İletişim Teknolojilerinde Veri Güvenliği ve Uzaktan Erişim: VPN Kullanımı Üzerine Bir Vaka Çalışması

Data Security and Remote Access in Communication Technologies: A Case Study on the Use of VPN

Bilgi Yönetimi Dergisi

Cilt: 6 Sayı: 2 Yıl: 2023

https://dergipark.org.tr/tr/pub/by

Hakemli Makaleler

Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 02.04.2023

Kabul tarihi: 31.12.2023

Yayınlanma tarihi: 31.12.2023

Article Info

Date submitted: 02.04.2023

Date accepted: 31.12.2023

Date published: 31.12.2023

Anahtar Sözcükler

Yeni Medya, İletişim Teknolojileri, Veri Güvenliği

Keywords

New Media, Communication Technologies, Data Security

DOI numarası

10.33721/by.1275605

ORCID

0000-0001-9414-4053 (1)

0000-0001-9196-1875 (2)

Mustafa AYDEMİR
Bağımsız Araştırmacı, Dr., aydemirmustafa4@gmail.com

Vedat FETAH
Ege Üniversitesi, Bilgi İşlem Daire Başkanlığı, Yüksek Mühendis, vedat.fetah@ege.edu.tr

Öz

Yeni medya sisteminin önemli bir alanını oluşturan iletişim teknolojileri, yoğun enformasyon akışının gerçekleştiği mecralardır. Son yıllarda veri yönetimi konusunda çeşitli uygulama örnekleri bulunmaktadır. İletişim alanı internet üzerinden eklektik ve sanal etkileşimli bir yapıya dönüştüğünden yasal ve yasadışı kullanımlar güvenlik alanını çatışmalı hale getirmektedir. Medya kullanımı, bireysel ölçekte gerçekleştiği mecralar dışında genellikle toplumsal sistemin ihtiyaçları ve yönelimleriyle şekillenmektedir. Günümüzde bilgiye ulaşma, sınırsız ve uzaktan erişim sağlayabilme konusunda eğilimler artış göstermektedir. İletişim konusu, bireyler arası süreçlerden insan-makine etkileşim alanına doğru gerçekleşmektedir. Bu noktada veri güvenliği ile erişim politikalarında önemli çözüm araçları bulunmaktadır. VPN uygulamaları, hesap aktivasyonları üzerinden şifrelenmiş verilerin aktarımı veya uzaktan erişimi konularında son kullanıcılara önemli kazanımlar sağlamaktadır. Bilgi kaynaklarının ve ilgili alandaki veri tabanlarının önemli derecede hassasiyet içermesi, özellikle uzaktan erişim politikaları konusunda süreli ya da süresiz olarak çeşitli yetki matrisleriyle belirlenmektedir. Kurumsal veri güvenliğinin KVKK, ISO27001 ve Cumhurbaşkanlığı DDO gibi denetleme mekanizmalarıyla biçimlendirilmesi, sunucu ve güvenlik duvarı gibi araçlar ile ilgili ağ servislerinin yönetiminde siber güvenlik çözümlerini de zorunlu hale getirmektedir. Bu çalışma, sistem ve cihaz güvenliği konusunda geliştirilen bir senaryo üzerinden kurumsal bir VPN yapısını mimari ve uygulama arayüzü vaka çalışması yöntemiyle analiz etmektedir.

Abstract

Communication technologies, which constitute an important area of the new media system, are the media where intensive information flow takes place. There are various examples of applications in data management in recent years. Since the field of communication has turned into an eclectic and virtual interactive structure via the Internet, legal and illegal uses make the security field conflictual. Media use is usually shaped by the needs and orientations of the social system, except for the media where it takes place on an individual scale. Today, trends are increasing in terms of accessing information, providing unlimited and remote access. The subject of communication is decoupled from the interpersonal processes to the human-machine interaction field. At this point, there are important solution tools in data security and access policies. VPN applications provide important benefits to end users in the transfer or remote access of encrypted data through account activations. The fact that information sources and databases in the relevant field contain a significant degree of sensitivity is determined by various authority matrices, especially for remote access policies, for a period of time or indefinitely.

**Bu makalenin araştırma ve yayın süreci "Araştırma ve Yayın Etiğine" uygun şekilde yürütülmüştür.*

The formatting of corporate data security with supervision mechanisms such as KVKK, ISO27001 and Presidential DDO also makes cyber security solutions mandatory in the management of network services related to tools such as servers and firewalls. This study analyzes the structure of an enterprise VPN through a scenario developed for system and device security using the architecture and application interface case study method.

1. Giriş

Yeni medya, web tabanlı teknolojik sistemlerin dijitalleşme ve etkileşim politikalarına uyumlu bir biçimde geliştirdikleri postmodern bir iletişim modelidir. Bireysel ve kurumsal nitelikli medya kullanım politikaları, veri yönetimi, dağıtımı, erişimi ve güvenliği gibi birçok alandan oluşmaktadır. İnternet, enformasyon kaynağı ve ağ yönetim birimi olarak çeşitli uygulamaların iç içe geçtiği teknik iletişim ve bilgi yönetim yapısını temsil etmektedir. Medya ve iletişim teknolojileri konusunda yaşanan gelişmeler, internet kullanıcılarının ağ gereksinimleri ile zaman ve mekândan bağımsız olarak yakınsak teknolojiler üzerinden şekillendirmektedir. Yeni medya düzeninin önemli bir gösterge alanı olarak süreç içerisinde sürekli çevrimiçi olma davranışlarının dijitalleşmiş toplumun bir kuralı haline gelmesiyle mesai kavramı anlamını yitirmektedir. Son birkaç yıllık süreçte pandemi ve deprem gibi bölgesel ve küresel çaplı konular, uzaktan çalışma sisteminin önemini ortaya çıkardığından doğal bir iletişim erişimi alanı olarak VPN kullanımı da genel kabul düzeyine erişebilmektedir.

Günümüzde internet kullanımı her geçen gün artmakta ve her alanda daha fazla veri paylaşımı yapılmaktadır. Bu artan veri paylaşımı ile birlikte, internet kullanıcılarının özel bilgilerinin korunması konusu da önem kazanmaktadır. Sanal Özel Ağ (VPN), bu ihtiyaca cevap veren bir teknolojidir. VPN, internet bağlantısı üzerinden kullanıcıların özel verilerini koruyarak bir ağa bağlanmalarını sağlamaktadır. VPN teknolojisi, internet kullanıcılarının verilerini şifreleyerek, internet bağlantılarını güvenli hale getiren bir yapıya sahiptir. VPN, özellikle çevrimiçi işlemler (eğitim, satın alma, sistem izleme gibi) yapılırken kişisel verilerin korunması için önemli bir uygulama olarak düşünülmektedir.

VPN teknolojisi, kullanıcının coğrafi konumunu gizleyerek, kullanıcının IP adresini tespit etmek isteyenlerin erişimini de engellemektedir. Bu sayede kullanıcıların anonim kalması sağlanmaktadır. VPN teknolojisi, halka açık Wi-Fi ağlarında kullanıcıların güvenliğini artırmanın dışında, iş dünyasında yaygın olarak kullanılabilmektedir. İletişim teknolojilerinin yayılım gösterdiği günümüz dijital kültürünün önemli bir alanı olan uzaktan erişimli iletişim sağlamak üzere birçok işletme, çalışanlarının evden çalışmasına izin vermektedir. Bununla birlikte söz konusu kurumun ya da işletmenin özel verileri, çalışanların evlerindeki internet bağlantıları üzerinden paylaşıldığı için güvenlik riski de ortaya çıkmaktadır. Bu durum, veri güvenliği açısından risk oluşturabildiğinden nitelikli ve siber güvenliği iyi olan VPN araçları kullanmak suretiyle işletmeler, özel verilerin güvenliği konusunda daha iyi kontrol sağlayabilmektedir.

VPN teknolojisi, yasaklı sitelere erişmek isteyen internet kullanıcıları için de faydalı olabilmektedir. Bazı ülkelerde, belirli sitelere erişim çeşitli gerekçelerle engellenmekte ya da sınırlama getirilebilmektedir. Ağ kullanıcıları bu engelleri VPN kullanarak aşabilmektedir. Ancak, VPN kullanımı da bazı dezavantajları da beraberinde getirebilmektedir. Örneğin VPN kullanımı, internet bağlantısını yavaşlatabilmekte ve bazı web sitelerine erişimde sorunlar yaşatabilmektedir. Bazı ülkelerde internet sitelerinin yasaklanması ve erişim konusundaki politikalar dışında bazı durumlarda VPN kullanımı da yasaklanabilmektedir.

Günümüzde birçok VPN hizmeti mevcuttur ve her biri farklı özellikler sunmaktadır. Bu nedenle, kullanıcıların ihtiyaçlarına uygun bir VPN hizmeti seçmeleri önemlidir. İyi bir VPN hizmetinin, hızlı ve güvenilir olması dışında, veri kaydı tutmaması ve kullanıcıların gizliliğini koruması da önemlidir. VPN hizmetlerinde kimi zaman kullanıcılar, ücretsiz VPN hizmetlerini tercih edebilmektedir. Ancak ücretsiz VPN hizmetlerinin, genellikle reklamlarla desteklenmesi ve kullanıcıların verilerini kaydederek üçüncü taraflarla paylaşabilmesi güvenli internet ve korumalı internet protokollerini de devre dışı bırakabilmektedir.

Güvenli bir VPN hizmeti kullanmak için bazı durumlarda para ödemek gerekebilmektedir. VPN kullanımı, özellikle işletmeler için önemlidir. Ancak, tüm çalışanların VPN kullanması, işletmenin internet bağlantısını yavaşlatabilir. Bu nedenle, sadece özel verilere erişim gerektiren çalışanların VPN kullanması önerilmektedir. Yakın dönemde yaşanan veri güvenliği sorunları karşısında ulusal/küresel

bazlı veri yönetim politikalarıyla birlikte bireysel ve kurumsal ağ yönetimleri denetlenebilir bir standart ve kalite protokolleriyle birlikte dijital envanter gibi başlıklarda düzenlenmektedir. Bu durum, teknoloji konusunda ortak bir dil ve eylem planı gerçekleştirerek güncel teknolojik modellerin yönetiminde ilkeli bir düzen de sağlayabilmektedir.

