INFORMATİON TECHNOLOGY
INTELLİGENCE CONSULTİNG

Information Technology Intelligence Consulting

ITIC

ITIC 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenlik Raporu

Haziran 2021

İçindekiler

Yönetici Özeti

Kurumsal şirketler, arka arkaya üçüncü yılda da (sırasıyla) IBM, Lenovo, Huawei ve Hewlett-Packard'ın görev açısından kritik sunucularını, başarıya ulaşan veri ihlali sayısı en az olan ve bilgisayar korsanları tarafından kırılması en zor olduğu kanıtlanmış en güvenli platformlar olarak sıralamıştır.

İşte bunlar, 15 farklı sunucu platformunun güvenlik özellikleri ve işlevlerinin karşılaştırıldığı en son ITIC Global Sunucu Donanım Güvenliği anketinin sonuçlarıdır. Ocak 2021'den Haziran 2021'in ortasına kadar ITIC'nin bağımsız web tabanlı anketinde, dünya genelinde 28 farklı dikey pazarda 1.100'ün üzerinde şirkete anket yapıldı.

IBM, Lenovo, Huawei, HPE ve Cisco, son 18 ayda küresel COVID-19 pandemisi döneminde güvenlik hack'lerinde ve veri ihlallerinde %42 oranında ciddi bir artış yaşanmasına rağmen en güvenilir ve en güvenli sunucu platformları olarak zirvedeki yerlerini korudu.

(Sırasıyla) IBM Z, IBM POWER, Lenovo ThinkSystem ve Huawei KunLun tarafından yönetilen en iyi sunuculardan her biri, COVID-19 döneminde bile ayrı ayrı en iyi güvenlik ve güvenilirlik/çalışma zamanı performansı sergiledi ve ITIC'in en son anketinde her bir güvenlik kategorisinde, tüm 15 ana akım sunucu donanımı platformu arasında kayda değer şekilde, aşağıdakiler de dahil olmak üzere en iyi güvenlik sonuçlarını elde etti:

- Başarıya ulaşan en az sayıda güvenlik saldırısı/veri ihlali.
- ***Herhangi bir*** sebeple en kısa plansız toplam sunucu aksama süresi ve bir güvenlik olayı neticesinde en kısa plansız sunucu aksama süresi.
- Saldırının başlangıcından şirketin izole edilip kapatılmasına kadar en hızlı Ortalama Tespit Süresi (MTTD).
- Sunucular, uygulamalar ve ağların tam çalışmaya dönmesini sağlayacak en hızlı Ortalama Düzeltme Süresi (MTTR).
- Herhangi bir güvenlik veri ihlalinin (örneğin fidye yazılım, e-dolandırıcılık veya CEO sahtekarlığı) doğrudan bir sonucu olarak, en az miktarda kayıp, çalıntı, imha edilmiş, hasar görmüş veya değiştirilmiş veri.
- Başarıya ulaşmış bir güvenlik saldırısı nedeniyle yaşanan en az miktarda parasal kayıp.
- Sunucu donanımının, alarm/uyarı veren ve güvenlik saldırıları ile veri ihlallerini geri püskürten bütünleşik güvenliğine duyulan maksimum güven.

Hewlett-Packard Enterprise (HPE) ve Cisco'nun kritik iş sistemleri de yüksek düzeyde bir güvenlik sağlamış, en güvenli ilk beş sunucu dağıtımını tamamlamıştır. Yelpazenin diğer ucunda, en yüksek sayıda başarılı yetkisiz güvenlik girişi yaratan markasız Beyaz kutu sunucularının saldırılara en açık sunucular olduğu kanıtlanmıştır.

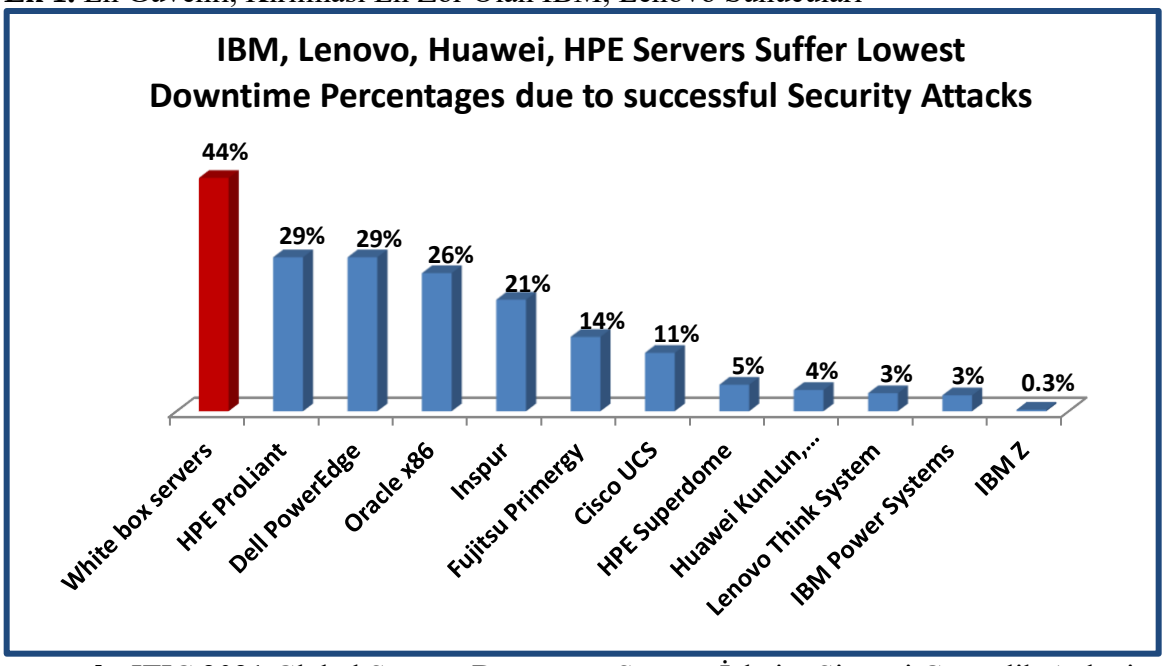
ITIC'in en son Küresel Güvenlik anketi, benzer şekilde IBM, Lenovo, Huawei ve HPE'nin görev açısından kritik sunucularının başarılı güvenlik saldırıları ve veri ihlalleri nedeniyle en düşük yüzdelerde aksama süresi yaşadığını ortaya koymuştur (**Bkz. Ek 1).**

Diğer tüm sunucu dağıtımlarını geride bırakan IBM Z anabilgisayarı, en son ITIC çalışmasında şimdiye kadarki en güçlü güvenlik ve güvenilirlik derecelerini elde etmesi açısından benzerlerinden üstündür.

Yüksek kaliteli IBM Z sunucularının yalnızca %0,3'lük ufak bir yüzdesi, başarıya ulaşan bir veri ihlali durumu yaşamıştır. Diğer ana akım donanım platformları arasında, IBM Power Systems ve Lenovo ThinkSystem kullanıcılarının yalnızca yüzde üçü (%3), sistemlerinin başarılı bir şekilde hacklendiğini, diğer taraftan Huawei KunLun sunucu müşterilerinin yüzde dörtten (%4) daha az bir kısmı ile PE Integrity Superdome sunucu müşterilerinin yüzde beşlik (%5) bir bölümü ise Ocak 2021'den Haziran 2021'in ortasına kadar başarılı bir güvenlik ihlali durumu yaşadıklarını bildirmiştir.

Cisco UCS sunucularının onda birinden biraz fazlası veya %11'lik bir kısmı başarıyla hacklenmiştir. Çoğu zaman ilk savunma hattı niteliği taşıyan ve en şiddetli saldırıları yaşayan birçok UCS sunucusunun özellikle uzak yerlerde ve ağ uç noktasında devreye alındığı dikkate alındığında, Cisco'nun donanımı son derece iyi bir performans göstermiştir. Markasız Beyaz kutu sunucuları yetkisiz güvenlik girişlerine karşı en savunmasız olan sunucular olup, ITIC anketine katılanların %44'ü bu sistemlerin başarıyla hacklendiğini bildirmiştir.

Ek 1. En Güvenli, Kırılması En Zor Olan IBM, Lenovo Sunucuları



Kaynak: ITIC 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenlik Anketi

Genel olarak, ITIC'in anket bulguları, en iyi performans gösteren platformlar ve en güvensiz öneriler arasında, sunucu donanımı güvenliği ve güvenilirliği konusunda belirgin ve giderek artan bir fark olduğunu ortaya koymaktadır. Küresel pandemi; COVID-19 bağlantılı veri ihlalleri, Fidye yazılım, e-dolandırıcılık, İş E-postası Güvenlik Tehdidi (BEC), CEO sahtekarlığı ve tüm şiddetiyle devam eden saldırılardan oluşan bir dalgayı tetikledi.

ITIC'in en son anket sonuçları, güvenilirliğin ve güvenliğin ayrılmaz bir biçimde iç içe geçtiğini ve hatta simbiyotik nitelikte olduğunu ortaya koymaktadır. Güvenlik ve veri ihlalleri; sunucu, uygulama ve ağ çalışma süresini ve kullanılabilirliğini anında bozmaktadır. Güvenlik saldırıları ve veri ihlalleri, pahalı ve tehlikelidir. Bu saldırılar, iş ortaklarının, müşterilerin ve tedarikçilerin yanı sıra şirketlerin fikri mülkiyetini riske atmaktadır. Başarılı bir güvenlik saldırısı, ayrıca çalışanların kişisel verilerini de açığa çıkarmaktadır.

İlk beşteki en güvenilir sunucu platformları olan IBM Z, IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun ve Fusion Servers, HPE Superdome Integrity ve Cisco UCS'nin (bu sıralamayla) ayrıca aşılması en zor güvenlik özelliğine sahip olması bir tesadüf değildir.

Giriş

Küresel pandemi, çok sayıda şirket ve tüketici cihazlarını ve yazılımını hedef alan her bir dikey pazarda, COVID-19 bağlantılı veri ihlalleri, Fidye Yazılım, E-dolandırıcılık, İş E-postası Güvenlik Tehdidi (BEC), CEO sahtekarlığı ve tüm şiddetiyle devam eden saldırılardan oluşan bir dalgayı tetikledi.

Hiç kimse ve hiçbir şey bağışık değildir. Bu durum, içsel, güçlü bir altyapı güvenliğini zorunlu hale getirmektedir.

