İSTANBUL GELİŞİM ÜNİVERSİTESİ

TEMEL AĞ GÜVENLİĞİ VE SİBER GÜVENLİK

Hazırlayan: **220174149– Yusuf Furkan ÇELİK**
220174037– Berkay TAN
220174139– Yakup İRŞAT

Ödev Danışmanı: **Ali ÇETİNKAYA 22.05.2023**

ÖDEV TANITIM FORMU

YAZAR ADI SOYADI	: Berkay TAN, Yusuf Furkan ÇELİK, Yakup İRŞAT
ÖDEVİN DİLİ	: Türkçe
ÖDEVİN ADI	: Temel Ağ Güvenliği ve Saldırı Analizi
BÖLÜM	: Bilgisayar Teknolojileri
PROGRAM	: Mekatronik
ÖDEVİN TÜRÜ	: Vize / Ders içi / Final
ÖDEVİN TES. TARİHİ	:19.05.2023
SAYFA SAYISI	: 18 Sayfa
ÖDEV DANIŞMANI	: Öğr. Gör. Ali ÇETİNKAYA

BEYAN

Bu ödevin/projenin hazırlanmasında bilimsel ahlak kurallarına uyulduğu, başkalarının ederlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğu, kullanılan verilerde herhangi tahrifat yapılmadığını, ödevin/projenin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir ödev/proje olarak sunulmadığını beyan eder, aksi durumda karşılaşacağım cezai ve/veya hukuki durumu kabul eder; ayrıca üniversitenin ilgili yasa, yönerge ve metinlerini okuduğumu beyan ederim.

Tarih
17.05.2023

Adı Soyadı
Berkay TAN

İmza

KABUL VE ONAY SAYFASI

220174149, 220174037, 220174139 numaralı Yusuf Furkan ÇELİK, Berkay TAN, Yakup İRŞAT'ın Adlı öğrencilerin Temel Ağ Güvenliği ve Saldırı Analizi çalışması, benim tarafımdan Vize/Ders içi/Final ödevi olarak kabul edilmiştir.

Öğretim Görevlisi

İÇİNDEKİLER

RESİMLER LİSTESİ

KISALTMALAR

VPN: VİRTUAL PRİVATE NETWORK
IP: INTERNET PROTOCOL ADDRESS
LAN: LOCAL AREA NETWORK
STS: SALDIRI TESPİT SİSTEMLERİ
NAT: NETWORK ADDRESS TRANSLATİON

ÖNSÖZ

Bu çalışmada, Temel Ağ Güvenli ve Siber Güvenliğin ne kadar önemli olduğuna ve siber saldırı tehditlerine karşı nasıl korunulacağını bildirmek amacıyla yazılmıştır. Bu makalenin hazırlanması sırasında, Türkçe kaynak bulmak zor ve meşakkatli bir süreçti. Kaynak bulabilmek için internet üzerinde kapsamlı bir arama yapmak gerekti ve kaynak bulunduktan sonra uzun süren bir okuma ve not çıkarma sürecinden sonra notlar üzerinden bir makale yazıldı. Öncelikle bu çalışma sırasında bizlere yardım eden sayın hocam Öğr. Gör. Ali ÇETİNKAYA ‘ya sonsuz teşekkürlerimizi sunarız.

