YAYGIN ŞIFRELEME

Korumaya Yönelik Yeni bir Paradigma

GIRIŞ

«15 yıldan uzun süredir profesyonel olarak bilgisayar korsanlığı yapıyorum. Teknolojileri daha güvenli hale getirmek için teknolojilerdeki siber güvenlik sorunlarını açığa çıkartıyorum. Ancak uzun yıllar boyunca bu işi yaptıktan sonra çabalarımın boşa çıktığını düşünüyorum. Çünkü aynı sorunların tekrar tekrar ortaya çıktığını görüyorum. Daha iyiye gitmiyoruz. Ve biz giderek teknolojiye daha bağımlı hale gelirken teknoloji ise giderek daha da güvensiz bir yapıya bürünüyor.»

Cesar Cerrudo, profesyonel bilgisayar korsanı ve IOActive Labs Teknolojiden Sorumlu Genel Müdür Yardımcısı,

Bilgisayar dünyasının değişen yüze, işletmelerin ve insanların internet üzerinden giderek birbirine daha bağlı hale geldiği bir dalgalanma etkisine yol açıyor.

Her işletme, kredi kartı işlemi gerçekleştiren bir benzinci bile teknolojiden yararlanıyor. Güvenli verilere ve süreçlere sahip olma ihtiyacı artık sadece büyük işletmeler için bir gereklilik olmanın da ötesine geçerek her boyuttaki işletme için temel bir teknoloji bileşenine dönüştü. Günümüzün sanallaştırılmış, internet bağlantılı, bulut odaklı dünyası sadece bilişim teknolojisi için değil, *işletmeler* için de artan ve karmaşık bir soruna dönüşüyor.

Siber uzayın güvenliğini sağlamak son derece güç. Suç mahallinin dünya çapında çok geniş bir coğrafyaya yayılması bu güçlüklerin en hafifi. Siber uzay ile fiziksel dünya arasındaki bütünleşmenin giderek artması hırsızlık, hasar ve yolsuzluğa yönelik fırsatların katlanarak artmasına neden oluyor. Suça yönelik Siber dünya ile fiziksel dünya arasındaki bağlantı yeni birliktelikleri ortaya çıkartırken suça yönelik hedefler de artıyor. Karmaşık siber ağlardaki açıkların azaltılması ve sonuçların en aza indirilmesi hedefler arasında yer almaktadır; ancak bu hedeflerin başarılması giderek daha güç hale gelmektedir.

Eğilim giderek hız kazanıyor ve güçlükler giderek daha da aşılması zor hale geliyor. Güvenlik açısından benimsenen temel yaklaşım, çevrenin yol açtığı yoğun saldırganlık özellikleri karşısında artık beklentileri karşılayamıyor. Bir paradigma kaymasına ihtiyaç duyuluyor ve böyle bir kayma çok yakında meydana gelecek.

Solitaire Interglobal Ltd. (SIL) 21 yılı aşkın bir süredir işletme ve güvenlik alanlarının farklı yönlerini izliyor.. Global Security Watch (GSW) üzerinden bilgilerin toplanması binlerce kuruluşa sürekli olarak eğilim ve risk bilgileri sağlamaktadır. Sunulan risklerin ve fırsatların küresel ve kapsamlı bir resmini etkili bir şekilde oluşturmak için SIL, güvenliğe bütüncül bir bakış açısıyla yaklaşmaktadır. Buna, dört ana alana odaklanan kapsamlı bir güvenlik bakış açısı dahildir. Bunlar genel olarak şu şekilde sınıflandırılabilir:

- Veriler – erişim (oku, kopyala) veya yönlendirme[1]
- Süreç güvenliği: uygulama, gizleme, kaçırma becerisi
- Mimari: iş modeli, süreç yapısı, üst veriler gibi fikri mülkiyet
- Fiziksel: fiziksel tesislere veya alanlara erişim[2]

Bu en yeni çalışmaya temel oluşturması için SIL, gerçek dünyadaki organizasyonlardan elde edilen araştırma verileri ve Global Security Watch'tan (GSW) alınan güvenlik bilgileri üzerinde analizler gerçekleştirmiştir. Tehdit türlerinde, kapsamlarında ve oranlarında son yıllarda önemli değişimlerin eşi görülmemiş derecelerde hız kazanarak devam etmesi şaşırtıcı değil.

GSW, güvenlik tehditlerinin detaylı evrimini ve işletme üzerindeki ilgili etkisini dünya çapında 21 yıldır takip eden ve şu anda 8.9 milyondan fazla kuruluşun bildirdiği bilgileri toplayan bir üye hizmet. GSW'dan alınan bilgiler işletme bakış açısından derin bir tehdit kaynağı doğurmakta ve araştırmalara katkı sağlamaktadır ve gerçek dünyada üretilen bilgilere dayanılarak üretilen bilgiler temel alınarak inşa edilmiştir. Tehdit ayak izlerinin ve diğer detaylı mekanizmaların GSW'da toplanmasına rağmen ana odak noktası işletme faaliyetinin etkisi, organizasyonel varlıklar, önleme ve iyileştirme masrafları ile ilgilidir.

Bulguların Özeti

GSW verilerinden elde edilen ve SIL'in son iki yılda gerçekleştirdiği 62 binin üzerinde hedeflendirilmiş güvenlik analizi ile desteklenen önemli bir bulgu, bazı kuruluşlar güvenlik saldırılarının farkında olsa da, çoğu kuruluşun bu saldırıların farkında olmadığı veya sadece kısmen farkında olduğudur. Ayrıca, inceleme kapsamındaki kuruluşların %91,3'ten fazlası kendilerine yöneltilen siber suçların tüm sonuçları hakkında farkındalığa sahip değildi. Bu kuruluşlar tarafından talep edilen tüm denetim ve analizler, açıkların kapsamının göz ardı edildiğini ya da organizasyonun işletme kısmı tarafından sadece kısmen teyit edildiğini gösterdi. En şaşırtıcı keşif ise, bu kuruluşların büyük bir çoğunluğunun sistemlerine yöneltilen *gerçek saldırılarının toplam sayıları hakkında bilgi sahibi olmamasıydı*[3].

Tehlikeyi arttıran bir nokta ise, bu saldırıların çoğunun bir defalık bir olay olmayıp, onun yerine önemli bir süre boyunca devam edecek bir hasar penceresini açmalarıdır. Aralık 2015 boyunca meydana gelen Amerikan Sağlık Sigortası Verileri (HIPAA) ihlalleri incelendiğinde bir örnek görülebilir.

> *«17 Ekim 2014 itibariyle meydana gelen 1.135 önemli Amerikan Sağlık Bilişim Teknolojileri (HITECH) ihlalinin %10'undan fazlası tek seferlik olaylar olmayıp süreklilik arz eden, bir yünden 2.891 güne kadar süren olaylardır. Bu veriler daha ayrıntılı olarak incelendiğinde şunlar tespit edilmiştir:*
> *-- 4 ihlal 2.000 günden uzun sürmüştür*
> *-- 7 ihlal 1.000 ile 1.500 gün arasında sürmüştür*

---

[1] *Veri güvenliği bir işletmenin bilgilerine yönelik bir tür erişimi içermektedir. Bu, özel içeriğin okunması veya bir kopyasının alınması şeklinde olabilir. Bir kuruluşun verilerinin tahrif edilmesi ise, bilgilerin değiştirilmesi veya içeriği değiştirecek biçimde silinmesi, veya öznitelikler ile yapılar arasındaki ilişkilerin değiştirilmesidir.*

[2] *Fiziksel güvenlik bu makalenin kapsamında yer almamaktadır.*

[3] *Saldırılar, kuruluşun bilişim ortamına yönelik başarılı girişimlerdir ve ilk müdahale veya ihlalin yanı sıra her bir başarılı hırsızlığı, imhayı veya engellemeyi (yani verilerin, araştırma veya sürecin ele geçirilmesi, hizmetin kullanılamaz hale getirilmesi vb.).*

-- 10 ihlal 500 ile 1.000 gün arasında sürmüştür
-- 35 ihlal 100 ile 500 gün arasında sürmüştür.»

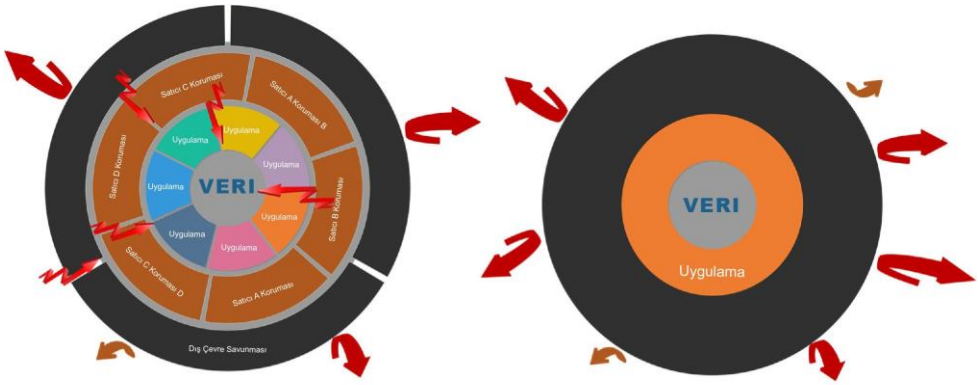
Kaynak: Melamedia, LLC analysis of Office of Civil Rights Data, 2015

Aktif saldırıların uzun dönemler boyunca var olması işletmenin faaliyetlerini yürütebilirliği üzerinde çok önemli bir olumsuz etkiye sahip olabilir. Bir saldırının üç aydan uzun sürmesi halinde işletmeler brüt gelirlerinde ve değerlerinde ortalama %16,2-%63,7 kayıpla karşılaşmaktadır.

Bulut uygulamanın hızlanmasıyla birlikte, dışarıya açık uygulamalardaki artış kuruluşların altyapılarını daha büyük ve kontrolü daha az olan bir kullanıcı tabanına maruz bırakmaktadır. Değişen pazar talepleri kuruluşu daha hızlı tasarım ve uygulama döngülerine sevk etmektedir. Bu yeni kullanıcı kümelerinin her biri, her bir yeni uygulama başarılı bir güvenlik saldırısı olasılığında bir artışa yol açmaktadır.

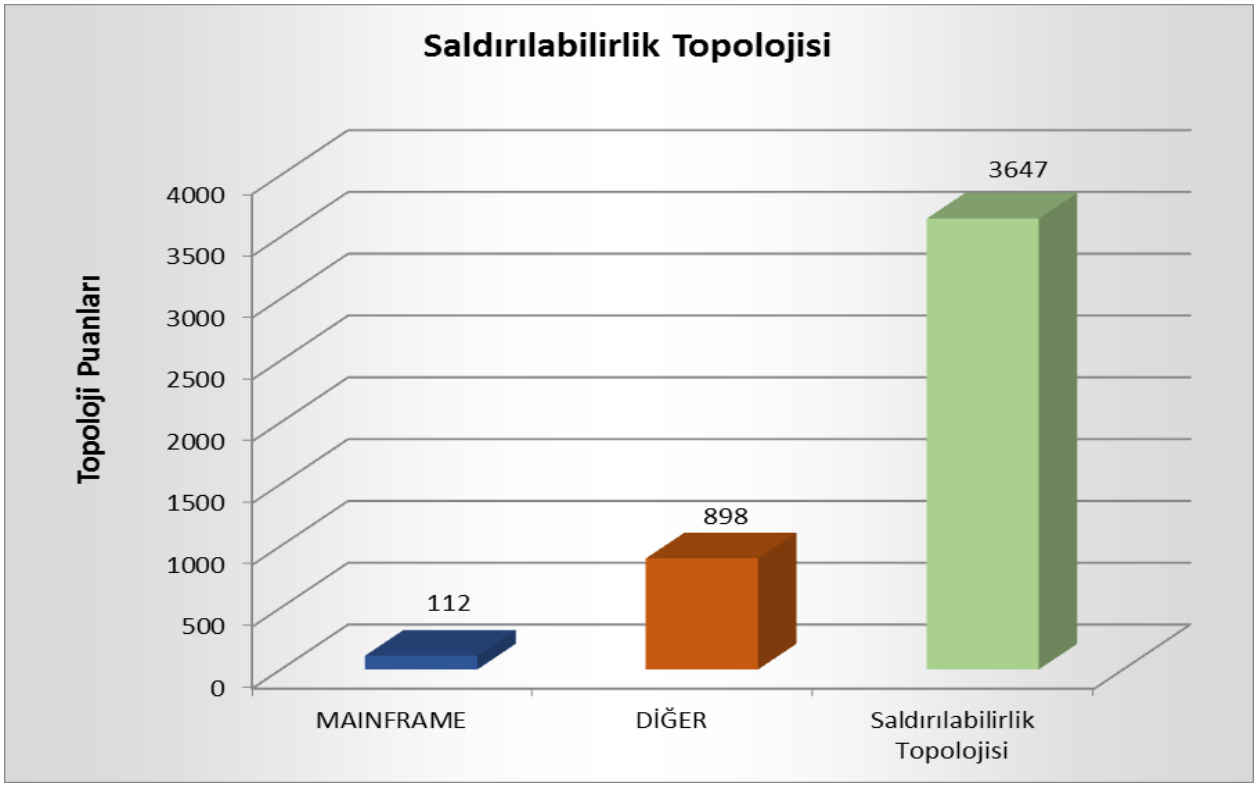
Taktiksel müdahalelerin güvenlik ve önleme katmanlarının eklenmesini içermesi halinde sonuçta ortaya çıkan mimari bir soğana benzemekte, ek güvenlik sağlamayı amaçlayan üst üste binmiş katmanlara sahip bir yapı haline gelmektedir. Ancak gerçekte, bu katmanların kendileri, saldırılabilirliği kolaylaştıran ek noktalara sahip bir topoloji oluşturabilmektedir.

Kısmi bir çözümün «eklendiği» her bir nokta, bilgi sahibi bir korsan için yeni bir hedefe dönüşmektedir. Katmanlar ne kadar karmaşık olursa, saldırılabilirlik topolojisi o kadar yükselir. Bu açıklık, sigorta şirketleri tarafından bir kuruluşun önemli bir siber hasara yönelik risklerini belirlemek için sigorta şirketleri tarafından giderek daha fazla kullanılan bir güvenlik risk profilinin parçasıdır.



Güvenliğe gösterilen bu ek vurgu sanallaştırma yazılımlarının daha fazla kullanılmasıyla ortaya çıkmaktadır. Bu sanal makinelerin her biri (VM'ler), yeni açık noktaları oluşturur ve güvenlik tehdidinin karmaşıklığını daha da artırır. Giderek daha çok kuruluşun hibrit bulut çözümlerini benimsemesi ve inşa etmesiyle birlikte tepkisellik ve esnek güvenlik uygulamaları da artan talep doğrultusunda gelişerek evrilmelidir.