ITIC'nin en son anketi, genel olarak ankete katılanların %73'ünün şirketlerinin gelecek 12 ila 18 ay arasında profesyonel bilgisayar korsanları tarafından hedef alınan bir saldırıya kurban gideceğinden endişe ettiğini ortaya koymuştur. Bu zaman çizelgesi, uzaktan eğitim gerçekleştirmiş olan ve şimdilerde sınıflara dönmeye hazırlanan ilk 12 yıllık eğitim uygulayan okullar, yüksek okullar ve üniversiteler, öğrenciler ve öğretmenlerin yaygın olarak aynı eğilimi gösterdiği süreyle aynı zamana denk gelmektedir. Aynı şekilde, birçok kurumsal işletme ve devlet kurumu, bir sağlık güvenliği önlemi olarak artık hibrit bir evden çalışma modeline geçiş yapıyor.

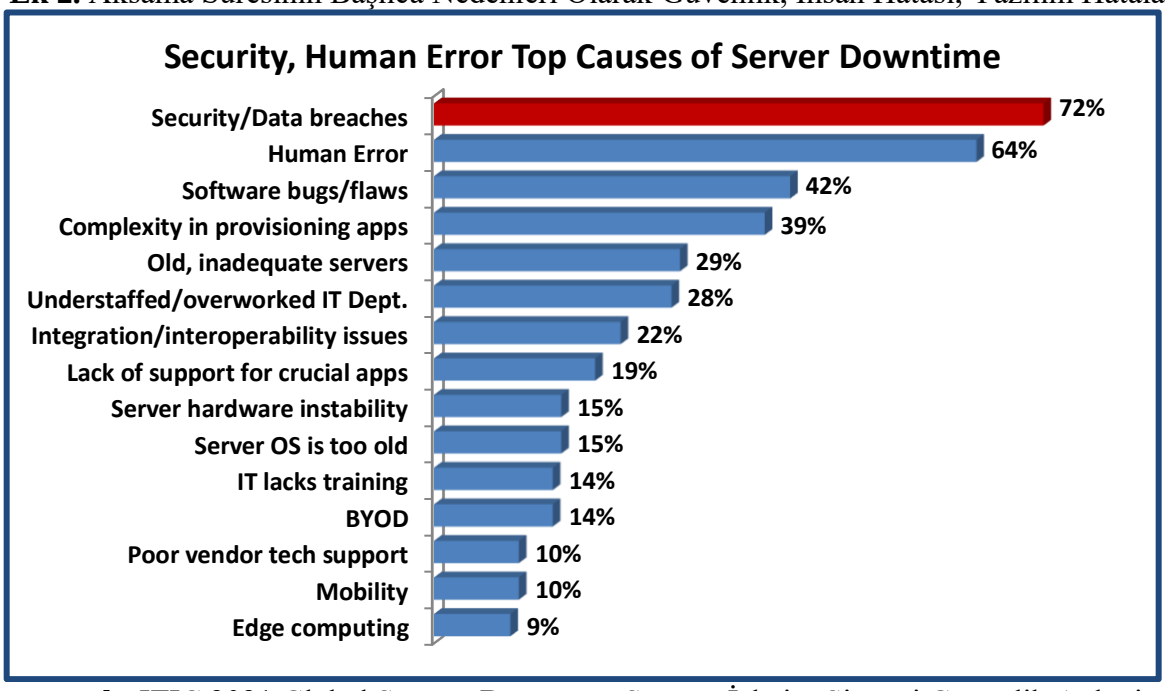
ITIC'in en son güvenlik anketi bulguları, 2020'nin başlangıcından bu yana siber güvenlik riskleriyle ilgili birçok uyarıyı bildirmiş olan çeşitli ABD Federal devlet kurumlarıyla da desteklenmektedir. Federal Soruşturma Bürosu (FBI); Ulusal Güvenlik Bakanlığı Siber Güvenlik ve Altyapı Güvenlik Ajansı (CISA) ile Menkul Kıymetler ve Borsa Komisyonu'nun (SEC) Uygunluk Denetimleri ve İncelemeleri Ofisi (OCIE).

FBI'ın Mayıs ve Haziran ayında yayınlanan uyarılarına göre, COVID-19 bağlantılı siber güvenlik tehditleri arasında eyalet işsizlik sigortası tazminatını ve Federal teşvik çeklerini, sağlık hizmetlerini, bankaları, yaşlıları, kripto para ve devletin dolandırıcılık programlarını hedef alan dolandırıcılıklar yer almaktadır. FBI, "pandemi sırasında eğitimlerine evden devam eden çocukları hedef alan, çevrim içi olarak yıkıcı bir davranış gösteren suçluların" dahil olduğu olaylar da yaşandığını belirtmektedir.

(Sırasıyla) IBM, Lenovo, Huawei, HPE ve Cisco tarafından açıklanan güçlü güvenlik sonuçları, küresel COVID-19 pandemisinin etkisi altında elde edildiği için bilhassa kayda değerdir. ITIC anketine katılanların yaklaşık %40'ı, sunucularının, işletim sistemlerinin ve kritik iş uygulamalarının, 2020'nin başlarında COVID-19'un başlamasından bu yana başarılı güvenlik saldırılarına maruz kaldığını bildirmiştir. Bu, sadece son altı ayda %31'in üzerine yüzde dokuzluk bir artış ve ITIC'in 2020 Küresel Sunucu Donanımı, Sunucu İşletim Sistemi Güvenilirlik anketinde şirketlerin %19'luk bir kısmının sunucularının başarıyla hacklendiğini belirtmesine göre yüzde 21'lik bir artış anlamına gelmektedir.

Güvenlik, tüm işletmeleri etkileyen bir teknoloji ve iş sorunudur. Katılımcıların yaklaşık %72'si, güvenlik ve veri ihlallerini sunucu, uygulama, veri merkezi, ağ uç noktası ve bulut ekosistem güvenilirliği için en büyük tehdit olarak görmüştür **(Bkz. Ek 2)**. Saldırılar, daha hedefe yönelik, nüfuz eden ve kötücül niteliktedir. Kurumsal ve bireysel müşteri mağdurlarına maksimum zararı ve hasarı vermek üzere tasarlanmıştır.

Ek 2. Aksama Süresinin Başlıca Nedenleri Olarak Güvenlik, İnsan Hatası, Yazılım Hataları



Kaynak: ITIC 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenlik Anketi

Tehdit Ortamı: Güvenlik Açıkları ile Veri İhlalleri, En Büyük ve En Maliyetli Güvenilirlik Tehdidi'dir

Veri ihlalleri, gelişmekte olan profesyonel korsan gruplar için büyük ve birincil bir faaliyet alanıdır. Başarılı bir güvenlik saldırısı, birçok açıdan maliyetlidir. IBM ve Ponemon Enstitüsü tarafından ortaklaşa yürütülen 2020 Veri İhlali Maliyeti Çalışması'na göre 2020 yılında veri ihlalinin ortalama $3,86 milyon değerinde bir maliyeti olmuştur[1]. Bu rakam, 2015'ten beri %10'luk bir artışı temsil etmektedir. Gerçek maliyetler, güvenlik saldırılarının süresine ve şiddetine göre değişecektir. Fidye yazılım saldırıları, artmaya devam etmektedir.

Ayrıca bu saldırılar çok maliyetlidir. 7 Mayıs 2021 tarihinde DarkSide bilgisayar korsanları tarafından gerçekleştirilen fidye yazılım saldırısı, Colonial Pipeline Co. şirketinin altı gün

[1] "2020 Veri İhlali Maliyeti Çalışması," IBM ve Ponemon Enstitüsü. URL: https://www.ibm.com/security/data-breach

boyunca faaliyetini durdurmasına neden olmuştur[2]. Colonial Pipeline, gaz ve dizel yakıtının %45'ini New Jersey'den ABD'nin Doğu Kıyısı'na Florida'ya tedarik etmektedir. Florida, Kuzey Karolina ve Virginia dahil olmak üzere birçok eyalette teslimatların durmasına ve gaz kıtlığına neden olmuştur. Ancak Colonial Pipeline'ın icra başkanı Joseph Blount'un bilgisayar korsanlarına 4,4 milyon ABD Doları değerinde fidye ödemeyi kabul etmesiyle son bulmuştur. Blount, Wall Street Gazetesi'ne verdiği açıklamada, yöneticilerin siber saldırının sistemlerini ne derece kötü şekilde ihlal ettiğini ve sonuç olarak veri hattını eski haline getirmenin ne kadar süreceğini bilemedikleri için 4,4 milyon ABD Doları değerindeki fidye ödemesine onay verdiğini belirtmiştir.

Colonial Pipeline Fidye Yazılım saldırısı, pek çok saldırıdan sadece bir tanesidir. Başarılı güvenlik saldırılarıyla ilişkili güvenlik açıklarının, risklerin ve yüksek maliyetlerin önemine vurgu yapmaktadır. Colonial Pipeline Fidye Yazılım korsan saldırısı, ayrıca birinci sınıf, güçlü bir güvenlik altyapısının yürürlükte olması gerektiğinin de altını çizmektedir. Sunucu donanımı, her bir kurumsal ağın ve ekosistemin temel unsurudur.

DTEX Sistemleri Raporu, "şirketlerin yalnızca %30'unun uzaktan çalışmaya tam geçişin güvenliğini sağlamaya hazır olduğunu" ortaya koymuştur. DTEX Sistemleri çalışması, ayrıca şirketlerin yaklaşık %75'inin evden çalışan kullanıcıların teşkil ettiği güvenlik riskleri konusunda endişeli olduğu, işletmelerin %73'ünün ise uzaktan çalışanlar tarafından VPN'lerinin devre dışı bırakılması durumunda kullanıcı faaliyetini kısmen gördüklerini veya hiç görmediklerini kabul ettiği sonucuna varmıştır. Endişe veren bulgulardan bir diğeri de, evden çalışan kişilerin dizüstü iş bilgisayarlarını kişisel amaçlarla kullanmalarıdır; ankete katılanların %25'i bu durumun istemsiz indirme riskini artırdığını kabul etmiş, %15'i ise firmalarının e-dolandırıcılık saldırılarına daha açık olduğunu belirtmiştir.

ITIC'in en son çalışması, Aksama Süresinin Saatlik Maliyetinin tırmanmaya devam ettiğini göstermektedir. KOBİ ve büyük işletmelerin %89'u için artık 300.000 ABD Dolarının üzerindedir. Genel olarak, orta ve büyük ölçekli şirketlerden ankete katılanların %42'si, ortalama tek bir saatlik aksama süresinin firmalarına bir milyonun (1 milyon ABD Dolarının) üzerinde bir maliyete neden olduğunu bildirmiştir. En kötü senaryoda, kullanımın en yoğun olduğu saatlerde görülen ve kritik iş faaliyetlerini kesintiye uğratan bir veri ihlali, şirketlere dakikada milyonlarca

[2] "Colonial Pipeline CEO'su, Bilgisayar Korsanlarına Neden 4,4 Milyon ABD Doları Tutarında Fidye Ödediğini Anlatıyor", Wall Street Gazetesi, 19 Mayıs 2021. URL: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

dolara mal olabilir. Hedefe yönelik bir fidye yazılım saldırısının sonucu olarak saatlerce veya günlerce uzun süreli bir kesinti yaşayan herhangi bir şirket, neredeyse şüphe götürmez şekilde milyonlarca dolar zarara uğrayacaktır.