Berkay TAN, Yakup İRŞAT, Yusuf Furkan ÇELİK
İstanbul 2023

ÖZET

İnsanlık varoluşundan bu yana çeşitli yollarla iletişime geçmektedir. Ayni insanın evrimleşmesi gibi iletişim araçları da insanlar gibi evrimleşti. Dumanla haberleşmeden zarf yoluyla haberleşmeye, zarftan ise internet üzerinden mesajlaşmaya kadar günümüze ulaştı. Ancak sosyalleşmek dışında da internet mecrası kullanılmaktadır. Bunun dışında haberleşme, E-ticaret gibi mecralar günümüzde son derece popülerlik kazanmaktadır. Ancak her popülerlik beraberinde tehlikenin de kapısını açmaktadır. Birçok ticaret veya özel bilgilerini internet üzerinde gizleyen kullanıcı ve firma sahiplerinin kişisel bilgi ve Ticaret birikimlerine büyük hasar verebilecek olan saldırgan kişilerin sayısı son zamanlarda bir hayli artmaktadır. Bu artış büyük kayıpların yaşanmaması amaçlı çeşitli koruma önlemleri alınmaktadır. Ancak basit önlemler ne yazık ki yetersiz kalmakta bu nedenle güçlü güvenlik duvarları ve çeşitli VPN gibi tedbirlerle korunmaya çalışılmaktadır. Çeşitli kategoride siber saldırılarda internetin yayılması ile görülmeye ve rastlanmaya başlamıştır. Bu konu çok büyük olaylarında yaşanması veya büyük ticari firmaların iflası gibi olaylarında yaşanmasında büyük derecede parmağı vardır. Bu tarz problemlerin yaşanmaması amaçlı gerek devletler gerek ise özel firmalar çeşitli güvenlik sistemlerine büyük paralar yatırmaktadırlar. Ancak bu çaplı güvenlik sistemlerine rağmen hala saldırganlar bazı güvenlik duvarlarını aşıp girmesi söz konusu olmaktadır.

Anahtar Kelimeler:

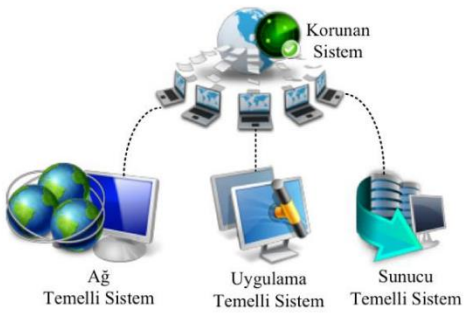
Temel
Ağ
Güvenlik
Siber
Saldırı
Analiz
IP (Internet Protocol Address)
VPN (Virtual Private Network)
Sanal
İnternet
LAN (Local Area Network)
Bilgisayar
Sistem
Elektronik Ticaret

GİRİŞ

İnsanlığın en başından bu yana teknoloji gelişir ve değişir. Günümüzdeki en gelişmiş ve yaygın olan teknolojilerden biri de internettir. İnternetin şu an neredeyse tüm dünya da kullanılması ve gün geçtikçe daha fazla cihaza entegre olmasıyla birlikte insanlarda güvensizlik hissi oluşmaya başladı. Bu güvensizlik hissini fark eden araştırmacılar bunu giderebilmek için yeni araştırmalar yapmaya ve yeni teknolojiler geliştirmeye başladılar. İnternet ortamında güvenliği sağlayabilmek için yapılan araştırmalar, güvenlik yazılımları ve uygulamarı son yıllarda oldukça kullanılmaya başlandı. Bu çalışmada siber saldırıları nasıl tespit ederiz, siber saldırılardan nasıl korunabiliriz ve bu saldırılardan nasıl kurtulabiliriz gibi soruları cevaplandıracağız.

1. TEMEL AĞ GÜVENLİĞİ

İnternet ağının en büyük avantajı tüm bilgisayarlarla bağlı oma özelliği olmasıdır. Ama bu avantaj beraberinde güvenlik anlamında da büyük dezavantaj etmeni oluşturmaktadır. Bu dezavantajın sebebi ne yazık ki gerekli tedbirlerin alınmamasından kaynaklanmaktadır. Gerekli tedbirlerin alınması halinde bu dezavantajı gerek minimum gerek ise sıfıra indirebiliriz ancak bu önlemler alınmadan internet ağının güvenli olması söz konusu bile değildir.



Resim 1-Saldırı tespit sistemi

İnsanların daha fazla sosyalleşebilmesini sağlayan internet sebebi ile toplumlarda iletişimin temeli genel anlamda ciddi seviyede değişikliğe uğramıştır. İnternetin ana amacı olan iletişimin geçmişi yüzyıllar öncesine kadar varmaktadır. Postayla başlayan bu serüven günümüzde iletişimde de büyük evrimleşmeyi sağlayan internet sayesinde de günümüze kadar gelişmiş ve gelişimini sürdürmektedir. İnternet ağı telefon veya radyo ağı gibi tek bir hizmet vermek amacıyla değil. Tek bir iletişimin birden fazla kullanıcıya ulaştırmak için kullanılmaktadır. Aynı zamanda bu sistem mesajlaşma, video aktarma, toplu yayınlama ve gerçek zamanlı paylaşım gibi birçok özelliği kullanmamıza olanak sağlamaktadır. Bu özelliklerin internetin yaygınlaşmasıyla dünyada oldukça büyük denilebilecek değişimlere neden olmuştur. Bu sebeple iletişim hizmeti veren sektörler arasında sınırlar giderek azalmaya başlamıştır.

