VİRUS TESBİT PROGRAMLARI KİŞİSEL BİLGİSAYAR STANDARTLARI VE KONTROLLERİ

Emin Doğan AYDIN

Sunuş

Bugüne kadar yayınlanmış olaylarda virüs saldırılarının İki genel etkisinin olduğu görülmüştür:

(1) Bazen disk formatlama komutuyla dosyaları silmek ve

(2) genellikle bir mesajı herhangi bir başka mesaj alan her adrese göndermek yolu ile yaratılan mesaj sayısında bir patlama meydana getirerek ağı fazlasıyla yüklemek.Yükleme Dilimi)

Virüslerin yarattığı belli problemler şunları kapsar:

*Bellek veya diski kullanılmaz veri ile doldurmak (mesela, "çöp").
*Dosyaları değiştirmek.
*PC'de Dosya Tahsis Tablosunu (DTT=FAT) dosyalar bulunamayacak şekilde değiştirmek. [Yükleme Dilimi]

Marmara Üniversitesi, İletişim Fakültesi, Bilişim Anabilim Dalı

*Yükleme dilimini bilgisayar çalışmayacak şekilde değiştirmek.
*Tüm bilgileri yok edecek şekilde disketleri formatlamak veya başlatmak. (Başlangıç durumuna getirmek)
*Tuş tanımlama tablosunu değiştirmek.
*Klavyeyi kilitlemek.
*Dosyaları veya programları değiştirmek.
*Uygunsuz mesajlar yazmak veya görüntülemek.
*Program çalıştırma süresini uzatmak.

Virüs bulaştırma programlarının birçok potansiyel yapıları vardır ve zarar, virüsün tasarımına ve bulaştığı programın özelliklerine bağlı olarak bulaşma esnasında veya daha sonra meydana gelebilir. Virüsler kendilerini hem programlara hem de veri dosyalarına ekleyebilir ve bir sistemde hıza yayılabilirler.

Bir virüsün faaliyetleri, bulaştığı program çalıştırılınca tetiklenebilir. Virüs, program çalıştığı süre içerisinde amaçlanan fonksiyonunu gerçekleştirmeden önce tarih ve saat gibi belirli şartları kontrol edebilir. Eğer şartlar sağlanmıyorsa virüs kendini kopyalayıp yani çoğaltıp, bulaştığı program bir daha çalıştırılana kadar faaliyetsiz kalır.

Virüsler kendilerini saklamak için çok geliştirilmiş yöntemleri kullanacak şekilde tasarlanabilir. Bu tip program için kullanılan genel terim Truva Atıdır, çünkü programlar, Yunan askerlerini saklamak için içi boşaltılan Truva Atına benzer bir şekilde, bir şeyi yapıyormuş gibi görünürler ama aslında başka bir iş yaparlar.

Bilgisayar bağlantıları, virüslerin ciddi bir tehdit olmasının ana sebebidir. Bilgisayar sistemleri giderek artan bir şekilde diğer bilgisayar sistemlerine bağlanma kabiliyetine sahip olmaktadır ve bu da muhtemel saldırı noktalarının sayısını artırmaktadır. Hatta virüsler bilgisayar sistemlerine meşru giriş hakkına sahip olan kimseler tarafından da yayılabilirler. Ağlar, birçok kullanıcının verileri, programları ve

bilgisayarları paylaşmalarını sağlar, ama ne yazık ki tahrip etmeyi seven kimselerin bu kullanıcılara bir virüs programıyla saldırmalarına da fırsat tanır.

Virüsler ayrıca LAN (Yerel Ağlar) ve WAN (Geniş Alan Ağları) adı verilen birbirleri arasında haberleşebilen sistemler gruplarında da yayılabilir. Uygun ağ teknikleri ile işletim sistemleri farklı bilgisayarlar bile virüsler de dahil olmak üzere program ve veri iletimi yapabilirler.

Büyük bilgisayarlar veya mini bilgisayarlar, kişisel bilgisayarlardan daha az virüslere maruz kalırlar. Bunun sebepleri aşağıda sıralanmıştır:

* Büyük bilgisayarların daha karmaşık işletim sistemleri vardır.

* Büyük bilgisayarların daha çok güvenlikleri vardır. Birçok kişisel bilgisayar işletim sistemleri tek kullanıcılı olarak tasarlanmışlardır ve orijinal olarak güvenlikleri en az seviyede tutulmuştur.

* Büyük bilgisayar birimlerinin güvenlik işleriyle ilgilenen çalışanları vardır. Virüsler böyle ortamlarda çok çabuk farkedilirler, halbuki bazı kişisel bilgisayar ortamlarında farkedilmeden uzun süre kalabilirler.

