KASPERSKY lab

Kaspersky Security for Internet Gateway

çözümünün avantajları ve stratejik önemi

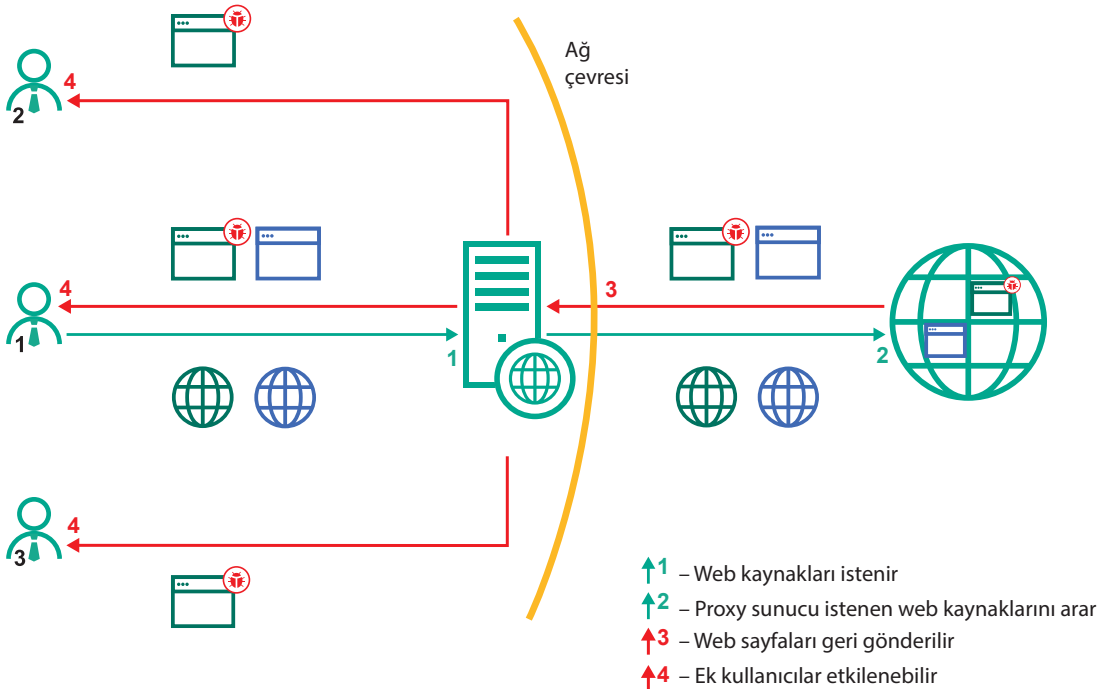
www.kaspersky.com
#truecybersecurity

Kaspersky Security for Internet Gateway çözümünün avantajları ve stratejik önemi

Mobilite, çalışma süreçlerine nüfuz etmesine rağmen güvenli bir ağ geçidi hâlâ kurumsal güvenlik senaryolarının büyük çoğunluğu için ilk savunma hattıdır. Ağ geçitleri yerini buluttaki muadili Bulut Güvenlik Ağ Geçidi'ne bıraksa da daima ilk savunma hattı olarak kalacaktır. Ağ geçitleri, kurumsal altyapı ve dış dünya arasında gerçekleşen tüm trafik için doğal bir dar boğaz olarak tehditlerin ilk aşamalarda ve nispeten daha az çabayla kontrol altına alınması için mükemmel avantajlar sağlar.

Katmanlı koruma konseptinde tehdidin uç noktaya ulaşmadan **önce** zayıflatılması risklerin önemli ölçüde azaltılmasını sağlar. Örneğin;

