KURUMSAL BİLGİ GÜVENLİĞİ ÜZERİNDE YENİ KAYITLI İNTERNET SİTELERİNİN ETKİSİNİN ANALİZ EDİLMESİ

S. Ganal, M. A. Yalçınkaya, E. U. Küçüksille
Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
Isparta, TÜRKİYE
samet.ganal@kuveytturk.com.tr, mehmetyalcinkaya@sdu.edu.tr, ecirkucuksille@sdu.edu.tr

ÖZET

İnternet üzerinde yayına başlaması üzerinden 14 gün geçmemiş ve Proxy uygulamaları tarafından henüz kategorize edilmemiş olan web siteleri, yeni kayıtlı web siteleri olarak adlandırılmaktadır. Kurumsal bilgi güvenliğini sağlamak için, yeni kayıtlı internet sitelerine yönelik ne tür bir politika uygulanması gerektiği, çözülmesi gereken bir problemdir. Bu çalışmada bir kurum bünyesinde yer alan 6000 kurum çalışanına ait bir yıllık internet aktivitesi incelenmiştir. Kurum çalışanlarının yeni kayıtlı internet sitelerine erişim oranları ve erişim nedenleri araştırılmıştır. Gerçekleştirilen çalışmada ayrıca, yeni kayıtlı internet siteleri ile ilgili bir test senaryosu oluşturulmuştur. Oluşturulan test senaryosunda, ilk 6 aylık sürede kullanıcıların yeni kayıtlı internet sitelerine erişimi açılmış, sonraki 6 aylık süre içinde ise engellenmiştir. Gerçekleştirilen test sonrasında kullanıcıların serbest erişim ve engelleme işlemlerine yönelik tepkileri analiz edilmiştir.

Anahtar Kelimeler: Yeni kayıtlı internet siteleri, kurumsal bilgi güvenliği, Proxy, zararlı yazılım.

ANALYSIS OF THE IMPACT OF NEWLY REGISTERED INTERNET SITES ON CORPORATE INFORMATION SECURITY

ABSTRACT

Websites that have not yet been categorized by proxy applications and that have not passed 14 days since its launch on the Internet are called newly registered web sites. To ensure corporate information security, what kind of policy should be applied to newly registered internet sites is a problem must be solved. In this study, one year internet activity belonging to 6000 institution employees in an institution was examined. Institution employees' access rates to new registered websites and reasons for access were investigated. In our study also, a test scenario related to newly registered internet sites has been established. In the test scenario that was created, users were allowed access to newly registered internet sites during the first 6 months, and they were blocked within the next 6 months.

Keywords: Newly registered web sites, enterprise information security, proxy, malware.

I. GİRİŞ (INTRODUCTION)

Günümüz teknoloji dünyasında kurumlar çalışanlarını zararlı yazılımlar ve oltalama saldırılardan korumayı amaçlamakta, bu ideallere ulaşmak için çeşitli internet sınırlandırmaları yapmaktadırlar. Yapılan internet sınırlandırmalarının en büyük sebebi kurumsal bilgi güvenliğini sağlamaktır. Bunun yanında kurum içi çalışma veriminin artırılması ve kurum imajına uygun şekilde duruş sergilenmesi amacıyla da sınırlandırmalar yapılabilmektedir.

Gelişen ve çoğalan internet kategorileri arasında yenice ortaya çıkan "Yeni Kayıtlı İnternet Siteleri" kategorisi; kurum güvenliğini yakından ilgilendirmektedir. Bunun yanı sıra kullanıcılar tarafından kurum internet politikalarının aşılması amacıyla da kullanılabilmektedir.

İnternet üzerinde yayına başlamasının üzerinden 14 gün geçmeyen ve bu süreçte proxy uygulaması tarafından herhangi bir kategorize işlemine tabi tutulmayan internet siteleri, yeni kayıtlı internet siteleri olarak tanımlanmaktadır. Bu tür internet

sitelerine erişim proxy uygulaması üzerinden engellenebilmekte ya da izin verilebilmektedir. Birçok firmada bu kategori varsayılanda izinli olarak gelmektedir.

