Zararlı Yazılım Tespit, Takip ve Analiz Yöntemleri Geliştirilmesi

Mustafa ALKAN, Burak ÇİFTER ve Elif Tuğba KILIÇ

***Özet*—Gelişen teknolojiyle birlikte siber saldırıların artması, hem kamu kurumlarının hem de özel kuruluşların daha güvenli sistemler kullanmasını zorunlu hale getirmektedir. Bu çalışmada sistemleri tehdit eden zararlı yazılımların tespit edilmesi, takip edilmesi ve müdahale edilmesi yöntemi geliştirilmeye çalışılmıştır. WEB sitelerinin takibini anlık yapan ve tamamen merkezi bulut tabanlı (Software as a Service-SaaS) olarak çalışan ve WEB tabanlı olarak platform bağımsız kullanılıp yönetilebilen bir yazılım sistemi geliştirilmeye çalışılmıştır. WEB sitelerini, sistemlerin DNS altyapılarını, SSL sertifikalarını, ağ erişim adımlarını, hem içeriğini hem de yapısal durumunu sürekli takip ederek "hack" edilip edilmediğini, güvenlik zafiyeti barındırıp barındırmadığını, özellikle zararlı yazılım yayıp yapmadığını analiz edecek olan bu uygulama ile zararlı yazılımlar tespit edilerek anlık (real time) bilgi ve alarm sağlayacaktır. Bu uygulama ile sisteme kullanıcı tarafından girilen WEB sitelerini, yine kullanıcının belirlediği aralıklarla kontrolü gerçekleştirip güvenlik problemlerini tespit ederek ve bununla ilgili yetkili yöneticileri uyararak acilen müdahale edilmesine destek vermektedir.**

Anahtar Kelimeler— Bilgi güvenliği, siber güvenlik, tehdit analizi, zararlı yazılım

***Abstract*—The increase of cyber attacks along with the developing technology makes it imperative to utilize more secure systems for both public and private organizations. In this study, the method of detection, monitoring, and intervention of the malicious software that threatens the systems has been tried to be developed. A software system implementing instantly the follow-up of WEB sites, running completely as centralized cloud-based (Software as a Service-SaaS), and able to use and manage the platform based on WEB has been tried to be developed. With this application that will analyze WEB sites, DNS infrastructure of the systems, SSL certificates, network access steps, whether it is hacked by continuously monitoring both its content and structural condition, whether it includes security weakness, and especially whether it spreads malicious software, real time information and alarm will be provided by detecting the malicious software. Moreover, with this application, by performing the control of the WEB sites entered by the user within the user-defined intervals, it identifies the security problems and gives support to intervene urgently by alerting the authorized managers.**

Index Terms— Information security, cyber security, threat analysis, malicious software

I. GİRİŞ

Türkiye'de de, dünyada olduğu gibi siber saldırılar ve siber güvenlik hassasiyeti son yıllarda artmıştır. Bunun sebebi ise artan iletişim kaynakları ve gelişen internet servisleri sayesinde hedef olmaya müsait sistemlerin atmasıdır.

Saldırıların dünya ve Türkiye gündemlerine hemen hemen eş zamanda girmeleri ise artık saldırıların ülke ve sınır tanımaması ve dünya gündeminde olan herhangi bir organize saldırının aynı anda Türkiye'yi de etkilemesinden kaynaklanmaktadır. Yani siber güvenlik gündemimiz sadece bizim tarafımızdan oluşturulmamakta, dünyadaki gelişmelerle aynı doğrultuda ilerlemektedir.

Bu durum çerçevesinde hem kamunun hem de özel kuruluşların bilgi güvenliği çalışmaları yapmaları kaçınılmazdır. Bilgi güvenliği tesis ve sistemlerinin hemen hepsi yurtdışı menşeilidir. Türkiye'de siber güvenlik alanında her alana uyarlanabilecek bir ürünün geliştirilmesi, ülke ekonomisi açısından yurtdışına yönelebilecek kaynağın yurtiçinde kalmasını sağlayacaktır.

Bununla birlikte, güvenlik yatırımlarının temel gerekçesi, tehdit durumunun ölçümlenmesidir. Türkiye'de hali hazırda güvenlik ihlal durumlarının kayıtlarının tutulduğu ve yıllık olarak yayınlanabilecek bir veri havuzu bulunmamaktadır. Bu uygulama sayesinde tüm kamu kurumlarının WEB altyapıları takip edilerek otomatik olarak hack edilen sistemler kayıt altına alınacak böylelikle resmi olarak her yıl yaşanan güvenlik ihlalleri ile ilgili rapor üretilebilecektir.

Söz konusu uygulama aynı zamanda kullanan kurumlara da ekonomik fayda sağlayacaktır. Özellikle veri çalınması veya web sitesinin hack edilmesi neticesinde yaşadıkları itibar kaybı, kurumlara doğrudan ve dolaylı ekonomik kayıp olarak dönmektedir. Bu sayede kurumların hem zafiyetleri proaktif olarak saldırganlardan önce tespit edilerek hem de saldırı durumunda yetkililere derhal haber verip müdahale etmeleri sağlanarak veri sızıntısı ve prestij kaybının önlenmesi sağlanacaktır. Aynı zamanda sosyal olarak uygulamayı kullanan özellikle merkezi takip yapan kurumların diğer kurumlardaki bilgi güvenliği ekipleri ile koordineli

Mustafa ALKAN Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği Bölümünde Bölüm Başkanı olarak görev yapmaktadır (Telefon: 0534 438 383 8, e-mail: malkan@gazi.edu.tr).

