infoblox.

ÖRNEK DURUM İNCELEMESİ

Avrupa'ya açılan kapı niteliğindeki Antwerp Limanı, nakliye şeritlerini 7x24x365 açık tutmak için Infoblox'a güveniyor

ÖZET - BENZERSIZ BIR İNOVASYON TARIHI

Belçika'nın Kuzey Denizi kıyısından 80 kilometre içerideki konumu sayesinde Antwerp Limanı, malların Avrupa hinterlandının derinlerine ulaştırılması için en hızlı ve sürdürülebilir bağlantıyı sunmaktadır.

Dünyanın en büyük 14. konteyner nakliye limanı olan Antwerp, yılda 231 milyon metrik tondan fazla yükü ve 14.000'den fazla deniz ticaret gemisini elleçleyerek sadece 20 yıl önce elleçlediği hacmi iki katına çıkarmıştır.

Antwerp'in Scheldt Halici'ndeki merkezi konumu ile Atlantik nakliye şeritleri ve kuzey orta Avrupa'ya kolay erişim imkanı sunması, limanı 12. yüzyıldan bu yana bir taşımacılık merkezi haline getirmiştir. Bu tarihi başlangıçtan itibaren Antwerp Limanı yüzyıllar boyunca istikrarlı bir şekilde büyümüş ve günümüzde teknolojik açıdan en gelişmiş liman tesislerinden biri haline gelmiştir. Geniş dijital altyapısı, iki yerinde veri merkezi ve liman içindeki 50'den fazla saha ile binlerce uç noktayı birbirine bağlayan 170 kilometreden fazla dark fiber içermektedir.

Infoblox, on yıldan uzun bir süredir temel DNS, DHCP ve IPAM (DDI) süreçlerini destekleyerek limanın ağ yapısında önemli bir unsur olmuştur. Limanın kapsamlı dijital altyapısı, liman işletmecisi, düzenleyici, mülk sahibi ve topluluk oluşturucu olarak görevlerini desteklemekte ve kuruluşu "Geleceğin Limanı" vizyonunu gerçekleştirmek için stratejik olarak konumlandırmaktadır.

Müşteri: *Antwerp Limanı*
Sektör: *Taşımacılık/Nakliye*
Konum: *Antwerp, Belçika*

GİRİŞİMLER:

- Sürekli çalışma için DDI'yi koruma
- Her yerden çalışan bir iş gücünü destekleme
- Uzaktan çalışanlar için şirket içi güvenliğe eşit güvenlik sağlama

SONUÇLAR:

- Optimize edilmiş güvenlik yığınıyla daha güçlü güvenlik duruşu
- Dağıtılmış bir iş gücüne sorunsuz geçiş
- Infoblox ile uzun yıllar boyunca mükemmel, güvenilir ağ performansı

ÇÖZÜMLER:

- Infoblox NIOS DDI
- BloxOne® Threat Defense
- Trinzic cihazları

Port of Antwerp

ZORLUKLAR

Geleceğin limanına doğru ilerlemeyi sürdürüyoruz

Taşımacılık ve denizcilik, Nesnelerin İnterneti'ne en çok yatırım yapan sektörler listesinin neredeyse tamamında en üst sırada ya da en üst sıralara yakın bir konumda yer alıyor. Antwerp Limanı da bu eğilimin bir simgesi ve IoT'nin ilk aşamalarını şekillendiren teknolojilerin ve en iyi uygulamaların çoğunu benimsedi. Son yıllarda limanın BT ekibi, gemi trafiği yönetimine ilişkin temel liman operasyonlarını mümkün olan en geniş ölçüde dijitalleştirdi. Bu çabalar, Antwerp'in artık üstün tonaj verimiyle dünya çapında tanındığı noktaya kadar, temel ölçütlerde istikrarlı ve önemli ilerlemeler sağladı.

Riskleri kontrol altında tutarken teknolojik yenilikleri benimsemek, Antwerp Limanı Siber Dayanıklılık yöneticisi Yannick Herrebaut için önemli bir iş önceliği. Bu ilerlemeyi, dijital inovasyonun liman operasyonlarının neredeyse her yönüne (dronlar, otonom gemiler ve dijital ikiz kullanımı gibi) yayılmasını sağlayacak bir sürecin başlangıcı olarak görüyor. "Dijital ve Enformasyondan Sorumlu Başkanımız, Geleceğin Limanı için statükoya meydan okumayı, sorunlar yerine fırsatları görmeyi ve teknolojiyi sürdürülebilir bir gelecek için kaldıraç olarak kullanmayı vurgulayan bir vizyon belirledi. Yetkinliklerimizle, farklı ekosistemler aracılığıyla tüm liman topluluğunu birbirine bağlamak istiyoruz," diye açıklıyor. "Bu yoldan bahsetmişken, CEO'muz misyonumuzu 'İnsanları, ekonomiyi ve iklimi uzlaştıran bir dünya limanı olmak istiyorum' olarak nitelendirdi."