Yeni kayıtlı internet sitelerinin engellenmediği durumlarda kullanıcılar proxy uygulaması tarafından henüz kategorize edilmemiş tüm yeni kayıtlı internet sitelerine erişebilme hakkına sahiptir. Bu durumda kullanıcı, içerisinde spam yaymak ya da oltalama saldırısı gerçekleştirmek amaçlı zararlı yazılımlar barındıran sitelere, yeni kayıt olduğu ve kategorize işlemine tabi tutulmadığı için erişebilmekte, kendisini ve içerisinde bulunduğu ağdaki tüm cihazları riske atabilmektedir [1].

Yeni kayıtlı internet siteleri kategorisinin bir diğer artısı ise kullanıcıların kurum internet politikalarını aşmasını çok daha zorlaştırmasıdır. Kullanıcılar kurum internetini kullandığı sürece mesai saatleri içinde veya dışında belirli internet politikalarına tabidir ve uymak zorundadır. Kimi zaman kullanıcılar bahis, yetişkin, dizi-film izleme siteleri gibi kurum ağından izin verilmeyen internet sitelerine erişmeyi denemektedir. Bu tür siteler arasında düzgün şekilde kategorize edilmiş olanlar hali hazırda proxy uygulaması tarafından engellenmektedir. Ama domain adı yeni alınan siteler proxy uygulaması tarafından kategorize edilene kadar erişime açık kalacaktır.

- dizimag.co
- dizimag.me
- dizimag.com
- dizimag.site
- dizimag1.co
- dizimag1.com
- dizimag2.co
- dizimag2.tr.gg
- dizimag4.com
- dizimagizle.com
- dizimagx.com
- dizimagyeni.com

Şekil 1. Kurum çalışanlarının erişmeye çalıştığı yeni kayıtlı site örnekleri

Şekil 1'de kurum kullanıcılarının 4 aylık bir periyotta erişmeye çalıştığı "dizimag" isimli bir dizi izleme sitesinin farklı domainlerden yaptığı yayınlar gösterilmiştir. Kullanıcılar asıl domain olan "dizimag.com"a erişmeye çalışmış ama bu internet sitesi "Streaming Media" kategorisinde olduğundan dolayı proxy uygulaması tarafından engellenmişlerdir. Yeni kayıtlı internet siteleri kategorisinin izinli olması durumunda kullanıcı erişmeye çalıştığı alan adını veya uzantısını değiştirip ilgili siteye erişim sağlayabilmekte, kurumun internet politikalarını atlatabilmektedir. İncelenen örneğin yanı sıra, içerisinde zararlı yazılım barındıran yeni kayıtlı internet sitelerinin alan adlarının rastgele oluşturulduğu ve anlamsız sözcükler içerdiği de görülmüştür [2].

Öte yandan kurum içerisinden yeni açılan internet sitelerine yönelik olarak yapılacak engelleme, kurum personelinin erişmesi gereken zararsız sitelere erişmesini de engelleyebilmektedir. Sonuç olarak, bu kategorinin erişime kapatılması halinde, türüne bakılmaksızın yeni kayıtlı tüm internet sitelerine yapılan istekler engellenecektir. Bu durumda kullanıcılar zararsız ve işleri gereği erişmeleri gereken internet sitesine erişemeyebilmekte, söz konusu kategori tabanlı engellemenin kurbanı olabilmektedir. Bu tür erişimi gerekli olan fakat ulaşılamayan internet siteleri üzerindeki engelin kaldırılması için bilgi teknoloji departmanına fazlaca talep gelebilmektedir. Belirli bir talep sayısının aşılması durumunda ise kullanıcılar kategoriye bakmadan farklı siteler için de erişim isteyebilmektedir. Bu durumda bilgi teknolojilerine gelen talep sayısı katlanarak artmaktadır. Talep sayısı arttıkça, söz konusu taleplerin çözülme süresi uzamakta, kullanıcının bilgi teknolojileri departmanına güveni azalmaktadır.