Şirketler, verimlilikten ve aksayan faaliyetlerden kaynaklı gözle görülür parasal kayıpların yanı sıra, iyileştirme çabalarına ve tam faaliyete geri dönüşe dahil olan iş gücü çalışma saatlerinin miktarını ve BT ve güvenlik yöneticilerinin sayısını dikkate almalıdır. Şirketler, ayrıca herhangi bir verinin veya fikri mülkiyetin (IP) kaybolmuş, çalınmış, hasar görmüş, tahribata uğramış veya değiştirilmiş olup olmadığını tespit etmelidir. Kuruluşlar, ayrıca güvenlik olayları ve veri ihlalleri ile ilişkili potansiyel para cezaları veya suça ilişkin cezalar/para cezalarının yanı sıra herhangi bir hukuk davasının maliyetini de hesaba katmalıdır. Bir kuruluşun itibarının zarar görmesi gibi hesaplanamayan nitelikteki bazı maliyetler, iş kaybıyla sonuçlanabilir.

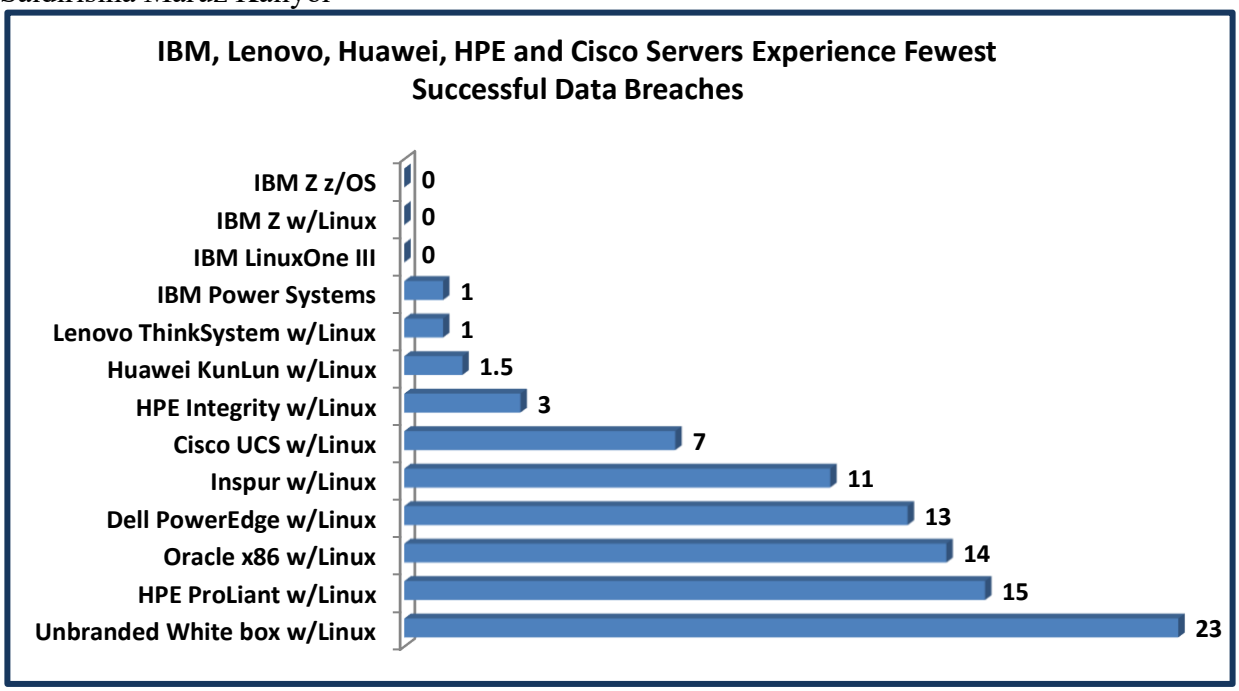
Bilgisayar korsanları, hedeflerini büyük bir kesinlikle özenle seçer ve her fırsattan yararlanma konusunda oldukça hızlıdırlar. COVID-19 pandemisi, buna tam bir örnek teşkil etmektedir. Bilgisayar korsanları, evden çalışan kişiler ile çevrim içi derslere ve Zoom derslerine giren uzaktan eğitim gören öğrencileri hedef almaktadır. Sözde "kolay hedefler" üzerine odaklanırlar. Tam zamanlı şirket içi güvenlik ve BT yöneticisi bulunmayan ve en güncel güvenlik yazılımlarını yüklememiş olan yerel belediyeler ile bölge belediyeleri, küçük ve orta ölçekli okul bölgeleri, hastaneler, sağlık hizmeti klinikleri, doktor muayenehaneleri ve banka şubeleri.

Sunucu Satıcıları: IBM, Lenovo, Huawei ve HPE Step Up Security

Sunucu güvenilirliğinde kalıcı olarak en iyi dereceleri elde etmiş olan IBM, Lenovo, Huawei, HPE gibi satıcıların aynı zamanda en güvenli donanım platformları arasında yer alması şaşırtıcı değildir. Bu satıcılar ve daha yakın zamanda Cisco, sunucu güvenliğini - Lenovo örneğinde sunucu, bilgisayar ve dizüstü bilgisayar güvenliğini - birinci sıraya taşımış ve son birkaç yıldır ağırlıklı olarak sunulan ürünlerinin içsel güvenliğini güçlendirmeye yatırım yapmıştır. Dolayısıyla, COVID-19 pandemisi vurduğunda zaten güçlü ve bütünleşik bir güvenliğe sahip olmaları, iyi bir konumda kalmalarını sağladı.

Ek 3'te belirtildiği üzere, en güvenli sunucu donanım platformları en az sayıda başarılı güvenlik ihlali yaşamıştır. z/OS ve Red Hat Enterprise Linux (RHEL) işletim sistemiyle çalışan IBM Z ile IBM LinuxONE III katılımcılarının tümü, bu platformların 16 aydır hiçbir başarılı güvenlik saldırısı yaşamadığını belirtmiştir. Bu platformları, sırasıyla IBM Power Systems ve Linux ThinkSystem izledi; Huawei KunLun'da ortalama iki güvenlik saldırısı; HPE Integrity'de başarılı üç adet yetkisiz güvenlik girişi ve Cisco'nun UCS sunucularına yönelik yedi adet veri ihlali. Markasız Beyaz kutu sunucuları, son 16 ayda ortalama 20 adet başarılı veri ihlaliyle saldırılara en açık sunucular olarak yerini almıştır.

Ek 3. IBM, Lenovo, Huawei, HPE ve Cisco Sunucuları, En Az Sayıda Başarılı Güvenlik Saldırısına Maruz Kalıyor



Kaynak: ITIC 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenlik Anketi

Veri ve Analiz: Satıcı Güvenlik Sonuçları

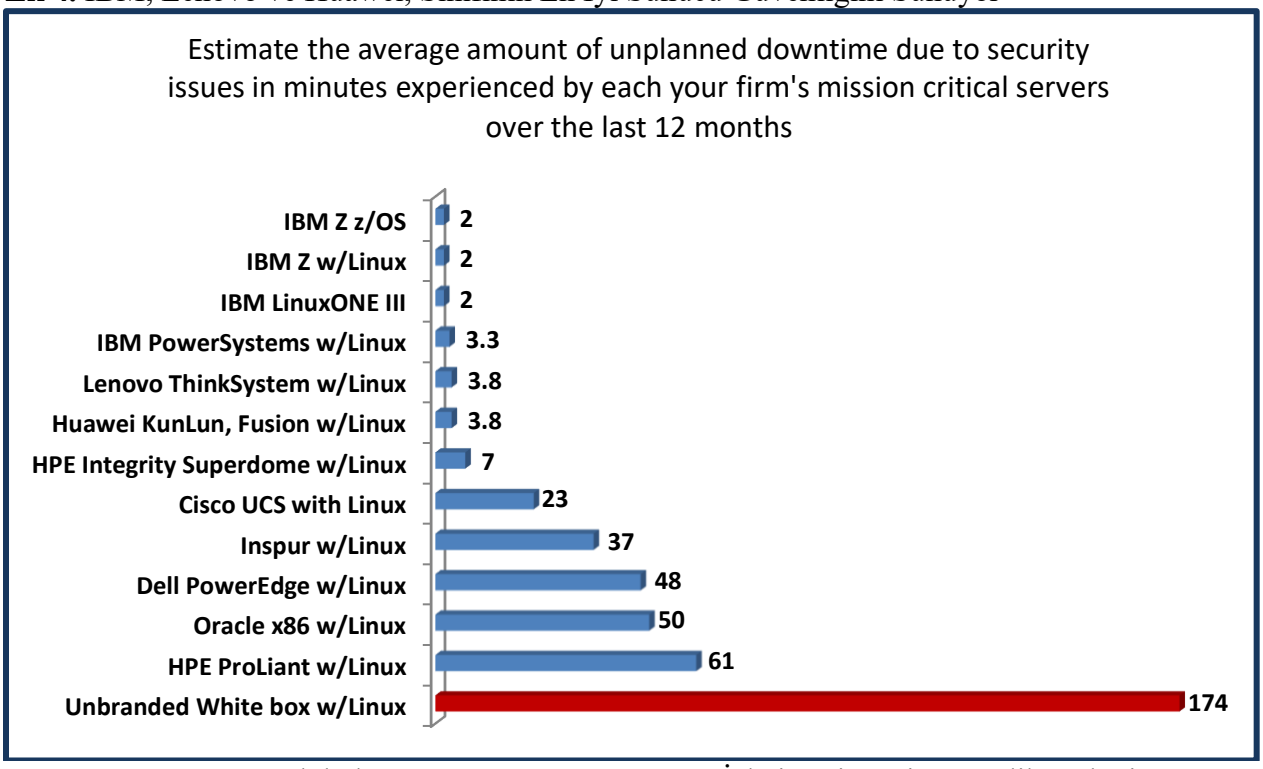
Tekrarlamak gerekirse, ITIC'in 2021 Global Sunucu Donanımı Güvenlik anketi, (sırasıyla) IBM Z, IBM Power Systems, Lenovo ThinkSystem ve Huawei KunLun ile Fusion sunucularının aşağıdakiler dahil olmak üzere her bir güvenlik kategorinde en iyi sonuçları elde ettiğini ortaya koymuştur:

- **Başarıya ulaşan** en az sayıda güvenlik saldırısı/veri ihlali.
- ***Herhangi bir*** sebeple en kısa plansız toplam sunucu aksama süresi ve bir güvenlik olayı neticesinde en kısa plansız sunucu aksama süresi.
- Saldırının başlangıcından şirketin izole edilip kapatılmasına kadar en hızlı Ortalama Tespit Süresi (MTTD).
- Sunucular, uygulamalar ve ağların tam çalışmaya dönmesini sağlayacak en hızlı Ortalama Düzeltme Süresi (MTTR).
- Herhangi bir güvenlik veri ihlalinin (örneğin fidye yazılım, e-dolandırıcılık veya CEO sahtekarlığı) doğrudan bir sonucu olarak, en az miktarda kayıp, çalıntı, imha edilmiş, hasar görmüş veya değiştirilmiş veri.
- Başarıya ulaşmış bir güvenlik saldırısı nedeniyle yaşanan en az miktarda parasal kayıp.
- Sunucu donanımının, alarm/uyarı veren ve güvenlik saldırıları ile veri ihlallerini geri püskürten bütünleşik güvenliğine duyulan maksimum güven.