* Büyük bilgisayar uygulamaları çoğunlukla eşsizdirler, böylece bir sisteme saldıran bir virüs, bir diğer sistemde aynı başarıyla işlevini yerine getiremeyecektir.

Virüsler genelde aşağıdaki şekillerde çalışırlar:

1. Bir programcı, bir başka bilgisayardaki bilgiyi değiştirmek veya tahrip edecek birkaç satır sayı veya harften başka bir şey olmayan bir virüs yazar. Eğlence veya öç alma amacıyla yapılabilir.

2. Virüs komutları, kelime işlemci, çarşaf düzenleme veya oyun bulunan meşru program içine saklanır. Bilgisayara bir disketle veya hatta telefon hatlarıyla bile bulaşabilir.

3. Bilgisayar asıl yazılımla beraber virüsü de okur.

4. Bilgisayar gizli virüsün komutlarını da yürütür. Bilgisayardan belli bir tarihte bilgi yok etmesini veya ekrana zararsız bir mesaj yazmasını isteyebilir. Hatta bilgisayara, makinaya sokulan her diske virüs bulaştırılmış bir programın kopyasını yazdırabilir.

5. Diğer bilgisayar kullanıcıları, virüs bulaşmış makinaya telefon hatlarıyla veya virüs bulaşmış bir disketle bağlanabilir. Bundan sonra bu bilgisayar sistemine bağlanan herkes virüsü daha da yayacaktır.

Muhtemel bir virüs saldırısının ihtar işaretleri şunlar olabilir:

* Kullanılabilir rasgele erişimli bellek (RAM) program yüklenmeden azalır.
* Disket sürücü ışığı beklenmedik şekilde yanar.
* Sistem oldukça yavaşlar.
* Programlar aniden olağan olmayan hata mesajları görüntülerler.
* DOS beklenmedik hata mesajları, özellikle de "Geçersiz Sürücü Tanımlaması" hatası verir.
* Dosya boyutları sebepsizce değişir.
* Dosya sayıları değişir.
* Dizin güncelleştirilmeleri farkedilir seviyede uzundur.
* Klavye tuşları aniden garip şeyler yapar.
* Sistem donar veya çöker.

Risk Değerlendirmesi

Bir virüsün, mali bir kuruluşun bilgisayar sistemine bulaşmasını öngörmek imkansız olsa da, olması halinde sonucu tam bir felakettir. Virüs ve diğer kişisel bilgisayar suçları tehtidini değerlendirmek için mali kuruluşlar virüs temasına maruz kalma olasılıklarını hesaplamalıdırlar. Nispeten az risk taşıyan yöntemler tek başına çalışan kişisel bilgisayarların kullanılması, ticari yazılımların tanınmış satıcılardan alınması ve programların diğer kullanıcılarla fiziki veya elektronik yöntemlerle değiştiriminin reddedilmesidir. Fakat bilgisayarların ağlarla birbirlerine bağlanması ve bildiri tahtası sistemleri gibi güvenilir olmayan kaynaklardan program kopyalarının kullanımı virüslerle teması ve kurum içerisinde virüslü yazılımın yayılmasını artıracaktır. Bunlara ek olarak ard niyetli çalışanların virüs sabotajı riski hala geçerli bir faktördür.

Mali kuruluşlar, virüs saldırısı ve yazılımlarının ve verilerinin çökmesine bağımlı potansiyel kayıplarını da değerlendirmelidirler. Aşağıdaki tablolardaki soru formunun kullanım amacı uygun önleme tekniklerinin kullanılabileceği yüksek risk taşıyan bölgeleri tespit etmektir. Genelde aşağıdaki değerlendirme nisbi riskin gösterimini sağlar.

Hayır veya bilinmeyen cevaplarının yüzdesi	Nisbi Risk
%20	Düşük
%50	Orta
%80	Yüksek

Günlük işlemler için verilerinin doğruluğuna ihtiyaç duyan veya verilerin yerine konulamaz olduğu mali kuruluşlarda, virüsten korunma teknikleri virüs teması ihtimali düşük olsa bile gerekli olabilir.

İş ağları virüs saldırıları konusunda üniversite ve araştırma ağlarından daha şanslıdırlar çünkü kullanıcı topluluğu genellikle küçüktür ve araştırma ağlarındaki kullanıcılardan daha çok tanımlanabilirdirler. Dahası özel iş ağları, açık araştırma ağlarınkinden daha yüksek seviyeli güvenlik sistemi kurabilirler.