Bu çalışmada 6000 kurum çalışanının bir yıllık internet aktivitesi incelenmiş olup, kullanıcıların yeni kayıtlı siteler ile etkileşimleri analiz edilmiştir. Kullanıcıların bu tür sitelere erişim sıklıkları, nedenleri ve bu sitelerin engellenmesi durumuna oluşan tepkileri ölçülmeye çalışılmıştır.

Gerçekleştirilen bu çalışma kapsamında kurum kullanıcılarının yeni kayıtlı internet sitelerine erişim istekleri ilk 6 ay boyunca açık bırakılmış, sonraki 6 aylık sürede ise engellenmiştir. Yapılan araştırmalar sonrasında yeni kayıtlı internet siteleri üzerinden toplamda 84419 adet vaka elde edilmiştir. Edinilen bu veri pek çok yönüyle incelenip, kurumların yeni kayıtlı internet sitelerine yönelik olarak ne tür politikalar izlemeleri gerektiği araştırılmıştır.

Literatürde yer alan çalışmalar incelendiğinde kurumsal bilgi güvenliğini sağlama üzerine çeşitli çalışmaların gerçekleştirildiği görülmektedir. Özenç tarafından gerçekleştirilen çalışmada; bilgi ve iletişim teknolojilerindeki bilgi güvenliğinin ekonomik boyutu, bilgi güvenliği konusuna Avrupa Birliğinin hukuki yaklaşımı, Avrupa Birliğinde güvenlik kültürüne ilişkin politikaların geliştirilmesi gibi konular incelenmiştir [3]. Şahinaslan ve arkadaşları tarafından gerçekleştirilen çalışmada ise; kurumlarda bilgi güvenliği farkındalığının önemine değinilmiş, kurum personellerinin bilgi güvenliği farkındalığını arttırmak amacıyla çeşitli yöntemler önerilmiştir [4]. Vural ve Sağıroğlu tarafından gerçekleştirilen çalışmada ise, kurumsal bilgi güvenliğini sağlamada mevcut bilgi güvenliği standartları ve yeni oluşturulmakta olan bilgi güvenliği standartları detaylı olarak incelenmiştir. Çalışmada ayrıca kurumsal bilgi güvenliğine yönelik güncel tehditlere ve bulgulara da yer verilmiştir [5]. Literatürde yer alan çalışmalar incelendiğinde kurumsal bilgi güvenliği üzerinde yeni kayıtlı internet sitelerinin etkisinin incelendiği bir çalışma bulunmamaktadır. Bu yönüyle bu çalışma, kurumsal bilgi güvenliği açısından özgün bir değer taşımaktadır.

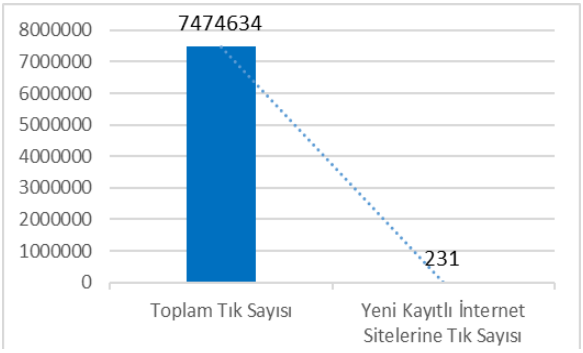
Gerçekleştirilen bu çalışmanın II. bölümünde kurum personelinin yeni kayıtlı internet siteleri ile karşılaşma durumları incelenmiştir. III. bölümde kurum personelinin yeni kayıtlı internet sitelerine erişme

amaçları incelenmiş, IV. bölümde ise çalışma kapsamında incelenen veri üzerinde yapılan testler ve elde edilen sonuçlar paylaşılmıştır. V. bölümde ise gerçekleştirilen çalışma, sonuçların sunulması ile tamamlanmıştır.