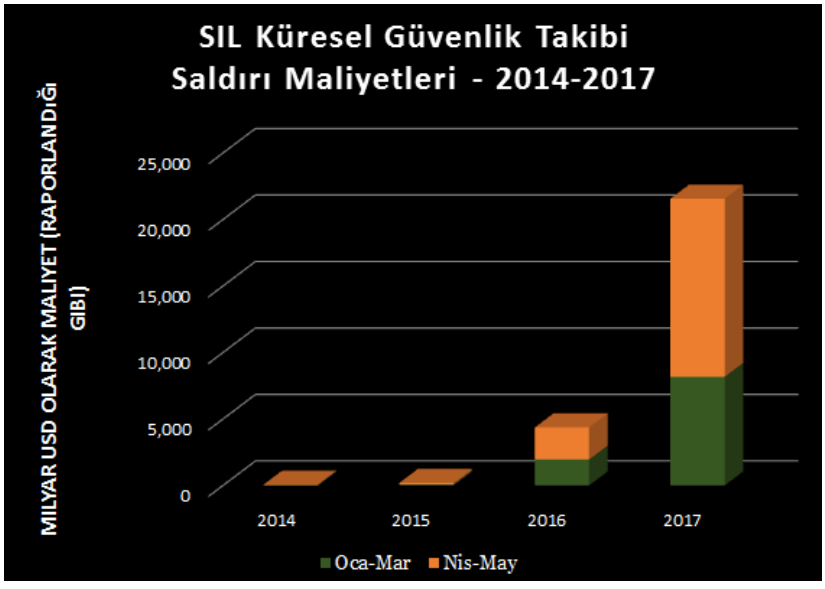
Saldırılabilirlik topolojisi temel mimariler arasında önemli farklar göstermektedir. 115 binin üzerinde işletmeden oluşan bir grup üzerinde gerçekleştirilen bir genel analiz, bu farkı burada görüldüğü gibi göstermiştir.



Bu önemli fark temel yapıdan ve platform mimarisinin ardından gerçekleştirilen stratejiden, çip tasarımından, işletim sisteminden ve yığın entegrasyonu yönteminden kaynaklanmaktadır.

Son dört yıl boyunca bildirilen saldırı detaylarına bakıldığında, hem saldırı sayısında hem de ilgili hasar maliyetlerinde katlanarak büyüyen bir artış görülmektedir.

Not: SIL, gerçek dünya, üretim uygulamalar hakkında verileri toplamaktadır. Bu veriler operasyonel uygulamalar, davranışlar ve kıstaslar hakkında tedarikçilerin iddiaları veya yapay piyasa göstergeleri ile kirletilen kuramsal bilgilerin yerine fiili bilgiler sağlamaktadır.



Değişen tek şey saldırı sayısı değildir. Son 20 yılda saldırıların görünümleri önemi bir değişim kaydetmiştir. 20 yıl önce güvenliğin çoğunlukla erişim kontrolü ile ilgilenmesi karşısında günümüzde, tehdit topolojisi çok daha karmaşık bir hal almıştır.

En hızlı gelişen tehdit vektörlerinden biri fidye yazılım saldırısıdır. Bu saldırı türünde, saldırı sonucunda dosyalar, dizinler ve sistemin diğer bileşenleri kilitlenir. Sistem sahibinden, gerçekten işe yarayabilecek veya yaramayacak bir kilit açma kodu için ödeme yapması istenir.

> *«Bu yıl 5 önemli güvenlik sorunu dalgasıyla vurulduk. Bunlardan bazıları kötü niyetli olurken, diğerleri ise şantaj amaçlıydı. Ana web sunucularımızı geri almak için 1 milyon USD'nin üzerinde bedel ödedik ve hâlâ korsanların bunlara nasıl erişebildiklerinden emin değiliz. Bizim için müşterilere, tonlarca zamana ve paraya mal oldu. Bu kesinlikle, hiç iyi bir his değil.»*
>
> CFO: Orta Ölçekli İmalatçı

Güvenlik Platformu Karşılaştırması

Güvenlik ölçümü, acı ve sorunların bulunmamasıyla değerlendirildiği için yansıtıcıdır. Güvenlik aksaklığı yüksek oranda görülebilir; ancak güvenliğin başarısı ise görünmez. Güvenlik ile ilişkili yansıtıcı ölçümlerin anlaşılmasını sağlamak için IBM, anketler yürütmesi, verileri toplaması ve kuruluşların IBM Z mainframe platformunu bilişim mimarisinin bir parçası olarak uyguladıklarında diğer emsal platform mimarilerine göre elde edecekleri faydaların ve ilgili maliyetlerin net bir şekilde anlaşılmasını sağlayan bir analiz gerçekleştirmesi için SIL'i görevlendirmiştir. Bu analiz, öncelikle bir işletme perspektifinden güvenliğin değerine yönelik olarak gerçekleştirilmiştir; böylece, görevleri işletmeye liderlik sunmak olan kişiler, güvenlik çözümlerini değerlendirirken IBM Z güvenlik tekliflerinin faydalarını anlayabileceklerdir.

Bu araştırma boyunca, yazılım ve donanımların ana davranışsal özellikleri çok sayıda fiili müşteri sistemi (9.602.000+) üzerinde yakından incelenmiştir. Bu müşterilerin hepsi, üretim ortamlarının bir parçası olarak güvenliği uygulamışlardır ancak güvenlik yöntemleri ve mekanizmaların karması bakımından farklılık göstermektedirler. Bunlar, HIPAA, PCI, SOX vb. gibi bilgilerin güvenliği için düzenlemelere tabi olan ve sektör standartlarını desteklemek için gereken organizasyonları içermektedir. Müşteri raporlarından ve onlara eşlik eden gerçek dünya detayları kümesinden elde edilen

bilgiler farklı güvenlik türlerini kullanmanın müşteriyi nasıl etkileyebileceği hakkında kuramsal olmanın yerine gerçekçi bir anlayış sağlamaları nedeniyle değerlidir.

Detaylı saldırı faaliyetlerinden ve GSW'nun etkisinden elde edilen 81 milyonun üzerindeki veri noktası beklenebilir maliyetler ve risk hakkında bir temel sağlamaktadır. Bu temel, günümüzün piyasalarında güvenliğin ve varlıkları korumanın anlaşılması için son derece önemlidir.

Araştırma verilerinin toplanması ve çözümlenmesinde çeşitli özelliklere ulaşılmıştır. Bu özellikler güvenli ortamın açık kapasitesini, verimini ve güvenilirliğini etkilemektedir. Ayrıca, güvenlik ve işletme faaliyetlerinin sinerjisi incelenmiştir. Temsil edilen davranış uygulamaya yönelik olası seçeneklere yansıtılmış ve modellenmiştir. Bu anlayışı oluşturmak için yalnızca sunucu performansından fazlası gerekmektedir çünkü, nihayetinde güvenliğin iş süreci ve faaliyetleri sekteye uğratmayıp koruması gerekmektedir. Güvenlik sistemlerinin kapasite talebi ve üretim etkileri önemli olsa da, bunların işletme koşullarına dönüşümü günümüz pazarını daha çok ilgilendirmektedir. İşletme perspektifi güvenilirlik, güvenlik dereceleri, personel seviyeleri, toplam güvenlik maliyeti (kurtarma dahil) ve diğer etkiler gibi çok çeşitli faktörleri kapsamaktadır. Bu durum bilişim müdürleri, baş teknoloji yöneticileri ve işletme liderliğinin günlük olarak alması gereken kararlarla doğrudan bağlantılıdır.

Perspektifler ve Görüşler

Analizin kendisinden kaynaklanan iki perspektif veya görüş kümesi bulunmaktadır. İlk perspektif, şunları içeren göreli faaliyet ve performans kategorileri ile ilgilidir:

- Operasyonel verimlilik
- Güvenliğin etkililiği
- Bilişim riski
- Esneklik ve çeviklik

Bu alanların her biri başka bir perspektif katmanına kapı açmaktadır. Bu katman dahilinde önem ve odak, güçlükleri ve güvenliğin alt bölümlerini dikkate alan organizasyon bölümüne göre farklılık göstermektedir. Bu sorumluluk ve farkındalık yapısında iki ana kısım bulunmaktadır: işletme ve teknik Teknik kısım tipik olarak kuruluşun ve güvenlik yönetiminin görünüşüyken, güçlük kapsamının artması ve siber suç yöneylerinin değişmesi güvenlik ile ilgili ana sorumluluğun işletmeye geçmesine sebep olmuştur.

Sonuç olarak, Bilişim Teknolojisi (IT) Bölümü, işletme birimlerini desteklemek üzere tasarlanmıştır. Araştırma verilerinin ana kaynaklarından biri, güvenliğin hem şirket yönetimi hem de faaliyet birimi yönetimi olarak işletme yönetimi açısından nasıl göründüğüdür. Araştırma kuruluşlarından elde edilen faaliyet örüntüleri, bunların işletme ölçütleri üzerindeki etkilerinin tespit edilmesi için karşılaştırma amacıyla dört alanda işlenmiştir. Bu işletme ölçütlerinin her biri, IBM Z güvenlik çözümünün görüntülenmesi sırasında ölçülebilir ve önemli farklara sahiptir ve organizasyonun kritik düşüncesi kapsamında dikkate alınmalıdır.

Teknik güvenlik yönü de çalışmada temsil edilmektedir. Bunların IT için nispeten geleneksel sorumluluklar olması, evrilen siber güvenlik dünyasındaki önemlerini azaltmamaktadır.

Kategorilerin çoğu, hem işletme hem de teknik bakış açılarına değinen bulgulara sahiptir. Organizasyonların günümüzde karşılaştığı güçlüklerin karmaşıklığı bakış açısının, yetkilerin, iş ihtiyaçlarının ve sorumluluğun karmaşıklaşmasına neden

olmaktadır. Bu araştırma, bu güçlük bileşenlerin bazılarının verilere dayanılarak ifade edilmesini sağlamaktadır.

Araştırmada platform türüne göre özetlenen tanemsi ölçütler, uygulayıcıların genel nüfusunda özel bir başarı kriterinin nasıl farklılaştığını göstermektedir. Bu ölçütler kapsam bakımından geniştir ve hem organizasyonel vasıflara hem de mali hususlar gibi alanlara değinmektedir. Kısa tanımlarla ve her bir platform uygulamasının odaklandırılmış net etkisiyle sunulmaktadırlar. Çeşitli sektörlerde anlamlı olabilmeleri için hepsi de, bir iş birimi temelinde[4] normalleştirilmiş ve organizasyon boyutu seviyelerine (küçük, orta, büyük ve çok büyük) göre kategorize edilmişlerdir. Temel ölçüm orta ölçekli bir şirkete dayandırılmıştır; böylece diğer tüm ölçütler bu standart ayar noktasına göre yapılan farklılaştırmalara dayanmaktadır. Bu çalışmada yer alan uygulamalar üretimdekiler ile sınırlı tutulmuştur.

OPERASYONEL VERİMLİLİK

Operasyonel verimlilik, bir işletmenin müşterilerine veya ortaklarına en maliyet verimli şekilde ürünlerini veya hizmetlerini sunarken aynı zamanda yüksek kalite standartlarını koruyabilme becerisidir. Operasyonel verimlilik, bir işletme operasyonunu çalıştırmaya yönelik girdi ile işletme tarafından kazanılan çıktı arasındaki oran olarak görülebilir. Operasyonel verimliliğin iyileştirilmesi sırasında çıktıların girdilere oranı daha elverişli hale gelir. Girdiler tipik olarak paraya (maliyet), kişilere (personel sayısı veya Tam Zamanlı Çalışan Eşdeğeri - FTE) veya zaman ve çabaya dayanmaktadır.

Güvenliğin operasyonel verimlilik bakış açısıyla ele alınması halinde, yapılan katkılar bu özel alanlardan temin edilir. Güvenliğin operasyonel veriminin ölçülmesindeki güçlük onun bütünleşik yapısından kaynaklanmaktadır. SIL analizi, şunları içeren ayrı öneme sahip çeşitli alanları incelemiştir:

- Personel yükü
- Toplam Sahiplik Maliyeti (TCO) bütünleştirmesi yoluyla hedeflendirilmiş giderler
- İş Yükü

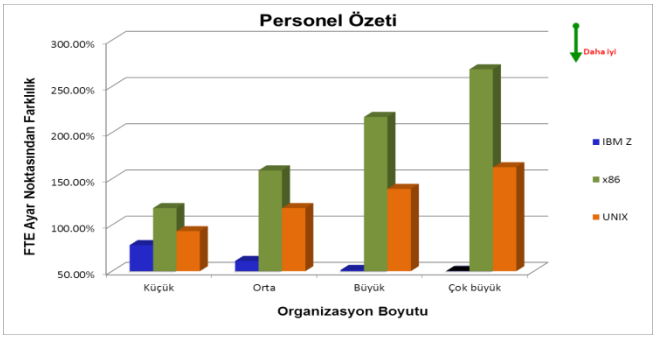
Bu alanlarda hem işletme bilgisi hem de teknik bilgi ihtiyaçlarına değinilmektedir. Ancak işletme değerlendirmesine karşı teknik değerlendirmenin farklı örüntülerini oluşturan verilerden ölçütler türetilir. Ölçütler, farklı grupların organizasyonel sorumluluklarına uygun hedefler ile hizalandırılmış güvenlik yönlerini stratejilendirmesi ve kontrol etmesini sağlamaktadır.

İŞE ALIM

Kendisini başka pek çok alanda gösteren temeldeki bir faktör, güvenlik yöneticisi ile altyapı arasındaki arayüzün verimidir. Yazılım, donanım ve işletim sistemi bileşenlerini ve istihdam üzerindeki sonraki etkisini içermektedir. İstihdam verimi arttıkça üretkenlik düzeyi de gelişmektedir. Güvenlik arenasında aynı görevin başarılması için gereken çaba, güvenlik personelinin her bir ferdinin daha üretken olmasını sağlayacak şekilde azaltılmaktadır.

[4] İş birimi esası yayınlanmış Uluslararası Birim Noktası Kullanıcı Grubu standartları kullanarak tanımlanmıştır ve fonksiyon noktası (FP) analizine dayanmaktadır.

Kullanıcı deneyimi üzerinde bu etkiyi sağlayan herhangi bir özel bileşenin verimini, detay yoğunluğu nedeniyle etkisini kaybeden aşırı detaylandırılmış karşılaştırmalardan başka ölçütlere ayırmak güçtür. Personelin, Tam Zaman Eşdeğerine (FTE) yönelik genel bir görünüm, platform karşılaştırması için bir genel ölçüt sunulması amacıyla gözden geçirilmiştir. Güvenlik personeli çalışmalarına yönelik genel ortalama, grafiğe başka bir karşılaştırma ölçütü olarak dahil edilmiştir. Bu ortalama, boyutuna bakılmaksızın tüm raporları birleştirmektedir.



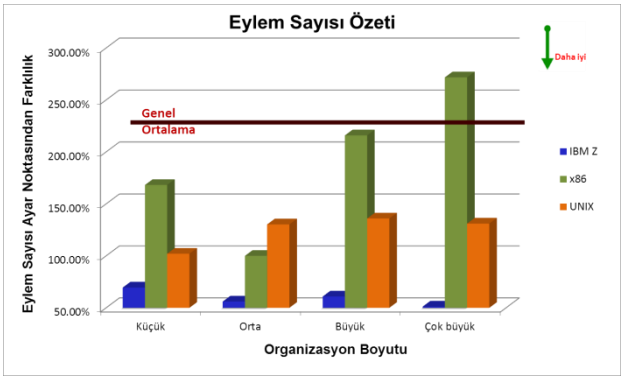
Karşılaştırmalı çaba seviyeleri, her bir işletim sistemi grubu için bir 'altın standardı' ortamın sağlanması için gerekenlerdir. Sistemlerin üzerindeki iş yükü, daha önceki karşılaşmalarda tanımlandığı gibi aynı karşılaştırma alanı düzeyinin sağlanması için eşit seviyelerde normalleştirilmiştir. Güvenlik bileşenleri için bu kadar çok seçenek bulunduğundan karşılaştırmayı sağlamaya yönelik ayar noktası, geleneksel müdahale alanının medyanıdır.