Şekil 1. Antwerp Limanı'nın Avrupa'nın kalbindeki stratejik konumu, limanın Belçika'nın en büyük ekonomik gücü haline gelmesini sağlamıştır.

Herrebaut ve limanın BT ekibi, bu tür yenilikleri gerçekten teşvik etmek ve mümkün kılmak için limanı her türlü çözümün uygulanabileceği ve test edilebileceği dijital bir oyun alanı olarak konumlandırmaları gerektiğine inanıyor. Bu amaçla limanın 5G teknolojisini ve dronlar, otonom gemiler, akıllı can simitleri ve diğer dijital ekipman türleri gibi çeşitli akıllı IoT cihazlarını yaygınlaştırma çabaları, Geleceğin Limanı'nın teknolojik temelini oluşturuyor. Ancak Herrebaut'un da belirttiği gibi, IoT cihazları ve araçları, liman gibi kritik bir ortamda konuşlandırılmak için gereken siber güvenlik korumalarından genellikle yoksun olma konusunda kötü bir üne sahip.

"Bizim için en önemli nokta, bunların her zaman güvenliğin temel bir unsur olarak değil de sonradan düşünülerek üretilmiş yeni teknolojiler olması" diyor. "Değer kanıtlama vakalarının gerçekleşmesini teşvik ediyoruz, ancak bunlar çekirdek ağımızdan uygun şekilde izole edilmeli. Çok umut verici vakalar zaman içinde operasyonel hale getirilecek, ancak o zaman güvenlik politikalarımıza uymaları gerekiyor. Amaç, Infoblox'un kritik bir unsur olduğu çekirdek ağımızın gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak. BloxOne Threat Defense'i siber güvenlik yığınımıza ekleyerek, bugünlerde çoğunlukla evden çalışan personelimizin tüm dizüstü bilgisayarları da dahil olmak üzere tüm yönetilen uç noktalarımızın güvenlik seviyesini artırabiliriz."

DURUM

Fidye Yazılımı Çağında Güvenli Bir Çalışma Ortamının Korunması

Antwerp Limanı'ndaki ekip, COVID salgınının başlangıcından bu yana, dünyanın dört bir yanındaki siber güvenlik karar vericilerinin boğuştuğu aynı zorluklarla karşı karşıya: giderek daha mobil hale gelen, evden çalışan personel ve kötü niyetli veri ihlallerinin yanı sıra fidye yazılımlarında endişe verici bir artış. Herrebaut, "Biz operasyonel bir şirketiz, bu nedenle gerçek düşman, en kötü senaryo kesinti süresi," diyor. "Açıkçası, fidye yazılımlarının neden olduğu kesinti süresini ne pahasına olursa olsun önlemeye çalışıyoruz."

Infoblox Q2 2021 Siber Tehdit İstihbarat Raporu'na göre, fidye yazılımlarıyla ilişkili toplam hasarın yılda 20 milyar dolara kadar çıkacağı tahmin ediliyor ve şu anda tüm siber saldırıların yüzde 10'undan fazlası fidye yazılımı içeriyor. Siber güvenlik araştırmacıları, bu artışın çoğunu COVID kaynaklı her yerden çalışma uygulamalarının getirdiği saldırı yüzeylerindeki büyük genişlemeye bağlıyor. Liman açısından, evden çalışma denizcilik sektörünün gerçekleri yüzünden biraz kısıtlanmış olsa da önemli bir eğilim oldu.

Antwerp toplamda yaklaşık 1.600 kişilik bir işgücüne sahip: bunların bini bilgi çalışanı, diğer 600'ü ise makine mühendisi, denizci veya gemi ve tekne personeli. Yine de karantinanın en yoğun olduğu dönemde liman çalışanlarının 700 kadarı evlerinden çalıştı. Herrebaut ve ekibi için, dağınık işgücü göz önüne alındığında limanın güvenlik duruşunu güçlendirmek bir zorunluluk haline geldi ve Infoblox'tan BloxOne Threat Defense doğal bir seçimdi.

ÇÖZÜM

BloxOne Threat Defense

BloxOne Threat Defense, güvenlik etkinliğini ve esnekliğini artırmak için kanıtlanmış bir çözümdür. Diğer çözümlerin algılayamadığı tehditleri algılamak için DNS düzeyinde çalışır ve saldırıları tehdit yaşam döngüsünün daha erken aşamalarında durdurur. Yaygın otomasyon ve ekosistem entegrasyonu sayesinde SecOps'ta verimliliği ve mevcut güvenlik yığınının etkinliğini artırır, dijital ve her yerden çalışma çabalarını güvence altına alır ve siber güvenlik için toplam maliyeti düşürür. Fidye yazılımı suçlularının ana hedefi olan taşımacılık sektöründeki kuruluşlar için BloxOne Threat Defense, günümüzün gelişen tehditlerine karşı kapsamlı koruma sağlar. DGA aileleri, veri sızıntısı, benzer alan adı kullanımı, hızlı akış ve diğerleri dahil olmak üzere çok çeşitli tehditleri algılamak ve önlemek için makine öğrenimine dayalı gelişmiş analitiği, son derece doğru ve toplu tehdit istihbaratını ve otomasyonu benzersiz bir şekilde birleştirir.