Burak ÇİFTER , BOA Bilgi Teknolojileri ve Güvenliği şirketinde güvenlik alaninda projelerde fiilen görev yapmaya devam etmektedir (Telefon: 0532 790 13 94, e-mail: burak@burakcifter.com).

Elif Tuğba KILIÇ Gazi Üniversitesi Fen Bilimleri Enstitüsü Kazaların Çevresel ve Teknik Araştırılması Bölümünde Yüksek Lisans eğitimine devam etmektedir (Telefon: 0537 931 90 66, e-mail: elif_tugba_kilic@hotmail.com).

çalışmasını sağlayacak bu sayede hem sosyal hem de organizasyonel anlamda fayda sağlayacaktır.

Ayrıca kullanıcıların da takip edilen sitelerde (özellikle e-devlet uygulamalarında) kendini daha güvende hissetmesini sağlayacak ve internet üzerinden hizmet kullanımına güvenlik kaygısı sebebiyle yanaşmayan insanların da bu mecraya taşınmasına yardımcı olacaktır.

II. SİBER GÜVENLİK

Siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür[1].

Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır[2].

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefleri erişilebilirlik, bütünlük (aslına uygunluk ve inkâr edilemezliği de kapsar) ve gizliliktir. Siber güvenliğin temel hedefleri, 10. Ulaştırma şurasında; erişilebilirlik, bütünlük ve gizlilik olarak ifade edilmiştir [3].

Bilgi güvenliği, bilginin ve bilgi teknolojileri altyapısının bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlemektir. Buna uygun tanımı: elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için duruma uygun güvenlik politikasının belirlenmesi ve uygulanması gereklidir.

A. Siber Güvenlik Politikaları

- Faaliyetlerin sorgulanması,
- Erişimlerin izlenmesi,
- Değişikliklerin kayıtlarının tutulup değerlendirilmesi,

Silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir.

Bilgisayar teknolojilerinde yer alan bilgisayar güvenliğinin amacı ise; kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır[4].

Güvenlik açıkları, gelişen teknolojiyle birlikte tüm firmalar tarafından çok ciddi para, zaman, kritik bilgi ve itibar gibi maddi ve manevi kayıplara sebep olmaktadır. Firmalar bilgi ve sistem güvenliği için astronomik rakamlar ödemekle beraber, buna rağmen hala ciddi kayıplar yaşamaktadır.

Bu çalışmada kullanılan yöntem ile WEB sitelerinin ve hizmet vermesi için kullandığı DNS sistemleri gibi bileşenlerin takibinin anlık yapılması sağlanarak, sistemlerin hack edilip edilmediğini, zararlı yazılım (malware) yayılıp yayılmadığını, güvenlik açıklarının olup olmadığı, sisteme DDOS (Distributed denial of service attack) saldırılarının olup olmadığının, SSL sertifikalarının doğruluğu ve güvenilirliğinin kontrol edilerek anlık (real time) bilgi sağlayacak siber saldırı takip ve uyarı sistemi geliştirililmiştir.

III. SİBER SALDIRILAR

Güvenlik açıkları, gelişen teknolojiyle birlikte tüm kamu kurumları ve özel şirketler tarafından çok ciddi para, zaman, kritik bilgi ve itibar gibi maddi ve manevi kayıplara sebep olmaktadır. Firmalar bilgi ve sistem güvenliği için astronomik rakamlar ödemekle beraber, buna rağmen hala ciddi kayıplar yaşamaktadır. Bunlara örnek olarak ünlü aktivist hacker gruplarından Anonymous, LuLzSec, Syrian Electronic Army, RedHack'in, devlet kurumları başta olmak üzere, birçok ülke, kurum ve firmalara karşı yaptığı saldırıları gösterebiliriz. Dünyaca ünlü elektronik devi SONY, uğradığı saldırı sonucu 600.000 USD zarar ettiğini ve bunun yanında müşterilerinin kredi kartı bilgilerinin çalındığını açıklamıştır. Saldırı sonrasında hacker grubu ise: "Çok basit bir yöntemle SONY 'nin tüm bilgilerine ulaştık. Bu kadar kolay ulaşılabilen bir şirkete neden güveniyorsunuz?" şeklinde bir açıklamada bulunmuştur[5].