2. Önceki Çalışmalar

VPN teknolojisi, internet kullanıcılarının verilerinin güvenliğini sağlanması için önemli bir protokoldür. Ayrıca, işletmeler için de özel nitelikli verilerinin korunması açısından sıklıklıkla tercih edilmektedir. İnternet kullanıcıları, kurum ağı ile etkileşim gerektiren durumlarda VPN teknolojisini kullanarak verilerinin güvenliğini şifreleme yöntemlerinin kullanılması ile daha güvenli hale getirebilmektedir. VPN hizmeti kullanmak, internet kullanımı sırasında kişisel verilerin güvenliği ve gizliliği için önemli bir adımdır. İnternet kullanıcıları, VPN teknolojisini kullanarak bağlantıları sırasında transfer etmiş oldukları verilerin daha güvenli bir kanaldan iletimini sağlayabilmektedir.

VPN protokolü, ağ üzerinden erişilebilen web tabanlı araçlar ile uçlar arasında veya farklı protokoller arasında güvenli iletişim kurmak amacıyla da kullanılmaktadır. VPN teknolojisinin kullanımı konusunda özellikle güvensiz bağlantı özelliği taşıyan uzak masaüstü konusu, kullanıcı ile araç arasındaki internet eksenli etkileşimin güvenli bir şekilde kurulmasını sağlamaktadır.

Uzak Masaüstü konusu, bağlantı ve protokol kavramlarıyla birlikte kullanılmaktadır. Erişim sağlanmak istenen bilgisayarlara fiziksel bir yakınlık ya da erişimin sağlanamadığı koşullarda bağlanmak üzere geliştirilen bir uygulamayı ifade etmektedir. Uzak masaüstü kavramı ilk kez 1954 yılında ele alınmıştır (Aburdune, 1991). Uzak masaüstü protokoller, teknolojik yapısı itibariyle değerlendirildiğinde, T120 serisi protokollere dayalı olarak tasarlanmıştır (ITU,1998). Uzak masaüstü protokolü (RDP), bir istemcinin bir Windows sunucusuyla iletişim kurmasını sağlamaktadır. RDP ile uzak bir istemciden bir sunucudaki uygulamaları çalıştırabilmektedir (Longzheng, vd.,2004; Lubonski, vd., 2005). Uzak masaüstü bağlantısı konusunda yapılan çalışmalarda (Malinowski, 2000) Laboratuvar tabanlı bir uygulama örneği üzerinden sistemi, Fujii ve Koike (2005) tarafından uzak masaüstü protokolü (RDP) konusunda, VNC tabanlı bir modelde VPN sistemi incelenmiştir. Longzheng vd., ağ trafiğinin sızmasını önlemek için kimlik doğrulama ve şifreleme kullanıldığı gerekçesiyle, kullanılan yöntemlerin güvenlik açıkları bulunabileceği ve siber saldırılarla karşılaşabileceği uygulama tabanlı bir çalışma gerçekleştirmişlerdir (Longzheng vd., 2004). Uzak masaüstü konusunun en çok kullanıldığı alanlardan birisi kuşkusuz e-öğrenme deneyimleri üzerinedir.

Uzak masaüstü bağlantı konusunu (Turing,1950; Holmes vd.,2019; Arslan,2020) içerisinde yapay zekanın eğitimde kullanım deneyimleri üzerinden ele alırken; diğer bazı araştırmacılar ise özellikle mevcut araçlardan üzerinden değelendirerek bunların en etkili şekilde kullanıldığı birkaç özel senaryo aracılığıyla konuyu incelemektedir (Ternauciuc ve Ivanc,2011; Arslan,2020). Dağıtılmış bilgi işlem ortamlarındaki temel bir sorun, bir ağ aracılığıyla güvenli kaynaklara otonom olarak erişmek için uzak bir bilgisayar sistemine güvenilip güvenilemeyeceğini belirlemeyi içeren çalışmalar bulunmaktadır. Örneğin Kennell ve Jamieson, uzaktaki bir bilgisayar sisteminin gerçek ve güvenilir olduğunu kanıtlaması için sorgulanabilecek bir yöntemi ve temsili bir bilgisayar sistemleri seti için bir özgünlük testinin uygulanmasını incelemişlerdir (2003). Uzak masaüstü erişimi, uzak ana bilgisayarın grafik ekranlarının sanallaştırılmasına ve bir ağ üzerinden bir istemciye sunulmasına olanak tanıyan kurumsal ağlarda yaygın olarak kullanılır ve istemci, tıpkı yerel masaüstü gibi uzak ana bilgisayardaki verilere ve uygulamaya erişebilir.

Huang vd., uzak masaüstü erişiminin güvenliğini denetlemek için proxy tabanlı yeni bir güvenlik denetim sistemi tasarlamış ve uygulamıştır. Sistemin içerisinde RDP, VNC ve X-Windows'un tüm erişim oturumlarını etkin bir şekilde izler ve kullanıcılardan gelen tüm grafik işlemlerini kaydederek tekrar oynatma işlevi sağladığını Performans testi sonucunda küçük işletmelerin çoğu için RDP oturumlarının tüm rutin denetim iş yükünün üstesinden gelmek için yalnızca bir proxy sunucusunun yeterli olduğunu gösterdiğini ortaya çıkarmışlardır (2009). Proxy tabanlı bir başka çalışmada ise cep telefonu üzerinden masaüstü bağlantısı kurmak üzere önerilen sistemin bir prototipi Android işletim sistemi kullanılarak uygulanmış ve bir Android işletim sistemine sahip sanal cihaz emülatörü üzerinde test edilerek, kullanıcı çabasını azaltmak ve cep telefonunun küçük ekranından kaynaklanan sorunları

çözmek için hücresel görüntüleyicide çeşitli işlevler sağlanmıştır (Kotkar vd.,2013; Ernest vd., 2015). VPN hizmetleri konusunda ön plana çıkan bir kavram olarak siber risk konusu çeşitli araştırmalarda ele alınmaktadır. Minghao vd., Windows 10 ve 7 platformlarındaki en popüler altı uzak masaüstü yazılımının yan kanal bilgi sızıntısını değerlendirmek için deneysel bir araştırma geliştirerek uzak masaüstü trafik şifreleme mekanizmasının yan kanal bilgi sızıntısını önlemek için yeterli olmadığını ve hem uzak masaüstü kullanıcılarının hem de sağlayıcılarının bu tür ciddi gizlilik sızıntısı sorunlarını tespit etmişlerdir (Minghao vd., 2019). VPN sisteminde bir sunucu bileşeni uzak bilgisayarda çalışır ve masaüstünü (yani ekranı) bir son kullanıcı cihazında çalışan istemci bileşeni ile paylaşmaktadır.

Son yıllarda siber güvenlik alanı ile veri güvenliği konusunda dikkat çeken bazı uygulamaların bir dizi güvenlik açığının tespit edilmesiyle, yaygın olarak kullanılan iki uzak masaüstü uygulamasında, Microsoft Uzak Masaüstü ve Real VNC'de bir dizi güvenlik açığı tespit edilmiştir. Bu alanda, Bitton ve Shabtai gibi araştırmacılar ise çalışmalarında bu konuda ağ tabanlı bir izinsiz giriş tespit sistemi (NIDS) önermişlerdir (2021).

3. VPN Mimarisi ve Tipolojileri

Enformasyon alanının; teknoloji, iletişim, etkileşim ve güvenlik ile ilgili eklektik hale gelmesinde kişiselleştirilmiş yapılar ile grup tabanlı eylemlerin önemli rolü bulunmaktadır. Yeni medya sistemiyle birlikte ağlar arası ilişkilere ve web tabanlı sistemlere yönelik evrensel ölçütlerde bazı protokoller ile iç yönetim ve denetime göre yapılan uygulamalara ağırlık verilmektedir. Günümüzde, bilişim ve teknoloji alanının temel etki alanlarından uzak kalmak bir tür gerileme ve dışlanma şeklinde düşünülmektedir. Briggs ve Burke'ye (2004, s.296) göre "Yeni iletişim teknolojileri daha bireysel seçeneklerin görülmesini ve duyulmasını sağlamaktadır". Teknolojinin özellikle sosyal ağlar üzerinden bireyleri ayrıştırması ya da sanal katılımcı kimliklere dönüştürmesine ek olarak kurumsal bazlı iş akış modellerinde de aktif katılım sağlamak önemlidir.

Bu noktada medyanın sosyo-psikolojik rolünün olması, gündemi ya da akışı kaçırma korkusuyla (FoMO) da ilişkilendirilmektedir. FoMO kavramı, literatür içerisinde ilk olarak 1985 yılında Watson ve Mayer tarafından kullanılmıştır (Batorski, 2011, s.24). Bu kavram, bazı görüşlere göre elektronik cihazların zorla kullanılması ve kontrol edilmesi hissiyle de bağlantılı olarak düşünülmektedir (Bright, vd., 2015). FoMO aynı zamanda, Aydemir'in ağ kullanıcıları üzerinde bir döngü de oluşturmaktadır (Aydemir,2018). Şekil 1'de görüldüğü üzere döngü konusu kullanıcı hesabı, bağlaşım, beğeni takip, gündemi yakalama ve etkileşim çabası ile kaygı endişe ve korku gibi dört farklı denklemden oluşmaktadır.

Şekil 1

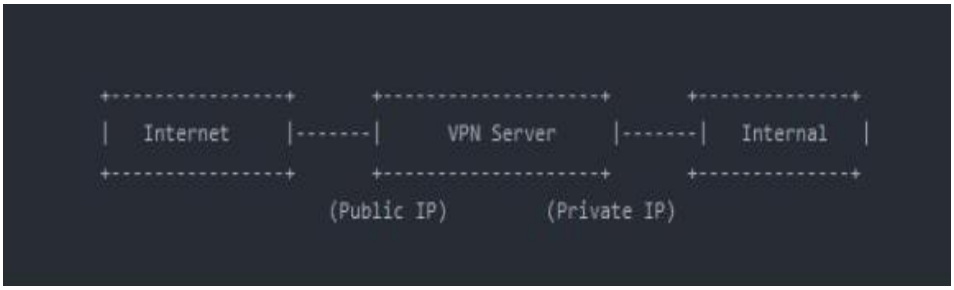
FoMO Döngüsünün Genel Görünümü (Aydemir, 2018, s.446)

FoMO kavramı, sadece medya içerikleri ya da sosyal ağlar ile sınırlı görülmemektedir. Bu görüş aynı zamanda teknolojik sistemler, kurumsal hesaplara erişim, iş düzeyinde yapılacaklar listelerine uyumluluk ve eğitim/e-eğitim modellerinde de geçerlilik kazanmaktadır. Son birkaç yılda pandemi, siber saldırılar, konvansiyonel savaşlar ile birlikte diğer sektörlerde olduğu gibi teknoloji alanı da

oldukça önemli hale gelmeye başlamıştır. VPN konusu da bu bağlamda yazılım ve mimari düzeyde ciddi bir gündem alanı haline gelmektedir. VPN mimarisi basit bir düzeyde aşağıda Şekil 2'de belirtildiği üzere üç temel araçtan oluşmaktadır. Bu araçlar, internet, VPN sunucusu ile Dahili yapılardan oluşmaktadır.

