ''Sevgili kullanıcı'' ya da ''Sayın Kullanıcı'' gibi hitaplar siber saldırganların toplu e-posta attığını gösterir.
- Resmi şirketler domain e-postalarına sahiptir. E-posta adresi komplike harf ve rakamlardan oluşuyorsa o bir phishing e-postasıdır.
- Resmi e-postalarda yazım hatası genelde olmaz. Kötü bir Türkçe ile yazılmış bir e-posta spam olabilir.
- Resmi e-postalarda beklenmedik .exe, .zip gibi dosya ekleri bulunmaz. Beklemediğiniz dosya eklerini açmayın ve cihazınıza indirmeyin.

Kimlik Doğrulama

Şirketinizin sağladığı cihazlarda iki etkenlü kimlik doğruluğunu sağlama var mı? Çok etkenlü kimlik doğruluğunu sağlama vasıtası ile şifrenizi ele geçiren siber saldırganların hesaplarınıza ulaşmasını engel olabilirsiniz.

Güçlü Şifreler

Ofis içi iletişimin tamamıyla online sağlandığı home-office çalışma modelinde güçlü şifreler ve doğru şifre paylaşımı oldukça önemlidir. Güvenilir parola yöneticileri vasıtası ile şifreleri açık bir biçimde yazmadan iş dostlarınızla paylaşmanız mümkün. Parola yöneticileri sveri ihlaline maruz kalmış şifreleri belirler ve sizin için güçlü şifreler oluşturur.

Şifreli İletişim

Ofis içi iletişimi home-office çalışırken Nasıl sağlıyorsunuz? Önemli şirket verilerini içeren dosya ve belgeleri güvenilir e-posta sağlayıcıları ve mesajlaşma programları üzerinden paylaşmanız gerekir.

ProtonMail, Mailfence, Tutanota ve Counterfence güvenilir e-posta hizmetleridir. E-postaları lisanslı bir antivirüs programı ile taramayı unutmayın.

Home-office çalışırken şifreleme sağlamayan Twitter, Instagram ya da Telegram kullanmaktan kaçının. Telegram uçtan uca şifrelemeyi ‘’Secret Chat’’ özelliği aktifleştirildiğinde sağlar. Aksi takdirde, Telegram üzerinden yapılan iletişim Telegram serverlarında saklanır.

Signal tüm iletişimlerinizi uçtan uca şifreler. Açık kaynak koduna sahiptir. Home-office çalışırken Signal kullanabilmeniz mümkün.

Güncel yazı ve projeleri instagram'da duyuruyorum. Takip et, iletişimde kalalım ✓@tahamumcu