> *«Üç yıl öncesi ile karşılaştırıldığında z (metindeki haliyle) platformundaki iş miktarının yaklaşık dört katı ile çalışıyoruz. O sırada iki kişiyi kaybettik ancak kalan kişiler yine de tüm işi üstleniyor.»*
>
> *Diğer platform gruplarımızdaki artış ile karşılaştırdığınızda, onlara yönelik işi gerçekleştirmek için neredeyse on katı daha fazla personele sahip olmalıyız.*
>
> CIO - Büyük Mali Hizmetler

Farklı güvenlik mimarilerinin değişen uygulama standardı kümelerine sahip olması nedeniyle, istihdamın değerlendirilmesi sırasında bu standartların kesinliğinin tutulması önemlidir. IBM Z'nin uygulanması ve kullanılması için fark edilir oranda daha az personele ihtiyaç duyulması, Z işletim yigininin bütünleşik yapısına doğrudan atfedilebilir. Bir işletmenin boyutu arttıkça veya bir işletme, bir bulut hizmet sunum modelinde ilerledikçe bu duruma özellikle dikkat edilmelidir. IBM Z, diğer alternatiflere göre %88,35 daha z güvenlik personeli süresi gerektirir.

Bu operasyonel verimliliğin önemli bir kısmını manuel görevlerin sayısı ve bu görevleri gerçekleştirmek için gereken sürenin uzunluğu oluşturmaktadır. Sayılan ve zamanlandırılan görevler, güvenlik personeli tarafından aynı seviyede inceleme özeninin başarılması için uygulanması gereken görevler, öncü faaliyetler ve müdahaleye yönelik değişikliklerdir. Platform farklarını kapsamlı bir şekilde anlamak için SIL'e 620'nin üzerinde müşteri tarafından detaylı video ve eylem tespit bilgisi sunulmuştur. Bu veriler bir zaman hareket ve eylem çerçevesi içinde birleştirilmiştir; nedensel zincirler ve verimlilikler bakımından analiz edilmiştir ve farklı platformların bir çalışma karşılaştırmasını oluşturmak için kullanılmıştır. Karşılaştırma verileri, işbu belgenin diğer kısımlarında açıklandığı üzere eşit bir oyun sahası sunmak için normalleştirilmiştir. Sonuçtaki eylemlerin karşılaştırması ve zaman çizelgesi karşılaştırması aşağıdaki şemalarda görülebilir.

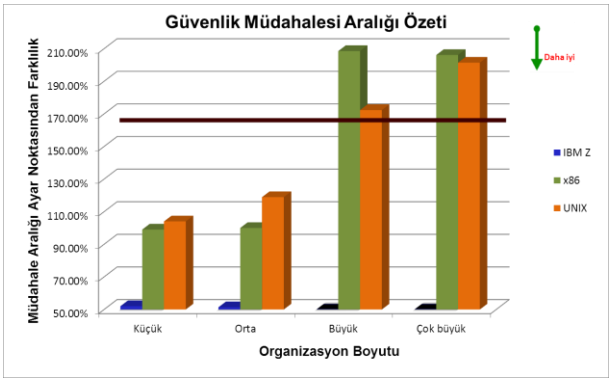
Güvenlik eylemi görevleri temeldeki platform ve organizasyon boyutu nedeniyle önemli değişikliklere uğrar. Genel olarak, organizasyon büyüdükte güvenlik uygulamasının da daha kapsamlı ve çeşitlendirilmiş olması gerekir. Platform türü, bu



artan gayretlere başka bir iş profili boyutu ekler. Güvenlik standartlarını sürdürmek için gerçekleştirilmesi gereken işlemlerin temel sayısı karşılaştırıldığında, IBM Z güvenlik personeli tarafından manuel olarak gerçekleştirilmesi gereken görevlerin sayısını, diğer platform görevlerine göre önemli oranda daha düşük olduğu bulunmuştur. Zaman ve hareket araştırmaları, Z güvenlik çözümlerinin, standart koruma seviyelerinin uygulanması için %81,17 daha az görev gerektirdiğini göstermektedir. Personel sorumluluklarına daha az görevin dahil edilmesi personelin üretkenliğini önemli oranda artırmaktadır. Bu aynı zamanda önemli oranda çok daha az sayıda program geçiş anahtarı gerektirmesi yoluyla güvenlik arenasında tutulması gereken FTE seviyesini azaltabilir ve böylece riski düşürür.

> *«Z platformlarımızdan sorumlu teknik güvenlik yetkilileri, öncü tedbirlerin alınması da dahil olmak üzere görevlerinin tamamını yerine getirmek için tutarlı bir şekilde yeterli zamana sahip oldu. UNIX ve Wintel ortamlarımızı destekleyenler için ise aynı şeyi söyleyemeyiz. Bunun nedeni, işleri yapmaları için gereken çaba ve süredeki farklılık. Z'nin korunması, diğer platformların aynı oranda korunması ile karşılaştırıldığında çok daha kolay ve çok daha verimli.»*

Güvenlik Direktörü: Orta Ölçekli İmalatçı



Güvenlik hedeflerinin yerine getirilmesi için gerekli süreler üzerinde, ona karşılık gelen bir etki bulunmaktadır. Çizelge, güvenlik değişikliği yanıt süreleri üzerindeki etkiyi göstermektedir. Bu ölçüt, platform grupları ile ilişkili yerleşik güvenlik çevikliğini göstermektedir. Burada belgelendirilen daha düşük yanıt çerçeveleri daha hızlı müdahaleyi belirtmektedir ve bu, güvenlik dünyasında saldırı hasarının en aza indirilmesi anlamına gelmektedir. Bu toplama dahil edilen zaman aralıkları, normal tasarım, bakım ve öncü davranışın parçası olanlardır. Saldırı incelemesinin bir parçası olan eylemler ve aralıklar bu görselleştirmeye dahil edilmemektedir.

Güvenlik personeli için normal, altın standardı faaliyetlere ilişkin faaliyet aralığı, Z uygulamaları için istihdamın bu yönü bakımından önemli avantajların bulunduğunu göstermektedir. Z üzerinde aynı faaliyetler, diğer platformlara oranla *%81,66* daha az süre tutmaktadır.

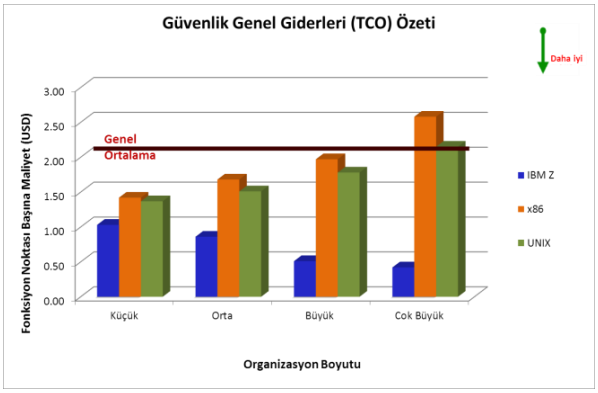
> *«Mainframe üzerindeki güvenliğimiz, organizasyonumuzun en az sorun yaşadığı alan. Mainframe bizim için en az soruna yol açtığından, çoğu*

zaman mainframe üzerinde bir güvenlik grubuna sahip olduğumuzu bile unutuyoruz.»

CIO - Orta Ölçekli Mali Grup

TOPLAM SAHİPLİK MALİYETİ

Toplam sahiplik maliyeti (TCO), operasyonel verimlilik bakımından işletme kısmındaki ana ölçütlerden birini sunmaktadır. Bu yüksek seviyeli ölçüt, güvenlik uygulamasının herhangi bir yönüne katkıda bulunan organizasyon dahilindeki tüm masrafları bir araya toplamaktadır. Araştırma analizinin bu kısmında, varlıkların korunmasına katkıda bulunan tüm masraflar özetlenmektedir. Fiziksel güvenlik dahil olmayıp, diğer tüm yönler bu araştırmaya dahildir. Bir kez daha, projeler ve bunların giderleri standart esasa göre normalleştirilmiştir. Bu, büyük ve küçük işletmeleri mümkün hale getirmekte ve masraflarının daha tutarlı bir şekilde karşılaştırılmasını sağlamaktadır.



TCO'nun güvenlik uygulaması için izole edilmesi, güvenliğin giderek artan miktarda bir organizasyon operasyonlarının tüm yönlerine dahil edilmesi nedeniyle daha güç hale gelmektedir. TCO'nun, fonksiyon noktaları gibi bir standart iş birimi tanımına dayanılarak normalleştirilmesi yoluyla, tutarlı bir karşılaştırma yapılabilir ve eğilimler vurgulanabilir. Harcama kalıpları, uygulama karmaşıklığı arttıkça platform türlerinin bazılarında artma eğilimleri göstermektedir. IBM Z'de ise aksi bir eğilim görülmektedir. İskelet yapı ve temelden yararlanmanın mali yatırım için maliyet verimli bir yapı sağladığı durumlarda birim giderdeki düşüş eğilimi bir ölçek verimliliği sağlamaktadır. Ekteki şemada görüldüğü üzere, Z güvenlik uygulamalarına ilişkin giderler diğer platformlarınkine oranla %83,72'ye varan oranda daha düşüktür. Bu durum kısmen tasarlanan güvenlik tabanı kombinasyonundan ve yüksek oranda ölçeklendirilebilir platformdan kaynaklanmaktadır. Bu sinerjinin verimi, mimari daha ağır bir şekilde yüklendikçe iş birimi maliyetinde önemi bir düşüş olarak görülmektedir. Bu ayak izi, mimarinin yüksek oranda ölçeklendirilebilir ortamlar için tasarlandığı tüm durumlarda bulunmaktadır ancak normalde, sadece donanımda daha fazla görülmektedir. Bu durumda, ölçeklenebilirliğe ilişkin tasarımın ortaklığı hem fiziksel donanım hem de işletim sisteminde bulunmaktadır.

«IBM mainframe'imiz bir şirket olarak yaptığımız diğer her şeyden çok daha düşük bir maliyete sahip. Finans çalışanlarımız maliyetlerin aşırı yüksek olduğunu ısrarla bize söyleseler de, masraflar aslında son üç yıl boyunca düştü. Onlara, sorunlarımız azaldığını, personelimiz azaldığını ve sorun çıkma olasılığının da azalması nedeniyle genel maliyetimizin düştüğünü söylüyorum.»

CFO - Çok Büyük Distribütör

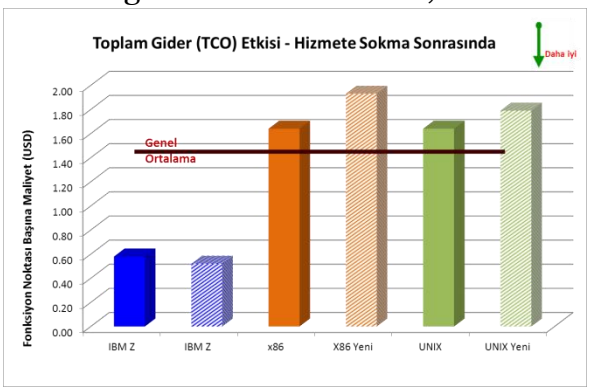
Tasarlanan ölçeklenebilirlik, özellikle sistemler daha karmaşıklaştığında, örneğin kullanıcılar ölçek büyülttüğünde, kendi cihazlarını getirmeleri (BYOD) daha yayınlaştığında veya yoğun bulut uygulamaları ve çoklu erişim kullanıldığında önem kazanıyor. Bulutun benimsenmesindeki artış ve buluttaki uygulamaların

kullanımındaki artış tepkisel güvenliğin sağlanmasında karşılaşılan zorlukları daha da artırmıştır. Bulut kullanım biçimi de güvenlik güçlüklerini etkilemektedir. Özel, devlete, topluma ait veya hibrit bulut kullanımı fark etmeksizin güvenlik uygulamaları sürekli evrim geçirmelidir.

Kontrolün ve erişilebilirliğin hibrit bulutların kullanımına göre dengelenmesinin avantajları daha iyi anlaşılır hale geldi ve bu bulut kullanım biçiminin benimsenmesi hibrit bulutun en popüler yeni uygulama seçeneği haline gelmesine neden olmuştur. Çok sayıda platform mimarisinin hepsinin güvenceye alınması gerektiği için bu durum en karmaşık senaryolardan birini sunmaktadır.

Güvenliğin bir dizi ek koruma bileşeniyle sağlandığı durumlarda veya ana güvenlik yönetişiminin sadece kullanılan uygulamada bulunduğu durumlarda genel masraf karşılaştırması yeni hizmetler eklendiğinde önemli bir sıçrama göstermektedir. Aşağıdaki çizelgede bu tür bir etki görülmektedir. Analizin bu kısmında yer alan projeler güvenlik kazanımının kısa vadeli etkisini göstermektedir. Her durumda, bu 16.027 organizasyon, mevcut bulut uygulamalarına tek bir bulut uygulaması eklemiştir. uygulamalar özel, kamu ve hibrit bulutlarını hedeflemiştir ve 1000'den fazla kullanıcı için tasarlanmıştır.

Fonksiyon noktalarına dayanan TCO, devralım sırasında mevcut olan kısa vadeli masraf farkını göstermektedir. İş birimi giderlerinin geneli üzerindeki etki, teknolojinin işletme üzerinde sahip olduğu etkiyi göstermektedir. Ek iş yükü, IBM Z uygulamasının daha yüksek fonksiyon noktası sayısı boyunca istikrarlı bir güvenlik maliyeti yayılmasını sağlamış ve hiçbir önemli masraf eklememiştir. Diğer platform grupları, lisanslar vb. hakkında ek masraf gerektirmiştir. Tek bir ek bulut uygulaması öncesindeki ortalama etki Z uygulamalarını ortalama *%14,02* oranında azaltırken, alternatif platform çözümleri ise *%19,62* kadar artırılmıştır. Özet grafik, mimari grupların her biri için ortalamayı göstermektedir. Her bir proje için temeldeki veriler, IBM Z uygulamalarından hiçbirinin fonksiyon puanı başına TCO'da bir artış göstermemesi, ancak bunlardan ikisinin sıfır etki göstermesi bakımından fark edilebilmektedir. Diğer mimariler, bireysel sonuçların *%2,9'dan %38,4'e kadar* değiştiğini göstermiştir. Etki örüntüsü, bulutu hedefleyen gelişmekte olan bir işletme, dağıtık kullanıcı aygıtlarında genişleme ve önemli miktarda yeni hizmetlerin sunulmaya başlanması çerçevesinde dikkate alındığında önemlidir.



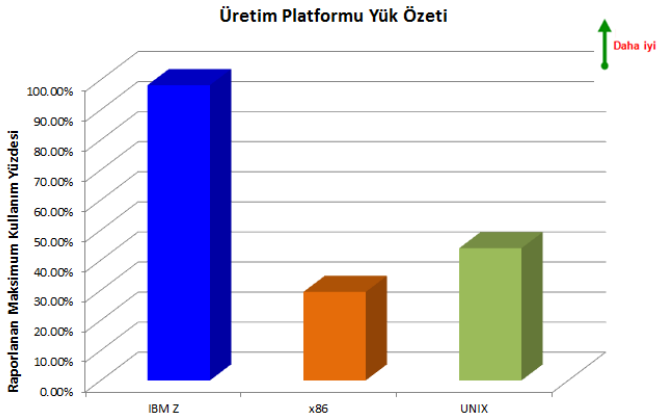
Güvenliğin asıl maliyetinin ve etkisinin iletilmesi ise başka bir güçlüktür. Güvenlik iyileştirmeleri ve geliştirmeye yönelik bir iş olgusunun dile getirilmesi sık ele alınan bir tartışma konusudur ve tüm dünya çapında güvenlik uzmanlarının dile getirdiği bir şikayet konusudur. Operasyonel verimliliğin bir yönü olarak güvenliğin maliyet etkisi işletme yöneticilerinin çoğunluğu tarafından net bir şekilde anlaşılmamaktadır. 2015-6 yılında 9,5 milyondan fazla kurumsal yönetici içeren bir araştırmada toplanan veri havuzunda, yöneticilerin %11'inden daha azı güvenlik harcamalarına ilişkin bir vaka incelemesi görmüştü. Bu insanların %0,9'undan daha azı güvenlik maliyetlerinin, ölçek ekonomilerinin ve tahmini giderlerin nasıl türetildiğini anladıklarını iddia etmiştir. Ne yazık ki stratejik organizasyonel kararların alınmasından sorumu kişilerin %35'inden daha azı güvenlik personelinin maliyetlerin nasıl tahminlendirileceğini veya hesaplanacağını anladıklarına inanmıştır. Bütün bunlar atanan genel güvenlik iş

yükü maliyetlerinin azalmasının veya artmasının beklenmediği ve değerlendirilmediği bir duruma katkıda bulunmaktadır. Bu özel kör nokta ile birlikte, şirket yönetimi IBM Z güvenlik uygulamalarının ölçeklendirilebilir verimliliğini anlamakta başarısız olmaktadır.