Şekil 2

Temel Bir VPN Mimarisinin Görünümü



VPN sistemi eş bağlantılara izin verecek şekilde kontrol edildiği ortak bir iletişim ağıdır (Ferguson ve Huston,1998). VPN, kullanıcının en az iki cihaz ile birbirinden farklı mekân ve ortamlar üzerinde erişim sağlamak, erişim paylaşımı oluşturmak ve yetkilendirme esaslarını; teknik altyapı ve yazılımlara göre değişkenlik göstermektedir. Bu model bir diyagram içermektedir. Bu diyagramda, üç bileşen bulunmaktadır. İlk aşamada *VPN Sunucusu*, gelen VPN bağlantılarını cihazınıza yönlendiren ve internet ve iç ağınız arasında güvenli trafik iletimi sağlayan sunucudur. İki ağ arabirimi vardır: biri internete bağlıyken diğeri dahili ağınıza bağlıdır. İkinci olarak *Dahili Ağ*, uzak yerlerden güvenli bir şekilde erişmek istediğiniz özel ağınızdır. Özel bir IP adresi aralığına sahip herhangi bir ağ olabilir. Son aşamada ise *Şifrelenmiş Tünel,* VPN sunucusu, internet ve dahili ağınız arasında bir ağ geçidi olarak hareket etmektedir. Uzaktaki bir cihazdan VPN sunucusuna bağlandığınızda, cihaz ve VPN sunucusu arasında şifrelenmiş bir "tünel" oluşturulur. Cihaz ve VPN sunucusu arasındaki tüm trafik şifrelenir ve herhangi biri tarafından ele geçirilemez veya okunamaz. Tünel kurulduktan sonra, dahili ağınızdaki kaynaklara fiziksel olarak orada bulunuyormuş gibi erişebilmek olanaklı hale gelmektedir. Bu, internetten erişilemeyen dosyaları, uygulamaları ve hizmetleri kullanmanızı sağlamaktadır.

VPN konusunda kullanım amaçları ve yetki esaslarıyla teknik uygulama modülleri üzerinden belirlenen çeşitli türler yer almaktadır. Başlıca VPN türleri arasında; PPTP (Point-to-Point Tunneling Protocol), L2TP/IPsec (Layer 2 Tunneling Protocol), Open VPN, SSTP (Secure Socket Tunneling Protocol), IKEv2 (Internet Key Exchange v2) gibi tipolojiler üzerinden çeşitlendirilmiş yapılar yer almaktadır (Krithikaa vd.,2016).

Sanal Özel Ağlar; Virtual Private Network (VPN), birçok farklı amaç için kullanılabilen bir teknolojidir ve internet üzerinden güvenli ve özel bir bağlantı sağlar. Kullanıcıların özel bilgilerini korumak için şifreli bir tünel oluşturur (Wood vd.,1988; Tarek ve Yasser,2011). Buna göre VPN türleri konusunda altı farklı türün olduğu saptanmıştır. Buna göre;

1. ***Uzaktan Erişim VPN:*** Uzaktan erişim VPN, kullanıcılara internet üzerinden şirket sunucularına güvenli bir şekilde erişim sağlamak için kullanılır. Bu tür VPN, şirket çalışanlarının işe bağlı kalmalarını ve evden veya uzaktan çalışmalarını sağlar. Bu VPN türü, genellikle işletmeler tarafından kullanılır ve kullanıcıların tüm trafiği şifrelenmektedir.

2. ***Site-to-Site VPN:*** Burada, ayrı ağlar arasında güvenli bir bağlantı oluşturmak için kullanılır. Bu VPN türü, bir şirketin iki veya daha fazla ofisi arasında iletişim sağlamak için kullanılmaktadır. Siteden siteye sanal özel ağlar, şirketler arasında hassas verilerin güvenli bir şekilde paylaşılmasını sağlar. Bu VPN türü, genellikle büyük işletmeler tarafından kullanılır ve tüm veri trafiği şifrelenmektedir.

3. ***Mobil VPN:*** Kullanıcıların seyahat ederken veya herhangi bir yerdeyken güvenli bir şekilde internete bağlanmalarını sağlar. Bu tür VPN, akıllı telefonlar ve tabletler gibi mobil cihazlarda kullanılabilir. Mobil VPN, kullanıcıların açık Wi-Fi ağlarını kullanırken özel bilgilerini korumalarını

sağlar. Bu VPN türü, genellikle seyahat eden iş insanları veya sık seyahat eden kullanıcılar tarafından kullanılmaktadır.

4. *Cloud VPN:* Bir veya daha fazla sanal sunucu üzerinde çalışan bir VPN'dir. Bu tür VPN, genellikle bulut hizmetleri sağlayıcıları tarafından sunulur ve kullanıcılara ölçeklenebilirlik ve yüksek kullanılabilirlik sağlamaktadır. Cloud VPN, genellikle küçük işletmeler veya bireysel kullanıcılar tarafından kullanılmaktadır.

5. *Layer 2 VPN:* Bu türün genel işleyişinde ayrı ağlar arasında güvenli bir bağlantı sağlanmaktadır. Bu tür VPN, ethernet bağlantılarına benzer şekilde çalışır ve veri trafiğini şifrelemektedir. Layer 2 VPN, genellikle ağ hizmet sağlayıcıları tarafından müşterilere sunulur ve kurumsal müşteriler tarafından kullanılmaktadır.

6. *SSL VPN:* SSL VPN, Secure Sockets Layer (SSL) protokolü kullanarak sanal özel ağ (VPN) bağlantısı sağlar. SSL VPN'ler, kullanıcılara internete bağlandıkları her yerden güvenli bir şekilde şirket kaynaklarına erişim imkânı sağlayan bir tür sanal özel ağdır.

VPN'ler birçok farklı tür ve tipolojide olabilir. Bazı VPN türleri, sanal özel ağlarını merkezi sunucularda yönetirken, diğerleri daha özerk bir yapıya sahiptir. Kullanıcıların ihtiyaçlarına ve hedeflerine göre farklı VPN türleri tercih edilebilir. Bu nedenle, doğru VPN türünü seçmek, kullanıcıların ihtiyaçlarını ve hedeflerini göz önünde bulundurmaları için önemlidir. VPN'ler, internet kullanıcılarının gizliliğini korumalarına ve internet erişimlerini güvence altına almalarına yardımcı olmak için tasarlanmıştır. VPN kullanım amaçları arasında şunlar yer almaktadır:

a) *Gizlilik ve Güvenlik*: VPN'ler, kullanıcıların internet faaliyetlerini gizli tutarak verilerinin üçüncü taraflar tarafından takip edilmesini önler. VPN'ler ayrıca, kullanıcıların internet bağlantılarını şifreleyerek, hackerların veya diğer kötü niyetli aktörlerin internet trafiğine müdahale etmesini önler.
b) *Sınırlı İçeriğe Erişim:* Bazı ülkeler belirli web sitelerine erişimi kısıtlayabilir veya engelleyebilir. VPN'ler, kullanıcıların bu engelleri aşmalarına ve engellenen içeriğe erişmelerine olanak tanır.
c) *Şirket İçi İnternet Erişimi*: Şirketler, çalışanlarının işle ilgili internet sitelerine erişimini sağlamak için VPN'ler kullanabilirler. Bu, şirketlerin bilgilerini ve verilerini korumalarına yardımcı olur ve çalışanların uzaktan çalışmasını kolaylaştırır.
d) *Halka Açık Wi-Fi Ağlarında Koruma:* Halka açık Wi-Fi ağları, kullanıcıların bilgilerini çalmak veya takip etmek için sıklıkla hedef alınır. VPN'ler, kullanıcıların bu riskleri minimize etmelerine yardımcı olur ve bilgilerinin güvende kalmasını sağlar.
e) *Çevrimiçi Alışveriş Güvenliği:* VPN'ler, kullanıcıların online alışveriş yaparken kişisel ve finansal bilgilerinin güvende kalmasını sağlar. Şifrelenmiş bir bağlantı kullanarak, hackerların bu bilgileri çalmasını önler.

3. 1. VPN Sunucu Sistem Gereksinimleri

VPN sunucusu, kullanıcılara internete erişim sağlarken aynı zamanda internet trafiğini şifreleyerek iletilmesini sağlamaktadır. Bununla birlikte, VPN sunucusu için doğru sistem gereksinimlerine sahip olmak da önemlidir. VPN sunucusuna temelde yedi farklı araç gerekmektedir. Bunlar; "CPU, RAM, Depolama, Ağ bağlantısı, İşletim sistemi, Güvenlik yazılımı ve Yedekleme" şeklinde sistematize edilmektedir. CPU merkezi işlem birimi olarak VPN sunucusu için veri şifreleme işlemi için yüksek bir işlem gücü gereklidir. VPN sunucusunun CPU'sunun yüksek bir saat hızına ve çok çekirdekli bir işlemciye de sahip olması gereklidir. Bu noktada günümüz işletim modelinde Intel Xeon veya AMD EPYC işlemci önerilmektedir. RAM, bilgisayar çevre birimi sınıfı olarak VPN sunucusunun veri şifrelemesi, kullanıcı kimlik doğrulama, günlük tutma ve veri yönetimi gibi işlemler için gerekli olan bir donanımdır. En az 64 GB DDR4 ECC RAM önerilmekle birlikte daha yüksek nitelikli bir RAM ile daha iyi performans sağlanacağı da kabul görmektedir. Depolama konusu; kullanıcı verileri, yapılandırma dosyaları ve günlükler gibi birçok veri depolanmasıdır. Sunucunun bu verileri depolayabilmek için yeterli bir depolama kapasitesine sahip olması önemlidir. 2 adet 1 TB boyutunda NVMe SSD RAID 1 disk yapısının depolama için yeterli olacağı öngörülmektedir. Ağ Bağlantısı, dördüncü sistem gereksinim ögesi olarak, kullanıcıların internete erişimini sağladığı için yüksek hızlı bir internet bağlantısına sahip olması gerekir. İdeal olarak, 2 adet 25 GbE ağ kartı ideal bir hız

sağlanması amacıyla önerilmektedir. İşletim Sistemi ise bir VPN sunucusunun çalışması için uygun bir işletim sistemi gereklidir. Linux tabanlı işletim sistemleri (örneğin, Ubuntu veya Debian) genellikle VPN sunucuları için tercih edilen seçenektir. Güvenlik Yazılımı, VPN sunucusu için internet trafiğini şifrelemek ve korumak için tasarlanmış bir yazılımı ifade etmektedir. Bir sistemde güvenlik yazılımı, sunucunun ve kullanıcı verilerinin güvenliği için kritik bir bileşendir. Sunucu bu bağlamda güncel ve güvenli bir VPN protokolü kullanarak iyi bir uyumluluk gösterebilmektedir. Son olarak Yedekleme modülü, veri kaybını önlemek için, VPN sunucusunun düzenli olarak yedeklenmesidir. Yedekleme hem sunucu yapılandırması hem de kullanıcı verileri için yapılmasıyla anlamlı hale gelmektedir.

