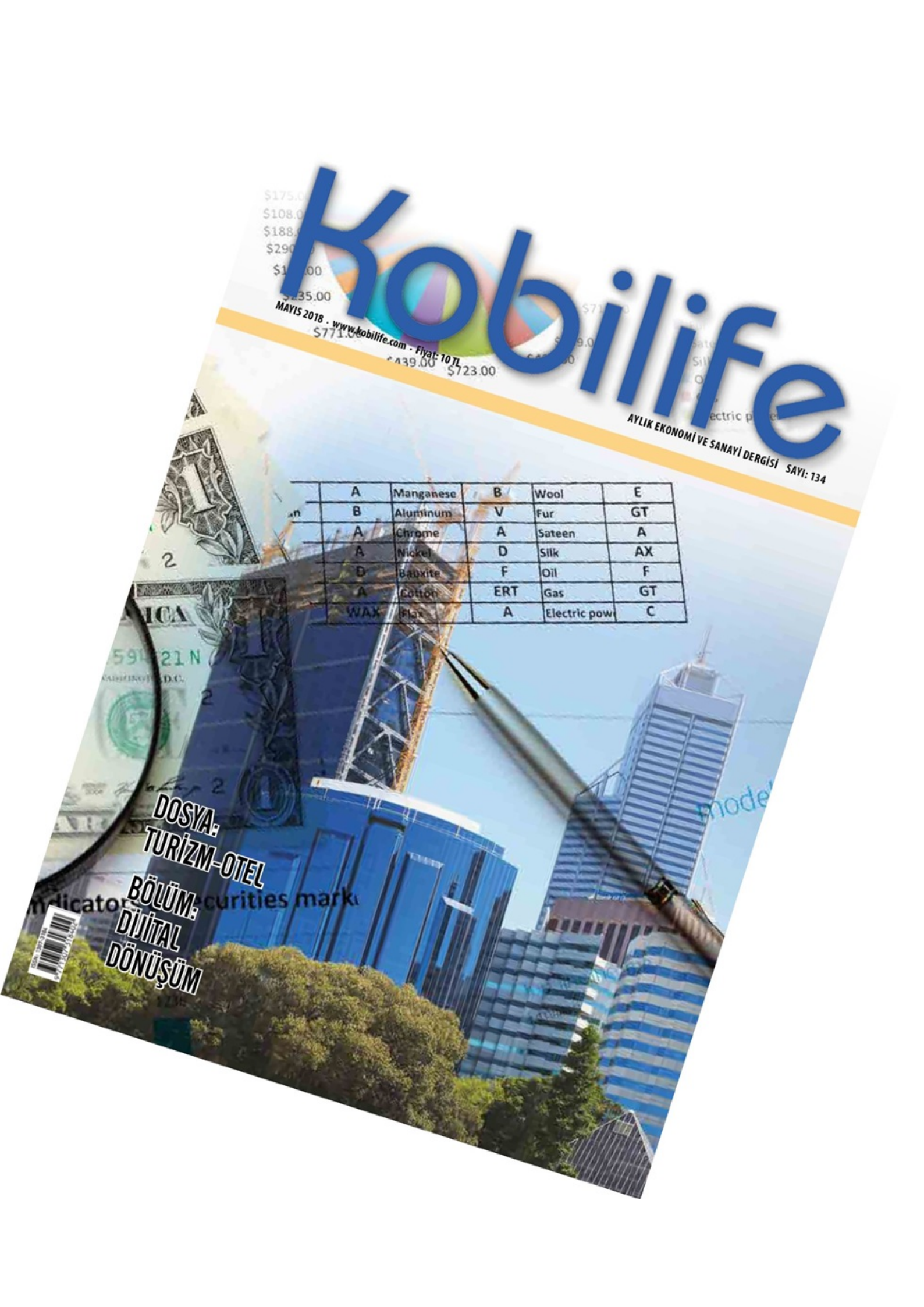
Kobilife

AYLIK EKONOMİ VE SANAYİ DERGİSİ SAYI: 134

MAYIS 2018 · www.kobilife.com · Fiyat: 10 TL



Yayın Adı : Kobi Life
Referans No : 77768848
Dağıtım alanı : Ulusal
Yayın Periyot : Aylık
Yayın Tipi : Dergi
Yayın Tarihi : 01.05.2018
Sayfa : 28
Tiraj : 14500
Reklam E.($) : 3930,61
AJANS PRESS