İŞYÜKÜ

TCO'nun ölçümü esasen bir işletme ölçütünde yer almaktadır. Büyüme ve masraflardan daha fazla yarar elde etme amacıyla ölçeklenebilirliğin temel özelliklerini barındırmaktadır. Ancak ölçüt, ham biçiminde ölçeklenebilirlik ve esneklik ile ilgilidir. Güvenlik kaynaklarının verimli bir şekilde yönetilmesi, güvenlik uygulamasının sürdürülmesi için gereken personel zamanının ve bütünleşik altyapı ve yazılım masraflarının kontrol edilmesine dayanmaktadır. Ölçeklenebilir ve esnek platform mimarisi zaman ve para kaynaklarının verimli bir şekilde harcanmasına temel oluşturmaktadır. Daha ölçeklendirilebilir bir platform daha aza uygulama projesinin uygulanmasının gerekmesi anlamına gelmektedir ve işletmeyi desteklemeyeyönelik bilişim kaynaklarının kabiliyetleri büyük oranda artırılmaktadır. Bu nedenle, ek iş yükünü uygulamaya koymak için az sayıda faaliyet gerektiren yüksek oranda ölçeklendirilebilir bir platform, bilişim hizmetleri gurubunun operasyonel verimliliğini artırmaktadır.

Uygulama ölçeklendirilebilirliğinin ve esnekliğinin bir boyutu, bir temel mimarinin güvenilmez ve hatalı performans öncesinde yüklenebileceği bir temel mimari seviyesidir. Bir makinenin teorik maksimum kapasitesinin daha yüksek bir yüzde ile kullanılabilmesi giderlerin ve riskin azalmasını sağlar. Çalışma grubunun bildirdiği maksimum üretim yükü platformun iş yükünü sürdürebilme kabiliyetinde operasyonların sorunsuz bir şekilde sürdürülmesinden sorumlu uzmanların güvenini belirtmek için kullanılmıştır. Daha yüksek bir seviyeye ulaşan ancak 10 dakikadan kısa bir süreye sahip olan iş yükleri bu analizin dışında bırakılmıştır.



«Bize sistemlerimizin normalde ne kadar yüksek çalştığını sorduğunuzda sadece size verileri göndermekle kalmadık, aynı zamanda bunları inceledik. Wintel platformlarımızdaki ortalama yükümüzün %14'ten az olduğunu, buna karşın mainframe'imizin tutarlı bir şekilde +%98 ile çalıştığını fark etmemiştim. Sanırım, bu platformun ne kadar verimli olduğunu hiç fark etmemişim. Nedense, tüm platformların aynı seviyede verime sahip olduğunu zannetmişim. Bu, kesinlikle hangi uygulamayı nerede barındırdığımızı daha yakından incelememize neden olacak.»

COO - Büyük Sağlık Kuruluşu

GÜVENLİĞİN ETKİLİLİĞİ

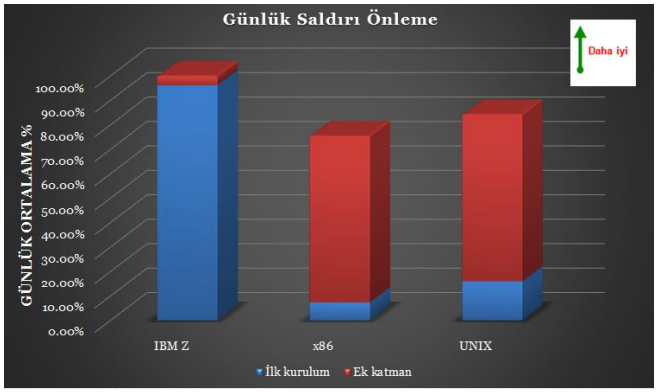
Güvenliğin etkililiği alanını incelemek için SIL, nesnel ve öznel ölütlerin kombinasyonu halinde ölçülebilir karşılaştırmalar tespit etmiştir. Nesnel ölçütler, hem rapor edilen

saldırılarda em de detaylı denetimlerde keşfedilenlerde güvenlik önlemlerinin başarılı saldırıları tespit ederek önleme kabiliyetini içermiştir. Bu ölçütte yer alan bilgiler organizasyonun hem teknik yönü hem de işletme yönünde uygulanabilirliğe sahiptir çünkü saldırıların miktarı büyük oranda organizasyon kâr hanesinde bir etkiye dönüştürülebilir.

Bu alanların her biri IBM Z siber güvenlik çözümü için birkaç önemli farklılaşma sağlamaktadır.

SALDIRIYA KARŞI DİRENÇ

Güvenlik başarısının ana ölçütü tuzağa düşürülen, nötrleştirilen veya herhangi bir hasar vermesi önlenen saldırıların sayısıdır. Bu ölçütte bir araya getirilen saldırılar, eklenti güvenlik duvarları ve güvenlik aygıtları tarafından engellenen saldırıları içermemektedir. Onun yerine, sadece platform üzerindeki güvenlik çözümü tarafından engellenmiş olanlar sayılmıştır. Bu sayılar, her bir VM'nin ayrı bir mantıksal yapıyı temsil etmesi nedeniyle bir platformda bulunan fiili VM sayısına göre normalize edilmiştir. Her bir VM'deki kullanıcıların sayısında hiçbir ayarlama yapılmadığı için bu bir gösterge ölçüttür.



Platformların her biri için ilk kurulum yoluyla sağlanan saldırı engelleme seviyesi, gereken veya kurulan her türlü ek güvenliğin temelini oluşturmaktadır. Bu grafik, ilk kurulumun ve ek katmanın sağladığı güvenliği, engellenen saldırıların bir yüzdesi olarak ifade etmektedir. İlk kurulumlara dayanılarak, temel IBM Z güvenlik çözümleri alternatif platform çözümlerinin başlangıç seviyesinin *13,21 katı* kadar fazla çözüm sağlamaktadır. Ayrıca Z çözümü, alternatif mimariler için gereken eklenebilir ilaveler olmadan dahi %92,1'i aşan temel bir koruma sağlamaktadır.

Ek güvenlik katmanları eklenti uygulamalar, taktikler ve teknikler vb.'dir. Bunlar organizasyondan organizasyona farklılık göstermektedir ancak, bireysel güvenlik gözetimi, duruluşu ve yönetimine dayanılarak değişkendirler. Ek güvenlik gereksinimlerinin seviyelerinin artması, güvenlik yazılımı ve personel açısından gayret düzeylerinde bir artışı göstermektedir.

Fikri mülkiyet sermayesi ve otomatik hizmetlerin birleşimi, IBM Z siber güvenlik çözümlerinin mimari tasarımıyla birleşerek önemli oranda çok daha yüksek bir yüzde ile saldırıların önlenmesini sağlamaktadır. Z platformu, diğer alternatif platform çözümleri için sunulan ek güvenlik taktikleri, teknikleri ve prosedürleri için yoğun, yetkin ve gayretli çabalar ile artırılan birleşik güvenlik temelinden *%20,74'e* varan oranda daha iyi temel saldırı müdahalesi sunmaktadır.

Güvenlik çözümünün etkililiğine yönelik daha fazla bilgi için daha derinlemesine bir bakış gerekmektedir. Güvenlik hizmetleri, her türlü donanım, yazılım ve ara yazılım bileşeni dahil mimarinin temeli ile başlar. Bunun üzerine organizasyonel politikalar, prosedürler, vaziyet ve yönetişim katmanlandırılır. Bunlar mevcut en iyi uygulamalar karşısında ölçülebilirken ve önemli bir farklılaşma olarak kabul edilirken bu araştırma platform donanımlarını, yazılımlarını ve işletim sistemleri dahil orta yazılımlarını birleştiren tedarikçi çözümlerinin incelenmesine odaklanmıştır.

«z (metindeki haliyle) platformunun neden daha az güvenlik sorunu çıkardığı hakkında kesinlikle hiçbir fikrim yok, ama hiçbir güvenlik sorunu yaşamadığımızı biliyorum. Güvenlik personeli sürekli olarak bana bu konuda bir şeyler söylüyor ve söyledikleri, bunun gerçekten işe yaradığını gösteriyor. Bu platform üzerinde en son bir güvenlik sorunu yaşadığımızda, bir kişinin başka bir kişinin parolasını çaldığını tespit ettik. Farklı bir platform üzerinde en son sorunu ise daha hemen hemen bir saat önce yaşadım. Şimdi bana hangisini tercih edeceğimi sorun!»

CIO - Büyük Distributor

Bütünleşik Z güvenliğinin doğası, ek koruma çözümleri ile oluşturulandan önemli oranda farklı. Güvenliğinin sağlanması gereken arayüzlerin daha geniş bir gruba sahip olması nedeniyle organizasyon verileri ve süreci koruması, aygıt düzeyinde tanımlandığında en savunmasız durumdadır. Daha etkili bir strateji, politika kontrolünü ve tanımını daha merkezi bir noktaya çeker. Yüksek oranda entegre ve bütünleşik Z güvenlik yığını bu alanda önemli bir avantaj sağlar.

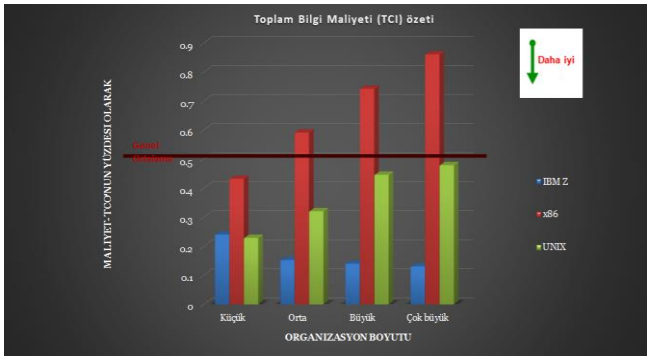
Karşılaştırmalı güvenlik etkililiğinin incelenmesine yönelik başka bir karmaşıklık faktörü, mobil hesaplamanın yükselişidir. Genel ağ bağlantıları ve kablosuz bağlantı noktaları giderek artarken, güvenlik riskindeki önemli bir artış bu bilinemeyen erişim noktalarının politkalarından, yönetişiminden ve etkililiğinden kaynaklanmaktadır. Güvenlik çözümünün merkezi olarak yönetilmek yerine dağıtılması tasarlandığı takdirde, uygulama ve veri artışına ilişkin risk profili önemli oranda yükselir. Bu tür giderek daha sık karşılaşılan topolojide Z çözümü mimari avantajlara sahiptir. Bu esnek uygulamalar için SIL risk profillemesi, Z platformu risk oranını alternatif çözümlerin herhangi birinin 1/20'sinden daha azına ayarlar.

MASRAFLAR VE GİDER

Güvenlik ile ilgili maliyetler hem TCO'nun geleneksel ölçütünü hem de bir organizasyon dahilindeki maliyet etmenlerinin genişletilmiş bir görünümünü sunan toplam bilişim maliyetinin (TCI) yeni ölçütünü içermektedir.

TCO sürekli bir operasyonun sürdürülmesi için gerekli masraflardan oluşmaktadır. Bu ölçütteki kategoriler bilişim teknolojileri operasyonel personelini; bozulma ve onarım uygulama desteğini; operasyonel personeli desteklemek veya sorunları çözmek için dış destek; elektrik ve soğutma masrafları; donanım ve yazılım bakımı ve lisanslandırma ve kat alanını içermektedir.

TCI organizasyonel bilim ve fikri mülkiyet (IP) varlıklarının ayakta tutulması ve korunması bakımından organizasyonel masrafların çerçevesini çizen bir ölçüttür. Bunlar verileri, iş sürecini, araştırma, uygulama yapısı ve diğer fikri mülkiyetleri içermektedir. Bu ölçüte dahil edilen masraflar varlıkları, personeli, elektriği, soğutmayı, güvenlik önlemlerini vb. tutan ve uygulayan, varlıkları güvenli ve çalışır durumda tutan altyapıyı içermektedir. Bu ölçüt, fikri mülkiyet (IP) kayıp ve zararının olumsuz etkilerini ve örneğin hizmetin sunulamaması ve hizmet dışı süreler gibi kaybolan fırsatları dikkate almaktadır. Bir organizasyon dahilindeki bilişim



güvenliğinin etkisini ve tesirini en iyi yansıtan ölçüt TCI'dır çünkü yansıtıcı güvenlik ölçütünün anlaşılmasını sağlamaktadır.

Farklı mimariler için TCI incelendiğinde ilgili konuları özetlemenin çeşitli yolları bulunmaktadır. Altyapı uygulamalarının boyutlarında geniş bir çeşitlilik bulunduğu için, toplam IT ve IP varlık değerine dayanarak özetleme istatistiksel olarak belirsizdir. Normalleştirilmiş bir karşılaştırma tabanı TCI'yı, TCO'nun bir yüzdesi olarak ifade eder. Bu analizin sonuçları şemada görülebilir.

IBM Z uygulamaları, çok çeşitli boyutlardaki kuruluşlar çapında *%84,83'e* varan oranda daha düşük TCI göstermektedir. Bu ölçütün yeni uygulama masrafları için önemli bir etmen olması nedeniyle düşük katsayı, Z ugulamalarının sunduğu verimli ölçeklendirmeyi desteklemektedir. TCI karşılaştırması bulunabilirlik maliyetini, saldırı etkisini ve hizmet dışı kalma süresi ölçütlerini içermektedir; bu yüzden, başka hiçbir ek görüşün dikkate alınması gerekmemektedir. Çözümler arasındaki fark büyük oranda şu alanlardaki üç katkıya dayanmaktadır:

- Personel maliyetleri
- Saldırı etkilerine bağlı maliyetler
- Altyapı mimarisi eklentileri

Personel kullanımı ve altyapı maliyetlerinin ikisi de denetlenebilirken, saldırı etkilerinin maliyeti ise hem nesnel hem de öngörülen öznel miktarların bir birleşimidir. Her durumda maliyetler doğruca müşteri raporlarından kaynaklanmaktadır ve değiştirilmemiştir; ancak onun yerine, bir araya getirilerek çalışma tabanı genelinde ortalaması alınmıştır.

IBM Z güvenlik yapılandırmalarıyla ilişkili maliyetler hem geleneksel maliyet tabanında hem de saldırılara bağlı olarak yansıyan maliyetler bakımından x86 ve UNIX güvenlik seçeneklerine göre daha düşüktür. Bu durum, yüksek entegrasyona sahip bir güvenlik paketi karşısında daha fazla risk ve açık oluşturan başka mimariler ile ekleme arasındaki farkı temsil etmektedir.