VPN sunucuları, birçok faktöre bağlı olarak değişen sistem gereksinimlerine sahip olabilir. Bu nedenle, bir VPN sunucusu kurmadan önce doğru donanım ve yazılım gereksinimlerini belirlemek önemlidir. Ayrıca, sunucunun kullanılacağı amaç ve kullanıcı sayısı da dikkate alınmalıdır. İyi bir VPN sunucusu, performans ve güvenilirlik açısından yüksek standartlara sahip olmalıdır. Bu nedenle, birçok VPN sunucusu, sunucu donanımına ve yazılımına özel gereksinimlere sahiptir. Bunlar arasında yüksek bellek ve işlemci gücü, yüksek bant genişliği ve özel donanım güvenliği cihazları yer alabilir. VPN sunucularının ayrıca belirli bir işletim sistemi gereksinimi de olabilir. Örneğin, bazı VPN çözümleri sadece Windows işletim sistemlerinde kullanılabilirken, diğerleri Linux veya macOS gibi diğer işletim sistemleri üzerinde çalışabilir. Bu nedenle, sunucu işletim sistemi seçimi de doğru bir şekilde yapılmalıdır. VPN sunucu kurulumunun başarısı, sistem gereksinimlerinin doğru şekilde belirlenmesi ve uygun donanım ve işletim sistemi seçimi ile başlar. Bu nedenle, bir VPN sunucusu kurulumu planlanırken, her adımın doğru şekilde planlanması ve uygulanması önemlidir. Ayrıca, sistem gereksinimlerinin belirlenmesi ve sunucu donanımı ve işletim sistemi seçimi konusunda yetkin, profesyonel bir teknik destek almak da büyük önem taşımaktadır.

3. 2. VPN Erişim Yetki Matrisi ve Kontrol Yönergeleri

VPN'ler kurumsal ağlara uzaktan erişim sağlamak için yaygın bir çözüm olmaya devam ediyor. Ancak, birçok organizasyon, sadece yetkili kullanıcıların ağa erişmesine izin vermek için VPN erişim yetki matrisleri kullanmaktadır. VPN erişim yetki matrisi, belirli bir ağa erişim izni olan kullanıcıların listesini içeren bir dokümandır. Bu matris, her kullanıcının erişebileceği kaynakları belirleyerek ağ güvenliği sağlamak için tasarlanmıştır. Örneğin, bir şirketin VPN erişim yetki matrisi, belirli bir departmana ait kullanıcılara, diğer departmanlara ait kullanıcılardan farklı bir ağ erişimi sağlayabilmektedir. VPN erişim yetki matrisleri, ağa erişim izinlerini sınırlandırarak ağ güvenliğini artırmak için kritik öneme sahiptir. Bu matrisler ayrıca, şirket içindeki bilginin sadece yetkili kişiler tarafından görülebilmesini sağlamak için kullanılmaktadır.

Günümüzün dijital çağı, insanların hemen hemen tüm işlemlerini internet üzerinden gerçekleştirdiği bir çağdır. Bu durum, özellikle işletmeler ve kurumlar için büyük bir önem taşımaktadır. İşletmeler, çalışanlarının, müşterilerinin ve kendilerine ait diğer verilerin internet üzerinden korunmasını sağlamak zorundadır. Bunun için ise, işletmeler ve kurumlar, VPN kullanımına başvurarak, internet üzerinden veri transferlerini güvenli hale getirmeye çalışmaktadırlar.

VPN kullanarak, internet üzerinden yapılan tüm işlemler, bir nevi "tünel" içinden geçer ve bu sayede üçüncü kişilerin erişimine kapalı hale gelir. Ancak, VPN kullanımı da güvenlik açıkları oluşturabilir. Bu açıkları önlemek için, VPN erişim yetki matrisi gibi bir sistem kullanılabilir.

Bununla birlikte, birçok organizasyon, bu matrislerin oluşturulması ve yönetimi için yeterli kaynaklara sahip olmadığından, yanlış yapılandırılmış matrisler oluşturma riskiyle karşı karşıya kalır. Bu nedenle, doğru bir VPN erişim yetki matrisi oluşturmak, ağ güvenliği açısından son derece önemlidir. Bir VPN erişim yetki matrisi oluşturmak için öncelikle hangi kullanıcılara hangi ağ kaynaklarına erişim izni verileceği belirlenmelidir. Bu, bir şirketin çalışanlarının departmanlarına, görevlerine, sorumluluklarına ve ihtiyaçlarına göre belirlenir. Bu adım tamamlandıktan sonra, her kullanıcının ağa erişim seviyesi belirlenmelidir. Kullanıcılar, belirli bir ağ kaynağına erişim iznine sahip olabilirken, diğerleri bu kaynağa erişim sağlayamamaktadır. Bir VPN erişim yetki matrisi oluştururken, her bir kullanıcının ağa erişim izinlerini açıkça tanımlayan bir doküman hazırlamak önemlidir.

VPN erişim yetki matrisi, organizasyonların bir VPN kullanırken hangi kullanıcıların ne tür kaynaklara erişebileceğini kontrol etmelerine yardımcı olur. Bu matris, kullanıcılara atanan roller ve bu rollerin hangi kaynaklara erişebileceği ile ilgilidir. VPN erişim yetki matrisi oluşturmak, bir organizasyonun güvenlik politikalarını uygulamasına ve kaynakları korumasına yardımcı olur. Bu matris, bir organizasyonun belirli bir rol için VPN erişimi sağladığı tüm kaynakları belirleyebilir ve organizasyonun, VPN üzerinden sadece belirli kaynaklara erişim izni verdiği kullanıcıları belirlemesine yardımcı olabilir. Matrisin oluşturulması, ayrıca bir organizasyonun çalışanlarının VPN kullanarak iş faaliyetlerini yürütürken hangi risklere maruz kalabileceğini anlamasına yardımcı olabilir. Örneğin, belirli bir çalışanın VPN üzerinden bir veri tabanına erişebilmesi, organizasyonun en önemli varlıklarından birini açık hale getirebilir ve bu nedenle, bu tür bir erişimi sınırlandırmak, organizasyonun güvenliğini artırmaya yardımcı olabilir. VPN erişim yetki matrisi oluştururken, beş aşamalı olarak kaynak belirleme, rollerin tanımlanması, kullanıcıların atanması, güncelleme ve kullanıcıların yetkilendirilmesi gibi organizasyon adımlarını izleyebilmektedir.

Bu süreçte, her kullanıcının kimlik doğrulaması, kullanıcının adı ve parolası gibi bilgilerle yapılır. Bu doğrulama işlemi hem kullanıcının kimliğinin hem de şifreleme anahtarlarının güvenliği açısından son derece önemlidir. Bu nedenle, VPN hizmeti sunan şirketler genellikle kullanıcı yetkilendirme sürecinde güçlü şifreleme algoritmaları kullanırlar.

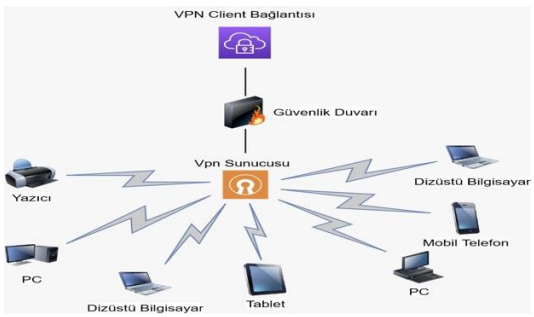
Ayrıca, VPN kullanıcıları genellikle farklı erişim seviyelerine sahiptir. Örneğin, bir şirketin yönetim ekibi, sadece kritik sistemlere erişebilirken, işçiler daha az kritik verilere erişebilirler. Bu nedenle, VPN erişim yetki matrisi, her kullanıcının erişebileceği kaynakları sınırlanması ve belirlenmesi için çeşitli yöntemler geliştirmektedir. VPN erişim kontrolü, bir VPN ağında erişim hakkına sahip olan cihazlar ve kullanıcılar için özel olarak tasarlanmış bir güvenlik mekanizmasıdır. Bu mekanizma, VPN ağını güvence altına almak ve yetkisiz erişimleri önlemek için kullanılmaktadır.

VPN erişim kontrolü, VPN sunucusu tarafından sağlanır ve ağda erişim izni verilen cihazlar ve kullanıcılar için belirli protokoller ve yöntemler kullanır. Bu protokoller arasında IPsec, SSL / TLS, L2TP ve PPTP gibi güvenli VPN protokolleri yer almaktadır.

VPN erişim yetki matrisinin oluşturulması, kurumun bilgi güvenliği politikalarının uygulanması için önemli bir adımdır. Bu yapı, işletmenin veya kurumun verilerinin güvenliğini arttırırken, aynı zamanda belirli kullanıcılara belirli kaynaklara erişim izni vererek iş süreçlerinin devamlılığını sağlar. Ancak, bu yapı sadece oluşturulmakla kalmaz, düzenli olarak güncellenmeli ve güvenlik politikaları ile uyumlu hale getirilmelidir. Aşağıda Şekil 3'de görüldüğü üzere VPN, kullanıcı bağlantısı çalışma diyagramı bağlantı, güvenlik duvarı sunucu ve bağlı araçlar (elektronik cihazlar) üzerinden genel durumu açıklamaktadır.