Aynı şekilde bu beraberlik, bilişim camiasında da birtakım değişikliklere sebebiyet getirmiştir. Veri işleme cihazı olarak kullanılan bilgisayar artık Web TV'lere, sayısal asistanlara, ağ kameralarına ve çeşitli iletişim iletişim yeteneklerini kullanan cihazlara devretmiştir. Bu değişimlerdeki en rahatsız eden güç internet bilgisayar ağı ve bunula birlikte gelen internet, elektronik ticaret, internet servis sağlayıcıları gibi çeşitli yeni oluşumlardır. Bunlar ise gelecekte kullanıcılara, iletişimi ve haberleşmenin gün geçtikçe daha çok internet ağı üzerine kaymasını göstermektedir. Elektronik ticaret gibi gerçek zamanda yapılan ve para transferinin söz konusu olduğu işlerde doğruluğun, profesyonelliğin, güvenlik önlemlerinin

çok yüksek olması gerekmektedir. Bu sebeple, bunun gibi ticaret uygulamaların yapacağı internet bağlantısı olan bilişim birimlerinin olduğu konuda yani bilgisayar ağı yönetiminin öneminin en iyi şekilde ilgili taraflarca anlaşılması ve kolay, hızlı, uygulanabilir, olması gerekmektedir. Ayrıca bilgisayar ağı hizmetlerinin kalitesi, kriptogrofi, sanal özel ağlar, internet hizmeti veren kuruluşlar mühendislik, iletişim stratejisi ile internet ve toplum politikaları gibi konular bazı herhangi bilgisayar ağının yönetimi etkileyen faktörler oluşmaktadır.

Resim 2-E-Ticaret

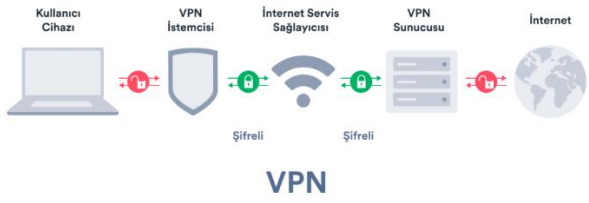
İnternetti kullanan kişilerin mahremiyetine zarar verme gibi önemli sorunlar oluşturan web güvenliği problemlerinden kaynaklanmaktadır. Bu sorunlar genellikle web tarayıcılarda bulunan kaynak kodların ya da javascript, activex, java ve benzeri aktif içerik sağlayan programlarındaki güvenlik boşlukları ve eksikliklerinden meydana gelmektedir. İnternet bilgi edinmek için çok pratik ve hızlı erişilebilen harika bir platformdur. Fakat bu harikalığın içinde bilgi kirliliği ve bilinin yok edilmesi gibi kritik problemlerde bu harikalığın beraberinde geliyor. İnternetteki bilgilerin doğru şekilde korunması internetin harikalığının yanındaki kusurları minimuma getirecektir. Bu korunmayı internet güvenlik duvarları sayesinde sağlanabilmektedir. Bu sistemin kullanımı bir güvenlik duvarı bir ağın internete bağlanmasını sağlarken güvenliği belirli seviyede tutan bir koruma şeklidir.

