Bilgi Sistemleri Güvenliği

İnternet ilk çıktığı zamana göre dramatik bir biçimde değişmiştir. Az sayıda üniversitenin ve devlet kurumlarının kullandığı bir araçtan üç milyardan daha fazla kullanıcıya sahip dünya çapında bir ağa doğru büyümüştür. Büyürken de insanların haberleşme ve iş yapma biçimlerini değiştirmiş, birçok fırsat ve fayda getirmiştir. Bugün internet büyümeye, yeni ve değişik yollarla genişlemeye devam etmektedir. İnternet başladığında, bu ağa bağlı cihazların çoğunluğu gerek kişisel kulanım için gerekse şirket içi kullanım için olan bilgisayarlardan oluşuyordu. Buna karşın, son yıllarda, bilgisayarların yanı sıra, akıllı telefonlar, akıllı arabalar, ev aletleri, yiyecek otomatları ve akıllı binalar gibi artan çeşitlilikte cihazlar internete bağlanmakta ve veri paylaşabilmektedir.

Bugün internet olarak bildiğimiz şey hızla Nesnelerin İnternetine (Internet of Things-loT) doğru genişlemekte ve günbegün yaşantımızı etkilemektedir. İnternet 1969'da resmi olarak başlamış olsa da insanların internete bağımlı hale gelmesi yenidir. Bugün, insanlar günlük yaşamlarının normal bir parçası olarak internet ve siber uzay ile etkileşimde bulunmaktadır. Bu etkileşim kişisel kullanım ve iş kullanımını içermektedir. Kullanıcılar şimdilerde hem özel verilerinin güvenliği hem de iş verilerinin güvenliğini düşünmek zorundadır. Güvenlik tehditleri internete bağlı cihazlarınızın kişisel ya da iş kullanımından kaynaklanabilmektedir. Zeki ve saldırgan olan siber suçlular, teröristler ve dolandırıcılar gölgelerde gizlenmektedir. Bilgisayarlarınızı ya da cihazlarınızı internete bağlamak onları anında saldırılar için hedef konumuna sokmaktadır. Bu saldırılar kurbanlarda hüsran ve sıkıntılar doğurmaktadır. Kişisel bilgileri çalınmış kimlik hırsızlığına (identity theff) maruz kalmış herkes bu sıkıntılara şahitlik edebilmektedir. Daha kötüsü, bilgisayarlar ve ağa bağlı cihazlara yapılan saldırılar e-ticaret'e (e-commerce) dayalı ulusal ve uluslararası ekonomi için tehdit oluşturmaktadır. Daha da önemlisi, siber saldırılar ulusal güvenliği tehdit etmektedir. Örneğin, terörist saldırganlar elektrik şebekelerini çökertebilmekte ve askeri iletişimi kesintiye uğratabilmektedir.

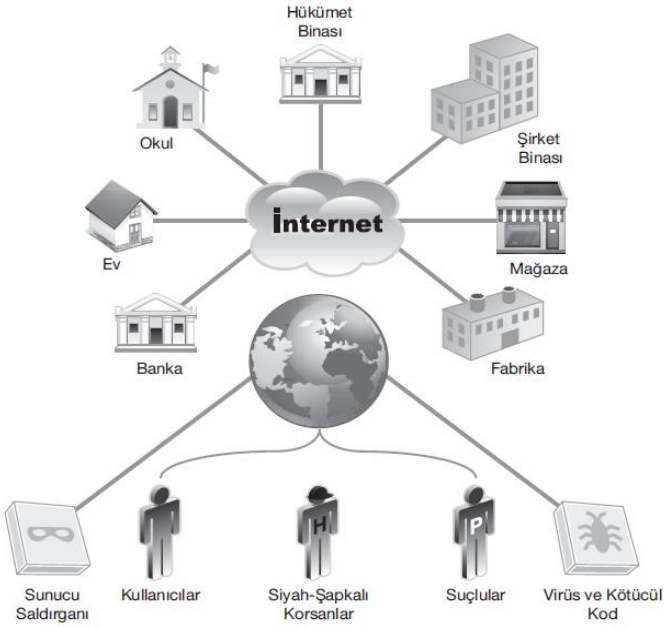
Dünyanın bilgisayar güvenliğinden anlayan ve bilgisayarları ve ağları suçlular ve teröristlerden koruyabilecek insanlara ihtiyacı vardır. Her şey hassas verilerinizin güvenliğini sağlamakla ilgilidir. Hassas veriniz varsa, onu korumak zorundasınız. Başlamanız için; bu bölüm, siber saldırıları anlamak ve durdurmak için gerekli bilgi sistemleri güvenliği kavramlarının ve terimlerinin tanımlarını size sunmaktadır.

Günümüzün interneti 2 milyardan fazla kullanıcılı dünya çapında bir ağdır. Dünya üzerindeki neredeyse her hükümeti, işyerini ve kuruluşu içermektedir. Fakat aynı ağda bu kadar çok kullanıcıya sahip olmak, tek başına, interneti oyun kurallarını değiştiren bir yenilikçi yapmak için yeterli değildir. Bu kullanıcıların bilgisayarlar üzerinden belgeleri ve kaynakları birbirine bağlamak için bir tür mekanizmaya ihtiyaçları vardır. Bir başka deyişle, bilgisayar A'da bulunan bir kullanıcı bilgisayar B üzerindeki bir dosyayı açmak için kolay bir yola ihtiyaç duymaktadır. Bu ihtiyaç, ağda bulunan makineler üzerindeki belge ve kaynakların nasıl ilişkilendirileceğini tanımlayan bir sistemi doğurmuştur. Bu sistemin adı World Wide Web (WWW)'dir. Siz onu siber uzay (cyberspace) veya kısaca Web olarak biliyor olabilirsiniz. Web'i şöyle düşünün: İnternet iletişim ağlarını birbirlerine bağlamaktadır. Web, ağa bağlı bilgisayarlar üzerinde bulunan web sitelerinin, web sayfalarının ve sayısal içeriğin bağlantısıdır. Siber uzay, dünya çapındaki bu elektronik erişim alanı içindeki erişilebilir kullanıcılar, ağlar, web sayfaları ve çalışan uygulamaların tümüdür.

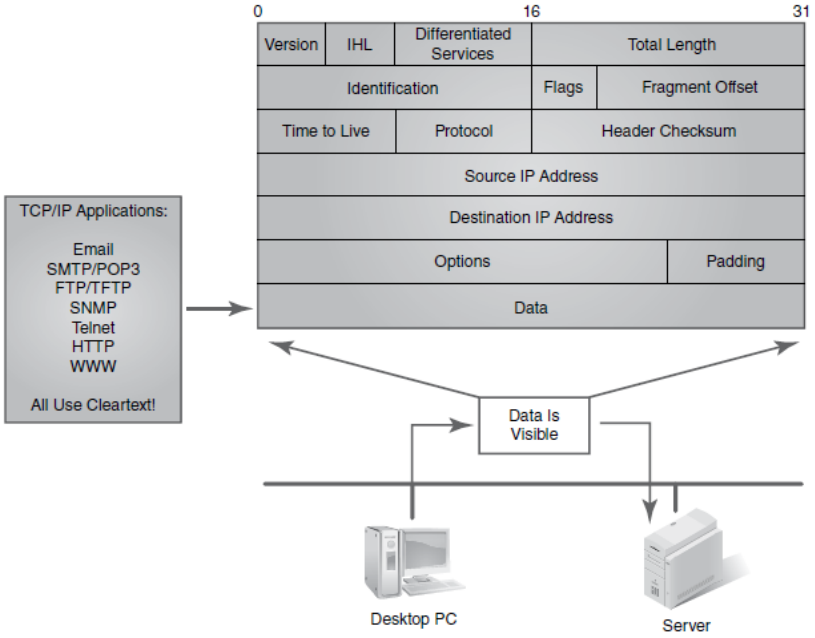
Siber uzaya bağlandığınız zaman, ne yazık ki, aynı zamanda kapıyı bir sürü kötü insana da açmış olursunuz. Bu insanlar, sizi bulmak ve verilerinizi çalmak istemektedirler. Kullanıcıları hayatlarının her alanında destekleyen bir Nesnelerin İnterneti (IoT) yaratan ve internete bağlanan her bilgisayar ya da cihaz tehlikededir. Dış uzay gibi, olgunlaşan internet de yeni bir sınır boyudur. Bir internet hükümeti veya merkezi otoritesi yoktur. İnternet zorluklarla ve kuşkulu davranışlarla doludur: Bu kuşkulu davranışlar sadece son üç yılda gördüğümüz veri ihlalleri dikkate alındığında bile bellidir. Amerika Birleşik Devletleri'nde, resmi ve özel sektörler yetkisiz erişimler ve veri ihlali saldırıları ile tehlikeye düşürülmüştür. Bu son saldırılar, kişiler, organize siber suçlular ve diğer ülkelerden saldırganlar tarafından yapılmıştır. ABD çıkarlarına karşı yapılan siber saldırıların sayısı artmaktadır.

Nesnelerin Interneti'nin (loT) şimdi, kişisel cihazlar, ev cihazları ve motorlu taşıtları da ağa bağlamasıyla, çalmak için her zamankinden daha çok veri bulunmaktadır. Tüm kullanıcılar bilgilerini saldırganlardan korumak zorundadırlar. **Siber güvenlik** *(cybersecurity)* ulusal güvenliğini korumak isteyen her hükümetin görevidir. Veri güvenliği bilgi varlıklarını ve hassas verilerini (örn., Vatandaşlık Numaraları, kredi kartı

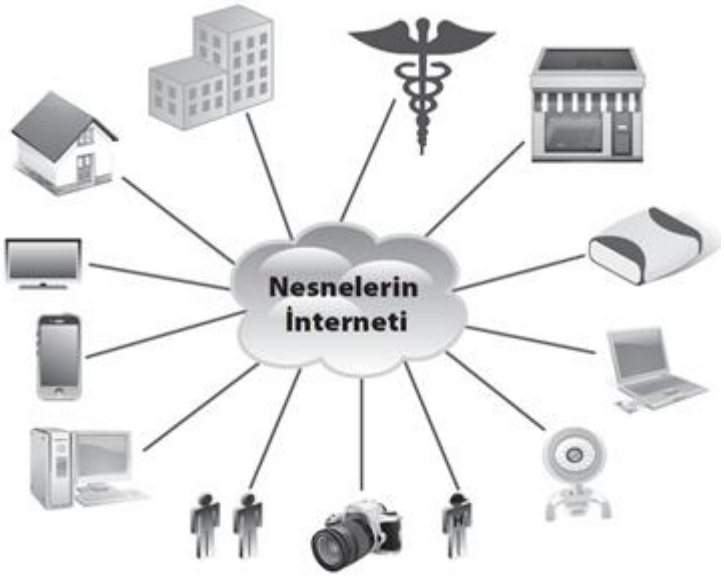
numaraları, ve benzeri) koruması gereken her kuruluşun sorumluluğudur. Ve kendi sahip olduğumuz veriyi korumak hepimizin görevidir. **Aşağıdaki şekil** bu yeni sınır boyunu göstermektedir.



Siber uzayı oluşturan bileşenler otomatik olarak güvenli değildir. Bu bileşenler kablolama, fiziksel ağlar, işletim sistemleri ve bilgisayarların internete bağlanmak için kullandığı yazılım uygulamalarını içermektedir. Sorunun kalbinde **iletim Kontrol Protokolü/İnternet Protokolü** *(Transport Control Protocol / Internet Protocol - TCP/IP)* haberleşme protokolündeki güvenlik eksikliği yatmaktadır. Bu protokol internet üzerindeki bilgisayarların haberleşmek için en çok kullandıkları dildir. **Protokol** haberleşme için kullanılan bir kurallar ve yöntemler listesidir. TCP/lP tek bir protokol değildir fakat bir ağ üzerinden haberleşmek için geliştirilmiş bir protokol takımıdır. En önemli iki protokolünün adını taşıyan, TCP/IP'de takımı oluşturan protokoller herhangi iki bilgisayarın haberleşmesine izin vermek için birlikte çalışmaktadırlar. TCP/IP ağa bağlı bilgisayarlar arasında veri göndermek için iletileri öbeklere veya paketlere ayırmaktadır. Sorun, her IP paketindeki verinin herkesin kullanabileceği basit yazılımlar ile okunabilir durumda olmasıdır. Verinin bu okunabilir durumu **açık metin** *(clear text – plain text)* olarak bilinmektedir. Bu, veriyi daha güvenli kılmak için bir TCP/IP paketi içinde gönderilen veriyi gizlemeniz ya da şifrelemeniz gerektiği anlamına gelmektedir. **Aşağıdaki şekil** TCP/IP paket yapısı içerisindeki veri alanlarını göstermektedir.



Bütün bunlar şu soruyu akla getirmektedir: İnternet bu kadar güvensiz ise neden herkes internete bu kadar istekle bağlanmıştır? Yanıt, Web'in 1990'ların ortalarından 2000'li yılların başlarına kadar yaşanan muazzam büyümesidir; internete bağlanmak herkese Web'e ve Web'in çok sayıdaki kaynaklarına anında erişim imkânı vermiştir. Kolay evrensel bağlantının cazibesi bağlanma taleplerinin itici gücü olmuştur. Bu talep ve ardından gelen büyüme, yüksek hızlı iletişim maliyetlerini düşürmeye yardımcı olmuştur. Ev halkı, ticarethaneler ve hükümetler uygun fiyatlı yüksek hızlı internet erişimine sahip olmuştur. Kablosuz ve hücresel bağlantıların giderek daha yaygın ve uygun fiyatlı olması ile bağlı kalmak, nerede olursanız olun ve hangi cihazla bağlanmış olursanız olun, daha kolay olmuştur. **Aşağıdaki şekil** IoT'nin dünyayı nasıl sayısal olarak bağlanmış bir bütün haline getirdiğini göstermektedir. Bir bilgisayar korsanı veya saldırgan herhangi bir IP-bağlı cihaza yetkisiz erişim sağlayabileceğinden, IoT risk, tehdit ve güvenlik açığı sorunlarını büyütmektedir. Bir IP-bağlı cihaza erişim bir kez sağlandığında, veriler çalınabilmekte veya saldırgan isterse bu cihaz hasara uğratılabilmektedir. Bilgisayar korsanlarının bu "karanlık kötü adam *(dark villain)"* doğası onların "siyah şapkalılar" olarak etiketlenmesinin sebeplerindendir.



İnternetin büyümesi aynı zamanda kuşaklararası farklardan da beslenmektedir. **Y Kuşağı** kültürü, "baby boomers" (2. Dünya savaşını izleyen yıllarda doğanlar) kuşağının emekli olmaya başlaması ile öne çıkmaktadır. Bu yeni kuşak, cep telefonları, **akıllı telefonlar** *ve "*daima-bağlı *(always-on)"* İnternet erişimi ile yetişmiştir. Bu cihazlar gerçek zamanlı iletişim sağlamaktadırlar. Günümüzün kişisel iletişimi IP-üzerinden-ses iletimi *(Voice over IP-VoIP),* metin mesajlaşma, anlık mesajlaşma *(Instant Messaging* - lM), ve sohbetin yanı sıra sesli ve görüntülü video konferansı da içermektedir. Bu gerçek zamanlı, Oturum Başlatma Protokolü-etkin (Session Initiation Protocol (SIP)-enabled) uygulamalar genel olarak **birleşik iletişim** *(unified communication)* olarak bilinmektedir. Birleşik iletişim uygulama örnekleri Google Hangouts anlık mesajlaşma servisi, Yahoo! Messenger, WebEx, GoToMeeting, ve Skype for Business'in çevrimiçi buluşma özelliklerini içermektedir.

Bu sırada, bir **bilgi güvenliği** *(information security)* savaşı şiddetle sürmektedir. Siber uzay savaş alanıdır ve düşmanlar hali hazırda kale duvarlarının içindedirler. İşi daha da kötü hale getiren ise düşmanın hem yerel alan ağlarında hem de dünyanın öbür ucunda olması yani her yerde olmasıdır. Düşman sizin hassas verinizi aramaktadır. Bu nedenle, saldırgan için oyunun adı yetkisiz erişim sağlamaktır. **Yetkisiz erişim** *(unauthorized accese)* saldırganın, sizin yetkilendirilmiş oturum açma kimliğinizi ve parolanızı sizin izniniz olmadan elde etmesi anlamına gelmektedir. Saldırgan, size ait bu giriş bilgilerini kullanarak, erişim izniniz olan tüm sistem ve uygulamalara erişim hakkı kazanmaktadır.

Eğer yetkisiz erişim sağlandı ise, yasal kullanıcının erişim denetimlerine bağlı olarak, hassas verilere erişilebilmekte ve indirilebilmektedir. Bu sebeple, bilgi teknolojisi altyapıları uygun güvenlik kontrollerine ihtiyaç duymaktadır. Bu güvenlik savaşı, bilgi sistemleri güvenliği ve bilgi güvencesi *(information assurance)* uzmanları - güvenlik ve ticari çıkarları savunmak için yeni bir siber savaşçı türü için muazzam bir talep yaratmıştır.

Riskler, Tehditler ve Zafiyetler

Bu bölüm siber uzayın tehlikelerini ortaya koymakta ve bu tehlikelerle nasıl bahşedileceğini tartışmaktadır. **Bilgi sistemlerinde** *(information systems) ve* BT altyapılarında sıklıkla karşılaşılan tehlikelerin nasıl tanınacağını ve onlarla nasıl savaşılacağını açıklamaktadır. Bilgisayarların nasıl daha güvenli hale getirileceğini anlamak için, önce riskler, tehditler ve zafiyetler kavramlarını anlamanız gerekmektedir.