Şekil 3

VPN Kullanıcı Bağlantısı Çalışma Diyagramı



VPN erişim yetki matrisinin oluşturulması için belirlenen kriterler, güvenlik politikaları ile uyumlu hale getirilmelidir. Bu politikalar, kullanıcı yetkilerinin tanımlanması, erişimin sağlanacağı cihaz ve donanımların kurumun alan adı yapısına sahip olup/olmaması, erişimi sağlayan kullancının erişim amacıyla kullanmış olduğu cihaza ait uç noktadaki güvenlik önlemlerinin alınması ile VPN ağına dahil olmalarını sağlayabilecek bir düzende oluşturulmalıdır. Ayrıca, bu yapı düzenli olarak güncellenmeli ve gerektiğinde değiştirilmelidir. Kurumun güvenlik politikalarının değişmesi veya kullanıcının rolü

ile sorumluluklarının değişmesi gibi durumlarda gereklidir. Sonuç olarak, VPN erişim yetki matrisi, işletmenin veya kurumun bilgi güvenliği politikalarına uygun olaracak şekilde kullanıcı rol ve yetkileri oluşturulmalıdır. Bu yapı, belirli kullanıcılara belirli kaynaklara erişim izni verilmesi veya engellenmesi için bir kriter sağlar. Bu yapı, işletmenin veya kurumun verilerinin güvenliğini arttırırken, iş süreçlerinin devamlılığını sağlamaktadır.

3. 3. VPN Yönetiminde Ulusal Hukuki Esaslar

Türkiye'de son yıllarda uluslararası standartlar kapsamında ISO-27001 sertifikası için KVKK ve Cumhurbaşkanlığı DDO tarafından belirlenen çalışma sistemleri geliştirilmektedir. Bu konuda, evrensel gelişmelere bağlı olarak geliştirilen ve düzenlenen güncel yasal mevzuatlar gereği, ilk aşamada 2019 yılında Resmi Gazetede, Bilgi ve iletişim Güvenliği Tedbirleri başlığıyla 06.07.2019 tarih, 30823 sayı ve 2019/12 konulu Cumhurbaşkanlığı genelgesi yayınlanmıştır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin koordinatörlüğünde hazırlanan Bilgi ve İletişim Güvenliği Rehberi de hazırlananarak ilgili hedefler çerçevesinde, 10 maddelik bir hedef planlaması yapıldığı (Bk. Şekil 4) görülmektedir.

Şekil 4

Bilgi ve İletişim Güvenliği Rehberinin Hedefleri (BİGR,2020, s.12)

Cumhurbaşkanlığı BİGDES sistemi üzerinden tüm kurumlar yapmış oldukları çalışmalar sonucunda elde ettikleri verilerin girişlerini yapmakla mükellef hale getirilmiştir. Bu bağlamda VPN konusunda, tedbir numarası maddeleri uyarınca, tedbir seviyeleri ve tedbir tanımlarıyla toplamda 9 maddede gerekli düzenleme ve denetlemeler gerçekleştirilmektedir. Buna göre; 3.1.6.8 Tedbir numarası, 1 numaralı tedbir seviyesi ve "İnternet Ortamından Kurum İçi Kaynaklara Erişim" tedbir adı başlığıyla, (BİGR,2020, s.50) VPN teknolojisinin kullanımı ile kısıtlı süre ve yetkillerle yapılması konusu ele alınmıştır. Bir başka maddede ise 3.1.6.32 Tedbir numarası, 3 numaralı tedbir seviyesi ve "Kuruma Uzaktan Bağlanan Cihazların Yönetimi", (BİGR,2020, s.52) tedbir adı başlığıyla kuruma uzaktan bağlanacak cihazlara yönelik denetimler ile kurum politikasına uymayan cihazlara izin verilmemesi hususu belirtilmektedir.

Rehberde 3.1.7.7 Tedbir numarası, 1 numaralı tedbir seviyesi ve "Ağda Kritik Veri Taşınması", (BİGR,2020, s.57) başlığında kritik verilerin ağ üzerinden taşınmasında şifre kullanımı yine, 3.1.14.7 Tedbir numarası 1 numaralı tedbir seviyesi ve "Kurum Kaynaklarına Uzaktan Erişim" (BİGR,2020, s.80) başlığıyla, bir başka güvenlik tedbiri olarak çift faktörlü doğrulama ve en az yetki prensibiyle sınırlama getirilmesi konusu ele alınmakta ve 3.1.6.8 kod numaralı tedbire de referans yapılmaktadır. DDO rehberinde 3.1.14.18 3 numaralı tedbir seviyesi ve "Erişimin Kurum Bilgisayarları ile Sınırlandırılması" (BİGR,2020, s.80) başlığıyla ise uzaktan çalışma konusunda sadece kurum tarafından sağlanan cihazların erişim için kullanılması ve bu cihazların sertifikalarının kullanılması üzerinde önemle durulmaktadır.

Burada ayrıca "Akıllı Telefon ve Tabletlerin Kabul Edilebilir Kullanımı", "Bulut Ortamı Güvenliği", "Güvensiz Ağlar Üzerinden Güvenli Haberleşme", ve "Kullanıcı Erişim Yönetimi" başlıklarıyla da VPN yönetimindeki esaslar ve kurallar belirlenmiştir. VPN konusunda güncel hukuki düzenlemelerin temel amacı Dijital Dönüşüm Ofisi başkanlığınca, tüm kamu kurum ve kuruluşlarında ortak veri ağı yönetim politikasını oluşturmak, güvenlik risklerini azaltmak, gerekli tedbirleri almak, denetimleri yapmak ve evrensel düzeyde maliyet yönetimini belirleyerek nitelikli insan ve cihaz yönetimini gerçekleştirmek üzere protokoller hazırlanmaktadır.

4. Yöntem

Bilgi ve iletişim teknolojilerine duyulan ihtiyacın sürekli olarak artış göstermesi nedeniyle ulusal ve küresel düzeyde yapılan yatırımlar önemli bir pazar oluşturmaktadır. Bu pazarı şekillendiren küresel teknoloji şirketleri kullanıcıların değişen talepleri, ihtiyaçları ve ani gelişen olaylara göre yeni ürünleri piyasaya sunmaktadır. Son yıllarda teknolojik araçların internet tabanlı enformasyon edinim alanlarında kişisel ve kurumsal zafiyetlere uğraması nedeniyle veri gizliliği veri güvenliği ve kişisel bilgiler gibi önemli bilgilerin korunması ve muhtemel siber güvenlik riski karşısında uçtan uca korumalı, şifrelenmiş ve güvenilir veri iletimi protokollerinin kullanımına duyulan ihtiyaç artış göstermiştir. Bu bağlamda, son yıllarda nitelikli bir veri denetim mekanizması olarak VPN kullanımları önemli hale gelmektedir.

Gizlilik, güvenilirlik ve erişilebilirlik esaslarına uygun bir şekilde izinsiz ve yetkisiz girişimler ile kurum kaynaklarının manipüle edilerek veri sızdırılması işlemlerine önlem amacıyla kullanımı büyük önem arz etmektedir. Çalışmanın amacı söz konusu teknolojik gelişmelerin VPN yönetimi kapsamında nasıl işlendiğini incelemek, uygulanan protokollerin ve belirlenen yönergelerin de çalışma matrislerini ortaya çıkarmaktır. Bu araştırmanın önemi, kamu ve özel kurumlarda VPN kullanımı konusundaki ölçütlerin ulusal ve küresel hukuk kuralları çerçevesinde gün geçtikçe önemli hale gelmesi nedeniyle bu sistemin genel işleyiş yapısı ve mimarisinin çözümlenmesine ek olarak çalışma protokollerinin yönergeler düzeyindeki kapsayıcı hedeflerin, geliştirilen örnek bir bağımsız model üzerinden incelenmesidir.

Çalışma evreni olarak kurum içerisinde bulunan ve sadece yetkili personelin erişiminin bulunduğu internet üzerinden erişilebilen sistemler seçilmiştir. Örneklem kapsamında ise kamu kurumları içerisinde VPN kullanımının son yıllarda en fazla rağbet gördüğü eğitim faaliyetlerinde bulunulan bir kamu kurumu üzerinden örnek bir model belirlenerek VPN yapısı değerlendirilmektedir.

Araştırma kapsamında yöntem olarak vaka çalışması seçilmiştir. Vaka çalışmaları bilimsel araştırmalarda son yıllarda özellikle teknolojik alanlarda yeni modellerin sunumu ve yapılanma biçimlerinin tasarımsal yapılarının aktarımında tercih edilmektedir. Vaka çalışmalarını, Green ve Thorogood "Bir alan, birey veya politika olabilecek belirli bir vaka üzerine yapılan derinlikli çalışmalar" olarak belirtmektedir. (2009, s.284) Vaka çalışmasının aynı zamanda "fenomen olarak kabul edilen bir olay sınıfının örneği üzerinde araştırmacının o olayın örnekleri üzerinde benzerlikler ve farklılıkları ele aldığını" ileri süren bazı görüşler de bulunmaktadır (George ve Bennett, 2005, s.17).Vaka çalışmaları, "karmaşık bir konunun gerçek yaşam bağlamında derinlemesine, çok yönlü bir anlayışı oluşturmak üzere kullanılan bir yaklaşım olarak özellikle sosyal bilimler alanında yaygın olarak kullanılan yerleşik bir araştırma tasarımıdır" (Crowe vd., 2011, s.1). Web tabanlı sistemler ve siber güvenlik alanı içerisinde bu alanda ele alınan çalışmalarda (Du vd., 2011; Blanco vd.,2020; Macnish & Van der Ham, 2020; Palacin vd., 2020) internet tabanlı modellerin uygulanma modelleri incelenirken, senaryolaştırma pratiği konusunda (Güneş vd, 2021) yaptıkları çalışmalarla dijital sistemleri ve sanal denklemde yurttaşlık yapısını da değerlendirmektedir.

Araştırmanın kapsamı içerisinde VPN üzerinden inceleme yapıldığından, bilgi ve iletişim teknolojilerinin teknik alt yapılarının kullanım yönergeleri ile kullanıcıların yetki ve sınırlılıkları olarak belirlenmesi nedeniyle sadece yeni modelin görünümü ve arayüzü incelenmektedir. Araştırmanın sınırlılıkları ise anket, birebir mülakat, telefon görüşmeleri, deney ve gözlem tekniklerini kullanmaması bunun yerine yeni ve bağımsız bir çalışma modelinin uyumluluk yapısını genel prensipleri yönüyle ele almasıdır.