Ek 4'te gösterildiği üzere, IBM Z, IBM Power Systems, Lenovo ThinkSystem ve Huawei KunLun'un görev açısından kritik sunucuları, başarılı güvenlik olaylarının ve veri ihlallerinin doğrudan sonucu olarak en kısa süreli plansız aksama süresi yaşamıştır.

IBM Z ve IBM LinuxONE III, güvenlik sorunları nedeniyle her bir sunucu başına toplamda ortalama sadece 2 dakikalık bir plansız aksama süresi yaşamıştır. Bu sunucuların hemen arkasından, bir güvenlik sorunu nedeniyle sunucu başına plansız kesinti süresi 3 dakikanın biraz üzerinde olan IBM'in POWER8 ve POWER9 sunucuları gelmektedir; Lenovo ThinkSystem donanımı ve Huawei KunLun ve Fusion sunucularının her biri, güvenlik olaylarıyla ilişkili olarak sunucu başına ortalama 3,8 dakikalık bir plansız aksama süresi yaşamıştır. Birçoğunda sunucu işletim sistemlerinin ve yazılım uygulamalarının lisanssız sürümleri çalıştırılan markasız Beyaz kutu sunucularının her biri, bir kez daha doğrudan güvenlik ile ilgili sorunlardan kaynaklanan, 174 dakikalık veya üç saate yakın bir aksama süresi yaşamıştır. Bu durum, en güvenli IBM Z sunucularını en az güvenli Beyaz kutu donanımına kıyasla 87 kata kadar daha güvenli ve güvenilir kılmaktadır, buna karşın IBM POWER8 ve POWER9 sunucuları, markasız Beyaz kutu sunucularından 58 kata kadar daha güvenlidir.

Ek 4. IBM, Lenovo ve Huawei, Sınıfının En İyi Sunucu Güvenliğini Sunuyor



Kaynak: ITIC 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenlik Anketi

Ortalama Tespit Süresi, Kritik Bir Barometredir

Güvenlik saldırıları ve veri ihlalleri, dijital çağda iş yapmanın gerçeklerinden biridir. Belirli bir noktada, her bir kuruluş ve bu kuruluşun kritik öneme sahip ana iş kolu sunucuları, sunucu işletim sistemleri ve uygulamaları, bir tür veri ihlali girişimine veya başarılı bir veri ihlaline maruz kalacaktır.

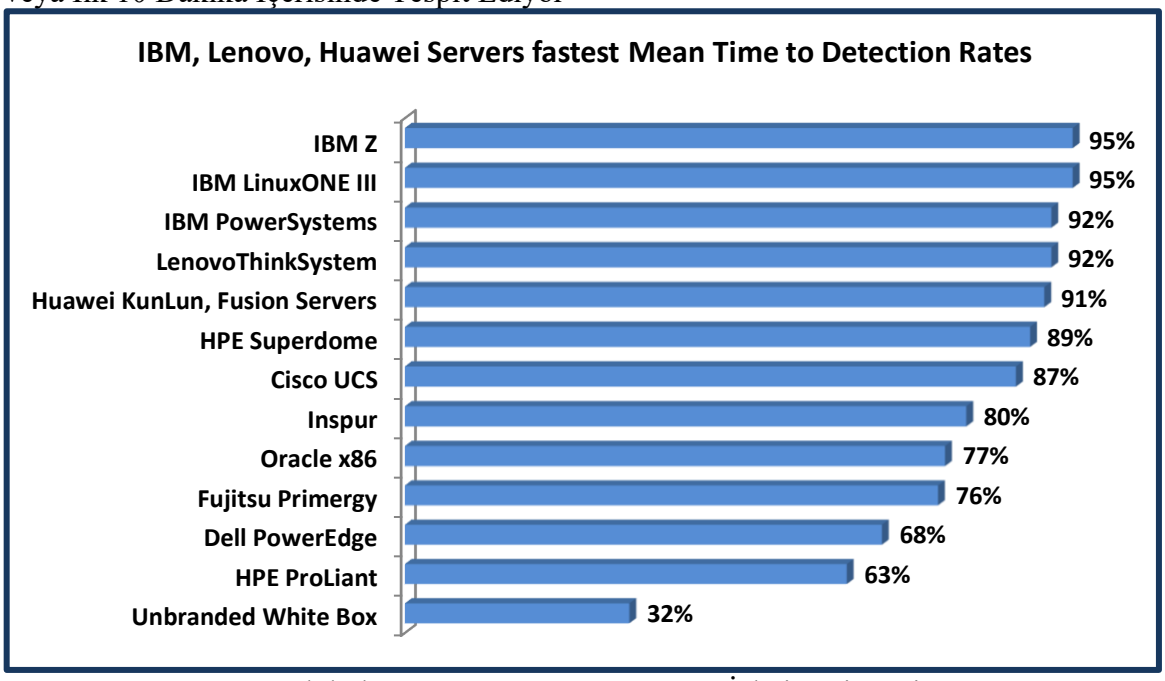
Kuruluşlar, tehlikenin farkına varan, uyarı ve alarmlar gönderen ve tehditleri diğerlerinden ayırma kabiliyetine sahip olan güçlü, bütünleşik bir sunucu ve altyapı güvenliğine dayanmalıdır. Şirket tarafında sıkı bir hazırlığa sahip olmak ve güvenlik uzmanlarından ve BT yöneticilerinden oluşan iyi eğitimli personellere sahip olmak, çok önemlidir.

Şirketin sunucu ve yazılımları, bir güvenlik sorununu ne kadar hızlı bir şekilde tespit edip bu soruna ne kadar hızlı yanıt verebilirse, saldırı ağ ekosisteminden içeri sızmadan, veri işlemlerini ve günlük operasyonları sekteye uğratmadan ve hassas verilere ve IP'ye erişim sağlamadan ***önce*** saldırının diğerlerinden ayrılıp engellenme şansı o kadar fazla olacaktır.

Ek 5, (sırasıyla) IBM Z, IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun ve Fusion Sunucularının, HPE Superdome ve Cisco UCS Sunucularının bir kez daha korsan saldırıları engellemede başarılı olduğunu göstermektedir. Bu sunucular, tüm sunucu platformları arasında en iyi Ortalama Tespit Süresi (MTTD) yüzdelerine sahiptir.

IBM Z ve IBM LinuxOne III anket katılımcılarının %95'lik ezici çoğunluğu, sunucularının bir güvenlik ihlali girişimini "Anında veya saldırının ilk 10 dakikası içerisinde" tespit edebildiğini ve saldırıyı devre dışı bıraktığını belirtmiştir. Bu platformları, sırasıyla IBM Power Systems, Lenovo ThinkSystem ve Huawei KunLun dağılımları izlemiştir; bu platformların her birindeki kullanıcıların %92'si, bir güvenlik ihlalini "Anında veya saldırının ilk 10 dakikası içerisinde" farkedebildiklerini ve geri püskürtebildiklerini belirtmiştir. Kritik çekirdek altyapı sunucuları, işletim sistemleri ve görev açısından kritik uygulamalar bir saldırıyı ne kadar hızlı geri püskürtebilirse, şirketin aksama süresi yaşama ihtimali veya çalınmış, değiştirilmiş, zarar görmüş veya güvenliği ihlal edilmiş verilere ve IP hırsızlığına maruz kalma olasılığı o kadar az olacaktır.

Ek 5. IBM, Lenovo ve Huawei Sunucularının %90'dan Fazlası, Güvenlik Saldırılarını Anında veya İlk 10 Dakika İçerisinde Tespit Ediyor



Kaynak: ITIC 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenlik Anketi

Sunucu Satıcısı Güvenlik Sonuçları

IBM Security Anketinde Öne Çıkanlar

- **IBM Z** sunucuları, genel güvenilirlik, erişilebilirlik, performans ve güvenlik konusunda diğer tüm sunucu platformları arasında en iyi dereceleri elde etmeye devam ediyor. "Z"'nin sıfır aksama süresi anlamına geldiği IBM Z ailesi, her bir güvenilirlik kategorisinde sürekli olarak **tüm** rakiplerinden üstün bir performans sergilemekte ve en düşük toplam sahip olma maliyetini (TCO) ve en hızlı yatırım getirisini (ROI) sunmaktadır. z13, z14 ve z15 Systems sunucuları, sunucu başına/bir yılda gerçekleşen plansız fiili aksama süresi açısından güvenilirlik/çalışma süresinde, uygulama kullanılabilirlik derecelerinde ve genel güvenlikte en iyi sonuçları elde etmiştir. IBM Z anabilgisayarı ve IBM LinuxONE dağıtımlarının her ikisi de, ITIC'in 2019 Global Sunucu Güvenilirliği anketinde Z ve LinuxONE platformlarının yaşadığı ortalama 0,74 saniyelik bir aksama süresine kıyasla, sunucu hatalarından kaynaklanan sunucu başına, yılda bir görülen *plansız* aksama süresinde bir dakikadan az, sadece 0,60'lık bir aksama süresine maruz kalarak tam bir hatalara dayanıklılık durumu sergilemektedir. Bir önceki yılın aynı dönemine göre sunucu başına aksama süresinde 0,14 saniyelik bir düşüş göz ardı edilebilir gibi görünse de, aslında aksama süresini yaklaşık %19 oranında azaltmakta ve IBM Z ve LinuxONE'ın toplam sahip olma maliyetini (TCO), 2019 yılındaki sunucu başına/dakikada 1.232 ABD Dolarından, ITIC 2021 Global Sunucu Donanımı Güvenliği çalışmasında sunucu başına/dakikada 1.002 ABD Doları'na, yani 230 ABD Doları kadar düşürmektedir. Genel

olarak IBM Z, ayda sadece 4,32 saniyelik neredeyse hissedilmeyen bir aksama süresi sergilemektedir. Aynı derecede önemli olan bir diğer şey de, güvenlik saldırılarının ve veri ihlallerinin sürekli olarak artması göz önüne alındığında IBM Z sunucusunun üstün güvenliğidir. Z, 2021 yılının Ocak ayından Haziran ayının ortasına kadar, başarılı veri ihlallerinde en düşük yüzdede (yüzde birden daha düşük bir yüzdede) kalmaya devam etmiştir. Üstelik, IBM Z ve LinuxONE III anket katılımcıları ayrıca Ortalama Tespit Süresini (MTTD) en hızlı olarak bildirmiş, ITIC kurum katılımcılarının %95'i, güvenlik ve BT yöneticilerinin bu platformlardaki saldırıları tespit edebildiklerini ve devre dışı bırakabildiklerini belirtmiştir. Bireysel ve toplu olarak bu sonuçlar, Z ve LinuxONE III ürünlerinin başarısına vurgu yapmaktadır. Platformların ayrıca IBM'in 2019'da Red Hat'i devralmasıyla güçlenmesi neticesinde, Z ve LinuxONE platformlarındaki Linux iş yüklerinde ciddi oranda bir artış görülmüştür. IBM yöneticileri, şirketin Linux MIPS'de %55'lik bir artış gördüğünü kamuoyuna açıklamıştır. Ayrıca IBM'in ilk 100 Z istemcisinin 92'sininin Linux iş yüklerini çalıştırdığını da belirtmiştir. Genel olarak, Z platformu, IBM'e göre yılda ortalama 100 ila 200 yeni devreye alım gerçekleştirmektedir.