GÜVENLİK RİSKİ FAKTÖR'LERİ

Güvenlik riski, belirli bir tehdidin bir süreç veya bir varlık ya da varlık grubundaki açıkları başarılı bir şekilde istismar etme, işletmeye veya kendisine hizmet ettiği müşterilere zarar verme potansiyeli olarak tanımlanabilir. Bu tür bir olayın meydana gelme olasılığı ile ilgili sonuçlarının bir birleşimi olarak ölçülür. SIL, bir kuruluşun genel riskinin konsolide bir görünümünü sunmak için kullanılan gerçek yapılar halinde risk profilleri oluşturur. Bu yapı uygulamalardan, arayüzlerden, yönetim yapılarından, sosyal mühendislik yönlerinden vb. bireysel riski barındırır. Bir güvenlik uygulamasındaki riskin profillendirilmesi amaçları için risk profilinin ana boyutları şunlardır:

- Saldırı eyleminin deneysel havuzu
- Saldırı maliyetleri
- Riske maruz kalma

Bilişim dünyasının değişen yapısı, yönetimin bakış açısından seçeneklere netlik kazandırılması için bir değişikliğin yapılmasını zorunlu kılmıştır. Müşterilerin belirttiği saldırı etkilerinden bazıları şunlardır:

- Hizmet kaybı
- Güven eksikliği nedeniyle müşterilerin kaybedilmesi
- Stratejik olmayan mimari değişiklikleri
- Eksik veya hasarlı verilerin kurtarılması

- Özel fikri sermayenin kaybedilmesi

Bu etmenler olasılık ve maliyet yönlerine sahiptir ve kuruluşun güvenlik uygulamasıyla doğrudan ilişkilidir.

> *«Pek çok farklı saldırı müşterinin kaybedilmesi, düzeltme maliyetleri ve diğer korkunç etkiler nedeniyle darbe almamıza yol açtı. Bütün bu deneyimler müşteri güveninde büyük bir kayba neden oldu. Hızla, iş yükünün bir kısmını büyük bir mainframe üzerinde çalıştıran bir Yönetimli Hizmet Sağlayıcısına (MSP) geçiyoruz çünkü bugünlerde tek güvenli yer bu gibi görünüyor.»*

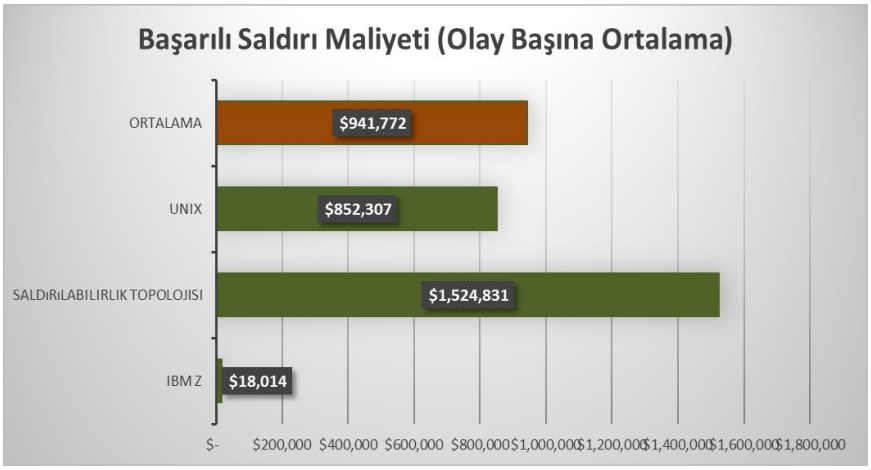
Direktör- Orta Ölçekli Dağıtım Şirketi

SALDIRI MALİYETLERİ

Saldırılar, bir işletmenin alanına başarılı birer baskın olarak tanımlanabilirler. Bu baskın hırsızlık, imha veya engelleme biçiminde olabilir. Mevcut korumaların, tüm platform düzeyinde güvenlik için gerekenden çok daha fazla farklı erişim noktasını kapsaması gerekmektedir. Bu durumda, işlemenin tüm yönleri üzerinde bir kontrole sahip olunmalıdır. Pek çok devlet ve güvenli kurulum, ana bilişim kürelerinin tahsisi ve ele alınmasına yönelik korumaya ihtiyaç duymaktadır: I/O, ağ erişimi, bellek yönetimi ve genel normal uygulama erişimi.

Bazı güvenlik saldırısı durumlarında bir kuruluşun maliyetlerinin değerlendirilmesi uzun sürebilir. Bu tür ertelemeli etkilere bir örnek, tescilli araştırmalar çalındığında görülebilmektedir. Özel fikri mülkiyetin kaybedilmesi pazarda önemli bir etkiye yol açabilir.

Bir saldırı ile ilişkili maliyetlerin ortalaması, farklı teknolojiler için göreli bir riski belirtmektedir. Ne yazık ki, çok sayıdaki küçük saldırıya yayılan ortalama maliyetler nedeniyle piyasada bir 'kabul edilebilir zarar' iklimi oluşmaktadır. Bu durum, güvenlik tanımlarında ve kontrolünde daha büyük ve daha ciddi gevşeklik için bir emsal teşkil etmiştir. Bir işletme, tekrarlı bir şekilde 'yönetilebilir' zararlara müsamaha göstermeye koşullandırıldığında bilgilerini ve operasyonlarını riske maruz bir durumda ve önemli bir hasara açık halde bırakmaktadır.



Bir saldırının yol açabileceği ortalama maliyet artar ve bu artışın hızı da artar. Bunun bir kısmı bulut uygulamalarının kapsamının genişletilmesinden kaynaklanmaktadır; burada daha çok insan ve veri her bir dönemdeki saldırılardan etkilenebilmektedir. Dikkate alınması gereken başka bir etmen ise saldırılardan sorumlu olanların

saldırılarında giderek ustalaşması ve daha saldırganlaşmalarıdır. Bu durum, bilişim bileşenleri seçilirken dikkate alınması gereken tehdit seviyesinde bir artışı göstermektedir.

Bir saldırının yol açabileceği ortalama maliyet pek çok farklı özellikten etkilenir. Algılama hızı ve etkililiği, saldırının daha çok hasara yol açma becerisinin izole edilebilmesi, iyileştirmenin kapsamlılığı vb. genel mali etkiyi etkilemektedir.

Z platformu için saldırı başına temel olarak daha düşük maliyet bütün bu etmenlerin sinerjisini göstermektedir. Genelde, Z güvenlik uygulamalarındaki iyileştirme, *%98,82* ortalama ile alternatif platformlara göre daha azdır. Biraz farklı bir bakış açısından bakıldığında işletmeler, uygulama platformlarının IBM Z olmaması halinde saldırı hasarının giderilmesine ortalama *84,65 kat* daha fazla para harcayacaktır.

Farklı güvenlik seviyelerini elde etmenin maliyeti önemlidir. Bu etmenleri anlamak için farklı güvenlik biçimleri kontrol seviyelerine bölünebilirler:

- Normal kurumsal
- Kredi kartı işleme dahil
- Bankacılık
- Sağlık
- Araştırma
- Savunma

Kritik işlevlere ve kontrollere dayanarak eşit şekilde ağırlıklandırıldığında farklı platformlar, aşağıdaki tabloda özetlenen güvenlik kapsamını sağlamaktadır. Herhangi bir güvenlik kurulumuna eklenti seçenekler uygulanabileceği için bu yapılandırma, sadece başta uygulanan kurulum ile birlikte temin edilen güvenlik özelliklerini ineceler.

Platformun Aslen Kapsadığı Güvenlik

Güvenlik Seviyesi Açıklaması	IBM Z	x86	UNIX
Normal kurumlar	%100,00	%18,16	%30,26
Kredi kartı işlemleri	%99,00	%11,04	%18,28
Bankacılık	%94,00	%5,26	%10,22
Sağlık	%100,00	%3,24	%8,51
Araştırma	%92,50	%2,86	%4,16
Güvenlik	%85,54	%0,26	%1,86

SIL'nin rastgele kullanıcılardan oluşan bir grup üzerinde, birbirinden farklı güvenlik açığı analizlerinden oluşan çalışmalar gerçekleştirmiştir. Bu ana çalışma kapsamındaki kullanıcılardan 14.625 kadarı, SIL güvenlik açığı analizleri sürecinde ayrıntılı olarak incelenmiştir. Kullanıcıların büyük çoğunluğu, sistemlerine yönelik saldırıların farkında değillerdi. Bulgular, kurumların bir kısmının güvenlik ihlallerinin farkında olduğunu gösteriyordu. Ancak en şaşırtıcı bulgu, güvenlik ihlalleri yaşadıkları halde, bunun farkında olmayan kurumlarin sayısının çokluğu olmuştur. Rastgele bir grup üzerinde gerçekleştirilen bu güvenlik açığı incelemelerinde; 8.2061 kurumun, işlemleri gerçek zamanlı olarak etkileyen ve bilgi çalan korsan etkenler tarafından etkilendiği belirlenmiştir.

Tespit edilen saldırıların, ön verilerin gösterdiğinden çok daha fazla olduğu gözlemlenmiştir. Özellikle fikri mülkiyet hırsızlığı durumunun olması halinde,

saldırıların sonuçlarının büyük bir çoğunluğunun, uzun süre fark edilemeyebileceği gerçeği mevcuttur.

Saldırıların süreleri, saldırıları gerçekleştirenlerin deneyimleri ile birlikte artış göstermektedir. Farkında olunmayan saldırıların üzerinde gerçekleştirilen incelemelerde, bu saldırıların ne süredir etkin oldukları incelenmiştir. Bu virüs saldırılarının %31,19'dan fazlasının iki yıldan daha uzun bir süredir etkin olduğu, %43,28'inin bir ila iki yıl arasında bir süredir etkin olduğu, %23,16 kadarının üç ay ile 12 ay arasında bir süredir etkin olduğu tespit edilmiştir. Saldırıların kalan kısmının kısa süreli saldırılardan, başlangıç tarihi tespit edilemeyen ve ayrıntılı iz bulma yöntemlerinden daha eski saldırılardan oluştuğu görülmektedir. Listede olmamalarından, Z dağıtımı sistemlerinin yoklukları ile fark edildiler.

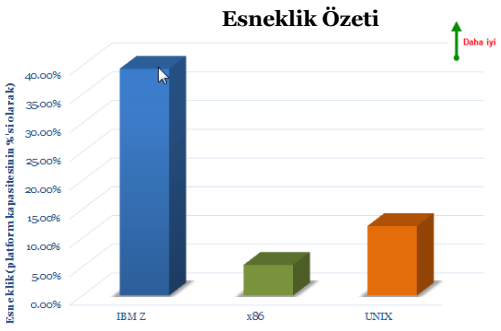
> *«Birleşme ve Satın Alma çalışmalarımızın sonucunda, dört ay önce bir şirket satın aldık. Buradaki temel amaçlarımızdan biri, bazı fikri mülkiyetlerine sahip olmaktı. Sistemleri üzerinde düzenlemelere başlamamızın ardından kısa bir süre sonra, casus programların sistemlerinde mevcut olduğunu fark ettik. Bu fikri mülkiyetin değerinin ciddi tehlike altında olması nedeniyle hukuk danışmanlarımız, gerçekleştirilen bu satın alma işlemini feshetmek için uğraşmakta. Ne berbat bir durum!»*

CIO (Bilgi Teknolojilerinden Sorumlu Yönetici) - Çok Büyük Biyolojik Yapı

Bu şekilde gerçekleşmiş olan uzun süreçli güvenlik açıkları ve gizli saldırılar, bir kurum için en tehlikeli risklerdendir. Uzun süreçli güvenlik açıklarının fark edilmesinin ardından, bir kurumun, bu durumdan nasıl etkileneceğini kestirmek zordur. Bu durum, kurumun müşteri güvenini önemli ölçüde kaybetmesine neden olabileceği gibi, uzun süreçli hukuki dava süreçleri ve müzmin iyileştirme süreçleri ile karşı karşıya gelmesine neden olur.

ESNEKLİK VE BECERİ

Başarılı bir güvenlik uygulamasının en önemli etkenleri; istenilmeyen, farklı düzlem ve şekillerdeki saldırılar ile başa çıkabilecek güvenlik önlemlerinin esnekliği ve gelen saldırılara karşılık verebilme hızıdır. Bir dağıtımın esnekliği, beklenilmeyen kaynak kullanımı sorunları ile genel platform bozulması yaşamadan başa çıkabilme olarak görülebilir. Kaynak kullanımı isteğinin yoğun olarak reddedilmesi sonucu ile dağıtımın çökmesi, sıra dışı olmalarına rağmen görülebilen durumlardır. Dayanıklı dağıtımlar, işletim sisteminin ve donanımın, esnekliği ve kapasitesine bağlıdır. Dağıtımlarda esneklik, satın alım ve değerlendirme hususlarında donanım ve işletim sistemleri için kullanılan yaygın bir ölçektir. Tabloda, farklı platform gruplarına ait esneklik puanları gösterilmektedir. Bu çalışma dahilinde esneklik puanı, dağıtım üretiminden başlayan kaydedilmiş ve bildirilmiş olan kesme noktaları sonucu belirlenmiştir. Puan; sıralanan işlem yönetimi ve algoritma hesaplama gücü, ara bellek sisteminde ve sistem bileşenlerinde biriken yükün genel çalışmayı kötü olarak etkilemeden kaldırabileceği iş yükünün yüzdesi olarak ifade edilmiştir.

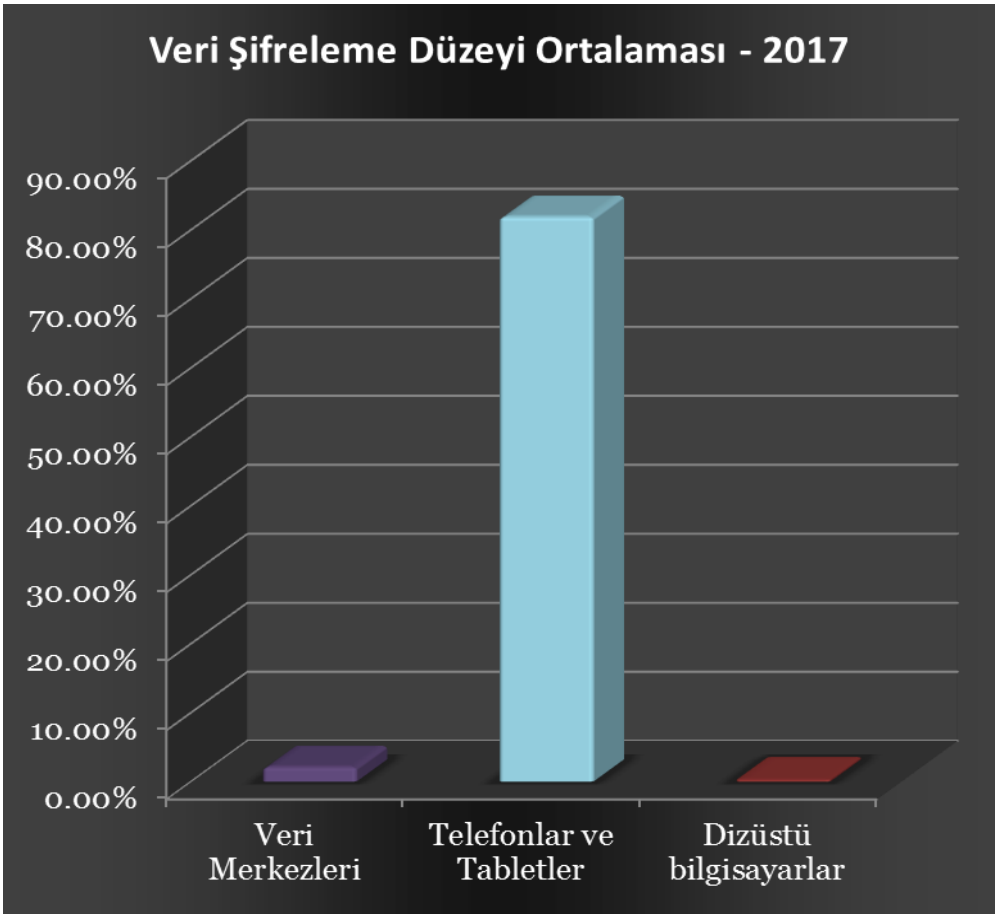


Z dağıtımı ve diğer çözümlerin esnekliği arasında azımsanmayacak miktarda fark vardır. IBM Z dağıtımlarının diğer seçenekler ile kıyaslandığında ortalama esnekliğinin, *7,41 kat*'a kadar olduğu gözlemlenmektedir. Bu, IT çözümleri açısından daha az mühendislik demektir ve bu da raporun önceki kısımlarında bildirilen Toplam Mülkiyet Maliyeti ve Toplam Yatırım Maliyeti edinilmesine katkıda bulunur.