Kurumun çalışanlarının uzaktan erişim ihtiyacını karşılayabilmek için bir VPN çözümü kullanılmıştır. Bu bağlamda kurum içi kaynaklara erişim amacıyla kullanıcılara VPN istemcisi kurulumunu anlatan web sitesi oluşturulmuştur. VPN bağlantısı, şifreleme teknolojisi kullanarak tüm verilerin güvenliği ve bütünlüğünü korur. Böylece, çalışanlar evlerindeki veya seyahat sırasındaki internet bağlantılarından bile kurum içi ağa güvenli bir şekilde bağlanabilirler. VPN ayrıca, kamuya açık Wi-Fi ağlarına bağlanmak zorunda kalan çalışanlar için de büyük bir avantaj sağlamaktadır. Bu tür ağlar genellikle güvensizdir ve bilgisayar korsanları tarafından kullanıcıların kişisel bilgilerini ele geçirmek için hedef alınmaktadır. Ancak, VPN kullanıcısı olarak, tüm internet trafiğiniz şifrelendiği için, bu tehlikelerden korunmanız mümkündür.

VPN yönetimi ve ağ trafiğinin şekillendirilmesi konusunda dikkat edilmesi gereken bazı noktalar da bulunmaktadır. Örneğin, VPN kullanıcıları her zaman güçlü şifreler ve iki faktörlü kimlik doğrulama gibi ek güvenlik önlemleri kullanmalıdır. Ayrıca, VPN sunucusunun ve yazılımının güncel ve yeterince güvenli olduğundan emin olunmalıdır.

Bu çalışma kapsamında kullanılan çalışma ortamı, eğitim veren bir kamu kurumu örneği üzerine geliştirilmiştir. Ancak çalışma kapsamında kullanılan yöntemler arasında anket, görüşme, deney ve gözlem yöntemleri kullanılmamıştır.

4. 1. Bulgular ve Analiz

Bir VPN kullanımının sistematize edilmesinde üç aşamalı çalışma modeli oluşturulmaktadır. İlk olarak VPN yönergesi oluşturularak, bir işletmenin VPN'leri nasıl kullanması gerektiğini belirten bir doküman hazırlanmaktadır. Yönerge, birçok farklı bileşenden oluşur, ancak çoğu, işletme için doğru VPN teknolojisinin seçiminden başlayarak, VPN'lerin nasıl yapılandırılacağı, kimlerin VPN'ye erişebileceği, hangi verilerin VPN üzerinden iletilip hangilerinin iletilmeyeceği ve VPN'in güvenliği gibi konuları kapsamaktadır.

Yönerge, işletme ihtiyaçlarına özel olarak hazırlanmalı ve tüm çalışanlar tarafından anlaşılabilir bir dil kullanılarak yazılmalıdır. Ayrıca, yönerge düzenli olarak gözden geçirilmeli ve güncellenmelidir. İşletmeler, yönergelerini, VPN teknolojilerindeki değişiklikleri takip edecek şekilde güncellemelidir. Oluşturulan VPN yönergesine uygun bir talep formu tasarlanarak birimlerden erişim istekleri resmi olarak alınmalıdır. Örnek bir form içeriğinde erişim isteğinde bulunan birim/personel bilgileri, erişilecek sistemin IP adresi ile birlikte MAC adres bilgisinin yanında kişiye ulaşabilecek iletişim bilgileri bulunmalıdır. Ayrıca oluşturulan bu talep formu herkese açık olarak hizmet veren bir web sitesi üzerinde yayınlanmalıdır. VPN uygulama aşaması, işletmenin bir VPN kullanırken izleyeceği adımların bir planını içerir. VPN'nin doğru bir şekilde yapılandırılması ve kullanılması, işletmenin siber güvenliği için son derece önemlidir. İşletmeler, aşağıdaki adımları izleyerek VPN uygulamasını gerçekleştirebilmektedir.

a. *İşletme İhtiyaçlarını Belirleme:* İşletme ihtiyaçlarına uygun bir VPN teknolojisi seçmek önemlidir. İşletmelerin, ihtiyaçlarını belirleyerek doğru teknolojiyi seçmeleri gerekir. Bu doğrultu da VPN'lerin farklı protokolleri vardır. En yaygın protokoller arasında PPTP, L2TP / IPSec, Open VPN ve IKEv2 yer alır. Her protokolün kendine özgü avantajları ve dezavantajları vardır. Bazıları daha hızlıdır, bazıları daha güvenlidir ve bazıları daha kolay kurulur.
b. *VPN Kurulum ve Kullanım Yönergesi Hazırlama:* İşletmeler, kullanacakları VPN için bir yönerge hazırlamalıdır. Yönerge, VPN'nin nasıl kullanılacağına ve kimlerin VPN'ye erişebileceğine dair ayrıntıları içermelidir.
c. *VPN Yönergesi ve Uygulama Aşamaları:* VPN'ler, işletmelerin özellikle uzaktan çalışanların güvenli erişimini sağlamalarına ve aynı zamanda iş verilerinin korunmasına yardımcı olurlar. Ancak, VPN'lerin doğru bir şekilde uygulanması önemlidir.

VPN Yönergesi, bir işletmenin belirli bir konu veya prosedürle ilgili resmi bir dokümanıdır. Bu doküman, belirli bir konuda kuralları ve prosedürleri belirleyerek, bir işletmedeki herkesin aynı saygı, tutum ve yaklaşımla hareket etmesini sağlar. VPN Yönergesi, VPN kullanımının amacını, kimlerin erişebileceğini, kimlerin erişemeyeceğini, hangi cihazların kullanılabileceğini, nasıl kurulacağını ve

nasıl kullanılacağını belirler. Bu şekilde, herkesin VPN kullanımı konusunda bilgili ve güvende olması sağlanır.

Kuruma ait bir VPN yönergesi hazırlarken, belirli bir süreç takip etmelidir. İlk olarak, yönerge için bir ekip belirlemek önemlidir. Bu ekip, işletmedeki farklı departmanlardan ve uzmanlıklardan insanları içerebilir. Bu, yönergenin, tüm departmanların ihtiyaçlarını karşılamasını sağlayacak ve herhangi bir güvenlik açığı veya riske karşı koruma sağlayacaktır. Daha sonra, yönergenin amacı belirlenmelidir. Amacı belirlemek, yönergenin tüm departmanların ihtiyaçlarını karşıladığından emin olmak için önemlidir. Bu aynı zamanda, yönergenin odaklanacağı alanları belirleyecektir. Örneğin, VPN yönergesinin amacı, işletmenin uzaktan çalışanlarının VPN kullanımını belirlemek ve düzenlemek olabilir.

Sonraki adım, yönergede yer alacak politikaları belirlemektir. Bu politikalar, VPN kullanımını belirleyecek olan kuralları ve prosedürleri belirler. Politikalar, belirli cihazların kullanımına izin verme, belirli ülkelerden gelen bağlantıları reddetme, belirli saatlerde bağlantı kurmaya izin verme veya belirli dosya türlerinin gönderimini engelleme gibi konuları ele alabilir. Yönergede yer alacak politikalar belirlendikten sonra, politikaların nasıl uygulanacağı belirlenmelidir. Bu konuda oluşturulacak bir Sıkça Sorulan Sorular bölümü ile VPN kullanıcılarının her zaman erişebileceği bir web sayfasında yayınlanmalıdır. Bu bölümde VPN kurulumu, kullanımı ve sıklıkla karşılaşılabilecek hatalarla ile ilgili bilgilendirmelerin yapılması önem arz etmektedir.

4. 2. VPN Kurulum ve Yönetim Senaryosu

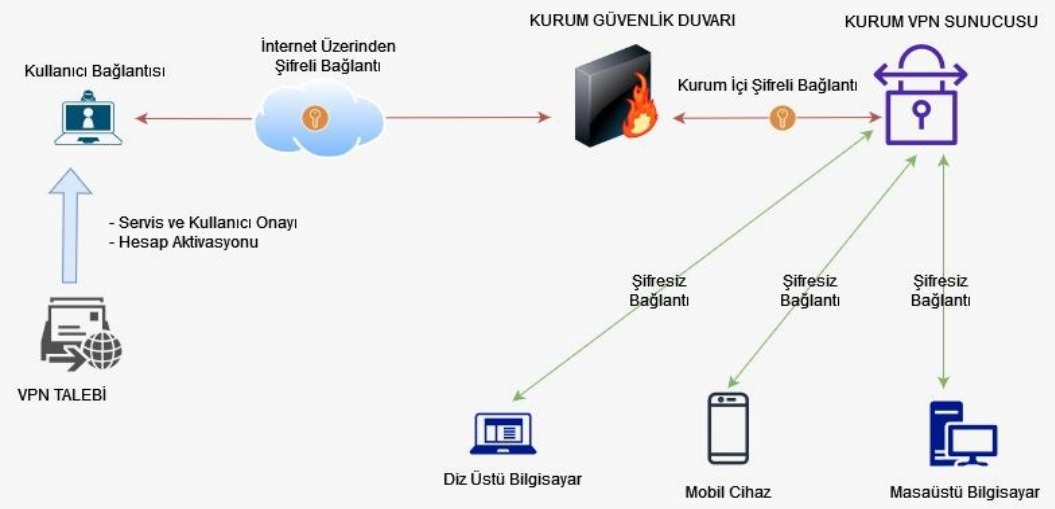
Araştırma kapsamında nitelikli bir vpn senaryosunun oluşturulması için bir kamu kurumunda bulunan yaklaşık 800 VPN kullanıcısının erişim ihtiyaçları doğrultusunda uzak masaüstü bağlantısı veya diğer erişim protokollerini kullanarak kuruma ait bilişim kaynaklarına erişim sağladığı bir yapı oluşturulmuştur. Bu model ortalama 15000 kişinin çalıştığı ve hizmet aldığı bir kurum üzerinden ele alınmaktadır. Araştırmanın önemli bir bölümünü oluşturan ölçütler konusunda VPN kullanıcılarının akademik ve idari kadroda bulunan kişilere tahsis edilmesi, öğrencilerin ise kamu kaynaklarına erişim kontrolü yönergelerine uygun olmaması nedeniyle kapsam dışı bırakılmasına karar verilmiştir. Yine VPN kullanımında ulusal sınırlar dışında uluslararası sınırlar göz önünde bulundurularak yurt içi erişimin yanı sıra yurt dışından bu kaynaklara erişim sağlayabileceği bir erişim yönergesi oluşturulmuştur. Sistem içerisinde en az bir bağlantı cihazı (cep telefonu, tablet, bilgisayar) üzerinden bağlantının gerçekleştirilebilmesi hedeflenmiştir. Bu bağlamda gerektiğinde tekli gerektiğinde çoklu kaynak konfigürasyonu kullanılarak VPN senaryosu uygulanmıştır.