II. KURUM PERSONELİNİN YENİ KAYITLI İNTERNET SİTELERİ İLE KARŞILAŞMA DURUMLARI (COMPETITIVE RESPONSES TO THE NEW RESERVED INTERNET SITES OF THE INSTITUTION PERSONNEL)

Bu bölümde kullanıcıların, yeni kayıtlı internet siteleri ve tüm internet sitelerine yaptıkları erişim sayıları ve detayları incelenmiştir. Elde edilen bulgular kullanılarak, kullanıcıların yeni kayıtlı internet siteleri ile hangi durumlarda karşılaştıkları yorumlanmıştır.

Şekil 2'de şirket personelinin bir aylık süre içinde erişim isteğinde bulunduğu toplam internet sitesi sayısı ve yeni kayıtlı internet sitesi sayısı gösterilmektedir.

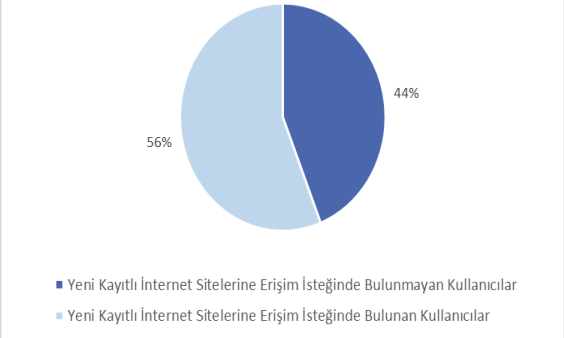


Şekil 2. Kurum personelinin bir ay sürecinde erişim isteğinde bulunduğu toplam internet sitesi sayısı ve yeni kayıtlı internet sitesi sayısı

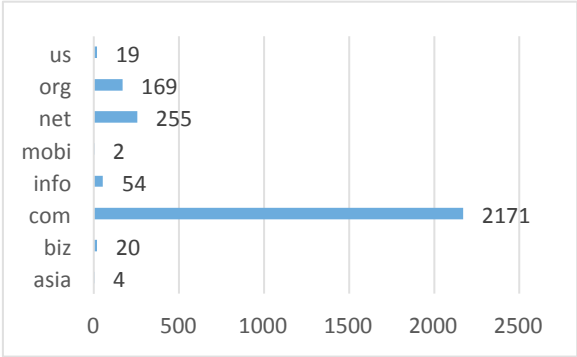
Gösterilen verilere göre kurum personeli ortalama bir günde neredeyse 7.5 milyon internet sitesine erişim isteği yapmaktadır. Yeni kayıtlı internet sitelerine yapılan 231 erişim isteği ise tüm erişim isteklerine oranla çok az bir değere karşılık gelmektedir. Bu iki erişim isteği sayısını birbirine oranladığımızda yeni kayıtlı internet sitelerine yönelik erişim isteğinin tüm erişim isteklerine oranı %0.003 olarak karşımıza çıkmaktadır.

Şekil 3' te, bir yıllık süre içinde, en az bir defa yeni kayıtlı internet sitelerine erişim isteğinde bulunan ve yeni kayıtlı internet sitelerine hiç erişim isteğinde bulunmayan kullanıcıların oranı gösterilmiştir. Bu süreçte 6000 kullanıcının %56' sı yeni kayıtlı internet sitelerine en az bir defa erişmeye çalışmıştır. Buna göre; uzun vadede kullanıcılar isteyerek ya da istemeyerek bir şekilde yeni kayıtlı internet siteleri ile karşılaşmaktadır.