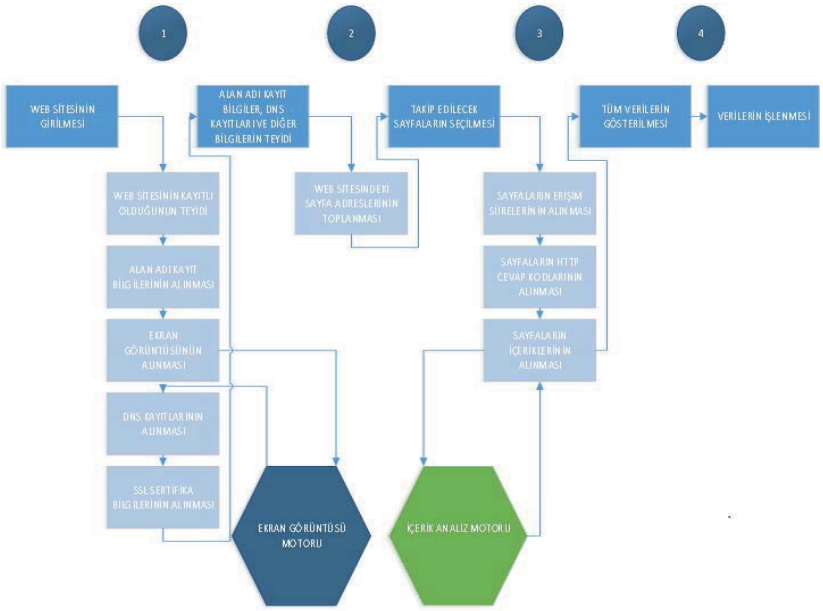
Ülkemizdeki WEB sistemlerinin birçoğunda tehdit durumunu takip edecek bir sistem olmamakla birlikte kritik altyapıların güncel takip edilememesinden kaynaklı siber saldırıların takibi yapılamamaktadır. Birçok kamu kurum ve kuruluşların "gov.tr" uzantılı siteleri son yıllarda hack olayları ile sıkça gündemde yer edinmiştir bunun en önemli sebebi sistemlerin siber saldırılara karşı zayıf olmasının yanı sıra anlık tehdit takibinin yapılmamasından kaynaklanmaktadır.

Bunun yanı sıra, ülkemizde en azından devlet sitelerini takip ederek karşılaştıkları hack saldırılarına ait kayıtları tutan bir sistem bulunmamakta, bu sebeple şu anda dahi kaç saldırı gerçekleştiği veya kaç kamu sitesinin hack edildiği, nasıl ve hangi yollarla saldırıların gerçekleştirildiği bilinememektedir.

Gelişen teknolojiyle birlikte siber saldırıların artması, kurumların ve şahısların daha güvenli sistemler kullanmasını zorunlu hale getirmektedir. e-devlet uygulamaları devlet politikası olarak desteklenmektedir ve devlet web sitelerinin güvenliği, güvenliğinin takibi, halkın bu sistemleri kullanmaya teşvik edilmesi için de oldukça önemlidir.

Bu gerekçeyle yola çıkılarak yapılan bu çalışma sayesinde;

- Öncelikle kritik altyapıya sahip kurumların siber güvenlik tehditlerine karşı uyarı/alarm alabilmeleri sağlanacak,
- Kritik altyapılara yapılacak olası siber saldırıların tespitinin yapılarak takip edilmesi,
- Web sayfaları üzerinden yayılan zararlı yazılım (Malware) ve gelişmiş kalıcı tehditler (APT – Advanced Persistent Threat) tespit edilecek ve yayılmasına izin verilmeden önlem alınması,
- Dijital sosyal medya ortamlarında ve saldırganların



Şekil. 1. Takip edilecek sistem girişi süreç akışı

kullandıkları paylaşım platformlarında kurumlarla ilgili bir ifşa veya ön hazırlık durumunun hemen tespit edilmesi

- Tespiti yapılan siber saldırılarla ilgili olarak yetkili birimlere alarm vermek ve gerekli ilk önlemlerin alınması sağlanabilecektir.

Bu çalışma ile Yazılım sisteminin software as a service (servis olarak yazılım hizmeti) amaçlı sistem tasarımı gerçekleştirilerek, sistemin kullanıma hazır hale getirilmesi ile internet servis sağlayıcılarının gereksinimleri karşılanabilecektir. Ayrıca devlet kurumlarının siber saldırılara karşı korunması hızlı, güvenilir ve doğru şekilde gerçekleştirilmiş olacaktır.

IV. WEB SİTESİNİN GİRİLMESİ VE İLK VERİLERİN TOPLANMASI

- WEB sitesi yöneticisi WEB alan adını websitesi.com sisteme kayıt eder.
- Alan adının kayıtlı olduğunun teyidi yapılır
- Alan adına ait kayıt bilgileri (WHOIS) sorgulanıp ilgili alanlar normalize/standardize edilir.
- WEB sitesinin son kullanıcı tarafından görüntülendiği şekilde ekran görüntüsü alınması için ekran görüntüsü alma motoru çalıştırılır.
- Alan adına ait DNS kayıtları (A, CNAME, PTR, MX, PTR, vb) alınır.
- WEB sitesinin eğer SSL sertifikası varsa bu sertifikaya ve sertifika sağlayıcısına ait bilgiler alınır.
- Bilgiler yönetici tarafından doğrulanmak üzere gösteriliyor ve doğruluğunun onaylanması istenir.

A. Sayfa Adresleri (URL) Ayıklama ve Adres Seçimi

WEB sitesi üzerindeki sayfaların adresleri (URL) link ayıklama motoru tarafından alınır; elde edilen URL'ler üzerinde takip edilmesi istenen URL'ler için ekleme ve çıkartma yapılmak üzere yöneticiye gösteriliyor ve onayı talep edilir.