- **IBM'in LinuxONE III sistemi,** IBM Z platformuna dayanmaktadır. Özellikle hibrit bulut ortamlarını ele alır ve Z'nin yaygın şifrelemesini kullanır. LinuxONE III platformu ve IBM z15, şeffaf, uçtan uca, veri düzeyinde koruma ve gizlilik sağlayan IBM Hyper Protect Data Controller'ı da bünyesinde barındırır. IBM Hyper Protect Data Controller, veriler kayıt sisteminden çıktığında bile şirketlerin verileri şifrelemesine, verilere erişim izni vermesine, erişim iznini geri çekmesine ve veri kontrolü sağlamasına olanak sağlar**.** Sonuç: IBM LinuxONE III, ITIC'in 2021 anketinde en yüksek güvenlik ve güvenilirlik derecelerini paylaşmış olup, LinuxONE III işletmelerinin %95'i veri ihlallerini "Saldırı anında ya da saldırının ilk 10 dakikasında" tespit etmiş ve bu veri ihlallerini devre dışı bırakmıştır.
- **IBM Power Systems** IBM Power Systems müşterilerinin %92'lik büyük çoğunluğu, BT ve güvenlik yöneticilerinin, saldırıları "Anında veya ihlalin ilk 10 dakikası içerisinde" tespit edebildiklerini ve önleyebildiklerini bildirmiştir. IBM'in POWER9 yatay ölçeklenebilir sistemleri, üç yıldır hizmettedir ve gelecek nesil Power10 sunucularının 2021 sonbaharında yola çıkması planlanmaktadır. IBM, performansın, görev açısından kritik iş yükleri desteğinin, gelişmiş analitik desteğinin, bellek içi veritabanlarının ve bütünleşik güvenliğin üzerinde özellikle durarak hattı sürekli olarak yenilemekte ve güncellemektedir. Power Systems modellerinin tümü buluta hazırdır. IBM Power Systems'ın güvenliği, yığındaki tüm katmanlarda, işlemcide, sistemlerde, sabit yazılımda, işletim sisteminde ve hipervizörde yerleşik olarak bulunmaktadır. Yonga içine yerleştirilmiş hızlandırılmış şifreleme sayesinde hareketli ve durağan veriler korunur. IBM, PowerVM hipervizörü için bildirilmiş herhangi bir güvenlik açığı olmadığını ileri sürmektedir. POWER9 sunucuları da buluta hazırdır ve yerleşik PowerVM sanallaştırma yeteneklerini içermektedir. POWER9 yatay ölçeklenebilir sunucuları, kuruluşların bulut ve yapay zeka stratejilerine entegre olacak şekilde tasarlanmıştır. Bu, SAP HANA'nın yanı sıra IBM'in Db2 ve Oracle veritabanları gibi görev açısından kritik iş yüklerini desteklemek için gerekli olan yüksek performansı ve RAS yeteneklerini sağlar. Power10, 7nm'lik bir biçim katsayısında enerji verimliliği ve performans için tasarlanmıştır. IBM, bunun POWER9'a kıyasla 3 kata kadar daha fazla bir işlemci enerji verimliliği, iş yükü kapasitesi ve kapsayıcı yoğunluğu artışı getireceğini hesaplamıştır. Ek olarak, yakında piyasaya sunulacak Power10 sunucuları da, bellek yoğun iş yüklerini desteklemek için bulut kapasitesini artıracak Çok Petabaytlı Bellek Kümeleri desteği de dahil olmak üzere çok sayıda gelişmiş yeteneği bünyesinde barındıracaktır. Power10'ın öne çıkan özelliklerinden biri de, uçtan uca güvenlik için şeffaf bellek şifrelemesi gibi donanım destekli güvenlik yeteneklerine sahip olmasıdır. IBM

Power10 işlemcisi, kuantum korumalı kriptografi ve tamamen benzer yapılı şifreleme gibi günümüzün en zorlu standartlarına ve geleceğin beklenen kriptolu şifreleme standartlarına uygun olarak IBM POWER9'a kıyasla, çekirdek başına AES şifreleme motoru sayısının dört kat fazla olduğu, önemli ölçüde daha hızlı bir şifreleme performansı sağlayacak şekilde tasarlanmıştır. Kapsayıcı güvenliği konusuna da yenilikler getirmektedir.

Lenovo Security Anketinde Öne Çıkanlar

- **Lenovo ThinkSystem** sunucuları, Intel x86 tabanlı tüm sunucular arasında en iyi MTTD oranlarını yakalamış sunucular olup, ankete katılanların %92'si BT ve güvenlik yöneticilerinin, saldırı ve veri ihlali girişimlerini anında veya yetkisiz güvenlik girişinin ilk 10 dakikası içerisinde tespit ettiklerini ve devre dışı bıraktıklarını ifade etmiştir. Bu bir tesadüf değildir. Lenovo, IBM'in x86 tabanlı sunucu işletmesini satın aldıktan sonra geçen yedi yılda ve IBM'in kişisel bilgisayar ve dizüstü bilgisayar alanını satın aldıktan sonra geçen on yılda, güvenliği en üst sıraya koymuştur. Sonuç olarak, Lenovo sunucuları ve masaüstü bilgisayarları, sunucuların ve masaüstü ve dizüstü bilgisayarlarının performansını, güvenilirliğini ve güvenliğini sürekli olarak geliştirmeye ve güçlendirmeye devam ettiği için gücüne güç katmıştır. Lenovo'nun teknik hizmet ve desteği de birinci sınıftır. Lenovo'nun ThinkSystem sunucuları, donanım sorunları nedeniyle sunucu başına 1,51 dakikalık bir aksama süresiyle, ortalamada bu zamana kadarki en iyi çalışma süresiyle güvenilirlik anlamında sürekli iyileşme göstermiştir. Lenovo, IBM gibi mükemmel ve etkili bir taktik ve stratejik güvenlik stratejisi oluşturmuş ve bu stratejiyi yürütmüştür. 2018 yılında Lenovo, kişisel ve dizüstü bilgisayarları için ThinkShield uçtan uca güvenlik teknolojisini gözler önüne serdi. Gelişmiş ThinkShield teknolojisi, güvenlik saldırılarındaki artış nedeniyle son üç yıldır Lenovo bilgisayarlarının ve sunucularının iyi bir konumda olmalarını sağladı. Küresel COVID-19 pandemisi döneminde pek çok kuruluş hem çalışanlar hem de benzer şekilde öğrenciler için uzaktan çalışmaya geçtiği için BT ve güvenlik yöneticileri veri ihlallerine ayak uydurma konusunda baskı altında kalmıştır. Lenovo'nun ThinkShield güvenlik çözümü, önemli bir destek sağlamaktadır. Örneğin ThinkShield, gözle görülür bir biçimde Think System SE350'i hesaba dahil etmektedir. Bu model, optimum bant genişliği sunmak, güvenliği güçlendirmek ve aksama süresini kısaltmak için ağ ucunu hedefleyen, Lenovo'nun ilk özel üretim uç sunucusudur. ThinkSystem SE350, küçük ayak izine sahip bir sunucudur. 1,75 inç yüksekliği, 8,1 inç genişliği ve 14,9 inç derinliğiyle duvara monte edilebilir, bir rafa konabilir veya bir askıya takılabilir. ThinkSystem SE350, ayrıca yüksek performanslı bir sunucu olarak tasarlanmıştır. Intel'in Xeon-D işlemcisine dayanan sunucu, 256GB'lık RAM ve 16TB'lık dahili katı hal depolama ile donatılmış şekilde gelmektedir. ThinkSystem SE350, kilitleme çerçevesi, saldırıları algılama, kurcalamaları algılama ve şifrelenmiş depolama gibi gelişmiş fiziksel güvenlik özelliklerine sahiptir. El değmeden devreye alma yazılımı özelliğine sahiptir. Lenovo'nun kapsayıcı stratejisi, yenilikçiliği güvenilir, esnek ve güvenli veri merkezi sistemleriyle birleştirir. Bu, Lenovo'nun sunucuları, ağları ve nihayetinde kurumsal müşterileri açısından geniş kapsamlı sonuçları olan bilinçli bir hamledir. İnsan hatası, sunucu aksama süresinin açık ara en büyük sebebidir. Son kullanıcılar, özellikle küresel COVID-19 pandemisi döneminde evden çalışan son kullanıcıların ve uzaktan eğitim gören öğrencilerin yüzdesinde ciddi bir artış görülmesi nedeniyle kapsayıcı güvenlik zincirinin geleneksel olarak en zayıf halkası içerisinde yer almaktadır. Lenovo'nun, sunucuların yanı sıra masaüstü bilgisayarlarını da kilitlemesi bu açıdan mantıklıdır. Lenovo, üretim tesislerinde ve global tedarik zincirinde sıkı güvenlik standartları,