Risk bir varlığa (asset) kötü bir şey olacak olması olasılığıdır. Bir varlığa etki edecek bazı olaylara maruz kalma düzeyidir. Bu varlık, BT güvenliği bağlamında, bir bilgisayar, bir veritabanı veya bir bilgi parçası olabilmektedir. Aşağıda bazı risk örnekleri verilmektedir:

- Veri kaybı
- Bir afetin binanızı yıkması sebebiyle uğradığınız iş kaybı
- Yasa ve yönetmeliklere uymamak

Tehdit (threat) bir varlığa hasar verebilecek herhangi bir eylemdir. Bilgi sistemleri hem doğal hem de insan kaynaklı tehditlerle karşı karşıya kalmaktadır. Sel, deprem ve şiddetli fırtına tehditleri, kuruluşların afetlerin verdiği hasardan kurtulmak ve işlerine devam edebilmek için planlar yaratmalarını gerektirmektedir. Bir **iş sürekliliği planı** *(business continuity plan – BCP)* bir kuruluşun işlevlerine, kuruluşun işini devam ettirebilmesi için o işleve ne kadar ihtiyaç duyduğuna göre öncelik atamaktadır. Bir **afet kurtarma planı** *(disaster recovery plan - DRP)* bir işyerinin yangın veya fırtına gibi bir büyük felaketten sonra nasıl tekrar ayakları üzerine kalkabileceğini tanımlamaktadır. Bir bilgisayar sistemi insan kaynaklı tehditler virüsler, kötücül kodlar ve yetkisiz erişimi içermektedir. Bir **virus,** bir sistem, uygulama veya veriye zarar vermek amacıyla yazılmış bir bilgisayar programıdır. **Kötücül kod** *(malicious code)* veya **kötücül yazılım** *(malware)* örneğin bir sabit diski silmek gibi spesifik bir eyleme neden olmak için yazılmış bir bilgisayar programıdır. Bu tehditler kişilere, işyerlerine veya kuruluşlara zarar verebilmektedir.

Bir zafiyet/güvenlik açığı *(vulnerability)* bir tehdidin gerçekleşmesine ya da bir varlık üzerinde etki etmesine olanak sağlayan bir zayıflıktır. Zafiyetin ne olduğunu anlamak için ateş yakmayı düşünün. Ateş yakmak mutlaka kötü bir şey değildir. Izgarada yemek pişiriyorsanız, ateş yakmanız gerekmektedir. Izgara, ateşi içinde tutacak şekilde tasarlanmıştır ve uygun kullanılırsa tehlike oluşturmamaktadır. Öte yandan, bir bilgisayar veri merkezi içinde ateş yakmak büyük olasılıkla hasara yol açacaktır. Ateş, ızgara için bir zafiyet değildir fakat bilgisayar veri merkezi için bir zafiyettir. Bir tehdit tek başına her zaman hasara neden olmaz; o tehdidin gerçekleşebilmesi için bir *zafiyet* olmalıdır.

Zafiyetler genellikle yasal yükümlülüklerle sonuçlanabilmektedir. Bir tehdidin gerçekleşmesine sebep olan bir zafiyet soruşturma ve yasal işleme yol açmaktadır. Bilgisayarlar faydalı olmak ve bir işe yaramak için yazılımları çalıştırmak zorundadır ve yazılımları da insanlar yazdığı için yazılım programları kaçınılmaz olarak hatalar (bug) içermektedirler. Bu nedenle, yazılım satıcıları, yazılımlarından kaynaklanan zafiyetlerin getireceği yasal yükümlülüklerden kendilerini korumak için **Son Kullanıcı Lisans Sözleşmesini** *(End-User License Agreemert* - **EULA)** kullanırlar. Bu sözleşme kullanıcı paketi açıp yazılımı kurduğunda devreye girmektedir. Tüm yazılım satıcıları EULA sözleşmelerini kullanmaktadır. Bu, BT sistemlerini ve verileri koruma yükünün dahili *(internaty)* bilgi sistemleri güvenliği uzmanlarına ait olduğu anlamına gelmektedir.

Son Kullanıcı Lisans Sözleşmeleri (EULA'lar)

EULA'lar kullanıcı ile yazılını satıcısı arasındaki lisans sözlenmeleridir. EULA'lar yazılım satıcılarını kusurlu yazılım davranışları sebebiyle ortaya çıkacak tazminat taleplerinden korumakladır. EULA'lar genellikle garanti koşullarını içermektedir. Bu yazılım satıcılarının, bilgisayar korsanlarının kötüye kullanabileceği yazılım hatalarından *(bugs) ve* zayıflıklarından doğan yükümlülüklerini sınırlamaktadır.

Aşağıda Microsof'un EULA'sından, şirketin yazılımı için sadece "sınırlı" garantiler verdiğini ifade eden bir alıntı verilmektedir. Bu EULA ayrıca, yazılım ürününün "olduğu gibi ve tüm hatalarıyla" sunulduğunu bildirmektedir.

> *DISCLAIMER OF WARRANTIES. THE LIMITED WARRANTY THAT APPEARS ABOVE IS THE ONLY EXPRESS WARRANTY MADE TO YOU AND IS PROVIDED IN LIEU OF ANY OTHER EXPRESS WARRANTIES (IF ANY) CREATED BY ANY DOCUMENTATION OR PACKAGING. EXCEPT FOR THE LIMITED WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW,*

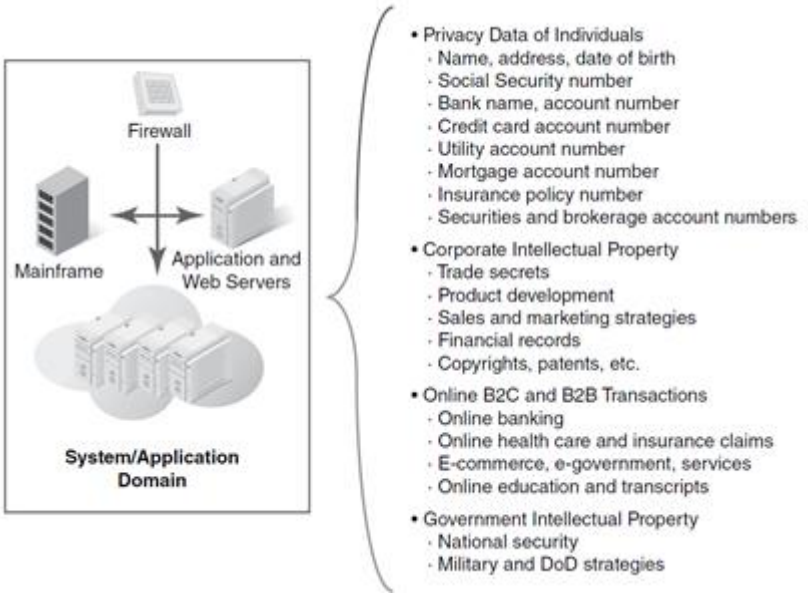
MICROSOFT AND ITS SUPPLIERS PROVIDE THE SOFTWARE PRODUCT AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS....

Microsoft'un EULA'sı ayrıca kendi mali yükümlülüklerini, yazılımın fiyatı ya da 5 dolar ile hangisi daha büyükse, sınırlamaktadır.

LIMITATION OF LIABILITY. ANY REMEDIES NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES), THE ENTIRE LIABILITY OF MICROSOFT AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS EULA AND YOUR EXCLUSIVE REMEDY FOR ALL OF THE FOREGOING (EXCEPT FOR ANY REMEDY OF REPAIR OR REPLACEMENT ELECTED BY MICROSOFT WITH RESPECT TO ANY BREACH OF THE LIMITED WARRANTY) SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR U.S.$5.00. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS (INCLUDING SECTIONS 9, 10 AND 11 ABOVE) SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

Bilgi Sistemleri Güvenliği Nedir?

Güvenlik (security) terimini parçalara ayırarak tanımlamak daha kolaydır. Bir bilgi sistemi, kişiler veya kuruluşlar için bilgi toplamak, işlemek ve depolamak için birlikte çalışan, donanım, işletim sistemi ve uygulama yazılımından oluşmaktadır. Bu nedenle, **bilgi sistemleri güvenliği** *(information systems security)* bilgi sistemlerini ve üzerlerindeki veriyi koruyan faaliyetler topluluğudur. Birçok ulusal ve uluslararası yasa bu tür güvenlik güvencelerini şu anda zorunlu kılmaktadır. Kuruluşlar bu ihtiyacı doğrudan karşılamak durumundadırlar. **Aşağıdaki şekilde** bir BT altyapısında yaygın olarak bulunan bilgi türlerini incelemektedir.



ABD Uyum (Compliance) Yasaları Bilgi Sistemleri Güvenliği İhtiyacının İtici Gücüdür

Siber uzay, insanlar ve kuruluşlar için yeni tehditler getirmektedir. Kişiler kendi mahremiyetlerini korumalıdır. İşletmeler ve kuruluşlar hem kendi fikri mülkiyetlerini hem de işledikleri kişisel ve özel verileri korumaktan sorumludurlar. Çeşitli yasalar, kuruluşların özel ve gizli verileri korumak için güvenlik kontrolleri kullanmasını gerektirmektedir. Aşağıdakiler, yakın zamanda çıkan bilgi güvenliği ile ilişkili ABD yasaları arasındadır:

Federal Bilgi Güvenliği Yönetim Yasası (Federal Information Security Management - FISMA) — 2002'de yasalaşan FISMA federal hükümet bünyesindeki sivil dairelerin federal işlemleri destekleyen kaynaklar üzerinde güvenlik kontrolleri sağlamasını gerektirmektedir.

Federal Bilgi Güvenliği Modernizasyon Yasası *(Federal Information Security Modernization Act* - FISMA) — 2014'de yasalaşan FISMA, FISMA 2002'yi modern tehditleri yanı sıra güvenlik kontrolleri ve en iyi uygulamalar bağlamında güncellemek için getirildi.

Sarbanes-Oxley Yasası (SOX) —2002'de yasalaşan SOX halka açık şirketlerin doğru ve güvenilir mali raporlar yayımlamalarını gerektirmektedir. Bu yasa kişisel bilginin güvenceye alınmasını gerektirmemektedir fakat finansal raporlamanın gizliliği ve bütünlüğü için güvenlik kontrollerini gerektirmektedir.

Gramm-Leach-Bliley Yasası (GLBA) — 1999'da yasalaşan GLBA, her tür finans kuruluşunun müşterilerinin kişisel mali bilgilerini korumasını gerektirmektedir.

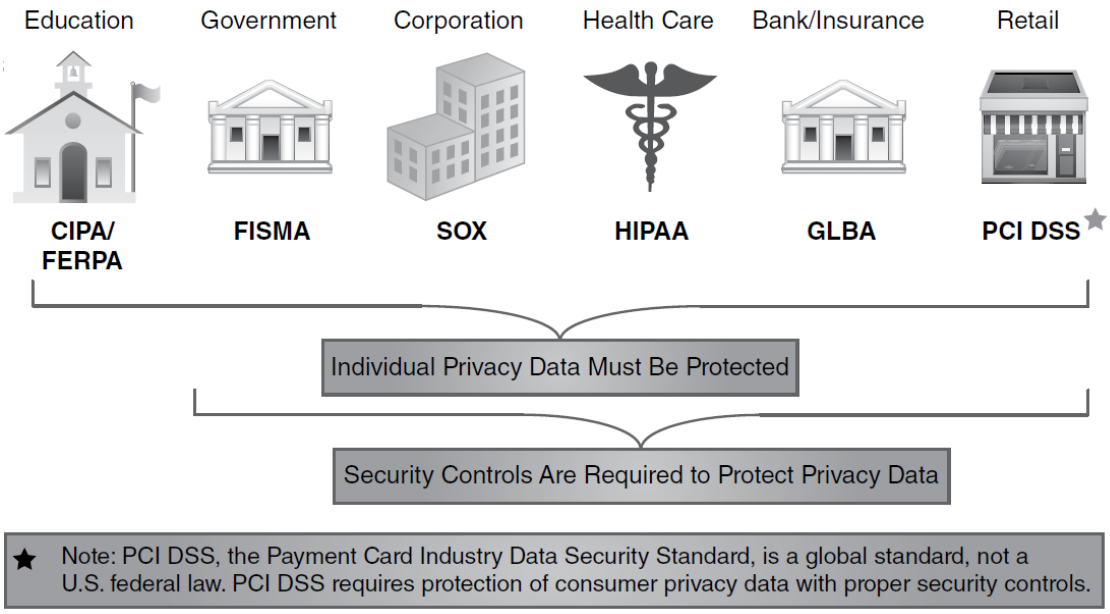
Sağlık Sigortası Taşınabilirlik ve Sorumluluk *(Health Insurance Portability and Accountability Act* - HIPAA)— 1996'da çıkan HIPAA, sağlık hizmeti veren kuruluşların hasta mahremiyetini korumak için güvenlik ve mahremiyet kontrolleri gerçekleştirmelerini gerektirir.

Çocukların İnternetten Korunması Kanunu *(Children's Internet Protection Act* - CIPA)— 2000'de geçen ve 2011'de güncellenen CIPA, devlet okullarının ve halka açık kütüphanelerin bir internet güvenliği politikası kullanmasını gerektirmektedir. Bu politika aşağıdaki konulara çözüm getirmelidir:

- Çocukların internette uygu1nsuz konulara erişimini sınırlamak
- E-posta, sohbet odaları ve diğer elektronik iletişim programlarını kullanırken çocukların güvenliğini garanti etmek
- Çocukların çevrimiçi bilgisayar korsanlığı ve diğer yasa dışı faaliyetlerini kısıtlamak
- Çocuklar hakkında kişisel bilgilerin izinsiz olarak dağıtılmaması ve açıklanmaması
- Çocukların zararlı içeriğe erişiminin kısıtlanması
- Çocukların sosyal medyanın kullanımı ve tehlikeleri konusunda uyarılması

Aile Eğitim Hakları ve Mahremiyet Yasası (Family Educational Rights and Privacy Act - FERPA)— 1974'de yasalaşan FERPA, öğrencilerin kişisel verilerini ve okul kayıtlarını korumaktadır.

Aşağıdaki şekil bu yasaları ilgili endüstrilere göre göstermektedir.



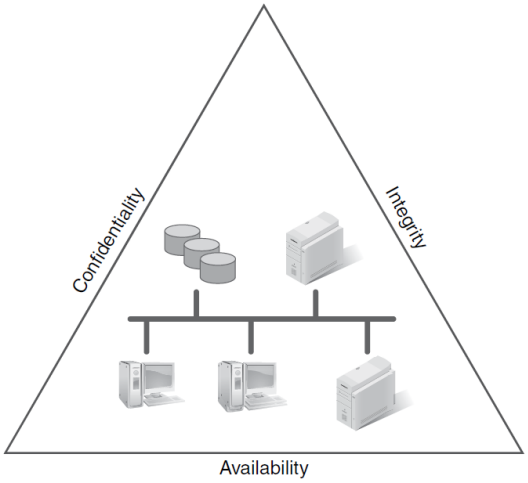
Ülkemizde ise aşağıdaki yasalar söz konuşudur

Bilgi Sistemleri Güvenliğinin İlkeleri

Çoğu insan kişisel bilginin güvenli olması gerektiği konusunda hemfikirdir. Fakat "güvenli bilgi" gerçekte ne anlama gelmektedir? Güvenli olan bilgi üç ana ilkeyi veya özelliği sağlamaktadır. Eğer bu üç ilkeyi sağlayabiliyorsanız, güvenli bilgi gereksinimlerini sağlamış olursunuz. Bu üç ilke aşağıdaki gibidir:

- **Gizlilik** *(Confidentiality):* Sadece yetkili kullanıcılar bilgiyi görebilmektedir.
- **Bütünlük** *(Integrity):* Sadece yetkili kullanıcılar bilgiyi değiştirebilmektedir.
- **Kullanılabilirlik** *(Availabiliy):* Bilgi yetkili kullanıcılann talep ettikleri her zaman erişilebilirdir.

Aşağıdaki şekil bilgi sistemleri güvenliğinin üç ilkesini göstermektedir. Bir güvenlik kontrolü tasarladığınız ya da kullandığınız zaman bu üç ilkeden bir veya birkaçında bir sorun çözüyorsunuz demektir.



Güvenlik konularına çözüm ararken, C-I-A (Confidentiality - Integrity - Availability) üçgenini kullanmalısınız. Tipik bir BT altyapısı için, kuruluşunuzun güvenlik temel hedeflerini bu üçlüyü kullanarak tanımlamalısınız. Bir kez tanımlandığında, bu hedefler koruduğunuz verinin türüne göre güvenlik kontrollerine ve gereksinimlerine dönüşecektir.

Gizlilik

Gizlilik *(Confidentiality)* genel bir terimdir. Bilgiyi hakkı olanlar dışındaki herkesten korumak anlamına gelmektedir. Gizli bilgi aşağıdakileri içermektedir:

- Kişilerin özel verileri
- İşletmelerin fikri mülkiyetleri
- Ülkeler ve hükümetler için ulusal güvenlik

Vatandaşların kişisel verilerini koruyan ABD uygunluk yasaları, işletmeler ve kuruluşların gizliliği garanti etmek için uygun güvenlik kontrollerine sahip olmalarını gerektirmektedir. E-ticaretin büyümesi ile daha çok insan kredi kartları ile çevrimiçi satın alma yapmaktadır. Bu durum, insanların e-ticaret web sitelerine kişisel verilerini girmelerini gerektirmektedir. Tüketiciler kişisel kimlik bilgilerini ve özel verilerini korumak için dikkatli olmalıdırlar. Yasalar kuruluşların müşterilerinin kişisel verilerini korumak için güvenlik kontrolleri kullanmalarını zorunlu tutmaktadır. Bir **güvenlik kontrolü** bir kuruluşun riski azaltmak için yaptığı bir şeydir. Bu tür kontrollere örnekler aşağıda verilmektedir:

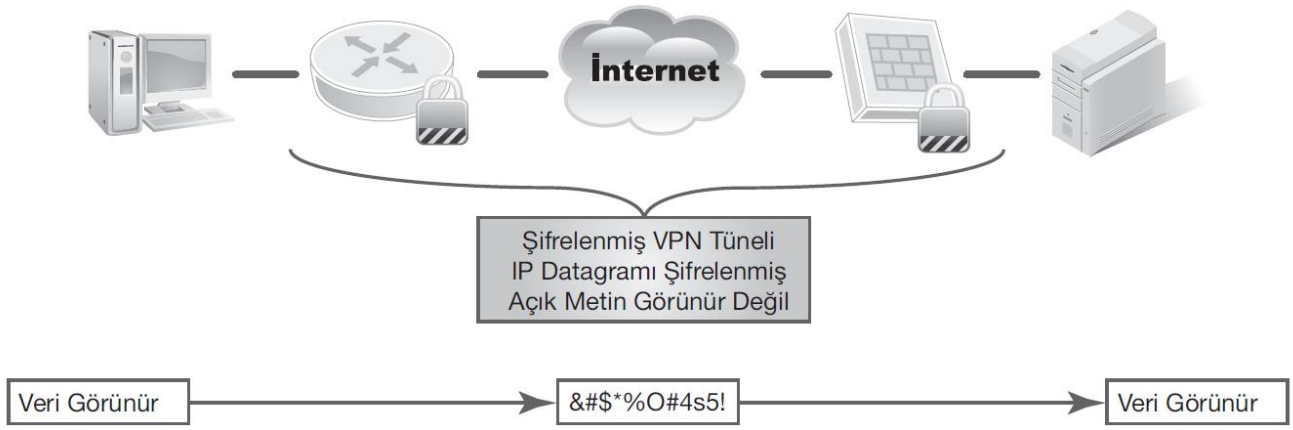
- Çalışanlar için yıllık güvenlik farkındalık eğitimi vermek. Bu, personele kişisel verilerin doğru kullanımını hatırlatmaya yardımcı olmaktadır. Ayrıca, kuruluşun güvenlik politikaları çerçevesi, standartları ve yönergeleri konusunda farkındalığı arttırmaktadır.
- Bir **BT güvenlik politika çerçevesi** *(IT security policy framework)* oluşturmak. Bir politika çerçevesi, güvenlik kontrollerinin nerede kullanılacağını belirlemektedir.
- Bir BT altyapısı için katmanlı bir güvenlik çözümü tasarlamak. Kişisel verileri ve fikri mülkiyeti koruyan veya bloke eden ne kadar çok katman veya bölme varsa verileri ve mülkiyeti bulmak ve çalmak o kadar zorlaşmaktadır.

