

Elk.Elo. Müh. E. Önder Köktürk
onder@kokturk.com

Mart ayı başında 1 haftadan kısa bir süre içinde ofislerdeki personel



Kişisel bilgisayarlarda notebook, tablet, telefon kullanım oranının artması ve bu cihazların üzerinde kamera

ve ses sistemlerinin hazır gelmesi olayı farklı bir noktaya taşıdı. Mobil olmayan masaüstü bilgisayarlar içinde çok ekonomik fiyatlara ekran üstü bir kamera bağlanabilir oldu. Son 5-10 yılda internet hızlarının artması, ürünlerin ev pazarına kadar yaygınlaşması, son kullanıcıların yazılım temelli ses ve görüntülü iletişimini rahatlıkla yapabilmesini sağladı. Bugün bize sıradan bir imkanmış gibi gelse de eskiden ses ve görüntülü bir yayın yapmak için pahalı sistemler gerekiyordu. Bugün herhangi bir son kullanıcı web veya facebook, instagram, youtube gibi sosyal medya ortamından bir klik ile çok kolay bir şekilde yayın yapabiliyor. Ama iş ortamlarına yönelik daha fazla kişinin karşılıklı etkileşimde bulunabileceği toplantılar için bu işe özgü çözümler kullanılması gerektiği öğrenildi.

Bu süreçte, ticari rekabet, reklam veya pazarlama gücü olan firmalar, kurumlarında söz sahibi teknik veya teknik olmayan kişiler, kendi bilgilerine veya çevresindekilerin kullandığı ürünleri sorup araştırmaya başladılar. Bu tip ortamlarda şirket içi fiziki toplantılardan daha farklı bir kültür gereksinimi ve deneyimi daha oluşmadan birkaç hafta içinde “o marka iyiymiş”, “şu marka şunu yapamıyormuş”, “o üründe sayı süre sınırı varmış”, “bizim merkez şunu almış”, “bizim merkez şunu almış, mecbur onu kullanacağız” gibi her kafadan bir ses çıkan bir döneme girildi.

Sonra “biz filanca ürünü denedik, iyiydi”, “şunda ses çok kötüydü”, “filanca kişi de bağlanınca sistem çöktü”, “ekranda donmalar var”, “ses ile görüntü eş zamanlı değil”, “tüh, kayıt etmeyi unut-

muşuz”, “bizim yazılımda kayıt imkanı yokmuş”, “hmm, bu ücretsiz sürümmüş, o yüzden filanca özellikler kapalı”, “ücretlisi de çok pahalıymış...” gibi söylemlerle beraber kullanımın yaygınlaşması ve ister sistemin altyapısına bağlı ister katılımcıların internet hat hızlarına bağlı kalite sorunlarının yaşandığı bu sistemin yavaştan benimsendiği ama kullanımının yer yer sıkıntılı ve zor olduğunu bir döneme girildi.

İş amaçlı toplantı yanında, evde kalan veya zamanı olan, hemen hemen her konuda yayın patlamasının yaşadığı yeni bir döneme geçildi. Bunu “hacklendik”, “o yazılımlar zararlıymış”, “bilgiler çalınıyormuş”, “filancanın banka hesabı boşaltılmış”, “Çin’in güvenlik standarttı ile ABD’ninkii uymuyormuş”, “32bit güvenlik kullanıyormuş, güvensizmiş” yarı yalan yanlış bir sürü söylemin ve tedirginliğin hakim olduğu, eldeki ürünlerin çelik çomak gibi değiştirildiği ve güvensizliğin arttığı bir dönem izledi.

Peki bu söylenen olumsuzlukların aslı var mıydı?

Çok kullanılan, kullanıcısı yüksek olan ortamlar, kötü niyetli kişiler tarafından da daha fazla ilgi odağı olurlar. Bu süreçte yıldızı daha da yükselen e-konferans yazılım firmalarından birisi müşterileri bilgilerini çaldırdı. (Bu durum pek çok firmanın başına gelen en istenmeyen en kötü şeylerden birisidir. Çünkü verisini çaldıran firmanın ticari itibarı, prestiji zedelenir, çalınan bilginin içeriğine göre kişiler, kurumlar maddi ve manevi zarar görebilir.) Eskiden bu konular daha sumen altı edilirken artık dünyada GDPR, ülkemizde KVKK’nın yasal düzenlemeleri ve çeşitli diğer sebeplerden bildirilmek zorunda kalınıyor veya şeffaflık, yeniden güven sağlama adına bizlerle paylaşıyor. Çalınan kişisel bilgiler (ad soyad, doğum tarihi, eposta adresi, giriş kodu ve

şifreler) genelde para ile satılır. Bunu alan kötü niyetli kişiler o kişilerin hesapları ile erişim sağlayarak büyük zararlar verirler.

