KÜÇÜK İŞLETMELER İÇİN BT GÜVENLİĞİ UYGULAMA KILAVUZU

İşletmenizin kapsamlı bir BT güvenliği korumasına sahip olduğundan nasıl emin olursunuz?

#protectmybiz

KASPERSKY lab

Küçük işletmeler çeşitli yapılara sahip olabilir. Ancak günümüz dünyasında, ister ofis dışında çalışan bir ekip, isterse de evden çalışan bir birey olun, hiçbir kuruluş çevrimiçi güvenliği yok sayma lüksüne sahip değildir. Çevrimiçi güvenlik herkesi etkileyen bir konudur.

Siber suçlar sık sık manşetlere çıkmasına rağmen, bu genellikle kurban çok büyük bir çok uluslu şirket veya hükümet olduğunda gerçekleşir. Ancak muhtemelen daha küçük olaylar aslında daha büyük öyküler içermektedir.

Yalnızca 2014 yılında, 143 milyon yeni kötü amaçlı yazılım örneği belirlenmiştir.[1] Bunların büyük çoğunluğu kendilerinin hedef olacağını düşünmeyen kişileri veya kuruluşları hedef almıştır.

Gerçekte herkes bir hedeftir. İyi haber şudur ki; hala hedef olmakla kurban olmak arasında çok büyük bir fark bulunmaktadır.

Genellikle konu sonunda hazırlıklı olmaya dayanır. Bu kılavuzu da bu nedenle hazırladık:
İşinizin güvenliğini koruma konusunda size gerekli bilgileri sunmak için.

? KÖTÜ AMAÇLI YAZILIM NEDİR?

Kötü amaçlı yazılım terimi, kötü bir amaçla tasarlanmış bilgisayar programları anlamına gelir. Bunlar genellikle kullanıcısının bilgisi olmadan cihazlara saldırır. Kaspersky Lab, kötü amaçlı yazılımların algılanması konusunda tüm diğer güvenlik tedarikçilerinden daha iyi en üst düzey puanlar almış olan bir dünya lideridir.[2]

? NEDEN KORUNMAYA İHTİYACIM VAR?

Siber suçluların işiniz üzerinde maliyet yaratan bir etkiye sahip olmaları için banka hesabınızı boşaltmaları gerekmez. Kötü amaçlı yazılımların neden olduğu kesinti, üretkenliğinizi ve nakit akışınızı etkileyerek, bir dizi istenmeyen sonuca neden olabilir. Bu sonuçlara karşı nispeten basit adımlarla kendinizi koruyabileceğiniz bilmek içinizin rahat olmasını sağlar.

1. AV Testleri
2. TOP3 2014 Bağımsız test sonuçları çalışması

GÜVENLİK KONTROL LİSTENİZ

İŞİNİZİ GÜVENLİK ALTINA ALMANIN İLK ADIMI, ÇALIŞMA ŞEKLİNİZE VE NERELERDE RİSKİ AZALTABİLECEĞİNİZE BAKMAKTIR. DOLAYISIYLA KENDİNİZE HIZLI BİR BT GÜVENLİĞİ SAĞLIK KONTROLÜ YAPIN:

KÖTÜ AMAÇLI YAZILIMA KARŞI KORUMA ✔

İşletme sigortası ile ilgili olarak, konu şirketinizi koruyacak ürünler olduğunda, alabileceğinizin en iyisini istersiniz. Virüslere karşı cihazlarınızı koruyan zengin özellikli bir yazılımı zaten daha önceden edinmemişseniz bunu bir öncelik haline getirmeniz gerekir.

Ne yazık ki, yalnızca çevrimiçi işlemler konusunda tedbirli olmak tek başına yeterli değildir. Bilinmeyen göndericilerden gelen eklentilerin açılmaması veya şüpheli sitelerden indirme yapılmaması gerektiğini hepimiz biliriz; ancak gerçekte pek çok virüs gizliliği ihlal edilmiş güvenilir kaynaklardan gelir.