- Web siteleri ve BT altyapısı üzerinde periyodik güvenlik risk değerlendirmesi, denetim, ve sızma testleri yapmak Bu, güvenlik uzmanlarının kontrolleri uygun yerleştirdiklerini doğrulama şeklidir. İnternet giriş ve çıkış noktalarında güvenlik olayı ve kaza izlemeyi etkinleştirmek. Bu ne geliyor ve ne gidiyoru görmek için bir mikroskop kullanmak gibidir.
- Otomatikleştirilmiş iş istasyonu ve sunucu anti-virüs ve kötücül yazılım koruması kullanmak. Bu, virüsleri ve kötücül yazılımları bilgisayarınızın dışında tutmanın yoludur.
- Hassas sistemler, uygulamalar ve veriler için bir oturum açma kimliği ve parolanın ötesinde daha sıkı erişim kontrolleri kullanmak. Oturum açma kimliği ve parolalar kullanıcının yalnızca tek bir kontrolüdür. Daha hassas sistemlere erişimde, kullanıcının kimliğini doğrulamak için ikinci bir test olmalıdır.
- Bilgisayarlarınızdaki ve sunuculardaki yazılımların zayıflıklarının güncelleme ve güvenlik yamaları ile en aza indirilmesi. Bu işletim sistemi ve uygulama yazılımının güncel tutulması için uygun yoldur.

Özel verilerin korunması veri gizliliğini garanti edilmesi işlemidir. Kuruluşlar bu iş için uygun güvenlik kontrollerini kullanmak zorundadırlar. Bazı örnekler aşağıda verilmektedir:

- Gizli verileri korumak için kuruluş genelinde geçerli politikalar, standartlar, prosedürler ve yönergeler tanımlanmalıdır. Bunlar kişisel bilginin nasıl ele alınıp işleneceğini gösteren komutlardır.
- Verileri BT altyapınız boyunca nasıl işleyeceğinizi tanımlayan bir veri **sınıflandırma standardı** *(data classification standard)* seçilmelidir. Bu verileri güvende tutmak için hangi kontrollere ihtiyaç olduğunu gösteren bir yol haritasıdır.
- Gizli veri içeren sistem ve uygulamalara erişim, sadece o verileri kullanmaya yetkili olanlarla sınırlandırılmalıdır.
- Kriptografi teknikleri kullanarak gizli verileri saklamak ve o verileri yetkisiz kullanıcılara karşı görünmez tutmak.
- Halka açık internet üzerinden geçen verileri şifrelemek
- Veritabanları ve veri depolama cihazlarında tutulan verileri şifrelemek

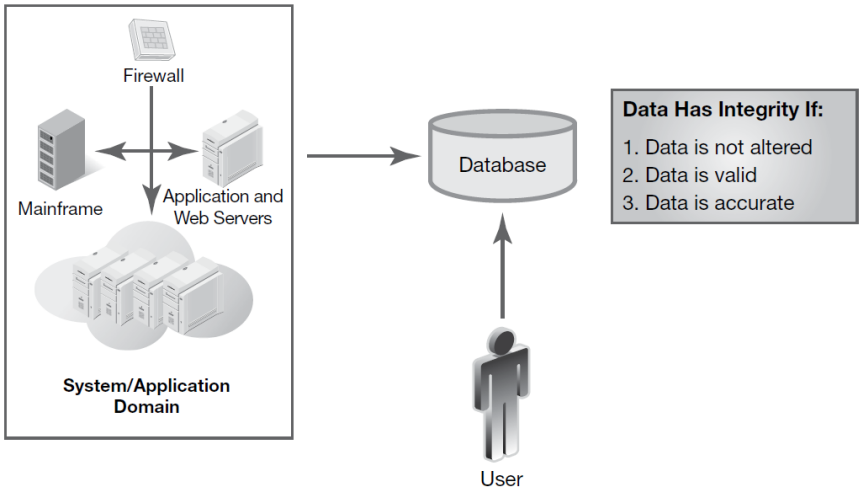
Bir ağ üzerinden başka bilgisayarlara veri göndermek, sizin gizli verileri yetkisiz kullanıcılardan korumak için özel adımlar atmanız gerektiği anlamına gelmektedir. **Kriptografi** veriyi gizleme ve yetkisiz kullanıcılardan uzak tutma uygulamasıdır. Şifreleme *(encryption)* veriyi açık metin(*plaintext*) halinden şifreli metin *(ciphertext)* haline dönüştürme işlemidir. Açık metin veri, herkesin okuyabileceği formattaki veridir. Şifreli metin ise açık metnin şifrelenmesi sonucu karıştırılmış biçimdeki veridir. Bu işlemin bir örneği **aşağıdaki şekilde** gösterilmektedir.



Bütünlük

Bütünlük *(Integrity)* verinin geçerlilik ve doğruluğu ile ilgilenmektedir. Bütünlüğü olmayan veri yani geçersiz veya doğru olmayan veri kullanışlı değildir. Veri ve bilgi, bazı kuruluşlar için fikri mülkiyet varlıklarıdır. Örnekler arasında telif hakları, patentler, gizli formüller ve müşteri veritabanları bulunmaktadır. Bu bilgilerin değeri büyük olabilmektedir. Yetkisiz değişiklikler, verilerin değerini düşürmektedir. Bu nedenle, bütünlük bir sistem

güvenliği ilkesidir. **Aşağıdaki şekilde** veri bütünlüğü ve bu verilerin kullanılabilir olup olmadığı ile ne denmek istendiğini göstermektedir. Özellikle de veriler iş operasyonları için kritik öneme sahipse, sabotaj ve veri bütünlüğünün bozulması bir kuruluşa yönelik ciddi tehditlerdir.



Kullanılabilirlik

Kullanılabilirlik *(Availability)* günlük hayatta yaygın bir terimdir. Örneğin, siz muhtemelen internet hizmetinin, TV hizmetinin, veya cep telefonu hizmetinin kullanılabilirliğine dikkat ediyorsunuzdur. Bilgi güvenliği bağlamında, kullanılabilirlik genellikle kullanıcıların bir sistem, uygulama veya verinin ulaşılabilir ve kullanılabilir olduğu zaman miktarı olarak ifade edilmektedir. Yaygın kullanılabilirlik süresi ölçütleri aşağıdakileri içermektedir:

- **Çalışma süresi *(Uptime)***: Çalışma süresi, bir sistemin, uygulamanın veya verinin erişilebilir olduğu toplam zaman miktarıdır. Çalışma süresi genellikle verilen bir takvim ayı için saniye, dakika ve saat cinsinden ölçülmektedir. Çalışma süresi sıklıkla mevcut zamanın bir yüzdesi olarak ifade edilmektedir, örneğin, %99,5 çalışma süresi.
- **Aksama süresi *(Downtime):*** Arızalı süre, bir sistem, uygulama veya verinin erişilebilir olmadığı toplam zaman miktarıdır. Arızalı süre de bir ay içinde saniye, dakika ve saat cinsinden ölçülmektedir.
- **Kullanılabilirlik *(Availability):*** Kullanılabilirlik K = (Toplam Çalışma Süresi) / (Toplam Çalışma Süresi + Toplam Aksama Süresi) formülü ile hesaplanmaktadır.
- **Arıza için ortalama süre *(Mean time to failure - MTTF):*** MTTF belli bir sistemde arızalar arasında geçen ortalama süredir. Yarı-iletkenler ve elektronik parçalar kolay bozulmaz ve çok büyük MTTF değerlerine [25 ya da daha fazla yıl vb.) sahiptir. Konektörler, kablolama, fanlar ve güç kaynaklan gibi fiziksel parçalar, aşınma ve yıpranmanın onları parçalayabileceği gerçeği dikkate alındığında, çok daha düşük MTTF değerlerine (5 yıl ya da daha az) sahiptirler.
- **Onarım için ortalama süre *(Mean time to repair - MTTR):*** MTTR, bir sistem, uygulama veya bileşeni onarmak için gerekli olan ortalama süredir. Amaç sistemi en kısa sürede ayağa kaldırmaktır.
- **Arızalar arası ortalama süre *(Mean time between failures – MTBR):*** *MTBF,* işlem sırasında bir BT sisteminin arızaları arasında geçen tahmini zamandır.
- **Kurtarma süresi hedefi *(Recovery time objective* - RTO**): RTO, bir kesintiden sonra bir sistem, uygulama ya da verinin geri kazanılarak tekrardan kullanılabilir duruma getirilmesi için gereken zamandır. İş sürekliliği planları tipik olarak kritik görev sistemler, uygulamalar ve veri erişimi için bir RTO tanımlamaktadır.

Aylık Kullanılabilirliği Nasıl Hesaplarız

Verilen bir 30 günlük takvim ayı için, toplam çalışma süresi miktarı eşittir:

- 30 gün x 24 saat/gün x 60 dakika/saat = 43.200 dakika

28 günlük bir takvim ayı (Şubat) için, toplam çalışma süresi miktarı eşittir:

- 28 gün x 24 saat/gün x 60 dakika/saat = 40.320 dakika

Aşağıdaki formülü kullanarak

- Kullanılabilirlik = (Toplam çalışma süresi) / (Toplam çalışma süresi + Toplam aksama süresi)

30 dakika planlanmış aksama (ya da servis dışı) süresi ile 30 günlük bir takvim ayı için kullanılabilirlik faktörü:

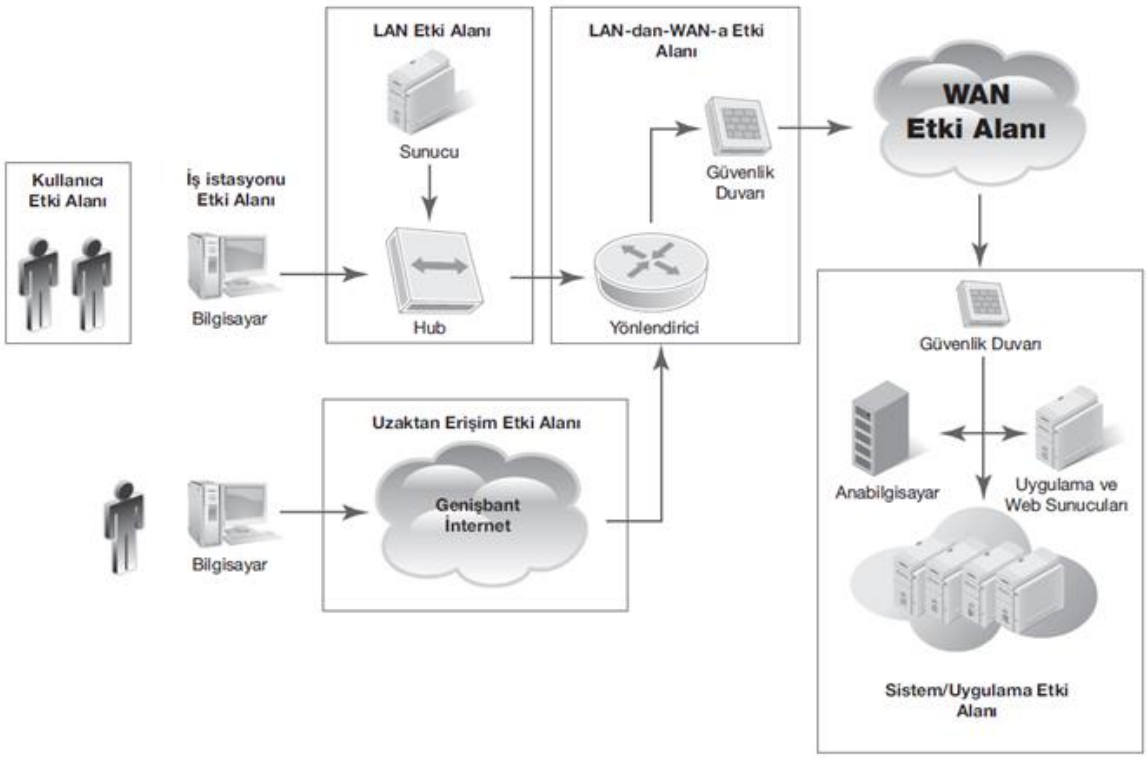
- Kullanılabilirlik = (43.200 dakika) / (43.200 + 30 dakika) = 0,9993 veya %99,93 olarak hesaplanmaktadır.

Telekomünikasyon ve internet hizmet sağlayıcıları müşterilerine **servis seviyesi anlaşmalar (service-level agreements SLAs)** sunmaktadırlar. Bir SLA, geniş alan ağları *(*wide area network - WAN) ve internet erişim hatları için asgari aylık hizmet kullanılabilirliğini garanti eden sözleşmedir. SLA'lar WAN servisleri ve adanmış internet erişim hatlarının kullanımına eşlik etmektedirler. Kullanılabilirlik, bir aylık çalışma süresi servis seviyesi taahhüdünü ölçmektedir. Yukarıda verilen aylık kullanılabilirlik örneğinde görüldüğü gibi 30 günlük bir takvim ayında 30 dakikalık bir servis dışı süresi yüzde 99,993 bir kullanılabilirliğe eşittir. Servis sağlayıcılar genellikle yüzde 99.5 ile yüzde 99,999 kullanılabilirlik arasında değişen SLA'lar önermektedirler.

Tipik bir BT Altyapısının Yedi Etki Alanı

Tipik bir BT altyapısında bilgi güvenliğinin üç ilkesi ne rol oynar? İlk olarak, tipik bir BT altyapısı nasıl görülür, ona bakalım. İster bir küçük işletme, büyük bir hükümet organı veya halka açık şirket olsun, çoğu BT altyapıları **aşağıdaki şekilde** gösterilen yedi etki alanından oluşmaktadır: Kullanıcı, İş istasyonu, LAN, LAN-WAN, WAN, Uzak Erişim, ve Sistem/Uygulama etki alanları.

Genellikle, bu yedi etki alanı tipik bir BT altyapısında mevcuttur. Her biri uygun güvenlik kontrollerini gerektirmektedir. Bu kontroller C-I-A üçlüsünün gereksinimlerini karşılamak zorundadır. Aşağıda bu yedi etki alanı ve günümüz BT ortamlarında sıklıkla bulacağınız risklere, tehditlere ve zafiyetlere genel bir bakış verilmektedir.



1. Kullanıcı Etki Alanı

Kullanıcı Etki Alanı bir kuruluşun bilgi sistemlerine erişen insanları ifade etmektedir.

Kullanıcı Etki Alanı Rolleri, Sorumlulukları ve İzlenebilirlik

Aşağıda. Kullanıcı Etki Alanında neler olması gerektiğine ilişkin genel bir açıklama verilmektedir:

- **Roller ve görevler (*Roles and tasks*):** Kullanıcılar, sistemlere, uygulamalara ve verilere, kendileri için tanımlanmış erişim haklarına göre erişebilmektedirler. Çalışanlar personel yönergelerine ve politikalarına uymalıdır.

Kullanıcı Etki Alanı **kabul edilebilir kullanım politikası *(acceptable use policy* - AUP)** belgesini bulacağınız yerdir. Bir AUP, kullanıcıların kuruluş-mülkiyetindeki BT varlıkları üzerinde ne yapmalarına izin verildiğini ve izin verilmediğini tanımlamaktadır. Çalışanların uymaları gereken bir kurallar kitabı gibidir. Bu kuralların ihlali işten atılmaya temel oluşturabilmektedir. Burası katmanlı bir güvenlik stratejisi için ilk savunma katmanının başladığı yerdir.

- **Sorumluluklar *(Responsibilities):*** Çalışanlar BT varlıkları üzerindeki kullanımlarından sorumludurlar. Birçok kuruluş için çalışanlarına bir AUP sunmak, yeni yasal düzenlemeler ışığında yapılacak en iyi uygulamadır. Kuruluşlar, personel, taşeronlar veya diğer üçüncü taraflar için kuruluş içi bilgiyi gizli tutmaları için sözleşme imzalamayı zorunlu tutabilmektedir. Bazı kuruluşlar hassas görevlere getirilecek personel için güvenlik soruşturmasını zorunlu tutabilmektedir. Bölüm müdürü veya insan kaynakları müdürü, genellikle çalışanların bir AUP belgesi imzalamalarından ve belgeye uygun davrandıklarını takipten sorumludurlar.
- **İzlenebilirlik *(Accountability):*** Genellikle, bir kuruluşun insan kaynakları bölümü doğru çalışan güvenlik kontrollerini uygulamaktan sorumludur. Bu kontroller hassas verilere erişim yetkisi verilecek kişiler için yaptırılmalıdır.