Şekil 4'te ise, kullanıcıların erişim isteğinde bulunduğu internet sitelerinin uzantılarının oranına yer verilmiştir. Buna göre; kullanıcılar büyük oranda "com" uzantısına ait yeni kayıtlı internet sitelerine erişmeye çalışmış, bunu "net" ve "org" uzantıları takip etmiştir. Devlet sitelerinin "gov" uzantısını, eğitim sitelerinin ise "edu" uzantısını kullanmasından dolayı bu internet siteleri direkt olarak kendi kategori bilgisini almaktadır. Kategori bilgisi girilen siteler yeni kayıtlı internet sitelerine dâhil edilmediği için kullanıcılar herhangi bir devlet veya eğitim sitesinden engellenme yaşamamıştır.



Şekil 3. Bir yıl içinde en az bir defa yeni kayıtlı internet sitelerine erişim isteğinde bulunan ve hiç erişim isteğinde bulunmayan kullanıcıların oranı

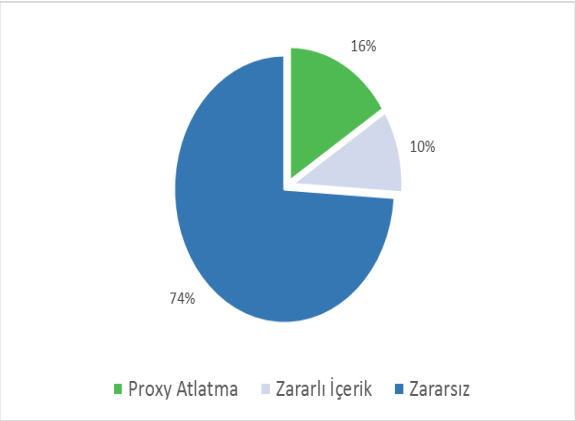


Şekil 4. Kurum personelinin erişim isteğinde bulunduğu internet sitelerinin uzantılarının oranı

III. KURUM PERSONELİNİN YENİ KAYITLI İNTERNET SİTELERİNİ ZİYARET ETME AMAÇLARI (THE GOVERNMENT PERSONNEL'S GOALS TO VISIT THE NEW REGISTERED INTERNET SITES)

Kullanıcılar işleri gereği bir internet sitesini ziyaret etmek isteyebilir, mailde kendilerine gönderilen bir linke tıklayabilir ya da engellendikleri siteye alternatif olarak başka bir site arayabilmektedirler. Tüm bu durumlar kullanıcıları yeni kayıtlı internet sitelerine yönlendiren etmenlerdir.

Gerçekleştirilen çalışma kapsamında kullanıcıların yeni kayıtlı internet sitelerine yapmış olduğu erişim isteklerinin kategori üzerinden analizi Şekil 5' de gösterilmiştir.



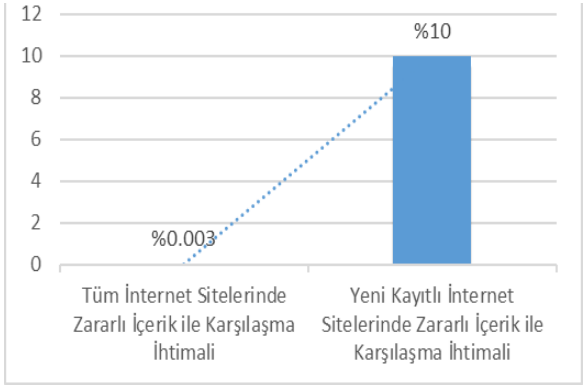
Şekil 5. Kurum personelinin yeni kayıtlı internet sitelerine isteklerin kategorilere göre oranı

Şekil 5' te görüldüğü üzere kullanıcıların erişmeye çalıştığı yeni kayıtlı internet sitelerinin %74'ü zararsız içeriğe sahiptir. Öte yandan erişilmeye çalışılan yeni kayıtlı internet sitelerinin %10'u, içerisinde zararlı yazılım barındırmaktadır. Erişilmeye çalışılan yeni kayıtlı internet sitelerinin %16'sı ise bahis, kaçak yayın ya da yetişkin içeriğine sahiptir ve internet politikası yasaklarını atlatmak için kullanılmaktadır.