B. İçerik ve Eğitim Verilerinin Oluşturulması

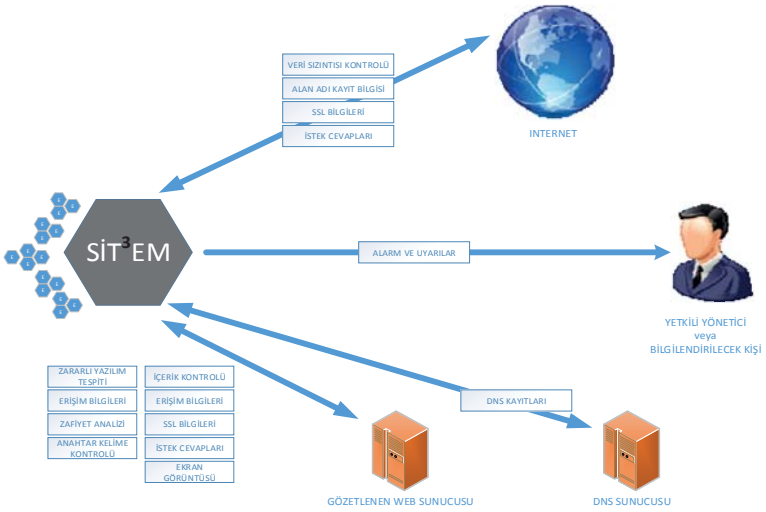
- Onay verilen sayfa adresleri (URL), sayfa motoruna iletilir
- URL'lere erişim süreleri alınır
- URL'lerin cevaben döndüğü HTTP hata kodları alınır (HTTP 10x, 20x, 30x, 40x, 50x gibi)
- URL'lerin içerikleri alınır ve içerik analiz motoruna gönderilir. İçerik analiz motoru sayfa içerikleri ile ilgili veri madenciliği (data mining), veri analizi (data analysis) ve metin madenciliği (text mining) yaparak içerik ile ilgili standart değerleri oluşturulur.

C. Onay ve Kayıt

Tüm veriler yönetici tarafından doğrulanmak üzere gösterilir. Onay verildiğinde veriler sisteme işleniyor ve sistem yeni eklenen siteyi analiz etmeye başlar.

Uygulama düzenli olarak verilen aralıklarla takip edilmesi istenen siteye normal bir ziyaretçi olarak girmektedir. Her girişinde ve siteyi normal bir ziyaretçi gibi gezmesi esnasında elde ettiği verileri analiz edip yorumlar ve daha önceki verileri ile karşılaştırır. Bu veriler ile ilişkili çeşitli diğer verileri ise internet üzerindeki veri kaynaklarından (DNS sunucuları, WHOIS kayıt sorgulama sunucuları gibi) kontrol eder.

İzlenen sitenin erişim bilgileri, sayfaların erişim süreleri ve erişilebilirlikleri, sayfaların içeriğindeki kritik HTML kodları



Şekil. 2. Genel çalışma düzeni

istenmeyen anahtar kelimeler ve sistemin hack edildiğine işaret eden imzalar, alan adı ile ilgili DNS sunucusundaki kayıt değişiklikleri ve alan adı kayıt (WHOIS) bilgilerinin değişiklikleri, SSL sertifikası verileri uygulama tarafından incelenir. Sayfalarda ve sitedeki dosyalarda zararlı yazılım taraması yapılır. Uygulama aynı zamanda WEB sitesinin ekran görüntüsünü alır ve ekran görüntüsü üzerinde resim işleme yaparak sitenin görsel değişiklik oranını hesaplar, eşik değerlerin üzerinde olup olmadığını kontrol eder. Bu uygulama sayesinde web sitesi üzerinde normalin üzerinde bir değişiklik varsa ve bunu anahtar kelimeleri kontrol ederek yakalayamasa dâhi, görsel değişiklik analizi tabanlı anormallik kontrolü ile sitenin hack edilip edilmediğini tespit ederek uyarı verir.

Sayfayla ilgili elde ettiği içeriği analiz ederek, içerikten XHTML iskeletini ve okunabilir içeriği (Human Readable) ayıklar, ayıkladığı XHTML içerisinde yapısal değişiklik olup olmadığını kontrol eder. Ayrıca XHTML içerisinde tehlikeli kabul edilen XHTML etiketlerini takip eder ve sitede tehlikeli kabul edilen XHTML etiketleri eklenmiş ise bunları bildirir.

Bu çalışmada WEB sayfasını ve WEB sitesi içerisindeki dosyaları zararlı yazılım analizi motorundan geçirir, böylelikle WEB sayfaları üzerinden yayılan zararlı yazılımlar ile APT ataklarının gerçekleştirilmesini engeller.

WEB sayfasının kullanıcıya gönderdiği SSL sertifikasını kontrol eden uygulama, bu sertifikanın doğruluğunu ve tutarlılığını kontrol ederek, sertifikanın gerçekten doğru sistem tarafından mı üretildiğini yoksa SSL araya-girme saldırısı mı gerçekleştirilmeye çalışıldığını tespit eder ve uyarı verir.

Bu çalışma çoklu dil desteği ve rol tabanlı kullanıcı erişimi (RBAC – Role Based Access Control) ile tasarlanmıştır. Kullanıcılar yönetici seviyesinde (Administrator) veya sadece takip edecek operatör seviyesinde (View Only Operator) yetkilendirilebilmektedir[6].

Uygulama sistem üzerinde aktif olarak gerçekleştirdiği bu analizlerin yanı sıra, takip ettiği web sitelerinden saldırganlar tarafından yaygın olarak kullanılan platformlarda bahsedilip bahsedilmediğini kontrol eder. Bu sayede, organize bir saldırı için birbiriyle iletişim kurmaya çalışan saldırganların iletişimleri yakalanarak, siber saldırıyla ilgili erken uyarı ve tehdit istihbaratı gerçekleştirilir. Aynı zamanda internet üzerinde WEB sitesi ile ilgili veri sızıntısı/ifşası bulunuyorsa bununla ilgili yöneticiye alarm verir.