Kapsamlı Şifreleme

Bir kurumun müşteri ve şirket verileri, temel kaynaklarıdır. İşletmenin fikri sermayesi ve piyasa getirilerinin temelini oluşturması nedeni ile paha biçilemez. Şifreleme, bu varlıkları koruma altına alarak, bilgisayar korsanlarının saldırılarına karşı savunmasız kalınması engellenir. Şu anda bu varlıkların bir kısmı korunmamakta.

Yaklaşım, veri iletiminin diğer alanlarında farklılık gösterir. Mobil cihazların kullanımı, temel tasarımlarından sonra dağıtılan şifrelemeleri alabilen, korsan karşıtı bir yaklaşım ile derlenmiştir. Farklı şifreleme düzlemlerini karşılaştırmak, aydınlatıcı olacaktır.



Bu özet, temel BT ve mobil veri iletimi yaklaşımları arasındaki temel farklılıkları gözler önüne serer. Veri merkezlerindeki kurumsal verilerin sadece %2,13 kadarı şifreliyken, mobil cihazlarda kullanılan platformlarda, bu oran yaklaşık olarak %82'dir. İletişim endüstrisi, şifrelemenin önemini erken fark etmiştir. Veri merkezlerindeki ve dizüstü bilgisayarlardaki değerli kurumsal verilerin şifreleme eksiklikleri çok ciddi seviyelerdedir.

SIL GSW verilerine göre, son üç yılda gerçekleşen 11,2 milyar güvenlik aşımı kaydının %3,5'dan az bir kısmı, şifrelenmiş verilerden oluşur. Bu durum, güvenliği aşılan bir sistemde bulunan verilerin, saldıranların inisiyatifinde olduğu anlamına

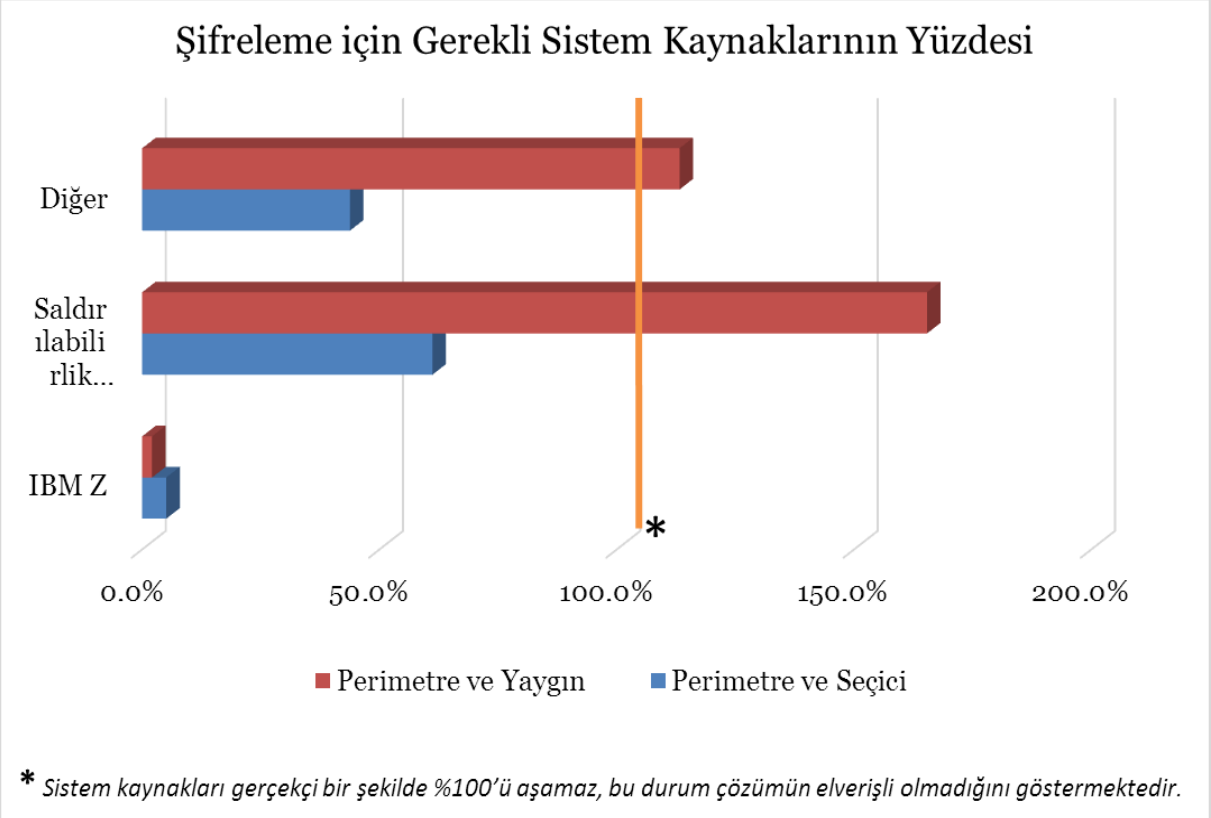
gelmektedir. Böyle bir öngörü eksikliği nedeni ile önemli ölçüde gizlilik ihlali sonucu müşteriler ve partnerlerde güven kaybı oluşması normaldir.

Düşük seviye şifrelemenin birden fazla temel nedeni vardır. Süre şartları ve sistem kapasitesi, kurumları, kaynak kullanımı nedeniyle bölümsel savunma teknikleri ve seçici şifreleme yöntemlerine itmiştir. Genel platform kapasitesinin %61,2'sini harcayan ve artış gösteren bölümsel savunma yerine, farklı bir yaklaşım benimseme ihtiyacı doğmuştur.

Günümüzün bilişim ortamlarında kullanılan temel yapılarda gerçekleşen yeni bir gelişim, piyasada ciddi bir değişim başlatmak üzere. Bu değişim, IBM Z şifrelemesinin seçici bir modelden, kapsamlı bir şifreleme modeline geçişidir. Bilişimin temel yapısında böyle önemli bir değişime gidilmesi ve bu değişimin güvenlik açısından etkisi, piyasada büyük bir değişken etki yaratacaktır.

Konseptin temeli, neyin şifrelenip neyin şifrelenmeyeceğini belirleyen bir katman oluşturmak yerine; şifrelemeyi, işleme sürecinin normal bir kısmı haline getirmek üzerine kuruludur. Seçici şifrelemede kullanılan karar verme katmanlarının kaldırılması sayesinde, genel kaynak kullanımında azalma ve mevcut piyasaya göre şifreleme kullanımının güçlüklerinin azaltılması etkisi yaratacaktır.

Kapsamlı şifrelemenin önündeki en büyük engel şifreleme kaynak kullanımının maliyeti ve şifrelemenin, platformlar üzerindeki yükünün fazlalığı olmuştur. Ancak bu araştırma dahilinde bilgilendirmede bulunan kurumlar için, mevcut olan seçici şifrelemede sistem işlem yükünün, %61'e varan oranda güvenlik işlemlerinden oluştuğu görülmektedir. Bu da altyapı kaynak kullanımının, performans düşüşlerinin ve benzeri olguların büyük oranda kaynağıdır.



* *Sistem kaynakları gerçekçi bir şekilde %100'ü aşamaz, bu durum çözümün elverişli olmadığını göstermektedir.*

Mevcut şifreleme kaynak kullanımını gösteren tablo, yukarıda gösterilmektedir. Kapsamlı şifrelemeye geçiş, mimari açıdan temel farklılıkları açığa çıkarır. Z mimarisinde, kapsamlı şifreleme sayesinde kaynak kullanımı azalırken, diğer mimarilerde kaynak kullanımının yükseldiği gözlemlenmektedir. Z mimarisine sahip

olmayan platformlarda kapsamlı şifrelemenin kullanılabilmesi için devasa bir topoloji dağıtımı gerçekleştirilmesi gerekir. Çalışma grubu dahilindeki platformların ortalama yükü hesaplandığında, mevcut sunucu sayısının ***12,2 kat*** kadar artırılması gerekmektedir.

Platform sayısında böyle bir değişiklik, işletme maliyetlerini önemli ölçüde artırır. Bu şekilde çözüme gitmeye çalışan bir kurumun; donanım, yazılım ve personel giderleri önemli ölçüde yükselecektir. Z mimarisi kullanmadan kapsamlı şifreleme bu şekilde gerçekleştirilebilir, ancak bu, ekleme ve paketler ile genişletilmiş mimarinin zaaflarını da beraberinde getirecektir.

Güncel gelişmeler gözardı edilse bile Z mimarisi, daha etkili ve daha az kaynak kullanan şifreleme sunmaktadır. ***8,5 kat***tan fazla güvenliği, ***%93'ten daha az bir genel maliyet*** ile ***%81 daha az kaynak kullanımı*** ile sunmaktadır. Bu rakamlar; sistem, güvenliği düşük olan seçici şifreleme kullandığında geçerli olan rakamlardır.

Daha hızlı bir şifreleme motoru ile kapsamlı şifrelemenin kullanılması ile diğer sistemlere göre ***18,1 kat daha hızlı*** çalışan bir sistemi ***1/20 maliyete*** sunar.

Günümüzde Z merkezi işlemcili sistemlerde kapsamlı şifreleme uygulanabilir bir seçenek iken, diğer mimarilerde elverişli değildir. Kapsamlı şifrelemenin bir sunucuda kullanılması için gerekli olan iş yükün, kısıtlayıcı olan x86 sistemlerdeki mimari ile 7,32 *kat* daha fazla işlemci gücü gerektirmektedir. Mevcut olan farklı platformların yonga tasarımında, işletim sistemi temelinde ve platform kaynak kısıtlamalarında böyle bir çözüm kullanmak için çığır açacak gelişimler gerekir. Bu tür gelişimler yonga tasarımında ve üretiminde, teknolojinin temeli mümkün var sayıldığında genel olarak iki ya da üç yıl süre içinde tasarlanan uzun dönemli değişimlerdir.

Bu gerçekleştirilmediği sürece, kapsamlı şifreleme, ilgili platformlarda mümkün olmayacaktır. İlgili platformlarda kurulmuş olan sistemler; yüksek riskli ve güvenlik açıkları ile çalışmaya, yüksek kurum kaynağı kullanmaya ve personelin çalışma vaktini yemeye devam edecektir.

Kapsamlı şifreleme katmanı sayesinde, güvenlik nedeni ile çalıştırılan işlemlerin yüzdelerinde büyük bir düşüş elde edilir. Son SIL çalışmalarında incelenen kurumlar, IBM Z sisteminde çalışan kapsamlı şifreleme geçerek ortalama işlemci kaynak kullanımında %91,7'ye varan azalma elde edebilirler.

Bilişim suçlarına maruziyetin yüksekliği nedeniyle, maliyet değişkeni temel hesaplamalarında bilgisayar korsanlarının gerçekleştirdiği saldırıların, kurumsal varlıklara oluşturabileceği hasar, hesaplamalara dahil edilir.

Güvenlik açısından, iş yükü ve karşılık verme hızı çok önemlidir. Bir kurumun tehditlere karşılık verme hızı ne kadar yüksekse, ilgili saldırıdan hasar alma riski o kadar düşüktür. Karşılık verme hızı, temel bir ölçek olarak sadece istenmeyen etkileri önlemekle kalmaz, bu işlemi gerçekleştirirken oluşan etkiyi en aza indirir. Yapılan çalışma dahilinde seçici ve kapsamlı şifreleme arasında gerçekleştirilen karşılaştırmada, gelen saldırıların %87,2 kadarının kapsamlı şifreleme sayesinde, bir karşılık verilmeden önlenebildiği gözlemlenmiştir.

Karşılık gerektiren saldırılarda ise kapsamlı şifrelemenin çok daha hızlı olduğu not edilmiştir. Güvenlik mimarisinin karmaşıklığının daha az olduğu kapsamlı şifrelemede, seçici şifreleme ile kıyaslandığında, aynı sorunun çözülmesi için daha az komut girilmesi gerektiği gözlemlenmiştir. Testlerde; kapsamlı şifrelemenin karşılık vermek için ihtiyaç duyduğu sürenin, seçici şifrelemenin karşılık vermek için ihtiyaç duyduğu sürenin sadece %14,2 kadarı olduğu

ve saldırıya açık olan topolojisinin daha az olduğu gözlemlenmiştir. Saldırıya açık olan katmanların daha az olması, tehditlerin daha az karmaşık olan ve daha fazla derinlemesine bir karşılık ile engellenmesi sağlanır. Karmaşıklığın daha az olması sayesinde, daha az korsan tehdidi ile karşılaşılır. Orta ölçekli müşterilerden oluşan test gruplarında gerçekleştirilen ölçümlerde, kapsamlı şifreleme öncesi ortalama 2.423 olan saldırıya açık katman, kapsamlı şifrelemeye geçilmesi ile 196'ya düşürülmüştür. Bu, karşılaşılan tehdit oranında yaklaşık olarak ***%92 düşüş demektir.***

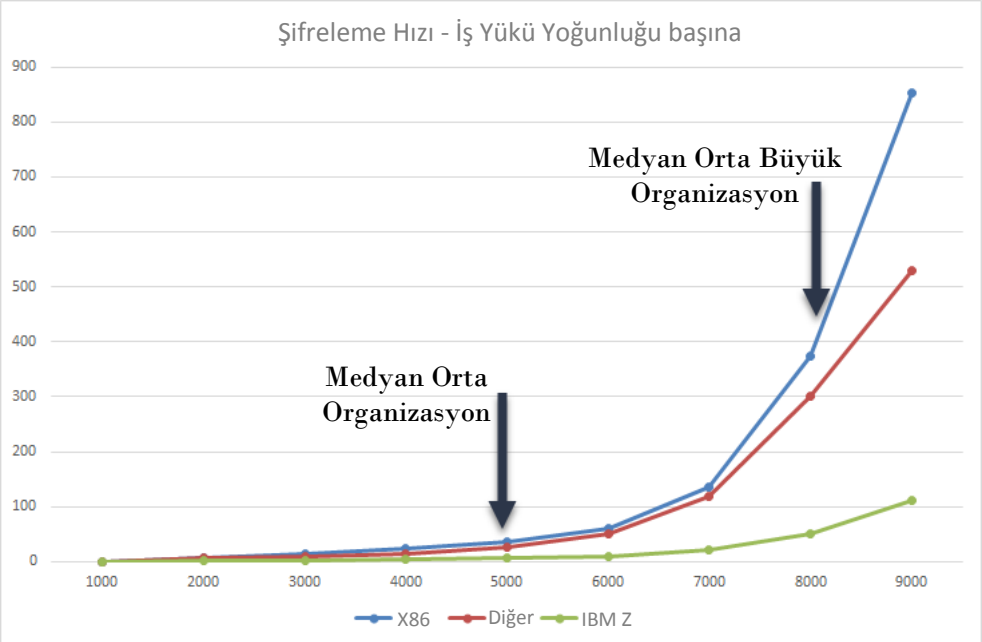
SLI, kapsamlı modelde harmanlanmış bir ölçüm ve emülasyon mekanizması kullanımıyla, saldırı ve maruziyet riski hakkında gerçekleştirdiği incelemede, bu yeni teknolojiyi test etmiştir. Veriler; aynı sayıda korunması gereken veri sunulduğunda, kapsamlı ve seçici şifreleme modelleri arasında, Z dağıtımlarında x86 sistemlere göre daha az manüel işlem gerekmesi ve işlemlerin çok daha hızlı gerçekleştiriyor olmasının yanı sıra, pek çok faktörün katkısıyla, maliyette %81,63'e varan azalma olduğunu göstermektedir.

