KASPERSKY lab

Kaspersky Security for Microsoft Office 365

YENİ NESİL E-POSTA KORUMASI

3.5m

e-posta her saniye gönderiliyor.

İşletmenizi zor duruma sokmak için bir tanesi bile yeterli.

Office 365, 7/24 siber tehditle karşılaştığında

Çoğu işletme, kullanıcıları sahte e-posta tehdidi konusunda eğitmek için zaman ve çaba harcamıştır. Peki siber suçlular ve istenmeyen e-posta gönderenler taktiklerini sürekli olarak değiştirdiğinde ne yapabilirsiniz?

E-posta, işletme için bir numaralı kötü amaçlı yazılım vektörü olduğunda[1], kendinizi korumak için varsayılan veya yerleşik güvenlik ayarlarına bağlı olmak risklidir.

Kaspersky Security for Microsoft Office 365, işletmenizin, üretkenliği yavaşlatmadan veya yasal trafiği yanlışlıkla silmeden, istenmeyen postaları ve kötü amaçlı e-postaları bir sorun haline gelmeden önce tespit etmesine ve bloke etmesine yardımcı olur.

Microsoft Office 365 gibi bu güvenlik çözümü de bulutta barındırılmaktadır. Tüm Kaspersky Lab çözümleri gibi, bu çözüm de dünyanın en çok test edilen, en çok ödül alan güvenlik[1] çözümü üzerine kurulmuştur.

1: Verizon Veri İhlali İnceleme Raporu 2017

İstenmeyen e-posta: basit bir rahatsızlıktan çok daha fazlası

Bant genişliğinden kaybedilen verimliliğe kadar; istenmeyen e-posta, işletmede basit bir sıkıntıdan çok daha fazlasıdır: Ortalama bir çalışan yılda 13 saat bu postaları taramaya ve silmeye vakit harcar.[2]

Üstelik, istenmeyen postalarla karıştırılan gerekli e-postalarını tespit etmek için kaybedilen zamanı da göz önüne almak gerekir. Engellenen posta bir yana, ancak posta otomatik olarak silindiğinde durum daha da kötüleşir; bu durum bulut e-postasındaki dahili güvenlik ayarlarıyla ilgili genel bir sorundur.

Tüm bunlardan bahsederken, çok sayıda istenmeyen postanın kötü amaçlı yazılım taşıdığını henüz dikkate almadık.
Tüm e-posta trafiğinin %58'i istenmeyen postadır. Buluta geçerek elde ettiğiniz zaman, kaynak ve para neden hiç kimsenin istemediği istenmeyen mesajlar için harcansın?

2: Atlassian: İş Sırasında Zaman Kaybı

İstenmeyen e-posta koruması

Kaspersky Security for Microsoft Office 365, sürekli gelişen istenmeyen e-posta tekniklerini tespit etmek ve engellemek için Kaspersky Security Network'ün makine öğrenimi ve gerçek zamanlı, bulut tabanlı tehdit bilgileri ile desteklenen yeni nesil istenmeyen e-posta tespiti ve analizini kullanır.

İçerik saygınlığı ile robotik istenmeyen e-posta koruması

Kaspersky Lab'in istenmeyen e-posta koruması sistemi, makine öğrenimi tabanlı tespit modelleri etrafında oluşturulmuştur. Robotik istenmeyen e-posta işleme özelliği Kaspersky Lab uzmanları tarafından denetlenerek, en karmaşık ve bilinmeyen istenmeyen postaların bile etkin bir şekilde tespit edilmesi sağlanır. Ayrıca, false positive sonuçlardan kaynaklanan değerli mesajların kaybı da en aza indirilir.

Kimliği doğrulanmış e-posta desteği

Kimlik sahtekarlığı, sosyal olarak geliştirilmiş sahte ve kötü amaçlı istenmeyen postaların ana araçlarından biridir. Sender Policy Framework (SPF), güvenilir kaynaklardan gelen e-postaların gerçek olduğunu onaylayarak kimlik sahtekarlığı riskini önemli ölçüde azaltır.

Kaspersky Security Network

Kaspersky Security Network, dünyanın dört bir yanından yeni istenmeyen postalar ile ilgili gerçek zamanlı bilgileri toplayarak, "ilk kez ortaya çıkan" ve yeni salgınlar gibi bilinmeyen istenmeyen postalara anında yanıt verir. Bu işlemi, BT personelinin müdahalesine gerek duymadan otomatik olarak yapar ve posta taşmasını ve bulaşmalarını önlemeye yardımcı olur.