Herrebaut, "BloxOne Threat Defense, liman için doğru zamanda ideal çözümdü" diye açıklıyor. "Bulut tabanlı bir teklif olduğu ve zaten Infoblox NIOS'a sahip olduğumuz için uygulama süresi çok kısaydı. Çalışmaya başlamak için yapmamız gereken tek şey politikaları tanımlamak ve ardından aracıları uç noktalarımıza dağıtmaktı. Her şey çok hızlı bir şekilde yerine getirildi, bu da kilitlenme durumu göz önüne alındığında büyük bir avantajdı.

SONUÇLAR

Güçlü güvenlik duruşu, sürekli çalışma süresi

Herrebaut ve ekibi, 2020'de tam kapanma emirleri çıktığında, uzaktaki çalışanlarını ve buna bağlı olarak temel ağ varlıklarını ve operasyonlarını korumak için iyi durumda olduklarını düşündüler. Tam ölçekli bir genişletilmiş algılama ve yanıt (EDR) çözümüne yükseltme yapılıyordu, liman uzun süredir güvenli bir VPN kullanıyordu ve tüm şirket dizüstü bilgisayarları malware önleme uygulamalarıyla donatılmıştı. Herrebaut, "Güçlü güvenlik önlemlerine sahip olduğumuzdan emin olsak da, EDR sistemlerinin ve malware önleme yazılımlarının bazı tehditleri gözden kaçırabileceğinin de farkındaydık. Bu nedenle ek bir güvenlik katmanına ihtiyacımız olduğunu hissettik" diyor. "BloxOne Threat Defense'in sunduğu şey, uzaktaki kullanıcılarımıza şirket içinde çalışırken sahip oldukları koruma düzeyinin aynısını sağlayabilmekti."

BloxOne Threat Defense, limanın bir şirket cihazında ziyaret edilmemesi gereken site kategorileri veya dark web ile ilgili herhangi bir şey gibi kurumsal ağda geçerli olan aynı tür içerik kısıtlamalarını yürürlüğe koymasını sağladı. BloxOne Threat Defense'ın benzersiz hibrit güvenliği, şirket içi ekosistemle sıkı bir şekilde entegre olurken çok çeşitli tehditleri algılamak için bulutun gücünü kullanıyor. BloxOne Threat Defense ayrıca liman ekibinin mevcut güvenlik yığınının performansını ve etkinliğini optimize etmesini sağlıyor. "BloxOne Threat Defense, mevcut güvenlik araçlarımıza ek olarak, ekibimizin tehditleri daha iyi tanımlamasını ve düzeltmesini mümkün kılıyor. Artık Infoblox çözümünden bilgi alıp SIEM çözümümüze aktarabiliyoruz. Bu da tehditleri belirlemek veya olumsuz şeylerin olmasını önlemek üzere müdahale etmek için bizi doğru şekilde yönlendiriyor."

Antwerp Limanı, BloxOne Threat Defense uygulaması aracılığıyla Infoblox ile ilişkisini genişlettikçe, ekip de orijinal NIOS DDI çözümünün güvenilirliği ve esnekliğini takdir etmeye devam ediyor. Herrebaut, "Infoblox'un güvenilir, performanslı ve güvenli BT hizmetleri sağlayarak işin temel başarısına nasıl katkıda bulunduğuna bakarsam, büyük ölçüde diyebilirim" diye açıklıyor. "Sağlam, her zaman açık DHCP, DNS ve IPAM olmadan, temel hizmetlerimizin çoğu çalışmayı durdurur ve çok sayıda kızgın mesai arkadaşımız olurdu. Infoblox ile limanın sürekli çalışmasını sağlayabiliyoruz. Bu da müşterilerimizin mutlu olmasını ve kâra geçmesini sağlıyor."

infoblox.

Infoblox, benzersiz performans ve koruma sağlamak için ağ ve güvenliği birleştirir. Fortune 100 şirketleri ve gelişmekte olan yenilikçiler tarafından güvenilen firmamız, ağınıza kimin ve neyin bağlandığı üzerinde gerçek zamanlı görünürlük ve kontrol sağlıyor. Böylece kuruluşunuz daha hızlı harekete geçerek tehditleri daha çabuk durdurabilir.

Kurumsal Merkez
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com