Günümüzde pek çok kurumda gözlemlenen platform çeşitliliğinin çokluğu sorununun ortadan kalkması sayesinde, sadece platform maliyetlerinde değil, ekipmanı kullanacak olan, güvenlik testlerinden sorumlu ve tüm güvenlik kaynaklarını yöneten personel harcamalarında da azalma sağlayacaktır. Personel ihtiyacının azaltılması, ekipman ihtiyacının azalmasından daha önemlidir. Günümüzde IBM Z platformlarını kullanan kurumlarda, %80 daha az güvenlikten sorumlu personel gereklidir. Kapsamlı şifrelemeye geçilmesi ile bu rakamın artmamasını sağlayabilirsiniz; üstelik diğer platformları kullananların, güvenlikten sorumlu personel ihtiyacı, her yıl artarak yükselmeye devam edecektir.

Böyle bir ortamda, kapsamlı şifreleme maliyetinin getirisinin makul olduğu tartışılamaz bir gerçektir. Piyasanın yaklaşımının değişmesi yönünde bir talep oluşması durumunda, ekleme ve paketler ile genişletilmiş mimariye yatırım yapan firmaların, kapsamlı şifrelemeyi kullanmak için kökten yenilikler ile gerekli mimari değişikliklere yatırım yapmaları gerekecektir. Bu değişiklikler için gerekli olan yatırımlar, bazı mimariler için oldukça zorlayıcı bir süreç olacaktır.

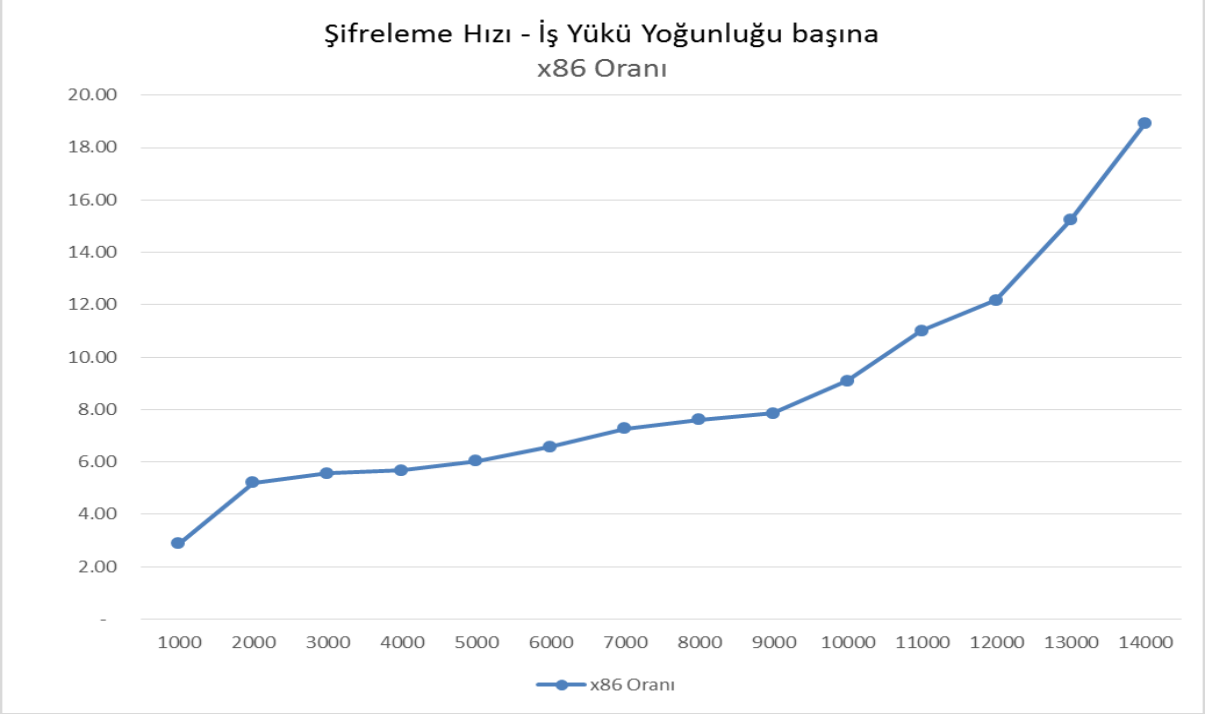
IBM merkezi işlemcili sistemli mimarilerde münferit işlemlerin hızı x86 sistemlerin hızına göre 2,87 ila 3,24 kat arası daha yüksektir, tabii kapsamlı topoloji göz önünde bulundurulduğunda bu çarpan sayısı önemli ölçüde artış gösterir. Bunun nedeni, kapsamlı modelin işlem yığınlarını münferit şifreleme olarak değil, komple bir birim olarak değerlendirmesini sağlayan işlem akışı mekanizmasıdır. Bu işlem akışı mekanizması sayesinde, sistem kapasitesinin güvenlik için ayırdığı işlem gücü önemli ölçüde düşmektedir ve bu da işlem hızını artırmakta ve ortalama işlem yükünü azaltmaktadır.

Bu modelin şifreleme verimliliği, şifreleme motorlarının hızını artıran katmanların artmasıyla alternatif platformlara göre 18,4 *kat* daha hızlı şifreleme sunmaktadır. Verimliliğin maliyet üzerindeki etkisi göz ardı edilemez. Kapsamlı şifrelemenin çalıştırma maliyeti diğer seçeneklerin çalıştırma maliyetinin %5,1 ila 8,0'ı arasındadır.



Güvenlik ihtiyacının artması ve diğer platformların bu ihtiyacı karşılamada çektikleri zorluk göz önünde bulundurulduğunda, edinilen kazancın miktarı daha da açık görülüyor. Diğer platformlarda gözlemlenen performans düşüşü nedeniyle sundukları hız, IBM Z platformunun sunduğu hızlar ile kıyaslanamayacak ölçüdedir. Bu düzeydeki performans düşüşleri, servis seviyesi anlaşmalarının (SLA) ve performans beklentilerinin karşılanamaması anlamına gelir. Aşağıdaki grafikten görülebileceği üzere, güvenlik ihtiyacı arttıkça, platform motoru üzerindeki iş yükü de artmaktadır. Mevcut işlem kaynaklarının daha büyük bir kısmının, görev dağıtımı ve diğer sistem etkinliklerine gittiğini görebilirsiniz. Kapsamlı şifreleme ihtiyacı belli bir seviyenin üstüne çıktığında, tüm sistem yanıt veremez hale gelir.

Mimari karşılık verme yetenekleri arasındaki farklılıkları, aşağıdaki özet tablodan görebilirsiniz.



x86 sistemlerdeki keskin performans düşüşü, mevcut mimarinin limitlerini göstermektedir. Daha fazla çekirdek ya da sanal işlemci eklenmesi, paralelleştirme açısından kısıtlı bir yük azalması sağlayabilir. Ancak bu, eklenen her bir sanal işlemci için fazladan iş yükünü artıracağı için sağladığı yük azalmasının etkilerini kaybeder.

SIL, bu karmaşık sorunu incelemek amacıyla, 117.000 kurumun son 14 aylık süre içindeki etkinliğini inceleme yoluna gitmiştir. Her bir çalışma kısmı için, bir ortam emüle edilmiş ve müşteriler tarafından sağlanan bilgiler ile günlük olarak incelenmiştir.

Bu model kapsamında, önce gerçek iş yükü oluşumu sonucu elde edilen sonuçlar ile kıyaslayan bir zorlama testi ile denetlenmiştir. Sonuçların doğruluğu onaylandıktan sonra, iş yükü ve eylemler, önce seçici şifreleme ile simüle edilmiş merkezi işlemciye transfer edilmiş ve sonra kapsamlı şifreleme ile simüle edilmiş merkezi işlemciye transfer edilmiştir.

Üç durum arasında eylem yükü, her bir eylem yükü için ayrı ayrı karşılaştırılmıştır. Kapsamlı şifreleme kullanan bir IBM Z platformu kullanılmış olsaydı, müşteriler tarafından sağlanan veriler dahilinde fark edilen ve bildirilen 1,16 milyar saldırının hiçbiri yaşanmamış olacaktı.

Seçici şifreleme modeli de saldırıların %92,1'ini engelleyerek önemli derecede koruma sağlamıştır. Ancak seçici şifreleme, hem daha yavaş hem de daha fazla sistem kapasitesi kullanmıştır. Şifreleme verimliliğinin kapsamlı modelde çok daha yüksek olduğu gözlemlenmiştir.

Verimli bir şifreleme, bir kurumun net karına doğrudan katkıda bulunur. Bahsedilen müşterilerden 14 ay süre ile gelen saldırı raporları uyarınca, toplam maliyet 1,3 milyar ABD Dolarının üstündedir. Sistem süresi, personel, iyileştirme masrafları ve piyasadaki pazar kaybını giderme masrafları, maliyete dahil edilmiştir. Kapsamlı

şifreleme kullanılmış olsaydı, 14 ayı geçen süre içinde gerçekleşen 1,16 milyar saldırın hiçbiri ve 1,3 milyar ABD Doları olan maliyetin tamamı yaşanmamış olurdu.

Kapsamlı şifre kullanımı, bir kurumun güvenlik risk profilini ve uygulama risk profilini önemli ölçüde düşürür. Sigorta şirketlerinin çoğunluğunun, işletme ve uygulama tabanlı risk profilleri bazlı finansal birikim ön koşullu olarak çalışmaları nedeniyle, riskleri azaltan her şey bir kurumun finansal dar boğaza girme ihtimalini azaltır. Sigorta şirketlerinin çoğu ön koşul olarak, şirketlerin BT bütçelerinin bir kısmını finansal birikim olarak ayırmalarını istemekteler. Bu ön koşul yedi - sekiz yıl önce başladı ve günümüzde bu istek daha da artıyor. Günümüzde IBM merkezi işlemcili mimariler; diğer mimariler veya x86 sunucu tarlaları ile kıyaslandıklarında, %80'e varan risk faktörü azalması sunmaktadır. Bu yüzde, genel BT bütçesi üzerinden hesaplanmıştır. Çünkü bilişim ortamı, saldırılardan veya güvenliğin aşılmasından tüm bileşenleri ile etkilenir. 12 milyon ABD Doları BT bütçeli bir kurumdan ön koşul olarak istenilen finansal birikim, x86 sistemlerde 764.400 ABD Doları, IBM Z sistemde ise sadece 160.524 ABD Dolarıdır.

Çalışma odaklarından bir diğeri de, şifreleme anahtarlarının çalınması üzerine olan saldırılardı. Çalınan bilgiler, sektörde platform içi eylemleri güvence altına almak için kullanılan ortak ve özel bir çiftlenimin bir kısmını içeriyordu. Z mimaride kullanılan donanımsal şifreleme modeli sayesinde, bu maruziyet hiç yaşanmadı. Çiftleme arasında uyuşma işlemi gerekmemesi nedeniyle, 14 aylık çalışma süresince başarılı bir saldırı hiç gerçekleşmemiştir.

Çalışma süresince şifreleme anahtarlarının çalınması nedeniyle, 6.587.500 ABD Dolarından fazla zarar oluşmuştur. Bu da donanımsal şifrelemenin, kapsamlı şifrelemenin en önemli avantajlarından biri olduğunu göstermektedir.

MSP

Bu şifreleme türü, yönetimli hizmet sağlayıcı (MSP) hizmeti ya da bulut hizmetleri sunanlar için çok önemli bir etkiye sahiptir. Yapısı nedeniyle bulut mimarisinde, risk katmanları daha da fazladır. Ortak bellekler veya paylaşılan kaynaklar, makinenin sadece kendisine gelen saldırılardan değil, başkalarının etkilendiği saldırılardan da hasar alma riski oluşturur. «Paralel bilgisayar korsanlığı» (sideways hacking) olarak da bilinen bu saldırı türünün gerçekleşmesi durumunda, MSP hizmetini alan bir kuruma gerçekleştirilen saldırının başarılı olması, MSP hizmeti sağlayıcı ve dolayısıyla o sağlayıcının tüm müşterileri de korsanların içten saldırmalarına olanak sağlar. MSP'ler fiyat sözleşmeleri ile çalıştıkları için MSP ile ilişkilendirilebilecek herhangi bir saldırı, MSP'nin net kazancını etkileyecektir. Kapsamlı şifreleme ile bu sorunlara çözüm sağlanarak, risk profili önemli ölçüde düşürülür.

GÜNCEL OLAYLAR

Bu SIL çalışması süresinde, dünyamızda bilişim güvenliğini önemli ölçüde etkileyen bir kaç olay yaşandı ve kapsamlı şifreleme ile tamamen önlenebilirdi. Bir fidye yazılımını taklit eden bir silah haline getirilmiş bir virüs yayıldı. Bu virüsün asıl amacı yok etmekti. Bu bilinçli saldırının amacı, derinlemesine ve kapsamlı bir hasar oluşturmaktı.

Ülkeler, hastaneler, hava limanları ve işletmeler hedef alındı, bunlara saldırıldı ve bunlar tahrip edildi. Bu saldırının oluşturduğu mali hasar halen tablolanıyor ve büyük bir ihtimalle önümüzdeki bir kaç yıl daha tablolanmaya devam edecektir. Açık olan şudur ki, bu tür saldırılar tekrarlanabilir tiptedir ve tekrarlanacaktır. Donanımsal ve

kapsamlı şifrelemenin Z mimarisi ile birlikte bu saldırılar, Z güvenlik katmanları sayesinde çiftlemelerde uyuşma işlemi istemi gerçekleşmeyeceği için engellenmiş olacaktı ve korsan saldırılarına karşı açık verilmeyecekti.

Trilyonlarca dolar zarar önlenmiş, şirketler zarar etmemiş ve insanlar zarar görmemiş olacaktı. Bilişim güvenliği yaklaşımında köklü değişikliklere gidilmesi kaçınılmaz bir hale gelmiştir.

Ancak günümüzde kapsamlı şifrelemeyi destekleyen Z mimarisinden başka bir yonga mimarisi bulunmamaktadır. Bunun nedeni mevcut olan diğer mimarilerin bant genişliği ve fazla iş yükü hususlarındaki teknik kısıtlamalardır. Bu durumda olan mimarilerin gerekli hazırlıkları yaparak sistemlerini kapsamlı şifrelemeye uyumlu hale getirmesi oldukça güç olacaktır, ancak bu, piyasanın ihtiyaç duyduğu bir değişimdir.

NET ETKİLERİ

Şifrelemenin Toplam Mülkiyet Maliyeti, şirketlerin BT bütçelerini tekrardan gözden geçirmelerine neden olacaktır. BT bütçelerinin büyük bir kısmını, uygulama geliştirme oluşturmaktadır. Çalışma gurubundaki kurumlar arasında bu rakam, ortalama %41,5 ila 68,2 arasındadır ve bu rakamda oluşacak olan her değişiklik, doğrudan kurumun kazancını etkileyecektir.