MassMail

Güvenilir bir kaynaktan gelen mesajların istenmeyen e-posta özellikleri olabilir, ancak aslında istenmeyen e-posta olmayabilir ve iş açısından da yararlı olabilir. Çalışan üretkenliğini sağlamak için bu mesajlar doğrudan silmek yerine, MassMail olarak etiketlenebilir veya özel bir klasöre taşınabilir.

Kimlik avı saldırıları: gönderideki tehdit

Siber suçlular, herhangi bir işletmenin kalbine giden en hızlı ve en doğrudan yol olduğu için saldırılarını başlatmak için e-postayı kullanır.

Bildirilen siber vakaların %21'i bir tür kimlik avı [3] içeriyor

Kullanıcıları eğitmek için elinizden geleni yapmanıza rağmen, iyi gizlenmiş bir e-postanın genellikle kullanıcıyı kötü amaçlı bir eke veya bağlantıya tıklamasına ikna etmeye yeterli olduğunu da bilirler. Kimlik avı saldırıları genellikle, kullanıcıları kötü amaçlı bir bağlantıya veya eke tıklamaya teşvik etmek üzere tasarlanmış, yasal iletiler olarak gösterilen e-postaları içerir. Bunların hepsini gördük – ÖZEL TEKLİF! GEÇ ÖDEME! KARGONUZ GECİKTİ! Bunlar, kullanıcıları düşünmeden tıklamaya ikna etmek için tasarlanmamıştır, kasıtlı olarak ikna edici dil ve teknikler kullanırlar.

Hedefe yönelik kimlik avı saldırıları bunu bir adım daha ileri götürür. Bunlar daha iyi hedeflenmiştir ve genellikle tam olarak yasal iletiler gibi görünen özel postalar ve eklerle şirkette çalışan belirli kişileri seçerler: mevcut bir iş ilanına referans veren bir e-postayla belirli bir İK yöneticisine gönderilen bir "iş başvurusu", muhasebe departmanında doğru kişiye gönderilen ve sizinle yasal olarak iş yapan bir firmaya referans veren bir fatura sık kullanılan örneklerdendir.

Son dönemde, CEO gibi şirketinizdeki birinden gelmiş gibi görünen 'İş E-postası Gizliliğinin Bozulması (BEC)' vakalarının yükselişine tanık olduk. Bunlar genellikle para transferlerini 'onaylar' veya hassas verileri ister. Çok detaylı şekilde uyarlandıkları için bu postalar genellikle istenmeyen e-posta tuzaklarından geçer çünkü büyük hacimlerde gönderilmezler ve genellikle yalnızca iyi seçilmiş birkaç çalışana gönderilir.

Bir dosya uzantısını gizleyerek veya e-posta adresini CEO'dan geldiği gibi göstererek siber suçlular zayıf güvenlik önlemlerini kolayca kendi çıkarları için kullanabilir.

3: Verizon Veri İhlali İnceleme Raporu 2017

Kimlik avı koruması teknolojileri

Kaspersky Security for Microsoft Office 365, kullanıcı hata yapmadan önce bilinmeyen tehditleri bile filtrelemek için sandboxing sistemleri ve makine öğrenimini kullanır. Dosya uzantısı gizli olduğunda bile, gerçek dosya türü tanıma işlemi dosya türünü tanır ve engeller.

Kaspersky Security for Microsoft Office 365'in yeni nesil kimlik avı koruması teknolojileri, verimliliği etkilemeden e-postanızı gelişmiş ve bilinmeyen tehditlere karşı korur:

Nöral ağ tabanlı kimlik avı koruması motoru

Tespit modelleri oluşturmak için 1000'den fazla kriter kullanarak bilinmeyen ve ilk kez ortaya çıkan kimlik avı saldırılarına karşı koruma sağlar. Kaspersky Security Network tarafından desteklenen, sürekli güncellenen tehdit veritabanlarımız, kötü amaçlı URL'lere ve diğer kimlik avı ile ilgili tehditlere karşı koruma sağlar.