politikalar ve prosedürler uygulamaktadır. Lenovo'nun Kalite Mühendisleri, şirkete daha fazla denetim yetkisi vererek ve cihazlarına ait bileşenlerin güvenliğine ilişkin daha fazla bilgi sağlayarak şirketin Güvenilir Tedarikçilerini diledikleri zaman denetleme hakkını saklı tutmaktadır. ThinkShield da ayrıca tasarım düzeyinde güvenlik sağlamaktadır. Bunlar arasında, mobil kullanıcıların umuma açık yerlerde bulunması durumunda "görsel hacklemenin" minimuma indirilmesine yardımcı olmak için cihazlarına yerleştirilen gizlilik ekranlarının ve dizüstü bilgisayar kamera perdelerinin yanı sıra güvenli BIOS ve sabit yazılımlar yer almaktadır. ThinkShield, FIDO sertifikalı kimlik denetleyiciler ve Intel Authenticate ile entegrasyon sağlayarak (7'ye kadar kimlik doğrulaması faktörü sunarak) kullanıcıların kimliklerini ve kimlik bilgilerini korumak üzere tasarlanmıştır. ThinkShield, ayrıca USB bağlantı noktalarını yalnızca klavyelere ve işaretleme aygıtlarına yanıt verecek şekilde yapılandırarak çalışan, BIOS tabanlı Akıllı USB koruması özelliğine de sahiptir. Lenovo, ayrıca açık sunucu, depolama, ağ oluşturma ve sistem yönetimi platformlarının mevcut ve eski ortamlarla sorunsuz bir şekilde entegre olmasına da vurgu yapmaktadır. ITIC analistleri ile ilk ağızdan yapılan görüşmelerde Lenovo müşterileri, ThinkSystem platformunun temel güvenilirliğine ve istikrarına katkı sağlayan unsurlar olarak, devreye alma kolaylığını, entegrasyon kolaylığını ve geriye uyumluluğu göstermiştir. Lenovo kullanıcıları, satıcının pazar sonrası hizmetini ve desteğini de ayrıca övmüştür. Lenovo'nun sistem tasarımı, görev açısından kritik veritabanlarını, şirket uygulamalarını, büyük veri analitiğini, bulut ve sanallaştırılmış ortamları desteklemektedir. Bu her iki sistem de, sistemin hiçbir zaman raftan kaldırılmasına gerek olmaması nedeniyle "ağ üzerinde çok büyük bilgi işlem faaliyetlerini" desteklemek ve hizmet sunmayı kolaylaştırmak için gerekli olan alanı minimuma indiren yüksek yoğunluklu, raf için optimize edilmiş, kapaksız bir pakete hataya dayanıklılık ve yüksek düzeyde kullanılabilirlik açısından sayısız özellik dahil etmektedir. Lenovo, Ağustos 2020'de, Advanced Micro Devices AMD EPYC 702 serisi işlemcilerine dayanan Think System tek soketli sunucularının birkaç yeni modelini piyasaya sürdü. Lenovo'nun sunucu portföyüne eklenen yeni ürünler, özellikle video güvenliği, yazılım tanımlı depolama ve ağ istihbaratı gibi, müşterilerin gelişen, veri yoğun iş yüklerini ele almak üzere tasarlanmıştır. Güvenliğin kritik öneme sahip olduğu sanallaştırılmış ve ağ uç noktası ortamlarını da desteklemektedirler. Sonuç, verimi ve güvenliği kolay ölçeklenebilirlik ile dengelemeye büyük önem atfeden müşteriler için gücü verimlilikle bir araya getiren bir çözümdür. Lenovo, iki yeni ThinkSystem sunucusunun "tek soketli sunucu fiyatına çift soketli sunucu performansı sağladığını" ve müşterilerin yazılım lisanslama maliyetlerini %73'e kadar düşürme, TCO'yu ise %46'ya kadar azaltma potansiyeli olduğunu ileri sürmektedir.

Cisco UCS Security Anketinde Öne Çıkanlar

- **Cisco'nun Birleşik Bilgi İşlem Sistemi (UCS)**, iyi bir performans sergilemeye devam etmekte olup, ilk olarak ITIC'in 2020 Global Sunucu Donanımı, Sunucu İşletim Sistemi Yıl Ortası Güncelleme Anketi'nde elde ettiği sunucu başına 2,3 dakikalık aksama süresini korumuştur. Cisco'nun sunucuları, Ocak ayından Haziran 2021'in ortasına kadar sunucu başına 2,3 dakikalık aksama süresinde sabit kalmıştır. Birçok Cisco UCS sunucusunun güvenlik saldırılarının ön saflarında bulunan ağ uç noktasında konumlandırıldığı dikkate alındığında bu oldukça büyük bir başarıdır. Buna rağmen Cisco UCS anketine katılanların %87'si, güvenlik saldırılarını anında veya ilk 10 dakika içerisinde tespit edebildiklerini, diğerlerinden ayırabildiklerini ve devre dışı bırakabildiklerini belirtmiştir. Cisco UCS anketine katılanlar, ayrıca sunucuların her birinin son 18 ayda yedi (7) başarılı güvenlik saldırısı yaşadığını bildirmiştir. Cisco, veri ihlallerindeki bu artışa karşılık olarak Cisco

UCS Güçlendirme Kılavuzu'nu. Bu belge, ücretsiz indirilerek kullanılabilir. Belgede, ağ güvenliğini iyileştirmek için kullanıcıların Cisco UCS platformu cihazlarının güvenliğini sağlamalarına yardımcı olacak ayrıntılı bilgiler yer almaktadır. Ağ aygıtı işlevlerinin kategorize edildiği üç düzlem etrafında yapılandırılmış olan bu belge, Cisco UCS Yazılımının her bir özelliğine ve referanslarla ilgili belgelere genel bir bakış sağlar. Buna ilave olarak Cisco, toplam sahip olma maliyetini iyileştirmeye ve kurulum ve devreye alımı hızlandırmaya yönelik birçok yönetim ve performans yükseltmelerini piyasaya çıkarmıştır. Cisco, UCS sunucusunun, bir yandan sermaye giderlerini %40'tan daha fazla düşürürken, diğer yandan kablolamada %86'lık bir azalmaya ve (gün veya hafta yerine) birkaç dakika içinde bir tedarik hazırlığına olanak sağlayacağını ileri sürmektedir. Üreticiler, bileşenler arasında ve bileşenler içinde %100 uyumluluk konusunda kullanıcılara güvence vermektedir. Ayrıca yük dengeleme bir mesele değildir.

HPE Security Anketinde Öne Çıkanlar

- **HPE'nin Superdome** sunucu hattı, (Integrity ve Flex modeller dahil olmak üzere) ayrıca müşterilerinin %92'lik bir çoğunluğu için beş ve altı dokuzluk yüksek güvenilirlik sergilemektedir. HPE anket katılımcılarının %89'u, firmalarının güvenlik ihlallerini "Anında veya ilk 10 dakika içerisinde" tespit ettiklerini ve devre dışı bıraktıklarını belirtmiştir. ITIC anket verileri, HPE Superdome sunucularının her birinin son 18 ay içinde üç (3) başarılı güvenlik saldırısı yaşadığını göstermektedir. Bu, HPE donanım platformlarını en güvenli ilk beş sistem arasına sokmaktadır. Superdome portföyü, HPE donanımının kendiliğinden güçlü kararlılığından da faydalanmaktadır. HPE, güvenliği, özellik/performans inovasyonunu ve pazar sonrası teknik hizmet ve desteği en üst sıraya koymuştur. Tüm bunlar, giderek güvensiz, karmaşık ve birbirine bağlı bir hal alan Dijital Çağ'da kritik önem taşımaktadır. HPE, KOBİ'lerden en büyük çok uluslu işletmelere kadar kurumsal işletmelere oldukça iyi bir şekilde entegre olmuştur. HPE Superdome Flex Sunucusu, hayati öneme sahip iş yüklerini korumak için RAS yeteneklerine ve uçtan uca güvenlik özelliğine sahiptir. HPE Superdome Flex Sunucusu, örneğin 32 sokete kadar ölçeklenebilirlik sunar. Bu, önceki nesil sunucuların ölçeklenebilirliğine kıyasla 2,3 kat daha fazladır. Aynı zamanda bellek içi bir tasarıma sahip olup, tek bir platformda 768GB - 48 TB arası bir bellek kapasitesi özelliğine sahiptir. HPE Superdome Flex Sunucusu, 4 soketlik artışlarla 4'ten 32 sokete kadar esnek bir şekilde ölçeklenen modüler bir tasarıma sahiptir. HPE, Superdome Flex sunucusunun 4 soketli olarak görev açısından kritik iş yükleri için daha maliyet etkin bir giriş noktasına sahip olduğunu, önceki modellere kıyasla %45'e kadar daha düşük bir edinim maliyeti sağladığını da ifade etmektedir. HPE, ayrıca Superdome Flex Sunucusunun entegre edildiği RAS yeteneklerinin beş dokuzluk, yani %99,999 oranında bir tekli sistem kullanılabilirliği sağladığını ileri sürerek güvenilirliğin altını çizmektedir. HPE, Superdome Flex sunucusunun hataları tahmine dayalı işleyen Hata Analiz Motoru sayesinde insan hatalarını azalttığını da öne sürmektedir. Güvenlik ve insan hataları, birbiriyle yakından ilişkili iki konu olup, güvenliğe ve güvenilirliğe zarar vermektedir. Bu motor, herhangi bir insan müdahalesine veya "operatör desteğine" ihtiyaç olmadan donanım hatalarını tahmin etmekte ve kendi kendine bir onarım süreci başlatmaktadır. HPE'nin "Önce sabit yazılım" yaklaşımıyla İşletim Sistemi katmanında herhangi bir aksaklık yaşanmadan önce bellek hataları dahil olmak üzere sabit yazılım düzeyindeki hataları içermektedir. HPE, ayrıca HPE Serviceguard for Linux (SGLX) tarafından sunulan yüksek kullanılabilirlik ve olağanüstü durum kurtarma kümeleme çözümüyle Linux iş yükleri için süreklilik sağlar. Bu, şirketlerin herhangi bir uzaklıkta

bulunan fiziksel veya sanal ortamlardaki çok sayıda altyapı ve uygulama hatalarına karşı Linux ile çalışan sunucularını korumalarına olanak tanır.