Kullanıcı Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

Kullanıcı Etki Alanı bir BT altyapısındaki en zayıf halkadır. Bilgisayar güvenliğinden sorumlu olan herkes, bir kimseyi kuruluşun sistemini, uygulamalarını veya verilerini tehlikeye atmak için neyin teşvik ettiğini anlamak zorundadır. **Aşağıdaki tablo** Kullanıcı Etki Alanında yaygın olarak bulunan riskler ve tehditlerin yanı sıra onları engellemek için kullanabileceğiniz planları listelemektedir.

RİSK, TEHDİT VEYA ZAFİYET	AZALTMA
Yetkisiz erişim	Kullanıcılarda, olta ***(phishing)*** e-postalar, hile bahaneleri, klavye kaydediciler, oturum açma kimliği ve parola bilgilerini elde etmek için bir BT çalışanı veya kuryeyi taklit eden sahtekârlar konularında farkındalık yaratılmalıdır.
Kullanıcı farkındalığı eksikliği	Güvenlik farkındalığı eğitimi düzenlenmeli, güvenlik farkındalığı posterleri asılmalı, afişlere hatırlatıcılar eklenmeli ve çalışanlara hatırlatma e-postaları gönderilmelidir.
Politikalara karşı kullanıcı duyarsızlığı	Yıllık güvenlik farkındalığı eğitimi düzenlenmeli, uygun kullanım politikaları yürürlüğe koyulmalı, personel yönerge ve el kitabı güncellenmeli, performans değerlendirmeleri sırasında konu gündeme getirilmelidir.
Güvenlik politikası ihlalleri	Çalışan izlemeye alınmalı, AUP belgesi ve çalışan el kitabı gözden geçirilmeli, performans değerlendirmeleri sırasında konu gündeme getirilmelidir.
Kişisel resim, müzik, ve videolar içeren USB sürücü ve CD-DVD vs kullanımı	CD/DVD sürücü ve USB portları iptal edilmeli. Sisteme sokulan medya sürücüleri, dosyalar ve e-posta eklentileri için otomatik olarak antivirüs taraması etkinleştirilmelidir. Bir antivirüs tarama sistemi bilgisayarınızın sabit diskindeki tüm yeni dosyalan virüslere karşı gözden geçirmektedir. Eklentisi olan e-postalar için antivirüs taraması kurulmalıdır.
Kullanıcının resim, müzik ve video indirmesi	İçerik filtreleme ***(Content filtering)*** ve e-posta eklentileri için antivirüs tarama etkinleştirilmelidir. İçerik filtreleyen ağ cihazları AUP tanımlamalarına uygun olarak spesifik alan isimlerine izin verecek veya ret edecek şekilde yapılandırılmıştır.
Kullanıcının sistemi, uygulamayı, veya verileri tahrip etmesi	Kullanıcıların erişimleri sadece kendiişlerini yapmak için gerekli olan sistem, uygulama ve verilerle sınırlanmalıdır. Yazma/silme izinleri sadece veri sahibine verilmelidir.

Kuruluşa saldırılar veya kızgın çalışanların sabotajları	Çalışanın normal dışı davranışları, düzensiz iş performansı ve BT altyapısının mesai saatleri dışı kullanımı takip edilmeli ve gözlemelidir. AUP izleme ve uyumunu temel alan BT erişim kontrol kilitleme prosedürleri başlatılmalıdır.
Kötü giden çalışan romantizmi	Çalışanın normal dışı davranışları ve BT altyapısının mesai saatleri dışı kullanımı takıp edilmeli ve gözlenmelidir. AUP izleme ve uyumunu temel alan BT erişim kontrol kilitleme prosedürleri başlatılmalıdır.
Çalışan şantajı veya gaspı	Çalışanın normal dışı davranışları ve BT altyapısının mesai saatleri dışı kullanımı takip edilmeli ve gözlenmelidir. Hassas görevlerde çalışan ve hassas verilere erişen personel için Saldırı Tespit Sistemi- Saldırı Önleme Sistemi ***(Intrusion Detection System - Intrusion Prevention System – IDS/IPS***) izlemesi etkinleştirilmelidir. IDS/IPS güvenlik cihazları içeri gelen ve dışarı giden trafik için IP veri akışlarını incelemektedir. Bir IDS/IPS üzerinde programlanmış alarm ve uyarılar normal dışı trafiği tespit etmeye yardım etmekte ve politika tanımlamalarına göre IP trafiğini engellemektedir.

2. İş İstasyonu Etki Alanı

Bir **iş istasyonu** *(workstation)* bir masaüstü bilgisayar, bir dizüstü bilgisayar, bir özel-amaçlı terminal veya ağınıza bağlanan başka herhangi bir cihaz olabilir. İş istasyonu bilgisayarları genellikle ince istemciler veya kalın istemcilerdir. Bir **ince istemci** *(thin client)* bir yazılım veya ağ üzerinde çalışan, sabit diski olmayan ve uygulamaları, verileri ve tüm veri işleme işleri için bir sunucuya gereksinim duyan gerçek bir bilgisayardır. İnce istemciler yaygın olarak büyük kuruluşlarda, kütüphanelerde ve okullarda kullanılmaktadırlar. Buna karşın, bir **kalın istemci** *(thick client) sabit* diski de içeren çok özellikli donanım ve uygulamalardır ve veriyi yerel olarak işlemekte, sunucuya sadece dosyalan depolamak için gitmektedir. Sıradan bir PC, kalın istemciye bir örnektir. İş istasyonları olarak kabul edilebilecek diğer cihazlar **kişisel dijital yardımcılar** *(personal digital assistants - PDA'lar),* akıllı telefonlar ve tablet PC'lerdir. Mobil cihazlarla ilgili daha fazla detayı "Uzaktan Erişim Etki Alanı" bölümünde bulabilirsiniz.

İş İstasyonu Etki Alanı Rolleri, Sorumluluklar ve İzlenebilirlik

Bu bölümde İş İstasyonu Etki Alanında nelerin bulunacağı konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler:** Bir kuruluşun personeli verimli olabilmek için gerekli erişime sahip olmalıdır. Donanımı yapılandırmak, sistemleri güçlendirmek ve antivirüs dosyalarını doğrulamak görevler arasında bulunmaktadır. **Sistemi sertleştirmek *(hardening)*** bilinen tüm tehditlere karşı kontrollerin yerleştirilmiş olduğundan emin olma sürecidir. Güçlendirme faaliyetleri tüm bilgisayarların en son yazılım revizyonlarına, güvenlik yamalarına ve sistem yapılandırmalarına sahip olduğundan emin olmayı içermektedir. İş istasyonu Etki Alanı ilave savunma katmanlarına da ihtiyaç duymaktadır; bu taktiğe **derinlemesine savunma *(defense in depth)*** adı verilmektedir. Bir başka yaygın savunma katmanı, BT altyapılarına bu etki alanından yapılacak girişleri korumak için iş istasyonu oturum açma kimliklerinin ve parolalarının kullanılmasıdır.
- **Sorumluluklar:** Bir kuruluşun masaüstü destek grubu İş İstasyonu Etki Alanından sorumludur. Tanımlı standartların uygulanmasını temin etmek kullanıcı iş istasyonları ve verilerin bütünlüğünü korumak için kritik öneme sahiptir. BT güvenlik personeli İş İstasyonu Etki Alanındaki kontrolleri korumak zorundadır. Genellikle, insan kaynakları bölümleri çalışanlar için uygun erişim kontrollerini onların görevlerine göre tanımlamaktadır. Ardından, BT güvenlik bölümü sistemlere, uygulamalara ve verilere erişim haklarını bu tanımlara göre atamaktadır.
- **İzlenebilirlik:** Bir kuruluşun BT masaüstü sistemler yöneticisi genellikle çalışanlara İş İstasyonu Etki Alanında en kapsamlı kullanım olanağını sağlamak konusunda yetkili ve sorumlu kılınmaktadır. BT güvenlik direktörü İş İstasyonu Etki Alanının politikaya uygunluğunu temin etmekle görevlidir.

İş İstasyonu Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

İş istasyonu Etki Alanı sıkı güvenlik ve erişim kontrolleri gerektirmektedir. Burası kullanıcıların sistemlere, uygulamalara ve verilere ilk eriştiği yerdir. İş İstasyonu Etki Alanı erişim için bir oturum açma kimliği ve parola gerektirmektedir. **Aşağıdaki tabloda** İş İstasyonu Etki Alanında yaygın olarak bulunan riskler, tehditler ve zafiyetler ile birlikte bunlara karşı korunma yollarım listelemektedir.

RİSK, TEHDİT VEYA ZAFİYET	AZALTMA
İş istasyonuna yetkisiz erişim	Erişim için iş istasyonları üzerinde parola koruma etkinleştirilmelidir. Kullanılmadığı zamanlarda otomatik ekran kilitleme etkinleştirilmelidir. Kullanıcılar için sistem yöneticisi (admin) hakları devre dışı bırakılmalıdır
Sistemlere, uygulamalara ve verilere yetkisiz erişim	Katı erişim kontrol politikaları, standartları, prosedürleri ve yönergeleri tanımlanmalıdır. Hassas veri içeren uygulamalara erişim için ikinci bir seviye veya doğrulama katmanı gerçekleştirilmelidir (örneğin, iki adımlı kimlik doğrulama)
Masaüstü veya dizüstü bilgisayar işletim sistemi yazılım zafiyetleri	Bir iş istasyonu işletim sistemi **zafiyet penceresi** *(vulnerability window)* politikası ve standardı tanımlanmalıdır. Zafiyet penceresi, bir iş istasyonunun bilinen bir zafiyete karşı yama yapılana kadar maruz kaldığı zaman boşluğudur. Süregelen güvenlik işlemlerinin bir parçası olarak sık sık **zafiyet değerlendirme** *(vulnerability assessment)* taramaları yapılmalıdır.
Masaüstü veya dizüstü bilgisayar uygulama yazılım zafiyetleri ve yazılım yama güncellemeleri	Bir iş istasyonu uygulama **yazılım zafiyet** *(software vulnerability)* politikası ve standardı tanımlanmalıdır. Uygulama yazılımı ve güvenlik yamaları tanımlanmış politikalar, standartlar, prosedürler ve kılavuzlara göre güncellenmelidir.
Kullanıcı iş istasyonunun ve dizüstü bilgisayarının virüsler, kötücül koddan, ya da kötücül yazılımdan etkilenmesi	İş istasyonu antivirüs ve kötücül kod politikaları, standartları, prosedürleri ve yönergeleri kullanılmalıdır. Uygun koruma ile kişisel iş istasyonlarını tarayan ve güncelleyen otomatik antivirüs koruma çözümü aktif edilmelidir.
Kullanıcının kuruluş bilgisayarlarına CD, DVD veya USB sürücü takması	Tüm CD, DVD ve USB portları devre dışı bırakılmalıdır. Takılan ve dosya barındıran tüm CD, DVD ve USB sürücüleri için otomatik antivirüs taraması etkinleştirilmelidir.
Kullanıcı tarafından internetten indirilen resim, müzik ve videolar	İçerik filtreleme ve internet giriş ve çıkış noktalarında antivirüs tarama kullanılmalıdır. Tüm yeni dosyalar için iş istasyonu otomatik taramaları etkinleştirilmeli ve bilinmeyen dosya tipleri karantinaya alınmalıdır.
Kullanıcının AUP ihlali, kuruluşun BT altyapısı için güvenlik riskleri yaratmaktadır	Tüm çalışanlar için yıllık güvenlik farkındalık eğitimi zorunlu tutulmalıdır. Yıl boyunca güvenlik farkındalığı kampanyaları ve programları düzenlenmelidir.
Çalışanlar ve kullanıcılar işyerinde kendi akıllı telefon veya tabletlerini kullanmak istemektedirler, bu da kuruluşun Kendi Cihazını Getir (Bring Your Own Device - BYOD) altyapı desteği sağlamasını gerektirmektedir	Çalışanların kendi kişisel akıllı telefonlarını veya mobil cihazlarını kullanmalarına izin veren bir BYOD politikası ve prosedürü geliştirilmelidir. BYOD politika ve prosedürleri, genel olarak kuruluşa, kullanıcının akıllı telefon veya mobil cihazındaki verileri cihazın kaybolması ya da çalışanın ilişiğinin kesilmesi durumunda silmesine izin vermektedir.

3. LAN Etki Alanı

Bir **yerel alan ağı (local area network - LAN)** birbirlerine ya da ortak bir bağlantı ortamına bağlanmış bir bilgisayarlar topluluğudur. Ağ bağlantı ortamı telleri, fiber-optik kabloları veya radyo dalgalarını içerebilmektedir. LAN'lar genellikle işleve veya bölüme göre organize edilmektedir.

LAN'a bir kez bağlanıldığında, bilgisayarınız sistemlere, uygulamalara, muhtemelen internete ve verilere erişebilmektedir. BT altyapısında üçüncü bileşen LAN Etki Alanıdır.

LAN Etki Alanının fiziksel kısmı aşağıdakilerden oluşmaktadır:

- **Ağ arayüz kartı *(Network interface card* - NIC):** Bilgisayar ile LAN fiziksel ortamı arasındaki arayüzdür. NIC kendisine ait benzersiz bir donanım tanımlayıcı olarak çalışan 6-byte'lık bir Ortam Erişim Kontrol ***(Media Access Control*** - MAÇ) katmanı adresine sahiptir.
- **Ethernet LAN:**Bu, 10/100/1.000 Mbps Ethernet ağı için geliştirilmiş **IEEE 802.3 CSMA/CD** standardı üzerine inşa edilmiş bir LAN çözümüdür. **Ethernet** en popüler LAN standardıdır. Günümüzün LAN standardı **Elektrik ve Elektronik Mühendisleri Enstitüsü *(Institute of Electricaland Electronics Engineers - IEEE)*** 802.3 **Taşıyıcı Duyarlı Çoklu Erişim/Çarpışma Tespiti *(Carrier Sense Multiple Access/Collision Detection - CSMA/CD)*** spesifikasyonudur. Ethernet, kampüs ve kent Ethernet omurgası bağlantıları için 10-Mbps, 100-Mbps, 1-Gbps, 10-Gbps, 40-Gbps ve şu anda 100-Gbps hızlarında mevcuttur.
- **Korumasız bükümlü-çift kablolama *(Unshielded twisted-pair cabling)*:** 100Mbps/1Gbps/10Gbps Ethernet LAN anahtarlarına fiziki olarak bağlanmak için RJ-45 konektörler ve jaklar kullanan iş istasyonu kablolamasıdır. Günümüzde, yüksek hızlı veri iletişimini desteklemek için, kuruluşlar Kategori 5 veya Kategori 6 UTP iletim ortamı kullanmaktadırlar.
- **LAN Anahtarı *(LAN switch)*:** Bu iş istasyonlarını fiziki bir Ethernet LAN'ına bağlayan bir cihazdır. Bir anahtar, her bir iş istasyonuna maksimum üretilen iş ve performansı verecek şekilde, iş istasyonlarına ve sunuculara adanmış Ethernet LAN bağlantısı sağlamaktadır. İki tip LAN anahtarı vardır. Bir **Katman 2 anahtar** MAC katmanı adresini incelemekte ve yönlendirme kararlarını MAC katmanı adres tablosuna göre vermektedir. Bir **Katman 3 anahtar** ağ katmanı adresini incelemekte ve paketleri yönlendirme protokolünün yol belirleme kararlarına göre yönlendirmektedir. Bir katman 3 anahtar bir yönlendirici ***(router)*** ile aynıdır.
- **Dosya sunucusu ve yazdırma sunucusu:** Bunlar şirket ya da bölüm içi dosya paylaşımı ve veri depolama sağlayan yüksek güçte bilgisayarlardır. Yazdırma servisleri bölüm içinde ortak yazıcı kullanımını desteklemektedir.
- **Kablosuz erişim noktası *(Wireless access point – WAP)* :** Kablosuz LAN'lar (*wireless* LAN-WLAN) için, radyo telsizleri IP paketlerini WLAN NIC'den bir **kablosuz erişim noktasına (WAP)** iletmek için kullanılmaktadır. WAP, mobil dizüstü bilgisayarların bağlanması için WLAN sinyalleri göndermektedir. WAP korumasız bükümlü-çift kablo üzerinden geriye LAN anahtarına bağlanmaktadır.

Ethernet anahtarları, tipik olarak, her iş istasyonu için 100-Mbps veya 1-Gbps bağlantı sağlamaktadır. Bugün, Ethernet LAN anahtarları 100-Mbps ve 1-Gbps masaüstü hızları ve 10-Gbps ve 40-Gbps omurga bağlantı hızlarını desteklemektedir. Bu omurga bağlantıları genellikle fiber optik kablolama kullanmaktadır.

LAN Etki Alanının mantıksal kısmı aşağıdakilerden oluşmaktadır:

- **Sistem yönetimi *(System administration)* :** Kullanıcı LAN hesaplarının, oturum açma kimliği ve parola erişim kontrolleri [kullanıcı bağlantı bilgisi) ile kurulması.
- **Dizin ve dosya servislerinin tasarımı:** Kullanıcının erişim hakkının olacağı sunucular, dizinler ve klasörler.
- **İş istasyonu ve sunucu TCP/IP yazılım ve iletişim protokollerinin yapılandırılması/konfigürasyonu:** Bu, IP adreslemesi, **IP varsayılan ağ geçidi yönlendiricisi, alt-ağ maske adresi *(IP default gatevvay router, subnetmask address),*** vb. ile ilgilidir. IP varsayılan ağ geçidi yönlendiricisi, LAN'ın giriş/çıkış noktası olarak çalışmaktadır. Alt-ağ maske adresi IP ağ numarası ve IP makine ***(host)*** numarasını belirlemektedir.
- **Sunucu disk depolama alanı tasarımı; kullanıcı verisinin yedeklenmesi ve kurtarılması:** Kullanıcı veri dosyaları için verinin günlük yedeklendiği ve arşivlendiği LAN disk depolama alanı sağlanmasıdır. Verinin kaybolması veya bozulması durumunda veri dosyaları yedekleme dosyalarından geri kazanılabilmektedir.
- **Sanal LAN'ların (VLAN'lar) Tasarımı:** Katman 2 ve Katman 3 LAN anahtarlar ile Ethernet portları, gerçekte farklı fiziki LAN'lar üzerinde bulunmalarına rağmen aynı VLAN üzerinde yer alacak şekilde yapılandırılabilmektedir. Bu, iş istasyonları ve sunucuları aynı Ethernet LAN veya yayımlama etki alanında *(broadcast domain)* olacak şekilde yapılandırmakla aynı olmaktadır.

