Ticaretin e-Hali

E-TİS

E-Ticaret İşveren Sendikası

E-TİCARET İŞVEREN SENDİKASI DERGİSİ

2025 | Sayı 3 / Yıl 4

E-TİS' den Türkiye İhracatçılar Meclisine Ziyaret

Türkiye' nin İlk E-Ticaret Esnaf Odası ile E-Ticarette Devrim!

E-Ticarette Stopaj Gündemi

E-TİS Berlin/Bremen Temasları

TİSK Ortak Yarınlar Ödül Programı

Türkiye' de E-Ticaretin Görünümü Raporu Yayınlandı

2025

Türkiye' de Sendikacılık

Ahilik Haftası

İnstagram Yasağı En Çok Kobileri Vurdu

Worldef Sınırları Aştı! İstanbul' da Uluslararası E-Ticaret Buluşması

Oniki E- Ticaret & E- İhracat ve Tedarikçi Zirvesi 16 Ekim 2025

T.C. Çalışma ve Sosyal Güvenlik Bakanlığı Genel Müdürlüğü Ziyaret

E-Ticaret Zirvesi 9 Aralık 2025 Çırağan Sarayı' nda !

E-Röportaj
Ender SATICI Pazarlama Türkiye Kurucusu

Şirketler için Siber Güvenliğin Önemi:

GİRİŞ:

Bu makale, şirketler için siber güvenliğin neden öncelikli bir konu olduğunu tartışmakta ve özellikle e-ticaret başta olmak üzere tüm dijital faaliyet yürüten şirketlerde veri güvenliği, kullanıcı bilinci, güvenlik uygulamaları ve tehdit türleri üzerine kapsamlı bir analiz sunmaktadır. Ayrıca, iç ve dış tehditlere karşı alınması gereken önlemler, güçlü parola uygulamaları ve felaket senaryolarına karşı yatırım planlarının önemi vurgulanmaktadır.

Veri Güvenliği:

Günümüzde şirketlerin tüm bilgileri dijital ortamlarda saklanmaktadır. Dijital ortamlarda saklanan ve işlenen bilgilerin mali değeri paha biçilemez durumdadır. Dijital ortamlarda saklanan verilere gelebilecek zararlar sonucu şirketlerin mali zarar görmeleri yanında itibar kayıpları yaşamaları kaçınılmazdır.

Şirketlerin sistemlerinin güvenliği her zaman arka plana atılmaktadır. Sistemlerin güvenliğini sağlamak için bu konuda uzman kişilerden danışmanlık alarak yatırım planı oluşturulması gerekmektedir.

Sistemlerin güvenlik zafiyetlerini azaltmak için yapılması gerekenlerin en başında kullanıcıların bilinçlendirilmesi, lisanslı yazılım ve programlar kullanılması ve güncellemelerin zamanında gecikmeden takip edilerek yapılmasıdır.

Şirketiniz İçin En İyi Güvenlik Uygulamaları:

· Risk Değerlendirmesi Gerçekleştirin - Koruduğunuz şeyin değerini bilmek, güvenlik harcamalarının haklı çıkarılmasına yardımcı olacaktır.

· Güvenlik İlkesi Oluşturma - Şirket kurallarını, iş görevlerini ve beklentileri açıkça gösteren bir ilke oluşturun .

· Fiziksel Güvenlik Önlemleri - Ağ dolaplarına, sunucu konumlarına ve yangın önleme işlevlerine erişimi kısıtlayın.

· İnsan Kaynakları Güvenlik Önlemleri - Çalışanlar arka plan kontrolleri ile düzgün bir şekilde araştırılmalıdır.

· Yedekleme Yapma ve Test Etme- Düzenli yedeklemeleri gerçekleştirin ve yedeklerden veri kurtarma testi yapın.

· Güvenlik Yamalarını ve Güncelleştirmelerini Koruma - Sunucu, istemci ve ağ aygıtı işletim sistemlerini ve programlarını düzenli olarak güncelleyin.

· Erişim Denetimlerini Çalıştırma - Güçlü kullanıcı kimlik doğrulamasının yanı sıra kullanıcı rollerini ve ayrıcalık düzeylerini yapılandırın.

· Olay Yanıtını Düzenli olarak Test Edin - Bir olay yanıt ekibi istihdam edin ve acil yanıt senaryolarını test edin.