Huawei Security Anketinde Öne Çıkanlar

- Genel merkezi Çin'in Şenzen şehrinde bulunan Huawei, son beş yılda yüksek donanımlı görev açısından kritik KunLun sunucusuyla ve genel amaçlı FusionServer x 86 tabanlı sunucularıyla dünya çapında ilk beşte yer alan sunucu donanımı satıcılarından biri haline gelmiştir. ITIC'in 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenilirlik Anketi ile ITIC 2021 Global Sunucu Donanımı Güvenlik Anketi'ne göre, Huawei KunLun ve Fusion Sunucuları da ilk üçteki en güvenilir ve güvenli donanım platformları arasında yer almaktadır. Huawei anket katılımcılarının %91'lik büyük bir çoğunluğu, BT ve güvenlik yöneticilerinin güvenlik ihlali girişimlerini "Anında veya 10 dakikanın altında bir sürede" tespit ettiğini ve devre dışı bıraktığını belirtmiştir. Huawei anket katılımcıları, KunLun ve Fusion sunucularının her birinin son 18 ay içinde 1,5 adet saldırı yaşadığını bildirmiştir. 2015 yılından bu yana Huawei, sunucularının gelişmiş özelliklerini, yapısal güvenliğini ve genel performansını güçlendirmiştir. Cisco, Fujitsu, HPE, IBM, Inspur, Lenovo gibi rakipler ve başka rakiplerle başarılı bir şekilde rekabet edebilmek için Huawei'nin sunucu ailesi, yüksek performanslı bir bilgi işlem (HPC) kullanmak üzere görev açısından kritik donanım için genel amaçlı raf ve blade sunucular dahil etmektedir. Huawei; Yapay Zeka, Büyük Veri Analitiği, Derin Öğrenme ve Makine Öğrenimi gibi gelişmekte olan bilişim yoğun uygulamaları desteklemek için sunucularını gelişmiş yeteneklerle donatmıştır. Huawei, "Proaktif Savunma Sistemi Nasıl Kurulur?" başlıklı bölümde yer alan en iyi uygulama belgeleri aracılığıyla güvenliğin altını çiziyor. Bunu daha akıllı bir tehdit algılama, tehdide müdahale, güvenlik operasyonları ve bakım sağlayan HiSec çözümü ile gerçekleştiriyor. Huawei, HiSec'in şirket ağlarına ve telekom altyapısına ait tehdit önleme kabiliyetlerini geliştirdiğini, dolayısıyla güvenliğin operasyon ve bakım (O&M) verimliliğini artırdığını ve O&M maliyetlerini azalttığını belirtmektedir. Ayrıca Huawei, veri merkezinde, bulutta ve ağda çeşitli sunucu çözümleri için birçok yeni güvenlik ürünü sunmaktadır.

Sonuçlar

Güvenlik; sunucu donanımının, sunucu işletim sistemlerinin ve kritik iş uygulamalarının güvenilirliğini ve kullanılabilirliğini olumsuz etkileyen bir numaralı sorundur. Tüm kuruluşlar, güvenliğe öncelik vermeli ve güvenlik ile ilgili riskleri kabul edilebilir bir seviyeye düşürmek için satıcılarıyla yakın çalışmalar içinde olmalıdır.

Sunucu aksama süresine eklenen her yeni saniye ve dakika ve uygulamaların kullanılamaması, iş operasyonlarını, çalışan verimliliğini ve geliri olumsuz etkilemektedir.

ITIC'in 2021 Global Sunucu Donanımı ve Sunucu İşletim Sistemi Güvenilirlik Anketi bulguları, IBM Z anabilgisayarı, IBM Power Systems ve hemen arkasından gelen Lenovo ThinkSystem,

Huawei KunLun ve HPE Integrity Superdome sunucularının, en güvenilir sunucu donanımı ürünleri olarak statülerini güçlendirmeye ve geliştirmeye devam ettiğini ortaya koymaktadır. IBM Z şirket platformu, kurumsal kullanıcılarının %93'ten daha fazlası için hataya dayanıklılık açısından altı ve yedi dokuzluk, yani %99,9999 ve %99,99999 oranında bir güvenilirlik sağlama konusunda tektir. Süper bilgisayarlar ve yüksek kullanılabilirliğe (HA) sahip donanımlar hariç hiçbir sunucu platformu, Z'nin güvenilirlik, kullanılabilirlik ve kusursuza yakın çalışma süresi ve güvenlik seviyesine ulaşmaya yaklaşamaz.

10 anket katılımcısından dokuzu, IBM Power Systems ve Lenovo ThinkSystem çözümlerinin her ikisinin de beş, hatta övgüyle bahsedilen altı dokuzluk, yani %99,999 ve %99,9999 oranında bir güvenilirlik ve kullanılabilirlik etkisi yarattığını doğrulamıştır. IBM Power Systems ve Lenovo ThinkSystem platformları, en kötü performansa sahip markasız Beyaz kutu sunucularına kıyasla 30 kata kadar daha güvenilir, 36 kata kadar ise daha maliyet etkindir.

Bir başka kayda değer başarı da, IBM ve Lenovo'nun ankette her bir güvenilirlik ve kullanılabilirlik kategorisinde birinci veya ikinci sırayı yakalamış olması veya her bir çalışma süresi, güvenlik veya yönetilebilirlik kriterinde birinci veya ikinci sırayı paylaşmış olmasıdır.

Güvenilirlik, statik değil değişkendir. Hiçbir sunucu, hiçbir tamamlayıcı parça (sabit sürücü, bellek ya da merkezi işlem birimi), işletim sistemi, uygulama, aygıt veya bağlanırlık mekanizması, içsel problemlerden veya arızalardan muaf değildir.

Sunucular, tüm ağ altyapısının ve genişletilmiş ağ ekosisteminin dayandığı temeldir. Sunucuların bozulması durumunda veri erişimi reddedilir. İş durur. Verimlilik durur. Gelir kaybı yaşanır. Tüm şirketlerin yaklaşık %88'i, verimliliği sağlamak ve kesintisiz veri erişimi sunmak için firmalarının sunucu donanımı, işletim sistemleri ve ana iş kolu uygulamaları için artık en az %99,99 oranında bir güvenilirliğe gereksinim duymaktadır. Yüksek güvenilirlik ve kullanılabilirlik, aynı zamanda şirketin günlük işlemlerini, veri varlıklarını ve fikri mülkiyetini (IP), çalışanların personel bilgilerini, iş süreçlerini ve gelir akışını da korumaktadır.

2021 yılı ve sonrasında, güvenlik, insan hataları ve son kullanıcılar, sunucuların, işletim sistemlerinin ve uygulamaların güvenilirliğini ve kullanılabilirliğini olumsuz etkileyebilecek en büyük tehditlerdendir.

Küresel COVID-19 pandemisinin ne kadar süreceğini kimse bilmiyor. Ayrıca pandemi resmen sona erse bile, negatif etkileri ve tesiri, özellikle güvenlik ve veri ihlali tehditleri açısından muhtemelen yıllarca devam edecektir.

Bu yeni normalde, organize hackerlar burada kalmaya devam edeceklerdir. Güvenlik açıklarından istifade etmek için bu pandemiden yararlanmayı sürdüreceklerdir. Hackerlar, kurum ve çalışan veri varlıklarını kar amaçlı olarak çalmak için her bir fırsatı değerlendirmeye devam edeceklerdir.

Sunucu güvenilirliği, kesintisiz veri ve uygulama erişimi ve güvenlik, her zaman gereklidir, fakat özellikle çalışmaların evden, eğitimin uzaktan yapıldığı COVID-19 döneminde bu gereklilik daha fazladır. Sunucu aksama süresine eklenen her yeni saniye ve dakika ve uygulamaların kullanılamaması, iş operasyonlarını, çalışan verimliliğini ve geliri olumsuz etkilemektedir.

Şirket sunucuları ve uygulamalarının önemli bir bölümü, artık sanallaştırılmış bulut ortamlarında ve ağ uç noktasında yer almaktadır. Pandemi 18 aydan uzun bir süre önce başladığından bu yana pek çok şirket, çalışanlarını evden çalışma sistemine geçirmiş; okul ve üniversiteler de uzaktan eğitimi benimsemiştir. Bu, tüm veri varlıklarının çalışabilirlik süresini ve kullanılabilirliğini sağlayacak olan kuruluşlar ve kendilerine aşırı görev atfedilen BT ve güvenlik yöneticileri üzerinde daha büyük bir baskı yaratmaktadır.

Güvenlik, son derece önemlidir. Satıcılar, entegre sunucu güvenliğini güçlendirmeye, hata tespit edildiğinde hızlıca onarım ve yama sağlamaya ve normatif bir kılavuzluk sağlamak için müşterilerle çalışmaya devam etmelidir. Kurumsal işletmeler, ayrıca veri merkezlerinde ve bulutta yer alan tüm sunucu ve ağ altyapısının ve temel iş uygulamalarının güvenilirliğini ve güvenliğini sağlamak için sorumluluk almalıdır. Şirketlerin, başta evden çalışanlar ve öğrenciler olmak üzere **tüm çalışanlar** için güçlü güvenlik politikalarını ve prosedürlerini uygulamaları ve yürürlüğe koymaları kritik önem taşımaktadır. Güvenilirlik ve güvenlik, ağ altyapısının esas temel unsurlarıdır. Kesintisiz günlük operasyonları ve güvenli veri erişimi sağlamak ve gelir akışını korumak için her ikisi de gereklidir.

ITIC'nin 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenlik Anketi, büyüklüğü ve dikey pazarı ne olursa olsun **tüm** kuruluşların, proaktif ve sürekli olarak her geçen gün daha sofistike ve hedefe yönelik bir özellik kazanan, giderek artan çeşitlilikte siber saldırıları tespit etmek ve önlemek için mücadele etmesinin gerekliliğine vurgu yapmaktadır.

Bu, tüm uygun güvenlik önlemlerinin uygulanması anlamına gelir. Üst düzey çalışanlardan daha düşük kademedeki sözleşmeli şirket çalışanlarına ve stajyerlere kadar **tüm şirket çalışanları** için güçlü bilgisayar güvenliği politikaları ve prosedürlerinin düzenlenmesi ve uygulanması mecburidir. Şirketler, güvenlik ürünlerinin satın alınması için yeterli miktarda bütçe ayırmalıdır ve gerekli zamanı ve uygun şirket içi ve şirket dışı üçüncü taraf kaynaklarını, son kullanıcılar ve BT yöneticileri ve güvenlik uzmanları için güvenlik araçları ve güvenlik eğitimi sağlamaya ayırmalıdır.

%100 dört dörtlük güvenlik diye bir şey yoktur. Ancak, güvenlik açığı testi ve güvenlik farkındalık eğitimiyle desteklenen çok katmanlı güvenlik savunmaları, veri ihlallerini ve fidye yazılım saldırılarını önleyebilir ve riski kabul edilebilir bir seviyeye düşürebilir.

Cisco, HPE ve Huawei'nin görev açısından kritik sistemleri de son derece iyi bir performans sergilemiş, küresel COVID-19 pandemisinin başlangıcından bu yana son 18 ay içerisinde herhangi bir güvenilirlik düşüşü yaşamamıştır. Cisco, HPE ve Huawei sunucuları, çekirdek donanımın içsel dayanıklılığına dayanarak IBM ve Lenovo ile neredeyse başa baş bir güvenilirlik derecesi elde etmiştir.

Cisco'nun UCS sunucuları, ITIC'in en son 2021 Global Sunucu Donanımı, Sunucu İşletim Sistemi Güvenilirlik Anketi Yıl Ortası Güncellemesi'nde güvenilirlik kazanımlarını sürdürmüştür. 2019 yılından bu yana Cisco UCS sunucu mağazaları, ITIC'in önceki güvenilirlik anketinde donanım hatalarından kaynaklanan aksama süresinin dört dakikanın biraz üzerinde (4,1 dakika) bir süreden sunucu başına/yılda iki dakikanın biraz üzerinde (2,3 dakika) bir süreye gerilediğini bildirmiştir. Bu,

son derece önemlidir. Cisco'nun UCS sunucularının önemli bir bölümü, uzun zamandır ekosistemin en savunmasız noktaları arasında olduğu düşünülen ağ uç noktasında devreye alınmaktadır.