Kullanıcılar kendi bölümlerinin LAN'larına ve görev gereksinimlerine göre diğer uygulamalara erişmektedir.

LAN Etki Alanı Rolleri, Sorumluluklar ve İzlenebilirlik

Bu bölümde LAN Etki Alanında nelerin bulunacağı konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler:** LAN Etki Alanı hem fiziksel ağ bileşenleri hem de kullanıcılar için servislerin mantıksal yapılandırmasını içermektedir. Fiziksel bileşenlerin yönetimi aşağıdakileri içermektedir:
  - Kablolama
  - NIC'ler
  - LAN anahtarları
  - Kablosuz erişim noktaları (WAP'lar)

LAN sistem yönetimi, kullanıcı hesaplarının ana listelerini ve erişim haklarını korumayı kapsamaktadır. LAN Etki Alanında, iki aşamalı kimlik doğrulama gerekli olabilmektedir. İki aşamalı doğrulama, kullanıcının kimliğini ikinci kez onaylattığı bir geçide benzemektedir. Bu işlem yetkisiz fiziksel erişim riskini azaltmaktadır.

- **Sorumluluklar:** LAN destek grubu LAN Etki Alanından sorumludur. Bu, hem fiziksel bileşenleri hem de mantıksal elemanları içermektedir. LAN sistem idarecileri bölümün dosya ve yazdırma servislerini sürdürmek ve desteklemek ve kullanıcılar için erişim kontrollerini yapılandırmak zorundadır.
- **İzlenebilirlik:** LAN yöneticisinin görevi LAN Etki Alanındaki verinin kullanımı ve bütünlüğünü maksimize etmektir. Genellikle, BT güvenlik direktörü LAN Etki Alanının politikaya uyumunu garanti etmelidir.

LAN Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler, Zafiyetler

LAN Etki Alanı, aynı zamanda güçlü güvenlik ve erişim kontrollerine gereksinim duymaktadır. Kullanıcılar şirket genelinde sistemlere, uygulamalara ve verilere erişebilmektedirler. Burası üçüncü savunma katmanının gerekli olduğu yerdir. Bu savunma BT altyapısını ve LAN Etki Alanını korumaktadır. **Aşağıdaki tabloda,** LAN Etki Alanında yaygın olarak bulunan riskler, tehditler ve zafiyetler ile birlikte uygun risk azaltıcı stratejileri de listelemektedir.

RİSK, TEHDİT VEYA ZAFİYET	**AZALTMA**
LAN'a yetkisiz erişim	Kablo dolapları, veri merkezleri ve bilgisayar odalarının güvenliğinin sağlandığından emin olunmalıdır. Uygun bir görevli kimliği olmayan kişilere izin verilmemelidir.
Sistemlere, uygulamalara ve verilere yetkisiz erişim	Katı erişim kontrol politikaları, standartlar, prosedürler ve yönergeler tanımlanmalıdır. Hassas sistemlere, uygulamalara ve verilere erişim için ikinci bir kimlik denetimi seviyesi kullanılmalıdır. Kullanıcıların LAN klasörlerine erişimleri ve spesifik dokümanlar için okuma/ yazma/silme hakları ihtiyaç halinde kısıtlanmalıdır.
LAN sunucu işletim sistemi yazılım zafiyetleri	Sunucu/masaüstü/dizüstü zafiyet penceresi politikaları, standartları ve yönergeleri tanımlanmalıdır. Yazılım açıklarını bulmak için periyodik olarak LAN Etki Alanı zafiyet değerlendirmeleri yapılmalıdır. Bir zafiyet değerlendirmesi, yazılımın içindeki kusur ve hataları belirleyen bir yazılım gözden geçirme faaliyetidir. Bu kusur ve hatalar yazılım yama ve düzeltmeleri yüklendiğinde yok olmaktadır.
LAN sunucu uygulama yazılım zafiyetleri ve yazılım yama güncellemeleri	Yazılım yamalarının vakit geçirmeden yüklenmesini zorunlu kılan katı bir yazılım zafiyet penceresi politikası tanımlanmalıdır.
WLAN'lardaki dolandırıcı kullanıcılar tarafından gerçekleştirilen yetkisiz erişim	Kablosuz erişim için parola isteyen WLAN **ağ anahtarları (network keys)** kullanılmalıdır. WAP'lardaki yayımlama **(broadcasting)** kapatılmalıdır. VVLAN erişimi onaylanmadan önce ikinci seviye kimlik doğrulama **(authentication)** yapılmalıdır.

WLAN üzerinden veri iletiminin gizliliğinin ihlal edilmesi	İş istasyonu ve WAP arasında gizliliği sağlamak için şifreleme gerçekleştirilmelidir.
Farklı donanım, işletim sistemi ve yazılıma sahip LAN sunucularının yönetim ve sorun gidermeyi güçleştirmesi	LAN sunucu ve yapılandırma standartları, prosedürleri ve yönergeleri oluşturulmalıdır.

4. LAN'dan WAN'a Etki Alanı

LAN'dan WAN'a Etki Alanı BT altyapısının bir geniş alan ağına ve internete bağlandığı yerdir. Maalesef, internete bağlanmak kötü adamlara kırmızı halı sermeye benzemektedir. İnternet açıktır, kamusal atandadır ve herkes tarafından kolayca erişilebilmektedir.

İnternet trafiğinin büyük çoğunluğu açık metin halindedir. Bu, trafiğin görünür olduğu ve mahrem olmadığı anlamına gelmektedir. Ağ uygulamaları iki yaygın taşıma protokolü kullanmaktadır: İletim Kontrol Protokolü *(Transmission Control Protocol* - TCP) ve Kullanıcı Veri Bloğu İletişim Kuralı *(User Datagram Protocol* - UDP). TCP ve UDP'nin her ikisi de (trafiğin ait olduğu) uygulamaya da işlevi belirlemek için port numaralarını kullanmaktadır; bu port numaraları bir TV'deki kanallar gibi iş görmekte, hangi istasyonu izlediğinizi belirlemektedir. Bir paket TCP veya UDP ile gönderildiğinde, o paketin ait olduğu port numarası paket başlığında yer almaktadır. Birçok servis belli bir port numarası ile ilişkilendirildiği için, port numarasını bilmek onun ne tür bir paket olduğunu açığa çıkarmaktadır. Bu, iletmekte olduğunuz şeyi dünyaya ilan etmeye benzemektedir.

Aşağıda çok kullanılan TCP ve UDP port numaralarına örnekler verilmektedir:

- **Port 80: Hiper Metin Aktarım Protokolü *(Hypertext Transfer Protocol - HTTP)*** : HTTP web tarayıcıları ile web siteleri arasındaki açık metin veri iletişimi protokolüdür.
- **Port 20 ve 21: Dosya Aktarım Protokolü *{File Transfer Protocol - FTP)*** FTP dosya aktarımı yapmak için kullanılan bir protokoldür. FTP bağlantı temelli bir veri iletimi için TCP'yi kullanmaktadır ancak parola da dahil olmak üzere veriler açık metin biçimindedir. *Bağlantılı* olmak *(connection-oriented)*, dosya aktarımının bütünlüğünü arttırmak için paketlerin tek tek numaralanması ve alındıklarında teyit edilmeleri anlamına gelmektedir.
- **Port 69: Önemsiz Dosya Aktarım Protokolü *(Trivial File Transfer Protocol TFTP)***: TFTP dosya aktarımı yapmak için kullanılan bir protokoldür. TFTP bağlantısız *(connectionless)* veri iletimi için UDP'yi kullanmaktadır ancak veriler açıkta gitmektedir. Bu protokol küçük dosyaların hızlı iletimi içindir ancak her paketin iletimini garanti etmemektedir.
- **Port 23:Terminal Ağı *(Telnet):*** Telnet bir başka cihaza uzaktan terminal erişimi gerçekleştirmek için kullanılan bir ağ protokolüdür. Telnet TCP'yi kullanmaktadır ve verileri açıkta göndermektedir.
- **Port 22: Güvenli Kabuk *(Secure Shell - SSH)*—**SSH bir başka cihaza uzaktan terminal erişimi gerçekleştirmek için kullanılan bir ağ protokolüdür. SSH, iletişimin gizliliğini korumak için veri iletimini şifrelemektedir.

Çok kullanılan, 0 ile 1023 arasındaki port numaralarının tam bir listesi İnternet Atanmış Numaralar Yetkilisi *(Internet Asigned Numbers Authority-IANA*) tarafından muhafaza edilmektedir. IANA küresel alan isim servisleri, IP adresleri ve diğer kaynakların birlikte çalışmasına yardımcı olmaktadır.

TCP/IP protokol takımı *güvenlikten yoksun olduğundan,* bu aileden protokollerle çalışırken güvenlik kontrollerine daha fazla ihtiyaç vardır. LAN'dan WAN'a Etki Alanı tipik bir BT altyapısı için dördüncü savunma katmanını temsil etmektedir.

LAN-WAN Etki Alanı Rolleri, Sorumlulukları ve İzlenebilirlik

Bu bölümde LAN'dan WAN'a Etki Alanında nelerin bulunacağı konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler –** LAN'dan WAN'a Etki Alanı hem fiziksel parçalar hem de güvenlik araçlarının mantıksal tasarımını içermektedir. Bir BT altyapısında güvenliği sağlamanın en karmaşık olduğu alanlardan biridir. Kullanıcılara mümkün olduğunca çok erişim sağlarken, güvenliği korumanız

gerekmektedir. Fiziksel kısımların servise kolay erişim verecek şekilde idare edilmesine ihtiyaç vardır. Güvenlik araçları politika tanımlarına uyacak şekilde yapılandırılmalıdır.

Bu, kullanılabilirliği *(availability)* en iyi hale getirmekte, veri bütünlüğünü sağlamakta ve gizliliği korumaktadır. LAN'dan WAN'a Etki Alanında roller ve görevler aşağıdakilerin yönetimini ve yapılandırmasını içermektedir:

- **IP yönlendiriciler *(IP routers):*** Bir IP yönlendirici, IP paketlerini İnternete ve WAN'a ulaştırmak (hem göndermek hem de almak) için kullanılan bir ağ cihazıdır. Yönlendiricide alınan yol belirleme kararları IP paketlerini yönlendirmektedir. Yapılandırma işleri IP yönlendirme ve erişim kontrol listelerini *(access control lists* - ACL'ler) içermektedir. ACL'ler bir filtre gibi trafiğe engel olmak veya izin vermek için kullanılmaktadırlar.
- **IP durum denetlemeli güvenlik duvarları *(IP Stateful firewalls) :* Durum denetlemeli bir İP güvenlik duvarı,** gelen *(inbound)* IP paketlerini IP, TCP ve UDP paket başlıklarına göre yapılandırılmış çeşitli ACL tanımlarına göre filtreleyen bir güvenlik cihazıdır. Durum denetlemeli bir güvenlik duvarı filtreleme için IP, TCP ve UDP paket başlıklarını inceleyebilmektedir.
- **Arındırılmış bölge *(Demilitarized zone - DMZ):*** DMZ, LAN'dan WAN'a Etki Alanı içerisinde gelen ve giden IP trafiği için bir tampon bölge olarak davranan bir LAN segmentidir. Web sunucuları, **vekil sunucular** *(proxy servers)* ve e-posta sunucuları gibi harici sunucular IP trafiğinin daha fazla izolasyonu ve taranması için bu bölgede konumlandırılabilmektedir.
- **Saldırı tespit sistemleri *(Intrusion Detection Systems - IDS):*** Bir IDS güvenlik aracı IP data akışını yaygın saldırı ve kötü niyetli örüntüler açısından incelemektedir. IDS'ler pasif olup en fazla bir alarm tetikleyecek kadar ileri giderler fakat trafiği aktif bir şekilde engellemezler.
- **Saldırı engelleme sistemleri *(Intrusiorı Prevention Systems - IPS)***: Bir IPS bir IDS'le aynı şeyi yapmaktadır, fakat zararlı olarak tespit edilen IP veri akışlarını engelleyebilmektedir. IPS'ler gerçek iletişim oturumunu sonlandırabilmekte, kaynak IP adresine göre filtreleyebilmekte ve hedef makineye erişimi engelleyebilmektedir.
- **Vekil sunucular *(Proxy servers):*** Bir vekil, bir iş istasyonu ile dış hedef arasında aracı olarak hareket etmektedir. Trafik bir vekil gibi davranan aracı sunucuya gitmektedir. Veri, vekil güvenlik duvarları veya uygulama ağ geçidi güvenlik duvarı tarafından BT altyapısına yönlendirilmeden önce analiz edilebilmekte ve uygun şekilde taranabilmektedir.
- **Web içerik filtresi *(Web content filter):*** Bu güvenlik cihazı, alan isimlerinin veya alan isimleri içindeki anahtar kelimelerin filtrelenmesine dayalı olarak içeriğin BT altyapısına girişini engelleyebilmektedir.
- **E-posta içerik filtresi ve karantina sistemi:** Bu güvenlik cihazı e-postaların veya bilinmeyen dosya eklerinin içinde bulunan içeriği uygun antivirüs taraması ve karantina kullanarak engelleyebilmektedir. İnceleme sonrasında, e-posta ve ekler kullanıcıya iletilebilmektedir.
- **Güvenlik bilgi ve olay yönetimi (Security İnformation and event management- SIEM):** SIEM, DMZ VLAN, güvenlik duvarları, IDS/IPS, ve diğer güvenlik cihazlarını da kapsayacak şekilde LAN'dan WAN'a Etki Alanındaki BT varlıklarını gizlilik, bütünlük ve kullanılabilirliği en üst düzeye çıkarmak amacıyla izlemeyi ve belirli durum ve koşullar tarafından tetiklenen güvenlik olaylarını ve alarmları gözlemeyi içermektedir.

- **Sorumluluklar:** LAN'dan WAN'a Etki Alanından ağ güvenliği grubu sorumludur. Bu hem fiziksel hem de mantıksal elemanları içermektedir. Grup üyeleri tanımlanmış güvenlik kontrollerini uygulamaktan sorumludurlar.
- **İzlenebilirlik:** Kuruluşunuzun WAN ağ yöneticisi LAN'dan WAN'a Etki Alanını yönetmekle görevlidir. Genellikle, BT direktörü LAN'dan WAN'a Etki Alanı güvenlik politikaları, standartları, prosedürleri ve yönergelerinin kullanımını garanti etmektedir.

LAN'dan WAN'a Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

LAN'dan WAN'a Etki Alanı, internete bağlanmanın riskleri ve tehditleri düşünüldüğünde, katı güvenlik kontrollerine ihtiyaç duymaktadır. Bu etki alanı tüm verilerin BT altyapısına girip çıktığı yerdir. LAN'dan WAN'a Etki Alanı, tüm kuruluş için internet erişimi sağlamakta ve WAN için giriş ve çıkış noktası gibi davranmaktadır.

Bu, aynı zamanda internet giriş/çıkış *(ingress/egress)* noktası olarak bilinmektedir. LAN'dan WAN'a Etki Alanı, dördüncü savunma katmanının gerekli olduğu yerdir. **Aşağıdaki tabloda** LAN'dan WAN'a Etki Alanında yaygın olarak bulunan riskleri, tehditleri ve zafiyetleri uygun risk azaltma stratejileri ile birlikte listelemektedir.

RİSK, TEHDİT, VEYA ZAFİYET	**AZALTMA**
Yetkisiz ağ sorgulaması *(probing)* ve port taraması	Tüm LAN-WAN Etki Alanı içinde, dış IP'ye sahip tüm cihazlar üzerinde *ping prob* gönderme ve port tarama devre dışı bırakılmalıdır. Ping, internet Kontrol Mesaj Protokolü *(Internet Control Message Protocol* ICMP) yankı-istek *(echo-request)ve* yankı-yanıt *(echo-reply)* mesajlarını kullanmaktadır. IDS/IPS ile sorgulama, tarama ve izleme için kullanılan IP port numaralarına izin verilmemelidir.
LAN'dan WAN'a Etki Alanı üzerinden yetkisiz erişim	Saldırı tespit ve önleme için katı güvenlik izleme kontrolleri uygulanmalıdır. Gelen IP trafiği üzerindeki anomaliler ve kötü niyetli trafik izlenmelidir. Eğer trafik kötücül ise anında engellenmelidir.
Halka açık dış IP'ler ve internet bağlantıları üzerinde Hizmet Reddi (Denial of Service DoS)/Dağıtık Hizmet Reddi *(Distributed Denial of Service* - DDoS) saldırıları	Bir yarı-açık TCP SYN paketleri akışı internet Servis Sağlayıcı *(Internet Service Provider*- ISP) hattı üzerinde ISP bağlantısına flood saldırısı başlattığında yukarı yönde *(upstream)* ISP'ler DoS/DDoS saldırı önlemesi ve IP paketlerinin düşürülmesi çabasına ortak olmak zorundadırlar.
IP yönlendirici, güvenlik duvarı, ve ağ cihazı işletim sistemi yazılım zafiyetleri	Katı bir sıfırıncı gün zafiyet penceresi tanımı belirlenmelidir. Güvenlik düzeltmeleri ve yazılım yaması gerektiren aygıtlar hemen güncellenmelidir.
IP yönlendirici, güvenlik duvarı, ve ağ cihazı yapılandırma dosyası hataları veya zayıflıkları	LAN'dan WAN'a Etki Alanındaki katmanlı güvenlik çözümü üzerinde yapılandırma sonrası sızma testleri yapılmalıdır. Gelen ve giden trafik test edilmeli ve açıkları giderilmelidir.
Uzak kullanıcıların kuruluşun altyapısına erişebilme ve hassas verileri indirebilme kabiliyeti	Kuruluşun veri sınıflandırma standardı uygulanmalı ve uygulatılmalıdır. Erişim kontrol listelerinde yer alan kaynak IP adresleri kullanılarak giden trafik reddedilmelidir. Uzaktan indirmeye izin veriliyorsa gerektiğinde şifrelenmelidir.
Bilinmeyen kaynaklardan bilinmeyen dosya tipinde eklentiler indirilmesi	Bilinmeyen kaynaklardan bilinmeyen tipte dosya indirilmesine karşı dosya aktarım izleme, tarama ve alarm kullanılmalıdır.
Yerel kullanıcılara ulaşan bilinmeyen e-posta eklentileri ve gömülü URL bağlantıları	Bilinmeyen dosya türleri için e-posta sunucusu ve eklenti antivirüs ve e-posta karantinaya alma kullanılmalıdır, içerik filtreleme politikalarına dayalı olarak alan adı web sitesi erişimi durdurulmalıdır.
Web'de sörf yapan ve işlerine odaklanmayan yerel kullanıcılar nedeniyle oluşan verimlilik kaybı	İnternet giriş/erişim noktalarında alan-ismi içerik filtreleme kullanılmalıdır.