Şekil 6. Kurum personelinin yeni kayıtlı internet sitelerine gerçekleştirdiği erişim istek sayıları

Şekil 6 incelenecek olursa; kullanıcılar bir yılda 84419 kez yeni kayıtlı internet sitelerine erişim isteğinde bulunmuşlardır. Yapılan erişim isteklerinin %10'u içerisinde zararlı yazılım barındıran bir yeni kayıtlı internet sitelerine yapılmıştır. Bu oran; 8442 erişim isteğine karşılık gelmektedir. Bu verinin 1 yıllık bir süreçte elde edildiği düşünülürse ortalama bir günde 23 defa içerisinde zararlı yazılım barındıran internet sitesine erişim isteğinde bulunulmuştur.

Şekil 7'de, kullanıcıların tüm internet sitelerinde zararlı yazılım ile karşılama oranı ve yeni kayıtlı internet sitelerinde zararlı yazılım ile karşılaşma oranı gösterilmiştir. Şekle göre kullanıcıların ziyaret ettiği tüm internet siteleri içerisinden yalnızca %0.003' lük kısmı zararlı yazılım barındırmaktadır. Yeni kayıtlı internet sitelerinde ise bu oran %10'a çıkmakta, neredeyse 3000 kat artmaktadır.



Şekil 7. Kurum personelinin erişim sağladığı tüm internet sitelerindeki zararlı yazılım oranı ile yeni kayıtlı internet sitelerindeki zararlı yazılım oranı

Şekil 8. Kurum personelinin kurum internet politikalarını atlatma istekleri

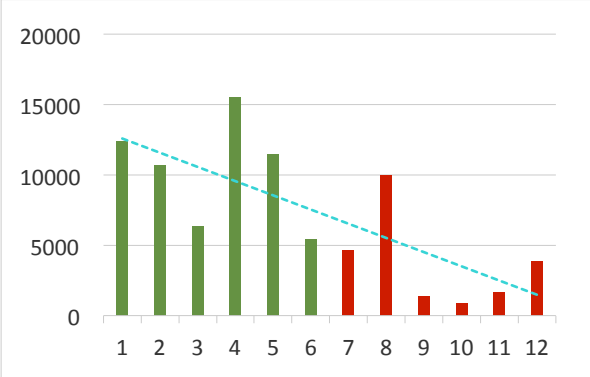
Şekil 8'de gösterildiği üzere bir yılda yeni kayıtlı internet sitelerine yapılan 84419 erişim isteğinin %16'sı kurum internet politikalarını atlatmaya yöneliktir. Bu oran bir yıl içinde bu alanda 13507 erişim isteği yapıldığı anlamına gelmektedir. Bu da ortalama bir günde 37 defa kurum internet yasaklarını atlatmaya yönelik erişim isteği yapılmaktadır.

Şekil 9. Kurum personelinin yeni kayıtlı zararsız internet sitelerine yönelik erişim isteği

Şekil 9'da gösterildiği üzere bir yılda yapılan 84419 yeni kayıtlı internet sitesi erişim isteğinin %74'ü erişime açık olması gereken zararsız sitelere yapmıştır ve bu oran 62470 erişim isteğine karşılık gelmektedir. Eldeki verinin bir yılda elde edildiği düşünülürse, yeni kayıtlı internet siteleri kategorisinden bir günde ortalama 171 erişimi isteğine izin verilmesi gerekilirken, söz konusu istekler engellenmektedir.

