ŞİRKETİNİZİN İÇİNDEKİ İRLANDALILARA DİKKAT!

ÜNLÜ TEKNİK DİREKTÖR MUSTAFA DENİZLİ'NİN TÜRKİYE - İRLANDA MİLLİ MAÇININ ARDINDAN "İRLANDA'YI YENDİK AMA ÖNEMLİ OLAN İÇİMİZDEKİ İRLANDALILARI YENMEK" CÜMLESİ HALA HAFIZALARDA... "KENDİ İÇİMİZDE BİZE RAKİP OLANLAR" İÇİN KULLANILAN BU SÖZ, GÜNÜMÜZ DÜNYASINDA ŞİRKETLERİN SİBER GÜVENLİĞİ KONUSUNDA GEÇERLİLİĞİNİ KORUYOR. UZMANLAR, ŞİRKETTEKİ KÖTÜ NİYETLİ ÇALIŞANLARA KARŞI SİBER UYARILARDA BULUNUYOR...

Fotoğraflar: *Dünya Gazetesi Fotoğraf Arşivi*

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. 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. Bilişim güvenliği alanında çözümler sunan Komtera Teknoloji, şirketleri iç tehditlere karşı uyararak iç tehditlerin ortaya çıkmasına neden olan beş hatayı şöyle sıraladı:

DÜZENLEMELERİ VE KURALLARI YANLIŞ 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 KİŞİSEL GÜVENLİK

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.

ONAYLANMAMIŞ SERVİSLERİ 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.

ŞİRKETİNİZDE İÇ GÜVENLİK İÇİN NELER YAPMALISINIZ?

1. **Çalışanlar kendi işleriyle ilgili olan kuralları tamamen doğru anlamazlarsa şirketi riske atan hatalar yapabilirler.**

2. **Güvenli hale getirilmeyen cihazlar, iç tehditlerin başlıca sebeplerinden biridir. Her çalışan kullandığı araçları güvenli kılacak adımların farkında olmalı.**

3. **Çalışanlarınızı hangi servisleri kullanıp kullanmayacakları, onları nasıl güvenli hale getirecekleri, hangi veriyi ne zaman, nerede depolayabilecekleri konusunda bilgilendirin.**

4. **Kural aşımını fark etmek içir proaktif bir yol izleyerek ve hatalarına dair onları uyararak risk oranını azaltabilirsiniz.**

5. **Kullanıcılar cihazlarını ve servislerini en son sürüm ile düzenli olarak güncellemezlerse şirketiniz sorunlara maruz kalabilir.**

ŞİRKET POLİTİKALARINI ÇİĞNEMEK

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 artırır 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 ObserveIT 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.