Bu çalışmada, bir eğitim kurumuna ait internet üzerinden erişilebilen varlıkların kurum dışında da yönetimini sağlamak, gerekli hallerde (personelin izinde olması, kurum dışı toplantıda bulunması, vb…) ihtiyaç duyulan işleri yürütmek için sistemlere hızlıca ve güvenilir bir şekilde ulaşılmasına imkân tanımak amacıyla VPN mimarisinin nasıl oluşturulacağı incelenmektedir. Bu çalışmada kullanılan veriler için X Üniversitesi Bilgi İşlem Daire Başkanlığı'ndan 04.05.2023 tarihli ve E.1253825 sayılı resmi yazı ile izin alınmıştır.

Araştırma kapsamında bağımsız bir vpn yönergesi sistematize edilmiştir. Çalışma kapsamında bu yönergenin işleyiş modülleri aşamalı olarak değerlendirilmiştir. Burada kullanılması planlanan VPN senaryosunun kriz anlarında (pandemi, deprem, vb.…) kurumun ihtiyaçlarını karşılaması ve işleyişin sürekliliğinin sağlanması amacıyla hayati önem arz etmektedir. Bu sebeple kurum içerisinde yapılandırılacak VPN sunucusunun kapasite planlamasının iyi bir şekilde yapılması gerekmektedir. Bu konuda dikkat edilmesi gereken parametreler ise uygulama sunucusunun kurulacağı donanımın üzerinde çalışacağı işletim sisteminin seçimi hem kaynak tüketimi hem de sunucu güvenliğini sağlanması açısından önemlidir. Kapasite planlaması yapılırken kurum içerisinde bu hizmetten faydalanacak olan personel sayısının iyi tespit edilmesi sunucu kaynak tüketimi değerlerinin hesaplanması açısından da yaklaşık değer olarak bilinmelidir.

Şekil 5

Kullanıcı Tabanlı Yönerge Senaryosuna Göre VPN Diyagramı



Şekil 5'te verilen görselde örnek bir VPN sunucu senaryosu verilmiştir. Daha önceki aşamalarda da belirtildiği üzere oluşturulan formlar ve yönergeler dikkate alınarak ilk önce kullanıcı ya da birim talebi alınmaktadır. Talebin uygulayıcılar tarafından uygun görülmesinin ardından kullanıcı ile ilgili ayarlamalar VPN sunucusu üzerinde tanımlanarak erişim bilgileri ve kurulum detaylarını içeren bilgilendirme talep eden birime iletilmelidir. Bu işlemlerden sonra kullanıcı yönergelere uygun olarak kurduğu VPN istemcisi ile internet üzerinden bağlantı gerçekleştirebilecek ve isteği ulaşmak istediği sunucuya kullanım politikasına uygun bir şekilde gerçekleşecektir. İstemci ve sunucu arasında kurulan bağlantı, sunucu yapılandırılması sırasında belirlenen şifreleme algoritmasına uygun olarak şifreli bir şekilde sağlanmalıdır.

5. Sonuç ve Öneriler

Bilgi ve iletişim teknolojilerinin, web tabanlı sistemler ve sanal eklentili ağ modelleriyle kurduğu etkileşimli yapılar, dijitalleşme süreçlerini de önemli ölçüde etkilemektedir. Günümüzde kişisel, özel ve kurumsal ölçekte tüm iletişim kanallarında zaman ve mekân sınırının yakınsak teknolojilerle kaldırılması sonucunda ortaya çıkan enformasyon akışı verilerin doğru analiz edilmesi ve kesintisiz olarak ihtiyaçların sağlanması noktasında da kullanılmaya başlanmıştır. İnternet, bireysel ya da toplu olarak erişim sağlanan sanal uzamda bağlantı kurulmasına kaynak oluşturmaktadır. İletişim alanında, özellikle ulusal sınırların aşılması, kültürel uyumluluk ve veri aktarımlarının düzenlenmesi gibi konularda, sanal düzlemde çeşitli uygulamalar geliştirilmektedir. Bu uygulamalar arasında, sanal özel ağlar ile verilere uzaktan erişim ya da aktarım imkanı sağlama yönelimi öne çıkmaktadır. Özellikle dış katılımcılara olan ihtiyacın artması, sanal-sosyal kimliklerin talepleri ve anlık veri akışı ihtiyaçları göz önüne alındığında, yeni iletişim politikaları ve stratejilerinin belirlenmesi zorunlu hale gelmektedir.

Kurumsal kaynaklara erişim amacıyla kullanılan VPN sunucuları sayesinde kuruma ait bilişim kaynaklarının belirli servislerinin tüm dünyaya erişime açılması yerine sadece ilgili kişilerin erişimine sunulması ile oluşabilecek siber güvenlik tehditleri minimum seviyelere indirilmiş olmaktadır. Ayrıca kuruma ait kaynaklara doğrudan erişim söz konusu olmayacağı için DDOS vb. ataklara maruz kalma oranlarında ciddi düşüşler görülebilecektir.

Kurumun yaşanacak herhangi bir felakette iş sürekliliğinin sağlanması amacıyla personeline uzaktan da işlerini devam ettirebilmeleri sağlanmaktadır. Özellikle pandemi ve doğal afet dönemlerinde kurumun kaynaklarına güvenli olarak erişilebilmesi sayesinde işlerin devamlılığı sağlanmıştır. Bu sayede kurumun pandemi döneminde uzaktan erişim yöntemiyle çalışma tarzını benimsemesi, personelin fiziksel olarak çalıştığı kuruma gelmemesi nedeniyle elektrik, su, gıda ve ulaşım giderleri gibi harcama kalemlerinde de kurumlar ciddi tasarruf sağlamıştır.

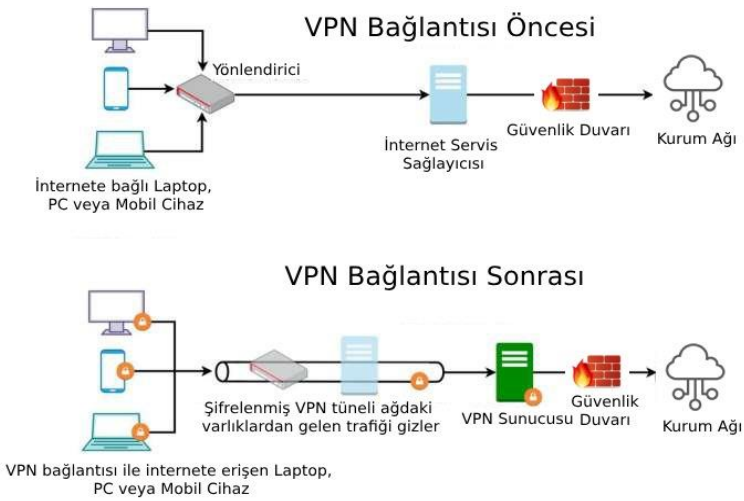
VPN kullanımı, internet kullanıcılarının veri güvenliği için en uygun yöntemlerden biridir. VPN sayesinde, internet aktiviteleriniz anonim hale gelir ve kişisel verilerinizin izlenmesi veya çalınması büyük oranda engellenmektedir. VPN kullanılarak erişim yetki matrisi oluşturulmasıyla, kurum içindeki verilerin güvenliği de sağlanabilmektedir. Bu sayede, sadece belirli kullanıcılar veya gruplar belirli kaynaklara erişebilir. Böylece, kurum içindeki verilerin güvenliği sağlanmaktadır. AES şifrelemesi gibi özelliklerle, VPN hizmeti sunan kurumlar üstün bir koruma oluşturmaktadır. Bu şifreleme yöntemi, güçlü şifreleme algoritmalarını ve anahtar değişim mekanizmalarını kullanarak verilerin güvenliğini sağlamaktadır. Vaka çalışması olarak bu araştırma çerçevesinde ise bir kamu kurumunun sanal özel ağ yapısına erişim örneği incelendiğinde, personeline güvenli bir internet üzerinden çalışma deneyimi sunan ve ayrıca kurum kaynaklarına izinsiz erişimi en düşük seviyede tuttuğu da görülebilmektedir.

Vpn kullanımı bulunmayan kurumlarda kurum içi kaynaklara erişim güvenlik duvarı üzerinde belirli port veya uygulamalara erişim izni verilmesi şeklinde gerçekleştirilmektedir. Bu yöntemin kullanımı sırasında kurum dışından kullanıcıların erişimine açılmış olan servis veya portlara herkesin erişebilmesi mümkün olabilmektedir. Aşağıda Şekil 6'da görüldüğü üzere VPN bağlantısının öncesi ve sonrasına ait bir mimari yapının genel görünümü incelendiğinde ilk dikkat çekici nokta olarak internete bağlı cihazlar ile şifrelenmiş VPN tüneli üzerinden grafiğin gizlenmesi için internet servis sağlayıcılarının VPN sunucusu üzerinden yeniden düzenlenmesidir.

Bu bağlamda Vpn protokolleri ile bağlantıların sağlanması durumunda ise dış dünyadan ilgili port veya servislere yetkisiz erişim istekleri işleme alınmayacağı gibi bu servis veya uygulamalara erişimler ne zaman ve hangi personel tarafından ne kadar süre ile yapıldığı gibi bilgiler kayıt altına alınabilmektedir. Bu sayede erişim yetki matrisinde belirlenen kullanıcı rollerine uygun olmayan girişimlere izin verilmemiş olacaktır. Ayrıca bununla ilgili personel hesabı giriş denemelerinin de kayıt altında tutulması mümkün olabilecektir. VPN kurulum öncesinde kurum dışından erişime izin verilen servis ve uygulamalara (uzak masaüstü bağlantısı, web sayfası erişimi, ssh erişimi, ftp erişimi, vb.) erişim herkes için mümkün olurken, VPN kurulumu sonrası erişim yetkisi tanımlanan personelin bağlanabilmesi mümkün olabilecektir.

Şekil 6

VPN Bağlantısının Öncesi ve Sonrasının Mimari Görünümü



Türkiye, web tabanlı sistemler, yazılım ve donanım araçları, yapay zekâ tabanlı uygulamalar ile bilişim çağının ihtiyaçlarına göre teknik politikalar üretmekle birlikte son yıllarda ağ tabanlı erişim modüllerinin uygulanması konusunda yenilikçi politikaları önemli ölçüde uygulama becerisini geliştirmektedir. Bu kapsamda özellikle kamu kurumlarında dijital dönüşümler, envanter kayıt sistemleri, sanal erişim modelleri ile gelişmiş ülke refleksini de göstermektedir. Türkiye aynı zamanda hukuki düzenlemeler ve AB uyumluluk yasalarıyla veri yönetimi ve siber güvenlik konularında da çeşitli politikalar ve uygulama yönergeleri geliştirmektedir. Günümüzde özel kurumların politikaları

ile kamu kurumlarının bu alandaki kullanım ve yetkilendirme politikalarında çeşitli farklılıklar bulunmaktadır.