Aşağıdaki yüksek riske ilişkin faktörler şunları kapsar:

* UNIX ve PC-DOS tabanlı işletim sistemleri
* Zayıf ağ yönetimi
* Serbest erişim/dial-up
* Homojen donanım ve işletim sistemleri
* Sınırlı şifre kontrolü
* Herhangi bir üniversitenin veya araştırma kuruluşunun bağlanmasına izin veren açık ağlar

Bedava yazılım ve ortak yazılımları özellikle yüksek risk taşırlar. Bedava yazılım bir ağdan ücretsiz olarak yüklenebilen, halka açık programlardır. Eğer bir üyelik ücreti söz konusuysa, buna da ortak yazılım denir.

Disk veya disket sıkıştırma yardımcı yazılımlarda virüs temasına yüksek oranda maruz kalan alanlardır. Eğer virüslü sıkıştırılmış program kullanılırsa sıkıştırılan veya açılan tüm programlara virüsü bulaştırabiir. Korsan kopya yazılımlar, yayın hakkı kanunlarına ve yetkilerine ters düşmenin yanı sıra, korsan yayının orijinal kaynağı bilinmediğinden dolayı yüksek bir risk de taşır.

Korunma Teknikleri:

Bilgisayarları tamamen izole etmenin yolu bulunmadığından, şu anda virüs sızma riskini ortadan kaldıracak bir me-

tod bilinmemektedir. Fakat aşağıdaki kontrol teknikleri virüsleri tespit edebilir veya bulaşmalarını engelleyebilir.

* Önemli veri dosyalarını ve programları düzenli bir şekilde yedekleyin.

* Yedeklemenin birçok neslini hazırlayın.

* Halka açık yazılım kullanmaktan kaçının. Böyle bir yazılımı kullanmak gerekliyse, kritik dosya ve sistemlerden ayrı bir yerde baştan sona test edin. Ekstra güvenlik için programları sistem saatini, Nisan 1, 13. Cuma veya tatiller ve diğer önemli tarihler gibi gelecek tarihlere ayarlayarak deneyin.

* Kullanmadan önce tüm yazılım ve verilerin kaynağını değerlendirin.

* Tüm yazılım ve verilerin yazma korumalı Ana kopyalarını bulundurun.

* Bir virüsün bilgisayara mütemadiyen bulaşmasını engellemek için işletim sistemini sabit diskte değil disketlerde saklayın.

* Disket sürücü tabanlı sistemleri yazma korumalı ve açıkça etiketlenmiş bir yükleme/başlatma disketi ile yükleyin/başlayın. Virüslü bir disket ileyüklenen/başlatılan sisteme virüs bulaşabilir.

* Sabit diskli bir sistemi, kurtarma operasyonu haricinde disketle yükleme/başlatmadan kaçının.

* Bülten tahtalarından program yüklemekten kaçının. Bülten tahtalarına erişmeniz gerekiyorsa bilgisayarı sadece disketlerle kullanın ve bu disketleri diğer yazılımlarınızdan uzak tutun. COMMAND.COM bulunduran dosyalara dikkat edin.

* Disketlerinizi orijinal yazma korumalı DOS disketinizle formatlayın.

* Yerel ağlarda virüs giriş riskini azaltmak için disksiz iş istasyonları kullanın.

*Bedava yazılımları ve ortak yazılımları kullanıcılara dağıtmadan önce bir test kişisel bilgisayarı üzerinde karantinaya alın.

* Satın alınan yazılımların mühürlü disket kutularında gelip gelmediğini kontrol edin.

* Tüm programların boylarını düzenli bir şekilde kontrol edin. Boylardan sapmalar virüs bulaşmasının kanıtı olabilir.

* Dosyaların veya programların son değiştirilme tarihlerini izleyin.

* Güvenilir kaynaklardan yazılım kullanın. Bir bilgisayar virüsünün en yaygın bulaşma metodu elektronik bülten tahtalarından olmaktadır. Halka açık programlar, bunların içine virüs yerleştiren kimselerin faaliyetlerine karşın çok korunmasızdırlar. Meşru bir program dolaşan bir virüsün taşıyıcısı olabilir. Bülten tahtalarından halka açık programların yüklenmesine izin vermeyecek politikalar geliştirin.

* DOS dizinini periyodik olarak CHKDSK komutu ile kontrol edin. Gizli dosyaların sayısındaki artış konusunda dikkatli olun. Orijinal bir DOS disketinde iki gizli dosya bulunur: IBMBIO.COM ve IBM DOS.COM (Eğer disketin etiketi varsa üç gizli dosya bulunacaktır.). Bazı yardımcı programları diski incelemek ve tüm dosyaların (gizli dosyalar da dahil) isimlerinin görüntülenmesinde kullanılabilir.