Şekil. 3. Birbirini tamamlayan motorlar

Çalışma kapsamında geliştirilen, sisteminin içeriği Web sitelerinin takibini anlık yapan ve tamamen WEB tabanlı (SaaS) olarak çalışan bir yazılımdır. WEB sitelerini sürekli takip ederek hack edilip edilmediğini, güvenlik açıklarını tespit eder. Takip edilen site üzerinden herhangi bir zararlı yazılım (malware) yayılıp yayılmadığını kontrol ederek anlık (real time) bilgi sağlar ve alarm üretir.

Uygulama, sisteme kullanıcı tarafından girilen WEB sitelerini yine kullanıcının belirlediği aralıklarla sürekli ziyaret ederek güvenlik problemlerini tespit eder ve bununla ilgili yöneticileri uyarır.

Uygulamanın ana modülleri aşağıda açıklanmıştır:

1. Erişim Kontrol Modülü

Günümüzde en çok karşılaşılan problemlerden biri sistemlerin servislerini durdurmaya veya aksatmaya yönelik saldırılardır. Servis aksatma (Denial of Service) saldırıları olarak isimlendirilen bu saldırıların mümkün olabilecek en kısa sürede bildirilmesi ve önlenmesi önemlidir. Bu çalışmada, bu tür atakların bildirilmesi ve önlenebilmesi için bir takım önlemler geliştirilmiştir. Periyodik aralıklarla alan adı cevap süreleri ve URL kontrolleri gibi unsurlara bakarak sunucuya yapılacak olan herhangi bir atağın önceden belirlenmesi sağlanmıştır.

2. Anahtar Kelime Kontrol Modülü

WEB uygulamaları veya WEB siteleri saldırganlar tarafından ele geçirildikten sonra içerikleri değiştirilmektedir. Bu değişiklikler genelde sitenin ele geçirildiğine dair ibarelerden oluşmaktadır. Bu modül sayesinde bu tip içerik değişikliklerine karşı web sitelerini periyodik aralıklarla takip ederek olası değişiklikler tesbit edilebilmektedir.

Bu takip süreçlerini gerçekleştirmek ve saldırı tespiti yapabilmek için sadece içerik değişikliklerine değil, URL tabanlı kontroller uygulayarak farklı vektörlerde değişiklik tespiti yapabilmektir.

3. Zararlı HTML Kod Tespit Modülü

Saldırganlar, gelişmiş kalıcı saldırılar olarak adlandırılan organize ataklar gerçekleştirdiklerinde ele geçirilen web siteleri üzerinden zararlı yazılım dağıtımı yapmaktadır. Bu modül saldırganlar tarafından ele geçirilen web siteleri üzerinden herhangi bir zararlı yazılım dağıtımı yapılıp yapılmadığını kontrol etmektedir.

Ayrıca bu tip saldırıların tespit edilebilmesi için site içerisinde bulunan ve saldırganlar tarafından eklenmiş olabilecek iframe, javascript, embedded gibi içerik kodlarına bakarak bildirim yapabilmektedir[7].

4. İçerik Değişiklik Modülü

Bu modül ile takibini gerçekleştirmek istediğiniz WEB uygulamasını veya WEB sitesini, uygulama veri tabanına ekledikten sonra eklediğiniz sitenin anlık görüntüsü veri tabanına kaydedilir. Bu işlemden sonra içerik değişimleri statik ve dinamik kodlar karşılaştırılarak bildirim sağlanır.

Ayrıca bu karşılaştırılmanın yapılabilmesi için gerekli periyodik aralıkların belirlenebilmesi noktasında esneklik sağlamaktadır. Statik ve dinamik karşılaştırma sonucunda şüpheli durumları tespit ederek doğruluk oranıyla birlikte bildirim gerçekleştirilmektedir.

5. Yapısal Değişiklik Kontrol Modülü

Bu modülde statik içeriğe ait değişimlerin belirlenebilmesi için birden fazla yöntem kullanmaktadır. İçerik Değişim kontrollerine benzer olarak sitenin sisteme bildiriminden sonra anlık XHTML içeriği alınarak statik içerik içerisinde dinamik analizler gerçekleştirilmektedir. Site içerisinde kullanılan, değiştirilen veya eklenen HTML etiketlerinin dahi belirlenerek kullanım oranlarının çıkarılması ve şüpheli durumların bildirilmesi sağlanmaktadır.

6. SQL Sızıntısı Zafiyeti Kontrol Modülü

Günümüzde web sitesi saldırılarının büyük bir bölümü SQL Enjeksiyon sayesinde gerçekleştirilmektedir.[8] WEB sitelerinin dinamik, değişken ve modüler yapılarından dolayı güvenlik kontrollerinin sürekli olarak gerçekleştirilmesi oldukça zordur.

Bu modül web sitelerini periyodik aralıklarla tarayarak SQL Enjeksiyon kaynaklı kritik güvenlik açıklarını tespit etmektedir. Aynı zamanda güvenlik açıklarını kritiklik düzeylerine göre sınıflandırabilmektedir.