İNTERNETTE GEZİNME DAVRANIŞLARI ✔

Personelinizi çevrimiçi eylemleri konusunda eğitmek sizi pek çok baş ağrısından kurtarabilir. Umarız, çalışanlarınız iş yerindeyken ziyaret etmemeleri gereken belirli site türleri olduğunu anlar. Ancak kişisel amaçla mobil cihazlar da kullanıyorlarsa (akıllı telefon veya tablet gibi), binadan ayrıldıktan sonra güvenlik konusunda daha az bilinçli davranabilirler. Dolayısıyla, iş makinelerinden erişilebilir olmamasını sağlamak için uygunsuz siteleri engellemek iyi bir fikirdir. BT güvenliği tehditleri konusunda genel farkındalığı artırmak da, çalışanların kişisel kullanımlarında güvenliklerini korumalarına yardımcı olur.

? BU BENİ NASIL ETKİLEYEBİLİR?

Hiç arkadaşınızdan veya aile üyenizden gelen ve açıldığında şüpheli görünen ilginç bir bağlantı içeren bir e-posta aldınız mı? Kötü amaçlı yazılım bir bilgisayarı etkilediğinde, bilgisayar kullanıcısının bilgisi olmadan bazı işlemler gerçekleştirebilir. Güvenilir kaynaklara her zaman güvenilememesinin nedeni de budur.

PAROLALAR ✔

Çalışanların ayrıca sembollerin, rakamların ve küçük ve büyük harflerin karışımından oluşan güçlü ve benzersiz şifreler kullandıklarından emin olmaları gerekir. Günlük kelimeler yalnızca doğru kelimeyi buluncaya kadar sözlükleri tarayan programlar tarafından kırılabilir. Ayrıca güçlü olsa bile, ele geçirilmiş bir parola birden fazla amaçla kullanılmışsa daha da büyük bir ihlale neden olabilir.

GÜNCELLEMELER ✔

Saniyede bir dört adet yeni kötü amaçlı yazılım algılanıyor.[3] Bunların önünde olmanız gerekir. Bu da, güvenlik yazılımınız için her gün otomatik güncellemeler almak, tüm diğer yazılımlarınızı mümkün oldukça güncellemek ve iş yerindeki herkesin aynı şeyi yaptığından emin olmak anlamına gelir. Unutmayın, güncellenmeyen yazılımlar siber suçluların, işletmelerin bilgilerine sızmak için kullandığı bir numaralı yoldur.

ŞU KLASİK PAROLA HATALARINDAN HİÇBİRİNİ YAPMADIĞINIZDAN EMİN OLUN:

1. "Parola" veya "123456" gibi hatırlaması kolay; ancak tahmin edilmesi de kolay bir parola kullanmak
2. E-posta adresinizi, adınızı veya kolayca edinilebilecek bir başka bilgiyi parola olarak kullanmak
3. Bir bilgisayar korsanının çok az araştırmayla yanıtlayabileceği, örneğin annenizin kızlık soyadı gibi parola hatırlatma soruları seçmek
4. Normal kelimeler üzerinde sonuna "1" rakamını eklemek gibi yalnızca çok küçük ve çok açık değişiklikler yapmak
5. Yaygın ifadeler kullanmak. "Seniseviyorum" gibi küçük cümleler bile kolayca kırılabilir

Ele geçirilmesi zor parolalar seçme konusunda daha fazla bilgi için konuyla ilgili blog yazımıza bakın.

3 AV Testleri

2014 YILINDA

295,500

YENİ MOBİL KÖTÜ AMAÇLI YAZILIM TEHDİTLERİ[4]

BANKACILIK ✔

Siber suçluların finansal bilgilerinizi ele geçirme konusunda sizi güvenilir sitelerin sahte versiyonlarına yönlendirmekten, faaliyetleriniz konusunda casusluk yapmak amacıyla kötü amaçlı yazılımlar kullanmaya kadar çeşitli yöntemleri vardır. Bu kişileri durdurmak için aktif önlemler almanız gerekir.