Kötü amaçlı ve kimlik avı yapan URL tehdidi bilgileri

Kaspersky Security Network (bizim gerçek dünyamız, büyük veri tabanlı tehdit bilgileri ağı) tarafından desteklenen, sürekli güncellenen veritabanları, otomatik olarak tespit edilen veri ve insan uzmanlığı tabanlı tehdit araştırmasıyla beslenir. Bu, kötü amaçlı web siteleri aracılığıyla izinsiz girişlerin yanı sıra, drive-by ve water-holing saldırılarını önlemeye yardımcı olur.

Kimlik avı mesajlarını silin, taşıyın veya etiketleyin:

Rızanız olmadan gönderilen postaların tümü istenmeyen e-posta değildir; bu postaların otomatik silinmesi, verimlilik sorunlarına veya olası yararlı iletişimlerin etkilenmesine neden olabilir. Kaspersky Lab'in kimlik avı koruması, potansiyel olarak yararlı toplu postaları işaretlemek için etiket tabanlı filtreleme ve özel etiketler sağlayarak, istenmeyen e-postaları silmek yerine önemsiz klasörüne taşır.

Önizlemesi yapılan e-posta eki analizi:

Bu benzersiz sistem sayesinde önemli veri veya mali kayıplara yol açan gelişmiş kimlik avı saldırılarına karşı korunun. Kimlik avı içeriği için PDF, RTF ve MSOffice dosyaları dahil olmak üzere önizlenebilen ekleri analiz eder.

Kötü amaçlı yazılım: fidye yazılımı, sıfır gün açığı ve tehlikeli e-posta ekleri

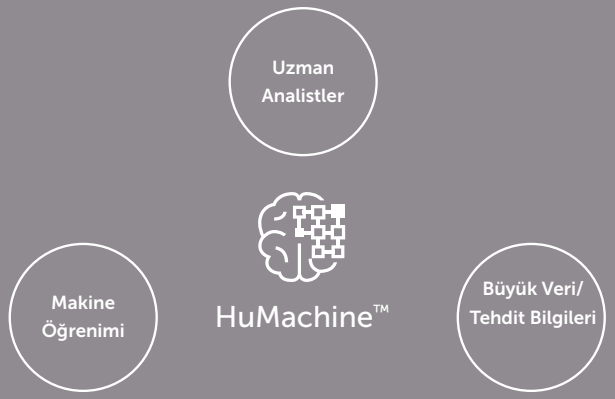
Kötü amaçlı yazılımların %66'sı kötü amaçlı e-posta ekleri aracılığıyla yüklenir.[4] Sıfır saat ve sıfır gün saldırıları genellikle Word, Excel, PowerPoint ve diğer iş uygulama dosyalarının içinde yer alır ve kullanıcının tıklamasını bekler.

Kötü amaçlı yazılımların %66'sı kötü amaçlı ekler aracılığıyla yüklenir

Çoğu durumda kötü amaçlı ekler, casus yazılım kullanarak kimlik doğrulama verilerini veya oturum açma bilgilerini çalmak üzere tasarlanmış kötü amaçlı yazılımlar taşır. Bu yazılımlar, kullanıcı farkında olmadan yüklenir. Diğer yaygın ek tabanlı saldırılar arasında fidye yazılımı bulunur. Çalıştırıldıktan sonra, kullanıcı verileri, fidye ödenene kadar şifrelenir.

HuMachine™ nedir?

Kaspersky Lab'in HuMachine© sistemi, bir işletmenin karşılaştığı her tür tehdide karşı koruma sağlamak üzere insan uzmanlığını büyük veri tehdit bilgileri ve makine öğrenimi ile birleştirir.



4: Verizon Veri İhlali İnceleme Raporu 2017.

Kötü amaçlı yazılımlara karşı koruma teknolojileri

Kaspersky Security for Microsoft Office 365 bir ekin veya dosyanın geçişine izin vermeden önce bu dosyaların gerçek doğasını belirlemek için korumalı alan, makine öğrenimi kullanır. Şüpheli dosyaların geçişine izin verilmeden önce kötü amaçlı yazılım olup olmadığını belirlemek için bu dosyalar güvenli bir alanda yürütülebilir.

HuMachine ile güçlendirilmiş çok katmanlı tehdit tespiti

Kaspersky Lab'in kendini kanıtlamış tehdit tespit becerileri, e-postadaki kötü amaçlı ekleri filtreleyen birden çok etkin güvenlik katmanı içerir. Makine öğrenimi tabanlı tespit modelleri, önceden bilinmeyen, sıfır saat kötü amaçlı yazılımlarını filtreler.