· Ağ İzleme, Analiz ve Yönetim Aracı Uygulayın - Diğer teknolojilerle bütünleşen bir güvenlik izleme çözümü seçin.

· Ağ Güvenliği Aygıtlarını Uygulama - Yeni nesil yönlendiricileri, güvenlik duvarlarını ve diğer güvenlik aygıtlarını kullanın.

· Kapsamlı Uç Nokta Güvenlik Çözümü Uygulama - Kurumsal düzeyde kötü amaçlı yazılımdan koruma ve virüsten koruma yazılımı kullanın.

· Kullanıcıları Eğitin - Kullanıcıları ve çalışanları güvenli prosedürlerde eğitin.

· Verileri Şifreleyin - E-posta dahil tüm hassas şirket verilerini şifreleyin.

Her Çevrimiçi Hesap için Benzersiz Parolalar Kullanın:

Umut URYAN
Sistem Merkezi CEO / ETİS Denetim Kurulu Üyesi

Muhtemelen birden fazla çevrimiçi (online) hesabınız vardır ve her hesabın benzersiz bir parolası olmalıdır. Hatırlanması gereken bir sürü parola var. Bununla birlikte, güçlü ve benzersiz parolalar kullanmamanın sonucu sizi ve verilerinizi siber suçlulara karşı savunmasız bırakır. Tüm online hesaplarınız için aynı parolayı kullanmak, tüm kilitli kapılarınız için aynı anahtarı kullanmak gibidir, eğer bir saldırgan anahtarınızı alırsa, sahip olduğunuz her şeye erişebilir. Örneğin suçlular phishing (oltalama) yoluyla parolanızı alırlarsa, diğer çevrimiçi hesaplarınıza girmeye çalışırlar. Tüm hesaplar için yalnızca bir parola kullanırsanız, tüm hesaplarınıza girebilir, tüm verilerinizi çalabilir veya silebilir ya da sizi taklit etmeye karar verebilirler.

Hatırlamak için çok fazla parola gerektiren çok sayıda çevrimiçi hesap kullanıyoruz. Parolaları yeniden kullanmaktan veya zayıf parolalar kullanmaktan kaçınmak için çözümlerden biri, parola yöneticisi kullanmaktır. Bir parola yöneticisi, farklı ve karmaşık parolalarınızı depolar ve şifreler. Bu yönetici, çevrimiçi hesaplarınıza otomatik olarak giriş yapmanıza yardımcı olabilir. Parola yöneticisine erişmek ve tüm hesaplarınızı ve parolalarınızı yönetmek için ana parolanızı hatırlamanız yeterlidir.

İyi bir parola seçmek için ipuçları:

· Herhangi bir dildeki sözlük kelimelerini veya isimleri kullanmayın
· Sözlük kelimelerinin yaygın yazım yanlışlarını kullanmayın
· Bilgisayar adlarını veya hesap adlarını kullanmayın
· Mümkünse "!" gibi özel karakterler kullanın @ # $% ^ & * ()
· On veya daha fazla karakter içeren bir parola kullanın

Şirket İçi Güvenlik Tehditleri:

Saldırılar, bir kuruluşun içinden kaynaklanabilir. Çalışan veya sözleşme ortağı gibi dahili bir kullanıcı kazara veya kasıtlı olarak şunları yapabilir:

· Gizli verileri yanlış kullanma
· İç sunucuların veya ağ altyapısı aygıtlarının işlemlerini tehdit etme
· Virüs bulaşmış USB ortamını kurumsal bilgisayar sistemine bağlayarak dış saldırıları kolaylaştırma
· Kötü amaçlı e-posta veya web siteleri aracılığıyla kötü amaçlı yazılımları (malware) ağa yanlışlıkla davet etme

İç tehditler ayrıca dış tehditlere göre daha fazla zarar verme potansiyeline sahiptir, çünkü dahili kullanıcılar binaya ve altyapı cihazlarına doğrudan erişebilir. Çalışanlar ayrıca kurumsal ağın, kaynaklarının ve gizli verilerinin yanı sıra farklı kullanıcı veya idari ayrıcalıkların düzeyleri hakkında bilgi sahibidir.

Saldırgan Türleri:

Saldırganlar, kişisel ya da finansal kazanç için güvenlik açığından yararlanmaya çalışan bireyler veya gruplardır. Saldırganlar, kredi kartlarından ürün tasarımlarına kadar değerli olabilecek her şeye ilgi duyuyor.