Dolandırıcıların bankanızın kimliğine büründükleri "kimlik avı" girişimlerine karşı uyanık olun: Her zaman güvenli bir tarayıcı kullanın ve herhangi bir siteye bilgilerinizi girmeden önce URL adresine dikkatli bir şekilde bakın. Ayrıca, e-posta mesajlarına görmemesi gereken kişilerin görebileceği bilgiler eklemekten kaçınmak da en iyisidir.

MOBİL CİHAZLAR ✔

Hareket halindeyken çalışmak artık günlük yaşamımızın bir parçası haline geldiği için siber suçlar da mobil cihazları gittikçe daha fazla hedefler oldu. 2014 yılında, her ay 295.500 yeni mobil kötü amaçlı yazılım tehdidi (özellikle akıllı telefonlar ve tabletler için yazılmış olanlar) belirlendi.[5] Telefonları ve tabletleri korumak, an az Mac'leri ve PC'leri korumak kadar önemli olmasına rağmen, şu anda küçük işletmelerin yalnızca %32'si mobil cihazların karşı karşıya olduğu risklerden haberdar.[6]

ŞİFRELEME ✔

Bilgisayarınızda saklı hassas verileriniz varsa bilgisayarınızın kaybolması veya çalınması durumunda bunların kullanılabilir olmaması için şifrelenmeleri gerekir. Bir işletme olarak elinizde tuttuğunuz bilgilerin korunması gereken son derece değerli varlıklar olduğunun farkına varmanız önemlidir.

? KİMLİK AVI NEDİR?

"Kimlik avı", siber suçluların sizi dolandırmak için kullanabilecekleri parolalar ve kredi kartı ayrıntıları gibi bilgileri edinmek umuduyla güvenilir bir kuruluşun kimliğine büründükleri durumdur.

4 ve 5 Kaspersky Lab'e Göre
6 Küresel Kurumsal BT Güvenliği Riskleri Anketi 2014

RİSKLERİ ANLAMAK

SİBER GÜVENLİK HAKKINDA KONUŞMAK GÜZELDİR; ANCAK ÇOĞUMUZ İÇİN BUNU ANLAMAK BAZEN ZOR OLABİLİR. BU SORUNLARIN GERÇEĞİNİ ZOR YOLDAN ÖĞRENMEK HİÇ KİMSENİN İSTEYECEĞİ BİR ŞEY DEĞİLDİR. BU NEDENLE, BİR DİZİ SENARYOYU, SONUÇLARINI VE BUNLARDAN NASIL KAÇINILABİLECEĞİNİ GÖSTEREREK KONUNUN ANLAŞILMASINI KOLAYLAŞTIRMAYA ÇALIŞTIK.

Çok pahalı bir fincan kahve

Günün son müşterisini uğurlayan Thomas, ofisi kilitleme işini iş ortağına bırakarak ayrılır. Ofisin hemen karşısında arkadaşıyla buluşacağı bir kafe bulunmaktadır. Tedarikçilerinden birisine ertesi gün ödeme yapılması gerektiğini hatırlayan Thomas bu işi unutmadan halletmeye karar verir.

Kafenin WiFi ağına bağlanmak için dizüstü bilgisayarını kullanır, bankanın web sitesine oturum açar ve para transferini yapar. Ödeme yapmayı unutmadığına memnun olarak, kafede oturur ve kahvesini yudumlar.

Hesabına bir sonraki kez baktığında hesapta para kalmadığını görür. O nedenini anlamaya çalışırken, personeli de ödemelerini beklemektedir.

BU NASIL OLDU?