* Amaç kodunu paylaşmaktan kaçının ve paylaşılan tüm kaynak kodlarını inceleyin. Kaynakta virüs saklamak çok daha zordur.

* Kullanılmış disketlerinizi yeniden formatlamak için her zaman DOS FORMAT komutunu kullanın, sadece dosyaları silmekten kaçının.

* Dosya ismine göre sıralandırılmış dizini yazıcıya yazdırın. (DIR/SORTPRN) .COM, .EXE, .BAT veya .SYS

uzantılı dosyaların boylarında açıklanamayan değişiklikleri kontrol edin. Aynı isimli fakat farklı uzantılı dosyaları inceleyin. Bu durumlar bir virüse hedef olmuş dosyaları gösterebilir.

* Şüpheli dosyaları tamamıyla ortadan kaldırın. DOS'un DEL/ERASE komutu, DIR komutuyla görünmeyecek şekilde sadece dosya adının ilk harini değiştirir. Silinmiş herhangi bir dosya üzerine yeni bir şey yazılana kadar aynı yerinde saklı kalır. Dosyanın veri alanının ve dizin girişini yardımcı programları kullanılabilir.

* Bilgisayar programlarının işleyişlerindeki değişiklikleri takip edin.

Ağ yöneticileri virüs saldırısı riskini aşağıdaki maddeleri uygulayarak azaltabilirler:

* Şifreyi sık sık değiştirerek.

* Resmi olarak üretim sistemlerinde kullanılması onaylanmamış yazılımları yasaklayarak.

* Sistem performansının ve kullanımını izleyerek ve açıklanmayan değişimleri inceleyerek.

* Sıradan kullanıcıların ayrıcalıklı erişim sağlamalarına imkan tanımayacak uygun erişim kontrolleri ve bütünlük önlemlerini uygulayarak.

* Program ve işletim sistemi erişimine sadece ihtiyaç duyanlara izin vermek.

* Belli veri nesnesine yazmayı sadece bir tek bireyle sınırlandırarak.

* Kullanıcılardan, sistemden aldıkları olağan dışı sonuçları ve sistemin olağan dışı davranışlarını en kısa zamanda bildirmelerini isteyerek.

* Bir virüs saldırısı durumunda kullanılacak planları geliştirerek ve sistemi yeniden işler hale getirecek kaynak-

ları tanımlayarak. Bu kaynak listesi bilgisayarda saklanmamalıdır.

* Uzaktan teşhis hatlarının kullanımını kontrol ederek.
* Sistem yazılımı [defaultlarını] muhtemel güvenlik çıklarını engelleyecek şekilde ayarlanmalıdır.

Tesbit Programları

Virüsleri tespit etmek için kullanılabilecek birçok yazılım ürünü vardır.

Ürünler genelde:

(1) virüslerinvarlığını tespit eden programlar veya

(2) virüslerce yapılandosya değişikliklerini tespit eden programlar olarak tanımlanablirler.

Virüslerin varlığını tespit etmek için tasarlanan ürünler bu işi şüpheli kodu, şüpheli metin dizilerini veya bilinen virüsleri tespit etmek için belirli dosya isimlerini arayarak yaparlar. Fakat bu sınırlı teknikler yeterli koruma sağlamayabilirler.

Virüslü dosyada yapılacak değişiklikleri tespit etmek için tasarlanan ürünler dosyadaki her bitin matematiksel toplamını alır. Bu toplam önceki değerle karşılaştırılır. Diğer yaklaşımlar dosya değişimlerini tespit etmek için karmaşık algoritmalar ve şifreleme tekniklerini kullanırlar. Bu virüs tespit me todlarına ilaveten, birçok programlar yükleme/başlangıç sektöründe yapılan değişiklikleri; yeni gizli dosyların varlığı ve işletim sistemini devre dışı bırakan diske yazma işlevlerini de kontrol ederler.

Kanun

14 Temmuz 1988 tarihinde A.B.D. Kaliforniya Temsilcisi Wally Herger, bilerek bir programın içerisine programı kullanan kimsenin zararına sebep olacak komutlar yerleştiren ve bunun varlığından haberdar etmeden programı dağıtan kimseye zorunlu kamu görevi veya ceza getiren H.R. 5061 no.lu Bilgisayar Virüsünün Durdurulması Yasası teklifini sunmuştur. Kararın ana amacı, zarar vermeyi amaçlayan bir virüsü yaymayı tasarlayan kimselere karşı caydırıcı bir tutum oluşturmaktır.