İnsanlık gerek internet kullanımında gerek günlük ise yaşamında gizliğine son derece önem vermekte ve bunun üzerine odaklanmaktadır. Birçok firma bu kullanıcı gizliliklerini bilgisayarlarda depolamaktadır. Diğer bir açıdan sitelerde bu tip gizli bilgiler içeren makineler ve internete bağlanan makineden ayırmanın ne kadar basit olduğu görülebilmektedir. Kullanıcı bilgisini bu yolla kenara ayırdığını ve internet âleminden kullanılan kullanılan hiçbir bilginin gizli olmadığını varsayalım bu durumda kullanıcı internet âleminden tedirgin olabilecek bir durum olur mu ki? Gizlilik tek korunması gereken değildir çünkü. Bilgileriniz gizli değilse eğer ve erişip veya başkalarının ona erişip erişmediği de umurunuzda değilse ne için neden onun için kullanıcılar yer harcıyor? Bilgiler gizli olmasa bile, yok edildiğinde veya değiştirildiğinde kullanıcıları olumsuz anlamda etkileyebilir. Bazı sonuçlar hazır hesaplanabilir giderlerdir. Eğer bu bilgileri kaybederseniz tekrar yapılanması için ücret ödemek durumunda kalabilirsiniz. O bilgiyi direk sattığınız bir

ürün olmasa da satış kaybı yaşanır. Bunların yanında da güvenlik problemleri ile ilgili görülmeyen giderlerde bulunmaktadır. Daha mühim olanda alıcının satıcıya karşı güven kaybı yaşanmasıdır.

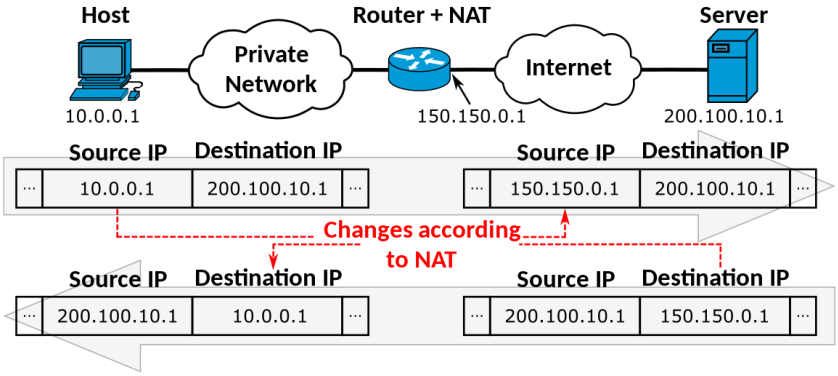
Resim 3-Saldırgan Temsili Görseli

Güvenlik suçları başla suçlara benzememektedir, nedeni bulunması zordur. Bir kullanıcının sitenize girdiğini bulmak satıcının birkaç ayını alabilir, bazen de hiç anlamayabilir. Bir yabancı sisteminize sızıp bilginize veya sisteminize hiçbir şey yapmadan gidebilir bunu sistemin sahibinin anlayıp onaylaması çok uzun zaman alabilir. Bunda sistem sahibine zaman kaybı ile sonuçlanır. Genellikle her şeye zarar veren saldırgandan hiçbir şeye saldırmayan saldırgandan daha kolay buluyor. Her şeye Zarar verilmişse yedeklerinizden tekrardan koyup sorunu çözebilirsiniz. Ama eğer hiçbir şey yapmamış bibi görünüyorsa bütün sistemi kontrol edip hiçbir şey olmadığından emin olana kadar uzun zaman boyunca kontrol edersiniz. Bir saldırgan internet âleminde sizin kimliğinizi bilgilerinizi kullanarak geziyor ya da yaptığı her hareketten siz mesul muşsunuz gibi gözüküyor olabilir. Bunun getirebileceği zorluklar zamandan çok daha fazla kayıplar la sonuçlanır. Ne yazık ki bu tip olaylara çok sıkça rastlanılmaktadır sizin adınıza tanıdıklarınıza nefret dolu söylemler veya saldırgan haberlerinde adınızın geçmesi gibi çok rahatsız edici durumlar meydana gelebilir. Bu tip mesajlara inşalar çok inansa da bu durumun temizlenmesi çok uzun zam alır ve zor olmaktadır. Bu tarz olaylar namınıza büyük kalıcı zararlar verebilir. Herhangi bir siteye erişim kazanmadan elektronik olarak mesaj göndermek uygun eğer mesaj site dışından geliyorsa sahte olabileceğini kandırmak çok basit olabilir. Ancak site erişimi olan bir saldırganın gönderdiği sahte mesaj sizden geliyor gibi görünür ki karşı taraf sizden geldiğini görür fakat siz göndermemiş olabilirsiniz. Bunun dışında saldırgan tehdit sizin listeniz ve kimlerle iletişime geçtiğinize dair kişilerin bilgilerine erişebilmektedir. Böyle bir tehdit olan saldırganın sitenize erişmeye ihtiyaç duymadan sahte mesaj göndererek birden fazla kişi listenize mesaj göndererek daha fazla avantajı olacaktır. Herhangi bir saldırgan sizin isminizi, namınızı kullanmasa bile sitenize izinsiz girmesi ününüz adına iyi değildir. Kullanıcıların markanıza olan güvenini büyük ölçüde sarsabilir. Ek olarak çoğu saldırgan çeşitleri bir bilgisayardan diğerine geçerek izlerinin bulunma risklerini azaltmak için bunun gibi birçok yola başvurmaktadırlar. Bu noktada sizin isminizi kullanarak kötü yazılım veya cinsel içerikli sitelerde ticaret gibi birçok kötü duruma karışması durumunda bunun gibi kötü ve zor durumlardan çıkılıp kurtulunması oldukça güçtür.