Şifrelemenin bilişim ortamının temel güvenlik ögesi haline gelmesi, BT bütçe maliyetlerinde yaklaşık olarak %22,1 oranında azalma sağlayarak, net etki yaratacaktır.

SONUÇ

«Bu tür eylemler, gerçekleştirildiği kuruma göre bir siber saldırının, savaş nedeni olabileceği anlamına gelmektedir. Perşembe günü, NATO genel sekreteri Jens Stoltenberg, »Madde 5 uyarınca müşterek savunma esası» nın faaliyete geçirilmesine neden olabileceğini söyledi.

Luke Graham |@LukeWGraham, Cuma, 30 Haz 2017 | 9:50 UTC -5, Tech Transformers, CNBC Ayrıntılı Rapor

IBM Z platformunun mevcut dağıtımı Toplam Mülkiyet Maliyeti, performans ve risk azaltma hususlarında piyasadaki diğer platformlara göre büyük bir avantaj sunmaktadır. Mevcut dağıtımdaki seçici şifreleme ve platformun yaygın risk vektörlerine karşı olan direnci, şirketlerin bilişim güvenlikleri için önemli bir temel oluşturmaktadır.

Ancak kapsamlı şifrelemenin denkleme girmesiyle, sadece Z dağıtımlarında değil, bilişim sektöründe köklü güvenlik değişikliği gerçekleşmiştir. Bu paradigma değişikliği, piyasalarda rekabet etmek isteyen bütün firmalar için oldukça zor bir mücadele olacaktır.

Ticaretini siber alemde gerçekleştiren şirketler ve bulut modeli ile çalışan şirketler, iş siber güvenliğe geldiğinde büyük bir hassasiyet göstermektedirler. İnternet kullanımı arttıkça kurumların verilerinin ve diğer fikri mülkiyet sermayelerinin güvenliklerine verdikleri önemde hızlı bir artış gözlemlenmektedir. Bu durum, zorlukları da beraberinde getirmektedir. Kurumlar, piyasa avantajlarını ve mali durumlarını korumakta zorlanmaktalar. IBM Z, uzun bir yüksek güvenlikli dağıtım ve varlık koruma geçmişine sahiptir. Bu geçmişi sayesinde engin bir deneyime sahiptir ve diğer sanallaştırmalarda olmayan erişim ve işlem güvenliği denetleyicileri gibi özellikler ile donatılmıştır.

Gerçekleştirilen çalışmada elde edilen bulgulara bazı örnekler aşağıda verilmektedir.

Özet

Kategori	Açıklama	Quick Byte
Karşılık Verme Hızı	Z platformunda, standart eylemler, diğer platformlardakine göre işlemci öz kaynakları *%85,80* daha az kullanılır.	Z dağıtımları tehditlere daha hızlı karşılık verir.
Risk	SIL risk profillemelerine göre Z platformları alternatif çözümlerin *1/20*'inden daha düşük bir risk oranına sahiptir.	Z platformları kullanıldığında, güvenlik riski önemli ölçüde düşer.
Etkin Güvenlik	İlk kurulumları göz önünde bulundurulduğunda temel Z güvenlik çözümleri, alternatif çözümler ile kıyaslandığında *8,5 kat*tan fazla güvenlik, %93'ten daha az bir genel maliyet ile %81 daha az kaynak kullanımı ile sunmaktadır.	IBM Z, en güvenli ortam uygulamasıdır.
Etkin Güvenlik	Z platformları, temel saldırı engellemede geliştirilmiş güvenlikli alternatif platform çözümleri ile kıyaslandığında *%20,74*'e kadar daha başarılıdır.	Z platformlarının sunduğu temel güvenlik düzeyi bile, geliştirilmiş güvenlikli alternatif platform çözümlerinden çok daha etkilidir.
İnsan Kaynağı Verimliliği	Süre devinim incelemeleri, Z güvenlik çözümlerinin standart koruma düzeyi için *%81* daha az işlem gerektirdiğini göstermektedir.	IBM Z, güvenli çalışma için daha az insan kaynağı gerektirir.
İyileştirme	Z güvenlik dağıtımları alternatif platformlar ile kıyaslandığında *%98,82* daha az iyileştirme masrafı oluşturur.	Z dağıtımlarında güvenlik tahribatlarının onarımı çok daha hesaplıdır.
Toplam Mülkiyet Maliyeti	Z güvenlik dağıtımlarının Toplam Mülkiyet Maliyeti, diğer platformlardan %83,72 daha düşüktür.	Bilişim güvenliği için harcadığınız para, Z ile size çok daha fazlasını kazandırır.
Toplam Yatırım Maliyeti	IBM Z dağıtımları, çeşitli boyutlardaki kurumlarda Toplam Yatırım Maliyetinde %84,83'e varan avantaj sunar.	Z ile bilişim yatırım masraflarınızı daha da düşürün!
Kapsamlı Şifreleme	IBM merkezi işlemcili mimariler, 18,4 kat daha hızlı şifrelemeyi, diğer platformların sadece %5 maliyetiyle sunar.	IBM Z ile kapsamlı şifrelemenin kapısını açın!
Risk Azaltma Kaynak Yaratımı	12 milyon ABD Doları BT bütçeli bir kurumdan ön koşul olarak istenilen finansal birikim, x86 sistemlerde 764.400 ABD Doları, IBM Z sistemde ise sadece 160.524 ABD Dolarıdır.	Z ile düşük risk, düşük bilişim güvenliği kaynak yatırımı demektir!
Emsalsiz!	Günümüzde kapsamlı şifrelemeyi destekleyen tek mimari, IBM Z mimarisidir.	IBM Z emsalsiz şifreleme gücü sunar.

Bilişim sektörünün değişken doğası daha da hızlanıyor. Daha hızlı değişim, yoğun saldırılar ve zorlu risk yönetimi görevleri; işte bunların hepsi mevcut tehlikeyi ve fırsatları göstermektedir.

SIL'nin tamamladığı çalışmanın temel amacı, gerçek uygulamada platform mimarilerinin ticari güvenlik alanındaki etkisini belirlemekti. Bu doğrultuda IBM'nin Z platformları, UNIX ve x86 ürünleri gibi köklü mimariler karşılaştırıldı.

Ortaya çıkan sonuç, sektörü kökten değiştiriciydi.

SOLİTAİRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL), uygulamalı ve tahmine dayalı performans modellemesi alanında uzman bir hizmet sağlayıcısıdır. 1978 yılında kurulan SIL, kapsamlı yapay zeka teknolojisi ve isabetli durum analizi amaçlı özel kaos matematiği birikimlerinden faydalanmaktadır. SIL incelemeleri; 5.900'den fazla müşteriye risk profilleme, performans temel neden analizleri, ortam etkisi, kaynak yönetimi, piyasa analizi, sorun analizi, uygulamada Fourdham verimlilik analizleri, kurumsal değişken fırsatları belirleme, maliyet ve gider tahlili gibi konularda hizmet sunmaktadır. SIL uluslararası olarak devlet kurumlarına ve ticari firmalara, firmalar için teklif talebi (RFP) sertifikalama hizmeti de sunar.

Pek çok ticari ve devlet kurumları donanım ve yazılım hizmeti firması, sundukları hizmetlerin kısıtlı yanları ve performans kapasitesi belgelendirmeleri için SIL ile birlikte çalışırlar. SIL de, bu firmalar ile üretimi artırma ve müşteri uygulamaları hususunda ölçeklenebilirlik hizmetler sunar. Risk profillerini ve risk azaltma stratejileri oluşturur. SIL, kurulduğu günden beri endüstri standartlarının oluşturulmasında ve performans belgelendirme alanlarında etkin bir rol oynamıştır. BT odaklı kurumsal maliyetler ve davranışsal analizlerin daha iyi anlaşılması amacı ile Operational Characterisation Master Study (OPMS) için bilgi toplama görevini üstlenmiştir. OPMS, SIL'nin buluşsal veri tabanını geliştirmeye devam etmiştir. Bu veri tabanının mevcut verisi, 475 PB'den fazla bilgi içermektedir. İstatistik veri tabanının boyutu, SIL'nin analitik tutarlılığını ve doğruluğunu rakipsiz olacak şekilde artırmıştır. Ortalama olarak SIL, yılda 2 milyondan fazla model ile mevcut müşterilerine ve ad hoc isteklere cevap vermektedir.

METODOLOJİ NOTLARI

IBM Z platformlarının, bir şirketin BT altyapısının temel bir bileşeni olarak kullanılmasının ve müşteri deneyimi üzerindeki etkisini belirlemek için önemli sayıda dağıtım incelenmiştir. Toplam hizmet dışı kalma vb her bir etken için çalışma özelliklerindeki farkların etki seviyeleri belirlenmiş ve bu farklılıklar belirlendikten sonra, ilgili kombinasyonlarda oluşan net etkileri anlamak için karşılaştırılmışlardır. Etkiler; genel performans ve kapasite kullanımı ve çeşitli iş birimleri ölçekleri alanlarında incelenmişlerdir.

SIL, gerçek sistemlerin ve gerçek işletmelerin operasyonel üretim davranışı verilerinin derlenmesi yaklaşımı ile hareket eder. Bu araştırma uyarınca bulguların doğrulanması için 9.602.042 ortam çalışması gözlemlenmiş, kaydedilmiş ve analiz edilmiştir. Müşteri deneyimi, dağıtım verileri ile karşılaştırılması için alınmıştır. 6,3 milyondan fazla müşteri geri bildirim profili, deneyimlerinin analizi ve BT ortamlarındakiler ve çalışma dahilindekiler ile karşılaştırılması için kullanılmıştır. Böylesine devasa bir müşteri ve sektör ampirik verilerinin kullanılması, gerçek ortamda oluşabilecek durumun daha doğru tespit edilmesine olanak sağlamıştır. Bu sistemlerden alınan veriler, mevcut operasyonel zorluklar ve faydalar hakkında doğru bir perspektifin oluşturulması için kullanılmıştır. Sistemlerin bildirilen davranışları incelenerek, mimarinin davranışsal analizlerinin, hem saf performans hem de net sektörel etkilerinin belirlenmesi için kullanılmıştır.

Bu çalışmanın bir amacı da yeni çıkan teknolojilerin genel performans, maliyet ve çok sayıda kurumun riskleri üzerindeki etkisinin, müşteriler tarafından sağlanan veriler ve ayrıntılı operasyonel emülasyonlar ile incelenmesidir. Bu emülasyon ile 14 ay süren günlük etkinlik süresince, müşterilerden gelen veriler ile, bu kurumların sanal ortamları oluşturulmuştur. İlgili çalışmanın sonuçları, bu raporun bulgular kısmındadır.

Bu çalışmada sunulan benzeri durumlarda SIL, operasyonel verilerin alımının da dahil edildiği ve yüksek ayrıntılı sistem etkinlik bilgilerini içeren bir metodoloji kullanır. Müşterilerin kendi platformlarından aldıkları bilgiler ile bu verilerin oluşturulduğu unutulmamalıdır. Bu çalışma uyarınca elde edilen verilerin hiçbirinin yapay sınamalarda veya laboratuvar ortamında oluşturulmuş testler ile elde edilmiş veri olmadığı, kurumlardan alınan gerçek operasyonel süreçler sonucu elde edilmiş verilerin derlenmesinden oluşturulduğu unutulmamalıdır. Yani veriler, kusursuz çalışan sınama ortamlarından alınmamış ve reel ortamda sürekli olarak kullanıldıkları kurumların koşullarından etkilenmişlerdir. Çalışma analizinin odağı; işletim sistemi ve donanımdaki ufak farklılıklardan oluşan farklılıkların belirlenmesi olmadığı için; benzer sistemlerden gelen veriler birleştirilerek ortalama mimarisel farklılıklar analiz edilmiştir. Bu da mimarisel strateji hakkında daha genel bir görüş edinilmesini sağlar.

Analizin ayrıntılılığının artırılması için çeşitli dağıtımlardan, kurulumlardan, farklı sanayilerden, coğrafyalardan ve farklı firmalardan bilgiler alınmıştır. Bu tür derlemelerde, bir kurumda birden fazla firmanın ürünlerinin olabilmesi nedeniyle örtüşme kaçınılmazdır. Bu durumlarda toplam ayrık yüzdesi %100'ü geçebilir. Birden fazla coğrafi konumda ya da endüstri sınıflandırmasında olan çok katmanlı dağıtıma sahip olan kurumlarda analizler, kurumların sunduğu verilerin ayrık kırılma noktaları belirlenerek rapora eklenmiştir. Uygun görülmeyen veriler, ek bir filtreleme işlemi ile rapora

eklenmemiştir. Bu uygun görülmeyen verilerde yer alan bozulma oranları; düşük performans ve yüksek maliyet gibi etkenlerin donanım ve yazılım tercihinden olmadığı anlaşıldığı için, çalışmanın analitik tabanından çıkartılmışlardır.

Çalışmada verilerin alındığı sektörler; üretim (%26,55), dağıtımcılık (%19,87), sağlık (%4,67), perakende (%12,83), finansal (%22,16), kamu (%6,54), iletişim (%3,88) ve karma grup (%3,50).

Veri sağlayan kurumların coğrafi ağırlıkları; %32,05 ile Kuzey Amerika, %10,58 ile Orta ve Güney Amerika, %33,62 ile Avrupa, %15,62 ile Asya ve Pasifik, %4,74 ile Afrika, ve %3,38 ile belirtilen coğrafi bölümlendirmelerin dışında kalan kurumlardan oluşur.

Kurumların stratejileri ve bütçeleri boyutlarına göre çeşitlilik gösterdiğinden, SIL tarafından küçük, orta, büyük ve çok büyük sınıflandırmalarından oluşan bir kategorilendirme ölçek katmanı daha eklenmiştir. Bu kategoriler, çalışan sayıları ve yıllık brüt gelirlerine göre belirlenmiştir. Çalışan sayısı çarpı yıllık brüt gelir yöntemi ile ölçeklendirilmişlerdir. Açıklamak gerekirse; küçük bir kurum 100 çalışandan daha az çalışana ve yılda 20 milyon ABD Dolarından daha az brüt gelire sahip ise 2000 değerindedir. Yani 100 (çalışan) X 20 (milyon dolar değerinden brüt gelir). 50 çalışanlı ve 40 milyon ABD Doları brüt gelirli bir şirket yukarıda belirtilen kurum ile aynı boyut kategorisine girer. SIL tarafından belirlenen boyut alt sınırları 2.000 (küçük), 10.000 (orta), 100.000 (büyük) ve 1.000.000 (çok büyük) olarak belirlenmiştir.

Bu çalışma dahilinde toplanılan bilgiler, SIL'nin 1978 yılından bu yana sürdürdüğü bir veri toplama ve sistem desteği programı amaçları ile derlenmiştir. Tüm testler, SIL müşteri tesislerinde, müşteri personeli tarafından gerçekleştirilmiştir. Testlerin sonuçları, SIL ile destek ilişkisine girmiş olan müşteriler tarafından kullanılan normal güvenli veri toplama noktalarından gönderilmiştir. Bilgiler, güvenli veri noktalarından gönderildiği için veriler, standart SIL yapay zeka işlemcisi tarafından standart biçimde, tüm müşteri referansları ayrıntıları çıkartılmıştır. Ardından, havuzda biriken veriler, analiz ve bulgulama için girilmiştir.

TELİF HAKKI VE FERAGAT

Bu belge, IBM finansmanlığı ile oluşturulmuştur. Belgede IBM de dahil olmak üzere, çeşitli firmalardan edinilen herkese açık olan materyal kullanılmış olabilir, ilgili firmaların belirtilen hususlardaki duruşlarını yansıtmayabilir.

ZSL03452-TRTR-00