Kişisel bilgisayar Standartları ve Kontrolleri:

Kişisel bilgisayarların artan kullanımı mali kuruluşlarda etkinliği ve verimliliği arttırmak için hayli önemli bir stratejidir. kişisel bilgisayarlar nispeten düşük maliyetli, küçük ve güçlüdürler. Donanım ve yazılım alternatifleri çoğalmaya devam ediyor. Fakat birçok alternatif var olan veya gelecekte olacak donanımlarla uyumlu olmayabilir. Bu yüzden koordinesiz seri alım kararları gereksiz harcamalarla ve etkisiz anapara yatırımlarla sonuçlanır. Kişisel bilgisayar kararları tek tek bölümler yerine tüm organizasyonun faydası ve ihtiyaçlarına dayalı olmalıdır. Alım kararı için bireyselleşmiş yaklaşımda bulunma isteği vardır. Ancak büyük yararlar sağlayabilmek için iyi tanımlanmış alım politikaları ve yöntemleri gereklidir. kişisel bilgisayarlar ancak, yönetim, standartlar ve kontroller geliştirdiğinde etkili ve verimli bir şekilde uygulanabilir. Bu yaklaşımın faydaları:

* Organizasyon içerisinde kişisel bilgisayarların kolaylaştırılmış yönetimi, kontrolü ve desteği.
* Arttırılmış esneklik.
* Azaltılmış veri işleme harcamaları.

* Veri işleme sistemlerinde artırılmış etkinlik ve verimlilik.
* Organizasyon içerisinde artırılmış yeknesaklık ve tutarlılık.
* Çapraz eğitim ve personel yedeklemesi için fırsatı artırmak.

Donanım, yazılım, işlemler ve belgelendirme için kişisel bilgisayar standartları ve kontrolleri tanımlanmalıdırlar.

Donanım Teknik Standartları

Mali kurumların her teçhizat parçası için standart donanım tanımlamaları bulunmalıdır. Standart donanım yapıları bakım-maliyeti kontrollerinin daha ucuza yapılabilmesini sağlar. Bazı mali kurumlar, diğer birimler arızalandığında ve bakım gerektiğinde kullanılmak üzere yedek bir kişisel bilgisayar alırlar. Bu yaklaşımı kolaylaştırmak için yeknesaklık gereklidir. Tipik donanım teknik standartaları tablosunda özetlenmiştir.

Yazılım Teknik Standartları

Yazılım teknik standartları belli donanım standartlarından daha önemli olabilir. Genelleştirilmiş yazılım paketlerini standartlaştırmak özellikle önemlidir.

* Elektronik çarşaflar/bülten tahtaları
* Çarşaf belgeleme sistemi
* Grafikler
* Kelime işleme
* Veri tabanı
* Dosya aktarımı
* Terminal taklidi

* İletişim
* Elektronik posta
* Mesaj yönlendirme
* Takvim yönetimi
* Buluşma zamanlaması
* Çalışma/işaretleme dosyaları
* Güvenlik sistemleri
* İşletim sistemleri ve uygulamalar

Yeknesak yazılım kullanımı çapraz eğitim ve personel yedeklemesi imkanını artırır. Ayrıca bazı durumlarda çoklu sistemleri kullanmak için tek lisans ücreti anlaşması yapmak mümkündür. Standart yazılım kullanıldığında yazılım güncelleştirmelerinin kontrolu ve kurulumu daha kolaydır.

Yönetim programlama dili konusunda da bir standart oluşturmalıdır. Business Basic oldukça popülerdir. Bu dilin endüstride kullanılan bir çok versiyonu vardır. Bu versiyonların birçoğu birbirleriyle uyumlu değildir ve belirli tip donanımla sınırlanmışlardır.

İşlevsel Standartlar

Çeşitli prosedür ve fonksiyonların etkinliğini ve verimini artırmak için kişisel bilgisayar işletim standartları belirlenmelidir.

Yardımcı olabilecek birçok fikir aşağıda sıralanmıştır:

* Programlar ve veri dosyaları yedeklenmelidir Öncelikli dosya ve programların kopyaları birden çok yerde saklanmalıdır. Kopyaların bölgeden uzak ve yangına dayanıklı kabinlerde saklanması tercih edilir.

* Sabit disk sürücülerde standart alt dizin isimleri kullanılmalıdır:

°SYSTEM : DOS disketindeki dosyalar
°LOTUS : Lotus 1-2-3 programı dosyaları
°WORD : Kelime işleme program dosyaları
°COMM : İletişim progamı dosyaları
°GRAPH : Grafik dosyaları

* Disket etiketleri, yapılandırmayı ve bulmayı kolaylaştırmak için renklerle kodlanmalıdırlar. Veri, yedek, program ve sistem disketleri de dahil her disket tipi için farklı renkler kullanılmalıdır.

* Her program disketinin etiketinde vesiyon numarası olmalıdır.