ŞİRKETLERİN SİBER GÜVENLİĞİNİ RİSKE ATAN 5 ÇALIŞAN HATASI
SİBER TEHDİT DIŞARIDA DEĞİL İÇERİDE
ÇALIŞANLARIN YAPTIĞI BU 5 HATA SİBER RİSKLERİ ARTIRIYOR

Hoşnutsuz eski çalışanlara ya da şu an beraber çalıştığınız kötü niyetleri olan kişilere karşı şirketinizin hassas verilerini nasıl koruyabilirsiniz? Bir ortağınız ya da tedarikçiniz bilerek veri çalıyorsa ne yapmalısınız? Peki çalışanlarınız tarafından şirketiniz için kritik önemdeki bilgilerin bilinçsizce riske atılabileceğini biliyor musunuz? Şirketler için asıl siber tehdidin dışarıdan değil içeriden geldiğine dikkat çeken Komtera Teknoloji uzmanları, şirketleri uyararak iç tehditlerin ortaya çıkmasına neden olan 5 hatayı sıralıyor.

Bir iş yerinde çalışmaya devam eden, eskiden çalışmış olan veya bir şekilde şirketle sıkı iş ilişkisinde bulunan kişilerin şirket için hassas bilgilere sahipken veri sızıntısına neden olmasına iç tehdit deniyor. Bu durum kötü niyetli kişiler tarafından gerçekleşeceği gibi çoğu zaman çalışanların istemeden yaptıkları hatalardan da kaynaklanabiliyor. Bilişim güvenliği alanındaki dağıtım ve çözümleriyle pazarda lider konumda bulunan Komtera Teknoloji'nin önerileriyle, çalışanlarınızın istemeden neden olduğu iç tehditleri engelleyebilir ve şirketiniz için genel risk seviyeni azaltabilirsiniz.

Çalışanlar tarafından bilinmeden yapılan bu hataların sonuçları, şirketler için diğer iç tehditlerle eşit derecede problemlere neden oluyor. Araştırmalar 2017'deki veri sızıntılarının dörtte birinin de bu hatalardan oluştuğu gösteriyor. Bu nedenle, verilerin yanlışlıkla nasıl kötüye kullanılabileceğini ve bilinçsizce oluşturulan iç tehditlerden nasıl sakınılabileceğini öğrenmek oldukça önemli.

Şirketlerde İç Tehdit Oluşmasına Neden Olan 5 Hata

İç tehditler, niyetlerinin gayet farkında olarak adım atıp şirkete zarar veren kişilerden oluşabileceği gibi, çalışanlar tarafından bilinçsizce yapılan hatalarla da ortaya çıkabilir. Komtera Teknoloji uzmanları, şirketleri iç tehditlere karşı uyararak iç tehditlerin ortaya çıkmasına neden olan 5 hatayı şöyle sıralıyor:

Düzenlemeleri ve Kuralları Yanlış Anlamak: Farklı şirketler farklı yasalar ve kurallara bağlı olarak çalışırlar. Eğer çalışanlarınız özellikle kendi işleriyle ilgili olan kuralları tamamen doğru anlamazlarsa şirketi riske atan hatalar yapabilirler. Bu nedenle, ekip arkadaşlarınızı ve özellikle yasalara, gerekliliklere çok dikkatli bir şekilde uyması gereken kıdemli üyelerinizi şirketin güvenliğine olumsuz etki yaratmamaları adına eğitmelisiniz.