Amatörler — Bu insanlara bazen Script Kiddies denir. Genellikle saldırıları başlatmak için internette bulunan mevcut araçları veya talimatları kullanarak, az ya da hiç beceriye sahip olmayan saldırganlardır. Bazıları sadece meraklıdır, diğerleri ise becerilerini göstermeye ve zarar vermeye çalışırlar. Temel araçlar kullanıyor olabilirler ama sonuçlar yine de yıkıcı olabilir.

Hackerlar— Bu saldırgan grubu erişim elde etmek için bilgisayarlara veya ağlara girerler. Giriş amacına bağlı olarak, bu saldırganlar beyaz, gri veya siyah şapkalılar olarak sınıflandırılır.

Beyaz şapkalı saldırganlar, sistemlerin güvenliğinin geliştirilebilmesi ve zayıf yönleri keşfetmek için ağlara veya bilgisayar sistemlerine girerler. Bu girişler önceden izin alınarak yapılır ve her sonuç sahibine bildirilir.

Siyah şapkalı saldırganlar, yasadışı kişisel, mali veya siyasi kazanç için herhangi bir güvenlik açığından yararlanırlar.

Gri şapkalı saldırganlar, beyaz ve siyah şapkalı saldırganların arasında bir yerdedirler. Gri şapkalı saldırganlar bir sistemde bir güvenlik açığı bulabilirler. Gri şapkalı hackerlar, bu eylem amaçlarına uyuyorsa güvenlik açığını sistem sahiplerine bildirebilir. Bazı gri şapkalı hackerlar, diğer saldırganların yararlanabilmesi için internette güvenlik açığı hakkındaki gerçekleri yayınlar.

Organize Hackerlar — Bu hackerlar siber suçlular, hacktivistler, teröristler ve devlet destekli bilgisayar korsanlarıdır. Siber suçlular genellikle kontrol, güç ve zenginlik odaklı profesyonel suç gruplarıdır. Suçlular son derece sofistike ve organize, ve hatta diğer suçlulara hizmet olarak siber suçları sağlayabilir. Hacktivistler, kendileri için önemli olan konularda farkındalık yaratmak için siyasi açıklamalar yaparlar. Devlet destekli saldırganlar hükümetleri adına istihbarat toplar ya da sabotaj yaparlar. Bu saldırganlar genellikle yüksek eğitimli ve iyi finanse edilirler ve saldırıları hükümetleri için yararlı olan belirli hedeflere odaklanır.

Sonuç:

Sonuç olarak, burada belirtilen hususların ötesinde, tüm iş süreçlerini dijital sistemler üzerinde yürüten şirketlerin yalnızca mevcut değerlerinin değil, itibarlarının ve gelecek planlarının da ciddi tehditler altında olduğu gerçeği göz ardı edilmemelidir. Şirket yöneticilerinin bu riskleri öngörerek düzenli yatırım planları oluşturması, hem mevcut durumu hem de gelecekteki sürdürülebilirliği güvence altına almak açısından kritik önem taşımaktadır.

Unutulmaması gereken temel nokta, hiçbir sistemin mutlak güvenlik sunmadığıdır; her zaman, güvenlik önlemlerini aşmaya çalışan tehdit unsurları var olacaktır. Bu nedenle, şirketinizin tüm operasyonlarını sürdüren bilişim altyapısı için güçlü destek ve kapsamlı yatırım stratejileri geliştirmeniz

gerekmektedir. Sunucularınızın güncellemelerinin ve yedeklemelerinin düzenli ve eksiksiz şekilde yapılmasını sağlamak, çalışanlarınızı bilinçlendirmeye yönelik kurum içi politikalar uygulamak ve korsan yazılımlardan kesinlikle uzak durmak bu stratejilerin temel taşlarıdır.

Ayrıca, şirket ağınızı dış tehditlerden korumak için güvenlik duvarları gibi ileri seviye ağ güvenlik cihazlarına ve kullanıcı bilgisayarlarında etkin antivirüs çözümlerine yatırım yapmaktan çekinmeyin. Unutmayın, bir felaket yaşandıktan sonra atılan adımlar çoğunlukla telafisi güç veya maliyetli kayıplara yol açar; bu yüzden, olası tehditler gerçekleşmeden önce önlemlerinizi almak en akılcı ve sürdürülebilir yaklaşım olacaktır.