* Önemli dosyalar ve programlar yazma korumalı dosyalarda saklanmalıdır.

* Genelleştirilmiş yazılım paketleri (elektronik çarşaflar, grafikler, veri tabanları, kelime işleme) için özel işletim standartları belirlenmelidir.

Belgelendirme Standartları

Hem kendinizce geliştirilmiş hem de satın alınmış yazılımlar için belgelendirme standartları belirlenmelidir. Bunlar aşağıdakileri içeren kullanıcı belgelendirmesini kapsarlar:

* Kurulum yöntemleri
* Detaylı işletim rehberi
*Özel öğreticilik
* İçerik tablosu
* Dizin
* Yedekleme yöntemleri
* Yeniden başlatma usulleri

* Problem çözme rehberi
* Çabuk danışma kartı
* Fonsiyon tuşu şablonları
* Sayfa numaraları
* Örnekler

Satın alınmış yazılım belgelendirmesi standartlarında şunlar da kapsanmalıdır. :

* Sistem disketinin birden çok kopyası veya kopyalama imkanı

* Satıcı tarafından sağlanan veya korunan kaynak kodu

Kendinizce geliştirilmiş yazılım standartlarına aşağıdakileri dekapsayan teknik belgelendirme de dahil edilmelidir:

* Detaylı kaynak kodu anlatımı
* Sistem akış diyagramları
* Ana dosyaların isim ve tanımları
* Sistemin anlatımsal tanımı
* Ana disket
* Test verisi sonuçları örnekleri
* Geliştirme tarihi
* En son yapılan değişikliğin tarihi
* Değişikliği yapan kimsenin ismi
* Değişikliklerin tanımı

Tüm teknik belgelendirme yetkili personelce rahatça erişilebilecek merkezi bir yerde saklanmalıdır.

Çarşaf Standartları ve Kontrolleri

Elektronik çarşaf yönetim bilgisinde büyük gelişmeler sağlayabilir ve mali bir kuruluşta verimliliği artırabilir. Birçok mali kuruluş bütçeleme, kayıt tutma, mali raporlama ve çeşitli işlemsel ve analitik fonksiyonlar ve usuller için çarşaf yazılımlarını kullanmaktadır. Fakat elektronik çarşaflara giderek artan bu bağımlılık Pandora'nın kutusunu açabilir çünkü bu aletin olağanüstü gücü birçok ciddi hata yapma ihtimalini de artırmaktadır.

Çarşaf hataları birçok sebepten oluşabilir, fakat genellikle aşağıda sıralanan hataların sonuçlarıdır:

* Hatalı veri girmek
* Yanlış formüller kullanmak
* Yanlış hücrelere atıfta bulunma
* Programın yanlış versiyonunun kullanılması
* Çarşafı kullanmayı ve gözden geçirmeyi yanlış anlamak

Çarşaf programlarının geliştirilmesini ve kullanımını standardize ve kontrol etme muhtemel hataların sayısını ve sonuçlarının zararını azaltabilir. Bir sonraki örnek tasarım, işlem ve belgelendirme rehberleri ciddi hataların çoğunu tespit etmeli ve önlemelidir.

Çarşaf Tasarım Standartları

1. Özel amaçlar için sürekli hücre blokları ayırın.
2. Aşağıdakileri içeren yapı ve etiketleri sürekli kullanın:

°Başlıkları aynı noktaya yerleştirme

°Önemli alanların altını çizmek için tekrarlanan etiketler kullanma

°Kolon başlıklarının altını eksi işaretiyle çizmek
°Ara toplam ve toplamların altını eşittir işaretiyle çizmek
°Karakter bilgisini merkezleyerek yapılandırma
°Veri tabanı işlemlerini yanıltabilecek, boş karakterlerle yapılandırmaktan kaçınmak

3. Makro komutlar için büyük harf ve hücre adresleri ve Dağılma aralığı isimleri için küçük harf kullanma

4. Tablodan bağımsız değişkenlerle ve hesaplamalarda kullanılan varsayımları belgeleyin ve isim ve atanan değerle tanımlayın. Bağımsız değişkenler için özel girdi alanı ayrılmalıdır.

5. Aşağıdakileri de içeren bağımlı değişkenleri belgeleyin:
°Bunları hesaplamak için kullanılan bağımsız değişkenler
°Yerleşim
°Atanan yokluk hali değerler

6. Baştaki birkaç hücreyi
°Dosya adı
°Hacim etiketi
°Çarşaf başlığı (diskteki çarşaf ismi) için kullanın

7. Anlamlı ve tanımlayıcı
°Dağılım aralığı isimleri,
°Etiketler,
°Satır sütun başlıkları,
°Yorum satırları kullanın.

8 Bir grup hücreyi (yaklaşık 10'dan 20'ye) sürekli olarak ayırın ve;

°Çarşafın nasıl çalıştığına dair yorumlar,
°Yazarın adı,
°Yaratım tarihi,
°Son gözden geçirme tarihi,
°Son kullanım tarihi,
°Son test tarihini saklamak için kullanın.