Peki hangimiz, sürücü olsun, yolcu olsun bir araca binmeden çevresini şöyle bir dolaşıp, göze çarpan bir olumsuzluk var mı diye bakıyor?

Kiminiz “biz tamirci miyiz?” “Motor meslek ustası mıyız?” diyor olabilir. Fakat bu araçlarda herhangi bir olumsuzluğun kendi canımıza veya diğer kişilerin canına etki edecek ölümcül kazalara neden olabileceği konusunda herkes hemfikir. Patlak veya inik bir lastik, yağ ya da yakıt sızıntısı olan bir araç hareket halinde iken maddi, manevi hasarlı bir kazaya neden olabilir. Aslında başında 5-10 saniyelik bir göz kontrolü ile bu riski azaltabilir.

Bilişim sistemlerini aynı yaklaşımla kullanmaya ne dersiniz?

Bilgisayar, mobil cihaz ekipmanlarınızın “işletim sistemlerinin orijinal ve güncel olması, güncel bir anti virüs yazılımı, internet erişimi için güvenlik duvarları, VPN bağlantılar kullanmak gerektirir...” gibi detaylara değinmeyeceğim. Bunlar imkanı olan veya farkındalığa sahip kurumlar ve kullanıcılar için olmazsa olmaz noktalar. Fakat en mükemmel sistemin en zayıf halkası her zaman son kullanıcıdır. Yazımız son kullanıcıların bilişim güvenliği bilincini arttırmaya ve farkındalık kazandırmaya yönelik hazırlanmıştır.

Bugün az çok herkes bir bilişim sistemine kayıt veya giriş yaparken bir kullanıcı adı ve şifre gerekeceğini biliyor.

1. Her yerde veya çoğunlukla aynı şifreyi kullanıyor musunuz?
2. Zorunlu durumlar hariç kayıt esnasında doğum tarihi, anne kızlık soyadı gibi size ait kritik kişisel veri sorularına doğru cevaplar veriyor musunuz?
3. Şifreleriniz isim, doğum tarihi (hasan1990 ..) gibi sosyal mühendislik



ile kolayca tahmin edilebilir içeriğe sahip mi?

4. Şifreleriniz 8 karakterden az ve sadece harf veya sayılardan mı oluşuyor?
5. Kullandığınız şifreler içinde 123456, password, 12345678, qwerty, 123456789, 12345, 1234, 111111, 1234567 var mı?
6. Şifreleri belirli sıklıkta değiştirmek size gereksiz veya zor geliyor mu?
7. Bir siteye adresi yazarak gitmek yerine Google veya benzeri arama motorlarına kelime yazıp ilk gelen linke tıklayarak gidenlerden misiniz?

Cevaplarınız çoğunlukla “evet” ise maalesef “yüksek risk” grubundasınız demektir. Peki, şifre güvenliği için neler yapabilirsiniz

Farklı şifreler kullanın

Verizon'un 2019 yılı veri sızıntı araştırma raporuna göre, araştırmaya katılanların %50'den fazlası aynı şifreyi birden fazla yerde (ortalama 15) tekrar kullanıyorlar. Evinizi, arabanızı ve ofisinizi kilitlemek için aynı anahtarı kullandığınızı ve anahtarın kötü niyetli kişilerde olduğunu düşünün.

Bu riski ortadan kaldırmak için her hesap için benzersiz bir şifre oluşturun. Her parolanın tahmin edilmesi zor, en az sekiz karakter ve karmaşık (büyük/küçük harf, sayı ve noktalama) işaretlerinden oluştuğuna emin olun. İnsanların yüzde 60'ı hatırlanması gereken çok fazla şifre olduğunu ve farklı şifreleri yönetmenin zor olduğunu söylüyor. Şifrelerinizi oluşturmanıza, korumanıza ve takip etmenize yardımcı olacak şifre yönetim yazılım çözümleri kullanmakta bir çözümdür. Bu yazılım-

lar karmaşık şifreler oluştururlar ve bilgileri kriptolayarak güvenli olarak saklarlar. Sizin kullanım esnasında sadece kasaya giriş şifresini bilmeniz yeterlidir. Bu size zor geliyor ise siber korsanların çevrimiçi olmalarından dolayı size fiziken uzak olduklarını varsayarak şifrelerinizi güvenli kağıt veya defter üzerinde, onları da güvenli bir yerde saklamanız yeterlidir.