Baştan Savma Kişisel Güvenlik: Hiç iş arkadaşınızın boş masası önünden geçerken bilgisayar ekranının tamamen aydınlık bir şekilde gözüktüğünü fark ettiniz mi veya yazıcının yanında duran, kimin olduğu belirsiz bir flash disk gördünüz mü? Güvenli hale getirilmeyen cihazlar, iç tehditlerin başlıca sebeplerinden biridir. Her çalışan kullandığı araçları güvenli kılacak adımların farkında olmalı ve onları her zaman uygulamalıdır, bilgisayarlarını evden işe getirseler ya da kullandıkları her cihazı şirket onlara sağlasa bile. Bu durum güçlü şifreler, çok faktörlü kimlik doğrulama, kişilerin birbirlerinin giriş kartlarını ödünç almaması gibi önlemlerle iyileştirilebilir. Güvenliğin düşünülmediği ya da baştan savma uygulandığı kişisel durumlar büyük bir iç tehdit yaratabilir.

Onaylanmamış Servisleri Kullanmak: SaaS (software as a service / hizmet olarak yazılım), bulut tabanlı uygulamalara internet üzerinden erişilmesi ve kullanılması demektir. SaaS araçları, depolama servisleri dahil, çalışanların işlerini daha hızlı ve etkili yapmasını sağlar. Tamamen iyi niyetli çalışanların bile zaman zaman hassas verileri bir kişisel bulut depolama hesabı kullanarak kendisine transfer edip depoladığı bilinen bir durumdur. Bu şekilde yoldayken veya evdeyken daha rahat çalışabilirler ancak iş yerlerini çok büyük boyutta bir tehlikeye açık hale getirirler. Çalışanlarınızı hangi servisleri kullanıp kullanamayacakları, onları nasıl güvenli hale getirecekleri, hangi veriyi ne zaman, nerede depolayabilecekleri konusunda bilinçlendirin. Böylece,

korunması gereken gizli verilerin bulut sistemiyle istenmeyen yerlere ulaşması ihtimali ortadan kalkmış olur.

Şirket Politikalarını Çiğnemek: Bir çalışan bir şirket politikasını unutabilir, anlamayabilir veya bilerek çiğneyebilir. Kötü niyetli köstebeklerin bu politikaları dinlemediği doğrudur ancak böyle bir niyeti olmayan çalışanlar da düşünmeden yaptıkları hareketlerle risk seviyesini arttırır ve tehditlere davetiye çıkarır. Çalışanların firma kurallarını ara ara baştan gözden geçirmelerini sağlamak ve kuralları gerektiğinde güncellemek iyi bir fikirdir ancak sadece kuralların yazılı olduğu bir şirket el kitabına güvenemezsiniz. Kural aşımını fark etmek için proaktif bir yol izleyerek ve hatalarına dair onları uyararak risk oranını azaltabilirsiniz. Bunun için ObservelT gibi kullanıcı risk analizi yapabilen analitik çözümler size yardımcı olabilecek araçlar kullanabilirsiniz.

Güncelleme Yapmamak: Kullanıcılar cihazlarını ve servislerini en son sürüm ile düzenli olarak güncellemezlerse şirketiniz sorunlara maruz kalabilir. Eğer bunu şahıslara bırakırsanız büyük problemlerle karşılaşabilirsiniz. Bu nedenle bir tür otomatik güncelleme sistemi uygulamanız gerekmektedir. Her ne kadar çok uzun sürecek bir güncellemenin bir iş gününün ortasında aniden başlayarak çalışmayı yavaşlatmasını ve çalışanları hayal kırıklığına uğratmasını istemeseniz de insan hatası veya tembelliği ile bir iç tehdidin ortaya çıkmasını engellemelisiniz. Bu otomasyon, güvenlik açıklarının ve kusurlarının şirketi zarara uğratmasından önce düzeltilmesinde önemli rol oynayabilir.