9. Tüm makroları belgelendirin. Karmaşık makrolar şöyle belgelendirilirler:

°Makroların üstüne makronun ne yaptığını gösteren bir başlık satırı yerleştirin.

°Solda Dağılma aralığı isimleri, ortada makro kodları ve sağda da yorum satırları olacak şekilde üç sütunlu yapı kullanın.

°Çok karmaşık makro komutlardan kaçının ve mantık olarak birbirine bağlı komutların aynı satırda yer alabilecek şekilde makroları birkaç hücreye dağıtın.

10. Anahtar formülleri çarşafın sürekli kullanılan bir bölmesinde tanımlayın ve metni bloklar halinde görüntüleyin:

°Formülden önce etiket öneki yerleştirin.
°Önceki ve formülü yorum alanına kopyalayın.
°Yorum alanında formülün ne hesapladığını ve nasıl çalıştığını yazın.

11. Karmaşık makrolar ve formüller için hücre-koruma özelliğini kullanın.

12. Veri giriş alanını hesaplamalardan ayırın.

13. Veri giriş alanını varolan kaynak belge formlarına benzer tasarlayın .

14. Girdi alanını, görüntüleyip bunu veri giriş formu olarak kullanarak veri giriş alanını veri alma formu olarak kullanın. Veri daha sonra formdan çarşafa geçirilebilir ve böylece girdi formu ve çarşafın girdi alanı tutarlı olur. Girdi formları, verinin girileceği yeri göstermek için tekrarlanan etiket kullanmalıdır (mesela bir seri tekrarlayan periyot).

15. Verileri kolonlar halinde yukarıdan aşağıya girin ve bu şekilde düzenleyin. Bu daha hızlı ve daha hassas girişi mümkün kılar.

16. Hücre formüllerinde mümkün olduğunca dağılma aralığı isimleri kullanın. Dağılma isimleri, dağılma aralığı sınırına yeni satırlar ve sütunlar eklendiğinde yeniden tanımlama gerektirebilirler.

İşlevsel Kontroller

1. Büyük çarşaflarda hızlı veri girişini mümkün kılmak için yeniden hesaplama özelliğini elle yapmaya ayarlayın.

2. Dosyaları ve çarşafları yedekleyin.

3. Önemli çarşafların yedek kopyalarını birden çok yerde saklayın.

4. Aşağıdaki metodları kullanarak çarşafı test edin.

°Toplamları hesap makinesi ile sağlayın.
°Çarşafı hem satır hem sütun olarak tarayın ve sonuçları karşılaştırın.

°Daha önceden belirlenmiş sonuçlarla test verisi kullanın.
°Kanıtlanmış bir örnekle karşılaştırın.

5. Önemli çarşafları yazma korumalı disketlerde saklayın.

6. Otomatik kayıt makrosunu kullanın.

7. Her hücre yerleşiminde saklanan formülleri gösteren çarşaf çıktıları basan bir yardımcı programı kullanın. Basılan formüller hatalara karşı elle kontrol edilmelidir.

Belgelendirme Standartları

1. Çarşafın amacını tanımlayın.

2. Çarşafın işlevini tanımlayın.

3. Neyin hesaplandığı,Verinin nereden alındığı, Sonuçların neye benzeyeceğini de dahil ederek karmaşık formüllerin nasıl çalıştığını açıklayın.

4. Acemi kullanıcıların karşılaşabileceği muhtemel problemleri tanımlayın.

5. Çarşaf mantığının kaynağı hakkında temel bilgiyi tanımlayın (metin, ekonomik teori, kanuni gereklilikler gibi).

6. Çarşafın yayınlandığı tarih ve çarşafı yaratmak için kullanılan yazılımın versiyon numarasını, Orijinal yazarın adını, Mevcut en son düzenlemenin tarihi ve sorumlu kimseyi belgelendirin.

7. Tüm Dağılma aralığı isimlerini ve tanımlarını listeleyin. Hücre adresleri yerine Dağılma aralığı isimlerinin kullanımı Dağılma aralığı son noktalarında yapılacak değişikliklerin tüm çarşafa sürekli olarak yansımasını da garanti ettiği gibi isimlendirilmiş dağılma aralığı kullanarak yeni fonksiyonların inşasını da kolaylaştırır.