Ne yazık ki; bilgisayarında yüklü kötü amaçlı yazılımdan koruma programı olmadığı için bilgisayarına kötü amaçlı bir tuş kaydetme programı yüklendi. Programı başlatan kişiler girdiği bilgilerin tümünün bir kaydını aldılar. Ve korunmayan halka açık WiFi'ı kullanırken işlem verilerinin ele geçirilmesi riski de vardı.

NE YAPABİLİRDİ?

Bankacılık işlemlerinin yalnızca kötü amaçlı yazılımdan koruma programlarının olduğu bilgisayarlardan ve her zaman güvenli bir tarayıcı üzerinden yapılması gerekir. Kaspersky'nin Güvenli Para özelliği ile, Thomas işlemin güvenli olduğundan kesinlikle emin olabilecekti.

Güvenli olmayan halka açık bir ağ kullandığı için aktardığı verilerin ele geçirilmesinin özel bir bağlantıya göre çok daha kolay olacağını da belirtmekte fayda vardır. Ancak Güvenli Para gibi bir özelliği kullanarak, kaygı duymadan çevrimiçi bankacılığın rahatlığından faydalanabilirdi.

Gittikçe daha sevimsiz hale gelen mesaj

Maria bir psikolog ve her sabah bir sonraki randevusunun onaylanıp onaylanmadığını görmek için web postasını açar. Gelen kutusunun en üstünde kullandığı bir sosyal ağdan gelen ve parolasını daha güçlü bir parolaya güncellemesini isteyen bir mesaj görür. Mesajda yer alan bağlantıya tıklar ve mevcut parolasını onaylar (bu parola bir öncekiyle aynıdır, yalnızca her iki harften birisini bir yıldız işaretiyle değiştirir).

Artık hesabına sızılmasının daha zor olacağı düşüncesiyle mutlu bir şekilde gelen kutusuna geri döner ve kısa süre sonra bu olayı unutur...

...Ta ki; ona terapiye gelen tüm müşterilerinin ayrıntılarını yayınlamakla tehdit eden şantajcılardan bir mektup alıncaya kadar.

BU NASIL OLDU?

Maria bir kimlik avı dolandırıcılığının kurbanı olmuştu. Girdiği site tıpkı daha önce binlerce kez ziyaret ettiği site gibi görünse de, aslında yalnızca sahte bir kopyaydı. Profil ayrıntılarına sahip olan dolandırıcılar mesleğinin ayrıntılarıyla da karşılaştılar. Aynı parolayı kullanarak iş e-postalarına ulaşmaya çalıştılar. Maria her iki hesap için de aynı parolayı kullandığından, tüm mesajlarını ve mesajların ekinde yer alan dosyaları okuyabildiler, bu dosyalardan birisi tüm müşterilerinin ve iletişim detaylarının bir listesini içeriyordu.

NEYİ FARKLI YAPABİLİRDİ?

İlk olarak, meşru sitelerin ve kuruluşların ayrıntılarını e-posta ile istemeyeceğinin farkında olmalıydı. İyi bir güvenlik yazılımı kullanıyor olsaydı, bağlantıya tıkladığında sitenin sahte olduğuna dair bir uyarı alırdı.

Diğer hatası ise hem profesyonel, hem de özel yaşamıyla ilgili yerlerde aynı parolayı kullanmaktı.

NEDEN KASPERSKY'Yİ SEÇMELİSİNİZ?

SİBER TEHDİTLERE KARŞI EN ETKİN, EN TEPKİSEL VE ETKİLİ KORUMAYI SAĞLAMA İŞİNİ MİSYONUMUZ HALİNE GETİRDİK. KASPERSKY SMALL OFFICE SECURITY'DE, BU UZMANLIĞI KULLANIŞLI OLDUĞU KADAR FAYDALI DA OLAN BİR ÇÖZÜME UYARLADIK. BÖYLECE SİZ EN İYİ YAPTIĞINIZ ŞEYE, YANİ İŞİNİZİ YÜRÜTMEYE DEVAM EDEBİLİRSİNİZ.