- Uç nokta seviyesinde denkleme insan faktörü de eklenir ve insan faktörünün etkisini tahmin etmek kolay değildir. Özellikle çalışma sürecinin sıkı güvenlik ilkelerine izin vermediği durumlarda sosyal mühendislik yönteminin akıllıca kullanımı güvenilir uç nokta koruma çözümlerini bile atlatabilir. Ağ geçidi düzeyindeki bir güvenlik çözümü bundan etkilenmez.
- Ağ geçidi güvenlik katmanın uygulanması durumunda risklerin daha çok azaltılacağı düşüncesi, kötü amaçlı yazılımların çoğunun tipik hazırlık/test modeline dayanır. Saldırganlar,özellikle uç noktayı araştırır ve güvenlik çözümlerinden kaçma hileleri de çoğu zaman bu ortama odaklanır. Aynı zamanda uç nokta koruması, kötü amaçlı yazılımları test etmek için yeniden oluşturulması en kolay seçenektir. Ancak proxy sunucu koruması son derece farklıdır. Saldırganların çoğu yalnızca test amacıyla geçit savunma sistemini yeniden oluşturmakla uğraşmaz.
- Uç nokta tabanlı koruma, kötü amaçlı yazılımı başarılı bir şekilde engellediğinde çoğunlukla hem kullanıcıyı hem de yöneticiyi uyarır. Toplu bir saldırı durumunda veya kötü amaçlı yazılımın proxy sunucu önbelleğine girmesi halinde ağın tamamı, kullanıcılara ve yönetim personeline uyarı göndermeye başlayabilir. Bu durum, başta BT personeli sayısı az olan ve bu tür durumlarla mücadele için gelişmiş bir çerçeveye sahip olmayan daha küçük işletmeler olmak üzere, şirketlerin ticari faaliyetlerini aksatmasına neden olabilir. Böyle bir ortamda uzman yardım masalarından alınan desteğin her saati finansal yükü artırır. Bu yük de aksamanın tamamı nedeniyle oluşan gelir kaybına eklenir. Açıkça görülebileceği üzere tehdidin ilk aşamada ağın giriş noktasında önlenmesi zamandan ve maliyetten tasarruf edilmesini sağlar.
- anıldıkları görevlerin yapısı gereği kasıtlı olarak güvenlik çözümleri uygulanmaz. Dolayısıyla, bu tür uç noktaların ağ geçidi düzeyinde korunması büyük önem taşır.



Ağ geçidi koruması olmadan saldırılar yayılabilir

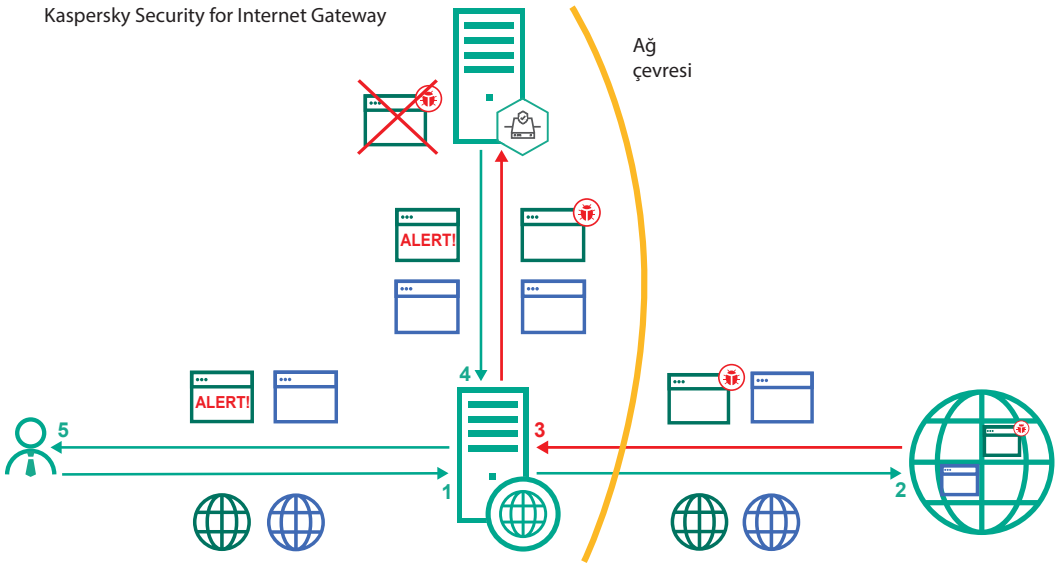
Proxy sunucu, saldırının ölüm zincirindeki ilk aşamalarda gelen tehditlerin kontrol altına alınabileceği iki boğazdan biridir(diğeri ise e-postadır). Proxy sunucu güvenlik çözümü, kurumsal BT ağını World Wide Web'in tehlikelerinden korur ve aynı zamanda internet kullanımını da yöneterek verimliliği artırır.