8. Tüm makroları listeleyin ve tanımlayın.

9. Çarşaf dosya adını, hacim etiketlerini ve disk ismini tanımlayın. Çıkarılmış, silinmiş veya ithal edilmiş dosyaların yerleri de belirlenmelidir.

10. Her diskte bulunan dosyaları disket etiketinde tanımlayın.

Sonuç olarak:

"Eğer bilgisayardan çıktıysa, doğru olmalıdır." Algılaması yanlış olabilir. Hataların nerelerde olabileceğini belirleyip, ciddi hataları indirgemek için koruyucu teknikler kullanarak, devrimci kullanıcılaryönetimin amaçlarına ulaşan etkili ve doğru çarşaf programları geliştirebilirler.

Aşağıdaki tablolarda;

° Bazı suç tekniklerinin sınıflandırılması,

° Genel bilişim kontrollarının ve yine

° Bilişim uygulama kontrollarının, bu suç sınıflandırmaları ile nasıl/muhtemel ilişkileri olabileceğinin kısa bir özeti verilmektedir.

KAYNAKÇA

1. Allen, B.; The biggest computer frauds: Lessons for CPAS, The journal of Accountancy, 1977.
2. American Bar Association (ABA), Criminal Justica Section, Task Force on Computer Crime.; American Bar Association Report on Computer Crime. Washington, D.C.: ABA, June, 1984.
3. American Institute of Certified Public Accountants.; American Institute of Certified Public Accountants (AICPA) Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries. New York: AICPA, 1984.
4. Baker, D.; An Agenda for the National Commission on Electronic Fund Transfers. In: Bank Administration, Vol. LI (1975, Dec.) 19.
5. Bequai, A.; Computer Crime, p 207. Lexington Books, 1978.
6. Bigelow, R., Nycum S.; Your Computer and the Law. Englewood Cliffs: Prentice-Hall 1975.
7. Bing, J., and Harvold, T.; Legal Decisions and Information Systems, Universitetforlaget, Oslo, 1977.
8. Bloom Becker, Jay.; Computer Crime, Computer Security, Computer Ethics. Los Angles: National Center for Computer Crime Data, 1986.
9. _____ The Computer Crime Law Reporter, with 1988 Update. Los Angles: National Center for Computer Crime Data, 1988.
10. _____. Introduction to Computer Crime, 2nd ed. Los Angles: National Center for Computer Cire Data, 1988.
11. _____. The Spread of Computer Crime. Los Angles: National Center for Computer Law Advisor, May, 1984.
12. _____. Commitment to Security. Los Angles: National Center for Computer Crime Data and RGE Associates, March, 1989.

13.Caldwell, M.; Jurisprudence in Interdisciplinary Environments. In: Jurimetrics Journal, Vol. 8 (1968) No. 3, 1
14. Computers, Society and Law: The Role of Legal Education. (Proceedings of the AFIPS/Standford Conference June 25-27, 1973). Ed. J. Leininger and B. Gilchrist. Montvale: AFIPS Press 1973.
15._____:Computer Security Handbook, The Practitioner's "Bible" Computer Security Institute, Massachusetts, 1987.
16.Cowan, Th.; Decision Theory in Law, Science and Technology. In: Communication Sciences and Law. Ed. L. Allen, M. Caldwell. New York.: Bobbs-Merrill 1965.
17.Danielsson, A., Törnebohm, H.; On Complex Systems with Human Components. Stockholm: Försvarets Forskningsanstalt (FOA P rap port C 8212-10).
18.Data Processing Management Association (DPMA). Data Processing Management Association Model Computer Crime Act. Park Ridge, IL: DPMA, 1987.
19._____. Data Processing Management Associaton Principles for Computer Crime. Park Ridge, IL: DPMA, 1987.
20.Dennis, F.W.; The Computer Criminal, Security world. p 26, September 1979.
21.Dopping, O.; Kort och brett om ADB, Lund, 1972.
22.Edelhartz, H.; The investigation of white collar crime, Washinton, 1977.
23.Federal Financial Institutions Examination Council (FFIEC). EDP Examination Handbook. Washington, D.C.: FFIEC, 1988.
24.Fitzgerald, K. J.; A Study in computer abuse, Caulfield, 1979.
25.Fitzgerald, K. J.; EDP losses and prevention, Caulfield Institute of Technology, Caulfield, 1980.
26.Göranzon, B.; Perspektiv paa datasystemutveckling, Lund, 1978.

27.Informatica e Dritto. Bibliografia Internazionale. Rivista trimestriale Florence: Istituto per la documentzione giuridica, Consiglio nazionale ricerche .
28.Law Enforcement Assistance Admistration, US Dept. of Justice, "Computer