

Telefonunuz Yakında Sizi Kulağınızdan Tanıyacak

Her insanda kendine özgü bir şekle sahip olan parmak izini, avuç içi damar dizilimini, göz retinasını tarayarak kimlik doğrulaması yapan biyometrik sistemlerle uzun zamandır tanışıyoruz. Hatta günümüzde parmak iziyle kimlik doğrulaması yapamayan cep telefonlarına dudak bükme başladı. Japon bilişim şirketi NEC ise bu konuya değişik bir yaklaşım getirerek, kulak içi boşluğundan yankılanan sesi analiz etme yoluyla kimlik doğrulama yapabileceğini keşfetmiş. Sistem, her insanın kulak boşluğunun farklı şekilde olması ve bunun da sesin



farklı şekilde yankılanmasına yol açması ilkesine dayanıyor. İçeri küçük bir ses veriyorsunuz, yankılanan sesin frekansını analiz ediyorsunuz ve cihazı kulağına tutan kişinin doğru kişi olup olmadığını anlıyorsunuz. Bu sayede telefonunuzun parmak izi algılayıcısını bulup parmağınızı basmanıza gerek kalmadan, sadece kula-

ğınıza tutarak kimlik doğrulaması yapabileceksiniz veya telefonun kulaklığı kulağınızda takılı olduğu sürece telefon doğru kişinin elinde olduğunu bilecek ve ona göre davranacak. Sistemin yaklaşık 1 saniyede doğrulama yapabildiği ve yüzde 99 doğru sonuç verdiği belirtiliyor. Detaylar bit.ly/earbiometrics adresinde.

İlk başta "bu da nereden çıktı" dedirtse de, kulak boşluğundan biyometrik kimlik doğrulaması yapmak günlük hayatta bir hayli işe yarayacak gibi duruyor.

Korsanların İnsafına Kalan Hastane 17 Bin Doları Ödedi

Bu köşeyi düzenli takip ediyorsanız "ransomware" adı verilen fidye yazılımlarıyla ilgili sıkça bir şeyler yazdığım dikkatinizi çekmiştir. Ama bu konuyla ilgili öyle haberler geliyor ki yazmadan da edemiyorum. Geçen ay Hollywood'daki Presbyterian Medical Center adlı sağlık kuruluşu, bu tür bir yazılımın kurbanı oldu. Büyük ihtimalle bir e-posta linkine tıkladığında sisteme giren şifreleme yazılımının sisteme bulaşmasıyla hastanenin elektronik hasta kayıt sistemine erişim tamamen devre dışı kaldı. Durum o kadar ciddi bir hal aldı ki, hastanedeki acil hastalar başka hastanelere nakledilirken, hastane ekibi hasta kayıtlarını düzenlemek ve doktorlarla paylaşmak için yeniden kâğıt, kalem ve faks kullanmak zorunda kaldı. Sorun saldırıdan 10 gün sonra, hastanenin kayıtlarını yeniden eski haline getirmeye yarayacak şifreleme anahtarını alabilmek için son çare olarak saldırıyı gerçekleştiren gruba 40 Bitcoin, yani yaklaşık 17 bin dolar fidye ödemesiyle çözülebildi. Bu olay, şimdiye dek gördüğüm siber saldırı çeşitleri arasında en can sıkıcısı olan fidye yazılımlarının kilit hizmet noktalarında ne kadar büyük tehditlere yol açabileceğini gözler önüne seriyor.

Bu konuda dikkatli olmakta ve bir an önce kullanıcı bilincini yerleştirmekte fayda var. Konuya dair *Los Angeles Times*'ta yayınlanan haberi bit.ly/hospitalransom adresinde okuyabilirsiniz.



Hastanenin fidye yazılımlarıyla olan macerası 10 günlük hizmet kesintisinin ardından 17 bin dolarlık fidyenin ödenmesiyle sonuçlandı.