Hiçbir satıcı rehavete kapılamaz. Dünya çapında global sunucu donanım pazarında yoğun bir rekabet vardır. Bu alıcı piyasasıdır ve öyle kalacaktır. Birçok şirket, özellikle KOBİ'ler, satın alma ile ilgili kararlarını fiyata göre alırken, şirketlerin önemli bir bölümü entegre güvenlik, gelişmiş yönetim, yapay zeka ve büyük veri analitiği işlevselliği ile donatılmış daha sağlam bir donanım satın almayı tercih etmektedir.

Anket verileri, kurumsal şirketlerin pazar sonrası satıcı teknik hizmetleri ve desteğine son derece önem verdiğini göstermektedir. Şirketler, problem çıkması durumunda satıcıların hızlı bir şekilde harekete geçmesini ister. Satıcılar, en uygun performansı ve kullanılabilirliği yakalamak ve devam ettirmek için sistem yapılandırmaları ve ürün yaşam çevrimleri için müşterilere gerçekçi öneriler ve normatif bir kılavuzluk sunmalıdır.

ITIC, her zaman olduğu gibi, satıcıların yama, onarım ve güncellemeleri zamanında ulaştırma ve potansiyel olarak performansı etkileyebilecek bilinen herhangi bir uyumsuzluk sorunu ile ilgili olarak ellerinden geldiğince müşterilerini bilgilendirme sorumluluğunu taşımalarını sağlamaktadır. Satıcılar ayrıca müşterilere karşı dürüst olmalı ve yedek parçaların teslimatında yaşanan sorunlar veya gecikmeler konusunda onları bilgilendirmelidir.

Öneriler

Hiçbir sunucu platformu, sunucu işletim sistemi veya iş uygulaması kusursuz bir güvenlik sağlamaz. Ancak, en güvenilir sunucu platformları arasında yer alan IBM, Lenovo, Huawei, HPE ve Cisco, en yüksek seviyede içsel güvenlik sağlamaktadır. Bu, müşterilerin en büyük ölçek ekonomisi elde etmelerine ve hassas IP ve veri varlıklarını korumalarına olanak sağlar. Güvenlik, yüzde elli elli bir önermedir. Satıcıların güçlü bir güvenlik sağlaması gerekirken, şirketler kendi sunucularının ve kapsayıcı ağ altyapısının güvenilirliğini sağlamaktan sorumludur. ITIC'in şirketlere şiddetle tavsiye ettiği hususlar aşağıdadır:

- **Envanter yapın.** Ağınızda ne olduğunu bilin. Bu, veri merkezi, uzak ofisler, genel, özel ve hibrit bulutlar, nesnelerin interneti (IoT) cihazları ve ağ uç noktası dahil olmak üzere tüm ağ ekosistemi genelindeki ***tüm*** sunucuların, önemli ana iş kolu uygulamalarının, ağ aygıtlarının (güvenlik duvarları, yönlendiriciler) kataloglanması anlamına gelir.
- **Uygun boyutlusunucu donanımı**. Sunucu donanımı, artması beklenen iş yükleri ve daha büyük uygulamaların yanı sıra mevcut iş yüklerini de barındıracak kadar sağlam olmalıdır.

- **Sunucu donanımını düzenli olarak değiştirin, güçlendirin ve yenileyin.** Bu, sistemin sağlığını korumak ve en yüksek sistem performansına ulaşmak için gerekli yama, güncelleme ve güvenlik onarımlarını ***ihtiyaç oldukça*** güncel tutmak anlamına gelir.
- **Yazılımı güncelleyin.** Mümkünse, sunucu işletim sistemlerinde ve temel sunucu tabanlı uygulamalarda asla iki revizyondan fazla revizyonun gerisinde kalmayın.
- **Güçlü güvenlik politikaları ve prosedürleri uygulayın.** Her büyüklükteki ve tüm dikey pazar segmentlerindeki şirketlerin geniş çaplı kurumsal güvenlik politikaları ve prosedürleri oluşturması zorunludur. Bu politika ve prosedürleri tüm çalışanlara basılı kopya ve e-posta ile dağıtın. Bilgisayar güvenliği politikaları, genel kurumsal yönergelerin ayrılmaz bir parçası olmalı ve birinci, ikinci ve üçüncü suçlar açısından belirli hüküm ve cezalar içermelidir. Şirketlerin de tüm çalışanların cinsel taciz eğitimine benzer şekilde zorunlu bilgisayar güvenliği eğitimine katılmalarını sağlamaları tavsiye edilmektedir.
- **Hizmet Seviyesi Anlaşmalarını (SLA) Yakından İzleyin.** Mutabık kalınan güvenilirlik seviyeleri sunmak için şirketinizin donanımının, yazılım satıcılarının ve bulut satıcılarının SLA'ların koşullarını sağlaması veya bu koşulları aşmasını sağlamak amacıyla SLA sözleşmelerine dikkatinizi verin.
- **Güvenlik açığı testi gerçekleştirin.** Birkaç örnek vermek gerekirse, fidye yazılım, e-dolandırıcılık saldırıları ve CEO sahtekarlığı gibi her türden güvenlik saldırılarında ve veri ihlallerinde sürekli bir artış olması göz önünde bulundurulduğunda, tüm kurumsal şirketlerin en az yılda bir kez ve gerektiğinde güvenlik açığı testi uygulaması gerekir. ITIC, şirketlerin bağımsız üçüncü taraf uzmanlarla çalışmasını tavsiye etmektedir.
- **Bir Yönetişim ve İyileştirme Planı Oluşturun.** Firmanızın başarılı bir güvenlik saldırısı yaşaması halinde bir iyileştirme ve yönetişim planının yürürlükte olmasını sağlayın. Bir veri ihlali veya ağ kesintisi olması durumunda kimin sorumlu kişi olduğu ile ilgili bir hiyerarşi belirleyin. Yönetişim ve İyileştirme planı, ayrıca belirli grup ve kişilere belirli görevler atamalı ve tayin etmelidir. Planın, tüm satıcılar ve üçüncü taraf hizmet sağlayıcıları için uygun iletişim bilgilerini içerdiğinden de emin olun.
- **Güvenlik ve BT Yöneticilerine Eğitim ve Sertifika Verin.** Güvenlik ve BT uzmanlarının yeterli eğitimi almasını ve gerekli güvenlik sertifikalarına sahip olmasını sağlayın.
- **Son kullanıcılara eğitim verin.** En son E-posta dolandırıcılığı, e-dolandırıcılık ve fidye yazılım tehditleri konusunda sözleşmeli çalışanların ve geçici işçilerin yanı sıra son kullanıcıların da yeterli güvenlik farkındalığı eğitimi almasını sağlayın.

Metodoloji

ITIC'in *2021 Global Sunucu Donanımı Güvenliği Güvenilirlik Anketi*, Ocak 2021'den Haziran 2021'in ortasına kadar dünya çapında binden fazla şirketteki üst düzey yöneticilere ve BT Müdürlerine anket yapmıştır. Bağımsız Web tabanlı ankette, çoktan seçmeli sorular ile bir Paragraf sorusu yer almıştır. ITIC, nesnelliği korumak için hiçbirsatıcı sponsorluğunu kabul etmemiştir. Hiçbir anket katılımcısı ücret almamıştır. ITIC analistleri, ayrıca değerli anektodsal veriler elde etmek ve güvenlik açıkları ve veri ihlallerinin şirket sunucusunun ve ağ altyapısının güvenilirliğine olan etkisi hakkında daha kapsamlı bir fikir edinmek ve kavramsal bilgiler elde etmek için iki düzine kadar ilk ağızdan müşteri görüşmesi gerçekleştirmiştir. Katılımcılar arasında üst yöneticiler, BT ve güvenlik yöneticileri ve son kullanıcılar yer almıştır. ITIC, kurcalamanın önüne geçmek ve aynı tarafların birden fazla yanıt vermesini engellemek için kimlik doğrulama ve izleme mekanizmalarını kullanmıştır.

Anket Demografisi

ITIC, araştırma için her büyüklükten ve 28 dikey pazar içerisinden 1,100 şirkete anket yapmıştır. Her büyüklükteki şirketler, iyi bir şekilde temsil edilmiştir. Katılımcılar, 50'den az çalışanı olan küçük ve orta boy işletmelerden (KOBİ'ler) 100.000'in üzerinde çalışanı olan çok uluslu işletmelere kadar farklı özellikteki şirketlerden gelmiştir.

Tüm pazar sektörleri eşit olarak temsil edilmiştir: Bir ila 100 çalışanı olan KOBİ'ler, katılımcıların %24'ünü oluşturmuştur. 101 ila 1.000 çalışanı olan küçük ve orta boy işletmeler (KOBİ'ler), katılımcıların %28'ini oluşturmuştur. Ankete katılanların geri kalan %43'ü, 1.001 ila 100.000'den fazla çalışanı olan büyük şirketlerden gelmiştir. Ankete katılanlar, 49 farklı dikey pazardan gelmiştir. Katılımcıların yaklaşık %61'i Kuzey Amerika'dan gelmiştir; %39'u ise Avrupa, Asya, Avustralya, Yeni Zelanda, Orta/Güney Amerika ve Afrika genelinde 22 ülkeden gelmiş olan uluslararası müşterilerdir.

Ekler

Bu bölüm, bu Raporda bahsi geçen çeşitli ITIC istatistiklerine ve anketlere bağlantılar sağlamaktadır.

ITIC Web Sitesi ve anket verilerine ve web günlüğü gönderilerine bağlantılar:

https://itic-corp.com/blog/2019/11/ibm-lenovo-hpe-and-huawei-servers-maintain-top-reliability-rankings-cisco-makes-big-gains-ibm-lenovo-hardware-up-to-24x-more-reliable-28x-more-economical-vs-least-reliable-white-box-servers/

https://itic-corp.com/blog/2019/11/1678/

https://itic-corp.com/blog/2019/08/itic-poll-human-error-and-security-are-top-issues-negatively-impacting-reliability/

https://itic-corp.com/blog/2019/08/itic-2019-server-reliability-mid-year-update-ibm-z-ibm-power-lenovo-system-x-hpe-integrity-superdome-huawei-kunlun-deliver-highest-uptime/

http://itic-corp.com/blog/2017/07/ibm-z14-mainframe-advances-security-reliability-processing-power/

http://itic-corp.com/blog/2017/06/ibm-lenovo-servers-deliver-top-reliability-cisco-ucs-hpe-integrity-gain/