Kamu kurumları arasında yüksek kullanıcı sayısına ve internet kullanımına ihtiyaç duyulan eğitim kurumları arasında özellikle üniversitelerde veri aktarımı ve erişim konuları önemli hale gelmektedir. Bu noktada ağ kaynaklarının kullanımında özellikle kullanıcı gruplarının hukuki gerekçeler ve standartlar nedeniyle sınırlandırılması söz konusu olabilmektedir. Örneğin, üniversitelerin sanal özel ağ konularında tüm gruplara erişim izni vermesi yerine sadece akademisyen ve idari birim görevlilerine bu erişim iznini vermesi, ağ politikaları ve hukuki stratejilerin doğal bir sonucudur. Zira öğrencilerin uğrayacağı ama özellikle neden olabileceği zafiyetler nedeniyle genel olarak muaf tutulabilecek olması nedeniyle sınırlandırılmış kullanıcı politikalarının uygulanması daha önemli görülmektedir.

Bu çalışmada, son yıllarda kullanım sahası ile kullanıcı sayısında artış eğilimi gösteren kamu ve özel nitelikli sanal özel ağların kullanımlarında; uygulama, yönerge, düzenleme ve denetim konusundaki politikaların nasıl belirlendiği ve çalışma alanı içerisindeki tüm paydaşların karşılıklı görev ve sorumluluk alanlarının nasıl biçimlendiği kurulum ve yönetim senaryosu üzerinden ele alınmıştır. Bu kapsamda, yüksek kullanıcı gruplarına sahip bir kamu kurumu olarak bir üniversitenin bu alandaki politikası incelenmiş ve bu konudaki stratejik eylem pratikleri değerlendirilmiştir. Sonuç olarak, bir kamu kurumunun internet tabanlı sanal özel ağlarının işleyişi örnek bir model üzerinden diyagram olarak biçimlendirilmiş, başarılı bir sistemin nasıl oluşturulabileceği ve uygulanabileceği konusundaki temel politikalar örnek bir senaryo üzerinden analiz edilmiştir.

Etik Kurul Kararları

Çıkar Çatışması: Yazarlar herhangi bir çıkar çatışmasının olmadığını beyan eder.

Etik Kurul İzni: Bu çalışmada kullanılan veriler için etik kurul kararına gerek duyulmamaktadır. Çalışma kapsamında kullanılan verilerin kullanımına yönelik Ege Üniversitesi Bilgi İşlem Daire Başkanlığı'ndan 04.05.2023 tarihli ve E.1253825 sayılı resmi yazı ile izin alınmıştır.

Yazar Katkı Beyanı: Yazarlar kaynak ve malzemelerin sağlanması, veri toplama, işleme, analiz ve yorum aşamalarında eşit oranda katkı sağladıklarını; literatür taraması, yazının yazılması, eleştirel inceleme,denetleme, fikir ve tasarım aşamalarının Mustafa Aydemir tarafından yürütüldüğünü beyan etmektedirler.

Finansal Destek: Yoktur**.**

Kaynakça

Aburdene, M. F., Mastascusa, E. J. ve Massengale, R. (1991). A Proposal For A Remotely Shared Control Systems Laboratory, Proceedings of the ASEE 1991 Frontiers in Education Conference, Session 24A3, 589-592.

Arslan, K. (2020). Eğitimde Yapay Zekâ ve Uygulamaları. *Batı Anadolu Eğitim Bilimleri Dergisi, 11*(1), 71-88.

Aydemir, M. (2018). Yeni Medyanın Kullanıcı Üzerinde Bağımlılık Etkisi: Fomo Kullanıcılar ve Genel Yönelimleri, 5. Uluslararası İletişim öğrencileri Sempozyumu, Community Ege, Tam Metin Bildiriler Kitabı, 440-455.

Batorski, D. (2011). An Ocean of Information, *Academia Focus on the Internet*, No:3, I:31,24-26.

Bitton R. ve Shabtai, A. (2021). A Machine Learning-Based Intrusion Detection System for Securing Remote Desktop Connections to Electronic Flight Bag Servers, in *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, 1164-1181, 1 May-June 2021, doi: 10.1109/TDSC.2019.2914035.

Blanco, JM., Cohen, J., Nitsch, H. (2020). Cyber intelligence against radicalisation and Violent extremism. In: Babak A, Douglas W, Blanco JM (eds) *Investigating Radicalization Trends: Case Studies In Europe And Asia*. Springer International Publishing, Cham, 55–80.

Briggs Asa, Peter Burke (2004), Medyanın Toplumsal Tarihi, Çev. İbrahim Şener, Ankara: İzdüşüm Yayınları.

Bright, L. F., Kleiser, S. B., ve Grau, S. L. (2015). Too Much Facebook? An Exploratory Examination of Social Media Fatigue, *Computers in Human Behavior*, Volume 44, Issue C, March 2015, 148-155, Amsterdam: Elsevier Science Publishers B. V.

CBDDO. (2020). Bilgi ve İletişim Güvenliği Rehberi, Erişim Adresi:https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf

Crowe, et al. (2011). The Case Study Approach. *BMC Medical Research Methodology* 2011, 11-100. doi:10.1186/1471-2288

D. Ernest vd., (2015). A Comparative Study Of Remote Access Technologies and Implementation of a Smartphone App for Remote System Administration Based on a Proposed Secure RFB Protocol. *International Journal of Science and Engineering Applications*. Volume 4 Issue 4,163-168.

Du, W., Tan, Xi., Luo, T., Jayaraman, K., ve Zhu, Z. (2011). Re-designing the Web's Access Control System, Y. Li (Ed.): *Data and Applications Security and Privacy* XXV, LNCS 6818, 4–11.

Ferguson, P. and Huston, G. (1998). What is a VPN? Erişim Adresi: https://www.potaroo.net/papers/vpn.pdf

Fujii, N. ve Koike, N., (2005). A Time-sharing Remote Laboratory for Hardware Design and Experiment with Shared Resources and Service Management, ITHET 6th Annual International Conference, Session T2B, 5-10.

George, AL., ve Bennett, A. (2005). *Case Studies And Theory Development In The Social Sciences* Cambridge, MA: MIT Press.

Green, J. ve Thorogood, N. (2009). *Qualitative Methods For Health Research*. 2. Edition. Los Angeles: Sage.

Güneş, B., Kayışoğlu, G., ve Bolat, P. (2021). Cyber Security Risk Assessment For Seaports: A Case Study Of A Container Port, *Computers & Security*, Volume 103, 2021, 102196, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102196.

Holmes, W., Bialik, M. ve Fadel, C. (2019). *Artificial intelligence in education: Promises and implications for teaching and learning*. Boston, MA: Center for Curriculum Redesign.

Huang, S., Lin, C., Luo, A., Chen, Z., Jiang, X., Wang, K., Zhang, H., ve Peng, X. (2009). Proxy-Based Security Audit System for Remote Desktop Access. *2009 Proceedings of 18th International Conference on Computer Communications and Networks*, San Francisco, CA, USA, 2009, 1-5. doi: 10.1109/ICCCN.2009.5235336.

ITU-T (1998). Multipoint communication service-Service definition, T.122, Erişim Adresi: http://www.itu.int

Kennell, R., ve Jamieson, Leah H. (2003). Establishing the Genuinity of Remote Computer Systems, Proceedings of the 12th USENIX Security Symposium, August 4–8, 2003, Washington, DC, USA.

Kotkar, A., Nalawade, A., Gawas, S., Patwardhan, A., ve Mangale, S. (2013). Android Based Remote Desktop Client, *International Journal of Innovative Research in Computer and Communication Engineering* Vol. 1, Issue 2, April 2013, 345-348.

Krithikaa, M., Priyadharsini, M. ve Subha, C. (2016). Virtual Private Network- A Survey, *International Journal of Trend in Research and Developmen*t, Volume 3(1), 78-81.

Longzheng, Cai., Shengsheng, Yu., ve Zhou, Jing-li. (2004). Research and implementation of remote desktop protocol service over SSL VPN, *IEEE International Conference on Services Computing, 2004. (SCC 2004). Proceedings. 2004*, Shanghai, China, 2004, 502-505, doi: 10.1109/SCC.2004.1358052.

Lubonski, M., Gay, V., ve Simmonds, A. (2005). A Conceptual Architecture for Adaptation in Remote Desktop Systems Driven by the User Perception of Multimedia, *2005 Asia-Pacific Conference on Communications*, Perth, WA, Australia, 2005, 891-895, doi: 10.1109/APCC.2005.1554191.

Macnish, K., ve Van der Ham, J. (2020). Ethics in cybersecurity research and practice. Technol. Soc. 63, 101382

Malinowski, A., Dahlstrom, J., Cortez, P. F., Dempsey, G. ve Mattus, C., (2000). Web-based remote active presence, Proceedings of the 2000 ASEE Annual Conference & Exposition, Session 3232.

Minghao, J., Gou, G., Shi, J., ve Xiong, G. (2019). I Know What You Are Doing With Remote Desktop. 1-7. 10.1109/IPCCC47392.2019.8958721.

Palacin, V., Gilbert, S., Orchard, S., Eaton, A., Ferrario, M.A., ve Happonen, A. (2020). Drivers of Participation In Digital Citizen Science: Case Studies On Järviwiki And Safecast. *Citizen Science: Theory Pract*. 5(1), 1–20 Article: 22, https://doi.org/10.5334/cstp.290

Resmî Gazete (2019). Bilgi ve İletişim Güvenliği Tedbirleri Konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi 06.07.2019 tarih ve 30823 sayılı Resmî Gazete.

Tarek S. VE Yasser, A. (2011). Effective and Extensive Virtual Private Network. *Journal of Information Security*, 2011, 2, 39-49.

Turing, A. (1950). Computing Machinery and Intelligence. *Mind, 49* (236), 433-460.

Wood, D., Stoss, V., Chan-Lizardo, L,. Papacostas, G. S., ve Stinson. M. E. (1988). Virtual Private Networks. In International Conference on Private Switching Systems and Networks. 132-136.