Resim 4-VPN Sunucusunun Bağlanma Sıralaması

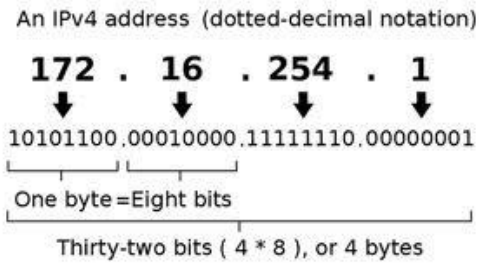
Ağ güvenliği, son zamanlarda özel sanal ağ (VPN) uygulamalarının yaygınlaşmasıyla son derece önem kazanmıştır. Firma kuruluşları kullanımı için ayarlanmış bir LAN'ın internete benzer herkese açık bir ağa bağlanılarak kullanımı, özel bilgilerin korunması konusunda son zamanlarda gündeme gelmiştir. Firmalar hem ağ içi iletişim kurması ve aynı zamanda da dış kaynaklardan yararlanılması konusundan talep istenilmiştir. Güvenlik duvarı (firewall) ağ güvenliğini sağlamak için kullanılan cihazın adıdır. Hem dıştan gelebilecek tehditleri engeller hem de özel ağı dışarıdan gizli tutmaya çalışır. En mühimi de şifreleme yeteneği ve adres dönüşüm (NAT) yeteneğidir.



Resim 5-NAT Adresleme

Genel anlamda her internet sitesi iyi uygulanmış güvenlik politikasına sahip olmalıdır. Böyle bir güvenlik politikası bağımsız güvenlik modellerinden oluşturulmuş olabilir, nedeni ise herhangi bir güvenlik modeli çeşitli metotlar ile uygulanabilen genel bir şekildir. Bir güvenlik modelini gerçekleştiren bir ürün güvenlik politikasını uygulanılmasına yarayan bir araç sunar. Benzer güvenlik sistemini diğer sistemlerle destekleyebilir. Site sahibinin sitesinin güvenliği üst seviyelere çıkarabilmesi için kullanılan tüm ürünler kendi sistemini sunmalıdır. Ve birleştirilen tüm ürünler sistemle bir bine birbirine bağlanır. Örneğin herhangi firewall ve işletim birimi birlikte çalışarak sahibi olunan sitenin güvenlik modelinin sunulması gerekir. Birçok sistem ve ürünler sitede birleştirildiğinde birbirini etkilemektedir. Ağlardaki birçok bireyi zaten bilinmektedir. Kullanan kitleler, birleşimler, dosyalar,

router'lar, yazıcılar ve çeşitli çevre birimleri bu bireyler bilgisayar ağlarında birbiriyle çok farklı yollara birbiriyle etkileşim halinde olurlar. Genellikle kullanılan kontrol kuralıdır. Bir bilgisayardaki dosyayı hangi kullanıcın görebileceği olabilir. Buna benze birçok örnekler oluşabilir.