5. WAN Etki Alanı

Geniş Alan Ağı *(Wide Area Network* - WAN) Etki Alanı, uzak yerleri birbirine bağlamaktadır. Ağ maliyetleri düştükçe, kuruluşlar daha hızlı internet ve WAN bağlantıları alabilir hale gelmektedir. Bugün telekomünikasyon servis sağlayıcıları aşağıdakileri satmaktadırlar:

- **Ulusal optik omurgalar:** Özel optik omurga ağları için optik omurga gövdeleri.
- **Uçtan uca IP aktarımı:** Servis sağlayıcının IP ağ altyapısını kullanarak IP hizmetleri ve bağlantı.
- **Çok bölgeli WAN bulut servisleri:** Çok bölgeli *(multisite)* servisler için, Çoklu Protokol **Etiket Anahtarlama (Multi protocol Label Svvitching - MPLS)** WAN servisleri gibi IP servisleri ve bağlantı önerilmektedir. MPLS, WAN'daki uç noktalar arasında sanal bağlantılar yapmak için etiketler *(label)* veya *tag'ler* kullanmaktadır.
- **Metropol Ethernet LAN bağlantısı:** Şehrin alan ağı içinde sunulan Ethernet LAN bağlantısıdır.

- **Adanmış İnternet erişimi:** Genellikle bir kuruluş içinde paylaşılan geniş bant internet iletişim bağlantısıdır.
- **Yönetilen Servisler:** 24 x 7 x 365 yönlendirici yönetimi ve güvenlik cihazları yönetimidir.
- **Servis seviyesi anlaşmalar *(Service-level agreements* - SLA'lar):** Kullanılabilirlik, paket kaybı ve sorunları gidermek için tepki süresi *(response time)* gibi aylık servis hizmetleri için sözleşme taahhütleridir.

WAN Etki Alanı genel BT altyapısı için beşinci güvenlik katmanım temsil etmektedir. WAN servisleri, müşterilerin yönlendirici ve güvenlik duvarları için adanmış internet erişimi ve yönetilen servisleri içermektedir. Servis kesilmesine karşı kullanılabilirlik ve tepki süreleri için yönetim anlaşmaları yaygındır. WAN hizmetini kullanılabilir tutmak için ağlar, yönlendiriciler ve donanım sürekli izlenmeli ve yönetilmelidir.

WAN Etki Alanı Rolleri, Sorumlulukları ve İzlenebilirlik

Burada WAN Etki Alanı içinde nelerin olabileceği konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler:** WAN Etki Alanı hem fiziksel bileşenler hem de yönlendirici ve iletişim araçlarının mantıksal tasarımını içermektedir. Bir BT altyapısında güvenliği sağlamak bakımından ikinci en karmaşık alandır. Hedeflenen, giren ve çıkanın güvenliğinden emin olunurken kullanıcılara mümkün olan en fazla erişimi sağlamaktır.
  WAN Etki Alanındaki roller ve görevler aşağıdakilerin yönetilmesini ve yapılandırılmasını içermektedir:
  - **WAN iletişim hatları:** Bunlar binanızda sona eren dijital veya optik bir servis olarak sağlanan fiziksel iletişim bağlantılarıdır. Geniş bant bağlantı hızları aşağıdaki değerler arasında değişebilmektedir:
    - Dijital servis için DS0 (64 Kbps) DS1 (1.544 Mbps) ve DS3 (45 Mbps)
    - Optik servis için OC-3 (155 Mbps) OC-12 (622 Mbps) ve OC-48 (2.488 Mbps)
    - Fiziksel mesafeye bağlı olarak 10/100/1000 Mbps Metro Ethernet LAN bağlantısı
  - **IP ağ tasarımı:** Bu, IP ağının ve adres şemasının mantıksal tasarımıdır. Bu, ağ mühendisliğini, alternatif yol tasarımlarını ve IP yönlendirme protokolünün seçimini gerektirmektedir.
  - **IP durum denetlemeli güvenlik duvarı:** Bu, IP paketlerini filtrelemek ve istenmeyen IP, TCP ve UDP paketlerinin ağa girişine veya çıkışma engel olmak için kullanılan bir güvenlik cihazıdır. Güvenlik duvarları LAN segmentlerini korumak için iş istasyonları veya yönlendiricilere yüklenebilmekte veya bağımsız cihazlar olarak görev yapabilmektedirler.
  - **IP yönlendirici yapılandırılması:** Bu, uzak konumlara IP bağlantısı için kullanılan WAN omurgası *(backbone)* ve geliştirilmiş yönlendiriciler *(edge routers)* için gerçek yönlendirici yapılandırma bilgisidir. Yapılandırma İP ağ tasarımı ve adresleme şemasının üzerine inşa edilmelidir.
  - **Sanal özel ağlar *(virtual private networks* - VPN):** VPN, bir uç noktasından diğerine adanmış bir şifreli tüneldir. VPN tüneli ortak interneti kullanan bir uzak iş istasyonu ile bir VPN yönlendirici arasında veya güvenli bir tarayıcı ile bir **Güvenli Soketler Katmanı Sanal Özel Ağ (Secure Sockets Layer Virtual Private Network - SSL-VPN)** web sitesi arasında yaratılabilmektedir.
  - **Çoklu protokol etiket anahtarlama *(Multiprotocol Label Switching* - MPLS):** MPLS müşterilerin performansı maksimize etmesine olanak sağlayan bir WAN yazılım özelliğidir. MPLS, IP paketlerini belirlenmiş uç noktaları arasındaki sanal tünellerden hızlı aktarım için etiketlemektedir. Bu, Katman 1 Katman 3 üstüne bindirmeli ağ *(overlay netvvork)* biçimidir ve uzun ömürlü bir akış yapılandırıldığında veya dinamik olarak belirlendiğinde, yönlendirme işlevleri yol belirleme işlemini atlamaktadır.
  - **Basit Ağ Yönetim Protokolü (Simple Network Management Protocol- SNMP) ağ izleme ve yönetimi:** SNMP ağ cihazlarında izleme, alarm ve performans için kullanılmaktadır.
  - **Yönlendirici ve ekipman bakımı:** Donanım *ve firmware* güncellemelerini gerçekleştirmek, yeni işletim sistemi yazılımı yüklemek ve yönlendiriciler ve filtreleri yapılandırmak için bir gerekliliktir.

- **Sorumluluklar:** WAN Etki Alanından ağ mühendisi veya WAN grubu sorumludur. Bu hem fiziksel hem de mantıksal elemanları kapsamaktadır. Ağ mühendisleri ve güvenlik uygulamacıları tanımlanmış güvenlik kontrollerini tanımlanmış politikalara göre ayarlamaktadırlar. IP ağ mühendisliğinin karmaşıklığı nedeniyle birçok grubun günümüzde WAN ve yönlendiricilerinin yönetimini servis sağlayıcılardan (dışardan) destek olarak aldığına dikkat etmek gerekir. Bu hizmet, sistemin kullanılabilirliğini ve problemlerin çabuk çözüleceğini garanti altına alan SLA'ları içermektedir. Bir WAN bağlantı kesintisi olduğunda, müşteriler servis sağlayıcılarının **ağ operasyon merkezini *(netvvork operations çenter* - NOC)** ücretsiz bir telefon hattından aramaktadırlar.
- **İzlenebilirlik:** Kuruluşunuzun BT ağ yöneticisi, WAN Etki Alanını korumak, güncelleştirmek ve teknik destek sağlamak zorundadır. Genellikle, BT güvenlik direktörü şirketin WAN Etki Alanı güvenlik politikaları, standartları, prosedürleri ve yönergelerini karşıladığını garanti etmektedir.

Bazı kuruluşlar halka açık interneti kendi WAN altyapısı olarak kullanmaktadırlar. Bu daha ucuz olmasına rağmen, internet mesajların teslimatını veya güvenliğini garanti etmemektedir.

WAN Etki Alanında (İnternet) Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

Telekomünikasyon servis sağlayıcıları uçtan uca iletişim için WAN bağlantısı sağlamakla görevlidir. Servis sağlayıcılar önce kendi ağ altyapılarının güvenliğini sağlama sorumluluğunu üstlenmek zorundadırlar. WAN iletişim servislerine kaydolan müşteriler, hizmet sözleşmelerindeki sorumluluk şartlarını, koşullarını ve sınırlamalarını gözden geçirmelidir. Bu önemlidir çünkü kuruluşlar, yönlendirici yönetimi ve güvenlik yönetimi ile ilgili görevlerinin nerede başlayıp nerede bittiğini anlamalıdırlar.

Bir WAN hizmetleri sözleşmesinin en kritik yönü, servis sağlayıcıların sorun giderme, ağ yönetimi ve güvenlik yönetimi servislerini nasıl sağladığıdır. WAN Etki Alanı, beşinci savunma katmanının gerekli olduğu yerdir. **Aşağıdaki tablo** riskleri, tehditleri ve WAN Etki Alanının internet segmentinde bulunan zafiyetleri ve uygun risk azaltma stratejilerini içermektedir.

RİSK, TEHDİT VEYA ZAFİYET	**AZALTMA**
Açık, kamusal alanda, bağlanmak isteyen herkes tarafından kolayca erişilebilmektedir	Kabul edilebilir kullanım politikaları "RFC 1087: Etik ve internet (*Ethics and the Internet)*" belgesine uygun olarak uygulanmalıdır. Sistemlere yetkisiz erişim, BT altyapılarına yönelik kötü niyetli saldırılar ve kötü niyetli kesintilerden kaynaklanan maddi kayıplarla ilgili yeni yasalar için öncülük edilmelidir.
İnternet trafiğinin çoğu açık metin olarak gönderilmektedir	Şifreleme ve VPN tünelleri olmadan özel iletişim için interneti kullanımı yasaklanmalıdır. Veri sınıflandırma standardınız varsa, politikalar, prosedürler ve yönergeler hassasiyetle uygulanmalıdır.
Gizli dinlemeye (eavesdropping) karşı zayıf	Uçtan uca güvenli IP iletişim için şifreleme ve VPN tünelleri kullanılmalıdır. Veri sınıflandırma standardınız varsa, politikalar, prosedürler ve yönergeler izlenmelidir.
Kötücül saldırılara karşı zayıf	Katmanlı LAN'dan WAN'a güvenlik önlemleri, IP durum denetlemeli güvenlik duvarlarıyla DMZ, güvenlik izlemesi için IDS/IPS ve bilinmeyen e-posta dosya ekleri için karantina devreye alınmalıdır.
DoS, DDoS, TCP SYN taşkını, ve IP adres yanıltması (*spoofing)* saldırılarına karşı zayıf	TCP SYN "açık bağlantılar" ve ICMP (yankı isteği) ping paketlerini engellemek için dış İP durum bilgisi tutan güvenlik duvarlarına ve IP yönlendirici WAN arabirimlerine filtreler uygulanmalıdır, internet servis sağlayıcınızı *(Internet Service Provider*- ISP) IP yönlendirici WAN arayüzlerine CERT Advisory CA-1996-21 uyarınca uygun filtreleri yerleştirmesi konusunda uyarmalısınız. *www.cert.org/advisories/CA-1996-21.html* adresinde bulunabilir.
Bilgi ve verilerin bozulmasına karşı zayıf	VPN'lerle IP veri iletimleri şifrelenmelidir. Test edilmiş kurtarma prosedürleri ile veriler yedeklenmeli ve veriler şirket dışında konumlanmış veri kasalarına kaydedilmelidir (çevrimiçi veya fiziksel veri yedekleme).
Doğası gereği güvenli olmayan TCP/IP uygulamaları (HTTP, FTP, TFTP vb.)	Verilerin düzgün bir şekilde taşınması ve TCP/IP uygulamalarının kullanılması için veri sınıflandırma standardınıza bakmalısınız. Doğru şifreleme olmadan TCP/IP uygulamaları hiçbir zaman gizli veriler için kullanılmamalıdır. Bir ağ

	yönetimi VLAN'ı oluşturulmalı ve ağ yönetimi için kullanılan TFTP ve SNMP trafiği normal trafikten ayırılmalıdır.
Bilgisayar korsanları, saldırganlar ve suçluların **Truva atları** *(trojans),* **solucanlar** *(worms)* ve kötücül yazılım e-postaları	LAN'dan WAN'a Etki Alanındaki tüm e-posta ekleri tür, virüs ve kötü amaçlı yazılımlar için taranmalıdır. Daha fazla güvenlik incelemesi yapılıncaya kadar bilinmeyen dosya ekleri ayrılmalı ve karantinaya alınmalıdır. Çalışanlara bilinmeyen taraflardan gelen gömülü URL bağlantıları ve e-posta ekleri gibi tehlikeler hatırlatılmalı, bağlantıları tıklarken ve dosyalar açarken dikkat etmelerini sağlamak için güvenlik bilinci eğitimi verilmelidir.

Telekomünikasyon servis sağlayıcıları WAN bağlantı hizmetleri satmaktadırlar. Bazı sağlayıcılar günümüzde güvenlik yönetim hizmetlerini de sağlamaktadır. Aşağıdaki bölümde, WAN bağlantı riskleri, tehditler ve zafiyetler ve risk azaltma stratejileri sunulmaktadır.

WAN Etki Alanında (Bağlantı) Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

Telekomünikasyon şirketleri müşteri IP trafiğini hazırlamak ve aktarmaktan sorumludurlar. Bazen bu IP trafiği, kuruluş çapında paylaşılan genişbant erişimi sağlayan özel internet erişimi ile birlikte gelmektedir. Eğer, kuruluşlar WAN altyapılarını dış kaynaktan temin ediyorsa, yönetim ve güvenlik, bu dış kaynak servis sağlayıcısını da kapsayacak şekilde genişletilmelidir. Kuruluşlar güvenlik politikalarını ve ihtiyaçlarını, kendi güvenlik sağlayıcısının gereğini yapması için tanımlamalıdır. **Aşağıdaki tabloda** WAN Etki Alanı içinde bulunan bağlantı ile ilişkili riskleri, tehditleri, zafiyetleri ve uygun risk azaltma stratejilerini listelemektedir.

RİSK, TEHDİT VEYA ZAFİYET	**AZALTMA**
Aynı servis sağlayıcı yönlendiricisi ve altyapısı üzerinde WAN IP trafiğinin akması	Gizli veri aktarımları, VPN tünellerini kullanan servis sağlayıcı WAN üzerinden şifrelenmelidir.
Yüksek WAN servis kullanılabilirliğini korumak	WAN hizmet kullanılabilirliği SLA'ları edinilmelidir. Yüzde 100 kullanılabilirlik gerekliyse, yedek internet ve WAN bağlantıları uygulamaya koyulmalıdır.
WAN performansını ve verimliliğini en üst düzeye çıkarma	Uzak sistemlere, uygulamalara ve verilere erişirken WAN optimizasyon ve veri sıkıştırma çözümleri kullanılmalıdır. Güvenlik politikaları ile uyumlu bir şekilde, giden yönlendirici WAN arayüzlerinde erişim kontrol listeleri *(access control lists – ACL'ler)* etkinleştirilmelidir.
SNMP ağ yönetimi uygulamaları ve protokollerinin (ICMR, Telnet, SNMR, DNS vb.) kötü amaçlı kullanımı	Ayrı WAN ağ yönetimi VLAN'ları oluşturulmalıdır. SNMP yönetici ve yönlendirici IP adreslerinin LAN'dan WAN'a Etki Alanı üzerinden geçişine izin veren katı güvenlik duvarı ACL'leri kullanılmalıdır.
24 x 7 x 365 SNMP alarmları ve güvenlik izleme	Güvenlik operasyonları ve izleme dışardan hizmet olarak alınmalıdır. Servisler, yönetilen güvenlik dahil edilecek şekilde genişletilmelidir.

6. Uzaktan Erişim Etki Alanı

Uzaktan Erişim Etki Alanı *(Remote Access Domain),* uzak kullanıcıları kuruluşun BT altyapısına bağlamaktadır. Uzaktan erişim, sahada veya evde çalışan personel (örneğin, dış satış temsilcileri, teknik destek uzmanları veya sağlık uzmanları) için kritik önem taşımaktadır. Küresel erişim, internete, e-postaya ve diğer iş uygulamalarına, **Kablosuz Bağlantı *(Wireless Fidelity,* Wi-Fi)** erişim noktası bulabileceğiniz herhangi bir yerden bağlanmayı kolaylaştırmaktadır. Uzaktan Erişim Etki Alanının olması gereklidir ancak kullanımı tehlikelidir. Uzaktan Erişim Etki Alanı, internetten birçok risk ve tehdit getirmektedir.

Bugünün mobil çalışanı aşağıdakilere gereksinim duymaktadır:

- **Kesintisiz cep telefonu hizmeti:** Mobil çalışanlar, ofis ve destek ekipleriyle irtibat kurmak için cep telefonu servisine ihtiyaç duymaktadır.