İki faktörlü kimlik doğrulama kullanarak bir adım daha ileri gidin

İki Adımlı Doğrulama (2FA veya MFA olarak da bilinir.) kullanmak, birisinin şifrenizi ele geçirse bile hesabınıza yetkisiz erişim elde etme şansını önemli ölçüde azaltır. Ancak, son kullanıcı anketlerine katılan her üç kişiden biri (% 30) 2FA kullanmadığını veya onun ne olduğunu bilmediklerini söylemektedir. 2FA, kullanıcı adınızın ve şifrenizin üstünde hesabınızda her oturum açışınızda ek bir güvenlik adımıdır. İkinci doğrulamaya örnekler: SMS ile gelen tek kullanımlık mesajlar, akıllı telefonlara yüklenen özel uygulamalar tarafından oluşturulan altı haneli kodlar veya USB noktalarına takılan fiziksel güvenlik anahtarları. Bugün regülasyonlar gereği finans/ internet bankacılığı uygulamalarında 2FA zorunludur. Bu sebeple toplumda bilinirlik ve kullanımı eskiye göre daha yaygındır. Sizde bunlar dışında kullandığınız eposta yazılımları, sosyal medya uygulamaları için 2FA güvenlik ayarlarını aktif ederek kullanım alanınızı genişletebilirsiniz.

Uygulamalarınızı güncel tutun.

Genellikle Siber korsanlar yazılım açıklarını ve zafiyetleri kullanarak bilgilerinize ve sistemlerinize erişirler. Çevrimiçi etkinliğinizi korumaya yardımcı olması için, tüm cihazlarınızda her zaman yazılımların en güncel sürümünü kullandığınızdan emin olun. Anket sonuçları, katılımcıların %79'unun yazılımlarını güncelleme-

onemini anladıklarını söylerken, üçte biri bunu düzenli olarak yapmadıklarını söylemektedirler. Yazılım güncellemeleri otomatik olarak ayarlansa da ara ara bu sürecin düzgün işlediğini manuel olarak kontrol etmelisiniz. Aşağıdaki işletim sistemlerini kullanıyorsanız, cihazlarınızdaki yazılımı nasıl kontrol edeceğinizi ve nasıl güncelleyeceğinizi öğrenebilirsiniz:

- | | |
|--------------------|--------|
| a. Windows desteği | b. Mac |
| c. Android | d.iOS |

Kamera ve mikrofon kullanımı

Notebook ve mobil cihazlarda ses ve görüntü donanımları cihaz ile gelir. Kamera ve mikrofon kullanacak bir uygulama açtığınızda kontrolün sizde olduğuna emin olmalısınız. Web kamerası gösterge ışığı yanıyor veya web kamerasını açmamış olsanız bile anormal davranıyorsa, bir şeylerin doğru olmayabileceğinin bir işaretidir. Bunun açık bir uygulamadan kaynaklanıp kaynaklanmadığını kontrol ederek, yazılımların başlangıç ayarlarının (kamera vs.) kapalı olarak ayarlanması önemlidir.

Ayrıca bazı zararlı yazılım bulaşmış makinelerdeki kamera ve mikrofonlar, cihaz sahibinin haberi ve kontrolü dışında da kullanılmaktadır. Bu sebeple, kullanılmadığı zaman dahili kamera ve mikrofon sensörü önüne bir yapışkan bant kapatmak harici cihazlar da ise kablusunu çıkarmak faydalı olabilir.

Ofis ortamı dışında özel alanlardan katıldığınız konferans uygulamaları için çoğunda var olan “sanal arka fon” özelliği ile görüntüde sizin (yüzünüz) dışınızda kalan sabit (oda içi) görüntüyü bulanık hale getirebilir veya bir fon resmi ile kaplayarak özelinizi gizleyebilirsiniz.

Sadece bu basit birkaç noktaya dikkat ederek siber dünyadaki güvenliğinizi arttırabilir ve risklerinizi azaltabilirsiniz.