Kaspersky Security Network

Bulut tabanlı global tehdit bilgileri ağımız, dünya çapında 60 milyondan fazla uç nokta sensöründen anonim olarak gelen verileri kullanarak, tehdit ortamı evrimleştiğinde bile en hızlı reaksiyon sürelerini ve en yüksek koruma düzeylerini mümkün kılar.

Ek filtreleme

Tehlikeli dosyaları sorun haline gelmeden bloke edin ve istenmeyen mesajları yönetin. Gerçek dosya türü tanıma özelliği, güvenli olarak görünen kötü amaçlı dosyaların geçmesini önler. Uzantıya göre ek filtreleme özelliği, istenmeyen dosya türlerinin bloke edilmesini veya etiketlenmesini sağlarken, makro algılama özelliği ise makro etkinleştirilmiş olası tehlikeli Office dosyalarına gerekli eylemlerin uygulanmasını sağlar. Esnek hariç tutmalar ve etiketleme özellikleri, filtreleme kriterine düşen sorunsuz postaların kaybının azaltılmasına yardımcı olur.

Kolay yönetilebilir, uygun maliyetli yeni nesil koruma

Rahatlık, kaynak verimliliği ve maliyet avantaji için bulutta çalışıyorsunuz. Kaspersky Security for Microsoft Office 365 ile, e-posta güvenliği için bunlardan hiçbirinden vazgeçmenize gerek yoktur. Tek bir sezgisel yönetim konsolu, tespit edilen tehditlerin ve istatistiklerin tek bir noktadan görüntülenmesi de dahil olmak üzere her şeyi yönetmenizi sağlar. Ek donanım veya BT güvenlik personeli eğitimine gerek yoktur: Kurulum için dağıtıcı bile yoktur.

Ayrıca bu, ürün internet akışınızı yavaşlatmadan veya yanlışlıkla silmeden işinizi yapmanıza yardımcı olacak şekilde tasarlanmıştır:

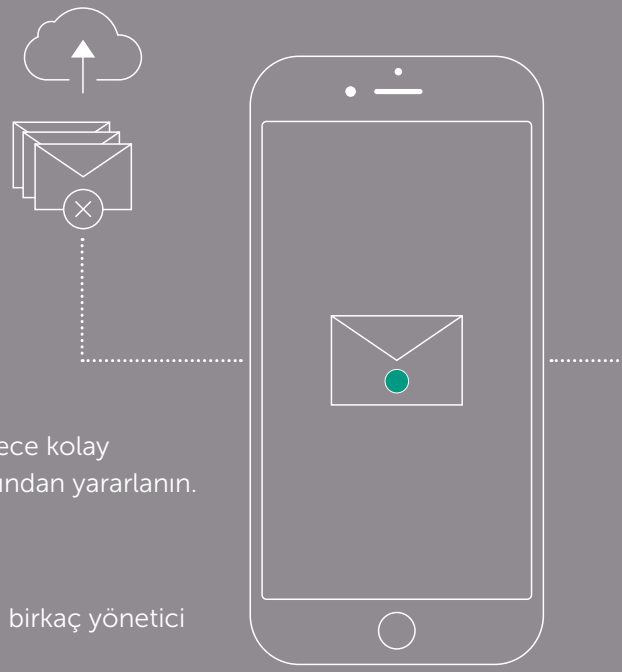
Kolay yönetim, idare ve entegrasyon

Bir bakışta pano:

Tek bir ekrandan günlük, haftalık ve aylık olarak tüm tehditleri ve istatistikleri görüntüleyin.

Kolay yapılandırma:

Tüm ayarlar, mükemmel yapılandırma ve inceleme kolaylığı için tek bir ekranda gruplanır.



Kullanımdan önce test edin:

Hangi posta kutularının korunacağını seçin; böylece kolay yapılandırma testi veya esnek politika uygulamasından yararlanın.

Çoklu kullanım:

Farklı hesaplar kullanarak çözümü yönetmek için birkaç yönetici etkinleştirin.