- **Kritik iletişimler için gerçek zamanlı erişim:** Cep telefonlarında metin mesajlaşma veya **anlık mesajlaşma *(instant messaging*- IM) sohbetinin** kullanımı kısa sorulara hızlı yanıtlar sağlamakta ve kullanıcıların o anda yaptıkları işi tamamen kesmesini gerektirmemektedir.
- **Bir mobil cihazdan e-postaya erişim:** E-postaların cep telefonları, akıllı telefonlar, tabletler, PDA'lar veya **BlackBerry** cihazlarıyla entegrasyonu, kullanıcılara önemli e-posta mesajlarına hızlı bir şekilde yanıt verme olanağı sunmaktadır.
- **Geniş bant Wi-Fi İnternet erişimi:** Bazı ülke çapında servis sağlayıcılar günümüzde Wi-Fi geniş bant erişim kartları sunmaktadır. Büyük metropol alanlarında kablosuz erişim imkanına izin vermektedirler.
- **Yerel Wi-Fi bağlantı noktası *(hotspot):*** Wi-Fi bağlantı noktaları havaalanları, kütüphaneler, kafeler ve perakendeciler dahil olmak üzere çok sayıda bulunmaktadır. Çoğu ücretsizdir, ancak bazıları kullanıcıların erişim için ödeme yapmasını gerektirmektedir.
- **Ev ofisine geniş bant İnternet erişimi:** Evden çalışan personel geniş bant internet erişimine ihtiyaç duymaktadır. Bu servis genellikle VoIP telefon ve dijital TV hizmetleri ile birlikte verilmektedir.
- **Bir şirketin BT altyapısına güvenli uzaktan erişim:** Uzaktan çalışanlar, tüm IP veri aktarımlarını halka açık internet üzerinden şifrelemek için güvenli VPN tünellerine ihtiyaç duymaktadırlar. Bu durum, eğer özel verilere uzaktan erişilecekse kritik bir önem taşımaktadır.

Bu etki alanının kapsamı, internet ve IP iletişim yoluyla uzaktan erişimle sınırlıdır. Uzaktan Erişim Etki Alanının mantıksal yapılandırması, IP ağ mühendisliği ve VPN çözümleri gerektirmektedir. Bu bölüm birçok uzaktan kullanıcı için önemli olan bireysel uzaktan erişime ve büyük ölçekli uzaktan erişime yöneliktir. Uzaktan Erişim Etki Alanı, tipik bir BT altyapısı için altıncı savunma katmanını temsil etmektedir.

Uzaktan Erişim Etki Alanı için Roller, Sorumluluklar ve İzlenebilirlik

Burada Uzaktan Erişim Alanında ne olması gerektiği konusunda genel bir bakış sunulmaktadır:

- **Roller ve görevler:** Uzaktan Erişim Etki Alanı, mobil kullanıcıları halka açık internet yoluyla BT sistemlerine bağlamaktadır. Mobil kullanıcının internete bağlanabilecek nitelikte bir uzaktan erişim IP cihazı olmalıdır. Dizüstü bilgisayarlara ilave olarak, mobil kullanıcılar akıllı telefonlar, tabletler ve elde taşınır bilgisayarlar olarak PDA'lar kullanabilmektedirler. Bu cihazlarda bulunan mobil yazılım, telefon görüşmeleri, sesli posta, e-posta, metin mesajlaşma ve uzaktan web taramasını mümkün kılmaktadır.

  Uzaktan Erişim Etki Alanında gerekli olan roller ve görevler aşağıda listelenen unsurların yönetim ve tasarımını içermektedir:

  - **Cep telefonları, akıllı telefonlar, PDA'lar ve BlackBerry üniteleri:** Şirket tarafından verilen cihazlara, tanımlanmış politikalara göre güncel ürün yazılımı, işletim sistemi yazılımı ve yamalar yüklenmelidir. Politika, bu ekipman üzerinde parolaların kullanılmasını gerektirmelidir.
  - **Dizüstü VPN istemci yazılımı:** Kuruluşlar, LAN'dan WAN'a Etki Alanı ve uzak kullanıcı dizüstü bilgisayarları arasında VPN tünellerini kullandığında, o kuruluşların özel gereksinimlerini karşılayan ve o kuruluşun diğer yazılımlarıyla uyumlu çalışan VPN yazılımının seçilmesi gerekmektedir.
  - **Güvenli tarayıcı yazılımı:** Güvenli Hiper Metin Aktarım Protokolü *(Hypertext Transfer Protocol* - HTTPS) kullanan web sayfaları güvenli tarayıcılara ihtiyaç duymaktadır. HTTPS, güvenli tarayıcılar ve güvenli web sayfaları arasındaki veri aktarımım şifrelemektedir.
  - **VPN yönlendiriciler, VPN güvenlik duvarları veya VPN yoğunlaştırdılar:** Uzaktan erişim VPN tünelleri, VPN yönlendirici, VPN güvenlik duvarı veya VPN yoğunlaştırıcıda *(concentrator),* genellikle LAN'dan WAN'a Etki Alanı içerisinde sona ermektedir. Tüm veriler, VPN istemcisi (uzak dizüstü bilgisayar) ile VPN yönlendiricisi, güvenlik duvarı veya yoğunlaştırıcı arasında şifrelenmektedir - *tünel (tunnel)* adı da buradan gelmektedir.
  - **Güvenli Soketler Katmanı *(Secure Sockets Layer* - SSL)/VPN web sunucusu:** SSL güvenli bir web sayfası ile güvenli bir tarayıcı arasında 128-bit şifreleme kullanmaktadır. Bu şifrelenmiş VPN tüneli uzak web sayfasının veri paylaşımı için uçtan uca gizlilik sağlamaktadır.

- **Kimlik doğrulama sunucusu *(Authentication servet):*** Uzaktan erişim talep eden kullanıcıları doğrulamak için ikinci seviye kimlik doğrulama gerçekleştiren bir sunucudur.

- **Sorumluluklar:** Genellikle ağ mühendisi veya WAN grubu Uzaktan Erişim Etki Alanından sorumludur. Bu hem donanım bileşenlerini hem de mantıksal elemanları içermektedir. Ağ mühendisleri ve güvenlik uygulamacıları politikalara göre güvenlik kontrollerini hayata geçirmekten sorumludurlar. Bu sorumluluklar, Uzaktan Erişim Etki Alanı için donanım ve mantıksal uzaktan erişim bağlantısının bakımı, güncellenmesi ve sorunlarını gidermeyi içermektedir. Bu sorumluluklar aşağıdakilerin yönetimini gerektirmektedir:
  - IP yönlendiriciler
  - IP durum denetlemeli güvenlik duvarları
  - VPN tünelleri
  - Güvenlik izleme cihazları
  - Kimlik doğrulama sunucuları

- **İzlenebilirlik:** Kuruluşunuzun WAN ağ yöneticisi Uzaktan Erişim Etki Alanından sorumludur. Genellikle, BT güvenlik direktörü Uzaktan Erişim Etki Alanı güvenlik planlarının, standartlarının, yöntemlerinin ve yönergelerinin kullanıldığından emin olmalıdır.

Uzaktan Erişim Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

Uzaktan erişim tehlikelidir ancak mobil çalışanlar için gereklidir. Bu, satış temsilcileri, danışmanlar ve destek personeli gibi mobil bir iş gücüne dayanan kuruluşlar için geçerlidir. Kuruluşlar maliyetleri düşürdükçe, birçok kuruluş personelini evden çalışmaya teşvik etmektedir. Bu durumda, WAN halka açık internettir. Bu bağlantıları güvenli hale getirmek en öncelikli iştir. Kullanıcıları doğrulamak ve verileri şifrelemek için kuruluşun sıkı veri sınıflandırma standardı kullanılmalıdır.

Uzaktan erişim güvenlik kontrolleri aşağıda listelenen maddeleri kullanmalıdır:

- **Tanımlama *(Identification):*** Bir kullanıcı adı, oturum açma kimliği veya hesap numarası gibi kimlik bilgilerini verme sürecidir.
- **Kimlik doğrulama *(Authentication):*** *Uzak* kullanıcıların, kullanıcının iddia ettiği kişi olduğunu kanıtlayan süreçtir. En yaygın kimlik doğrulama yöntemi, bir parola sağlamaktır. Birçok kuruluş, **belirteç *(token)*** (donanım veya yazılım), biyometrik parmak izi okuyucu veya akıllı kart gibi ikinci seviye doğrulama hizmetleri kullanmaktadır. Bir belirteç, rastgele bir sayı gönderen bir donanım aygıtı veya kullanıcıya bir sayıyı metin olarak mesaj atan bir yazılım belirteci olabilmektedir. Biyometrik parmak izi okuyucu, kullanıcının parmak izi sistemde saklanan parmak iziyle eşleştiğinde erişime izin vermektedir. Akıllı kart, bir belirtece benzer şekilde davranan bir kredi kartına benzemektedir. Akıllı kartın, kullanıcıyı bir akıllı kart okuyucu üzerinden doğrulayan bir mikro işlemci yongası vardır.
- **Yetkilendirme *(Authorization):*** Belirli bir kullanıcıya, bir kuruluşun BT varlıklarını, sistemlerini, uygulamalarını ve verilerini kullanma haklarını verme sürecidir.
- **İzlenebilirlik:** Kullanıcı eylemlerini kaydetme işlemidir. Kaydedilen bilgiler çoğunlukla kullanıcıları sistem olayları ile ilişkilendirmek için kullanılmaktadır.

Aşağıdaki tabloda Uzaktan Erişim Etki Alanı riskleri, tehditleri ve zafiyetleri ile birlikte risk azaltma stratejilerini listelemektedir.

RİSK, TEHDİT VEYA ZAFİYET	AZALTMA
Kaba kuvvet (Brute-force) kullanıcı kimliği ve parola saldırıları	Periyodik olarak değiştirme (örneğin, her 30 veya 60 günde) gerektiren kullanıcı kimliği ve parola politikaları oluşturulmalıdır. Giriş şifreleri kullanılmalı, şifreler sekiz karakterden daha uzun olmalı ve şifreler sayı ve harf içermelidir.

Çoklu oturum açma denemeleri ve erişim kontrolü saldırıları	Oturum açma denemeleri girişimi için otomatik engelleme ayarlanmalıdır (örneğin, üç oturum açma girişimi başarısız olduktan sonra kullanıcı erişimi engellenmelidir).
BT sistemlerine, uygulamalara ve verilere yetkisiz uzaktan erişim	Hassas verilere, uygulamalara ve verilere birinci seviye (örneğin, kullanıcı kimliği ve parola) ve ikinci seviye (örneğin, belirteçler, biyometrikler ve akıllı kartlar) kimlik doğrulama güvenliği uygulanmalıdır.
Özel veri veya gizli verinin uzaktan ifşa edilmesi	Veritabanları veya sabit disklerdeki tüm özel veriler şifrelenmelidir. Veri çalınırsa, veri şifreli olduğu için hırsız onu kullanamaz veya satamaz.
Mevcut veri sınıflama standartlarını ihlal eden veri sızıntısı	Kuruluşun veri sınıflandırma standardına uygun olarak veri sızıntısı güvenlik izleme araçları ve izleme de dahil olmak üzere, LAN'dan WAN'a Etki Alanında güvenlik önlemleri uygulanmalıdır.
Mobil çalışanın dizüstü bilgisayarının çalınması	Çalışanın özel veya gizli veriye erişimi varsa sabit disk üzerindeki veriler şifrelenmelidir. Kayıp ya da çalınan bir dizüstü bilgisayar, kullanıcısı tarafından bildirildiğinde gerçek zamanlı cihaz kilitleme kuralları uygulanmalıdır.
Mobil çalışanın belirtecinin, diğer kimlik doğrulamasının çalınması	Bir belirteç kaybolursa veya bir kimlik doğrulama aracı tehlikeye düştüyse gerçek zamanlı cihaz kilitleme kuralları uygulanmalıdır.

7. Sistem/Uygulama Etki Alanı

Sistem/Uygulama Etki Alanı tüm kritik önem taşıyan sistemleri, uygulamaları ve verileri tutmaktadır. Yetkili kullanıcılar bu etki alanındaki birçok bileşene erişebilmektedir. Güvenli erişim, ikinci seviye kontrolleri gerektirebilmektedir.

Güvenlik kontrolleri, özel verileri ve fikri mülkiyet haklarını korumaktadır. Verileri şifrelemek, sahte kullanıcıları durdurabilmektedir. Veri arayan bilgisayar korsanları, insanların bunları nerede sakladığını ve nasıl bulacaklarını iyi bilmektedir. Verileri veritabanlarında ve depolama aygıtlarında şifrelemek, ek bir güvenlik katmanı sağlamaktadır.

İkinci seviye kimlik doğrulamasını gerektirebilecek uygulamalara örnekler aşağıda verilmektedir:

- **İnsan kaynakları ve bordro:** Sadece bordro bölümünde çalışan personelin bu özel verilere ve gizli bilgilere erişmesi gerekmektedir.
- **Muhasebe ve finans:** Üst düzey müdürler, sağlıklı iş kararları vermek için muhasebe ve finansal verilere erişmeye ihtiyaç duymaktadır. Mali verileri güvence altına almak, erişimi sadece veriye erişime gereksinim duyanlar ile sınırlandıran benzersiz güvenlik kontrollerini gerektirmektedir. Halka açık şirketler, güvenlik gerektiren Sarbanes-Oxley (SOX) uyum yasalarına tabidir.
- **Müşteri ilişkileri yönetimi *(Customer relationship management* - CRM):** Müşteri hizmetleri temsilcileri, müşteri satın alma geçmişi ve kişisel veriler içeren bilgiye gerçek zamanlı olarak erişmek zorundadır.
- **Satış siparişi girişi:** Satış uzmanları, satış siparişi girişi ve sipariş izleme sistemine erişmek zorundadırlar. Kişisel müşteri verileri güvenli bir şekilde tutulmalıdır.

Sistem/Uygulama Etki Alanı Rolleri, Sorumluluklar ve İzlenebilirlik

Bu bölümde Sistem/Uygulama Etki Alanında neler bulunması gerektiği konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler -** Sistem/Uygulama Etki Alanı, donanım, işletim sistemi yazılımı, uygulamalar ve verilerden oluşmaktadır. Bu etki alanı, donanım ve onun mantıksal tasarımını içermektedir. Bir organizasyonun görev kritik uygulamaları ve fikri mülkiyet varlıkları burada bulunmaktadır. Bu etki alanı fiziksel ve mantıksal olarak güvence altına alınmalıdır.

Sistem/Uygulama Etki Alanı kapsamını riskleri azaltma konusuna sınırladık. Bunlar arasında aşağıdaki maddeler bulunmaktadır:

- **Bilgisayar odalarına, veri merkezlerine ve kablo dolaplarına fiziksel erişim:** Personelin güvenli alana girmesine izin vermek için prosedür ayarlanmalıdır.
- **Sunucu mimarisi:** Sunucu kullanımlarını birleştirmek ve maliyetleri düşürmek için blade sunucular ve rafları kullanan birleşik bir sunucu tasarımı uygulanmalıdır.
- **Sunucu işletim sistemleri ve çekirdek ortamlar:** Yazılım güncelleştirme ve yamaları yüklenerek işletim sistemi yazılımlarının saldırıya açık olma süresi azaltılmalıdır.
- **Sanallaştırma sunucuları:** Fiziksel ve mantıksal sanal ortamları ayrı tutulmalı ve katmanlı güvenlik çözümleri buluta genişletilmelidir. Sanallaştırma, bir fiziksel sunucu kullanarak birçok işletim sistemi ve uygulamasının yüklenmesini sağlamaktadır.
- **Uygulama sunucularının sistem yönetimi:** Kullanıcılar için sürekli sunucu ve sistem yönetimi sağlamaktadır.
- **Veri sınıflandırma standardı:** Verilerin doğru şekilde işlenmesine ilişkin veri sınıflandırma standartları, prosedürleri ve yönergeleri gözden geçirilmelidir. Taşınırken ve depolanırken özel verilerin güvenliği sağlanmalıdır.
- **Yazılım geliştirme yaşam döngüsü *(Software development life cycle* - SDLC)—**Yazılım tasarlarken ve geliştirirken güvenli yazılım geliştirme yaşam döngüsü taktikleri uygulanmalıdır.
- **Test ve kalite güvencesi:** Güvenlik açıklarını ve yazılım zayıflıklarını doldurmak için sağlam yazılım testleri, nüfuz etme-sızma *(penetration)* testleri ve kalite güvence yöntemleri uygulanmalıdır.
- **Depolama, yedekleme ve kurtarma işlemleri:** Veri sınıflandırma standardında belirtilen veri saklama, yedekleme ve kurtarma planları takip edilmelidir.
- **Veri arşivleme ve saklama—**Politikalar, standartlar, prosedürler ve yönergeler dijital depolama ve saklama gereksinimleriyle karşılaştırılmalıdır.
- **İş sürekliliği planı *(Business continuity plan* - BCP)—**Bir iş etki analizi *(business impact analysis* - BIA) çalışması yapılmalıdır ve hangi bilgisayar kullanımlarının iş sürekliliği için kritik olduğuna karar verilmelidir. Her bir sistem için RTO'lar tanımlanmalıdır. İşin devam etmesi için en önemli olan şeylere odaklanan bir BCP hazırlanmalıdır.
- **Felaketten kurtarma planı *(Disaster Recovery Plan* - DRP) -** BCP'ye dayalı bir felaketten kurtarma planı hazırlanmalıdır. Önce en önemli bilgisayar sistemleri için DRP öğeleri başlatılmalıdır. Bir DRP ekibi ve uzak veri merkezi kurulmalıdır.

- **Sorumluluklar—**Sistem/Uygulama Etki Alanı sorumluluğu, sistem ve uygulamalar direktörü ve yazılım geliştirme direktörünün üzerindedir. Bu etki alanı aşağıdaki unsurları içermektedir:
  - Sunucu sistemlerinin yönetimi
  - Veritabanı tasarımı ve yönetimi
  - Sistem ve uygulamalar için erişim haklarının tasarımı
  - Yazılım geliştirme
  - Yazılım geliştirme proje yönetimi
  - Yazılım kodlama
  - Yazılım testi
  - Kalite güvencesi
  - Üretim desteği

- **İzlenebilirlik:** Sistem ve uygulamalar direktörü ve yazılım geliştirme direktörü, kuruluşun üretim sistemlerinden ve kullanımlarından sorumludur. BT müdürü genellikle Sistem/Uygulama Etki Alanı güvenlik politikalarının, standartlarının, prosedürlerinin ve yönerge ilkelerinin uygunluğundan sorumludur.