Kaspersky Security for Internet Gateway çözümünün temel özellikleri ve yararları:

- Modern kötü amaçlı yazılımların ve fidye yazılımlarının büyük bir kısmına karşı koruma. Eski kötü amaçlı yazılımların yeniden kullanılma oranı göz önüne alındığında, statik makine öğrenimi tabanlı algoritmaların ve emülasyon destekli koruma alanlarının gelen tehditlerin **%95**'ini nasıl filtrelediği daha iyi anlaşılabilir.
- Kaspersky Lab, Kaspersky Security Network aracılığıyla en yeni tehditleri bile keşfedildikten hemen sonra hiçbir hatalı pozitif sonuç üretmeden tespit eder. Böylece güncellemeler için beklemeniz gerekmez.
- Çözüm mimarisi, "SSL bumping" olarak da bilinen kurumsal trafik izlemenin kolay bir şekilde uygulanmasını sağlar. Bu özellik, temelde internet iletişimleri için fiili standart haline gelen SSL şifreli web trafiğini kontrol eder ve korur.
- Kötü amaçlı ve kimlik avı web siteleri kullanıcıyı tehdit etmeden önce bu siteleri engellemek için özel sezgisel algoritmaların yanı sıra kapsamlı tehdit istihbaratından faydalanılır.
- Çözüm, yükü fazla olan sistemler için ölçeklenebilirdir. Böylece birden çok düğüm yönetimi ve hiyerarşik dağıtım sağlanır.
- KOBİ'ler, hedefli saldırılara büyük kuruluşlara kıyasla daha az maruz kalmasına rağmen daha büyük bir hedefe ulaşmaya yönelik yüklenici zincirinin bir parçası olarak saldırıya uğrayabilirler. Bu tür saldırıların başarılı olma riski, ünlü Kaspersky Lab APT tehdit avcıları tarafından sürekli olarak güncellenen hedefli saldırılarla ilişkili ana bilgisayarlar veritabanının yardımıyla önemli ölçüde azaltılabilir. Ayrıca işletmeniz Kaspersky Anti-Targeted Attack (KATA) çözümünü de satın alırsa, Kaspersky Security for Internet Gateway çözümü, web sensörü olarak Kaspersky Anti Targeted Attack ile entegre edilir, böylece tespit özellikleri daha da geliştirebilir.
- Ağa giren ve ağdan çıkan bazı dosya türlerinin iletimi İçerik Filtreleme tarafından kısıtlanabilir. Bu özellik virüsün yayılması ve hassas verilerin sızması riskini azaltır.
- Belirli web kaynağı kategorilerinin kullanımını sınırlandırmak için etkili Web Kontrol senaryoları uygulanabilir. Ayrıca özel kurallar oluşturulabilir. Bu özellik dikkat dağınıklığına neden olan etkenleri ortadan kaldırarak verimliliğin artmasına yardımcı olur ve aynı zamanda virüs bulaşma riskini azaltır. Çünkü korsan yazılımlar veya yasa dışı içerikler sunan belirli web kaynakları aynı zamanda kötü amaçlı yazılım siteleri de olabilir.
- Başarılı olay yanıtının temelinde iyi görünürlük yatar. Kaspersky Security for Internet Gateway, yöneticilerin dikkat etmelerini gerektiren olaylara hızlı bir şekilde tepki vermelerine yardımcı olan kapsamlı özelliklere sahiptir. Bu özellikler arasında olay takibi için web tabanlı pano, olay merkezli tehdit analizi ve mevcut Güvenlik Bilgisi Olay Yönetimi (SIEM) sistemleriyle entegrasyon yer alır.
- Çoklu müşteri mimarisi, servis sağlayıcıları ve aynı anda farklı alanlarda çalışan işletmeler için birden çok sistemin tek bir konsoldan yönetimini kolaylaştırır. Her bir sistemin kendi yöneticisi ve bu yöneticilerin role bağlı ayrıcalıkları olabilir.
- Son derece hassas verilerle çalışan ve/veya güvenlik olaylarına karşı toleransı düşük olan şirketler ve kuruluşlar için mevcut web ağ geçici korumasının yanı sıra Kaspersky Security for Internet Gateway çözümünü de uygulamak son derece mantıklıdır. Kaspersky Security for Internet Gateway, güçlü bir ek güvenlik katmanı olarak fazladan hatalı pozitif sonuçlar üretmeden tespit oranlarını artırır.

Sonuç

Her şirketin güvenliği için en ön cephenin korunmasının değeri göz ardı edilemez. Kaspersky Lab'in kapsamlı güvenlik çözümleri yelpazesiyle BT ağınızın her düzeyini koruma altına almak işletme verilerinizin güvenliğini sağlar ve işlerinizin rayında gitmesine yardımcı olur.



↑1 – Web kaynakları istenir
↑2 – Proxy sunucusu istenen web kaynaklarını arar
↑3 – Web sayfaları geri gönderilir
↑4 – Kötü amaçlı içerik engellenir
↑5 – Kullanıcı sadece temiz sayfaları alır

Kaspersky Security for Internet Gateway, tehditler kullanıcıya ulaşmadan önce onları engeller

Kaspersky Lab
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr