Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 1-39
DOI: 10.46373/hafebid.1602901

ISSN: 2618-6241
e-ISSN: 2667-5757

Kobi ve Orta Ölçekli İşletmelerde Optimum Maliyetle Güvenlik Risklerinin Yönetimi ve Siber Güvenlik Uygulamaları

Burak SARAL[1]*, Mustafa Cem KASAPBAŞI[2]

[1]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0009-0002-0409-1790, (https://orcid.org/0009-0002-0409-1790)
[2]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0000-0001-6444-6659, (https://orcid.org/0000-0001-6444-6659)

Geliş Tarihi: 17.12.2024
Kabul Tarihi: 26.12.2024

***Sorumlu Yazar e mail:** burak@kampist.org

Atıf/Citation: Saral, B., Kasapbaşı, M. C., "Kobi ve Orta Ölçekli İşletmelerde Optimum Maliyetle Güvenlik Risklerinin Yönetimi ve Siber Güvenlik Uygulamaları", Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 1-39.

Araştırma Makalesi/ ***Research Article***

Öz

Dijitalleşmenin hızla yaygınlaşması, küçük ve orta ölçekli işletmeler (KOBİ'ler) için yeni fırsatlar yaratırken, aynı zamanda siber güvenlik tehditlerine karşı kırılganlıklarını artırmaktadır. KOBİ'ler, büyük ölçekli işletmelere kıyasla sınırlı bütçeler ve kaynaklarla çalıştıklarından, siber tehditlere karşı etkili koruma sağlamak için maliyet etkin güvenlik stratejilerine ihtiyaç duymaktadır. Bu durum, KOBİ'lerin siber güvenlik yatırımlarını optimize etme ve risk yönetiminde yenilikçi çözümler geliştirme gerekliliğini doğurmaktadır. Bu çalışma, KOBİ'lerin karşılaştığı başlıca siber tehditlere odaklanarak, bu tehditlere karşı etkin ve sürdürülebilir güvenlik stratejilerinin nasıl uygulanabileceğini araştırmaktadır. Özellikle, düşük maliyetli ancak etkili güvenlik çözümleri ve modern siber tehditlerle mücadelede kullanılabilecek yöntemler üzerinde durulmuştur. KOBİ'lere özgün bir bakış açısı sunarak, simülasyon ortamında gerçekleştirilen saldırı analizleriyle güvenlik önlemlerinin etkinliği değerlendirilecek ve elde edilen bulgular üzerinden KOBİ'ler için pratik öneriler sunulacaktır. Makale, KOBİ'lerin kaynaklarını en verimli şekilde kullanarak operasyonel sürekliliklerini nasıl koruyabileceklerine dair rehber niteliğinde bir çalışma sunmayı amaçlamaktadır. Bu bağlamda, atak simülasyonları ve güvenlik katmanlarının performans analizleri, önerilen stratejilerin gerçek dünyadaki uygulanabilirliğini göstermesi açısından önemli bir katkı sağlamaktadır.

Anahtar sözcükler: KOBİ, siber güvenlik, maliyet optimizasyonu, risk yönetimi, siber tehditler

Management Of Security Risks and Cybersecurity Practices With Optimal Costs in Smes and Medium-Sized Enterprises

Abstract

The rapid spread of digitalization creates new opportunities for small and medium-sized enterprises (SMEs) while simultaneously increasing their vulnerability to cybersecurity threats. SMEs, working with limited budgets and resources compared to large-scale enterprises, require cost-effective security strategies to ensure effective protection against cyber threats. This situation necessitates optimizing cybersecurity investments and developing innovative solutions for risk management. This study focuses on the major cybersecurity threats faced by SMEs and explores how effective and sustainable security strategies can be implemented to address these threats. Particular emphasis is placed on low-cost yet effective security solutions and methods to combat modern cyber threats. By offering SMEs a unique perspective, the study evaluates the effectiveness of security measures through attack simulations and provides practical recommendations based on the findings. The article aims to serve as a guide for SMEs on how to maintain operational continuity by utilizing their resources most efficiently. In this context, attack simulations and performance analyses of security layers contribute significantly by demonstrating the real-world applicability of the proposed strategies.

Keywords: SME, cybersecurity, cost optimization, risk management, cyber threats

1. Giriş

Günümüz dünyasında dijitalleşmenin hızla yaygınlaşması, işletmeler için büyük fırsatlar sunduğu gibi, beraberinde ciddi güvenlik risklerini de getirmektedir. Özellikle küçük ve orta ölçekli işletmeler (KOBİ'ler), büyük şirketler kadar geniş bütçelere sahip olmadığından, siber güvenlik yatırımlarını maliyet açısından oldukça etkin bir şekilde planlamak zorundadır [1]. Ancak sınırlı bütçeler ve kaynaklar, bu tarz işletmelerin siber tehditlere karşı savunmasız kalma riskini artırmaktadır. Bu nedenle, KOBİ'lerin siber güvenlik stratejilerini hem maliyet hem de etkinlik açısından optimize etmeleri faaliyetlerinin devamlılığı ve yerel / küresel ekonomiye katkılarının artarak devam edebilmesi için büyük önem taşımaktadır [2].

KOBİ'ler, çoğunlukla dijital altyapılarını güçlendirmeye çalışırken, aynı zamanda veri güvenliğini sağlama, bilgi teknolojileri altyapısını koruma ve siber ataklara karşı önlem alma yükümlülüğü altındadır. Bununla birlikte, bu işletmelerin karşılaştığı siber tehditler büyük ölçüde çeşitlilik göstermekte ve sürekli olarak gelişmektedir. Bu dinamik ortamda, işletmelerin risk yönetimi stratejilerini belirlerken hem mevcut tehditler hem de maliyet faktörlerini dikkate alması gerekmektedir [3]. Siber tehditler arasında fidye yazılımları, kimlik avı saldırıları ve DDoS saldırıları gibi problemler özellikle KOBİ'leri hedef almaktadır. Örneğin, 2023 yılında KOBİ'lerin %73'ünün veri ihlali veya siber saldırı yaşadığını raporlanmıştır [4].

Bu dinamik ortamda, işletmelerin risk yönetimi stratejilerini belirlerken hem mevcut tehditler hem de maliyet faktörlerini dikkate alması gerekmektedir. Bu kapsamda, bulut tabanlı siber güvenlik çözümleri gibi yenilikçi teknolojiler, KOBİ'lerin sınırlı kaynaklarını etkin bir şekilde kullanmasını sağlamaktadır [5]. Bulut bilişim teknolojileri, altyapı maliyetlerini düşürdüğü gibi, daha esnek ve hızlı bir güvenlik yapısı oluşturma imkanı sunmaktadır.

Bu çalışmada, KOBİ'ler ve orta ölçekli işletmeler için optimum maliyetle siber güvenliğin nasıl sağlanabileceği ve güvenlik risklerinin nasıl yönetilebileceği üzerinde durulacaktır. Özellikle, bu işletmelerin kısıtlı kaynaklarını en verimli şekilde kullanarak, siber tehditlere karşı etkin çözümler geliştirmesi için uygulanabilir stratejiler önerilecektir. Ayrıca, başarılı güvenlik uygulamaları ve vaka analizleri ile işletmelerin karşılaştığı gerçek dünyadaki sorunlar ve bunlara yönelik çözümler de detaylandırılacaktır ve istatistiki olarak sunulacaktır.

Bu bağlamda, KOBİ'lerin siber güvenlik yatırımlarını nasıl planlamaları gerektiği, hangi teknolojilerin kullanılabileceği ve bütçe kısıtlamaları altında güvenliği en üst düzeye çıkarmak için atılacak adımlar bu tezin temel sorunsallarını oluşturmaktadır.

2. Yöntem

Küçük ve Orta Ölçekli İşletmelerde (KOBİ'ler) siber güvenlik yönetimi, genellikle sınırlı bütçeler ve kaynaklarla gerçekleştirilmek zorunda olduğu için maliyet etkin çözümler sunan çok katmanlı bir güvenlik modeli önerilecektir. Bu yöntem, siber tehditlere karşı geniş kapsama alanını en düşük maliyetle sağlayacak güvenlik katmanları sunmayı amaçlar. Aşağıdaki adımlar ve süreçler, bu modelin temel yapı taşlarını oluşturmaktadır.

2.1. Simülasyon Ortamı ve Yapılacak Testler

Atak simülasyonu, bir kuruluşun bilgi sistemlerinin güvenliğini değerlendirmek amacıyla gerçekleştirilen kontrollü ve etik siber atak denemeleridir. Bu yöntem, gerçek dünyadaki atak senaryolarını taklit ederek, sistemlerin savunma mekanizmalarının etkinliğini test etmeyi ve olası güvenlik açıklarını belirlemeyi amaçlar. Sızma testleri olarak da bilinen bu uygulamalar, saldırganların kullanabileceği yöntemleri simüle ederek, sistemlerin ne kadar dayanıklı olduğunu ölçer ve gerekli güvenlik iyileştirmelerinin yapılmasına olanak tanır [5].

Bu süreç, olası güvenlik açıklarını ve zayıf noktaları tespit etmenin yanı sıra, mevcut güvenlik çözümlerinin hangi alanlarda daha fazla optimize edilmesi gerektiğini anlamaya da olanak tanır. Yapılacak testlerde, atak simülasyonu sistemi kullanılarak gerçek saldırı senaryoları taklit edilecek ve KOBİ ortamları için fidye yazılımı, kimlik avı, zararlı yazılım ve botnet saldırıları gibi madde 3.2'de açıklanan güvenlik önlemleri ile madde 3.3'te önerilen stratejilerin etkinliği detaylı bir şekilde değerlendirilecektir. Bu yaklaşım, hem mevcut güvenlik katmanlarının performansını ölçmeyi hem de KOBİ'ler için daha güçlü ve verimli bir güvenlik altyapısı oluşturmak adına iyileştirme alanlarını belirlemeyi amaçlamaktadır.

2.2. İşletim Sistemi

Test ortamında bulunan cihazlar Windows 10 22H2 (OS Build 19045.5198) versiyonu ile yapılandırılmış ve tüm güncellemeleri yüklenmiştir.

2.3. Yeni Nesil Güvenlik Duvarı Sistemi

Test ortamında, güvenlik seviyesini en üst düzeye çıkarmak amacıyla Yeni Nesil Güvenlik Duvarı yapılandırılmış ve konumlandırılmıştır [6]. Bu güvenlik duvarı üzerinde SSL Denetimi özelliği etkinleştirilerek şifreli trafik üzerinde derinlemesine analiz yapılması sağlanmıştır. Ayrıca, gelişmiş güvenlik politikalarının uygulanabilmesi için URL Filtresi, DNS Filtresi, Uygulama Kontrolü, IPS ve Antivirüs modülleri aktif hale getirilmiştir.

Bu yapılandırma, test ortamındaki güvenlik açıklarını belirlemek ve saldırılara karşı maksimum koruma sağlamak için tasarlanmıştır. Özellikle SSL trafiğinin çözülmesi, zararlı yazılımların ve diğer siber tehditlerin tespit edilme oranını artırırken, URL ve DNS filtreleme gibi özellikler, kötü niyetli sitelere ve alan adlarına erişimi engellemeyi hedeflemiştir. IPS ve Antivirüs ise, ağ içindeki anormal hareketleri ve kötü amaçlı yazılımları proaktif olarak engelleyerek daha güvenli bir ortam oluşturmayı amaçlamıştır.

Bu kapsamda, Yeni Nesil Güvenlik Duvarı ile yapılan testler, hem gelişmiş koruma seviyelerini değerlendirerek mevcut güvenlik önlemlerinin etkinliğini test etmeyi hem de olası iyileştirme alanlarını belirlemeyi amaçlamaktadır.

2.4. Atak Kategorileri

Madde 2.6'da tanımlanan simülasyon ortamındaki son kullanıcı cihazlarına, Tablo 1'de belirtilen 15 farklı atak kategorisi kapsamında toplam 4.622 farklı siber atak gerçekleştirilmiştir. Bu ataklar,

sistemlerin farklı güvenlik yapılandırmalarına karşı gösterdiği direnci analiz etmek amacıyla, Tablo 2'de yer alan 8 farklı güvenlik statüsü durumuna ayrı ayrı uygulanmıştır. Her bir güvenlik statüsü için tüm atakların tekrarlanması sonucunda, toplamda 36.976 atak eylemi gerçekleştirilerek kapsamlı bir test süreci yürütülmüştür.

Bu testler, modern siber tehditlerin KOBİ'ler üzerindeki etkisini anlamak ve mevcut güvenlik önlemlerinin hangi tehditlere karşı etkili olduğunu belirlemek amacıyla detaylı bir şekilde tasarlanmıştır. Elde edilen veriler, hem mevcut güvenlik çözümlerinin performansını ölçmek hem de KOBİ'ler için daha güçlü ve kapsamlı bir güvenlik stratejisi oluşturmak için temel teşkil etmektedir.

Tablo 1. Atak Kategorileri ve Atak Sayıları

Sıra	**Kategori**	**Atak Sayısı**
1	Arka Kapı	178
2	Bilgi Hırsızlığı	66
3	Botnet	12
4	Casus Yazılım	94
5	Fidye Yazılımı	428
6	Hackleme Aracı	30
7	İndirici İndirme	40
8	Silici	36
9	Solucan	22
10	Truva Atı	180
11	Uç Nokta Atakları	2.842
12	Uzak Kod Çalıştırma	4
13	Yetki Yükseltme	8
14	Yükleyici	58
15	Zararlı Yazılım	624
	Toplam	**4.622**

2.5. Güvenlik Statüleri

Tablo 2. Güvenlik Statüleri ve Toplam Atak Sayıları

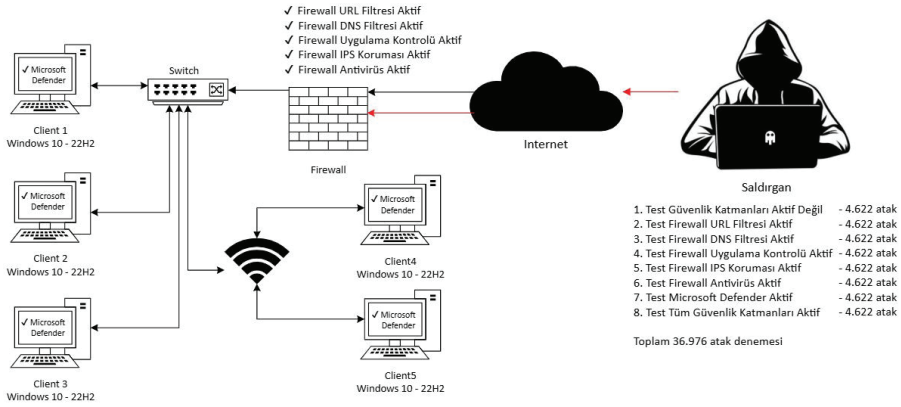
Sıra	Güvenlik Statüsü	Atak Sayısı
1	Güvenlik Katmanları Aktif Değil	4.622
2	Güvenlik Duvarı URL Filtresi Aktif	4.622
3	Güvenlik Duvarı DNS Filtresi Aktif	4.622
4	Güvenlik Duvarı Uygulama Kontrolü Aktif	4.622
5	Güvenlik Duvarı IPS Koruması Aktif	4.622
6	Güvenlik Duvarı Antivirüs Aktif	4.622
7	Microsoft Defender Aktif	4.622
8	Tüm Güvenlik Katmanları Aktif	4.622
	Toplam Yapılan Atak Sayısı	36.976

Simülasyonlar sırasında, Tablo 1'de belirtilen farklı siber saldırı teknikleri, belirlenen sayılarda son kullanıcı cihazlarına uygulanacaktır. Bu süreçte, Tablo 2'de yer alan güvenlik statüleri tek tek devreye alınarak, her bir statünün etkinliği ayrı ayrı değerlendirilecektir. Her güvenlik statüsünün ataklara karşı sağladığı koruma oranları, simülasyon sonuçlarına göre ölçülecek ve analiz edilecektir.

Son aşamada, Tablo 2'de 8. sırada belirtilen tüm güvenlik katmanları bir arada aktif hale getirilerek, bu katmanların birlikte sağladığı toplam koruma oranı ortaya konulacaktır. Simülasyonlar sonucunda, saldırıların engellenme oranları istatistiksel yöntemlerle analiz edilecek ve güvenlik katmanlarının bireysel ve kolektif etkinlikleri üzerine çıkarımlar yapılacaktır. Bu çalışma, güvenlik stratejilerinin optimize edilmesine yönelik önemli veriler sağlayacaktır.

2.6. Simülasyon Ortamı

Yapılacak testlerin temel amacı, önerilen güvenlik katmanlarının gerçek dünyadaki siber saldırı senaryolarında ne kadar etkili olduğunu ölçmek ve KOBİ'ler gibi sınırlı kaynaklara sahip işletmeler için güvenlik çözümlerinin verimliliğini değerlendirmektir.



Şekil 1. Simülasyon Ortamı

Şekil 1 görülebilen simülasyon ortamı, farklı türdeki siber saldırıların kontrollü bir şekilde taklit edilmesini sağlar. Bu süreçte, önerilen güvenlik katmanları birer birer test edilerek her birinin belirli tehditlere karşı etkinliği analiz edilmektedir. Bu testler, zararlı yazılımlar, kimlik avı saldırıları, fidye yazılımları ve diğer yaygın siber tehditlere karşı alınan önlemlerin gerçek koşullarda nasıl performans gösterdiğini anlamaya yönelik önemli veriler sunar.

Simülasyonların sonunda elde edilen bulgular, KOBİ'ler için uygulanabilir güvenlik çözümlerinin etkinliğini somut verilerle ortaya koyar. Ayrıca, bu süreç, güvenlik stratejilerinde mevcut zayıflıkları belirleyerek daha güçlü bir savunma altyapısının oluşturulmasına rehberlik eder. Böylece işletmeler, hem mevcut kaynaklarını daha etkili bir şekilde kullanabilir hem de güvenlik açıklarını en aza indirerek operasyonel ortamlarını daha güvenli hale getirebilirler.

3. Atak Türleri

Simülasyon ortamında gerçekleştirilen 15 farklı siber atak türü, KOBİ'ler ve diğer kurumların karşılaşabileceği en yaygın ve etkili tehditleri kapsamlı bir şekilde yansıtmaktadır. Bu ataklar, modern siber güvenlik sistemlerinin güçlü ve zayıf yönlerini test ederek, kurumların

güvenlik açıklarını anlamalarına ve risk yönetimi stratejilerini geliştirmelerine yardımcı olmaktadır. Aşağıda, bu atak türleri genel hatlarıyla ele alınmıştır: [7]

Arka Kapı (Backdoor): Saldırganların sistemlere yetkisiz erişim sağlamasına olanak tanıyan zararlı yazılımlar, özellikle gizli veri sızıntıları ve kalıcı tehdit oluşturma amacıyla kullanılır.

Bilgi Hırsızlığı (Information Theft): Kullanıcıların hassas verilerini ele geçirmek için tasarlanan bu saldırılar, genellikle finansal ve ticari bilgileri hedef alır.

Botnet: Çeşitli cihazları ele geçirip bir ağ üzerinden koordine edilen bu saldırılar, dağıtık hizmet reddi (DDoS) gibi büyük ölçekli tehditlerde kullanılır.

Casus Yazılım (Spyware): Kullanıcıların sistemlerine sızarak veri toplama ve faaliyetlerini izleme amacı güden yazılımlar, özellikle işletmelerin gizliliğini tehdit eder.

Fidye Yazılımı (Ransomware): Sistemlere sızarak verileri şifreleyen ve erişim karşılığında fidye talep eden saldırılar, KOBİ'ler için büyük mali kayıplara yol açabilir.

Hackleme Araçları: Güvenlik açıklarını keşfetmek veya sistemlere yetkisiz erişim sağlamak için kullanılan araçlar, özellikle sistem yöneticilerinin bilinçsizce kullandığı zafiyetleri hedef alır.

İndirici İndirme (Downloader): Zararlı yazılımları sisteme yüklemek için kullanılan bu araçlar, genellikle diğer saldırıların başlangıç aşamasında devreye girer.

Silici (Wiper): Sistemlerdeki verileri tamamen yok etmeyi amaçlayan bu saldırılar, özellikle kuruluşların operasyonel sürekliliğini tehdit eder.

Solucan (Worm): Ağ bağlantıları üzerinden yayılan ve kendini çoğaltan bu zararlı yazılımlar, kısa sürede geniş bir sisteme yayılabilir.

Truva Atı (Trojan): Meşru bir yazılım gibi görünen ancak zararlı işlemler gerçekleştiren bu yazılımlar, genellikle kullanıcıların dikkatini çekmeden sistemlere yerleşir.

Uç Nokta Atakları (Endpoint Attacks): Cihazların uç noktalarını hedef alarak veri sızıntısı veya sistemi devre dışı bırakmayı amaçlayan saldırılar, özellikle zayıf güvenlik protokollerinden faydalanır.

Uzak Kod Çalıştırma (Remote Code Execution): Saldırganların, hedef sistem üzerinde zararlı kod çalıştırmasını sağlayan bu saldırılar, genellikle sistemin tüm kontrolünü ele geçirme amacı taşır.

Yetki Yükseltme (Privilege Escalation): Sistem içindeki kullanıcı yetkilerini artırmayı hedefleyen bu saldırılar, saldırganlara kritik verilere erişim imkanı sağlar.

Yükleyici (Loader): Zararlı yazılımların sistemlere yüklenmesi için kullanılan bir ara yazılım türüdür ve genellikle diğer saldırıların tamamlayıcı unsuru olarak çalışır.

Zararlı Yazılım (Malware): Genel bir kavram olarak zararlı yazılımlar, sistemlerin işleyişini bozmayı veya veri çalmayı amaçlayan çeşitli yazılım türlerini kapsar.

Bu atak türleri, modern işletmelerin karşı karşıya olduğu siber tehditlerin çeşitliliğini ve karmaşıklığını ortaya koymaktadır. Her bir türün sistemlere olan etkisi, güvenlik açıklarının kapatılmasının ve güçlü bir siber güvenlik altyapısının gerekliliğini vurgulamaktadır.

4. Güvenlik Test Katmanları

Madde 2.6'da belirtilen simülasyon ortamında yer alan cihazlar, belirlenen güvenlik katmanları ve statüler doğrultusunda test edilecektir. Bu testlerin amacı, her bir güvenlik katmanının bağımsız ve bir arada çalıştığında siber tehditlere karşı ne kadar etkili olduğunu ölçmektir. Simülasyon ortamındaki cihazlara aşağıdaki statülerde madde 2.4'de belirtilen ataklar uygulanarak cihazların karşı karşıya kaldığı ataklara karşı gösterdiği direnç ve güvenlik performansı detaylı bir şekilde analiz edilecektir.

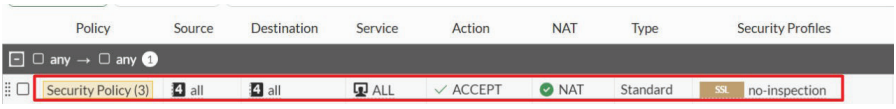
4.1. Güvenlik Katmanları Aktif Değil

Madde 2.2'de belirtilen Windows konfigürasyonunda Microsoft Defender ve Windows güvenlik özelliklerini (gerçek zamanlı koruma, Antivirüs, güvenlik duvarı, bulut tabanlı koruma, kimlik avı koruması, SmartScreen, istenmeyen uygulama engelleme) gibi özellikleri devre dışı bırakmak için, powershell yönetici yetkisi ile çalıştırılarak işletim sistemindeki tüm temel güvenlik katmanları devre dışı bırakılmıştır [8].

Denetim Masası – Internet Özellikleri üzerinden "Internet – Yerel Internet – Güvenilen Siteler

– Yasaklı Siteler" kategorilerindeki tüm güvenlik önlemleri en düşük seviye çekilmiştir.

Madde 2.3'de belirtilen Yeni Nesil Güvenlik Duvarı üzerinde herhangi bir yönden herhangi bir yöne doğru tüm istekleri izin veren ve üzerinde hiçbir güvenlik politikası bulunmayan Şekil 2'de görülen "Security Policy" kuralı yazılmıştır.



Şekil 2. Güvenlik Duvarı Güvenlik Önlemi Yok

Yukarıda belirtilen işlemler yapılarak tüm güvenlik katmanları devre dışı bırakılarak madde 2.4'deki ilgili atak simülasyonları çalıştırılmış ve güvenliksiz ortamın etkinliği ve siber tehditlere karşı direncini ölçmek amacıyla detaylı analizler gerçekleştirilmiştir. Bu analizlerin sonucunda, Madde 4.1'de ayrıntılı olarak sunulan bulgular elde edilmiştir. Bu bulgular güvenlik katmanları aktif değilken başarılı olan atakları ortaya koyarak, analizler için detaylı veriler sunmaktadır.

4.2. Yeni Nesil Güvenlik Duvarında SSL Denetiminin Aktif Hale Getirilmesi

Madde 4.3, 4.4, 4.5, 4.6, 4.7 ve 4.9 daki tüm testlerde SSL Denetimi özelliği aktif hale getirilmiş ve uç nokta cihazlara SSL denetimi için gerekli olan SSL sertifikası yüklenmiştir. Bu sayede Yeni Nesil Güvenlik Duvarının şifreli trafik üzerindeki görünürlüğü artırılmış, tehdit algılama ve önleme süreçlerinde daha etkin bir rol oynaması sağlanmıştır. Şifrelenmiş veri trafiğinin çözülmesi, kötü amaçlı yazılımların, kimlik avı ataklarının ve diğer siber tehditlerin güvenlik katmanları tarafından fark edilmesini kolaylaştırmıştır. Bu yöntem, yalnızca ağ güvenliğini güçlendirmekle kalmamış, aynı zamanda güvenlik duvarının uygulama bazlı ve kullanıcı bazlı politika uygulamalarında daha hassas ve verimli olmasına da olanak tanımıştır [9].

Bu yaklaşım, özellikle modern şifreleme protokollerinin yaygınlaştığı günümüzde, güvenlik tehditlerini önleme açısından kritik bir gereklilik olarak değerlendirilmektedir.

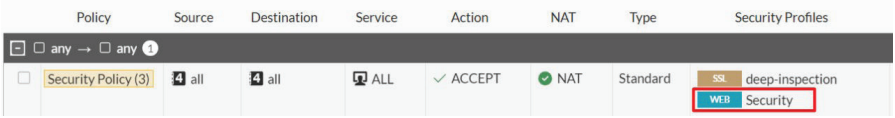
4.3. Yeni Nesil Güvenlik Duvarında URL Filtresinin Aktif Hale Getirilmesi

Güvenlik Duvarı URL filtresi, internet üzerinden belirli web sitelerinin ve URL'lerin erişimini engellemeye yarayan bir güvenlik özelliğidir. Bu özellik, ağda zararlı içeriklere veya istenmeyen sitelere erişimi kısıtlamak amacıyla kullanılır. Güvenlik Duvarı belirli URL'leri veya alan adlarını listeden çıkararak, kullanıcıların bu sitelere erişmelerini engeller. Genellikle kullanım amaçları aşağıdaki gibidir [10].

1. Zararlı Sitelerden Korunma: Kullanıcıların kötü amaçlı yazılım (malware) barındıran veya kimlik avı (phishing) içeren sitelere erişmelerini engeller.
2. Veri Güvenliği: Kurumsal ağlarda, gizli veya hassas bilgilerin dışarıya sızmasını engellemek amacıyla belirli URL'leri engeller.

3. İnternet Kullanımını Kontrol Etme: Özellikle okul veya işyerlerinde, çalışanların veya öğrencilerin zaman kaybettiren veya zararlı içeriklere sahip sitelere girmelerini önler.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Yeni Nesil Güvenlik Duvarı üzerinde URL filtresi Şekil 3'da görüldüğü şekilde eklenmiştir.



Şekil 3. Sadece Güvenlik Duvarı URL Filtresi Aktif

İlgili politika varsayılan modda aktif hale getirilmiş, engelleme ve izin verme için herhangi bir özelleştirme yapılmamıştır.

Yukarıda belirtilen test ortamında, Güvenlik Duvarı URL Filtresi aktif hale getirilerek atak simülasyonları uygulanmıştır. Bu testler, URL filtresi etkin bir şekilde çalışırken, siber tehditlere karşı etkinliğini ve sağladığı koruma düzeyini değerlendirmek amacıyla gerçekleştirilmiştir. Yapılan analizlerin sonucunda, Madde 6.2'de ayrıntılı olarak sunulan bulgular elde edilmiştir. Bu bulgular, URL filtresinin güçlü ve zayıf yönlerini ortaya koyarak, önerilen stratejilerin etkinliğine ilişkin değerli iç görüler sağlamaktadır.

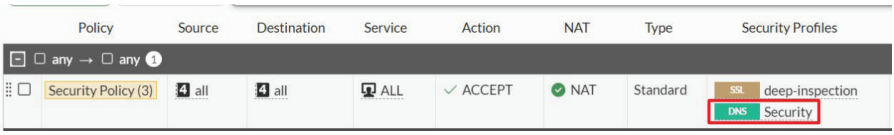
4.4. Yeni Nesil Güvenlik Duvarında DNS Filtresinin Aktif Hale Getirilmesi

Yeni Nesil Güvenlik Duvarı DNS filtresi, ağda yapılan DNS sorgularını kontrol ederek belirli alan adlarına (domain) erişimi engelleyen bir güvenlik özelliğidir. Bu filtre, DNS (Domain Name System) sorgularını, yani bir web sitesine erişim sağlamak için kullanılan IP adreslerini çevirme işlemini denetler. DNS filtresi temel olarak şu işlere yarar [11].

1. Zararlı Siteleri Engelleme: DNS filtresi, kötü amaçlı yazılım içeren veya kimlik avı (phishing) amacı güden sitelere yapılan DNS sorgularını engeller. Bu sayede kullanıcılar bu tür zararlı sitelere erişim sağlayamaz.
2. İstenmeyen İçeriği Engelleme: Çeşitli kategorilerdeki (örneğin, yetişkin içerik, kumar, şiddet) istenmeyen sitelere erişimi engelleyerek, ağ güvenliğini artırır ve kullanıcıların zararlı içeriklere ulaşmalarını önler.
3. Veri Güvenliği: Özel verilerin sızmasını önlemek amacıyla, yalnızca güvenli ve onaylı DNS sunucuları üzerinden yapılan bağlantılara izin verir.

Bu şekilde DNS filtresi, ağda zararlı ve istenmeyen trafiği engelleyerek daha güvenli bir internet deneyimi sağlar.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Yeni Nesil Güvenlik Duvarı üzerinden DNS filtresi Şekil 4'de görüldüğü şekilde eklenmiştir.



Şekil 4. Sadece Güvenlik Duvarı DNS Filtresi Aktif

İlgili politika varsayılan modda aktif hale getirilmiş, engelleme ve izin verme için herhangi bir özelleştirme yapılmamıştır.

Testler yukarıda belirtilen ortama yapılarak madde 6.3 deki bulgular elde edilmiştir.

4.5. Yeni Nesil Güvenlik Duvarında Uygulama Kontrolünün Aktif Hale Getirilmesi

Yeni Nesil Güvenlik Duvarı Uygulama Kontrolü, bir ağ güvenlik özelliği olarak, ağda çalışan uygulamaların internet bağlantılarını

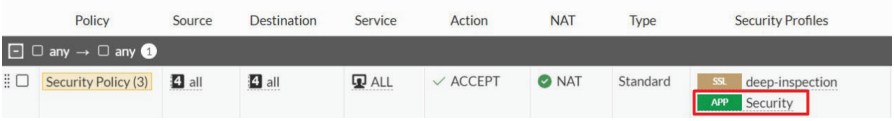
kontrol etmeye ve denetlemeye yarar. Bu özellik, yalnızca onaylı ve güvenli uygulamaların internete bağlanmasına izin verirken, kötü amaçlı veya istenmeyen uygulamaların ağ üzerinden veri gönderip almasını engeller. Uygulama kontrolü, özellikle kurumsal ağlarda veri sızıntılarını ve zararlı yazılım (malware) aktivitelerini önlemek için önemli bir güvenlik katmanı sunar [12].

Temel olarak bu özellik şu amaçlarla kullanılır:

1. Zararlı Uygulamaların Engellenmesi: Güvenlik duvarı, kötü amaçlı yazılımlar veya zararlı uygulamalar tarafından yapılan internet bağlantılarını tespit eder ve engeller.
2. Ağ İzinlerinin Sınırlanması: Yalnızca belirli, izin verilen uygulamaların dışa ve içe bağlantı kurmasını sağlar, böylece yetkisiz yazılımlar ağda çalışamaz.
3. İzinsiz Veri Paylaşımının Önlenmesi: Kullanıcılar veya yazılımlar tarafından yapılan veri paylaşımını izler ve kontrol eder, hassas bilgilerin dışarıya sızmasını engeller.

Bu şekilde, uygulama kontrolü, sadece ağda izin verilen yazılımlar tarafından yapılan trafiğe izin vererek ağın güvenliğini artırır.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Güvenlik Duvarı üzerinden Uygulama Kontrolü **Şekil 5**'de görüldüğü şekilde eklenmiştir.



Şekil 5. Sadece Güvenlik Duvarı Uygulama Kontrolü Aktif

İlgili politika varsayılan modda aktif hale getirilmiş, engelleme ve izin verme için herhangi bir özelleştirme yapılmamıştır.

Testler yukarıda belirtilen ortama yapılarak madde 6.4 deki bulgular elde edilmiştir.

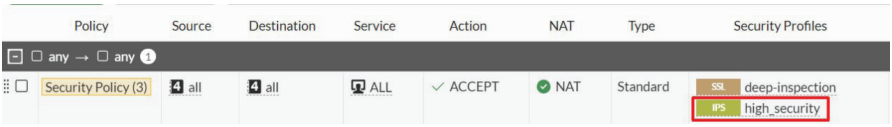
4.6. Yeni Nesil Güvenlik Duvarında IPS Korumasının Aktif Hale Getirilmesi

Yeni Nesil Güvenlik Duvarı IPS (Intrusion Prevention System) koruması, ağ güvenliğini sağlamak için kullanılan bir teknolojidir. Bu özellik, ağda gerçekleşebilecek potansiyel atakları tespit eder ve engeller. IPS, genellikle Güvenlik Duvarı cihazları ile entegre çalışır ve kötü niyetli trafik, exploitler veya atak kalıplarını analiz ederek, saldırganların sisteme zarar vermesini önler [13].

1. Atak Tespiti ve Engelleme: IPS, ağdaki anormal trafiği ve bilinen atak tekniklerini tanıyan bir dizi imzaya sahip olup, bu tür aktiviteleri anında tespit eder ve engeller. Bu, zararlı yazılımların, DDoS ataklarının ve diğer kötü amaçlı faaliyetlerin ağda yayılmasını önler.
2. Gelişmiş Tehdit Öncesi Koruma: IPS, ataklar ağ içine girmeden önce, gelen trafiği analiz ederek, potansiyel tehditleri önler. Bu, sistemlerin korunmasına yardımcı olur ve ağ üzerindeki güvenliği artırır.
3. Gerçek Zamanlı Müdahale: IPS, sadece tehditleri tespit etmekle kalmaz, aynı zamanda bu tehditlere karşı anında müdahale ederek, atakları bloke eder. Bu, ağın kesintisiz bir şekilde çalışmasını sağlar.

Güvenlik Duvarı IPS koruması, ağdaki zararlı etkinlikleri gerçek zamanlı olarak tespit edip engelleyerek, ağ güvenliğini önemli ölçüde artıran bir özelliktir.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Güvenlik Duvarı üzerinden Uygulama Kontrolü Şekil 6'de görüldüğü şekilde eklenmiştir.



Şekil 6. Sadece Güvenlik Duvarı IPS Koruması Aktif

İlgili politika varsayılan modda aktif hale getirilmiş, engelleme ve izin verme için herhangi bir özelleştirme yapılmamıştır.

Testler yukarıda belirtilen ortama yapılarak madde 6.5'deki bulgular elde edilmiştir.

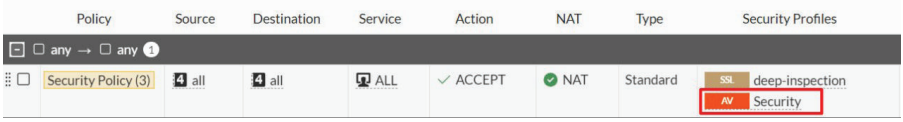
4.7. Yeni Nesil Güvenlik Duvarında Antivirüs Korumasının Aktif Hale Getirilmesi

Yeni Nesil Güvenlik Duvarı Antivirüs koruması, bir ağ güvenlik duvarı üzerinde çalışan ve ağ trafiği içerisindeki kötü amaçlı yazılımları tespit ederek engellemeye yönelik bir özelliktir. Bu, güvenlik duvarının gelen ve giden trafiği analiz etmesini ve potansiyel tehditleri, özellikle virüsleri ve zararlı yazılımları tanımlayıp engellemesini sağlar [14].

1. Kötü Amaçlı Yazılımların Engellenmesi: Antivirüs koruması, ağ üzerinden gelen verileri tarar ve virüsler, solucanlar, truva atları gibi kötü amaçlı yazılımların sistemlere girmesini engeller.
2. Gelişmiş Tehdit Koruması: Bu sistem, daha önce bilinmeyen zararlı yazılımları tespit etmek için davranış tabanlı analiz yöntemleri kullanabilir. Bu sayede, yeni ve bilinmeyen tehditlere karşı da koruma sağlar.
3. Ağ Üzerindeki Taramalar: Güvenlik Duvarı Antivirüs, ağdaki tüm veriyi kontrol ederek, virüslerin yayılmasını engeller. Hem dışardan gelen tehditlere hem de iç ağdaki cihazlar arasındaki tehditlere karşı koruma sunar.

Güvenlik Duvarı Antivirüs koruması, ağ güvenliği sağlamak ve sistemleri kötü amaçlı yazılımlardan korumak için kritik bir bileşendir.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Güvenlik Duvarı üzerinden Antivirüs özelliği Şekil 7'de görüldüğü şekilde eklenmiştir.



Şekil 7. Sadece Güvenlik Duvarı Antivirüs Koruması Aktif İlgili politika içerisinde herhangi bir özelleştirme yapılmamıştır.

Testler yukarıda belirtilen ortama yapılarak madde 6.6'daki bulgular elde edilmiştir.

4.8. Yalnız Microsoft Defender'ın Aktif Hale Getirilmesi

Microsoft Defender, Windows işletim sistemi üzerinde yerleşik olarak bulunan bir güvenlik yazılımıdır. Bu yazılım, cihazları virüsler, zararlı yazılımlar, kimlik avı atakları ve diğer güvenlik tehditlerine karşı korur. Microsoft Defender, sürekli çalışan bir Antivirüs programı olarak, kullanıcıların internet üzerinde güvenli bir şekilde gezinmesini ve dosyaları güvenle indirmesini sağlar. Ayrıca, cihazda bulunan dosyaları tarar, tehditlere karşı gerçek zamanlı koruma sağlar ve sistemdeki olası zayıf noktaları tespit eder [15].

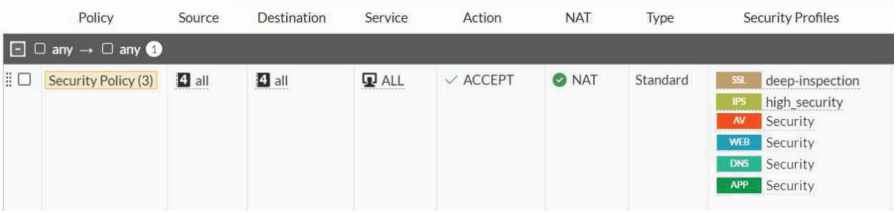
1. Gerçek Zamanlı Koruma: Virüsler, solucanlar, truva atları ve diğer zararlı yazılımlar sisteme girmeden önce tespit edilip engellenir.
2. İnternet Güvenliği: Microsoft Defender, web tarayıcıları üzerinden gelen tehditleri izler ve internet üzerinde güvenli bir gezinme deneyimi sunar.
3. Performans ve Uyumluluk: Microsoft Defender, sistem kaynaklarını optimize ederek cihazın performansını etkilemeden güvenlik sağlar.
4. Kimlik Avı Koruması: Microsoft Defender, kimlik avı atakları ve dolandırıcılık e- postalarını tespit ederek kullanıcıyı uyarır.

Bu özellikler, kullanıcıların cihazlarını tehditlerden korur ve güvenlik sağlar.

Tüm Yeni Nesil Güvenlik Duvarı güvenlik katmanları kapalıyken ve Windows üzerindeki temel tüm güvenlik katmanları aktifken herhangi bir özelleştirme olmadan yapılan testlerde madde 6.7'deki bulgular elde edilmiştir.

4.9. Tüm Güvenlik Katmanlarının Bir Arada Aktif Hale Getirilmesi

Madde 4.3, 4.4, 4.5, 4.6 ve 4.7 deki Yeni Nesil Güvenlik Duvarı üzerindeki tüm güvenlik katmaları varsayılan modda açılmış ve Şekil 8'de görüleceği üzere politikada bir arada uygulanmıştır.



Şekil 8. Tüm Güvenlik Duvarı güvenlik katmanları aktif

Microsoft Defender varsayılan ayarları ile madde 4.8'de belirtildiği gibi aktif hale getirilmiştir.

Bu şekilde hem Yeni Nesil Güvenlik Duvarı özelliklerinin hem de Microsoft Defender'ın birlikte sağladıkları güvenliğin ölçülmesi hedeflenmiştir. Tüm güvenlik katmanları aktifken yapılan simülasyonlarda madde 6.8'deki bulgular elde edilmiştir.

5. Veri

Bu çalışmada kullanılan veri seti, tezdeki analizlerin tekrarlana bilirliğini ve şeffaflığını artırmak amacıyla GitHub platformunda depolanmıştır. Veri setine https://github.com/buroxy/attackdata bağlantısı üzerinden erişilebilir [16].

Veri seti, Excel biçimindedir ve gerekli açıklamaları içeren bir README dosyası ile birlikte paylaşılmıştır. Bu dosya, veri setinin yapısını, değişkenlerin anlamlarını detaylı olarak açıklamaktadır. Çalışmanın tekrar edilebilirliği ve farklı araştırmacılar tarafından kullanılabilirliği için veri seti herkese açık olarak yayınlanmıştır.

6. Bulgular

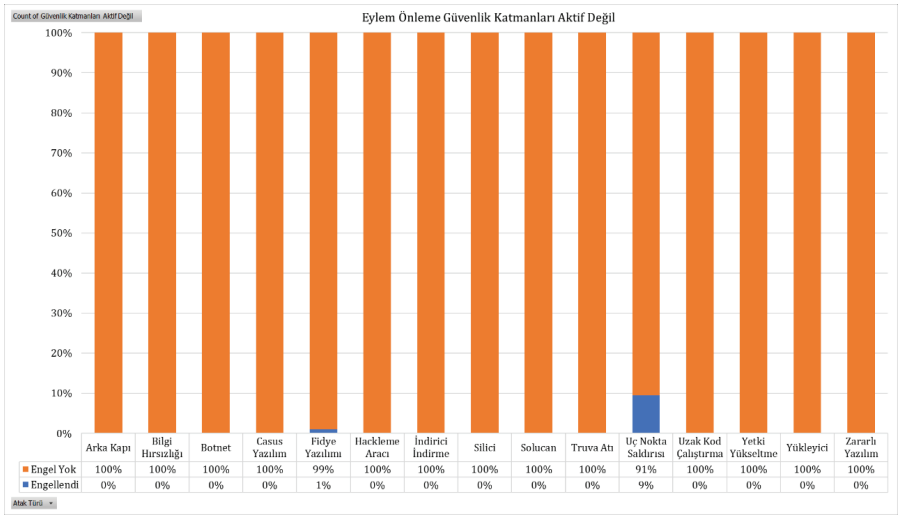
Madde 2.6'de belirtilen test ortamı için madde 0'de bulunan 8 durum statüsü, madde 2.4'deki test atak kategorileri ile ayrı ayrı uygulanarak test edilmiştir.

Yapılan çalışmada tehditlerin gerçekleşmesi için tüm eylemler adım adım uygulanmıştır.

6.1. Hiçbir Güvenlik Katmanı Aktif Değilken

Madde 4.1'de belirtildiği üzere Windows üzerinde varsayılan olarak bulunan Microsoft Defender devre dışı bırakılarak Windows işletim sisteminin çekirdek seviyede güvenliği ölçülmesi amaçlanmıştır.

Şekil 9, Windows işletim sistemi üzerinde hiçbir güvenlik katmanı aktif değilken gerçekleştirilen saldırılara karşı sistemin gösterdiği savunma performansını özetlemektedir. Test ortamında gerçekleştirilen bu saldırılar, işletim sisteminin core (çekirdek) servislerinin belirli saldırı türlerini sınırlı da olsa önleyebildiğini göstermektedir. Ancak genel sonuçlar, güvenlik katmanlarının devre dışı olduğu bir sistemin siber saldırılara karşı büyük ölçüde savunmasız olduğunu ortaya koymaktadır.



Şekil 9. Hiçbir güvenlik katmanı aktif değilken eylem önleme sonucu

Şekil 9'de görüldüğü üzere, fidye yazılımı kategorisindeki saldırıların yalnızca %1'i, uç nokta saldırılarının ise %9'u Windows core servisleri tarafından engellenebilmiştir. Diğer kategorilerde, saldırıların %100'ü başarıyla gerçekleştirilmiştir. Bu sonuç, Windows işletim sistemi üzerinde yerleşik güvenlik önlemlerinin, belirli durumlarda minimal koruma sağlamakla birlikte, kapsamlı bir güvenlik stratejisi olmadan etkisiz kaldığını açıkça göstermektedir.

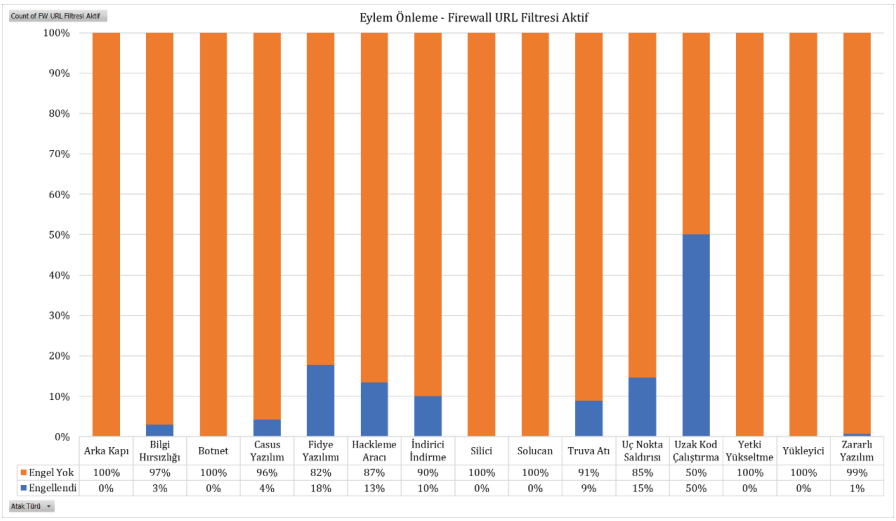
Şekil 17'ya bakıldığında, Windows core servislerinin tüm saldırıların yalnızca %6'sını engellemede başarılı olduğu belirtilmektedir. Bu oran, core servislerin yalnızca kısıtlı bir güvenlik sağlayabildiğini ve modern tehditlere karşı yeterli olmadığını ortaya koymaktadır.

Sonuç olarak, hiçbir ek güvenlik katmanı etkinleştirilmediğinde, Windows işletim sistemi siber saldırılara karşı genel olarak savunmasızdır. Bu durum, işletim sisteminin güvenlik açıklarını kapatmak ve tehditleri etkili bir şekilde engellemek için çok katmanlı bir güvenlik stratejisinin gerekliliğini bir kez daha vurgulamaktadır. Uygulamalı testler, entegre güvenlik katmanlarının etkinleştirilmesinin saldırılara

karşı direnci önemli ölçüde artıracağını ve sistem güvenliğini üst seviyeye taşıyacağını göstermektedir.

6.2. Güvenlik Duvarı URL Filtresi Aktifken

Şekil 10, sadece Güvenlik Duvarı URL filtresinin aktif olduğu madde 4.3'de belirtilen test ortamında, belirli saldırı türlerini engelleme yeteneğini değerlendirmektedir. Test ortamında yapılan analizler, Güvenlik Duvarı URL filtresinin bazı tehdit kategorilerinde kısmi koruma sağladığını ancak genel olarak tek başına yeterli olmadığını göstermektedir.



Şekil 10. Güvenlik Duvarı URL filtresi aktifken eylem önleme sonucu

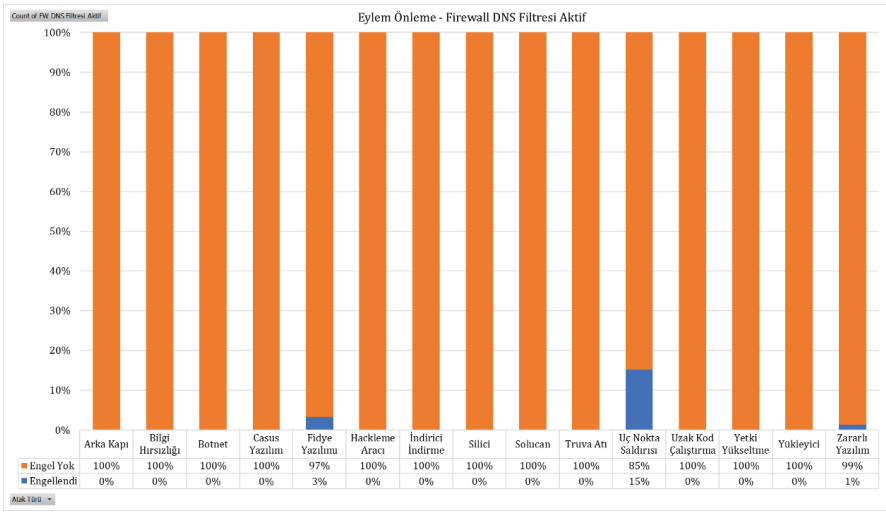
Eylem önleme sonuçlarına göre, Bilgi Hırsızlığı kategorisinin yalnızca %3'ü, Casus Yazılım kategorisinin %4'ü, Fidye Yazılımı kategorisinin %18'i, Hackleme Aracı kategorisinin %87'si, İndirici İndirme kategorisinin %10'u, Truva Atı kategorisinin %9'u, Uç Nokta Atakları kategorisinin %15'i, Uzaktan Kod Çalıştırma kategorisinin %50'si ve Zararlı Yazılım kategorisinin %1'i Güvenlik Duvarı URL

filtresi tarafından engellenmiştir. Bu oranlar, Güvenlik Duvarı URL filtresinin bazı kategorilerde daha başarılı olduğunu, özellikle hackleme araçları (%87) ve uzaktan kod çalıştırma (%50) gibi belirli tehditlerde etkili olduğunu ortaya koymaktadır. Ancak birçok tehdit türü (örneğin, bilgi hırsızlığı ve fidye yazılımı gibi) karşısında etkisinin oldukça sınırlı olduğu görülmektedir. Güvenlik Duvarı URL filtresi, güvenlik stratejisinin bir parçası olarak önemli bir yere sahip olsa da, tek başına uygulanması durumunda cihazlar ciddi ölçüde savunmasız kalmaktadır. Bu durum, çok katmanlı güvenlik çözümlerinin gerekliliğini açıkça ortaya koymaktadır. Şekil 17'da görüldüğü üzere, Güvenlik Duvarı URL filtresi tüm saldırıların yalnızca %11'ini engelleyebilmiştir. Bu oran, Güvenlik Duvarı URL filtresinin yalnızca bir yardımcı güvenlik katmanı olarak değerlendirilmesi gerektiğini ve diğer güvenlik önlemleriyle birleştirildiğinde daha etkili bir savunma sağlayacağını göstermektedir.

Sonuç olarak, Güvenlik Duvarı URL filtresi tek başına belirli tehdit türlerine karşı kısmi bir koruma sağlayabilse de, geniş kapsamlı bir güvenlik stratejisinin bir parçası olarak kullanıldığında daha iyi sonuçlar elde edilebileceği açıktır. Sistem güvenliği açısından, farklı güvenlik katmanlarının entegrasyonu ve uyum içinde çalışması, ağ savunmasını optimize etmek için kritik bir önem taşımaktadır.

6.3. Güvenlik Duvarı DNS Filtresi Aktifken

Güvenlik Duvarı DNS filtresi aktifken uygulanan ataklarda Güvenlik Duvarı DNS filtresinin atakları engelleme konusunda yetkinliği değerlendirilmiştir. Şekil 29, Güvenlik Duvarı DNS filtresinin aktif olduğu madde 4.4'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını özetlemektedir. Test ortamında uygulanan saldırılar, Güvenlik Duvarı DNS filtresinin belirli tehdit kategorilerinde kısmi bir koruma sağladığını, ancak genel olarak tek başına uygulandığında cihazların savunmasız kaldığını göstermektedir.



Şekil 11. Güvenlik Duvarı DNS filtresi aktifken eylem önleme sonucu

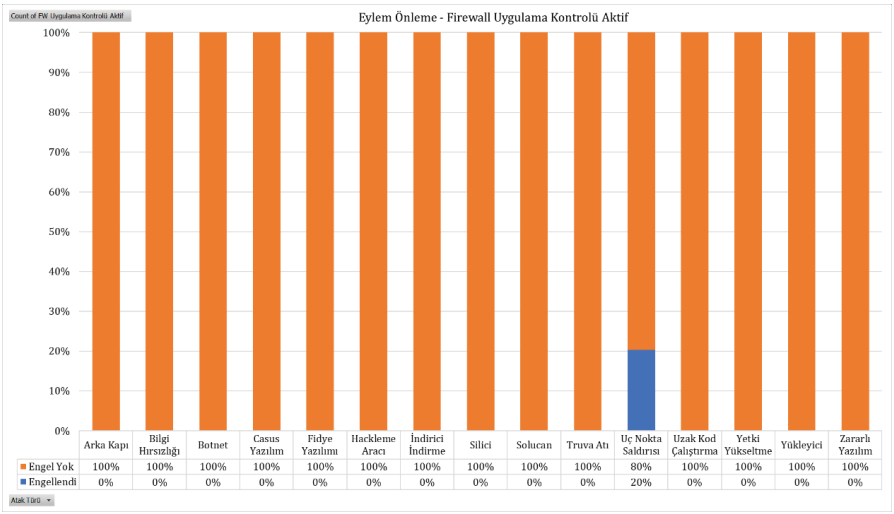
Eylem önleme sonuçlarına göre, Fidye Yazılımı kategorisindeki saldırıların yalnızca %3'ü, Uç Nokta Saldırıları kategorisindeki saldırıların %15'i ve Zararlı Yazılım kategorisindeki saldırıların %1'i Güvenlik Duvarı DNS filtresi tarafından engellenebilmiştir. Diğer tehdit kategorilerinde ise saldırıların tamamının başarılı olduğu dikkat çekmektedir. Bu durum, Güvenlik Duvarı DNS filtresinin güvenlik açısından tek başına yeterli olmadığını ve yalnızca sınırlı bir koruma sağlayabildiğini açıkça ortaya koymaktadır. Şekil 17'ya bakıldığında, Güvenlik Duvarı DNS filtresi tüm saldırıların yalnızca %10'unu engelleyebilmiştir. Bu oran, DNS filtrelemenin bazı durumlarda etkili bir savunma mekanizması olabileceğini ancak daha geniş kapsamlı bir güvenlik politikası içinde kullanılmasının zorunlu olduğunu göstermektedir. DNS filtresi, özellikle fidye yazılımı ve uç nokta saldırıları gibi belirli tehdit türlerinde sınırlı da olsa etkili olurken, diğer tehdit kategorilerinde neredeyse hiçbir koruma sağlayamamaktadır.

Sonuç olarak, Güvenlik Duvarı DNS filtresi tek başına uygulandığında, cihazlar ciddi ölçüde savunmasızdır. Güvenlik Duvarı DNS filtresi, diğer güvenlik katmanlarıyla birlikte kullanıldığında daha

etkin bir savunma sağlayabilir. Ancak, modern tehditlerin karmaşıklığı ve saldırganların sürekli gelişen teknikleri değerlendirildiğinde, DNS filtrelemenin yalnızca bir yardımcı güvenlik aracı olarak değerlendirilmesi ve diğer katmanlarla entegrasyonunun sağlanması gerektiği açıkça görülmektedir. Bu bağlamda, DNS filtresinin çok katmanlı bir güvenlik çözümünün parçası olarak kullanılmasının sistem güvenliğini artıracağı söylenebilir.

6.4. Güvenlik Duvarı Uygulama Kontrolü Aktifken

Şekil 12, Güvenlik Duvarı Uygulama Kontrolü'nün aktif olduğu madde 4.5'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını göstermektedir. Güvenlik Duvarı Uygulama Kontrolü'nün belirli tehdit türlerine karşı sınırlı bir koruma sağladığını, ancak tek başına genel güvenlik için yetersiz olduğunu ortaya koymaktadır.



Şekil 12. Güvenlik Duvarı uygulama kontrolü aktifken eylem önleme sonucu

Eylem önleme sonuçlarına göre, yalnızca Uç Nokta Saldırıları kategorisindeki saldırıların

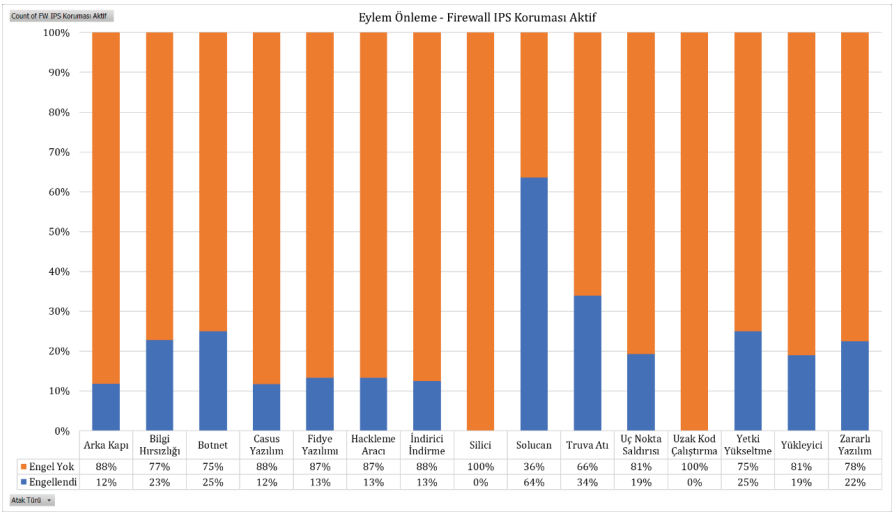
%20'si Güvenlik Duvarı Uygulama Kontrolü tarafından engellenebilmiştir. Diğer tehdit kategorilerinde herhangi bir engelleme sağlanamamıştır. Bu durum, Güvenlik Duvarı Uygulama Kontrolü'nün tek başına siber saldırılara karşı yeterli bir savunma sağlamadığını ve güvenlik katmanlarının birlikte kullanılmasının önemini bir kez daha vurgulamaktadır. Şekil 17'da görüleceği üzere, Güvenlik Duvarı Uygulama Kontrolü tüm saldırıların yalnızca

%13'ünü engellemiştir. Bu oran, Güvenlik Duvarı Uygulama Kontrolü'nün belirli tehditlere karşı etkili bir araç olabileceğini ancak kapsamlı bir güvenlik stratejisi içinde yardımcı bir bileşen olarak değerlendirilmesi gerektiğini göstermektedir. Uygulama kontrolü, özellikle belirli uygulamalardan gelen tehditlere karşı bir bariyer oluşturabilir, ancak saldırganların farklı teknikler kullanarak bu katmanı aşabileceği unutulmamalıdır.

Sonuç olarak, Güvenlik Duvarı Uygulama Kontrolü tek başına uygulanmaya devam ettiğinde cihazlar savunmasız kalmaktadır. Bu durum, siber güvenlikte çok katmanlı yaklaşımların kritik önemini bir kez daha göstermektedir. Uygulama kontrolü, diğer güvenlik katmanları ile entegre edildiğinde daha etkili bir savunma sağlamakta ve modern tehditlere karşı daha güçlü bir koruma oluşturabilmektedir. Bu bağlamda, Güvenlik Duvarı Uygulama Kontrolü'nün, ağ güvenliğinde destekleyici bir katman olarak kullanılması gerektiği açıktır.

6.5. Güvenlik Duvarı IPS Koruması Aktifken

Şekil 13, Güvenlik Duvarı IPS (Saldırı Önleme Sistemi) korumasının aktif olduğu madde 4.6'da belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını detaylandırmaktadır. Test ortamında yapılan analizler, IPS korumasının belirli tehdit kategorilerinde diğer koruma önlemlerine kıyasla daha tatmin edici bir başarı sağladığını, ancak tek başına tam koruma sağlamadığını göstermektedir.



Şekil 13. Güvenlik Duvarı IPS koruması aktifken eylem önleme sonucu

Eylem önleme sonuçlarına göre: Arka Kapı saldırılarının %12'si, Bilgi Hırsızlığı saldırılarının

%23'ü, Botnet saldırılarının %25'i, Casus Yazılım saldırılarının %12'si, Fidye Yazılımı saldırılarının %13'ü, Hackleme Aracı ve İndirici İndirme kategorilerindeki saldırıların %13'ü, Solucan saldırılarının %64'ü, Truva Atı saldırılarının %34'ü, Uç Nokta Saldırılarının %19'u, Yetki Yükseltme saldırılarının %25'i, Yükleyici saldırılarının %19'u ve Zararlı Yazılım kategorisindeki saldırıların %22'si Güvenlik Duvarı IPS koruması tarafından engellenmiştir.

Bu oranlar, Güvenlik Duvarı IPS korumasının özellikle Solucan (%64) ve Truva Atı (%34) gibi tehdit türlerinde daha etkili olduğunu göstermektedir.

Şekil 17'da görüldüğü üzere Güvenlik Duvarı IPS koruması, tüm saldırıların yalnızca %19'unu engelleyebilmiştir. Bu, IPS'in ağ güvenliği için önemli bir bileşen olduğunu, ancak diğer güvenlik katmanlarıyla birleştirilmesi gerektiğini göstermektedir. IPS, saldırıların sistem üzerinde oluşturabileceği zararları azaltmak için önemli bir savunma hattı oluşturabilir, ancak modern tehditlerin çeşitliliği karşısında tek başına yeterli bir koruma sağlayamamaktadır.

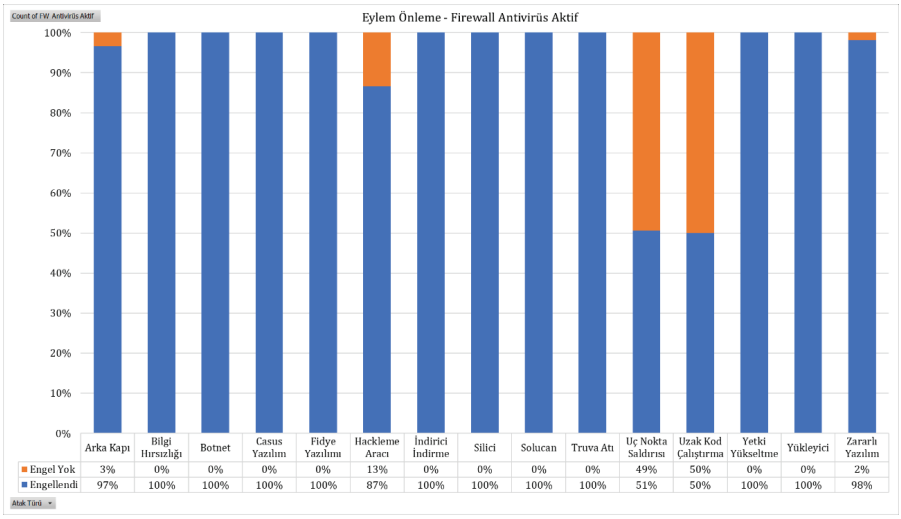
Sonuç olarak, Güvenlik Duvarı IPS koruması diğer güvenlik önlemlerine kıyasla daha tatmin edici sonuçlar sunmakta olsa da çok katmanlı bir güvenlik stratejisi içinde bir destekleyici katman olarak kullanılması gereklidir. IPS'in, Güvenlik Duvarı, DNS Filtreleme ve diğer güvenlik çözümleriyle birlikte entegre bir şekilde kullanılması, daha geniş kapsamlı bir koruma sağlayarak cihazların modern tehditlere karşı dayanıklılığını artıracaktır.

6.6. Güvenlik Duvarı Antivirüs Aktifken

Güvenlik Duvarı Antivirüs korumasının aktif olduğu madde 4.7'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını detaylandırmaktadır. Test ortamında yapılan analizler, Güvenlik Duvarı Antivirüs özelliğinin birçok tehdit kategorisinde etkili koruma sağladığını ancak tüm tehditler için tam koruma sunmadığını ortaya koymaktadır.

Eylem önleme sonuçlarına göre: Arka Kapı kategorisindeki saldırıların %3'ü, Hackleme Aracı kategorisindeki saldırıların %13'ü, Uç Nokta Saldırılarının %51'i, Uzak Kod Çalıştırma kategorisindeki saldırıların %50'si ve Zararlı Yazılım kategorisindeki saldırıların %2'si Güvenlik Duvarı Antivirüs tarafından engellenememiştir.

Buna karşın, diğer tehdit kategorilerinde (örneğin, bilgi hırsızlığı, botnet, casus yazılım ve fidye yazılımı gibi) %100'e yakın bir başarı oranı elde edilmiştir. Bu durum, Güvenlik Duvarı Antivirüs'ün genel koruma kapasitesinin oldukça yüksek olduğunu ancak belirli saldırı türlerinde hala iyileştirmeye ihtiyaç duyulduğunu göstermektedir.



Şekil 14. Güvenlik Duvarı Antivirüs aktifken eylem önleme sonucu

Şekil 17'ya göre, Güvenlik Duvarı Antivirüs koruması tüm saldırıların %69'unu engellemeyi başarmıştır. Bu, Güvenlik Duvarı Antivirüs'ün diğer güvenlik önlemlerine kıyasla daha geniş bir koruma alanı sağladığını ortaya koymaktadır. Ancak, kalan %31'lik saldırı oranı, Güvenlik Duvarı Antivirüs'ün tek başına tam bir güvenlik çözümü sağlayamayacağını göstermektedir.

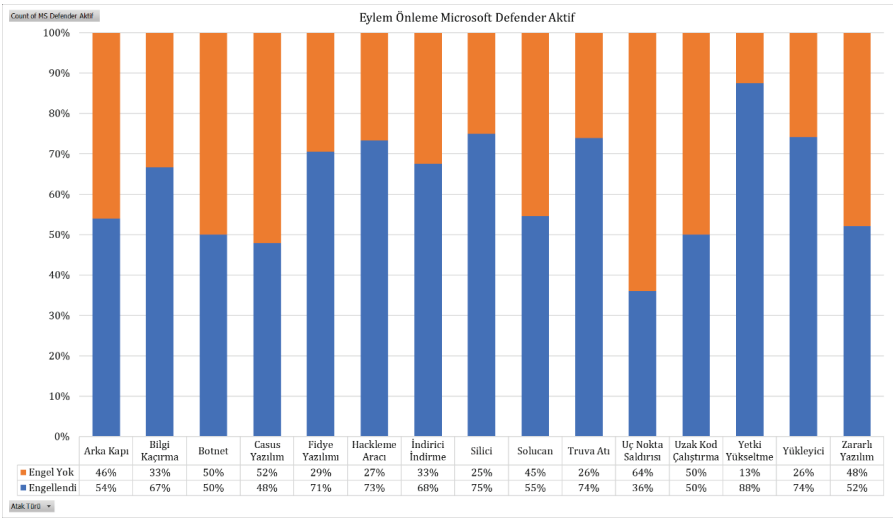
Sonuç olarak, Güvenlik Duvarı Antivirüs, ağ güvenliği stratejisinde güçlü bir bileşen olarak öne çıkmaktadır. Ancak, sistemin tam anlamıyla korunması için diğer güvenlik katmanlarıyla entegre bir şekilde çalışması gerekmektedir. Modern siber tehditlerin çeşitliliği ve karmaşıklığı göz önüne alındığında, Güvenlik Duvarı Antivirüs koruması çok katmanlı bir güvenlik yaklaşımının bir parçası olarak kullanılmalı ve diğer teknolojilerle desteklenmelidir. Bu entegre yaklaşım, cihazların daha güçlü ve kapsamlı bir koruma altında olmasını sağlayacaktır.

6.7. Microsoft Defender Aktifken

Microsoft Defender'ın aktif olduğu madde 4.8'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını detaylı bir şekilde sunmaktadır. Test ortamında yapılan analizler, Microsoft Defender'ın belirli tehdit kategorilerinde güçlü bir koruma sağladığını ancak tüm tehditlere karşı tek başına tam bir güvenlik sunamayacağını açıkça göstermektedir.

Eylem önleme sonuçlarına göre: Arka Kapı kategorisinde %54, Bilgi Kaçırma kategorisinde

%67, Botnet kategorisinde %50, Casus Yazılım kategorisinde %48, Fidye Yazılımı kategorisinde %29, Hackleme Aracı kategorisinde %73,İndirici İndirme kategorisinde %68, Silici kategorisinde %75, Solucan kategorisinde %55, Truva Atı kategorisinde %74, Uç Nokta Saldırıları kategorisinde %36, Uzak Kod Çalıştırma kategorisinde %50, Yetki Yükseltme kategorisinde %88, Yükleyici kategorisinde %74 ve Zararlı Yazılım kategorisinde %52 başarı oranı sağlanmıştır.



Şekil 15. Microsoft Defender aktifken eylem önleme sonucu

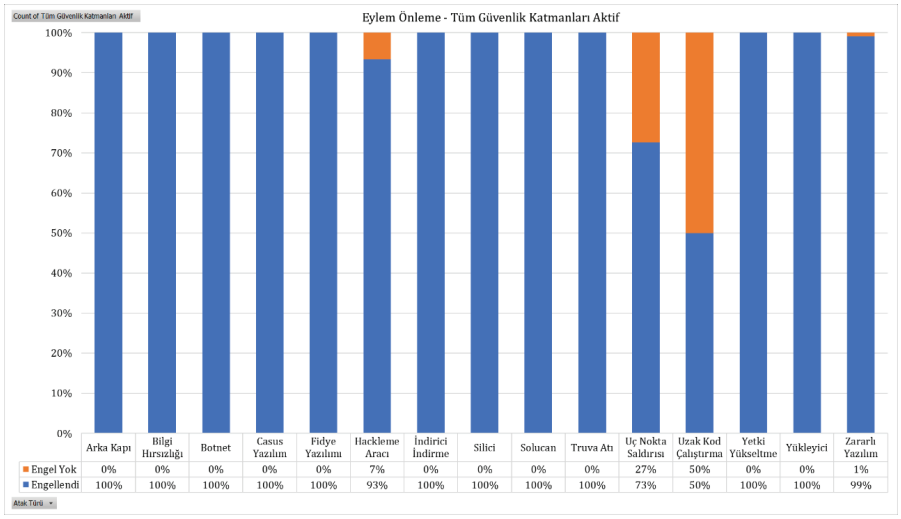
Bu sonuçlar, Microsoft Defender'ın birçok tehdit kategorisinde etkili bir savunma sağladığını, özellikle Yetki Yükseltme %88, Silici %75 ve Truva Atı %74 gibi kategorilerde yüksek engelleme oranlarına ulaştığını göstermektedir. Ancak, Fidye Yazılımı %29 ve Uç Nokta Saldırıları %36 gibi kategorilerde başarı oranlarının nispeten düşük olması, Microsoft Defender'ın tek başına tüm tehditlere karşı tam koruma sağlayamadığını ortaya koymaktadır.

Şekil 17'da görüldüğü üzere Microsoft Defender, tüm saldırıların yalnızca %46'sını engellemede başarılı olmuştur. Bu oran, Defender'ın güvenlik çözümünde önemli bir rol oynadığını ancak diğer güvenlik katmanlarıyla desteklenmediği sürece cihazların tam anlamıyla güvende kalamayacağını göstermektedir.

Microsoft Defender, modern tehditlere karşı güçlü bir savunma mekanizması sunan bir güvenlik aracı olarak öne çıkmaktadır. Ancak, "sıfır güven" yaklaşımı göz önüne alındığında, Defender'ın tek başına kullanılması cihazların güvenliği için yeterli değildir. Bu nedenle, çok katmanlı bir güvenlik stratejisinin bir parçası olarak değerlendirilmesi kritik öneme sahiptir. Microsoft Defender, Güvenlik Duvarı, IPS ve diğer güvenlik çözümleriyle entegre bir şekilde kullanıldığında daha etkili bir koruma sağlamakta ve tehditlerin büyük bir kısmını engelleyebilmektedir. Bu entegre yaklaşım, modern siber tehditlere karşı daha kapsamlı ve dayanıklı bir savunma sağlar.

6.8. Tüm Güvenlik Katmanları Aktifken

Şekil 16, madde 4.3, 4.4, 4.5, 4.6, 4.7 ve 4.8 belirtilen tüm güvenlik katmanlarının bir arada aktif olduğu madde 4.9'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını detaylandırmaktadır. Test ortamında yapılan analizler, çok katmanlı güvenlik mimarisinin, her bir güvenlik katmanının tek başına sağladığı korumadan çok daha yüksek bir başarı oranı elde ettiğini göstermektedir.



Şekil 16. Tüm güvenlik katmanları aktifken eylem önleme sonucu

Eylem önleme sonuçlarına göre, tüm güvenlik katmanları aktifken: Hackleme Aracı kategorisindeki saldırıların yalnızca %7'si, Uç Nokta Saldırıları kategorisindeki saldırıların

%27'si, Uzak Kod Çalıştırma kategorisindeki saldırıların %50'si engellenememiştir.

Buna karşın, diğer tüm tehdit kategorilerinde (örneğin, Arka Kapı, Bilgi Hırsızlığı, Botnet, Fidye Yazılımı ve Solucan gibi) %100'e yakın bir başarı oranı sağlamıştır. Bu sonuçlar, çok katmanlı güvenlik mimarisinin tehditleri önlemede etkili olduğunu ortaya koymaktadır.

Şekil 17'da görüldüğü üzere, tüm güvenlik katmanlarının bir arada kullanıldığı senaryoda, tüm saldırıların %83'ü engellenebilmiştir. Bu oran, tüm katmanların bir arada çalışmasının, tehditlerin büyük bir kısmını etkisiz hale getirdiğini göstermektedir. Ancak, belirli kategorilerde hala engellenemeyen saldırılar bulunması, çok katmanlı güvenlik stratejisinin sürekli izlenmesi, geliştirilmesi ve güncellenmesi gerektiğini vurgulamaktadır.

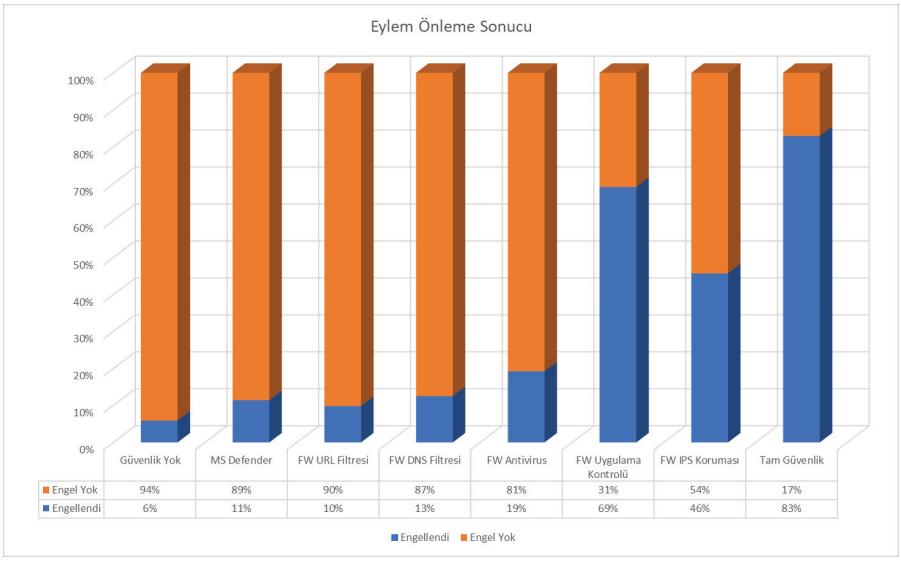
Tüm güvenlik katmanlarının aktif olduğu bir yapı, siber tehditlere karşı güçlü bir savunma mekanizması sağlamaktadır. Katmanlı

güvenlik mimarisi, farklı tehditlere karşı her güvenlik katmanının benzersiz yeteneklerini birleştirerek saldırı yüzeyini azaltır.

Sonuç olarak, tüm güvenlik katmanlarının birlikte kullanıldığı çok katmanlı mimari, modern siber tehditlere karşı kapsamlı ve etkili bir koruma sağlamakta, ancak kalan risklerin de göz önünde bulundurulması gerektiğini açıkça ortaya koymaktadır. Bu bağlamda, entegre güvenlik çözümlerinin proaktif önlemlerle desteklenmesi, cihazların ve ağların daha güvenli hale gelmesini sağlayacaktır.

6.9. Bulguların Karşılaştırılması

Her bir eylemi önlemeye dair sonuç çıktıları Şekil 17'de görüldüğü gibidir.



Şekil 17. Güvenlik Katmanları Eylem Önleme Sonucu Grafiği

Şekil 17'da güvenlik katmanlarının etkinleştirilmesi durumunda alınan sonuçları ve bu katmanların saldırılara karşı sağladığı koruma seviyelerini net bir şekilde ortaya koymaktadır. Grafik, güvenlik

katmanlarının ayrı ayrı kullanıldığında, her birinin belirli ölçüde koruma sağladığını ancak tek başına yeterli olmadığını göstermektedir. Örneğin, DNS filtresi, IPS koruması veya URL filtreleme gibi yöntemler belirli saldırı türlerini önleyebilse de, diğer katmanların eksik olduğu durumlarda sistemin büyük ölçüde savunmasız kaldığı görülmektedir.

Tüm güvenlik katmanlarının bir arada kullanıldığı senaryoda, saldırıların büyük bir çoğunluğunun etkisiz hale getirildiği (saldırıların %83'ü engellenmiş, %17 saldırı başarılı olmuştur) dikkat çekmektedir. Bu durum, katmanlı güvenlik stratejisinin önemini vurgulamaktadır. Her bir güvenlik katmanı, farklı tehdit türlerine karşı koruma sağlarken, birlikte kullanıldıklarında sistemin genel güvenlik seviyesi önemli ölçüde artmaktadır. Ancak, tüm katmanların bir arada kullanılmasına rağmen, hala küçük bir kısmın (saldırıların %17'si) başarılı olduğu göz önünde bulundurulduğunda, güvenlik stratejilerinin sürekli güncellenmesi ve tehditlerin dinamik yapısına uygun hale getirilmesi gerektiği sonucuna varılabilir.

Bu grafik, güvenlik açıklarının sadece tek bir yöntemle değil, farklı tekniklerin bir arada ve uyum içinde kullanılmasıyla minimize edilebileceğini göstermektedir. Ayrıca, herhangi bir güvenlik katmanındaki bir arıza ya da zayıflığın tüm sistemi tehdit edebileceği gerçeği, bütüncül bir güvenlik yaklaşımının önemini bir kez daha ortaya koymaktadır. Bu bağlamda, proaktif güvenlik yönetimi, düzenli izleme ve tehdit analizi gibi süreçlerin, ağ güvenliğini sürdürülebilir kılmak için kritik olduğu vurgulanmalıdır.

7. Sonuç

Yapılan simülasyonların analizlerinden çıkan sonuçlar, her güvenlik katmanının siber tehditleri önleme noktasında birbirinden bağımsız ancak tamamlayıcı bir şekilde fayda sağladığını açıkça ortaya koymaktadır. Bu bağlamda, özellikle KOBİ'ler için güvenlik altyapısının birden fazla katmandan oluşmasının kritik öneme sahip olduğu

anlaşılmaktadır. Katmanlardan herhangi birinde meydana gelebilecek bir aksaklık, atakların başarıya ulaşma olasılığını artırabileceğinden, güvenlik katmanlarının birlikte ve uyum içinde çalışması gerekliliği ön plana çıkmaktadır.

Özellikle, Microsoft Defender ve Güvenlik Duvarı katmanlarının birlikte kullanılması, madde 4.3, 4.4, 4.5, 4.6, 4.7 ve 4.8 belirtilen özelliklerin bir arada etkinleştirilmesi durumunda, KOBİ'lerin karşılaşabileceği tehditlere karşı daha güçlü bir savunma hattı oluşturulabileceği tespit edilmiştir. Bu yaklaşım, farklı güvenlik katmanlarının birbirlerini destekleyerek tehdit yüzeyini en aza indirdiğini göstermektedir.

Bununla birlikte, analizlerin bir diğer çarpıcı bulgusu, güvenlik ürünlerinin yalnızca varsayılan ayarlarla çalıştırılmasının etkili bir koruma sağlamada eksik kaldığıdır. Siber tehditlerin sürekli evrildiği bir ortamda, bu ürünlerin etkili olabilmesi için doğru şekilde yapılandırılması hayati bir öneme sahiptir. Varsayılan ayarlar genellikle genel kullanım senaryolarına göre tasarlandığı için, her işletmenin özel ihtiyaçlarına ve tehdit profiline göre optimize edilmemiş olabilir. Bu durum, güvenlik ekiplerinin ve IT yöneticilerinin konfigürasyon süreçlerine daha fazla önem vermesi gerektiğini ortaya koymaktadır.

Sonuç olarak, KOBİ'lerin kapsamlı bir güvenlik stratejisi oluştururken, çok katmanlı bir yaklaşımı benimsemeleri ve güvenlik ürünlerini doğru yapılandırmaları gerekmektedir. Bu iki temel ilke, modern tehditlere karşı etkili bir savunma sağlamanın anahtarları olarak öne çıkmaktadır.

7.1. Öneriler

Bunların yanında %100 güvenliğe ulaşmak ulaşılması neredeyse imkânsız bir hedeftir. Yukarıda uyguladığımız bu güvenlik katmanlarına temel olarak her KOBİ'nin sahip olması gerekmektedir. Bunun yanı sıra son kullanıcıların bilinçlendirilmesi, güvenlik ürünlerinin temel konfigürasyonlarının engelleyemediği %17'lik atakların hiç ortaya çıkmaması için kritik öneme sahiptir.

Giderek karmaşıklaşan siber tehditlerle karşı karşıya kalırken kısıtlı bütçeler, yetersiz insan kaynağı ve teknik altyapı eksiklikleri gibi faktörler, KOBİ'lerin güvenlik risklerini etkili bir şekilde yönetmesini engelleyebilir. Yapılan araştırmalarda, KOBİ'lerin siber güvenlik önlemlerini uygularken maliyet etkin ve pratik çözümler arayışında olduğu sonucuna ulaşılmıştır. Bu çalışma, optimum maliyetle Windows üzerinde bulunan ücretsiz koruma ve önüne konulacak bir Yeni Nesil Güvenlik Duvarı sayesinde güvenlik risklerini azaltmayı araştırmıştır ve KOBİ'ler için uygulanabilir strateji sunmuştur.

Sonuç olarak, bu en temel model KOBİ'lerin temel güvenlik ihtiyaçlarına uygun, düşük maliyetli ancak etkili bir çözümdür. Özellikle çalışan farkındalığı ve çok faktörlü kimlik doğrulama (MFA) gibi insan faktörüne dayalı önlemler KOBİ'lerin güvenlik stratejilerine ayrıca ekstra fayda sağlayacaktır.

Öneriler:

1. Katmanlı Güvenlik Modelinin Uygulanması: KOBİ'lerin, düşük maliyetli güvenlik önlemlerini aşamalı olarak devreye sokarak bütüncül bir güvenlik altyapısı kurması önerilmektedir. Bu kapsamda Microsoft Defender üzerinde bulunan XDR teknolojileri, hem uç nokta hem de ağ düzeyinde geniş kapsamlı koruma sağlayarak atak riskini azaltır.
2. Personel Eğitimi ve Farkındalık Programları: Çalışanların siber güvenlik konusunda düzenli olarak eğitilmesi, sosyal mühendislik atakları ve veri sızıntılarına karşı etkin bir önlem olacaktır. Özellikle KOBİ'lerde insan hatası büyük bir risk faktörü olduğundan, çalışanların bilinçlendirilmesi öncelikli olmalıdır.
3. Veri Şifreleme ve USB Portlarının Engellenmesi: Özellikle hassas verilerin bulunduğu yerel disklerin şifrelenmesi ve yetkisiz USB cihazlarının engellenmesi, veri sızıntılarına karşı güçlü bir savunma sağlar. Bu tür önlemler, maliyet etkin olmaları açısından KOBİ'ler için uygundur.
4. Yama ve Güncelleme Yönetimi: Sistemlerin güvenliğini artırmak için düzenli yama ve güncelleme politikalarının

uygulanması hayati öneme sahiptir. Otomatik güncelleme süreçlerinin kullanılması, güvenlik açıklarının en aza indirgenmesini sağlayacaktır.

Bu öneriler, KOBİ'lerin siber güvenlik altyapılarını güçlendirmek ve siber ataklara karşı dirençlerini artırmak için önemli bir rehber sunmaktadır. Siber güvenlik önlemlerinin aşamalı olarak uygulanması ve sürdürülebilir bir güvenlik politikası izlenmesi, KOBİ'lerin uzun vadeli başarısı için kritik önemdedir.

7.2. Gelecekte Yapılabilecek Çalışmalar

Bu çalışmanın sonuçları, KOBİ'lerin güvenlik altyapılarında çok katmanlı bir yaklaşımın önemini vurgulamış olsa da, gelecekte daha kapsamlı araştırmalara ihtiyaç duyulmaktadır. Özellikle aşağıdaki konuların araştırılması ve geliştirilmesi, güvenlik çözümlerinin etkinliğini artırmak açısından faydalı olacaktır:

Dinamik Tehdit Modelleme: Tehditlerin sürekli değişen doğası göz önüne alındığında, farklı katmanlardaki güvenlik çözümlerinin gerçek zamanlı tehditlere nasıl uyum sağladığını anlamak için dinamik modelleme yöntemleri geliştirilebilir. Bu, KOBİ'lerin karşılaşabileceği özel tehdit türlerini daha iyi tahmin etmeye olanak tanıyabilir [17].

Otomasyon ve Yapay Zeka Kullanımı: Güvenlik ürünlerinin konfigürasyon süreçlerinin daha etkin bir şekilde yapılabilmesi için yapay zeka tabanlı araçlar geliştirilebilir. Bu araçlar, KOBİ'lerin tehdit profillerini analiz ederek optimum güvenlik yapılandırmalarını otomatik olarak önerebilir [18].

Eğitim ve Farkındalık Programları: Güvenlik çözümlerinin teknik bileşenlerinin ötesinde, insan faktörünün etkisini değerlendiren çalışmalar yapılmalıdır. Özellikle KOBİ'lerde çalışanların siber güvenlik farkındalığını artırmak için etkili eğitim yöntemleri araştırılabilir [19].

Ekonomik ve Operasyonel Etki Analizleri: Çok katmanlı güvenlik stratejilerinin KOBİ'lere olan mali ve operasyonel etkileri üzerine detaylı analizler yapılabilir. Bu, KOBİ'lerin sınırlı bütçeleriyle en uygun güvenlik yatırımlarını belirlemesine yardımcı olabilir.

Yukarıda belirtilen gelecek çalışmaların gerçekleştirilmesi, modern tehditlere karşı daha etkin ve sürdürülebilir bir savunma mekanizmasının oluşturulmasına katkı sağlayacaktır.

Teşekkür

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli Hocam Dr. Mustafa Cem KASAPBAŞI'na teşekkürlerimi sunarım.

Bu çalışmanın tamamlanmasında desteğini ve yardımlarını gördüğüm Vildan KALKAVAN'a teşekkür ederim.

Referanslar

[1] <https://ekokobi.com/kobiler-icin-dijitallesmenin-maliyet-etki-analizi-ve-yatirim-stratejileri>, (Erişildi : 4.12.2024).

[2] <https://siberulak.com/kalkani-guclendirmek-kobiler-icin-siber-guvenlik-stratejileri>, (Erişildi : 17.12.2024).

[3] <https://kobitek.com/kobileri-siber-riskler-degil-bilgisizlik-tehlikeye-atiyor>, (Erişildi : 5.12.2024).

[4] <https://www.tripwire.com/state-of-security/business-impact-report-small-businesses-and-cyberattacks>, (Erişildi : 7.12.2024).

[5] Kara, Ş., Zengin, A. ve Hızal, S., "Ağ Sistemlerinin Güvenliği İçin Siber Saldırıların Ayrık Olaylı Sistem Tanımlama Tabanlı Modellenmesi ve Simülasyonu," Mühendislik Bilimleri ve Araştırmaları Dergisi, 5(2), (2023), sayfalar 186-202. Doi: 10.46387/bjesr.1268038

[6] Neupane, K., Haddad, R. ve Chen, L., Next Generation Firewall for Network Security: A Survey, 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), (s. 202-209), (2011, Nisan), Paris, IEEE.

[7] Hatipoğlu, C. ve Tunacan, T., Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması, BŞEÜ Fen Bilimleri Dergisi, 8(1), (2021), sayfalar 430-445. Doi: 10.35193/bseufbd.838732

[8] <https://learn.microsoft.com/en-us/powershell/module/defender/set-mppreference>, (Erişildi : 17.12.2024).

[9] Radivilova, T., Kirichenko, L. ve Ageyev, D., Gizli Tehditlerin Tespiti İçin SSL/TLS Trafiğinin Şifre Çözümü, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), (s. 187-191), (2018, Mayıs), Kiev, IEEE.

[10] Banday, M. T. ve Shah, N. A., A Concise Study of Web Filtering, Sprouts: Working Papers on Information Systems, 10(31), (2010), sayfalar 1-11. Doi: http://sprouts.aisnet.org/10-31

[11] <https://blog.safedns.com/dns-filtering-dns-firewall-any-difference/>, (Erişildi : 6.12.2024).

[12] <https://www.diligent.com/resources/blog/application-controls>, (Erişildi : 6.12.2024).

[13] Abdelkarim, A. A. ve Nasereddin, H. H. O., Intrusion Prevention System, International Journal of Academic Research, 3(1), (2011), sayfalar 432-434.

[14] <https://www.paloaltonetworks.com/cyberpedia/firewall-vs-antivirus>, (Erişildi : 7.12.2024).

[15] Ishihara, Y., Develop of a Sample Classifier Through Multivariate Analysis for Coffee Bitterness Levels Using a Voltammetric Electronic Tongue, HCI International 2022 Posters, Communications in Computer and Information Science, 1583, (s. 3-10), (2022, Haziran), Gothenburg, İsveç. DOI: 10.1007/978-3-031-06394-7_3

[16] <https://github.com/buroxy/attackdata>, (Erişildi : 21.12.2024).

[17] <https://thecyberexpress.com/adaptive-cybersecurity-strategies>, (Erişildi : 20.12.2024).

[18] Kant, D. ve Johannsen, A., Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs), Electronic Imaging 2022, (s. 1-7), (2022, Ocak), Brandenburg, Society for Imaging Science and Technology.

[19] Bada, M. ve Nurse, J. R. C., Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs), Information and Computer Security, 27(3), (2019), sayfalar 393-410. Doi: https://doi.org/10.1108/ICS-07-2018-0080