Yedekleme:

Birçok kullanıcı, sorunsuz e-postaları istenmeyen e-postayla karıştırma konusunda sorun yaşamaktadır. Şüpheli postalara ne olacağı hususunda daha düşük false positive oranı sonuç ve yönetici kontrolü sayesinde, Kaspersky Security for Microsoft Office 365 bu sorunu önemli ölçüde azaltır. Silinen e-postalar yedeklerde saklanarak aranabilir ve geri yüklenebilir. Böylece, "e-postaların kaybolması" sorunu ortadan kalkar.

Bildirim:

İstenmeyen e-posta, kimlik avı, virüs saldırıları veya ek politikası ihlalleri için yönetici bildirimleriyle olaylara hızla müdahale edin.

Tek oturum açma:

Farklı uç noktalar, cihazlar ve Exchange Online için güvenliği yönetmek üzere tek bir konsoldan oturum açın.

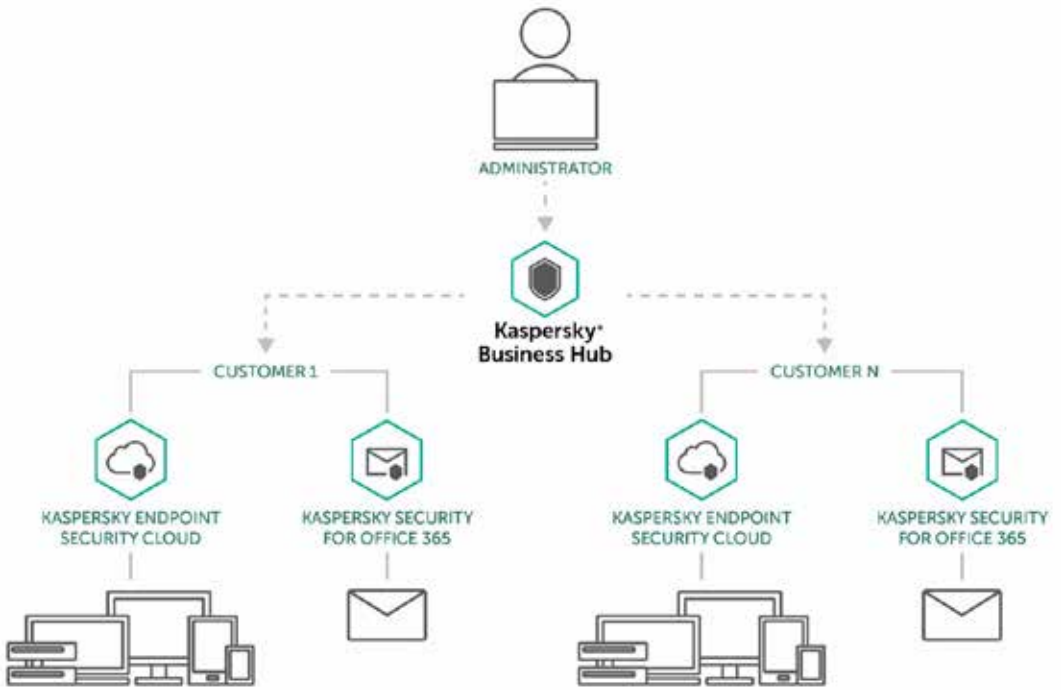
Kaspersky® Business Hub

Kaspersky Business Hub – şirketinizin korumasını yönetmek için merkezi konsol.

Farklı cihazlar ve verimlilik araçları için sezgisel arabirimimizi, basit yönetimi ve üstün korumayı deneyimleyin. İstediğiniz cihazdan bağlanın; istediğiniz zaman, istediğiniz yerde, kontrol sizde.

Aşağıdaki ürünler Kaspersky Business Hub'dan yönetilir:

- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365



Kaspersky® Security for Microsoft Office 365

Microsoft Office 365 postanızı korumak söz konusu olduğunda, en iyi strateji tehditlerin bir sorun haline gelmeden önce tespit edilip engellendiğinden emin olmaktır.

Kaspersky Security for Microsoft Office 365 bunu, internet trafiğinizi yavaşlatmadan veya yanlışlıkla silmeden yapmanıza yardımcı olacak şekilde tasarlanmıştır.

Yeni nesil güvenlik teknolojilerimizin Microsoft Office 365 postanızın güvenliğini ve yönetimini nasıl daha da kolaylaştırabileceğini keşfedin.

cloud.kaspersky.com adresinden ücretsiz olarak deneyin.