Resim 6-IP Adresinin Binary Gösterimi

Sonuç olarak internete bağlanmayı amaçlayan tüm firmaların ihtiyaçları olan IP adresi vardır. Bu adresler iç network'te kullanılması durumunda, İnternet üzerinden giriş daha kolay bir hale gelinmektedir. Bu durum pekiyi olmadığı için engellenmesi iç networke internette olmayan kayıtlı IP adresleri kullanılmaktadır. Bu nedenle içten internete gidilen trafiğin IP adreslerinin değişimi router veya Firwall, internet üzerinden gelebilecek saldırıları veya izinsiz yerel ağa girişleri engellemek amacı ile kurulan yerel ağ ve internet arasında bulunan sunucuda yüklenen güvenlik yazılımları verilen genelleme ismidir. Bu tip yazılımlar sanal âlemin güvenliğini en üst seviyeye çıkarır. Diğer hizmet veren güvenlik bölümleri E-mail virüs tarama sistemi proxy'le diğer sisteme benzer ancak genel güvenlik kuralları destekler, firewall kadar geniş alanlı değillerdir. Proxy'ler çift internet kart ile desteklenirse şayet ciddi ölçüde ağ güvenliğinde iyi iş sağlayabilmektedirler.

2. SİBER SALDIRILAR VE TESPİT SİSTEMLERİ

Teknolojinin ilerlemesi ile insanlar güvenlik yazılımlarına daha fazla ihtiyaç duyar. Bu yazılımların asıl amacı kişiyi, cihazlarını ve kişinin verilerini kötü amaçlı kişilerden ve saldırılardan koruyabilmektir. Bilginin depolandığı yere göre ve bilginin önemine göre kullanılacak yazılımın güvenlik düzeyi farklılık gösterebilir. Teknoloji ve yazılım dünyası sürekli bir güncelleme ve değişim içinde olduğu için bu yazılımlar da işlevini koruyabilmesi için sürekli güncellenme halinde olmalıdır bu da ancak yapılan saldırı çeşitlerini tespit edip öğrenerek olur. Bu tespiti yapabilmek için öncelikli olarak saldırının ne olduğunu bilmemiz gerekir. Saldırı bir bilgiye izinsiz olarak ulaşmak, değiştirmek, kullanılamaz duruma getirmek olarak tanımlanabilir. Bu gibi önlemek amacıyla saldırı tespit sistemleri geliştirilmiştir. Saldırı tespit sistemlerinin görevi sistemde olan izinsiz girişleri ve değişimleri tespit edip kullanıcıya uyarı verip daha sonrasında bu girişimleri engellemektir. Saldırı tespit sistemleri birçok farklı alanda kullanıldığı için sınıflandırılır ve bu sınıflandırılmada şöyle kriterler vardır:

- Sistemin mimarı yapısı
- Koruyacağı sistemin yapısı
- Veri işleme aralığı
- Kullanılan bilginin kaynağ
- Yazılımın saldırı tespit yöntemi

Bu kriterler saldırı tespit sisteminin nerede kullanılacağını gösterir ve önemlidir.

2.1. Siber Saldırı Çeşitleri

Bir siber saldırıya karşı açık oluşturabilecek üç durum vardır:

- Donanımsal ve Yazılımsal Hatalar,
- Çevrimçi ortamda önemli sistemlere erişim verilmesi,
- İnternetin çalışmasını sağlayan sistemlerin şifresiz ve savunmasız olması, adresleme sistemi gibi tasarım hataları.

Siber saldırılar çok farklı yöntemler ile yapılabilir en çok bilinenlerden bazıları şunlardır:

2.1.1. Casus Yazılımlar (Truva Atı)

Saldırıyı yapan kişiler truva atı gibi casus yazılımlar sayesinde bilgisayarın arka kapısından girer ve sistemi değiştirme, kullanıcının şifrelerine erişme gibi birçok işlemi gerçekleştirebilir. Truva atı sisteme girdikten sonra depolamaya kendini kaydeder ve kendisini yerleştiren saldırganın istediklerini yapar.

2.1.2. Olta (Phishing)

Çoğunluk gerçek olmayan web siteleri kullanılarak yapılır. Bir market veya alışveriş sitesinden gelen bir e-posta gibi gözüküp aslında kullanıcıyı tuzağa düşürmeyi amaçlar.