Sistem/Uygulama Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

Sistem/Uygulama Etki Alanı, kuruluşun verisinin adeta bir hazine olduğu yerdir. Bunlar kişisel müşteri verileri, fikri mülkiyet hakları veya ulusal güvenlik bilgileri olabilmektedir. Bunlar, bir BT sistemi içinde saldırganların en çok aradığı bilgilerdir. Bu hazineyi korumak her organizasyonun amacıdır. Veri kaybı, Sistem/Uygulama Etki Alanındaki en büyük tehdittir.

Bir veri sınıflandırma standardıyla, veri türleri benzer gruplar halinde izole edilebilmektedir. Veriler ne kadar önemliyse o kadar derin gizleyip saklamak gerekmektedir. Uzun süre depolanacak verilerin şifrelenmesi değerlendirilmelidir. **Aşağıdaki tabloda,** Sistem/Uygulama Etki Alanı için yaygın olan riskler, tehditler ve zafiyetler ile birlikte risk azaltma stratejilerini listelemektedir.

RİSK, TEHDİT VEYA ZAFİYET	**AZALTMA**
Veri merkezlerine, bilgisayar odalarına ve kablo dolaplarına izinsiz erişim	Tesisleri güvenli hale getirmek için personel ve ziyaretçiler için politikalar, standartlar, prosedürler ve yönergeler uygulanmalıdır.
Bakımların gerçekleştirilmesi için sunucuların kesinti süresi	Sunucuları, depolamayı ve ağ oluşturmayı bir araya getiren bir sistem oluşturulmalıdır.
Sunucu işletim sistemleri yazılım zafiyeti	Sunucu işletim sistemi ortamları için zafiyet penceresi tanımlanmalıdır. Güçlendirilmiş sunucu işletim sistemleri kullanılmalıdır ve bakımları düzenli olarak yapılmalıdır.
Doğası gereği güvenli olmayan bulut hesaplama sanal ortamlar	Ayrı VLAN'larda sanal güvenlik duvarları ve sunucu segmentasyonu uygulanmalıdır. Sanal bir güvenlik duvarı, sanal ortamlarda kullanılan yazılım tabanlı bir güvenlik duvarıdır.
istemci/sunucu ve web uygulamalarının güvenlik açığı içermeye yatkınlığı	Çalıştırmadan önce sıkı yazılım ve web uygulaması testleri ve penetasyon testleri yapılmalıdır.
Sistemlere yetkisiz erişim	ikinci seviye kimlik doğrulamanın sıkı kullanımı ile ilgili veri sınıflandırma standartları izlenmelidir.
Bireylerin kişisel verilerinin tehlikeye düştüğü veri ihlalleri	Özel veri öğeleri farklı veritabanlarına ayırılmalıdır. Arşivleme amacıyla, veritabanları ve depolama aygıtlarında yatan hassas veriler şifrelenmelidir.
Verilerin kaybolması veya bozulması	Aylık veri arşivleme için günlük veri yedekleme ve kurum dışı veri depolama yapılmalıdır. Belirlenmiş kurtarma süresi hedeflerine (RTO - recovery time objectives) uygun veri kurtarma prosedürleri tanımlanmalıdır.
Yedeklenen medyanın yeniden kullanılmasıyla yedeklenen verilerin kaybedilmesi	Uzun süreli depolama için tüm veriler dijital verilere dönüştürülmelidir. Tanımlanmış RTO'lara dayalı olarak yedeklemeler kurum dışı veri kasalarında tutulmalıdır.
Kritik iş fonksiyonlarının kurtarılmasının potansiyel olarak yararlı olamayacak kadar uzun zaman alması	Kritik uygulamalarda işlemlerin devamlılığı (kullanılabilirliği) için taktik-adımlar sağlayan bir iş sürekliliği planı geliştirilmelidir.
Felaketten sonra uzunca bir süre BT sistem kesintilerinin sürmesi	Operasyonları sürdürmek için görev, kritik uygulama ve verilerin geri kazanılmasına özgü bir felaketten kurtarma planı geliştirilmelidir.

BT Altyapısı Güvenliğindeki En Zayıf Halka

Kullanıcı, güvenlik açısından en zayıf halkadır. Bilgi sistemleri güvenlik uzmanları bile hatalar yapabilmektedir. İnsan hatası, herhangi bir organizasyon için büyük bir risk ve tehdittir. Hiçbir grup, herhangi bir kişinin davranışını tamamen kontrol edememektedir. Bu nedenle, her organizasyon kötü niyetli kullanıcılar, eğitimsiz kullanıcılar ve dikkatsiz kullanıcılar için hazırlıklı olmalıdır.

Aşağıda belirtilen stratejiler, riskin azaltılmasına yardımcı olabilmektedir:

- Her bir iş başvurusunun geçmişi dikkatlice kontrol edilmelidir.
- Her personel için düzenli bir değerlendirme yapılmalıdır.

- Hassas sistemlere, uygulamalara ve verilere erişim farklı personel pozisyonları arasında dönüşümlü yapılmalıdır.
- Sağlam uygulama ve yazılım testleri uygulanmalı ve kalite kontrolü yapılmalıdır.
- Tipik bir BT sisteminin yedi etki alanı boyunca düzenli olarak güvenlik planlan gözden geçirilmelidir.
- Yıllık güvenlik kontrol denetimleri yapılmalıdır.

Saygın ve etkili bir meslek oluşturmak için, bilgi sistemleri güvenlik uzmanları etiğe ve mesleki davranış kurallarına uygun hareket etmelidir. Bu bölüm, bu öğretinin neden mesleğin temelini oluşturduğunu açıklamaktadır.

Etik ve İnternet

Herhangi bir hava trafik kontrolörü olmadığını ve uçakların serbestçe uçtuğunu düşünün. Kalkış ve inişler son derece tehlikeli olacaktır. Muhtemelen çok daha fazla kaza olacaktır. Böyle bir durum ciddi bir karışıklık yaratacaktır.

İnanılması zor fakat siber uzayda *(cyberspace)* hava trafik kontrolörleri gibi işlev gören bir makam bulunmamaktadır. Daha da kötüsü, çevrim içi insan davranışları çoğu kez normal sosyal ortamlardan daha az olgundur. Siber uzay bugünün kötü adamları için yeni bir oyun alanı haline gelmiştir. Bu nedenle, sistem güvenlik uzmanlarına yönelik olarak talep hızla artmaktadır.

ABD hükümeti ve İnternet Mimari Kurulu *(Internet Architecture Board* - IAB), ABD vatandaşlarına yönelik internet kabul edilebilir kullanımı ile ilgili bir politika belirlemiştir. Bununla birlikte, bu bir yasa ya da bir görev değildir; çünkü siber uzay küresel olup kesin sınırları olmadığından bu politika uygulanabilir değildir. Kullanımı, sağduyu ve kişisel dürüstlüğe dayanmaktadır. Yukarıdaki kutuda verilen açıklama, IAB'nin etik ve internet standartlarını sunmaktadır.

Etik, kişisel dürüstlük meselesidir. Güvenlik mesleği, doğru olanı yapmak ve yanlış olanı durdurmaktır; interneti kullanmak herkesin paylaştığı önemli bir ayrıcalıktır. İnternet, sınırları, kültürel önyargıları olmayan önyargısız bir iletişim aracıdır. Kullanıcıların internete bağlanma hakkı vardır. Bu hak, minnettarlık duyulacak bir şeydir. Ne yazık ki, kötü adamlar suç işlemek ve sorun yaratmak için siber uzayı kullanmaktadır. Bu durum, sistem güvenlik uzmanlarına yönelik küresel bir ihtiyaç yaratmaktadır.

BT Güvenlik Politikası Çerçevesi

Siber uzay, kullanıcıların güvenliği konusunda bazı güvenceler olmaksızın gelişmeye devam edemez. Yasalar, kuruluşların kişisel verilerini mahrem tutmalarını gerektirmektedir. İşletmeler, herhangi birinin, şirket verilerini çalabilecekleri bir internet üzerinde etkin bir şekilde çalışamazlar.

BT güvenliği, herhangi bir kurumun hayatta kalabilmesi için çok önemlidir. Bu bölüm size bir BT güvenlik politikası çerçevesi *(security policy frametvork)* tanıtmaktadır. Çerçeve, riskleri ve tehditleri azaltacak politikalar, standartlar, prosedürler ve yönergelerden oluşmaktadır.

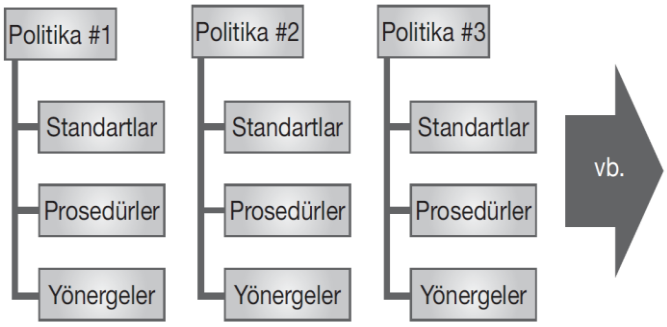
Tanımlar

Bir BT güvenlik politikası çerçevesi dört temel bileşeni içermektedir:

- **Politika *(Policy):*** Bir politika, bir kuruluştan sorumlu kişilerin bir dizi eylem veya yön belirlediklerini gösteren kısa bir yazılı ifadedir. Bir politika, üst yönetimden gelir ve kuruluşun tamamı için geçerlidir.
- **Standart *(Standard):*** Bir standart, donanım, yazılım ve bunların nasıl kullanılacağına ilişkin ayrıntılı bir yazılı tanımdır. Standartlar, BT sistemi boyunca tutarlı güvenlik denetimlerinin kullanılmasını sağlamaktadır.
- **Prosedürler *(Procedures):*** Bunlar, politikaların ve standartların nasıl kullanılacağıyla ilgili yazılı talimatlardır. Güvenlik kontrolleri için bir eylem planı, kurulum, test ve denetimi içerebilmektedir.
- **Yönergeler *(Guidelines):*** Bir yönerge, politikayı, standartları veya prosedürleri kullanmak için önerilen bir eylem yoludur. Yönergeler, kullanıma ilişkin olarak spesifik veya esnek olabilmektedir.

Aşağıdaki şekil, hiyerarşik bir BT güvenlik politikası çerçevesinin bir örneğidir. Politikalar bir kuruluşun tamamı için geçerlidir. Standartlar belirli bir politikaya özeldir. Prosedürler ve yönergeler kullanımın

tanımlanmasına yardımcı olmaktadır. Her bir politika ve standart içinde, tipik bir BT altyapısının yedi etki alanının etkisini belirleyiniz. Bu, BT altyapısı boyunca rolleri, sorumlulukları ve izlenebilirliği tanımlamanıza yardımcı olacaktır.



Temel BT Güvenlik Politikaları

Kuruluşunuzun BT güvenlik politikası çerçevesinin odak noktası, riskleri, tehditleri ve zafiyetleri azaltmaktır. Politika tanımını ve standartları pratik tasarım gereksinimleriyle ilişkilendirmek önemlidir. Bu tasarım gereksinimleri en iyi güvenlik kontrollerinin ve önlemlerin düzgün şekilde uygulanmasını sağlayacaktır. Politika bildirimleri *(statements),* standartlar, prosedürler ve yönergelere atıf yapmanın yanı sıra sınırlar belirlemelidir. Politikalar, yasa ve yönetmeliklere uymak için güvenlik kontrollerinin ve önlemlerinin nasıl kullanılması gerektiğini tanımlamaktadır.

Bazı temel BT güvenlik ilkelerine örnekler aşağıda listelenmektedir:

- **Kabul edilebilir kullanım politikası *(Acceptable use policy* - AUP):** AUP, kuruluşa ait BT varlıklarının kullanımı ile ilgili olarak izin verilen ve verilmeyen eylemleri tanımlamaktadır. Bu politika Kullanıcı Etki Alanına özgüdür ve bir kuruluş ile çalışanları arasındaki riski azaltmaktadır.
- **Güvenlik Farkındalığı Politikası: Bu** politika tüm personelin, kuruluşun güvenlik politikası kapsamında güvenliğin ve davranış beklentilerinin öneminin farkına varmasını nasıl sağlayacağını tanımlamaktadır. Bu politika, Kullanıcı Etki Alanına özgüdür ve kuruluşun güvenlik farkındalık tutumunu değiştirmeniz gerektiğinde devreye girmektedir.
- **Varlık sınıflama politikası:** Bu politika, bir kuruluşun veri sınıflandırma standardını tanımlamaktadır. Hangi BT varlıklarının kuruluşun misyonu için kritik olduğunu söylemektedir. Genellikle kuruluşun sistemlerini, kullanımlarını ve veri önceliklerini tanımlamakta ve tipik bir BT altyapısının yedi etki alanı içerisindeki varlıklarını belirlemektedir.
- **Varlık koruma politikası:** Bu politika, kuruluşların kritik öneme sahip BT sistemleri ve verileri için bir öncelik tanımlamasına yardımcı olmaktadır. Bu politika, bir kuruluşun **işletme etki analizi *(business impact analysis* - BIA)** ile uyumludur ve bir felâket sonrası kuruluşun faaliyetine devam etme kabiliyetini tehdit eden riskleri ele almak için kullanılmaktadır.
- **Varlık yönetim politikası:** Bu politika, güvenlik işlemlerini ve tipik bir BT altyapısının yedi etki alanı içerisindeki tüm BT varlıklarının yönetimini içermektedir.
- **Zafiyet değerlendirme ve yönetimi:** Bu politika, üretim işletim sistemi ve uygulama yazılımı için kuruluş genelinde zafiyet penceresi tanımlamaktadır. Bu politikadan kuruluş genelinde zafiyet değerlendirme ve yönetim standartları, prosedürleri ve yönergeleri geliştirilmektedir.
- **Tehdit değerlendirme ve izleme:** Bu politika, kuruluş çapında bir tehdit değerlendirmesi ve izleme otoritesi tanımlamaktadır. Bu politikanın, LAN'dan WAN'a Etki Alanı ve AUP uyumluluğu ile ilgili belirli ayrıntıları da içermesi gerekmektedir.

Kuruluşların BT güvenlik politikası çerçevelerini kendi ortamlarına uyarlaması gerekmektedir. Birçok kuruluş, BT kurulumlannın güvenlik değerlendirmesini yaptıktan sonra, politika tanımlarını gördükleri açıklara ve maruz kaldıkları güvenlik tehditlerine göre biçimlendirmektedir. Politikalar genelde kuruluşun üst düzey yönetimi ve hukuk bürosunun incelemesi ve onayını gerektirmektedir.

Veri Sınıflama Standartları

Bir veri sınıflandırma standardının hedefi ve amacı, bir kuruluşun farklı veri türlerini nasıl ele alması ve ne şekilde koruma altına alması gerektiği konusunda tutarlı bir tanım sağlamaktır. Güvenlik denetimleri farklı veri türlerini korumaktadır. Bu güvenlik kontrolleri tipik bir BT altyapısının yedi etki alanı içerisindedir. Prosedürler ve yönergeler, veri güvenliğini sağlamak için tipik bir BT altyapısının yedi etki alanı içerisindeki verilerin nasıl ele alınacağını tanımlamalıdır.

Son uyum yasalarına göre işletmeler ve kuruluşlar için, veri sınıflandırma standartları tipik olarak aşağıdaki ana kategorileri içermektedir:

- **Kişisel veri (Private data):** İnsanlar hakkında kişisel olarak tutulması gereken verilerdir. Yasal uyumluluk için kuruluşlar uygun güvenlik kontrolleri kullanmalıdır.
- **Gizli (Confidential):** Kuruluşa ait bilgi veya verilerdir. Fikri mülkiyet, müşteri listeleri, fiyatlandırma bilgileri ve patentler gizli verilere örnektir.
- **Yalnızca dahili kullanım (Internal use only):** Bir kuruluş tarafından dahili olarak paylaşılan bilgi veya verilerdir. Gizli bilgi ya da veriler dahil edilemese de, iletişim kuruluşu terk etmeye yönelik değildir.
- **Herkese açık etki alanı verileri (Public domain data):** Web sitesi içeriği, teknik incelemeler ve benzerleri gibi halkla paylaşılan bilgi veya verilerdir.

Kuruluşunuzun veri sınıflandırma standardına bağlı olarak, en yüksek hassaslık derecesine sahip verileri depolama aygıtlarında ve sabit sürücülerde olsa bile şifrelemek gerekebilmektedir. Örneğin, uzaktan erişim için ortak internet kullanırken şifreleme ve VPN teknolojisi kullanmak gerekebilmektedir. Ancak, dahili LAN iletişimi ve sistemlere, uygulamalara veya verilere dahili erişim, şifreleme kullanmayı gerektirmeyebilir.

Kullanıcıların, müşterilerin kişisel verilerine girmeleri kısıtlanabilmekte ve yalnızca belirli veri parçalarına erişebilmelerine izin verilebilmektedir. Müşteri hizmetleri temsilcileri, bir müşterinin tüm kişisel verilerine erişmeden müşteri hizmeti sağlayabilmektedir. Örneğin, müşterinin Sosyal Güvenlik numarası veya hesap numaralarının bütününü görülmeyebilmekte; yalnızca son dört basamak görünebilmektedir. Hassas veri öğesinin bazı karakterlerini gizleme yöntemi **maskeleme (masking)** olarak adlandırılmaktadır.

Kuruluşlar BT güvenlik politikası çerçevesini tanımlamaya bir varlık sınıflandırma politikası tanımlayarak başlamalıdır. Bu politika, karşılık olarak, kendini bir veri sınıflandırma standardı ile doğrudan karşılaştırmaktadır. Bu standart bir kuruluşun verilerini güvence altına alma ve koruma biçimini tanımlamaktadır. Veri sınıflandırma standardınızdan yararlanarak, tipik bir BT altyapısının yedi etki alanından herhangi birinde kişisel veya gizli verilerin dolaşıp dolaşmadığının değerlendirilmesi gerekmektedir. Verilerin nasıl sınıflandırıldığına ve kullanıldığına bağlı olarak, BT altyapısı boyunca uygun güvenlik kontrollerinin kullanılması gerekmektedir.