Konu siber güvenlik olduğunda, küçük işletmelerin benzersiz bir konumda olduklarını anlıyoruz. Bu işletmeler büyük kuruluşların karşı karşıya olduğu tehditlerin pek çoğuyla karşılaşıyor, buna karşılık ev kullanıcılarının bazılarıyla aynı güvenlik açıklarını paylaşıyorlar. Bu benzersiz konumun güvenlik konusuna kendi yaklaşımını hak ettiğini düşünüyoruz.

Bir tüketici ürününü yalnızca bir küçük işletme çözümü olarak yeniden paketlemek yeterli değildir. Örneğin, bu ürün sunucular için koruma sağlamaz; ancak pek çok küçük işletme bir sunucu kullanıyor veya yakında kullanmaya başlayacak. Ev kullanıcılarının aksine, işletmelerin birden fazla cihazı kolayca koruyabilmeleri gerekir.

Ancak, büyük bir şirket için geliştirilmiş bir çözümden yalnızca bazı işlevleri çıkarmak da işe yaramaz. Küçük işletmelerin özel BT ekipleri veya uzmanlar için geliştirilmiş karmaşık yazılımlarla uğraşacak zamanları yoktur.

Kaspersky Small Office Security karmaşık olmadan kapsamlı olacak şekilde tasarlanmıştır, böylece güvenlik konusu kaynaklarınızı kurutmadan içiniz rahat edebilir. Bu yazılım sizi yavaşlatmaz ve çok çeşitli cihazları kapsar, böylece işiniz sizi nereye götürürse götürsün korunursunuz.

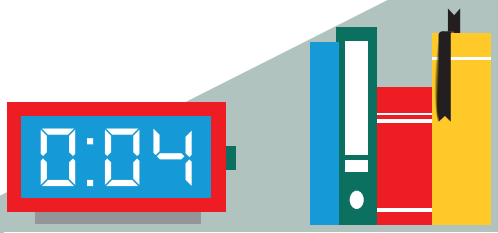
? PEKİ AMA KENDİMİ ÜCRETSİZ KORUYAMAZ MIYIM?

Ücretsiz güvenlik çözümleri olsa da, bunlar kapsamlı bir koruma sağlamazlar. Aslında, bu çözümler kasıtlı olarak geliştirilmesi gereken alanlar bırakırlar. Böylece kullanıcıları paralı sürüme geçmeye teşvik ederler.

İşiniz söz konusu olduğunda, korumanızın her zaman olabileceğinin en iyisi olması gerekir.

GERÇEKLEŞTİRMEK

GÜVENLİK POLİTİKANIZIN BİR PARÇASI OLARAK DİKKATE ALMANIZ GEREKEN ALANLARI TANIMLADIĞIMIZA GÖRE, ARTIK SIRA BUNLARI ÖZEL BİR ÇÖZÜM YARDIMIYLA NASIL UYGULAYACAĞINIZI DÜŞÜNMEYE GELDİ.



GÜNCELLEMELERİN DÜZENLİ OLARAK YAPILMASINI SAĞLAYIN

Konu Kaspersky Small Office Security olduğunuzda, endişelenmeniz gerekmez. Korumanızı gerçek zamanlı olarak otomatik güncelleyerek, sizi ortaya çıkan yeni tehditlerin önünde tutarız.

GÜÇLÜ PAROLALAR KULLANIN

Kaspersky Password Manager'ı kullanarak bunu çalışanlarınız için daha kolay hale getirin. Bu uygulama otomatik olarak güçlü parolalar oluşturur ve bunları şifrelenmiş bir veritabanında saklar. Böylece, yalnızca tek bir ana parolayı hatırlamanız yeterli olur ve çok daha güvende olursunuz.