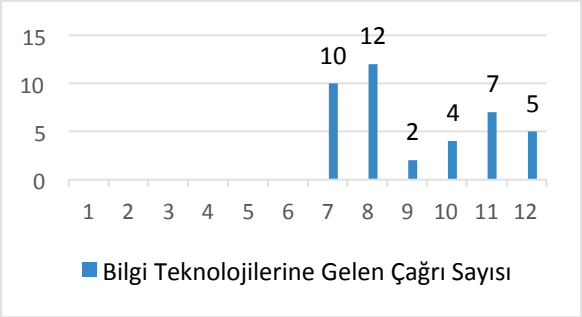
IV. YENİ KAYITLI İNTERNET SİTELERİ ÜZERİNDE DÖNEMSEL ERİŞİM TESTLERİNİN GERÇEKLEŞTİRİLMESİ (REALIZATION OF PERIODIC ACCESS TESTS ON NEW REGISTERED INTERNET SITES)

Gerçekleştirilen çalışma kapsamında yapılan test işleminde kurum ağından yeni kayıtlı internet sitelerine erişim için 2 farklı senaryo oluşturulmuş ve her iki durum sonunda elde edilen veriler analiz edilmiştir. Oluşturulan senaryoya göre 6 aylığına kurum ağından, yeni kayıtlı internet sitelerine erişim durumu açık bırakılmıştır. İkinci senaryoda ise, sonraki 6 aylık sürede kurum ağından yeni kayıtlı internet sitelerine erişim engellenmiştir. Toplam bir yıllık süreçte kullanıcıların bu internet kategorisine adaptasyonları ve tepkileri ölçülmeye çalışılmıştır.



Şekil 10. Kurum personelinin yeni kayıtlı internet siteleriyle olan etkileşimlerinin ay bazında gösterimi

Şekil 10'da kullanıcıların bir yıllık yeni kayıtlı internet siteleriyle olan etkileşimleri gösterilmiştir. Buna göre ilgili kategorinin kullanıcıların erişimine açık olduğu aylarda yüksek sayıda etkileşim aldığı ve kullanıcılar tarafından yüksek oranda kullanıldığı görülmüştür. İlgili kategorinin erişime kapatıldığı sonraki aylarda ise etkileşim istekleri büyük oranda azaldığı görülmektedir.



Şekil 11. Kurum personelinin erişimin engellendiği yeni kayıtlı internet sitelerinin erişimlerine açılması için oluşturdukları çağrı talepleri

İkinci 6 aylık sürede yapılan engelleme ile kullanıcıların yeni kayıtlı internet sitelerine erişimlerinin kapatılmasıyla, günde ortalama 125 adet kullanıcının erişim isteği engellenmiştir. Bu denli çok engelleme yapılmasına karşın kullanıcılar tarafından erişim isteği amacıyla açılan çağrı sayısı beklenenin çok altında kalmıştır. Kullanıcıların engellendikleri yeni kayıtlı internet sitelerinin erişimlerine açılması için oluşturdukları çağrı talepleri Şekil 10' da gösterilmiştir.

V. SONUÇ VE DEĞERLENDİRME (CONCLUSION AND EVALUATION)

Elde edilen veriler ışığında yeni kayıtlı internet siteleri kategorisinin erişime kapatılması ve erişime açık tutulması durumuna incelenmiştir.

Yeni kayıtlı internet sitelerine erişimin açık bırakılması durumlarında;

- Bir günde ortalama bir kullanıcı, içerisinde zararlı içerik bulunan yeni kayıtlı internet sitesine erişecektir. Kullanıcının eriştiği zararlı içeriğe göre olay sonrası müdahale ekibinin hızlı reaksiyon vermesi gerekecektir.
- Bir günde yeni kayıtlı internet sitelerine yönelik ortalama 37 erişim isteği kurum internet politikalarını atlatmak için yapılacaktır. Normalde erişilmemesi gereken bu sitelerin görüntülenmesi kurum kimliğine yakışmayacak durumlar ortaya çıkarabilmektedir.
- Kullanıcılar normalde erişmesi gereken yeni kayıtlı internet sitelerine erişimde sorun yaşamayacaktır. Bu durum kullanıcıların sürekli kısıtlı bir internet politikasında olduğu izlenimini azaltacaktır.