Bunun yanında, periyodik aralıklarla sistemi taramasının yanı sıra güvenlik açıklarına dair detaylı rapor sunabilmekte ve sunduğu rapor içerisinde tespit edilen her güvenlik açığına dair detaylı bilgi barındırmaktadır.

7. WEB Ekran Görüntüsü Analiz Modülü

Bu modül veri tabanına herhangi bir WEB sitesi dâhil edildikten sonra alan adı bazlı ekran görüntülerini periyodik aralıklarla almaya başlayacaktır. Uygulama periyodik olarak aldığı ekran görüntülerini piksel tabanlı karşılaştırarak değişim oranlarına göre bildirim yapacaktır.[9]

8. DNS Kayıt Kontrol Modülü

Uygulama ilk kurulum esnasında WEB sitesine ait DNS kayıtlarını veri tabanı üzerinde saklamakta. Olası DNS değişikliklerine veya şüpheli işlemlere karşı periyodik olarak tarama yapmaktadır. Bunun yanında tüm DNS kayıtlarını tek tek inceleyerek değişiklikleri tespit etmekte, değişikliğin yapıldığı andan itibaren bildirim sağlayarak sitenin istenmeyen durumlarda servis dışı kalmasını önlemektedir[10].

9. Alan Adı Kayıtları Kontrol Modülü

Bu modül sitelere ait whois bilgilerinde saldırılardan kaynaklı olabilecek değişiklikleri tespit ederek bildirmeyi amaçlamaktadır. Hizmet alınan firmaya veya sunucuya ait isim sunucuları, kayıtlı elektronik posta adresleri gibi birçok farklı unsura bakarak sitenin risk altında olup olmadığını belirlemektedir. Ayrıca olası atakları ve belirlediği değişiklikleri doğruluk oranlarına göre bildirerek, olası bir saldırıdan kaynaklı oluşabilecek hasarı en az kayıpla sonlandırılmasına ve önlem alınmasına yardımcı olmaktadır.

10. Ağ Yolu Kontrol Modülü

Bu modül web sitesine erişim esnasında kullanıcının hangi olağan yollardan geçtiğini öğrenerek bunun dışında erişimde geçilen yolları tespit etmekte. Trafiğin saldırgan tarafından yönlendirildiği durumlarda siteye erişim engellenebilmekte veya değiştirilebilmektedir. Bu gibi durumlara karşı, uygulama bu iletişim yollarını sürekli takip ederek, gerçekleşen değişiklikleri anında bildirmektedir. Düzenlenen saldırılara karşı anında aksiyon alınabilmesi için uygulama kullanıcılarını bildirim yapılmaktadır

11. SSL Sertifikası Kontrol Modülü

Uygulama kontrol ettiği WEB siteleri üzerinde SSL Sertifikalarının doğruluğunu teyit etmek için bir takım kontroller gerçekleştirmektedir. SSL sertifikasının doğrulanmış bitiş tarihi, seri numarası ve imza algoritması gibi kontroller gerçekleştirilmesi oldukça önemlidir. Bu modülle doğrulama işlemlerini gerçekleştirememesi durumunda kontrol paneli üzerinden anında bildirim gerçekleştilmesi sağlanmaktadır.

12. Zararlı Yazılım Kontrol Modülü

Bu modül sayesinde gelişmiş kalıcı tehditler adı verilen organize ve ısrarlı düzenlenen saldırılara karşı güvenlik çözümleri geliştirilmiştir. Zararlı yazılım analizi ve kontrolü bu süreçlerden sadece bir tanesidir. Bu modül web siteleri üzerinde bulunan zararlı yazılım yayılması amacıyla yaygın olarak kullanılan PDF, HTML/JS, EXE, DLL ve benzeri uzantılardaki dosyaları anti-virüs taramasından geçirerek zararlı içeriklere sahip dosyaları listeleyebilmektedir.

Bunun yanında site üzerinde belli uzantılarda tespit edilen dosyaları birden fazla anti-virüs ile tarayarak ve aynı zamanda statik analiz süreçlerine tabii tutarak zararlı olabilecek dosyaları belirlemektedir. WEB siteleri üzerinden zararlı yazılım dağıtımı yapıldığını tespit etmesi durumunda anında bildirim sağlamaktadır. Tüm tarama süreçleri uygulama üzerinden ve periyodik aralıklarla gerçekleştirilmektedir.

13. Veri Sızıntısı Takip Modülü

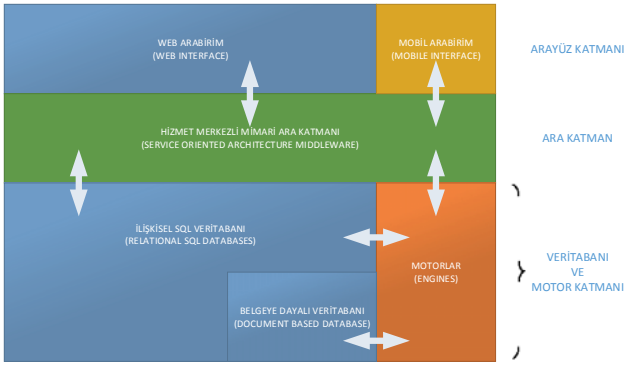
Veri sızıntıları günümüzde birçok kuruluşun en büyük problemlerinden biridir. Saldırganlar ele geçirdikleri sistemlere ait gizli/önemli bilgileri kurumlardan çalarak çoğu zaman internet üzerinden yayınlamaktadır. [11]

Bu modül ile benzeri durumlara karşı veri sızıntısını önlemek adına çözümler geliştirilmiştir. Bir çok veriyi sosyal medya platformları, IRC benzeri sohbet ortamları, web tabanlı metin saklama alanları gibi birçok platformu sürekli tarayarak takip etmektedir. Ayrıca muhtemel veri sızıntılarına karşı tespit ettiği bilgileri site/içerik sahipleri ile paylaşarak anında bildirim sağlamaktadır.