HASSAS/KRİTİK VERİLERİ ŞİFRELEYİN VE YEDEKLEYİN

Kaspersky Small Office Security ile, kritik bilgilerinizi kolayca şifrelenmiş "kasalarda" saklayabilirsiniz. Ayrıca geri yükleme işlevi, bilgisayarlarınız veya sunucularınız çökse bile, önemli verilerinizin kaybolmayacağı anlamına gelir.

TÜM CİHAZLARINIZI DAHİL EDİN

Kaspersky Small Office Security, desteklenen tabletler ve akıllı telefonlar için koruma sunar. Ve cihazlarınız kaybolur veya çalınırsa uygulama onların yerlerini bulmanıza ve tüm hassas bilgileri uzaktan silmenize yardımcı olur.

KÖTÜ KİŞİLERİ ENGELLEYİN

Ödüllü Güvenli Para özelliğimiz, birkaç tıklamayla etkinleştirilebilir ve internette gezinmelerin son derece güvenli olmasını sağlar. Bu özelliği etkileşimde bulunduğunuz sitelerin kötü amaçlarla ele geçirilmediğini doğrulamak için kullanarak, bir ihlal olasılığını anında önleyebilirsiniz. Bu arada kötü amaçlı yazılımdan koruma, anti-spam ve güvenlik duvarı işlevleri, diğer çevrimiçi eylemleriniz sırasında kapıları suçlulara kapalı tutar.

İŞLETMENİZİ ŞİMDİ KORUYUN.

Küçük işletmelerin benzersiz taleplerini karşılamak üzere tasarlanmış olan Kaspersky Small Office Security, gelişmiş korumayı sizinki gibi şirketler için vazgeçilmez olan kullanım kolaylığı ile bir araya getirir.

kaspersky.com/protectmybusiness adresini ziyaret edin ve Kaspersky Small Office Security'nin işinizi nasıl koruyabileceğini keşfedin.

İŞLETMENİZİ ŞİMDİ KORUYUN

İLETİŞİME KATILIN

#protectmybiz

Bizi YouTube'da izleyin

Bizi Facebook'ta beğenin

Blogumuzu gözden geçirin

Bizi Twitter'da takip edin

LinkedIn'de bize katılın

kaspersky.com/protectmybusiness adresinden daha fazla bilgi alabilirsiniz

KASPERSKY LAB HAKKINDA

Kaspersky Lab, bugün uç nokta koruma çözümleri alanında dünyanın en büyük özel tedarikçisidir. Şirket uç nokta kullanıcılarına yönelik güvenlik çözümleri üreten tedarikçiler arasında dünyada ilk dört arasında yer alır*. 17 yıldan daha uzun bir geçmişiyle BT güvenliği konusunda birçok yeniliğe imza atan Kaspersky Lab, büyük kuruluşlar, KOBİ'ler ve tüketicilere yönelik verimli dijital güvenlik çözümleri sunar. İngiltere'de tescilli bir holding şirketine sahip olan Kaspersky Lab, bugün dünya çapında 200'ün üzerinde ülke ve bölgede faaliyet göstermekte, dünyanın dört bir köşesindeki 400 milyonun üzerinde kullanıcıya koruma sağlamaktadır. www.kaspersky.com adresinden daha fazla bilgi alabilirsiniz.

* Şirket, 2013 IDC Dünya Çapında Uç Nokta Güvenliği Gelirleri değerlendirmesinde Tedarikçi kategorisinde dördüncü sırada yer almıştır. Bu değerlendirme, Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares (Dünya Çapında Uç Nokta Güvenliği 2014–2018 Tahminleri ve 2013 Tedarikçi Pazar Payları) (IDC No. 250210, Ağustos 2014) başlıklı IDC raporunda yayınlanmıştır. Raporda yazılım tedarikçileri, 2013 yılındaki uç nokta güvenliği çözümlerinin satışından elde edilen kazanca göre sıralanmıştır.