Yeni kayıtlı internet sitelerine erişimin engellenmesi durumlarında;

- Bir günde ortalama 177 erişim isteğine izin verilmesi gerektiği halde, yeni kayıtlı internet sitelerine yönelik olduğu için engellenecektir. Gereksiz yere engellenen kullanıcıların iş aktiviteleri aksayacak, bilgi teknolojilerine bu konuyla ilgili talep açacaklardır. Bilgi teknolojileri departmanı, gelen yeni kayıtlı internet sitesi erişimlerini incelemek için ekstra bir efor sarf etmek zorunda kalacaktır.
- Kullanıcıların kurum internet politikalarını atlatması ciddi derecede zorlaşacaktır.
- %10'luk zararlı içeriğine sahip yeni kayıtlı internet sitelerinden hiçbir kullanıcı enfekte olmayacak, bu kategoriden dolayı olay sonrası müdahaleye gerek kalmayacaktır.

Devlet, eğitim gibi kendine ait site uzantısı olan internet sitelerinin doğrudan kategorize edilmesi ve

yeni kayıtlı internet sitelerine dâhil olmaması bu kategoriye erişimi kapatmak isteyen kurumlar için büyük artı sağlamaktadır. Sonuç olarak kategori erişime kapatılsa da kullanıcılar devlet ve eğitim sitelerine problemsiz erişmeye devam edecektir.

Kullanıcılar tarafından yapılan erişim isteklerinin yalnızca %0.003'ünün yeni kayıtlı internet sitelerine yönelik olmasına rağmen bir yıllık süreçte kullanıcıların %56'sı yeni kayıtlı internet siteleri ile etkileşime girmiştir. Kullanıcılar tarafından yapılan erişim istekleri incelendiğinde;

- %74'ünün zararsız sitelere erişmek istediği,
- %10' unun içeriğinde zararlı olduklarını bilmedikleri sitelere erişmek istediği,
- %16' sının ise kurum internet yasaklarını atlatmak için erişmek istediği tespit edilmiştir.

Buna göre kullanıcılar sadece %16'lık bir oranda bu kategoriyi zafiyet olarak kullanmak istemiştir. Geri kalan tüm istekler masum internet siteleri ya da içeriğinde zararlı olduğu bilinmeyen internet sitelerinden oluşmaktadır.

Yapılan tüm bu testlerin sonucunda kullanıcıların yeni kayıtlı internet sitelerine erişimini açık bırakmanın ne denli tehlikeli boyutlara ulaşabileceği, kapatmanın ise kısıtlama ve sonrasında mağduriyet oluşturabileceği gösterilmiştir. Kurumlar bu noktada yeni kayıtlı internet siteleri kategorisinin artılarını ve eksilerini kendi kurumsal politikalarına göre değerlendirmeli ve gerekli düzenlemeleri gerçekleştirmelidir.

KAYNAKLAR

[1] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster, "Building a Dynamic Reputation System for DNS". In USENIX Security Symposium, Washington, USA, pp. 273-290, August 2010.

[2] Y. He, Z. Zhong, S. Krasser, and Y. Tang, "Mining DNS For Malicious Domain Registrations". In 6th Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Chicago, USA, pp. 1-6, October 2010.

[3] K. Özenç, "Bilgi Ve İletişim Teknolojilerinde Kişisel Ve Kurumsal Bilgi Güvenliğinin Sağlanması." Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTurkey), Ankara, Türkiye, Ss. 183-190, 13-14 Aralık 2007.

[4] E. Şahinaslan, A. Kantürk, Ö. Şahinaslan, ve E. Borandağ, "Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi Ve Oluşturma Yöntemleri". XI. Akademik Bilişim Konferansı, Şanlıurfa, Türkiye, Ss. 605- 610, Şubat 2009.

[5] Y. Vural, Ş. Sağıroğlu, "Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt 23, Sayı 2, Ss. 507-522, 2008.