2.1.3. Bukalemun

Normal bir uygulama gibi gözükse de arka da bilgisayardaki kullanıcı verilerini taklit ederek gizli bir dosyaya kaydeder, sonrasında sistemin bir süre için kapatılacağını söyleyen bir uyarı gönderir ve bu sırada kullanıcı verileri saldırganın eline geçer.

3. SONUÇ

Bu çalışmada internet ortamında güvenliğin ne kadar önemli olduğundan ve bu güvenliği nasıl sağlayabileceğimizden bahsettik. İnternet ortamında insanlar saldırıya uğrayabilir ve bazı insanlar kötü niyetli eylemlerde bulunabilir. Bu eylemlerden korunmak için daha önce yapılan saldırılar analiz edilip elde edilen verilere göre bir yazılım geliştirilmelidir. Kullanıcıların ise kendi korunmak istedikleri saldırılara ve korumak istedikleri bilginin önemine göre kendi koruma yazılımını seçmeliler. Ayrıca bu kötü amaçlı yazılımlardan korunmanın bir diğer yolu da cihazımızda olan anormallikleri takip etmeli ve bilmediğimiz e-posta ve sitelere tıklamamalıyız. Temel ağ güvenliğinde ise internet bağlanmayı amaçlayan tüm cihazların ihtiyaçları olan IP adresi vardır. Bu adresler iç network'te kullanılması durumunda, İnternet üzerinden giriş daha kolay bir hale gelinmektedir. Bu durum pekiyi olmadığı için engellenmesi iç networke internette olmayan kayıtlı IP adresleri kullanılmaktadır. Bu nedenle içten internete gidilen trafiğin IP adreslerinin değişimi router veya Firwall, internet üzerinden gelebilecek saldırıları veya izinsiz yerel ağa girişleri engellemek amacı ile kurulan yerel ağ ve internet arasında bulunan sunucuda yüklenen güvenlik yazılımları verilen genelleme ismidir. Bu tip yazılımlar sanal âlemin güvenliğini en üst seviyeye çıkarır. Diğer hizmet veren güvenlik bölümleri E-mail virüs tarama sistemi proxy'le diğer sisteme benzer ancak genel güvenlik kuralları destekler, firewall kadar geniş alanlı değillerdir. Proxy'ler çift internet kart ile desteklenirse şayet ciddi ölçüde ağ güvenliğinde iyi iş sağlayabilmektedirler.

KAYNAKÇA

Ali EKŞİM, M. K. (2019). Açık Kaynak İstihbaratı Üzerinden Siber Saldırı Tespiti Yöntemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 577-591.

ASLAY, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum. *IJMSIT*, 24-28.

Bölük, G. (2014). *AKILLI ŞEBEKELERDE AĞ GÜVENLİĞİ* . İSTANBUL: PROCEEDING BOOK.

DEMİRCİ, D. D. (2022). Siber Güvenlik. *Deneyap Türkiye*, 1-64.

EROL, M. (2005). SALDIRI TESPİT SİSTEMLERİNDE İSTATİSTİKSEL ANORMALLİK BELİRLEME KULLANIMI. 2-16.

Fırlar, T. (2003). Ağ güvenliği. *sau Fen Lisesi enstüsü Dergisi*, 9-12.

KURT, A. (2021). AĞ TABANLI SALDIRI TESPİT SİSTEMLERİNDE TOPLULUK ÖĞRENME YÖNTEMLERİNİN KARŞILAŞTIRMALI PERFORMANS ANALİZİ. *T.C. SAKARYA ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ*, 6-33.

Muhammet Baykara, R. D. (2019). Saldırı Tespit Ve Engelleme Araçlarının incelenmesi. *DÜMF Mühendiilik Dergisi*, 58-71.

Özgü Can, M. F. (2014). KURUMSAL AĞ VE SİSTEM GÜVENLİĞİ POLİTİKALARININ ÖNEMİ VE BİR DURUM ÇALIŞMASI. *TÜBAV BİLİM DERGİSİ*, 17-25.

Siber Saldırılarla Savaşan Tehdit Önleme Plaormları. (tarih yok). *FireEye*, 1-2.