V.BU ÇALIŞMADA İZLENECEK YÖNTEM VE TEKNİKLER

Çalışma kapsamında öncelikle Şekil 2'de geliştirilen kavramlar, Şekil 3'te gösterilen uygulamanın içeriğinde bahsedilen modüler motorlar ile ilgili akademik araştırmalar, daha önce geliştirilmiş teknikler incelenecek olup buna gore yeni yaklaşımlar ve çalışmalar gerçekleştirilebilecektir. Çalışma kapsamında nesne tabanlı ve katmanlı yapı olarak geliştirilecek sistem, temelde üç ana kısımdan oluşmaktadır:

- Ara Yüz Katmanı
- İş Katmanı
- Veri Tabanı ve Motor Katmanı



Şekil. 4. Yazılım mimarisi-katmanlar

A. Arayüz Katmanı

Web ve Mobil arabirim, ara katman üzerinden verileri alacak ve yönetici veya kullanıcılara gösterecektir. Ara katman kullanımı sayesinde hiçbir şekilde uygulamaların doğrudan veritabanına erişmemesi sağlanacak böylelikle güvenlik ihlallerinin önüne geçilecektir. Zira ara katman, sadece kendisi üzerinde tanımlanan komutlara cevap veren ve sadece belirli sorguları veritabanında çalıştırmak üzere tasarlanmaktadır.

B. İş Katmanı

Kurumlar veya kullanıcılar, kendi geliştirdikleri uygulamalar veya farklı programlar üzerinden de kendi sistemlerine ait verileri almak ve görüntülemek istedikleri durumda buna cevap verebilmek amacıyla ara katman tamamen API ve SOAP yaklaşımıyla tasarlanmıştır. Ara katman erişimleri temin edilen API-KEY ile PKI ile gerçekleştirilerek ve trafik SSL üzerinden gerçekleştirilerek güvenliği sağlanmaya çalışılmıştır.

C. Veri Tabanı ve Motor Katmanı

Motorlar topladıkları verileri ve yaptıkları analiz sonuçlarını iki farklı mimarideki veri tabanına doğrudan kaydedetmektedir. İlişkisel verilerden oluşan verileri SQL tabanlı veri tabanına, belgeye dayalı verileri ise NoSQL veri tabanına işlenmektedir.

Site kurulumu safhasında sitelerle ilgili temel bilgilerin toplanarak kaydedilmesi için, ara katman (iş katmanı) sadece kendine ayrılmış alandaki motora istek göndererek gerekli verileri alıp temel değerler olarak veri tabanına işlenmektedir.

Bu çalışmada çeşitli dilleri en uygun oldukları alanlarda kullanarak ve kesinlikle bir dil bağımlılığı olmadan geliştirilmeye çalışılmıştır.

VI. SONUÇ

Sonuç olarak: Öncelikle kritik altyapıya sahip kurumların siber güvenlik tehditlerine karşı uyarı/alarm alabilmeleri sağlanmıştır. Yazılım sisteminin Software as a Service Servis olarak yazılım hizmeti amaçlı sistem tasarımının gerçekleştirilerek, sistemin kullanıma hazır hale getirilmesi ile internet servis sağlayıcılarının gereksinimleri karşılanacaktır. Ayrıca devlet kurumlarının siber saldırılara karşı korunması hızlı, güvenilir ve doğru şekilde gerçekleştirilebilecektir.

Geliştirilecek ürün, WEB sitelerinin ve bağlı oldukları DNS servislerinin güvenlik durumlarını sürekli takip edecek, sitelere karşı gerçekleştirilen bir siber saldırıyı tespit ettiği anda ilgili kişilere alarm vererek derhal müdahale edilmesini sağlayacaktır.

Siber saldırı gözlem ve kayıt ürünü olarak; özellikle kamu sitelerinin siber saldırı sebebiyle erişilmez duruma gelmeleri, siteye propaganda mesajı bırakılması, siteye bir zararlı yazılım/virus/solucan bulaşması veya bulaştırılması, sitelerin güvenli iletişim kurmalarını sağlayan SSL sertifikalarında bozulma gerçekleştirilmesi durumunda derhal uyarı verecek ve bu saldırıyla ilgili bilgileri, saldırı sonucundaki durumu daha sonradan incelenebilmesi için kayıt altına alacaktır. Bunun yanında;

- Kritik altyapılara yapılacak olası siber saldırıların tespitinin yapılarak takip edilmesi sağlanacak,
- WEB sayfaları üzerinden yayılan zararlı yazılım (Malware) ve gelişmiş kalıcı tehditler (APT – Advanced Persistent Threat) tespit edilecek ve yayılmasına izin verilmeden önlem alınması sağlanabilecek,
- Dijital sosyal medya ortamlarında ve saldırganların kullandıkları paylaşım platformlarında kurumlarla ilgili bir ifşa veya ön hazırlık durumu hemen tespit edilebilecek ve gerekli tedbir alınabilecek,
- Tespiti yapılan siber saldırılarla ilgili olarak yetkili birimlere alarm vermek ve gerekli ilk önlemleri alması sağlanacaktır.

KAYNAKÇA

[1] Bilgi Güvenliği Derneği Siber Güvenlik Ulusal Strateji Belgesi
[2] http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php
[3] http://www.ubak.gov.tr/BLSM_WIYS/HGB/tr/Belgelik/20130430_162338_10472_1_66697.pdf
[4] http://tr.wikipedia.org/wiki/Bilgisayar_g%C3%BCvenli%C4%9Fi
[5] http://www.turk-internet.com/portal/yazigoster.php?yaziid=31969
[6] Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (August 1996). "Role-Based Access Control Models" (PDF). IEEE Computer (IEEE Press) 29 (2): 38–47.
[7] http://www.w3.org/TR/html-markup/syntax.html#doctype-syntax (Haziran 2013)
[8] www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet (Haziran 2013)
[9] Deltchev, Krassen. "Yeni Web 2.0 Saldırıları" . Lisans Tez . Ruhr-University Bochum . 18 Şubat 2010
[10] http://www.icann.org/en/news/announcements/announcement-23aug13-en.htm
[11] http://wikileaks.org/syria-files/ Ağustos2013

Mustafa ALKAN Erciyes Üniversitesi Mühendislik Fakültesi, Elektronik Mühendisliği Bölümünden mezun olan Alkan, Aynı Fakültede Araştırma Görevlisi olarak göreve başladı. Yüksel Lisans ve Doktora eğitimini Erciyes Üniversitesinde tamamladı. 1994-2001 Yıllarında Elektronik Bölüm Başkanlığı, Meslek Yüksekokulu Müdürlüğü görevlerinde bulundu. 1998 Yılında Doçent oldu. 2001-2012 Yıllarında Bilgi Teknolojileri ve İletişim Kurumunda Kurum Başkan yardımcısı olarak görev yaptı. 2012 Yılında Prof. oldu. Halen Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği Bölümünde Bölüm Başkanı olarak görev yapmaktadır.
Elektronik ve Bilişim alanında ulusal ve uluslar arası dergi ve sempozyumlar da yayınlanmış 100 den fazla eseri bulunmaktadır. Bilgi Güvenliği, Kriptoloji, İnternet Alan Adları, IPv6, Siber Güvenlik, Elektronik İmza, Kayıtlı Elektronik Posta Sistemleri, gibi konularda proje çalışmaları bulunmaktadır. Dünya Bilgi Toplumu Zirvesi Ulusal Koordinasyon Kurulu Başkanlığı, Elektronik İmza Koordinasyon Kurulu Başkanlıkları gibi görevleri yürütmüştür. Bilişim alanında yapılan birçok Ulusal ve Uluslararası Konferansın eş başkanlığını yapmaktadır.

Burak ÇİFTER 2000'lerin başından beri bilgi güvenliği alanında denetmen ve danışman ünvanlarıyla görev aldı. Yerli ve yabancı bir çok finans kurumuna, telekom servis sağlayıcısına ve kamu kurumlarına hizmet ve destek verdi.
Özellikle uygulama ve ağ güvenliği alanında yaptığı çalışmalarda yaygın kullanılan bir çok ticari ve açık kaynak kodlu yazılımda güvenlik açıkları buldu. Çoğunlukla yabancı güvenlik komünitelerinde faliyet gösterdi.
2010 yılında BOA Bilgi Teknolojileri ve Güvenliği şirketini kurdu ve güvenlik alanındaki çalışmalarını bu çatı altına topladı. Halen güvenlik alaninda projelerde fiilen görev yapmaya devam eden Burak Çifter, artan ulusal risk ve milli çozüm ihtiyacı sebebiyle çalışmalarını ulusal kritik altyapılar ve milli siber güvenlik üzerine yoğunlaştırdı. Bilgi Güvenliği Derneği'nin aktif üyesi olan Burak Çifter, siber güvenlik ile ilgili fikirlerini ve güncel olayları blog'unda (http://www.burakcifter.com/) paylaşmaktadır."

Elif Tuğba KILIÇ 05 Aralık 1987 yılında Ankara'da doğdu. 2001-2005 yılları arasında lise eğitimini yabancı dil ağırlıklı eğitim almak suretiyle Antalya Atatürk Lisesi'nde tamamladı. 2005-2009 yılları arasında Kara Harp Okulu'nda lisans eğitimini tamamladı ve 2009 yılında Muhabere Teğmen olarak mezun oldu. 2009-2010 yılları arasında MEBS Okulu ve Eğitim Merkezi Komutanlığı (ANKARA)'nda icra edilen 56'ncı Dönem Muhabere Sınıfı Subay Temel Kursu'nu 2'ncilikle bitirdi. Subay Temel Kursu'nu tamamlamayı müteakip 2010-2012 yılları arasında GES K.lığı (ANKARA)'nda görev yaptı. K.K.K.lığının 2012 Yılı Genel Atamaları ile MEBS Okl.ve Eğt.Mrk.K.lığı (ANKARA)'na atanmıştır. 2012 Yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü Kazaların Çevresel ve Teknik Araştırılması Bölümünde Yüksek Lisans eğitimine başlamıştır ve hali hazırda eğitim süreci devam etmektedir. bekar olup, İngilizce bilmektedir.